Citrix ADC 13.1

Machine translated content

Disclaimer

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

Contents

Notes de mise à jour Citrix ADC

October 5, 2021

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

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

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

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

Notes de mise à jour pour Citrix ADC 13.1-4.43 Release

October 5, 2021

Ce document de notes de mise à jour décrit les améliorations et modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1 à 4.43 de Citrix ADC.

Remarques

- Ce document de notes de mise à jour n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.
- La section Problèmes résolus répertorie les correctifs après la version 13.0-82.x.

Nouveautés

Les améliorations et modifications disponibles dans la version 13.1 à 4.43.

Authentification, autorisation et audit

La traversée du domaine racine vers le domaine arborescente pour l'authentification SSO Kerberos est prise en charge

La traversée du domaine racine vers le domaine d'arborescence est désormais prise en charge pendant l'authentification SSO Kerberos pour le serveur principal à partir de l'appliance Citrix ADC. Pour de plus amples informations, consultez https://docs.citrix.com/fr-fr/citrix-adc/current-release/aaa-tm/single-sign-on-types/kerberos-single-sign-on/setup-citrix-adc-single-sign-on.html

[NSAUTH-9836]

Gestion des bots

Journalisation verbale pour la gestion des bots Citrix ADC

Si le trafic entrant est identifié comme un bot, l'appliance Citrix ADC vous permet désormais de configurer la fonctionnalité de journalisation détaillée du bot pour consigner les détails supplémentaires de l'en-tête HTTP, tels que l'adresse de domaine, l'URL, l'en-tête de l'agent utilisateur et l'en-tête de cookie. Les détails du journal sont ensuite envoyés au serveur ADM à des fins de surveillance et de dépannage. Le message de consignation verbeux n'est pas stocké dans le fichier ns.log.

Pour de plus amples informations, consultez https://docs.citrix.com/fr-fr/citrix-adc/current-release/bot-management/bot-detection.html

[NSBOT-273]

Appliance SDX Citrix ADC

Améliorations apportées à la page de formation du cluster sur une appliance Citrix ADC SDX

Les modifications suivantes sont apportées à l'interface graphique de la `Add Node to Cluster` page. Le système invite désormais l'utilisateur à ajouter une adresse SNIP tout en ajoutant un nouveau nœud à un cluster. Ces améliorations résolvent les problèmes de sécurité liés à la vérification stricte de l'adresse IP source.

- Un champ facultatif pour SNIP est désormais fourni.
- Un `Add` bouton est également fourni pour créer des SNIP dynamiquement tout en ajoutant un nœud à l'adresse IP du cluster (CLIP).

[NSSVM-4170]

Un administrateur SDX Citrix ADC peut désormais déverrouiller un utilisateur avant l'expiration de l'intervalle de verrouillage. Le verrouillage n'est pas applicable si un utilisateur se connecte au service de gestion via la console. L'intervalle de verrouillage passe également de quelques secondes à quelques minutes. Valeur minimale = 1 minute. Valeur maximale = 30 minutes.

Pour déverrouiller un utilisateur à l'aide de l'interface graphique :

1. Accédez à **Configuration > Système > Administration des utilisateurs > Utilisateurs**.
2. Sélectionnez l'utilisateur à déverrouiller.
3. Cliquez sur **Déverrouiller**.**Pour déverrouiller un utilisateur à l'aide de l'interface de ligne de commande :**

À l'invite de commandes, tapez :

```
set systemuser id=<ID> unlock=true
<!--NeedCopy-->
```

[NSSVM-4144]

Citrix Gateway

Nouvelles langues prises en charge

Le portail utilisateur Citrix Gateway est désormais disponible en russe, en coréen et en chinois (traditionnel).

[CGOP-17095]

Prise en charge de l'authentification OAuth-OpenID Connect pour Gateway Insight

Citrix Gateway Insight signale désormais les événements liés à l'authentification OAuth-OpenID Connect (ouvertures de session utilisateur réussies et échecs).

[CGOP-16907]

Citrix Web App Firewall

Extraction d'adresses IP du client à l'aide d'une expression de stratégie avancée

L'appliance Citrix ADC utilise une expression de stratégie avancée pour extraire l'adresse IP du client à partir d'un en-tête de demande HTTP, d'un corps de requête et d'une URL de demande. La valeur extraite est ensuite envoyée au serveur ADM pour la journalisation d'audit, les informations de sécurité et le calcul de la géolocalisation du client.

Pour de plus amples informations, consultez https://docs.citrix.com/fr-fr/citrix-adc/current-release/bot-management/bot-detection.html

[NSWAF-7260]

Option d'activation pour le mécanisme de détection de BOT TPS

L'option Activer est désormais disponible pour chaque règle de détection de bot TPS dans la configuration du profil de bot. Par défaut, la valeur est ON. ;

Pour plus d'informations, consultez [https://docs.citrix.com/fr-fr/citrix-adc/current-release/bot-management/bot-detection.html] ;
[NSHELP-25777]

Équilibrage de charge

Prise en charge de la redirection HTTP vers HTTPS sur les serveurs virtuels de commutation de contenu

Les serveurs virtuels de commutation de contenu du type de service SSL prennent désormais en charge la redirection du trafic HTTP. Deux nouveaux paramètres : `HttpsRedirectUrl` et `RedirectFromPort` sont ajoutés à la `add cs vserver` commande. Tout le trafic HTTP arrivant sur le port spécifié dans le `RedirectFromPort` paramètre est redirigé vers l'URL spécifiée dans le `HttpsRedirectUrl` paramètre. S'il n' `HttpsRedirectUrl` est pas configuré, le trafic HTTP est redirigé vers la valeur de l'en-tête de l'hôte dans la requête HTTP entrante.

Pour de plus amples informations, consultez https://docs.citrix.com/fr-fr/citrix-adc/current-release/ssl/how-to-articles/ssl-config-https-vserver-to-accept-http-traffic.html

[NSLB-8224]

Prise en charge de la synchronisation de la commande save config sur les sites GSLB distants

Vous pouvez maintenant synchroniser la `save ns config` commande sur des sites GSLB distants. Pour activer cette fonctionnalité, un nouveau paramètre `GSLBSyncSaveConfigCommand` est ajouté à la `set gslb parameter` commande. Après avoir activé l'option `GSLBSyncSaveConfigCommand`, la `save ns config` commande est traitée comme une autre commande GSLB et est synchronisée avec les sites GSLB distants. Vous devez activer l' `AutomaticConfigSync` option de synchronisation de la `save ns config` commande.

Pour de plus amples informations, consultez https://docs.citrix.com/fr-fr/citrix-adc/current-release/global-server-load-balancing/synchronizing-configuration-in-gslb-setup/real-time-synchronization.html

[NSLB-7831]

Prise en charge des arguments de script sécurisés pour les moniteurs utilisateur

Un nouveau paramètre, `-secureargs`, est ajouté à la `add lb monitor` commande. Ce paramètre stocke les arguments du script dans un format chiffré au lieu d'un format de texte brut. Vous pouvez

sécuriser les données sensibles liées aux scripts du moniteur utilisateur à l'aide de ce paramètre, par exemple, le nom d'utilisateur et le mot de passe. Citrix vous recommande d'utiliser un `-secureargs` paramètre au lieu du `-scriptargs` paramètre pour toutes les données sensibles liées aux scripts. Si vous choisissez d'utiliser les deux paramètres ensemble, le script spécifié dans -scriptname doit accepter les arguments dans l'ordre : `<scriptargs> <secureargs>`. En d'autres termes, vous devez spécifier les premiers paramètres dans `<scriptargs>` et le reste des paramètres dans en `<secureargs>` conservant l'ordre défini pour les arguments. Les arguments sécurisés ne s'appliquent qu'au répartiteur interne.

Pour de plus amples informations, consultez https://docs.citrix.com/fr-fr/citrix-adc/current-release/load-balancing/load-balancing-custom-monitors/configure-user-monitor.html

[NSLB-6314]

Mise en réseau

Prise en charge des jeux de données de type numérique pour les ACL étendues

L'appliance Citrix ADC prend désormais en charge le jeu de données de type de numéro pour les listes de contrôle d'accès étendues. Vous pouvez utiliser le jeu de données de type de numéro pour spécifier le port source ou le port de destination ou les deux pour une règle ACL étendue.

[NSNET-20235]

Prise en charge de RHI pour une adresse VIP liée à un IPset

Une appliance Citrix ADC annonce une adresse VIP liée à un IPset en tant qu'itinéraire du noyau si toutes les conditions suivantes sont remplies :

- L' `host route` option est activée pour l'adresse VIP.
- L'IPSet est lié à une configuration, par exemple, des serveurs virtuels d'équilibrage de charge multi-IP.

[NSNET-20209]

Prise en charge de l'enregistrement Citrix ADC CPX avec ADM à l'aide de montages de volume

Citrix ADC CPX prend désormais en charge l'enregistrement auprès de Citrix ADM en utilisant des montages de volume via Kubernetes ConfigMaps et Secret. Citrix ADC CPX lance l'enregistrement auprès de l'agent ADM avec les détails de configuration dérivés des montages de volume situés dans le système de fichiers de Citrix ADC CPX.

[NSNET-19058]

Plateforme

Prise en charge de VMware ESX 7.0 update 2a sur l'instance Citrix ADC VPX

L'instance Citrix ADC VPX prend désormais en charge la mise à jour 2a de VMware ESX version 7.0 (Build 17867351).

Pour de plus amples informations, consultez https://docs.citrix.com/fr-fr/citrix-adc/current-release/deploying-vpx/supported-hypervisors-features-limitations.html

[NSPLAT-20104]

Prise en charge du processeur AMD pour l'instance Citrix ADC VPX sur ESXi

L'instance Citrix ADC VPX sur l'hyperviseur VMware ESXi prend désormais en charge les processeurs AMD. Pour de plus amples informations, consultez https://docs.citrix.com/fr-fr/citrix-adc/current-release/deploying-vpx/install-vpx-on-xenserver.html

[NSPLAT-17853]

Prise en charge de l'abonnement Citrix ADC VPX 5000 sur Azure Marketplace

Le plan d'abonnement Citrix ADC VPX 5000 est désormais pris en charge sur Azure Marketplace. Ce plan basé sur un abonnement offre les licences suivantes :

- Standard
- Advanced
- Premium

Pour de plus amples informations, consultez https://docs.citrix.com/fr-fr/citrix-adc/current-release/deploying-vpx/deploy-vpx-on-azure.html#citrix-adc-vpx-licensing

[NSPLAT-13663]

Stratégies

Prise en charge des champs d'en-tête IP dans l'expression de stratégie avancée

L'expression de stratégie avancée vous permet désormais de récupérer les champs d'en-tête suivants à partir d'un paquet IP.

- DSCP
- ECN
- TTL
- Version
- Identification

- Longueur de la tête
- Checksum d'en-tête
- Options
- Charge utile

[NSPOLICY-2441]

Suppression des fonctionnalités obsolètes à partir de Citrix ADC version 13.1

De nombreuses fonctionnalités obsolètes sont désormais supprimées et ne sont plus configurables sur une appliance Citrix ADC.

Ces informations incluent :

- La fonction de filtrage (également connue sous le nom de filtrage de contenu ou CF) : actions, stratégies et liaison.
- Les fonctionnalités SPDY, Sure Connect (SC), Priority Queuing (PQ), HTTP Denial of Service (DoS) et HTML Injection.
- Stratégies classiques pour SSL, la commutation de contenu, la redirection du cache, la compression et le pare-feu d'application.
- Les `domain` paramètres `url` et dans les stratégies de commutation de contenu.
- Expressions classiques dans les règles de persistance de l'équilibrage de charge.
- Le `pattern` paramètre dans les actions de réécriture.
- Le `bypassSafetyCheck` paramètre dans les actions de réécriture.
- `SYS.EVAL\\_CLASSIC\\_EXPR` dans les expressions avancées.
- L'entité `patclass` de configuration.
- La valeur `HTTP.REQ.BODY` sans argument dans les expressions avancées.
- Préfixes Q et S dans les expressions avancées.
- Le `policyType` paramètre du paramètre cmp. (commande CLI `set cmp parameter`.)

Comme déjà documenté, vous pouvez utiliser l' `nspepi` outil pour la conversion. Vous devez exécuter l'outil sur une appliance Citrix ADC version 13.0 ou 12.1.

Pour de plus amples informations, consultez https://docs.citrix.com/fr-fr/citrix-adc/current-release/appexpert/policies-and-expressions/introduction-to-policies-and-exp/classic-policy-deprecation-faq.html

De plus, pour utiliser la dernière version des outils afin de migrer de la configuration classique vers la configuration avancée, et des domaines de trafic vers les partitions d'administration, consultez https://github.com/citrix/ADC-scripts

[NSPOLICY-186]

Système

Afficher les statistiques du pont QUIC

La `stat` commande de pont QUIC fournit désormais un résumé détaillé des statistiques de pont QUIC.

[NSBASE-13883]

Suppression des fonctionnalités obsolètes dans Citrix ADC 13.1 et suivantes

Les fonctionnalités obsolètes suivantes et leurs configurations ne sont plus prises en charge et sont supprimées de l'appliance Citrix ADC :

- SureConnect (SC)
- Queueing prioritaire (PQ)
- Protection DoS HTTP (HDOSP)
- `HTMLInjection`

Comme alternative, Citrix vous recommande d'utiliser AppQoE pour SureConnect, Priority Queueing et HTTP DoS Protection et d'utiliser des mesures côté client pour `HTMLInjection`.

Pour de plus amples informations, consultez https://docs.citrix.com/fr-fr/citrix-adc/current-release/appexpert/policies-and-expressions/introduction-to-policies-and-exp/classic-policy-deprecation-faq.html

[NSBASE-13780]

Interface utilisateur

Prise en charge de l'API par lots pour les appels NITRO

L'appliance Citrix ADC prend désormais en charge l' `batchapi` API. L' `batchapi` API peut gérer plusieurs appels NITRO en une seule demande et ainsi minimiser le trafic réseau. Vous pouvez effectuer les opérations suivantes à l'aide de la commande `batchapi` :

- Vous pouvez utiliser l'API par lots pour créer, mettre à jour et supprimer simultanément plusieurs ressources hétérogènes.
- Vous pouvez utiliser l'API par lots pour obtenir plusieurs ressources hétérogènes.

[NSCONFIG-4061]

Problèmes résolus

Les problèmes résolus dans la version 13.1—4.43.

Authentification, autorisation et audit

Lorsque vous liez un moniteur LDAP à un service, le moniteur tombe en panne car l'appliance Citrix ADC envoie un mot de passe incorrect à Active Directory.

[NSHELP-27961]

Dans un AD à cascade multiple, le compte d'un utilisateur n'est pas verrouillé si un utilisateur n'est pas trouvé dans la dernière cascade.

[NSHELP-27948]

Lorsqu'une appliance Citrix ADC est configurée pour l'authentification SAML, la solution matérielle-logicielle vide le cœur à l'aide d'un certificat autre que RSA.

[NSHELP-27813]

Dans certains cas, une appliance Citrix ADC peut se bloquer lors du traitement de la demande d'authentification de certains utilisateurs lorsque l'accès basé sur les rôles est configuré.

[NSHELP-27655]

Les utilisateurs ne peuvent pas se connecter via l'application Citrix Workspace si Azure AD est configuré en tant que fournisseur d'identité OAuth sur le serveur virtuel d'authentification Citrix ADC.

[NSHELP-27462]

Dans certains cas, l'authentification SAML échoue avec l'application Workspace si l'on accède à l'application via StoreFront.

[NSHELP-27338]

Dans certains cas, une requête HTTP POST envoyée à un serveur virtuel Authentication, Authorization and Auditing-TM n'est pas traitée correctement si la demande ne contient pas de cookie d'authentification. Le corps POST est perdu pendant le traitement.

[NSHELP-27227]

L'appliance Citrix ADC se bloque fréquemment lors du traitement du trafic Authentication, Authorization, and Auditing-TM et 401 LB.

[NSHELP-27094]

Dans certains cas, une appliance Citrix ADC se bloque lors de l'authentification des utilisateurs pour Citrix Gateway et de l'authentification, de l'autorisation et de l'audit - déploiement géré du trafic.

[NSHELP-26555]

En cas de saisie d'un OTP incorrect, un message d'erreur `Email Auth failed. No further action to continue` s'affiche.

[NSHELP-26400]

Dans certains scénarios, la commande de groupe d'authentification, d'autorisation et d'audit de liaison peut échouer si le nom de la stratégie est plus long que le nom de l'application intranet.

[NSHELP-25971]

Une appliance Citrix ADC configurée en tant que fournisseur d'identité (IdP) SAML tronque l'état du relais à partir du fournisseur de services (SP) s'il contient des guillemets.
[NSHELP-20131]

La vérification du test de connectivité réseau échoue en raison d'un problème de déchiffrement du mot de passe. Toutefois, la fonctionnalité d'authentification fonctionne correctement.

[NSAUTH-10216]

Gestion des bots

Dans le mécanisme de détection de robot Transaction Per Second (TPS), le serveur d'applications principal renvoie une réponse 304 lors de la récupération de réponse après le défi CAPTCHA.

[NSBOT-626]

Mise en cache

Dans une configuration haute disponibilité, la synchronisation HA échoue pour le paramètre de cache `memLimit` lors d'un basculement HA.

[NSHELP-28428]

Dans une configuration haute disponibilité, le nœud principal se bloque après avoir accédé à un pointeur NULL au lieu d'un objet mis en cache.

[NSHELP-26967]

Appliance SDX Citrix ADC

Sur une appliance Citrix ADC SDX, la restauration d'instance peut échouer si l'instance a été créée avec la version logicielle 13.0-76.x ou antérieure.

[NSHELP-28429]

Dans une appliance Citrix ADC SDX, le service de gestion signale une utilisation incorrecte des données des instances ADC.

[NSHELP-28208]

Sur une appliance Citrix ADC SDX, vous ne pouvez pas modifier l'invite de l'interface de ligne de commande dans la console du service de gestion.

[NSHELP-28030]

Sur une appliance Citrix ADC SDX, le service de gestion peut signaler une utilisation élevée de la mémoire d'environ 80 % en raison de l'augmentation des tâches et des planificateurs exécutés dans l'inventaire.

[NSHELP-27805]

Sur une appliance Citrix ADC SDX, la mise à niveau peut échouer si les fichiers système (snmpd.conf et ntp.conf) contiennent des caractères de retour chariot.

[NSHELP-27713]

Sur une appliance Citrix ADC SDX, le service de gestion peut signaler une utilisation élevée de la mémoire d'environ 80 % en raison de l'augmentation des tâches et des planificateurs exécutés dans l'inventaire.

[NSHELP-27396]

Citrix Gateway

Un message d'erreur apparaît lorsque vous tentez de modifier les attributs CSS d'un thème personnalisé.

[NSHELP-28648]

L'ouverture de session à Citrix Workspace échoue si les stratégies de répondeur qui peuvent passer à un état bloqué pendant l'évaluation sont liées au serveur virtuel.

[NSHELP-27819]

Lorsque vous accédez à l'appliance Citrix Gateway à l'aide du VPN sans client, un vidage de mémoire peut être généré.

[NSHELP-27653]

L'appliance Citrix Gateway peut se bloquer lors du traitement du trafic UDP initié par le serveur.

[NSHELP-27611]

Les utilisateurs peuvent voir les boîtes aux lettres des autres utilisateurs lorsqu'ils se connectent à Microsoft Outlook. Pour contourner ce problème, désactivez le multiplexage.

[NSHELP-27538]

Une appliance Citrix ADC peut se bloquer si les commandes liées à EDT, telles que `clearconfigkill ica connection`, ou `stop dtls listener` sont traitées par l'appliance.

[NSHELP-27398]

L'appliance Citrix Gateway peut tomber en panne pendant le traitement du trafic UDP.

[NSHELP-27317]

Le dispositif Citrix Gateway se bloque lorsqu'une stratégie Syslog est liée à un serveur virtuel et que l'action Syslog correspondante est modifiée.

[NSHELP-27171]

Les journaux Citrix ADC peuvent être inondés du message de journal `GwInsight: Func=ns\\_sslvpn\\_send\\_app\\_launch\\_fail\\_record Appflow policy evaluation has failed` lorsque Gateway Insight est activé.

[NSHELP-26750]

Le dispositif Citrix Gateway se bloque lorsque vous essayez d'effacer la configuration si les deux conditions suivantes sont remplies :

- Un profil SSL et une paire de clés de certificat sont liés au moniteur TCP par défaut.
- Le même moniteur TCP par défaut est lié à une action Syslog.

[NSHELP-26685]

Lorsque vous entrez le nom de domaine complet en tant que proxy dans la page Créer un profil de trafic Citrix Gateway, le message `Invalid Proxy Value` apparaît.

[NSHELP-26613]

Lors de la création d'un profil client RDP à l'aide de l'interface graphique Citrix ADC, un message d'erreur apparaît lorsque les conditions suivantes sont remplies :

- Une clé pré-partagée (PSK) par défaut est configurée.
- Vous essayez de modifier le minuteur de validité du cookie RDP dans le champ Validité du cookie RDP (secondes).

[NSHELP-25694]

L'OID SNMP envoie un ensemble incorrect de connexions actuelles au serveur virtuel VPN.

[NSHELP-25596]

Si vous renommez un serveur virtuel VPN lié à un serveur STA, l'état du serveur STA apparaît en panne lorsque vous exécutez la commande show.

[NSHELP-24714]

Dans de rares cas, l'appliance Citrix Gateway peut se bloquer si l'adresse IP intranet (IIP) est activée et qu'il existe des connexions initiées par le serveur à l'adresse IIP.

[NSHELP-23819]

La sortie de la `show tunnel global` commande inclut des noms de stratégie avancés. Auparavant, la sortie n'affichait pas les noms de stratégie avancés.

Exemple :

Nouvelle sortie :

> Nom de la
> stratégie globale de show tunnel : ns_tunnel_nocmp Priorité : 0

Nom de la stratégie : ns_adv_tunnel_nocmp Type : Stratégie avancée
Priorité : 1 Point de liaison
global : REQ_DEFAULT

Nom de la stratégie : ns_adv_tunnel_msdocs Type : Stratégie avancée
Priorité : 100 Point de liaison
global : RES_DEFAULT
Terminé

Sortie précédente :

> Nom de la
> stratégie globale de show tunnel : ns_tunnel_nocmp Priorité : 0 Désactivé

Stratégies avancées :

Point de liaison global : REQ_DEFAULT
Nombre de stratégies liées : 1

Terminé

[NSHELP-23496]

Si vous avez configuré la gestion des comptes RADIUS pour l'événement de démarrage/arrêt ICA, l'ID de session dans la demande de gestion de compte RADIUS pour le démarrage ICA est affiché sous la forme de zéro.

[NSHELP-22576]

Citrix Web App Firewall

Dans une configuration de cluster Citrix ADC, l'un des nœuds se bloque si un ou plusieurs nœuds sont mis à niveau à partir de Citrix ADC version 12.0, 12.1 ou 13.0 build 52.x ou antérieure. Le blocage se produit en raison d'une incompatibilité du format et de la taille des cookie du Web App Firewall.

[NSWAF-7689]

Dans Web App Firewall, le `Cookie-transformation` paramètre fractionne les valeurs du cookie côté réponse s'il a une virgule comme délimiteur.

[NSHELP-28411]

Une appliance Citrix ADC peut tomber en panne si des violations d'injection de commande sont observées dans un ordre spécifique et si les conditions suivantes sont remplies :

- Plusieurs cookies sont présents dans la demande
- `URLDecodeRequestCookies` la fonctionnalité est désactivée

[NSHELP-28365]

Une appliance Citrix ADC peut afficher une utilisation élevée de la mémoire lors de l'analyse des réponses HTTP avec l'attribut Samesite et la fonctionnalité de pare-feu d'application Web activés.

[NSHELP-27722]

La fonctionnalité de piratage de cookie ne prend pas en charge le navigateur Internet Explorer car les navigateurs Internet Explorer ne réutilisent pas les connexions SSL. En raison de cette limitation, plusieurs redirections sont envoyées pour une demande entraînant éventuellement une `MAX REDIRECTS EXCEEDED` erreur dans le navigateur Internet Explorer.

[NSHELP-27193]

Après une mise à niveau vers Citrix ADC version 13.0 build 76.29 et avec la fonctionnalité de téléchargement de fichiers activée sur l'appliance, le problème suivant est observé :

- Les contrôles de protection par script SQL et intersite bloquent le processus de téléchargement de fichiers pour toutes les applications Web.

[NSHELP-27140]

Équilibrage de charge

Dans une configuration GSLB, les états des services distants ne sont pas mis à jour une fois les statistiques effacées sur le site GSLB. Pour contourner le problème, effacez à nouveau les statistiques sur le même site GSLB. Les états des services distants sont ensuite mis à jour.

[NSHELP-28169]

Dans une configuration haute disponibilité, le nœud secondaire peut se bloquer si les conditions suivantes sont remplies :

- La quantité de mémoire physique sur les deux nœuds est différente l'une de l'autre.
- Les sessions de données ne sont pas correctement synchronisées.

[NSHELP-26503]

Dans une configuration de cluster, l'adresse IP du service GSLB n'est pas affichée dans l'interface graphique lorsqu'on y accède via des liaisons de serveur virtuel GSLB. Il ne s'agit que d'un problème d'affichage et il n'y a aucun impact sur la fonctionnalité.

[NSHELP-20406]

Divers

Une appliance Citrix ADC ajoute des informations L2 supplémentaires lorsqu'un tunnel ou des serveurs virtuels de type de service (TOS) sont créés.

[NSHELP-27825]

Mise en réseau

Après la mise à niveau d'une appliance Citrix ADC BLX (version 13.0 build 82.x) exécutée sur un hôte Linux basé sur Debian, SSH ne fonctionne pas comme prévu en mode partagé.

[NSNET-23020]

Après la mise à niveau d'une appliance Citrix ADC BLX vers la version 13.1 build 4.x, le pare-feu d'application Web peut bloquer de manière incorrecte une demande sans en-tête de type de contenu.

[NSNET-21415]

Dans un dispositif Citrix ADC BLX, le NSVLAN lié aux `non-dpdk` interfaces balisées peut ne pas fonctionner comme prévu. NSVLAN lié avec des `non-dpdk` interfaces non balisées fonctionne correctement.

[NSNET-18586]

Dans une appliance Citrix ADC, la couche de pilote interne peut utiliser un tampon de données incorrect entraînant une corruption des données, ce qui entraîne le blocage de l'appliance.

[NSHELP-27858]

Problème résolu :

Citrix ADC CPX déployé en tant que sidecar et connecté à plusieurs réseaux n'a pas pu choisir l'adresse IP source correcte pour le sous-réseau de destination.

[NSHELP-27810]

Dans une configuration haute disponibilité, la synchronisation HA peut échouer pour les configurations de profil WAF et de fichier d'emplacement.

[NSHELP-27546]

Les boucles de paquets sont observées dans une configuration d'équilibrage de charge si toutes les conditions suivantes sont remplies :

- Le serveur virtuel est configuré pour écouter sur le port 80 et le paramètre de basculement de connexion (`connfailover`) est défini sur stateless.
- Le serveur virtuel reçoit deux paquets de demandes qui ont :
  - Port source = 80
  - Port de destination = numéro autre que 80

- Adresse IP de destination = adresse IP (VIP) du serveur virtuel

[NSHELP-22431]

Plateforme

`Failed to create target instance` un message d'erreur s'affiche sur la console GCP même si vous ne créez aucune instance cible. Ce problème se produit lorsque vous ne disposez pas de l'autorisation `compute.targetInstances.get` IAM dans votre compte de service GCP. À partir de cette version, Citrix ADC VPX crée des instances cibles uniquement pour les machines virtuelles qui utilisent la fonctionnalité VIP Scaling.

[NSPLAT-20952]

L'appliance Citrix ADC génère des alertes de limite de débit de faux paquets par seconde (PPS) avant même que l'appliance Citrix ADC n'atteigne sa limite PPS pour la licence.

[NSHELP-26935]

Stratégies

La variable NS avec une portée globale ne fonctionne pas pour le trafic HTTP/2.

[NSHELP-27095]

SSL

Dans une configuration de cluster, lorsque deux certificats installés sont les émetteurs d'un certificat de serveur doté de l'extension OCSP AIA, la solution matérielle-logicielle devient inaccessible si vous supprimez le certificat de serveur.

[NSHELP-28058]

Dans une configuration haute disponibilité, l'actualisation automatique des LCR échoue par intermittence si les deux conditions suivantes sont remplies :

- Les fichiers sont synchronisés entre le nœud principal et le nœud secondaire.
- Le fichier CRL est en cours de téléchargement à partir du serveur CRL en même temps.

[NSHELP-27435]

Sur une appliance Citrix ADC, une notification d'expiration de faux certificat est consignée le lendemain lorsqu'une paire de clés de certificat est ajoutée avec -ExpiryMonitor activé.

[NSHELP-27348]

Dans une base de données de cluster, la liaison n'est pas mise à jour correctement si vous liez une stratégie SSL à un serveur virtuel au point de liaison Hello du client plusieurs fois et avec des priorités

différentes. Par conséquent, une erreur apparaît lorsque vous supprimez la stratégie, même après la dissolution de la liaison du serveur virtuel.

[NSHELP-27301]

L'appliance Citrix ADC se bloque lors du redémarrage si vous modifiez le nom du certificat intégré (`ns-server-certificate`) dans le fichier de configuration.

[NSHELP-26858]

Dans une configuration de cluster, vous pouvez rencontrer les problèmes suivants :

- Commande manquante pour la liaison de la paire de clés de certificat par défaut aux services internes SSL sur le CLIP. Toutefois, si vous effectuez une mise à niveau à partir d'une version antérieure, vous devrez peut-être lier la paire de clés de certificat par défaut aux services internes SSL concernés sur le CLIP.
- Différence de configuration entre le CLIP et les nœuds de la commande set par défaut pour les services internes.
- Commande de liaison de chiffrement par défaut manquante aux entités SSL dans la sortie de la commande show running config exécutée sur un nœud. L'omission n'est qu'un problème d'affichage et n'a aucun impact fonctionnel. La liaison peut être visualisée à l'aide de la `show ssl <entity> <name>` commande.

[NSHELP-25764]

Système

Une appliance Citrix ADC peut tomber en panne avec une réponse ICAP OPTIONS. Le problème se produit lorsque la valeur d'en-tête autorisée contient une valeur autre que 204.

[NSHELP-27879]

Dans AppFlow, le nombre d'octets de couche 4 pour les enregistrements de flux ne correspond pas aux transactions du serveur virtuel HTTP. La valeur de comptage est inférieure à la valeur du nombre d'octets du serveur virtuel de couche 7.

[NSHELP-27495]

Le compteur TCPCurClientConn affiche une valeur élevée si l'appliance Citrix ADC est enregistrée sur Citrix ADM.

[NSHELP-27463]

Une appliance Citrix ADC peut se bloquer lorsque la fonctionnalité AppFlow est désactivée et réactivée.

[NSHELP-27236]

Dans de rares cas, une appliance Citrix ADC peut envoyer des numéros de séquence TCP SACK incorrects au client lors du transfert depuis le serveur principal. Le problème se produit si l'option TCP Selective ACK (SACK) est activée dans un profil TCP.

[NSHELP-24875]

Un dispositif Citrix ADC peut se bloquer lorsqu'une stratégie avec l' `HTTP.REQ.*` expression est liée au point de liaison RESPONSE du serveur virtuel HTTP_QUIC. Le problème ne se produit pas si vous liez la même stratégie à un serveur virtuel de type HTTP ou SSL avec le serveur virtuel HTTP_QUIC.

[NSBASE-14612]

Interface utilisateur

Dans l'interface graphique du Gestionnaire de stratégies de compression, impossible de lier une stratégie de compression à un protocole HTTP en spécifiant un point de liaison et un type de connexion appropriés.

[NSUI-17682]

Lorsque vous récupérez le contenu d'un fichier à partir d'une instance ADC à l'aide de la commande `show systemfile`, un message d'erreur d'échec de téléchargement apparaît sur la console ADC. Le problème se produit si le contenu du fichier commence par des octets NULL.

[NSHELP-28227]

Le flot `admautoregd` SYSLOG entraîne une mauvaise classification et un mauvais diagnostic de la définition des ressources client
(CRD) en raison d'un problème système interne (fichier binaire Python manquant).

Correction : pour arrêter de surveiller le `admautoregd` processus après 30 minutes si le binaire python est toujours manquant.

[NSHELP-28185]

Il peut y avoir une perte de configuration si une instance VPX sur AWS, configurée avec KEK, est mise à niveau vers Citrix ADC version 13.0 build 76.x ou ultérieure. Toutes les données sensibles chiffrées à l'aide de KEK échouent si la configuration est chargée après un redémarrage.

[NSHELP-28010]

Une barre oblique inverse supplémentaire est incorrectement introduite si des caractères spéciaux sont utilisés dans les arguments de certaines commandes SSL, telles que `create ssl rsakey` et `create ssl cert`.

[NSHELP-27378]

Dans une configuration haute disponibilité, la synchronisation HA ou la propagation HA peut échouer si l'une des conditions suivantes est remplie :

- Le mot de passe du nœud RPC comporte des caractères spéciaux.
- Le mot de passe du nœud RPC comporte 127 caractères (nombre maximal de caractères autorisés).

[NSHELP-27375]

L' `nsconfigaudit` outil peut se bloquer si la taille du fichier de configuration d'entrée est très importante.

[NSHELP-27263]

Vous ne pouvez pas lier un service ou un groupe de services à un serveur virtuel d'équilibrage de charge prioritaire à l'aide de l'interface graphique Citrix ADC.

[NSHELP-27252]

La fonctionnalité de création de rapports peut cesser de fonctionner si l'horloge système est mise à jour sur un dispositif Citrix ADC.

[NSHELP-25435]

Dans un dispositif Citrix ADC VPX, une opération de définition de la capacité peut échouer après l'ajout d'un serveur de licences. Le problème se produit car les composants liés à Flexera prennent plus de temps à initialiser en raison du grand nombre de licences prises en charge de type « check-in and check-out » (CICO).

[NSHELP-23310]

L'appel GET de l'API `botprofile\\_logexpression\\_binding` NITRO ne renvoie aucune réponse si l'expression de journal est liée à un profil de bot.

[NSCONFIG-5490]

Dans une configuration de cluster, lorsque vous liez un profil de Web App Firewall avec les règles affinées, puis avec des `non-fine-graned` règles à la même URL, les règles affinées sont supprimées de la base de données. Par conséquent, seules les règles non affinées sont affichées sur l'adresse IP du cluster.

[NSCONFIG-5389]

Problèmes connus

Les problèmes qui existent dans la version 13.1 à 4.43.

AppFlow

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

[NSINSIGHT-943]

Authentification, autorisation et audit

Une appliance Citrix ADC n'authentifie pas les tentatives de connexion par mot de passe en double et empêche le verrouillage des comptes.

[NSHELP-563]

Le schéma LoginSchema DualAuthPushOrOTP.xml n'apparaît pas correctement dans l'écran de l'éditeur de schéma de connexion de l'interface graphique Citrix ADC.

[NSAUTH-6106]

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

Solution :

Connectez-vous au Citrix ADC actif principal dans le cluster et exécutez la `show adfsproxyprofile <profile name>` commande. Il afficherait l'état du profil proxy.

[NSAUTH-5916]

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

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

Solution :

Fermez et ouvrez l'option Tester l'accessibilité LDAP.

[NSAUTH-2147]

Mise en cache

Une appliance Citrix ADC peut tomber en panne si la fonctionnalité de mise en cache intégrée est activée et que la mémoire de l'appliance est insuffisante.

[NSHELP-22942]

Appliance SDX Citrix ADC

Sur une appliance Citrix ADC SDX, la création d'une instance ADC à l'aide de l'image XVA de la version logicielle 12.0 échoue. Par conséquent, l'instance est inaccessible.

[NSHELP-28408]

Sur une appliance Citrix ADC SDX, les instances ADC n'atteindront pas leur capacité maximale lorsque vous configurez le mode d'allocation de débit en rafale.

[NSHELP-27477]

Les pertes de paquets sont observées sur une instance VPX hébergée sur un dispositif Citrix ADC SDX si les conditions suivantes sont remplies :

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

[NSHELP-21992]

Citrix Gateway

Le plug-in EPA pour Windows n'utilise pas le proxy configuré de la machine locale et se connecte directement au serveur de passerelle.

[NSHELP-24848]

Gateway Insight n'affiche pas d'informations précises sur les utilisateurs du VPN.

[NSHELP-23937]

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

- L'appliance Citrix Gateway est configurée pour la fonctionnalité Always On
- La solution matérielle-logicielle est configurée pour l'authentification par certificat avec une authentification à deux facteurs. `off`

[NSHELP-23584]

Parfois, lorsque vous parcourez les schémas, le message d'erreur `Cannot read property 'type 'of undefined` s'affiche.

[NSHELP-21897]

La configuration du serveur virtuel SOCKS Proxy CR pour un dispositif Citrix Gateway échoue si vous utilisez un nom de domaine complet (FQDN) pour Virtual Delivery Agent (VDA).
Solution : utilisez une adresse IP pour le VDA.

[NSHELP-8549]

L'échec du lancement de l'application dû à un ticket STA non valide n'est pas signalé dans Gateway Insight.

[CGOP-13621]

Le rapport Gateway Insight affiche incorrectement la valeur `Local` au lieu de la valeur `SAML` dans le champ Type d'authentification pour les échecs d'erreur SAML.

[CGOP-13584]

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

[CGOP-13511]

Tout en acceptant les connexions hôtes locales à partir du navigateur, la boîte de dialogue Accepter la connexion pour macOS affiche le contenu en anglais, quelle que soit la langue sélectionnée.

[CGOP-13050]

Le texte `Home Page` de l'application Citrix SSO > Page d'accueil est tronqué pour certaines langues.

[CGOP-13049]

Un message d'erreur apparaît lorsque vous ajoutez ou modifiez une stratégie de session à partir de l'interface graphique Citrix ADC.

[CGOP-11830]

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

[CGOP-7269]

Dans un déploiement de cluster, si vous exécutez `force cluster sync` la commande sur un nœud non CCO, le fichier ns.log contient des entrées de journal en double.

[CGOP-6794]

Équilibrage de charge

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

[NSLB-7679]

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

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

[NSHELP-28080]

La génération des alarmes SNMP peut être retardée si la synchronisation de la configuration du site principal vers les sites subordonnés échoue.

[NSHELP-23391]

Divers

Lorsqu'une synchronisation forcée a lieu dans une configuration haute disponibilité, la solution matérielle-logicielle exécute la `set urlfiltering parameter` commande sur le nœud secondaire.

Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le `TimeOfDayToUpdateDB` paramètre.

[NSSWG-849]

Une appliance Citrix ADC peut redémarrer en raison de la stagnation du processeur de gestion si le problème de connectivité se produit avec le fournisseur tiers de filtrage d'URL.

[NSHELP-22409]

Mise en réseau

Une appliance Citrix ADC BLX en mode DPDK peut se bloquer si un profil de pare-feu d'application Web est configuré avec des contrôles de protection de sécurité avancés.

Solution :

Supprimez la configuration de protection de sécurité avancée pour WAF.

[NSNET-22654]

Après une mise à niveau de l'appliance Citrix ADC BLX 13.0 61.x vers la version 13.0 64.x, les paramètres du fichier de configuration BLX sont perdus. Le fichier de configuration BLX est ensuite réinitialisé par défaut.

[NSNET-17625]

Les opérations d'interface suivantes ne sont pas prises en charge dans une appliance Citrix ADC BLX :

- Désactiver
- Activer
- Reset

[NSNET-16559]

Sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure), une appliance Citrix ADC BLX est toujours déployée en mode partagé, quels que soient les paramètres du fichier de configuration BLX (`/etc/blx/blx.conf`). Ce problème se produit car `mawk`, qui est présent par défaut sur les systèmes Linux basés sur Debian, n'exécute pas certaines des commandes `awk` présentes dans le fichier `blx.conf`.

Solution :

Installez `gawk` avant d'installer une appliance Citrix ADC BLX. Vous pouvez exécuter la commande suivante dans l'interface de ligne de commande de l'hôte Linux pour effectuer l'installation `gawk` :

- apt-get install gawk

[NSNET-14603]

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

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

Solution :

Exécutez les commandes suivantes dans l'interface de ligne de commande de l'hôte Linux avant d'installer une appliance Citrix ADC BLX :

```
1 -  dpkg --add-architecture i386
2 -  apt-get update
3 -  apt-get dist-upgrade
4 -  apt-get install libc6:i386
5 <!--NeedCopy-->
```

[NSNET-14602]

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

[NSNET-5233]

Dans un déploiement NAT à grande échelle de deux appliances Citrix ADC dans une configuration haute disponibilité, IPsec ALG peut ne pas fonctionner correctement si la configuration haute disponibilité comporte `stayprimary` ou défini des `staysecondary` options.

[NSNET-1646]

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

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

Solution :

Effectuez le basculement HA manuel successif uniquement après la fin de la synchronisation HA (les deux nœuds sont en état de réussite de la synchronisation).

[NSHELP-25598]

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

[NSHELP-21082]

Dans une configuration haute disponibilité (HA), si l'ARP gratuit (GARP) est désactivé, le routeur amont risque de ne pas diriger le trafic vers le nouveau serveur principal après un basculement HA.

[NSHELP-20796]

Plateforme

Lorsque vous effectuez une mise à niveau de versions 13.0/12.1/11.1 vers une version 13.1 ou que vous passez d'une version 13.1 à une version 13.0/12.1/11.1, certains packages python ne sont pas installés sur les appliances Citrix ADC. Ce problème est résolu pour les versions Citrix ADC suivantes :

- 13.1-4.x
- 13.0—82.31 et versions ultérieures
- 12.1—62.21 et versions ultérieures

Les packages python ne sont pas installés lorsque vous rétrogradez les versions de Citrix ADC de 13.1-4.x vers l'une des versions suivantes :

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

[NSPLAT-21691]

Le provisionnement d'une instance VPX avec la version 12.0 XVA échoue sur un dispositif Citrix ADC SDX exécutant la version 13.1.

Seules les versions 12.1 et ultérieures de VPX sont prises en charge. Mettez à niveau la version VPX avant de mettre à niveau le SBI vers la version 13.1.

[NSPLAT-21442]

Lorsque les licences NetScaler hébergées sur NetScaler MAS expirent, l'appliance Citrix ADC passe à une période de grâce de 30 jours. Si des licences valides sont mises à jour pendant la période de grâce, l'appliance Citrix ADC continue de fonctionner normalement. Si ce n'est pas le cas, les licences sont révoquées et l'appliance cesse de fonctionner.

[NSPLAT-6417]

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

[NSPLAT-4520]

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

[NSPLAT-4451]

Stratégies

Les connexions peuvent se bloquer si la taille des données de traitement est supérieure à la taille de la mémoire tampon TCP par défaut configurée.Solution : définissez la taille de la mémoire tampon TCP sur la taille maximale des données à traiter.

[NSPOLICY-1267]

SSL

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

Solution :

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

[NSSSL-9572]

La commande Mettre à jour n'est pas disponible pour les commandes d'ajout suivantes :

```
1 -  add azure application
2 -  add azure keyvault
3 -  add ssl certkey with hsmkey option
4 <!--NeedCopy-->
```

[NSSSL-6484]

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

[NSSSL-6478]

Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance Citrix ADC ne renvoie pas d'erreur.

[NSSSL-6213]

Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
ERREUR : actualisation de la liste de réactivation désactivée

[NSSSL-6106]

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

[NSSSL-4427]

Un message d'avertissement incorrect `Warning: No usable ciphers configured on the SSL vserver/service`, s'affiche si vous essayez de modifier le protocole SSL ou le chiffrement dans le profil SSL.

[NSSSL-4001]

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

[NSSSL-3184]

Système

Si l'appliance Citrix ADC est enregistrée sur le serveur ADM, une fuite de mémoire est observée sur l'appliance, même avec un trafic très faible.

[NSHELP-25347]

Dans une configuration de cluster, la `set ratecontrol` commande ne fonctionne qu'après le redémarrage de l'appliance Citrix ADC.

Solution :

Utilisez la `nsapimgr\\_wr.sh -ys icmp\\_rate\\_threshold=<new value>` commande.

[NSHELP-21811]

La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si la solution matérielle-logicielle ne reçoit pas la trame de paramètres max_concurrent_stream du client.

[NSHELP-21240]

Lorsqu'une appliance Citrix ADC envoie une interruption `tcpSynFloodAttack` SNMP, le message de `unackSynCount` journal contient des caractères de chaîne au lieu de valeurs entières.

[NSHELP-20401]

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

[NSHELP-10972]

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

[NSBASE-8506]

Prise en charge ICAP pour Citrix ADC

Une appliance Citrix ADC prend désormais en charge le protocole ICAP (Internet Content Adaptation Protocol) pour le service de transformation de contenu sur le trafic HTTP et HTTPS. L'appliance agit en tant que client ICAP et interagit avec des serveurs ICAP tiers, tels que l'antimalware et la prévention des fuites de données (DLP). Les serveurs ICAP effectuent une transformation de contenu sur les messages HTTP et HTTPS et répondent à la solution matérielle-logicielle en tant que messages modifiés. Les messages adaptés sont soit une réponse ou une demande HTTP, soit HTTPS. Pour de plus amples informations, consultez https://docs.citrix.com/en-us/netscaler/12-1/security/icap-for-remote-content-inspection.html

[NSBASE-825]

Interface utilisateur

Dans l'interface graphique Citrix ADC, le `Help` lien présent sous l' `Dashboard` onglet est rompu.

[NSUI-14752]

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

Solution :

Configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de l'interface de ligne de commande Citrix ADC.

[NSUI-13024]

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

[NSUI-6838]

Le chargement et l'ajout d'un fichier de liste de révocation de certificats (CRL) échouent dans la configuration d'une partition d'administration.

[NSHELP-20988]

Lorsque vous passez à une version antérieure d'une appliance Citrix ADC version 13.0-71.x vers une version antérieure, certaines API NITRO peuvent ne pas fonctionner en raison des modifications des autorisations de fichier.

Solution :

Modifiez l'autorisation `/nsconfig/ns.conf` pour à 644.

[NSCONFIG-4628]

Si vous (administrateur système) effectuez toutes les étapes suivantes sur un dispositif Citrix ADC, les utilisateurs système risquent de ne pas se connecter à l'appliance Citrix ADC rétrogradée.

1. Mettez à niveau l'appliance Citrix ADC vers l'une des versions suivantes :
   - 13.0 52.24 construire
   - 12.1 57,18 construire
   - 11.1 65.10 build
2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
3. Réduisez l'appliance Citrix ADC vers une version antérieure.

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

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

Solution :

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

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

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

[NSCONFIG-3188]

Prise en main de Citrix ADC

January 21, 2021

Cette rubrique décrit les fonctionnalités de base et les détails de configuration d'une appliance Citrix ADC. Les administrateurs système et réseau qui installent et configurent l'équipement réseau peuvent se référer au contenu.

Présentation de Citrix ADC

L'appliance Citrix ADC est un commutateur d'application qui effectue une analyse du trafic spécifique à l'application afin de distribuer, d'optimiser et de sécuriser intelligemment le trafic réseau de couche 4 de couche 7 (L4-L7) pour les applications Web. Par exemple, une appliance Citrix ADC équilibre la charge des décisions sur des requêtes HTTP individuelles au lieu de connexions TCP de longue durée. La fonction d'équilibrage de charge aide à ralentir la défaillance d'un serveur avec moins de perturbations pour les clients. Les fonctions ADC peuvent être classées de façon générale comme suit :

1. Changement de données
2. Sécurité du pare-feu
3. Optimisation
4. Infrastructure des stratégies
5. Flux de paquets
6. Limitation du système

Changement de données

Lorsqu'il est déployé devant des serveurs d'applications, un Citrix ADC assure une distribution optimale du trafic en fonction de la manière dont il dirige les demandes client. Les administrateurs peuvent segmenter le trafic d'application en fonction des informations contenues dans le corps d'une requête HTTP ou TCP, et en fonction des informations d'en-tête L4 à L7 telles que l'URL, le type de données d'application ou les cookies. De nombreux algorithmes d'équilibrage de charge et des vérifications approfondies de l'intégrité des serveurs améliorent la disponibilité des applications en veillant à ce que les demandes des clients soient dirigées vers les serveurs appropriés.

Sécurité du pare-feu

La sécurité et la protection Citrix ADC protègent les applications Web contre les attaques de la couche Application. Une appliance ADC autorise les demandes client légitimes et peut bloquer les demandes malveillantes. Il fournit des défenses intégrées contre les attaques par déni de service (DoS) et prend en charge des fonctionnalités qui protègent contre les surtensions légitimes dans le trafic des

applications qui, autrement, écraseraient les serveurs. Un pare-feu intégré disponible protège les applications Web contre les attaques de couche Application, y compris les exploits par débordement de tampon, les tentatives d'injection SQL, les attaques de scripts intersites, etc. En outre, le pare-feu offre une protection contre le vol d'identité en sécurisant les informations confidentielles de l'entreprise et les données sensibles des clients.

Optimisation

L'optimisation décharge les opérations gourmandes en ressources, telles que le traitement SSL (Secure Sockets Layer), la compression des données, le maintien en vie du client, la mise en mémoire tampon TCP et la mise en cache du contenu statique et dynamique à partir des serveurs. Cela améliore les performances des serveurs de la batterie de serveurs et accélère donc les applications. Une appliance ADC prend en charge plusieurs optimisations TCP transparentes qui atténuent les problèmes causés par une latence élevée et des liaisons réseau encombrées. Accélérer ainsi la livraison des applications tout en ne nécessitant aucune modification de configuration des clients ou des serveurs.

Infrastructure des stratégies

Une stratégie définit des détails spécifiques sur le filtrage et la gestion du trafic sur un Citrix ADC. Il se compose de deux parties : l'expression et l'action. L'expression définit les types de requêtes correspondant à la stratégie. L'action indique à l'appliance ADC ce qu'il faut faire lorsqu'une requête correspond à l'expression. Par exemple, l'expression peut correspondre à un modèle d'URL spécifique pour une attaque de sécurité avec le configuré pour supprimer ou réinitialiser la connexion. Chaque stratégie a une priorité et les priorités déterminent l'ordre dans lequel les stratégies sont évaluées.

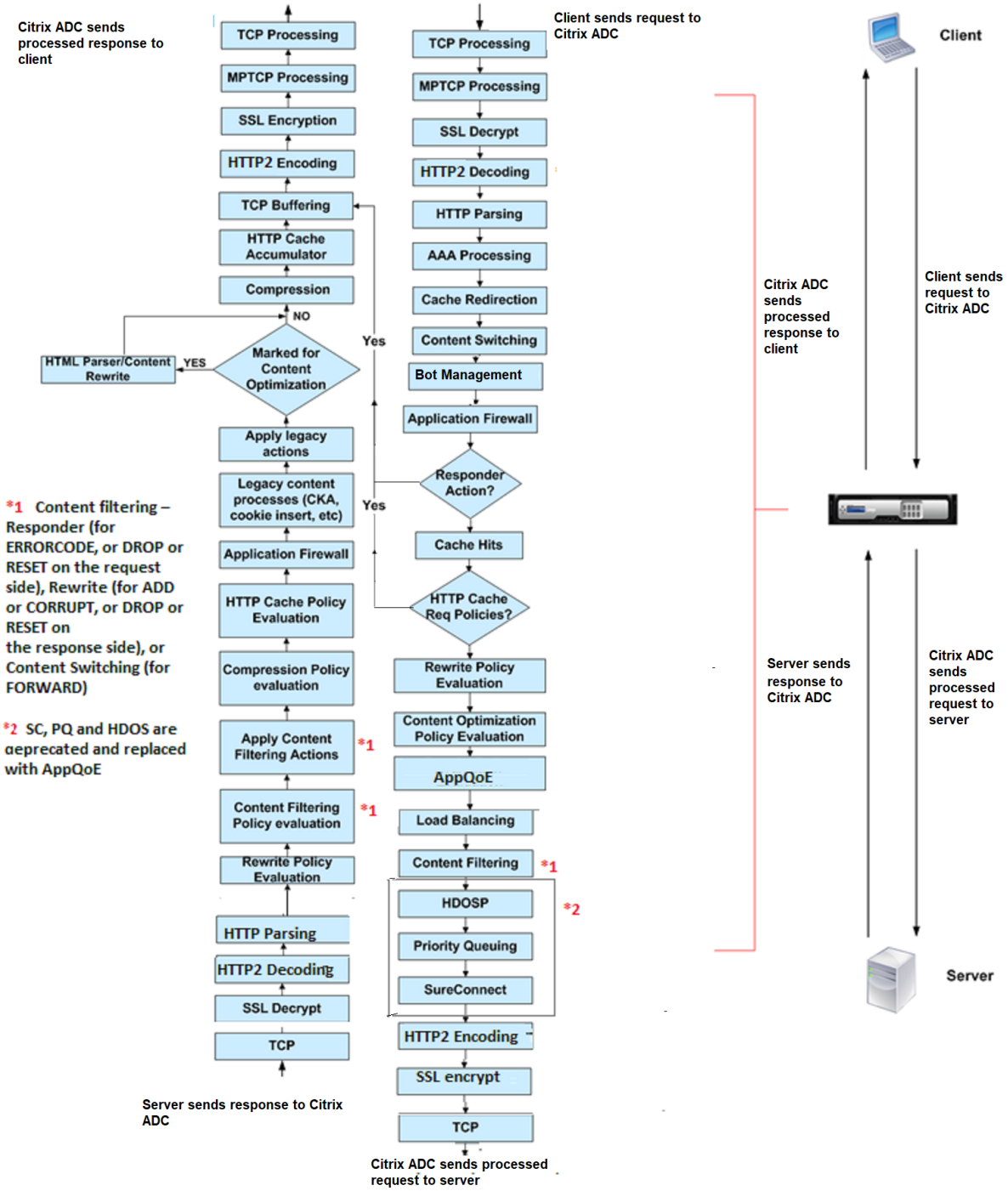
Lorsqu'une appliance ADC reçoit du trafic, la liste de stratégies appropriée détermine le traitement du trafic. Chaque stratégie de la liste contient une ou plusieurs expressions qui définissent ensemble les critères qu'une connexion doit respecter pour correspondre à la stratégie.

Pour tous les types de stratégie sauf la réécriture, l'appliance implémente uniquement la première stratégie ayant une correspondance de requête. Pour les stratégies de réécriture, l'appliance ADC évalue les stratégies dans l'ordre et exécute les actions associées dans le même ordre. La priorité des politiques est importante pour obtenir les résultats que vous voulez.

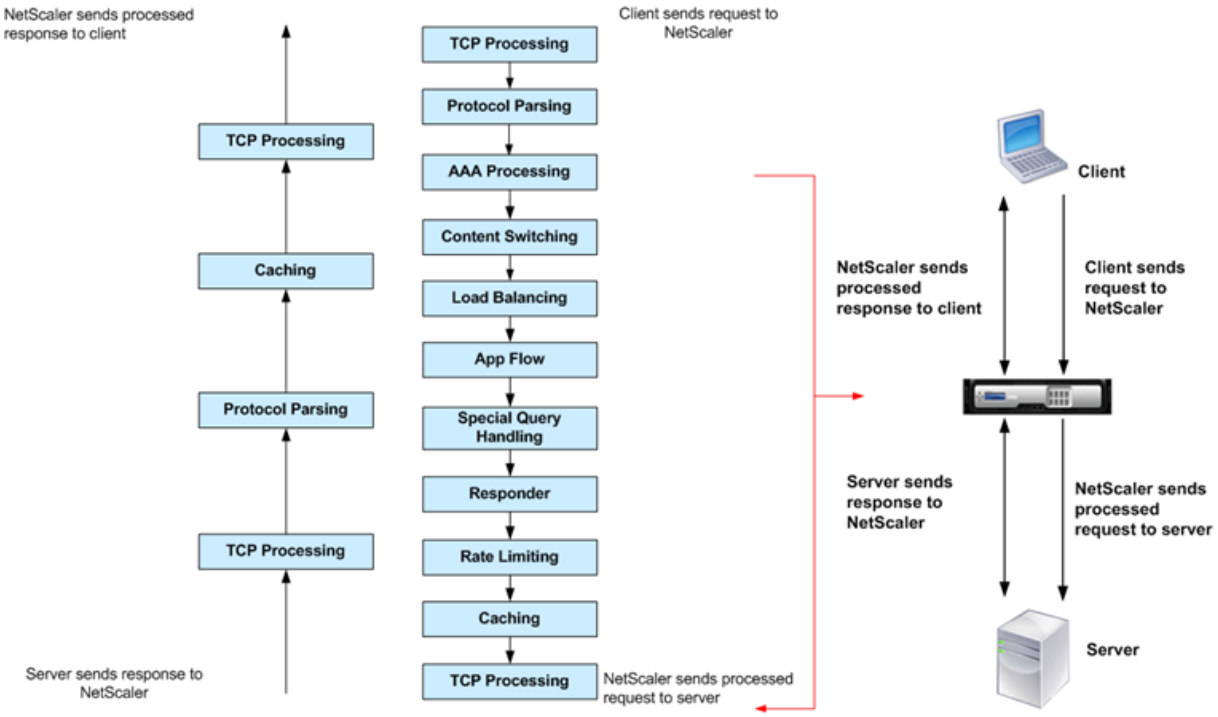
Flux de paquets

Selon la configuration requise, vous pouvez choisir de configurer plusieurs fonctionnalités. Par exemple, vous pouvez choisir de configurer à la fois la compression et le déchargement SSL. Par conséquent, un paquet sortant peut être compressé puis chiffré avant d'être envoyé au client.

La figure suivante illustre le flux de paquets DataStream dans l'appliance Citrix ADC. DataStream est pris en charge pour les bases de données MySQL et MS SQL.



La figure suivante illustre le flux de paquets DataStream dans l'appliance Citrix ADC. DataStream est pris en charge pour les bases de données MySQL et MS SQL. Pour plus d'informations sur la fonction DataStream, voir DataStream.



> **Remarque :** Si le trafic est destiné à un serveur virtuel de commutation de contenu, l'appliance évalue les stratégies dans l'ordre suivant :
>
> 1. lié au remplacement global.
> 2. lié à l'équilibrage de charge serveur virtuel.
> 3. lié au serveur virtuel de commutation de contenu.
> 4. lié à la valeur par défaut globale.
>
> De cette façon, si une règle politique est vraie et que l'expression gotopriorityexpression est END, nous arrêtons l'évaluation des politiques.
> Dans la commutation de contenu, si aucun serveur virtuel d'équilibrage de charge n'est sélectionné ou lié au serveur virtuel de commutation de contenu, nous évaluons les stratégies de répondeur liées uniquement au serveur virtuel de commutation de contenu.

Limitation du système

Il existe des limitations système pour chaque fonctionnalité Citrix ADC lorsque vous installez le logiciel Citrix ADC 9.2 ou version ultérieure. Pour plus d'informations, consultez l'article Citrix, CTX118716.

Quelle est la place d'une appliance Citrix ADC dans le réseau ?

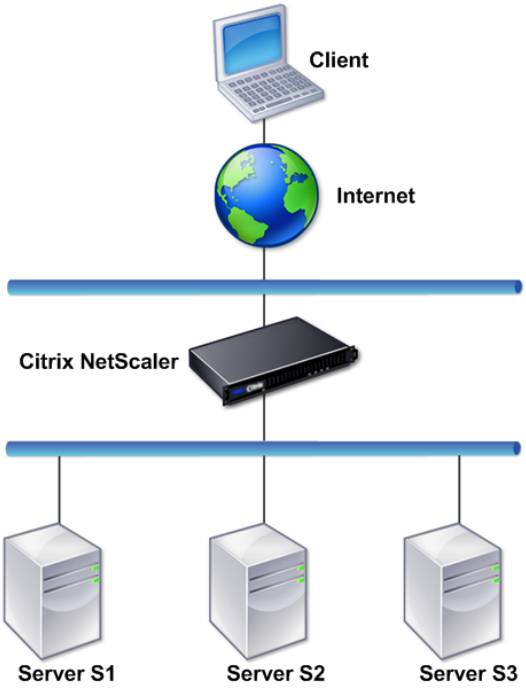
August 20, 2021

Une appliance Citrix ADC réside entre les clients et les serveurs, de sorte que les demandes des clients et les réponses du serveur passent par elle. Dans une installation standard, les serveurs virtuels configurés sur l'appliance fournissent des points de connexion que les clients utilisent pour accéder aux applications derrière l'appliance. Dans ce cas, l'appliance possède des adresses IP publiques associées à ses serveurs virtuels, tandis que les serveurs réels sont isolés dans un réseau privé. Il est également possible de faire fonctionner l'appliance en mode transparent en tant que pont L2 ou routeur L3, ou même de combiner des aspects de ces modes et d'autres.

Modes de déploiement physique

Une appliance Citrix ADC résidant logiquement entre les clients et les serveurs peut être déployée dans l'un ou l'autre des deux modes physiques : en ligne et à un bras. En mode Inline, plusieurs interfaces réseau sont connectées à différents segments Ethernet et l'appliance est placée entre les clients et les serveurs. L'appliance dispose d'une interface réseau distincte pour chaque réseau client et d'une interface réseau distincte pour chaque réseau serveur. L'appliance et les serveurs peuvent exister sur différents sous-réseaux dans cette configuration. Il est possible que les serveurs se trouvent dans un réseau public et que les clients accèdent directement aux serveurs via l'appliance, l'appliance appliquant en toute transparence les fonctionnalités L4-L7. Habituellement, les serveurs virtuels (décrits plus loin) sont configurés pour fournir une abstraction des serveurs réels. La figure suivante illustre un déploiement standard en ligne.

Figure 1. Déploiement en ligne



En mode à un bras, une seule interface réseau de l'appliance est connectée à un segment Ethernet. Dans ce cas, l'appliance n'isole pas les côtés client et serveur du réseau, mais donne accès aux applications via des serveurs virtuels configurés. Le mode à un bras permet de simplifier les modifications réseau nécessaires à l'installation de Citrix ADC dans certains environnements.

Pour obtenir des exemples de déploiement en ligne (à deux bras) et à un bras, reportez-vous à la section Présentation des topologies communes de réseau.

Citrix ADC en tant que périphérique L2

Un dispositif Citrix ADC fonctionnant en tant que périphérique L2 fonctionnera en mode L2. En mode L2, l'appliance ADC transfère les paquets entre les interfaces réseau lorsque toutes les conditions suivantes sont remplies :

- Les paquets sont destinés à l'adresse MAC (Media Access Control) d'un autre périphérique.
- L'adresse MAC de destination se trouve sur une interface réseau différente.
- L'interface réseau est membre du même réseau local virtuel (VLAN).

Par défaut, toutes les interfaces réseau sont membres d'un VLAN prédéfini, VLAN 1. Les demandes et réponses du protocole ARP (Address Resolution Protocol) sont transmises à toutes les interfaces

réseau qui sont membres du même VLAN. Pour éviter le pontage des boucles, le mode L2 doit être désactivé si un autre périphérique L2 fonctionne en parallèle avec l'appliance Citrix ADC.

Pour plus d'informations sur la façon dont les modes L2 et L3 interagissent, consultez Modes de transfert de paquets.

Pour plus d'informations sur la configuration du mode L2, reportez-vous à la section « Activer et désactiver le mode de couche 2 » dans Modes de transfert de paquets.

Citrix ADC en tant que périphérique de transfert de paquets

Une appliance Citrix ADC peut fonctionner comme un périphérique de transfert de paquets, et ce mode de fonctionnement est appelé mode L3. Lorsque le mode L3 est activé, l'appliance transmet tous les paquets monodiffusion reçus qui sont destinés à une adresse IP qui n'appartient pas à l'appliance, s'il existe un itinéraire vers la destination. L'appliance peut également acheminer des paquets entre des VLAN.

Dans les deux modes de fonctionnement, L2 et L3, l'appliance abandonne généralement les paquets qui se trouvent dans :

- Cadres multidiffusion
- Trames de protocole inconnues destinées à l'adresse MAC d'une appliance (non IP et non ARP)
- Protocole Spanning Tree (sauf si BridgeBPDU est ON)

Pour plus d'informations sur la façon dont les modes L2 et L3 interagissent, consultez Modes de transfert de paquets.

Pour plus d'informations sur la configuration du mode L3, voir Modes de transfert de paquets.

Comment une appliance Citrix ADC communique avec les clients et les serveurs

January 21, 2021

Une appliance Citrix ADC est généralement déployée devant une batterie de serveurs et fonctionne comme un proxy TCP transparent entre les clients et les serveurs, sans nécessiter de configuration côté client. Ce mode de fonctionnement de base est appelé technologie Request Switching et est le cœur de la fonctionnalité de Citrix ADC. Le changement de demande permet à une appliance de multiplexer et de décharger les connexions TCP, de maintenir les connexions persistantes et de gérer le trafic au niveau de la demande (couche d'application). Ceci est possible car l'appliance peut séparer la requête HTTP de la connexion TCP sur laquelle la requête est remise.

Selon la configuration, une appliance peut traiter le trafic avant de transférer la demande à un serveur. Par exemple, si le client tente d'accéder à une application sécurisée sur le serveur, l'appliance peut effectuer le traitement SSL nécessaire avant d'envoyer du trafic au serveur.

Pour faciliter un accès efficace et sécurisé aux ressources du serveur, une appliance utilise un ensemble d'adresses IP collectivement appelées adresses IP appartenant à Citrix ADC. Pour gérer votre trafic réseau, vous attribuez des adresses IP appartenant à Citrix ADC à des entités virtuelles qui deviennent les éléments constitutifs de votre configuration. Par exemple, pour configurer l'équilibrage de charge, vous créez des serveurs virtuels pour recevoir les demandes des clients et les distribuer aux services, qui sont des entités représentant les applications sur vos serveurs.

Présentation des adresses IP détenues par Citrix ADC

Pour fonctionner en tant que proxy, une appliance Citrix ADC utilise une variété d'adresses IP. Les principales adresses IP détenues par Citrix ADC sont les suivantes :

- Adresse IP Citrix ADC (NSIP)

  L'adresse NSIP est l'adresse IP pour la gestion et l'accès général au système à l'appliance elle-même, ainsi que pour la communication entre les appliances dans une configuration haute disponibilité.

- Adresse IP du serveur virtuel (VIP)

  Une adresse VIP est l'adresse IP associée à un serveur virtuel. Il s'agit de l'adresse IP publique à laquelle les clients se connectent. De nombreux VIP peuvent être configurés pour une appliance qui gère un large éventail de trafic.

- Adresse IP du sous-réseau (SNIP)

  Une adresse SNIP est utilisée dans la gestion des connexions et la surveillance du serveur. Vous pouvez spécifier plusieurs adresses SNIP pour chaque sous-réseau. Les adresses SNIP peuvent être liées à un VLAN.

- Jeu d'adresses IP

  Un jeu d'adresses IP est un ensemble d'adresses IP configurées sur l'appliance en tant que SNIP. Un ensemble d'adresses IP est identifié avec un nom significatif qui aide à identifier l'utilisation des adresses IP qu'il contient.

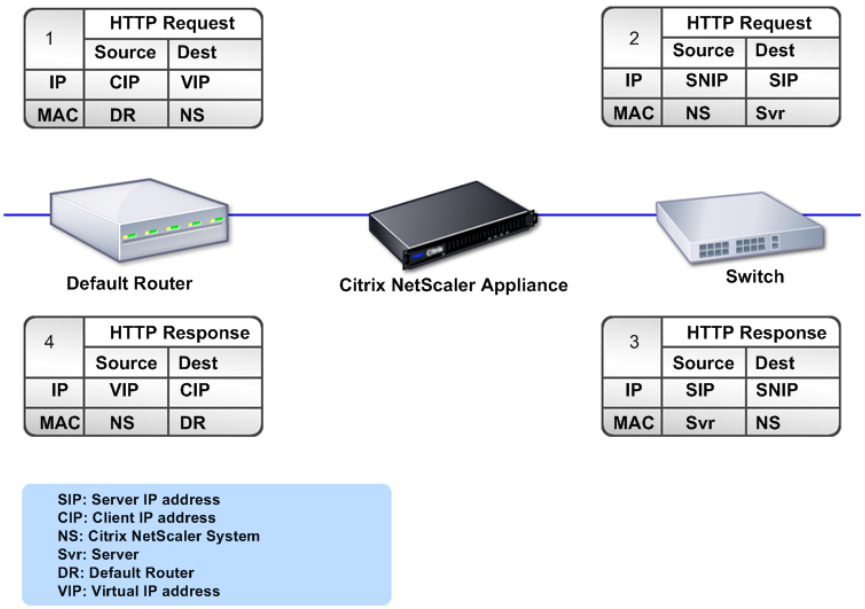
- Profil net

  Un profil réseau (ou profil réseau) contient une adresse IP ou un jeu d'adresses IP. Un profil réseau peut être lié à l'équilibrage de charge ou au changement de contenu de serveurs virtuels, de services, de groupes de services ou de moniteurs. Lors de la communication avec des serveurs physiques ou des homologues, l'appliance utilise les adresses spécifiées dans le profil comme adresses IP source.

Comment les flux de trafic sont gérés

Étant donné qu'une appliance Citrix ADC fonctionne comme un proxy TCP, elle traduit les adresses IP avant d'envoyer des paquets à un serveur. Lorsque vous configurez un serveur virtuel, les clients se connectent à une adresse VIP sur l'appliance Citrix ADC au lieu de se connecter directement à un serveur. Selon les paramètres du serveur virtuel, l'appliance sélectionne un serveur approprié et envoie la demande du client à ce serveur. Par défaut, l'appliance utilise une adresse SNIP pour établir des connexions avec le serveur, comme illustré dans la figure suivante.

Figure 1. Connexions basées sur le serveur virtuel



En l'absence d'un serveur virtuel, lorsqu'une appliance reçoit une demande, elle transmet la demande de manière transparente au serveur. C'est ce qu'on appelle le mode de fonctionnement transparent. Lorsqu'elle fonctionne en mode transparent, une appliance convertit les adresses IP source des demandes de clients entrantes vers l'adresse SNIP mais ne modifie pas l'adresse IP de destination. Pour que ce mode fonctionne, le mode L2 ou L3 doit être configuré de manière appropriée.

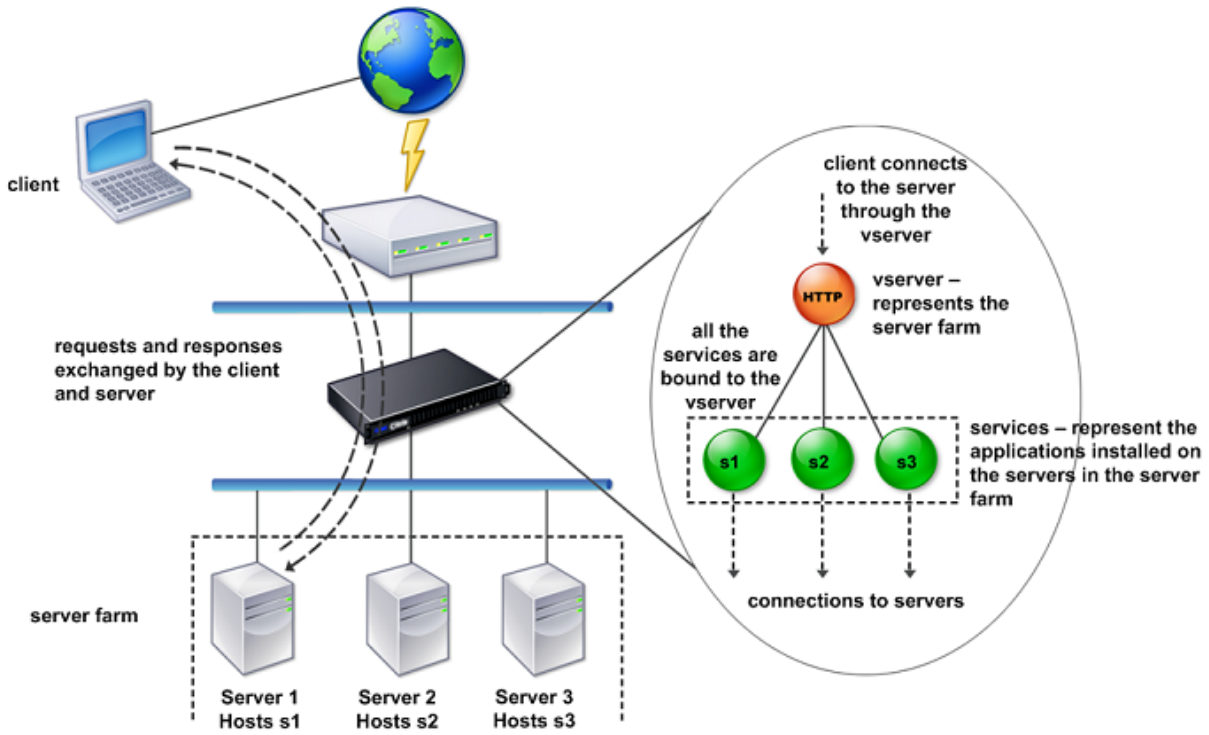
Dans les cas où les serveurs ont besoin de l'adresse IP du client réelle, l'appliance peut être configurée pour modifier l'en-tête HTTP en insérant l'adresse IP du client comme champ supplémentaire ou configurée pour utiliser l'adresse IP du client au lieu d'une adresse SNIP pour les connexions aux serveurs.

Blocs de construction de la gestion du trafic

La configuration d'une appliance Citrix ADC est généralement construite avec une série d'entités virtuelles qui servent de blocs de construction pour la gestion du trafic. L'approche par bloc de construction permet de séparer les flux de trafic. Les entités virtuelles sont des abstractions, représentant généralement des adresses IP, des ports et des gestionnaires de protocole pour le traitement du trafic. Les clients accèdent aux applications et aux ressources via ces entités virtuelles. Les entités les plus couramment utilisées sont les serveurs et services virtuels. Les serveurs virtuels représentent des groupes de serveurs dans une batterie de serveurs ou un réseau distant, et les services représentent des applications spécifiques sur chaque serveur.

La plupart des fonctionnalités et des paramètres de trafic sont activés via des entités virtuelles. Par exemple, vous pouvez configurer une appliance pour compresser toutes les réponses du serveur à un client connecté à la batterie de serveurs via un serveur virtuel particulier. Pour configurer l'appliance pour un environnement particulier, vous devez identifier les fonctionnalités appropriées, puis choisir la bonne combinaison d'entités virtuelles pour les distribuer. La plupart des fonctionnalités sont fournies via une cascade d'entités virtuelles qui sont liées les unes aux autres. Dans ce cas, les entités virtuelles sont comme des blocs assemblés dans la structure finale d'une application livrée. Vous pouvez ajouter, supprimer, modifier, lier, activer et désactiver les entités virtuelles pour configurer les entités. La figure suivante illustre les concepts abordés dans cette section.

Figure 2. Fonctionnement des blocs de construction de la gestion du trafic

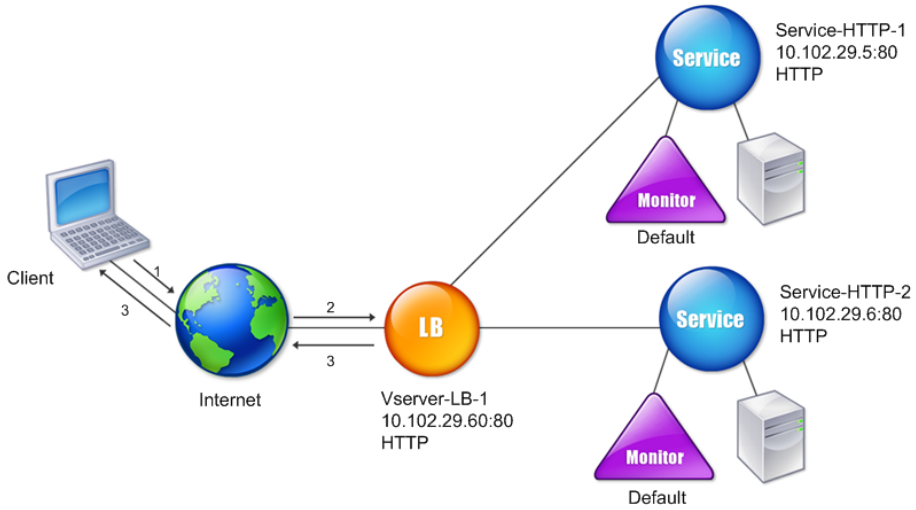


Une configuration simple d'équilibrage de charge

Dans l'exemple illustré dans la figure suivante, l'appliance Citrix ADC est configurée pour fonctionner comme un équilibreur de charge. Pour cette configuration, vous devez configurer des entités virtuelles spécifiques à l'équilibrage de charge et les lier dans un ordre spécifique. En tant qu'équilibreur de charge, une appliance distribue les demandes des clients sur plusieurs serveurs et optimise ainsi l'utilisation des ressources.

Les éléments de base d'une configuration d'équilibrage de charge standard sont les services et les serveurs virtuels d'équilibrage de charge. Les services représentent les applications sur les serveurs. Les serveurs virtuels abstraits les serveurs en fournissant une adresse IP unique à laquelle les clients se connectent. Pour vous assurer que les demandes client sont envoyées à un serveur, vous devez lier chaque service à un serveur virtuel. Autrement dit, vous devez créer des services pour chaque serveur et lier les services à un serveur virtuel. Les clients utilisent l'adresse VIP pour se connecter à une appliance Citrix ADC. Lorsque l'appliance reçoit des demandes client envoyées à l'adresse VIP, elle les envoie à un serveur déterminé par l'algorithme d'équilibrage de charge. L'équilibrage de charge utilise une entité virtuelle appelée moniteur pour déterminer si un service configuré spécifique (serveur et application) est disponible pour recevoir des demandes.

Figure 3. Serveur virtuel, services et moniteurs d'équilibrage de charge



Outre la configuration de l'algorithme d'équilibrage de charge, vous pouvez configurer plusieurs paramètres qui affectent le comportement et les performances de la configuration d'équilibrage de charge. Par exemple, vous pouvez configurer le serveur virtuel pour maintenir la persistance en fonction de l'adresse IP source. L'appliance dirige ensuite toutes les demandes provenant d'une adresse IP spécifique vers le même serveur.

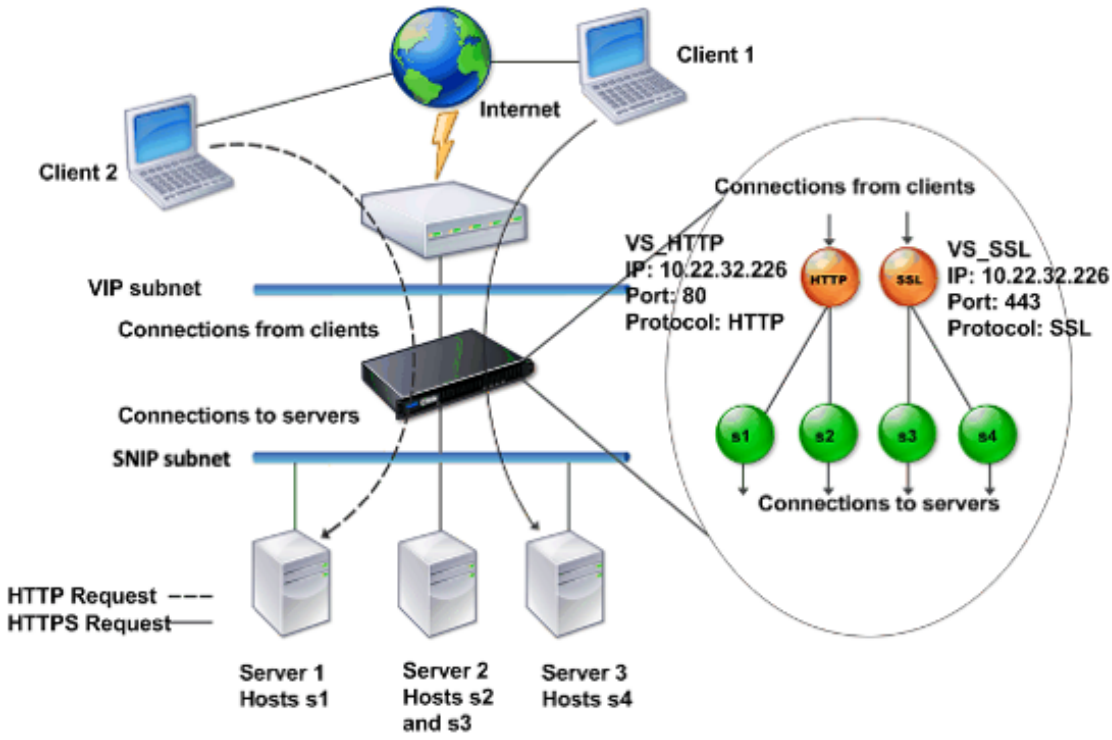
Présentation des serveurs virtuels

Un serveur virtuel est une entité Citrix ADC nommée que les clients externes peuvent utiliser pour accéder aux applications hébergées sur les serveurs. Il est représenté par un nom alphanumérique, une adresse IP virtuelle (VIP), un port et un protocole. Le nom du serveur virtuel n'a qu'une signification locale et est conçu pour faciliter l'identification du serveur virtuel. Lorsqu'un client tente d'accéder à des applications sur un serveur, il envoie une demande au VIP au lieu de l'adresse IP du serveur physique. Lorsque l'appliance reçoit une demande à l'adresse VIP, elle met fin à la connexion sur le serveur virtuel et utilise sa propre connexion avec le serveur au nom du client. Les paramètres de port et de protocole du serveur virtuel déterminent les applications que le serveur virtuel représente. Par exemple, un serveur Web peut être représenté par un serveur virtuel et un service dont le port et le protocole sont respectivement définis sur 80 et HTTP. Plusieurs serveurs virtuels peuvent utiliser la même adresse VIP mais différents protocoles et ports.

Les serveurs virtuels sont des points pour fournir des fonctionnalités. La plupart des fonctionnalités, telles que la compression, la mise en cache et le déchargement SSL, sont normalement activées sur un serveur virtuel. Lorsque l'appliance reçoit une demande à une adresse VIP, elle choisit le serveur virtuel approprié par le port sur lequel la demande a été reçue et son protocole. L'appliance traite ensuite la demande en fonction des fonctionnalités configurées sur le serveur virtuel.

Dans la plupart des cas, les serveurs virtuels fonctionnent en tandem avec les services. Vous pouvez lier plusieurs services à un serveur virtuel. Ces services représentent les applications exécutées sur des serveurs physiques dans une batterie de serveurs. Une fois que l'appliance traite les demandes reçues à une adresse VIP, elle les transmet aux serveurs conformément à l'algorithme d'équilibrage de charge configuré sur le serveur virtuel. La figure suivante illustre ces concepts.

Figure 4. Plusieurs serveurs virtuels avec une seule adresse VIP



La figure précédente montre une configuration composée de deux serveurs virtuels avec une adresse VIP commune mais des ports et protocoles différents. Chacun des serveurs virtuels a deux services qui lui sont liés. Les services s1 et s2 sont liés à VS_HTTP et représentent les applications HTTP sur les serveurs 1 et 2. Les services s3 et s4 sont liés à VS_SSL et représentent les applications SSL sur les serveurs 2 et 3 (le serveur 2 fournit à la fois des applications HTTP et SSL). Lorsque l'appliance reçoit une demande HTTP à l'adresse VIP, elle traite la demande comme spécifié par les paramètres de VS_HTTP et l'envoie au serveur 1 ou au serveur 2. De même, lorsque l'appliance reçoit une demande HTTPS à l'adresse VIP, elle la traite comme spécifié par les paramètres de VS_SSL et elle l'envoie au serveur 2 ou au serveur 3.

Les serveurs virtuels ne sont pas toujours représentés par des adresses IP, des numéros de port ou des protocoles spécifiques. Ils peuvent être représentés par des caractères génériques, auquel cas ils sont appelés serveurs virtuels génériques. Par exemple, lorsque vous configurez un serveur virtuel avec un caractère générique au lieu d'un VIP, mais avec un numéro de port spécifique, l'appliance intercepte et traite tout le trafic conforme à ce protocole et destiné au port prédéfini. Pour les serveurs virtuels comportant des caractères génériques au lieu de VIP et de numéros de port, l'appliance intercepte et traite tout le trafic conforme au protocole.

Les serveurs virtuels peuvent être regroupés dans les catégories suivantes :

- Serveur virtuel d'équilibrage de charge

  Reçoit et redirige les demandes vers un serveur approprié. Le choix du serveur approprié est

basé sur la méthode d'équilibrage de charge que l'utilisateur configure.

- Serveur virtuel de redirection de cache

  Redirige les demandes client de contenu dynamique vers les serveurs d'origine et les demandes de contenu statique vers les serveurs de cache. Les serveurs virtuels de redirection de cache fonctionnent souvent en conjonction avec les serveurs virtuels d'équilibrage de charge.

- Serveur virtuel de commutation de contenu

  Dirige le trafic vers un serveur sur la base du contenu demandé par le client. Par exemple, vous pouvez créer un serveur virtuel de commutation de contenu qui dirige toutes les demandes d'images client vers un serveur qui ne sert que les images. Les serveurs virtuels de commutation de contenu fonctionnent souvent en conjonction avec des serveurs virtuels d'équilibrage de charge.

- Serveur virtuel de réseau privé virtuel (VPN)

  Décrypte le trafic qui transite via un tunnel et l'envoie aux applications intranet.

- Serveur virtuel SSL

  Reçoit et déchiffre le trafic SSL, puis redirige vers un serveur approprié. Choisir le serveur approprié est similaire à choisir un serveur virtuel d'équilibrage de charge.

Présentation des services

Les services représentent des applications sur un serveur. Bien que les services soient normalement combinés avec des serveurs virtuels, en l'absence d'un serveur virtuel, un service peut toujours gérer le trafic spécifique à l'application. Par exemple, vous pouvez créer un service HTTP sur une appliance Citrix ADC pour représenter une application de serveur Web. Lorsque le client tente d'accéder à un site Web hébergé sur le serveur Web, l'appliance intercepte les requêtes HTTP et crée une connexion transparente avec le serveur Web.

En mode service uniquement, une appliance fonctionne en tant que proxy. Il met fin aux connexions client, utilise une adresse SNIP pour établir une connexion au serveur et traduit les adresses IP source des requêtes client entrantes en une adresse SNIP. Bien que les clients envoient des demandes directement à l'adresse IP du serveur, le serveur les voit comme provenant de l'adresse SNIP. L'appliance traduit les adresses IP, les numéros de port et les numéros de séquence.

Un service est également un point d'application d'entités. Prenons l'exemple de l'accélération SSL. Pour utiliser cette fonctionnalité, vous devez créer un service SSL et lier un certificat SSL au service. Lorsque l'appliance reçoit une demande HTTPS, elle déchiffre le trafic et l'envoie, en texte clair, au serveur. Seul un ensemble limité de fonctionnalités peut être configuré dans le cas du service uniquement.

Les services utilisent des entités appelées moniteurs pour suivre l'état des applications. Chaque service a un moniteur par défaut, qui est basé sur le type de service, qui lui est lié. Comme spécifié par les paramètres configurés sur le moniteur, l'appliance envoie des sondes à l'application à intervalles réguliers afin de déterminer son état. Si les sondes échouent, l'appliance marque le service comme étant hors service. Dans de tels cas, l'appliance répond aux demandes des clients avec un message d'erreur approprié ou réachemine la demande selon les stratégies d'équilibrage de charge configurées.

Présentation de la gamme de produits Citrix ADC

August 20, 2021

La gamme de produits Citrix ADC optimise la livraison d'applications sur Internet et sur les réseaux privés, combinant la sécurité, l'optimisation et la gestion du trafic au niveau de l'application en une seule appliance intégrée. Vous pouvez installer un appliance Citrix ADC dans votre salle des serveurs et acheminer toutes les connexions vers vos serveurs gérés via celle-ci. Les fonctionnalités de Citrix ADC que vous activez et les stratégies que vous définissez sont ensuite appliquées au trafic entrant et sortant.

Une appliance Citrix ADC peut être intégrée à n'importe quel réseau en complément des équilibreurs de charge, serveurs, caches et pare-feu existants. Il ne nécessite aucun logiciel côté client ou serveur supplémentaire et peut être configuré à l'aide des utilitaires de configuration de l'interface utilisateur graphique et CLI basés sur le Web Citrix ADC.

Cette rubrique comprend les sections suivantes :

- Plates-formes matérielles Citrix ADC
- Éditions Citrix ADC
- Versions prises en charge sur le matériel ADC
- Navigateurs pris en charge

Plates-formes matérielles Citrix ADC

Le matériel Citrix ADC est disponible sur une variété de plates-formes qui ont une gamme de spécifications matérielles :

Plateforme matérielle Citrix ADC MPX

Plateforme matérielle Citrix ADC SDX

Éditions Citrix ADC

Le système d'exploitation Citrix ADC est disponible en trois éditions :

- Standard
- Avancé
- Premium

Les éditions Standard et Advanced disposent de fonctionnalités limitées. Des licences de fonctionnalités sont requises pour toutes les éditions.

Pour plus d'informations sur les éditions logicielles Citrix ADC, consultez la fiche technique Citrix ADC Editions.

Pour plus d'informations sur la façon d'obtenir et d'installer des licences, consultez Licences.

Versions prises en charge sur le matériel Citrix ADC

Consultez les tableaux de matrice de compatibilité suivants pour toutes les plates-formes matérielles Citrix ADC et les versions logicielles prises en charge sur ces plates-formes :

Matrice de compatibilité matérielle et logicielle Citrix ADC MPX

Matrice de compatibilité matériel-logicielle Citrix ADC SDX

Navigateurs pris en charge

Pour accéder à l'interface graphique Citrix ADC, votre station de travail doit disposer d'un navigateur Web pris en charge.

Le tableau suivant répertorie les navigateurs compatibles pour NetScaler GUI version 12.0, 12.1 et 13.0 :

OS	Navigateur	Versions
Windows 7 et versions ultérieures	Internet Explorer	11, Edge, & versions ultérieures
Windows 7 et versions ultérieures	Mozilla Firefox	45 et versions ultérieures
Windows 7 et versions ultérieures	Chrome	60 et versions ultérieures
MAC	Mozilla Firefox	45 et versions ultérieures
MAC	Safari	10.1.1 et versions ultérieures

Les versions de navigateur compatibles pour Citrix ADC 11.1 sont les suivantes :

OS	Navigateur	Versions
Windows 7 et versions ultérieures	Internet Explorer	8,9,10, 11, Bord
Windows 7 et versions ultérieures	Mozilla Firefox	45 et versions ultérieures
Windows 7 et versions ultérieures	Chrome	60 et versions ultérieures
MAC	Mozilla Firefox	45 et versions ultérieures
MAC	Safari	10.1.1 et versions ultérieures

Installer le matériel

January 21, 2021

Avant d'installer une appliance Citrix ADC, consultez la liste de vérification de pré-installation.

Pour utiliser l'appliance SDX, vous devez effectuer les tâches suivantes en suivant les instructions données dans les ressources fournies dans le tableau. Effectuez les tâches dans l'ordre donné.

Tâche

Description

1. Lire la sécurité, les mises en garde, les avertissements et d'autres informations

   Lisez les informations de prudence et de danger que vous devez savoir avant d'installer le produit.

2. Préparer l'installation

   Déballez votre appareil et assurez-vous que toutes les pièces ont été livrées, préparez le site et le rack et suivez les précautions élémentaires de sécurité électrique avant d'installer votre nouvel appareil.

3. Installer le matériel

   Montez l'appliance en rack, installez les émetteurs-récepteurs (si disponible) et connectez l'appliance au réseau et à une source d'alimentation.

4. Configurez l'appliance.

Configurez les paramètres initiaux de l'appliance Citrix ADC à l'aide de l'interface graphique ou de la console série.

Suivez les étapes indiquées dans les documentations suivantes pour effectuer ces tâches :

- Documentation matérielle Citrix ADC MPX
- Documentation matérielle Citrix ADC SDX

Accéder à une appliance Citrix ADC

August 20, 2021

Une appliance Citrix ADC dispose à la fois d'une interface de ligne de commande (CLI) et d'une interface graphique. L'interface graphique inclut un utilitaire de configuration pour la configuration de l'appliance et un utilitaire statistique, appelé Tableau de bord. Pour un accès initial, toutes les appliances sont livrés avec l'adresse IP Citrix ADC (NSIP) par défaut 192.168.100.1 et le masque de sous-réseau par défaut 255.255.0.0. Vous pouvez affecter un nouveau NSIP et un masque de sous-réseau associé lors de la configuration initiale.

Si vous rencontrez un conflit d'adresse IP lors du déploiement de plusieurs unités Citrix ADC, recherchez les causes possibles suivantes :

- Avez-vous sélectionné un NSIP qui est une adresse IP déjà attribuée à un autre périphérique de votre réseau ?
- Avez-vous attribué le même NSIP à plusieurs appliances Citrix ADC ?
- Le NSIP est accessible sur tous les ports physiques. Les ports d'un Citrix ADC sont des ports hôtes et non des ports de commutateur.

Le tableau suivant récapitule les méthodes d'accès disponibles.

Méthode d'accès	Port	Adresse IP par défaut requise ? (A/N)
CLI	Console	N
CLI et GUI	Ethernet	O

Interface de ligne de commande

Accédez à l'interface de ligne de commande localement en connectant une station de travail au port de la console, ou à distance en vous connectant via le shell sécurisé (SSH) à partir de n'importe quel poste de travail sur le même réseau.

Connectez-vous à l'interface de ligne de commande via le port de la console

L'appliance dispose d'un port console permettant de se connecter à un poste de travail informatique. Pour vous connecter à l'appliance, vous avez besoin d'un câble multisegment série et d'une station de travail dotée d'un programme d'émulation de terminal.

Pour vous connecter à l'interface de ligne de commande via le port de la console, procédez comme suit :

1. Connectez le port de la console à un port série de la station de travail. Pour plus d'informations, voir Connecter le câble de la console.
2. Sur le poste de travail, démarrez HyperTerminal ou tout autre programme d'émulation de terminal. Si l'invite d'ouverture de session n'apparaît pas, vous devrez peut-être appuyer une ou plusieurs fois sur ENTRÉE pour l'afficher.
3. Dans Nom d'utilisateur, tapez `nsroot`. Dans Mot de passe, tapez `nsroot` et si ce mot de passe ne fonctionne pas, essayez de taper le numéro de série de l'appliance. Le code à barres du numéro de série est disponible à l'arrière de l'appliance.

Connectez-vous à l'interface de ligne de commande à l'aide de SSH

Le protocole SSH est la méthode d'accès à distance privilégiée pour accéder à une appliance à distance depuis n'importe quelle station de travail sur le même réseau. Vous pouvez utiliser SSH version 1 (SSH1) ou SSH version 2 (SSH2).

Si vous n'avez pas de client SSH fonctionnel, vous pouvez télécharger et installer l'un des programmes client SSH suivants :

- PuTTY

  Logiciel Open Source pris en charge sur plusieurs plates-formes. Disponible sur :

  http://www.chiark.greenend.org.uk/~sgtatham/putty/

- `Vandyke` Logiciel SecureCRT

  Logiciels commerciaux pris en charge sur la plate-forme Windows. Disponible sur :

  http://www.vandyke.com/products/securecrt/

Ces programmes sont testés par l'équipe Citrix ADC, qui a vérifié qu'ils fonctionnent correctement avec une appliance Citrix ADC. D'autres programmes peuvent également fonctionner correctement, mais n'ont pas été testés.

Pour vérifier que le client SSH est correctement installé, utilisez-le pour vous connecter à n'importe quel périphérique de votre réseau qui accepte les connexions SSH.

Pour ouvrir une session sur une appliance Citrix ADC à l'aide d'un client SSH, procédez comme suit :

1. Sur votre poste de travail, démarrez le client SSH.

2. Pour la configuration initiale, utilisez l'adresse IP par défaut (NSIP), qui est 192.168.100.1. Pour un accès ultérieur, utilisez le NSIP qui a été attribué lors de la configuration initiale. Sélectionnez SSH1 ou SSH2 comme protocole.
3. Dans Nom d'utilisateur, tapez `nsroot`. Dans Mot de passe, tapez `nsroot` et si ce mot de passe ne fonctionne pas, essayez de taper le numéro de série de l'appliance. Le code à barres du numéro de série est disponible à l'arrière de l'appliance. Par exemple.

```
login as: nsroot


Using keyboard-interactive authentication.


Password:


Last login: Tue Jun 16 10:37:28 2009 from 10.102.29.9




Done


>

<!--NeedCopy-->
```

Interface de Citrix ADC

> **Important :**
>
> Une paire de clés de certificat est requise pour l'accès HTTPS à l'interface graphique Citric ADC. Sur ADC, une paire de clés de certificat est automatiquement liée aux services internes. Sur une appliance MPX ou SDX, la taille de clé par défaut est de 1024 octets et sur une instance VPX, la taille de clé par défaut est de 512 octets. Cependant, la plupart des navigateurs aujourd'hui n'acceptent pas une clé inférieure à 1024 octets. Par conséquent, l'accès HTTPS à l'utilitaire de configuration VPX est bloqué.

En outre, si une licence n'est pas présente sur une appliance MPX au démarrage, et que vous ajoutez une licence ultérieurement et que vous redémarrez l'appliance, vous risquez de perdre la liaison du certificat.

Citrix vous recommande d'installer une paire de clés de certificat d'au moins 1024 octets sur l'appliance pour l'accès HTTPS à l'interface graphique. Installez également une licence appropriée avant de démarrer l'appliance.

L'interface graphique comprend un utilitaire de configuration et un utilitaire statistique, appelé Dashboard, auquel vous accédez via une station de travail connectée à un port Ethernet de l'appliance.

La configuration système requise pour le poste de travail exécutant l'interface graphique est la suivante :

- Pour les stations de travail Windows, un processeur Pentium 166 MHz ou plus rapide.
- Pour les stations de travail Linux, une plate-forme Pentium exécutant le noyau Linux v2.2.12 ou supérieur, et la `glibc` version 2.12—11 ou ultérieure. Un minimum de 32 Mo de RAM est requis et 48 Mo de RAM est recommandé. La station de travail doit prendre en charge le mode couleur 16 bits, les gestionnaires de fenêtres KDE et KWM utilisés conjointement, avec des écrans configurés sur des hôtes locaux.
- Pour les stations de travail Solaris, Sun exécutant Solaris 2.6, Solaris 7 ou Solaris 8.

Votre poste de travail doit disposer d'un navigateur Web pris en charge pour accéder à l'utilitaire de configuration et au Tableau de bord.

Les navigateurs suivants sont pris en charge.

Système d'exploitation : Windows 7

Navigateur : Internet Explorer (version 9, 10 et 11), Mozilla Firefox (version 3.6.25 et supérieure), Google Chrome (dernière).

Système d'exploitation : Windows 64 bits

Navigateur : Internet Explorer (version 8, 9, 10 et 11), Google Chrome (version la plus récente)

Système d'exploitation :
Navigateur MAC : Mozilla Firefox (version 3.6.25 et supérieure), Safari (version 5.1.3 et supérieure), Google Chrome (version la plus récente)

Utiliser l'interface graphique Citrix ADC

Une fois connecté à l'utilitaire de configuration, vous pouvez configurer l'appliance via une interface graphique qui inclut une aide contextuelle.

Pour vous connecter à l'interface graphique, procédez comme suit :

1. Ouvrez votre navigateur Web et entrez Citrix ADC IP (NSIP) en tant qu'adresse HTTP. Si vous n'avez pas encore configuré la configuration initiale, entrez le NSIP (http://192.168.100.1) par défaut. La page d'ouverture de session Citrix s'affiche.

Remarque : si vous avez deux appliances Citrix ADC dans une configuration haute disponibilité, n'accédez pas à l'interface graphique en entrant l'adresse IP de l'appliance Citrix ADC secondaire. Si vous le faites et que vous utilisez l'interface graphique pour configurer l'appliance secondaire, vos modifications de configuration ne sont pas appliquées à l'appliance Citrix ADC principale.

2. Dans la zone de texte Nom d'utilisateur, tapez `nsroot`.
3. Dans la zone de texte Mot de passe, tapez le mot de passe administratif que vous avez attribué au `nsroot` compte lors de la configuration initiale et cliquez sur **Connexion**. Si ce mot de passe ne fonctionne pas, essayez de taper le numéro de série de l'appliance. Le code à barres du numéro de série est disponible à l'arrière de l'appliance.

   Pour accéder à l'aide en ligne, sélectionnez Aide dans le menu Aide en haut à droite.

Utiliser l'utilitaire statistique

Tableau de bord, l'utilitaire statistique, est une application basée sur un navigateur qui affiche des graphiques et des tableaux sur lesquels vous pouvez surveiller les performances d'une appliance Citrix ADC.

Pour vous connecter au Tableau de bord, procédez comme suit :

1. Ouvrez votre navigateur Web et entrez le NSIP en tant qu'adresse HTTP. La page d'ouverture de session Citrix s'affiche.
2. Dans la zone de texte Nom d'utilisateur, tapez `nsroot`.
3. Dans la zone de texte Mot de passe, tapez le mot de passe administratif que vous avez affecté au `nsroot` compte lors de la configuration initiale. Si ce mot de passe ne fonctionne pas, essayez de taper le numéro de série de l'appliance. Le code à barres du numéro de série est disponible à l'arrière de l'appliance.

Configurer ADC pour la première fois

August 20, 2021

Pour connaître la configuration initiale d' une appliance Citrix ADC MPX, reportez-vous à la section Configuration initiale d'une appliance Citrix MPX.

Pour connaître la configuration initiale d' une appliance Citrix SDX, reportez-vous à la section Configuration initiale d'une appliance Citrix SDX.

API NITRO

Vous pouvez utiliser l'API NITRO pour configurer l'appliance Citrix ADC. NITRO expose ses fonctionnalités via des interfaces REST (Representational State Transfer). Par conséquent, les applications NITRO peuvent être développées dans n'importe quel langage de programmation. En outre, pour les applications qui doivent être développées avec Java, .NET ou Python, les API NITRO sont exposées par le biais de bibliothèques pertinentes qui sont packagées en tant que kits de développement logiciel (SDK) séparés. Pour plus d'informations, voir API NITRO.

Sécurisez votre déploiement Citrix ADC

October 5, 2021

Pour maintenir la sécurité tout au long du cycle de vie du déploiement de l'appliance Citrix ADC, Citrix vous recommande de prendre en compte les aspects de sécurité suivants :

- Sécurité physique
- Sécurité de l'appliance
- Sécurité du réseau
- Administration et gestion

Différents déploiements peuvent nécessiter des considérations de sécurité différentes. Les directives de déploiement sécurisé Citrix ADC fournissent des conseils de sécurité généraux pour vous aider à décider d'un déploiement sécurisé approprié en fonction de vos exigences de sécurité spécifiques.

Pour plus d'informations sur les directives relatives au déploiement sécurisé de l'appliance Citrix ADC, reportez-vous aux directives de déploiement sécurisé Citrix ADC.

Configurer la haute disponibilité

August 20, 2021

Vous pouvez déployer deux appliances Citrix ADC dans une configuration haute disponibilité, où une unité accepte activement les connexions et gère les serveurs tandis que l'unité secondaire surveille le premier. L'appliance Citrix ADC qui accepte activement les connexions et gère les serveurs est appelée unité principale et l'autre unité secondaire dans une configuration haute disponibilité. En cas de panne dans l'unité principale, l'unité secondaire devient l'unité principale et commence à accepter activement les connexions.

Chaque appliance Citrix ADC d'une paire haute disponibilité surveille l'autre en envoyant des messages périodiques, appelés messages de pulsation ou vérifications d'intégrité, afin de déterminer

l'état ou l'état du nœud homologue. Si une vérification de l'état d'une unité principale échoue, l'unité secondaire tente à nouveau la connexion pour une période spécifique. Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité. Si une nouvelle tentative ne réussit pas à la fin de la période spécifiée, l'unité secondaire prend le relais de l'unité principale dans un processus appelé basculement. La figure suivante montre deux configurations haute disponibilité, l'une en mode à bras unique et l'autre en mode à deux bras.

Figure 1. Haute disponibilité en mode monobras

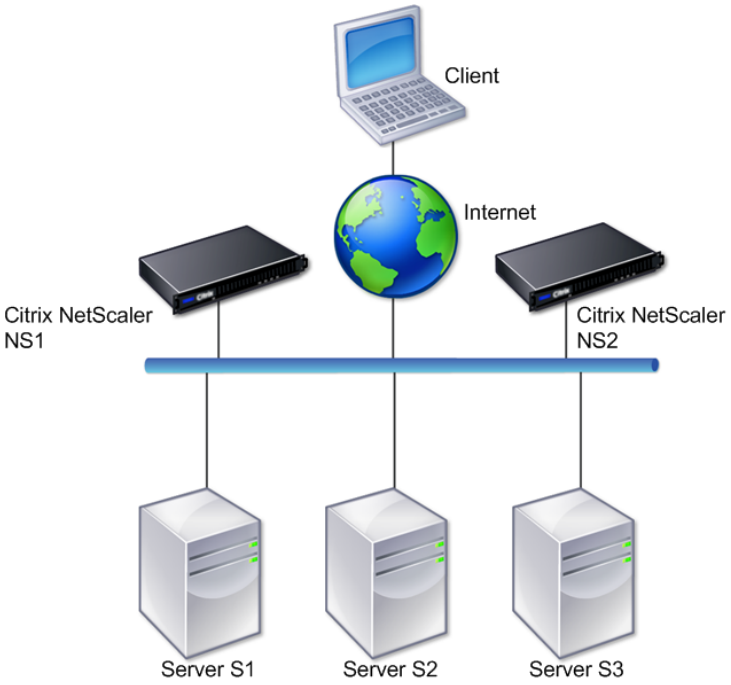
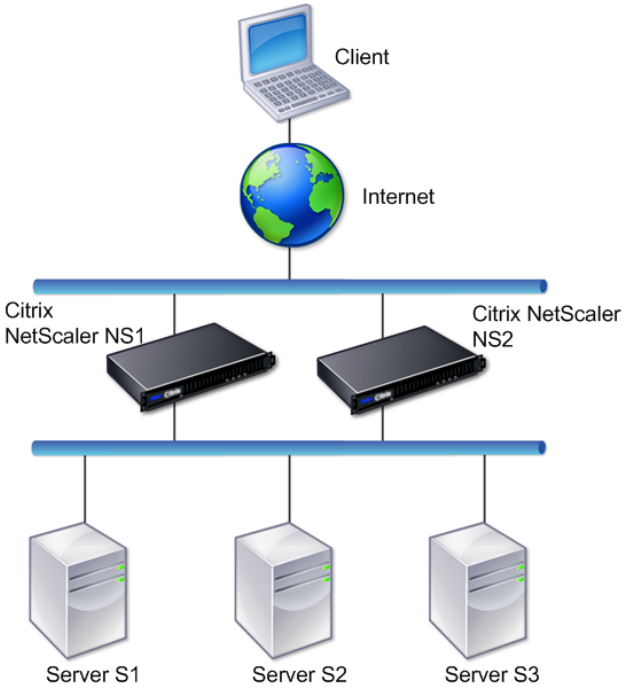


Figure 2. Haute disponibilité en mode à deux bras



Dans une configuration à un bras, NS1 et NS2 ainsi que les serveurs S1, S2 et S3 sont connectés au commutateur.

Dans la configuration à deux bras, NS1 et NS2 sont tous deux connectés à deux commutateurs. Les serveurs S1, S2 et S3 sont connectés au second commutateur. Le trafic entre le client et les serveurs passe par NS1 ou NS2.

Pour configurer un environnement de haute disponibilité, configurez une appliance ADC comme principale et une autre comme secondaire. Effectuez les tâches suivantes sur chacune des appliances ADC :

- Ajoutez un nœud.
- Désactivez la surveillance de la haute disponibilité pour les interfaces inutilisées.

Ajouter un nœud

Un nœud est une représentation logique d'une appliance Citrix ADC homologue. Il identifie l'unité homologue par ID et NSIP. Une appliance utilise ces paramètres pour communiquer avec l'homologue et suivre son état. Lorsque vous ajoutez un nœud, les unités primaires et secondaires échangent des messages de pulsation de manière asynchrone. L'ID de nœud est un entier qui ne doit pas être supérieur à 64.

Via l'interface de ligne de commande

Pour ajouter un nœud à l'aide de l'interface de ligne de commande, procédez comme suit :

À l'invite de commandes, tapez les commandes suivantes pour ajouter un nœud et vérifiez que le nœud a été ajouté :

- add HA node <id> <IPAddress>
- show HA node <id>

Exemple

```
1  add HA node 0 10.102.29.170
2   Done
3  > show HA node 0
4  1)      Node ID:      0
5          IP:   10.102.29.200 (NS200)
6          Node State: UP
7          Master State: Primary
8          SSL Card Status: UP
9          Hello Interval: 200 msecs
10         Dead Interval: 3 secs
11         Node in this Master State for: 1:0:41:50 (days:hrs:min:
               sec)
12 <!--NeedCopy-->
```

Via l'interface graphique

Pour ajouter un nœud à l'aide de l'interface graphique, procédez comme suit :

1. Accédez à **Système** > **Haute disponibilité** .
2. Cliquez sur **Ajouter** dans l'onglet **Nœuds** .
3. Dans la page **Créer un nœud HA**, dans la zone de texte **Adresse IP du nœud distant**, tapez l'adresse NSIP (par exemple, 10.102.29.170) du nœud distant.
4. Assurez-vous que la case à cocher **Configurer le système distant pour participer à la configuration de la haute disponibilité** est cochée. Fournissez les informations d'identification de connexion du nœud distant dans les zones de texte sous **Informations d'identification de connexion du système distant**.
5. Activez la case à cocher **Désactiver le moniteur HA sur les interfaces/canaux qui sont en panne** pour désactiver le moniteur HA sur les interfaces qui sont en panne.

Vérifiez que le nœud que vous avez ajouté apparaît dans la liste des nœuds de l'onglet Nœuds.

Désactiver la surveillance de la haute disponibilité pour les interfaces inutilisées

Le moniteur de haute disponibilité est une entité virtuelle qui surveille une interface. Vous devez désactiver le moniteur pour les interfaces qui ne sont pas connectées ou utilisées pour le trafic. Lorsque le moniteur est activé sur une interface dont le statut est DOWN, l'état du nœud devient NOT UP. Dans une configuration haute disponibilité, un nœud principal entrant dans un état NOT UP peut provoquer un basculement de haute disponibilité. Une interface est marquée comme DOWN dans les conditions suivantes :

- L'interface n'est pas connectée
- L'interface ne fonctionne pas correctement
- Le câble reliant l'interface ne fonctionne pas correctement

Via l'interface de ligne de commande

Pour désactiver le moniteur de haute disponibilité pour une interface inutilisée à l'aide de l'interface de ligne de commande, procédez comme suit :

À l'invite de commandes, tapez les commandes suivantes pour désactiver le moniteur de haute disponibilité pour une interface inutilisée et vérifier qu'elle est désactivée :

- set interface <id> -haMonitor OFF
- Afficher l'interface <id>

  Exemple

```
1  > set interface 1/8 -haMonitor OFF
2   Done
3  > show interface 1/8
4          Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
5          flags=0x4000 <ENABLED, DOWN, down, autoneg, 802.1q>
6          MTU=1514, native vlan=1, MAC=00:d0:68:15:fd:3d, downtime
               238h55m44s
7          Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
8                   throughput 0
9
10         RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
11         TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
12         NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0)
               Muted(0)
13         Bandwidth thresholds are not set.
14 <!--NeedCopy-->
```

  Lorsque le moniteur de haute disponibilité est désactivé pour une interface inutilisée, la sortie de la commande show interface pour cette interface n'inclut pas "HAMON."

Via l'interface graphique

Pour désactiver le moniteur de haute disponibilité pour les interfaces inutilisées à l'aide de l'interface graphique, procédez comme suit :

1. Accédez à Système > Réseau > Interfaces.
2. Sélectionnez l'interface pour laquelle le moniteur doit être désactivé.
3. Cliquez sur Ouvrir. La boîte de dialogue Modifier l'interface s'affiche.
4. Dans Surveillance HA, sélectionnez l'option OFF.
5. Cliquez sur OK.
6. Vérifiez que, lorsque l'interface est sélectionnée, « Surveillance HA : OFF » apparaît dans les détails en bas de la page.

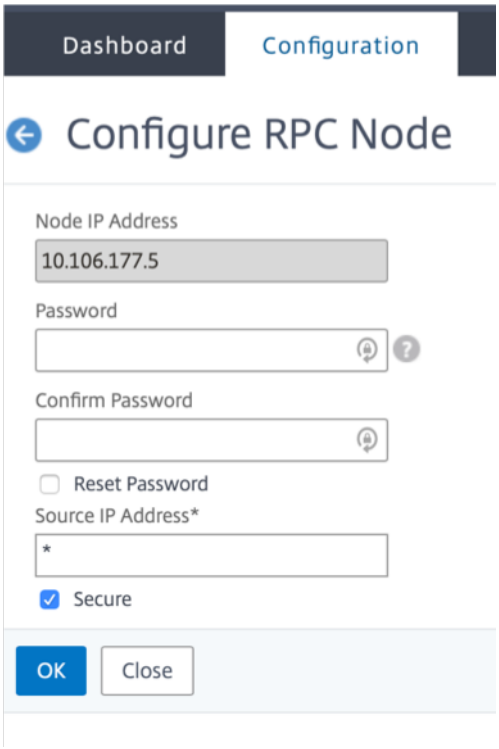
Modifier le mot de passe d'un nœud RPC

August 20, 2021

Pour communiquer avec d'autres appliances Citrix ADC, chaque appliance requiert une connaissance des autres appliances, y compris la procédure d'authentification sur l'appliance Citrix ADC. Les nœuds RPC sont des entités système internes utilisées pour la communication système à système des informations de configuration et de session. Un nœud RPC existe sur chaque appliance Citrix ADC et stocke des informations, telles que les adresses IP de l'autre appliance Citrix ADC et les mots de passe utilisés pour l'authentification. L'appliance Citrix ADC qui contacte l'autre appliance Citrix ADC vérifie le mot de passe dans le nœud RPC.

Pour modifier le mot de passe d'un nœud RPC à l'aide de l'interface graphique graphique

1. Accédez à **Système** > **Réseau** > **RPC**.
2. Dans le volet **RPC**, sélectionnez le nœud, puis cliquez sur **Modifier**.
3. Dans **Configurer le nœud RPC**, tapez le nouveau mot de passe.
4. Dans **Adresse IP source**, tapez l'adresse IP du nœud existant à utiliser pour communiquer avec le nœud du système homologue.



5. Sélectionnez **Sécuriser**, puis cliquez sur **OK**.

> **Remarque**
>
> Pour une sécurité renforcée, Citrix vous recommande d'activer l'option **Secure** sur les nœuds RPC. Lorsque vous activez l'option **Secure**, l'appliance crypte toutes les communications RPC envoyées d'un nœud ADC à d'autres nœuds ADC, sécurisant ainsi la communication RPC. Cette communication sécurisée utilise le numéro de port 3008. Si le pare-feu entre les nœuds ADC bloque le numéro de port 3008, débloquez et continuez. Sinon, la synchronisation de configuration et la propagation de la configuration peuvent échouer.

Pour modifier le mot de passe d'un nœud RPC à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes :

```
set ns rpcNode <IPAddress> {
 -password }
  [-secure ( YES | NO )]
show ns rpcNode
<!--NeedCopy-->
```

Exemple :


```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES
 Done
> show rpcNode
.
.
.
 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
     SrcIP:  *           Secure:  ON
Done
>

<!--NeedCopy-->
```

Configurer une appliance FIPS pour la première fois

August 20, 2021

Une paire de clés de certificat est requise pour l'accès HTTPS à l'utilitaire de configuration et pour les appels de procédure distante sécurisés. Les nœuds RPC sont des entités système internes utilisées pour la communication système à système des informations de configuration et de session. Un nœud RPC existe sur chaque appliance. Ce nœud stocke le mot de passe, qui est comparé à celui fourni par l'appliance contactant. Pour communiquer avec d'autres appliances Citrix ADC, chaque appliance requiert une connaissance des autres appliances, y compris la manière de s'authentifier sur l'autre appliance. Les nœuds RPC conservent ces informations, qui incluent les adresses IP des autres appliances Citrix ADC et les mots de passe utilisés pour s'authentifier sur chacun d'eux.

Sur une appliance virtuelle Citrix ADC MPX, une paire de clés de certificat est automatiquement liée aux services internes. Sur une appliance FIPS, une paire de clés de certificat doit être importée dans le module de sécurité matérielle (HSM) d'une carte FIPS. Pour ce faire, vous devez configurer la carte FIPS, créer une paire de clés de certificat et la lier aux services internes.

Configurer HTTPS sécurisé à l'aide de l'interface de ligne de commande

Pour configurer HTTPS sécurisé à l'aide de l'interface de ligne de commande, procédez comme suit :

1. Initialisez le module de sécurité matérielle (HSM) sur la carte FIPS de l'appliance. Pour plus d'informations sur l'initialisation du HSM, voir Configurer le HSM.
2. Si l'appliance fait partie d'une configuration de haute disponibilité, activez la carte SIM. Pour plus d'informations sur l'activation de la carte SIM sur les appliances principale et secondaire, voir Configurer les appliances FIPS dans une configuration haute disponibilité.

3. Importez la clé FIPS dans le HSM de la carte FIPS de l'appliance. À l'invite de commandes, tapez :

   ```
   import ssl fipskey serverkey -key ns-server.key -inform PEM
   ```

4. Ajoutez une paire de clés de certificat. À l'invite de commandes, tapez :

   ```
   add certkey server -cert ns-server.cert -fipskey serverkey
   ```

5. Liez la clé de certificat créée à l'étape précédente aux services internes suivants. À l'invite de commandes, tapez :

   ```
   bind ssl service nshttps-127.0.0.1-443 -certkeyname server
   bind ssl service nshttps-::11-443 -certkeyname server
   ```

Configurer HTTPS sécurisé à l'aide de l'interface graphique

Pour configurer HTTPS sécurisé à l'aide de l'interface graphique, procédez comme suit :

1. Initialisez le module de sécurité matérielle (HSM) sur la carte FIPS de l'appliance. Pour plus d'informations sur l'initialisation du HSM, voir Configurer le HSM.
2. Si l'appliance fait partie d'une configuration de haute disponibilité, activez le système d'information sécurisé (SIM). Pour plus d'informations sur l'activation de la carte SIM sur les appliances principale et secondaire, voir Configurer les appliances FIPS dans une configuration haute disponibilité.
3. Importez la clé FIPS dans le HSM de la carte FIPS de l'appliance. Pour plus d'informations sur l'importation d'une clé FIPS, reportez-vous à la section Importer une clé FIPS existante .
4. Accédez à Gestion du trafic > SSL > Certificats.
5. Dans le volet d'informations, cliquez sur Installer.
6. Dans la boîte de dialogue Installer le certificat, tapez les détails du certificat.
7. Cliquez sur Créer, puis sur Fermer.
8. Accédez à Gestion du trafic > Équilibrage de charge > Services.
9. Dans le volet d'informations, sous l'onglet Action, cliquez sur Services internes.
10. Sélectionnez nshttps-127.0.0.1-443 dans la liste, puis cliquez sur Ouvrir.
11. Sous l'onglet Paramètres SSL, dans le volet Disponible, sélectionnez le certificat créé à l'étape 7, cliquez sur Ajouter, puis cliquez sur OK.
12. Sélectionnez nshttps- : :11-443 dans la liste, puis cliquez sur Ouvrir.
13. Sous l'onglet Paramètres SSL, dans le volet Disponible, sélectionnez le certificat créé à l'étape 7, cliquez sur Ajouter, puis cliquez sur OK.
14. Cliquez sur OK.

Configurer RPC sécurisé à l'aide de l'interface de ligne de commande

Pour configurer RPC sécurisé à l'aide de l'interface de ligne de commande, procédez comme suit :

1. Initialisez le module de sécurité matérielle (HSM) sur la carte FIPS de l'appliance. Pour plus d'informations sur l'initialisation du HSM, voir Configurer le HSM.
2. Activez le système d'information sécurisé (SIM). Pour plus d'informations sur l'activation de la carte SIM sur les appliances principale et secondaire, voir Configurer les appliances FIPS dans une configuration haute disponibilité.
3. Importez la clé FIPS dans le HSM de la carte FIPS de l'appliance. À l'invite de commandes, tapez :

   ```
   import ssl fipskey serverkey -key ns-server.key -inform PEM
   ```

4. Ajoutez une paire de clés de certificat. À l'invite de commandes, tapez :

   ```
   add certkey server -cert ns-server.cert -fipskey serverkey
   ```

5. Liez la paire de clés de certificat aux services internes suivants. À l'invite de commandes, tapez :

   ```
   bind ssl service nsrpcs-127.0.0.1-3008 -certkeyname server
   ```

   ```
   bind ssl service nskrpcs-127.0.0.1-3009 -certkeyname server
   ```

   ```
   bind ssl service nsrpcs-::1l-3008 -certkeyname server
   ```

6. Activez le mode RPC sécurisé. À l'invite de commandes, tapez :

   set ns rpcnode <IP address> -secure YES

   Pour plus d'informations sur la modification du mot de passe d'un nœud RPC, voir Modifier le mot de passe d'un nœud RPC.

Configurer RPC sécurisé à l'aide de l'interface graphique

Pour configurer RPC sécurisé à l'aide de l'interface graphique, procédez comme suit :

1. Initialisez le module de sécurité matérielle (HSM) sur la carte FIPS de l'appliance. Pour plus d'informations sur l'initialisation du HSM, voir Configurer le HSM.
2. Activez le système d'information sécurisé (SIM). Pour plus d'informations sur l'activation de la carte SIM sur les appliances principale et secondaire, Configurez les appliances FIPS dans une configuration haute disponibilité.
3. Importez la clé FIPS dans le HSM de la carte FIPS de l'appliance. Pour plus d'informations sur l'importation d'une clé FIPS, consultez la section Importer une clé FIPS existante .
4. Accédez à Gestion du trafic > SSL > Certificats.
5. Dans le volet d'informations, cliquez sur Installer.
6. Dans la boîte de dialogue Installer le certificat, tapez les détails du certificat.
7. Cliquez sur Créer, puis sur Fermer.

8. Accédez à Gestion du trafic > Équilibrage de charge > Services.
9. Dans le volet d'informations, sous l'onglet Action, cliquez sur Services internes.
10. Sélectionnez nsrpcs-127.0.0.1-3008 dans la liste, puis cliquez sur Ouvrir.
11. Sous l'onglet Paramètres SSL, dans le volet Disponible, sélectionnez le certificat créé à l'étape 7, cliquez sur Ajouter, puis cliquez sur OK.
12. Sélectionnez nskrpcs-127.0.0.1-3009 dans la liste, puis cliquez sur Ouvrir.
13. Sous l'onglet Paramètres SSL, dans le volet Disponible, sélectionnez le certificat créé à l'étape 7, cliquez sur Ajouter, puis cliquez sur OK.
14. Sélectionnez nsrpcs- : :11-3008 dans la liste, puis cliquez sur Ouvrir.
15. Sous l'onglet Paramètres SSL, dans le volet Disponible, sélectionnez le certificat créé à l'étape 7, cliquez sur Ajouter, puis cliquez sur OK.
16. Cliquez sur OK.
17. Accédez à Système > Réseau > RPC.
18. Dans le volet d'informations, sélectionnez l'adresse IP, puis cliquez sur Ouvrir.
19. Dans la boîte de dialogue Configurer le nœud RPC, sélectionnez Sécurisé.
20. Cliquez sur OK.

Topologies réseau communes

August 20, 2021

Comme décrit dans la section « Mode de déploiement physique » de la section Où se trouve une appliance Citrix ADC dans le réseau ?, vous pouvez déployer l'appliance Citrix ADC soit en ligne entre les clients et les serveurs, soit en mode à bras unique. Le mode Inline utilise une topologie à deux bras, qui est le type de déploiement le plus courant.

Configurer une topologie commune à deux bras

Dans une topologie à deux bras, une interface réseau est connectée au réseau client et une autre interface réseau est connectée au réseau serveur, ce qui garantit que tout le trafic circule à travers l'appliance. Cette topologie peut vous obliger à reconnecter votre matériel et peut également entraîner un temps d'arrêt momentané. Les variations de base de la topologie à deux bras sont plusieurs sous-réseaux, généralement avec l'appliance sur un sous-réseau public et les serveurs sur un sous-réseau privé, et le mode transparent, avec l'appliance et les serveurs sur le réseau public.

Configuration d'une topologie simple de sous-réseau à deux bras multiples

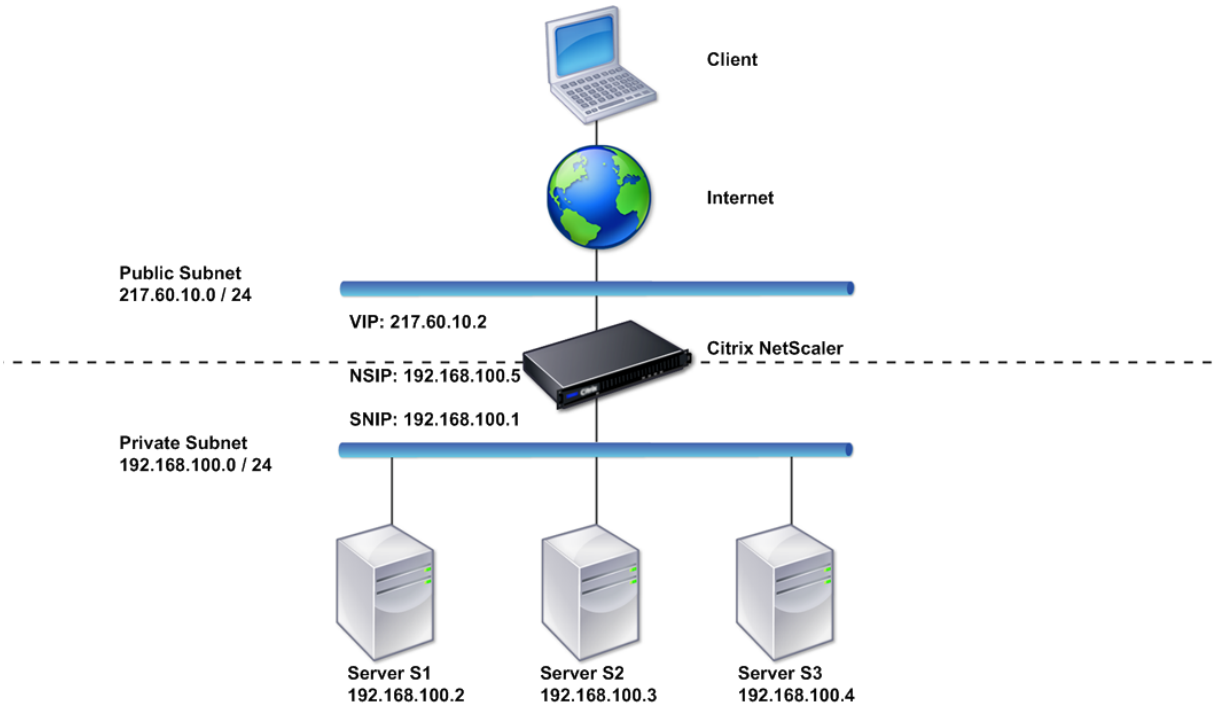
L'une des topologies les plus couramment utilisées a l'appliance Citrix ADC en ligne entre les clients et les serveurs, avec un serveur virtuel configuré pour traiter les demandes des clients. Cette configura-

tion est utilisée lorsque les clients et les serveurs résident sur différents sous-réseaux. Dans la plupart des cas, les clients et les serveurs résident respectivement sur des sous-réseaux publics et privés.

Par exemple, considérez une appliance déployée en mode à deux bras pour gérer les serveurs S1, S2 et S3, avec un serveur virtuel de type HTTP configuré sur l'appliance et avec des services HTTP exécutés sur les serveurs. Les serveurs se trouvent sur un sous-réseau privé et un SNIP est configuré sur l'appliance pour communiquer avec les serveurs. L'option Utiliser SNIP (USNIP) doit être activée sur l'appliance afin qu'elle utilise le SNIP au lieu du MIP.

Comme le montre la figure suivante, le VIP se trouve sur le sous-réseau public 217.60.10.0, et le NSIP, les serveurs et le SNIP sont sur le sous-réseau privé 192.168.100.0/24.

Figure 1. Diagramme topologique pour le mode à deux bras, sous-réseaux multiples



Pour déployer une appliance Citrix ADC en mode à deux bras avec plusieurs sous-réseaux, procédez comme suit :

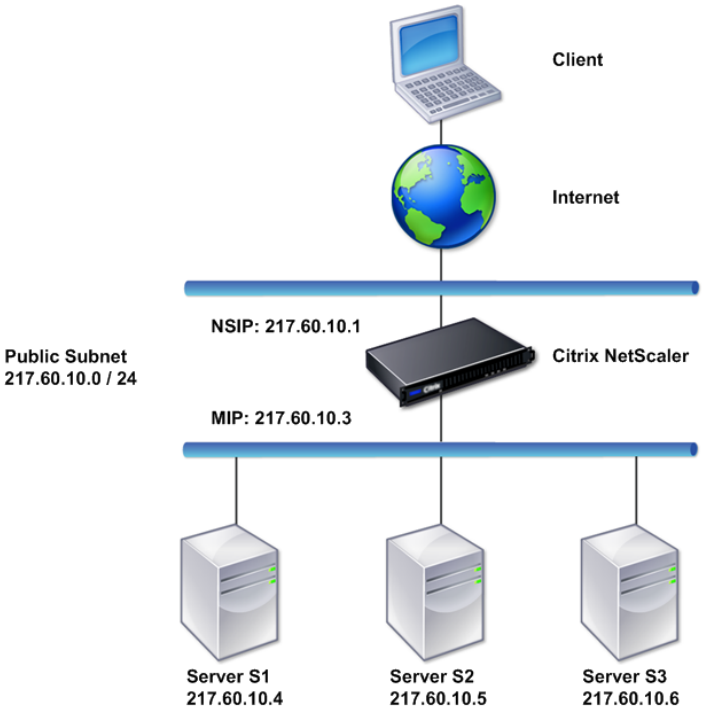
1. Configurez le NSIP et la passerelle par défaut, comme décrit dans Configuration de l'adresse IP NetScaler (NSIP).
2. Configurez le SNIP, comme décrit dans Configuration des adresses IP de sous-réseau.
3. Activez l'option USNIP, comme décrit dans la section Pour activer ou désactiver le mode USNIP .

4. Configurez le serveur virtuel et les services, comme décrit dans la section Création d'un serveur virtuel et la section Configuration des services .
5. Connectez l'une des interfaces réseau à un sous-réseau privé et l'autre interface à un sous-réseau public.

Configurer une topologie transparente simple à deux bras

Utilisez le mode transparent si les clients doivent accéder directement aux serveurs, sans serveur virtuel intervenant. Les adresses IP du serveur doivent être publiques car les clients doivent pouvoir y accéder. Dans l'exemple illustré dans la figure suivante, une appliance Citrix ADC est placée entre le client et le serveur, de sorte que le trafic doit passer par l'appliance. Vous devez activer le mode L2 pour le pontage des paquets. Le NSIP et le MIP sont sur le même sous-réseau public, 217.60.10.0/24.

Figure 2. Diagramme topologique pour deux bras, mode transparent



Pour déployer une appliance Citrix ADC en mode transparent à deux bras, procédez comme suit :

1. Configurez le NSIP et la passerelle par défaut, comme décrit dans Configuration de l'adresse IP NetScaler (NSIP).
2. Activez le mode L2, comme décrit dans Activation et désactivation du mode de couche 2.
3. Configurez la Gateway par défaut des serveurs gérés en tant que MIP.

4. Connectez les interfaces réseau aux ports appropriés du commutateur.

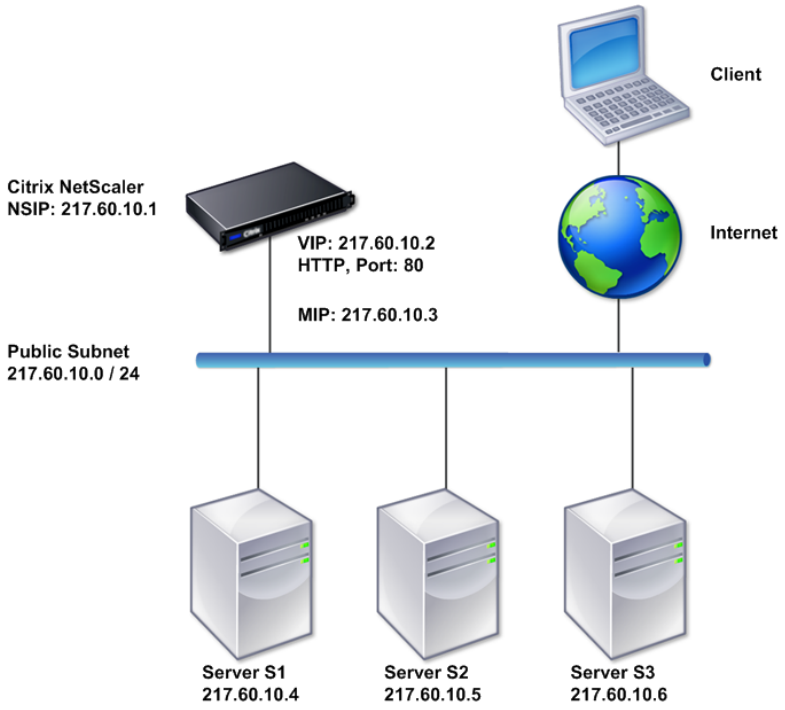
Configurer des topologies communes à un bras

Les deux variantes de base de la topologie à un seul bras sont celles d'un seul sous-réseau et de plusieurs sous-réseaux.

Configurer une topologie de sous-réseau simple à un bras

Vous pouvez utiliser une topologie à un bras avec un seul sous-réseau lorsque les clients et les serveurs résident sur le même sous-réseau. Par exemple, considérez une appliance Citrix ADC déployée en mode monobras pour la gestion des serveurs S1, S2 et S3. Un serveur virtuel de type HTTP est configuré sur une appliance ADC et les services HTTP s'exécutent sur les serveurs. Comme indiqué dans la figure suivante, l'adresse IP Citrix ADC (NSIP), l'adresse IP mappée (MIP) et les adresses IP du serveur se trouvent sur le même sous-réseau public, 217.60.10.0/24.

Figure 3. Diagramme de topologie pour le mode à un bras, sous-réseau unique



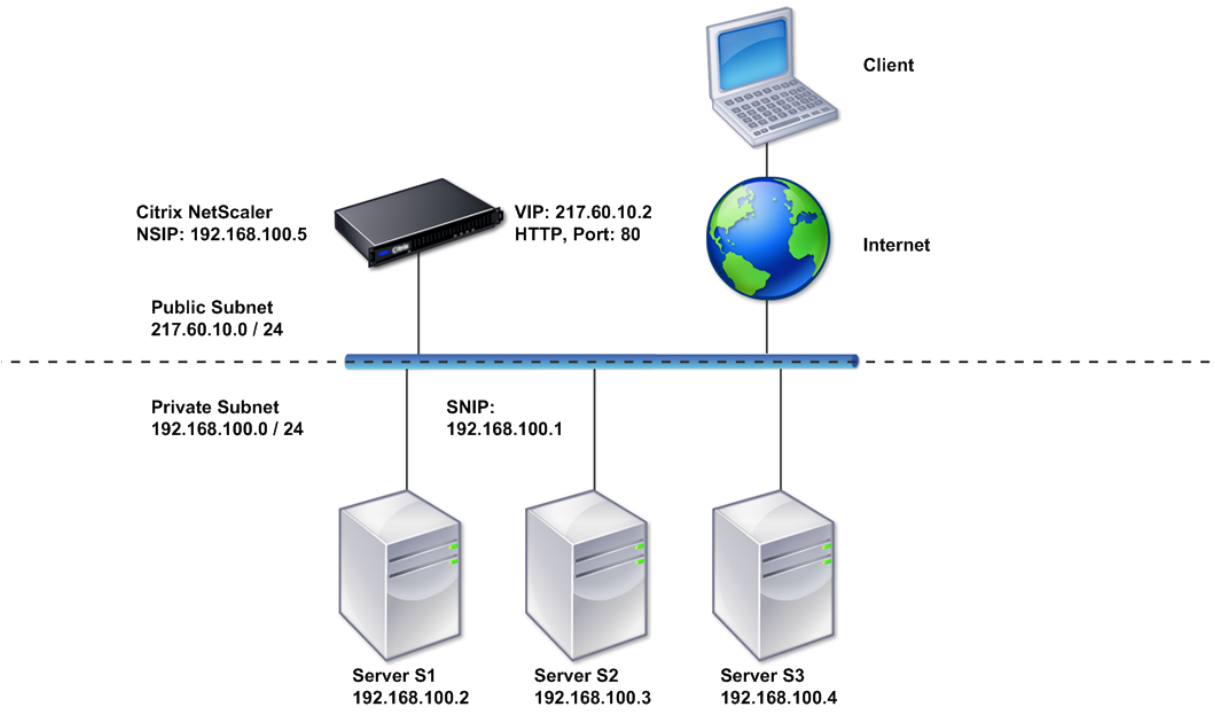
Pour déployer une appliance Citrix ADC en mode monobras avec un seul sous-réseau, procédez comme suit :

1. Configurez le NSIP et la passerelle par défaut, comme décrit dans la section Configuration de l'adresse IP Citrix ADC (NSIP).
2. Configurez le serveur virtuel et les services, comme décrit dans la section Création d'un serveur virtuel et la section Configuration des services .
3. Connectez l'une des interfaces réseau au commutateur.

Configuration d'une topologie de sous-réseau simple à un bras multiple

Vous pouvez utiliser une topologie à un bras avec plusieurs sous-réseaux lorsque les clients et les serveurs résident sur les différents sous-réseaux. Par exemple, considérez une appliance Citrix ADC déployée en mode monobras pour gérer les serveurs S1, S2 et S3, avec les serveurs connectés au commutateur SW1 sur le réseau. Un serveur virtuel de type HTTP est configuré sur l'appliance et les services HTTP s'exécutent sur les serveurs. Ces trois serveurs se trouvent sur le sous-réseau privé, donc une adresse IP de sous-réseau (SNIP) est configurée pour communiquer avec eux. L'option Utiliser l'adresse IP du sous-réseau (USNIP) doit être activée pour que l'appliance utilise le SNIP au lieu d'un MIP. Comme le montre la figure suivante, l'adresse IP virtuelle (VIP) se trouve sur le sous-réseau public 217.60.10.0/24 ; les adresses IP NSIP, SNIP et le serveur sont sur le sous-réseau privé 192.168.100.0/24.

Figure 4. Diagramme topologique pour le mode à un bras, plusieurs sous-réseaux



Pour déployer une appliance Citrix ADC en mode à un bras avec plusieurs sous-réseaux, procédez comme suit :

1. Configurez le NSIP et la passerelle par défaut, comme décrit dans Configuration de l'adresse IP NetScaler (NSIP).
2. Configurez le SNIP et activez l'option USNIP, comme décrit dans Configuration des adresses IP de sous-réseau.
3. Configurez le serveur virtuel et les services, comme décrit dans la section Création d'un serveur virtuel et la section Configuration des services .
4. Connectez l'une des interfaces réseau au commutateur.

Paramètres de gestion du système

January 21, 2021

Une fois votre configuration initiale en place, vous pouvez configurer des paramètres pour définir le comportement de l'appliance Citrix ADC et faciliter la gestion des connexions. Vous disposez d'un certain nombre d'options pour gérer les requêtes et les réponses HTTP. Les modes de routage, de pontage et de transfert MAC sont disponibles pour la gestion des paquets non adressés à l'appliance Citrix ADC. Vous pouvez définir les caractéristiques de vos interfaces réseau et agréger les interfaces. Pour éviter les problèmes de synchronisation, vous pouvez synchroniser l'horloge Citrix avec un serveur NTP (Network Time Protocol). L'appliance Citrix ADC peut fonctionner dans différents modes DNS, y compris en tant que serveur de noms de domaine (ADNS) faisant autorité. Vous pouvez configurer SNMP pour la gestion du système et personnaliser la journalisation syslog des événements système. Avant le déploiement, vérifiez que votre configuration est complète et correcte.

Paramètres système

January 21, 2021

La configuration des paramètres système inclut des tâches de base telles que la configuration des ports HTTP pour activer le maintien de la connexion et le déchargement du serveur, la définition du nombre maximal de connexions pour chaque serveur et la définition du nombre maximal de requêtes par connexion. Vous pouvez activer l'insertion d'adresse IP du client pour les situations dans lesquelles une adresse IP proxy ne convient pas, et vous pouvez modifier la version du cookie HTTP.

Vous pouvez également configurer une appliance Citrix ADC pour ouvrir des connexions FTP sur une plage contrôlée de ports plutôt que des ports éphémères pour les connexions de données. Cela

améliore la sécurité, car l'ouverture de tous les ports sur le pare-feu n'est pas sécurisée. Vous pouvez définir la plage entre 1 024 et 64 000.

Avant le déploiement, consultez les listes de vérification pour vérifier votre configuration. Pour configurer les paramètres HTTP et la plage de ports FTP, utilisez l'interface graphique Citrix ADC.

Vous pouvez modifier les types de paramètres HTTP décrits dans le tableau suivant.

Type de paramètre : Informations de port HTTP

Spécifie : les ports HTTP du serveur Web utilisés par vos serveurs gérés. Si vous spécifiez les ports, l'appliance effectue une commutation de demande pour toute demande client dont le port de destination correspond à un port spécifié.

> Remarque : si une demande client entrante n'est pas destinée à un service ou à un serveur virtuel spécifiquement configuré sur l'appliance, le port de destination de la requête doit correspondre à l'un des ports HTTP configurés globalement. Cela permet à l'appliance d'effectuer le maintien de la connexion et le déchargement du serveur.

Type de paramètre : Limites

Spécifie : le nombre maximal de connexions à chaque serveur géré et le nombre maximal de demandes envoyées sur chaque connexion. Par exemple, si vous définissez Max Connections sur 500 et que l'appliance gère trois serveurs, elle peut ouvrir un maximum de 500 connexions à chacun des trois serveurs. Par défaut, l'appliance peut créer un nombre illimité de connexions à l'un des serveurs qu'elle gère. Pour spécifier un nombre illimité de requêtes par connexion, définissez Max Requests sur 0.

> Remarque : Si vous utilisez le serveur HTTP Apache, vous devez définir Max Connections égales à la valeur du paramètre MaxClients dans le fichier httpd.conf Apache. La définition de ce paramètre est facultative pour les autres serveurs Web.

Type de paramètre : Insertion IP du client

Spécifie : Activer/désactiver l'insertion de l'adresse IP du client dans l'en-tête de requête HTTP. Vous pouvez spécifier un nom pour le champ d'en-tête dans la zone de texte adjacente. Lorsqu'un serveur Web géré par une appliance reçoit une adresse IP de sous-réseau, le serveur l'identifie comme adresse IP du client. Certaines applications ont besoin de l'adresse IP du client à des fins de journalisation ou pour déterminer dynamiquement le contenu à desservir par le serveur Web.

Vous pouvez activer l'insertion de l'adresse IP du client réelle dans la requête d'en-tête HTTP envoyée par le client à un, à certains ou à tous les serveurs gérés par l'appliance. Vous pouvez ensuite accéder à l'adresse insérée via une modification mineure du serveur (à l'aide d'un module Apache, d'une interface ISAPI ou d'une interface NSAPI).

Type de paramètre : Version du cookie

Spécifie : la version du cookie HTTP à utiliser lorsque la persistance COOKIEINSERT est configurée sur un serveur virtuel. La version par défaut, la version 0, est le type le plus courant sur Internet. Vous pouvez également spécifier la version 1.

Type de paramètre : Requests/Réponses

Spécifie : Options pour gérer certains types de requêtes et activer/désactiver la journalisation des réponses d'erreur HTTP.

Type de paramètre : Insertion d'en-tête de serveur

Spécifie : Insérer un en-tête de serveur dans les réponses HTTP générées par Citrix ADC.

Pour configurer les paramètres HTTP à l'aide de l'interface graphique, procédez comme suit :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres HTTP**.
3. Dans la boîte de dialogue **Configurer les paramètres HTTP**, spécifiez des valeurs pour certains ou tous les paramètres qui apparaissent sous les en-têtes répertoriés dans le tableau ci-dessus.
4. Cliquez sur **OK**.

Pour définir la plage de ports FTP à l'aide de l'interface graphique, procédez comme suit :

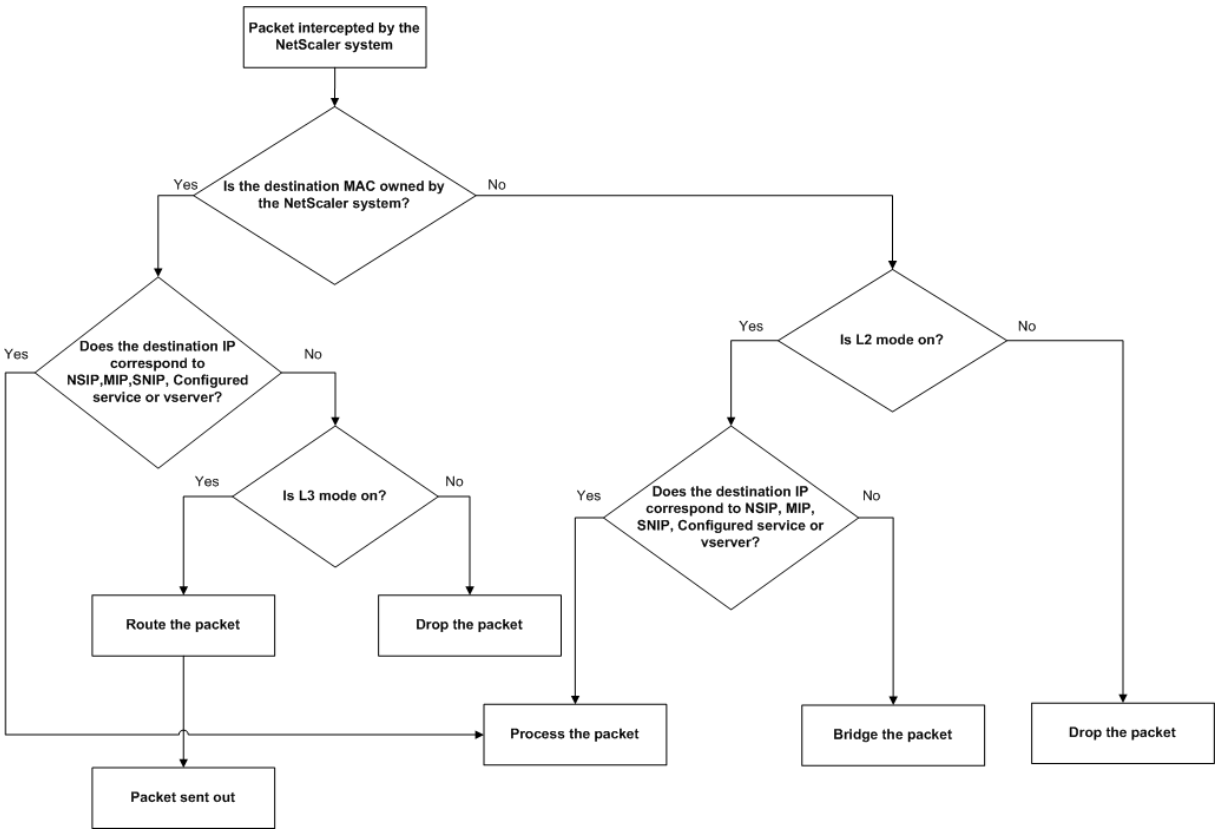
1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres système globaux**.
3. Sous **Plage de ports FTP,** dans les zones de texte **Port de départ** et **Port de fin**, saisissez respectivement les numéros de port le plus bas et le plus élevé pour la plage que vous souhaitez spécifier (par exemple, 5000 et 6000).
4. Cliquez sur **OK**.

Modes de transfert de paquets

January 21, 2021

L'appliance Citrix ADC peut acheminer ou pont des paquets qui ne sont pas destinés à une adresse IP appartenant à l'appliance (c'est-à-dire que l'adresse IP n'est pas le NSIP, un MIP, un SNIP, un service configuré ou un serveur virtuel configuré). Par défaut, le mode L3 (routage) est activé et le mode L2 (pontage) est désactivé, mais vous pouvez modifier la configuration. L'organigramme suivant montre comment l'appliance évalue les paquets et traite, routage, ponts ou abandonne ces paquets.

Figure 1. Interaction entre les modes Couche 2 et Couche 3



Une appliance peut utiliser les modes suivants pour transférer les paquets qu'elle reçoit :

- Mode Couche 2 (L2)
- Mode couche 3 (L3)
- Mode de transfert basé sur Mac

Activer et désactiver le mode couche 2

Le mode Couche 2 contrôle la fonction de transfert de couche 2 (pontage). Vous pouvez utiliser ce mode pour configurer un dispositif Citrix ADC pour qu'il se comporte comme un périphérique de couche 2 et qu'il relie les paquets qui ne lui sont pas destinés. Lorsque ce mode est activé, les paquets ne sont transférés à aucune des adresses MAC, car les paquets peuvent arriver sur n'importe quelle interface de l'appliance et chaque interface possède sa propre adresse MAC.

Lorsque le mode de couche 2 est désactivé (qui est la valeur par défaut), l'appliance supprime les paquets qui ne sont pas destinés à l'une de ses adresses MAC. Si un autre périphérique de couche 2 est installé en parallèle avec l'appliance, le mode de couche 2 doit être désactivé pour éviter le pontage des boucles (couche 2). Vous pouvez utiliser l'utilitaire de configuration ou la ligne de commande pour activer le mode de couche 2.

Remarque : l'appliance ne prend pas en charge le protocole spanning tree. Pour éviter les boucles, si vous activez le mode L2, ne connectez pas deux interfaces de l'appliance au même domaine de

diffusion.

Pour activer ou désactiver le mode de couche 2 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer/désactiver le mode de couche 2 et vérifiez qu'il a été activé/désactivé :

- enable ns mode <Mode>
- disable ns mode <Mode>
- afficher le mode ns

Exemples

```
    > enable ns mode l2
    Done
    > show ns mode

    Mode Acronym Status
    ------- ------- ------
    1) Fast Ramp FR ON
    2) Layer 2 mode L2 ON
    .
    .
    .
    Done
    >

    > disable ns mode l2
    Done
    > show ns mode

    Mode Acronym Status
    ------- ------- ------
    1) Fast Ramp FR ON
    2) Layer 2 mode L2 OFF
    .
    .
    .
    Done
    >
<!--NeedCopy-->
```

Pour activer ou désactiver le mode de couche 2 à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.

2. Dans le volet d'informations, sous **Modes** et **fonctionnalités**, cliquez sur **Configurer les modes**.
3. Dans la boîte de dialogue **Configurer les modes**, pour activer le mode Couche 2, activez la case à cocher **Mode Couche 2**. Pour désactiver le mode Couche 2, désactivez la case à cocher.
4. Cliquez sur **OK**. Le message Activer/désactiver le(s) mode(s) ? s'affiche dans le volet d'informations.
5. Cliquez sur **Yes**.

Activer et désactiver le mode couche 3

Le mode de couche 3 contrôle la fonction de transfert de couche 3. Vous pouvez utiliser ce mode pour configurer une appliance Citrix ADC afin d'examiner sa table de routage et les paquets de transfert qui ne lui sont pas destinés. Lorsque le mode de couche 3 est activé (qui est la valeur par défaut), l'appliance effectue des recherches sur les tables de routage et transmet tous les paquets qui ne sont destinés à aucune adresse IP appartenant à l'appareil. Si vous désactivez le mode de couche 3, l'appliance supprime ces paquets.

Pour activer ou désactiver le mode de couche 3 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer/désactiver le mode de couche 3 et vérifiez qu'il a été activé/désactivé :

- enable ns mode <Mode>
- disable ns mode <Mode>
- afficher le mode ns

Exemples

```
> enable ns mode l3
Done
> show ns mode

Mode Acronym Status
------- ------- ------
1) Fast Ramp FR ON
2) Layer 2 mode L2 OFF
.
.
.
9) Layer 3 mode (ip forwarding) L3 ON
.
.
```



```
15      .
16      Done
17      >
18
19      > disable ns mode l3
20      Done
21      > show ns mode
22
23      Mode Acronym Status
24      ------- ------- ------
25      1) Fast Ramp FR ON
26      2) Layer 2 mode L2 OFF
27      .
28      .
29      .
30      9) Layer 3 mode (ip forwarding) L3 OFF
31      .
32      .
33      .
34      Done
35      >
36  <!--NeedCopy-->
```

Pour activer ou désactiver le mode de couche 3 à l'aide de l'interface graphique

1. Dans le volet de navigation, développez Système, puis cliquez sur Paramètres.
2. Dans le volet d'informations, sous Modes et fonctionnalités, cliquez sur Configurer les modes.
3. Dans la boîte de dialogue Configurer les modes, pour activer le mode de couche 3, activez la case à cocher Mode de couche 3 (transfert IP). Pour désactiver le mode de couche 3, désactivez la case à cocher.
4. Cliquez sur OK. Le message Activer/désactiver le(s) mode(s) ? s'affiche dans le volet d'informations.
5. Cliquez sur Yes.

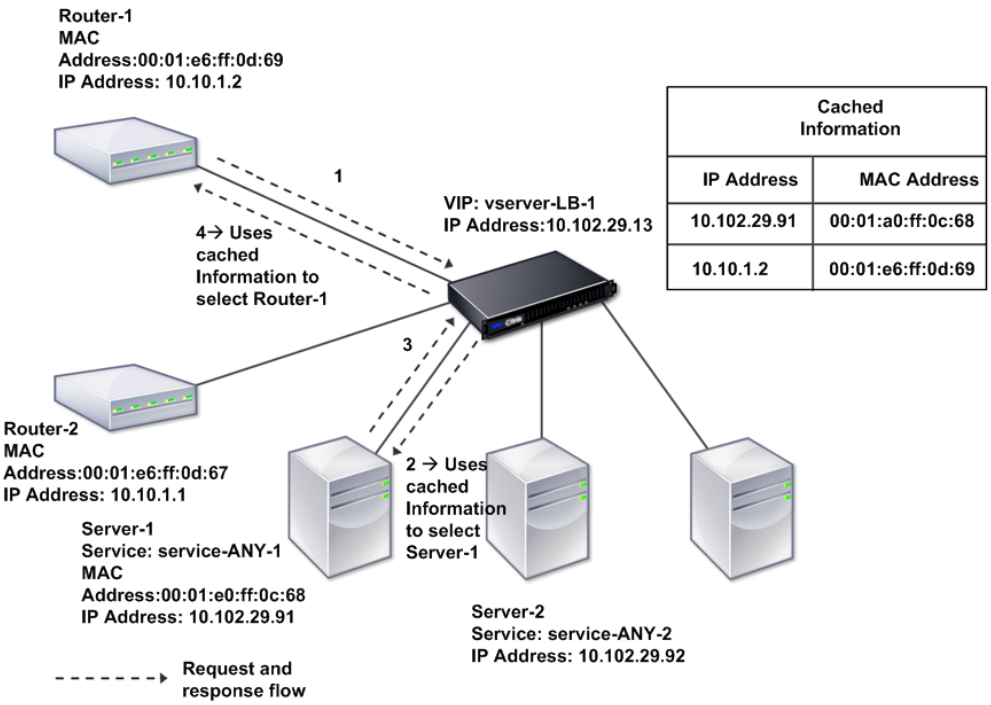
Activer et désactiver le mode de transfert basé sur MAC

Vous pouvez utiliser le transfert basé sur Mac pour traiter le trafic plus efficacement et éviter les recherches ARP ou plusieurs itinéraires lors du transfert de paquets, car l'appliance Citrix ADC se souvient de l'adresse MAC de la source. Pour éviter plusieurs recherches, l'appliance met en cache l'adresse MAC source de chaque connexion pour laquelle elle effectue une recherche ARP et renvoie les données à la même adresse MAC.

Le transfert basé sur Mac est utile lorsque vous utilisez des périphériques VPN car l'appliance garantit que tout le trafic circulant à travers un VPN particulier passe par le même périphérique VPN.

La figure suivante montre le processus de transfert basé sur Mac.

Figure 2. Processus de transfert basé sur Mac



Lorsque le transfert basé sur Mac est activé, l'appliance met en cache l'adresse MAC de :

- Source (un périphérique de transmission tel que routeur, pare-feu ou périphérique VPN) de la connexion entrante.
- Serveur qui répond aux demandes.

Lorsqu'un serveur répond via une appliance, l'appliance définit l'adresse MAC de destination du paquet de réponse sur l'adresse mise en cache, en veillant à ce que le trafic circule de manière symétrique, puis transfère la réponse au client. Le processus contourne les fonctions de recherche de table de routage et de recherche ARP. Toutefois, lorsqu'une appliance initie une connexion, elle utilise les tables de routage et ARP pour la fonction de recherche. Pour activer le transfert basé sur Mac, utilisez l'utilitaire de configuration ou la ligne de commande.

Certains déploiements nécessitent que les chemins entrants et sortants passent par différents routeurs. Dans ces situations, le transfert basé sur Mac rompt la conception de la topologie. Pour un site GSLB (Global Server Load Balancing) qui nécessite que les chemins entrants et sortants passent par

différents routeurs, vous devez désactiver le transfert basé sur Mac et utiliser le routeur par défaut de l'appliance comme routeur sortant.

Lorsque le transfert basé sur Mac est désactivé et que la connectivité de couche 2 ou de couche 3 est activée, une table de routage peut spécifier des routeurs distincts pour les connexions sortantes et entrantes. Pour désactiver le transfert basé sur Mac, utilisez l'utilitaire de configuration ou la ligne de commande.

Pour activer ou désactiver le transfert basé sur Mac à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer/désactiver le mode de transfert basé sur Mac et vérifier qu'il a été activé/désactivé :

- <enable ns mode <Mode>
- <disable ns mode <Mode>
- <show ns mode
  Example

  "' pre codeblock

  ```
  enable ns mode mbf
  Done
  show ns mode
  ```

  ```
  1   Mode                          Acronym           Status
  2   -------                       -------           ------   1)  Fast
      Ramp                     FR                ON   2)  Layer 2
      mode                  L2                OFF   .   .   .   6)
      MAC-based forwarding        MBF               ON   .   .   .
        Done  >
  ```

  ```
  disable ns mode mbf
  Done
  show ns mode
  ```

  ```
  1   Mode                          Acronym           Status
  2   -------                       -------           ------   1)  Fast
      Ramp                     FR                ON   2)  Layer 2
      mode                  L2                OFF   .   .   .   6)
      MAC-based forwarding        MBF               OFF   .   .   .
         Done  >  <!--NeedCopy--> ```
  ```

Pour activer ou désactiver le transfert basé sur Mac à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Dans le volet d'informations, sous Groupe **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.
3. Dans la boîte de dialogue **Configurer les modes**, pour activer le mode de transfert basé sur **Mac, activez la case à cocher Transfert basé sur MAC**. Pour désactiver le mode de transfert basé sur Mac, désactivez la case à cocher.
4. Cliquez sur **OK**. Le message Activer/désactiver le(s) mode(s) ? s'affiche dans le volet d'informations.
5. Cliquez sur **Yes**.

Interfaces réseau

August 20, 2021

Les interfaces Citrix ADC sont numérotées en notation slot/port. Outre la modification des caractéristiques des interfaces individuelles, vous pouvez configurer des réseaux locaux virtuels pour limiter le trafic à des groupes d'hôtes spécifiques. Vous pouvez également agréger des liaisons dans des canaux à grande vitesse.

LAN virtuels

L'appliance Citrix ADC prend en charge le port (couche 2) et les réseaux locaux virtuels (VLAN) balisés IEEE802.1Q. Les configurations VLAN sont utiles lorsque vous devez restreindre le trafic à certains groupes de stations. Vous pouvez configurer une interface réseau pour appartenir à plusieurs VLAN à l'aide du balisage IEEE 802.1q.

Vous pouvez lier vos VLAN configurés à des sous-réseaux IP. L'appliance ADC (si elle est configurée comme routeur par défaut pour les hôtes des sous-réseaux) effectue alors le transfert IP entre ces VLAN.

L'appliance Citrix ADC prend en charge les types de VLAN suivants.

- VLAN par défaut

  Par défaut, les interfaces réseau d'une appliance Citrix ADC sont incluses dans un seul VLAN basé sur un port en tant qu'interfaces réseau non marquées. Ce VLAN par défaut a un VID de 1 et existe de façon permanente. Il ne peut pas être supprimé et son VID ne peut pas être modifié.

- VLAN basés sur des ports

  Un ensemble d'interfaces réseau qui partagent un domaine de diffusion de couche 2 commun et exclusif définissent l'appartenance à un VLAN basé sur un port. Vous pouvez configurer

plusieurs VLAN basés sur des ports. Lorsque vous ajoutez une interface à un nouveau VLAN en tant que membre non marqué, elle est automatiquement supprimée du VLAN par défaut.

- VLAN taggé

  Une interface réseau peut être un membre balisé ou non marqué d'un VLAN. Chaque interface réseau est un membre non marqué d'un seul VLAN (son VLAN natif). L'interface réseau non marquée transmet les trames du VLAN natif en tant que trames non balisées. Une interface réseau balisée peut faire partie de plus d'un VLAN. Lorsque vous configurez le balisage, assurez-vous que les deux extrémités du lien ont des paramètres VLAN correspondants. Vous pouvez utiliser l'utilitaire de configuration pour définir un VLAN balisé (nsvlan) qui peut avoir des ports liés en tant que membres balisés du VLAN. La configuration de ce VLAN nécessite un redémarrage de l'appliance ADC et doit donc être effectuée lors de la configuration réseau initiale.

Lier les canaux d'agrégation

L'agrégation de liens combine les données entrantes provenant de plusieurs ports en une seule liaison haute vitesse. La configuration du canal d'agrégation de liaison augmente la capacité et la disponibilité du canal de communication entre une appliance Citrix ADC et d'autres périphériques connectés. Un lien agrégé est également appelé canal.

Lorsqu'une interface réseau est liée à un canal, les paramètres du canal ont priorité sur les paramètres de l'interface réseau. Une interface réseau peut être liée à un seul canal. La liaison d'une interface réseau à un canal d'agrégation de liaison modifie la configuration du VLAN. Autrement dit, la liaison des interfaces réseau à un canal les supprime des VLAN auxquels elles appartenaient à l'origine et les ajoute au VLAN par défaut. Toutefois, vous pouvez lier le canal à l'ancien VLAN, ou à un nouveau. Par exemple, si vous avez des interfaces réseau 1/2 et 1/3 liées à un VLAN avec ID 2, puis que vous les liez pour lier le canal agrégé LA/1, les interfaces réseau sont déplacées vers le VLAN par défaut, mais vous pouvez les lier au VLAN 2.

Remarque : Vous pouvez également utiliser le protocole LACP (Link Aggregation Control Protocol) pour configurer l'agrégation de liens. Pour plus d'informations, voir Configuration de l'agrégation de liens à l'aide du protocole de contrôle d'agrégation de liens.

Synchronisation de l'horloge

January 21, 2021

Vous pouvez configurer votre appliance Citrix ADC pour synchroniser son horloge locale avec un serveur NTP (Network Time Protocol). Cela garantit que son horloge a les mêmes paramètres de date et d'heure que les autres serveurs de votre réseau. NTP utilise le port UDP (User Datagram

Protocol) 123 comme couche de transport. Vous devez ajouter des serveurs NTP dans le fichier de configuration NTP afin que l'appliance reçoive périodiquement des mises à jour à partir de ces serveurs.

Si vous n'avez pas de serveur NTP local, vous pouvez trouver une liste de serveurs NTP publics à accès libre sur le site NTP officiel à l'adresse http://www.ntp.org.

Pour configurer la synchronisation d'horloge sur votre appliance, procédez comme suit :

1. Connectez-vous à la ligne de commande et entrez la commande shell.
2. À l'invite du shell, copiez le fichier ntp.conf du répertoire /etc dans le répertoire /nsconfig. Si le fichier existe déjà dans le répertoire /nsconfig, assurez-vous de supprimer les entrées suivantes du fichier ntp.conf :

   ```
   restrict localhost

   restrict 127.0.0.2
   ```

   Ces entrées sont obligatoires uniquement si vous souhaitez exécuter le périphérique en tant que serveur de temps. Toutefois, cette fonctionnalité n'est pas prise en charge sur l'appliance Citrix ADC.
3. Modifiez /nsconfig/ntp.conf en tapant l'adresse IP du serveur NTP souhaité sous le serveur du fichier et limitez les entrées.
4. Créez un fichier nommé rc.netscaler dans le répertoire /nsconfig, si le fichier n'existe pas déjà dans le répertoire.
5. Modifiez /nsconfig/rc.netscaler en ajoutant l'entrée suivante : `/usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ntpd.log &`

   Cette entrée démarre le service ntpd, vérifie le fichier ntp.conf et consigne les messages dans le répertoire /var/log.

   Remarque : Si la différence de temps entre l'appliance Citrix ADC et le serveur de temps est supérieure à 1000 s, le service ntd se termine par un message au journal ADC. Pour éviter cela, vous devez démarrer ntpd avec l'option -g, qui synchronise de force l'heure. Ajoutez l'entrée suivante dans /nsconfig/rc.netscaler :

   ```
   /usr/sbin/ntpd -g -c /nsconfig/ntp.conf -l /var/log/ntpd.log &
   ```

   Si vous ne voulez pas synchroniser de force l'heure lorsqu'il y a une grande différence, vous pouvez définir la date manuellement, puis recommencer ntpd. Vous pouvez vérifier la différence de temps entre l'appliance et le serveur de temps en exécutant la commande suivante dans l'interpréteur de commandes :

   ```
   1 ntpdate -q <IP address or domain name of the NTP server>
   2 <!--NeedCopy-->
   ```


6. Redémarrez l'appliance pour activer la synchronisation de l'horloge.

   Remarque : si vous souhaitez démarrer la synchronisation de l'heure avant de redémarrer l'appliance, entrez la commande suivante (que vous avez ajoutée au fichier rc.netscaler à l'étape 5) à l'invite du shell :

```
1 /usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ ntpd.log &
2 <!--NeedCopy-->
```

Configuration DNS

January 21, 2021

Vous pouvez configurer une appliance Citrix ADC pour qu'elle fonctionne comme un serveur de noms de domaine faisant autorité (ADNS), un serveur proxy DNS, un résolveur de fin ou un redirecteur. Vous pouvez ajouter des enregistrements de ressources DNS tels que des enregistrements SRV, des enregistrements AAAA, des enregistrements A, des enregistrements MX, des enregistrements NS, des enregistrements CNAME, des enregistrements PTR et des enregistrements SOA. En outre, l'appliance peut équilibrer la charge sur les serveurs DNS externes.

Une pratique courante consiste à configurer une appliance en tant que redirecteur. Pour cette configuration, vous devez ajouter des serveurs de noms externes. Après avoir ajouté les serveurs externes, vous devez vérifier que votre configuration est correcte.

Vous pouvez ajouter, supprimer, activer et désactiver des serveurs de noms externes. Vous pouvez créer un serveur de noms en spécifiant son adresse IP ou configurer un serveur virtuel existant en tant que serveur de noms.

Lors de l'ajout de serveurs de noms, vous pouvez spécifier des adresses IP ou des adresses IP virtuelles (VIP). Si vous utilisez des adresses IP, l'appliance équilibre les demandes adressées aux serveurs de noms configurés de manière ronde. Si vous utilisez des VIP, vous pouvez spécifier n'importe quelle méthode d'équilibrage de charge.

Ajouter un serveur de noms à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un serveur de noms et vérifier la configuration :

- <add dns nameServer <IP>
- <show dns nameServer <IP>

  Exemple

“‘ pre codeblock

```
add dns nameServer 10.102.29.10
Done
show dns nameServer 10.102.29.10
1) 10.102.29.10 - State: DOWN
Done
```

“‘

Ajouter un serveur de noms à l’aide de l’interface graphique

1. Accédez à **Gestion du trafic** > **DNS** > **Serveurs de noms**.
2. Dans le volet d’informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un serveur de noms**, sélectionnez **Adresse IP**.
4. Dans la zone de texte **Adresse IP**, tapez l’adresse IP du serveur de noms (par exemple, 10.102.29.10). Si vous ajoutez un serveur de noms externe, désactivez la case à cocher **Local** .
5. Cliquez sur **Créer**, puis sur **Fermer**.
6. Vérifiez que le serveur de noms que vous avez ajouté s’affiche dans le volet **Serveurs de noms** .

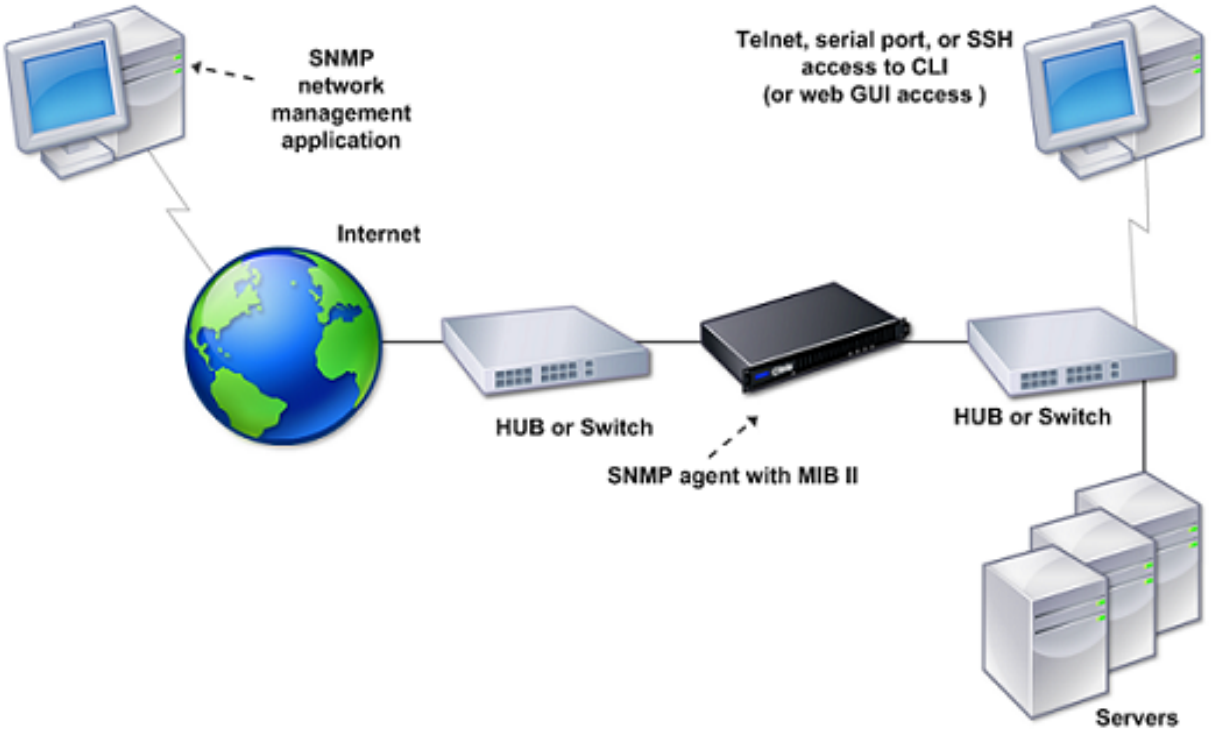
Configuration SNMP

August 20, 2021

L’application de gestion réseau SNMP (Simple Network Management Protocol), exécutée sur un ordinateur externe, interroge l’agent SNMP sur l’appliance Citrix ADC. L’agent recherche dans la base d’informations de gestion (MIB) les données demandées par l’application de gestion réseau et envoie les données à l’application.

La surveillance SNMP utilise des messages d’interruptions et des alarmes. Les messages d’interruptions SNMP sont des événements asynchrones que l’agent génère pour signaler des conditions anormales, qui sont indiqués par des alarmes. Par exemple, si vous souhaitez être informé lorsque l’utilisation du processeur est supérieure à 90 %, vous pouvez configurer une alarme pour cette condition. La figure suivante illustre un réseau doté d’une appliance Citrix ADC sur laquelle SNMP est activé et configuré.

Figure 1. SNMP sur l’appliance Citrix ADC



L'agent SNMP sur une appliance Citrix ADC prend en charge SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2) et SNMP version 3 (SNMPv3). Comme il fonctionne en mode bilingue, l'agent peut gérer les requêtes SNMPv2, telles que Get-Bulk, et SNMPv1. L'agent SNMP envoie également des interruptions conformes à SNMPv2 et prend en charge les types de données SNMPv2, tels que counter64. Les gestionnaires SNMPv1 (programmes sur d'autres serveurs qui demandent des informations SNMP à l'appliance ADC) utilisent le fichier NS-MIB-SMIV1.mib lors du traitement des requêtes SNMP. Les gestionnaires SNMPv2 utilisent le fichier NS-MIB-SMIV2.mib.

L'appliance Citrix ADC prend en charge les MIB spécifiques à l'entreprise suivantes :

- Sous-ensemble de groupes MIB-2 standard. Fournit des groupes MIB-2 SYSTEM, IF, ICMP, UDP et SNMP.
- Un MIB d'entreprise système. Fournit une configuration et des statistiques spécifiques au système.

Pour configurer SNMP, vous spécifiez les gestionnaires qui peuvent interroger l'agent SNMP, ajouter des écouteurs d'interruption SNMP qui recevront les messages d'interruption SNMP et configurer les alarmes SNMP.

Ajouter des gestionnaires SNMP

Vous pouvez configurer une station de travail exécutant une application de gestion conforme à la version 1, 2 ou 3 de SNMP pour accéder à une appliance. Un tel poste de travail est appelé gestionnaire SNMP. Si vous ne spécifiez pas de gestionnaire SNMP sur l'appliance, celle-ci accepte les requêtes

SNMP provenant de toutes les adresses IP du réseau et y répond. Si vous configurez un ou plusieurs gestionnaires SNMP, l'appliance accepte les requêtes SNMP à partir de ces adresses IP spécifiques et y répond. Lorsque vous spécifiez l'adresse IP d'un gestionnaire SNMP, vous pouvez utiliser le paramètre netmask pour accorder l'accès à partir de sous-réseaux entiers. Vous pouvez ajouter un maximum de 100 gestionnaires ou réseaux SNMP. Pour ajouter un gestionnaire SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un gestionnaire SNMP et vérifier la configuration :

```
add snmp manager <IPAddress> ... [-netmask <netmask>]
show snmp manager <IPAddress>
```

Exemple :

```
1 add snmp manager 10.102.29.5 -netmask 255.255.255.255
2 Done
3 show snmp manager 10.102.29.5
4 10.102.29.5 255.255.255.255
5 Done
6 <!--NeedCopy-->
```

Pour ajouter un gestionnaire SNMP à l'aide de l'interface graphique :

1. Dans le volet de navigation, développez **Système**, développez **SNMP**, puis cliquez sur **Gestionnaires**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un gestionnaire SNMP**, dans la zone de texte **Adresse IP**, tapez l'adresse IP de la station de travail exécutant l'application de gestion (par exemple, 10.102.29.5).
4. Cliquez sur **Créer**, puis sur **Fermer**.
5. Vérifiez que le gestionnaire SNMP que vous avez ajouté apparaît dans la section **Détails** en bas du volet.

Ajouter des écouteurs SNMP interruptions

Après avoir configuré les alarmes, vous devez spécifier l'écouteur d'interruption auquel l'appliance enverra les messages d'interruption. Outre la spécification de paramètres tels que l'adresse IP et le port de destination de l'écouteur d'interruption, vous pouvez spécifier le type d'interruption (générique ou spécifique) et la version SNMP.

Vous pouvez configurer un maximum de 20 écouteurs d'interruptions pour recevoir des interruptions génériques ou spécifiques.

Pour ajouter un écouteur d'interruption SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour ajouter une interruption SNMP et vérifier qu'elle a été ajoutée :

- `add snmp trap specific <IP>`
- `show snmp trap`

Exemple :

```
1 Trap type: SPECIFIC
2 Destination IP: 10.102.29.3
3 TD: 0
4 Destination Port: 162
5 Source IP: NetScaler IP
6 Version: V2
7 Min-Severity: -
8 AllPartition: DISABLED
9 Community: public
10 <!--NeedCopy-->
```

Pour ajouter un écouteur d'interruption SNMP à l'aide de l'interface graphique

1. Dans le volet de navigation, développez Système, développez **SNMP**, puis cliquez sur **interruptions**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une destination d'interruption SNMP**, dans la zone de texte **Adresse IP de destination**, tapez l'adresse IP (par exemple, 10.102.29.3).
4. Cliquez sur **Create**, puis cliquez sur **Close**.
5. Vérifiez que l'interruption SNMP que vous avez ajoutée s'affiche dans la section **Détails** en bas du volet.

Configurer les alarmes SNMP

Vous configurez les alarmes de sorte que l'appliance génère un message d'interruption lorsqu'un événement correspondant à l'une des alarmes se produit. La configuration d'une alarme consiste à activer l'alarme et à définir le niveau de gravité auquel une interruption est générée. Il existe cinq niveaux de gravité : Critique, Major, Mineure, Avertissement et Information. Une interruption n'est envoyée que lorsque la gravité de l'alarme correspond à la gravité spécifiée pour l'interruption.

Certaines alarmes sont activées par défaut. Si vous désactivez une alarme SNMP, l'appliance ne génère pas de messages d'interruption lorsque des événements correspondants se produisent.

Par exemple, si vous désactivez l'alarme SNMP d'échec de connexion, l'appliance ne génère pas de message d'interruption en cas d'échec de connexion.

Pour activer ou désactiver une alarme à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver une alarme et vérifier qu'elle a été activée ou désactivée :

- set snmp alarm <trapName> [-state ENABLED | DISABLED]
- show snmp alarm <trapName>

Exemple

```
set snmp alarm LOGIN-FAILURE -state ENABLED
Done
show snmp alarm LOGIN-FAILURE
Alarm Alarm Threshold Normal Threshold Time State Severity Logging
----- --------------- ---------------- ---- -------- --------- --------
LOGIN-FAILURE N/A N/A N/A ENABLED - ENABLED
Done
<!--NeedCopy-->
```

Pour définir la gravité de l'alarme à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir la gravité de l'alarme et vérifier que la gravité a été correctement définie :

- set snmp alarm <trapName> [-severity <severity>]
- show snmp alarm <trapName>

Exemple :

```
set snmp alarm LOGIN-FAILURE -severity Major
Done
show snmp alarm LOGIN-FAILURE
Alarm Alarm Threshold Normal Threshold Time State Severity Logging
----- --------------- ---------------- ---- -------- --------- --------
LOGIN-FAILURE N/A N/A N/A ENABLED Major ENABLED
Done
<!--NeedCopy-->
```

Pour configurer les alarmes à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, SNMP, puis cliquez sur **Alarmes**.

2. Dans le volet d'informations, sélectionnez une alarme (par exemple, ÉCHEC DE CONNEXION), puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer l'alarme SNMP**, pour activer l'alarme, sélectionnez Activé dans la liste déroulante **État**. Pour désactiver l'alarme, sélectionnez Désactivé.
4. Dans la liste déroulante **Gravité**, sélectionnez une option de gravité (par exemple, Major).
5. Cliquez sur **OK**, puis sur **Fermer**.
6. Vérifiez que les paramètres de l'alarme SNMP que vous avez configuré sont correctement configurés en affichant la section **Détails** en bas du volet.

Vérifier la configuration

January 21, 2021

Une fois que vous avez terminé la configuration de votre système, complétez les listes de vérification suivantes pour vérifier votre configuration.

Liste de vérification de la configuration

- La construction en cours d'exécution est :
- Il n'y a aucun problème d'incompatibilité. (Les problèmes d'incompatibilité sont documentés dans les notes de publication de la version.)
- Les paramètres de port (vitesse, duplex, contrôle de flux, surveillance) sont les mêmes que le port du commutateur.
- Une quantité suffisante d'adresses IP SNIP a été configurée pour prendre en charge toutes les connexions côté serveur pendant les heures de pointe.
  - Le nombre d'adresses IP SNIP configurées est:__
  - Le nombre attendu de connexions serveur simultanées est :
    [] 62 000 [] 124 000 [] Autres __

Liste de contrôle de la configuration de la topologie

Les routes ont été utilisées pour résoudre des serveurs sur d'autres sous-réseaux.

Les itinéraires entrés sont :

- Si l'appliance Citrix ADC se trouve dans une topologie public-privé, NAT inverse a été configuré.
- Les paramètres de basculement (haute disponibilité) configurés sur l'appliance ADC résolvent dans une configuration à un ou deux bras. Toutes les interfaces réseau inutilisées ont été désactivées :

_____

- Si l'appliance ADC est placée derrière un équilibreur de charge externe, la stratégie d'équilibrage de charge sur l'équilibreur de charge externe n'est pas la « connexion minimale ».

  La stratégie d'équilibrage de charge configurée sur l'équilibreur de charge externe est la suivante :

  _____

- Si l'appliance ADC est placée devant un pare-feu, le délai d'expiration de la session sur le pare-feu est défini sur une valeur supérieure ou égale à 300 secondes.

  Remarque : Le délai d'expiration de la connexion TCP inactive sur une appliance Citrix ADC est de 360 secondes. Si le délai d'expiration du pare-feu est également défini sur 300 secondes ou plus, l'appliance peut effectuer efficacement le multiplexage des connexions TCP, car les connexions ne seront pas fermées plus tôt.

  La valeur configurée pour le délai d'expiration de la session est : _____

Liste de vérification de la configuration du serveur

- « Keep-alive » a été activé sur tous les serveurs.

  La valeur configurée pour le délai d'expiration Keep-alive est : _____

- La Gateway par défaut a été définie sur la valeur correcte. (La Gateway par défaut doit être une appliance Citrix ADC ou un routeur en amont.) La Gateway par défaut est :

  _____

- Les paramètres du port du serveur (vitesse, duplex, contrôle du flux, surveillance) sont les mêmes que les paramètres du port du commutateur.

  _____

- Si Microsoft® Internet Information Server est utilisé, la mise en mémoire tampon est activée sur le serveur.
- Si un serveur Apache est utilisé, le paramètre MaxConn (nombre maximal de connexions) est configuré sur le serveur et sur l'appliance Citrix ADC.

  La valeur MaxConn (nombre maximal de connexions) qui a été définie est la suivante :

  _____

- Si un serveur Netscape Enterprise est utilisé, le nombre maximal de requêtes par paramètre de connexion est défini sur l'appliance Citrix ADC. La valeur maximale des requêtes par connexion définie est la suivante :

  _____

Liste de vérification de la configuration des fonctionnalités logicielles

- La fonction mode Couche 2 doit-elle être désactivée ? (Désactiver si un autre périphérique de couche 2 fonctionne en parallèle avec une appliance Citrix ADC.)

  Raison de l'activation ou de la désactivation :

  _____

- La fonction de transfert basé sur Mac doit-elle être désactivée ? (Si l'adresse MAC utilisée par le trafic de retour est différente, elle doit être désactivée.)

  Raison de l'activation ou de la désactivation :

  _____

- La réutilisation basée sur l'hôte doit-elle être désactivée ? (Y a-t-il un hébergement virtuel sur les serveurs ?)

  Raison de l'activation ou de la désactivation :

  _____

- Est-ce que les paramètres par défaut de la fonction de protection contre les surtensions doivent être modifiés ?

  Raison de la modification ou de la non-modification :

  _____

Liste de contrôle d'accès

- Les adresses IP du système peuvent être ping à partir du réseau côté client.
- Les adresses IP système peuvent être ping à partir du réseau côté serveur.
- Le (s) serveur (s) géré (s) peut (s) être (s) pingé (s) via Citrix ADC.
- Les hôtes Internet peuvent être pingés à partir des serveurs gérés.
- Le ou les serveurs gérés sont accessibles via le navigateur.
- Vous pouvez accéder à Internet à partir du ou des serveurs gérés à l'aide du navigateur.
- Le système est accessible en utilisant SSH.
- L'accès de l'administrateur à tous les serveurs gérés fonctionne.

> Remarque : Lorsque vous utilisez l'utilitaire ping, assurez-vous que ICMP ECHO est activé sur le serveur ping, sinon votre ping ne réussira pas.

Liste de contrôle du pare-feu

Les exigences de pare-feu suivantes ont été respectées :

- UDP 161 (SNMP)
- UDP 162 (interruptions SNMP)
- TCP/UDP 3010 (INTERFACE GRAPHIQUE)
- HTTP 80 (GUI)
- TCP 22 (SSH)

Trafic d'équilibrage de charge sur une appliance Citrix ADC

January 21, 2021

La fonction d'équilibrage de charge distribue les demandes des clients sur plusieurs serveurs afin d'optimiser l'utilisation des ressources. Dans un scénario réel où un nombre limité de serveurs fournissent un service à un grand nombre de clients, un serveur peut être surchargé et dégrader les performances de la batterie de serveurs. Une appliance Citrix ADC utilise des critères d'équilibrage de charge pour éviter les goulots d'étranglement en transférant chaque requête client au serveur le mieux adapté à la gestion de la demande lorsqu'elle arrive.

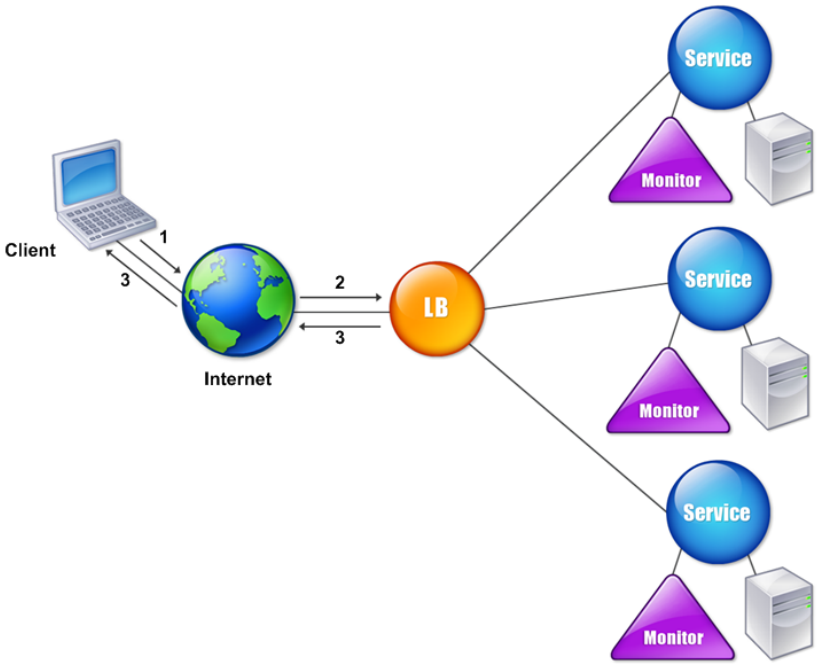
Pour configurer l'équilibrage de charge, vous définissez un serveur virtuel pour proxy de plusieurs serveurs dans une batterie de serveurs et équilibrez la charge entre eux.

Lorsqu'un client initie une connexion au serveur, un serveur virtuel met fin à la connexion client et initie une nouvelle connexion avec le serveur sélectionné, ou réutilise une connexion existante avec le serveur, pour effectuer l'équilibrage de charge. La fonction d'équilibrage de charge assure la gestion du trafic de la couche 4 (TCP et UDP) à la couche 7 (FTP, HTTP et HTTPS).

L'appliance Citrix ADC utilise un certain nombre d'algorithmes, appelés méthodes d'équilibrage de charge, pour déterminer comment répartir la charge entre les serveurs. La méthode d'équilibrage de charge par défaut est la méthode Moins de connexions.

Un déploiement d'équilibrage de charge standard comprend les entités décrites dans la figure suivante.

Figure 1. Architecture d'équilibrage de charge



Les entités fonctionnent comme suit :

- **Serveur virtuel**. Entité représentée par une adresse IP, un port et un protocole. L'adresse IP du serveur virtuel (VIP) est généralement une adresse IP publique. Le client envoie des demandes de connexion à cette adresse IP. Le serveur virtuel représente une banque de serveurs.
- **Service**. Représentation logique d'un serveur ou d'une application s'exécutant sur un serveur. Identifie l'adresse IP du serveur, un port et un protocole. Les services sont liés aux serveurs virtuels.
- **Objet serveur**. Entité représentée par une adresse IP. L'objet serveur est créé lorsque vous créez un service. L'adresse IP du service est prise comme nom de l'objet serveur. Vous pouvez également créer un objet serveur, puis créer des services à l'aide de l'objet serveur.
- **Moniteur**. Entité qui suit l'état des services. L'appliance sonde périodiquement les serveurs à l'aide du moniteur lié à chaque service. Si un serveur ne répond pas dans un délai de réponse spécifié et que le nombre de sondes spécifié échoue, le service est marqué comme DOWN. L'appliance effectue ensuite l'équilibrage de la charge entre les services restants.

Équilibrage de charge

August 20, 2021

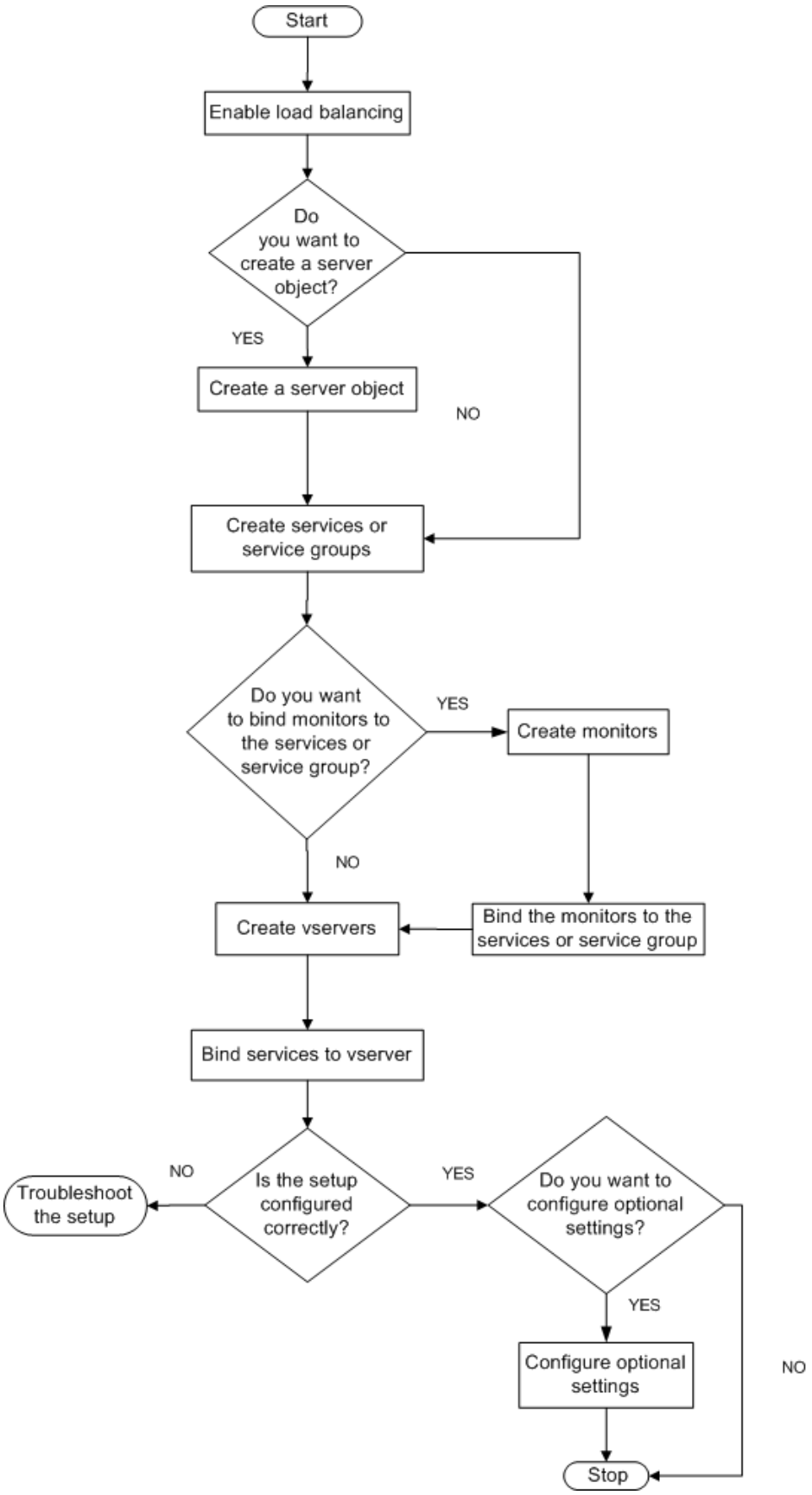
Pour configurer l'équilibrage de charge, vous devez d'abord créer des services. Ensuite, vous créez des serveurs virtuels et liez les services aux serveurs virtuels. Par défaut, l'appliance Citrix ADC lie un moniteur à chaque service. Après avoir lié les services, vérifiez votre configuration en vous assurant que tous les paramètres sont corrects.

> Remarque : Après avoir déployé la configuration, vous pouvez afficher des statistiques indiquant le fonctionnement des entités de la configuration. Utilisez l'utilitaire statistique ou la <vserverName> commande
> stat lb vserver.

Le cas échéant, vous pouvez affecter des pondérations à un service. La méthode d'équilibrage de charge utilise ensuite le poids attribué pour sélectionner un service. Toutefois, pour commencer, vous pouvez limiter les tâches facultatives à la configuration de certains paramètres de persistance de base, pour les sessions qui doivent maintenir une connexion à un serveur particulier, et certains paramètres de configuration de base de protection.

L'organigramme suivant illustre la séquence des tâches de configuration.

Figure 1. Séquence de tâches pour configurer l'équilibrage de charge



Activer l'équilibrage de charge

Avant de configurer l'équilibrage de charge, assurez-vous que la fonction d'équilibrage de charge est activée.

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer l'équilibrage de charge et vérifier qu'il est activé :

- enable feature lb
- Afficher la fonctionnalité

  Exemple

  "‘ pre codeblock

  ```
  enable feature lb
  Done
  show feature
  ```

  ```
  1   Feature                  Acronym          Status
  2   -------                  -------          ------   1)  Web
      Logging                WL               OFF   2)  Surge
      Protection           SP               OFF   3)  Load Balancing
                LB               ON   .   .   .   9)  SSL
      Offloading             SSL              ON   .   .   .  Done
      <!--NeedCopy--> ```
  ```

Pour activer l'équilibrage de charge à l'aide de l'interface graphique

1. Dans le volet de navigation, développez Système, puis cliquez sur Paramètres.
2. Dans le volet d'informations, sous Modes et fonctionnalités, cliquez sur Modifier les fonctionnalités de base.
3. Dans la boîte de dialogue Configurer les fonctionnalités de base, activez la case à cocher Équilibrage de charge, puis cliquez sur OK.
4. Dans la ou les fonctions Activer/Désactiver ?, cliquez sur Oui.

Configurer des services et un serveur virtuel

Lorsque vous avez identifié les services que vous souhaitez équilibrer la charge, vous pouvez implémenter votre configuration initiale d'équilibrage de charge en créant les objets de service, en créant un serveur virtuel d'équilibrage de charge et en liant les objets de service au serveur virtuel.

Pour implémenter la configuration d'équilibrage de charge initiale à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour implémenter et vérifier la configuration initiale :

- <add service <name> <IPaddress> <serviceType> <port>
- <add lb vserver <vServerName> <serviceType> [<IPaddress> <port>]
- <bind lb vserver <name> <serviceName>
- <show service bindings <serviceName>

Exemple

```
> add service service-HTTP-1 10.102.29.5 HTTP 80
 Done
> add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
 Done
> bind lb vserver vserver-LB-1 service-HTTP-1
 Done
> show service bindings service-HTTP-1
    service-HTTP-1 (10.102.29.5:80) - State : DOWN

      1)      vserver-LB-1 (10.102.29.60:80) - State : DOWN
 Done
<!--NeedCopy-->
```

Pour implémenter la configuration d'équilibrage de charge initiale à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge.
2. Dans le volet d'informations, sous Mise en route, cliquez sur Assistant Équilibrage de charge et suivez les instructions pour créer une configuration d'équilibrage de charge de base.
3. Revenez au volet de navigation, développez Équilibrage de la charge, puis cliquez sur Serveurs virtuels.
4. Sélectionnez le serveur virtuel que vous avez configuré et vérifiez que les paramètres affichés en bas de la page sont correctement configurés.
5. Cliquez sur Ouvrir.
6. Vérifiez que chaque service est lié au serveur virtuel en confirmant que la case Actif est cochée pour chaque service sous l'onglet Services.

Paramètres de persistance

August 20, 2021

Vous devez configurer la persistance sur un serveur virtuel si vous souhaitez maintenir les états des connexions sur les serveurs représentés par ce serveur virtuel (par exemple, les connexions utilisées dans le commerce électronique). L'appliance utilise ensuite la méthode d'équilibrage de charge configurée pour la sélection initiale d'un serveur, mais transmet à ce même serveur toutes les demandes ultérieures du même client.

Si la persistance est configurée, elle remplace les méthodes d'équilibrage de charge une fois le serveur sélectionné. Si la persistance configurée s'applique à un service en panne, l'appliance utilise les méthodes d'équilibrage de charge pour sélectionner un nouveau service et le nouveau service devient permanent pour les demandes ultérieures du client. Si le service sélectionné est hors service, il continue de répondre aux demandes en attente, mais n'accepte pas de nouvelles demandes ou connexions. Après l'expiration de la période d'arrêt, les connexions existantes sont fermées. Le tableau suivant répertorie les types de persistance que vous pouvez configurer.

Type de persistance	Connexions persistantes
IP source, ID de session SSL, règle, DESTIP, SRCIPDESTIP	250K
CookieInsert, URL passive, ID de serveur personnalisé	Limite de mémoire. Dans le cas de CookieInsert, si le délai d'expiration n'est pas égal à 0, tout nombre de connexions est autorisé jusqu'à ce que la mémoire soit limitée.

Tableau 1. Limitations du nombre de connexions persistantes simultanées

Si la persistance configurée ne peut pas être maintenue en raison d'un manque de ressources sur une appliance, les méthodes d'équilibrage de charge sont utilisées pour la sélection du serveur. La persistance est maintenue pendant une période configurée, en fonction du type de persistance. Certains types de persistance sont spécifiques à certains serveurs virtuels. Le tableau suivant montre la relation.

Persistence TypeHeader 1	HTTP	HTTPS	TCP	UDP/IP	SSL_Pont
IP source	OUI	OUI	OUI	OUI	OUI
CookieInsert	OUI	OUI	NON	NON	NON

Persistence TypeHeader 1	HTTP	HTTPS	TCP	UDP/IP	SSL_Pont
ID de session SSL	NON	OUI	NON	NON	OUI
URL passive	OUI	OUI	NON	NON	NON
ID de serveur personnalisé	OUI	OUI	NON	NON	NON
Règle	OUI	OUI	NON	NON	NON
SRCIPDESTIP	S.O.	S.O.	OUI	OUI	S.O.
DESTIP	S.O.	S.O.	OUI	OUI	S.O.

Tableau 2. Types de persistance disponibles pour chaque type de serveur virtuel

Vous pouvez également spécifier la persistance d'un groupe de serveurs virtuels. Lorsque vous activez la persistance sur le groupe, les demandes du client sont dirigées vers le même serveur sélectionné, quel que soit le serveur virtuel du groupe qui reçoit la demande du client. Lorsque le temps configuré pour la persistance s'écoule, n'importe quel serveur virtuel du groupe peut être sélectionné pour les requêtes client entrantes.

Deux types de persistance couramment utilisés sont la persistance basée sur les cookies et la persistance basée sur les ID de serveur dans les URL.

Configurer la persistance basée sur les cookies

Lorsque vous activez la persistance basée sur les cookies, l'appliance Citrix ADC ajoute un cookie HTTP dans le champ d'en-tête Set-Cookie de la réponse HTTP. Le cookie contient des informations sur le service auquel les requêtes HTTP doivent être envoyées. Le client stocke le cookie et l'inclut dans toutes les demandes suivantes, et ADC l'utilise pour sélectionner le service pour ces demandes. Vous pouvez utiliser ce type de persistance sur des serveurs virtuels de type HTTP ou HTTPS.

L'appliance Citrix ADC insère le cookie <NSC_XXXX>= <ServiceIP> <ServicePort>

où :

- <<NSC_XXXX> est l'ID du serveur virtuel dérivé du nom du serveur virtuel.
- <<ServiceIP> est la valeur hexadécimale de l'adresse IP du service.
- <<ServicePort> est la valeur hexadécimale du port du service.

ADC chiffre ServiceIP et ServicePort lorsqu'il insère un cookie et les déchiffre lorsqu'il reçoit un cookie.

Remarque : Si le client n'est pas autorisé à stocker le cookie HTTP, les requêtes suivantes n'ont pas le cookie HTTP, et la persistance n'est pas respectée.

Par défaut, l'appliance ADC envoie le cookie HTTP version 0, conformément à la spécification Netscape. Il peut également envoyer la version 1, en conformité avec la RFC 2109.

Vous pouvez configurer une valeur de délai d'attente pour la persistance basée sur les cookies HTTP. Tenez compte de ce qui suit :

- Si le cookie HTTP version 0 est utilisé, l'appliance Citrix ADC insère le temps universel coordonné (GMT) absolu de l'expiration du cookie (l'attribut expire du cookie HTTP), calculé comme la somme de l'heure GMT actuelle sur une appliance ADC, et la valeur de délai d'expiration.
- Si un cookie HTTP version 1 est utilisé, l'appliance ADC insère un délai d'expiration relatif (attribut Max-Age du cookie HTTP). Dans ce cas, le logiciel client calcule le temps d'expiration réel.

Remarque : la plupart des logiciels clients actuellement installés (navigateurs Microsoft Internet Explorer et Netscape) comprennent la version 0 des cookies HTTP ; cependant, certains serveurs proxy HTTP comprennent la version 1 des cookies HTTP.

Si vous définissez la valeur du délai d'expiration sur 0, l'appliance ADC ne spécifie pas le délai d'expiration, quelle que soit la version du cookie HTTP utilisée. Le délai d'expiration dépend alors du logiciel client, et ces cookies ne sont pas valides si ce logiciel est arrêté. Ce type de persistance ne consomme aucune ressource système. Par conséquent, il peut accueillir un nombre illimité de clients persistants.

Un administrateur peut modifier la version du cookie HTTP.

Pour modifier la version du cookie HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
set ns param [-cookieversion ( 0 | 1 )]
<!--NeedCopy-->
```

Exemple :

```
set ns param -cookieversion 1
<!--NeedCopy-->
```

Pour modifier la version du cookie HTTP à l'aide de l'interface graphique

1. Accédez à Système > Paramètres.
2. Dans le volet d'informations, cliquez sur Modifier les paramètres HTTP.
3. Dans la boîte de dialogue Configurer les paramètres HTTP, sous Cookie, sélectionnez Version 0 ou Version 1.

Remarque : Pour plus d'informations sur les paramètres, voir Configurer la persistance en fonction des cookies.

Pour configurer la persistance basée sur les cookies à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la persistance en fonction des cookies et vérifier la configuration :

```
set lb vserver <name> -persistenceType COOKIEINSERT

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
Done
show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: COOKIEINSERT (version 0)
    Persistence Timeout: 2 min
    .
    .
    .
 Done
<!--NeedCopy-->
```

Pour configurer la persistance basée sur les cookies à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer la persistance (par exemple, vserver-LB-1), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Méthode et persistance, dans la liste Persistance, sélectionnez COOKIEINSERT.
4. Dans la zone de texte Délai d'expiration (min), tapez la valeur de délai d'expiration (par exemple, 2).
5. Cliquez sur OK.

6. Vérifiez que le serveur virtuel pour lequel vous avez configuré la persistance est correctement configuré en sélectionnant le serveur virtuel et en affichant la section Détails en bas du volet.

Configurer la persistance en fonction des ID de serveur dans les URL

L'appliance Citrix ADC peut maintenir la persistance en fonction des ID de serveur dans les URL. Dans une technique appelée persistance passive URL, ADC extrait l'ID du serveur de la réponse du serveur et l'intègre dans la requête URL de la requête client. L'ID du serveur est une adresse IP et un port spécifiés en tant que nombre hexadécimal. ADC extrait l'ID du serveur des requêtes client suivantes et l'utilise pour sélectionner le serveur.

La persistance passive des URL nécessite la configuration d'une expression de charge utile ou d'une expression d'infrastructure de stratégie spécifiant l'emplacement de l'ID de serveur dans les demandes du client. Pour plus d'informations sur les expressions, voir Configuration et référence des stratégies.

Remarque : Si l'ID de serveur ne peut pas être extrait des demandes client, la sélection du serveur est basée sur la méthode d'équilibrage de charge.

Exemple : Expression de charge utile

L'expression, URLQUERY contient sid= configure le système pour extraire l'ID du serveur de la requête URL d'une requête client, après avoir fait correspondre le jeton sid=. Ainsi, une requête avec l'URL `http://www.citrix.com/index.asp?\\&sid;=c0a864100050` est dirigée vers le serveur avec l'adresse IP10.102.29.10 et le port 80.

La valeur de délai d'expiration n'affecte pas ce type de persistance, qui est maintenue tant que l'ID du serveur peut être extrait des requêtes du client. Ce type de persistance ne consomme pas de ressources système, il peut donc accueillir un nombre illimité de clients persistants.

> Remarque : Pour plus d'informations sur les paramètres, voir Équilibrage de charge.

Pour configurer la persistance en fonction des ID de serveur dans les URL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la persistance en fonction des ID de serveur dans les URL et vérifiez la configuration :

```
set lb vserver <name> -persistenceType URLPASSIVE

<show lb vserver <name>
<!--NeedCopy-->
```

Exemple :


```
set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
Done
show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: URLPASSIVE
    Persistence Timeout: 2 min
    .
    .
    .
Done
<!--NeedCopy-->
```

Pour configurer la persistance en fonction des ID de serveur dans les URL à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer la persistance (par exemple, vserver-LB-1), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Méthode et persistance, dans la liste Persistance, sélectionnez URLPASSIVE.
4. Dans la zone de texte Délai d'expiration (min), tapez la valeur de délai d'expiration (par exemple, 2).
5. Dans la zone de texte Règle, entrez une expression valide. Vous pouvez également cliquer sur Configurer en regard de la zone de texte Règle et utiliser la boîte de dialogue Créer une expression pour créer une expression.
6. Cliquez sur OK.
7. Vérifiez que le serveur virtuel pour lequel vous avez configuré la persistance est correctement configuré en sélectionnant le serveur virtuel et en affichant la section Détails en bas du volet.

Configurer les fonctionnalités pour protéger la configuration d'équilibrage de charge

August 20, 2021

Vous pouvez configurer la redirection d'URL pour fournir des notifications de dysfonctionnements du serveur virtuel, et vous pouvez configurer les serveurs virtuels de sauvegarde pour qu'ils prennent le

relais si un serveur virtuel principal devient indisponible.

Configurer la redirection d'URL

Vous pouvez configurer une URL de redirection pour communiquer l'état de l'appliance en cas d'arrêt ou de désactivation d'un serveur virtuel de type HTTP ou HTTPS. Cette URL peut être un lien local ou distant. L'appliance utilise la redirection HTTP 302.

Les redirections peuvent être des URL absolues ou des URL relatives. Si l'URL de redirection configurée contient une URL absolue, la redirection HTTP est envoyée à l'emplacement configuré, quelle que soit l'URL spécifiée dans la requête HTTP entrante. Si l'URL de redirection configurée contient uniquement le nom de domaine (URL relative), la redirection HTTP est envoyée à un emplacement après avoir ajouté l'URL entrante au domaine configuré dans l'URL de redirection.

Remarque : si un serveur virtuel d'équilibrage de charge est configuré à la fois avec un serveur virtuel de sauvegarde et une URL de redirection, le serveur virtuel de sauvegarde a priorité sur l'URL de redirection. Dans ce cas, une redirection est utilisée lorsque les serveurs virtuels principal et de sauvegarde sont en panne.

Pour configurer un serveur virtuel pour rediriger les demandes client vers une URL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur virtuel afin de rediriger les demandes du client vers une URL et vérifier la configuration :

```
set lb vserver <name> -redirectURL <URL>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
    > set lb vserver vserver-LB-1 -redirectURL <http://www.newdomain.
       com/mysite/maintenance>
     Done
    > show lb vserver vserver-LB-1
        vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jun 17 08:56:34 2009 (+666 ms)
        .
        .
        .
        Redirect URL: <http://www.newdomain.com/mysite/maintenance>
        .
```



```
12          .
13          .
14       Done
15      >
16 <!--NeedCopy-->
```

Pour configurer un serveur virtuel pour rediriger les requêtes client vers une URL à l'aide de l'interface graphique graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer la redirection d'URL (par exemple, vserver-LB-1), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Avancé, dans la zone de texte URL de redirection, tapez l'URL (par exemple `http://www.newdomain.com/mysite/maintenance`), puis cliquez sur OK.
4. Vérifiez que l'URL de redirection que vous avez configurée pour le serveur apparaît dans la section Détails au bas du volet.

Configurer les serveurs virtuels de sauvegarde

Si le serveur virtuel principal est hors service ou désactivé, l'appliance peut diriger les connexions ou les demandes du client vers un serveur virtuel de sauvegarde qui transfère le trafic client aux services. L'appliance peut également envoyer un message de notification au client concernant la panne ou la maintenance du site. Le serveur virtuel de sauvegarde est un proxy et est transparent pour le client.

Vous pouvez configurer un serveur virtuel de sauvegarde lorsque vous créez un serveur virtuel ou lorsque vous modifiez les paramètres facultatifs d'un serveur virtuel existant. Vous pouvez également configurer un serveur virtuel de sauvegarde pour un serveur virtuel de sauvegarde existant, créant ainsi un serveur virtuel de sauvegarde en cascade. La profondeur maximale des serveurs virtuels de sauvegarde en cascade est de 10. L'appliance recherche un serveur virtuel de sauvegarde qui est en service et y accède pour diffuser le contenu.

Vous pouvez configurer la redirection d'URL sur le serveur principal pour une utilisation lorsque les serveurs virtuels principal et de sauvegarde sont en panne ou ont atteint leurs seuils de traitement des demandes.

Remarque : Si aucun serveur virtuel de sauvegarde n'existe, un message d'erreur s'affiche, sauf si le serveur virtuel est configuré avec une URL de redirection. Si un serveur virtuel de sauvegarde et une URL de redirection sont tous deux configurés, le serveur virtuel de sauvegarde a priorité.

Pour configurer un serveur virtuel de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur de sauvegarde et vérifier la configuration :

```
set lb vserver <name> [-backupVserver <string>]

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
    > set lb vserver vserver-LB-1 -backupVserver vserver-LB-2
     Done
    > show lb vserver vserver-LB-1
        vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jun 17 08:56:34 2009 (+661 ms)
        .
        .
        .
        Backup: vserver-LB-2
        .
        .
        .
     Done
    >
<!--NeedCopy-->
```

Pour configurer un serveur virtuel de sauvegarde à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le serveur virtuel de sauvegarde (par exemple, vserver-LB-1), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Avancé, dans la liste Sauvegarder le serveur virtuel, sélectionnez le serveur virtuel de sauvegarde (par exemple, vServer-LB-2, puis cliquez sur OK.
4. Vérifiez que le serveur virtuel de sauvegarde que vous avez configuré apparaît dans la section Détails en bas du volet.

   Remarque : Si le serveur principal tombe en panne, puis remonte, et que vous souhaitez que le serveur virtuel de sauvegarde fonctionne comme serveur principal jusqu'à ce que vous rétab-

lissiez explicitement le serveur virtuel principal, activez la case à cocher Désactiver le serveur principal lors de l'arrêt.

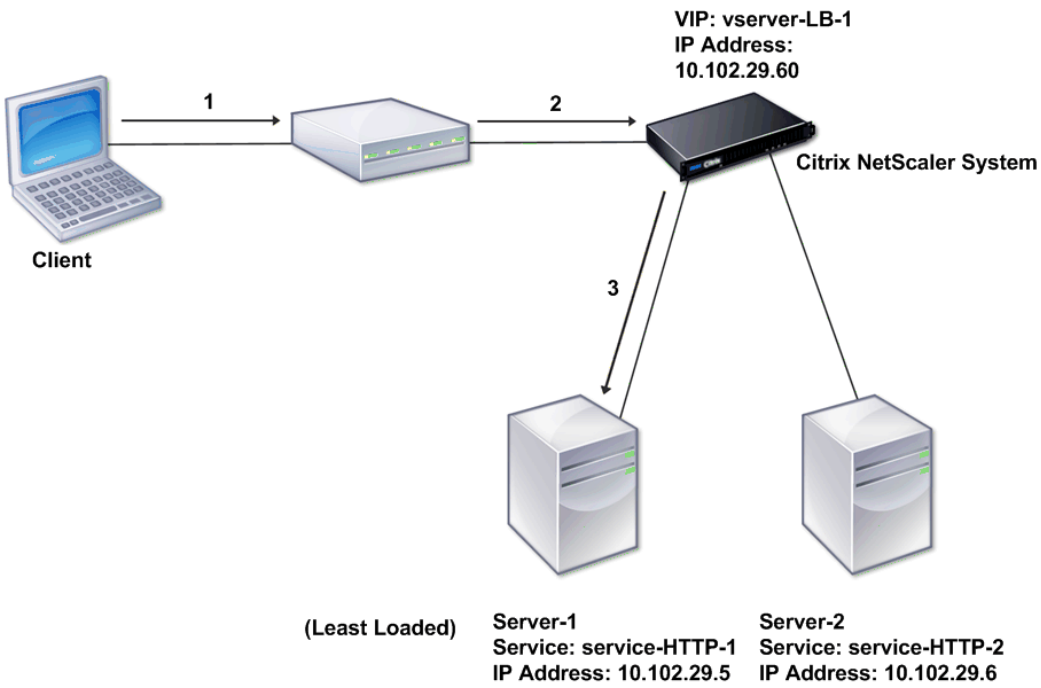
Un scénario d'équilibrage de charge typique

August 20, 2021

Dans une configuration d'équilibrage de charge, les appliances Citrix ADC sont logiquement situées entre le client et la batterie de serveurs et gèrent le flux de trafic vers les serveurs.

La figure suivante illustre la topologie d'une configuration d'équilibrage de charge de base.

Figure 1. Topologie d'équilibrage de charge de base

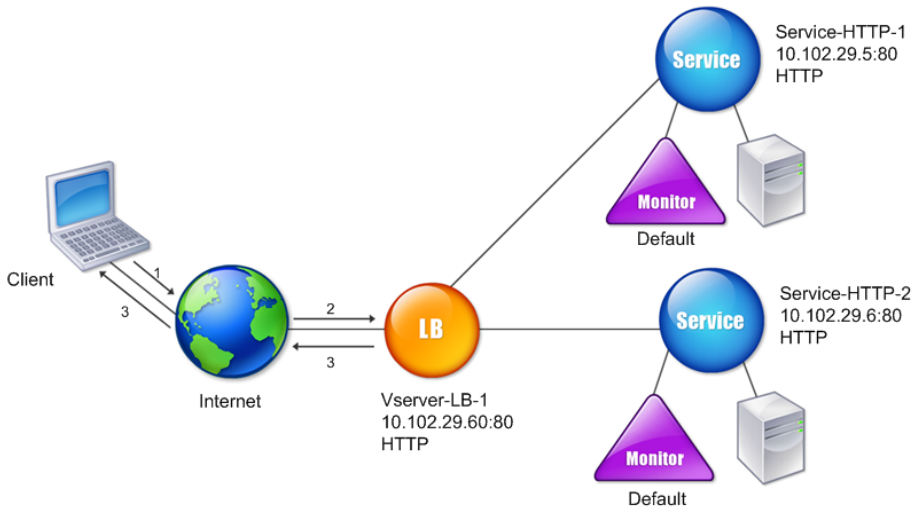


Le serveur virtuel sélectionne le service et l'affecte pour répondre aux demandes du client. Considérons le scénario de la figure précédente, où les services Service-HTTP-1 et Service-HTTP-2 sont créés et liés au serveur virtuel nommé Serveur virtuel-LB-1. Virtual Server-LB-1 transfère la demande client à Service-HTTP-1 ou Service-HTTP-2. Le système sélectionne le service pour chaque requête à l'aide de la méthode d'équilibrage de charge des connexions les plus limitées. Le tableau suivant répertorie les noms et les valeurs des entités de base qui doivent être configurées sur le système.

Tableau 1. Valeurs des paramètres de configuration LB

La figure suivante montre les valeurs d'échantillon d'équilibrage de charge et les paramètres requis décrits dans le tableau précédent.

Figure 2. Modèle d'entité d'équilibrage de charge



Les tableaux suivants répertorient les commandes utilisées pour configurer cette configuration d'équilibrage de charge à l'aide de l'interface de ligne de commande.

Tâche	Commande
Pour activer l'équilibrage de charge	enable feature lb
Pour créer un service nommé Service-HTTP-1	add service service-HTTP-1 10.102.29.5 HTTP 80
Pour créer un service nommé Service-HTTP-2	add service service-HTTP-2 10.102.29.6 HTTP 80
Pour créer un serveur virtuel nommé vserver-LB-1	add lb vserver vserver-LB-1 HTTP 10.102.29.60 80

Tâche	Commande
Pour lier un service nommé Service-HTTP-1 à un serveur virtuel nommé vserver-LB-1	bind lb vserver vserver-LB-1 service-HTTP-1
Pour lier un service nommé service-HTTP-2 à un serveur virtuel nommé vserver-LB-1	bind lb vserver vserver-LB-1 service-HTTP-2

Tableau 2. Tâches de configuration initiales

Pour plus d'informations sur les tâches de configuration initiales, voir Configuration de l'équilibrage de charge de base.

Tâche	Commande
Pour afficher les propriétés d'un serveur virtuel nommé vserver-LB-1	show lb vserver vserver-LB-1
Pour afficher les statistiques d'un serveur virtuel nommé vserver-LB-1	stat lb vserver vserver-LB-1
Pour afficher les propriétés d'un service nommé Service-HTTP-1	show service service-HTTP-1
Pour afficher les statistiques d'un service nommé Service-HTTP-1	stat service service-HTTP-1
Pour afficher les liaisons d'un service nommé Service-HTTP-1	show service bindings service-HTTP-1

Tableau 3. Tâches de vérification

Tâche	Commande
Pour configurer la persistance sur un serveur virtuel nommé vserver-LB-1	set lb vserver vserver-LB-1 -persistenceType SOURCEIP -persistenceMask 255.255.255.255 -timeout 2
Pour configurer la persistance COOKIEINSERT sur un serveur virtuel nommé vserver-LB-1	set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
Pour configurer la persistance URLPassive sur un serveur virtuel nommé vserver-LB-1	set lb vserver vserver-LB-1 -persistenceType URLPASSIVE

Tâche	Commande
Pour configurer un serveur virtuel pour rediriger la demande client vers une URL sur un serveur virtuel nommé vserver-LB-1	set lb vserver vserver-LB-1 -redirectURL http://www.newdomain.com/mysite/maintenance
Pour définir un serveur virtuel de sauvegarde sur un serveur virtuel nommé vserver-LB-1	set lb vserver vserver-LB-1 -backupVserver vserver-LB-2

Tableau 4. Tâches de personnalisation

Pour plus d'informations sur la configuration de la persistance, consultez Choix et configuration des paramètres de persistance. Pour plus d'informations sur la configuration d'un serveur virtuel pour rediriger une demande client vers une URL et sur la configuration d'un serveur virtuel de sauvegarde, voir Configuration des fonctionnalités pour protéger la configuration d'équilibrage de charge.

Cas d'utilisation : Comment forcer les options de cookie Secure et HttpOnly pour les sites Web utilisant l'appliance Citrix ADC

October 5, 2021

Les administrateurs Web peuvent forcer Secure, ou HttpOnly, ou les deux indicateurs sur l'ID de session et les cookies d'authentification générés par les applications Web. Vous pouvez modifier les entêtes Set-Cookie pour inclure ces deux options en utilisant un serveur virtuel d'équilibrage de charge HTTP et en réécrivant des stratégies sur une appliance Citrix ADC.

- **HttpOnly** - Cette option sur un cookie oblige les navigateurs Web à renvoyer le cookie à l'aide du protocole HTTP ou HTTPS uniquement. Les méthodes non HTTP telles que les références JavaScript document.cookie ne peuvent pas accéder au cookie. Cette option permet de prévenir le vol de cookie dus à des scripts intersites.

  > REMARQUE
  >
  > Vous ne pouvez pas utiliser l'option HttpOnly lorsqu'une application Web a besoin d'accéder au contenu des cookies à l'aide d'un script côté client, tel que JavaScript ou une applet Java côté client. Vous pouvez utiliser la méthode mentionnée dans ce document pour réécrire uniquement les cookies générés par le serveur et non les cookies générés par l'appliance Citrix ADC. Par exemple, AppFirewall, persistance, cookies de session VPN, etc.

- **Sécurisé** - Cette option sur un cookie permet aux navigateurs Web de renvoyer uniquement la valeur du cookie lorsque la transmission est chiffrée par SSL. Cette option peut être utilisée pour

empêcher le vol de cookies par écoute de connexion.

> REMARQUE
>
> La procédure suivante ne s'applique pas aux serveurs virtuels VPN.

Pour configurer l'appliance Citrix ADC pour forcer les indicateurs Secure et HttpOnly pour un serveur virtuel HTTP existant à l'aide de l'interface de ligne de commande

1. Créez une action de réécriture.

   Cet exemple est configuré pour définir les indicateurs Secure et HttpOnly. Si l'une ou l'autre est manquante, modifiez-la si nécessaire pour d'autres combinaisons.

   ```
   add rewrite action act_cookie_Secure replace_all http.RES.
      full_Header ""Secure; HttpOnly; path=/"" -search "regex(re!(
      path=/\\; Secure; HttpOnly)|(path=/\\; Secure)|(path=/\\;
      HttpOnly)|(path=/)!)"
   <!--NeedCopy-->
   ```

   Cette stratégie remplace toutes les instances de « path=/ », « path=/ ; Secure », « path=/ ; Secure ; HttpOnly » et « path=/ ; HttpOnly » par « Secure ; HttpOnly ; path=/ ». Cette expression régulière (regex) échoue si la casse ne correspond pas.

2. Créez une stratégie de réécriture pour déclencher l'action.

   ```
   add rewrite policy rw_force_secure_cookie "http.RES.HEADER("Set-
      Cookie").EXISTS" act_cookie_Secure
   <!--NeedCopy-->
   ```

3. Liez la stratégie de réécriture au serveur virtuel à sécuriser. Si `Secure` l'option est utilisée, un serveur virtuel SSL doit être utilisé.

   ```
   bind lb vserver mySSLVServer -policyName rw_force_secure_cookie -
      priority 100 -gotoPriorityExpression NEXT -type RESPONSE
   <!--NeedCopy-->
   ```

Exemples :

L'exemple suivant montre le cookie avant de définir l'indicateur HttpOnly.

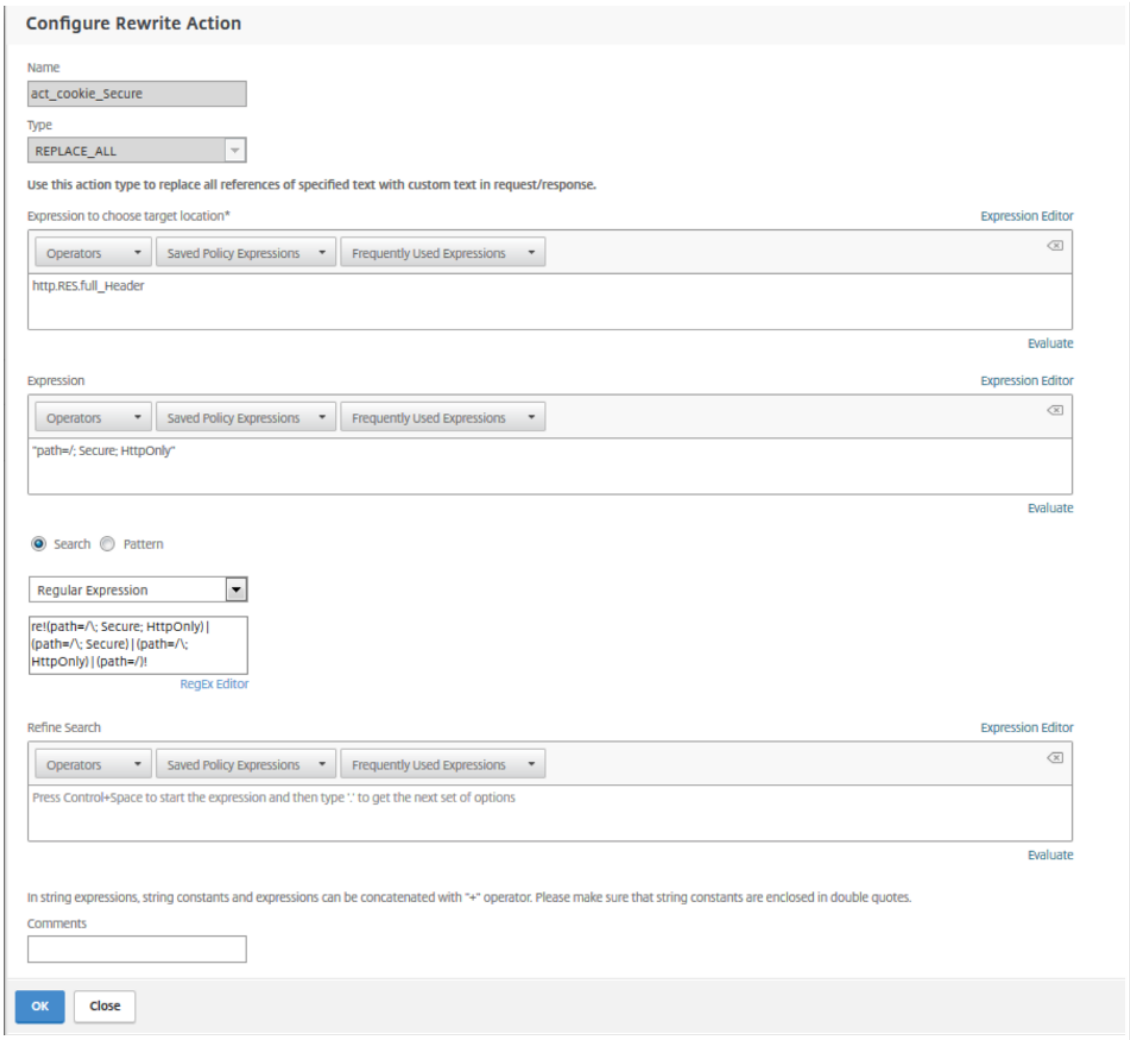
```
Set-Cookie: CtxsAuthId=C5614491; path=/Citrix/ProdWeb
<!--NeedCopy-->
```

L'exemple suivant montre le cookie après avoir défini l'indicateur HttpOnly.

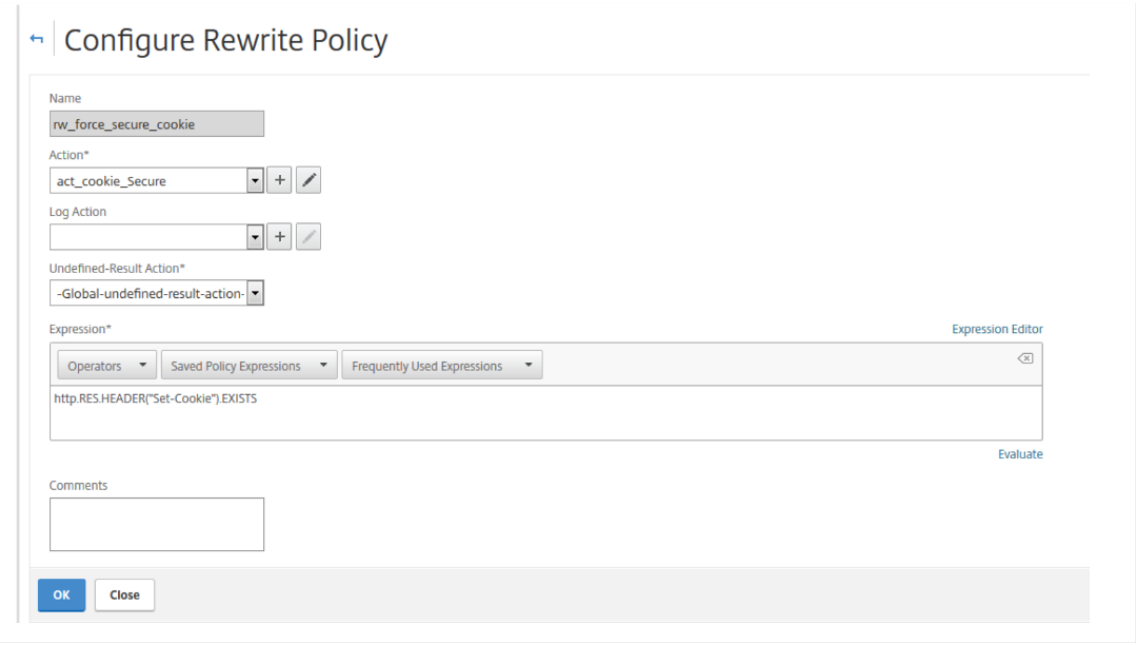

```
1 Set-Cookie: CtxsAuthId=C5614491; Secure; HttpOnly; path=/Citrix/ProdWeb
     /
2 <!--NeedCopy-->
```

Pour configurer l'appliance Citrix ADC pour forcer les indicateurs Secure et HttpOnly pour un serveur virtuel HTTP existant à l'aide de l'interface graphique

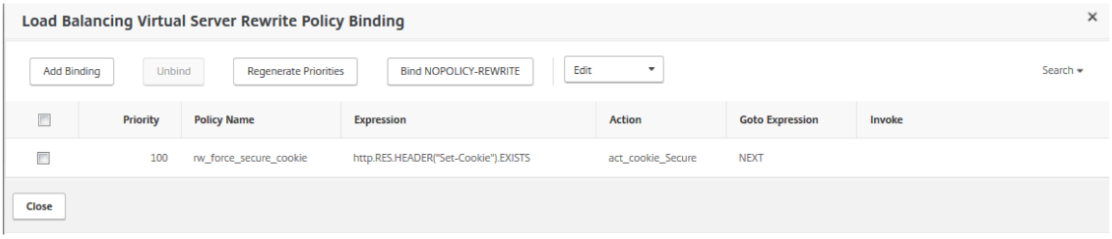
1. Accédez à **AppExpert > Réécriture > Actions**, puis cliquez sur **Ajouter** pour ajouter une nouvelle action de réécriture.



2. Accédez à **AppExpert > Réécriture > Stratégies**, puis cliquez sur **Ajouter** pour ajouter une nouvelle stratégie de réécriture.



3. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis liez la stratégie de réécriture (réponse) au serveur virtuel SSL correspondant.



Accélérez le trafic équilibré de charge en utilisant la compression

October 5, 2021

La compression est un moyen populaire d'optimiser l'utilisation de la bande passante, et la plupart des navigateurs Web prennent en charge les données compressées. Si vous activez la fonctionnalité de compression, l'appliance Citrix ADC intercepte les demandes des clients et détermine si le client peut accepter du contenu compressé. Après avoir reçu la réponse HTTP du serveur, la solution matérielle-logicielle examine le contenu pour déterminer s'il est compressible. Si le contenu est compressible, l'appliance le compresse, modifie l'en-tête de réponse pour indiquer le type de compression effectué et transfère le contenu compressé au client.

La compression Citrix ADC est une fonctionnalité basée sur des règles. Une stratégie filtre les demandes et les réponses pour identifier les réponses à compresser, et spécifie le type de compression à appliquer à chaque réponse. L'appliance fournit plusieurs stratégies intégrées pour compresser les

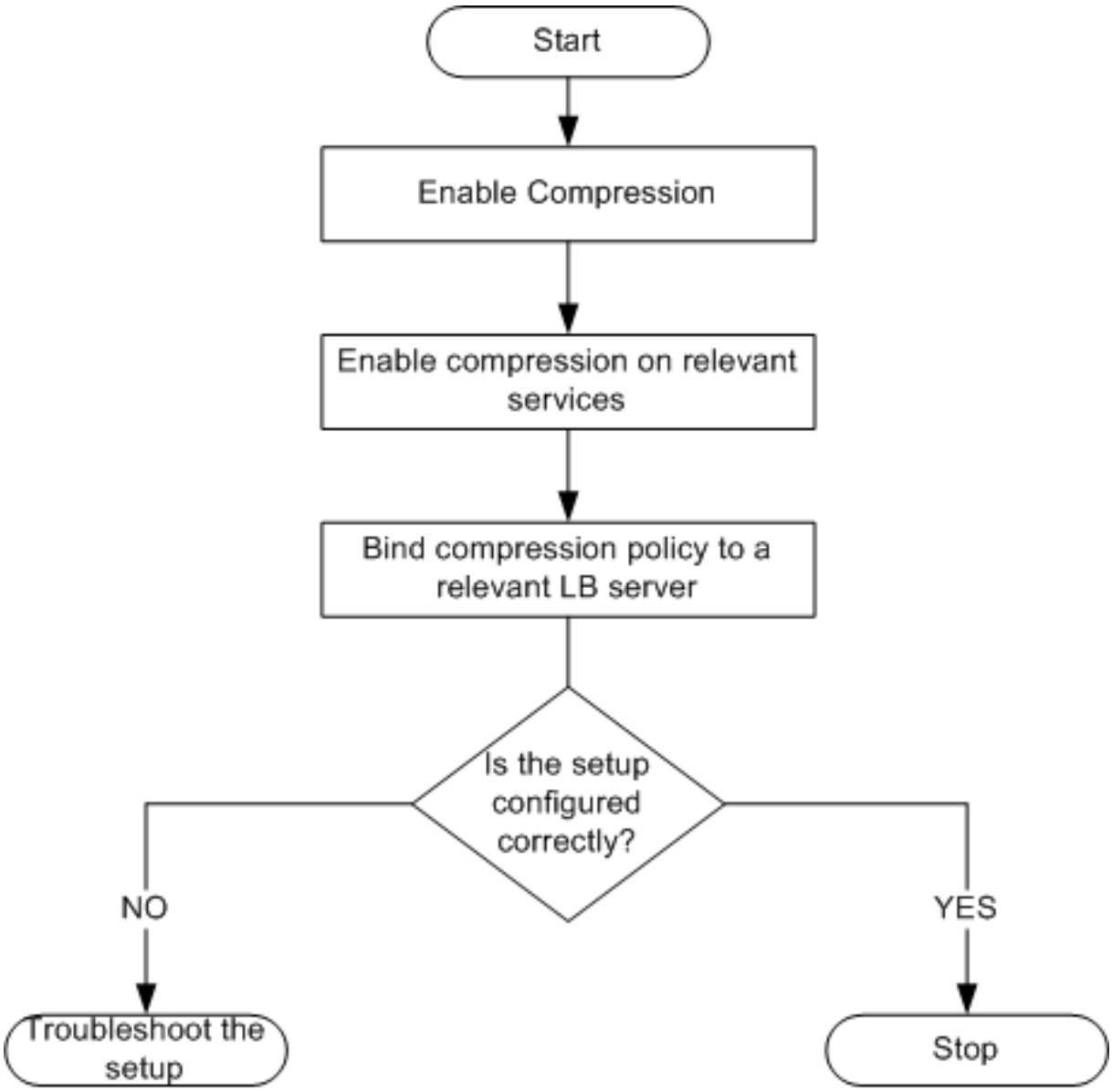
types MIME courants tels que text/html, text/plain, text/xml, text/css, text/rtf, application/msword, application/vnd.ms-excel et application/vnd.ms-powerpoint. Vous pouvez également créer des stratégies personnalisées. La solution matérielle-logicielle ne compresse pas les types MIME compressés tels que les formats application/octet-stream, binary, bytes et image compressée tels que GIF et JPEG.

Pour configurer la compression, vous devez l'activer globalement et sur chaque service qui fournira des réponses que vous souhaitez compresser. Si vous avez configuré des serveurs virtuels pour l'équilibrage de charge ou la commutation de contenu, vous devez lier les stratégies aux serveurs virtuels. Dans le cas contraire, les stratégies s'appliquent à tout le trafic qui passe par l'appliance.

Séquence de tâches de configuration de compression

L'organigramme suivant montre la séquence des tâches de configuration de la compression de base dans une configuration d'équilibrage de charge.

Figure 1. Séquence de tâches de configuration de la compression



> Remarque : Les étapes de la figure ci-dessus supposent que l'équilibrage de charge a déjà été configuré.

Activer la compression

Par défaut, la compression n'est pas activée. Vous devez activer la fonction de compression pour permettre la compression des réponses HTTP envoyées au client.

Pour activer la compression à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer la compression et vérifier la configuration :

- enable ns feature CMP
- show ns feature

```
    > enable ns feature CMP


    Done

    > show ns feature


           Feature                        Acronym              Status

           -------                        -------              ------

    1)     Web Logging                    WL                   ON

    2)     Surge Protection               SP                   OFF

    .

    7) Compression Control CMP ON

       .

    Done
<!--NeedCopy-->
```

Pour activer la compression à l'aide de l'interface graphique

1. Dans le volet de navigation, développez Système, puis cliquez sur Paramètres.

2. Dans le volet d'informations, sous Modes et fonctionnalités, cliquez sur Modifier les fonctionnalités de base.
3. Dans la boîte de dialogue Configurer les fonctionnalités de base, activez la case à cocher Compression, puis cliquez sur OK.
4. Dans la ou les fonctions Activer/Désactiver ? , cliquez sur Oui.

Configurer les services pour compresser les données

Outre l'activation globale de la compression, vous devez l'activer sur chaque service qui distribuera les fichiers à compresser.

Pour activer la compression sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer la compression sur un service et vérifier la configuration :

- set service <name> -CMP YES
- show service <name>

```
> show service SVC_HTTP1


SVC_HTTP1 (10.102.29.18:80) - HTTP


State: UP


Last state change was at Tue Jun 16 06:19:14 2009 (+737 ms)


Time since last state change: 0 days, 03:03:37.200


Server Name: 10.102.29.18


Server ID : 0   Monitor Threshold : 0


Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits


Use Source IP: NO
```



```
26
27
28 Client Keepalive(CKA): NO
29
30
31 Access Down Service: NO
32
33
34 TCP Buffering(TCPB): NO
35
36
37 HTTP Compression(CMP): YES
38
39
40 Idle timeout: Client: 180 sec   Server: 360 sec
41
42
43 Client IP: DISABLED
44
45
46 Cacheable: NO
47
48
49 SC: OFF
50
51
52 SP: OFF
53
54
55 Down state flush: ENABLED
56
57 1)      Monitor Name: tcp-default
58
59
60 State: DOWN     Weight: 1
61
62
63 Probes: 1095    Failed [Total: 1095 Current: 1095]
64
65
66 Last response: Failure - TCP syn sent, reset received.
67
68
69 Response Time: N/A
70
```



```
71
72 Done
73
74 <!--NeedCopy-->
```

Pour activer la compression sur un service à l'aide de l'interface graphique

1. Accédez à Traffic Management > Load Balancing > Services.
2. Dans le volet d'informations, sélectionnez le service pour lequel vous souhaitez configurer la compression (par exemple, Service-HTTP-1), puis cliquez sur Ouvrir.
3. Sous l'onglet Avancé, sous Paramètres, activez la case à cocher Compression, puis cliquez sur OK.
4. Vérifiez que, lorsque le service est sélectionné, Compression HTTP (CMP) : ON apparaît dans la section **Détails** en bas du volet.

Liaison d'une stratégie de compression à un serveur virtuel

Si vous liez une stratégie à un serveur virtuel, la stratégie est évaluée uniquement par les services associés à ce serveur virtuel. Vous pouvez lier des stratégies de compression à un serveur virtuel à partir de la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge) ou de la boîte de dialogue Gestionnaire des stratégies de compression. Cette rubrique inclut des instructions pour lier des stratégies de compression à un serveur virtuel d'équilibrage de charge à l'aide de la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge).

Pour lier ou annuler la liaison d'une stratégie de compression à un serveur virtuel à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier ou délier une stratégie de compression à un serveur virtuel d'équilibrage de charge et vérifiez la configuration :

- (bind|unbind) lb vserver <name> -policyName <string>
- show lb vserver <name>

Exemple :

```
1 > bind lb vserver lbvip -policyName ns_cmp_msapp
2 Done
3 > showlbserverlbvip
4
5 lbvip(8.7.6.6:80)-HTTPType:ADDRESS
6 State:UP
7 LaststatechangewasatThuMay2805:37:212009(+685ms)
```



```
Timesincelaststatechange:19days,04:26:50.470
EffectiveState:UP
ClientIdleTimeout:180sec
Downstateflush:ENABLED
DisablePrimaryVserverOnDown:DISABLED
PortRewrite:DISABLED
No.ofBoundServices:1(Total)1(Active)
ConfiguredMethod:LEASTCONNECTION
CurrentMethod:RoundRobin,Reason:Boundservice'sstatechangedtoUP
Mode:IP
Persistence:NONE
VserverIPandPortinsertion:OFF
Push:DISABLEDPushVServer:
PushMultiClients:NO
PushLabelRule:

BoundServiceGroups:
1)GroupName:Service-Group-1

1)Service-Group-1(10.102.29.252:80)-HTTPState:UPWeight:1

1)Policy:ns_cmp_msappPriority:0

Done

<!--NeedCopy-->
```

Pour lier ou délier une stratégie de compression à un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel auquel vous souhaitez lier ou annuler la liaison d'une stratégie de compression (par exemple, vServer-LB-1), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Stratégies, cliquez sur Compression.
4. Procédez comme suit :
   - Pour lier une stratégie de compression, cliquez sur Insérer une stratégie, puis sélectionnez la stratégie que vous souhaitez lier au serveur virtuel.
   - Pour annuler la liaison d'une stratégie de compression, cliquez sur le nom de la stratégie que vous souhaitez délier du serveur virtuel, puis cliquez sur Unbind Policy.
5. Cliquez sur OK.

Sécurisez le trafic à charge équilibrée en utilisant SSL

October 5, 2021

La fonction de déchargement SSL Citrix ADC améliore de manière transparente les performances des sites Web qui effectuent des transactions SSL. En déchargeant les tâches de chiffrement et de déchiffrement SSL gourmandes en CPU du serveur Web local vers l'appliance, le déchargement SSL garantit la livraison sécurisée des applications Web sans pénalisation des performances lorsque le serveur traite les données SSL. Une fois le trafic SSL déchiffré, il peut être traité par tous les services standard. Le protocole SSL fonctionne de manière transparente avec différents types de données HTTP et TCP et fournit un canal sécurisé pour les transactions utilisant ces données.

Pour configurer SSL, vous devez d'abord l'activer. Ensuite, vous configurez les services HTTP ou TCP et un serveur virtuel SSL sur l'appliance, puis liez les services au serveur virtuel. Vous devez également ajouter une paire de clés de certificat et la lier au serveur virtuel SSL. Si vous utilisez des serveurs Outlook Web Access, vous devez créer une action pour activer la prise en charge SSL et une stratégie pour appliquer l'action. Un serveur virtuel SSL intercepte le trafic chiffré entrant et le décrypte à l'aide d'un algorithme négocié. Le serveur virtuel SSL transmet ensuite les données déchiffrées aux autres entités de l'appliance pour un traitement approprié.

Pour plus d'informations sur le déchargement SSL, consultez Déchargement et accélérationSSL.

Séquence de tâches de configuration SSL

Pour configurer SSL, vous devez d'abord l'activer. Vous devez ensuite créer un serveur virtuel SSL et des services HTTP ou TCP sur l'appliance Citrix ADC. Enfin, vous devez lier un certificat SSL valide et les services configurés au serveur virtuel SSL.

Un serveur virtuel SSL intercepte le trafic chiffré entrant et le décrypte à l'aide d'un algorithme négocié. Le serveur virtuel SSL transfère ensuite les données déchiffrées aux autres entités de l'appliance Citrix ADC pour un traitement approprié.

L'organigramme suivant montre la séquence des tâches de configuration d'une configuration de déchargement SSL de base.

Figure 1. Séquence de tâches pour configurer le déchargement SSL

Activer le déchargement SSL

Commencez par activer la fonctionnalité SSL. Vous pouvez configurer des entités SSL sur l'appliance sans activer la fonctionnalité SSL, mais elles ne fonctionneront pas tant que vous n'aurez pas activé SSL.

Activer SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer le déchargement SSL et vérifier la configuration :

```
-  enable ns feature SSL
-  show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable ns feature ssl

Done


> show ns feature


Feature Acronym Status


------- ------- ------


1) Web Logging WL ON


2) SurgeProtection SP OFF


3) Load Balancing LB ON . . .


 9) SSL Offloading SSL ON


10) Global Server Load Balancing GSLB ON . .

```



```
29
30 Done >
31 <!--NeedCopy-->
```

Activer SSL à l'aide de l'interface graphique

Procédez comme suit :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Dans le volet d'informations, sous **Modes et fonctionnalités**, cliquez sur **Modifier les fonctionnalités de base**.
3. Activez la case à cocher **Déchargement SSL**, puis cliquez sur **OK**.
4. Dans la ou les **fonctions Activer/Désactiver ?**, cliquez sur **Oui**.

Créer des services HTTP

Un service de la solution matérielle-logicielle représente une application sur un serveur. Une fois configurés, les services sont désactivés jusqu'à ce que la solution matérielle-logicielle puisse atteindre le serveur sur le réseau et en surveiller l'état. Cette rubrique décrit les étapes de création d'un service HTTP.

Remarque : Pour le trafic TCP, effectuez les procédures suivantes, mais créez des services TCP à la place des services HTTP.

Ajouter un service HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un service HTTP et vérifier la configuration :

```
1 -  add service <name> (<IP> | <serverName>) <serviceType> <port>
2 -  show service <name>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add service SVC_HTTP1 10.102.29.18 HTTP 80
2
3
4  Done
5
6
7 > show service SVC_HTTP1
8
```



```
9
10          SVC_HTTP1 (10.102.29.18:80) - HTTP
11
12
13          State: UP
14
15
16          Last state change was at Wed Jul 15 06:13:05 2009
17
18
19          Time since last state change: 0 days, 00:00:15.350
20
21
22          Server Name: 10.102.29.18
23
24
25          Server ID : 0   Monitor Threshold : 0
26
27
28          Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
29
30
31          Use Source IP: NO
32
33
34          Client Keepalive(CKA): NO
35
36
37          Access Down Service: NO
38
39
40          TCP Buffering(TCPB): NO
41
42
43          HTTP Compression(CMP): YES
44
45
46          Idle timeout: Client: 180 sec   Server: 360 sec
47
48
49          Client IP: DISABLED
50
51
52          Cacheable: NO
53
```



```
54
55          SC: OFF
56
57
58          SP: OFF
59
60
61          Down state flush: ENABLED
62
63
64
65
66
67  1)      Monitor Name: tcp-default
68
69
70                  State: UP       Weight: 1
71
72
73                  Probes: 4       Failed [Total: 0 Current: 0]
74
75
76                  Last response: Success - TCP syn+ack received.
77
78
79                  Response Time: N/A
80
81
82   Done
83  <!--NeedCopy-->
```

Ajouter un service HTTP à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > Déchargement SSL > Services**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un service**, tapez le nom du service, l'adresse IP et le port (par exemple, SVC_HTTP1, 10.102.29.18 et 80).
4. Dans la liste **Protocole**, sélectionnez le type de service (par exemple, HTTP).
5. Cliquez sur **Créer**, puis cliquez sur **Fermer**. Le service HTTP que vous avez configuré apparaît dans la page Services.
6. Vérifiez que les paramètres que vous avez configurés sont correctement configurés en sélection-

nant le service et en affichant la section Détails en bas du volet.

Ajouter un serveur virtuel SSL

Dans une configuration de déchargement SSL de base, le serveur virtuel SSL intercepte le trafic chiffré, le déchiffre et envoie les messages en texte clair aux services liés au serveur virtuel. Le déchargement du traitement SSL gourmand en CPU vers l'appliance permet aux serveurs principaux de traiter un plus grand nombre de demandes.

Ajouter un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel SSL et vérifier la configuration :

```
1 -  add lb vserver <name> <serviceType> [<IPAddress> <port>]
2 -  show lb vserver <name>
3 <!--NeedCopy-->
```

> **Attention :** Pour garantir la sécurité des connexions, vous devez lier un certificat SSL valide au serveur virtuel SSL avant de l'activer.

Exemple :

```
1  > add lb vserver vserver-SSL-1 SSL 10.102.29.50 443
2    Done
3
4
5    > show lb vserver vserver-SSL-1
6
7
8    vserver-SSL-1 (10.102.29.50:443) - SSL Type: ADDRESS
9
10
11   State: DOWN[Certkey not bound] Last state change was at Tue Jun 16
        06:33:08 2009 (+176 ms)
12
13
14   Time since last state change: 0 days, 00:03:44.120
15
16
17   Effective State: DOWN Client Idle Timeout: 180 sec
18
19
20   Down state flush: ENABLED
```



```
21
22
23    Disable Primary Vserver On Down : DISABLED
24
25
26    No. of Bound Services : 0 (Total) 0 (Active)
27
28
29    Configured Method: LEASTCONNECTION Mode: IP
30
31
32    Persistence: NONE
33
34
35    Vserver IP and Port insertion: OFF
36
37
38    Push: DISABLED Push VServer: Push Multi Clients: NO Push Label Rule:
          Done
39  <!--NeedCopy-->
```

Ajouter un serveur virtuel SSL à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > Déchargement SSL > Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un serveur virtuel (déchargement SSL)**, tapez le nom du serveur virtuel, l'adresse IP et le port.
4. Dans la liste **Protocole**, sélectionnez le type de serveur virtuel, par exemple SSL.
5. Cliquez sur **Créer**, puis cliquez sur **Fermer**.
6. Vérifiez que les paramètres que vous avez configurés sont correctement configurés en sélectionnant le serveur virtuel et en affichant la section Détails en bas du volet. Le serveur virtuel est marqué comme étant en panne car aucune paire de clés de certificat et de services n'y sont liés.

> **Attention :** Pour garantir la sécurité des connexions, vous devez lier un certificat SSL valide au serveur virtuel SSL avant de l'activer.

Liez les services au serveur virtuel SSL

Après avoir déchiffré les données entrantes, le serveur virtuel SSL transfère les données aux services que vous avez liés au serveur virtuel.

Le transfert de données entre la solution matérielle-logicielle et les serveurs peut être chiffré ou en texte clair. Si le transfert de données entre l'appliance et les serveurs est chiffré, l'intégralité de la transaction est sécurisée de bout en bout. Pour plus d'informations sur la configuration du système pour une sécurité de bout en bout, consultez Déchargement et accélération SSL.

Lier un service à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier un service au serveur virtuel SSL et vérifier la configuration :

```
- bind lb vserver <name> <serviceName>
- show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> bind lb vserver vserver-SSL-1 SVC_HTTP1



  Done


  > show lb vserver vserver-SSL-1 vserver-SSL-1 (10.102.29.50:443) -
     SSL Type:


  ADDRESS State: DOWN[Certkey not bound]


  Last state change was at Tue Jun 16 06:33:08 2009 (+174 ms)


  Time since last state change: 0 days, 00:31:53.70


  Effective State: DOWN Client Idle


  Timeout: 180 sec


  Down state flush: ENABLED Disable Primary Vserver On Down :
```



```
28
29
30    DISABLED No. of Bound Services : 1 (Total) 0 (Active)
31
32
33    Configured Method: LEASTCONNECTION Mode: IP Persistence: NONE Vserver
          IP and
34
35
36    Port insertion: OFF Push: DISABLED Push VServer: Push Multi Clients:
         NO Push Label Rule:
37
38
39
40
41
42    1) SVC_HTTP1 (10.102.29.18: 80) - HTTP
43
44
45    State: DOWN Weight: 1
46
47
48    Done
49  <!--NeedCopy-->
```

Liaison d'un service à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Déchargement SSL > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Sous l'onglet **Services**, dans la colonne **Actif**, cochez les cases en regard des services que vous souhaitez lier au serveur virtuel sélectionné.
4. Cliquez sur **OK**.
5. Vérifiez que le compteur Nombre de services liés dans la section Détails en bas du volet est incrémenté du nombre de services liés au serveur virtuel.

Ajouter une paire de clés de certificat

Un certificat SSL fait partie intégrante du processus d'échange de clés SSL et de chiffrement/déchiffrement. Le certificat est utilisé lors d'une connexion SSL pour établir l'identité du serveur SSL. Vous pouvez utiliser un certificat SSL valide existant que vous possédez sur l'appliance Citrix ADC, ou vous pouvez créer votre propre certificat SSL. L'appliance prend en charge les certificats RSA jusqu'à 4096 bits.

Les certificats ECDSA avec seulement les courbes suivantes sont pris en charge :

- prime256v1 (P_256 sur ADC)
- secp384r1 (P_384 sur l'ADC)
- secp521r1 (P_521 sur ADC ; pris en charge sur VPX uniquement)
- secp224r1 (P_224 sur ADC ; pris en charge sur VPX uniquement)

> **Remarque :** Citrix vous recommande d'utiliser un certificat SSL valide qui a été émis par une autorité de certification approuvée. Les certificats non valides et les certificats auto-créés ne sont pas compatibles avec tous les clients SSL.

Avant qu'un certificat puisse être utilisé pour le traitement SSL, vous devez l'associer à la clé correspondante. La paire de clés de certificat est ensuite liée au serveur virtuel et utilisée pour le traitement SSL.

Ajouter une paire de clés de certificat à l'aide de l'interface de ligne de commande

> **Remarque :** Pour plus d'informations sur la création d'une paire de clés de certificat ECDSA, voir Créer une paire de clés de certificat ECDSA.

À l'invite de commandes, tapez les commandes suivantes pour créer une paire de clés de certificat et vérifier la configuration :

```
1 -  add ssl certKey <certkeyName> -cert <string> [-key <string>]
2 -  show sslcertkey <name>
3 <!--NeedCopy-->
```

Exemple :

```
1  > add ssl certKey CertKey-SSL-1 -cert ns-root.cert -key ns-root.key
2
3   Done
4
5
6  > show sslcertkey CertKey-SSL-1
7
8
9     Name: CertKey-SSL-1 Status: Valid,
10
11
12    Days to expiration:4811 Version: 3
13
14
15    Serial Number: 00 Signature Algorithm: md5WithRSAEncryption Issuer:
         C=US,ST=California,L=San
```



```
16
17
18    Jose,O=Citrix ANG,OU=NS Internal,CN=de fault
19
20
21    Validity Not Before: Oct 6 06:52:07 2006 GMT Not After : Aug 17
          21:26:47 2022 GMT
22
23
24    Subject: C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS Internal,
          CN=d efault Public Key
25
26
27    Algorithm: rsaEncryption Public Key
28
29
30    size: 1024
31
32
33  Done
34 <!--NeedCopy-->
```

Ajouter une paire de clés de certificat à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > SSL > Certificats**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Installer le certificat**, dans la zone de texte Nom de la paire de clés de certificat, tapez un nom pour la paire de clés de certificat que vous souhaitez ajouter, par exemple CertKey-SSL-1.
4. Sous **Détails**, dans Nom du fichier de certificat, cliquez sur **Parcourir (Appliance)** pour localiser le certificat. Le certificat et la clé sont tous deux stockés dans le dossier /nsconfig/ssl/ de l'appliance. Pour utiliser un certificat présent sur le système local, sélectionnez Local.
5. Sélectionnez le certificat que vous souhaitez utiliser, puis cliquez sur **Sélectionner**.
6. Dans Nom du fichier de clé privée, cliquez sur **Parcourir (Appliance)** pour localiser le fichier de clé privée. Pour utiliser une clé privée présente sur le système local, sélectionnez Local.
7. Sélectionnez la clé que vous souhaitez utiliser, puis cliquez sur **Sélectionner**. Pour chiffrer la clé utilisée dans la paire de clés de certificat, tapez le mot de passe à utiliser pour le chiffrement dans la zone de texte Mot de passe.
8. Cliquez sur **Installer**.
9. Double-cliquez sur la paire de clés de certificat et, dans la fenêtre Détails du certificat, vérifiez

que les paramètres ont été correctement configurés et enregistrés.

Liaison d'une paire de clés de certificat SSL au serveur virtuel

Après avoir associé un certificat SSL à la clé correspondante, liez la paire de clés de certificat au serveur virtuel SSL afin qu'elle puisse être utilisée pour le traitement SSL. Les sessions sécurisées nécessitent l'établissement d'une connexion entre l'ordinateur client et un serveur virtuel SSL sur l'appliance. Le traitement SSL est ensuite effectué sur le trafic entrant sur le serveur virtuel. Par conséquent, avant d'activer le serveur virtuel SSL sur l'appliance, vous devez lier un certificat SSL valide au serveur virtuel SSL.

Liez une paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une paire de clés de certificat SSL à un serveur virtuel et vérifier la configuration :

```
-  bind ssl vserver <vServerName> -certkeyName <string>
-  show ssl vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> bind ssl vserver Vserver-SSL-1 -certkeyName CertKey-SSL-1

Done

> show ssl vserver Vserver-SSL-1



    Advanced SSL configuration for VServer Vserver-SSL-1:

    DH: DISABLED

    Ephemeral RSA: ENABLED Refresh Count: 0

```



```
21      Session Reuse: ENABLED Timeout: 120 seconds
22
23
24      Cipher Redirect: ENABLED
25
26
27      SSLv2 Redirect: ENABLED
28
29
30      ClearText Port: 0
31
32
33      Client Auth: DISABLED
34
35
36      SSL Redirect: DISABLED
37
38
39      Non FIPS Ciphers: DISABLED
40
41
42      SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
43
44
45
46
47
48  1) CertKey Name: CertKey-SSL-1 Server Certificate
49
50
51  1) Cipher Name: DEFAULT
52
53
54     Description: Predefined Cipher Alias
55
56
57  Done
58  <!--NeedCopy-->
```

Liez une paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > Déchargement SSL > Serveurs virtuels**.

2. Sélectionnez le serveur virtuel auquel vous souhaitez lier la paire de clés de certificat, par exemple, vServer-SSL-1, puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue **Configurer le serveur virtuel (déchargement SSL)**, sous l'onglet **Paramètres SSL**, sous **Disponible**, sélectionnez la paire de clés de certificat que vous souhaitez lier au serveur virtuel. Cliquez ensuite sur **Ajouter**.
4. Cliquez sur **OK**.
5. Vérifiez que la paire de clés de certificat que vous avez sélectionnée apparaît dans la zone Configuré.

Configurer la prise en charge de Outlook Web

Si vous utilisez des serveurs Outlook Web Access (OWA) sur votre appliance Citrix ADC, vous devez configurer l'appliance pour insérer un champ d'en-tête spécial, FRONT-END-HTTPS : ON, dans les requêtes HTTP dirigées vers les serveurs OWA, afin que les serveurs génèrent des liens URL `https://` au lieu de `http://`.

Remarque : Vous pouvez activer la prise en charge d'OWA pour les serveurs et services virtuels SSL basés sur HTTP uniquement. Vous ne pouvez pas l'appliquer aux serveurs et services virtuels SSL basés sur TCP.

Pour configurer la prise en charge d'OWA, procédez comme suit :

- Créez une action SSL pour activer la prise en charge d'OWA.
- Créez une stratégie SSL.
- Liez la stratégie au serveur virtuel SSL.

Créer une action SSL pour activer la prise en charge d'OWA

Avant de pouvoir activer la prise en charge d'Outlook Web Access (OWA), vous devez créer une action SSL. Les actions SSL sont liées aux stratégies SSL et sont déclenchées lorsque les données entrantes correspondent à la règle spécifiée par la stratégie.

Créer une action SSL pour activer la prise en charge d'OWA à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une action SSL afin d'activer la prise en charge d'OWA et de vérifier la configuration :

```
1 -  add ssl action <name> -OWASupport ENABLED
2 -  show SSL action <name>
3 <!--NeedCopy-->
```

Exemple :


```
1      > add ssl action Action-SSL-OWA -OWASupport enabled
2
3
4
5
6      Done
7
8
9      > show SSL action Action-SSL-OWA
10
11
12     Name: Action-SSL-OWA
13
14
15     Data Insertion Action: OWA
16
17
18     Support: ENABLED
19
20
21     Done
22 <!--NeedCopy-->
```

Créer une action SSL pour activer la prise en charge d'OWA à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > SSL > Stratégies**.
2. Dans le volet d'informations, sous l'onglet **Actions**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action SSL**, dans la zone de texte Nom, tapez Action-SSL-OWA.
4. Sous Outlook Web Access, sélectionnez **Activé**.
5. Cliquez sur **Créer**, puis cliquez sur **Fermer**.
6. Vérifiez que Action-SSL-OWA apparaît dans la page **Actions SSL** .

Créer des stratégies SSL

Les stratégies SSL sont créées à l'aide de l'infrastructure de stratégies. Chaque stratégie SSL est liée à une action SSL, et l'action est exécutée lorsque le trafic entrant correspond à la règle configurée dans la stratégie.

Créer une stratégie SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une stratégie SSL et vérifier la configuration :

```
1 -  add ssl policy <name> -rule <expression> -reqAction <string>
2 -  show ssl policy <name>
3 <!--NeedCopy-->
```

Exemple :

```
1  > add ssl policy-SSL-1 -rule ns_true -reqaction Action-SSL-OWA
2
3  Done
4
5  > show ssl policy-SSL-1
6
7  Name: Policy-SSL-1 Rule: ns_true
8
9  Action: Action-SSL-OWA Hits: 0
10
11 Policy is bound to following entities
12
13 1) PRIORITY : 0
14
15 Done
16 <!--NeedCopy-->
```

Créer une stratégie SSL à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > SSL > Stratégies**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une stratégie SSL**, dans la zone de texte Nom, tapez le nom de la stratégie SSL (par exemple, Policy-SSL-1).
4. Dans **Demander** une action, sélectionnez l'action SSL configurée que vous souhaitez associer à cette stratégie (par exemple, Action-SSL-OWA). L'expression générale ns_true applique la stratégie à tout le trafic d'établissement de liaison SSL réussi. Toutefois, pour filtrer des réponses spécifiques, vous pouvez créer des stratégies avec un niveau de détail supérieur. Pour plus d'informations sur la configuration des expressions de stratégie granulaires, consultez Actions et stratégies SSL.
5. Dans **Expressions nommées**, choisissez l'expression générale intégrée ns_true et cliquez sur

Ajouter une expression. L'expression ns_true apparaît désormais dans la zone de texte Expression.

6. Cliquez sur **Créer**, puis cliquez sur **Fermer**.
7. Vérifiez que la stratégie est correctement configurée en sélectionnant la stratégie et en affichant la section Détails en bas du volet.

Liez la stratégie SSL au serveur virtuel SSL

Après avoir configuré une stratégie SSL pour Outlook Web Access, liez la stratégie à un serveur virtuel qui interceptera le trafic Outlook entrant. Si les données entrantes correspondent à l'une des règles configurées dans la stratégie SSL, la stratégie est déclenchée et l'action qui lui est associée est exécutée.

Liez une stratégie SSL à un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une stratégie SSL à un serveur virtuel SSL et vérifier la configuration :

```
- bind ssl vserver <vServerName> -policyName <string>
- show ssl vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> bind ssl vserver Vserver-SSL-1 -policyName Policy-SSL-1

 Done

> show ssl vserver Vserver-SSL-1

Advanced SSL configuration for VServer Vserver-SSL-1:

DH: DISABLED

Ephemeral RSA: ENABLED

Refresh Count: 0

Session Reuse: ENABLED

Timeout: 120 seconds

Cipher Redirect: ENABLED
```



```
20
21 SSLv2 Redirect: ENABLED
22
23 ClearText Port: 0
24
25 Client Auth: DISABLED
26
27 SSL Redirect: DISABLED
28
29 Non FIPS Ciphers: DISABLED
30
31 SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
32
33 1) CertKey Name: CertKey-SSL-1 Server Certificate
34
35 1) Policy Name: Policy-SSL-1 Priority: 0
36
37 1) Cipher Name: DEFAULT Description: Predefined Cipher Alias
38
39 Done
40 <!--NeedCopy-->
```

Liez une stratégie SSL à un serveur virtuel SSL à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > Déchargement SSL > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel (par exemple, vServer-SSL-1), puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le serveur virtuel (déchargement SSL)**, cliquez sur **Insérer une stratégie**, puis sélectionnez la stratégie que vous souhaitez lier au serveur virtuel SSL. Vous pouvez également double-cliquer sur le champ Priorité et saisir un nouveau niveau de priorité.
4. Cliquez sur **OK**.

Caractéristiques en un coup d'œil

August 20, 2021

Les fonctionnalités de Citrix ADC peuvent être configurées indépendamment ou en combinaison pour répondre à des besoins spécifiques. Bien que certaines fonctionnalités correspondent à plus

d'une catégorie, les nombreuses fonctionnalités de Citrix ADC peuvent généralement être classées en tant que fonctionnalités de commutation d'applications et de gestion du trafic, fonctionnalités d'accélération des applications, fonctionnalités de sécurité et de pare-feu des applications, et fonctionnalité de visibilité des applications.

Pour comprendre l'ordre dans lequel les fonctions effectuent leur traitement, reportez-vous à la section Ordre de traitement des fonctionnalités .

Fonctions de commutation des applications et de gestion du trafic

October 5, 2021

Vous trouverez ci-dessous les fonctionnalités de commutation d'applications et de gestion du trafic.

Déchargement SSL

Décharge de manière transparente le chiffrement et le déchiffrement SSL des serveurs Web, libérant ainsi les ressources du serveur pour répondre aux demandes de contenu. SSL pèse lourdement sur les performances d'une application et peut rendre inefficaces de nombreuses mesures d'optimisation. Le déchargement et l'accélération SSL permettent d'appliquer tous les avantages de la technologie Citrix Request Switching au trafic SSL, garantissant une livraison sécurisée des applications Web sans dégrader les performances de l'utilisateur final.

Pour plus d'informations, voir Déchargement et accélération SSL.

Listes de contrôle d'accès

Compare les paquets entrants aux listes de contrôle d'accès (ACL). Si un paquet correspond à une règle ACL, l'action spécifiée dans la règle est appliquée au paquet. Sinon, l'action par défaut (ALLOW) est appliquée et le paquet est traité normalement. Pour que la solution matérielle-logicielle compare les paquets entrants aux listes de contrôle d'accès, vous devez appliquer les listes de contrôle d'accès. Toutes les listes de contrôle d'accès sont activées par défaut, mais vous devez les appliquer pour que l'appliance Citrix ADC puisse comparer les paquets entrants avec eux. Si une liste de contrôle d'accès n'est pas obligatoire pour faire partie de la table de choix, mais doit tout de même être conservée dans la configuration, elle doit être désactivée avant l'application des listes de contrôle d'accès. Une appliance ADC ne compare pas les paquets entrants aux listes ACL désactivées.

Pour plus d'informations, voir Liste de contrôle d'accès.

Équilibrage de charge

Les décisions d'équilibrage de charge sont basées sur une variété d'algorithmes, notamment le tourniquet, le moins de connexions, la moindre bande passante pondérée, le moins de paquets pondéré, le temps de réponse minimal et le hachage basé sur l'URL, l'adresse IP source du domaine ou l'adresse IP de destination. Les protocoles TCP et UDP sont tous deux pris en charge, de sorte que l'appliance Citrix ADC peut équilibrer la charge de tout le trafic qui utilise ces protocoles comme opérateur sous-jacent (par exemple, HTTP, HTTPS, UDP, DNS, NNTP et le trafic général du pare-feu). En outre, l'appliance ADC peut maintenir la persistance de la session en fonction de l'adresse IP source, du cookie, du serveur, du groupe ou de la session SSL. Il permet aux utilisateurs d'appliquer la vérification étendue du contenu (ECV) personnalisée aux serveurs, caches, pare-feu et autres périphériques d'infrastructure afin de s'assurer que ces systèmes fonctionnent correctement et fournissent le bon contenu aux utilisateurs. Il peut également effectuer des vérifications de l'état à l'aide d'URL ping, TCP ou HTTP, et l'utilisateur peut créer des moniteurs basés sur des scripts Perl. Pour fournir une optimisation WAN à grande échelle, les appliances CloudBridge déployées dans les centres de données peuvent être équilibrées par le biais d'appliances Citrix ADC. La bande passante et le nombre de sessions simultanées peuvent être considérablement améliorés.

Pour plus d'informations, voir Équilibrage de charge.

Domaines de trafic

Les domaines de trafic permettent de créer des partitions ADC logiques au sein d'une seule appliance Citrix ADC. Ils vous permettent de segmenter le trafic réseau pour différentes applications. Vous pouvez utiliser des domaines de trafic pour créer plusieurs environnements isolés dont les ressources n'interagissent pas entre elles. Une application appartenant à un domaine de trafic spécifique communique uniquement avec les entités et traite le trafic au sein de ce domaine. Le trafic appartenant à un domaine de trafic ne peut pas franchir la limite d'un autre domaine de trafic. Par conséquent, vous pouvez utiliser des adresses IP dupliquées sur l'appliance tant qu'une adresse n'est pas dupliquée dans le même domaine.

Pour plus d'informations, voir Domaines de trafic.

Traduction d'adresses réseau

La traduction d'adresses réseau (NAT) implique la modification des adresses IP source et/ou de destination, et/ou des numéros de port TCP/UDP, des paquets IP qui passent par l'appliance Citrix ADC. L'activation de la NAT sur l'appliance améliore la sécurité de votre réseau privé et le protège d'un réseau public tel qu'Internet, en modifiant les adresses IP sources de votre réseau lorsque les données passent par l'appliance Citrix ADC.

L'appliance Citrix ADC prend en charge les types de traduction d'adresses réseau suivants :

INAT : Dans le NAT entrant (INAT), une adresse IP (généralement publique) configurée sur l'appliance Citrix ADC écoute les demandes de connexion pour le compte d'un serveur. Pour un paquet de demande reçu par l'appliance sur une adresse IP publique, l'ADC remplace l'adresse IP de destination par l'adresse IP privée du serveur. En d'autres termes, la solution matérielle-logicielle agit comme un proxy entre les clients et le serveur. La configuration INAT implique des règles INAT, qui définissent une relation 1:1 entre l'adresse IP de l'appliance Citrix ADC et l'adresse IP du serveur.

RNAT : dans Reverse Network Address Translation (RNAT), pour une session initiée par un serveur, l'appliance Citrix ADC remplace l'adresse IP source dans les paquets générés par le serveur par une adresse IP (type SNIP) configurée sur l'appliance. La solution matérielle-logicielle empêche ainsi l'exposition de l'adresse IP du serveur dans l'un des paquets générés par le serveur. Une configuration RNAT implique une règle RNAT, qui spécifie une condition. La solution matérielle-logicielle effectue un traitement RNAT sur les paquets qui correspondent à la condition.

Traduction NAT46 sansétat : Stateless NAT46 permet la communication entre les réseaux IPv4 et IPv6, via la traduction de paquets IPv4 vers IPv6 et vice versa, sans conserver les informations de session sur l'appliance Citrix ADC. Une configuration NAT46 sans état implique une règle INAT IPv4-IPv6 et un préfixe IPv6 NAT46.

Traduction NAT64avec état : La fonctionnalité NAT64 avec état permet la communication entre les clients IPv4 et les serveurs IPv6 via la traduction de paquets IPv6 vers IPv4, et vice versa, tout en conservant les informations de session sur l'appliance Citrix ADC. Une configuration NAT64 avec état implique une règle NAT64 et un préfixe NAT64 IPv6.

Pour plus d'informations, voir Configuration de la traduction d'adresses réseau.

Prise en charge du protocole TCP multichemin

Les appliances Citrix ADC prennent en charge le protocole Multipath TCP (MPTCP). MPTCP est une extension de protocole TCP/IP qui identifie et utilise plusieurs chemins disponibles entre les hôtes pour maintenir la session TCP. Vous devez activer MPTCP sur un profil TCP et le lier à un serveur virtuel. Lorsque MPTCP est activé, le serveur virtuel fonctionne comme une Gateway MPTCP et convertit les connexions MPTCP avec les clients en connexions TCP qu'il maintient avec les serveurs.

Pour plus d'informations, voir MPTCP (Multi-Path TCP).

Commutation de contenu

Détermine le serveur auquel envoyer la demande sur la base des stratégies de commutation de contenu configurées. Les règles de stratégie peuvent être basées sur l'adresse IP, l'URL et les en-têtes HTTP. Cela permet de prendre des décisions de changement en fonction des caractéristiques de l'utilisateur et de l'appareil, telles que l'identité de l'utilisateur, le type d'agent utilisé et le contenu demandé par l'utilisateur.

Pour plus d'informations, voir Commutation de contenu.

Équilibrage global de charge serveur (GSLB)

Étend les fonctionnalités de gestion du trafic d'un NetScaler pour inclure des sites Internet distribués et des entreprises internationales. Que les installations soient réparties sur plusieurs emplacements réseau ou sur plusieurs clusters en un seul emplacement, NetScaler maintient la disponibilité et répartit le trafic entre eux. Il prend des décisions DNS intelligentes pour empêcher les utilisateurs d'être envoyés vers un site en panne ou en surcharge. Lorsque la méthode GSLB basée sur la proximité est activée, NetScaler peut prendre des décisions d'équilibrage de charge en fonction de la proximité du serveur DNS local (LDNS) du client par rapport aux différents sites. Le principal avantage de la méthode GSLB basée sur la proximité est un temps de réponse plus rapide résultant de la sélection du site disponible le plus proche.

Pour plus d'informations, voir Global Server Load Balancing.

Routage dynamique

Permet aux routeurs d'obtenir automatiquement des informations de topologie, des itinéraires et des adresses IP des routeurs voisins. Lorsque le routage dynamique est activé, le processus de routage correspondant écoute les mises à jour des itinéraires et publie les itinéraires. Les processus de routage peuvent également être placés en mode passif. Les protocoles de routage permettent à un routeur en amont d'équilibrer la charge du trafic vers des serveurs virtuels identiques hébergés sur deux unités NetScaler autonomes à l'aide de la technique Equal Cost Multipath.

Pour plus d'informations, reportez-vous à la section Configuration des routes dynamiques.

Équilibrage de la charge de liaison

Équilibre la charge de plusieurs liaisons WAN et assure le basculement des liaisons, ce qui optimise davantage les performances du réseau et assure la continuité de l'activité. Garantit que les connexions réseau restent hautement disponibles, en appliquant un contrôle intelligent du trafic et des vérifications de l'état pour répartir efficacement le trafic sur les routeurs en amont. Identifie la meilleure liaison WAN pour acheminer le trafic entrant et sortant en fonction des stratégies et des conditions réseau, et protège les applications contre les défaillances de WAN ou de liaison Internet en fournissant une détection rapide des pannes et un basculement sur incident.

Pour plus d'informations, voir Équilibrage de charge de liaison.

Optimisation TCP

Vous pouvez utiliser des profils TCP pour optimiser le trafic TCP. Les profils TCP définissent la façon dont les serveurs virtuels NetScaler traitent le trafic TCP. Les administrateurs peuvent utiliser les profils TCP intégrés ou configurer des profils personnalisés. Après avoir défini un profil TCP, vous pouvez le lier à un seul serveur virtuel ou à plusieurs serveurs virtuels.

Voici quelques-unes des principales fonctionnalités d'optimisation qui peuvent être activées par les profils TCP :

- TCP Keep-Avie : vérifie l'état opérationnel des homologues à des intervalles de temps spécifiés pour éviter que la liaison ne soit interrompue.
- Accusé de réception sélectif (SACK) — Améliore les performances de transmission des données, en particulier dans les réseaux LFN (Long Fat Networks).
- Mise à l'échelle de la fenêtre TCP : permet un transfert efficace de données sur les réseaux longs (LFN).

Pour plus d'informations sur les profils TCP, voir Configuration des profils TCP.

CloudBridge Connector

La fonctionnalité Citrix NetScaler CloudBridge Connector, un élément fondamental du framework Citrix OpenCloud, est un outil utilisé pour créer un centre de données étendu dans le cloud. OpenCloud Bridge vous permet de connecter une ou plusieurs appliances Citrix ADC ou NetScaler virtuelles sur le cloud à votre réseau sans reconfigurer votre réseau. Les applications hébergées dans le cloud semblent s'exécuter sur un réseau d'entreprise contigu. L'objectif principal d'OpenCloud Bridge est de permettre aux entreprises de déplacer leurs applications vers le cloud tout en réduisant les coûts et le risque de défaillance des applications. En outre, OpenCloud Bridge augmente la sécurité du réseau dans les environnements cloud. Un pont OpenCloud est un pont réseau de couche 2 qui connecte un dispositif Citrix ADC ou un dispositif virtuel NetScaler sur une instance de cloud à un dispositif Citrix ADC ou NetScaler virtuel sur votre réseau local. La connexion est établie via un tunnel qui utilise le protocole GRE (Generic Routing Encapsulation). Le protocole GRE fournit un mécanisme d'encapsulation de paquets provenant d'une grande variété de protocoles réseau à transférer via un autre protocole. Ensuite, la suite de protocoles IPSec (Internet Protocol security) est utilisée pour sécuriser la communication entre les pairs dans OpenCloud Bridge.

Pour plus d'informations, voir CloudBridge.

DataStream

La fonctionnalité NetScaler DataStream fournit un mécanisme intelligent de commutation de demande au niveau de la couche de base de données en distribuant les demandes en fonction de la requête SQL envoyée.

Lorsqu'il est déployé devant des serveurs de base de données, NetScaler assure une distribution optimale du trafic provenant des serveurs d'applications et des serveurs Web. Les administrateurs peuvent segmenter le trafic en fonction des informations contenues dans la requête SQL et en fonction des noms de base de données, des noms d'utilisateur, des jeux de caractères et de la taille des paquets.

Vous pouvez configurer l'équilibrage de charge pour basculer les demandes en fonction d'algorithmes d'équilibrage de charge, ou vous pouvez élaborer les critères de commutation en configurant la commutation de contenu pour prendre une décision en fonction des paramètres de requête SQL, tels que le nom d'utilisateur, les noms de base de données et les paramètres de commande. Vous pouvez également configurer des moniteurs pour suivre l'état des serveurs de base de données.

L'infrastructure de stratégie avancée de l'appliance Citrix ADC inclut des expressions que vous pouvez utiliser pour évaluer et traiter les demandes. Les expressions avancées évaluent le trafic associé aux serveurs de base de données MySQL. Vous pouvez utiliser des expressions basées sur les demandes (expressions commençant par MYSQL.CLIENT et MYSQL.REQ) dans des stratégies avancées pour prendre des décisions de changement de demande au niveau du point de liaison du serveur virtuel de commutation de contenu et des expressions basées sur les réponses (expressions commençant par MYSQL.RES) pour évaluer les réponses du serveur aux utilisateurs moniteurs de santé configurés.

> Remarque : DataStream est pris en charge pour les bases de données MySQL et MS SQL.

Pour plus d'informations, voir DataStream.

Fonctionnalités d'accélération des applications

August 20, 2021

- AppCompress

  Utilise le protocole de compression gzip pour fournir une compression transparente pour les fichiers HTML et texte. Le taux de compression standard de 4:1 permet de réduire jusqu'à 50 % les besoins en bande passante hors du datacenter. Cela permet également d'améliorer considérablement le temps de réponse de l'utilisateur final, car il réduit la quantité de données qui doivent être transmises au navigateur de l'utilisateur.

- Redirection de cache

  Gère le flux du trafic vers un proxy inverse, un proxy transparent ou une batterie de cache proxy de transfert. Inspecte toutes les demandes, identifie les demandes non mises en cache et les envoie directement aux serveurs d'origine via des connexions persistantes. En redirigeant intelligemment les requêtes non mises en cache vers les serveurs Web d'origine, l'appliance Citrix

ADC libère les ressources du cache et augmente les taux d'utilisation du cache tout en réduisant la consommation globale de bande passante et les délais de réponse pour ces demandes.

Pour plus d'informations, voir Redirection du cache.

- AppCache

  Aide à optimiser le contenu Web et la diffusion des données d'application en fournissant une mise en cache Web conforme rapide en mémoire HTTP/1.1 et HTTP/1.0 pour le contenu statique et dynamique. Ce cache intégré stocke les résultats des demandes d'application entrantes même lorsqu'une demande entrante est sécurisée ou que les données sont compressées, puis réutilise les données pour répondre aux demandes ultérieures pour les mêmes informations. En diffusant des données directement à partir du cache intégré, l'appliance peut réduire les temps de régénération des pages en éliminant la nécessité d'entonnoir les demandes de contenu statique et dynamique vers le serveur.

  Pour plus d'informations, consultez la section Mise en cache intégrée.

- Mise en mémoire tampon TCP

  Mémorise la réponse du serveur et la livre au client à la vitesse du client, déchargeant ainsi le serveur plus rapidement et améliorant ainsi les performances des sites Web.

Fonctionnalités de sécurité des applications et de pare-feu

October 5, 2021

Vous trouverez ci-dessous les fonctionnalités de sécurité et de pare-feu.

Défense contre les attaques par déni de service (DoS)

Détecte et arrête les attaques malveillantes par déni de service distribué (DDoS) et les autres types d'attaques malveillantes avant qu'elles n'atteignent vos serveurs, ce qui les empêche d'affecter les performances du réseau et des applications. L'appliance Citrix ADC identifie les clients légitimes et augmente leur priorité, ce qui empêche les clients suspects d'utiliser un pourcentage disproportionné de ressources et de paralyser votre site. La solution matérielle-logicielle offre une protection au niveau de l'application contre les types d'attaques malveillantes suivants :

- Attaques par inondation SYN
- Les attaques de pipeline
- Attaques en forme de larme
- Attaques terrestres
- Attaques fraggle

- Attaques de connexion Zombie

La solution matérielle-logicielle se défend de manière agressive contre ces types d'attaques en empêchant l'allocation de ressources serveur pour ces connexions. Cela permet d'isoler les serveurs du flot écrasant de paquets associé à ces événements.

L'appliance protège également les ressources réseau contre les attaques ICMP en utilisant la limitation de débit ICMP et l'inspection agressive des paquets ICMP. Il effectue un réassemblage IP puissant, supprime une variété de paquets suspects et mal formés et applique des listes de contrôle d'accès (ACL) au trafic du site pour une protection supplémentaire.

Pour plus d'informations, voir Protection par déni de service HTTP.

Filtrage de contenu

Offre une protection contre les attaques malveillantes des sites Web au niveau de la couche 7. La solution matérielle-logicielle inspecte chaque demande entrante en fonction des règles configurées par l'utilisateur en fonction des en-têtes HTTP, et exécute l'action configurée par l'utilisateur. Les actions peuvent inclure la réinitialisation de la connexion, la suppression de la demande ou l'envoi d'un message d'erreur au navigateur de l'utilisateur. Cela permet à la solution matérielle-logicielle de filtrer les demandes indésirables et de réduire l'exposition de vos serveurs aux attaques.

Cette fonctionnalité peut également analyser les requêtes HTTP GET et POST et filtrer les signatures erronées connues, ce qui lui permet de défendre vos serveurs contre les attaques HTTP.

Pour plus d'informations, voir Filtrage de contenu.

Répondeur

Fonctionne comme un filtre avancé et peut être utilisé pour générer des réponses de la solution matérielle-logicielle vers le client. Certaines utilisations courantes de cette fonctionnalité sont la génération de réponses de redirection, les réponses définies par l'utilisateur et les réinitialisations.

Pour plus d'informations, voir Répondeur.

Réécrire

Modifie les en-têtes HTTP et le corps du texte. Vous pouvez utiliser la fonction de réécriture pour ajouter des en-têtes HTTP à une requête ou une réponse HTTP, apporter des modifications à des en-têtes HTTP individuels ou supprimer des en-têtes HTTP. Il vous permet également de modifier le corps HTTP des requêtes et des réponses.

Lorsque l'appliance reçoit une demande ou envoie une réponse, elle vérifie les règles de réécriture et, s'il existe des règles applicables, elle les applique à la demande ou à la réponse avant de la transmettre au serveur Web ou à l'ordinateur client.

Pour plus d'informations, voir Réécriture.

Protection contre les surtensions

Réglemente le flux des demandes des utilisateurs vers les serveurs et contrôle le nombre d'utilisateurs pouvant accéder simultanément aux ressources sur les serveurs, en mettant en file d'attente toute demande supplémentaire une fois que vos serveurs ont atteint leur capacité. En contrôlant la vitesse à laquelle les connexions peuvent être établies, l'appliance bloque les surtensions de demandes d'être transmises à vos serveurs, évitant ainsi la surcharge du site.

Pour plus d'informations, voir Protection contre les surtensions.

Citrix Gateway

Citrix Gateway est une solution d'accès sécurisé aux applications qui fournit aux administrateurs des stratégies et des contrôles d'action granulaires au niveau des applications pour sécuriser l'accès aux applications et aux données tout en permettant aux utilisateurs de travailler de n'importe où. Il offre aux administrateurs informatiques un point de contrôle unique et des outils pour garantir la conformité aux réglementations et les plus hauts niveaux de sécurité des informations à l'échelle de l'entreprise et à l'extérieur. En même temps, il offre aux utilisateurs un point d'accès unique (optimisé pour les rôles, les appareils et les réseaux) aux applications et données d'entreprise dont ils ont besoin. Cette combinaison unique de capacités permet de maximiser la productivité de la main-d'œuvre mobile d'aujourd'hui.

Pour plus d'informations, consultez Citrix Gateway.

Pare-feu d'application

Protège les applications contre toute utilisation abusive par des pirates et des logiciels malveillants, tels que les attaques de script intersite, les attaques par débordement de la mémoire tampon, les attaques par injection SQL et la navigation forcée, en filtrant le trafic entre chaque serveur Web protégé et les utilisateurs qui se connectent à n'importe quel site Web sur ce serveur Web. Le pare-feu de l'application examine tout le trafic pour y trouver des preuves d'attaques sur la sécurité du serveur Web ou d'utilisation abusive des ressources du serveur Web, et prend les mesures appropriées pour empêcher ces attaques de se produire.

Pour plus d'informations, reportez-vous à la section Pare-feu d'application.

Fonctionnalité de visibilité des applications

August 20, 2021

- Citrix Application Delivery Management

  Citrix Application Delivery Management (ADM) est un collecteur hautes performances qui offre une visibilité de l'expérience utilisateur de bout en bout sur le trafic Web et HDX (ICA). Il collecte les enregistrements AppFlow HTTP et ICA générés par les appliances Citrix ADC et remplit les rapports analytiques couvrant les statistiques de couche 3 à 7. Citrix ADM fournit une analyse approfondie des cinq dernières minutes de données en temps réel et des données historiques collectées au cours des dernières heures, un jour, une semaine et un mois.

  Le tableau de bord analytique HDX (ICA) vous permet d'effectuer une analyse descendante à partir des utilisateurs HDX, des applications, des ordinateurs de bureau et même des informations de niveau passerelle. De même, les analyses HTTP fournissent une vue d'ensemble des applications Web, des URL consultées, des adresses IP du client et des adresses IP du serveur, et d'autres tableaux de bord. L'administrateur peut effectuer une analyse vers le bas et identifier les points de difficultés à partir de n'importe lequel de ces tableaux de bord, selon le cas d'utilisation.

- Visibilité améliorée des applications à l'aide d'AppFlow

  L'appliance Citrix ADC est un point central de contrôle pour tout le trafic d'application dans le datacenter. Il recueille des informations de flux et de session utilisateur utiles pour la surveillance des performances des applications, l'analyse et les applications décisionnelles. AppFlow transmet ces informations à l'aide du format IPFIX (Internet Protocol Flow Information Export), qui est un standard ouvert Internet Engineering Task Force (IETF) défini dans la RFC 5101. IPFIX (la version standardisée de NetFlow de Cisco) est largement utilisé pour surveiller les informations de flux réseau. AppFlow définit de nouveaux éléments d'information pour représenter les informations au niveau de l'application.

  En utilisant UDP comme protocole de transport, AppFlow transmet les données collectées, appelées *enregistrements de flux*, à un ou plusieurs collecteurs IPv4. Les collecteurs regroupent les enregistrements de flux et génèrent des rapports en temps réel ou historiques.

  AppFlow fournit une visibilité au niveau de la transaction pour les flux HTTP, SSL, TCP et SSL_TCP. Vous pouvez échantillonner et filtrer les types de flux que vous souhaitez surveiller.

  Pour limiter les types de flux à surveiller, en échantillonnant et en filtrant le trafic d'application, vous pouvez activer AppFlow pour un serveur virtuel. AppFlow peut également fournir des statistiques pour le serveur virtuel.

  Vous pouvez également activer AppFlow pour un service spécifique, représentant un serveur d'applications, et surveiller le trafic vers ce serveur d'applications.

  Pour plus d'informations, voir AppFlow.

- Analyses de flux

La performance de votre site Web ou application dépend de la manière dont vous optimisez la diffusion du contenu le plus fréquemment demandé. Des techniques telles que la mise en cache et la compression aident à accélérer la fourniture de services aux clients, mais vous devez être en mesure d'identifier les ressources demandées le plus fréquemment, puis de mettre en cache ou de compresser ces ressources. Vous pouvez identifier les ressources les plus fréquemment utilisées en regroupant des statistiques en temps réel sur le trafic des sites Web ou des applications. Des statistiques telles que la fréquence d'accès à une ressource par rapport à d'autres ressources et la quantité de bande passante consommée par ces ressources vous aident à déterminer si ces ressources doivent être mises en cache ou compressées pour améliorer les performances du serveur et l'utilisation du réseau. Des statistiques telles que les temps de réponse et le nombre de connexions simultanées à l'application vous aident à déterminer si vous devez améliorer les ressources côté serveur.

Si le site Web ou l'application ne change pas fréquemment, vous pouvez utiliser des produits qui collectent des données statistiques, puis analyser manuellement les statistiques et optimiser la diffusion du contenu. Toutefois, si vous ne souhaitez pas effectuer d'optimisation manuelle, ou si votre site Web ou application est de nature dynamique, vous avez besoin d'une infrastructure capable non seulement de collecter des données statistiques, mais aussi d'optimiser automatiquement la fourniture de ressources en fonction des statistiques. Sur l'appliance Citrix ADC, cette fonctionnalité est fournie par la fonctionnalité Stream Analytics. La fonctionnalité fonctionne sur une seule appliance Citrix ADC et recueille des statistiques d'exécution en fonction des critères que vous définissez. Lorsqu'elle est utilisée avec les stratégies Citrix ADC, la fonctionnalité vous fournit également l'infrastructure dont vous avez besoin pour une optimisation automatique du trafic en temps réel.

Pour plus d'informations, voir Action Analytics.

Solutions Citrix ADC

January 21, 2021

Les solutions Citrix ADC simplifient la tâche de configuration des configurations fréquemment déployées. Vérifiez cet espace de temps en temps pour trouver des solutions supplémentaires.

Cette section comprend les solutions suivantes.

- Configuration de Citrix ADC pour Citrix Virtual Apps and Desktops
- Préférence de zone optimisée pour l'équilibrage de la charge du serveur global (GSLB)
- Prise en charge Anycast dans Citrix ADC
- Déploiement d'une plateforme de publicité numérique sur AWS avec Citrix ADC
- Amélioration de l'analyse des flux de clics dans AWS à l'aide de Citrix ADC

- Citrix ADC dans un cloud privé géré par Microsoft Windows Azure Pack et Cisco ACI

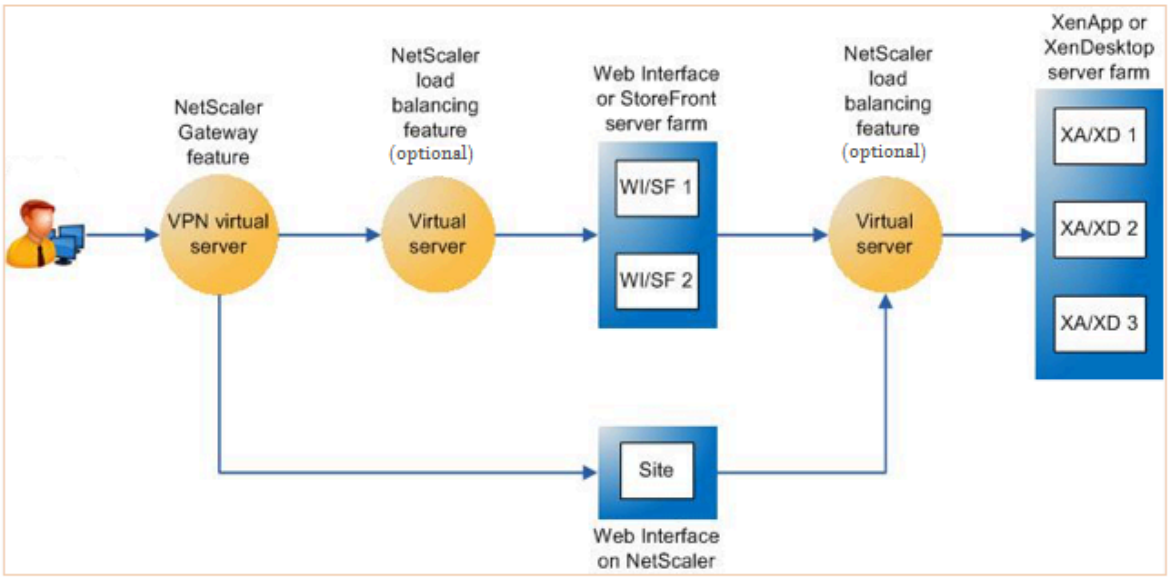
Configuration de Citrix ADC pour Citrix Virtual Apps and Desktops

January 21, 2021

Une appliance Citrix ADC peut fournir un accès distant sécurisé et équilibré de la charge à vos applications Citrix Virtual Apps and Desktops. Vous pouvez utiliser la fonctionnalité d'équilibrage de charge Citrix ADC pour répartir le trafic sur le serveur Citrix Virtual Apps and Desktops. Vous pouvez utiliser la fonctionnalité Citrix Gateway pour fournir un accès distant sécurisé aux serveurs.

Citrix ADC peut également accélérer et optimiser le flux de trafic et offrir des fonctionnalités de visibilité utiles pour les déploiements Citrix Virtual Apps and Desktops.

Figure 1. Appliance Citrix ADC dans Citrix Virtual Apps and Desktops Configuration



La figure précédente montre les composantes impliquées dans ce déploiement :

- **NetScaler Gateway.** Fournit l'URL pour l'accès des utilisateurs et assure la sécurité en authentifiant les utilisateurs.
- **Serveur virtuel d'équilibrage de charge Citrix ADC.** La charge équilibre le trafic pour l'interface Web ou les serveurs StoreFront. Vous pouvez également déployer un serveur virtuel

d'équilibrage de charge devant les serveurs Citrix Virtual Apps et Desktop pour équilibrer la charge des composants clés tels que XML Broker et Desktop Delivery Controller (DDC).

- **Interface Web ou StoreFront ou Interface Web sur Citrix ADC.** Fournit l'interface à travers laquelle vous pouvez accéder aux applications.

  Remarque : L'interface Web sur Citrix ADC (WiONs) est une personnalisation du produit Interface Web, hébergé sur l'appliance Citrix ADC.

- **Citrix Virtual Apps and Desktops.** Fournit les applications auxquelles vos utilisateurs souhaitent accéder.

Pour configurer Citrix ADC pour Citrix Virtual Apps and Desktops à l'aide de l'interface graphique Citrix ADC

Conditions préalables

- Les serveurs Citrix Virtual Apps et Desktop sont configurés et disponibles.
- Interface Web, StoreFront ou Interface Web sur les serveurs Citrix ADC sont configurés et disponibles.
- Vous avez une connaissance pratique de Citrix Gateway, Citrix ADC, Citrix Virtual Apps and Desktops et StoreFront/Interface Web sur Citrix ADC.
- Assurez-vous que vous avez configuré un serveur virtuel et un service et que vous avez lié le service au serveur virtuel. Pour plus d'informations, consultez :
  - Équilibre de charge XenDesktop
  - Équilibre de charge XenApp

Procédure :

1. Ouvrez une session sur l'appliance Citrix ADC et, sous l'onglet **Configuration**, cliquez sur **XenApp et XenDesktop**.
2. Dans le volet **Détails**, cliquez sur **Démarrer**. Si le programme d'installation existe sur Citrix ADC, cliquez sur le lien **Modifier** correspondant à chacune des sections que vous souhaitez modifier.
3. Sélectionnez le produit (StoreFront, Interface Web ou Interface Web sur Citrix ADC) qui, dans votre déploiement, fournit l'interface permettant d'accéder aux applications Citrix Virtual Apps and Desktops.
4. Configurez l'accès à distance sécurisé.
   a) Dans la section **Paramètres NetScaler Gateway**, spécifiez les détails du serveur virtuel VPN et cliquez sur **Continuer**.
   b) Dans la section **Certificat de serveur**, choisissez un certificat existant ou installez un nouveau certificat et cliquez sur **Continuer**.

c) Dans la section **Authentification**, configurez le mécanisme d'authentification principal à utiliser et spécifiez les détails du serveur ou utilisez un serveur existant, puis cliquez sur **Continuer**.

d) Dans la section **StoreFront**, spécifiez les détails du serveur qui fournit l'interface permettant d'accéder aux applications et cliquez sur **Continuer**.

e) Vous pouvez utiliser l'une des options suivantes comme serveur StoreFront.

i. Serveur virtuel LB pointant vers plusieurs serveurs SF.
ii. Interface Web ou serveur StoreFront directement accessible depuis l'appliance Citrix ADC.
iii. Interface Web sur Citrix ADC.

5. Cliquez sur **Terminé** pour terminer la configuration.

Préférence de zone optimisée pour l'équilibrage de la charge du serveur global (GSLB)

August 20, 2021

La préférence de zone alimentée par GSLB est une fonctionnalité qui intègre Citrix Virtual Apps and Desktops, StoreFront et Citrix ADC pour fournir aux clients un accès au datacenter le plus optimisé en fonction de l'emplacement du client.

Dans un déploiement distribué Citrix Virtual Apps and Desktops, StoreFront peut ne pas sélectionner un centre de données optimal lorsque plusieurs ressources équivalentes sont disponibles à partir de plusieurs centres de données. Dans de tels cas, StoreFront sélectionne au hasard un centre de données. Il peut envoyer la demande à n'importe quel serveur Citrix Virtual Apps and Desktops de n'importe quel centre de données, quelle que soit la proximité du client qui effectue la demande.

L'adresse IP du client est examinée lorsqu'une requête HTTP arrive à l'appliance Citrix Gateway. L'adresse IP réelle du client est utilisée pour créer la liste des préférences du centre de données qui est transférée à StoreFront. Si l'appliance Citrix ADC est configurée pour insérer l'en-tête de préférence de zone, StoreFront 3.5 ou version ultérieure peut utiliser les informations fournies par l'appliance pour réorganiser la liste des contrôleurs de remise et se connecter à un Controller de remise optimal dans la même zone que le client. StoreFront sélectionne le serveur virtuel VPN de passerelle optimal pour la zone de centre de données sélectionnée, ajoute ces informations au fichier ICA avec les adresses IP appropriées et les envoie au client. StoreFront tente ensuite de lancer des applications hébergées sur les Delivery Controller du centre de données préféré avant d'essayer de contacter des contrôleurs équivalents dans d'autres centres de données.

Pour plus d'informations sur la configuration de cette solution, cliquez ici.

Pour obtenir une vue d'ensemble vidéo sur la solution de préférence de zone alimentée par GSLB, cliquez surhttps://www.youtube.com/watch?v=Y8DELum0Xp0.

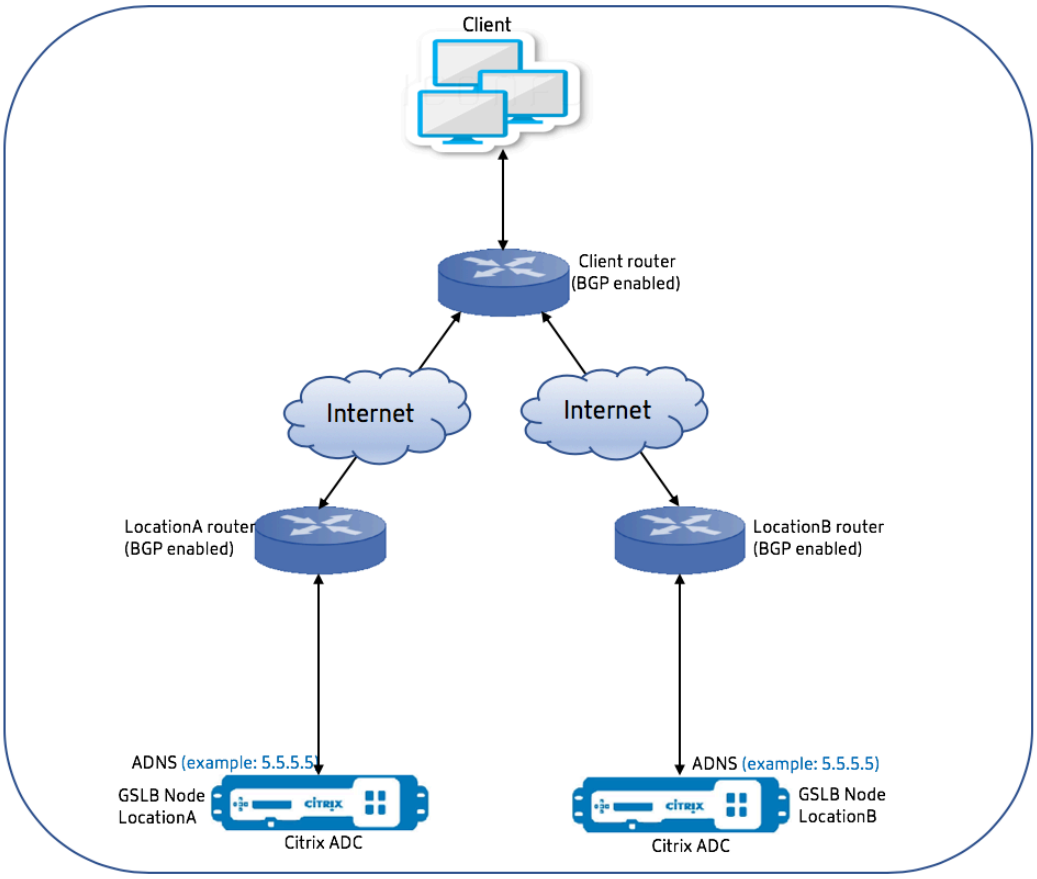
Prise en charge Anycast dans Citrix ADC

January 21, 2021

Anycast est un type de réseau dans lequel un ensemble de serveurs partage une adresse IP. La demande du client est dirigée vers le serveur topographiquement le plus proche en fonction de leurs tables de routage. Ce routage réduit les problèmes de latence, garantit une haute disponibilité et minimise les temps d'arrêt.

Citrix ADC prend en charge le réseau anycast avec Global Server Load Balancing (GSLB) et les fonctionnalités DNS.

Le diagramme suivant illustre un diagramme topologique d'Anycast dans Citrix ADC.



GSLB Anycast

La fonction Citrix ADC GSLB assure l'équilibrage de la charge entre les sites distribués à l'échelle mondiale ainsi que la reprise après sinistre et assure une disponibilité continue des applications.

Lors d'une panne, GSLB assure une reprise après sinistre immédiate en acheminant le trafic vers le centre de données le plus proche ou le plus performant. Toutefois, GSLB ne peut pas contrôler les éléments suivants :

- Comment le trafic DNS est routé vers les nœuds GSLB dans différents emplacements géographiques.
- Combien de latence est ajoutée pendant que les requêtes DNS sont routées vers les nœuds GSLB.

Dans une configuration GSLB typique, chaque centre de données dispose d'un nœud GSLB configuré avec le serveur ADNS (Autoritative Domain Name Server) spécifique au site pour recevoir des requêtes DNS. L'ADNS de chaque site est configuré comme serveur de noms dans le résolveur DNS. À mesure que le nombre de nœuds GSLB augmente, le nombre d'enregistrements de serveur de noms augmente également. Dans de tels cas, en cas de défaillance d'un centre de données, LDNS doit réessayer la résolution avec un serveur de noms différent. Cette nouvelle tentative ajoute à la latence dans la résolution DNS.
En outre, chaque fois qu'un nœud GSLB est ajouté, les enregistrements du serveur de noms doivent être mis à jour.

Pour surmonter ces inconvénients, vous pouvez utiliser Anycast ADNS. Dans Anycast ADN, une seule adresse IP ADNS est utilisée pour tous les nœuds GSLB et le trafic DNS est routé vers les nœuds GSLB à l'aide d'un routage dynamique.

Par exemple, si un site GSLB est DOWN, la table de routage est mise à jour et l'itinéraire vers ce site est supprimé. Par conséquent, Les requêtes DNS ne sont pas envoyées aux sites qui sont en panne. En conséquence, il n'y a pas de nouvelles tentatives.

Si un nouveau nœud GSLB est ajouté, le nouveau nœud reçoit la même adresse IP ADNS. Le routage dynamique met automatiquement à jour les tables de routage avec des itinéraires vers de nouveaux sites en fonction des algorithmes de routage. Par conséquent, vous n'avez pas à mettre à jour les enregistrements du serveur de noms DNS. Le déploiement de nouveaux sites GSLB est simplifié et plus rapide avec Anycast.

Comment configurer une adresse IP ADNS en mode anycast

Activez le routage de l'hôte sur l'adresse IP ADNS dans une appliance Citrix ADC et définissez le niveau RHI (Route Health Injection) approprié. La plupart du temps, il n'y aurait pas de serveurs virtuels sur l'IP de l'ADNS et par conséquent, le niveau RHI doit être sélectionné comme NONE. L'activation de la route de l'hôte sur l'adresse IP de l'ADNS en fait une route du noyau. Vous pouvez ensuite activer le

routage dynamique de votre choix et configurer le protocole de routage pour redistribuer les routes du noyau.

Configuration IP de l'ADNS — Exemple

À l'invite de commandes, tapez ;

```
add service adns_public 5.5.5.5 ADNS 53

set ip 5.5.5.5 -hostRoute ENABLED -vserverRHILevel ALL_VSERVERS
<!--NeedCopy-->
```

Configuration BGP dans le site GSLB — Exemple

```
Site1#sh run
!
hostname Site1
!
log syslog
log record-priority
!
ns route-install bgp
!
interface lo0
 ip address 127.0.0.1/8
 ipv6 address fe80::1/64
 ipv6 address ::1/128
!
interface vlan0
 ip address 10.102.148.94/25
 ipv6 address fe80::e84c:f4ff:fe74:4588/64
!
interface vlan2
 ip address 172.18.30.15/24
!
router bgp 5
 redistribute kernel -----> redistributing the kernel routes
 neighbor 172.18.30.30 remote-as 4
 neighbor 172.18.30.30 advertisement-interval 1
 neighbor 172.18.30.30 timers 4 16
!
End

```



```
30 Site1#
31 <!--NeedCopy-->
```

Table de routage de site GSLB - Exemple

```
1  Site1#sh ip route
2  Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
3         O - OSPF, IA - OSPF inter area
4         N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
5         E1 - OSPF external type 1, E2 - OSPF external type 2
6         i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
7         ia - IS-IS inter area, I - Intranet
8         * - candidate default
9
10 K       5.5.5.5/32 via 0.0.0.0 ------------------------------------->
       Kernel Route for ADNS
11 C       10.102.148.0/25 is directly connected, vlan0
12 C       127.0.0.0/8 is directly connected, lo0
13 B       172.18.10.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
14 B       172.18.20.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
15 C       172.18.30.0/24 is directly connected, vlan2
16 B       192.168.3.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
17 B       192.168.5.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
18 B       192.168.10.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
19
20 Gateway of last resort is not set
21 Site1#
22 <!--NeedCopy-->
```

DNS Anycast

Vous pouvez utiliser Anycast DNS pour les serveurs virtuels proxy DNS sur Citrix ADC. Lorsqu'il y a plusieurs serveurs de noms DNS configurés, le résolveur DNS répond selon la méthode round robin. Par exemple, si le résolveur ne reçoit aucune réponse du premier serveur, il bascule vers le second serveur après l'expiration de la valeur de délai configurée. Le passage du premier serveur au second serveur ajoute à la latence dans la résolution DNS. Si les résolveurs DNS sont configurés avec Anycast, cette latence peut être éliminée.

Configuration DNS — Exemple

À l'invite de commandes, tapez ;


```
add lb vserver dns DNS 5.5.5.50 53

set ip 5.5.5.50 -hostRoute ENABLED -vserverRHILevel ALL_VSERVERS
<!--NeedCopy-->
```

Déploiement d'une plateforme de publicité numérique sur AWS avec Citrix ADC

August 20, 2021

Avec la nature évolutive des plateformes numériques, un large éventail d'applications publicitaires sont disponibles. Par exemple, les médias sociaux, le publipostage, les vidéos, les bannières, les pops, les interstitiels, les médias riches et ainsi de suite. Les annonceurs adoptent les réseaux de publicité vidéo à un rythme rapide, constituant près de 40 % du trafic publicitaire. Mais avec plus d'utilisation des mobiles par les utilisateurs modernes, l'exécution de publicités vidéo sur la plate-forme mobile a vu une augmentation considérable.

Les plateformes publicitaires numériques sont confrontées à plusieurs défis. Voici quelques-uns des défis suivants :

- Menaces de sécurité
- Coûts opérationnels élevés
- Une large gamme d'appareils sont disponibles pour envoyer du trafic sur Internet. Les différents protocoles de communication en temps réel posent les défis suivants :
  - WebRTC
  - Diffusion adaptative
  - UDP pour la vidéo, où WebRTC utilise UDP sur HTTP

Pour faire face au comportement complexe des plates-formes publicitaires, la solution Citrix ADC, avec sa suite complète de fonctionnalités et de fonctionnalités bien intégrées à AWS, offre un accès instantané, sécurisé et fiable à l'inventaire des publicités numériques, partout et à tout moment. Citrix ADC joue un rôle essentiel dans la fourniture des applications SaaS et Web pour les plates-formes numériques.

Intégration d'une plateforme publicitaire numérique avec Citrix ADC

Présentation de la plateforme de publicité numérique

La plateforme de publicité numérique se compose des éléments clés suivants :

- Échange d'annonces

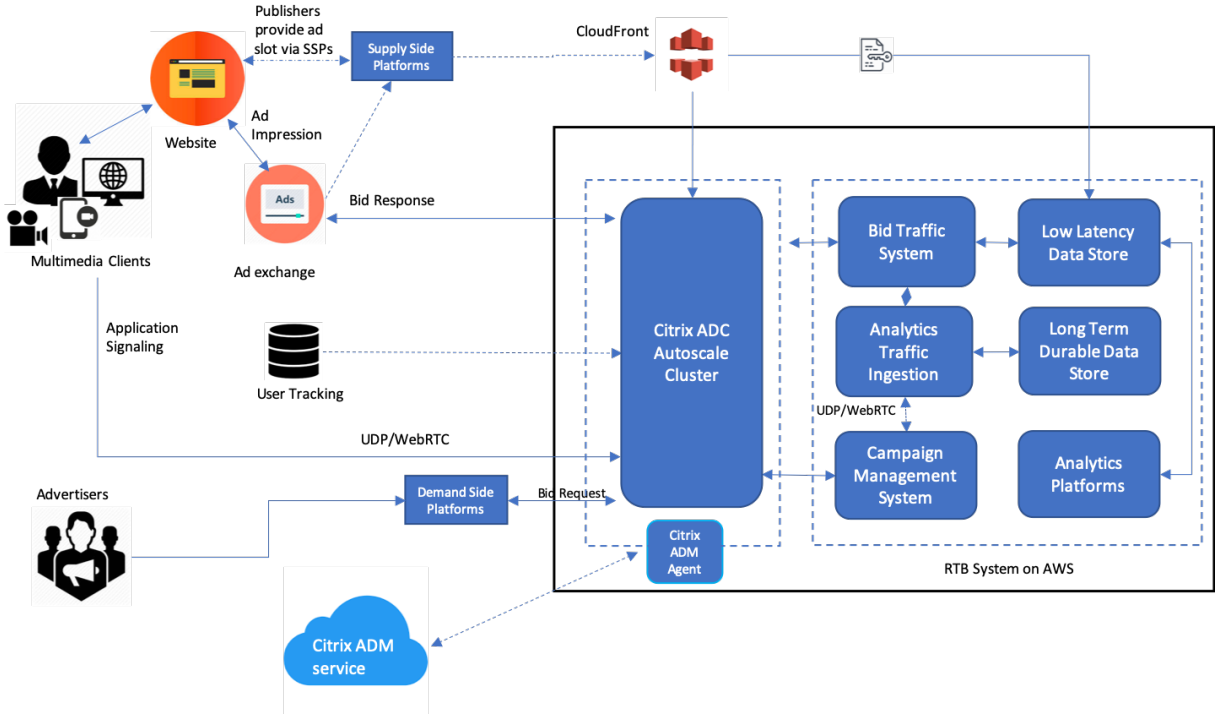
- Réseau publicitaire
- Plateforme côté demande (DSP)
- Plateforme côté approvisionnement (SSP)
- Systèmes d'enchères en temps réel (RTB)

Voici un aperçu du processus suivi dans un système publicitaire.

- La première transaction se produit lorsque l'utilisateur visite le site Web.
- Cela déclenche une demande d'enchère/de publicité (y compris les informations démographiques de l'utilisateur) qui est envoyée au serveur publicitaire ou à l'éditeur en contactant un échange d'annonces.
- Les éditeurs d'annonces envoient la demande de publicité à un échange publicitaire par l'intermédiaire de SSP.
- L'échange publicitaire soumet cette demande et les données qui l'accompagnent à DSP indiquant qu'une demande d'impression ou de publicité est disponible. Par conséquent, plusieurs annonceurs peuvent automatiquement soumettre des enchères en temps réel pour placer leurs publicités.
- Pendant ce temps, les annonceurs doivent configurer leurs campagnes dans DSP. Utilisez les informations sur l'utilisateur de Data Management Platform (DMP) pour évaluer le montant qu'il est prêt à payer pour la diffusion d'une publicité à l'utilisateur.
- Les DSP soumettent ces soumissions en temps réel sur chaque impression de publicité parce qu'elles sont servies à l'échange de publicité.
- Quel que soit le soumissionnaire qui soumet le plus d'offres dans un délai fixé par l'échange publicitaire ou les FSSP, obtient un créneau publicitaire par les éditeurs pour diffuser leurs publicités. Sinon, ils perdent l'occasion d'obtenir la bonne publicité pour leur population clé.

Comment la plateforme de publicité numérique est intégrée à Citrix ADC

Le diagramme suivant illustre la manière dont les différents composants de la plate-forme publicitaire communiquent avec Citrix ADC et Citrix Application Delivery Management (ADM) pour diffuser des publicités en ligne.



Comment Citrix ADC contribue

Dans le processus de publication d'annonces, la solution Citrix ADC aide à gérer et traiter l'afflux incohérent du trafic d'enchères. Il sert de point d'entrée pour tout le trafic afin d'assurer l'évolutivité et la disponibilité dans toutes les zones de disponibilité. Pour répondre à la nature élastique du trafic publicitaire, il est déployé dans un groupe de mise à l'échelle automatique devant les applications Web et les serveurs de base de données.

La plate-forme publicitaire sur AWS avec la solution Citrix ADC vous permet d'obtenir des performances en temps réel, une grande évolutivité et une haute disponibilité dans le monde entier. Vous pouvez acheter et vendre des publicités multimédia riches, vidéo, mobiles et natives en temps réel. Il réduit le coût opérationnel global et la latence associés à l'exécution d'une plateforme publicitaire. Il s'agit du proxy le plus performant avec les nombreuses fonctionnalités de suppression gracieuse des serveurs back-end lors de la mise à l'échelle automatique, du multiplexage des connexions et de s'assurer que le trafic de l'utilisateur final n'est jamais affecté. Citrix ADC prend en charge l'équilibrage de charge des protocoles HTTP, UDP, WebRTC et RTSP utilisés dans les plates-formes publicitaires.

Citrix ADC s'intègre de manière cohérente à l'environnement AWS avec les attributs clés suivants :

- Changement de contenu : passez à la bonne plate-forme en fonction du nom d'hôte.
- Protection de la sécurité : utilisez la fonctionnalité de pare-feu d'applications Web (WAF), la limitation de débit (via l'IP du client) et la protection contre les attaques DDoS.
- Mise à l'échelle automatique du trafic frontal et back-end.
- Visibilité de bout en bout et détection des anomalies sur les appliances ADC à l'aide d'ADM.

- Faible latence.

Comment Citrix ADM contribue

Citrix ADC utilise Citrix ADM pour surmonter les défis suivants auxquels sont confrontées les plateformes publicitaires numériques :

- Identifier les écarts de tendance par rapport aux performances attendues
- Analyse des performances des applications en temps réel
- Surveillance des capacités

Avantages de l'intégration de plateformes publicitaires avec Citrix ADC et ADM

La solution Citrix ADC offre les fonctionnalités et avantages suivants à un fournisseur de plateformes publicitaires numériques.

Faible coût

- Intégré au service AWS Autoscaling, l'instance Citrix ADC VPX peut augmenter ou réduire automatiquement vos ressources front-end et back-end. Cela fournit une configuration zéro touche répondant à l'élasticité des plateformes publicitaires.
- Consolidation de la fourniture de tous les types de trafic à partir d'un seul point.

Pour plus d'informations sur AWS Autoscaling, voir Ajouter un service AWS Autoscaling principal.

Haute disponibilité

- Si une zone de disponibilité devient indisponible, Citrix ADC applique sa capacité de tolérance aux pannes pour détecter automatiquement les serveurs dans une autre zone de disponibilité, sans interruption de trafic.
- En outre, Il met fin gracieusement aux serveurs en évitant la perte de connexions client.

Pour plus d'informations, voir Comment fonctionne la haute disponibilité sur AWS.

Analyse des performances des applications

L'analyse intelligente et l'analyse des performances des applications Citrix ADM garantissent :

- Bénéficiez d'une visibilité sur les problèmes (anomalies de réponse du serveur, erreurs 5XX, etc.) qui affectent l'expérience de l'utilisateur final.
- Avertissez l'administrateur de prendre immédiatement des mesures correctives.

Pour plus d'informations, voir Indicateurs de performance pour l'analyse des applications.

Sécurité par pare-feu riche

Les vulnérabilités de sécurité les plus courantes se produisent dans les applications Web plutôt que dans les réseaux. Il est essentiel de protéger vos applications Web contre les accès non autorisés tels que les robots, les vols de données et les attaques de couches d'applications.

Citrix ADC offre une sécurité complète et intégrée de couche 4 à 7 qui comprend :

- Web App Firewall (WAF) pour protéger vos applications Web, identifier et atténuer les robots malveillants grâce à des signatures de robots régulièrement mises à jour et à une détection basée sur le comportement.
- Limitation des tarifs pour empêcher une plate-forme publicitaire d'être débordée.

Pour plus d'informations, consultez Citrix Web App Firewall.

Sélectionnez le type d'instance AWS approprié pour la plate-forme publicitaire

Choisissez le type d'instance AWS approprié pour ADC en fonction des deux facteurs suivants :

- Nombre d'utilisateurs accédant simultanément à la plateforme publicitaire.
- Nombre moyen d'utilisateurs sur la plateforme.

Citrix ADC peut être déployé dans diverses instances EC2, dont c5, c5n, m5, etc. Pour les plates-formes publicitaires, utilisez les types d'instance AWS suivants :

- c5 ou c5n est approprié pour gérer le trafic lourd SSL.
- c5.large peut gérer jusqu'à 1000 TPS SSL.

Pour plus d'informations, consultez la matrice de support VPX-AWS.

Amélioration de l'analyse du flux de clics dans AWS à l'aide de Citrix ADC

October 5, 2021

Les clients accèdent de plus en plus aux produits de l'entreprise via diverses applications telles que les applications mobiles, les applications SaaS, etc. Par conséquent, les applications peuvent devenir une mine de données sur l'expérience client. Pour suivre le comportement des clients en ligne, les entreprises centrées sur le client forment des profils basés sur les données pour chacun de leurs clients à l'aide de ces données de comportement client.

Un flux de clics est une séquence ou un flux d'événements qui représentent les actions des utilisateurs (clics) sur un site Web ou une application mobile. Toutefois, la portée du parcours de clics s'étend au-delà des clics. Il comprend les recherches de produits, les impressions, les achats et tout événement de ce type pouvant être pertinent pour l'entreprise. La simple collecte et le stockage des données de

l'expérience client n'ont pas beaucoup de valeur. Il est nécessaire de distribuer les données très complexes de manière transparente aux bons fournisseurs au bon moment. Les entreprises peuvent tirer profit des données et prendre rapidement des décisions conscientes pour améliorer leurs stratégies. Par conséquent, les entreprises utilisent de plus en plus l'analyse des flux de clics pour obtenir des informations sur le parcours de l'expérience client des applications.

Ce document vous permet de bien comprendre pourquoi les données Clickstream sont de la plus haute importance, comment elles sont collectées, stockées, distribuées et transformées en analyses significatives et exploitables.

Citrix ADC s'intègre à Citrix ADM et ajoute de la valeur aux services AWS tels qu'Amazon Kinesis Data Firehose pour doter les entreprises de la meilleure solution d'analyse qui tourne autour des flux de clics des utilisateurs.

Cette solution Citrix ADC vous aide à résoudre des problèmes commerciaux complexes de manière efficace et en toute simplicité. Citrix ADC et AWS Kinesis permettent de capturer les problèmes liés au flux de travail mal conçu. Citrix ADM permet de capturer les problèmes liés aux performances des applications Web et du réseau en appliquant des filtres pertinents. La conjonction de Citrix ADC avec Citrix ADM et AWS Kinesis vous aide à gérer et à analyser l'afflux massif de données de flux de clics à chaque phase. Cette solution est hautement disponible, évolutive, robuste et garantit que la livraison est continue et sécurisée. Ainsi, vous pouvez obtenir des informations exploitables.

Pourquoi les entreprises optent pour Clickstream Analytics ?

Les entreprises optent pour le flux de clics principalement pour comprendre comment les utilisateurs interagissent avec l'application et pour obtenir des informations sur l'amélioration des objectifs de l'application. Clickstream Analytics est un cas d'utilisation de récupération d'informations qui suit le comportement de votre utilisateur, ses habitudes de navigation, etc. Clickstream Analytics vous donne des informations sur :

- Quel lien vos clients cliquent le plus souvent et à quel moment ?
- Où se trouvait le visiteur avant d'accéder à mon site Web ?
- Combien de temps le visiteur a-t-il passé sur chaque page ?
- Quand et où le visiteur a-t-il cliqué sur le bouton « retour » du navigateur Web ?
- Quels articles le visiteur a-t-il ajoutés (ou supprimés de) son panier d'achat ?
- À partir de quelle page le visiteur a-t-il quitté mon site Web ?

Service d'analyse pour gérer les données Clickstream à l'aide d'Amazon Kinesis

Vous pouvez utiliser Amazon Kinesis pour effectuer des analyses de flux de clics. Amazon kinesis permet l'analyse des flux de clics avec les services suivants :

- Amazon Kinesis Data Firehose

- Analyses de données Amazon Kinesis
- Amazon Kinesis Data Streams

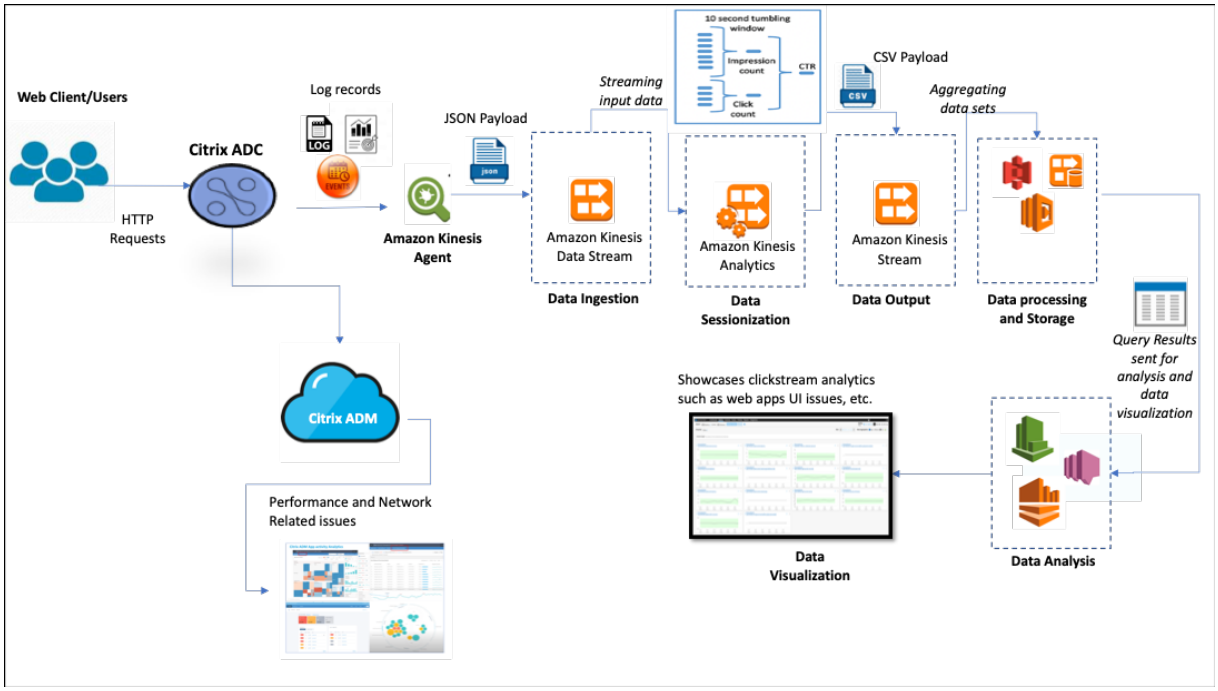
Avec Amazon Kinesis, vous pouvez collecter et analyser vos énormes ensembles de données à n'importe quelle échelle. AWS Kinesis peut gérer des données provenant de différentes sources, telles que :

- Applications mobiles et Web (par exemple, jeux, commerce électronique)
- Appareils IoT
- Applications de réseaux sociaux
- Services de trading financier
- Services géospatiaux

Comment Citrix ADC permet l'analyse du flux de clics

La solution Citrix ADC rassemble et fournit des informations en toute sécurité sur les activités des utilisateurs, telles que les sites Web visités, la bande passante dépensée, le flux de navigation. Les entreprises analysent ce débit élevé et ces données de flux de clics continus pour corroborer l'efficacité des éléments suivants :

- Présentation du site
- Campagnes marketing
- Nouvelles fonctionnalités de l'application



Grâce à la capacité de Citrix ADC à fournir une protection réseau résiliente pour les environnements d'entreprise, le coût du serveur est réduit en déchargeant les tâches gourmandes en calcul et en exé-

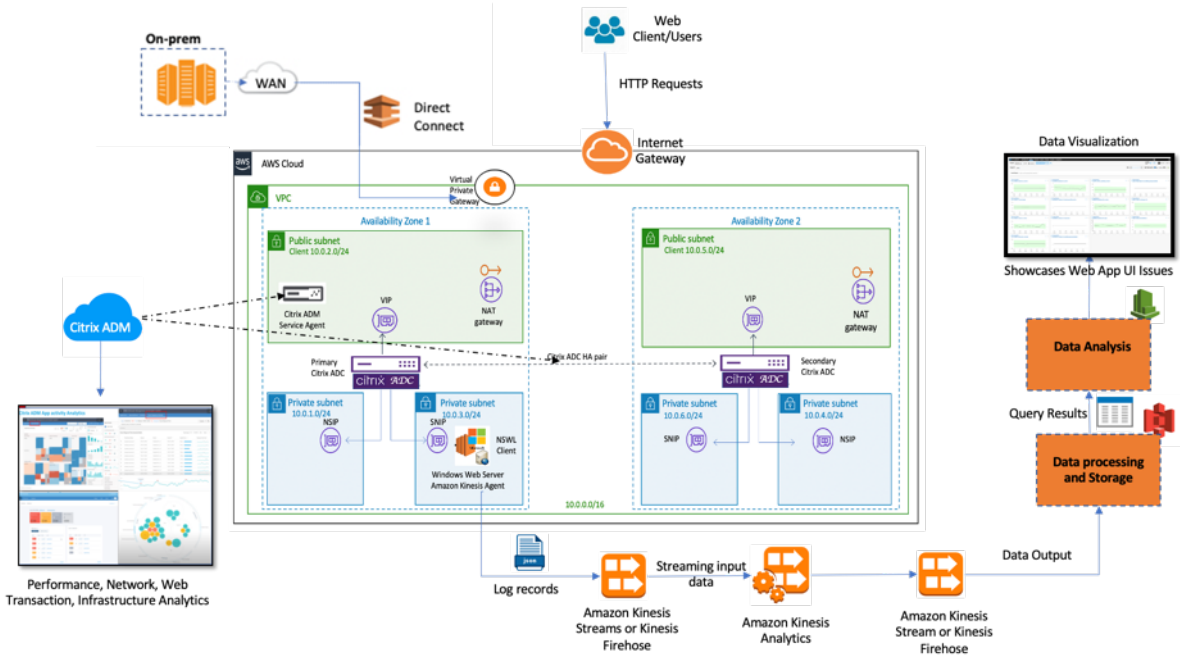
cutant des sessions sur ces données. Cela aide les entreprises à identifier les événements en temps réel avec une haute disponibilité, une sécurité et une faible latence toujours.

Pour plus d'informations sur la configuration, voir Configurer la solution Citrix ADC pour l'analyse des flux de clics.

Comment Citrix ADC et Citrix ADM complètent l'environnement AWS

Le diagramme suivant illustre le flux de travail des utilisateurs de bout en bout pour effectuer des analyses de flux de clics dans l'infrastructure AWS. Ce diagramme vous aide à comprendre les processus suivants :

- Interaction de l'utilisateur avec Citrix ADC
- Comment Citrix ADC capture les actions des utilisateurs et génère des données de parcours de navigation
- Comment les données de parcours de clics sont transmises aux services AWS (Amazon Kinesis)
- Comment Amazon Kinesis traite les journaux de données et les stocke pour produire des analyses de flux de clics significatives



Citrix ADC s'intègre parfaitement à l'environnement AWS et à Citrix ADM, ce qui aide les entreprises à être compatibles avec les volumes variables et la diversité des données de parcours de navigation. Il fournit des services permettant de charger et d'analyser les connaissances en streaming en toute simplicité. Vous pouvez également créer des applications de connaissances en streaming personnalisées pour des besoins spécifiques.

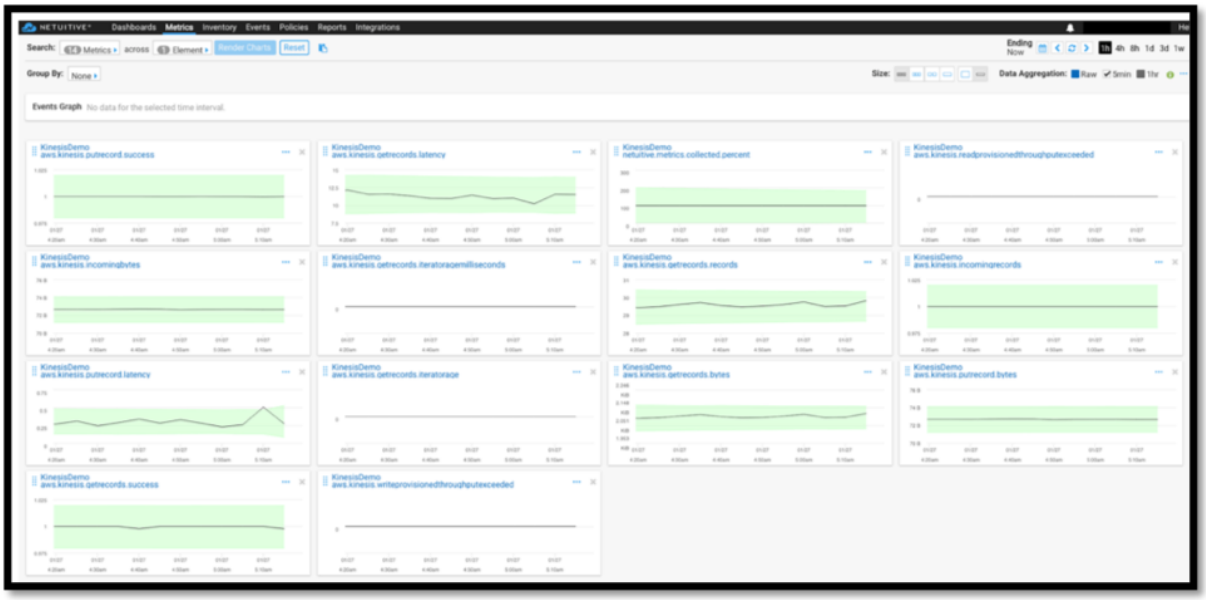
Amazon Kinesis

L'environnement AWS dispose de différents services qui effectuent des analyses sur les événements utilisateur, les journaux et les métriques capturés par Citrix ADC. Les données peuvent être des flux de clics sur le site Web, des transactions financières, des flux de médias sociaux, des journaux informatiques et des événements de localisation.

- Amazon Kinesis Data Streams effectue des analyses dans des scénarios impliquant un flux de données en temps réel évolutif et durable qui peut capturer en continu des Go de données par seconde à partir de plusieurs sources.
- Amazon Kinesis Data Analytics peut être utilisé pour les scénarios avec une latence plus faible entre la génération de session, car l'agrégation des différents ensembles de données prend moins de temps.
- Amazon Kinesis Agent for Microsoft Windows collecte, analyse, filtre et diffuse les données d'entrée vers les flux de données Kinesis.
- Une fois les données stockées dans le cloud, vous pouvez implémenter le pipeline de données exact pour obtenir les résultats souhaités. Par exemple, vous pouvez utiliser ces informations dans Amazon Quick Sight, qui est un outil de visualisation utilisé pour créer des tableaux de bord.

Le tableau de bord AWS Kinesis propose les offres suivantes :

- Présentation des problèmes d'interface utilisateur des applications Web
- Visualisations en temps quasi réel des mesures d'utilisation du Web telles que les événements par heure, le nombre de visiteurs et les référents.
- Analyse par session



Analyse Citrix ADM

En utilisant Citrix ADM avec Citrix ADC, vous bénéficiez d'une vue unique sur tous les environnements professionnels. Les journaux capturés Citrix ADC sont introduits dans Citrix ADM, qui traite vos applications individuelles comme une entité unique. Vous pouvez obtenir des informations précieuses et résoudre efficacement les problèmes grâce aux fonctionnalités ADM suivantes :

- Analyses intelligentes
- Analyse des transactions Web
- Détection des anomalies
- Problèmes liés aux performances et au réseau

Le tableau de bord des services ADM suivant vous permet d'obtenir des informations précieuses pour résoudre efficacement les problèmes.

Comment Citrix ADM est en corrélation avec l'analyse Clickstream

Les données d'analyse des flux de clics peuvent être corrélées avec les analyses ADM pour décrire, prédire et améliorer les performances de l'application.

Pour plus d'informations sur Citrix ADM, consultez Citrix ADM

Par exemple, une organisation lors de l'analyse de ses journaux constate que la plupart des utilisa-

teurs abandonnent leurs sites. Mais pour trouver la cause profonde de ce comportement utilisateur, ils doivent savoir quelle partie de leur application fonctionne mal. Avec les données d'analyse du parcours de navigation et les analyses ADM, vous pouvez obtenir les informations suivantes pour analyser la raison de l'abandon d'un site par les utilisateurs :

- L'utilisateur abandonne-t-il en raison d'erreurs de latence, 5xx ?
- Y a-t-il des erreurs SSL Handshake ?
- Y a-t-il une partie de l'application qui présente des problèmes de performances ou de réseau ?
- Y a-t-il une erreur 404 ou le temps de chargement de la page prend une éternité pour répondre, etc.
- Les clients sont-ils confrontés à des anomalies de réponse du serveur ?

Le service Citrix ADM fournit des informations Web qui permettent aux administrateurs informatiques d'accélérer la résolution des problèmes grâce aux fonctionnalités suivantes :

- Assure une surveillance intégrée et en temps réel de toutes les applications Web desservies par Citrix ADC.
- Obtenez une vue globale des performances de l'application en termes de temps, de latence et de comportement habituel de l'utilisateur grâce à des outils d'observabilité (tels que le graphique de service global).
- Effectuez des analyses intelligentes pour comprendre les anomalies de réponse du serveur.
- Les informations SSL contribuent à la résolution des erreurs 5xx et 4xx.
- Pour conserver les enregistrements de toutes les sessions Web qui incluent :
  - Journaux détaillés de chaque transaction Web
  - Fonction de recherche pour trouver les journaux pertinents
  - Possibilité d'isoler un utilisateur ADC-to-end par rapport à Problème ADC-to-Server

Types de données exportées par ADC pour Clickstream Analytics

Citrix ADC capture les différentes sources qui génèrent différentes formes de données, qui sont les suivantes :

- Journaux du serveur Web

  La fonctionnalité de journalisation du serveur Web envoie les journaux des requêtes HTTP et HTTPS à un système client à des fins de stockage et de récupération. Ces journaux contiennent une énorme quantité de données, ce qui est difficile à comprendre et à comprendre. Les outils analytiques aident à la comprendre et à en apporter de la valeur. Pour plus d'informations sur la configuration, consultez la **section Configuration de la journalisation Web** de ce document.

- Syslogs

  Les Syslogs sont principalement utilisés pour la gestion des systèmes. La surveillance proactive du Syslog est rentable car elle réduit considérablement les temps d'arrêt des serveurs et

autres périphériques de votre infrastructure. Syslog identifie les problèmes réseau critiques et les signale de manière proactive.

- Journaux d'accès

  Les journaux d'accès stockent des informations sur les événements survenus sur votre serveur Web. Par exemple, lorsqu'une personne visite votre site Web, un journal est enregistré et stocké pour fournir à l'administrateur du serveur Web des informations telles que l'adresse IP du visiteur, les pages qu'il consultait, les codes d'état, le navigateur utilisé. L'accès aux journaux peut être accablant, s'il y a un manque de connaissances appropriées pour les comprendre.
  Vous pouvez programmer l'intégration de votre système avec :

  - Citrix ADC pour une livraison transparente
  - Kinesis pour obtenir des informations exploitables utiles aux entreprises

- Journaux d'audit

  La fonctionnalité Audit Logging vous permet de consigner les états Citrix ADC et les informations d'état collectées par divers modules dans le noyau et dans les démons de niveau utilisateur.

- Journaux d'erreurs

  Le fichier journal des erreurs permet aux administrateurs de fournir plus d'informations concernant une erreur spécifique survenue sur le serveur Web.

Configurez la solution Citrix ADC pour l'analyse des flux de clics

La fonctionnalité de journalisation du serveur Web vous permet d'envoyer des journaux de requêtes HTTP et HTTPS à un système client à des fins de stockage et de récupération.

Pour configurer Citrix ADC pour la journalisation du serveur Web, vous devez :

- Activer la fonctionnalité de journalisation Web
- Configurez la taille de la mémoire tampon pour stocker temporairement les entrées de journal car le serveur de journaux Web s'exécute sur Citrix ADC.

Pour configurer la journalisation du serveur Web à l'aide de l'interface de ligne de commande :

1. Activez la fonctionnalité de journalisation du serveur Web.

```
enable ns feature WL
<!--NeedCopy-->
```

2. [Facultatif] Modifier/Configurer la taille du tampon pour stocker les informations enregistrées.

```
set ns weblogparam -bufferSizeMB 60
<!--NeedCopy-->
```


3. Installez le client de journalisation Web Citrix ADC (NSWL). Pour plus d'informations, reportez-vous à la section Installation du client Citrix ADC Web Logging (NSWL).
4. Installez le client NSWL sous Windows en effectuant les opérations suivantes sur le système sur lequel vous avez téléchargé le package.
   a) Extrayez et copiez< release number >< build number > le fichier nswl_win–.zip du package sur un système Windows sur lequel vous souhaitez installer le client NSWL.
   b) Sur le système Windows, décompressez le fichier dans un répertoire (appelé < NSWL-HOME>). Les répertoires bin, samples et autres sont extraits.
   c) À l'invite de commandes, exécutez la commande suivante à partir du < NSWL-HOME > répertoire \ bin :

```
nswl -install -f < path of the log.conf file >\log.conf
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour désinstaller le client NSWL, à l'invite de commandes, exécutez la commande suivante à partir du < NSWL-HOME > répertoire \ bin :

```
nswl -remove
<!--NeedCopy-->
```

5. Après avoir installé le client NSWL, configurez le client NSWL à l'aide de l'exécutable NSWL. Ces configurations sont stockées dans le fichier de configuration du client NSWL (log.conf).

   Exécutez les commandes suivantes à partir du répertoire dans lequel se trouve l'exécutable NSWL :

```
\ns\bin
<!--NeedCopy-->
```

6. Dans le fichier de configuration du client NSWL (log.conf), ajoutez l'adresse IP Citrix ADC (NSIP) à partir de laquelle le client NSWL collecte les journaux en exécutant ce qui suit dans l'invite de commande du système client :

```
nswl -addns -f < Path to the configuration(log.conf) file >\log.
    conf
<!--NeedCopy-->
```

7. Entrez le NSIP (adresse IP) de l'appliance Citrix ADC, le nom d'utilisateur `nsroot` et le mot de passe en tant que « ID d'instance/mot de passe défini » de manière à ce que :

- Le client NSWL se connecte à l'ADC après avoir ajouté l'adresse IP NetScaler (NSIP) au fichier de configuration NSWL
- ADC met en mémoire tampon les entrées du journal des demandes HTTP et HTTPS avant de les envoyer au client.
- Le client peut filtrer les entrées (en modifiant le fichier log.conf) avant de les stocker.

> Remarque
>
> Modifiez le mot de passe par défaut de Citrix ADC, puis procédez à la configuration. Tapez la commande suivante pour modifier le mot de passe :

```
set system user nsroot -password <your password>
<!--NeedCopy-->
```

Configuration de l'agent Amazon Kinesis

Effectuez les étapes suivantes dans la console Web AWS pour configurer l'agent Amazon Kinesis :

1. Créez un fichier de configuration (appsettings.json) et déployez-le. Les fichiers de configuration définissent des ensembles de sources, de cuvettes et de tuyaux qui connectent les sources aux cuvettes, ainsi que des transformations facultatives.

   L'exemple suivant est un fichier de `appsettings.json` configuration complet qui configure Kinesis Agent pour diffuser les événements du journal des applications Windows vers Kinesis Data Firehose.

```
{

"Sources": [
    {

        "Id": "NSWLog",
        "SourceType": "DirectorySource",
        "Directory": "C:\Users\Administrator\Downloads\nswl_win
           -13.0-52.24\bin",
        "FileNameFilter": "*.log"
        "RecordParser": "TimeStamp",
        "TimestampFormat": "yyyy-MM-dddd HH:mm:ss.ffff", //
           Optional parameter required only by the timestamp
           record parser
        "TimeZoneKind": "UTC", //Local or UTC
        "SkipLines": 0 //Skip a number of lines at the beginning
           of each file
     }

```



```
16      ],
17  "Sinks": [
18      {
19
20          "Id": "ApplicationLogKinesisFirehoseSink",
21          "SinkType": "KinesisFirehose",
22          "StreamName": "Delivery-ik-logs",
23          "AccessKey": "Your Access Key",
24          "SecretKey": "YourSecretKey",
25          "Region": "ap-south-1"
26       }
27
28      ],
29  "Pipes": [
30      {
31
32      "Id": "ApplicationLogSourceToApplicationLogKinesisFirehoseSink
            ",
33      "SourceRef": "ApplicationLogSource",
34      "SinkRef": "ApplicationLogKinesisFirehoseSink"
35       }
36
37      ],
38  "Telemetrics":
39      {
40
41      "off": "true"
42       }
43
44   }
45
46  <!--NeedCopy-->
```

2. Configurez un agent Kinesis sur les sources de données pour collecter des données et les envoyer en continu à Amazon Kinesis Firehose/Kinesis Data Analytics. Pour plus d'informations, consultez Démarrage avec Amazon Kinesis Agent for Microsoft Windows.
3. Créez un flux de diffusion de données de bout en bout à l'aide d' Amazon Kinesis Firehose. Le flux de livraison transmet vos données de l'agent à la destination. La destination inclut Amazon Kinesis Analytics, Amazon Redshift, Amazon Elasticsearch service et Amazon S3. Pour la source, choisissez **Direct PUT ou d'autres sources** pour créer un flux de diffusion Kinesis Data Firehose.
4. Traitez les données de journal entrantes à l'aide de requêtes SQL dans Amazon Kinesis Analytics.
5. Chargez les données traitées depuis Kinesis Analytics vers Amazon Elasticsearch Service pour

indexer les données.

6. Analysez et visualisez les données traitées à l'aide d'outils de visualisation, tels que Kibana et AWS QuickInsight Services.

Références

- Afficher et exporter les messages syslog
- Citrix Networking pour Hybrid Multi Cloud
- Écriture dans AWK Kinesis Data Streams à l'aide de Kinesis Agent

Citrix ADC dans un cloud privé géré par Microsoft Windows Azure Pack et Cisco ACI

August 20, 2021

Vous pouvez utiliser une appliance Citrix ADC pour l'équilibrage de charge dans un cloud privé géré via Microsoft Windows Azure Pack. Le réseau pour le cloud privé est automatisé à l'aide de Cisco ACI et Citrix ADC.

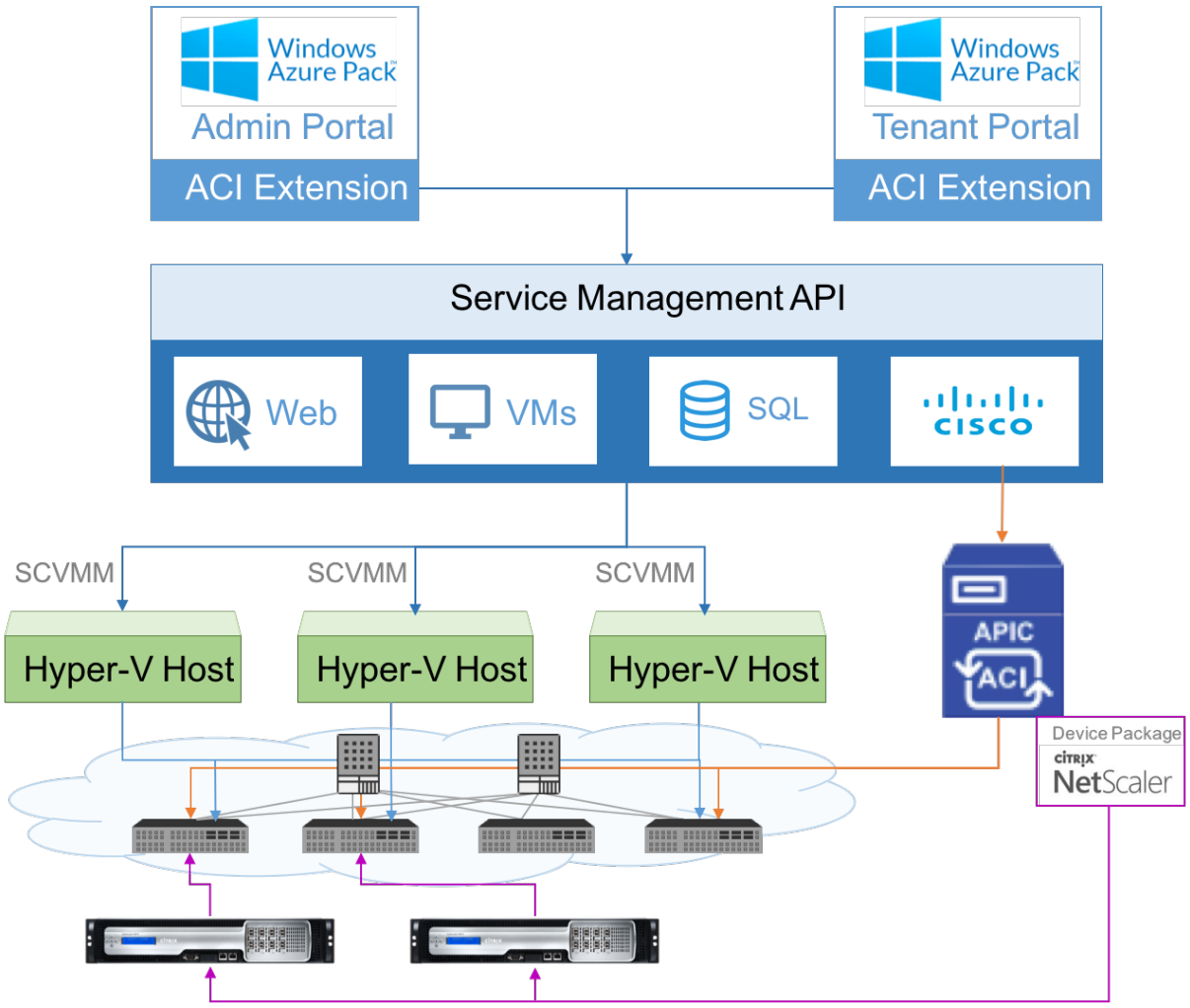
Cette solution implique de nombreux points d'intégration, tels que Windows Azure Pack (WAP) vers Cisco APIC, Cisco APIC vers System Center Virtual Machine Manager (SCVMM) et Cisco APIC vers Citrix ADC. En tant que locataire dans le cloud privé, vous pouvez activer NAT, fournir des services réseau et ajouter un équilibreur de charge.

WAP prend en charge les portails de locataire et d'administrateur où un administrateur peut effectuer des tâches administratives telles que l'enregistrement ACI, la plage VIP, l'association de périphériques Citrix ADC avec le cloud de machine virtuelle, la création de compte utilisateur locataire. Les locataires peuvent ouvrir une session sur le portail des locataires WAP et configurer le réseau, les domaines de pont et le routage et transfert virtuels (VRF), et utiliser les fonctionnalités d'équilibrage de charge Citrix ADC et RNAT.

> **Important**
>
> - Dans cette solution, l'appliance Citrix ADC fournit uniquement l'équilibrage de charge de base.
> - Les locataires peuvent déployer plusieurs adresses VIP avec différents ports pour le même réseau, mais doivent s'assurer que la combinaison IP et port est unique.
> - Le package de périphériques Citrix ADC prend en charge uniquement le déploiement à contexte unique. Chaque client reçoit une instance Citrix ADC dédiée.
> - WAP prend en charge les appliances Citrix ADC MPX et les appliances virtuelles Citrix ADC

> VPX, y compris les instances Citrix ADC VPX déployées sur la plate-forme Citrix ADC SDX.

L'illustration suivante donne une vue d'ensemble de la solution :



Conditions préalables

Assurez-vous que :

- Vous avez une connaissance conceptuelle des composants Cisco ACI et des Citrix ADC.
  - Pour plus d'informations sur Cisco ACI et ses composants, consultez la documentation produit à l'adresse suivante : http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
  - Pour plus d'informations sur les Citrix ADC, consultez la documentation produit Citrix ADC à l'adresse http://docs.citrix.com/.
- Tous les composants requis de Cisco ACI, y compris Cisco APIC dans le datacenter, sont configurés et configurés. Pour plus d'informations sur Cisco ACI et ses composants, consultez

la documentation produit à l'adresse suivante : http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

- Vous savez comment intégrer Cisco ACI avec Microsoft Windows Azure Pack. Consultez la documentation du produit à l'adresse suivante : http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/virtualization/b_ACI_Virtualization_Guide_2_2_1.html.
- Vous avez une connaissance conceptuelle de Microsoft Windows Azure Pack. Consultez la documentation du produit à l'adresse suivante : https://www.microsoft.com/en-in/cloud-platform/windows-azure-pack.
- Vous avez installé le logiciel Citrix ADC version 11.1 ou ultérieure.
- Vous configurez les Citrix ADC dans Cisco ACI, de sorte qu'ils puissent être gérés à l'aide de Cisco APIC.
- À partir de Cisco APIC, assurez-vous que :
  - La connectivité de gestion de Cisco APIC à Citrix ADC est établie.
  - Vous téléchargez le package de périphérique Citrix ADC version *11.1-52.3* et enregistrez le périphérique Citrix ADC dans Cisco ACI à l'aide de Cisco APIC.
  - Vous configurez l'appliance Citrix ADC dans le locataire commun de Cisco APIC et assurez-vous qu'il n'y a pas de défauts dans Cisco APIC.
  - Vous avez configuré toutes les configurations spécifiques APIC telles que, pool VLAN, L3OutServicesDom, L3ExtOUt, pool de ressources. Pour plus d'informations, consultez la *documentation de Cisco*.

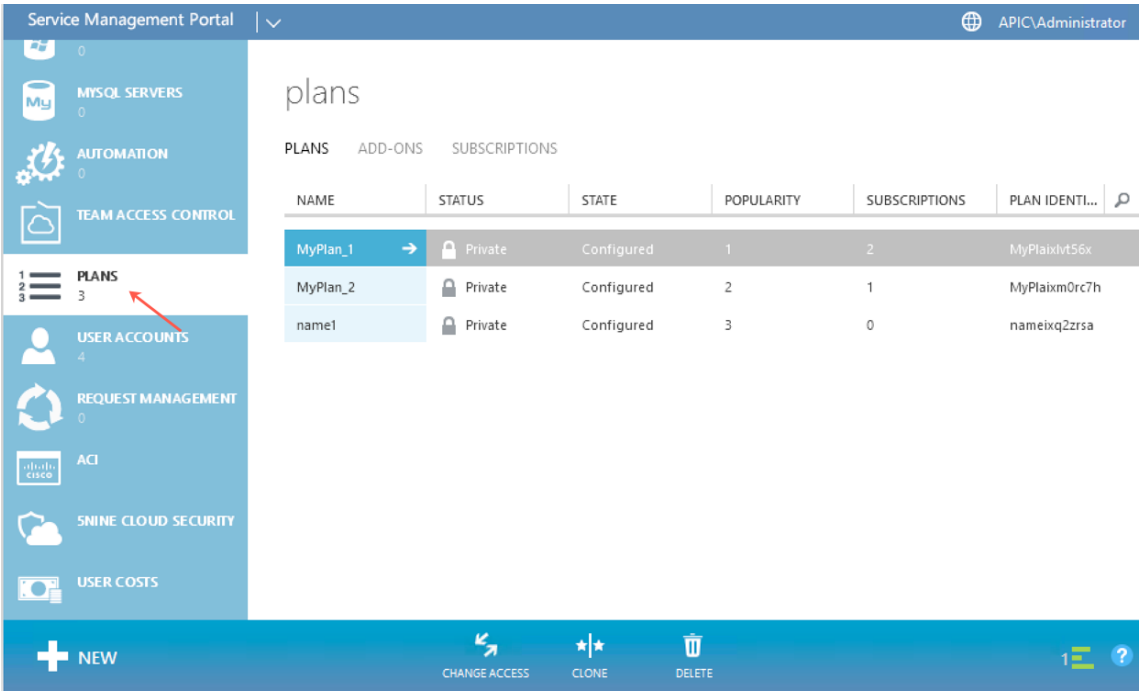
Création d'un équilibreur de charge Citrix ADC dans un plan dans le portail de gestion des services (portail d'administration)

January 21, 2021

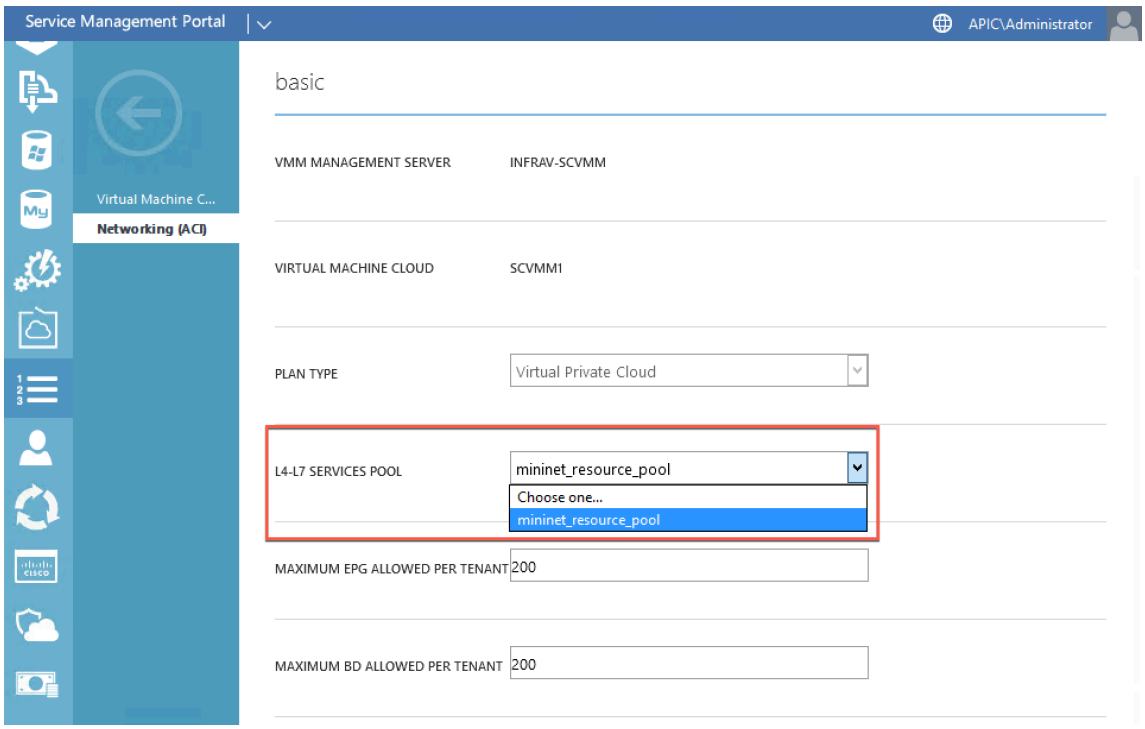
Le portail de gestion des services dans WAP permet à un administrateur d'enregistrer Cisco APIC auprès de WAP et de créer un plan d'hébergement. Dans le cadre du plan, vous pouvez spécifier la plage VIP, associer l'équilibreur de charge Citrix ADC au plan et créer des comptes d'utilisateurs locataires.

Pour créer un équilibreur de charge Citrix ADC dans un plan dans le portail d'administration :

1. Connectez-vous au portail de gestion des services (portail d'administration).
2. Dans le volet de navigation, sélectionnez **PLANS**.



3. Dans le volet Plans, sélectionnez le plan que vous souhaitez ajouter un équilibreur de charge.
4. Dans le volet du plan sélectionné, sélectionnez **Mise en réseau (ACI)**.
5. Dans le volet Mise en **réseau (ACI)**, dans la liste déroulante **POOL DE SERVICES L4-L7**, sélectionnez le pool de ressources L4-L7 que vous aviez créé dans Cisco APIC.



6. Créez un compte utilisateur locataire et associez l'utilisateur au plan que vous avez créé.

Configuration d'un équilibreur de charge Citrix ADC à l'aide du portail de gestion des services (portail client)

August 20, 2021

Dans WAP, une fois que le locataire crée le domaine de pont (BD), VRF et un réseau, le locataire peut configurer un équilibreur de charge Citrix ADC via le portail de gestion des services (Portail client).

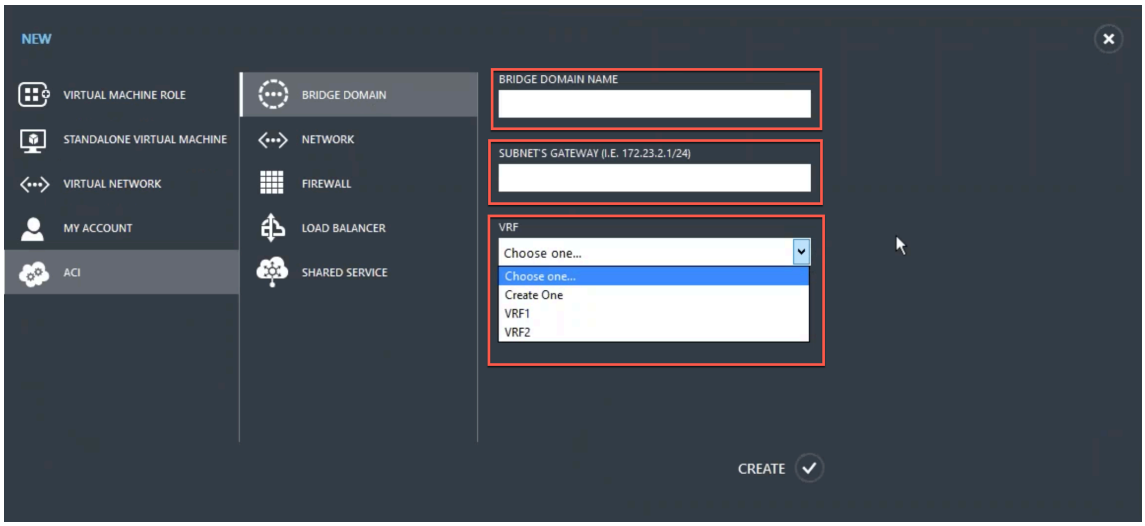
Pour configurer Citrix ADC Load Balancer dans Service Management Portal (portail client)

1. Ouvrez une session sur le portail de gestion des services (portail des locataires).
2. Créez un domaine de pont et VRF, comme suit :

   a. Dans le volet de navigation, sélectionnez **ACI**.

   b. Cliquez sur **NEW**.

   c. Dans le volet **NEW**, sélectionnez **BRIDGE DOMAIN**.



   d. Dans le champ **BRIDGE DOMAIN**, entrez le nom de domaine du pont (par exemple, BD01).

   e. (Facultatif) Dans le champ **SUBNET'S GATEWAY**, entrez la Gateway du sous-réseau (par exemple, 192.168.1.1/24).

   f. Dans le champ **VRF**, sélectionnez une VRF qui fait déjà partie de l'abonnement ou sélectionnez **Créer un** pour créer une VRF.

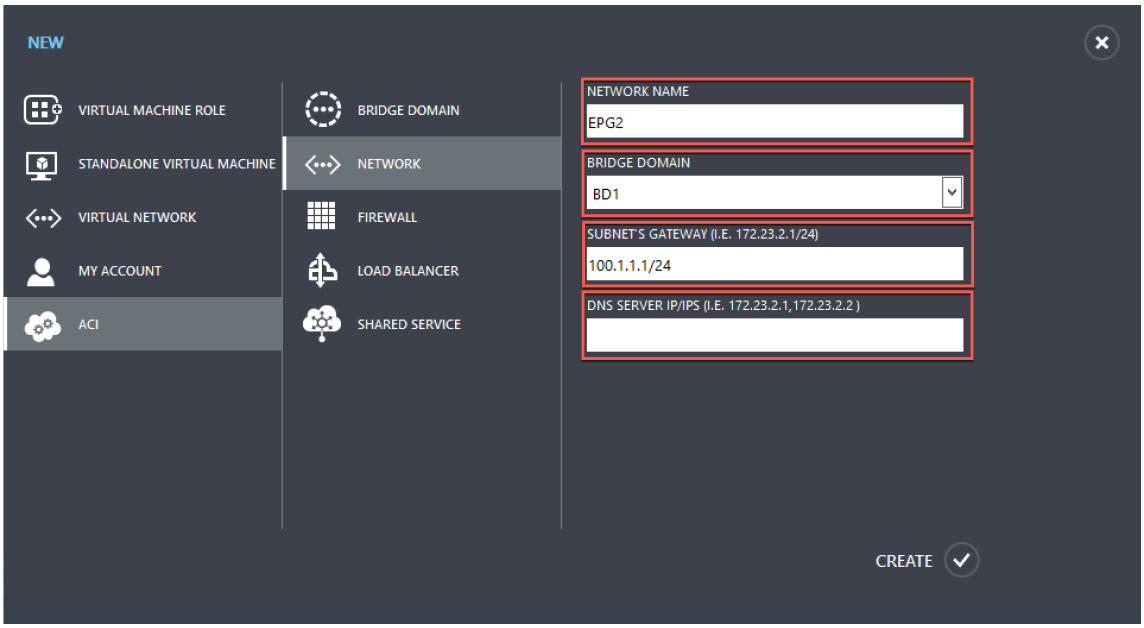
   g. Cliquez sur **CREATE**.

3. Créez un réseau et associez-le au domaine de pont que vous avez créé. Procédez comme suit :

   a. Dans le volet de navigation, sélectionnez **ACI**.

   b. Cliquez sur **NEW**.

c. Dans le volet **NEW**, sélectionnez **NETWORK**.



d. Dans le champ **NETWORK NAME**, entrez le nom du réseau (par exemple, S01).

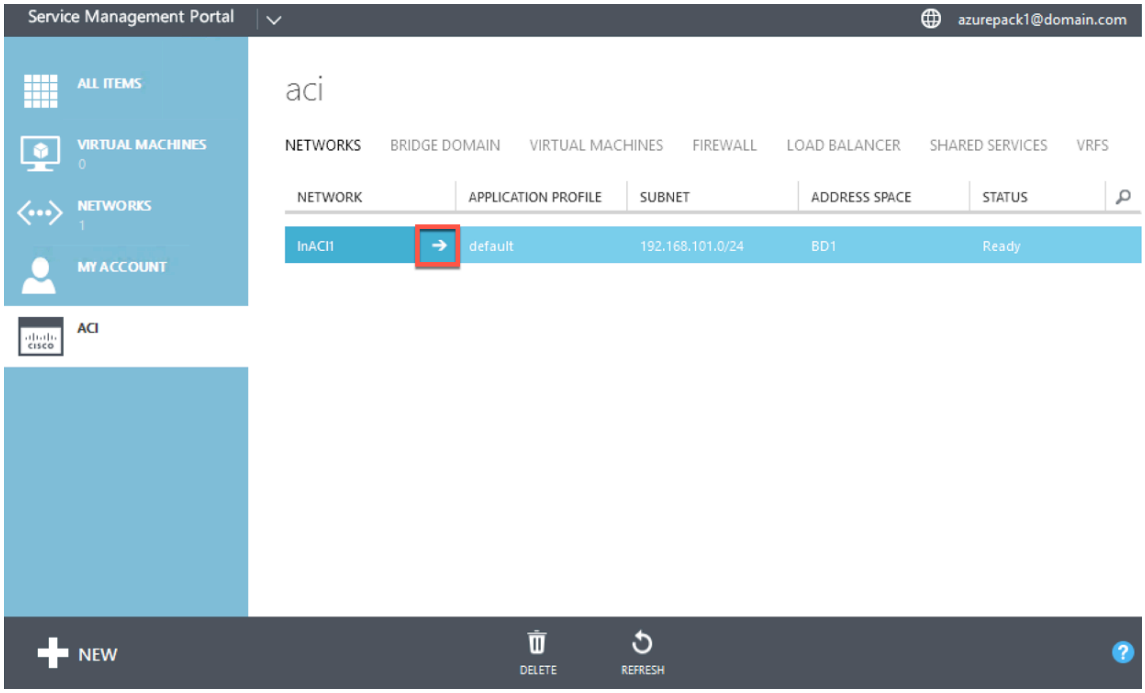
e. Dans la liste déroulante **BRIDGE DOMAIN**, sélectionnez le domaine de pont que vous avez créé. (par exemple, BD01).

f. Dans le champ **GATEWAY** du sous-réseau, entrez l'adresse de Gateway du sous-réseau (par exemple, 172.23.2.1/24).

g. (Facultatif) Dans le champ **DNS SERVER IP/IPS**, entrez les détails du serveur DNS.

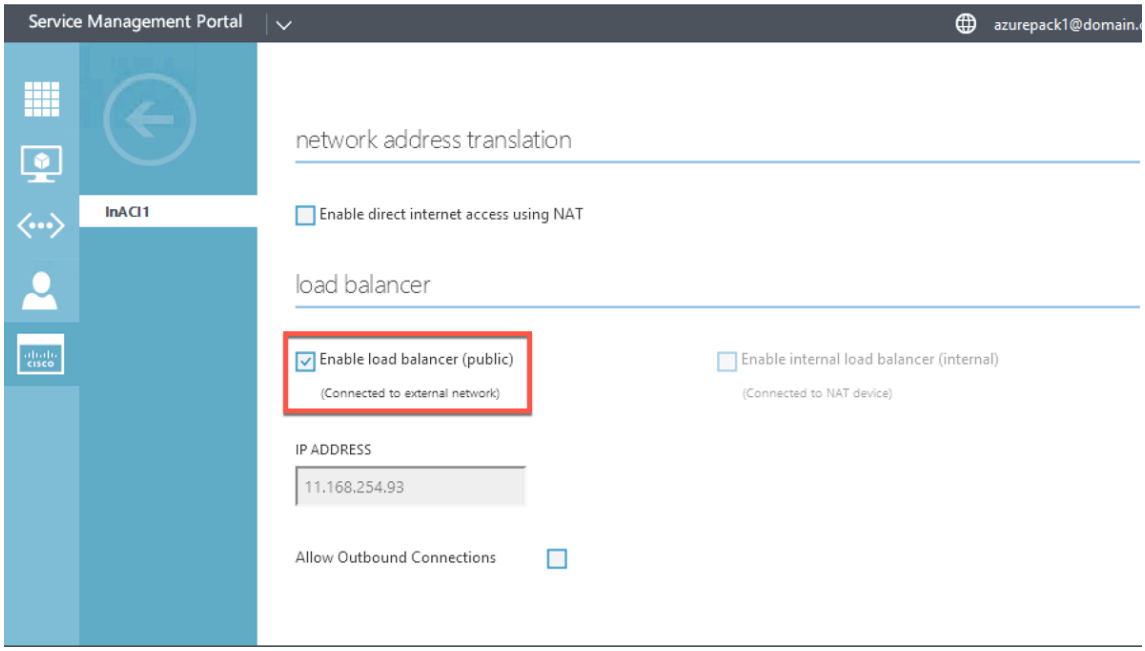
h. Cliquez sur **CREATE**.

4. Dans le volet **ACI**, sélectionnez **NETWORKS**.

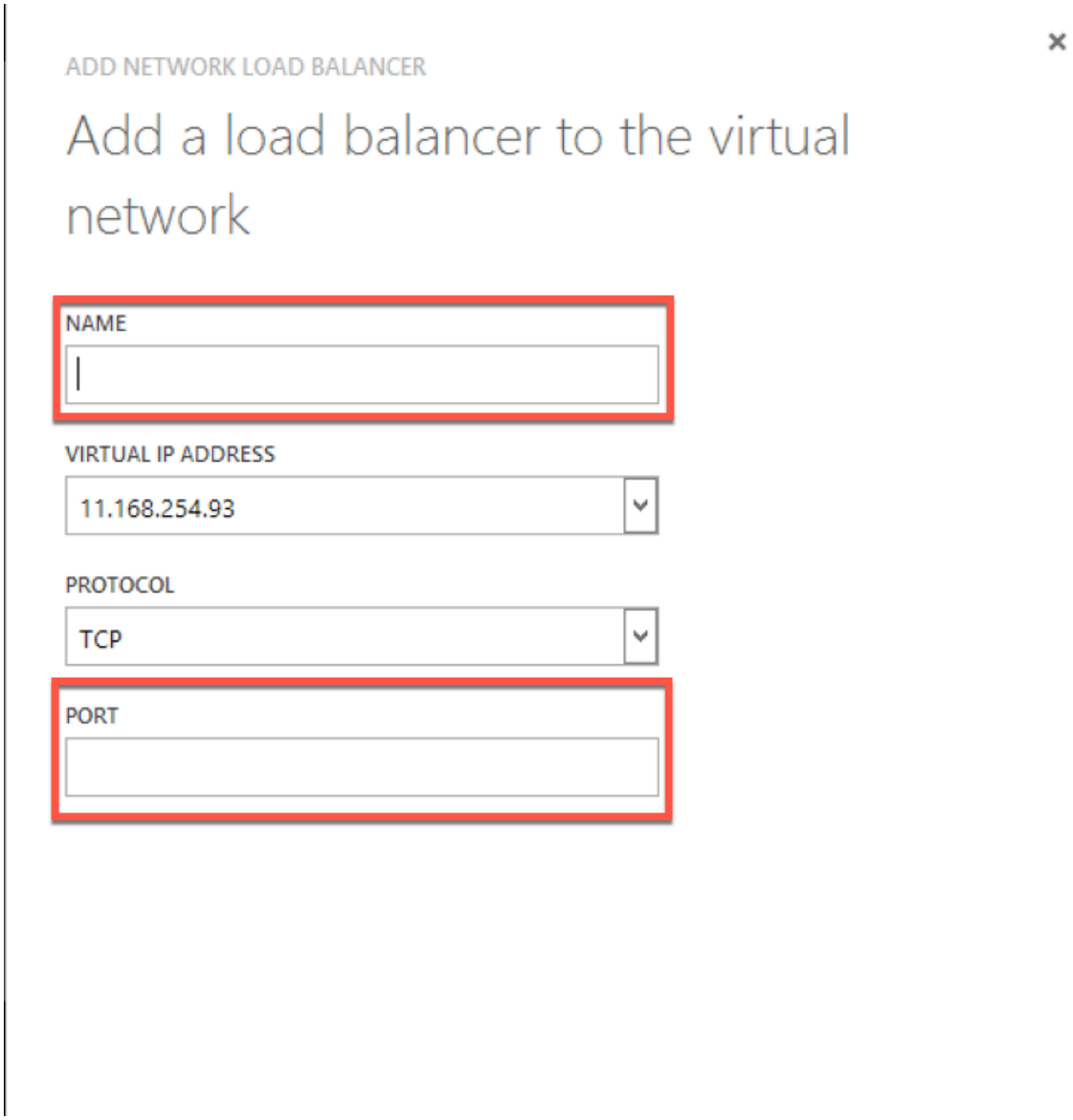


5. Double-cliquez sur le réseau que vous avez créé. Ensuite, dans le volet réseau, sélectionnez **Activer l'équilibrage de charge (public)**. Dans le champ **ADRESSE IP**, un VIP est automatiquement attribué à partir de la plage VIP configurée par l'administrateur dans le portail d'administration. Pour plus d'informations, voir Création d'un équilibreur de charge Citrix ADC dans un plan dans le portail de gestion des services (portail d'administration).

6. Double-cliquez sur le réseau que vous avez créé. Ensuite, dans le volet réseau, sélectionnez **Activer l'équilibrage de charge (public)**. Dans le champ **ADRESSE IP**, un VIP est automatiquement attribué à partir de la plage VIP configurée par l'administrateur dans le portail d'administration. Pour plus d'informations, voir Création d'un équilibreur de charge Citrix ADC dans un plan dans le portail de gestion des services (portail d'administration).



7. Dans le volet réseau, sélectionnez l'onglet **Équilibreurs de charge**, puis cliquez sur **AJOUTER**.



8. Dans le volet **ADD NETWORK LOAD BALANCER**, procédez comme suit :

   a. Dans le champ **NAME**, entrez le nom de l'équilibreur de charge.

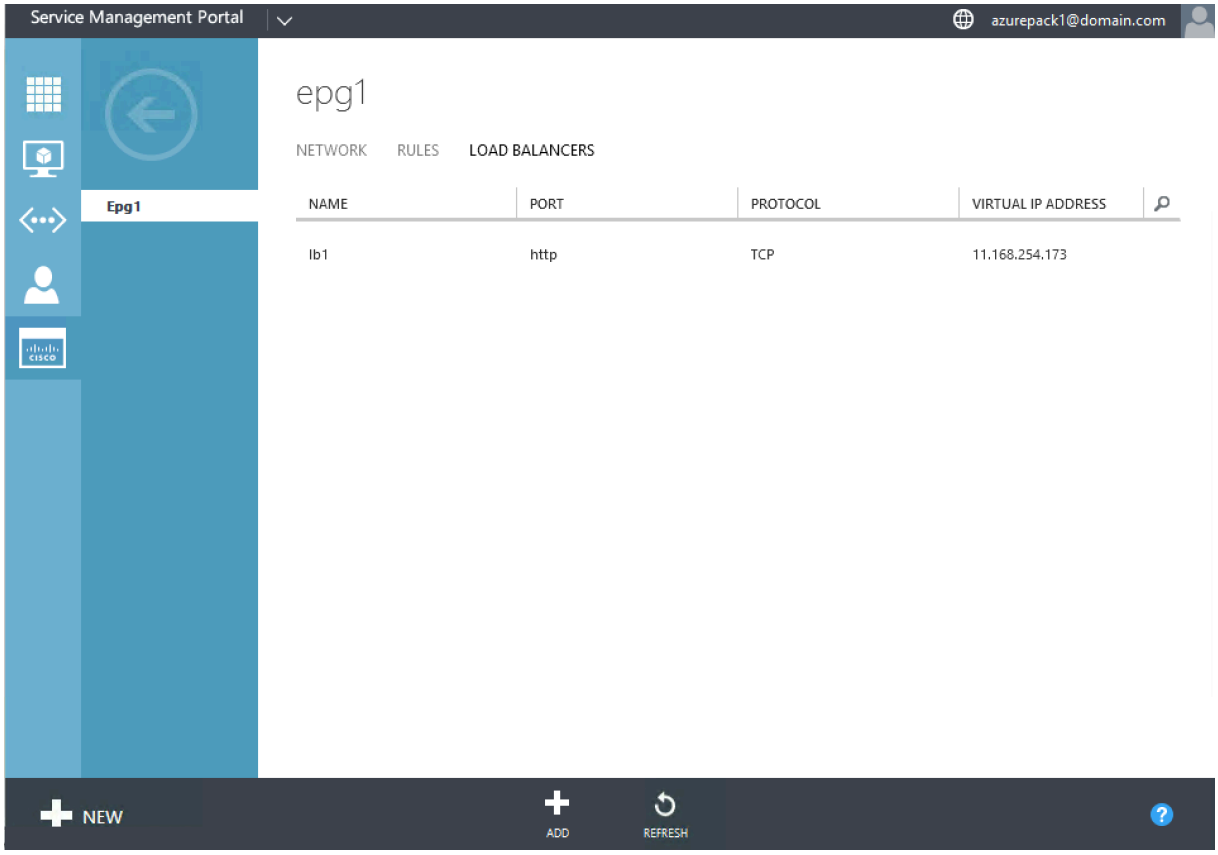
   b. Le cas échéant, dans le champ **VIRTUAL IP ADDRESS**, affectez à l'équilibreur de charge une adresse VIP de la plage VIP que vous avez définie précédemment.

   c. Le cas échéant, dans le champ **PROTOCOLE**, sélectionnez **TCP**.

   d. Dans le champ **PORT**, entrez le numéro de port.

9. Cliquez sur **CREATE**.

   L'équilibreur de charge Citrix ADC s'affiche dans l'onglet **LOAD BALANCERS** et Citrix ADC Load Balancer est prêt pour le chemin de données.



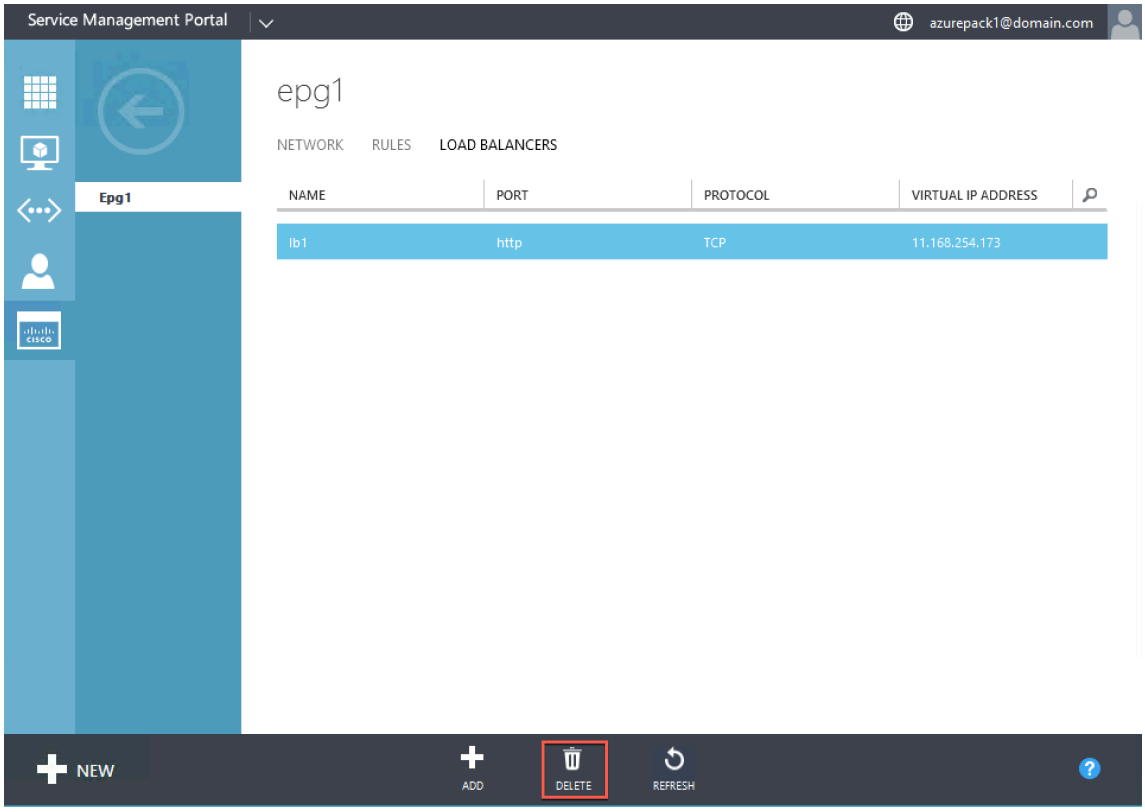
Suppression d'un équilibreur de charge Citrix ADC du réseau

January 21, 2021

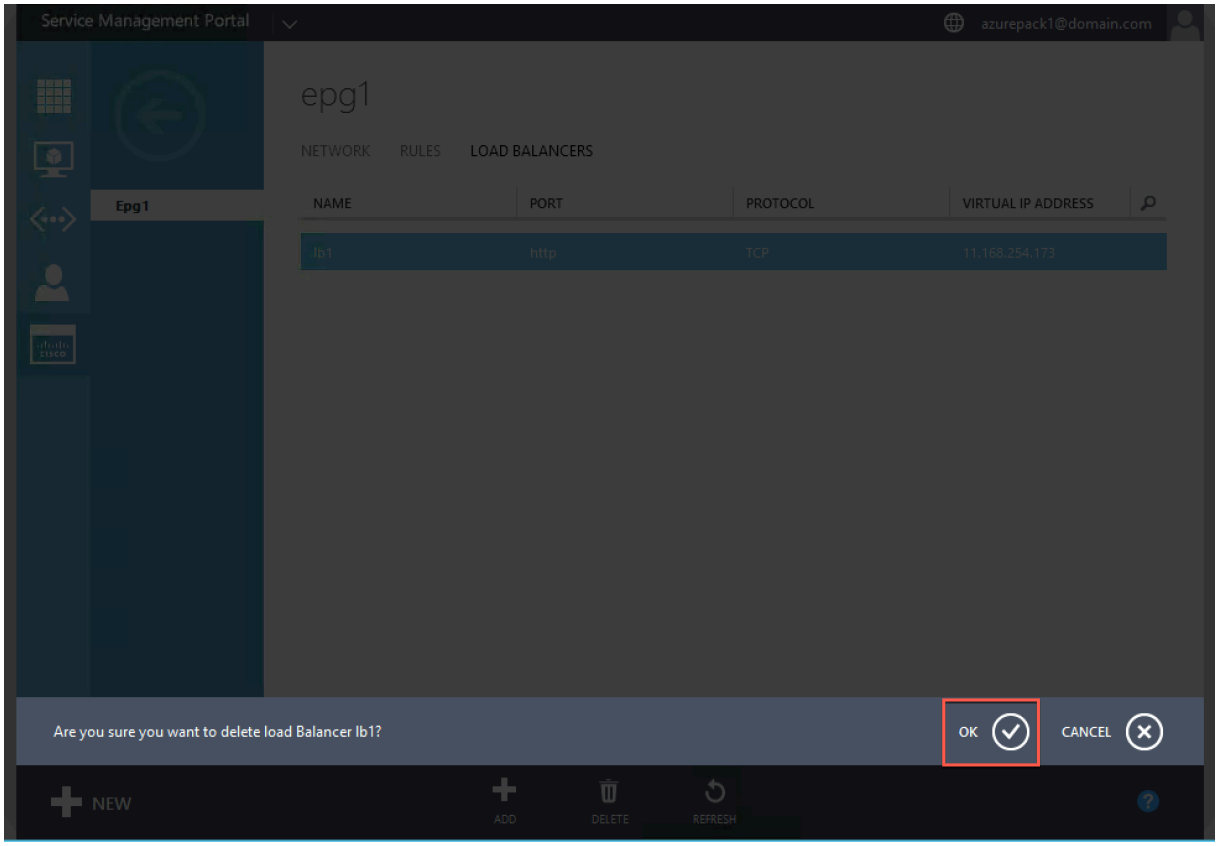
À l'aide du portail de gestion des services (Portail client), vous pouvez supprimer à partir du Réseau l'équilibreur de charge Citrix ADC que vous avez créé.

Pour supprimer un équilibreur de charge Citrix ADC du réseau :

1. Ouvrez une session sur le portail de gestion des services (portail des locataires).
2. Dans le volet de navigation, sélectionnez **ACI**.
3. Dans le volet **ACI**, sous l'onglet **RÉSEAUX**, cliquez sur le réseau que vous avez créé.
4. Dans le volet du réseau sélectionné, sélectionnez l'équilibreur de charge Citrix ADC et cliquez sur **SUPPRIMER**.



5. Cliquez sur **OK** pour supprimer l'équilibreur de charge Citrix ADC.



Solution native de cloud Citrix pour microservices basée sur Kubernetes

August 20, 2021

Alors que les entreprises se transforment pour innover plus rapidement et se rapprocher des clients, elles revoient l'architecture de leur processus interne et dépassent les frontières au sein de leur organisation. Ils retirent les silos pour rassembler les bons ensembles de compétences dans la même équipe. L'un des objectifs est de créer et de fournir des applications logicielles avec rapidité, agilité et efficacité. À cet égard, des architectures d'applications modernes basées sur des microservices sont adoptées par un nombre croissant d'entreprises.
À l'aide d'une architecture de microservices, vous pouvez créer des applications sous forme d'ensembles de services faiblement couplés qui peuvent être déployés, mis à jour et mis à l'échelle indépendamment.

Cloud native est une approche qui repose sur l'architecture de microservices pour créer et déployer des applications avec les attributs clés suivants :

- Déploie des applications sous forme de microservices ou de conteneurs à couplage lâche
- implique un très haut degré d'automatisation

- Implémente des processus DevOps agiles et des workflows de livraison continus
- Centres autour des API pour l'interaction et la collaboration

Comment Kubernetes aide-t-il dans le parcours natif du cloud ?

Pour fournir les niveaux d'agilité et de stabilité souhaités, les applications natives du cloud nécessitent des niveaux élevés d'automatisation, de sécurité, de mise en réseau et de surveillance de l'infrastructure. Vous avez besoin d'un système d'orchestration de conteneurs capable de gérer efficacement les conteneurs à grande échelle. Kubernetes est devenue la plate-forme la plus populaire pour le déploiement et l'orchestration de conteneurs. Kubernetes résume la tâche complexe d'exécution, de déploiement et de gestion des conteneurs des développeurs et des opérateurs et planifie automatiquement les conteneurs entre un cluster de nœuds. Kubernetes et l'écosystème Cloud Native Computing Foundation (CNCF) vous aident à construire une plateforme pour les solutions natives dans le cloud.

Certains des principaux avantages de l'utilisation de Kubernetes :

- Simplifie le déploiement des applications, qu'il s'agisse d'une infrastructure locale, hybride ou de cloud public
- Accélère le développement et le déploiement des applications
- Augmente l'agilité, la flexibilité et l'évolutivité des applications

Qu'est-ce que la solution native de Citrix Cloud ?

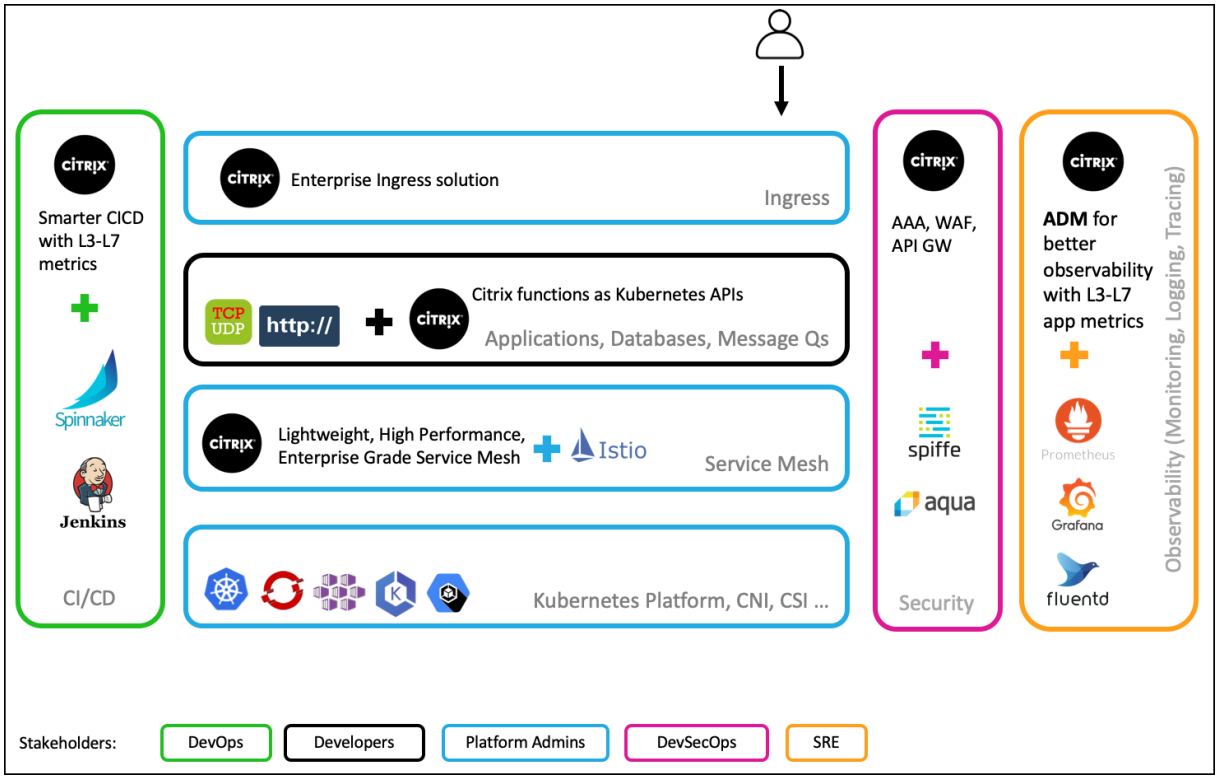
Pour maximiser les avantages de l'utilisation de Kubernetes en production, vous devez intégrer Kubernetes avec plusieurs outils, composants fournisseurs et open source. Garantir une fiabilité et une sécurité de qualité production pour leur application native dans le cloud est un défi auquel doivent faire face de nombreuses entreprises.
En tant que fournisseur de produits ADC Citrix leader du secteur, Citrix propose une solution native de cloud Citrix pour relever les défis dans un environnement de production Kubernetes.

La solution native du cloud Citrix exploite les fonctionnalités avancées de gestion du trafic, d'observabilité et de sécurité complètes des ADC Citrix pour garantir une fiabilité et une sécurité de niveau entreprise. Il peut fournir une visibilité complète du trafic des applications dans votre environnement Kubernetes, rendre des commentaires immédiats et vous aider à obtenir des informations significatives sur les performances de l'application.

Le tableau suivant répertorie les principales exigences des différentes parties prenantes lors de la mise en œuvre d'une solution Ingress.

Intervenants	Fonction Job	les besoins
Administrateurs de plate-forme	Garantir la disponibilité des clusters Kubernetes	Des méthodes plus simples de gestion des applications déployées sur plusieurs clusters, des opérations et de la gestion du cycle de vie des plates-formes
DevOps	Accélérer le déploiement des applications en production	Intégration avec le pipeline CI/CD, prise en charge des techniques de déploiement comme Canary et bleu-vert pour un déploiement plus rapide
Développeurs	Développer et tester des microservices	Méthodes d'acheminement du trafic dans le cluster Kubernetes, suivi et débogage, limitation de débit pour les applications et authentification pour les applications
SREs	Garantir la disponibilité des applications pour respecter les accords de niveau de service	Télémétrie avancée pour les applications et l'infrastructure
SecOPs	Garantir la conformité en matière	Trafic d'entrée sécurisé, protection des API, maillage de service pour une communication sécurisée entre les microservices au sein du cluster Kubernetes

Le diagramme suivant explique la solution native du cloud Citrix et comment elle répond aux divers défis auxquels les parties prenantes sont confrontées dans leur parcours natif dans le cloud.



La solution native du cloud Citrix offre les principaux avantages suivants :

- Fournit une solution Kubernetes Ingress avancée qui répond aux besoins des développeurs, des SRE, des DevOps et des administrateurs de réseau ou de cluster.
- Élimine le besoin de réécrire les applications héritées basées sur le trafic TCP ou UDP tout en les déplaçant dans un environnement Kubernetes.
- Sécurise les applications avec des stratégies Citrix ADC exposées en tant qu'API Kubernetes.
- Aide à déployer des microservices performants pour le trafic Nord-Sud et le trafic Est-Ouest.
- Fournit une vue tout-en-un de tous les microservices à l'aide du graphique de service Citrix ADM.
- Permet un dépannage plus rapide des microservices sur différents types de trafic, y compris TCP, UDP, HTTP, HTTPS et SSL.
- Sécurise les API.
- Automatise le pipeline CI/CD pour les déploiements Canaries.
- Fournit des intégrations prédéfinies avec les outils open source du CNCF.

Pour plus d'informations sur les différents composants de la solution native de cloud Citrix, consultez les liens suivants :

- Solution d'entrée de Kubernetes
- Service mesh
- Solutions pour l'observabilité
- Passerelle API pour Kubernetes

Solution d'entrée de Kubernetes

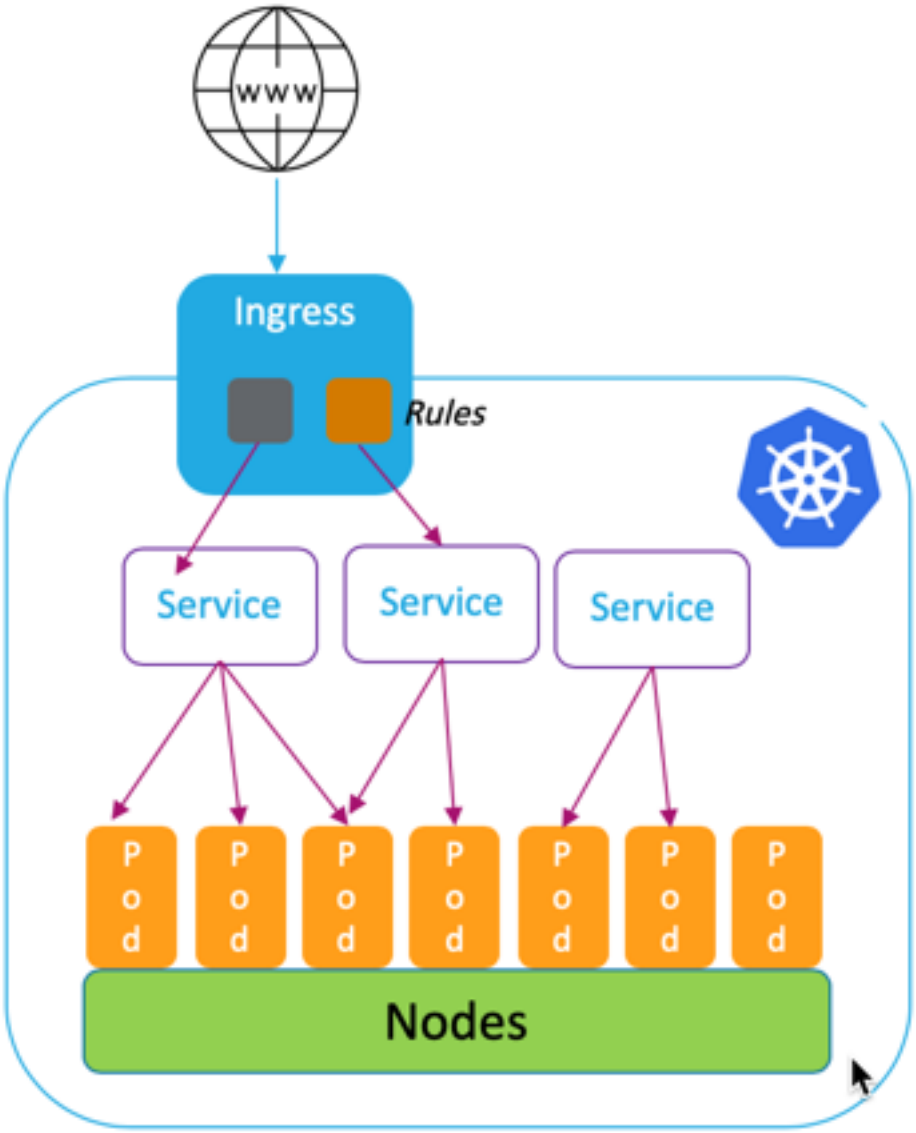
August 20, 2021

Cette rubrique fournit une vue d'ensemble de la solution Kubernetes Ingress fournie par Citrix et explique les avantages.

Qu'est-ce que Kubernetes Ingress ?

Lorsque vous exécutez une application dans un cluster Kubernetes, vous devez fournir aux utilisateurs externes un moyen d'accéder aux applications depuis l'extérieur du cluster Kubernetes. Kubernetes fournit un objet appelé Ingress qui fournit le moyen le plus efficace d'exposer plusieurs services à l'aide d'une adresse IP stable. Un objet d'entrée Kubernetes est toujours associé à un ou plusieurs services et agit comme un point d'entrée unique permettant aux utilisateurs externes d'accéder aux services exécutés à l'intérieur du cluster.

Le diagramme suivant explique comment fonctionne Kubernetes Ingress.



L'implémentation de Kubernetes Ingress comprend les composants suivants :

- **Ressource d'entrée**. Une ressource Ingress vous permet de définir des règles pour accéder aux applications depuis l'extérieur du cluster.
- **Contrôleur d'entrée**. Un contrôleur d'entrée est une application déployée dans le cluster qui interprète les règles définies dans l'entrée. Ingress Controller convertit les règles d'entrée en instructions de configuration pour une application d'équilibrage de charge intégrée au cluster. L'équilibreur de charge peut être une application logicielle exécutée dans votre cluster Kubernetes ou une appliance matérielle s'exécutant en dehors du cluster.
- **Dispositif d'entrée**. Un périphérique d'entrée est une application d'équilibrage de charge telle

que Citrix ADC CPX, VPX ou MPX qui effectue l'équilibrage de charge selon les instructions de configuration fournies par le contrôleur Ingress.

Qu'est-ce que la solution Kubernetes Ingress de Citrix ?

Dans cette solution, Citrix fournit une implémentation du contrôleur d'entrée Kubernetes pour gérer et acheminer le trafic vers votre cluster Kubernetes en utilisant Citrix ADC (Citrix ADC CPX, VPX ou MPX). Le Citrix ingress controller intègre Citrix ADC à votre environnement Kubernetes et configure Citrix ADC CPX, VPX ou MPX conformément aux règles d'entrée.

Les solutions standard Kubernetes Ingress fournissent un équilibrage de charge uniquement à la couche 7 (trafic HTTP ou HTTPS). Parfois, vous devez exposer de nombreuses applications héritées qui reposent sur TCP, UDP ou applications et qui ont besoin d'un moyen d'équilibrer la charge de ces applications. La solution Citrix Kubernetes Ingress fournit la prise en charge du trafic TCP, TCP-SSL et UDP en dehors de l'entrée HTTP ou HTTPS standard. En outre, il fonctionne de manière transparente sur plusieurs clouds ou centres de données locaux.

Citrix ADC fournit des stratégies de gestion du trafic de niveau entreprise telles que les stratégies de réécriture et de répondeur pour équilibrer efficacement la charge du trafic à la couche 7. Cependant, Kubernetes Ingress ne dispose pas de telles stratégies de gestion du trafic de niveau entreprise. Avec la solution Kubernetes Ingress de Citrix, vous pouvez appliquer des stratégies de réécriture et de répondeur pour le trafic des applications dans un environnement Kubernetes à l'aide de CRD fournis par Citrix.

La solution Kubernetes Ingress de Citrix prend également en charge le déploiement canari automatisé pour votre pipeline d'applications CI/CD. Dans cette solution, Citrix ADC est intégré à la plateforme Spinnaker et sert de source pour fournir des mesures précises pour l'analyse du déploiement Canary à l'aide de Kayenta. Après avoir analysé les mesures, Kayenta génère un score agrégé pour le Canari et décide de promouvoir ou d'échouer la version Canary. Vous pouvez également réglementer la distribution du trafic vers la version Canary à l'aide de l'infrastructure de stratégie Citrix ADC.

Le tableau suivant résume les avantages offerts par la solution Ingress de Citrix par rapport à Kubernetes Ingress.

Fonctionnalités	Kubernetes Ingress	Solution d'entrée de Citrix
Prise en charge HTTP et HTTPS	Oui	Oui
Routage URL	Oui	Oui
TLS	Oui	Oui
Équilibrage de charge	Oui	Oui
TCP, TCP-SSL	Non	Oui

Fonctionnalités	Kubernetes Ingress	Solution d'entrée de Citrix
UDP	Non	Oui
HTTP/2	Oui	Oui
Prise en charge automatisée du déploiement canari avec des outils CI/CD	Non	Oui
Prise en charge de l'application des stratégies de réécriture et de réponse Citrix ADC	Non	Oui
Authentification (OAuth), TLS mutuel (MTL))	Non	Oui
Prise en charge de l'application de stratégies Citrix Rate Limitation	Non	Oui

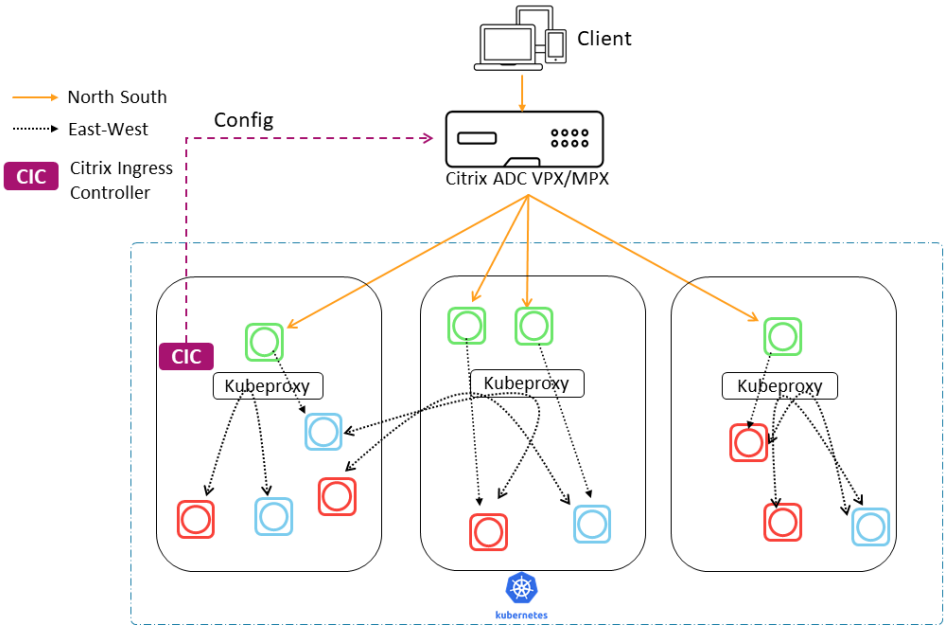
Options de déploiement de la solution Kubernetes Ingress

La solution Kubernetes Ingress de Citrix vous offre une architecture flexible en fonction de la façon dont vous souhaitez gérer vos environnements Citrix ADC et Kubernetes.

Entrée unifiée (à un niveau)

Dans une architecture d'entrée unifiée (à niveau unique), un périphérique Citrix MPX ou VPX déployé en dehors du cluster Kubernetes est intégré à l'environnement Kubernetes à l'aide du Citrix ingress controller. Le Citrix ingress controller est déployé en tant qu'espace dans le cluster Kubernetes et automatise la configuration de Citrix ADC en fonction des modifications apportées aux microservices ou aux ressources Ingress. Le périphérique Citrix ADC exécute des fonctions telles que l'équilibrage de charge, la terminaison TLS et les optimisations de protocole HTTP ou TCP sur le trafic entrant, puis achemine le trafic vers le microservice correct au sein d'un cluster Kubernetes. Cette architecture convient le mieux dans les scénarios où la même équipe gère la plate-forme Kubernetes et d'autres infrastructures réseau, y compris les contrôleurs de livraison d'applications (ADC).

Le diagramme suivant montre un déploiement utilisant l'architecture d'entrée unifiée.



Une solution Ingress unifiée offre les principaux avantages suivants :

- Fournit un moyen d'étendre les fonctionnalités de votre infrastructure Citrix ADC existante à l'environnement Kubernetes
- Permet d'appliquer des stratégies de gestion du trafic pour le trafic entrant
- Fournit une architecture simplifiée adaptée aux équipes DevOps averties du réseau
- Prise en charge de la multilocation

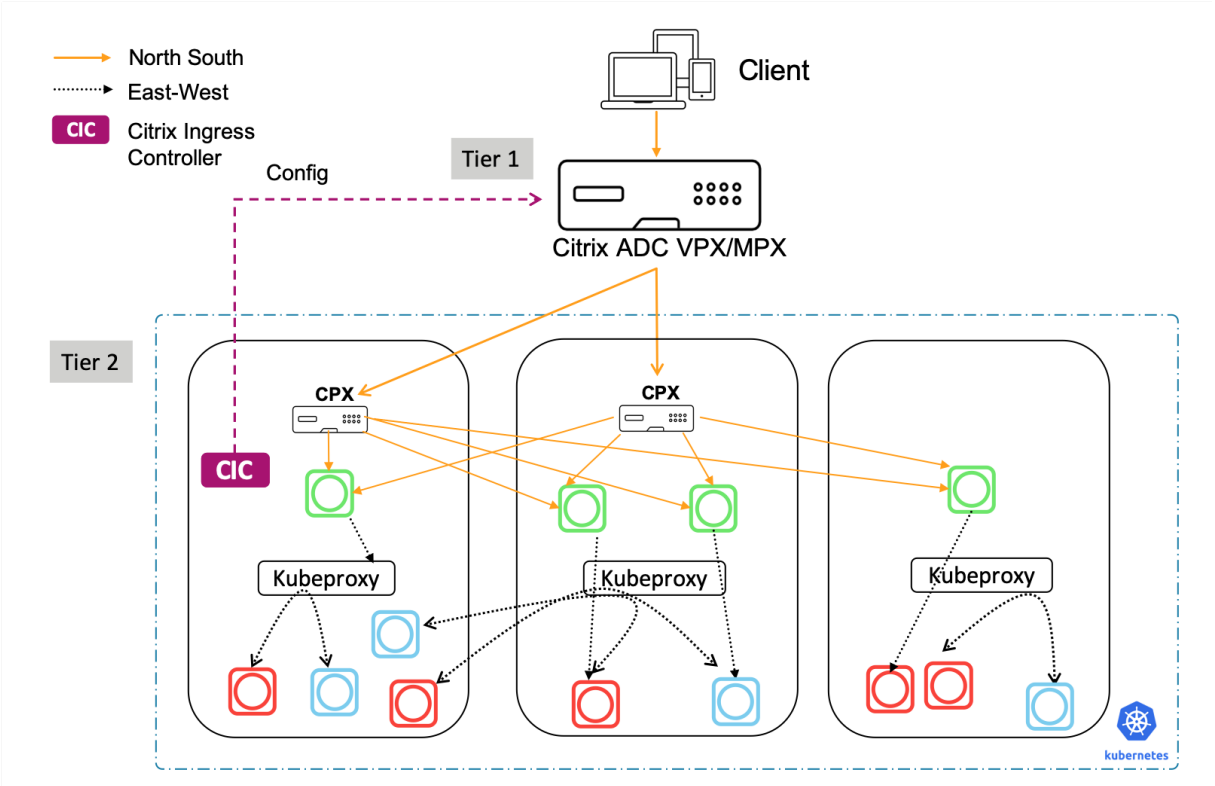
Pression à deux niveaux

Dans une architecture à deux niveaux, Citrix ADC (MPX ou VPX) déployé en dehors du cluster Kubernetes agit au niveau 1 et équilibre la charge du trafic Nord-Sud vers les CPX Citrix ADC exécutés à l'intérieur du cluster. Citrix ADC CPX agit au niveau 2 et effectue l'équilibrage de charge pour les microservices au sein du cluster Kubernetes.

Dans les scénarios où des équipes distinctes gèrent la plate-forme Kubernetes et l'infrastructure réseau, l'architecture à deux niveaux convient le mieux.

Les équipes de mise en réseau utilisent Citrix ADC de niveau 1 pour les cas d'utilisation tels que GSLB, la terminaison TLS sur la plate-forme matérielle et l'équilibrage de charge TCP. Les équipes de plate-forme Kubernetes peuvent utiliser Citrix ADC (CPX) de niveau 2 pour l'équilibrage de charge de couche 7 (HTTP/HTTPS), le TLS mutuel et l'observabilité ou la surveillance des microservices. Le Citrix ADC (CPX) de niveau 2 peut avoir une version logicielle différente de celle du Citrix ADC de niveau 1 pour prendre en charge les nouvelles fonctionnalités disponibles.

Le diagramme suivant montre un déploiement avec architecture à deux niveaux.



Une entrée à deux niveaux offre les avantages clés suivants :

- Garantit une vitesse élevée de développement d'applications pour les développeurs ou les équipes de plateformes
- Permet d'appliquer des stratégies de gestion du trafic pilotées par les développeurs pour les microservices au sein du cluster Kubernetes
- Permet l'évolutivité du cloud et la multilocation

Pour plus d'informations, consultez la documentation Citrix ingress controller.

Mise en route

Pour commencer à utiliser la solution Kubernetes Ingress de Citrix, vous pouvez essayer les exemples suivants :

- Équilibre de charge Trafic d'entrée avec Citrix ADC CPX dans Minikube
- Trafic d'entrée Nord-Sud à l'aide du proxy Citrix ADC CPX
- Équilibrage de la charge trafic des microservices Est-Ouest à l'aide du proxy Citrix ADC CPX
- Plongée profonde sur les fonctionnalités de Kubernetes avec Citrix ADC CPX

Service mesh

August 20, 2021

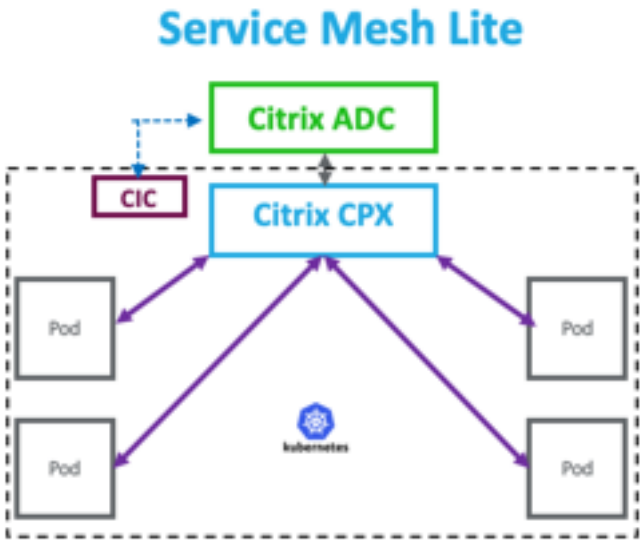
Un maillage de service est une couche d'infrastructure permettant de gérer la communication service-service pour les applications natives dans le cloud à l'aide d'API. Il fournit un moyen de connecter, de sécuriser et de surveiller vos microservices. Citrix fournit deux solutions pour répondre aux exigences de votre maillage de service :

- Service mesh lite
- Service mesh (intégration de Citrix ADC avec Istio)

Service mesh lite

Une implémentation à part entière du maillage de service-mesh est complexe et nécessite une courbe d'apprentissage abrupte. Si vous recherchez une implémentation simplifiée d'un service mesh offrant des avantages similaires, Citrix propose une solution appelée service mesh lite avec une complexité moindre. Dans cette solution, un Citrix ADC CPX s'exécute comme un équilibreur de charge centralisé dans le cluster Kubernetes et équilibre la charge du trafic Est-Ouest entre les microservices. Citrix ADC CPX applique des stratégies pour le trafic entrant et interconteneur.

Le diagramme suivant montre une architecture lite de maillage de service.



Pour plus d'informations, reportez-vous à la documentation Service Mesh Lite.

Service mesh (intégration de Citrix ADC avec Istio)

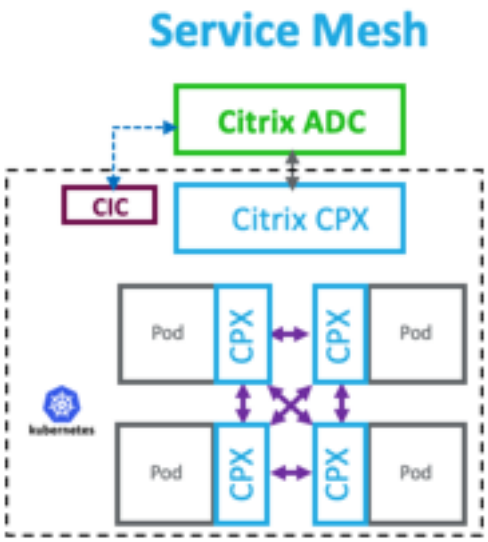
Citrix fournit une solution de maillage de service en intégrant Citrix ADC à Istio. Istio, un maillage de service open source et indépendant de la plate-forme, est l'une des implémentations de maillage de service les plus populaires. En intégrant Citrix ADC à Istio, vous pouvez tirer parti des fonctionnalités Citrix ADC pour sécuriser et optimiser le trafic des applications dans le maillage de service.

Citrix ADC peut être intégré à Istio de la manière suivante :

- Citrix ADC MPX, VPX ou CPX en tant que passerelle d'entrée Istio vers le maillage de service pour exposer le trafic vers le cluster Kubernetes.
- Citrix ADC CPX en tant que proxy sidecar avec conteneurs d'application dans le maillage de service pour contrôler la communication entre les applications.

Vous pouvez utiliser l'intégration indépendamment ou vous pouvez combiner les deux façons d'avoir une solution de plan de données unifié.

Le diagramme suivant présente une architecture de maillage de service.



Le maillage de service est idéal pour les applications hautement sécurisées et offre également les avantages suivants.

- Offre une gestion du trafic à grain fin (modularisé) par conteneur
- Assure une observabilité, des analyses et une sécurité plus riches (Mutual TLS) grâce à l'implémentation sidecar
- Permet un déploiement canari automatisé pour chaque conteneur avec Citrix ADC CPX intégré
- Prise en charge de la portabilité cloud

- Permet de décharger certaines des fonctions exécutées par les applications vers le sidecar
- Fournit une latence latence latérale inférieure
- Fournit des intégrations avec des outils open source
- Offre une évolutivité

Pour plus d'informations, consultez la documentation sur l'intégration Citrix ADC avec Istio.

Solutions pour l'observabilité

August 20, 2021

Dans une architecture basée sur les microservices, la visibilité des communications de service à service est essentielle pour créer une architecture efficace et résiliente. Les méthodes traditionnelles de journalisation et de surveillance ne sont pas capables de relever les défis d'une architecture de microservices. Les solutions d'observabilité de Citrix vous permettent de voir ce qui se passe lorsque vos services interagissent les uns avec les autres et d'obtenir des informations significatives sur votre système.

Citrix fournit les solutions suivantes pour répondre aux besoins d'observabilité de votre architecture de microservices :

- Graphe et analyse du service Citrix ADM
- Exportateur d'observabilité Citrix ADC

Graphe et analyse du service Citrix ADM

Citrix Application Delivery Management (ADM) est une solution de gestion centralisée qui offre une visibilité et une automatisation à l'échelle de l'entreprise pour les tâches de gestion qui doivent être exécutées sur plusieurs instances.

Dans une architecture de microservices, le dépannage est difficile car une seule demande d'utilisateur final peut s'étendre sur plusieurs microservices.

Le graphique et l'analyse des services de Citrix ADM fournissent une visibilité sur les interactions entre les microservices et permettent d'identifier et de résoudre les problèmes en fonction de diverses mesures telles que la latence et les erreurs HTTP.

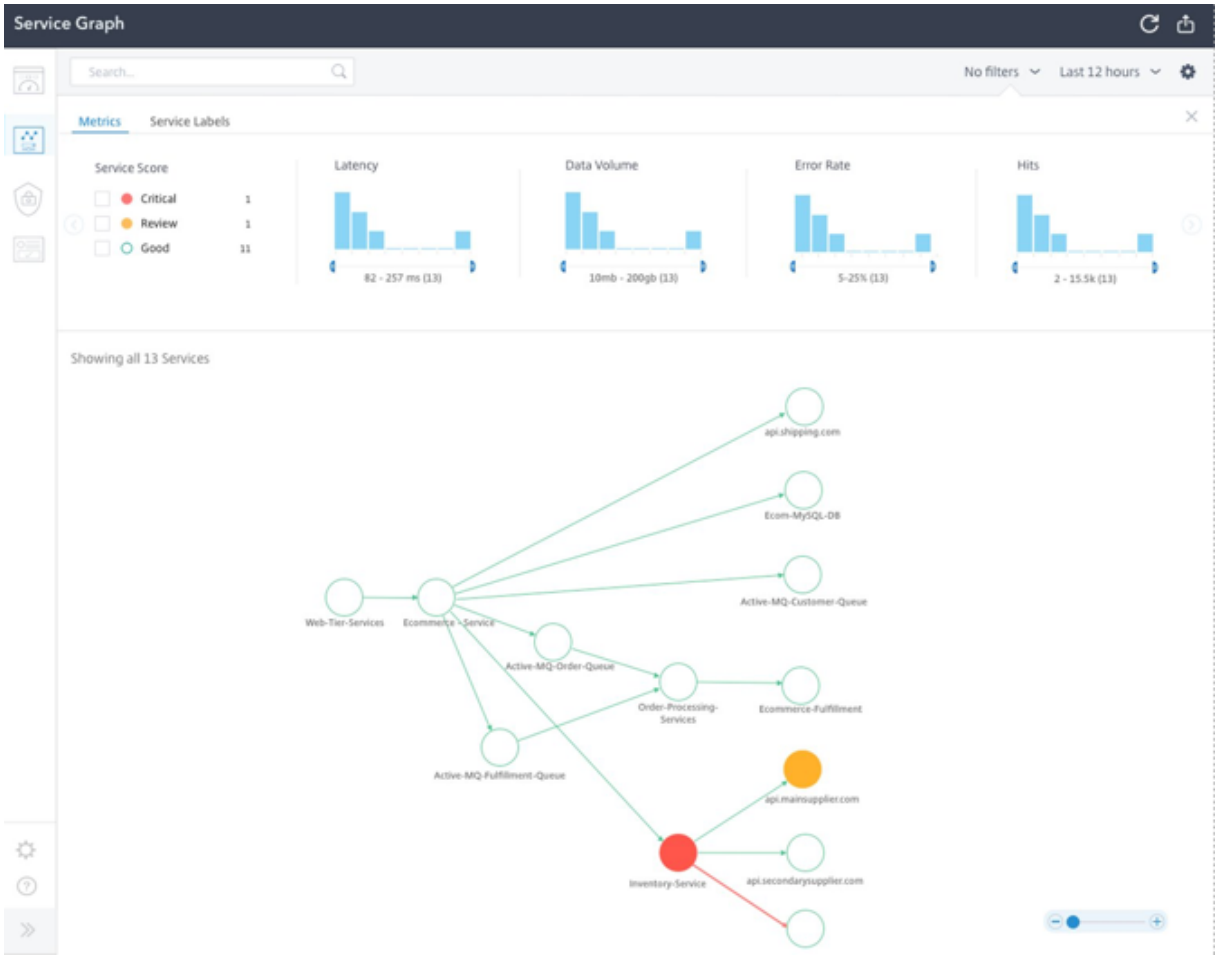
Citrix ADM fournit également des analyses avancées basées sur des mesures et des journaux de transactions collectés à partir de Citrix ADC.

La solution Citrix ADM offre les avantages suivants :

- Fournit un seul panneau de verre pour les applications sur les conteneurs, sur site ou dans le cloud

- Offre une meilleure observabilité et un dépannage plus rapide pour les microservices
- Prise en charge du déploiement Canary

Le diagramme suivant présente un exemple de graphique de service pour une application qui contient plusieurs microservices.



Pour plus d'informations sur la configuration de Citrix ADM Service Graph and Analytics, reportez-vous au Service Graph et à la documentation Analytics .

Exportateur d'observabilité Citrix ADC

L'exportateur d'observabilité Citrix ADC est un conteneur qui collecte des mesures et des transactions à partir de Citrix ADC et les transforme en formats appropriés (tels que JSON, AVRO) pour les points de terminaison pris en charge. Vous pouvez exporter les données collectées par l'exportateur d'observabilité Citrix ADC vers le point de terminaison souhaité. En analysant les données, vous pouvez obtenir des informations précieuses au niveau des microservices pour les applications mandatées par les ADC Citrix.

Prise en charge du traçage distribué

Les traceurs distribués vous permettent de visualiser le flux de données entre vos microservices et d'identifier les goulots d'étranglement dans votre architecture de microservices. OpenTracing est une spécification et un ensemble standard d'API pour la conception et la mise en œuvre du suivi distribué.

Citrix observability exporter implémente le suivi distribué pour Citrix ADC et prend actuellement en charge Zipkin en tant que traceur distribué.

Vous pouvez améliorer l'analyse des traces en utilisant Elasticsearch et Kibana avec Zipkin. Elasticsearch assure la conservation à long terme des données de trace. Kibana vous permet d'obtenir des informations beaucoup plus approfondies sur les données en fournissant un outil pour explorer et visualiser les messages de journal.

Collecte des transactions et support en streaming

L'exportateur d'observabilité Citrix ADC prend en charge la collecte des transactions et leur diffusion en continu vers les points de terminaison. Actuellement, l'exportateur d'observabilité Citrix ADC prend en charge Elasticsearch et Kafka comme points de terminaison de transaction.

Pour plus d'informations, consultez la documentation de l'exportateur d'observabilité Citrix ADC.

Activer les analyses à l'aide d'annotations dans le fichier YAML Citrix ingress controller

Vous pouvez activer l'analyse à l'aide du profil analytique défini comme une annotation intelligente dans Ingress ou service de type LoadBalancer configuration. Vous pouvez définir les paramètres spécifiques que vous devez surveiller en les spécifiant dans la configuration d'entrée ou de service de l'application. Pour plus d'informations sur l'activation de l'analyse à l'aide d'annotations, voir Analytics utilisant des annotations.

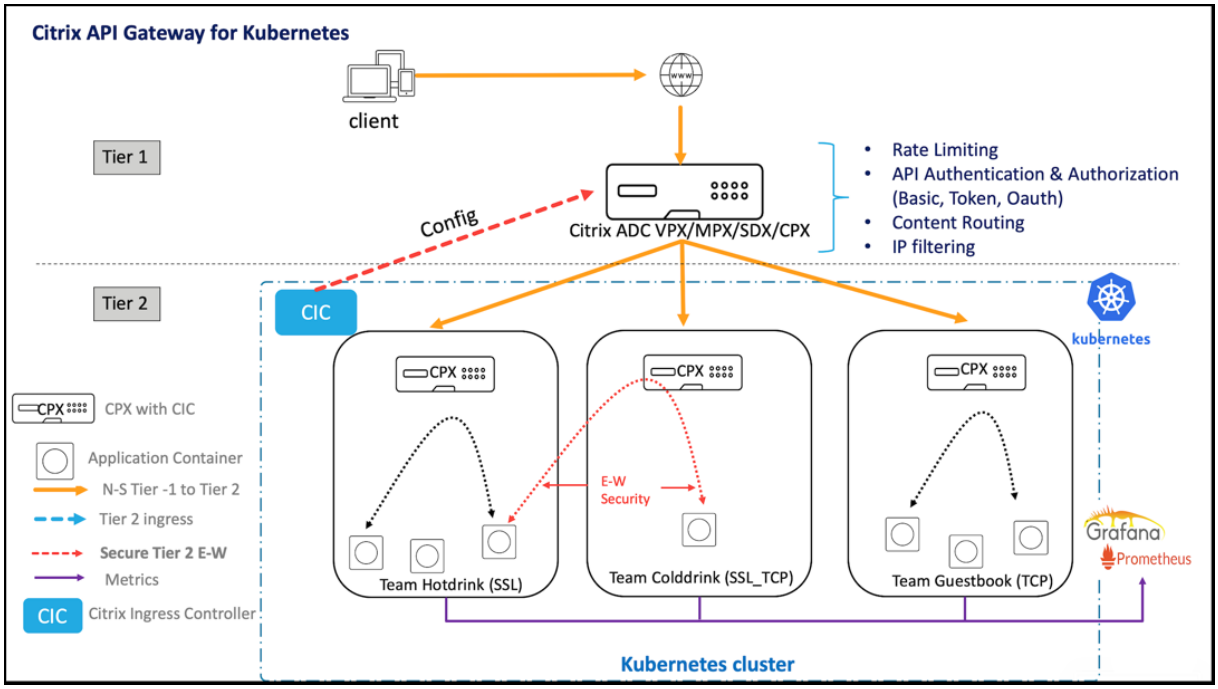
Passerelle API pour Kubernetes

August 20, 2021

Une passerelle API sert de point d'entrée unique pour vos API et garantit un accès sécurisé et fiable à plusieurs API et microservices de votre système.

Citrix fournit une passerelle API de qualité entreprise pour le trafic d'API Nord-Sud vers le cluster Kubernetes. La passerelle
API s'intègre à Kubernetes via le contrôleur d'entrée Citrix et Citrix ADC (Citrix ADC MPX, VPX ou CPX) déployé comme Ingress Gateway pour les déploiements sur site ou dans le cloud.

Le diagramme suivant présente une topologie à deux niveaux pour la passerelle API.



À l'aide de la passerelle API proposée par Citrix, vous pouvez exécuter les fonctionnalités suivantes :

- Appliquer les stratégies d'authentification
- Accès limité aux services
- Routage de contenu avancé
- Transformation flexible et complète des transactions HTTP à l'aide des stratégies de réécriture et de réponse
- Appliquer des stratégies de pare-feu d'applications

Comment fonctionne la passerelle API

La passerelle API est construite sur la passerelle d'entrée Citrix et utilise des extensions d'API Kubernetes telles que les définitions de ressources personnalisées (CRD). À l'aide des CRD, vous pouvez configurer automatiquement la passerelle ADC et API Citrix dans la même instance.

Citrix fournit les CRD suivants pour la passerelle API :

- Auth CRD
- Limite de débit CRD
- Routage de contenu CRD
- Réécriture et répondeur CRD
- WAF CRD

Principaux avantages de l'utilisation de la passerelle API

Voici les principaux avantages de la passerelle API offerte par Citrix :

- Utilise la gestion avancée du trafic et les fonctionnalités de sécurité complètes de Citrix ADC.
- Optimisez vos déploiements en consolidant plusieurs fonctions réseau en un seul composant de la passerelle d'entrée Citrix.
- Réduit la complexité opérationnelle et les coûts associés au déploiement de plusieurs composants.
- Garantit de meilleures performances pour le trafic de votre application en réduisant plusieurs sauts de déchiffrement TCP ou TLS tout en utilisant des composants distincts.
- Simplifie le déploiement et l'intégration dans vos environnements Kubernetes en utilisant directement les cartes YamLS ou les cartes de pilotage.

Déploiement de la passerelle API

Pour plus d'informations sur la configuration des fonctionnalités de passerelle API à l'aide de CRD, consultez la documentation du contrôleur d'entrée Citrix :

- Authentification
- Limitation du taux
- Routage de contenu avancé
- Réécriture et stratégies de répondeur
- Stratégies de pare-feu d'applications Web

Déployer une instance de Citrix ADC VPX sur AWS

October 5, 2021

> **Remarque**
>
> La connexion du service Citrix ADM est activée par défaut, après avoir installé ou mis à niveau Citrix ADC ou Citrix Gateway vers la version 13.0 build 61.xx et supérieure. Pour plus d'informations, voir Gouvernance des données et Citrix ADM service se connectent.

Le produit Citrix ADC VPX est une appliance virtuelle qui peut être hébergée sur une grande variété de plateformes de virtualisation et de cloud :

- Citrix Hypervisor
- VMware ESX
- Microsoft Hyper-V
- Linux KVM
- Amazon Web Services
- Microsoft Azure

- Plate-forme Google Cloud

Pour plus d'informations, consultez la fiche technique Citrix ADC VPX.

Pour plus d'informations sur le provisionnement d'une instance Citrix ADC VPX sur une appliance SDX, consultez Provisioning Citrix ADC instances.

Citrix Application Delivery Management pour Citrix ADC VPX

Le logiciel Citrix Application Delivery Management est une solution de gestion centralisée qui simplifie les opérations en offrant aux administrateurs une visibilité à l'échelle de l'entreprise et en automatisant les tâches de gestion qui doivent être exécutées sur plusieurs instances.

Vous pouvez gérer et surveiller les instances Citrix ADC VPX en plus d'autres produits de mise en réseau d'applications Citrix tels que Citrix Gateway, Citrix ADC SDX, Citrix ADC CPX et Citrix SD-WAN. Vous pouvez utiliser le logiciel Application Delivery Management pour gérer, surveiller et dépanner l'ensemble de l'infrastructure de livraison d'applications à partir d'une console unifiée unique.

Pour plus d'informations, consultez la documentation Citrix Application Delivery Management.

Matrice de prise en charge et directives d'utilisation

October 5, 2021

Ce document répertorie les différents hyperviseurs et fonctionnalités prises en charge sur une instance Citrix ADC VPX, leurs directives d'utilisation et leurs limitations connues.

Tableau 1. Instance VPX sur Citrix Hypervisor

Version Citrix Hypervisor	SysID	Modèles VPX
8.2 pris en charge à partir de 13.0, 64.x, 8.0, 7.6, 7.1	450000	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10 G, VPX 15 G, VPX 25 G, VPX 40 G

Tableau 2. Instance VPX sur le serveur VMware ESXi

Version ESX	Date de sortie d'ESX	Numéro de build ESX	Version Citrix ADC VPX	SysID	Modèles VPX
ESX 7.0 update 2a	2021/04/29	17867351	13.1-4.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESX 7.0 update 1d	2021/02/02	17551050	13.0-82.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESX 7.0 update 1c	2020/12/17	17325551	13.0-79.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX	Numéro de build ESX	Version Citrix ADC VPX	SysID	Modèles VPX
ESX 7.0 update 1b	10/06/2020	16850804	13.0-76.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 7.0b	06/23/2020	16324942	13.0-71.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 7.0 GA	04/02/2020	15843807	13.0-71.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX	Numéro de build ESX	Version Citrix ADC VPX	SysID	Modèles VPX
ESXi 6.7 P04	11/19/2020	17167734	13.0-67.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 P03	08/20/2020	16713306	13.0-67.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 P02	04/28/2020	16075168	13.0-67.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX	Numéro de build ESX	Version Citrix ADC VPX	SysID	Modèles VPX
ESXi 6.7 P01	12/05/2019	15160138	13.0-67.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 Update 3	08/20/2019	14320388	13.0-58.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 U2	04/11/2019	13006603	13.0-47.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX	Numéro de build ESX	Version Citrix ADC VPX	SysID	Modèles VPX
ESXi 6.5 GA	11/15/2016	4564106	13.0-47.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.5 U1g	3/20/2018	7967591	13.0 47.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.0 Update 3	2/24/2017	5050593	12.0-51.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX	Numéro de build ESX	Version Citrix ADC VPX	SysID	Modèles VPX
ESXi 6.0 Express Patch 11	10/5/2017	6765062	12.0-56.x et versions ultérieures	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Tableau 3. VPX sur Microsoft Hyper-V

Version Hyper-V	SysID	Modèles VPX
2012, 2012 R2, 2016, 2019	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000

Tableau 4. Instance VPX sur KVM générique

Version KVM générique	SysID	Modèles VPX
RHEL 7.4, RHEL 7.5 (à partir de Citrix ADC version 12.1 50.x), RHEL 7.6, RHEL 8.0, Ubuntu 16.04, Ubuntu 18.04, RHV 4.2	450070	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10 G, VPX 15 G. VPX 25G, VPX 40G, VPX 100G

Points à noter :

Lorsque vous utilisez les hyperviseurs KVM, tenez compte des points suivants.

- L'instance VPX est qualifiée pour les versions de version de l'Hypervisor mentionnées dans le tableau 1—4, et non pour les versions de correctifs dans une version. Toutefois, l'instance VPX devrait fonctionner de manière transparente avec les versions de correctifs d'une version prise en charge. Si ce n'est pas le cas, consignez un dossier de support pour le dépannage et le débogage.
- Avant d'utiliser RHEL 7.6, effectuez les étapes suivantes sur l'hôte KVM :

1. Modifiez /etc/default/grub et ajoutez `"kvm_intel.preemption_timer=0"` à la variable `GRUB_CMDLINE_LINUX`.
2. Régénérez le fichier grub.cfg à l'aide de la commande `"## grub2-mkconfig -o /boot/grub2/grub.cfg"`.
3. Redémarrez la machine hôte.

- Avant d'utiliser Ubuntu 18.04, effectuez les étapes suivantes sur l'hôte KVM :

1. Modifiez /etc/default/grub et ajoutez `"kvm_intel.preemption_timer=0"` à la variable `GRUB_CMDLINE_LINUX`.
2. Régénérez le fichier grub.cfg à l'aide de la commande `"## grub-mkconfig -o /boot/grub/grub.cfg "`.
3. Redémarrez la machine hôte.

Tableau 5. Instance VPX sur AWS

Version AWS	SysID	Modèles VPX
S.O.	450040	VPX 10, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX BYOL (VPX 8000, VPX 10G, VPX 15G et VPX 25G sont disponibles uniquement avec BYOL avec des types d'instance EC2 (C5, M5 et C5n)

Tableau 6. Instance VPX sur Azure

Version Azure	SysID	Modèles VPX
S.O.	450020	VPX 10, VPX 200, VPX 1000, VPX 3000, VPX BYL

Tableau 7. Matrice de fonctionnalités VPX

	VPX on XenServer		VPX on VMware ESX				VPX on Microsoft Hyper-V	VPX on generic KVM			VPX on AWS	VPX on Azure
Features	PV	SR-IOV	PV	SR-IOV	Emulated	PCI Passthrough	PV	PV	SR-IOV	PCI Passthrough		
Multi-PE Support	√	√	√	√	√	√	√	√	√	√	√	√
Clustering Support	√	*√	√	*√	√	√	√	√	*√	√	X	X
VLAN Tagging	√	√	√	√	√	√	√ ((Only on 2012R2))	√	√	√	X	X
Detecting Link Events	**X	***√	**X	***√	**X	***√	**X	**X	***√	***√	**X	**X
Interface Parameter Configuration	X	X	X	X	X	√	X	X	X	√	X	X
Static LA	**√	***√	**√	X	**√	***√	**√	**√	***√	***√	X	X
LACP	X	***√	**√	X	**√	***√	X	**√	***√	***√	X	X
Static CLAG	X	X	X	X	X	X	X	X	X	X	X	X
LACP CLAG	X	X	**√	X	**√	***√	X	**√	***√	***√	X	X
Hot-Plug	X	X	X	X	X	X	X	X	X	X	√	X

1. La prise en charge du clustering est disponible sur SRIOV pour les interfaces client et serveur et non pour le fond de panier.
2. Les événements DOWN de l'interface ne sont pas enregistrés dans les instances Citrix ADC VPX.
3. Pour LA statique, le trafic peut toujours être envoyé sur l'interface dont l'état physique est DOWN.
4. Pour LACP, le périphérique homologue connaît l'événement DOWN de l'interface basé sur le mécanisme de délai d'expiration LACP.
    - Délai d'expiration court : 3 secondes
    - Délai d'attente long : 90 secondes
5. Pour LACP, ne partagez pas les interfaces entre les machines virtuelles.
6. Pour le routage dynamique, le temps de convergence dépend du protocole de routage car les événements de liaison ne sont pas détectés.
7. La fonctionnalité Routage statique surveillé échoue si vous ne liez pas les moniteurs à des routes statiques, car l'état de l'itinéraire dépend de l'état du VLAN. L'état du VLAN dépend de l'état de la liaison.
8. La détection de défaillance partielle ne se produit pas en haute disponibilité en cas de défaillance de liaison. Une condition cérébrale divisée à haute disponibilité peut se produire en cas de défaillance de liaison.

- Lorsqu'un événement de lien (désactiver/activer, réinitialiser) est généré à partir d'une instance VPX, l'état physique du lien ne change pas. Pour LA statique, tout trafic initié par le pair est supprimé sur l'instance.
- Pour que la fonctionnalité de balisage VLAN fonctionne, procédez comme suit :

Sur VMware ESX, définissez l'ID VLAN du groupe de ports sur 1 à 4095 sur le vSwitch du serveur VMware ESX. Pour plus d'informations sur la définition d'un ID VLAN sur le vSwitch du serveur VMware ESX, consultez Solutions VLAN VMware ESX Server 3 802.1Q.

Tableau 8. Navigateurs pris en charge

Système d'exploitation	Navigateur et versions
Windows 7	Internet Explorer - 8, 9, 10 et 11 ; Mozilla Firefox 3.6.25 et versions ultérieures ; Google Chrome - 15 et versions ultérieures
Windows 64 bits	Internet Explorer - 8, 9 ; Google Chrome - 15 et versions ultérieures
MAC	Mozilla Firefox - 12 et versions ultérieures ; Safari - 5.1.3 ; Google Chrome - 15 et versions ultérieures

Directives d'utilisation

Suivez ces instructions d'utilisation :

Consultez la section **Considérations relatives au processeur VMware ESXi** dans le document Performance Best Practices for VMware vSphere 6.5. Voici un extrait :

- Il n'est pas recommandé que les machines virtuelles dont la demande en CPU/mémoire est élevée se trouvent sur un hôte/un cluster surengagé.
- Dans la plupart des environnements, ESXi permet des niveaux significatifs de surengagement du processeur sans affecter les performances des machines virtuelles. Sur un hôte, vous pouvez exécuter plus de processeurs virtuels que le nombre total de cœurs de processeur physiques de cet hôte.
- Si un hôte ESXi devient saturé en processeur, c'est-à-dire que les machines virtuelles et les autres charges sur l'hôte exigent toutes les ressources CPU dont dispose l'hôte, les charges de travail sensibles à la latence risquent de ne pas fonctionner correctement. Dans ce cas, vous pouvez réduire la charge du processeur, par exemple en mettant hors tension certaines machines virtuelles ou en les migrant vers un autre hôte (ou en autorisant DRS à les migrer automatiquement).

- Citrix recommande la dernière version de compatibilité matérielle pour utiliser les derniers jeux de fonctionnalités de l'hyperviseur ESXi pour la machine virtuelle. Pour plus d'informations sur la compatibilité matérielle et la version ESXi, consultez la documentation VMware.
- Le Citrix ADC VPX est un dispositif virtuel hautes performances sensible à la latence. Pour fournir les performances attendues, le dispositif nécessite la réservation du processeur virtuel, la réservation de la mémoire et l'épinglage du processeur virtuel sur l'hôte. En outre, l'hyper thread doit être désactivé sur l'hôte. Si l'hôte ne répond pas à ces exigences, des problèmes tels que basculement haute disponibilité, pic de processeur dans l'instance VPX, lenteur dans l'accès à l'interface de ligne de commande VPX, plantage du démon pit boss, pertes de paquets et faible débit se produisent.

Un Hypervisor est considéré comme surprovisionné si l'une des deux conditions suivantes est remplie :

- Le nombre total de cœurs virtuels (vCPU) provisionnés sur l'hôte est supérieur au nombre total de cœurs physiques (PCPU).
- Le nombre total de machines virtuelles provisionnées consomme plus de vCPU que le nombre total de PCUs.

  Si une instance est surprovisionnée, il se peut que l'hyperviseur ne garantisse pas les ressources réservées (telles que le processeur, la mémoire et autres) pour l'instance en raison des surcharges de planification de l'hyperviseur, des bogues ou des limitations avec l'hyperviseur. Ce comportement peut entraîner un manque de ressources CPU pour Citrix ADC et peut entraîner les problèmes mentionnés au premier point sous **Directives d'utilisation**. En tant qu'administrateurs, il est recommandé de réduire la location de l'hôte afin que le nombre total de vCPU provisionnés sur l'hôte soit inférieur ou égal au nombre total de PCUs.

  Exemple

  Pour l'hyperviseur ESX, si le `%RDY%` paramètre d'un vCPU VPX est supérieur à 0 dans la sortie de la `esxtop` commande, l'hôte ESX est dit avoir des surcharges de planification, ce qui peut entraîner des problèmes de latence pour l'instance VPX.

  Dans ce cas, réduisez la location sur l'hôte afin qu'elle `%RDY%` revienne toujours à 0. Vous pouvez également contacter le fournisseur de l'hyperviseur pour trier la raison du non-respect de la réservation de ressources effectuée.

- L'ajout à chaud n'est pris en charge que pour les interfaces PV et SRIOV avec Citrix ADC sur AWS. Les instances VPX avec interfaces ENA ne prennent pas en charge le branchement à chaud, et le comportement des instances peut être imprévisible en cas de tentative de connexion à chaud.
- La suppression à chaud via la console Web AWS ou l'interface de ligne de commande AWS n'est pas prise en charge avec les interfaces PV, SRIOV et ENA pour Citrix ADC. Le comportement des instances peut être imprévisible si la suppression à chaud est tentée.

Commandes pour contrôler l'utilisation du processeur du moteur de paquets

Vous pouvez utiliser deux commandes (`set ns vpxparam` et `show ns vpxparam`) pour contrôler le comportement d'utilisation du processeur du moteur de paquets (hors gestion) des instances VPX dans les environnements d'hyperviseur et de cloud :

- `set ns vpxparam [-cpuyield (YES | NO | DEFAULT)] [-masterclockcpu1 (YES | NO)]`

  Autoriser chaque machine virtuelle à utiliser des ressources CPU qui ont été allouées à une autre machine virtuelle mais qui ne sont pas utilisées.

  `Set ns vpxparam` paramètres :

  -cpuyield : libère ou ne libère pas des ressources CPU allouées mais inutilisées.

  - **OUI** : autorise l'utilisation des ressources CPU allouées mais inutilisées par une autre machine virtuelle.
  - **NON** : réservez toutes les ressources CPU pour la machine virtuelle à laquelle elles ont été allouées. Cette option affiche un pourcentage plus élevé dans les environnements d'hyperviseur et de cloud pour l'utilisation du processeur VPX.
  - **DEFAULT** : Non.

  > **Remarque**
  >
  > Sur toutes les plates-formes Citrix ADC VPX, l'utilisation du processeur virtuel sur le système hôte est de 100 %. Tapez la commande `set ns vpxparam -cpuyield YES` pour remplacer cette utilisation.

  Si vous souhaitez définir les nœuds du cluster sur « rendement », vous devez effectuer les configurations supplémentaires suivantes sur CCO :

  - Si un cluster est formé, tous les nœuds présentent « Yield=Default ».
  - Si un cluster est formé à l'aide des nœuds déjà définis sur « Yield=YES », les nœuds sont ajoutés au cluster en utilisant le rendement « DEFAULT ».

  > Remarque :
  >
  > Si vous souhaitez définir les nœuds du cluster sur « Yield=YES », vous pouvez effectuer des configurations appropriées uniquement après la formation du cluster, mais pas avant la formation du cluster.

  -masterclockcpu1 : Vous pouvez déplacer la source d'horloge principale de CPU0 (CPU de gestion) vers CPU1. Ce paramètre a les options suivantes :

  - **OUI** : Autorisez la machine virtuelle à déplacer la source d'horloge principale de CPU0 vers CPU1.

  - **NON** : VM utilise CPU0 pour la source d'horloge principale. Par défaut, CPU0 est la principale source d'horloge.

- `show ns vpxparam`

  Affichez les `vpxparam` paramètres actuels.

Autres références

- Pour les produits Citrix Ready, visitez Citrix Ready Marketplace.
- Pour obtenir le support produit Citrix Ready, consultez la page FAQ.
- Pour les versions matérielles VMware ESX, consultez Mise à niveau de VMware Tools.

Optimisation des performances Citrix ADC VPX sur VMware ESX, Linux KVM et Citrix Hypervisors

October 5, 2021

Les performances de Citrix ADC VPX varient considérablement en fonction de l'hyperviseur, des ressources système allouées et des configurations de l'hôte. Pour atteindre les performances souhaitées, suivez d'abord les recommandations de la fiche technique VPX, puis optimisez-la davantage en utilisant les meilleures pratiques fournies dans ce document.

Instance Citrix ADC VPX sur les hyperviseurs VMware ESX

Cette section contient des détails sur les options et paramètres configurables, ainsi que d'autres suggestions qui vous aident à optimiser les performances de l'instance Citrix ADC VPX sur les hyperviseurs VMware ESX.

- Configuration recommandée sur les hôtes ESX
- Citrix ADC VPX avec interfaces réseau E1000
- Citrix ADC VPX avec interfaces réseau VMXNET3
- Citrix ADC VPX avec interfaces réseau SR-IOV et PCI passthrough

Configuration recommandée sur les hôtes ESX

Pour obtenir des performances élevées pour VPX avec les interfaces réseau E1000, VMXNET3, SR-IOV et PCI passthrough, suivez ces recommandations :

- Le nombre total de processeurs virtuels (vCPU) provisionnés sur l'hôte ESX doit être inférieur ou égal au nombre total de processeurs physiques (PCPU) sur l'hôte ESX.

- L'affinité NUMA (Non-Uniform Memory Access) et l'affinité CPU doivent être définies pour l'hôte ESX pour obtenir de bons résultats.

  — Pour trouver l'affinité NUMA d'une Vmnic, connectez-vous à l'hôte localement ou à distance, et tapez :

```
#vsish -e get /net/pNics/vmnic7/properties | grep NUMA
Device NUMA Node: 0
<!--NeedCopy-->
```

  - Pour définir l'affinité NUMA et vCPU pour une machine virtuelle, consultez la documentation VMware.

Citrix ADC VPX avec interfaces réseau E1000

Effectuez les paramètres suivants sur l'hôte VMware ESX :

- Sur l'hôte VMware ESX, créez deux cartes réseau virtuelles à partir d'un commutateur pNIC. Plusieurs vNIC créent plusieurs threads Rx dans l'hôte ESX. Cela augmente le débit Rx de l'interface pNIC.
- Activez les VLAN au niveau du groupe de ports vSwitch pour chaque carte réseau virtuelle que vous avez créée.
- Pour augmenter le débit de transmission vNIC (Tx), utilisez un thread Tx distinct dans l'hôte ESX par vNIC. Utilisez la commande ESX suivante :
  - Pour ESX version 5.5 :

```
esxcli system settings advanced set -o /Net/NetTxWorldlet -
   i
<!--NeedCopy-->
```

  - Pour ESX version 6.0 et ultérieure :

```
esxcli system settings advanced set -o /Net/NetVMTxType -i 1
<!--NeedCopy-->
```

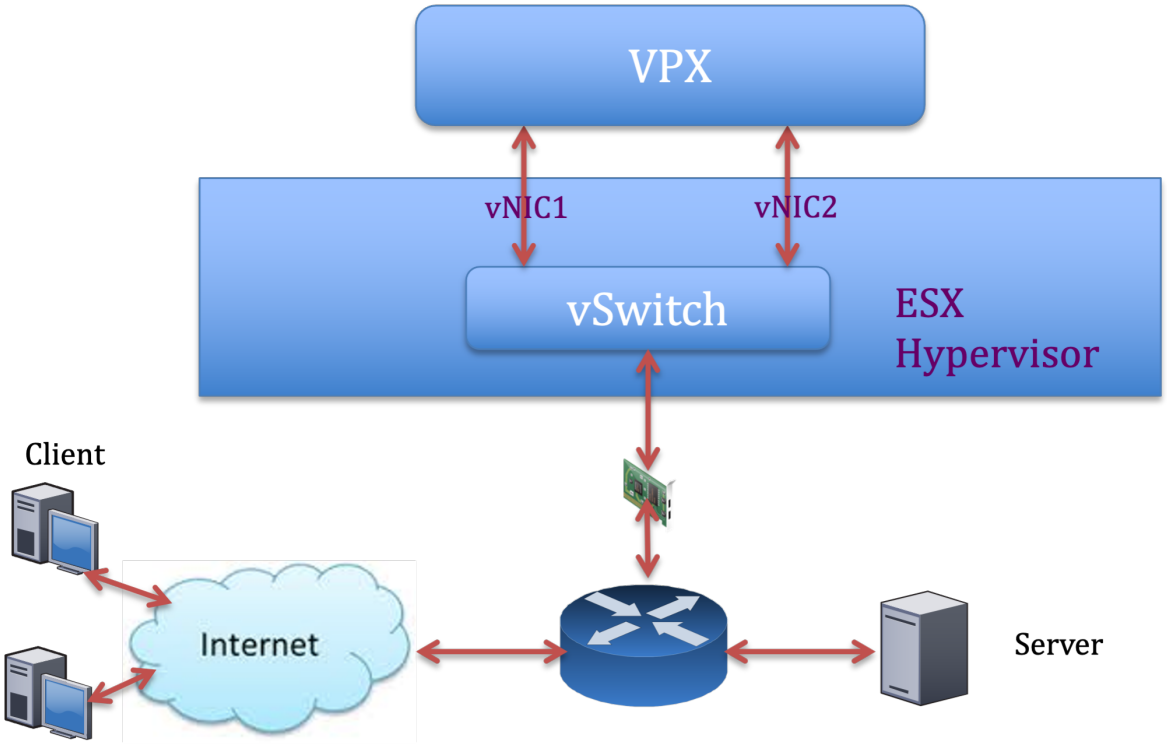
- Pour augmenter encore le débit de la carte réseau vNIC Tx, utilisez un thread d'achèvement Tx et une file d'attente de threads Rx par périphérique (NIC) distincts. Utilisez la commande ESX suivante :

```
esxcli system settings advanced set -o /Net/
   NetNetqRxQueueFeatPairEnable -i 0
<!--NeedCopy-->
```


> Remarque :
>
> Assurez-vous de redémarrer l'hôte VMware ESX pour appliquer les paramètres mis à jour.

Deux cartes réseau virtuelles par déploiement de PNIC

Voici un exemple de commande de topologie et de configuration pour le modèle de déploiement de **deux cartes réseau virtuelles par pNIC** qui offre de meilleures performances réseau.



Exemple de configuration Citrix ADC VPX :

Pour réaliser le déploiement indiqué dans l'exemple de topologie précédent, effectuez la configuration suivante sur l'instance Citrix ADC VPX :

- Côté client, liez le SNIP (1.1.1.2) à l'interface réseau 1/1 et activez le mode de balise VLAN.

```
1  bind vlan 2 -ifnum 1/1  - tagged
2  bind vlan 2 -IPAddress 1.1.1.2 255.255.255.0
3  <!--NeedCopy-->
```

- Côté serveur, liez le SNIP (2.2.2.2) à l'interface réseau 1/1 et activez le mode de balise VLAN.

```
1  bind vlan 3 -ifnum 1/2  - tagged
2  bind vlan 3 -IPAddress 2.2.2.2 255.255.255.0
3  <!--NeedCopy-->
```


- Ajoutez un serveur virtuel HTTP (1.1.1.100) et liez-le à un service (2.2.2.100).

```
add lb vserver v1 HTTP 1.1.1.100 80 -persistenceType NONE -
   Listenpolicy None -cltTimeout 180
add service s1 2.2.2.100 HTTP 80 -gslb NONE -maxClient 0 -maxReq
   0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
   180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
bind lb vserver v1 s1
<!--NeedCopy-->
```

> Remarque :
>
> Assurez-vous d'inclure les deux entrées suivantes dans la table de routage :
>
> - Sous-réseau 1.1.1.0/24 avec passerelle pointant vers SNIP 1.1.1.2
> - Sous-réseau 2.2.2.0/24 avec passerelle pointant vers SNIP 2.2.2.2

Citrix ADC VPX avec interfaces réseau VMXNET3

Pour obtenir des performances élevées pour VPX avec les interfaces réseau VMXNET3, effectuez les paramètres suivants sur l'hôte VMware ESX :

- Créez deux vNIC à partir d'un commutateur virtuel PNIC. Plusieurs vNIC créent plusieurs threads Rx dans l'hôte ESX. Cela augmente le débit Rx de l'interface pNIC.
- Activez les VLAN au niveau du groupe de ports vSwitch pour chaque carte réseau virtuelle que vous avez créée.
- Pour augmenter le débit de transmission vNIC (Tx), utilisez un thread Tx distinct dans l'hôte ESX par vNIC. Utilisez les commandes ESX suivantes :
  - Pour ESX version 5.5 :

```
esxcli system settings advanced set  -o /Net/NetTxWorldlet  -i
<!--NeedCopy-->
```

  - Pour ESX version 6.0 et ultérieure :

```
 esxcli system settings advanced set -o /Net/NetVMTxType  -i 1
 <!--NeedCopy-->
```

Sur l'hôte VMware ESX, effectuez la configuration suivante :

- Sur l'hôte VMware ESX, créez deux cartes réseau virtuelles à partir d'un vSwitch PNIC. Plusieurs vNIC créent plusieurs threads Tx et Rx dans l'hôte ESX. Cela augmente le débit Tx et Rx de l'interface pNIC.
- Activez les VLAN au niveau du groupe de ports vSwitch pour chaque carte réseau virtuelle que vous avez créée.

- Pour augmenter le débit Tx d'une vNIC, utilisez un thread d'achèvement Tx et une file d'attente de threads Rx par périphérique (NIC) distincts. Utilisez la commande suivante :

```
esxcli system settings advanced set -o /Net/
   NetNetqRxQueueFeatPairEnable -i 0
<!--NeedCopy-->
```

- Configurez une machine virtuelle pour qu'elle utilise un thread de transmission par vNIC, en ajoutant le paramètre suivant à la configuration de la machine virtuelle :

```
ethernetX.ctxPerDev = "1"
<!--NeedCopy-->
```

Pour plus d'informations, consultez la section Meilleures pratiques pour le réglage des performances des charges de travail Telco et NFV
dans vSphere

> Remarque :
>
> Assurez-vous de redémarrer l'hôte VMware ESX pour appliquer les paramètres mis à jour.

Vous pouvez configurer VMXNET3 en tant que **deux cartes réseau virtuelles par déploiement PNIC** . Pour plus d'informations, consultez la section Deux cartes réseau virtuelles par déploiement de pNIC.

Citrix ADC VPX avec interfaces réseau SR-IOV et PCI passthrough

Pour obtenir des performances élevées pour VPX avec des interfaces réseau SR-IOV et PCI passthrough, reportez-vous à la section Configuration recommandée sur les hôtes ESX.

Instance Citrix ADC VPX sur plate-forme Linux-KVM

Cette section contient des détails sur les options et paramètres configurables, ainsi que d'autres suggestions qui vous aident à obtenir des performances optimales de l'instance Citrix ADC VPX sur la plate-forme Linux-KVM.

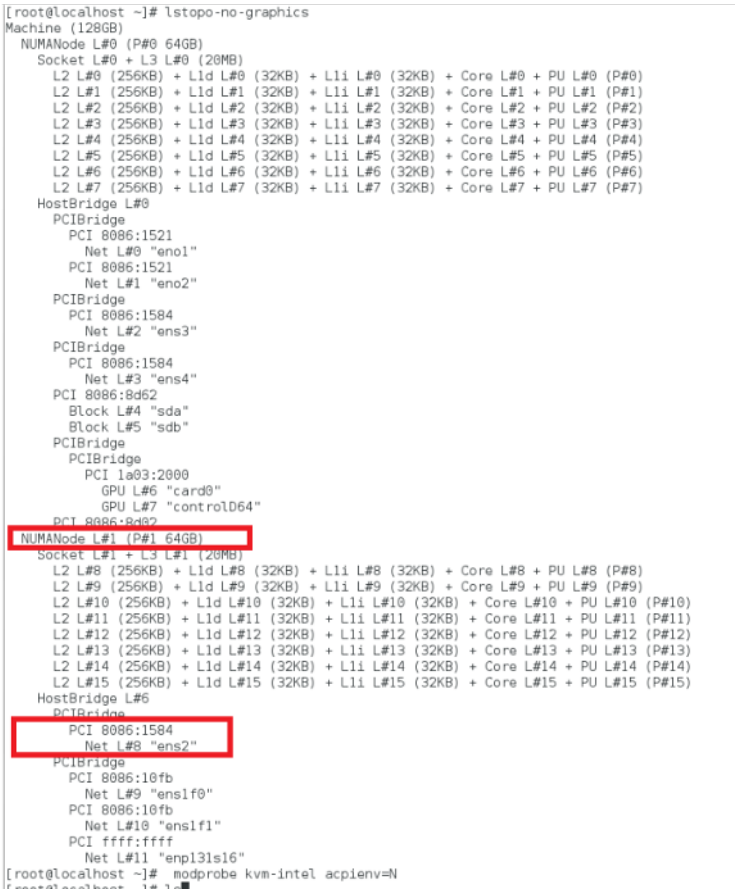
- Paramètres de performance pour KVM
- Citrix ADC VPX avec interfaces réseau PV
- Citrix ADC VPX avec interfaces réseau relais SR-IOV et Fortville PCIe

Paramètres de performance pour KVM

Effectuez les paramètres suivants sur l'hôte KVM :

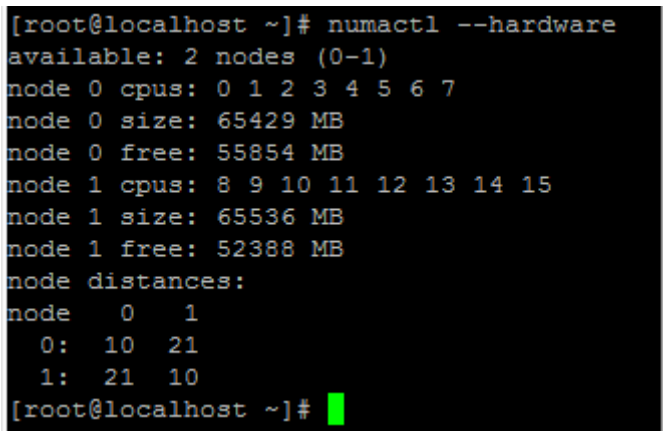
Recherchez le domaine NUMA de la carte réseau à l'aide de la `lstopo` commande :

Assurez-vous que la mémoire du VPX et du processeur est épinglée au même emplacement. Dans la sortie suivante, la carte réseau 10G « ens2” est liée au domaine NUMA #1.



Allouez la mémoire VPX du domaine NUMA.

La `numactl` commande indique le domaine NUMA à partir duquel la mémoire est allouée. Dans la sortie suivante, environ 10 Go de RAM sont alloués à partir du nœud NUMA #0.



Pour modifier le mappage des nœuds NUMA, procédez comme suit.

1. Modifiez le .xml du VPX sur l’hôte.


```
/etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

2. Ajoutez la balise suivante :

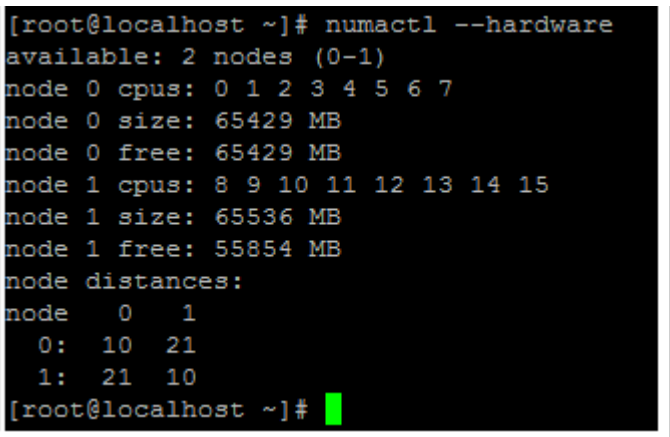
```
<numatune>
<memory mode="strict" nodeset="1"/>   This is the NUMA domain
   name
</numatune>
<!--NeedCopy-->
```

3. Arrêtez le VPX.
4. Exécutez la commande suivante :

```
virsh define /etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

   Cette commande met à jour les informations de configuration de la machine virtuelle avec les mappages de nœuds NUMA.

5. Mettez le VPX sous tension. Vérifiez ensuite la sortie de la `numactl -hardware` commande sur l'hôte pour voir les allocations de mémoire mises à jour pour le VPX.



Épinglez les vCPU de VPX aux cœurs physiques.

- Pour afficher les mappages vCPU vers PCPU d'un VPX, tapez la commande suivante

```
virsh vcpupin <VPX name>
<!--NeedCopy-->
```



```
root@localhost qemu]#  virsh vcpupin NS-VPX-DVR
CPU: CPU Affinity
----------------------------------
  0: 8
  1: 9
  2: 10
  3: 11
```

Les vCPU 0—4 sont mappés sur les cœurs physiques 8 à 11.

- Pour afficher l'utilisation actuelle du PCPU, tapez la commande suivante :

```
mpstat -P ALL 5
<!--NeedCopy-->
```

```
[root@localhost qemu]# mpstat -P ALL 5
Linux 3.10.0-123.el7.x86_64 (localhost.localdomain)     05/17/2016      _x86_64_        (16 CPU)

02:26:20 PM  CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
02:26:25 PM  all    0.24    0.00    1.67    0.00    0.00    0.00    0.00   17.32    0.00   80.78
02:26:25 PM    0    0.20    0.00    1.00    0.00    0.00    0.00    0.00    0.00    0.00   98.80
02:26:25 PM    1    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    2    0.20    0.00    0.40    0.00    0.00    0.00    0.00    0.00    0.00   99.40
02:26:25 PM    3    0.00    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.80
02:26:25 PM    4    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    5    0.60    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.20
02:26:25 PM    6    0.40    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    7    1.62    0.00    1.42    0.00    0.00    0.00    0.00    0.00    0.00   96.96
02:26:25 PM    8    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM    9    0.00    0.00    7.60    0.00    0.00    0.00    0.00   92.40    0.00    0.00
02:26:25 PM   10    0.20    0.00    7.00    0.00    0.00    0.00    0.00   92.80    0.00    0.00
02:26:25 PM   11    0.00    0.00    8.60    0.00    0.00    0.00    0.00   91.40    0.00    0.00
02:26:25 PM   12    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   13    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   14    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   15    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
```

Dans cette sortie, 8 correspond au processeur de gestion et 9 à 11 aux moteurs de paquets.

- Pour changer le vCPU en épinglage PCPU, il existe deux options.
  - Modifiez-le au moment de l'exécution après le démarrage du VPX à l'aide de la commande suivante :

```
virsh vcpupin <VPX name> <vCPU id>  <pCPU number>
virsh vcpupin NetScaler-VPX-XML 0 8
virsh vcpupin NetScaler-VPX-XML 1 9
virsh vcpupin NetScaler-VPX-XML 2 10
virsh vcpupin NetScaler-VPX-XML 3 11
<!--NeedCopy-->
```

  - Pour apporter des modifications statiques au VPX, modifiez le `.xml` fichier comme précédemment avec les balises suivantes :

    1. Modifiez le fichier .xml du VPX sur l'hôte


```
/etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

2. Ajoutez la balise suivante :

```
<vcpu placement='static' cpuset='8-11'>4</vcpu>
    <cputune>
        <vcpupin vcpu='0' cpuset='8'/>
        <vcpupin vcpu='1' cpuset='9'/>
        <vcpupin vcpu='2' cpuset='10'/>
        <vcpupin vcpu='3' cpuset='11'/>
    </cputune>
<!--NeedCopy-->
```

3. Arrêtez le VPX.
4. Mettez à jour les informations de configuration de la machine virtuelle avec les mappages de nœuds NUMA à l'aide de la commande suivante :

```
virsh define /etc/libvirt/qemu/ <VPX_name>.xml
<!--NeedCopy-->
```

5. Mettez le VPX sous tension. Vérifiez ensuite la sortie de la `virsh vcpupin <VPX name>` commande sur l'hôte pour voir l'épinglage du processeur mis à jour.

Éliminez les frais généraux d'interruption de l'hôte.

- Détectez VM_EXITS à l'aide de la `kvm_stat` commande.

  Au niveau de l'hyperviseur, les interruptions de l'hôte sont mappées sur les mêmes processeurs sur lesquels les vCPU du VPX sont épinglés. Cela peut entraîner le retrait périodique des processeurs virtuels sur le VPX.

  Pour trouver les sorties de machine virtuelle effectuées par les machines virtuelles exécutant l'hôte, utilisez la `kvm_stat` commande.

```
[root@localhost ~]# kvm_stat -1  | grep EXTERNAL
kvm_exit(EXTERNAL_INTERRUPT)  1728349 27738
[root@localhost ~]#
<!--NeedCopy-->
```

  Une valeur supérieure de l'ordre de 1+M indique un problème.

  Si une seule machine virtuelle est présente, la valeur attendue est comprise entre 30 et 100 K. Tout ce qui dépasse peut indiquer qu'un ou plusieurs vecteurs d'interruption d'hôte sont mappés sur le même processeur.

- Détectez les interruptions de l'hôte et migrez les interruptions de l'hôte.

  Lorsque vous exécutez la `concatenate` commande pour le fichier « /proc/interrupts », elle affiche tous les mappages d'interruption de l'hôte. Si un ou plusieurs IRQ actifs sont mappés sur le même PCPU, le compteur correspondant est incrémenté.

  Déplacez toutes les interruptions qui se chevauchent avec les processeurs Citrix ADC VPX vers des processeurs inutilisés :

```
1  echo 0000000f > /proc/irq/55/smp_affinity
2  0000000f - - > it is a bitmap, LSBs indicates that IRQ 55 can
      only be scheduled on pCPUs 0 - 3
3  <!--NeedCopy-->
```

- Désactivez la balance IRQ.

  Désactivez le démon d'équilibrage de l'IRQ, de sorte qu'aucune replanification ne se produise à la volée.

```
1  service irqbalance stop
2  service irqbalance show - To check the status
3  service irqbalance start - Enable if needed
4  <!--NeedCopy-->
```

  Assurez-vous d'exécuter la commande `kvm_stat` pour vous assurer qu'il n'y a pas beaucoup de compteurs.

Citrix ADC VPX avec interfaces réseau PV

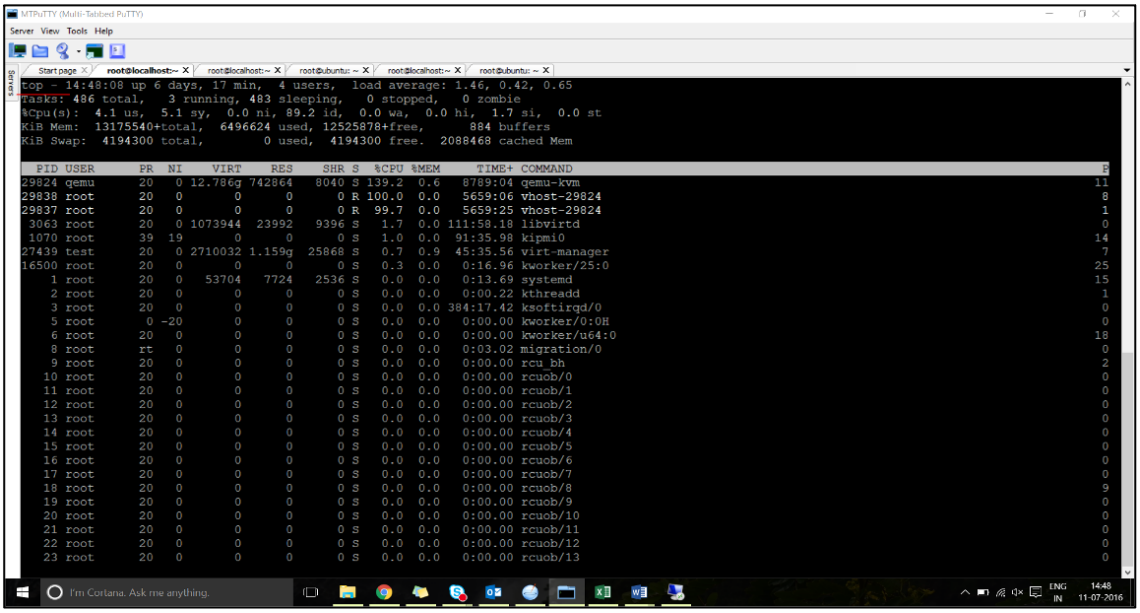
Vous pouvez configurer des interfaces réseau de para-virtualisation (PV), SR-IOV et PCIe passthrough en tant que déploiement de **deux cartes réseau virtuelles par pNIC** . Pour plus d'informations, consultez la section Deux cartes réseau virtuelles par déploiement de pNIC.

Pour des performances optimales des interfaces PV (virtio), procédez comme suit :

- Identifiez le domaine NUMA auquel le slot/carte d'interface réseau PCIe est lié.
- La mémoire et le processeur virtuel du VPX doivent être épinglés au même domaine NUMA.
- Le thread Vhost doit être lié aux processeurs du même domaine NUMA.

Liez les threads de l'hôte virtuel aux processeurs correspondants :

1. Une fois le trafic démarré, exécutez la `top` commande sur l'hôte.



2. Identifiez l'affinité du processus hôte virtuel (nommé sous le nom `vhost-<pid-of-qemu>`).
3. Liez les processus vHost aux cœurs physiques du domaine NUMA identifié précédemment à l'aide de la commande suivante :

```
taskset -pc <core-id> <process-id>
<!--NeedCopy-->
```

Exemple :

```
taskset -pc 12 29838
<!--NeedCopy-->
```

4. Les cœurs de processeur correspondant au domaine NUMA peuvent être identifiés à l'aide de la commande suivante :

```
[root@localhost ~]# virsh capabilities | grep cpu
<cpu>
    </cpu>
        <cpus num='8'>
            <cpu id='0' socket_id='0' core_id='0' siblings='0'/>
            <cpu id='1' socket_id='0' core_id='1' siblings='1'/>
            <cpu id='2' socket_id='0' core_id='2' siblings='2'/>
            <cpu id='3' socket_id='0' core_id='3' siblings='3'/>
            <cpu id='4' socket_id='0' core_id='4' siblings='4'/>
            <cpu id='5' socket_id='0' core_id='5' siblings='5'/>
            <cpu id='6' socket_id='0' core_id='6' siblings='6'/>
            <cpu id='7' socket_id='0' core_id='7' siblings='7'/>
        </cpus>
```



```
14
15          <cpus num='8'>
16          <cpu id='8' socket_id='1' core_id='0' siblings='8'/>
17          <cpu id='9' socket_id='1' core_id='1' siblings='9'/>
18          <cpu id='10' socket_id='1' core_id='2' siblings='10'/>
19          <cpu id='11' socket_id='1' core_id='3' siblings='11'/>
20          <cpu id='12' socket_id='1' core_id='4' siblings='12'/>
21          <cpu id='13' socket_id='1' core_id='5' siblings='13'/>
22          <cpu id='14' socket_id='1' core_id='6' siblings='14'/>
23          <cpu id='15' socket_id='1' core_id='7' siblings='15'/>
24          </cpus>
25
26      <cpuselection/>
27      <cpuselection/>
28
29  <!--NeedCopy-->
```

Liez le processus QEMU au cœur physique correspondant :

1. Identifiez les cœurs physiques sur lesquels le processus QEMU est exécuté. Pour plus d'informations, reportez-vous à la sortie précédente.
2. Liez le processus QEMU aux mêmes cœurs physiques auxquels vous liez les vCPU, à l'aide de la commande suivante :

```
1 taskset -pc 8-11 29824
2 <!--NeedCopy-->
```

Citrix ADC VPX avec interfaces réseau relais SR-IOV et Fortville PCIe

Pour des performances optimales des interfaces réseau relais SR-IOV et Fortville PCIe, procédez comme suit :

- Identifiez le domaine NUMA auquel le slot/carte d'interface réseau PCIe est lié.
- La mémoire et le processeur virtuel du VPX doivent être épinglés au même domaine NUMA.

Exemple de fichier XML VPX pour vCPU et épinglage de mémoire pour Linux KVM :

```
1     <domain type='kvm'>
2         <name>NetScaler-VPX</name>
3         <uuid>138f7782-1cd3-484b-8b6d-7604f35b14f4</uuid>
4         <memory unit='KiB'>8097152</memory>
5         <currentMemory unit='KiB'>8097152</currentMemory>
6         <vcpu placement='static'>4</vcpu>
7
```



```
8       <cputune>
9           <vcpupin vcpu='0' cpuset='8'/>
10          <vcpupin vcpu='1' cpuset='9'/>
11          <vcpupin vcpu='2' cpuset='10'/>
12          <vcpupin vcpu='3' cpuset='11'/>
13      </cputune>
14
15      <numatune>
16      <memory mode='strict' nodeset='1'/>
17      </numatune>
18
19      </domain>
20  <!--NeedCopy-->
```

Instance Citrix ADC VPX sur Citrix Hypervisors

Cette section contient des détails sur les options et paramètres configurables, ainsi que d'autres suggestions qui vous aident à obtenir des performances optimales de l'instance Citrix ADC VPX sur Citrix Hypervisors.

- Paramètres de performance pour Citrix Hypervisors
- Citrix ADC VPX avec interfaces réseau SR-IOV
- Citrix ADC VPX avec interfaces para-virtualisées

Paramètres de performance pour Citrix Hypervisors

Recherchez le domaine NUMA de la carte réseau à l'aide de la commande « xl » :

```
1  xl info -n
2  <!--NeedCopy-->
```

Épinglez les vCPU de VPX aux cœurs physiques.

```
1  xl vcpu-pin <Netsclaer VM Name>  <vCPU id>  <physical CPU id>
2  <!--NeedCopy-->
```

Vérifiez la liaison des vCPU.

```
1  xl vcpu-list
2  <!--NeedCopy-->
```

Allouez plus de 8 processeurs virtuels aux machines virtuelles Citrix ADC.

Pour configurer plus de 8 processeurs virtuels, exécutez les commandes suivantes à partir de la console Citrix Hypervisor :


```
xe vm-param-set uuid=your_vms_uuid VCPUs-max=16
xe vm-param-set uuid=your_vms_uuid VCPUs-at-startup=16
<!--NeedCopy-->
```

Citrix ADC VPX avec interfaces réseau SR-IOV

Pour des performances optimales des interfaces réseau SR-IOV, procédez comme suit :

- Identifiez le domaine NUMA auquel l'emplacement PCIe ou la carte réseau est lié.
- Épinglez la mémoire et le processeur virtuel du VPX au même domaine NUMA.
- Liez le vCPU Domain-0 au processeur restant.

Citrix ADC VPX avec interfaces para-virtualisées

Pour des performances optimales, deux cartes réseau virtuelles par PNIC et une configuration vNIC par pNIC sont recommandées, comme dans d'autres environnements PV.

Pour obtenir des performances optimales des interfaces para-virtualisées (netfront), procédez comme suit :

- Identifiez le domaine NUMA auquel l'emplacement PCIe ou la carte réseau est lié.
- Épinglez la mémoire et le processeur virtuel du VPX au même domaine NUMA.
- Liez le vCPU Domain-0 au processeur restant du même domaine NUMA.
- Épinglez les threads Rx/Tx hôtes de vNIC aux vCPU du domaine 0.

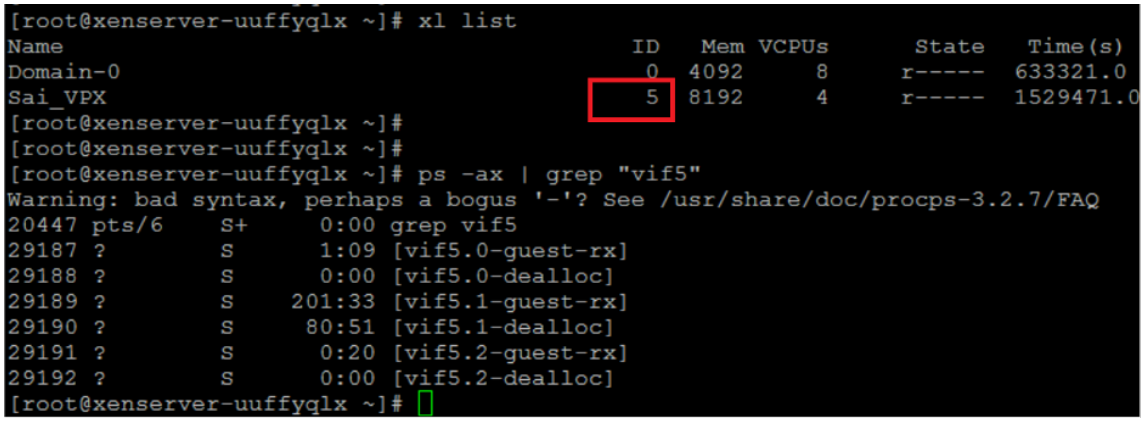
Épinglez les threads hôtes aux vCPU Domain-0 :

1. Recherchez l'ID Xen du VPX à l'aide de la `xl list` commande sur le shell hôte Citrix Hypervisor.
2. Identifiez les threads hôtes à l'aide de la commande suivante :

   ```
   ps -ax | grep vif <Xen-ID>
   <!--NeedCopy-->
   ```

   Dans l'exemple suivant, ces valeurs indiquent :

   - **vif5.0** - Les threads de la première interface allouée à VPX dans XenCenter (interface de gestion).
   - **vif5.1** - Les threads de la deuxième interface affectée à VPX et ainsi de suite.



3. Épinglez les threads aux vCPU du domaine 0 à l'aide de la commande suivante :

```
taskset  - pc <core-id> <process-id>
<!--NeedCopy-->
```

Exemple :

```
taskset -pc 1 29189
<!--NeedCopy-->
```

Appliquez les configurations Citrix ADC VPX au premier démarrage de l'appliance Citrix ADC dans le cloud

October 5, 2021

Vous pouvez appliquer les configurations Citrix ADC VPX lors du premier démarrage de l'appliance Citrix ADC dans un environnement cloud. Cette étape est abordée comme étape de **pré-démarrage** dans ce document. Par conséquent, dans certains cas, comme les licences groupées ADC, une instance VPX spécifique est mise en place en beaucoup moins de temps. Cette fonctionnalité est disponible dans Microsoft Azure, Google Cloud Platform et AWS Clouds.

Qu'est-ce que les données utilisateur

Lorsque vous provisionnez une instance VPX dans un environnement cloud, vous avez la possibilité de transmettre des données utilisateur à l'instance. Les données utilisateur vous permettent d'effectuer des tâches de configuration automatisées courantes, de personnaliser les comportements de démarrage des instances et d'exécuter des scripts après le démarrage de l'instance. Au premier démarrage, l'instance Citrix ADC VPX effectue les tâches suivantes :

- Lit les données utilisateur.

- Interprête la configuration fournie dans les données utilisateur.
- Applique la configuration nouvellement ajoutée au démarrage.

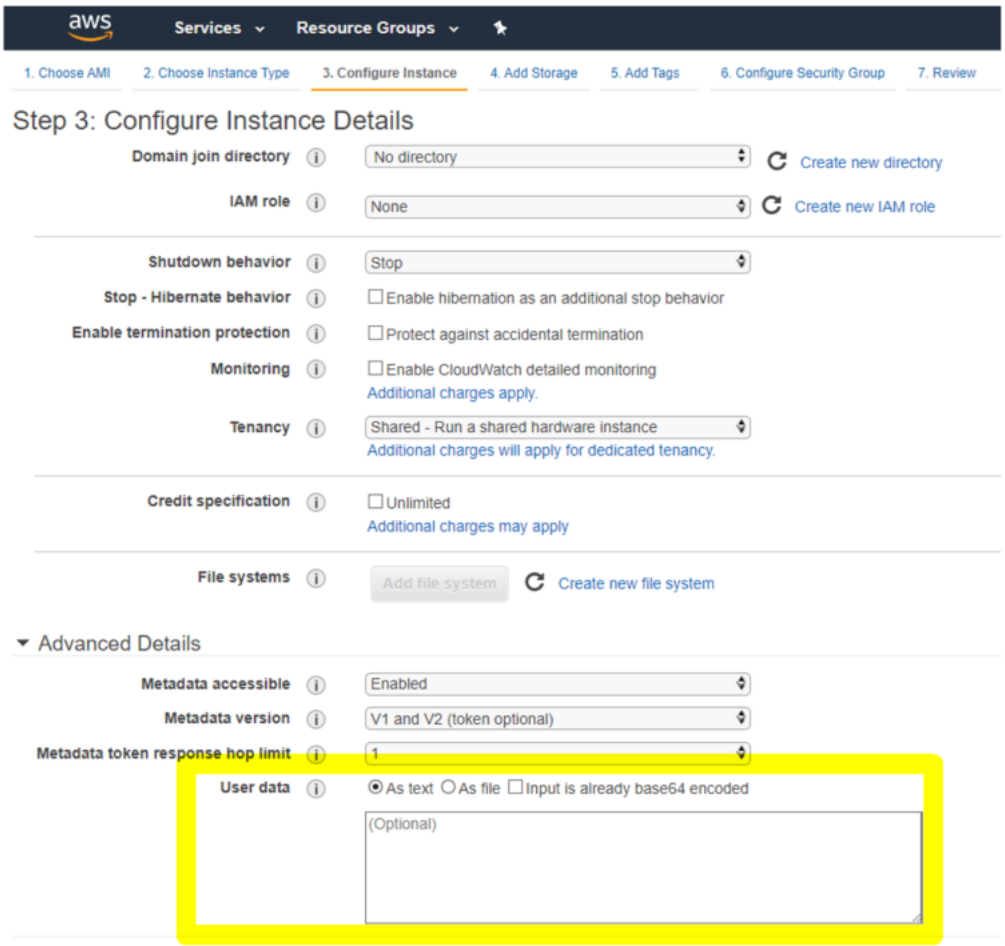
Comment fournir des données utilisateur de pré-démarrage dans une instance cloud

Vous pouvez fournir des données utilisateur de pré-démarrage à l'instance cloud au format XML. Différents clouds ont des interfaces différentes pour fournir des données utilisateur.

Fournir des données utilisateur de pré-démarrage à l'aide de la console AWS

Lorsque vous provisionnez une instance Citrix ADC VPX à l'aide de la console AWS, accédez à **Configurer les détails de l'instance > Détails avancés**et indiquez la configuration des données utilisateur avant le démarrage dans le champ **Données utilisateur** .

Pour obtenir des instructions détaillées sur chacune des étapes, voir Déployer une instance Citrix ADC VPX sur AWS à l'aide de la console Web AWS.
Pour plus d'informations, consultez la documentation AWS sur le lancement d'une instance.



Fournir des données utilisateur de pré-démarrage à l'aide de l'AWS CLI

Saisissez la commande suivante dans l'interface de ligne de commande AWS :

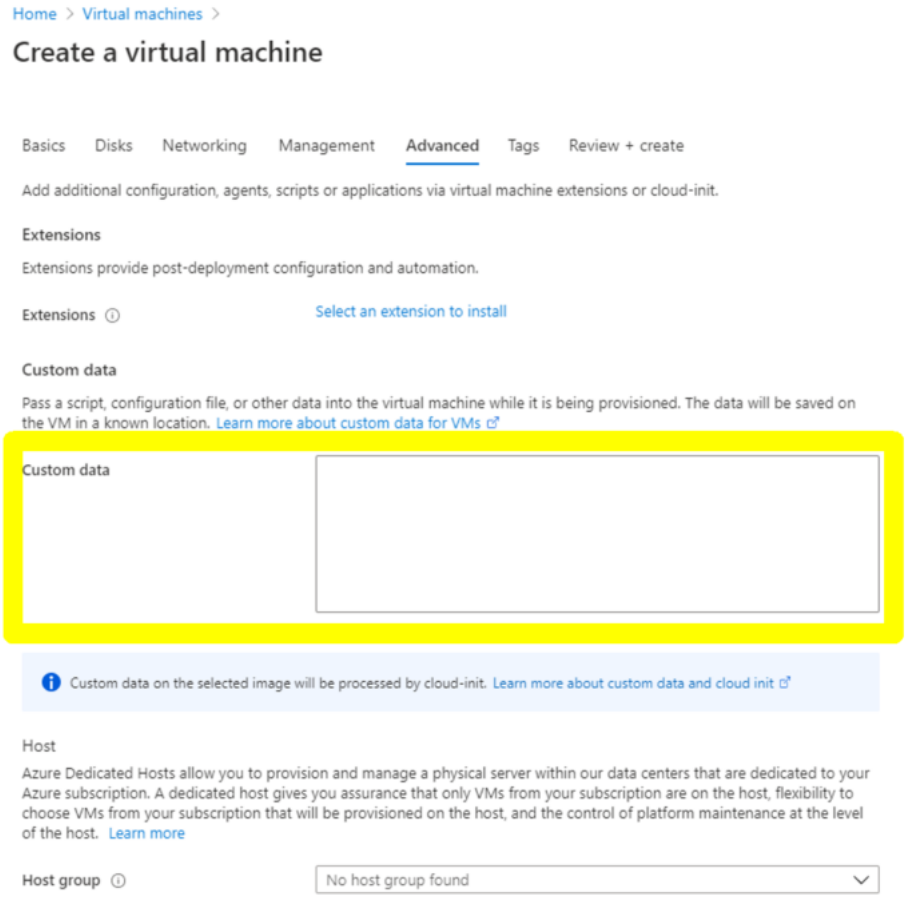
```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 1 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --user-data file://my_script.txt
<!--NeedCopy-->
```

Pour plus d'informations, consultez la documentation AWS sur les instances en cours d'exécution.

Pour plus d'informations, consultez la documentation AWS sur l'utilisation des données utilisateur d'instance.

Fournir des données utilisateur de pré-démarrage à l'aide de la console Azure

Lorsque vous provisionnez une instance Citrix ADC VPX à l'aide de la console Azure, accédez à **Créer une machine virtuelle > onglet Avancé** . Dans le champ **Données personnalisées**, indiquez la configuration des données utilisateur avant le démarrage.



Fournir des données utilisateur de pré-démarrage à l'aide de l'interface de ligne de commande Azure

Saisissez la commande suivante dans l'interface de ligne de commande Azure :

```
az vm create \
  --resource-group myResourceGroup \
  --name MyVm \
  --image debian \
  --custom-data MyCloudInitScript.txt \
<!--NeedCopy-->
```

Exemple :

```
az vm create --resource-group MyResourceGroup -name MyVm --image debian
    --custom-data MyCloudInitScript.txt
<!--NeedCopy-->
```

Vous pouvez transmettre vos données personnalisées ou votre configuration de pré-démarrage sous

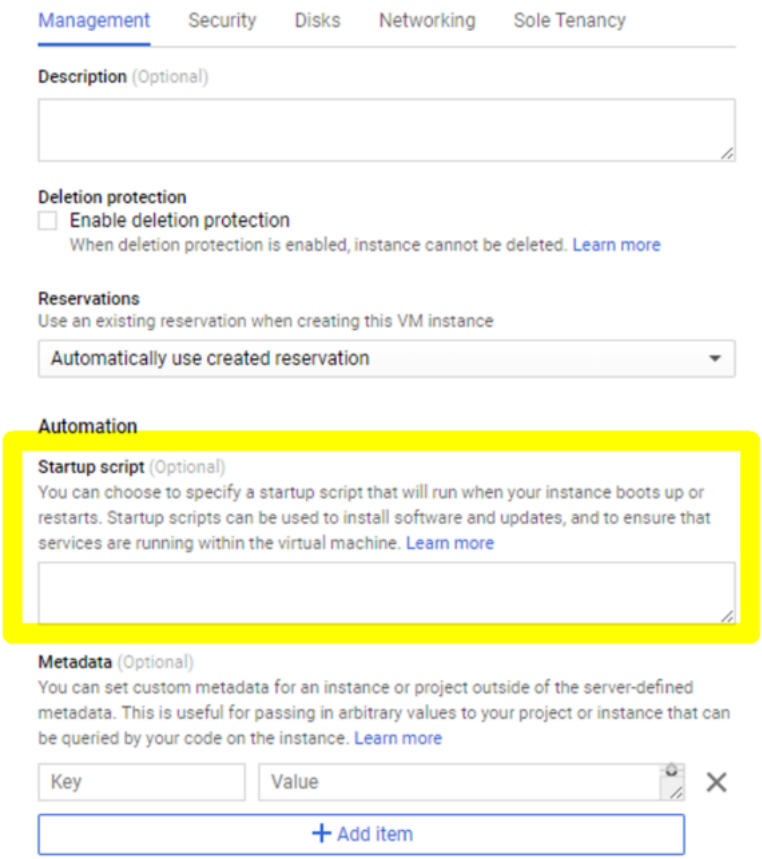
forme de fichier au paramètre « —custom-data ». Dans cet exemple, le nom de fichier est **MyCloudInitScript.txt**.

Pour plus d'informations, consultez la documentation Azure CLI.

Fournir des données utilisateur de pré-démarrage à l'aide de la console GCP

Lorsque vous provisionnez une instance Citrix ADC VPX à l'aide de la console GCP, renseignez les propriétés de l'instance. Développez **la gestion, la sécurité, les disques, la mise en réseau et la location exclusive**. Accédez à l'onglet **Gestion** . Dans la section **Automation**, indiquez la configuration des données utilisateur de **pré-démarrage dans le champ Script** de démarrage.

Pour plus d'informations sur la création de l'instance VPX à l'aide de GCP, voir Déployer une instance Citrix ADC VPX sur Google Cloud Platform.



Fournir des données utilisateur de pré-démarrage à l'aide de l'interface de ligne de commande g

Saisissez la commande suivante dans l'interface de ligne de commande GCP :


```
gcloud compute instances create INSTANCE_NAMES --metadata-from-file=
    startup-script=LOCAL_FILE_PATH
<!--NeedCopy-->
```

metadata-from-file - Lit la valeur ou les données utilisateur à partir d'un fichier stocké dans le <LOCAL_FILE_PATH>.

Pour plus d'informations, consultez la documentation de l'interface de ligne de commande gcloud

Format de données utilisateur de prédémarrage

Les données utilisateur de pré-démarrage doivent être fournies à l'instance cloud au format XML. Les données utilisateur de prédémarrage Citrix ADC que vous fournissez via l'infrastructure cloud pendant le démarrage peuvent comprendre les quatre sections suivantes :

- Configuration Citrix ADC représentée par la <NS-CONFIG> balise.
- Démarrage personnalisé du Citrix ADC représenté avec la <NS-BOOTSTRAP> balise.
- Stockage de scripts utilisateur dans Citrix ADC représenté par la <NS-SCRIPTS> balise.
- Configuration des licences regroupées représentée par la <NS-LICENSE-CONFIG> balise.

Vous pouvez fournir les quatre sections précédentes dans n'importe quel ordre dans la configuration de prédémarrage ADC.
Assurez-vous de suivre strictement la mise en forme affichée dans les sections suivantes tout en fournissant les données utilisateur de pré-démarrage.

> Remarque :
>
> La configuration complète des données utilisateur de pré-démarrage doit être incluse dans la <NS-PRE-BOOT-CONFIG> balise, comme illustré dans les exemples suivants.

Exemple 1 :

```
<NS-PRE-BOOT-CONFIG>
     <NS-CONFIG>          </NS-CONFIG>
     <NS-BOOTSTRAP>       </NS-BOOTSTRAP>
     <NS-SCRIPTS>         </NS-SCRIPTS>
     <NS-LICENSE-CONFIG>  </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Exemple 2 :

```
<NS-PRE-BOOT-CONFIG>
    <NS-LICENSE-CONFIG> </NS-LICENSE-CONFIG>
    <NS-SCRIPTS>        </NS-SCRIPTS>
```



```
4       <NS-BOOTSTRAP>       </NS-BOOTSTRAP>
5       <NS-CONFIG>          </NS-CONFIG>
6   </NS-PRE-BOOT-CONFIG>
7   <!--NeedCopy-->
```

Utilisez la <NS-CONFIG> balise pour fournir les configurations Citrix ADC VPX spécifiques qui doivent être appliquées à l'instance VPX au stade de pré-démarrage.

> REMARQUE :
>
> La <NS-CONFIG> section doit comporter des commandes ADC CLI valides. Les CLI ne sont pas vérifiés pour les erreurs syntaxiques ou le format.

Configurations Citrix ADC

Utilisez la <NS-CONFIG> balise pour fournir les configurations Citrix ADC VPX spécifiques qui doivent être appliquées à l'instance VPX au stade de pré-démarrage.

> REMARQUE :
>
> La <NS-CONFIG> section doit comporter des commandes ADC CLI valides. Les CLI ne sont pas vérifiés pour les erreurs syntaxiques ou le format.

Exemple :

Dans l'exemple suivant, la <NS-CONFIG> section contient les détails des configurations. Un VLAN de l'ID « 5 » est configuré et lié au SNIP (5.0.0.1). Un serveur virtuel d'équilibrage de charge (4.0.0.101) est également configuré.

```
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>
        add vlan 5
        add ns ip  5.0.0.1  255.255.255.0

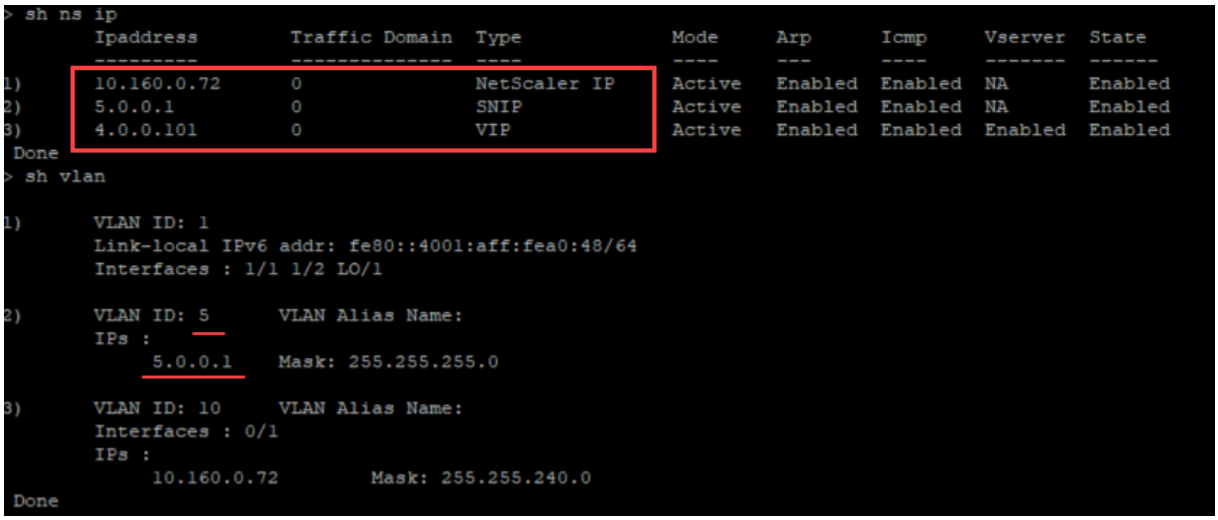
        bind vlan 5 -IPAddress  5.0.0.1  255.255.255.0
        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201  5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip
D SABLED -usip
NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
        add lb vserver preboot_v4_101 HTTP  4.0.0.101  80 -persistenceType NONE -cltTimeout 180
    </NS-CONFIG>

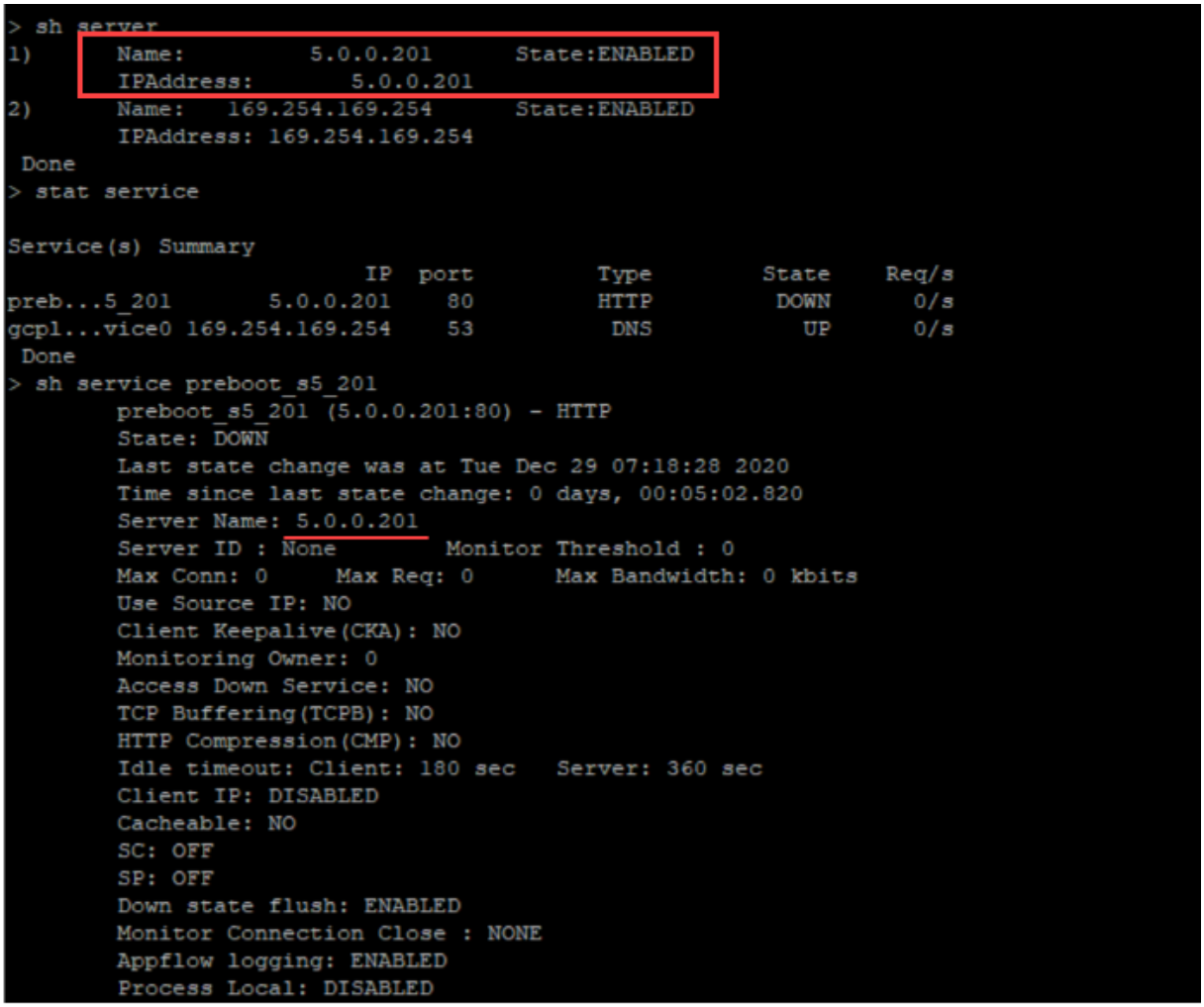
</NS-PRE-BOOT-CONFIG>
```


Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
     <NS-CONFIG>
         add vlan 5
         add ns ip 5.0.0.1 255.255.255.0
         bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
         enable ns feature WL SP LB RESPONDER
         add server 5.0.0.201 5.0.0.201
         add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip
 NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -
    TCPB NO -CMP NO
         add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180
     </NS-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

L'instance Citrix ADC VPX fournit la configuration appliquée dans la <NS-CONFIG> section, comme illustré dans les illustrations suivantes.





Scripts utilisateur

Utilisez la <NS-SCRIPTS> balise pour fournir tout script qui doit être stocké et exécuté dans une instance Citrix ADC VPX.

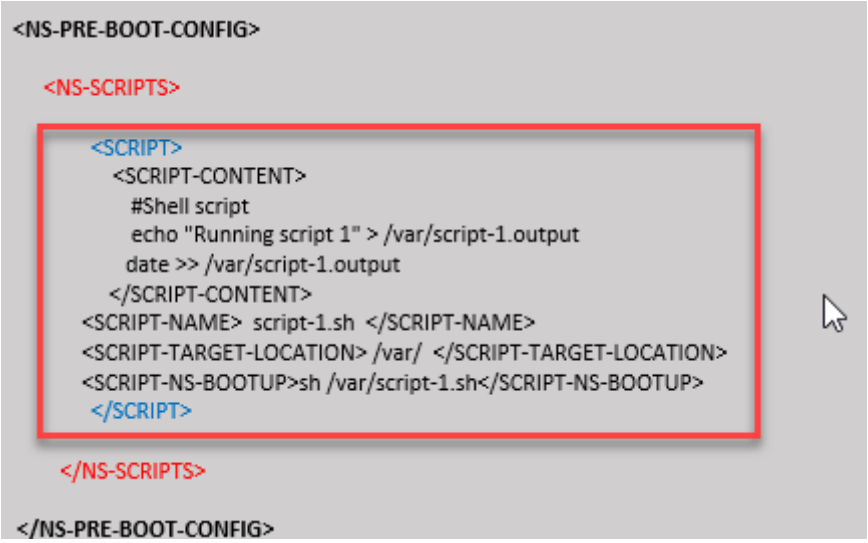
Vous pouvez inclure de nombreux scripts dans la <NS-SCRIPTS> balise. Chaque script doit être inclus dans la <SCRIPT> balise.
Chaque <SCRIPT> section correspond à un script et contient tous les détails du script à l'aide des sous-balises suivantes.

- **<SCRIPT-NAME>:** Indique le nom du fichier de script qui doit être stocké.
- **<SCRIPT-CONTENT>:** Indique le contenu du fichier qui doit être stocké.
- **<SCRIPT-TARGET-LOCATION>:** Indique l'emplacement cible désigné où ce fichier doit être stocké. Si l'emplacement cible n'est pas fourni, le fichier ou le script est enregistré par défaut dans le répertoire « /nsconfig ».
- **<SCRIPT-NS-BOOTUP>:** Spécifiez les commandes que vous utilisez pour exécuter le script.

- Si vous utilisez la <SCRIPT-NS-BOOTUP> section, les commandes fournies dans la section sont stockées dans “/nsconfig/nsafter.sh «, et les commandes sont exécutées après le démarrage du moteur de paquets dans le cadre de l’exécution de” nsafter.sh ».
- Si vous n’utilisez pas la <SCRIPT-NS-BOOTUP> section, le fichier de script est stocké à l’emplacement cible que vous spécifiez.

Exemple 1 :

Dans cet exemple, la <NS-SCRIPTS> balise contient des détails sur un seul script : script-1.sh. Le script “script-1.sh” est enregistré dans le répertoire « /var ». Le script est rempli avec le contenu spécifié et est exécuté avec la commande « sh /var/script-1.sh » après le démarrage du moteur de paquets.



Vous pouvez copier la configuration affichée dans la capture d’écran précédente à partir d’ici :

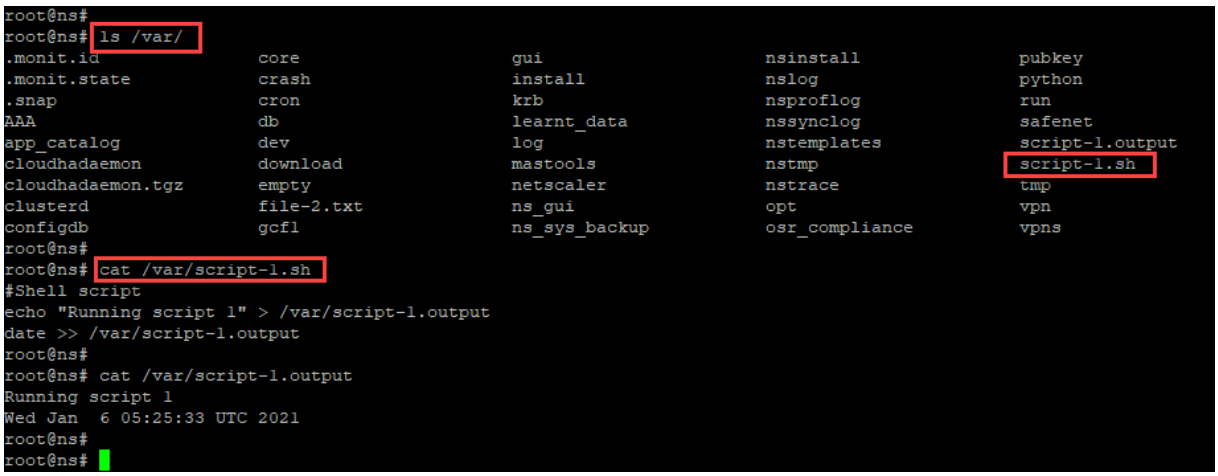
```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
    <SCRIPT>
            <SCRIPT-CONTENT>
                #Shell script
                echo "Running script 1" > /var/script-1.output
                date >> /var/script-1.output
            </SCRIPT-CONTENT>

                <SCRIPT-NAME> script-1.sh </SCRIPT-NAME>
                <SCRIPT-TARGET-LOCATION> /var/ </SCRIPT-TARGET-LOCATION
                    >
                <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP
                    >
        </SCRIPT>
    </NS-SCRIPTS>
</NS-PRE-BOOT-CONFIG>
```



```
16 <!--NeedCopy-->
```

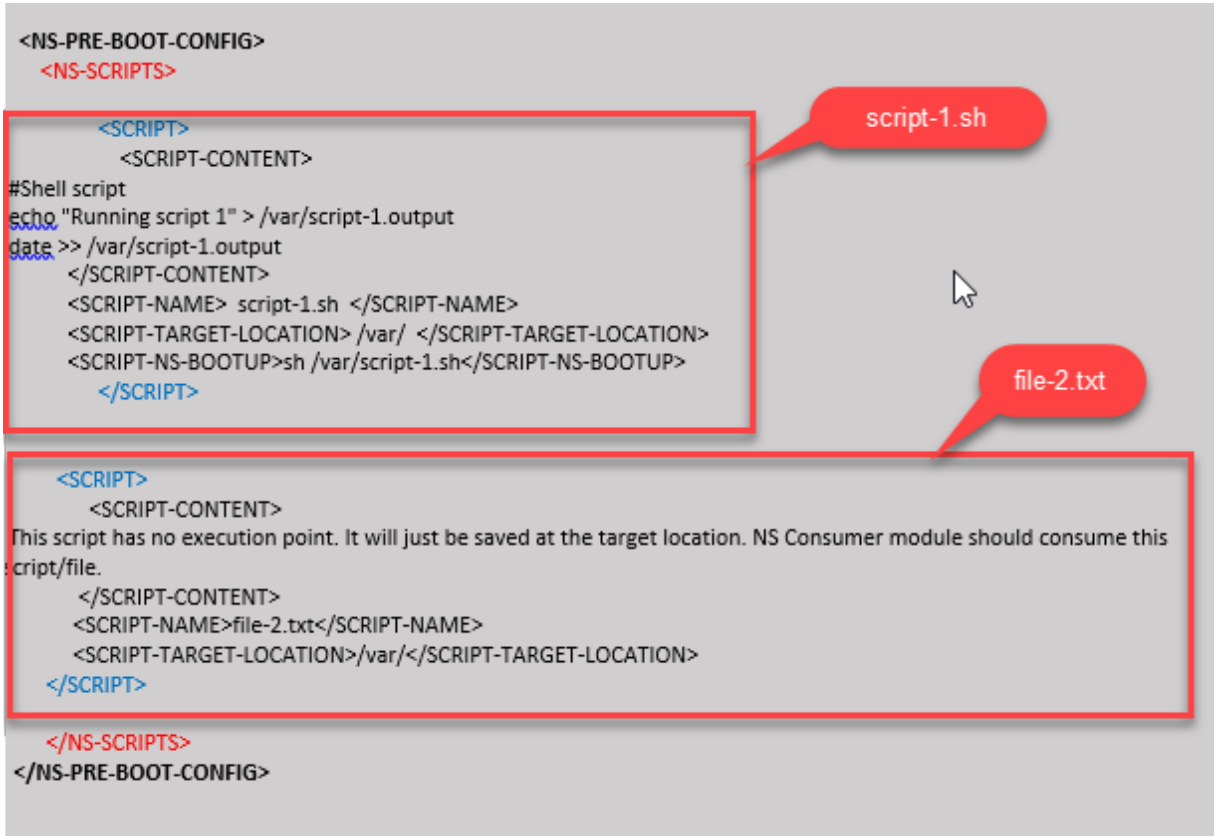
Dans l'instantané suivant, vous pouvez vérifier que le script "script-1.sh" est enregistré dans le répertoire « /var/ ». Le script "Script-1.sh" est exécuté et le fichier de sortie est créé de manière appropriée.



Exemple 2 :

Dans l'exemple suivant, la <NS-SCRIPTS> balise contient des détails sur deux scripts.

- Le premier script est enregistré sous le nom "script-1.sh" dans le répertoire « /var ». Le script est rempli avec le contenu spécifié et est exécuté avec la commande « sh /var/script-1.sh » après le démarrage du moteur de paquets.
- Le second script est enregistré sous le nom "file-2.txt" dans le répertoire « /var ». Ce fichier contient le contenu spécifié. Mais il n'est pas exécuté car la commande d'exécution de démarrage n' <SCRIPT-NS-BOOTUP> est pas fournie.



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
        <SCRIPT>
            <SCRIPT-CONTENT>
               #Shell script
               echo "Running script 1" > /var/script-1.output
               date >> /var/script-1.output
            </SCRIPT-CONTENT>

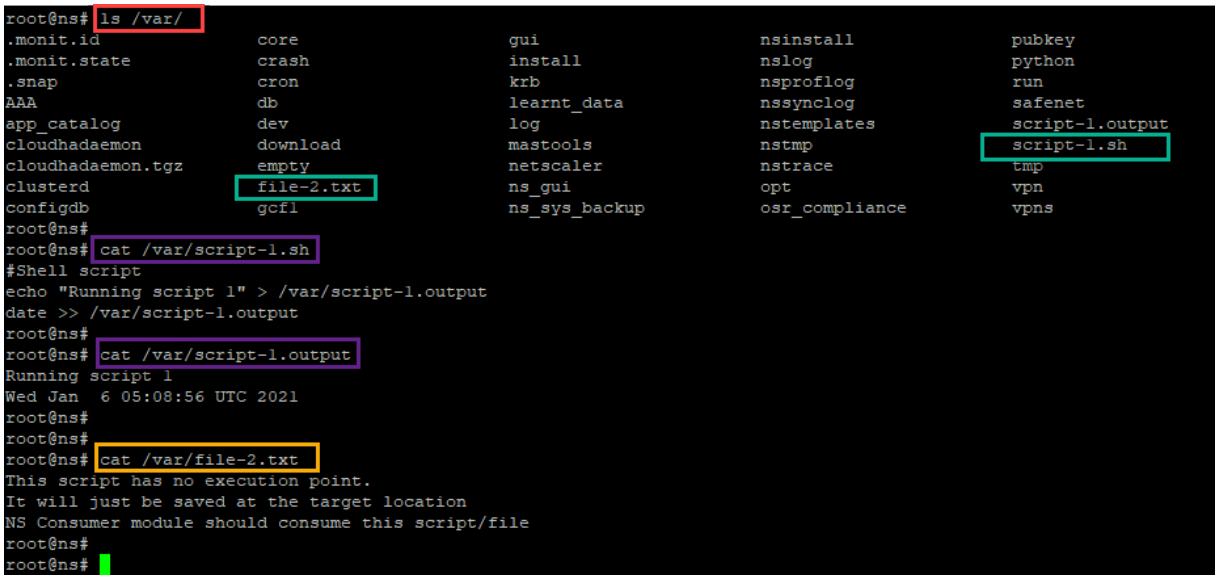
            <SCRIPT-NAME>  script-1.sh  </SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION> /var/  </SCRIPT-TARGET-LOCATION>
            <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP>
            </SCRIPT>

        <SCRIPT>
            <SCRIPT-CONTENT>
                This script has no execution point.
                It will just be saved at the target location
                NS Consumer module should consume this script/file
            </SCRIPT-CONTENT>
```



```
            <SCRIPT-NAME>file-2.txt</SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION>/var/</SCRIPT-TARGET-LOCATION>
        </SCRIPT>
    </NS-SCRIPTS>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Dans l'instantané suivant, vous pouvez vérifier que script-1.sh et file-2.txt sont créés dans le répertoire « /var/ ». Le fichier Script-1.sh est exécuté et le fichier de sortie est créé de manière appropriée.



Licences

Utilisez la <NS-LICENSE-CONFIG> balise pour appliquer les licences regroupées Citrix ADC lors du démarrage de l'instance VPX. Utilisez la <LICENSE-COMMANDS> balise dans <NS-LICENSE-CONFIG> la section pour fournir les commandes de licence regroupées. Ces commandes doivent être valides syntaxiquement.

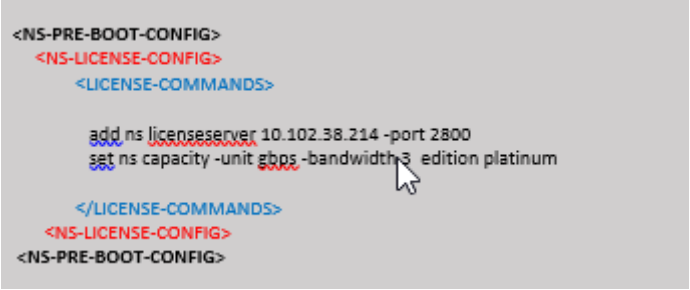
Vous pouvez spécifier les détails de licence regroupés tels que le type de licence, la capacité et le serveur de licences dans la <LICENSE-COMMANDS> section à l'aide des commandes de licences groupées standard. Pour plus d'informations, voir Configurer les licences de capacité regroupées Citrix ADC.

Après avoir appliqué le <NS-LICENSE-CONFIG>, le VPX arrive avec l'édition demandée au démarrage, et VPX tente d'extraire les licences configurées à partir du serveur de licences.

- Si la récupération de la licence est réussie, la bande passante configurée est appliquée à VPX.
- Si la récupération des licences échoue, la licence n'est pas extraite du serveur de licences dans les 10 à 12 minutes environ. Par conséquent, le système redémarre et entre dans un état sans licence.

Exemple :

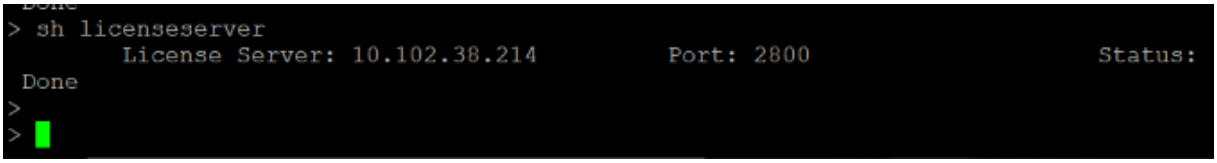
Dans l'exemple suivant, après avoir appliqué le <NS-LICENSE-CONFIG>, le VPX arrive avec l'édition Premium au démarrage, et VPX tente d'extraire les licences configurées à partir du serveur de licences (10.102.38.214).



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
   <NS-LICENSE-CONFIG>
        <LICENSE-COMMANDS>
            add ns licenseserver 10.102.38.214 -port 2800
            set ns capacity -unit gbps -bandwidth 3  edition platinum
        </LICENSE-COMMANDS>
    </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Comme indiqué dans l'illustration suivante, vous pouvez exécuter la commande « show license server » et vérifier que le serveur de licences (10.102.38.214) est ajouté au VPX.



Bootstrapping

Utilisez la <NS-BOOTSTRAP> balise pour fournir les informations de démarrage personnalisées. Vous pouvez utiliser les <NEW-BOOTSTRAP-SEQUENCE> balises <SKIP-DEFAULT-BOOTSTRAP> et dans la <NS-BOOTSTRAP> section. Cette section informe l'appliance Citrix ADC si l'amorçage par défaut doit être évité ou non. Si le démarrage par défaut est évité, cette section vous offre la possibilité de fournir une nouvelle séquence de démarrage.

Configuration d'amorçage par défaut

La configuration d'amorçage par défaut dans l'appliance Citrix ADC suit les attributions d'interface suivantes :

- **Eth0** - Interface de gestion avec une certaine adresse NSIP.
- **Eth1** - Interface client avec une certaine adresse VIP.
- **Eth2** - Interface serveur avec une certaine adresse SNIP.

Personnalisation de la configuration de bootstrap

Vous pouvez ignorer la séquence d'amorçage par défaut et fournir une nouvelle séquence d'amorçage pour l'instance Citrix ADC VPX. Utilisez la <NS-BOOTSTRAP> balise pour fournir les informations de démarrage personnalisées. Par exemple, vous pouvez modifier le démarrage par défaut, où l'interface de gestion (NSIP), l'interface VIP et l'interface orientée serveur (SNIP) sont toujours fournies dans un certain ordre.

Le tableau suivant indique le comportement d'amorçage avec les différentes valeurs autorisées pour <SKIP-DEFAULT-BOOTSTRAP> et les <NEW-BOOTSTRAP-SEQUENCE> balises.

SKIP-DEFAULT-BOOTSTRAP	NEW-BOOTSTRAP-SEQUENCE	Comportement Bootstrap
OUI	OUI	Le comportement d'amorçage par défaut est ignoré et une nouvelle séquence d'amorçage personnalisée fournie dans la <NS-BOOTSTRAP> section est exécutée.
OUI	NON	Le comportement d'amorçage par défaut est ignoré. Les commandes d'amorçage fournies dans cette <NS-CONFIG> section sont exécutées.

Vous pouvez personnaliser la configuration d'amorçage à l'aide des trois méthodes suivantes :

- Fournissez uniquement les détails de l'interface
- Fournir les détails de l'interface ainsi que les adresses IP et le masque de sous-réseau
- Fournir des commandes liées au bootstrap dans la <NS-CONFIG> section

Méthode 1 : amorçage personnalisé en spécifiant uniquement les détails de l'interface

Vous spécifiez les interfaces de gestion, orientées client et orientées serveur, mais pas leurs adresses IP et masques de sous-réseau. Les adresses IP et les masques de sous-réseau sont renseignés en interrogeant l'infrastructure cloud.

Exemple d'amorçage personnalisé pour AWS

Vous fournissez la séquence d'amorçage personnalisée, comme illustré dans l'exemple suivant. Pour plus d'informations, voir Comment fournir des données utilisateur de pré-démarrage dans une instance cloud. L'interface Eth1 est assignée en tant qu'interface de gestion (NSIP), Eth0 comme interface client (VIP) et interface Eth2 en tant qu'interface serveur (SNIP). La section contient <NS-BOOTSTRAP> uniquement les détails de l'interface et non les détails des adresses IP et des masques de sous-réseau.

```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

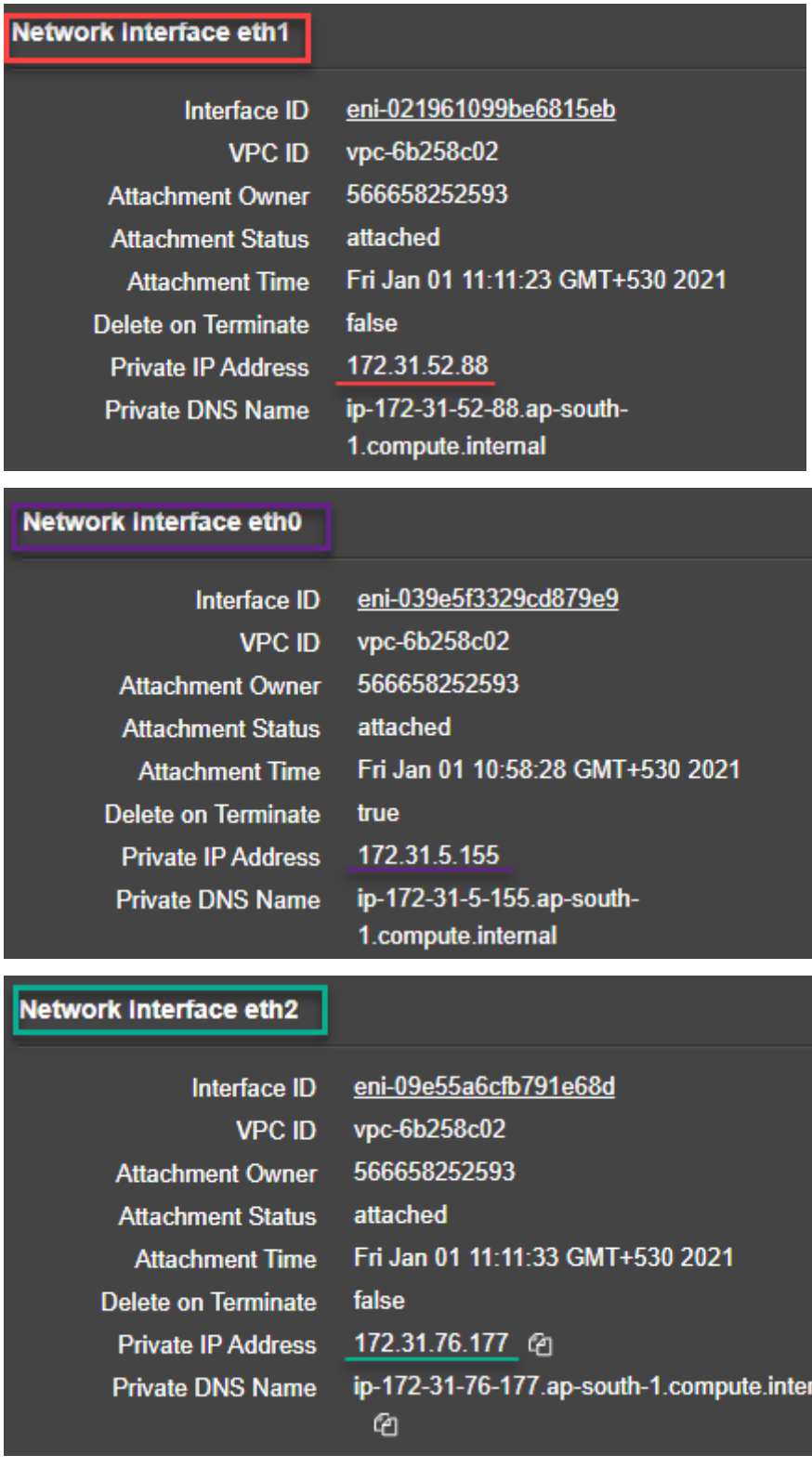
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

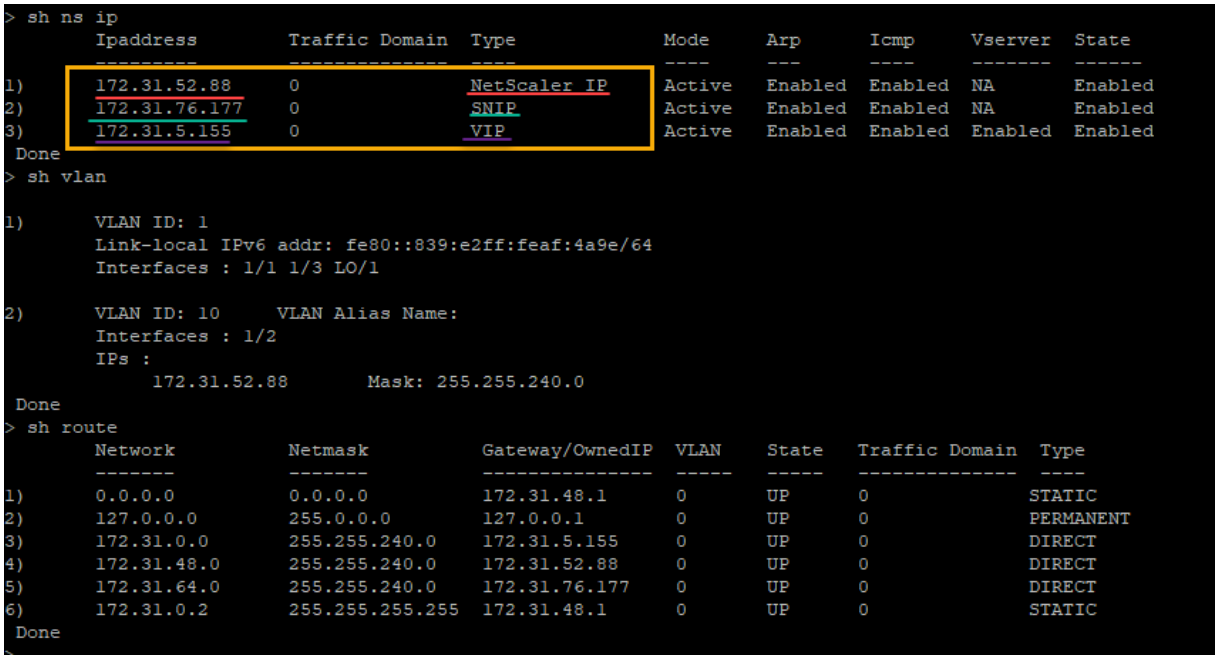
    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Une fois l'instance de machine virtuelle créée, dans le portail AWS, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

1. Accédez au **portail AWS > instances EC2**et sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Dans l'onglet **Description**, vous pouvez vérifier les propriétés de chaque interface réseau, comme illustré dans les illustrations suivantes.



Vous pouvez exécuter la commande `show nsip` dans **ADC CLI**et vérifier les interfaces réseau appliquées à l'instance ADC VPX lors du premier démarrage de l'appliance ADC.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.31.76.177    0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.31.5.155     0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.0.0       255.255.240.0    172.31.5.155     0       UP      0               DIRECT
4)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
5)      172.31.64.0      255.255.240.0    172.31.76.177    0       UP      0               DIRECT
6)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
```

Exemple de bootstrap personnalisé pour Azure

Vous fournissez la séquence d'amorçage personnalisée, comme illustré dans l'exemple suivant. Pour plus d'informations, voir Comment fournir des données utilisateur de pré-démarrage dans une instance cloud. L'interface Eth2 est assignée en tant qu'interface de gestion (NSIP), Eth1 comme interface client (VIP) et interface Eth0 en tant qu'interface serveur (SNIP). La section contient <NS-BOOTSTRAP> uniquement les détails de l'interface et non les détails des adresses IP et des masques de sous-réseau.


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

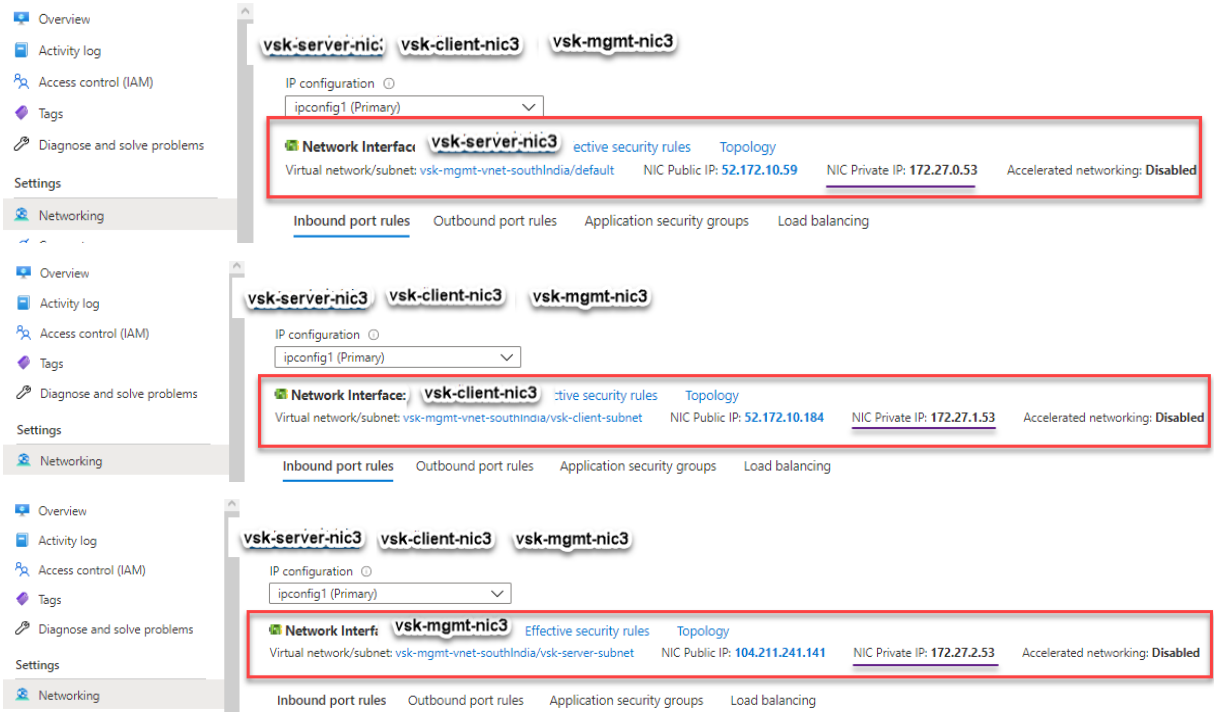
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
```

Vous pouvez constater que l'instance Citrix ADC VPX est créée avec trois interfaces réseau. Accédez au **portail Azure > Instance de machine virtuelle > Mise en réseau**et vérifiez les propriétés réseau des trois cartes réseau, comme illustré dans les illustrations suivantes.



Vous pouvez exécuter la commande « show nsip » dans l'interface de ligne de commande ADC et véri-

fier que la nouvelle séquence d'amorçage spécifiée dans la section <NS-BOOTSTRAP> est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.27.2.53      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.53      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.27.1.53      0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:c26c/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.53        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.53      0       UP      0               DIRECT
4)      172.27.1.0       255.255.255.0    172.27.1.53      0       UP      0               DIRECT
5)      172.27.2.0       255.255.255.0    172.27.2.53      0       UP      0               DIRECT
6)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
7)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
8)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
>
```

Exemples de bootstrap personnalisés pour GCP

Vous fournissez la séquence d'amorçage personnalisée, comme illustré dans l'exemple suivant. Pour plus d'informations, voir Comment fournir des données utilisateur de pré-démarrage dans une instance cloud. L'interface Eth1 est assignée en tant qu'interface de gestion (NSIP), Eth0 comme interface client (VIP) et interface Eth2 en tant qu'interface serveur (SNIP). La section contient <NS-BOOTSTRAP> uniquement les détails de l'interface et non les détails des adresses IP et des masques de sous-réseau.


```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Une fois l'instance de machine virtuelle créée dans le portail GCP, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

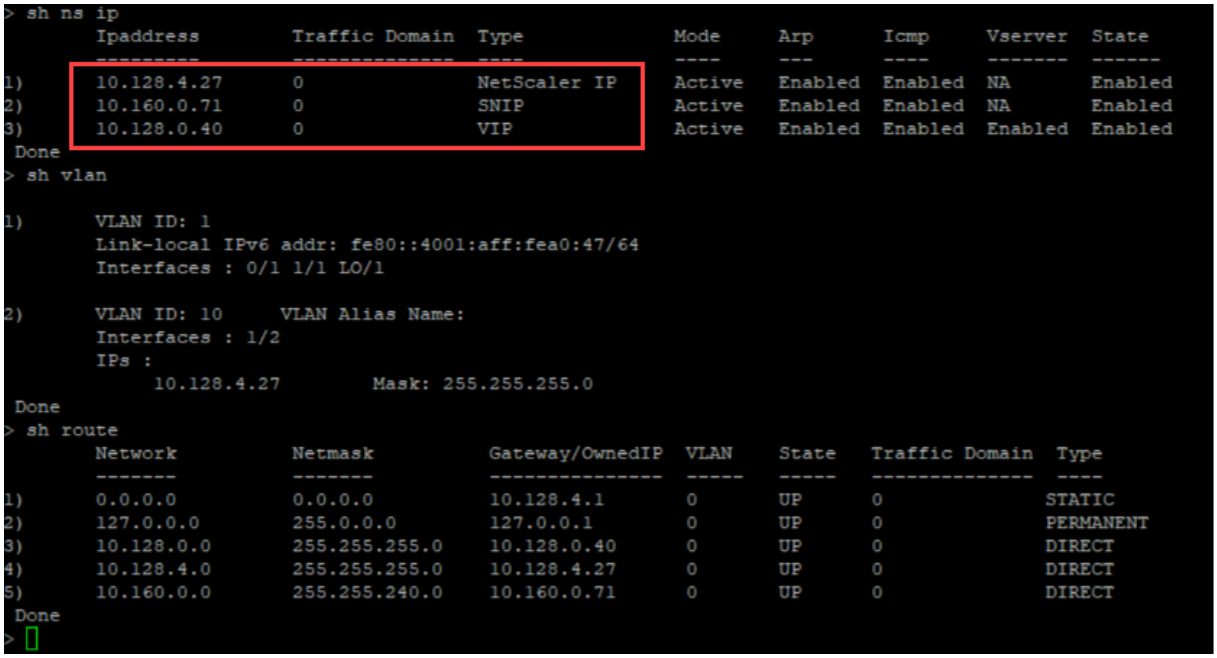
1. Sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Accédez aux propriétés de l'interface réseau et vérifiez les détails de la carte réseau comme suit :

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	10.160.0.71	–	35.244.56.180 (ephemeral)	Premium	Off	View details
nic1	vsk-vpc-network-1	asia-south1-subnet-1	10.128.0.40	–	35.244.40.113 (ephemeral)	Premium		View details
nic2	vsk-vpc-network-2	asia-south1-subnet-5	10.128.4.27	–	34.93.241.147 (ephemeral)	Premium		View details

Public DNS PTR Record
None

Vous pouvez exécuter la commande `show nsip` dans **ADC CLI**et vérifier les interfaces réseau appliquées à l'instance ADC VPX lors du premier démarrage de l'appliance ADC.



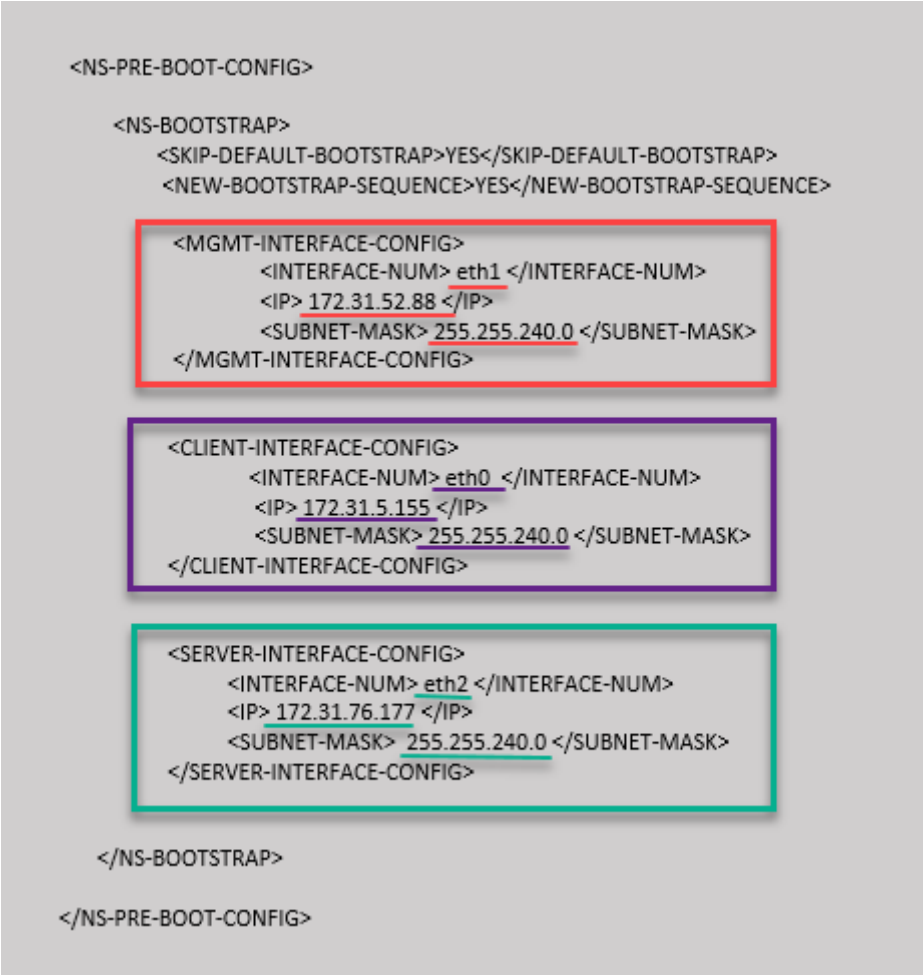
Méthode 2 : amorçage personnalisé en spécifiant les interfaces, adresses IP et masques de sous-réseau

Vous spécifiez les interfaces de gestion, orientées client et serveur, ainsi que leurs adresses IP et leur masque de sous-réseau.

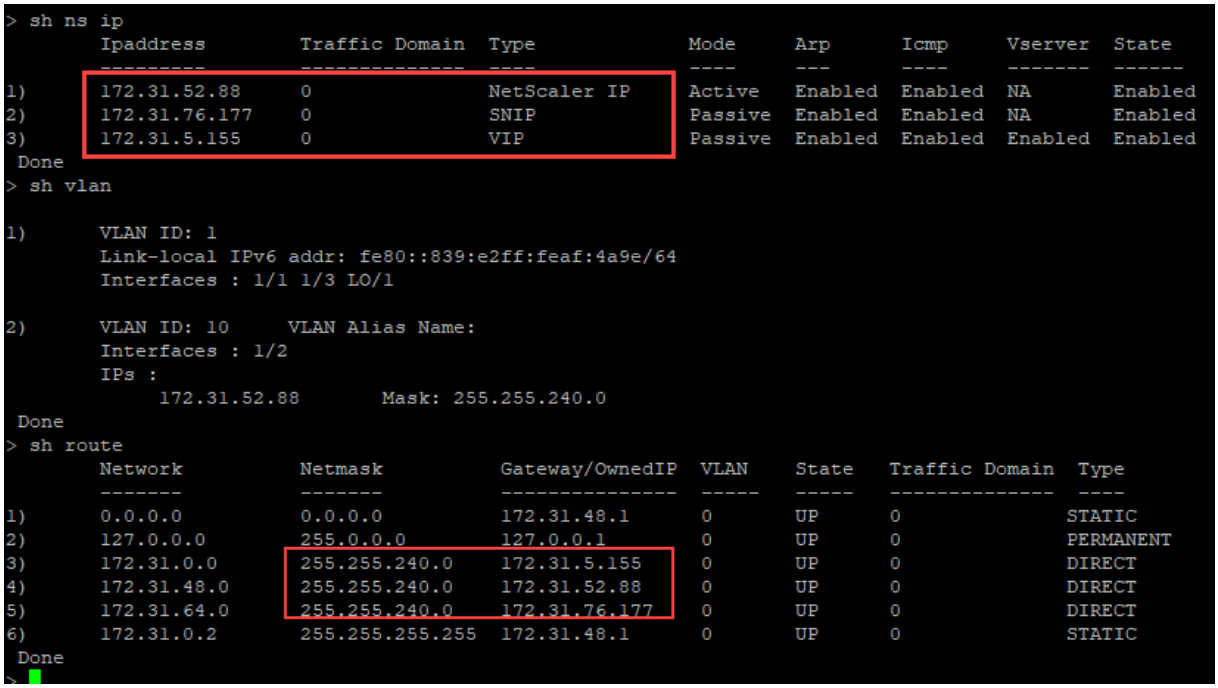
Exemples de bootstrap personnalisés pour AWS

Dans l'exemple suivant, vous ignorez le bootstrap par défaut et exécutez une nouvelle séquence d'amorçage pour l'appliance Citrix ADC. Pour la nouvelle séquence d'amorçage, vous spécifiez les détails suivants :

- **Interface de gestion :** Interface - Eth1, NSIP - 172.31.52.88 et masque de sous-réseau - 255.255.240.0
- **Interface client :** Interface - Eth0, VIP - 172.31.5.155 et masque de sous-réseau - 255.255.240.0.
- **Interface serveur :** Interface - Eth2, SNIP - 172.31.76.177 et masque de sous-réseau - 255.255.240.0.



Vous pouvez exécuter la commande `show nsip` dans l'interface de ligne de commande ADC et vérifier que la nouvelle séquence d'amorçage spécifiée dans la section `<NS-BOOTSTRAP>` est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -----
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.31.76.177    0               SNIP             Passive  Enabled  Enabled  NA       Enabled
3)      172.31.5.155     0               VIP              Passive  Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.0.0       255.255.240.0    172.31.5.155     0       UP      0               DIRECT
4)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
5)      172.31.64.0      255.255.240.0    172.31.76.177    0       UP      0               DIRECT
6)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
>
```

Exemple de bootstrap personnalisé pour Azure

Dans l'exemple suivant, une nouvelle séquence d'amorçage pour ADC est mentionnée et l'amorçage par défaut est ignoré. Vous fournissez les détails de l'interface ainsi que les adresses IP et les masques de sous-réseau comme suit :

- Interface de gestion (eth2), NSIP (172.27.2.53) et masque de sous-réseau (255.255.255.0)
- Interface client (eth1), VIP (172.27.1.53) et masque de sous-réseau (255.255.255.0)
- Interface serveur (eth0), SNIP (172.27.0.53) et masque de sous-réseau (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
            <IP> 172.27.2.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>

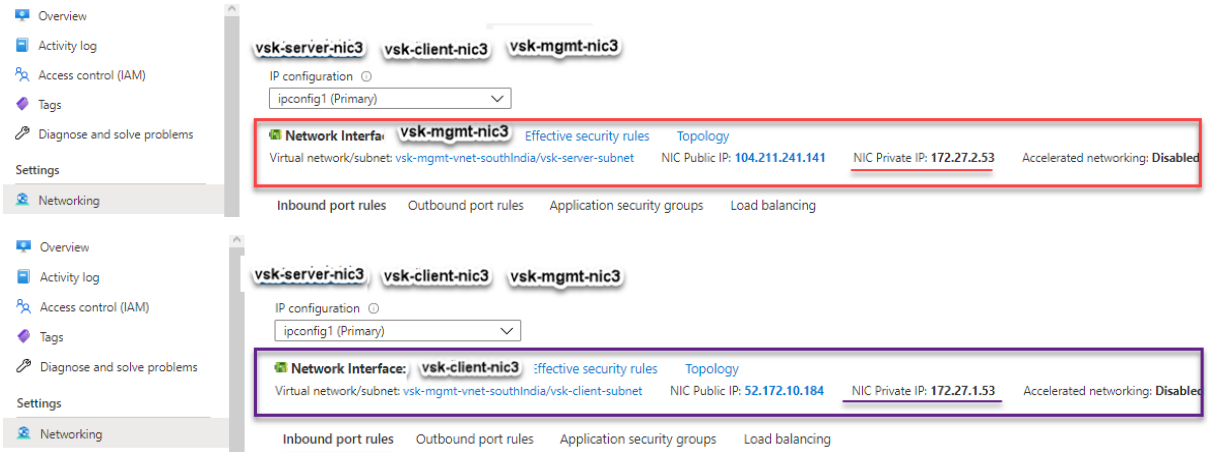
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
            <IP> 172.27.1.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
            </CLIENT-INTERFACE-CONFIG>

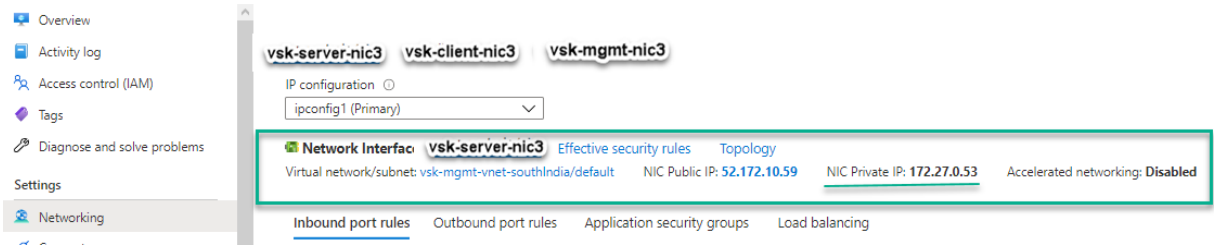
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
            <IP> 172.27.0.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
```

Vous pouvez constater que l'instance Citrix ADC VPX est créée avec trois interfaces réseau. Accédez au **portail Azure > Instance de machine virtuelle > Mise en réseau**et vérifiez les propriétés réseau des trois cartes réseau, comme illustré dans les illustrations suivantes.





Vous pouvez exécuter la commande `show nsip` dans l'interface de ligne de commande ADC et vérifier que la nouvelle séquence d'amorçage spécifiée dans la section <NS-BOOTSTRAP> est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.27.2.53      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.53      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.27.1.53      0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:c26c/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.53        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.53      0       UP      0               DIRECT
4)      172.27.1.0       255.255.255.0    172.27.1.53      0       UP      0               DIRECT
5)      172.27.2.0       255.255.255.0    172.27.2.53      0       UP      0               DIRECT
6)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
7)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
8)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

Exemple de bootstrap personnalisé pour GCP

Dans l'exemple suivant, une nouvelle séquence d'amorçage pour ADC est mentionnée et l'amorçage par défaut est ignoré. Vous fournissez les détails de l'interface ainsi que les adresses IP et les masques de sous-réseau comme suit :

- Interface de gestion (eth2), NSIP (10.128.4.31) et masque de sous-réseau (255.255.255.0)
- Interface client (eth1), VIP (10.128.0.43) et masque de sous-réseau (255.255.255.0)
- Interface serveur (eth0), SNIP (10.160.0.75) et masque de sous-réseau (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>
   <NS-BOOTSTRAP>
         <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
         <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
          <MGMT-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth2 </INTERFACE-NUM>
               <IP> 10.128.4.31 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
           </MGMT-INTERFACE-CONFIG>
          <CLIENT-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth1 </INTERFACE-NUM>
               <IP> 10.128.0.43 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
          </CLIENT-INTERFACE-CONFIG>
          <SERVER-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth0 </INTERFACE-NUM>
               <IP> 10.160.0.75 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
          </SERVER-INTERFACE-CONFIG>
   </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

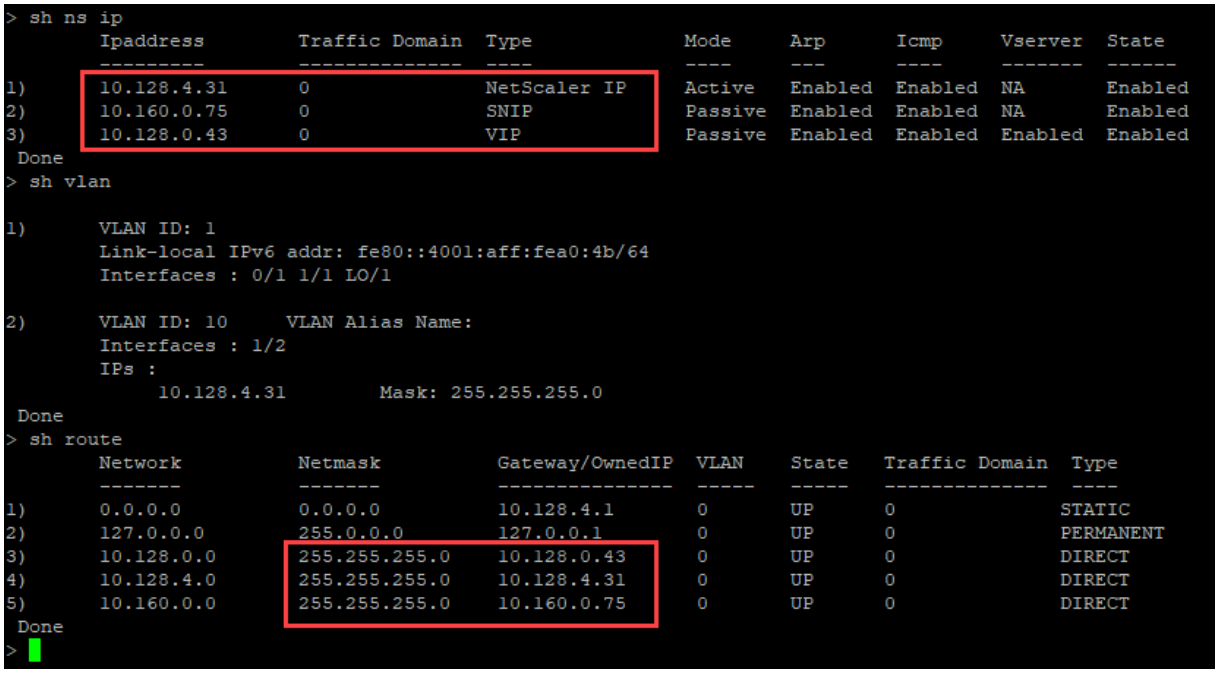
Une fois l'instance de machine virtuelle créée dans le portail GCP avec le bootstrap personnalisé, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

1. Sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Accédez aux propriétés de l'interface réseau et vérifiez les détails de la carte réseau comme suit.

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	vsk-defnw-st-ip1 (10.160.0.75)	–	34.93.216.90 (ephemeral)	Premium	Off	View details
nic1	vsk-vpc-network-1	asia-south1-subnet-1	vsk-vpc-nw1-st-ip1 (10.128.0.43)	–	35.244.40.113 (ephemeral)	Premium		View details
nic2	vsk-vpc-network-2	asia-south1-subnet-5	vsk-nw2-st-ip-1 (10.128.4.31)	–	34.93.202.214 (ephemeral)	Premium		View details

Vous pouvez exécuter la commande `show nsip` dans l'interface de ligne de commande ADC et vérifier que la nouvelle séquence d'amorçage spécifiée dans la section <NS-BOOTSTRAP> est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.



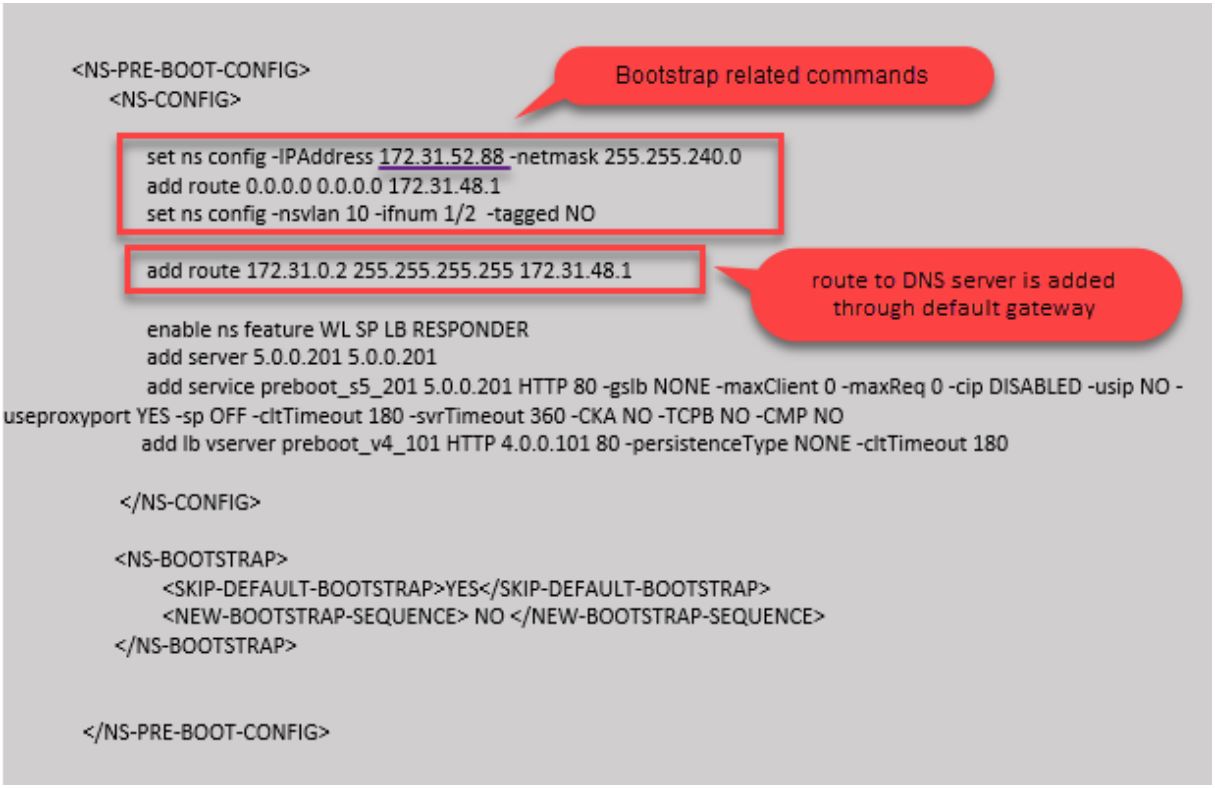
Méthode 3 : Bootstrap personnalisé en fournissant des commandes liées au bootstrap dans la section <NS-CONFIG>

Vous pouvez fournir les commandes associées au bootstrap dans la section <NS-CONFIG>. Dans la section <NS-BOOTSTRAP>, vous devez spécifier la valeur <NEW-BOOTSTRAP-SEQUENCE> « Non » pour exécuter les commandes d'amorçage de la section <NS-CONFIG>. Vous devez également fournir les commandes pour attribuer NSIP, routage par défaut et NSVLAN. En outre, fournissez les commandes pertinentes pour le cloud que vous utilisez.

Avant de fournir un bootstrap personnalisé, assurez-vous que votre infrastructure cloud prend en charge une configuration d'interface particulière.

Exemple d'amorçage personnalisé pour AWS

Dans cet exemple, les commandes liées au bootstrap sont fournies dans la section <NS-CONFIG>. La section <NS-BOOTSTRAP> indique que le démarrage par défaut est ignoré et que les informations d'amorçage personnalisées fournies dans la section <NS-CONFIG> sont exécutées. Vous devez également fournir les commandes permettant de créer NSIP, d'ajouter un itinéraire par défaut et d'ajouter un NSVLAN.



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>

        set ns config -IPAddress 172.31.52.88 -netmask 255.255.240.0
        add route 0.0.0.0 0.0.0.0 172.31.48.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add route 172.31.0.2 255.255.255.255 172.31.48.1

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO - useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

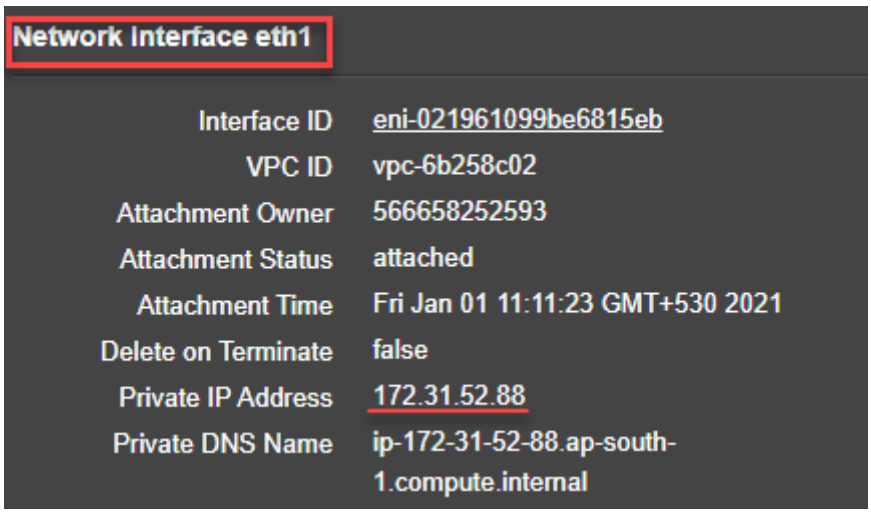
    <NS-BOOTSTRAP>
     <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
     <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
```

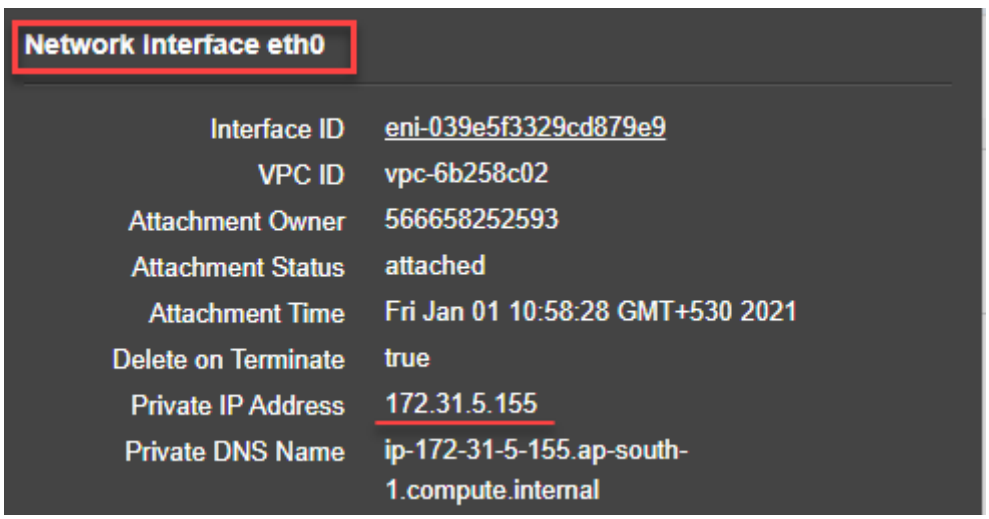


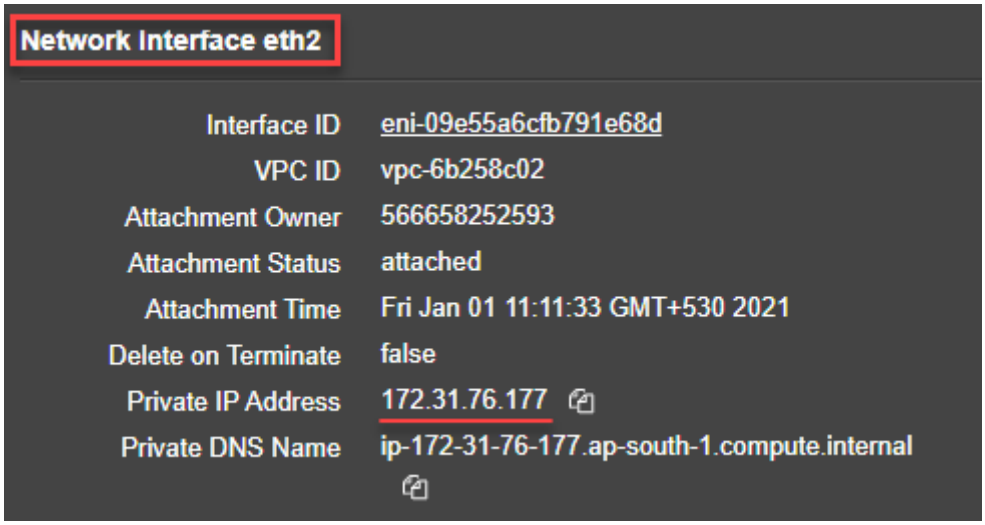
```
19      </NS-BOOTSTRAP>
20
21
22  </NS-PRE-BOOT-CONFIG>
23  <!--NeedCopy-->
```

Une fois l'instance de machine virtuelle créée, dans le portail AWS, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

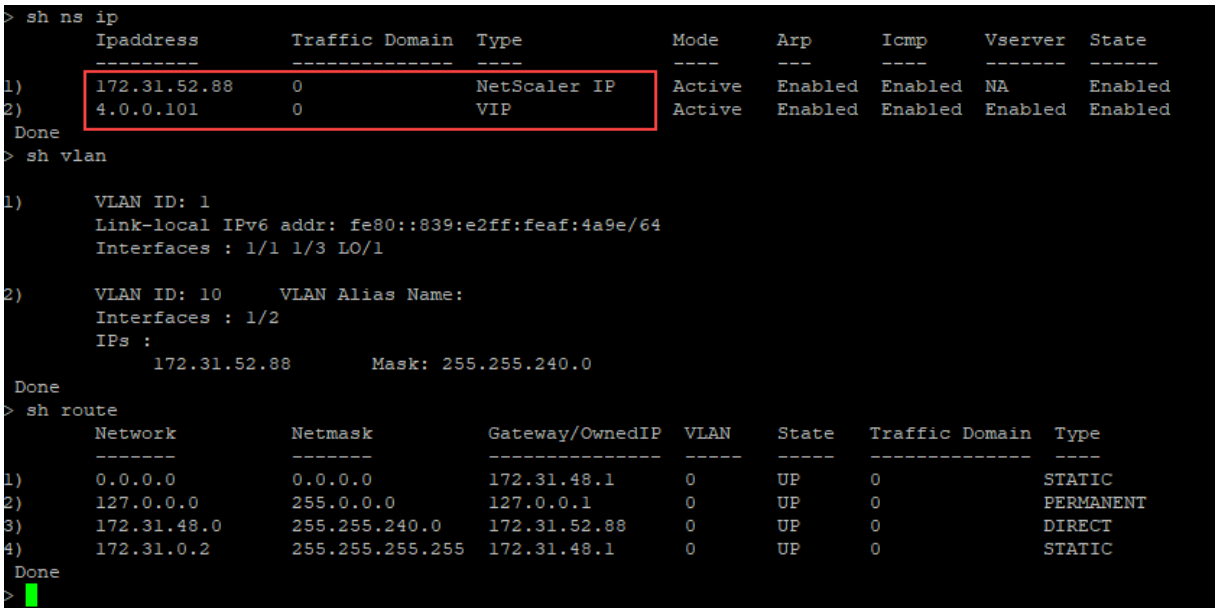
1. Accédez au **portail AWS > instances EC2**et sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Dans l'onglet **Description**, vous pouvez vérifier les propriétés de chaque interface réseau, comme illustré dans les illustrations suivantes.







Vous pouvez exécuter la commande `show nsip` dans **ADC CLI**et vérifier les interfaces réseau appliquées à l'instance ADC VPX lors du premier démarrage de l'appliance ADC.

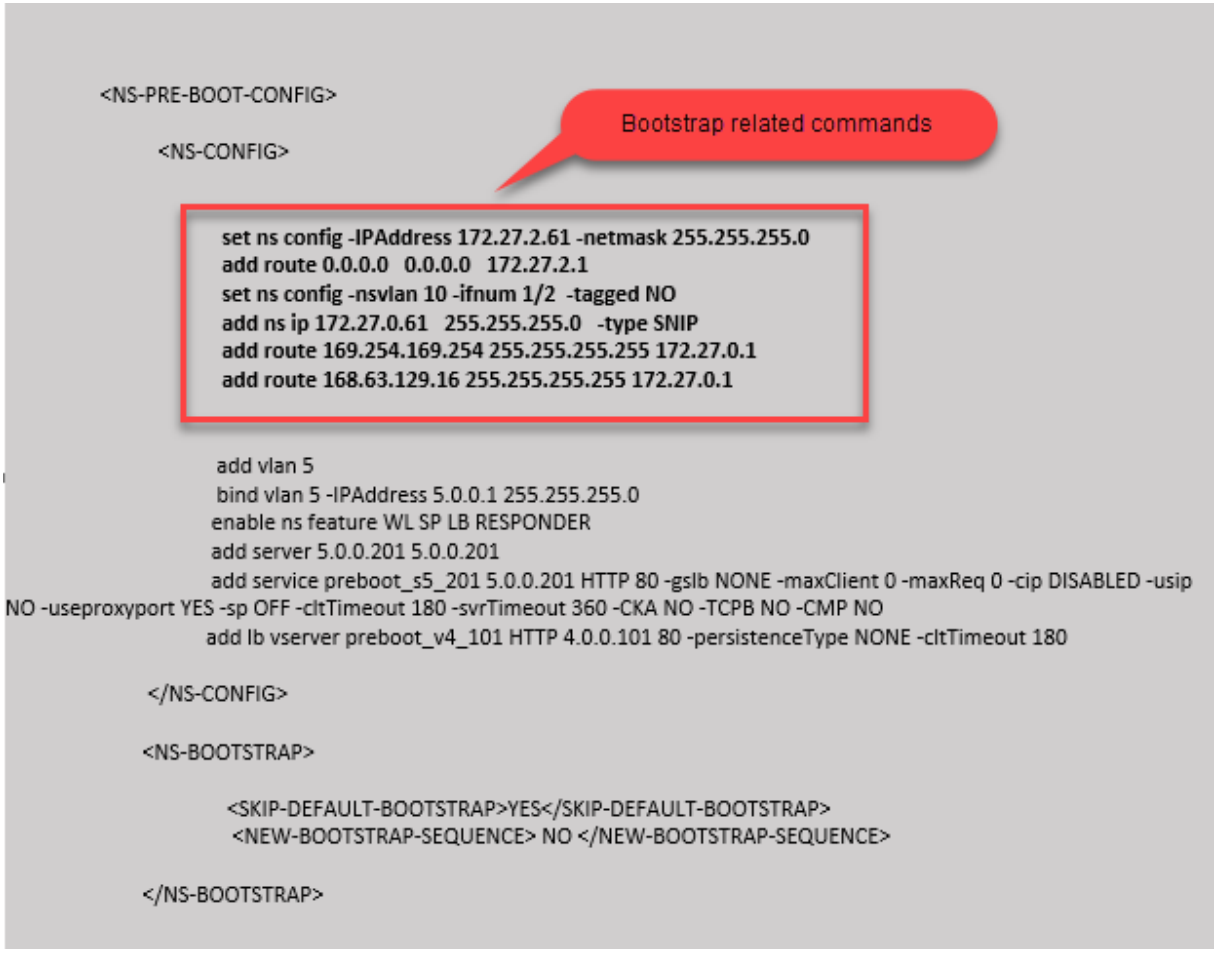


Exemple de bootstrap personnalisé pour Azure

Dans cet exemple, les commandes liées au bootstrap sont fournies dans la section <NS-CONFIG>. La section <NS-BOOTSTRAP> indique que le démarrage par défaut est ignoré et que les informations d'amorçage personnalisées fournies dans la section <NS-CONFIG> sont exécutées.

> Remarque :
>
> Pour le cloud Azure, le serveur de métadonnées d'instance (IMDS) et les serveurs DNS sont accessibles uniquement via l'interface principale (Eth0). Par conséquent, si l'interface Eth0 n'est

> pas utilisée comme interface de gestion (NSIP), l'interface Eth0 doit au moins être configurée comme SNIP pour l'accès IMDS ou DNS pour fonctionner. La route vers le point de terminaison IMDS (169.254.169.254) et le point de terminaison DNS (168.63.129.16) via la passerelle d'Eth0 doit également être ajoutée.




```
<NS-PRE-BOOT-CONFIG>

   <NS-CONFIG>

        set ns config -IPAddress 172.27.2.61 -netmask 255.255.255.0
        add route 0.0.0.0   0.0.0.0   172.27.2.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add ns ip 172.27.0.61   255.255.255.0   -type SNIP
        add route 169.254.169.254 255.255.255.255 172.27.0.1
        add route 168.63.129.16 255.255.255.255 172.27.0.1

        add vlan 5
        bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
        enable ns feature WL SP LB RESPONDER
```



```
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

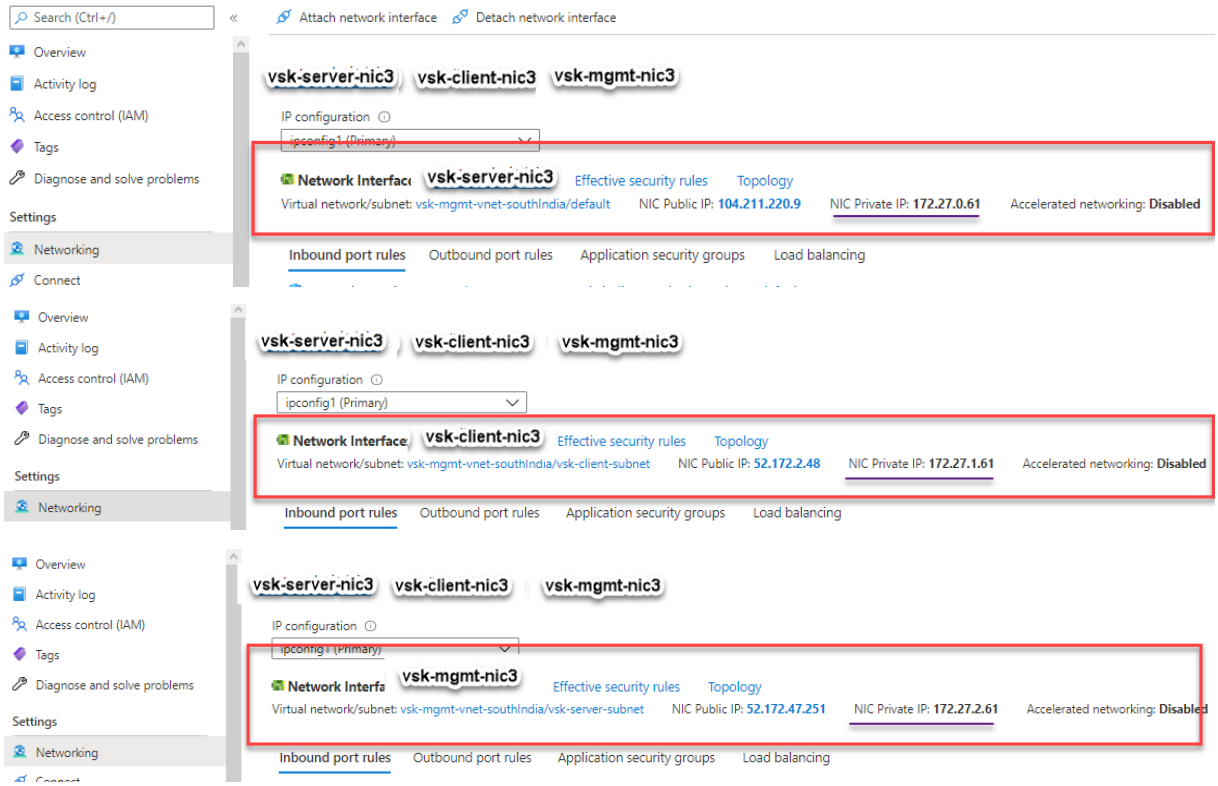
    <NS-BOOTSTRAP>

    <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
    <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>

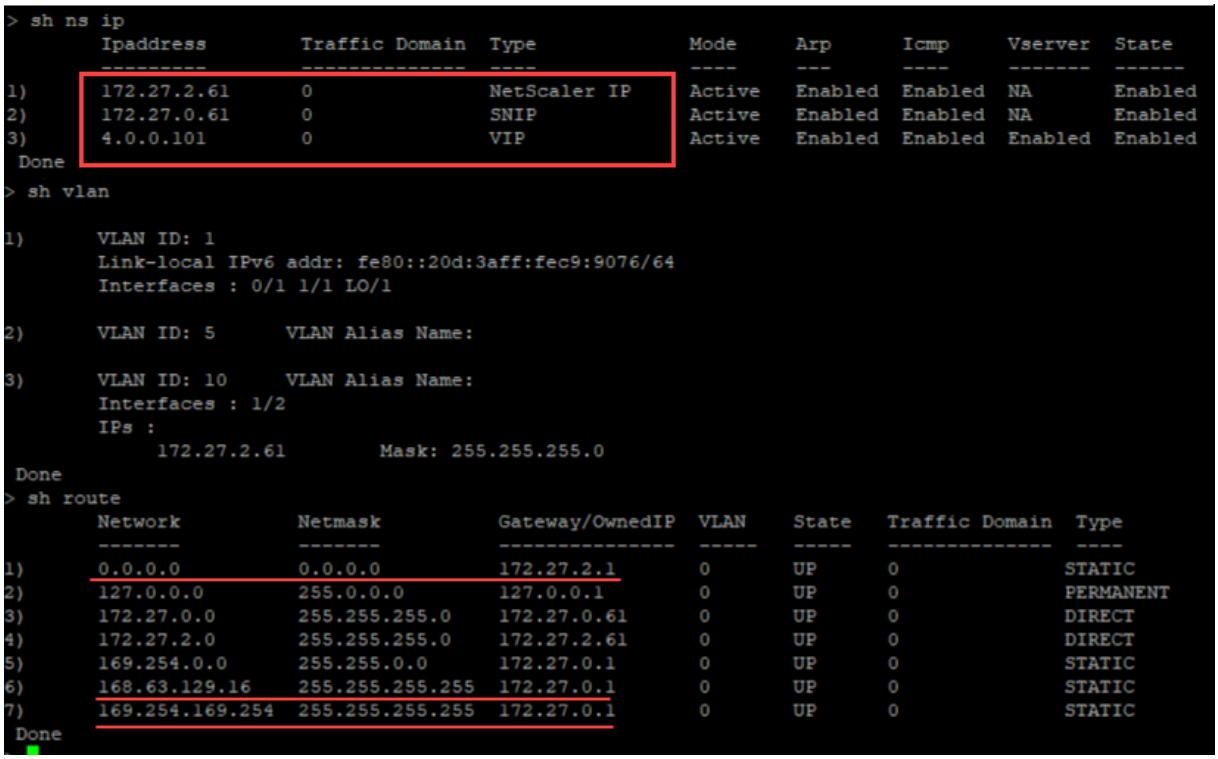
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Vous pouvez constater que l'instance Citrix ADC VPX est créée avec trois interfaces réseau. Accédez au **portail Azure > Instance de machine virtuelle > Mise en réseau**et vérifiez les propriétés réseau des trois cartes réseau, comme illustré dans les illustrations suivantes.

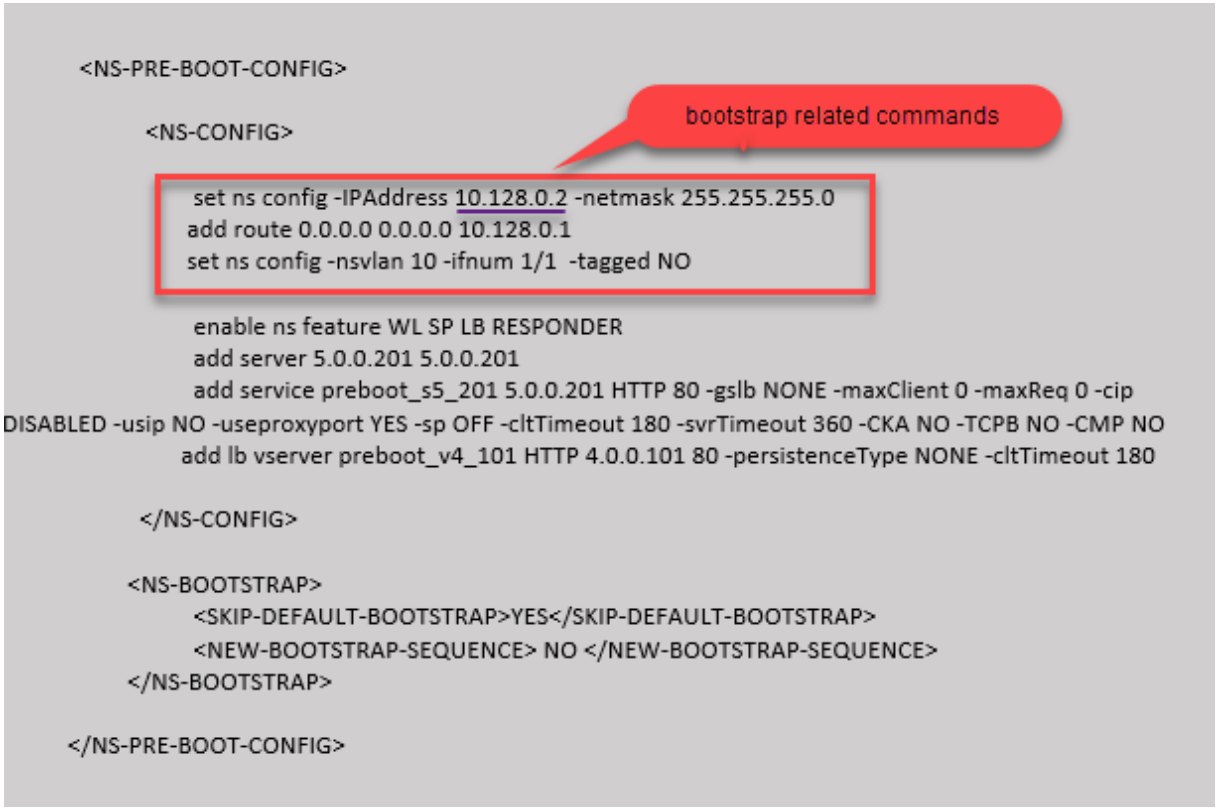


Vous pouvez exécuter la commande `show nsip` dans l'interface de ligne de commande ADC et vérifier que la nouvelle séquence d'amorçage spécifiée dans la section <NS-BOOTSTRAP> est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.



Exemple de bootstrap personnalisé pour GCP

Dans cet exemple, les commandes liées au bootstrap sont fournies dans la section <NS-CONFIG>. La section <NS-BOOTSTRAP> indique que le démarrage par défaut est ignoré et que les informations d'amorçage personnalisées fournies dans la section <NS-CONFIG> sont appliquées.



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>

        set ns config -IPAddress 10.128.0.2 -netmask 255.255.255.0
        add route 0.0.0.0 0.0.0.0 10.128.0.1
        set ns config -nsvlan 10 -ifnum 1/1  -tagged NO

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

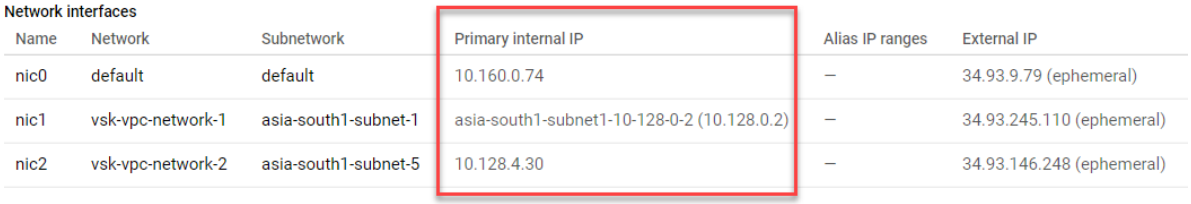
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
```



```
18          <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
19      </NS-BOOTSTRAP>
20
21  </NS-PRE-BOOT-CONFIG>
22  <!--NeedCopy-->
```

Une fois l'instance de machine virtuelle créée dans le portail GCP avec le bootstrap personnalisé, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

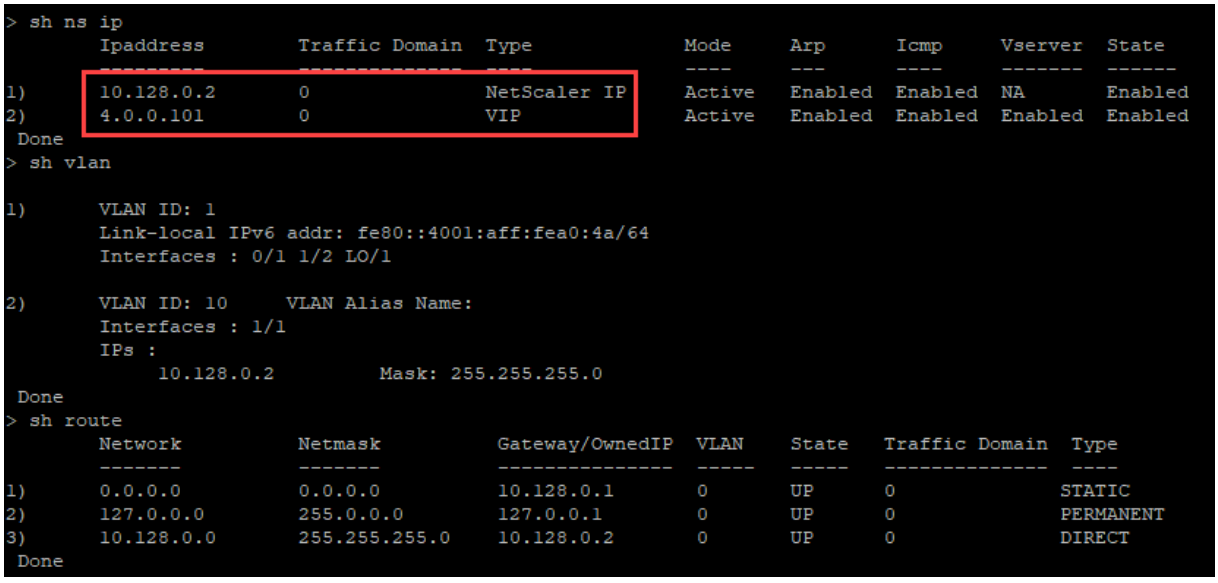
1. Sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Accédez aux propriétés de l'interface réseau et vérifiez les détails de la carte réseau, comme indiqué dans l'illustration.



Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP
nic0	default	default	10.160.0.74	–	34.93.9.79 (ephemeral)
nic1	vsk-vpc-network-1	asia-south1-subnet-1	asia-south1-subnet1-10-128-0-2 (10.128.0.2)	–	34.93.245.110 (ephemeral)
nic2	vsk-vpc-network-2	asia-south1-subnet-5	10.128.4.30	–	34.93.146.248 (ephemeral)

Vous pouvez exécuter la commande `show nsip` dans **ADC CLI**et vérifier que les configurations fournies dans la section `<NS-CONFIG>` précédente sont appliquées au premier démarrage de l'appliance ADC.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      10.128.0.2       0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::4001:aff:fea0:4a/64
        Interfaces : 0/1 1/2 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/1
        IPs :
             10.128.0.2         Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.128.0.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      10.128.0.0       255.255.255.0    10.128.0.2       0       UP      0               DIRECT
 Done
```

Impact de l'attachement et du détachement de cartes réseau dans AWS et Azure

AWS et Azure offrent la possibilité d'attacher une interface réseau à une instance et de détacher une interface réseau d'une instance. La fixation ou le détachement d'interfaces peuvent modifier la position

de l'interface. Citrix vous recommande donc de ne pas détacher les interfaces de l'instance ADC VPX. Si vous détachez ou attachez une interface lorsque le démarrage personnalisé est configuré, l'instance Citrix ADC VPX réattribue l'adresse IP principale de la nouvelle interface disponible dans la position de l'interface de gestion en tant que NSIP. Si aucune autre interface n'est disponible après celle que vous avez détachée, la première interface est alors l'interface de gestion de l'instance ADC VPX.

Par exemple, une instance Citrix ADC VPX est créée avec 3 interfaces : Eth0 (SNIP), Eth1 (NSIP) et Eth2 (VIP). Si vous détachez l'interface Eth1 de l'instance, qui est une interface de gestion, ADC configure la prochaine interface disponible (Eth2) comme interface de gestion. Ainsi, l'instance ADC VPX est toujours accessible via l'adresse IP principale de l'interface Eth2. Si Eth2 n'est pas non plus disponible, l'interface restante (Eth0) devient l'interface de gestion. Par conséquent, l'accès à l'instance ADC VPX continue d'exister.

Considérons une affectation différente des interfaces comme suit : Eth0 (SNIP), Eth1 (VIP) et Eth2 (NSIP). Si vous détachez Eth2 (NSIP), car aucune nouvelle interface n'est disponible après Eth2, la première interface (Eth0) devient l'interface de gestion.

Installer une instance Citrix ADC VPX sur un serveur nu

August 20, 2021

Un bare metal est un serveur physique entièrement dédié qui offre une isolation physique, entièrement intégré dans l'environnement cloud. Il est également connu sous le nom de serveur à locataire unique. La location unique vous permet d'éviter l'effet de voisin bruyant. Avec le métal nu, vous n'êtes pas témoin de l'effet voisin bruyant parce que vous êtes le seul utilisateur.

Un serveur nu installé avec un hyperviseur fournit une suite de gestion pour créer des machines virtuelles sur le serveur. L'hyperviseur n'exécute pas les applications nativement. Son but est de virtualiser vos charges de travail en machines virtuelles distinctes afin d'obtenir la flexibilité et la fiabilité de la virtualisation.

Conditions préalables à l'installation de l'instance Citrix ADC VPX sur des serveurs nus

Un serveur nue doit être obtenu auprès d'un fournisseur de cloud qui répond à toutes les exigences système requises pour l'hyperviseur concerné.

Installer l'instance Citrix ADC VPX sur des serveurs nus

Pour installer des instances Citrix ADC VPX sur un serveur nue, vous devez d'abord obtenir un serveur nue avec des ressources système adéquates auprès d'un fournisseur de cloud. Sur ce serveur nu,

tous les hyperviseurs pris en charge tels que Linux KVM, VMware ESX, Citrix Hypervisor ou Microsoft Hyper-V doivent être installés et configurés avant de déployer l'instance ADC VPX.

Pour plus d'informations sur la liste des différents hyperviseurs et fonctionnalités pris en charge sur une instance Citrix ADC VPX, consultez Matrice de support et directives d'utilisation.

Pour plus d'informations sur l'installation d'instances Citrix ADC VPX sur différents hyperviseurs, consultez la documentation correspondante.

- **Citrix Hypervisor :** voir Installer une instance Citrix ADC VPX sur Citrix Hypervisor.
- **VMware ESX :** voir Installer une instance Citrix ADC VPX sur VMware ESX.
- **Microsoft Hyper-V :** voir Installer une instance Citrix ADC VPX sur un serveur Microsoft Hyper-V.
- **Plateforme KVM Linux :** consultez Installer une instance Citrix ADC VPX sur la plate-forme Linux-KVM.

Installer une instance Citrix ADC VPX sur Citrix Hypervisor

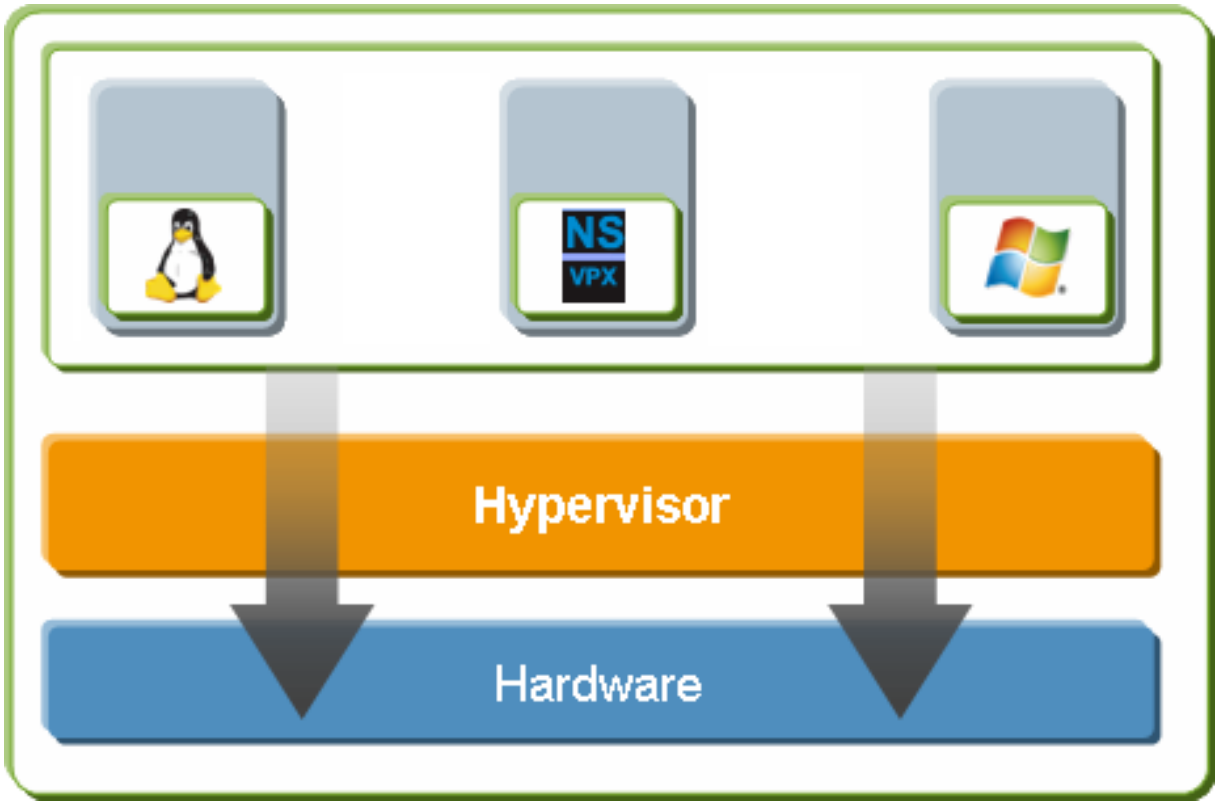
October 5, 2021

Pour installer des instances VPX sur Citrix Hypervisor, vous devez d'abord installer l'hyperviseur sur une machine disposant de ressources système adéquates. Pour effectuer l'installation de l'instance Citrix ADC VPX, vous utilisez Citrix XenCenter, qui doit être installé sur une machine distante pouvant se connecter à l'hôte de l'hyperviseur via le réseau.

Pour plus d'informations sur l'hyperviseur, consultez la documentation Citrix Hypervisor.

La figure suivante illustre l'architecture de solution bare-metal de l'instance Citrix ADC VPX sur l'hyperviseur.

figure. Une instance Citrix ADC VPX sur Citrix Hypervisor



Conditions préalables à l'installation d'une instance Citrix ADC VPX sur l'hyperviseur

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Installez Hypervisor version 6.0 ou ultérieure sur du matériel répondant à la configuration minimale requise.
- Installez XenCenter sur une station de travail de gestion qui répond à la configuration système minimale requise.
- Obtenez les fichiers de licence du dispositif virtuel. Pour plus d'informations sur les licences de dispositifs virtuels, reportez-vous au *Guide des licences Citrix ADC VPX* à l'adresse http://support.citrix.com/article/ctx122426.

Configuration matérielle requise pour l'hyperviseur

Le tableau suivant décrit la configuration matérielle minimale requise pour une plate-forme Hypervisor exécutant une instance Citrix ADC VPX.

Tableau 1. Configuration système minimale requise pour l'hyperviseur exécutant une instance VPX nCore

Composant	Exigences
UC	2 processeurs x86 64 bits ou plus avec assistance à la virtualisation (Intel-VT) activée. Pour exécuter l'instance Citrix ADC VPX, la prise en charge matérielle de la virtualisation doit être activée sur l'hôte Hypervisor. Assurez-vous que l'option BIOS pour la prise en charge de la virtualisation n'est pas désactivée. Pour plus de détails, consultez la documentation du BIOS. À partir de la version 13.1 de Citrix ADC, l'instance Citrix ADC VPX sur l'hyperviseur VMware ESXi prend en charge les processeurs AMD.
RAM	3 Go
Espace disque	Stockage connecté localement (PATA, SATA, SCSI) avec 40 Go d'espace disque. Remarque : L'installation de l'hyperviseur crée une partition de 4 Go pour le domaine de contrôle de l'hôte de l'hyperviseur. L'espace restant est disponible pour l'instance Citrix ADC VPX et d'autres machines virtuelles.
CARTE RÉSEAU	Une carte réseau 1 Gbit/s ; recommandé : deux cartes réseau 1 Gbit/s

Pour plus d'informations sur l'installation de l'hyperviseur, consultez la documentation sur l'hyperviseur à l'adresse http://support.citrix.com/product/xens/.

Le tableau suivant répertorie les ressources informatiques virtuelles que l'hyperviseur doit fournir pour chaque dispositif virtuel VPX nCore.

Tableau 2. Ressources informatiques virtuelles minimales requises pour exécuter une instance nCore VPX

Composant	Exigences
Mémoire	2 Go
Processeur virtuel	2
Interfaces réseau virtuelles	2

> Remarque : Pour une utilisation en production de l'instance
> Citrix ADC VPX, Citrix recommande que la priorité du processeur (dans les propriétés de la machine virtuelle) soit définie au niveau le plus élevé, afin d'améliorer le comportement de planification et la latence du réseau.

Configuration système requise pour XenCenter

XenCenter est une application cliente Windows. Il ne peut pas être exécuté sur la même machine que l'hôte de l'hyperviseur. Pour plus d'informations sur la configuration système minimale requise et l'installation de XenCenter, consultez les documents Hypervisor suivants :

- Configuration système requise
- Installation

Installez les instances Citrix ADC VPX sur l'hyperviseur à l'aide de XenCenter

Après avoir installé et configuré Hypervisor et XenCenter, vous pouvez utiliser XenCenter pour installer des dispositifs virtuels sur l'hyperviseur. Le nombre de dispositifs virtuels que vous pouvez installer dépend de la quantité de mémoire disponible sur le matériel qui exécute l'hyperviseur.

Après avoir utilisé XenCenter pour installer l'instance Citrix ADC VPX initiale (image .xva) sur l'hyperviseur, vous pouvez utiliser le Command Center pour provisionner l'instance Citrix ADC VPX. Pour plus d'informations, consultez la documentation Command Center .

Pour installer des instances Citrix ADC VPX sur l'hyperviseur à l'aide de XenCenter, procédez comme suit :

1. Démarrez XenCenter sur votre poste de travail.
2. Dans le menu Serveur, cliquez sur Ajouter .
3. Dans la boîte de dialogue Ajouter un nouveau serveur, dans la zone de texte Nom d'hôte, tapez l'adresse IP ou le nom DNS de l'hyperviseur auquel vous souhaitez vous connecter.
4. Dans les zones de texte Nom d'utilisateur et Mot de passe, tapez les informations d'identification de l'administrateur, puis cliquez sur Connexion. Le nom de l'hyperviseur apparaît dans le volet de navigation avec un cercle vert, ce qui indique que l'hyperviseur est connecté.
5. Dans le volet de navigation, cliquez sur le nom de l'hyperviseur sur lequel vous souhaitez installer l'instance Citrix ADC VPX.
6. Dans le menu VM, cliquez sur Importer .
7. Dans la boîte de dialogue Importer, dans le nom du fichier d'importation, accédez à l'emplacement où vous avez enregistré le fichier image .xva de l'instance Citrix ADC VPX. Assurez-vous que l'option VM exportée est sélectionnée, puis cliquez sur Suivant.

8. Sélectionnez l'hyperviseur sur lequel vous souhaitez installer le dispositif virtuel, puis cliquez sur Suivant.
9. Sélectionnez le référentiel de stockage local dans lequel stocker le dispositif virtuel, puis cliquez sur Importer pour commencer le processus d'importation.
10. Vous pouvez ajouter, modifier ou supprimer les interfaces réseau virtuelles si nécessaire. Lorsque vous avez terminé, cliquez sur Suivant.
11. Cliquez sur Terminer pour terminer le processus d'importation.

    Remarque : Pour afficher l'état du processus d'importation, cliquez sur l'onglet **Journal** .
12. Si vous souhaitez installer un autre dispositif virtuel, répétez les étapes 5 à 11.

> **Remarque**
>
> Après la configuration initiale de l'instance VPX, si vous souhaitez mettre à niveau l'appliance vers la dernière version logicielle, reportez-vous à la section Mise à niveau ou rétrogradation du logiciel système.

Configurer les instances VPX pour utiliser des interfaces réseau de virtualisation d'E/S à racine unique (SR-IOV)

August 20, 2021

Après avoir installé et configuré une instance Citrix ADC VPX sur XenServer, vous pouvez configurer l'appliance virtuelle pour qu'elle utilise des interfaces réseau SR-IOV.

Limitations

XenServer ne prend pas en charge les fonctionnalités suivantes sur les interfaces SRIOV :

- Commutation de mode L2
- Mise en cluster
- Partitionnement d'administrateur [mode VLAN partagé]
- Haute disponibilité [Actif - Mode actif]
- Cadres Jumbo
- Protocole IPv6 dans un environnement de cluster

Conditions préalables

Sur l'hôte XenServer, assurez-vous que vous :

- Ajoutez la carte réseau (NIC) Intel 82599 à l'hôte.
- Bloquez la liste du `ixgbevf` pilote en ajoutant l'entrée suivante au fichier **/etc/modprobe.d/blacklist.conf** :

  liste noire ixgbevf
- Activez SR-IOV Virtual Functions (VFS) en ajoutant l'entrée suivante au fichier **/etc/modprobe.d/ixgbe** :

  options ixgbe max_vfs=* <number_of_VFs>*

  où **<number_VFs> est le nombre de VF SR-IOV que vous souhaitez créer.
- Vérifiez que SR-IOV est activé dans le BIOS.

La version 3.22.3 du pilote IXGBE est recommandée.

Attribuer des VF SR-IOV à l'instance VPX à l'aide de l'hôte XenServer

Pour affecter des interfaces réseau SR-IOV à l'instance Citrix ADC VPX, procédez comme suit :

1. Sur l'hôte XenServer, utilisez la commande suivante pour affecter les VF SR-IOV à l'instance Citrix ADC VPX :

   xe host-call-plugin plugin=iovirt host-uuid=*<Xen host UUID>* **fn=assign_free_vf args:uuid**=*<Netscalar VM UUID>* **args:ethdev**=*<interface name>* **args:mac=***<Mac addr>*

   Où :

   - *<Xen host UUID>* est l'UUID de l'hôte XenServer.
   - *<NetScaler VM UUID>* est l'UUID de l'instance Citrix ADC VPX.
   - *<interface name>* est l'interface des VF SR-IOV.
   - *<MAC address >* est l'adresse MAC du SR-IOV VF.

   > **Remarque**
   >
   > Spécifiez l'adresse MAC que vous souhaitez utiliser dans le paramètre Args:Mac=. S'il n'est pas spécifié, le `iovirt` script génère et attribue une adresse MAC de manière aléatoire. De plus, si vous souhaitez utiliser les VF SR-IOV en mode Agrégation de liens, assurez-vous de spécifier l'adresse MAC 00:00:00:00.
2. Démarrez l'instance Citrix ADC VPX.

Annuler l'affectation de VF SR-IOV à l'instance VPX à l'aide de l'hôte XenServer

Si vous avez attribué un VF SR-IOV incorrect ou si vous souhaitez modifier un VF SR-IOV assigné, vous devez annuler l'attribution et réaffecter les VF SR-IOV à l'instance Citrix ADC VPX.

Pour annuler l'affectation de l'interface réseau SR-IOV affectée à une instance Citrix ADC VPX, procédez comme suit :

1. Sur l'hôte XenServer, utilisez la commande suivante pour affecter les VF SR-IOV à l'instance Citrix ADC VPX et redémarrez l'instance Citrix ADC VPX :

   xe host-call-plugin plugin<Netscalar_VM_UUID> =iovirt **host-uuid=<Xen_host_UUID>fn=**unassign_al**

   Où :

   - **<Xen_host_UUID>- UUID de l'hôte XenServer.
   - *<Netscalar_VM_UUID>* - L'UUID de l'instance Citrix ADC VPX

2. Démarrez l'instance Citrix ADC VPX.

Configuration du VLAN sur l'interface SR-IOV

> **Important**
>
> Lorsque vous affectez les VF SR-IOV à l'instance Citrix ADC VPX, assurez-vous que vous spécifiez l'adresse MAC 00:00:00:00:00:00 pour les VFS.

Pour utiliser les fonctions virtuelles SR-IOV en mode d'agrégation de liens, vous devez désactiver la vérification d'usurpation des fonctions virtuelles que vous avez créées. Sur l'hôte XenServer, utilisez la commande suivante pour désactiver la vérification d'usurpation :

ip link set <*interface_name*> **vf** <*VF_id*> **spoofchk** off

Où :

- <interface_name>est le nom de l'interface.
- <VF_id>est l'ID de la fonction virtuelle.

Après avoir désactivé la vérification d'usurpation pour toutes les fonctions virtuelles que vous avez créées, redémarrez l'instance Citrix ADC VPX et configurez l'agrégation des liens. Pour obtenir des instructions, voir Configurer l'agrégation de liens.

Configurer VLAN sur l'interface SR-IOV

Vous pouvez configurer VLAN sur les fonctions virtuelles SR-IOV. Pour obtenir des instructions, reportez-vous à la section Configuration d'un VLAN.

> **Important**
>
> Assurez-vous que l'hôte XenServer ne contient pas de paramètres VLAN pour l'interface VF.

Installer une instance Citrix ADC VPX sur VMware ESX

October 5, 2021

Avant d'installer les instances Citrix ADC VPX sur VMware ESX, assurez-vous que VMware ESX Server est installé sur une machine disposant de ressources système adéquates. Pour installer une instance Citrix ADC VPX sur VMware ESXi, vous utilisez le client VMware vSphere. Le client ou l'outil doit être installé sur une machine distante pouvant se connecter à VMware ESX via le réseau.

Cette section inclut les rubriques suivantes :

- Conditions préalables
- Installation d'une instance Citrix ADC VPX sur VMware ESX

> **Important**
>
> Vous ne pouvez pas installer VMware Tools standard ni mettre à niveau la version de VMware Tools disponible sur une instance Citrix ADC VPX. Les outils VMware pour une instance Citrix ADC VPX sont fournis dans le cadre de la version du logiciel Citrix ADC.

Conditions préalables

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Installez VMware ESX sur du matériel qui répond à la configuration minimale requise.
- Installez VMware Client sur une station de travail de gestion qui répond à la configuration système minimale requise.
- Téléchargez les fichiers de configuration de l'appliance Citrix ADC VPX.
- Étiquetez les ports réseau physiques de VMware ESX.
- Obtenir des fichiers de licence VPX. Pour plus d'informations sur les licences d'instance Citrix ADC VPX, consultez le *Guide des licences Citrix ADC VPX* à l'adresse http://support.citrix.com/article/ctx131110.

Configuration matérielle requise pour VMware ESX

Le tableau suivant décrit la configuration système minimale requise pour les serveurs VMware ESX exécutant Citrix ADC VPX nCore Virtual Appliance.

Tableau 1. Configuration système minimale requise pour un serveur VMware ESX exécutant une instance Citrix ADC VPX

Composant	Exigences
-	2 processeurs x86 64 bits ou plus avec assistance à la virtualisation (Intel-VT) activée. Pour exécuter l'instance Citrix ADC VPX, la prise en charge matérielle de la virtualisation doit être activée sur l'hôte VMware ESX. Assurez-vous que l'option BIOS pour la prise en charge de la virtualisation n'est pas désactivée. Pour plus d'informations, consultez la documentation de votre BIOS.
RAM	3 Go
Espace disque	40 Go d'espace disque disponible
Réseau	Une carte réseau (NIC) 1 Gbit/s ; deux cartes réseau 1 Gbit/s recommandées

Pour plus d'informations sur l'installation de VMware ESX, reportez-vous à la section http://www.vmware.com/.

Le tableau suivant répertorie les ressources informatiques virtuelles que le serveur VMware ESX doit fournir pour chaque appliance virtuelle VPX nCore.

Tableau 2. Ressources de calcul virtuel minimales requises pour exécuter une instance Citrix ADC VPX

Composant	Exigences
Mémoire	4 Go
Processeur virtuel	2
Interfaces réseau virtuelles	1. Dans ESX, vous pouvez installer un maximum de 10 interfaces réseau virtuelles si le matériel VPX est mis à niveau vers la version 7 ou supérieure.
Espace disque	20 Go

> Remarque
>
> Ceci s'ajoute à toutes les exigences de disque pour l'Hypervisor.

Pour une utilisation en production du dispositif virtuel VPX, l'allocation de mémoire complète doit être réservée. Des cycles de processeur (en MHz) égaux au moins à la vitesse d'un cœur de processeur

de l'ESX doivent être réservés.

Configuration système requise pour VMware vSphere Client

VMware vSphere est une application cliente qui peut s'exécuter sur les systèmes d'exploitation Windows et Linux. Il ne peut pas s'exécuter sur la même machine que le serveur VMware ESX. Le tableau suivant décrit la configuration minimale requise.

Tableau 3. Configuration système minimale requise pour l'installation de VMware vSphere Client

Composant	Exigences
Système d'exploitation	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « Matrices de compatibilité vSphere » à l'adresse http://kb.vmware.com/.
UC	750 MHz ; 1 gigahertz (GHz) ou plus rapide recommandé
RAM	1 Go ; 2 Go recommandés
NIC (NICE)	Carte réseau 100 Mbit/s ou plus rapide

Configuration système requise pour OVF Tool 1.0

OVF Tool est une application cliente qui peut s'exécuter sur les systèmes Windows et Linux. Il ne peut pas s'exécuter sur la même machine que le serveur VMware ESX. Le tableau suivant décrit la configuration minimale requise.

Tableau 4. Configuration minimale requise pour l'installation d'outils OVF

Composant	Exigences
Système d'exploitation	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.
UC	750 MHz minimum, 1 GHz ou plus rapide recommandé
RAM	1 Go minimum, 2 Go recommandés
NIC (NICE)	Carte réseau 100 Mbit/s ou plus rapide

Pour plus d'informations sur l'installation d'OVF, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.

Téléchargement des fichiers d'installation Citrix ADC VPX

Le package de configuration d'instance Citrix ADC VPX pour VMware ESX respecte la norme de format Open Virtual Machine (OVF). Vous pouvez télécharger les fichiers depuis le site Web de Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l' adresse http://www.citrix.com, cliquez sur le **lien Nouveaux utilisateurs**et suivez les instructions pour créer un nouveau compte Citrix.

Une fois connecté, naviguez dans le chemin suivant à partir de la page d'accueil Citrix :

Citrix.com > **Téléchargements > Citrix ADC > Appliances virtuelles**.

Copiez les fichiers suivants sur une station de travail située sur le même réseau que le serveur ESX. Copiez les trois fichiers dans le même dossier.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (par exemple, NSVPX-ESX-13.0-71.44_NC_64-Disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (par exemple, NSVPX-ESX-13.0-71.44_NC_64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (par exemple, NSVPX-ESX-13.0-71.44_NC_64.mf)

Étiqueter les ports réseau physiques de VMware ESX

Avant d'installer un dispositif virtuel VPX, étiquetez toutes les interfaces que vous prévoyez d'attribuer aux dispositifs virtuels, dans un format unique, par exemple, NS_NIC_1_1, NS_NIC_1_2, etc. Dans les grands déploiements, l'étiquetage dans un format unique permet d'identifier rapidement les interfaces allouées à l'appliance virtuelle VPX parmi les autres interfaces utilisées par d'autres machines virtuelles, telles que Windows et Linux. Un tel étiquetage est particulièrement important lorsque différents types de machines virtuelles partagent des interfaces.

Pour étiqueter les ports réseau physiques du serveur VMware ESX, procédez comme suit :

1. Ouvrez une session sur le serveur VMware ESX à l'aide du client vSphere.
2. Dans vSphere Client, sélectionnez l'onglet Configuration, puis cliquez sur Mise en réseau.
3. Dans le coin supérieur droit, cliquez sur Ajouter un réseau.
4. Dans l'Assistant Ajout d'un réseau, pour **Type de connexion**, sélectionnez **Machine virtuelle**, puis cliquez sur Suivant.
5. Parcourez la liste des adaptateurs physiques vSwitch et choisissez le port physique qui correspond à l'interface 1/1 sur les dispositifs virtuels.
6. Entrez l'étiquette de l'interface, par exemple, **NS_NIC_1_1** comme nom du vSwitch associé à l'interface 1/1 des dispositifs virtuels.

7. Cliquez sur Suivant pour terminer la création du vSwitch. Répétez la procédure, en commençant par l'étape 2, pour ajouter toute interface supplémentaire à utiliser par vos dispositifs virtuels. Étiquetez les interfaces de manière séquentielle, dans le format approprié (par exemple, NS_NIC_1_2).

Installer une instance Citrix ADC VPX sur VMware ESX

Après avoir installé et configuré VMware ESX, vous pouvez utiliser le client VMware vSphere pour installer des dispositifs virtuels sur le serveur VMware ESX. Le nombre de dispositifs virtuels que vous pouvez installer dépend de la quantité de mémoire disponible sur le matériel qui exécute VMware ESX.

Pour installer des instances Citrix ADC VPX sur VMware ESX à l'aide de VMware vSphere Client, procédez comme suit :

1. Démarrez le client VMware vSphere sur votre station de travail.
2. Dans la zone de texte **Adresse IP/Nom**, tapez l'adresse IP du serveur VMware ESX auquel vous souhaitez vous connecter.
3. Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur, puis cliquez sur Connexion.
4. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.
5. Dans la boîte de dialogue **Déployer un modèle OVF**, dans **Déployer à partir d'un fichier**, accédez à l'emplacement où vous avez enregistré les fichiers de configuration de l'instance Citrix ADC VPX, sélectionnez le fichier .ovf, puis cliquez sur **Suivant**.
6. Mappez les réseaux affichés dans le modèle OVF du dispositif virtuel aux réseaux que vous avez configurés sur l'hôte ESX. Cliquez sur **Suivant** pour commencer à installer un dispositif virtuel sur VMware ESX. Une fois l'installation terminée, une fenêtre contextuelle vous informe de la réussite de l'installation.
7. Vous êtes maintenant prêt à démarrer l'instance Citrix ADC VPX. Dans le volet de navigation, sélectionnez l'instance Citrix ADC VPX que vous avez installée et, dans le menu contextuel, sélectionnez Mettre **sous tension**. Cliquez sur l'onglet **Console** pour émuler un port de console.
8. Si vous souhaitez installer un autre dispositif virtuel, répétez l'étape 6.

> **Remarque**
>
> Par défaut, l'instance Citrix ADC VPX utilise des interfaces réseau E1000.
>
> Après l'installation, vous pouvez utiliser vSphere client ou vSphere Web Client pour gérer les appliances virtuelles sur VMware ESX.
>
> Pour que la fonctionnalité de balisage VLAN fonctionne, sur VMware ESX, définissez l'ID VLAN du groupe de ports sur All (4095) sur le vSwitch du serveur VMware ESX. Pour plus d'informations sur la définition d'un ID VLAN sur le vSwitch de VMware ESX server, reportez-vous à la section

> http://www.vmware.com/pdf/esx3_vlan_wp.pdf.

Migration d'une instance Citrix ADC VPX à l'aide de VMware vMotion

Vous pouvez migrer une instance Citrix ADC VPX à l'aide de VMware vSphere vMotion.

Suivez ces instructions d'utilisation :

- VMware ne prend pas en charge la fonctionnalité VMotion sur les machines virtuelles configurées avec les interfaces PCI Passthrough et SR-IOV.
- Les interfaces prises en charge sont E1000 et VMXNET3. Pour utiliser vMotion sur votre instance VPX, assurez-vous que l'instance est configurée avec une interface prise en charge.
- Pour plus d'informations sur la façon de migrer une instance à l'aide de VMware VMotion, consultez la documentation VMware.

Configurer une instance Citrix ADC VPX pour utiliser l'interface réseau VMXNET3

August 20, 2021

Après avoir installé et configuré l'instance Citrix ADC VPX sur VMware ESX, vous pouvez utiliser le client Web VMware vSphere pour configurer l'appliance virtuelle de manière à utiliser les interfaces réseau VMXNET3.

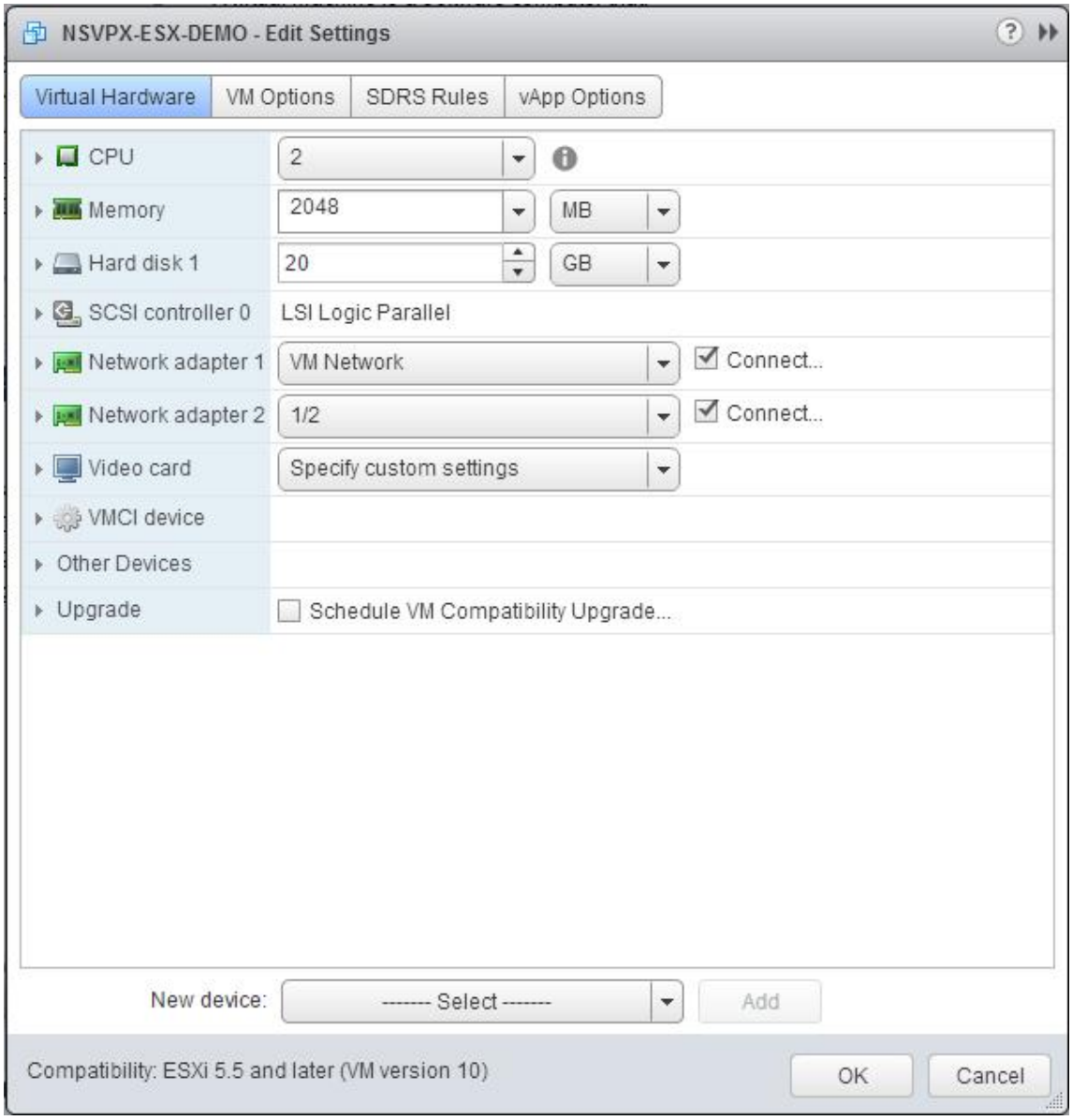
Pour configurer les instances Citrix ADC VPX de manière à utiliser les interfaces réseau VMXNET3 à l'aide de VMware vSphere Web Client :

1. Dans vSphere Web Client, sélectionnez Hôtes et clusters.
2. Mettez à niveau le paramètre de compatibilité de l'instance Citrix ADC VPX vers ESX, comme suit :

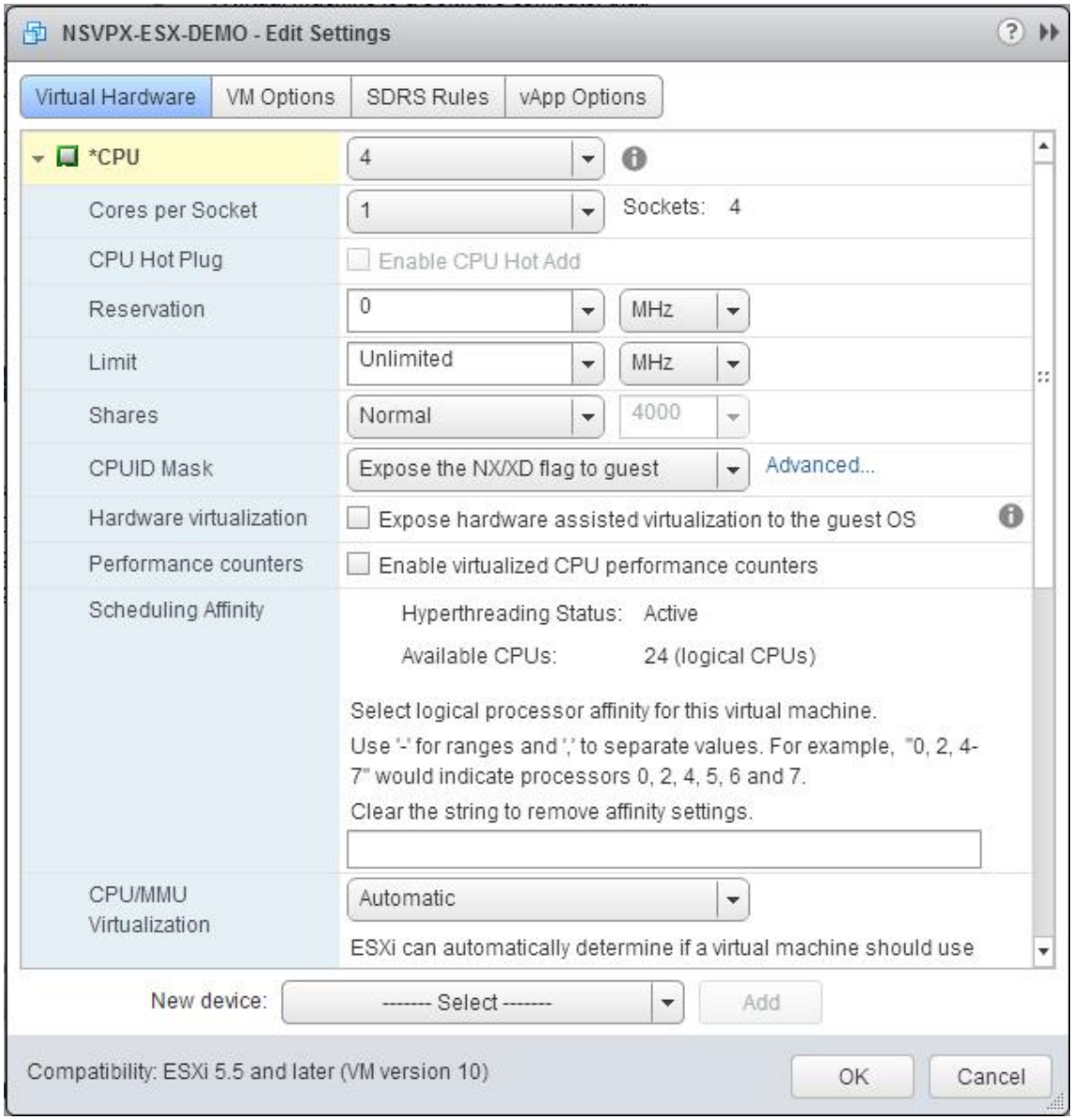
   a. Mettez hors tension l'instance Citrix ADC VPX.

   b. Cliquez avec le bouton droit de la souris sur l'instance Citrix ADC VPX et sélectionnez Compatibilité > Mettre à niveau la compatibilité des machines virtuelles.

   c. Dans la boîte de dialogue Configurer la compatibilité des machines virtuelles, sélectionnez ESXi 5.5 et versions ultérieures dans la liste déroulante Compatible avec, puis cliquez sur OK.
3. Cliquez avec le bouton droit de la souris sur l'instance Citrix ADC VPX et cliquez sur Modifier les paramètres.



4. Dans la boîte de dialogue <virtual_appliance> - Edit Settings, cliquez sur la section CPU.



5. Dans la section CPU, mettez à jour les éléments suivants :

   - Nombre de processeurs
   - Nombre de sockets
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

   a. Dans la liste déroulante CPU, sélectionnez le nombre de CPU à affecter à l'appliance virtuelle.

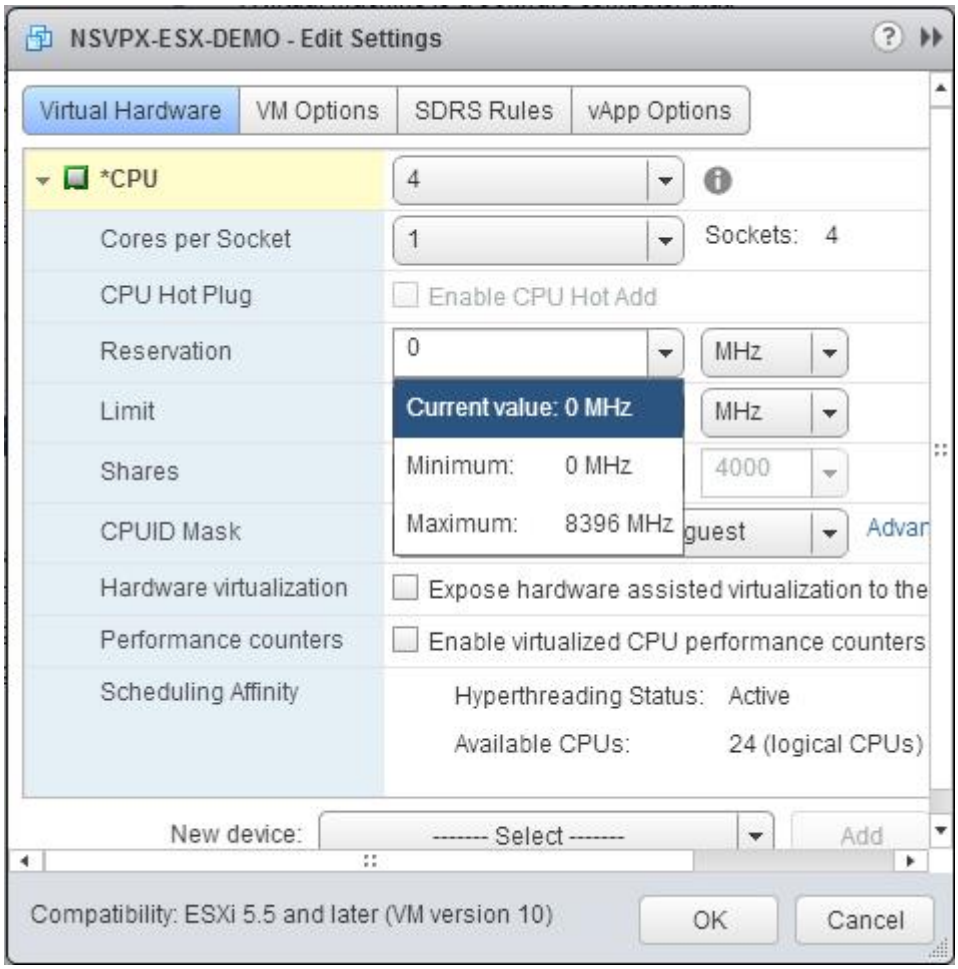
   b. Dans la liste déroulante Cœurs par socket, sélectionnez le nombre de sockets.

   c. (Facultatif) Dans le champ CPU Hot Plug, activez ou désactivez la case à cocher Activer l'ajout

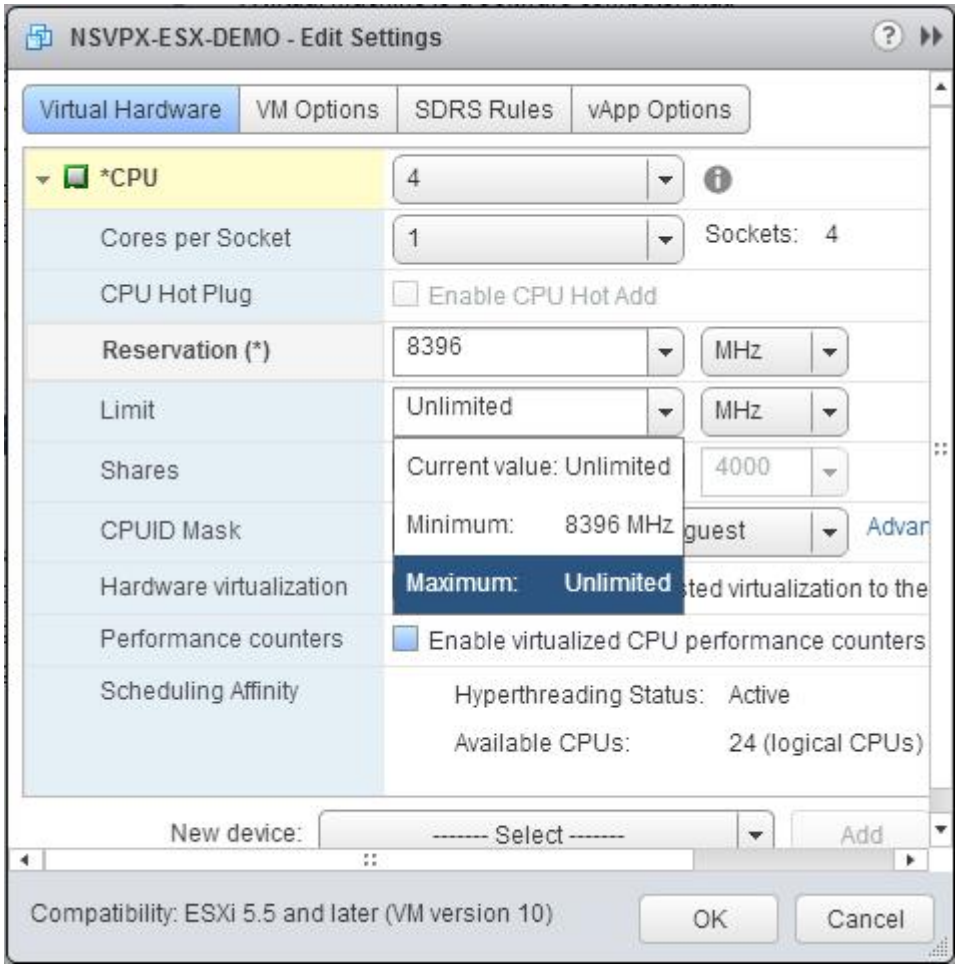
à chaud du processeur.

Remarque : Citrix recommande d'accepter la valeur par défaut (désactivée).

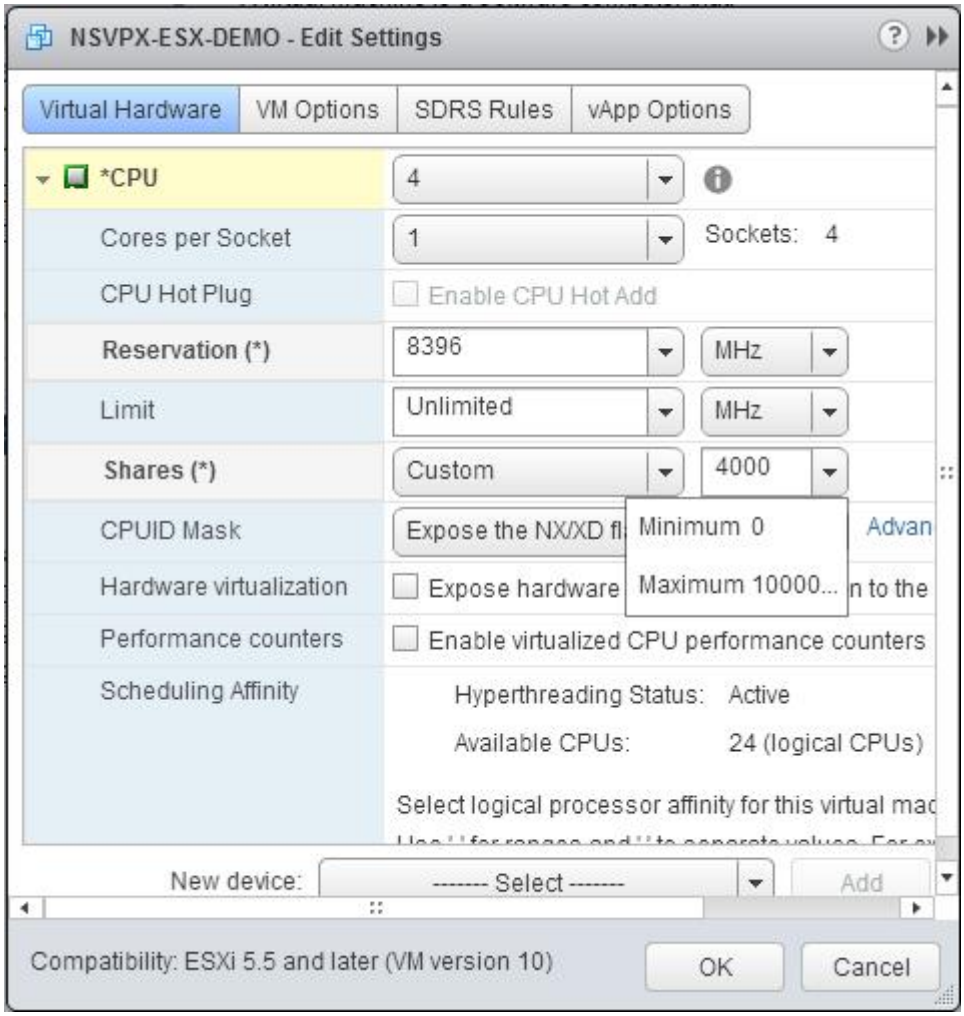
d. Dans la liste déroulante Réservation, sélectionnez le nombre qui est affiché comme valeur maximale.



e. Dans la liste déroulante Limite, sélectionnez le nombre affiché comme valeur maximale.



f. Dans les listes déroulantes Parts, sélectionnez Personnalisé et le nombre affiché comme valeur maximale.



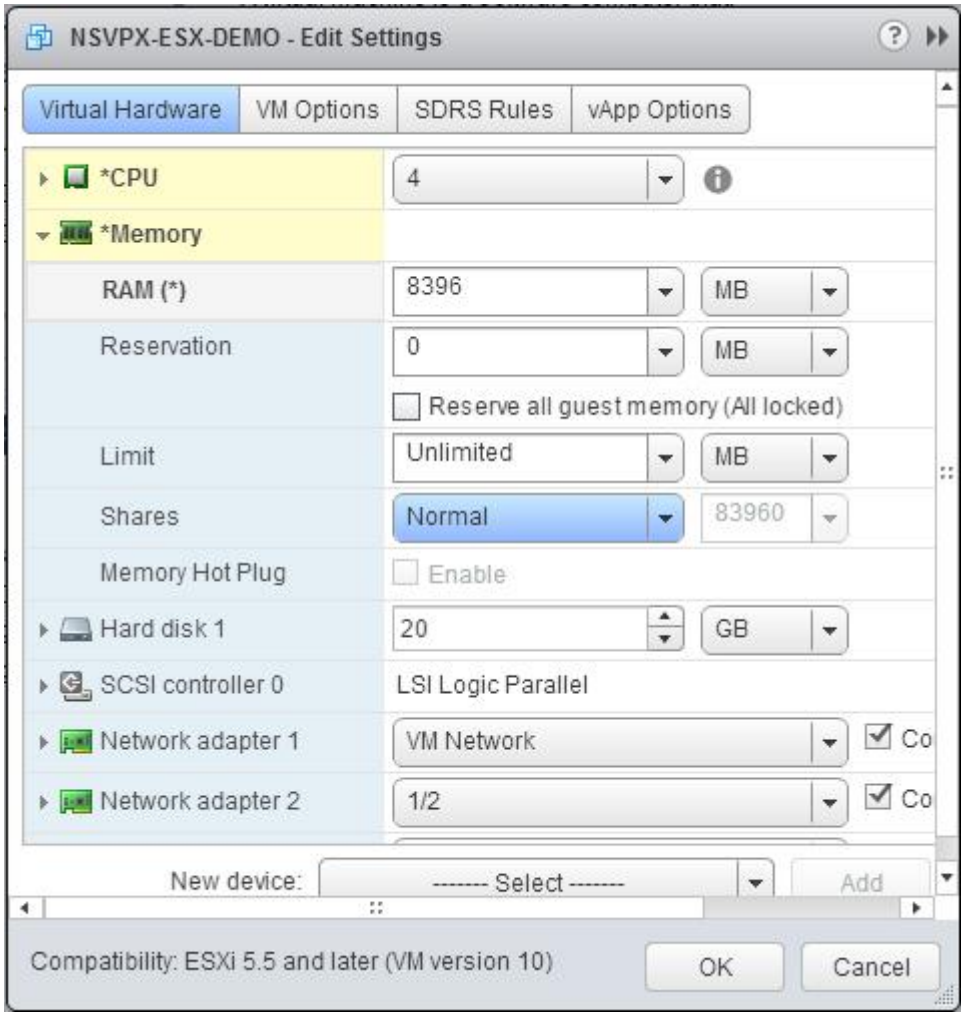
6. Dans la section Mémoire, mettez à jour les éléments suivants :

   - Taille de la RAM
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

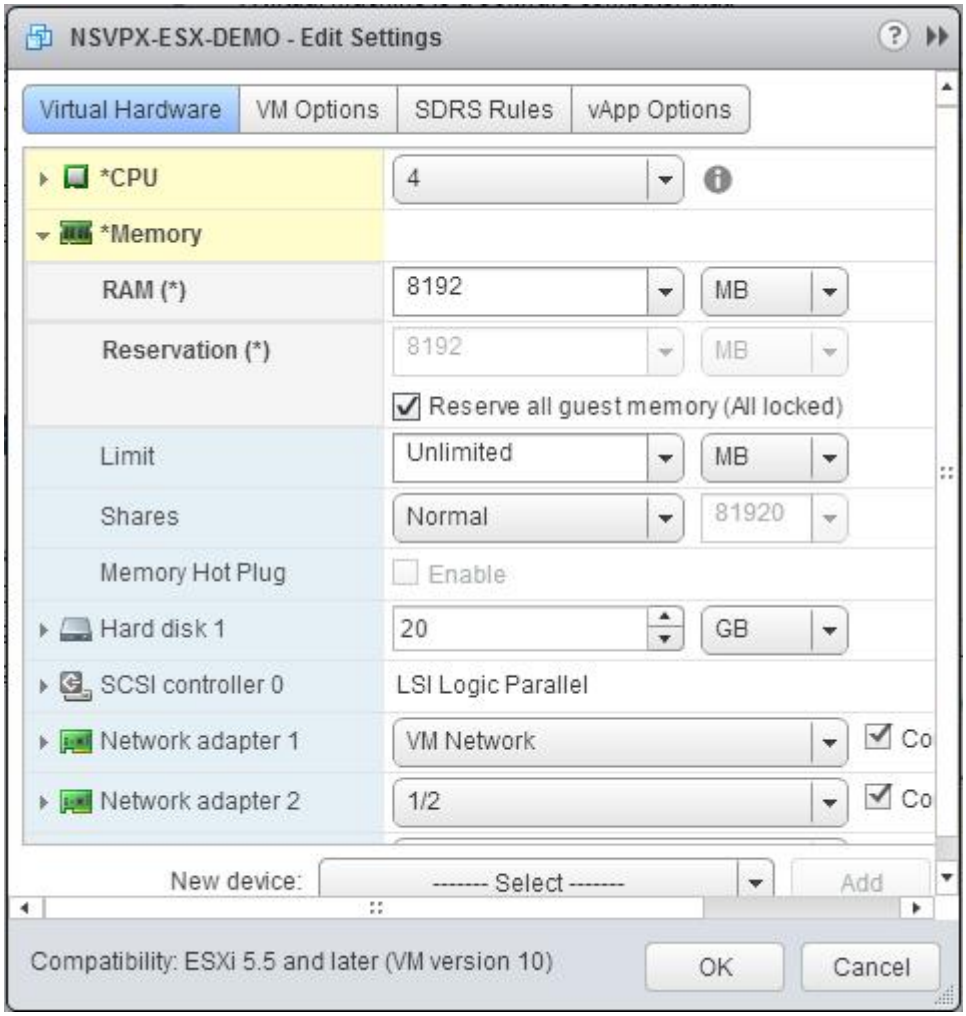
   a. Dans la liste déroulante RAM, sélectionnez la taille de la RAM. Il doit s'agir du nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de processeurs virtuels est de 4, la RAM doit être de 4 x 2 Go = 8 Go.

   Remarque : pour une édition avancée ou Premium de l'appliance Citrix ADC VPX, assurez-vous d'allouer 4 Go de RAM à chaque vCPU. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.

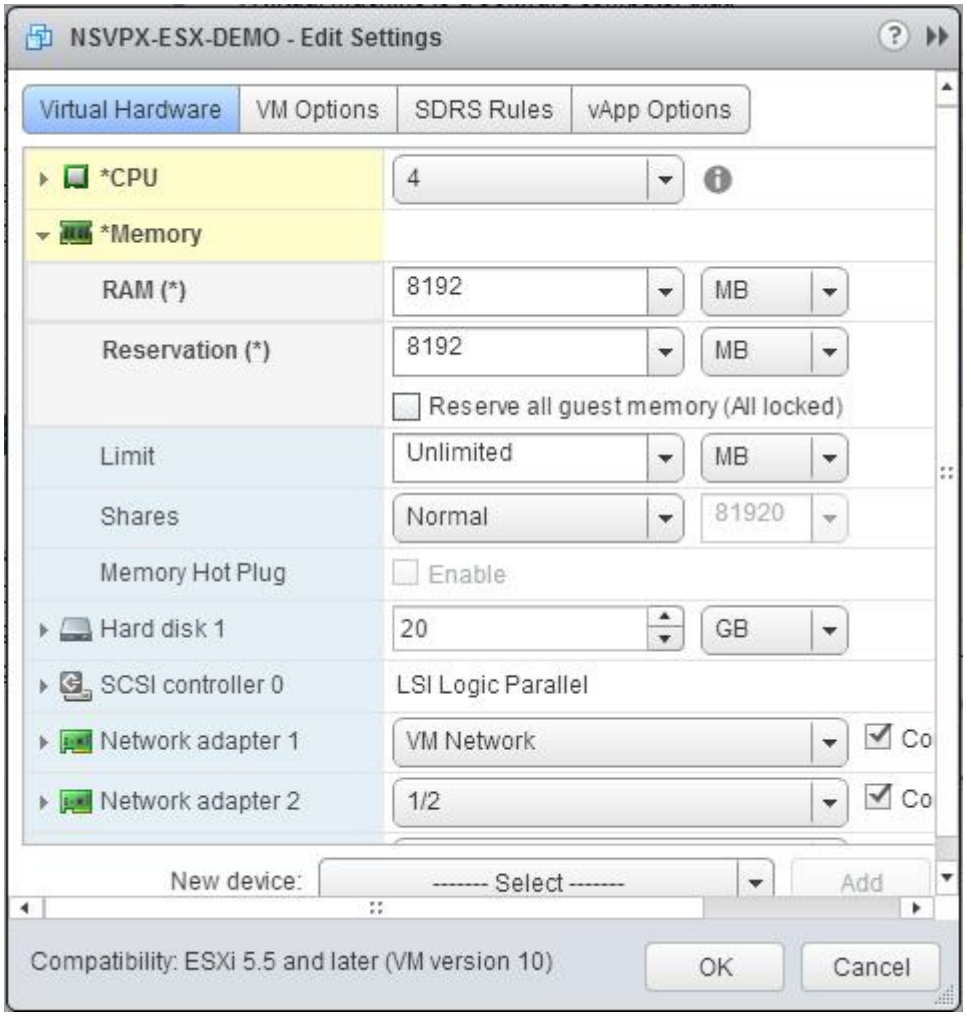


b. Dans la liste déroulante Réservation, entrez la valeur de la réservation mémoire et activez la case à cocher Réserver toute la mémoire invitée (Tout verrouillé). La réservation de mémoire doit correspondre au nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de processeurs virtuels est de 4, la réservation de mémoire doit être de 4 x 2 Go = 8 Go.

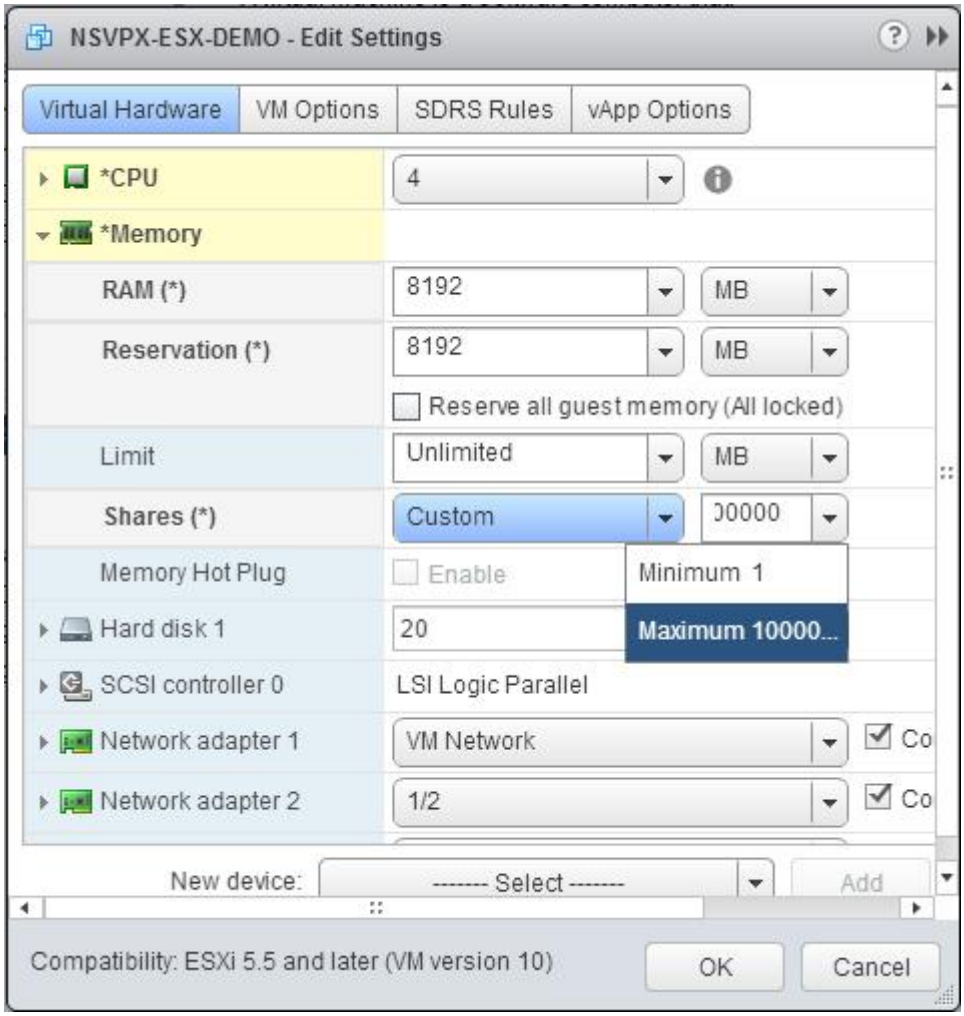
Remarque : pour une édition avancée ou Premium de l'appliance Citrix ADC VPX, assurez-vous d'allouer 4 Go de RAM à chaque vCPU. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.



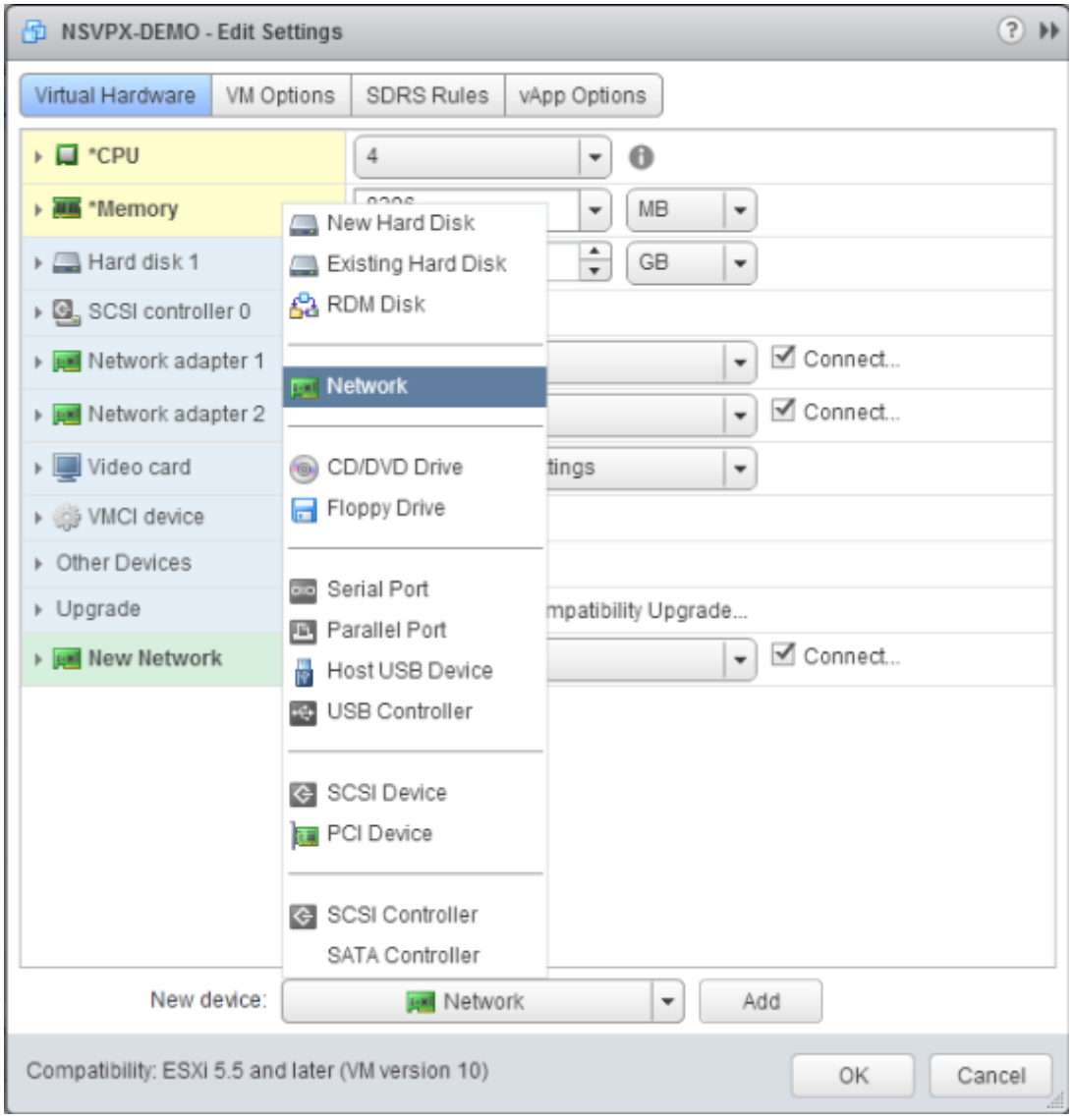
c. Dans la liste déroulante Limite, sélectionnez le nombre affiché comme valeur maximale.



d. Dans les listes déroulantes Partages, sélectionnez Personnalisé et le nombre qui s'affiche comme valeur maximale.



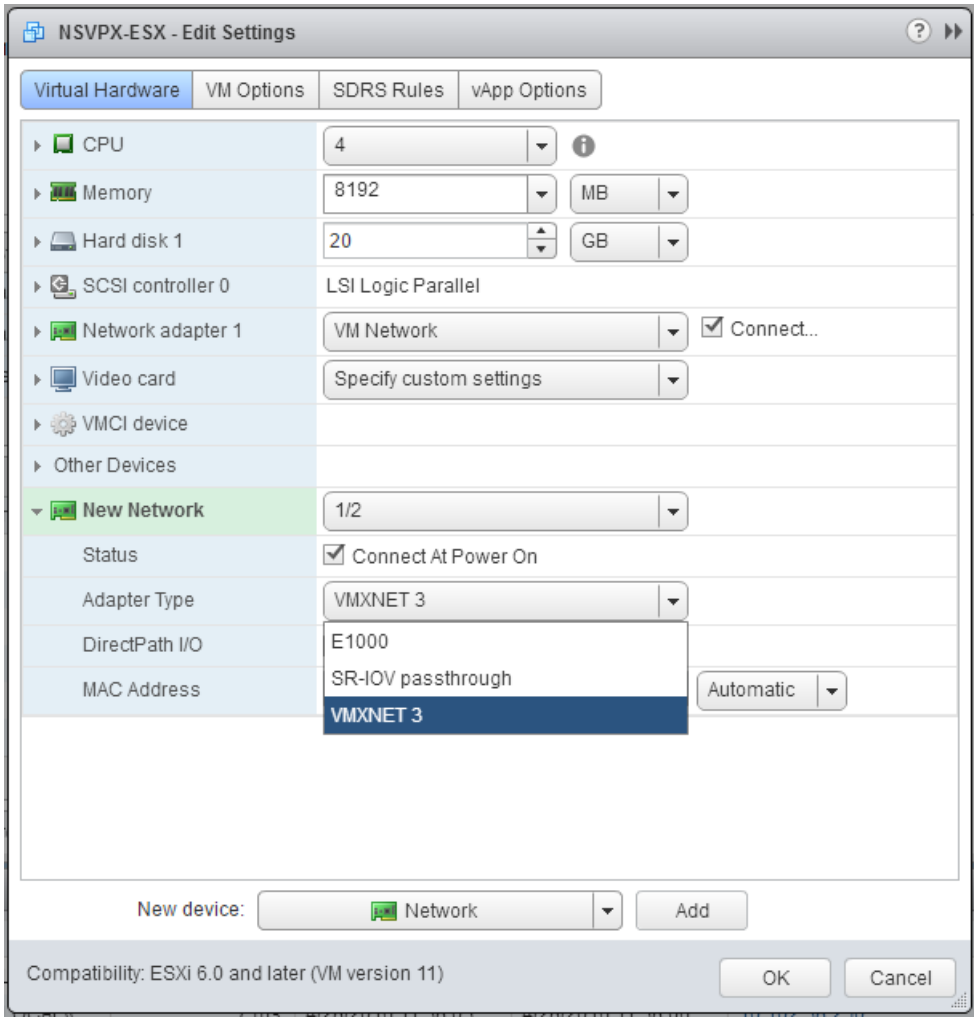
7. Ajoutez une interface réseau VMXNET3. Dans la liste déroulante Nouveau périphérique, sélectionnez Réseau et cliquez sur Ajouter.



8. Dans la section Nouveau réseau, dans la liste déroulante, sélectionnez l'interface réseau et procédez comme suit :

   a. Dans la liste déroulante Type d'adaptateur, sélectionnez VMXNET3.

   > **Important**
   >
   > L'interface réseau E1000 par défaut et VMXNET3 ne peuvent pas coexister, assurez-vous de supprimer l'interface réseau E1000 et d'utiliser VMXNET3 (0/1) comme interface de gestion.



9. Cliquez sur OK.
10. Mettez sous tension l'instance Citrix ADC VPX.
11. Une fois l'instance Citrix ADC VPX sous tension, vous pouvez utiliser la commande suivante pour vérifier la configuration :

> Afficher le résumé de l'interface

La sortie doit afficher toutes les interfaces que vous avez configurées :

```
1 > show interface summary
2 ---------------------------------------------------------------------------

3       Interface  MTU        MAC                Suffix
4 ---------------------------------------------------------------------------

5 1     0/1        1500       00:0c:29:89:1d:0e  NetScaler Vir...rface,
      VMXNET3
```



```
6  2     1/1        9000       00:0c:29:89:1d:18    NetScaler Vir...rface,
       VMXNET3
7  3     1/2        9000       00:0c:29:89:1d:22    NetScaler Vir...rface,
       VMXNET3
8  4     LO/1       9000       00:0c:29:89:1d:0e    Netscaler Loopback
      interface
```

> **Remarque**
>
> Après avoir ajouté une interface VMXNET3 et redémarré l'appliance Citrix ADC VPX, l'hyperviseur VMware ESX peut modifier l'ordre dans lequel la carte réseau est présentée à l'appliance VPX. Par conséquent, la carte réseau 1 peut ne pas toujours rester 0/1, ce qui entraîne une perte de connectivité de gestion à l'appliance VPX. Pour éviter ce problème, modifiez le réseau virtuel de la carte réseau en conséquence.
>
> Il s'agit d'une limitation de l'hyperviseur VMware ESX.

Configurer une instance Citrix ADC VPX pour utiliser l'interface réseau SR-IOV

August 20, 2021

Une fois que vous avez installé et configuré l'instance Citrix ADC VPX sur VMware ESX, vous pouvez utiliser le client Web VMware vSphere pour configurer l'appliance virtuelle afin qu'elle utilise les interfaces réseau SR-IOV (SR-IOV) à racine unique.

Limitations

Un Citrix ADC VPX configuré avec une interface réseau SR-IOV présente les limitations suivantes :

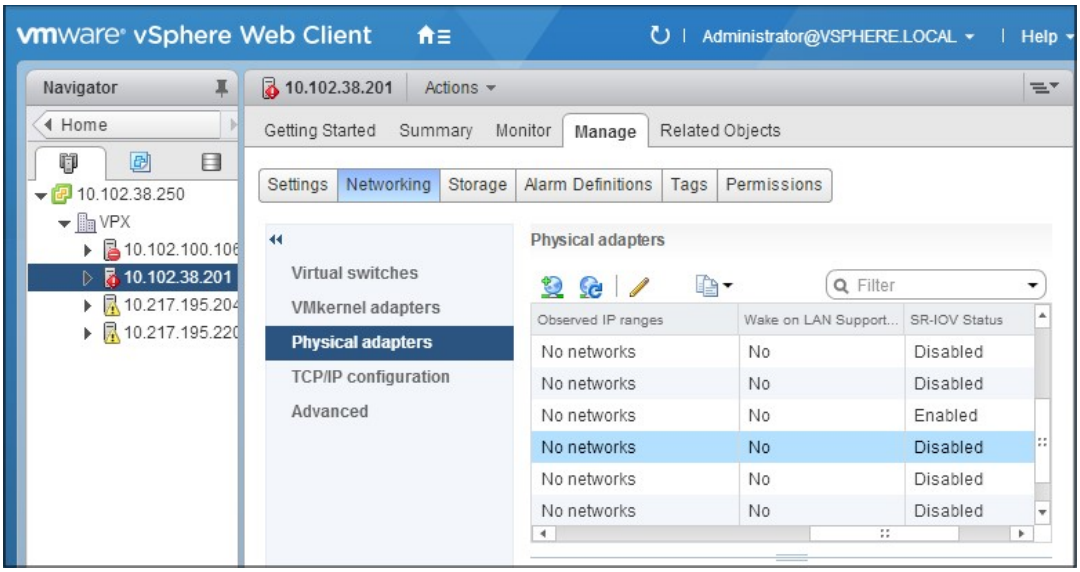
- Les fonctionnalités suivantes ne sont pas prises en charge sur les interfaces SR-IOV utilisant la carte réseau Intel 82599 10G sur ESX VPX :
  - Commutation de mode L2
  - Agrégation de liens statiques et LACP
  - Mise en cluster
  - Partitionnement d'administrateur [mode VLAN partagé]
  - Haute disponibilité [Actif - Mode actif]
  - Cadres Jumbo
  - IPv6
- Les fonctionnalités suivantes ne sont pas prises en charge sur l'interface SR-IOV avec une carte réseau Intel 82599 10G sur KVM VPX :

- Agrégation de liens statiques et LACP
- Commutation de mode L2
- Mise en cluster
- Partitionnement d'administrateur [mode VLAN partagé]
- Haute disponibilité [Actif — Mode actif]
- Cadres Jumbo
- IPv6
- La configuration VLAN sur l'interface Hypervisor for SR-IOV VF via `ip link` commande n'est pas prise en charge

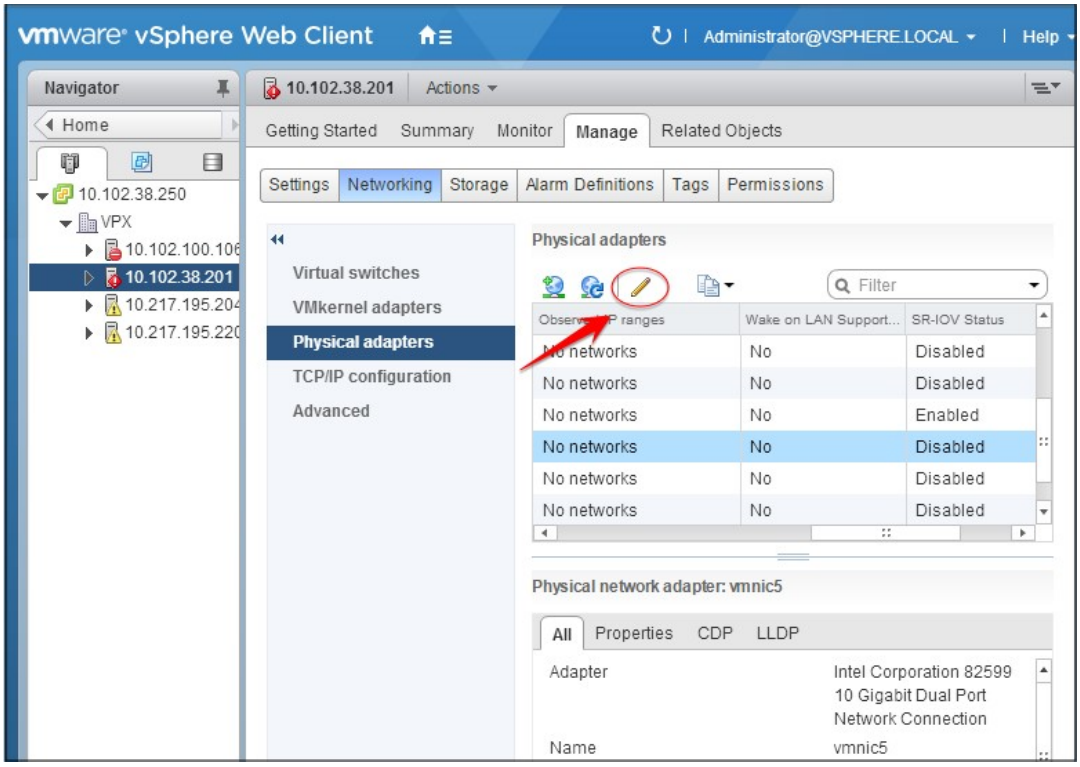
Conditions préalables

Assurez-vous que vous :

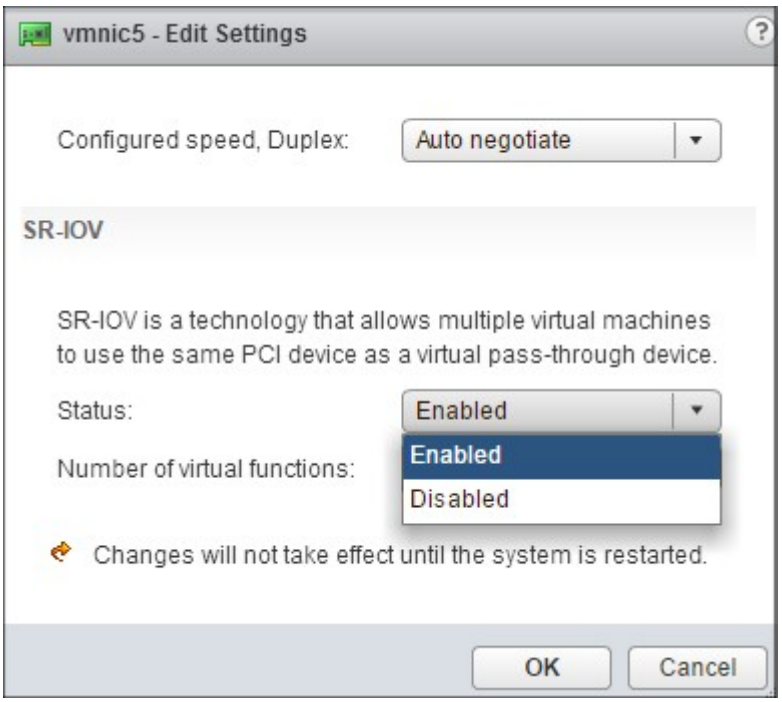
- Ajoutez la carte réseau (NIC) Intel 82599 à l'hôte ESX. La version 3.7.13.7.14iov du pilote IXGBE est recommandée.
- Activez SR-IOV sur la carte physique de l'hôte, comme suit :
  1. Dans vSphere Web Client, accédez à l'hôte.
  2. Sous l'onglet **Gérer > Mise en réseau**, sélectionnez **Cartes physiques** . Le champ Statut SR-IOV indique si une carte physique prend en charge SR-IOV.



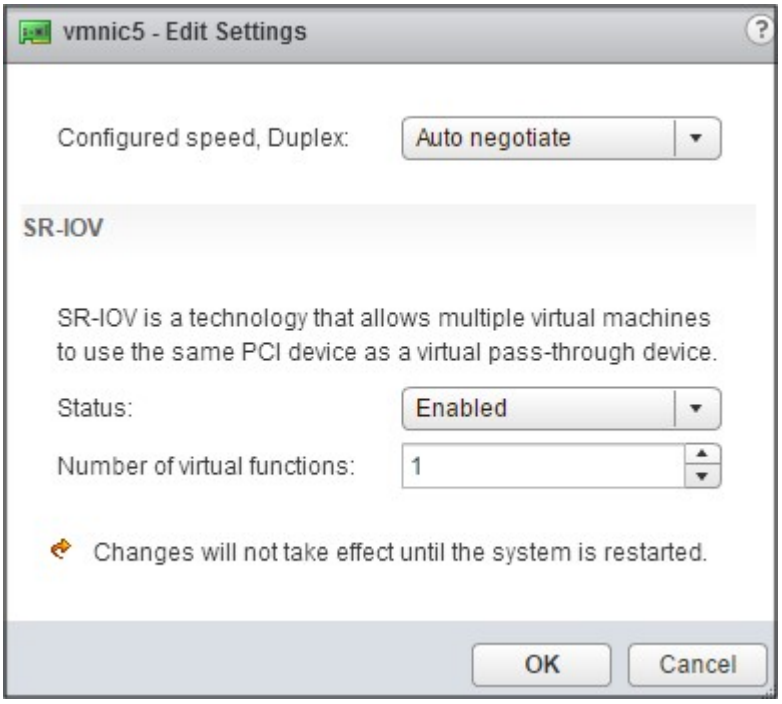
  3. Sélectionnez l'adaptateur physique, puis cliquez sur l'icône en forme de crayon pour ouvrir la boîte de dialogue **Modifier les paramètres** .



4. Sous SR-IOV, sélectionnez **Activé** dans la liste déroulante **Statut** .



5. Dans le champ **Nombre de fonctions virtuelles**, entrez le nombre de fonctions virtuelles que vous souhaitez configurer pour la carte.



6. Cliquez sur **OK**.
7. Redémarrez l'hôte.

- Créez un commutateur virtuel distribué (DVS) et `Portgroups`. Pour obtenir des instructions, reportez-vous à la documentation VMware.

> **Remarque**
>
> Citrix a qualifié la configuration SR-IOV sur DVS et `Portgroups` uniquement.

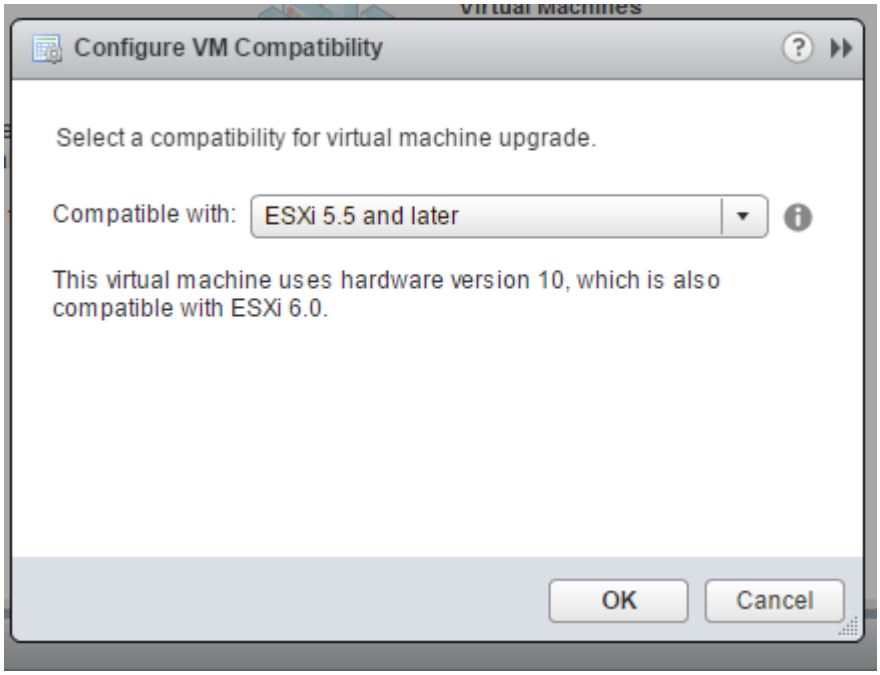
Pour configurer les instances Citrix ADC VPX pour qu'elles utilisent l'interface réseau SR-IOV à l'aide de VMware vSphere Web Client :

1. Dans vSphere Web Client, sélectionnez **Hôtes et clusters**.
2. Mettez à niveau le paramètre de compatibilité de l'instance Citrix ADC VPX vers ESX 5.5 ou version ultérieure, comme suit :

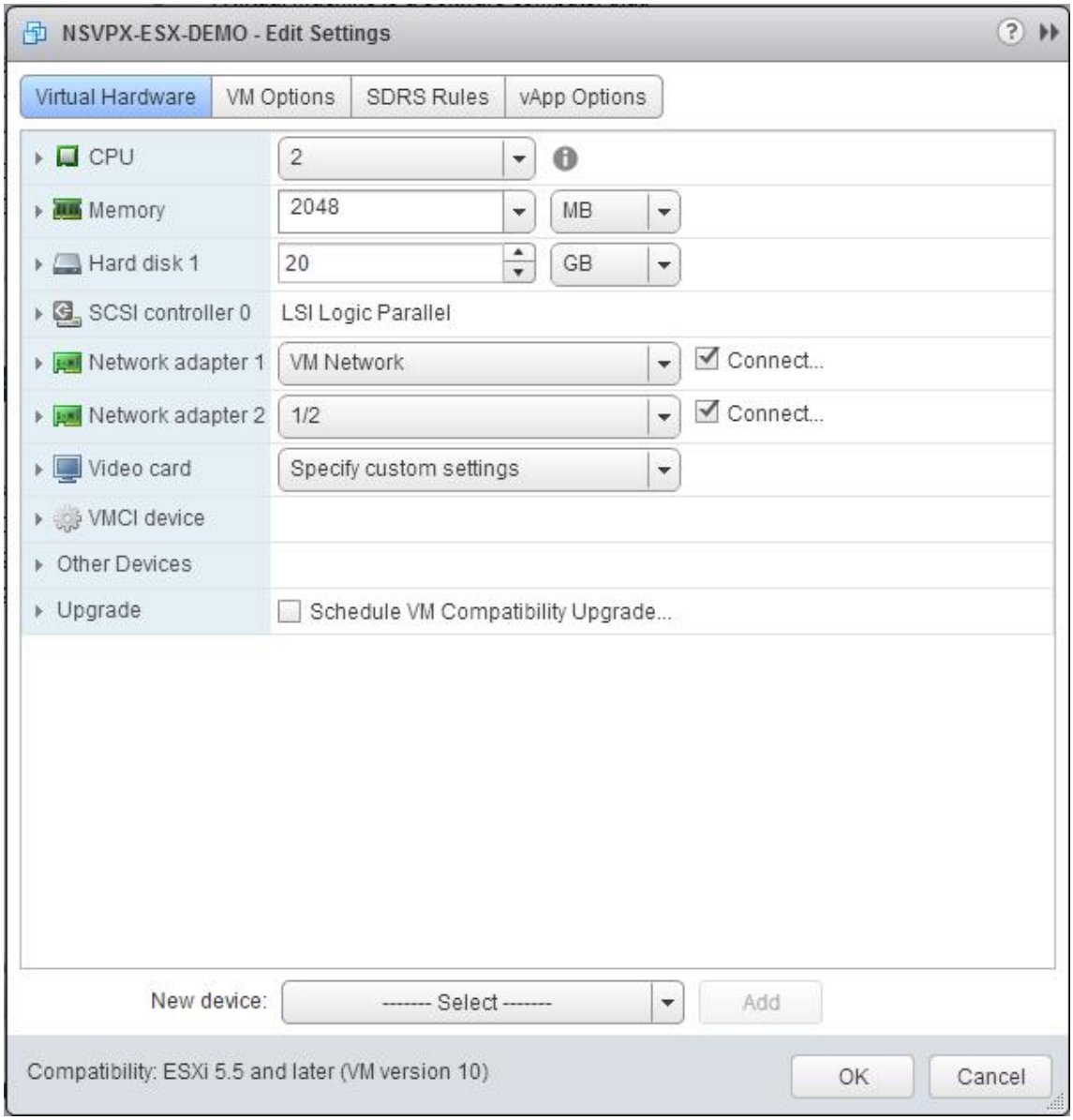
   a. Mettez hors tension l'instance Citrix ADC VPX.

   b. Cliquez avec le bouton droit de la souris sur l'instance Citrix ADC VPX et sélectionnez **Compatibilité > Mettre à niveau la compatibilité des machines virtuelles**.

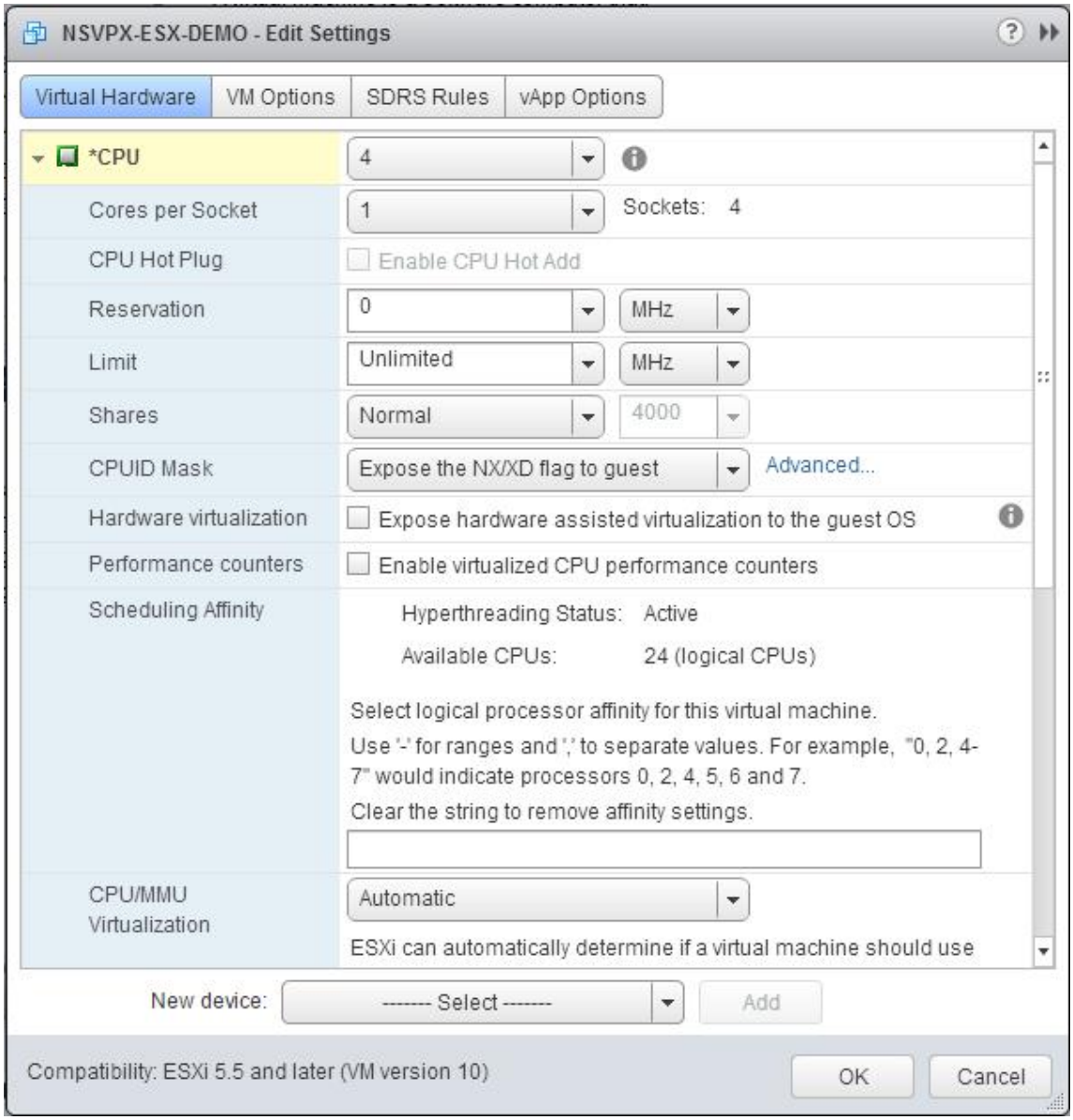
   c. Dans la boîte de dialogue **Configurer la compatibilité des machines virtuelles**, sélectionnez **ESXi 5.5 et versions ultérieures** dans la liste déroulante **Compatible avec**, puis cliquez sur **OK**.



3. Cliquez avec le bouton droit de la souris sur l'instance Citrix ADC VPX et cliquez sur **Modifier les paramètres**.



4. Dans la boîte de dialogue **<virtual_appliance> - Edit Settings**, cliquez sur la section **CPU**.



5. Dans la section **CPU**, mettez à jour les paramètres suivants :

   - Nombre de processeurs
   - Nombre de sockets
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

   a. Dans la liste déroulante **CPU**, sélectionnez le nombre de CPU à affecter à l'appliance virtuelle.

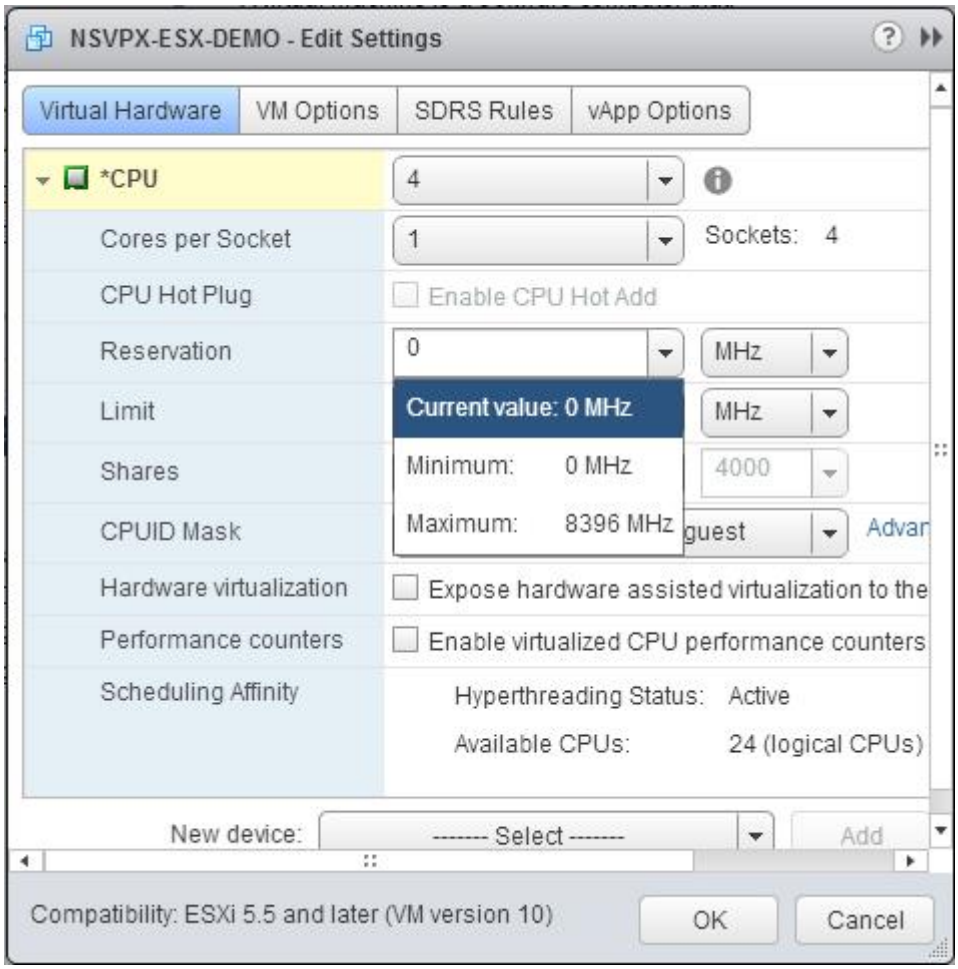
   b. Dans la liste déroulante **Cœurs par socket**, sélectionnez le nombre de sockets.

   c. (Facultatif) Dans le champ **Plug à chaud CPU**, activez ou **désactivez la case à cocher Activer**

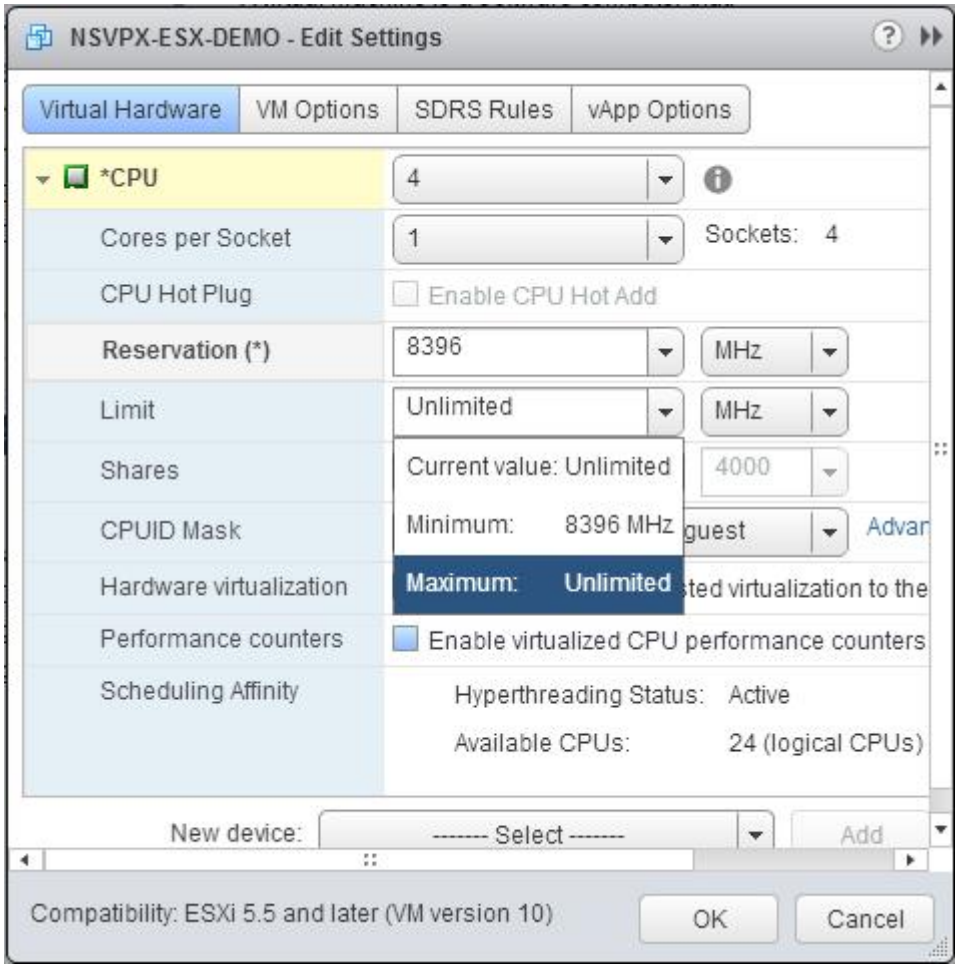
l'ajout à chaud CPU .

Remarque : Citrix recommande d'accepter la valeur par défaut (désactivée).

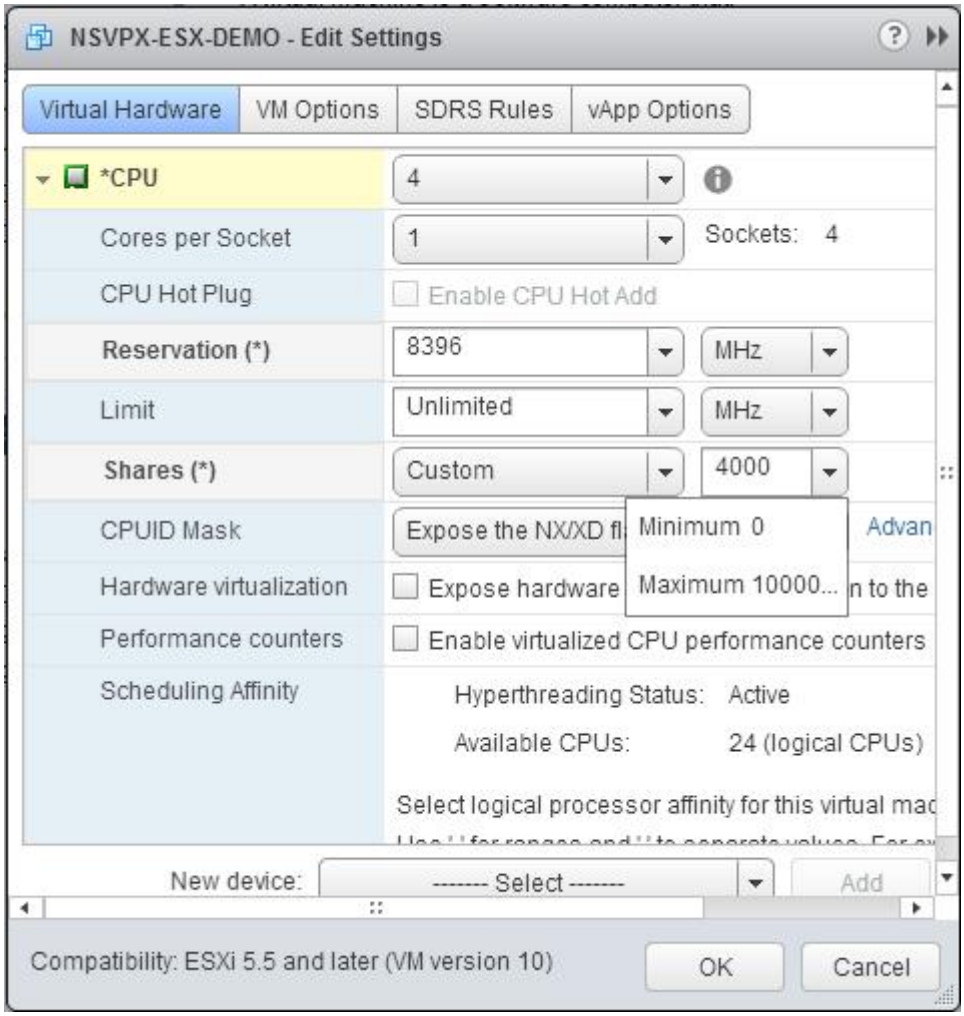
d. Dans la liste déroulante **Réservation**, sélectionnez le nombre qui est affiché comme valeur maximale.



e. Dans la liste déroulante **Limite**, sélectionnez le nombre affiché comme valeur maximale.



f. Dans les listes déroulantes **Parts**, sélectionnez **Personnalisé** et le nombre affiché comme valeur maximale.



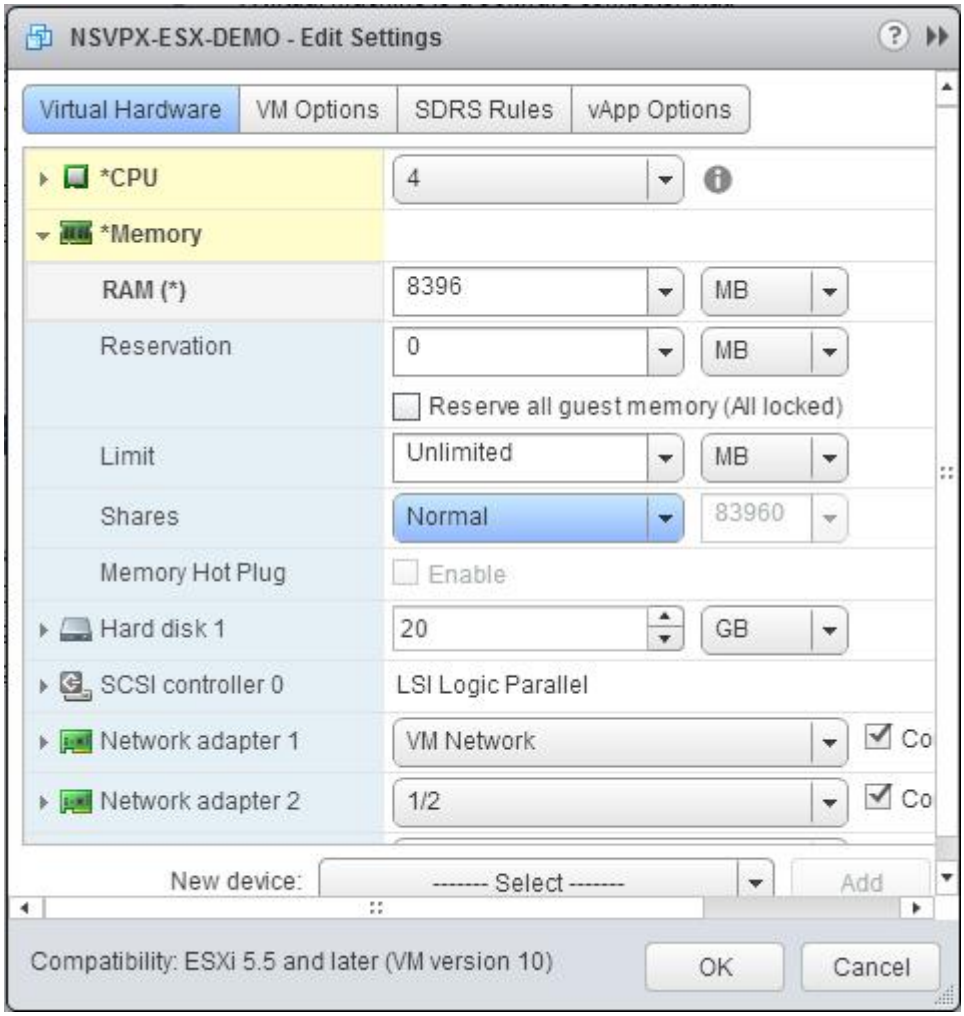
6. Dans la section **Mémoire**, mettez à jour les paramètres suivants :

   - Taille de la RAM
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

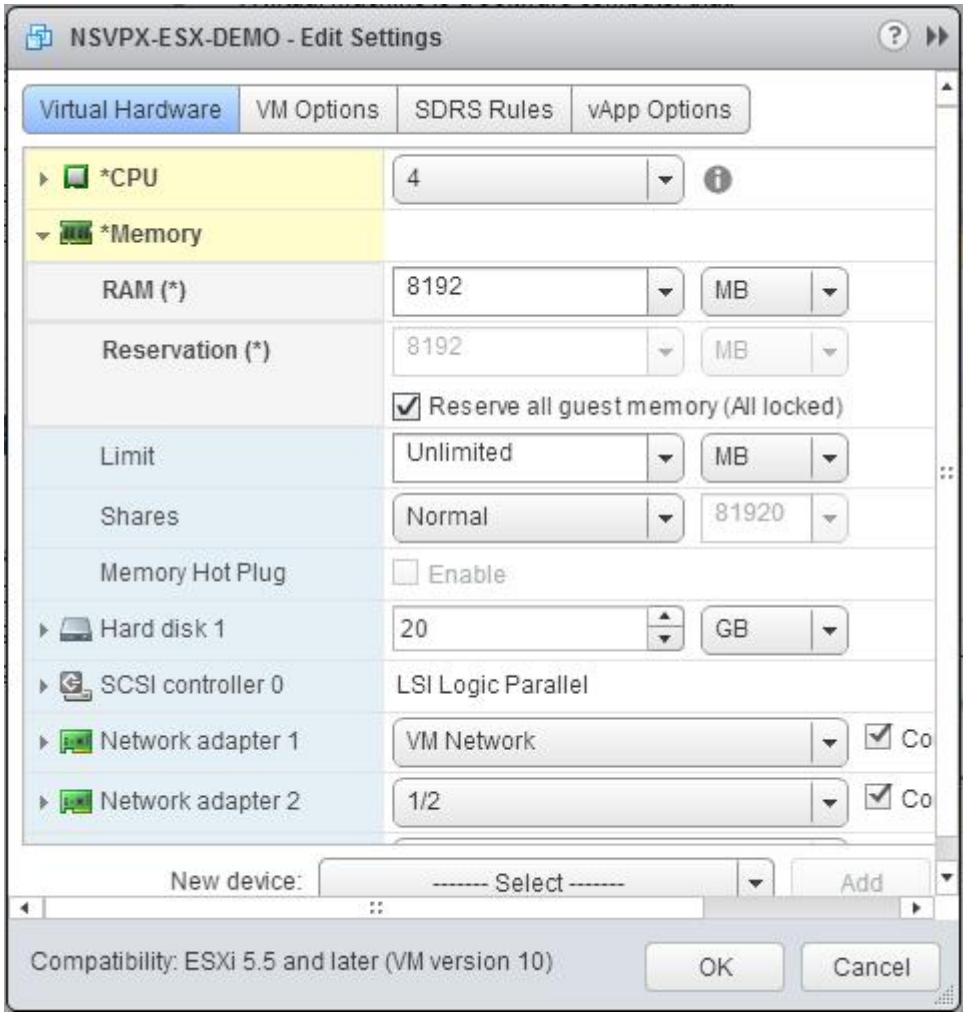
   a. Dans la liste déroulante **RAM**, sélectionnez la taille de la RAM. Il doit s'agir du nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 2 Go = 8 Go.

   Remarque : Pour l'édition Advanced ou Premium de l'appliance Citrix ADC VPX, assurez-vous d'allouer 4 Go de RAM à chaque vCPU. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.

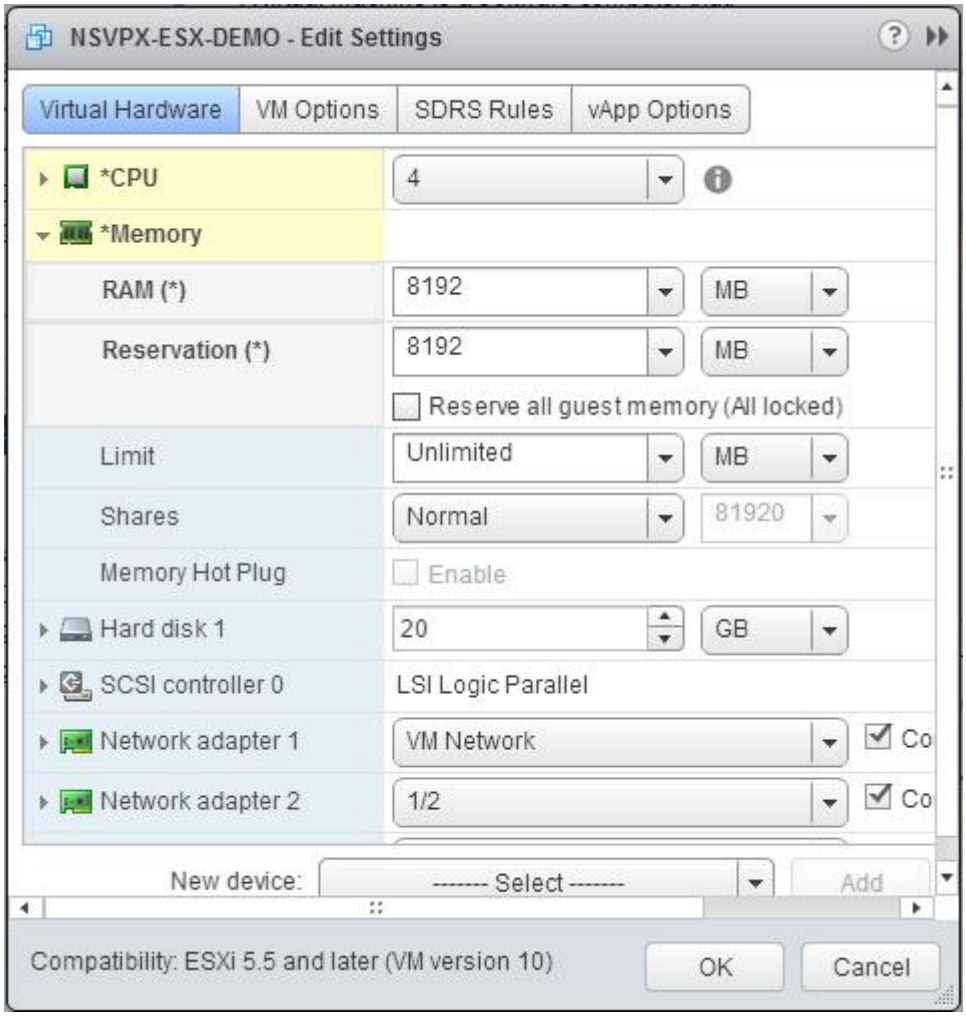


b. Dans la liste déroulante **Réservation**, entrez la valeur de la réservation mémoire et activez la case à cocher **Réserver toute la mémoire invitée (Tout verrouillé)**. La réservation de mémoire doit correspondre au nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de processeurs virtuels est de 4, la réservation de mémoire doit être de 4 x 2 Go = 8 Go.

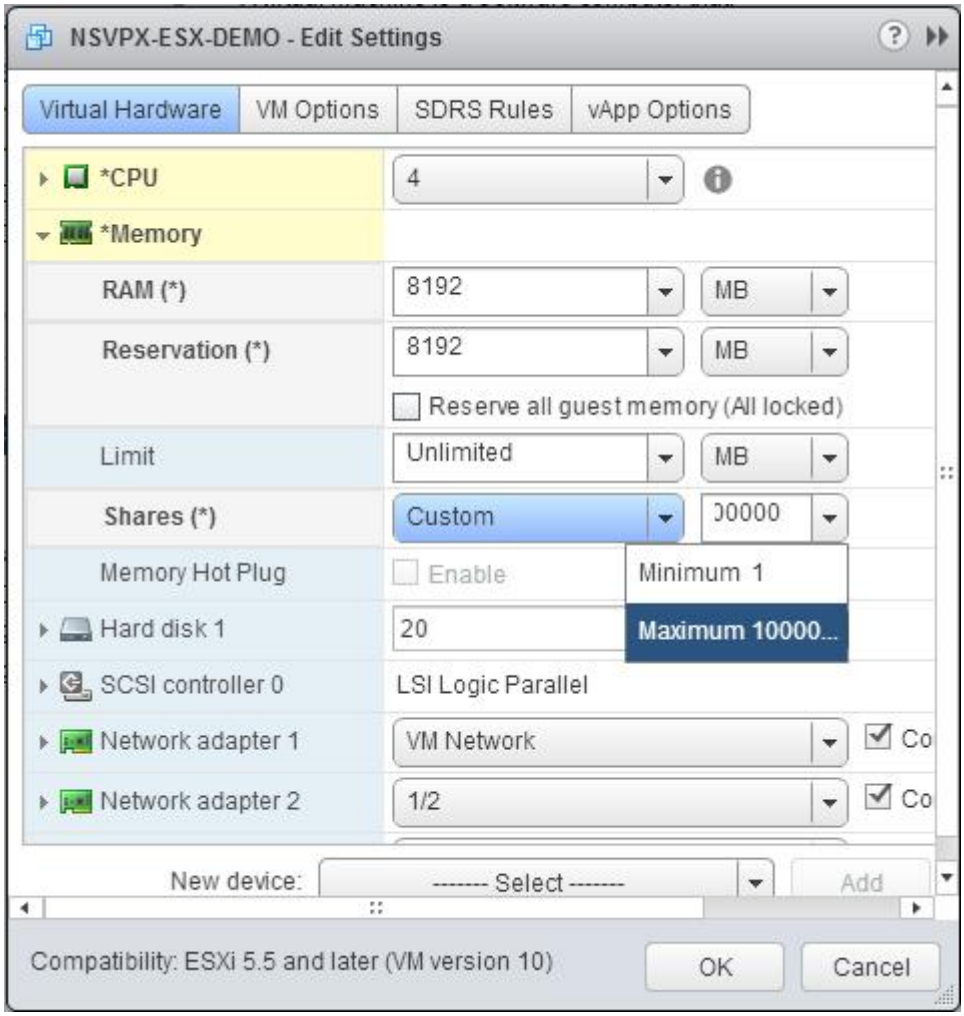
Remarque : Pour l'édition Advanced ou Premium de l'appliance Citrix ADC VPX, assurez-vous d'allouer 4 Go de RAM à chaque vCPU. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.



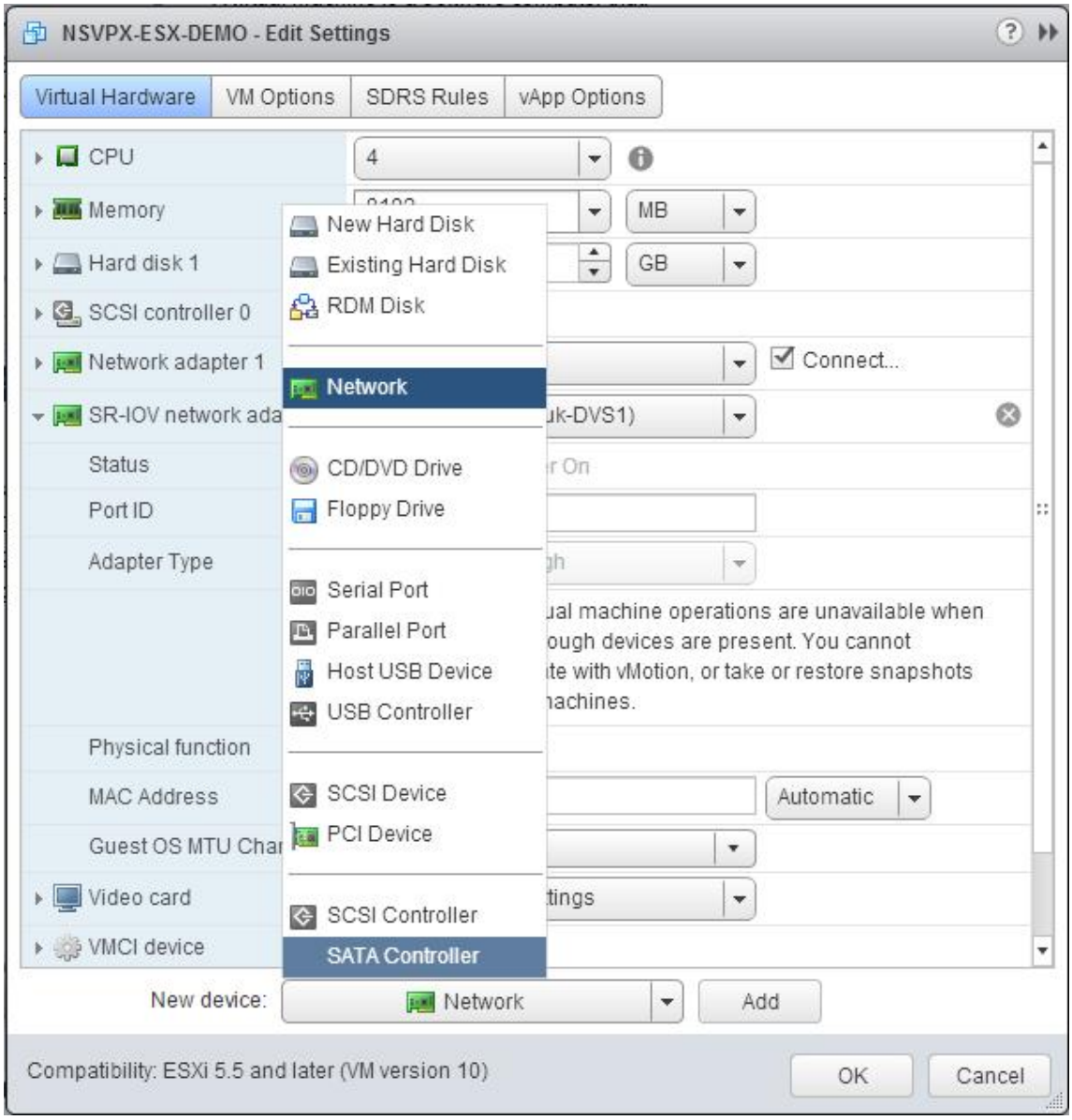
c. Dans la liste déroulante **Limite**, sélectionnez le nombre affiché comme valeur maximale.



d. Dans les listes déroulantes **Parts**, sélectionnez **Personnalisé**, puis sélectionnez le nombre affiché comme valeur maximale.

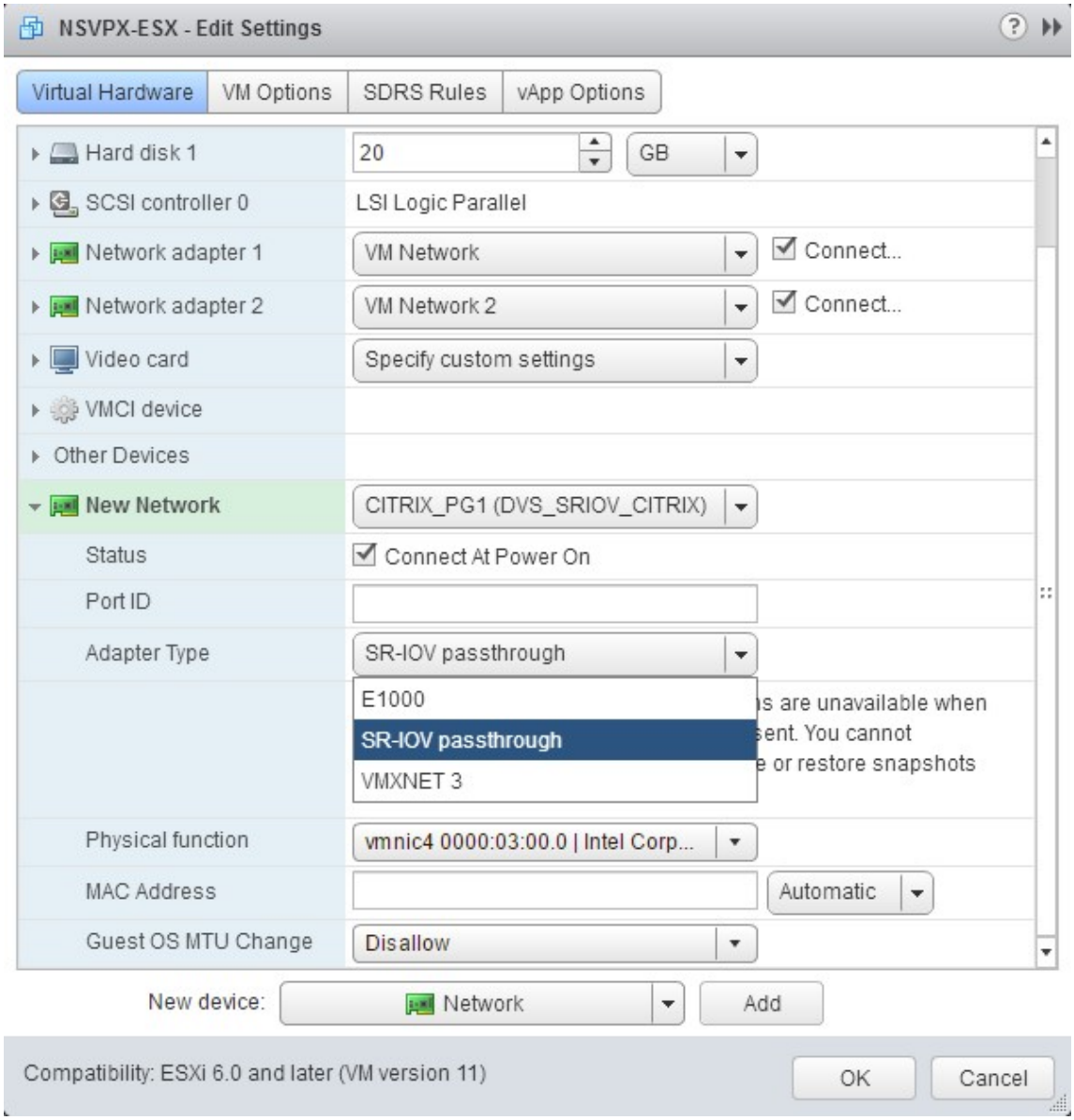


7. Ajouter une interface réseau SR-IOV. Dans la liste déroulante **Nouvel appareil**, sélectionnez **Réseau**, puis cliquez sur **Ajouter**.

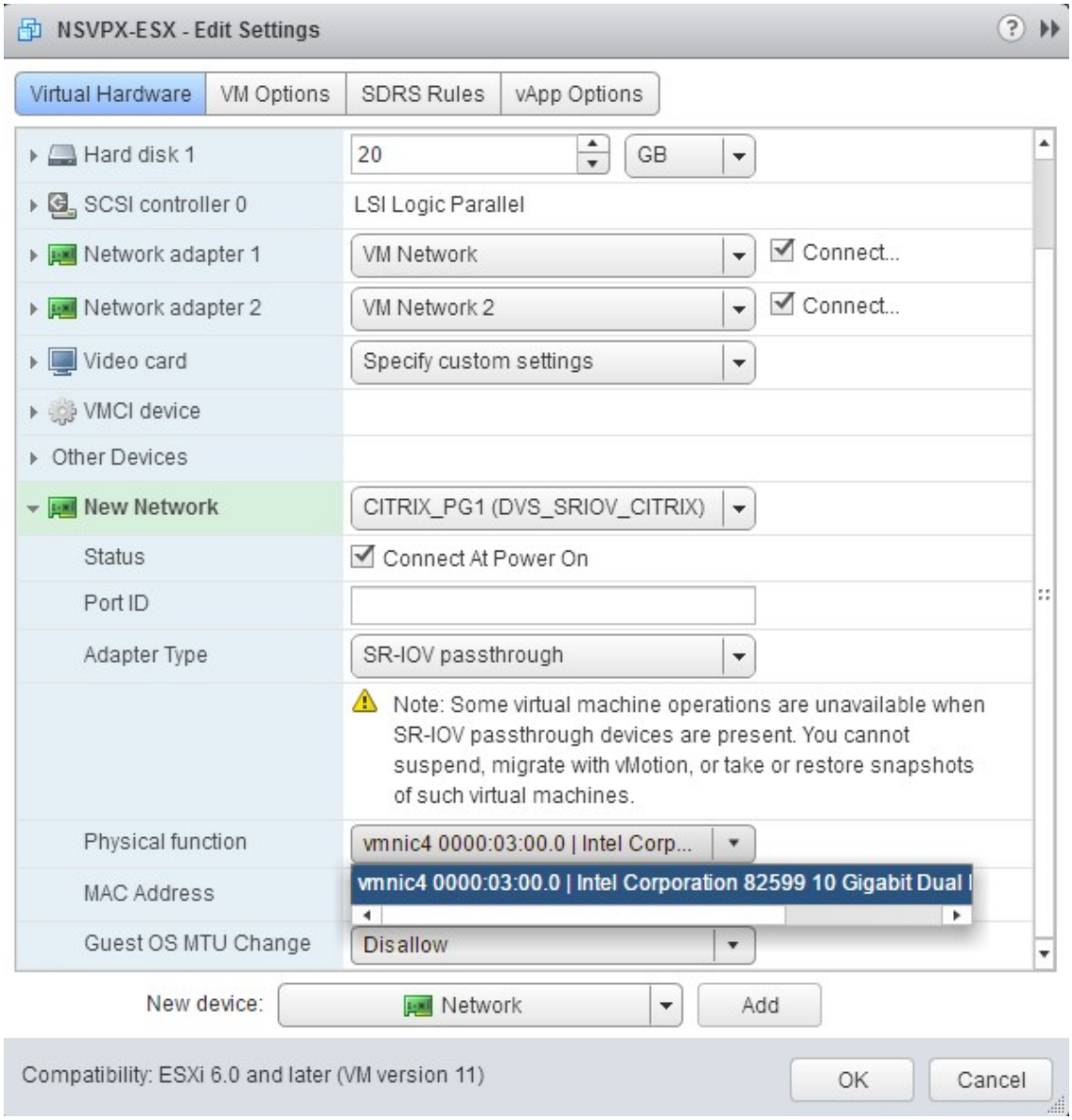


8. Dans la section **Nouveau réseau**. Dans la liste déroulante, sélectionnez celui `Portgroup` que vous avez créé, puis procédez comme suit :

   a. Dans la liste déroulante **Type d'adaptateur**, sélectionnez **Passthrough SR-IOV** .

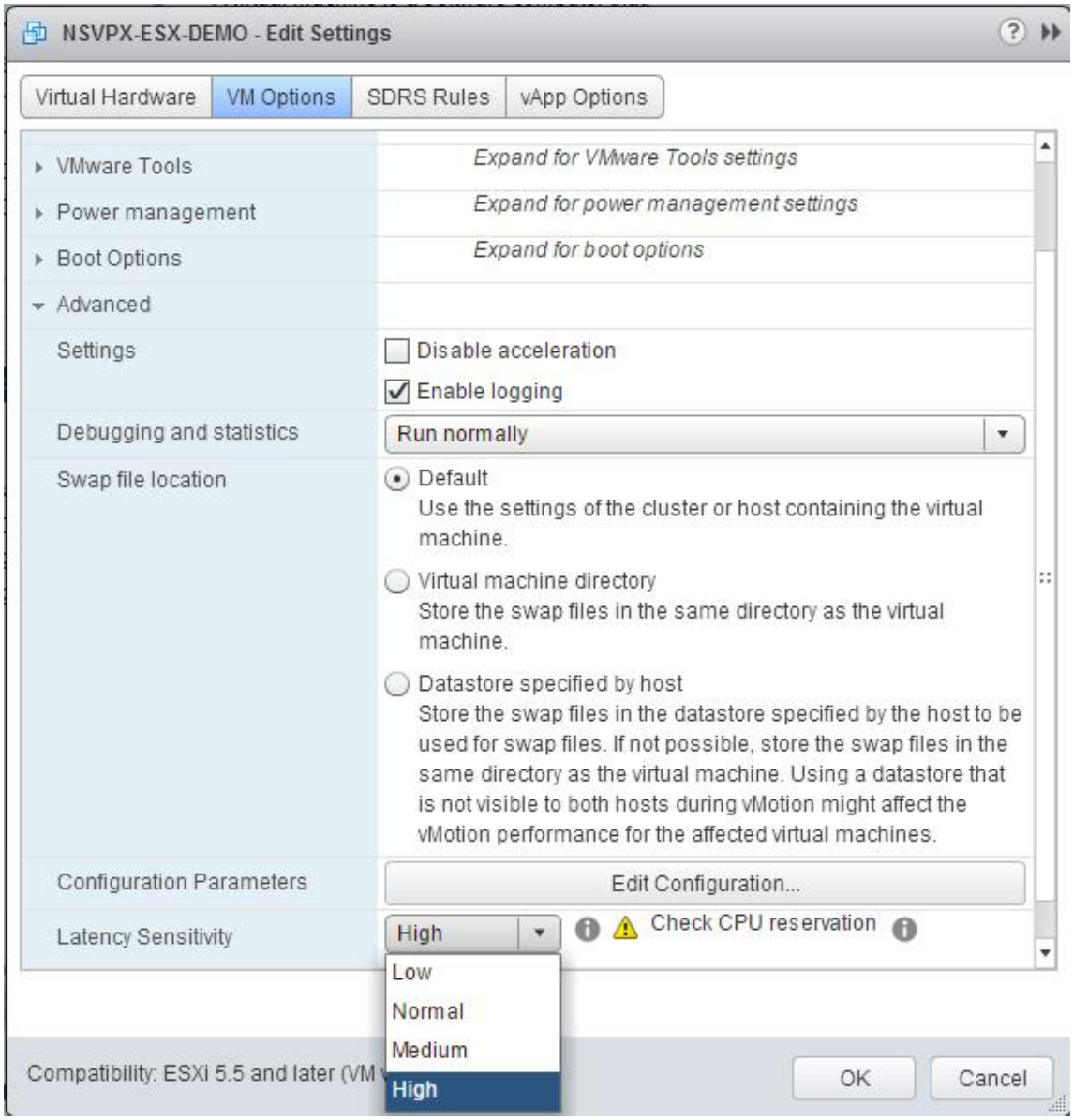


b. Dans la liste déroulante **Fonction physique**, sélectionnez l'adaptateur physique mappé avec le `Portgroup`.



c. Dans la liste déroulante **Modification du MTU du système d'exploitation invité**, sélectionnez **Disallow** .

9. Dans la boîte de dialogue **<virtual_appliance> - Edit Settings**, cliquez sur l'onglet **VM Options**.
10. Sous l'onglet **Options de la machine virtuelle**, sélectionnez la section **Avancé** . Dans la liste déroulante **Sensibilité à la latence**, sélectionnez **Élevé** .



11. Cliquez sur **OK**.
12. Mettez sous tension l'instance Citrix ADC VPX.
13. Une fois l'instance Citrix ADC VPX sous tension, vous pouvez utiliser la commande suivante pour vérifier la configuration :

    > Afficher le résumé de l'interface

La sortie doit afficher toutes les interfaces que vous avez configurées :

```
1 > show interface summary
2 ---------------------------------------------------------------------------

3       Interface  MTU        MAC                Suffix
```



```
4  ----------------------------------------------------------------------------

5  1     0/1        1500       00:0c:29:1b:81:0b    NetScaler Virtual
       Interface
6  2     10/1       1500       00:50:56:9f:0c:6f    Intel 82599 10G VF
       Interface
7  3     10/2       1500       00:50:56:9f:5c:1e    Intel 82599 10G VF
       Interface
8  4     10/3       1500       00:50:56:9f:02:1b    Intel 82599 10G VF
       Interface
9  5     10/4       1500       00:50:56:9f:5a:1d    Intel 82599 10G VF
       Interface
10 6     10/5       1500       00:50:56:9f:4e:0b    Intel 82599 10G VF
       Interface
11 7     LO/1       1500       00:0c:29:1b:81:0b    Netscaler Loopback
       interface
12  Done
13 > show inter 10/1
14 1)      Interface 10/1 (Intel 82599 10G VF Interface) #1
15         flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
16         MTU=1500, native vlan=55, MAC=00:50:56:9f:0c:6f, uptime 0
               h21m53s
17         Actual: media FIBER, speed 10000, duplex FULL, fctl NONE,
               throughput 10000
18         LLDP Mode: NONE,                LR Priority: 1024
19
20         RX: Pkts(838020742) Bytes(860888485431) Errs(0) Drops(2527)
               Stalls(0)
21         TX: Pkts(838149954) Bytes(860895860507) Errs(0) Drops(0) Stalls
               (0)
22         NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
23         Bandwidth thresholds are not set.
24  Done
```

Migration du Citrix ADC VPX de E1000 vers les interfaces réseau SR-IOV ou VMXNET3

August 20, 2021

24 mai 2018

Vous pouvez configurer vos instances Citrix ADC VPX quittant qui utilisent des interfaces réseau E1000

pour utiliser les interfaces réseau SR-IOV ou VMXNET3.

Pour configurer une instance Citrix ADC VPX existante pour utiliser des interfaces réseau SR-IOV, consultez Configurer une instance Citrix ADC VPX pour utiliser l'interface réseau SR-IOV.

Pour configurer une instance Citrix ADC VPX existante pour utiliser les interfaces réseau VMXNET3, consultez Configurer une instance Citrix ADC VPX pour utiliser l'interface réseau VMXNET3.

Configurer une instance Citrix ADC VPX pour utiliser l'interface réseau PCI

August 20, 2021

Généralités

Après avoir installé et configuré une instance Citrix ADC VPX sur VMware ESX Server, vous pouvez utiliser vSphere Web Client pour configurer l'appliance virtuelle de manière à utiliser les interfaces réseau PCI.

La fonction PCI passthrough permet à une machine virtuelle invitée d'accéder directement aux périphériques PCI et PCIe physiques connectés à un hôte.

Conditions préalables

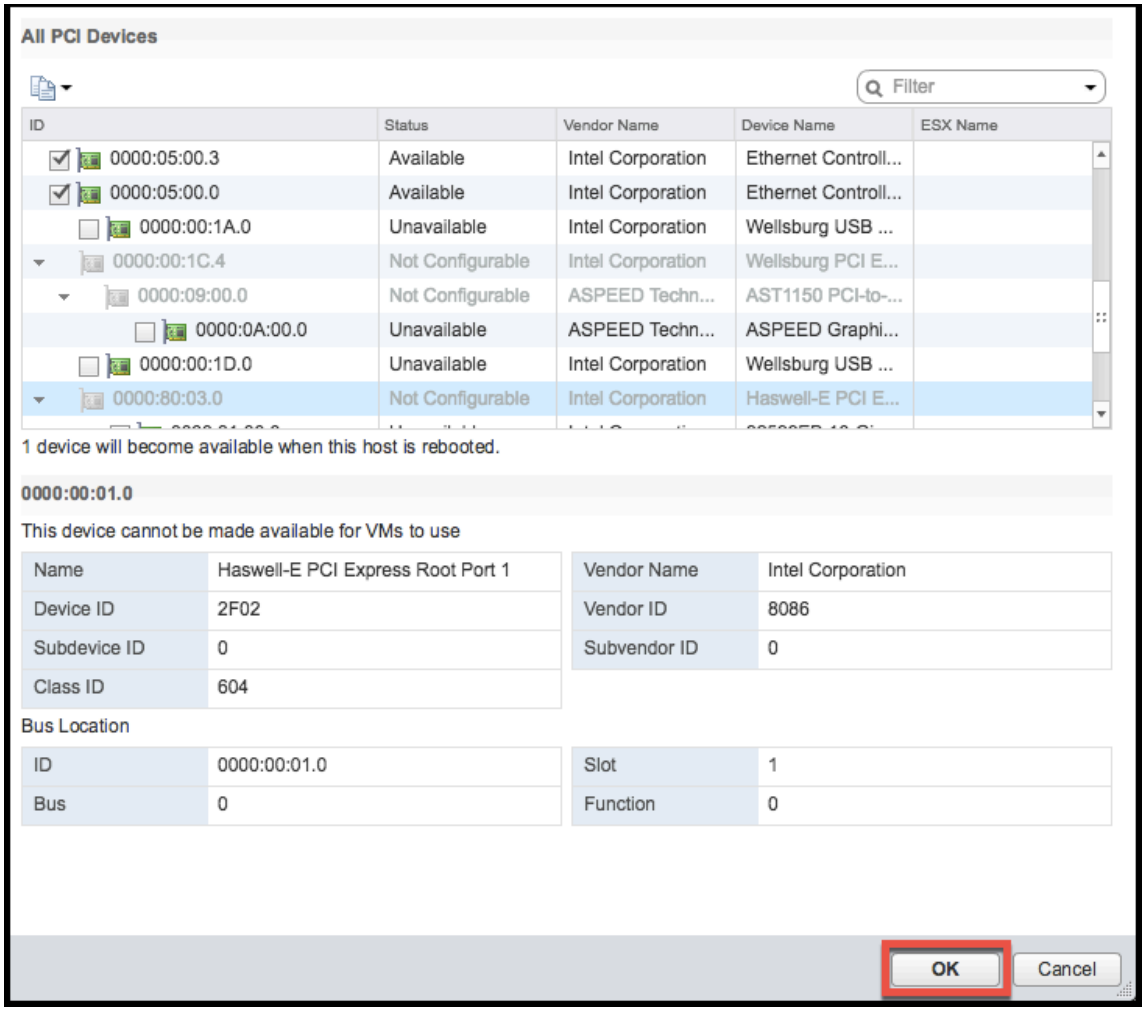
- La version du microprogramme de la carte réseau Intel XL710 sur l'hôte est 5.04.
- Périphérique PCI connecté à l'hôte et configuré sur celui-ci
- NIC prises en charge :
  - Carte réseau Intel X710 10G
  - Carte réseau Intel XL710 à double port 40G
  - Carte réseau Intel XL710 à port unique 40G

Configurer les périphériques passthrough sur un hôte

Avant de configurer un périphérique PCI passthrough sur une machine virtuelle, vous devez le configurer sur la machine hôte. Procédez comme suit pour configurer les périphériques passthrough sur un hôte.

1. Sélectionnez l'hôte dans le panneau Navigateur de vSphere Web Client.
2. Cliquez sur **Gérer** > **Paramètres** > **Périphériques PCI** . Tous les périphériques passthrough disponibles s'affichent.

3. Cliquez avec le bouton droit sur le périphérique que vous souhaitez configurer, puis cliquez sur **Modifier**.
4. La fenêtre **Modifier la disponibilité des périphériques PCI** s'affiche.
5. Sélectionnez les périphériques à utiliser pour la transmission, puis cliquez sur **OK**.

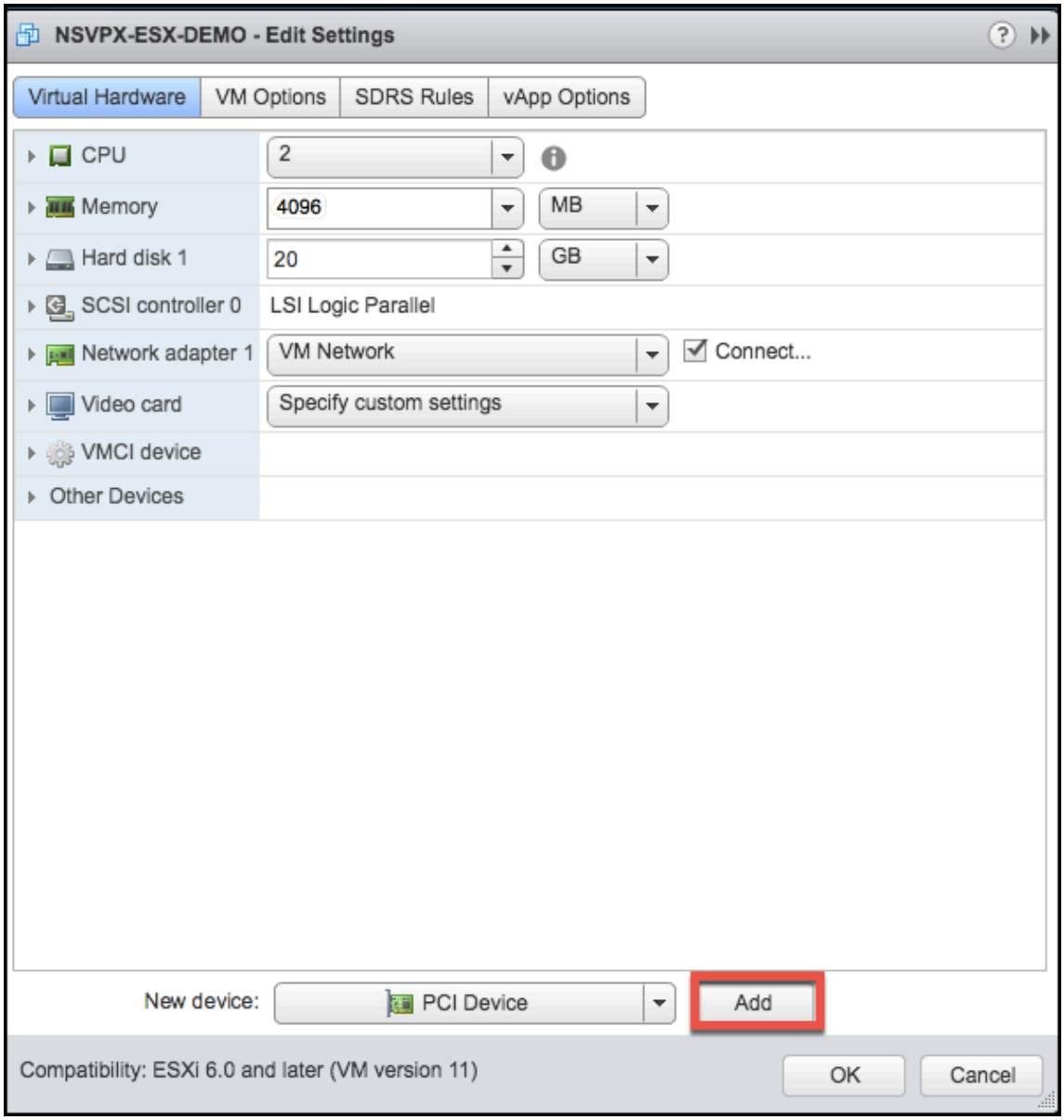


6. Redémarrez la machine hôte.

Configurer des périphériques passthrough sur une instance Citrix ADC VPX

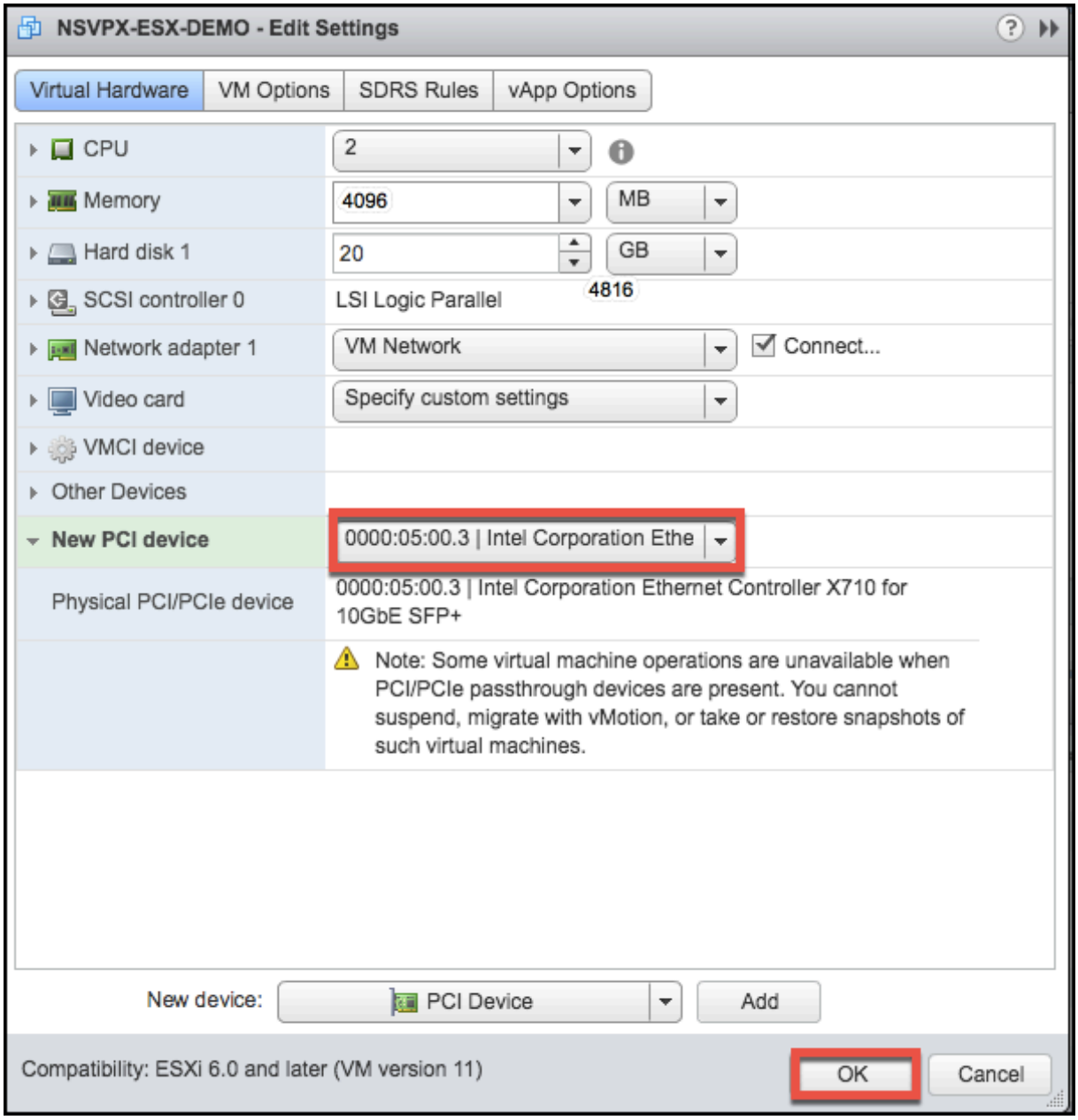
Procédez comme suit pour configurer un périphérique PCI passthrough sur une instance Citrix ADC VPX.

1. Mettez hors tension la machine virtuelle.
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
3. Sous l'onglet **Matériel virtuel**, sélectionnez **Périphérique PCI** dans le menu déroulant **Nouveau périphérique**, puis cliquez sur **Ajouter** .



4. Développez **Nouveau périphérique PCI** et sélectionnez le périphérique de transmission à connecter à la machine virtuelle dans la liste déroulante, puis cliquez sur **OK** .

> **Remarque**
>
> L'interface réseau VMXNET3 et l'interface réseau PCI ne peuvent pas coexister.



1. Mettez sous tension la machine virtuelle invitée.

Vous avez terminé les étapes de configuration de Citrix ADC VPX pour utiliser les interfaces réseau PCI passthrough.

Installer une instance Citrix ADC VPX sur le cloud VMware sur AWS

August 20, 2021

VMware Cloud (VMC) sur AWS vous permet de créer des centres de données définis par logiciel

cloud (SDDC) sur AWS avec le nombre souhaité d'hôtes ESX. Le VMC sur AWS prend en charge les déploiements Citrix ADC VPX. VMC fournit une interface utilisateur identique à vCenter sur site. Il fonctionne identique aux déploiements Citrix ADC VPX basés sur ESX.

Conditions préalables

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Un SDDC VMware doit être présent avec au moins un hôte.
- Téléchargez les fichiers d'installation de l'appliance Citrix ADC VPX.
- Créez des segments réseau appropriés sur VMware SDDC auxquels les machines virtuelles se connectent.
- Obtenir des fichiers de licence VPX. Pour plus d'informations sur les licences d'instance Citrix ADC VPX, consultez le *Guide de licences Citrix ADC VPX* à l'adresse http://support.citrix.com/article/ctx131110.

Configuration matérielle du cloud VMware

Le tableau suivant répertorie les ressources informatiques virtuelles que le SDDC VMware doit fournir pour chaque appliance virtuelle VPX nCore.

Tableau 1. Ressources de calcul virtuel minimales requises pour exécuter une instance Citrix ADC VPX

Composant	Exigences
Mémoire	2 Go
Processeur virtuel	2
Interfaces réseau virtuelles	Dans VMware SDDC, vous pouvez installer un maximum de 10 interfaces réseau virtuelles si le matériel VPX est mis à niveau vers la version 7 ou supérieure.
Espace disque	20 Go

> Remarque
>
> Ceci s'ajoute à toutes les exigences de disque pour l'Hypervisor.

Pour une utilisation en production de l'appliance virtuelle VPX, l'allocation complète de mémoire doit être réservée.

Configuration système requise pour OVF Tool 1.0

OVF Tool est une application cliente qui peut s'exécuter sur les systèmes Windows et Linux. Le tableau suivant décrit la configuration minimale requise.

Tableau 2. Configuration minimale requise pour l'installation d'outils OVF

Composant	Exigences
Système d'exploitation	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « OVF Tool User Guide » à l'adressehttp://kb.vmware.com/.
UC	750 MHz minimum, 1 GHz ou plus rapide recommandé
RAM	1 Go minimum, 2 Go recommandés
CARTE RÉSEAU	Carte réseau 100 Mbit/s ou plus rapide

Pour plus d'informations sur l'installation d'OVF, recherchez le fichier PDF « OVF Tool User Guide » à l'adressehttp://kb.vmware.com/.

Téléchargement des fichiers d'installation Citrix ADC VPX

Le package d'installation d'instance Citrix ADC VPX pour VMware ESX respecte la norme de format OVF (Open Virtual Machine). Vous pouvez télécharger les fichiers à partir du site Web Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l' adresse http://www.citrix.com. Cliquez sur le **lien Nouveaux utilisateurs**et suivez les instructions pour créer un compte Citrix.

Une fois connecté, naviguez dans le chemin suivant à partir de la page d'accueil Citrix :

Citrix.com > **Téléchargements > Citrix ADC > Appliances virtuelles**.

Copiez les fichiers suivants sur une station de travail sur le même réseau que le serveur ESX. Copiez les trois fichiers dans le même dossier.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (par exemple, NSVPX-ESX-13.0-79.64-Disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (par exemple, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (par exemple, NSVPX-ESX-13.0-79.64.mf)

Installer une instance Citrix ADC VPX sur le cloud VMware

Après avoir installé et configuré VMware SDDC, vous pouvez utiliser le SDDC pour installer des appliances virtuelles sur le cloud VMware. Le nombre d'appliances virtuelles que vous pouvez installer dépend de la quantité de mémoire disponible sur le SDDC.

Pour installer des instances Citrix ADC VPX sur le cloud VMware, procédez comme suit :

1. Ouvrez VMware SDDC sur votre station de travail.
2. Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur, puis cliquez sur Connexion.
3. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.
4. Dans la boîte de dialogue **Déployer le modèle OVF**, dans **Déployer à partir du fichier**, accédez à l'emplacement où vous avez enregistré les fichiers d'installation d'instance Citrix ADC VPX, sélectionnez le fichier .ovf et cliquez sur **Suivant** .

   > **Remarque :** Par défaut, l'instance Citrix ADC VPX utilise des interfaces réseau E1000. Pour déployer ADC avec l'interface VMXNET3, modifiez l'OVF pour utiliser l'interface VMXNET3 au lieu de l'E1000.

5. Mappez les réseaux affichés dans le modèle OVF de l'appliance virtuelle aux réseaux que vous avez configurés sur VMware SDDC. Cliquez sur **Suivant** pour démarrer l'installation d'une appliance virtuelle sur VMware SDDC.
6. Vous êtes maintenant prêt à démarrer l'instance Citrix ADC VPX. Dans le volet de navigation, sélectionnez l'instance Citrix ADC VPX que vous avez installée et, dans le menu contextuel, sélectionnez **Mettez sous tension**. Cliquez sur l'onglet **Console** pour émuler un port de console.
7. Si vous souhaitez installer un autre dispositif virtuel, répétez l'opération à partir de l'étape 6.
8. Spécifiez l'adresse IP de gestion du même segment que celui sélectionné pour être le réseau de gestion. Le même sous-réseau est utilisé pour la passerelle.
9. Le SDDC VMware exige que les règles NAT et pare-feu soient créées explicitement pour toutes les adresses IP privées appartenant à des segments réseau.

Installer une instance Citrix ADC VPX sur le serveur Microsoft Hyper-V

August 20, 2021

Pour installer des instances Citrix ADC VPX sur Microsoft Windows Server, vous devez d'abord installer Windows Server, avec le rôle Hyper-V activé, sur une machine disposant des ressources système adéquates. Lors de l'installation du rôle Hyper-V, assurez-vous de spécifier les cartes d'interface

réseau sur le serveur qui sera utilisé par Hyper-V pour créer les réseaux virtuels. Vous pouvez réserver certaines cartes d'interface réseau pour l'hôte. Utilisez Hyper-V Manager pour effectuer l'installation de l'instance Citrix ADC VPX.

L'instance Citrix ADC VPX pour Hyper-V est livrée au format disque dur virtuel (VHD). Il inclut la configuration par défaut pour des éléments tels que le CPU, les interfaces réseau, ainsi que la taille et le format du disque dur. Après avoir installé l'instance Citrix ADC VPX, vous pouvez configurer les cartes réseau sur l'appliance virtuelle, ajouter des cartes réseau virtuelles, puis affecter l'adresse IP Citrix ADC, le masque de sous-réseau et la Gateway, et terminer la configuration de base de l'appliance virtuelle.

Après la configuration initiale de l'instance VPX, si vous souhaitez mettre à niveau l'appliance vers la dernière version logicielle, reportez-vous à la section Mise à niveau d'une appliance autonome Citrix ADC VPX.

> **Remarque**
>
> Le protocole ISIS (Intermediate System-to-Intermediate System) n'est pas pris en charge sur l'appliance virtuelle Citrix ADC VPX hébergée sur la plate-forme HyperV-2012.

Conditions préalables à l'installation de l'instance Citrix ADC VPX sur les serveurs Microsoft

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Activez le rôle Hyper-V sur les serveurs Windows. Pour plus d'informations, consultez http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx.
- Téléchargez les fichiers d'installation de l'appliance virtuelle.
- Obtenez les fichiers de licence d'instance Citrix ADC VPX. Pour plus d'informations sur les licences d'instance Citrix ADC VPX, consultez le *Guide de licences Citrix ADC VPX* à l'adresse http://support.citrix.com/article/ctx131110.

Configuration matérielle requise pour le serveur Microsoft

Le tableau suivant décrit la configuration système minimale requise pour les serveurs Microsoft.

Tableau 1. Configuration minimale requise pour les serveurs Microsoft

Composant	Exigences
UC	Processeur 64 bits 1,4 GHz
RAM	8 Go
Espace disque	32 Go ou plus

Le tableau suivant répertorie les ressources informatiques virtuelles pour chaque instance Citrix ADC VPX.

Tableau 2. Ressources de calcul virtuel minimales requises pour exécuter une instance Citrix ADC VPX

Composant	Exigences
RAM	4 Go
CPU virtuel	2
Espace disque	20 Go
Interfaces réseau virtuelles	1

Télécharger les fichiers d'installation de Citrix ADC VPX

L'instance Citrix ADC VPX pour Hyper-V est fournie au format de disque dur virtuel (VHD). Vous pouvez télécharger les fichiers à partir du site Web Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l' adresse http://www.citrix.com, cliquez sur **Connexion > Mon compte > Créer un compte Citrix**, puis suivez les instructions pour créer un compte Citrix.

Pour télécharger les fichiers d'installation d'instance Citrix ADC VPX, procédez comme suit :

1. Depuis un navigateur Web, accédez à http://www.citrix.com/.
2. Connectez-vous avec votre nom d'utilisateur et votre mot de passe.
3. Cliquez sur **Téléchargements**.
4. Dans le menu déroulant **Sélectionner un produit**, sélectionnez **Citrix ADC (NetScaler ADC)**.
5. Sous **Citrix ADC Version X.X > Appliances virtuelles**, cliquez sur **Citrix ADC VPX version X.X**
6. Téléchargez le fichier compressé sur votre serveur.

Installer l'instance Citrix ADC VPX sur les serveurs Microsoft

Après avoir activé le rôle Hyper-V sur Microsoft Server et extrait les fichiers de l'appliance virtuelle, vous pouvez utiliser le Gestionnaire Hyper-V pour installer l'instance Citrix ADC VPX. Après avoir importé la machine virtuelle, vous devez configurer les cartes réseau virtuelles en les associant aux réseaux virtuels créés par Hyper-V.

Vous pouvez configurer un maximum de huit cartes réseau virtuelles. Même si la carte réseau physique est DOWN, l'appliance virtuelle suppose que la carte réseau virtuelle est mise hors tension, car elle peut toujours communiquer avec les autres appliances virtuelles sur le même hôte (serveur).

> **Remarque**
>
> Vous ne pouvez pas modifier les paramètres pendant l'exécution de l'appliance virtuelle. Arrêtez l'appliance virtuelle, puis apportez des modifications.

Pour installer l'instance Citrix ADC VPX sur Microsoft Server à l'aide du Gestionnaire Hyper-V :

1. Pour démarrer le Gestionnaire Hyper-V, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le volet de navigation, sous **Gestion Hyper-V**r, sélectionnez le serveur sur lequel vous souhaitez installer l'instance Citrix ADC VPX.
3. Dans le menu **Action**, cliquez sur **Importer une machine virtuelle**.
4. Dans la boîte de dialogue **Importer une machine virtuelle**, dans **Emplacement**, spécifiez le chemin d'accès du dossier contenant les fichiers logiciels d'instance Citrix ADC VPX, puis sélectionnez **Copier la machine virtuelle (créez un nouvel ID unique)** . Ce dossier est le dossier parent qui contient les dossiers Instantanés, Disques durs virtuels et Machines virtuelles.
5. Remarque : Si vous avez reçu un fichier compressé, assurez-vous d'extraire les fichiers dans un dossier avant de spécifier le chemin d'accès au dossier.
6. Cliquez sur **Importer**.
7. Vérifiez que le dispositif virtuel que vous avez importé est répertorié sous **Machines virtuelles**.
8. Pour installer un autre dispositif virtuel, répétez les étapes **2** à **6** .

> **Important**
>
> Assurez-vous d'extraire les fichiers dans un autre dossier à l'étape **4**.

Mise en service automatique d'une instance Citrix ADC VPX sur Hyper-V

Le provisionnement automatique de l'instance Citrix ADC VPX est facultatif. Si le provisionnement automatique n'est pas effectué, l'appliance virtuelle fournit une option pour configurer l'adresse IP, etc.

Pour configurer automatiquement l'instance Citrix ADC VPX sur Hyper-V, procédez comme suit.

1. Créez une image ISO conforme à la norme ISO9660 à l'aide du fichier xml comme illustré dans l'exemple. Assurez-vous que le nom du fichier xml est **userdata**.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<Environment xmlns:oe=`"http://schemas.dmtf.org/ovf/environment/1`
    "

xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"

oe:id=""
```



```
8
9  xmlns=`"http://schemas.dmtf.org/ovf/environment/1`">
10
11 <PlatformSection>
12
13 <Kind>HYPER-V</Kind>
14
15 <Version>2013.1</Version>
16
17 <Vendor>CISCO</Vendor>
18
19 <Locale>en</Locale>
20
21 </PlatformSection>
22
23 <PropertySection>
24
25 <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"
      />
26
27 <Property oe:key="com.citrix.netscaler.platform" oe:value="NS1000V
      "/>
28
29 <Property oe:key="com.citrix.netscaler.orch_env" oe:value="cisco-
      orch-env"/>
30
31 <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="
      10.102.100.122"/>
32
33 <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
      255.255.255.128"/>
34
35 <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
      10.102.100.67"/></PropertySection>
36
37 </Environment>
38 <!--NeedCopy-->
```

2. Copiez l'image ISO sur le serveur hyper-v.
3. Sélectionnez l'appliance virtuelle que vous avez importée, puis dans le menu **Action**, sélectionnez **Paramètres**. Vous pouvez également sélectionner l'appliance virtuelle, puis cliquer avec le bouton droit et sélectionner **Paramètres**. La fenêtre **Paramètres** du dispositif virtuel sélectionné s'affiche.

4. Dans la fenêtre **Paramètres**, sous la section Matériel, cliquez sur **Contrôleur IDE** .
5. Dans le volet droit de la fenêtre, sélectionnez **Lecteur de DVD** et cliquez sur **Ajouter** . Le lecteur de DVD est ajouté sous la section **Controller IDE** dans le volet gauche de la fenêtre.
6. Sélectionnez le **lecteur de DVD** ajouté à l'étape 5. Dans le volet droit de la fenêtre, sélectionnez le bouton **radio Fichier image**, puis cliquez sur **Parcourir** et sélectionnez l'image ISO que vous avez copiée sur le serveur Hyper-V, à l'étape 2.
7. Cliquez sur **Apply**.

> **Remarque**
>
> L'instance du dispositif virtuel apparaît dans l'adresse IP par défaut, lorsque :
>
> - Le lecteur de DVD est joint et le fichier ISO n'est pas fourni.
> - Le fichier ISO n'inclut pas le fichier de données utilisateur.
> - Le nom ou le format du fichier de données utilisateur n'est pas correct.

Pour configurer des cartes réseau virtuelles sur l'instance Citrix ADC VPX, procédez comme suit :

1. Sélectionnez l'appliance virtuelle que vous avez importée, puis dans le menu **Action**, sélectionnez **Paramètres**.
2. Dans la boîte de dialogue **Paramètres pour <virtual appliance name>**, cliquez sur **Ajouter du matériel** dans le volet gauche.
3. Dans le volet droit, dans la liste des périphériques, sélectionnez **Carte réseau**.
4. Cliquez sur **Ajouter**.
5. Vérifiez que la **carte réseau (non connectée)** s'affiche dans le volet gauche.
6. Sélectionnez la carte réseau dans le volet gauche.
7. Dans le volet droit, dans le menu **Réseau**, sélectionnez le réseau virtuel auquel connecter la carte.
8. Pour sélectionner le réseau virtuel pour les autres cartes réseau que vous souhaitez utiliser, répétez les étapes **6** et **7** .
9. Cliquez sur **Appliquer**, puis sur **OK**.

Pour configurer l'instance Citrix ADC VPX :

1. Cliquez avec le bouton droit sur l'appliance virtuelle précédemment installée, puis sélectionnez **Démarrer**.
2. Accédez à la console en double-cliquant sur le dispositif virtuel.
3. Tapez l'adresse IP Citrix ADC, le masque de sous-réseau et la Gateway de votre appliance virtuelle.

Vous avez terminé la configuration de base de votre appliance virtuelle. Tapez l'adresse IP dans un navigateur Web pour accéder à l'appliance virtuelle.

> **Remarque**
>
> Vous pouvez également utiliser le modèle de machine virtuelle (VM) pour provisionner l'instance Citrix ADC VPX à l'aide de SCVMM.
>
> Si vous utilisez la solution d'association de cartes réseau Microsoft Hyper-V avec des instances NetScaler VPX, consultez l'article CTX224494 pour plus d'informations.

Installer une instance Citrix ADC VPX sur la plate-forme Linux-KVM

August 20, 2021

Pour configurer un Citrix ADC VPX pour la plate-forme KVM Linux, vous pouvez utiliser l'application graphique Virtual Machine Manager (Virtual Manager). Si vous préférez la ligne de commande Linux-KVM, vous pouvez utiliser le `virsh` programme.

Le système d'exploitation Linux hôte doit être installé sur du matériel approprié à l'aide d'outils de virtualisation tels que le module KVM et QEMU. Le nombre de machines virtuelles pouvant être déployées sur l'Hypervisor dépend des besoins de l'application et du matériel choisi.

Une fois que vous avez provisionné une instance Citrix ADC VPX, vous pouvez ajouter d'autres interfaces.

Limitations et directives d'utilisation

Recommandations générales

Pour éviter tout comportement imprévisible, appliquez les recommandations suivantes :

- Ne modifiez pas le MTU de l'interface VNet associée à la machine virtuelle VPX. Arrêtez la machine virtuelle VPX avant de modifier les paramètres de configuration, tels que les modes d'interface ou le processeur.
- Ne forcez pas l'arrêt de la machine virtuelle VPX. Autrement dit, n'utilisez pas la commande **Force off** .
- Toutes les configurations effectuées sur l'hôte Linux peuvent ou non être persistantes, en fonction de vos paramètres de distribution Linux. Vous pouvez choisir de rendre ces configurations persistantes afin d'assurer un comportement cohérent lors des redémarrages du système d'exploitation Linux hôte.
- Le package Citrix ADC doit être unique pour chacune des instances Citrix ADC VPX provisionnées.

Limitations

- La migration en direct d'une instance VPX exécutée sur KVM n'est pas prise en charge.

Conditions préalables à l'installation d'une instance Citrix ADC VPX sur la plate-forme Linux-KVM

August 20, 2021

Vérifiez la configuration système minimale requise pour un serveur KVM Linux exécuté sur une instance Citrix ADC VPX.

Exigence du processeur :

- Processeurs x86 64 bits dotés de la fonctionnalité de virtualisation matérielle incluse dans les processeurs Intel VT-X.

Pour vérifier si votre processeur prend en charge l'hôte Linux, entrez la commande suivante à l'invite de commandes Linux de l'hôte :

```
\*.egrep '^flags.\*(vmx|svm)' /proc/cpuinfo*
<!--NeedCopy-->
```

Si les paramètres du **BIOS** de l'extension précédente sont désactivés, vous devez les activer dans le BIOS.

- Fournir au moins 2 cœurs CPU à Host Linux.
- Il n'y a pas de recommandation spécifique pour la vitesse du processeur, mais plus la vitesse est élevée, meilleures sont les performances de l'application VM.

Mémoire requise (RAM) :

Minimum 4 Go pour le noyau Linux hôte. Ajoutez davantage de mémoire selon les besoins des machines virtuelles.

Disque dur requis :

Calculez l'espace requis pour le noyau et la machine virtuelle hôte Linux. Une seule machine virtuelle Citrix ADC VPX nécessite 20 Go d'espace disque.

Configuration logicielle requise

Le noyau hôte utilisé doit être un noyau Linux 64 bits, version 2.6.20 ou ultérieure, avec tous les outils de virtualisation. Citrix recommande des noyaux plus récents, tels que 3.6.11-4 et versions ultérieures.

De nombreuses distributions Linux telles que Red Hat, CentOS et Fedora ont testé les versions du noyau et les outils de virtualisation associés.

Configuration matérielle requise pour les machines virtuelles invitées

Citrix ADC VPX prend en charge le type de disque dur IDE et VirtiO. Le type de disque dur a été configuré dans le fichier XML, qui fait partie du package Citrix ADC.

Exigences de mise en réseau

Citrix ADC VPX prend en charge les interfaces réseau para-virtualisées VirtiO, SR-IOV et PCI Passthrough.

Pour plus d'informations sur les interfaces réseau prises en charge, voir :

- Provisionner l'instance Citrix ADC VPX à l'aide de Virtual Machine Manager
- Configurer une instance Citrix ADC VPX pour utiliser les interfaces réseau SR-IOV
- Configurer une instance Citrix ADC VPX pour utiliser les interfaces réseau PCI

Interface source et modes

Le type de périphérique source peut être Bridge ou MacVTap. Dans MacVTAP, quatre modes sont possibles : VEPA, Bridge, Private et Pass-Through. Vérifiez les types d'interfaces que vous pouvez utiliser et les types de trafic pris en charge, comme suit :

Pont :

- Pont Linux.
- `Ebtables` et `iptables` les paramètres sur l'hôte Linux peuvent filtrer le trafic sur le pont si vous ne choisissez pas le bon paramètre ou si vous ne désactivez pas les `IPtable` services.

MacVTap (mode VEPA) :

- Meilleure performance qu'un pont.
- Les interfaces du même périphérique inférieur peuvent être partagées entre les machines virtuelles.
- Communication inter-VM utilisant la même
- l'appareil inférieur n'est possible que si le commutateur en amont ou en aval prend en charge le mode VEPA.

MacVTap (mode privé) :

- Meilleure performance qu'un pont.
- Les interfaces du même périphérique inférieur peuvent être partagées entre les machines virtuelles.
- La communication inter-VM utilisant le même périphérique inférieur n'est pas possible.

MacVTap (mode pont) :

- Meilleur comparativement au pont.

- Les interfaces situées sur le même appareil inférieur peuvent être partagées entre les machines virtuelles.
- La communication entre machines virtuelles utilisant le même périphérique inférieur est possible si la liaison inférieure du périphérique est UP.

MacVTap (mode Pass-through) :

- Meilleur comparativement au pont.
- Les interfaces hors du même appareil inférieur ne peuvent pas être partagées entre les machines virtuelles.
- Une seule machine virtuelle peut utiliser le périphérique inférieur.

> Remarque : Pour obtenir les meilleures performances de l'instance VPX, assurez-vous que les `lro` fonctionnalités `gro` et sont désactivées sur les interfaces source.

Propriétés des interfaces source

Assurez-vous de désactiver les fonctions generic-receve-offload (`gro`) et large receve-offload (`lro`) des interfaces source. Pour désactiver les `lro` fonctionnalités `gro` et, exécutez les commandes suivantes à l'invite du shell Linux hôte.

```
ethtool -K eth6 gro off
ethool -K eth6 lro off
```

Exemple :

```
1     [root@localhost ~]# ethtool -K eth6
2
3                   Offload parameters for eth6:
4
5                                       rx-checksumming: on
6
7                                       tx-checksumming: on
8
9                   scatter-gather: on
10
11                  tcp-segmentation-offload: on
12
13                  udp-fragmentation-offload: off
14
15                  generic-segmentation-offload: on
16
17                  generic-receive-offload: off
18
19                  large-receive-offload: off
```



```
20
21                      rx-vlan-offload: on
22
23                      tx-vlan-offload: on
24
25                      ntuple-filters: off
26
27                      receive-hashing: on
28
29      [root@localhost ~]#
30  <!--NeedCopy-->
```

Exemple :

Si le pont Linux hôte est utilisé comme périphérique source, comme dans l'exemple suivant, et que les `lro` fonctionnalités doivent être désactivées sur les interfaces VNet, qui sont les interfaces virtuelles connectant l'hôte aux machines virtuelles invitées.

```
1       [root@localhost ~]# brctl show eth6_br
2
3       bridge name     bridge  id              STP enabled interfaces
4
5       eth6_br         8000.00e0ed1861ae          no          eth6
6
7                                                              vnet0
8
9                                                              vnet2
10
11      [root@localhost ~]#
12  <!--NeedCopy-->
```

Dans l'exemple précédent, les deux interfaces virtuelles sont dérivées de eth6_br et sont représentées par vnet0 et vnet2. Exécutez les commandes suivantes pour désactiver `gro` et désactiver `lro` les fonctionnalités de ces interfaces.

```
1       ethtool -K vnet0 gro off
2               ethtool -K vnet2 gro off
3               ethtool -K vnet0 lro off
4                       ethtool -K vnet2 lro off
5   <!--NeedCopy-->
```

Mode promiscuité

Le mode promiscuous doit être activé pour que les fonctionnalités suivantes fonctionnent :

- Mode L2
- Traitement du trafic multidiffusion
- Diffuser
- Trafic IPV6
- MAC virtuel
- Routage dynamique

Utilisez la commande suivante pour activer le mode promiscuité.

```
[root@localhost ~]# ifconfig eth6 promisc
[root@localhost ~]# ifconfig eth6
eth6       Link encap:Ethernet  HWaddr 78:2b:cb:51:54:a3
           inet6 addr: fe80::7a2b:cbff:fe51:54a3/64 Scope:Link
           UP BROADCAST RUNNING PROMISC MULTICAST  MTU:9000  Metric:1
           RX packets:142961 errors:0 dropped:0 overruns:0 frame:0
           TX packets:2895843 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:14330008 (14.3 MB)  TX bytes:1019416071 (1.0 GB)

[root@localhost ~]#
<!--NeedCopy-->
```

Module requis

Pour de meilleures performances réseau, assurez-vous que le module vhost_net est présent dans l'hôte Linux. Pour vérifier l'existence du module vhost_net, exécutez la commande suivante sur l'hôte Linux :

```
lsmod | grep "vhost_net"
<!--NeedCopy-->
```

Si vhost_net n'est pas encore en cours d'exécution, entrez la commande suivante pour l'exécuter :

```
modprobe vhost_net
<!--NeedCopy-->
```

Provisionner l'instance Citrix ADC VPX à l'aide d'OpenStack

August 20, 2021

Vous pouvez provisionner une instance Citrix ADC VPX dans un environnement OpenStack à l'aide de la commande **Nova boot** (CLI OpenStack) ou Horizon (tableau de bord OpenStack).

Le provisioning d'une instance VPX implique éventuellement l'utilisation de données provenant du lecteur de configuration. Le lecteur de configuration est un lecteur de configuration spécial qui se fixe à l'instance en tant que périphérique de CD-ROM lorsqu'il démarre. Ce lecteur de configuration peut être utilisé pour transmettre la configuration réseau telle que l'adresse IP de gestion, le masque réseau, la Gateway par défaut et pour injecter des scripts client.

Dans une appliance Citrix ADC, le mécanisme d'authentification par défaut est basé sur un mot de passe. Désormais, le mécanisme d'authentification par paires de clés SSH est pris en charge pour les instances Citrix ADC VPX dans l'environnement OpenStack.

La paire de clés (clé publique et clé privée) est générée avant d'utiliser le mécanisme de cryptographie à clé publique. Vous pouvez utiliser différents mécanismes, tels que Horizon, Puttygen.exe pour Windows et `ssh-keygen` pour l'environnement Linux, pour générer la paire de clés. Reportez-vous à la documentation en ligne des mécanismes respectifs pour plus d'informations sur la génération de paires de clés.

Une fois qu'une paire de clés est disponible, copiez la clé privée dans un emplacement sécurisé auquel les personnes autorisées ont accès. Dans OpenStack, la clé publique peut être déployée sur une instance VPX à l'aide de la commande Horizon ou Nova boot. Lorsqu'une instance VPX est provisionnée à l'aide d'OpenStack, elle détecte d'abord que l'instance démarre dans un environnement OpenStack en lisant une chaîne BIOS spécifique. Cette chaîne est « OpenStack Foundation » et pour les distributions Red Hat Linux, elle est stockée dans /etc/nova/release. Il s'agit d'un mécanisme standard disponible dans toutes les implémentations OpenStack basées sur la plateforme d'hyperviseur KVM. Le disque doit comporter une étiquette OpenStack spécifique.

Si le lecteur de configuration est détecté, l'instance tente de lire la configuration réseau, les scripts personnalisés et la paire de clés SSH si elle est fournie.

Fichier de données utilisateur

L'instance Citrix ADC VPX utilise un fichier OVF personnalisé, également connu sous le nom de fichier de données utilisateur, pour injecter des scripts personnalisés de configuration réseau. Ce fichier est fourni dans le cadre du lecteur de configuration. Voici un exemple de fichier OVF personnalisé.

```
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1"
xmlns:cs="http://schemas.citrix.com/openstack">
<PlatformSection>
<Kind></Kind>
<Version>2016.1</Version>
```

 
```

```
<Vendor>VPX</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
<Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
<Property oe:key="com.citrix.netscaler.orch_env" oe:value="openstack-
   orch-env"/>
<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"/>
<Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
   255.255.255.0"/>
<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="10.1.2.1
   "/>
</PropertySection>
 <cs:ScriptSection>
   <cs:Version>1.0</cs:Version>
     <ScriptSettingSection xmlns="http://schemas.citrix.com/openstack"
        xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
         <Scripts>
           <Script>
                 <Type>shell</Type>
                 <Parameter>X Y</Parameter>
                <Parameter>Z</Parameter>
                <BootScript>before</BootScript>
                  <Text>
                       #!/bin/bash
                       echo "Hi, how are you" $1 $2 >> /var/sample.txt
                  </Text>
           </Script>
           <Script>
                 <Type>python</Type>
                 <BootScript>after</BootScript>
                  <Text>
                      #!/bin/python
print("Hello");
                  </Text>
           </Script>
   <Script>
                 <Type>perl</Type>
                 <BootScript>before</BootScript>
                  <Text>
                      !/usr/bin/perl
my $name = "VPX";
print "Hello, World $name !\n" ;
                  </Text>
```



```
52             </Script>
53             <Script>
54                  <Type>nscli</Type>
55                  <BootScript>after</BootScript>
56                  <Text>
57                   add vlan 33
58  bind vlan 33 -ifnum 1/2
59                  </Text>
60             </Script>
61           </Scripts>
62       </ScriptSettingSection>
63  </cs:ScriptSection>
64 </Environment>
65 <!--NeedCopy--> ```
```

Dans le fichier OVF précédant « PropertySection » est utilisé pour la configuration réseau NetScaler alors qu' <cs:ScriptSection> il est utilisé pour enfermer tous les scripts. <Scripts></Scripts> sont utilisées pour regrouper tous les scripts ensemble. Chaque script est défini entre les <Script> </Script> balises. Chaque balise de script comporte les champs/balises suivants :

a) <Type> : Spécifie la valeur du type de script. Valeurs possibles : Shell/Perl/Python/NSLCI (pour les scripts CLI NetScaler)

b) <Parameter> : Fournit des paramètres au script. Chaque script peut avoir plusieurs <Parameter> balises.

c) <BootScript> : Spécifie le point d'exécution du script. Valeurs possibles pour cette balise : avant/après. « avant » indique que le script est exécuté avant l'apparition de PE. « after » indique que le script sera exécuté après l'arrivée de PE.

d) <Text> : Colle le contenu d'un script.

> **Remarque**
>
> Actuellement, l'instance VPX ne prend pas en charge la désinfection des scripts. En tant qu'administrateur, vous devez vérifier la validité du script.
>
> Toutes les sections ne doivent pas être présentes. Utilisez une « PropertySection » vide pour définir uniquement les scripts à exécuter au premier démarrage ou une fenêtre vide pour définir uniquement la configuration réseau.
>
> Une fois que les sections requises du fichier OVF (fichier de données utilisateur) sont remplies, utilisez ce fichier pour provisionner l'instance VPX.

Configuration réseau

Dans le cadre de la configuration réseau, l'instance VPX lit :

- Adresse IP de gestion
- Masque réseau
- Gateway par défaut

Une fois les paramètres lus avec succès, ils sont renseignés dans la configuration NetScaler, afin de permettre la gestion à distance de l'instance. Si les paramètres ne sont pas lus correctement ou si le lecteur de configuration n'est pas disponible, l'instance passe au comportement par défaut, qui est :

- L'instance tente de récupérer les informations d'adresse IP à partir de DHCP.
- Si DHCP échoue ou s'arrête, l'instance présente la configuration réseau par défaut (192.168.100.1/16).

Script client

L'instance VPX permet d'exécuter un script personnalisé pendant le provisionnement initial. L'appliance prend en charge les scripts de type Shell, Perl, Python et Citrix ADC CLI.

Authentification par paire de clés SSH

L'instance VPX copie la clé publique, disponible dans le lecteur de configuration dans le cadre des métadonnées d'instance, dans son fichier « authorized_keys ». Cela permet à l'utilisateur d'accéder à l'instance avec une clé privée.

> **Remarque**
>
> Lorsqu'une clé SSH est fournie, les informations d'identification par défaut (nsroot/nsroot) ne fonctionnent plus. Si un accès par mot de passe est nécessaire, ouvrez une session avec la clé privée SSH respective et définissez manuellement un mot de passe.

Avant de commencer

Avant de provisionner une instance VPX sur un environnement OpenStack, extrayez le `.qcow2` fichier du fichier .tgz et générez

Une image OpenStack de l'image qcow2. Procédez comme suit :

1. Extrayez le `.qcow2` fichier du `.tqz` fichier en tapant la commande suivante

```
tar xvzf <TAR file>
tar xvzf <NSVPX-KVM-12.0-26.2_nc.tgz>
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
```

2. Créez une image OpenStack à l'aide du `.qcoz2` fichier extrait à l'étape 1 en tapant la commande suivante.


```
openstack image create --container-format bare --property
    hw_disk_bus=ide --disk-format qcow2 --file <path to qcow2 file>
     --public <name of the OpenStack image>

glance image-create --name="NS-VPX-12-0-26-2" --property
    hw_disk_bus=ide --ispublic=
true --container-format=bare --disk-format=qcow2< NSVPX-KVM
    -12.0-26.2_nc.qcow2
```

Figure 1 : L'illustration suivante fournit un exemple de sortie pour la commande glance image-create.

```
+------------------+--------------------------------------------------------+
| Field            | Value                                                  |
+------------------+--------------------------------------------------------+
| checksum         | 154ade3fc7dca7d1706b1d03d7d97552                       |
| container_format | bare                                                   |
| created_at       | 2017-03-13T08:52:31Z                                   |
| disk_format      | qcow2                                                  |
| file             | /v2/images/322c1e0f-cce8-4b7b-b53e-bd8152c388ed/file   |
| id               | 322c1e0f-cce8-4b7b-b53e-bd8152c388ed                   |
| min_disk         | 0                                                      |
| min_ram          | 0                                                      |
| name             | VPX-KVM-12.0-26.2                                      |
| owner            | 58d17d81df5d4406afbb4fdab3a58d79                       |
| properties       | hw_disk_bus='ide'                                      |
| protected        | False                                                  |
| schema           | /v2/schemas/image                                      |
| size             | 784338944                                              |
| status           | active                                                 |
| updated_at       | 2017-03-13T08:52:43Z                                   |
| virtual_size     | None                                                   |
| visibility       | public                                                 |
+------------------+--------------------------------------------------------+
```

Provisionnement de l'instance VPX

Vous pouvez provisionner une instance VPX de deux façons en utilisant l'une des options suivantes :

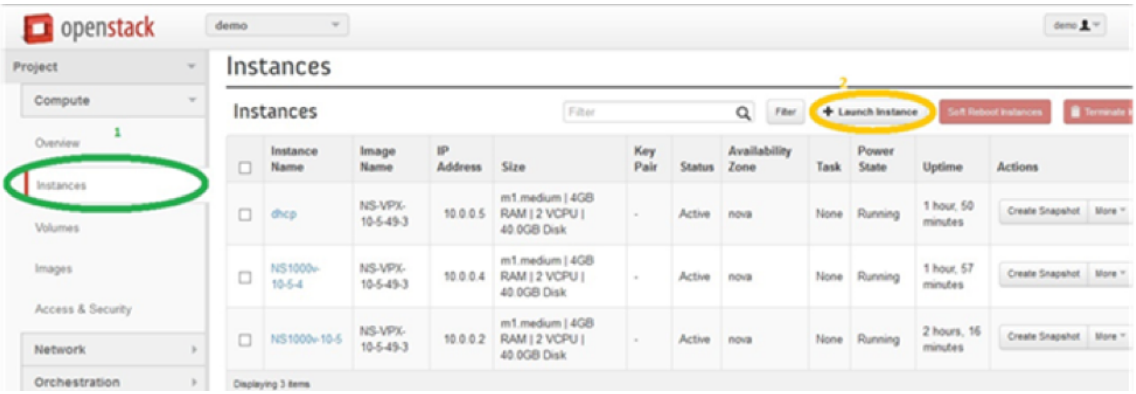
- Horizon (tableau de bord OpenStack)
- Commande de démarrage Nova (CLI OpenStack)

Provisionner une instance VPX à l'aide du tableau de bord OpenStack

Procédez comme suit pour provisionner l'instance VPX à l'aide d'Horizon :

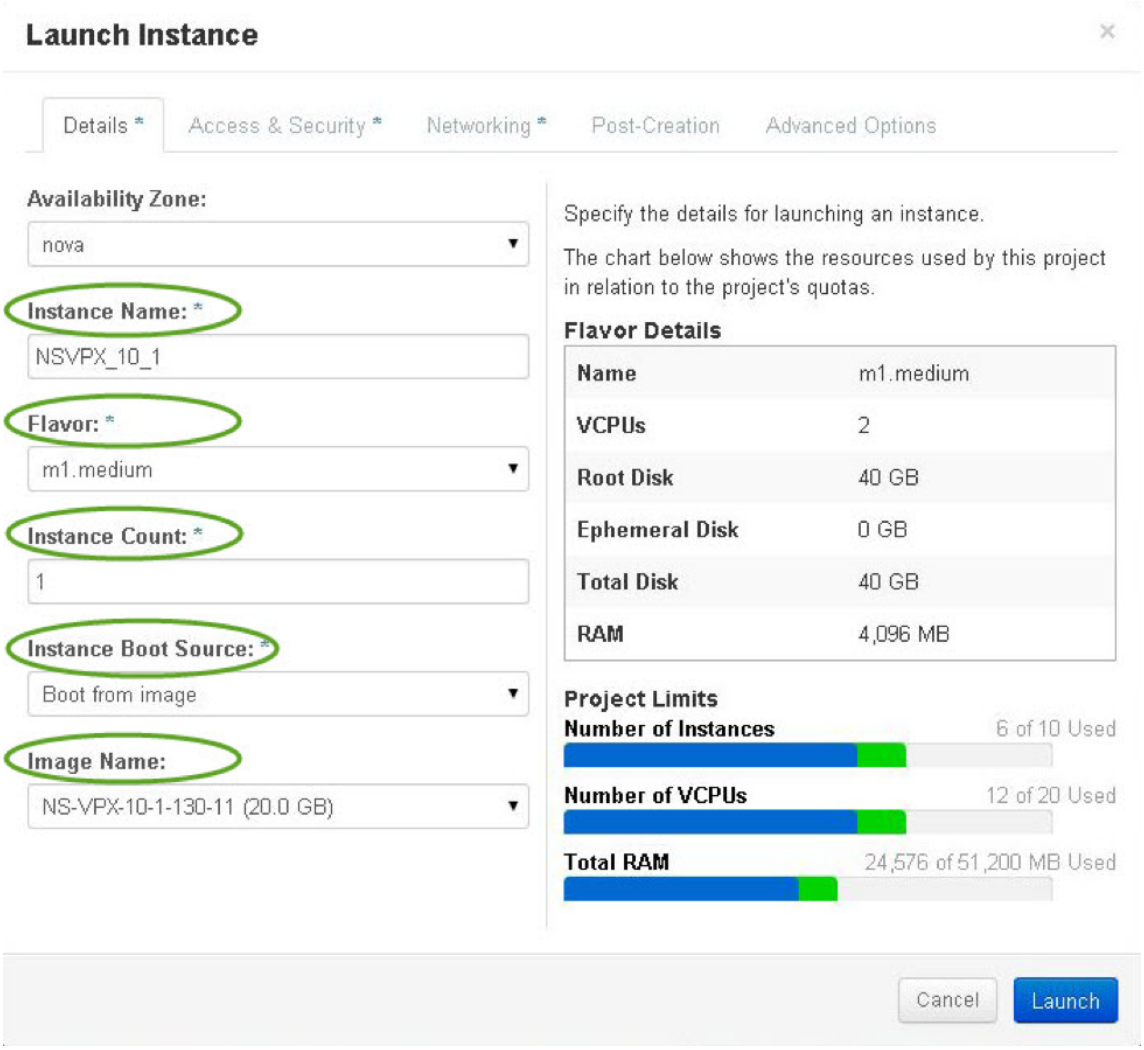
1. Connectez-vous au tableau de bord OpenStack.
2. Dans le panneau Projet situé à gauche du tableau de bord, sélectionnez **Instances**.

3. Dans le panneau Instances, cliquez sur **Lancer une instance** pour ouvrir l'Assistant Lancement d'instance.



4. Dans l'assistant de lancement d'instance, entrez les détails, tels que :

   a) Nom de l'instance
   b) Saveur d'instance
   c) Nombre d'instances
   d) Source de démarrage d'instance
   e) Nom de l'image



5. Déployez une nouvelle paire de clés ou une paire de clés existante via Horizon en procédant comme suit :

   a) Si vous n'avez pas de paire de clés existante, créez la clé à l'aide des mécanismes existants. Si vous avez une clé existante, ignorez cette étape.

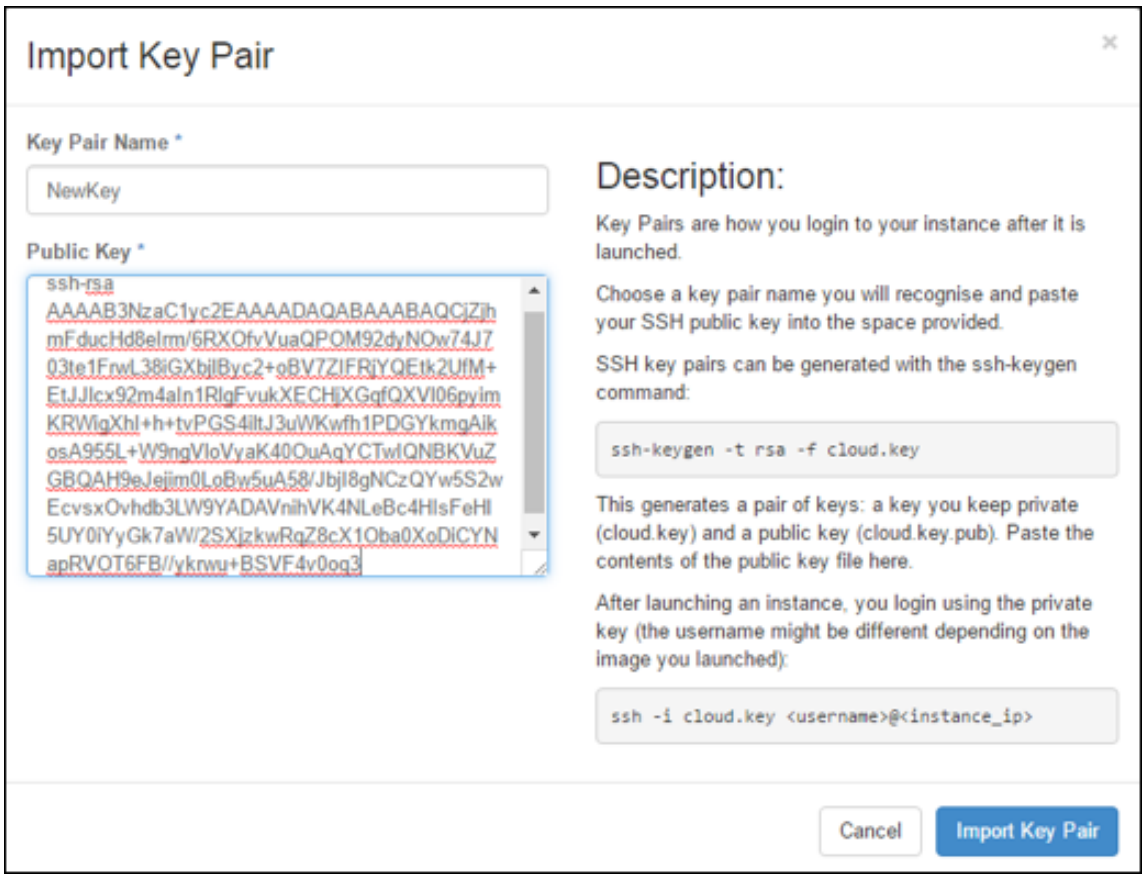
   b) Copier le contenu de la clé publique.

   c) Accédez à **Horizon > Instances > Créer de nouvelles instances**.

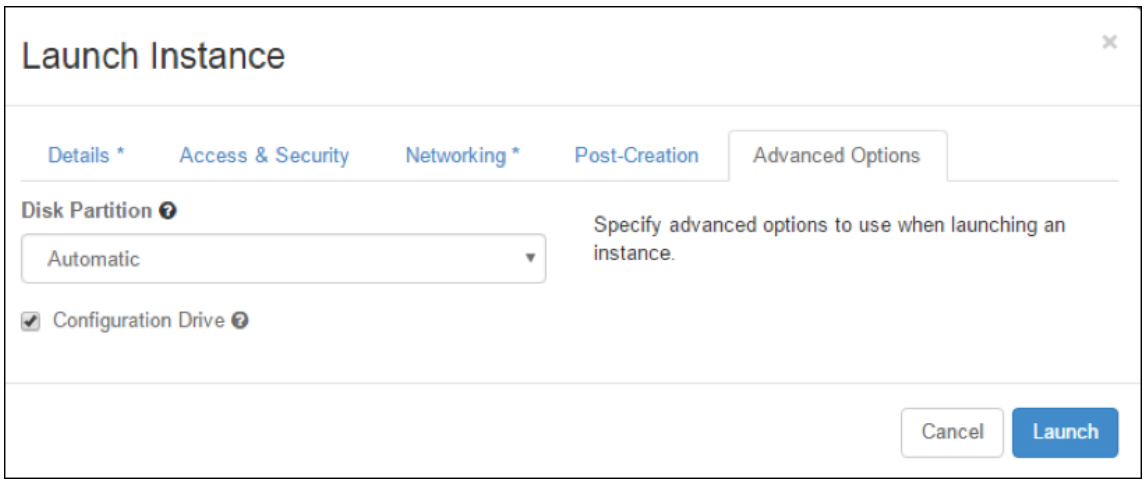
   d) Cliquez sur **Accès et sécurité**.

   e) Cliquez sur le signe+ en regard du menu déroulant **Paire de clés** et indiquez les valeurs des paramètres affichés.

   f) Collez le contenu de la *clé publique dans la zone Clé publique*, donnez un nom à la clé et cliquez sur **Importer la paire de clés** .



6. Cliquez sur l'onglet **Création de publications** dans l'Assistant. Dans le script de personnalisation, ajoutez le contenu du fichier de données utilisateur. Le fichier de données utilisateur contient l'adresse IP, les détails du masque réseau et de la passerelle, ainsi que les scripts client de l'instance VPX.
7. Une fois qu'une paire de clés est sélectionnée ou importée, cochez l'option config-drive et cliquez sur **Launch**.



Provisionner l'instance VPX à l'aide de l'interface de ligne de commande OpenStack

Procédez comme suit pour provisionner une instance VPX à l'aide de l'interface de ligne de commande OpenStack.

1. Pour créer une image à partir de qcow2, tapez la commande suivante :

   ```
   openstack image create --container-format bare --property hw_disk_bus=
   ide --diskformat qcow2 --file NSVPX-OpenStack.qcow2 --public VPX-ToT-
   Image
   ```

2. Pour sélectionner une image pour créer une instance, tapez la commande suivante :

   ```
   openstack image list | more
   ```

3. Pour créer une instance d'une saveur particulière, tapez la commande suivante pour choisir un ID de saveur dans une liste :

   ```
   openstack flavor list
   ```

4. Pour attacher une carte réseau à un réseau particulier, tapez la commande suivante pour choisir un ID réseau dans une liste réseau :

   ```
   openstack network list
   ```

5. Pour créer une instance, tapez la commande suivante :

   ```
   1 openstack server create --flavor FLAVOR_ID --image IMAGE_ID --key-
       name KEY_NAME
   2 --user-data USER_DATA_FILE_PATH --config-drive True --nic net-id=
       net-uuid
   3 INSTANCE_NAME
   4 openstack server create --image VPX-ToT-Image --flavor m1.medium
       --user-data
   5 ovf.xml --config-drive True --nic net-id=2734911b-ee2b-48d0-a1b6-3
       efd44b761b9
   6 VPX-ToT
   ```

Figure 2 : L'illustration suivante fournit un exemple de sortie.

Field	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	None
OS-EXT-SRV-ATTR:hypervisor_hostname	None
OS-EXT-SRV-ATTR:instance_name	instance-000001c2
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	None
OS-SRV-USG:terminated_at	None
accessIPv4	
accessIPv6	
addresses	
adminPass	pFVvMtq7N8Z6
config_drive	True
created	2017-03-13T10:32:59Z
flavor	m1.medium (3)
hostId	
id	a1fe991e-3604-43a0-9dd6-59fa0f3749df
image	VPX-ToT-Image (f0c2f9d1-08f2-4b2e-9943-2ee6bc2edbc7)
key_name	None
name	VPX-ToT
os-extended-volumes:volumes_attached	[]
progress	0
project_id	58d17d81df5d4406afbb4fdab3a58d79
properties	
security_groups	[{u'name': u'default'}]
status	BUILD
updated	2017-03-13T10:33:00Z
user_id	a6347b33916b4eb1b1f76360a9c8f935

Provisionner l'instance Citrix ADC VPX à l'aide de Virtual Machine Manager

August 20, 2021

Virtual Machine Manager est un outil de bureau pour gérer les invités de machines virtuelles. Il vous permet de créer de nouveaux invités VM et différents types de stockage, et de gérer des réseaux virtuels. Vous pouvez accéder à la console graphique des invités de machines virtuelles à l'aide de la visionneuse VNC intégrée et afficher les statistiques de performances, localement ou à distance.

Après avoir installé votre distribution Linux préférée, avec la virtualisation KVM activée, vous pouvez procéder au Provisioning des machines virtuelles.

Lorsque vous utilisez Virtual Machine Manager pour provisionner une instance Citrix ADC VPX, vous avez deux options :

- Entrez manuellement l'adresse IP, la Gateway et le masque de réseau
- Attribuer automatiquement l'adresse IP, la Gateway et le masque de réseau (provisionnement automatique)

Vous pouvez utiliser deux types d'images pour provisionner une instance Citrix ADC VPX :

- RAW
- QCOW2

Vous pouvez convertir une image Citrix ADC VPX RAW en image QCOW2 et provisionner l'instance Citrix ADC VPX. Pour convertir l'image RAW en une image QCOW2, tapez la commande suivante :

```
qemu-img convert -O qcow2 original-image.raw image-converted.qcow
```

Par exemple :

```
qemu-img convert -O qcow2 NSVPX-KVM-11.1-12.5_nc.raw NSVPX-KVM-11.1-12.5_nc
.qcow
```

Un déploiement Citrix ADC VPX type sur KVM comprend les étapes suivantes :

- Vérification des conditions préalables pour le provisionnement automatique d'une instance Citrix ADC VPX
- Provisionnement de l'instance Citrix ADC VPX à l'aide d'une image RAW
- Provisionnement de l'instance Citrix ADC VPX à l'aide d'une image QCOW2
- Ajout d'interfaces supplémentaires à une instance VPX à l'aide de Virtual Machine Manager

Vérifier les conditions préalables pour le provisionnement automatique d'une instance Citrix ADC VPX

Le provisionnement automatique est une fonctionnalité facultative qui implique l'utilisation de données provenant du lecteur de CD-ROM. Si cette fonctionnalité est activée, vous n'avez pas besoin d'entrer l'adresse IP de gestion, le masque réseau et la Gateway par défaut de l'instance Citrix ADC VPX lors de l'installation initiale.

Vous devez effectuer les tâches suivantes avant de pouvoir provisionner automatiquement une instance VPX :

1. Créez un fichier XML OVF (Open Virtualization Format) personnalisé ou un fichier de données utilisateur.
2. Convertissez le fichier OVF en image ISO à l'aide d'une application en ligne (par exemple PowerISO).
3. Montez l'image ISO sur l'hôte KVM à l'aide de n'importe quel outil SCP (Secure Copy).

Exemple de fichier XML OVF :

Voici un exemple de contenu d'un fichier XML OVF, que vous pouvez utiliser comme exemple pour créer votre fichier.

```
1 <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2
3 <Environment xmlns:oe="`http://schemas.dmtf.org/ovf/environment/1"`
4
5 xmlns:xsi="`http://www.w3.org/2001/XMLSchema-instance"`
6
7 oe:id=""
```



```
8
9  xmlns="`http://schemas.dmtf.org/ovf/environment/1"`
10
11 xmlns:cs="`http://schemas.citrix.com/openstack">`
12
13 <PlatformSection>
14
15 <Kind></Kind>
16
17 <Version>2016.1</Version>
18
19 <Vendor>VPX</Vendor>
20
21 <Locale>en</Locale>
22
23 </PlatformSection>
24
25 <PropertySection>
26
27 <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
28
29 <Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
30
31 <Property oe:key="com.citrix.netscaler.orch_env" oe:value="KVM"/>
32
33 <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"/>
34
35 <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
      255.255.255.0"/>
36
37 <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="10.1.2.1
      "/>
38
39 </PropertySection>
40
41 </Environment>
42 <!--NeedCopy-->
```

Dans le fichier XML OVF précédent, « PropertySection » est utilisé pour la configuration réseau NetScaler. Lorsque vous créez le fichier, spécifiez les valeurs des paramètres qui sont mis en surbrillance à la fin de l'exemple :

- Adresse IP de gestion
- Masque réseau
- Gateway

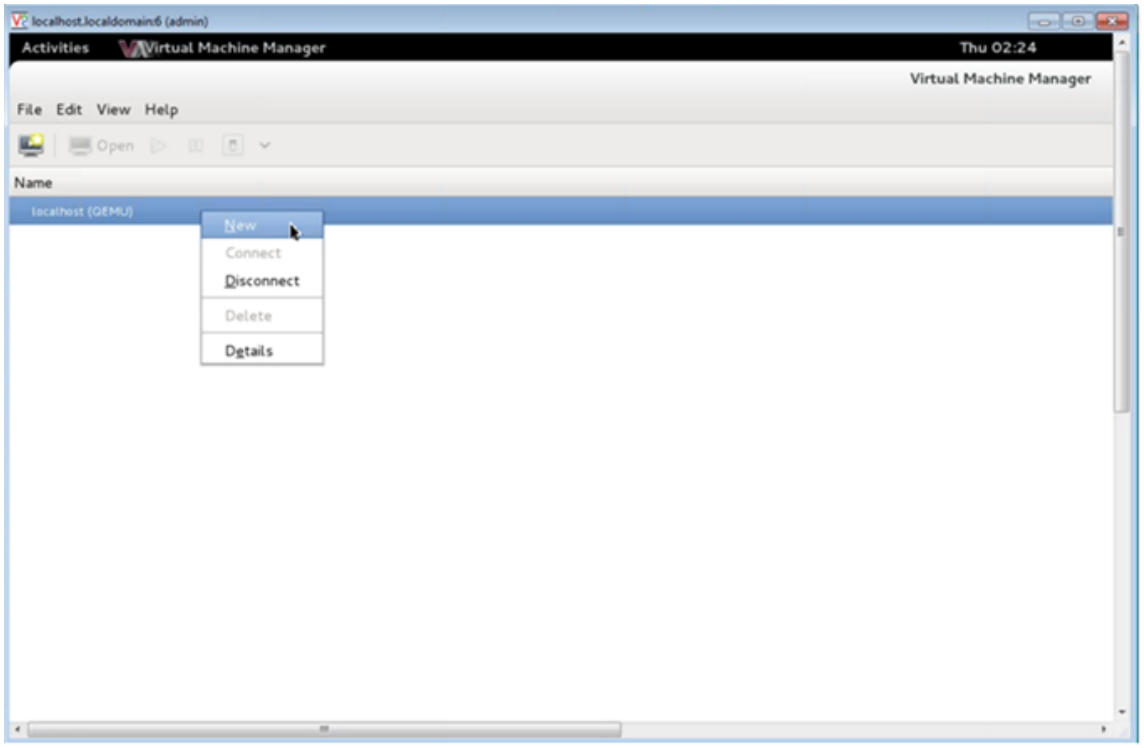
> **Important**
>
> Si le fichier OVF n'est pas correctement formaté XML, l'instance VPX se voit attribuer la configuration réseau par défaut, et non les valeurs spécifiées dans le fichier.

Provisionner l'instance Citrix ADC VPX à l'aide d'une image RAW

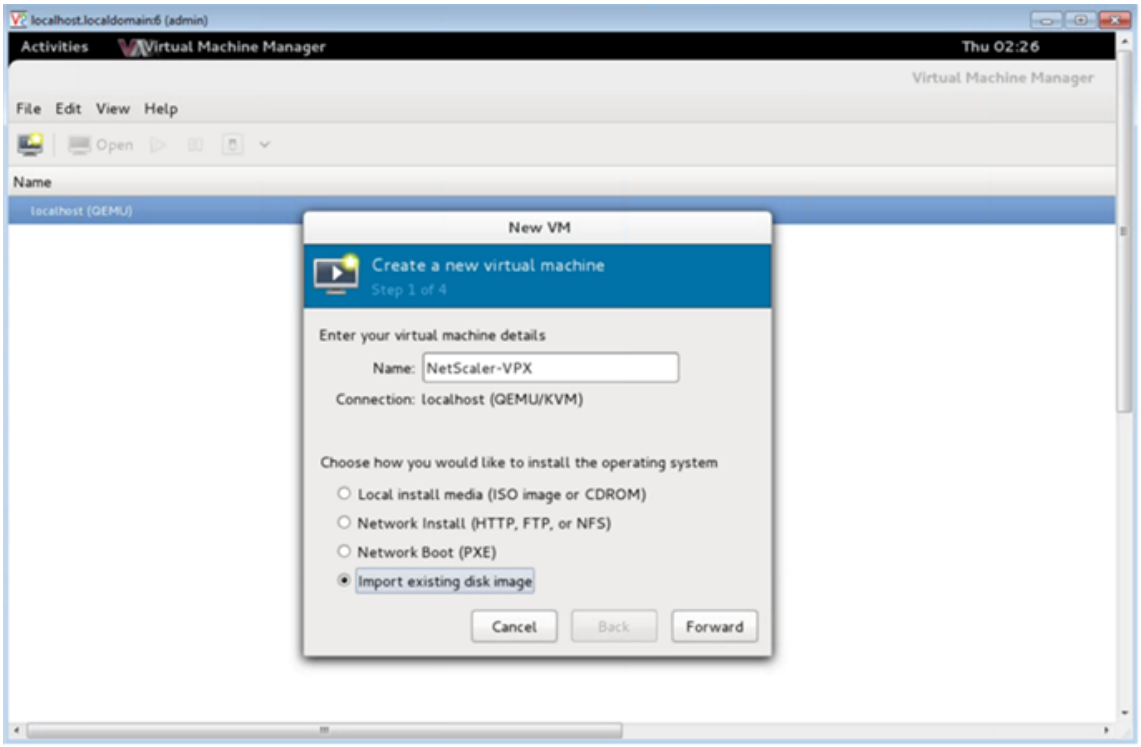
Virtual Machine Manager vous permet de provisionner une instance Citrix ADC VPX à l'aide d'une image RAW.

Pour provisionner une instance Citrix ADC VPX à l'aide de Virtual Machine Manager, procédez comme suit :

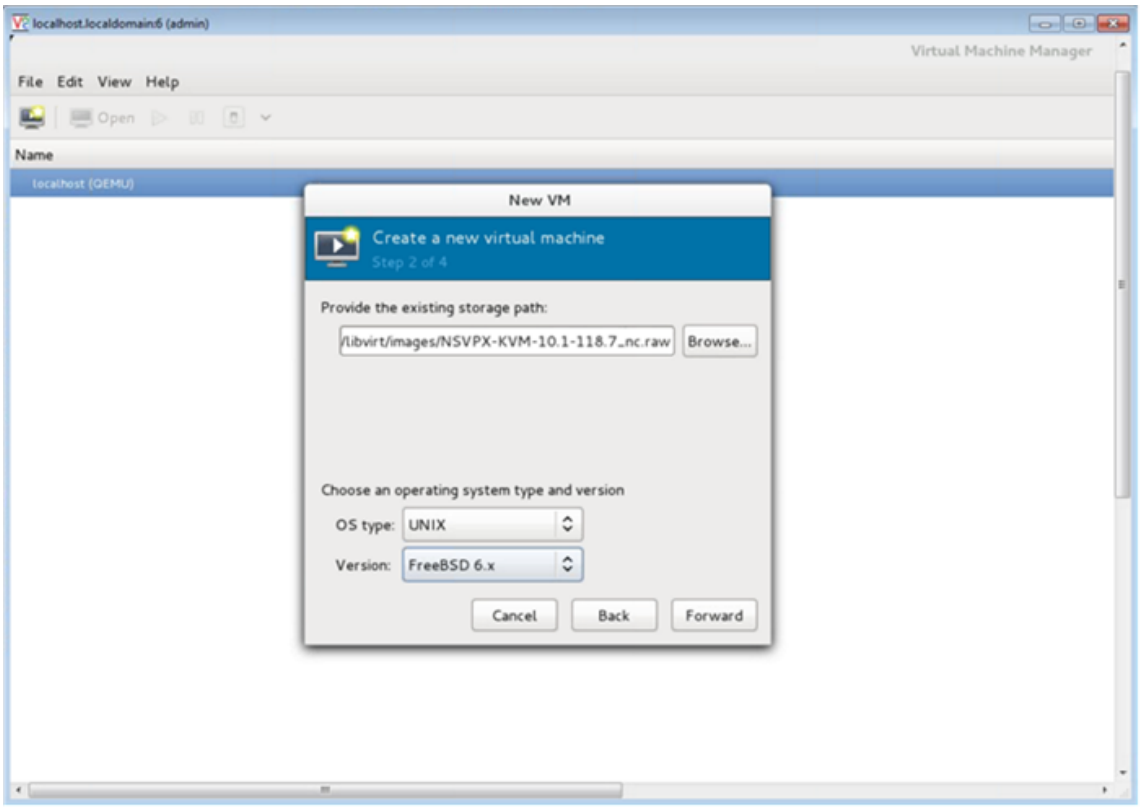
1. Ouvrez Virtual Machine Manager (**Application** > **Outils système** > **Virtual Machine Manager**) et entrez les informations d'identification d'ouverture de session dans la fenêtre **Authentifier** .
2. Cliquez sur l'icône  ou cliquez avec le bouton droit sur **localhost (QEMU)** pour créer une nouvelle instance Citrix ADC VPX.



3. Dans la zone de texte **Nom**, entrez un nom pour la nouvelle machine virtuelle (par exemple, NetScaler-VPX).
4. Dans la fenêtre **Nouvelle machine virtuelle**, sous « Choisissez comment vous souhaitez installer le système d'exploitation », sélectionnez **Importer une image disque existante**, puis cliquez sur **Transférer** .

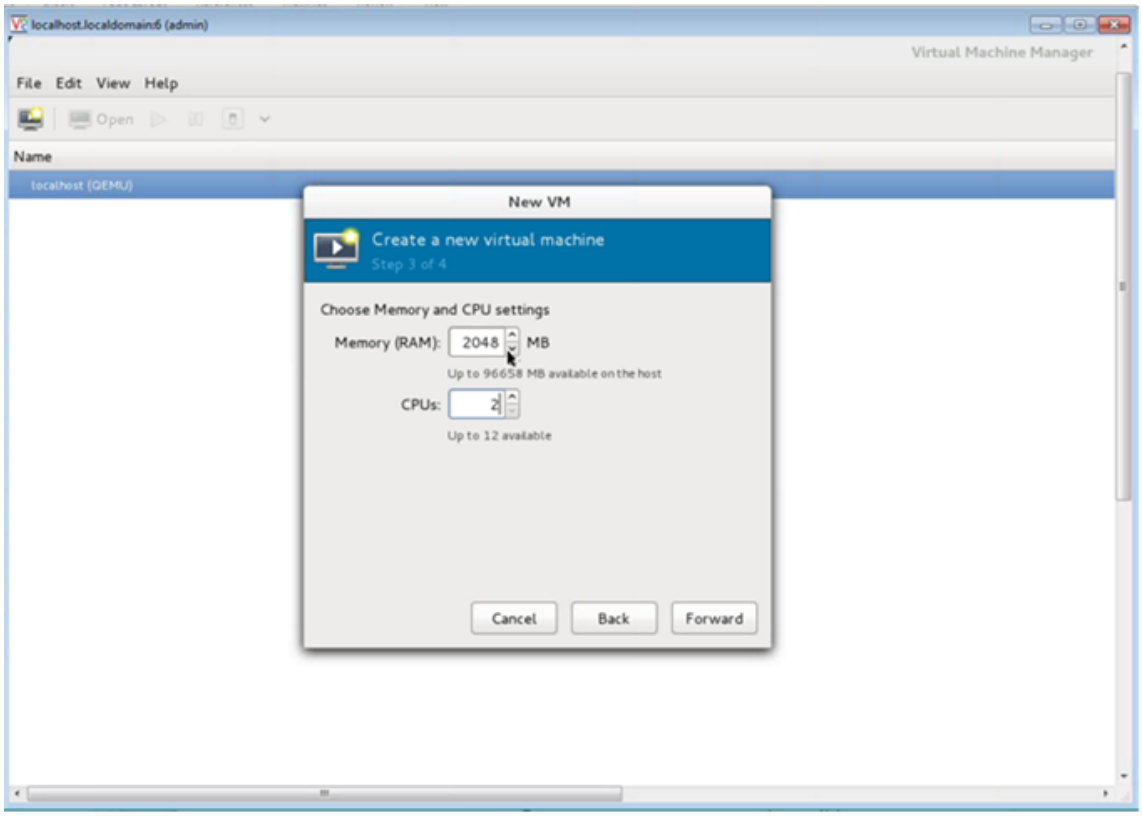


5. Dans le champ **Fournissez le chemin de stockage existant**, accédez au chemin d'accès à l'image. Choisissez le type d'OS sous UNIX et la version sous FreeBSD 6.x. Cliquez ensuite sur **Transférer**.

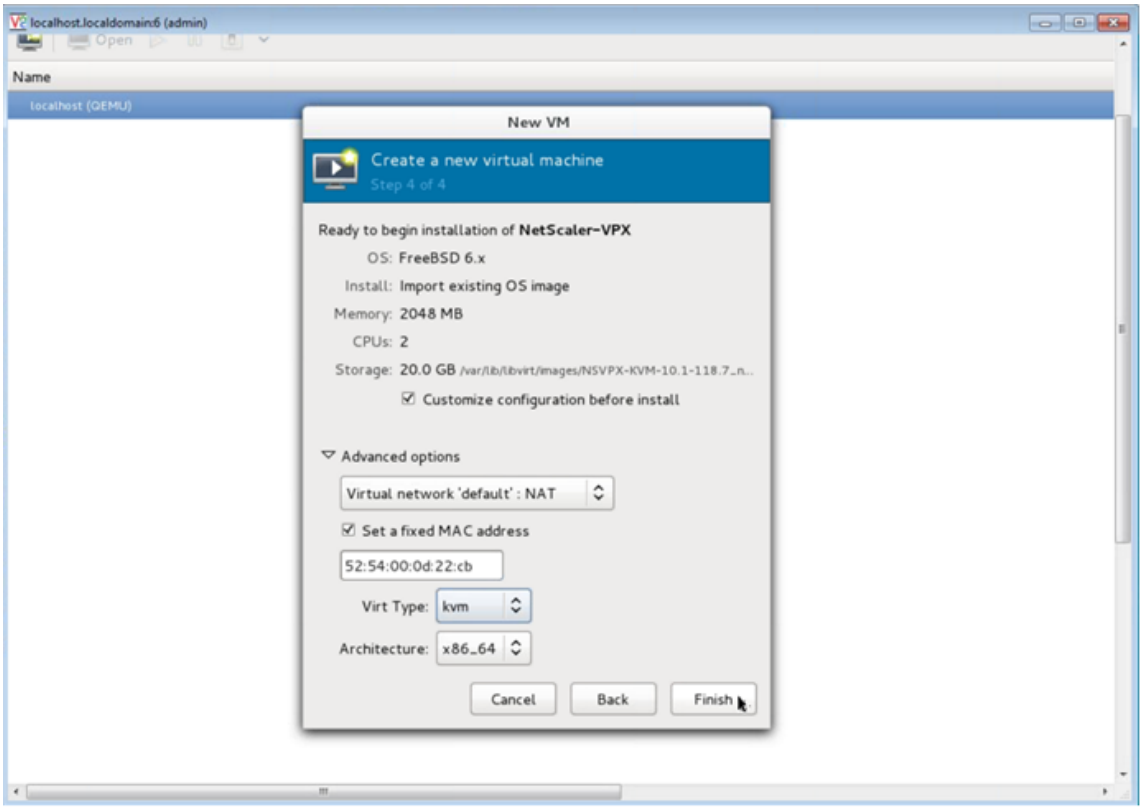


6. Sous **Choisir les paramètres de mémoire et de processeur**, sélectionnez les paramètres suivants, puis cliquez sur **Transférer** :

   - Mémoire vive (RAM) — 2048 Mo
   - CPU — 2

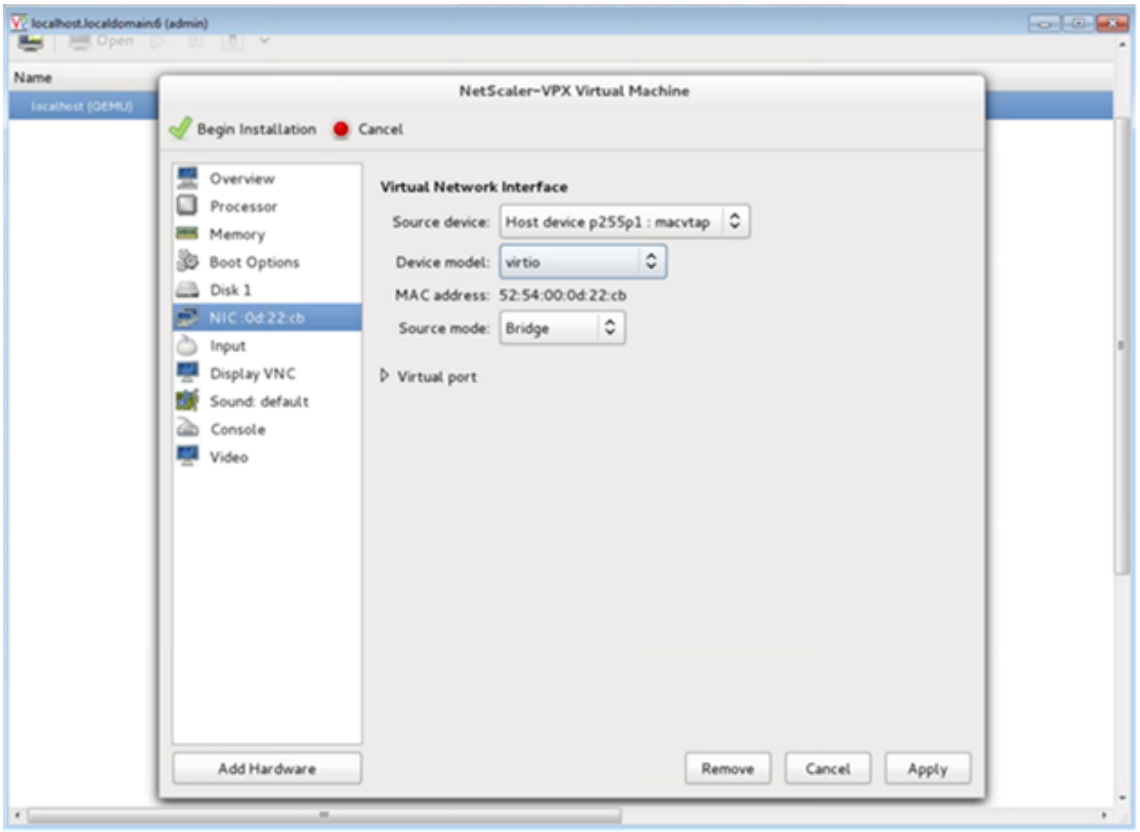


7. Activez la case à cocher **Personnaliser la configuration avant l'installation** . Le cas échéant, sous **Options avancées**, vous pouvez personnaliser l'adresse MAC. Assurez-vous que le **type Virt** sélectionné est KVM et que l'architecture sélectionnée est x86_64. Cliquez sur **Terminer**.



8. Sélectionnez une carte réseau et fournissez la configuration suivante :

   - Périphérique source `ethX macvtap` ou Bridge
   - Modèle d'appareil— `virtio`
   - Mode source : Bridge



9. Cliquez sur **Apply**.
10. Si vous souhaitez configurer automatiquement l'instance VPX, consultez la section **Activation de l'auto-provisioning en attachant un lecteur de CDROM** dans ce document. Sinon, cliquez sur **Commencer l'installation**. Une fois que vous avez provisionné Citrix ADC VPX sur KVM, vous pouvez ajouter d'autres interfaces.

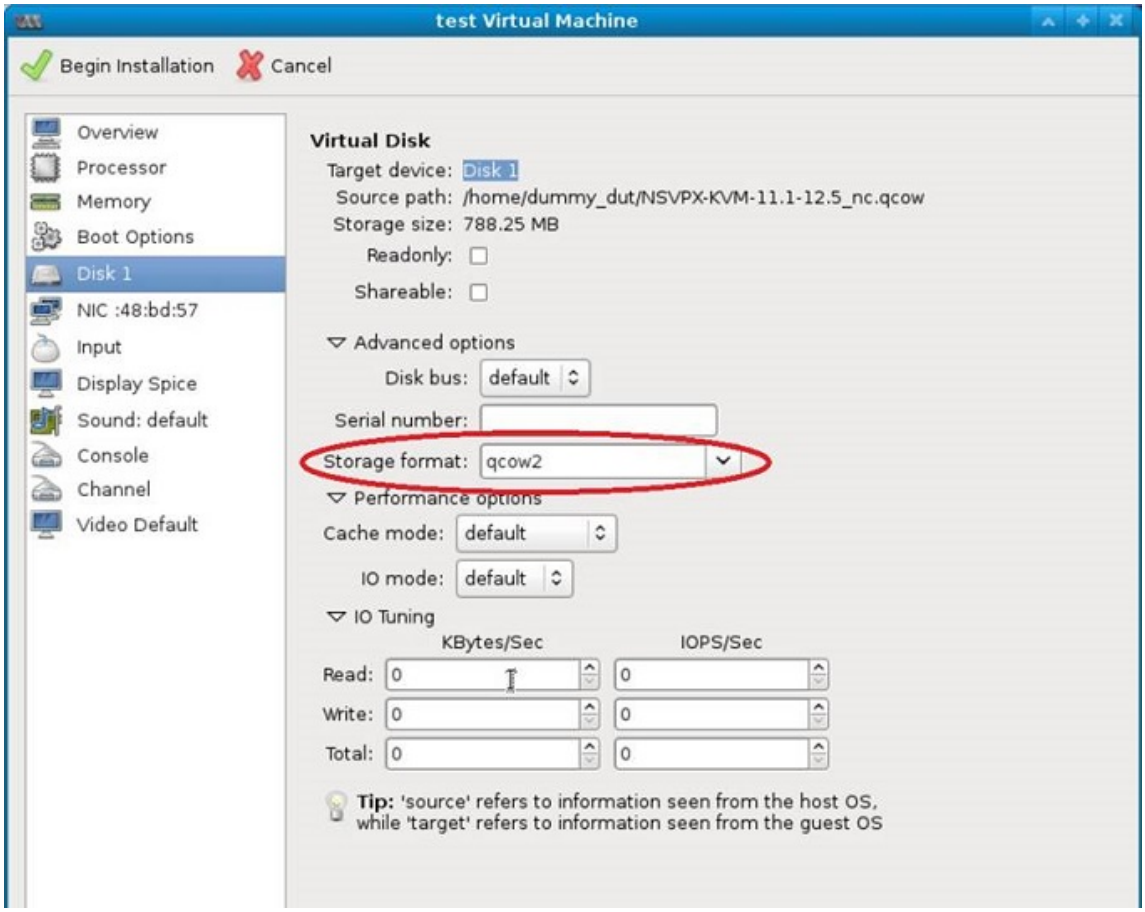
Provisionner l'instance Citrix ADC VPX à l'aide d'une image QCOW2

À l'aide de Virtual Machine Manager, vous pouvez provisionner l'instance Citrix ADC VPX à l'aide d'une image QCOW2.

Pour provisionner une instance Citrix ADC VPX à l'aide d'une image QCOW2, procédez comme suit :

1. Suivez les **étapes 1** à **8** de la section Provisionner l'instance Citrix ADC VPX à l'aide d'une image RAW.

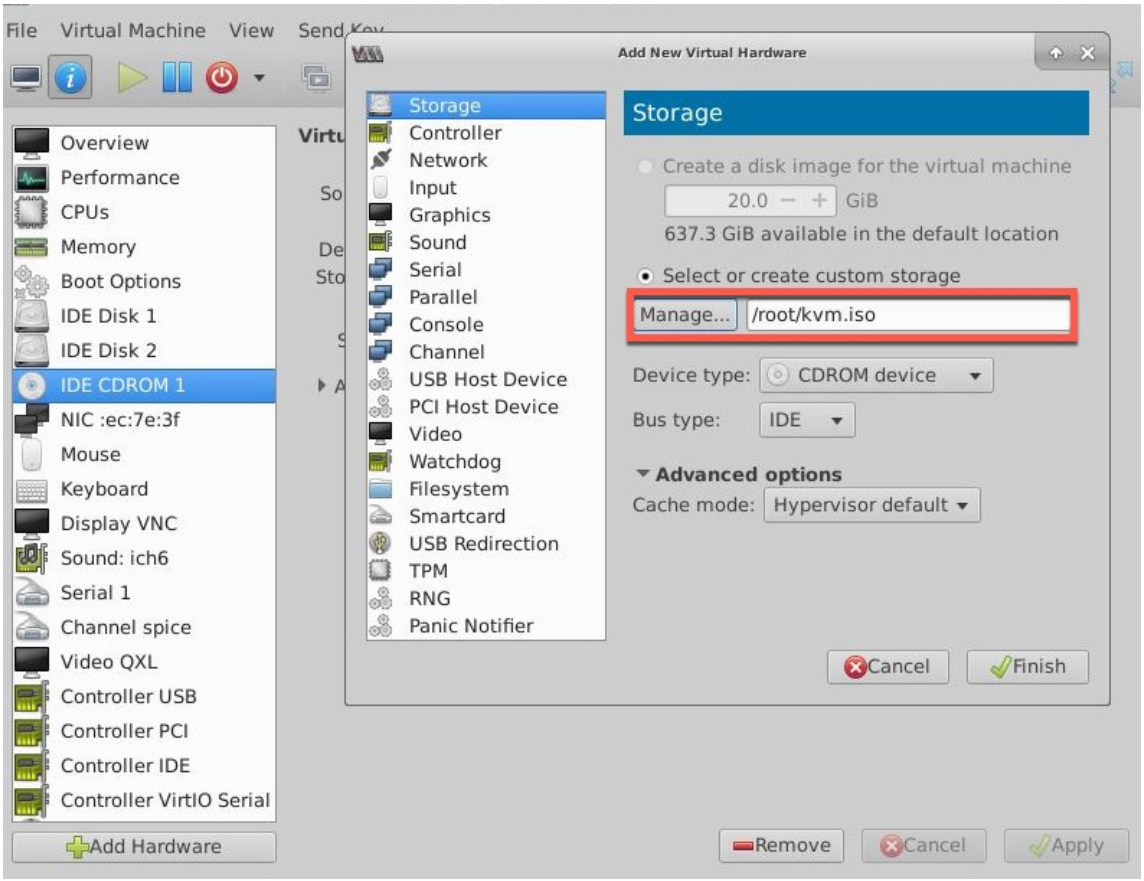
   Remarque : Assurez-vous de sélectionner l'image **qcow2**à l'**étape 5**.
2. Sélectionnez **Disque 1** et cliquez sur **Options avancées** .
3. Sélectionnez **qcow2** dans la liste déroulante Format de stockage.



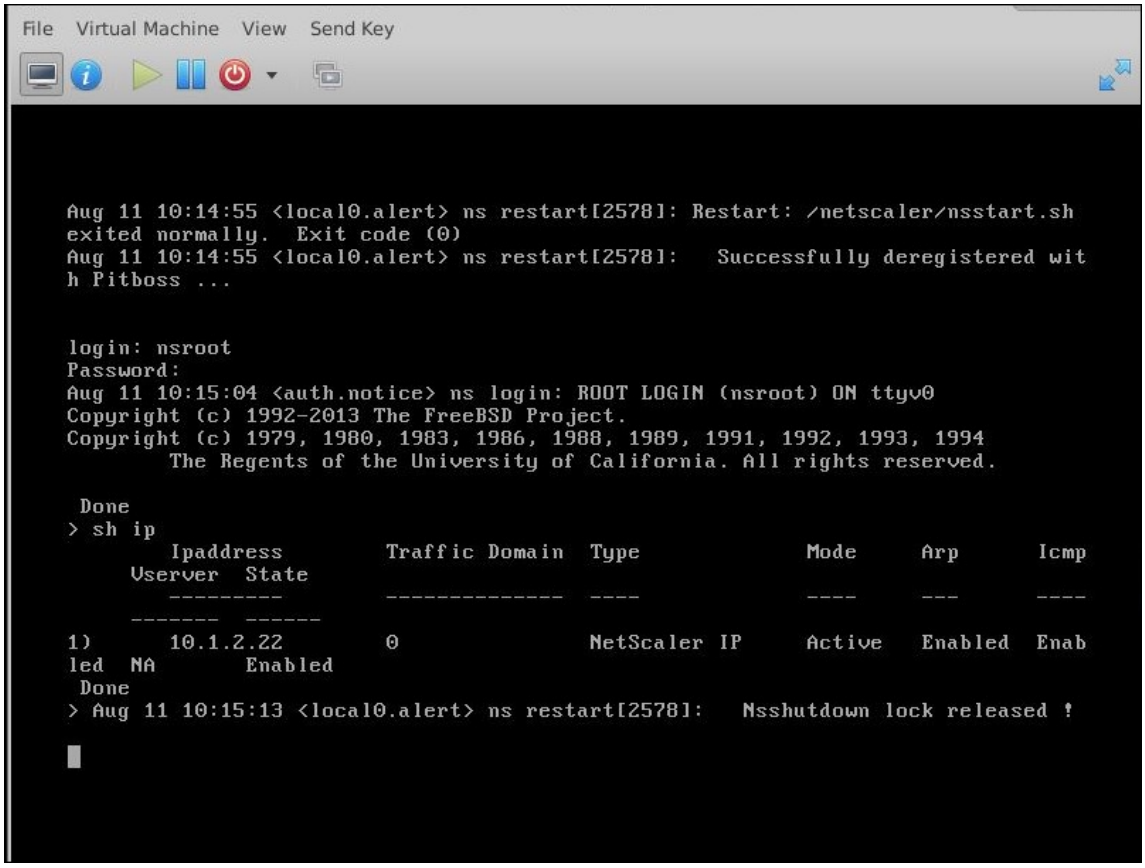
4. Cliquez sur **Appliquer**, puis sur **Commencer l'installation**. Une fois que vous avez provisionné Citrix ADC VPX sur KVM, vous pouvez ajouter d'autres interfaces.

Activer le provisioning automatique en attachant un lecteur de CD-ROM

1. Cliquez sur Ajouter **du matériel > Stockage > Type de périphérique > Périphérique CD-ROM**.
2. Cliquez sur **Gérer** et sélectionnez le fichier ISO approprié que vous avez monté dans la section « Prérequis pour le provisionnement automatique d'une instance Citrix ADC VPX », puis cliquez sur **Terminer**. Un nouveau CDROM sous Ressources sur votre instance Citrix ADC VPX est créé.



3. Mettez l'instance VPX sous tension, et il provisionnera automatiquement avec la configuration réseau fournie dans le fichier OVF, comme indiqué dans l'exemple de capture d'écran.



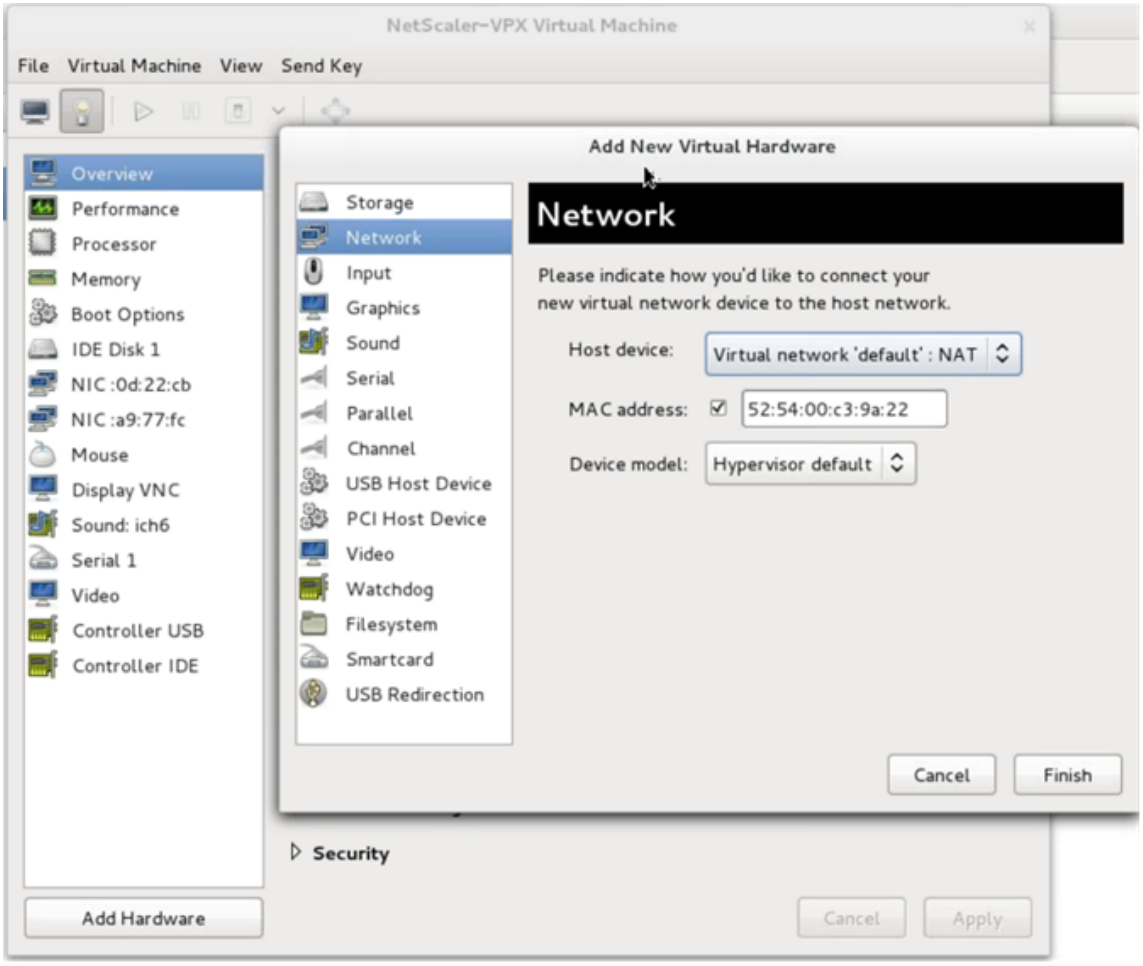
4. Si la mise en service automatique échoue, l'instance affiche l'adresse IP par défaut (192.168.100.1). Dans ce cas, vous devez terminer la configuration initiale manuellement. Pour plus d'informations, voir Configurer l'ADC pour la première fois.

Ajoutez d'autres interfaces à l'instance Citrix ADC VPX à l'aide de Virtual Machine Manager

Après avoir provisionné l'instance NetScaler VPX sur KVM, vous pouvez ajouter des interfaces supplémentaires.

Pour ajouter d'autres interfaces, procédez comme suit.

1. Arrêtez l'instance NetScaler VPX exécutée sur le KVM.
2. Cliquez avec le bouton droit sur l'instance VPX et choisissez **Ouvrir** dans le menu contextuel.
3. Cliquez sur l'icône de  dans l'en-tête pour afficher les détails du matériel virtuel.
4. Cliquez sur **Ajouter du matériel**. Dans la **fenêtre Ajouter un nouveau matériel virtuel**, sélectionnez **Réseau**dans le menu de navigation.



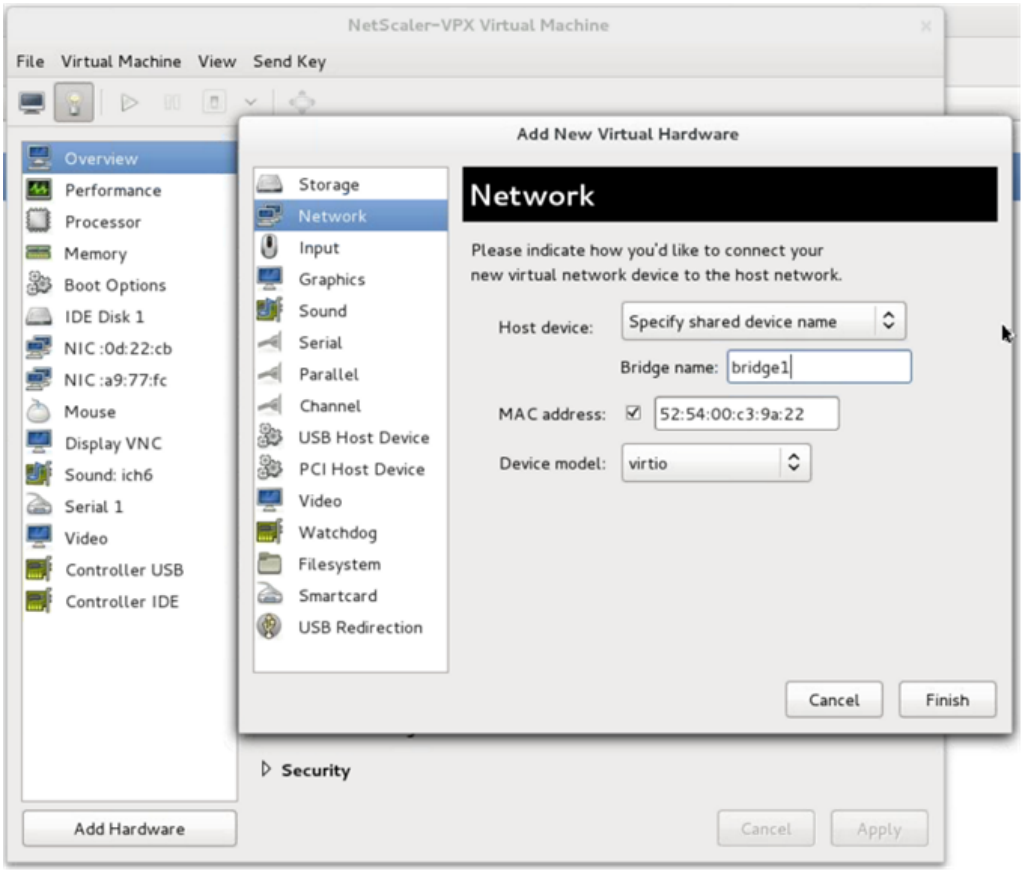
5. Dans le champ **Périphérique hôte**, sélectionnez le type d'interface physique. Le type de périphérique hôte peut être Bridge ou MacVTap. Dans le cas d'un MacVTAP, quatre modes possibles sont VEPA, Bridge, Private et Pass-Through.

    a) Pour Bridge

        i. Périphérique hôte : sélectionnez l'option « Spécifier le nom de périphérique partagé ».

        ii. Indiquez le nom du pont configuré dans l'hôte KVM.

            Remarque : vérifiez que vous avez configuré un pont Linux dans l'hôte KVM, lié l'interface physique au pont et placé le pont dans l'état UP.



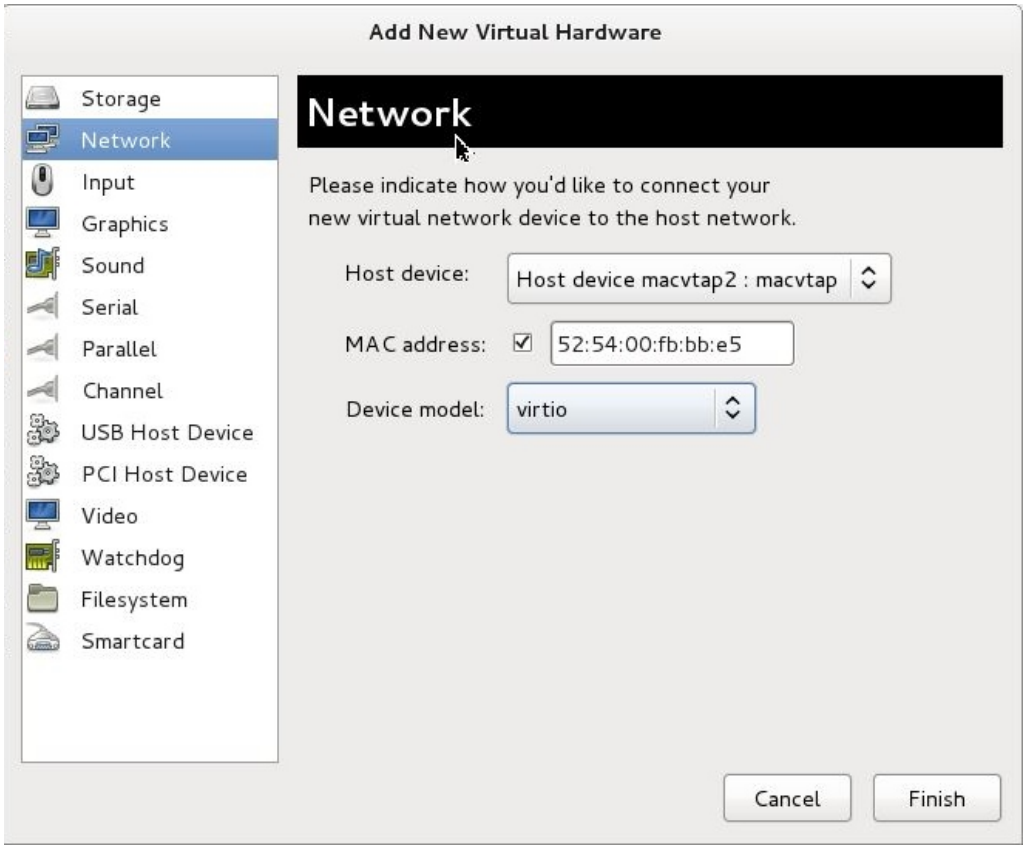
iii. Modèle d'appareil—`virtio`.

iv. Cliquez sur Terminer.

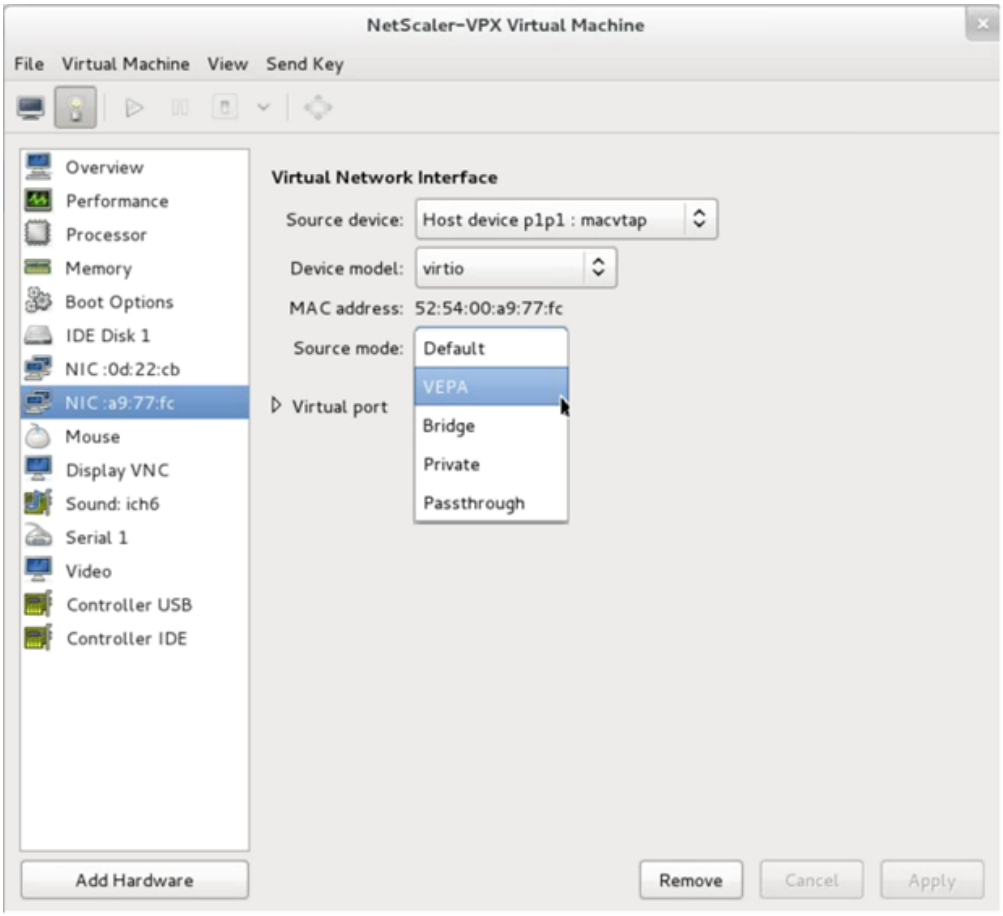
b) Pour MacVTap

i. Périphérique hôte : sélectionnez l'interface physique dans le menu.

ii. Modèle d'appareil—`virtio`.



iii. Cliquez sur Terminer. Vous pouvez afficher la carte réseau nouvellement ajoutée dans le volet de navigation.



iv. Sélectionnez la carte réseau nouvellement ajoutée et sélectionnez le mode Source pour cette carte réseau. Les modes disponibles sont VEPA, Pont, Privé et Passthrough. Pour plus de détails sur l'interface et les modes, voir Interface source et modes.

v. Cliquez sur Apply.

6. Si vous souhaitez configurer automatiquement l'instance VPX, consultez la section « Ajout d'un lecteur de configuration pour activer le provisionnement automatique » dans ce document. Sinon, mettez l'instance VPX sous tension pour terminer manuellement la configuration initiale.

> **Important**
>
> Les configurations de paramètres d'interface telles que la vitesse, le duplex et la négociation automatique ne sont pas prises en charge.

Configurer une instance Citrix ADC VPX pour utiliser les interfaces réseau SR-IOV

August 20, 2021

Vous pouvez configurer une instance Citrix ADC VPX exécutée sur une plate-forme Linux-KVM à l'aide de la virtualisation d'E/S à racine unique (SR-IOV) avec les cartes réseau suivantes :

- Intel 82599 10G
- Intel X710 10G
- Intel XL710 40G
- Intel X722 10G

Cette section décrit comment :

- Configurer une instance Citrix ADC VPX pour utiliser l'interface réseau SR-IOV
- Configurer l'interface LA/LACP statique sur l'interface SR-IOV
- Configurer VLAN sur l'interface SR-IOV

Limitations

Gardez à l'esprit les limitations lors de l'utilisation des cartes réseau Intel 82599, X710, XL710 et X722. Les fonctionnalités suivantes ne sont pas prises en charge.

Limitations pour la carte réseau Intel 82599 :

- Commutation de mode L2.
- Partitionnement administrateur (mode VLAN partagé).
- Haute disponibilité (mode actif-actif).
- Cadres Jumbo.
- IPv6 : Vous ne pouvez configurer que 30 adresses IPv6 uniques dans une instance VPX si vous disposez d'au moins une interface SR-IOV.
- La configuration VLAN sur l'interface Hypervisor for SRIOV VF via `ip link` commande n'est pas prise en charge.
- Les configurations de paramètres d'interface telles que la vitesse, le duplex et les négociations automatiques ne sont pas prises en charge.

Limitations pour les cartes réseau Intel X710 10G, Intel XL710 40G et Intel X722 10G :

- Commutation de mode L2.
- Partitionnement administrateur (mode VLAN partagé).
- Dans un cluster, les trames Jumbo ne sont pas prises en charge lorsque la carte réseau XL710 est utilisée comme interface de données.
- La liste des interfaces réordonne lorsque les interfaces sont déconnectées et reconnectées.
- Les configurations de paramètres d'interface telles que la vitesse, le duplex et les négociations automatiques ne sont pas prises en charge.
- Le nom de l'interface est 40/X pour les cartes réseau Intel X710 10G, Intel XL710 40G et Intel X722 10G

- Jusqu'à 16 interfaces relais Intel XL710/X710/X722 SRIOV ou PCI peuvent être prises en charge sur une instance VPX.

> **Remarque :** pour les cartes réseau Intel X710 10G, Intel XL710 40G et Intel X722 10G pour prendre en charge IPv6, vous devez activer le mode de confiance sur les fonctions virtuelles (VF) en tapant la commande suivante sur l'hôte KVM :
>
> ```
> ## ip link set <PNIC> <VF> trust on
> ```
>
> Exemple :
>
> ```
> ## ip link set ens785f1 vf 0 trust on
> ```

Conditions préalables

Avant de configurer une instance Citrix ADC VPX pour qu'elle utilise des interfaces réseau SR-IOV, effectuez les tâches préalables suivantes. Reportez-vous à la colonne NIC pour plus d'informations sur la façon d'effectuer les tâches correspondantes.

Tâche	Carte réseau Intel 82599	Cartes réseau Intel X710, XL710 et X722
1. Ajoutez la carte réseau à l'hôte KVM.	-	-
2. Téléchargez et installez le dernier pilote Intel.	Pilote IXGBE	Pilote I40E
3. Liste de blocage du pilote sur l'hôte KVM.	Ajoutez l'entrée suivante dans le fichier /etc/modprobe.d/blacklist.conf : `blacklist ixgbevf`. Utilisez le pilote IXGBE version 4.3.15 (recommandé).	Ajoutez l'entrée suivante dans le fichier /etc/modprobe.d/blacklist.conf : `blacklist i40evf`. Utilisez le pilote i40e version 2.0.26 (recommandé).

Tâche	Carte réseau Intel 82599	Cartes réseau Intel X710, XL710 et X722
4.Activez SR-IOV Virtual Functions (VF) sur l'hôte KVM. Dans les deux commandes des deux colonnes suivantes : `number_of_VFs` = le nombre de VF virtuels que vous souhaitez créer. `device_name` = le nom de l'interface.	Si vous utilisez une version antérieure du noyau 3.8, ajoutez l'entrée suivante au fichier /etc/modprobe.d/ixgbe et redémarrez l'hôte KVM : `options ixgbe max_vfs =<number_of_VFs>`. Si vous utilisez la version 3.8 du noyau ou une version ultérieure, créez des VF à l'aide de la commande suivante : `echo <number_of_VFs> > /sys/class/net/<device_name>/device/sriov_numvfs`. Voir l'exemple de la figure 1.	Si vous utilisez une version antérieure du noyau 3.8, ajoutez l'entrée suivante au fichier /etc/modprobe.d/i40e.conf et redémarrez l'hôte KVM : `options i40e max_vfs=<number_of_VFs>`. Si vous utilisez la version 3.8 du noyau ou une version ultérieure, créez des VF à l'aide de la commande suivante : `echo<number_of_VFs> > /sys/class/net/<device_name>/device/sriov_numvfs`. Voir l'exemple de la figure 2.
5. Rendez les VFS persistants en ajoutant les commandes que vous avez utilisées pour créer des VFS, au fichier rc.local.	Voir l'exemple de la figure 3.	Voir l'exemple de la figure 3.

> **Important**
>
> Lorsque vous créez les VF SR-IOV, assurez-vous que vous n'attribuez pas d'adresses MAC aux VF.

Figure 1 : activer les VF SR-IOV sur l'hôte KVM pour la carte réseau Intel 82599 10G.

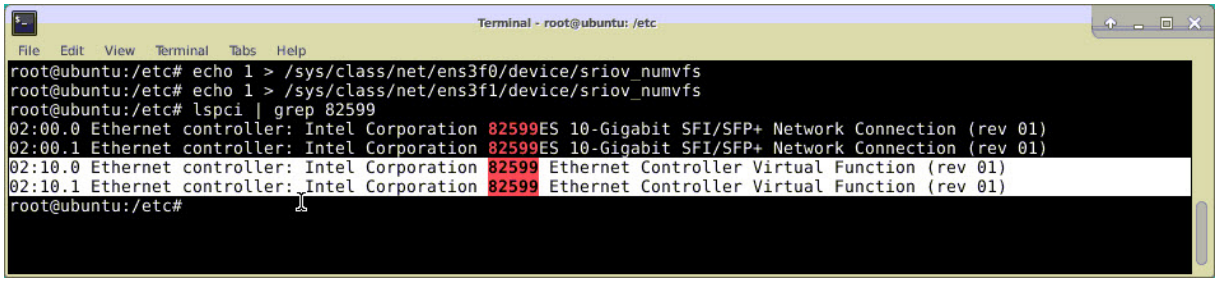


Figure 2 : activer les VF SR-IOV sur l'hôte KVM pour les cartes réseau Intel X710 10G et XL710 40G.

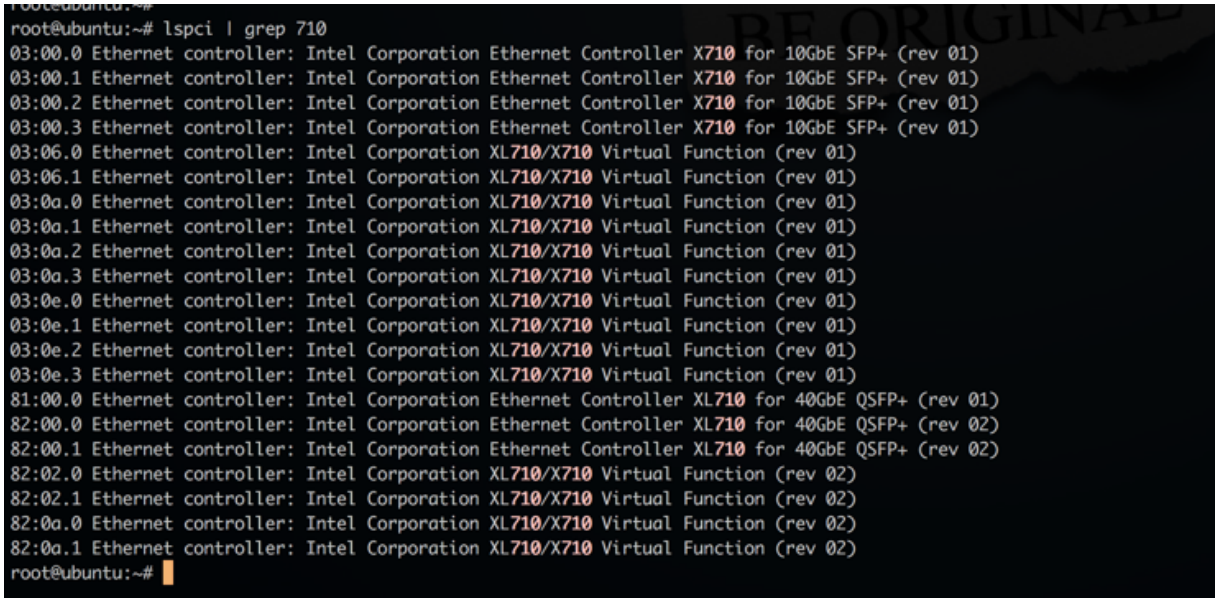


Figure 3 : activer les VF SR-IOV sur l'hôte KVM pour la carte réseau Intel X722 10G.

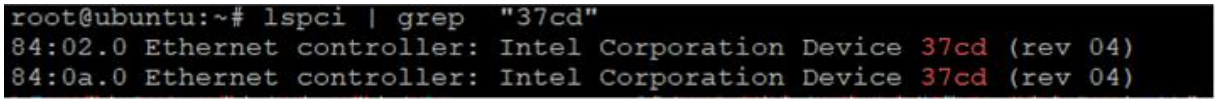
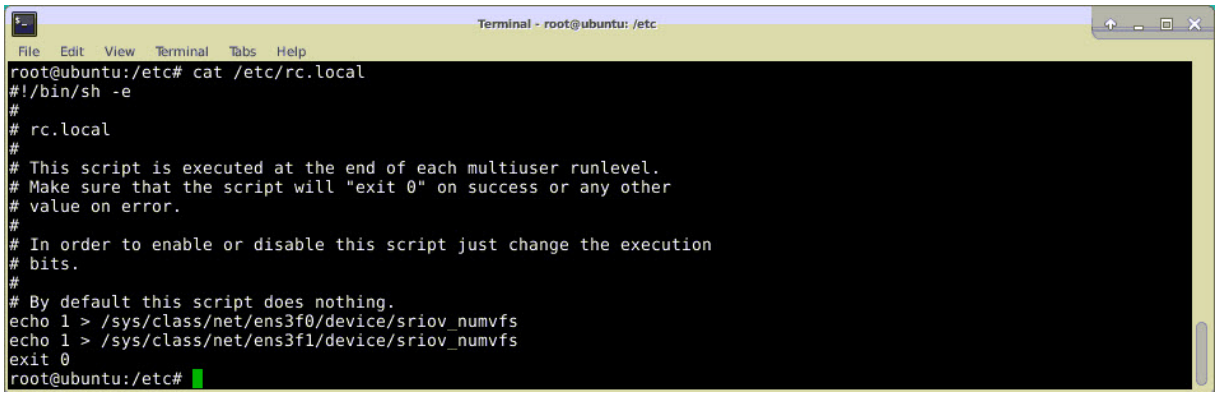


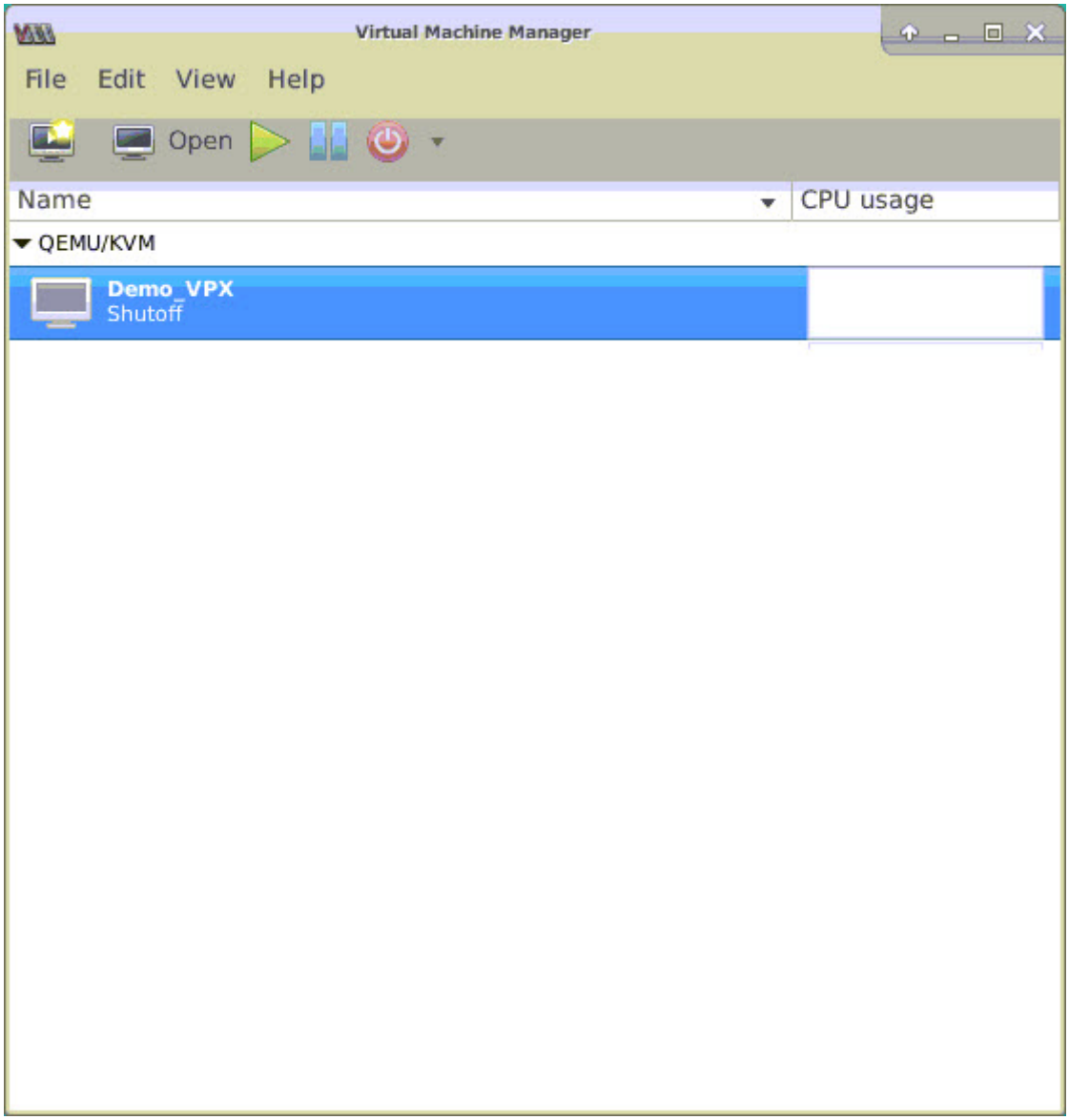
Figure 4 : Rendre les VF persistants.



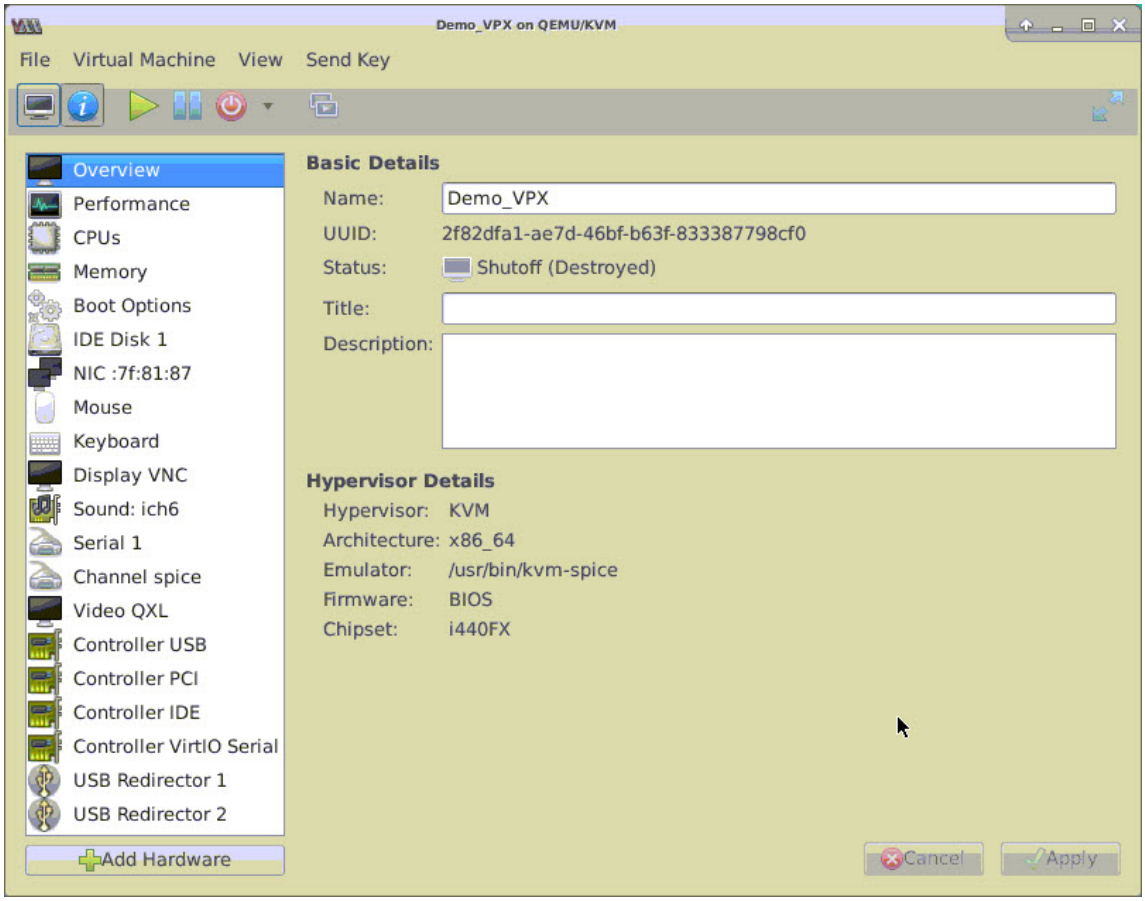
Configurer une instance Citrix ADC VPX pour utiliser l'interface réseau SR-IOV

Pour configurer l'instance Citrix ADC VPX pour qu'elle utilise l'interface réseau SR-IOV à l'aide de Virtual Machine Manager, procédez comme suit :

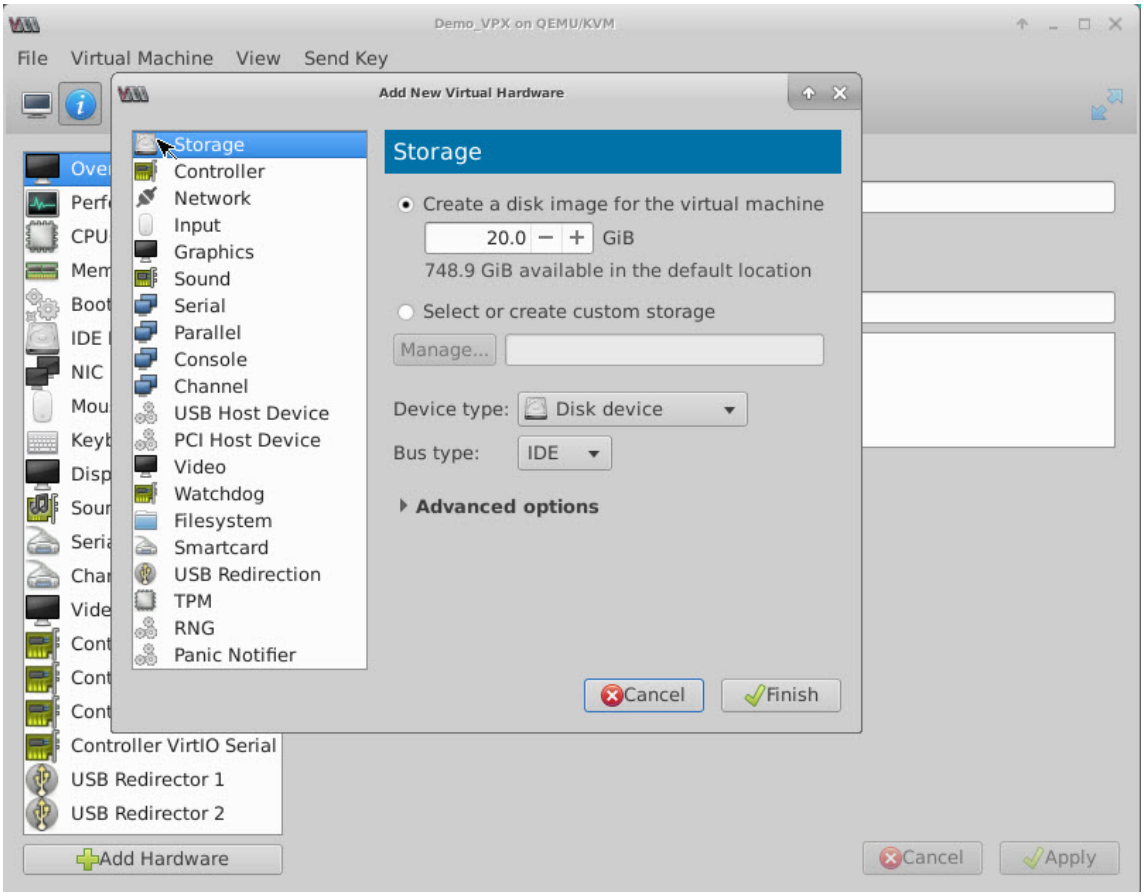
1. Mettez hors tension l'instance Citrix ADC VPX.
2. Sélectionnez l'instance Citrix ADC VPX, puis sélectionnez Ouvrir.



3. Dans la <virtual machine on KVM>fenêtre, sélectionnez l'icône **i** .



4. Sélectionnez **Ajouter du matériel**.



5. Dans la boîte de dialogue **Ajouter un nouveau matériel virtuel**, procédez comme suit :

   a) Sélectionnez PCI Host Device.

   b) Dans la section Périphérique hôte, sélectionnez le VF que vous avez créé, puis cliquez sur Terminer.

Figure 4 : VF pour carte réseau Intel 82599 10G

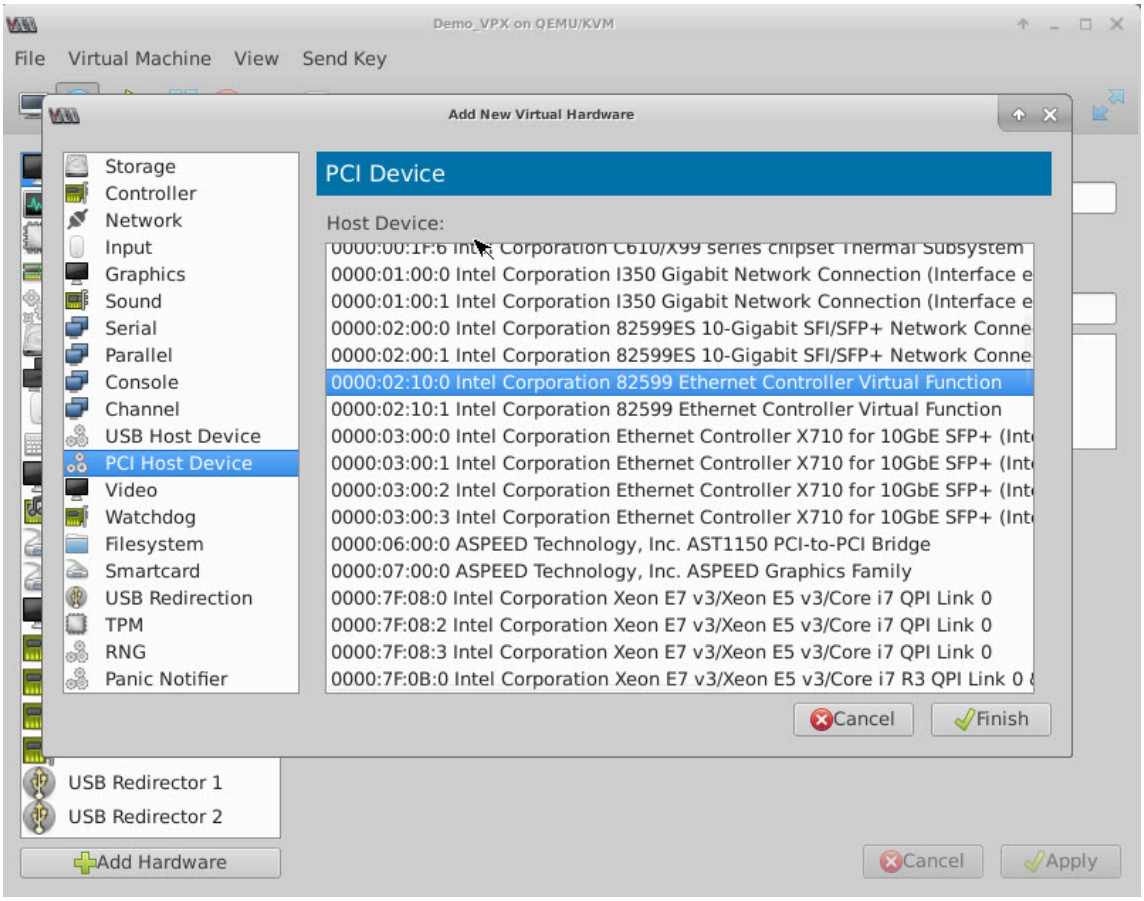


Figure 5 : VF pour carte réseau Intel XL710 40G

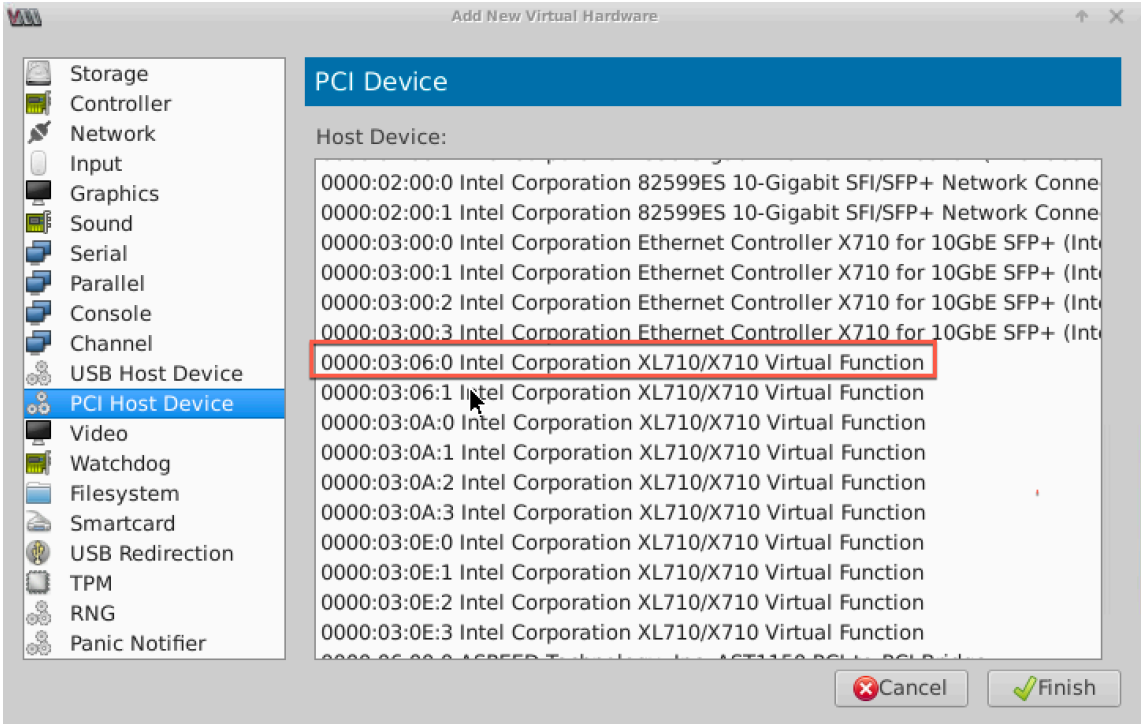
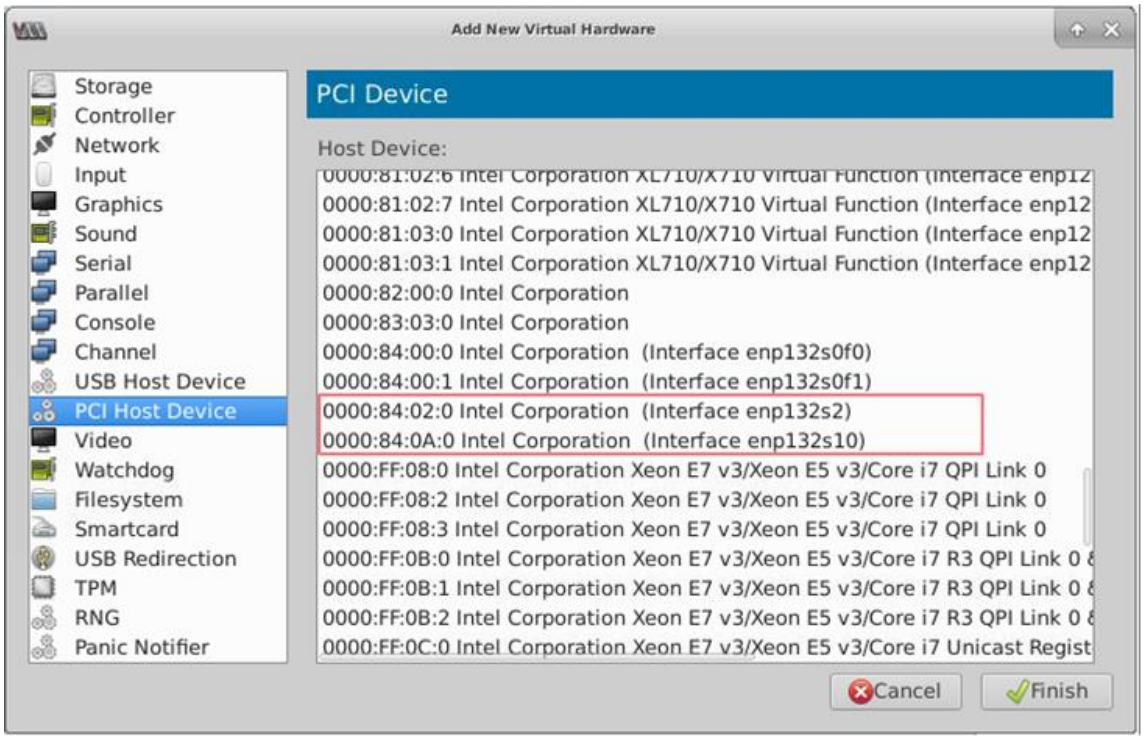


Figure 6 : VF pour carte réseau Intel X722 10G



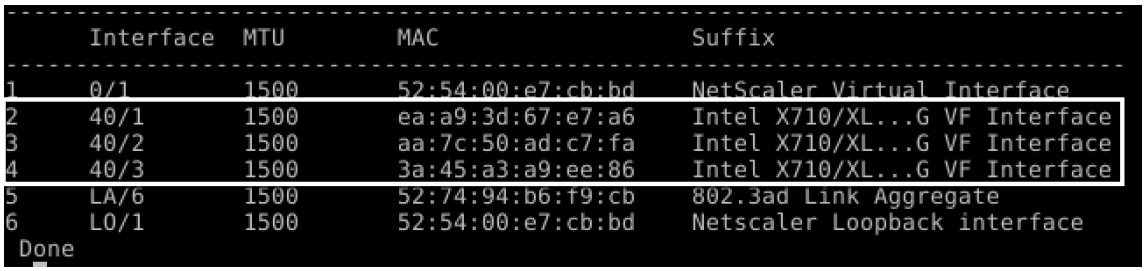
6. Répétez les étapes 4 et 5 pour ajouter les VF que vous avez créées.
7. Mettez sous tension l'instance Citrix ADC VPX.
8. Une fois l'instance Citrix ADC VPX sous tension, utilisez la commande suivante pour vérifier la configuration :

```
1 show interface summary
2 <!--NeedCopy-->
```

La sortie affiche toutes les interfaces que vous avez configurées.

Figure 6 : récapitulatif de sortie pour la carte réseau Intel 82599.

Figure 7. Résumé de la sortie pour les cartes réseau Intel X710 et XL710.



Configurer l'interface LA/LACP statique sur l'interface SR-IOV

> **Important**
>
> Lorsque vous créez les VF SR-IOV, assurez-vous que vous n'attribuez pas d'adresses MAC aux VF.

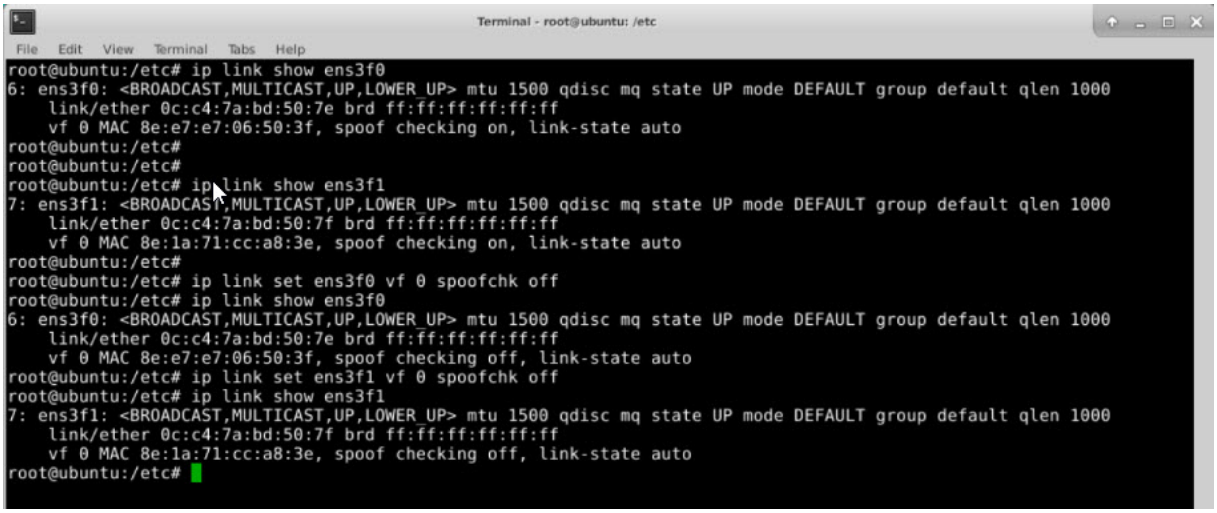
Pour utiliser les VF SR-IOV en mode d'agrégation de liens, désactivez la vérification d'usurpation des VF que vous avez créées. Sur l'hôte KVM, utilisez la commande suivante pour désactiver la vérification d'usurpation :

```
*ip link set \<interface\\_name\> vf \<VF\\_id\> spoofchk off*
```

Où :

- Interface_name : est le nom de l'interface.
- vf_id — est l'id de la fonction virtuelle.

Exemple :



Après avoir désactivé la vérification d'usurpation pour toutes les VF que vous avez créées. Redémarrez l'instance Citrix ADC VPX et configurez l'agrégation des liens. Pour obtenir des instructions détaillées, voir Configuration de l'agrégation de liens.

Configuration du VLAN sur l'interface SR-IOV

Vous pouvez configurer VLAN sur les VF SR-IOV. Pour obtenir des instructions détaillées, reportez-vous à la section Configuration d'un VLAN.

> **Important**
>
> Assurez-vous que l'hôte KVM ne contient pas de paramètres VLAN pour l'interface VF.

Configurer une instance Citrix ADC VPX pour utiliser les interfaces réseau PCI

August 20, 2021

Après avoir installé et configuré une instance Citrix ADC VPX sur la plate-forme Linux-KVM, vous pouvez utiliser Virtual Machine Manager pour configurer l'appliance virtuelle de manière à utiliser les interfaces réseau PCI.

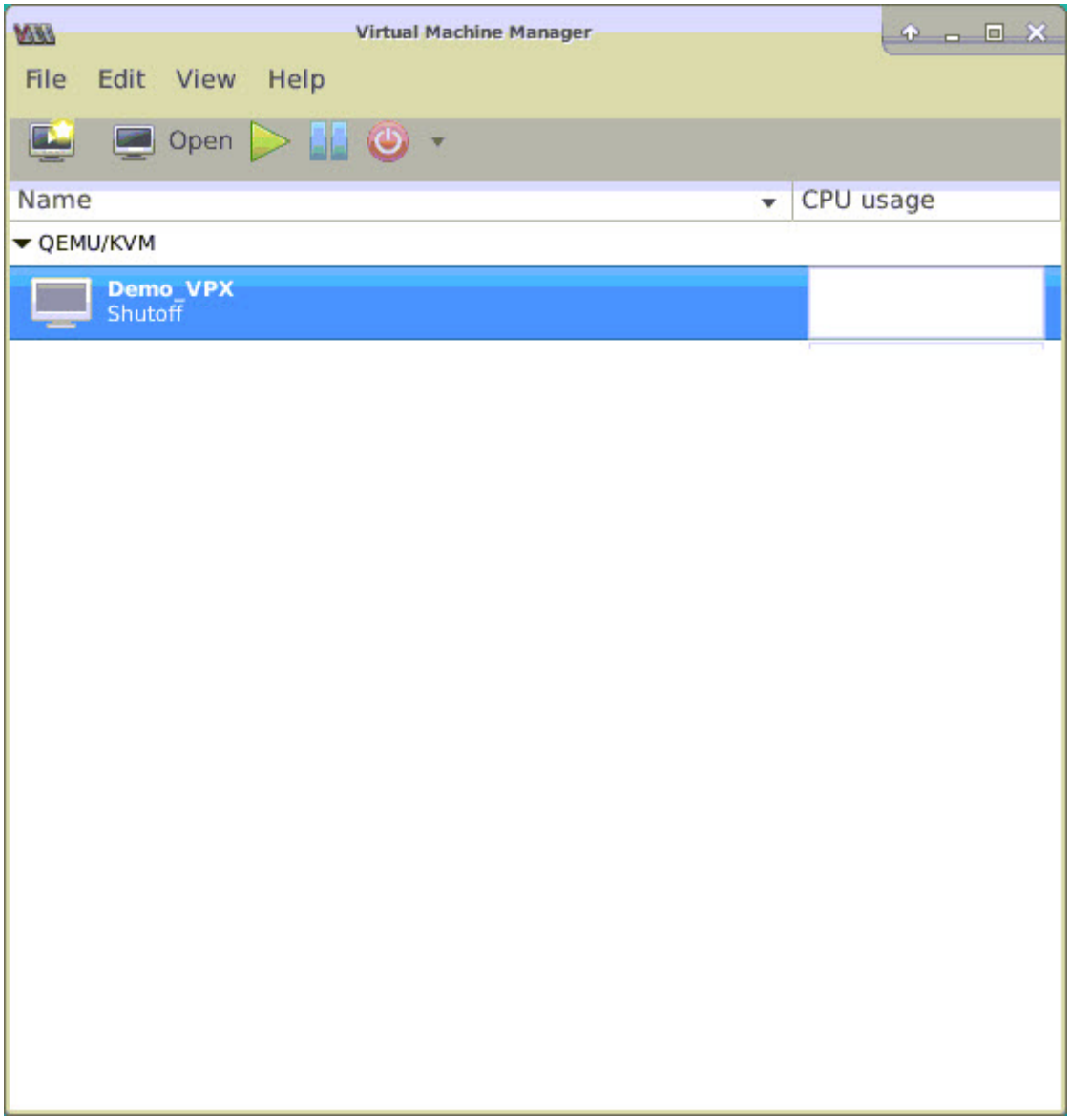
Conditions préalables

- La version du microprogramme de la carte réseau (NIC) Intel XL710 sur l'hôte KVM est 5.04.
- L'hôte KVM prend en charge l'unité de gestion de la mémoire d'entrée-sortie (IOMMU) et Intel VT-d, et ils sont activés dans le BIOS de l'hôte KVM. Sur l'hôte KVM, pour activer IOMMU, ajoutez l'entrée suivante au fichier **/boot/grub2/grub.cfg**:**intel_iommu=1**

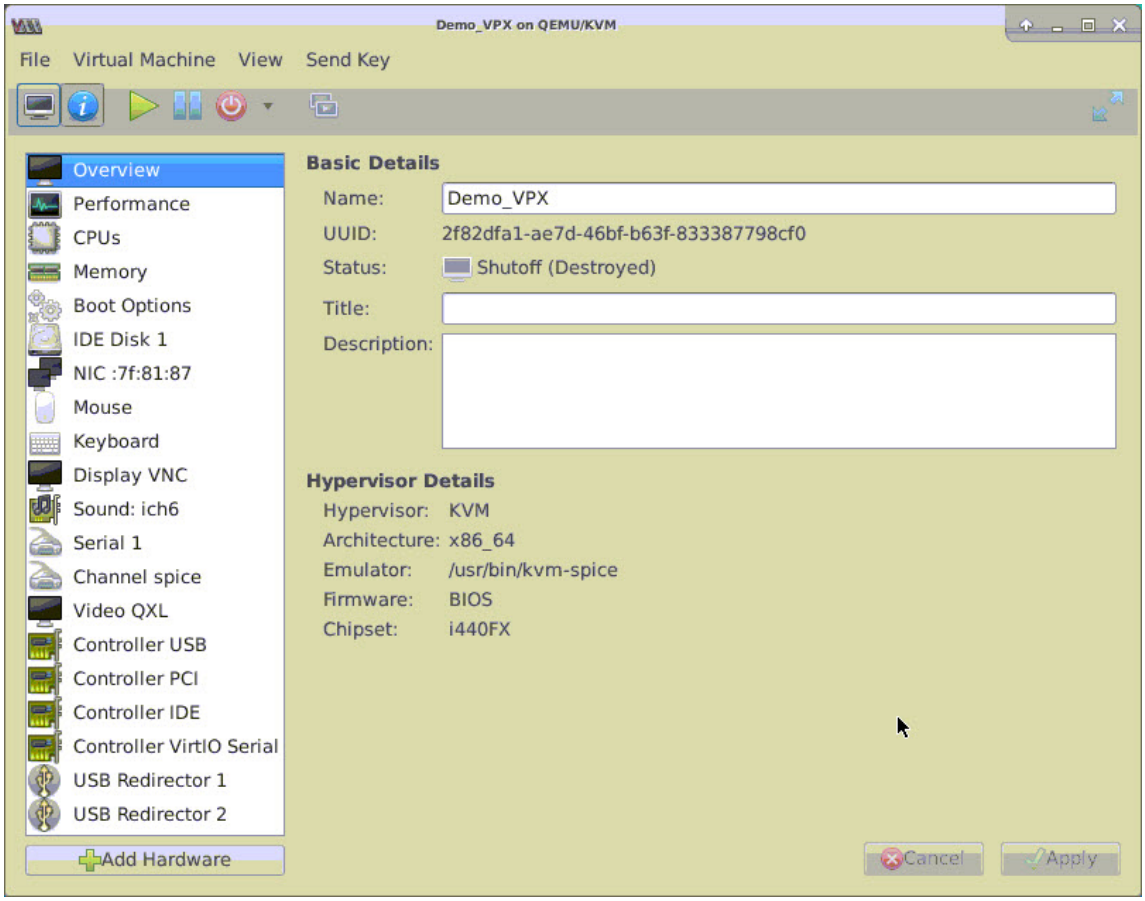
- Exécutez la commande suivante et redémarrez l'hôte KVM : **GRUB2-MKConfig —o /boot/-grub2/grub.cfg**

Pour configurer les instances Citrix ADC VPX pour qu'elles utilisent des interfaces réseau PCI à l'aide du Gestionnaire de machines virtuelles :

1. Mettez hors tension l'instance Citrix ADC VPX.
2. Sélectionnez l'instance Citrix ADC VPX et cliquez sur **Ouvrir**.



3. Dans la fenêtre **Virtual_machine sur KVM**, cliquez sur l'icône **i.**

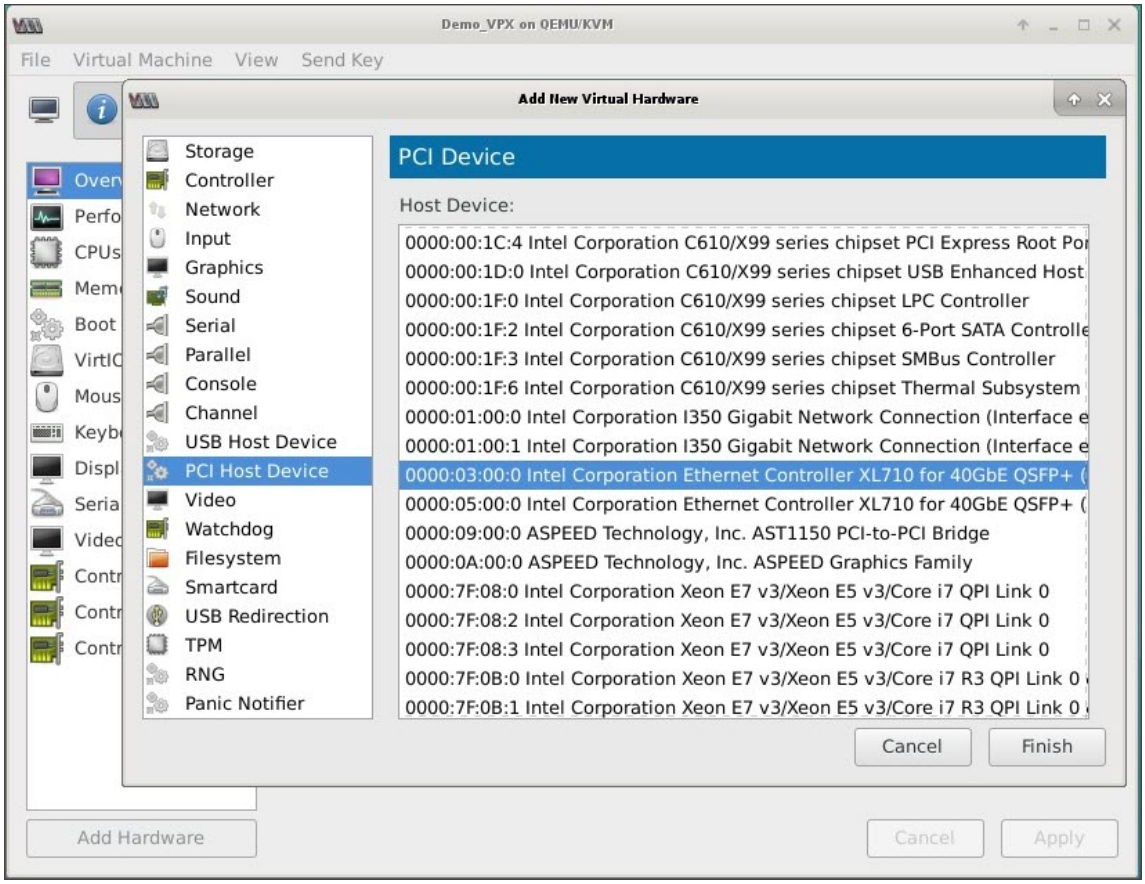


4. Cliquez sur **Ajouter du matériel**.
5. Dans la boîte de dialogue **Ajouter un nouveau matériel virtuel**, procédez comme suit :

   a. Sélectionnez **PCI Host Device**.

   b. Dans la section **Périphérique hôte**, sélectionnez la fonction physique Intel XL710.

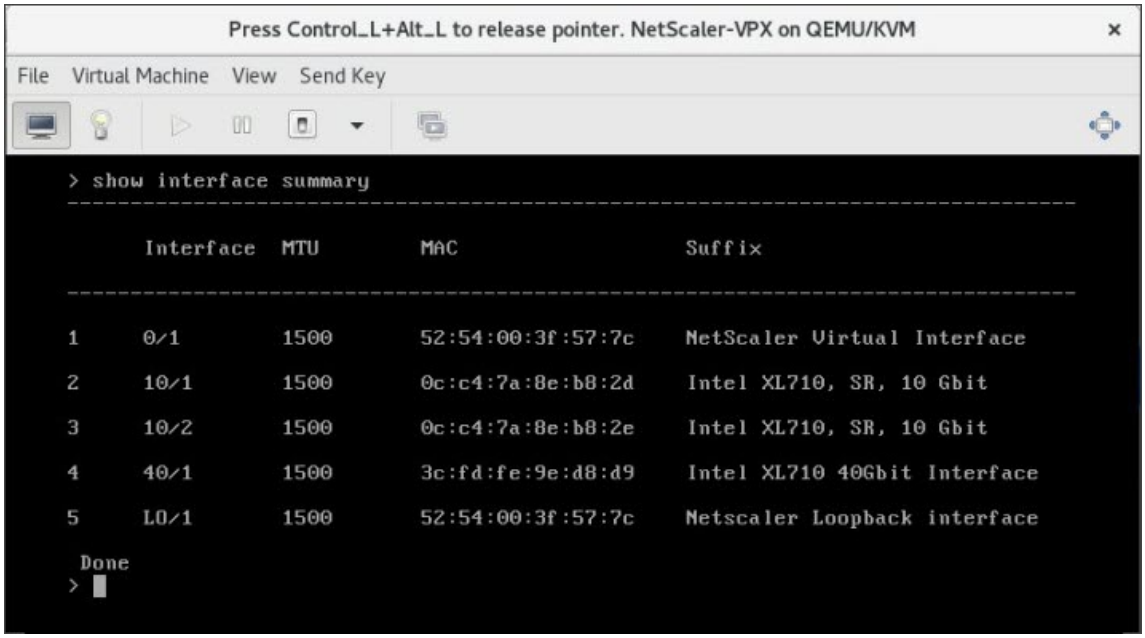
   c. Cliquez sur **Terminer**.



6. Répétez les étapes **4** et **5** pour ajouter d'autres fonctions physiques Intel XL710.
7. Mettez sous tension l'instance Citrix ADC VPX.
8. Une fois l'instance Citrix ADC VPX sous tension, vous pouvez utiliser la commande suivante pour vérifier la configuration :

```
COMMAND
> show interface summary
```

La sortie doit afficher toutes les interfaces que vous avez configurées :



Provisionnez l'instance Citrix ADC VPX à l'aide du virsh programme

August 20, 2021

Le `virsh` programme est un outil de ligne de commande permettant de gérer les invités de machines virtuelles. Sa fonctionnalité est similaire à celle de Virtual Machine Manager. Il vous permet de modifier l'état d'un invité VM (démarrage, arrêt, pause, etc.), de configurer de nouveaux invités et appareils et de modifier les configurations existantes. Le `virsh` programme est également utile pour le script des opérations de gestion des invités de machines virtuelles.

Pour provisionner Citrix ADC VPX à l'aide du `virsh` programme, procédez comme suit :

1. Utilisez la commande tar pour décompresser le package Citrix ADC VPX. Le package NSVPX-KVM-*_NC.tgz contient les composants suivants :

   - Fichier XML de domaine spécifiant les attributs VPX [NSVPX-KVM-*_NC.xml]
   - Check sum de l'image de disque NS-VM [CheckSum.txt]
   - Image de disque NS-VM [NSVPX-KVM-*_NC.raw]

   Exemple :

```
tar -xvzf NSVPX-KVM-10.1-117_nc.tgz
NSVPX-KVM-10.1-117_nc.xml
NSVPX-KVM-10.1-117_nc.raw
checksum.txt
<!--NeedCopy-->
```


2. Copiez le fichier XML NSVPX-KVM-*_NC.xml dans un fichier nommé <DomainName> -NSVPX-KVM-*_NC.xml. Le <DomainName> est également le nom de la machine virtuelle. Exemple :

```
cp NSVPX-KVM-10.1-117_nc.xml NetScaler-VPX-NSVPX-KVM-10.1-117_nc.
   xml
<!--NeedCopy-->
```

3. Modifiez le fichier <DomainName> -nsvpx-kvm-*_nc.xml pour spécifier les paramètres suivants :

   - name (name) : spécifiez le nom.
   - Mac : spécifiez l'adresse MAC.
     Remarque : Le nom de domaine et l'adresse MAC doivent être uniques.
   - fichier source : spécifiez le chemin absolu de la source de l'image disque. Le chemin du fichier doit être absolu. Vous pouvez spécifier le chemin d'accès au fichier image RAW ou à un fichier image QCOW2.

     Si vous souhaitez spécifier un fichier image RAW, spécifiez le chemin d'accès source de l'image disque comme indiqué dans l'exemple suivant :

     Exemple :

```
<name>NetScaler-VPX</name>
<mac address='52:54:00:29:74:b3'/>
<source file='/root/NSVPX-KVM-10.1-117_nc.raw'/>
<!--NeedCopy-->
```

     Spécifiez le chemin absolu de source d'image disque QCOW2 et définissez le type de pilote comme **qcow2**, comme illustré dans l'exemple suivant :

     Exemple :

```
<name>NetScaler-VPX</name>
<mac address='52:54:00:29:74:b3'/>
<driver name ='qemu' type='qcow2'/>
<source file='/root/NSVPX-KVM-10.1-117_nc.qcow'/>*
<!--NeedCopy-->
```

4. Modifiez le fichier <DomainName> -nsvpx-kvm-*_nc.xml pour configurer les détails réseau :

   - source dev : spécifiez l'interface.
   - mode : spécifiez le mode. L'interface par défaut est **Macvtap Bridge**.

   Exemple : Mode : MacVTap Bridge Définissez l'interface cible comme `ethx` et le mode comme pont Type de modèle comme `virtio`

```
<interface type='direct'>
```



```
        <mac address='52:54:00:29:74:b3'/>
        <source dev='eth0' mode='bridge'/>
        <target dev='macvtap0'/>
        <model type='virtio'/>
        <alias name='net0'/>
        <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
           function='0x0'/>
     </interface>
<!--NeedCopy-->
```

Ici, eth0 est l'interface physique attachée à la machine virtuelle.

5. Définissez les attributs de machine virtuelle dans le <DomainName>fichier -NSVPX-KVM-*_NC.xml à l'aide de la commande suivante : `virsh` définir <DomainName>-NSVPX-KVM-*_NC.xml Exemple :

```
virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml
<!--NeedCopy-->
```

6. Démarrez la machine virtuelle en entrant la commande suivante : `virsh` start [<DomainName>|<DomainUUI
Exemple :

```
virsh start NetScaler-VPX
<!--NeedCopy-->
```

7. Connectez la machine virtuelle invitée via la `virsh` console de console [<DomainName><DomainUUID>|
|<DomainID>] Exemple :

```
virsh console NetScaler-VPX
<!--NeedCopy-->
```

Ajout d'interfaces supplémentaires à l'instance Citrix ADC VPX à l'aide `virsh` du programme

Après avoir provisionné Citrix ADC VPX sur KVM, vous pouvez ajouter des interfaces supplémentaires.

Pour ajouter d'autres interfaces, procédez comme suit :

1. Arrêtez l'instance Citrix ADC VPX exécutée sur le KVM.
2. Modifiez le fichier <DomainName>-NSVPX-KVM-*_NC.xml à l'aide de la commande : `virsh` edit [<DomainName>|<DomainUUID>]
3. Dans le fichier <DomainName> -nsvpx-kvm-*_nc.xml, ajoutez les paramètres suivants :

   a) **Pour MacVTap**

- Type d'interface : spécifiez le type d'interface comme « direct ».
- Adresse MAC : spécifiez l'adresse MAC et assurez-vous que l'adresse MAC est unique sur toutes les interfaces.
- source dev : spécifiez le nom de l'interface.
- mode : spécifiez le mode. Les modes pris en charge sont : Bridge, VEPA, Private et Pass-Through
- type de modèle : spécifiez le type de modèle comme `virtio`

Exemple :

Mode : Pass-through MacVTap

Définissez l'interface cible comme
`ethx`, le mode comme
pont et le type de modèle comme
`virtio`

```
<interface type='direct'>
      <mac address='52:54:00:29:74:b3'/>
      <source dev='eth1' mode='passthrough'/>
      <model type='virtio'/>
 </interface>
<!--NeedCopy-->
```

Ici eth1 est l'interface physique attachée à la machine virtuelle.

b) **Pour le mode Pont**

Remarque : vérifiez que vous avez configuré un pont Linux dans l'hôte KVM, lié l'interface physique au pont et placé le pont dans l'état UP.

- Type d'interface : spécifiez le type d'interface comme « pont ».
- Adresse MAC : spécifiez l'adresse MAC et assurez-vous que l'adresse MAC est unique sur toutes les interfaces.
- pont source : spécifiez le nom du pont.
- type de modèle : spécifiez le type de modèle comme `virtio`

Exemple : Mode Pont

```
<interface type='bridge'>
      <mac address='52:54:00:2d:43:a4'/>
      <source bridge='br0'/>
      <model type='virtio'/>
 </interface>
<!--NeedCopy-->
```


Gérer les machines virtuelles invitées Citrix ADC VPX

August 20, 2021

Vous pouvez utiliser Virtual Machine Manager et le `virsh` programme pour effectuer des tâches de gestion telles que le démarrage ou l'arrêt d'un invité de machine virtuelle, la configuration de nouveaux invités et de nouveaux périphériques, la modification de configurations existantes et la connexion à la console graphique via Virtual Network Computing (VNC).

Gérer les machines virtuelles invitées VPX à l'aide de Virtual Machine Manager

- Répertorier les invités VM

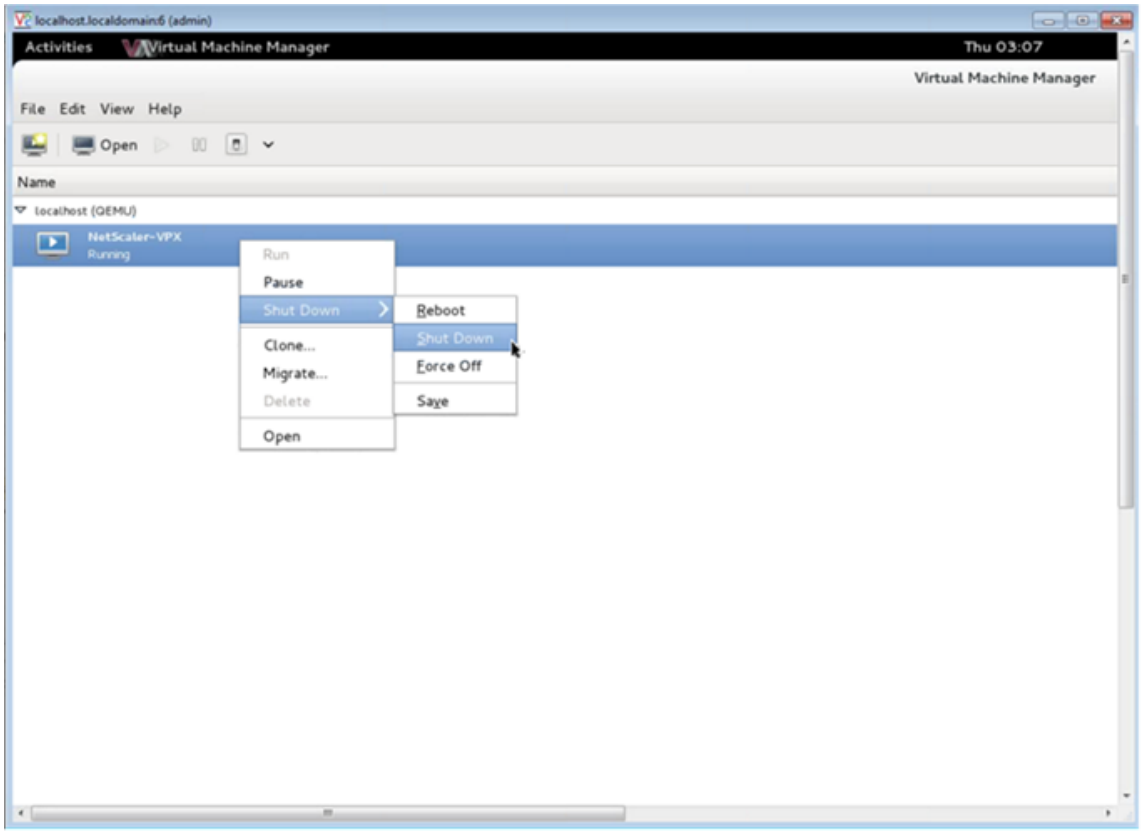
  La fenêtre principale du Virtual Machine Manager affiche une liste de tous les invités de machine virtuelle pour chaque serveur hôte de machine virtuelle auquel il est connecté. Chaque entrée Invité de machine virtuelle contient le nom de la machine virtuelle, ainsi que son état (en cours d'exécution, pause ou arrêt) affiché comme dans l'icône.

- Ouvrir une console graphique

  L'ouverture d'une console graphique à un invité de machine virtuelle vous permet d'interagir avec la machine comme vous le feriez avec un hôte physique via une connexion VNC. Pour ouvrir la console graphique dans Virtual Machine Manager, cliquez avec le bouton droit sur l'entrée VM Guest et sélectionnez l'option Ouvrir dans le menu contextuel.

- Démarrer et arrêter un invité

  Vous pouvez démarrer ou arrêter un invité de machine virtuelle à partir du Gestionnaire de machine virtuelle. Pour modifier l'état de la machine virtuelle, cliquez avec le bouton droit sur l'entrée VM Guest et sélectionnez Exécuter ou l'une des options Arrêter dans le menu contextuel.



- Redémarrer un invité

  Vous pouvez redémarrer un invité de machine virtuelle à partir du Gestionnaire de machine virtuelle. Pour redémarrer la machine virtuelle, cliquez avec le bouton droit sur l'entrée VM Guest, puis sélectionnez Arrêter > Redémarrer dans le menu contextuel.

- Supprimer un invité

  La suppression d'un invité de machine virtuelle supprime sa configuration XML par défaut. Vous pouvez également supprimer les fichiers de stockage d'un invité. Cela efface complètement l'invité.

  1. Dans Virtual Machine Manager, cliquez avec le bouton droit sur l'entrée VM Guest.
  2. Sélectionnez Supprimer dans le menu contextuel. Une fenêtre de confirmation s'ouvre. Remarque : l'option Supprimer n'est activée que lorsque l'invité de la machine virtuelle est arrêté.
  3. Cliquez sur Supprimer.
  4. Pour effacer complètement l'invité, supprimez le fichier .raw associé en cochant la case Supprimer les fichiers de stockage associés.

Gérer les machines virtuelles invitées Citrix ADC VPX à l'aide du programme `virsh`

- Répertorier les invités VM et leurs états actuels.

Pour utiliser `virsh` pour afficher des informations sur les invités

```
virsh list --all
```

La sortie de la commande affiche tous les domaines avec leurs états. Exemple de sortie :

```
Id Name                 State
----------------------------------
  0 Domain-0           running
  1 Domain-1           paused
  2 Domain-2           inactive
  3 Domain-3           crashed
<!--NeedCopy-->
```

- Ouvrez une console `virsh`.

  Connectez la machine virtuelle invitée via la console

  ```
  virsh console [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Exemple :

  ```
  virsh console NetScaler-VPX
  ```

- Démarrez et arrêtez un invité.

  Vous pouvez commencer à utiliser DomainName ou Domain-UID.

  ```
  virsh start [<DomainName> | <DomainUUID>]
  ```

  Exemple :

  ```
  virsh start NetScaler-VPX
  ```

  Pour arrêter un invité :

  ```
  virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Exemple :

  ```
  virsh shutdown NetScaler-VPX
  ```

- Redémarrer un invité

  ```
  virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Exemple :

  ```
  virsh reboot NetScaler-VPX
  ```

  Supprimer un invité

  Pour supprimer une machine virtuelle invitée, vous devez arrêter l'invité et annuler la définition de <DomainName>-NSVPX-KVM-*_NC.xml avant d'exécuter la commande delete.


```
virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
virsh undefine [<DomainName> | <DomainUUID>]
<!--NeedCopy-->
```

Exemple :

```
virsh shutdown NetScaler-VPX
virsh undefine NetScaler-VPX
<!--NeedCopy-->
```

> Remarque : La commande delete ne supprime pas le fichier image disque qui doit être supprimé manuellement.

Provisionner l'instance Citrix ADC VPX avec SR-IOV, sur OpenStack

August 20, 2021

Vous pouvez déployer des instances Citrix ADC VPX hautes performances qui utilisent la technologie de virtualisation des E/S à racine unique (SR-IOV), sur OpenStack.

Vous pouvez déployer une instance Citrix ADC VPX qui utilise la technologie SR-IOV, sur OpenStack, en trois étapes :

- Activez SR-IOV Virtual Functions (VF) sur l'hôte.
- Configurez et rendez les VFS disponibles pour OpenStack.
- Provisionnez le Citrix ADC VPX sur OpenStack.

Conditions préalables

Assurez-vous que vous :

- Ajoutez la carte réseau (NIC) Intel 82599 à l'hôte.
- Téléchargez et installez le dernier pilote IXGBE d'Intel.
- Liste de blocage du pilote IXGBEVF sur l'hôte. Ajoutez l'entrée suivante dans le fichier /etc/modprobe.d/blacklist.conf : Liste des blocs `ixgbevf`

> **Remarque**
>
> La version du `ixgbe` pilote doit être minimale 5.0.4.

Activer les VF SR-IOV sur l'hôte

Pour activer les VF SR-IOV, effectuez l'une des opérations suivantes :

- <number_of_VFs>Si vous utilisez une version du noyau antérieure à 3.8, ajoutez l'entrée suivante au fichier /etc/modprobe.d/ixgbe et redémarrez l'hôte : options ixgbe max_vfs=
- Si vous utilisez le noyau 3.8 version ou ultérieure, créez des VF à l'aide de la commande suivante :

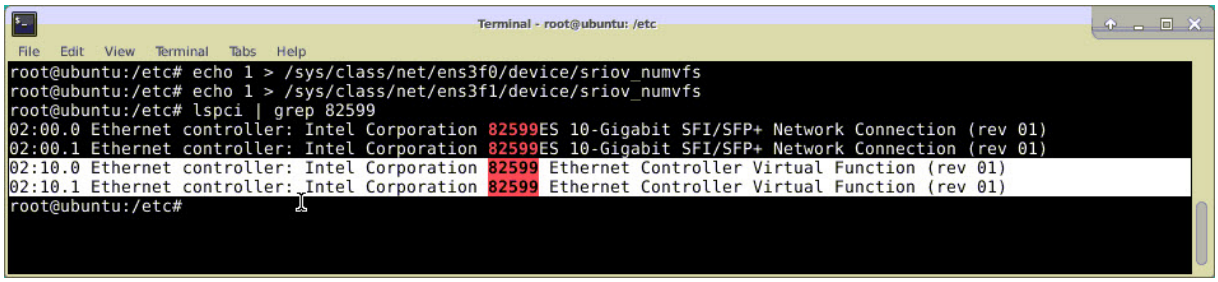
```
1     echo <number_of_VFs> > /sys/class/net/<device_name>/device/
         sriov_numvfs
2 <!--NeedCopy-->
```

Où :

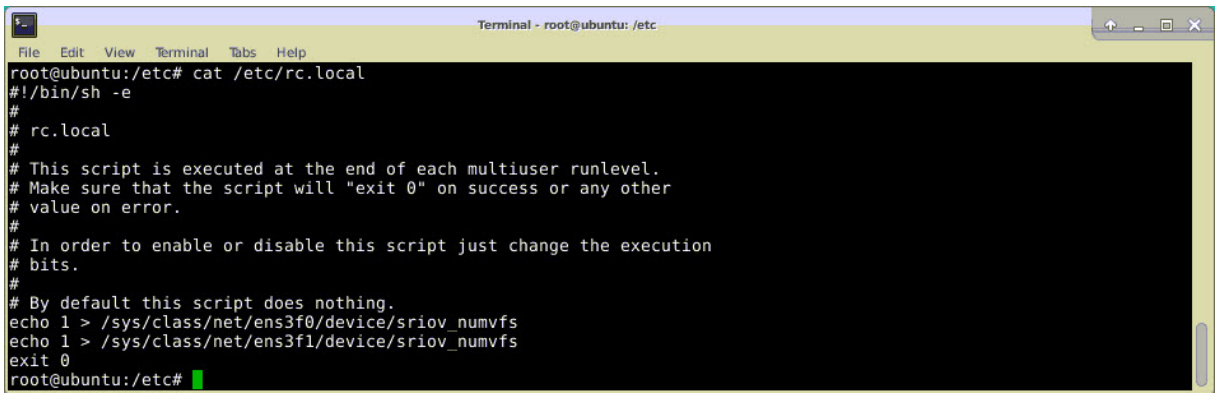
- Number_of_VFS est le nombre de fonctions virtuelles que vous souhaitez créer.
- nom_périphérique est le nom de l'interface.

> **Important**
>
> Lorsque vous créez les VF SR-IOV, assurez-vous que vous n'attribuez pas d'adresses MAC aux VF.

Voici un exemple de quatre VF en cours de création.



Rendez les VFS persistants, ajoutez les commandes que vous avez utilisées pour créer des VFS au fichier **rc.local** . Voici un exemple montrant le contenu du fichier rc.local.



Pour plus d'informations, consultez ce guide de configuration Intel SR-IOV.

Configurer et rendre les VFS disponibles pour OpenStack

Suivez les étapes indiquées sur le lien ci-dessous pour configurer SR-IOV sur OpenStack :https://wiki.openstack.org/wiki/SR-IOV-Passthrough-For-Networking.

Provisionner l'instance Citrix ADC VPX sur OpenStack

Vous pouvez provisionner une instance Citrix ADC VPX dans un environnement OpenStack à l'aide de l'interface de ligne de commande OpenStack.

Le provisioning d'une instance VPX implique éventuellement l'utilisation de données provenant du lecteur de configuration. Le lecteur de configuration est un lecteur de configuration spécial qui se fixe à l'instance lors du démarrage. Ce lecteur de configuration peut être utilisé pour transmettre des informations de configuration réseau telles que l'adresse IP de gestion, le masque réseau et la passerelle par défaut, etc., à l'instance avant de configurer les paramètres réseau de l'instance.

Lorsque OpenStack provisionnera une instance VPX, il détecte d'abord que l'instance démarre dans un environnement OpenStack, en lisant une chaîne de BIOS spécifique (OpenStack Foundation) qui indique OpenStack. Pour les distributions Red Hat Linux, la chaîne est stockée dans /etc/nova/release. Il s'agit d'un mécanisme standard disponible dans toutes les implémentations OpenStack basées sur la plate-forme hyper-viseur KVM. Le disque doit comporter une étiquette OpenStack spécifique. Si le lecteur de configuration est détecté, l'instance tente de lire les informations suivantes à partir du nom de fichier spécifié dans la commande de `nova` démarrage. Dans les procédures ci-dessous, le fichier est appelé « userdata.txt ».

- Adresse IP de gestion
- Masque réseau
- Gateway par défaut

Une fois les paramètres lus avec succès, ils sont remplis dans la pile NetScaler. Cela aide à gérer l'instance à distance. Si les paramètres ne sont pas lus correctement ou si le lecteur de configuration n'est pas disponible, l'instance passe au comportement par défaut, qui est :

- L'instance tente de récupérer les informations d'adresse IP à partir de DHCP.
- Si DHCP échoue ou temporisation, l'instance affiche la configuration réseau par défaut (192.168.100.1/16).

Provisionner l'instance Citrix ADC VPX sur OpenStack via CLI

Vous pouvez provisionner une instance VPX dans un environnement OpenStack à l'aide de l'interface de ligne de commande OpenStack. Voici le résumé des étapes pour provisionner une instance Citrix ADC VPX sur OpenStack :

1. Extraction du `.qcow2` fichier du fichier .tgz

2. Création d'une image OpenStack à partir de l'image qcow2
3. Provisionnement d'une instance VPX

Pour provisionner une instance VPX dans un environnement OpenStack, procédez comme suit.

1. Extrayez le. `qcow2` fichier à partir du `.tqz` fichier en tapant la commande :

```
tar xvzf <TAR file>
tar xvzf NSVPX-KVM-12.0-26.2_nc.tgz
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
<!--NeedCopy-->
```

2. Créez une image OpenStack à l'aide du `.qcoz2` fichier extrait à l'étape 1 en tapant la commande suivante :

```
glance image-create --name="<name of the OpenStack image>" --
    property hw_disk_bus=ide --is-public=true --container-format=
    bare --disk-format=qcow2< <name of the qcow2 file>

glance image-create --name="NS-VPX-12-0-26-2" --property
    hw_disk_bus=ide --is-public= true --container-format=bare --
    disk-format=qcow2< NSVPX-KVM-12.0-26.2_nc.qcow2
<!--NeedCopy-->
```

L'illustration suivante fournit un exemple de sortie pour la commande glance image-create.

Property	Value
checksum	735dae4ea6e46e39ed3f0acfba02e755
container_format	bare
created_at	2017-02-16T10:03:29Z
disk_format	qcow2
hw_disk_bus	ide
id	aeaa13e9-b49b-411c-ab54-c61820a8e2f3
min_disk	0
min_ram	0
name	NSVPX-KVM-12.0-26.2
owner	06c41a73b32f4b48af55359fd7d3502c
protected	False
size	717946880
status	active
tags	[]
updated_at	2017-02-16T10:03:38Z
virtual_size	None
visibility	private

3. Une fois qu'une image OpenStack est créée, provisionnez l'instance Citrix ADC VPX.

```
nova boot --image NSVPX-KVM-12.0-26.2 --config-drive=true --
   userdata
./userdata.txt --flavor m1. medium --nic net-id=3b258725-eaae-
455e-a5de-371d6d1f349f --nic port-id=218ba819-9f55-4991-adb6-
02086a6bdee2 NSVPX-10
<!--NeedCopy-->
```

Dans la commande précédente, userdata.txt est le fichier qui contient les détails tels que l'adresse IP, le masque de réseau et la passerelle par défaut de l'instance VPX. Le fichier de données utilisateur est un fichier personnalisable par l'utilisateur. NSVPX-KVM-12.0-26.2 est le nom de l'appliance virtuelle que vous souhaitez provisionner. —NIC port-id=218ba819-9f55-4991-adb6-02086a6bdee2 est le VF OpenStack.

L'illustration suivante donne un exemple de sortie de la commande nova boot.

Property	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	-
OS-EXT-SRV-ATTR:hypervisor_hostname	-
OS-EXT-SRV-ATTR:instance_name	instance-0000003c
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	-
OS-SRV-USG:terminated_at	-
accessIPv4	
accessIPv6	
adminPass	43EjPdM5shLz
config_drive	True
created	2017-02-20T11:53:37Z
flavor	m1.medium (3)
hostId	
id	6b9f6968-aab9-463c-b619-d58c73db3187
image	NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)
key_name	-
metadata	{}
name	NSVPX-10
os-extended-volumes:volumes_attached	[]
progress	0
security_groups	default
status	BUILD
tenant_id	06c41a73b32f4b48af55359fd7d3502c
updated	2017-02-20T11:53:38Z
user_id	418524f7101b4f0389ecbb36da9916b5

L'illustration suivante montre un exemple du fichier userdata.txt. Les valeurs contenues dans les<PropertySection></PropertySection> balises sont celles qui sont configurables par l'utilisateur et contiennent des informations telles que l'adresse IP, le masque de réseau et la passerelle par défaut.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1">
<PlatformSection>
<Kind>NOVA</Kind>
<Version>2013.1</Version>
<Vendor>Openstack</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"
   />
<Property oe:key="com.citrix.netscaler.platform" oe:value="vpx"/>
citrix.com 4
<Property oe:key="com.citrix.netscaler.orch_env"
oe:value="openstack-orch-env"/>
```



```
<Property oe:key="com.citrix.netscaler.mgmt.ip"
oe:value="10.1.0.100"/>
<Property oe:key="com.citrix.netscaler.mgmt.netmask"
oe:value="255.255.0.0"/>
<Property oe:key="com.citrix.netscaler.mgmt.gateway"
oe:value="10.1.0.1"/>
</PropertySection>
</Environment>
<!--NeedCopy-->
```

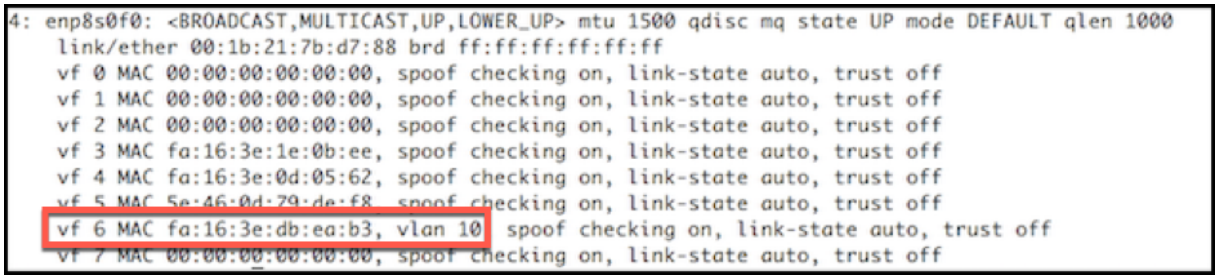
Configurations supplémentaires prises en charge : création et suppression de VLAN sur des VF SR-IOV de l'hôte

Tapez la commande suivante pour créer un VLAN sur le VF SR-IOV :

```
ip link show enp8s0f0 vf 6 vlan 10
```

Dans la commande précédente, « enp8s0f0" est le nom de la fonction physique.

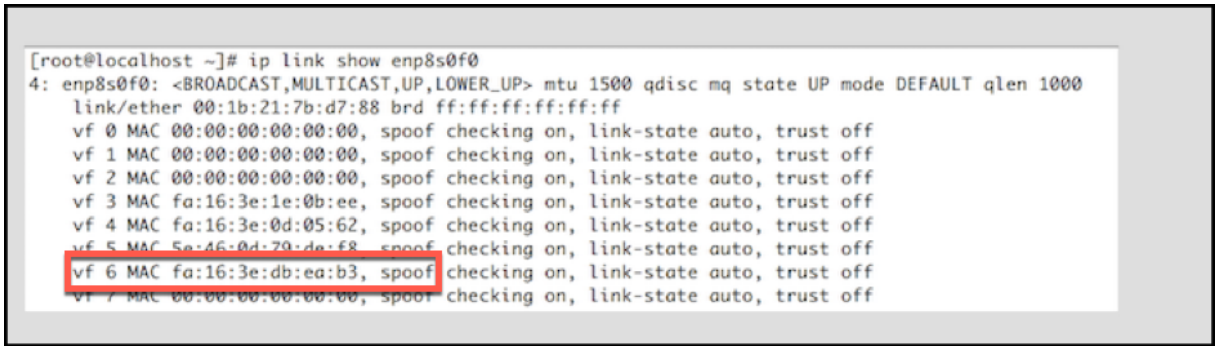
Exemple : VLAN 10, créé sur vf 6



Tapez la commande suivante pour supprimer un VLAN sur le VF SR-IOV :

```
ip link show enp8s0f0 vf 6 vlan 0
```

Exemple : VLAN 10, supprimé de vf 6



Ces étapes complètent la procédure de déploiement d'une instance Citrix ADC VPX qui utilise la technologie SRIOV, sur OpenStack.

Configurer une instance Citrix ADC VPX sur KVM pour utiliser les interfaces hôtes OVS DPDK

August 20, 2021

Vous pouvez configurer une instance Citrix ADC VPX exécutée sur KVM (Fedora et RHOS) pour utiliser Open vSwitch (OVS) avec Data Plane Development Kit (DPDK) pour de meilleures performances réseau. Ce document explique comment configurer l'instance Citrix ADC VPX pour qu'elle fonctionne sur les `vhost-user` ports exposés par OVS-DPDK sur l'hôte KVM.

OVS est un commutateur virtuel multicouche sous licence Apache 2.0 open source. DPDK est un ensemble de bibliothèques et de pilotes permettant un traitement rapide des paquets.

Les versions suivantes de Fedora, RHOS, OVS et DPDK sont qualifiées pour la configuration d'une instance Citrix ADC VPX :

Fedora	RHOS
Fedora 25	RHOS 7.4
OVS 2.7.0	OVS 2.6.1
DPDK 16.11.12	DPDK 16.11.12

Conditions préalables

Avant d'installer DPDK, assurez-vous que l'hôte dispose de pages gigantesques de 1 Go.

Pour plus d'informations, consultez cette documentation relative à la configuration système requise pour DPDK. Voici un résumé des étapes requises pour configurer une instance Citrix ADC VPX sur KVM pour utiliser des interfaces hôtes basées sur OVS DPDK :

- Installez DPDK.
- Construire et installer OVS.
- Créez un pont OVS.
- Attachez une interface physique au pont OVS.
- Connectez des `vhost-user` ports au chemin de données OVS.
- Provisionnez un KVM-VPX avec des `vhost-user` ports OVS-DPDK.

Installer DPDK

Pour installer DPDK, suivez les instructions données dans ce document Open vSwitch with DPDK .

Construire et installer OVS

Téléchargez OVS depuis la page de téléchargementd'OVS. Ensuite, créez et installez OVS à l'aide d'un chemin de données DPDK. Suivez les instructions fournies dans le document Installer Open vSwitch .

Pour plus d'informations, consultez DPDK Getting Started Guide for Linux.

Créer un pont OVS

Selon vos besoins, tapez la commande Fedora ou RHOS pour créer un pont OVS :

Commande Fedora :

```
> $OVS_DIR/utilities/ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
    datapath_type=netdev
<!--NeedCopy-->
```

Commande RHOS :

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
<!--NeedCopy-->
```

Attacher l'interface physique au pont OVS

Liez les ports à DPDK, puis attachez-les au pont OVS en tapant les commandes Fedora ou RHOS suivantes :

Commande Fedora :

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface
    dpdk0 type=dpdk  options:dpdk-devargs=0000:03:00.0

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface
    dpdk1 type=dpdk  options:dpdk-devargs=0000:03:00.1
<!--NeedCopy-->
```

Commande RHOS :

```
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
    options:dpdk-devargs=0000:03:00.0


ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface dpdk1 type=dpdk
    options:dpdk-devargs=0000:03:00.1
<!--NeedCopy-->
```


Le `dpdk-devargs` indiqué dans les options spécifie le BDF PCI de la carte réseau physique respective.

Connectez des `vhost-user` ports au chemin de données OVS

Tapez les commandes Fedora ou RHOS suivantes pour attacher des `vhost-user` ports au chemin de données OVS :

Commande Fedora :

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user1 -- set
    Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-
    user1  mtu_request=9000

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user2 -- set
    Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-
    user2  mtu_request=9000

chmod g+w  /usr/local/var/run/openvswitch/vhost*
<!--NeedCopy-->
```

Commande RHOS :

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
    type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000

ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2
    type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000

chmod g+w /var/run/openvswitch/vhost*
<!--NeedCopy-->
```

Provisionner un KVM-VPX avec des `vhost-user` ports OVS-DPDK

Vous pouvez provisionner une instance VPX sur Fedora KVM avec des `vhost-user` ports OVS-DPDK uniquement à partir de l'interface de ligne de commande à l'aide des commandes QEMU suivantes : **commande Fedora** :

```
qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \

-object memory-backend-file,id=mem,size=4096M,mem-path=/dev/hugepages,
    share=on -numa node,memdev=mem \

-mem-prealloc -smp sockets=1,cores=2 -drive file=<absolute-path-to-disc
    -image-file>,if=none,id=drive-ide0-0-0,format=<disc-image-format> \
```



```
6
7  -device ide-drive,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0-0-0,
       bootindex=1 \
8
9  -netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \
10
11 -device virtio-net-pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,
       bus=pci.0,addr=0x3 \
12
13 -chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-
       user1> \
14
15 -netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device
       virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \
16
17 -chardev socket,id=char1,path=</usr/local/var/run/openvswitch/vhost-
       user2> \
18
19 -netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device
       virtio-net
20
21 pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \
22
23 --nographic
24 <!--NeedCopy-->
```

Pour RHOS, utilisez l'exemple de fichier XML suivant pour provisionner l'instance Citrix ADC VPX, à l'aide de `virsh`.

```
1  <domain type='kvm'>
2
3    <name>dpdk-vpx1</name>
4
5    <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
6
7    <memory unit='KiB'>16777216</memory>
8
9    <currentMemory unit='KiB'>16777216</currentMemory>
10
11   <memoryBacking>
12
13     <hugepages>
14
15       <page size='1048576' unit='KiB'/>
16
```



```
17      </hugepages>
18
19    </memoryBacking>
20
21    <vcpu placement='static'>6</vcpu>
22
23    <cputune>
24
25      <shares>4096</shares>
26
27      <vcpupin vcpu='0' cpuset='0'/>
28
29      <vcpupin vcpu='1' cpuset='2'/>
30
31      <vcpupin vcpu='2' cpuset='4'/>
32
33      <vcpupin vcpu='3' cpuset='6'/>
34
35      <emulatorpin cpuset='0,2,4,6'/>
36
37    </cputune>
38
39    <numatune>
40
41      <memory mode='strict' nodeset='0'/>
42
43    </numatune>
44
45    <resource>
46
47      <partition>/machine</partition>
48
49    </resource>
50
51    <os>
52
53      <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
54
55      <boot dev='hd'/>
56
57    </os>
58
59    <features>
60
61      <acpi/>
```



```
62
63      <apic/>
64
65    </features>
66
67    <cpu mode='custom' match='minimum' check='full'>
68
69      <model fallback='allow'>Haswell-noTSX</model>
70
71      <vendor>Intel</vendor>
72
73      <topology sockets='1' cores='6' threads='1'/>
74
75      <feature policy='require' name='ss'/>
76
77      <feature policy='require' name='pcid'/>
78
79      <feature policy='require' name='hypervisor'/>
80
81      <feature policy='require' name='arat'/>
82
83  <domain type='kvm'>
84
85    <name>dpdk-vpx1</name>
86
87    <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
88
89    <memory unit='KiB'>16777216</memory>
90
91    <currentMemory unit='KiB'>16777216</currentMemory>
92
93    <memoryBacking>
94
95      <hugepages>
96
97        <page size='1048576' unit='KiB'/>
98
99      </hugepages>
100
101   </memoryBacking>
102
103   <vcpu placement='static'>6</vcpu>
104
105   <cputune>
106
```



```
107     <shares>4096</shares>
108
109     <vcpupin vcpu='0' cpuset='0'/>
110
111     <vcpupin vcpu='1' cpuset='2'/>
112
113     <vcpupin vcpu='2' cpuset='4'/>
114
115     <vcpupin vcpu='3' cpuset='6'/>
116
117     <emulatorpin cpuset='0,2,4,6'/>
118
119   </cputune>
120
121   <numatune>
122
123     <memory mode='strict' nodeset='0'/>
124
125   </numatune>
126
127   <resource>
128
129     <partition>/machine</partition>
130
131   </resource>
132
133   <os>
134
135     <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
136
137     <boot dev='hd'/>
138
139   </os>
140
141   <features>
142
143     <acpi/>
144
145     <apic/>
146
147   </features>
148
149   <cpu mode='custom' match='minimum' check='full'>
150
151     <model fallback='allow'>Haswell-noTSX</model>
```



```
152
153     <vendor>Intel</vendor>
154
155     <topology sockets='1' cores='6' threads='1'/>
156
157     <feature policy='require' name='ss'/>
158
159     <feature policy='require' name='pcid'/>
160
161     <feature policy='require' name='hypervisor'/>
162
163     <feature policy='require' name='arat'/>
164
165     <feature policy='require' name='tsc_adjust'/>
166
167     <feature policy='require' name='xsaveopt'/>
168
169     <feature policy='require' name='pdpe1gb'/>
170
171     <numa>
172
173       <cell id='0' cpus='0-5' memory='16777216' unit='KiB' memAccess='
             shared'/>
174
175     </numa>
176
177   </cpu>
178
179   <clock offset='utc'/>
180
181   <on_poweroff>destroy</on_poweroff>
182
183   <on_reboot>restart</on_reboot>
184
185   <on_crash>destroy</on_crash>
186
187   <devices>
188
189     <emulator>/usr/libexec/qemu-kvm</emulator>
190
191     <disk type='file' device='disk'>
192
193       <driver name='qemu' type='qcow2' cache='none'/>
194
195       <source file='/home/NSVPX-KVM-12.0-52.18_nc.qcow2'/>
```



```
196
197         <target dev='vda' bus='virtio'/>
198
199         <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
               function='0x0'/>
200
201       </disk>
202
203       <controller type='ide' index='0'>
204
205         <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
               function='0x1'/>
206
207       </controller>
208
209       <controller type='usb' index='0' model='piix3-uhci'>
210
211         <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
               function='0x2'/>
212
213       </controller>
214
215       <controller type='pci' index='0' model='pci-root'/>
216
217       <interface type='direct'>
218
219         <mac address='52:54:00:bb:ac:05'/>
220
221         <source dev='enp129s0f0' mode='bridge'/>
222
223         <model type='virtio'/>
224
225         <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
               function='0x0'/>
226
227       </interface>
228
229       <interface type='vhostuser'>
230
231         <mac address='52:54:00:55:55:56'/>
232
233         <source type='unix' path='/var/run/openvswitch/vhost-user1' mode=
               'client'/>
234
235         <model type='virtio'/>
```



```
236
237       <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
             function='0x0'/>
238
239     </interface>
240
241     <interface type='vhostuser'>
242
243       <mac address='52:54:00:2a:32:64'/>
244
245       <source type='unix' path='/var/run/openvswitch/vhost-user2' mode=
             'client'/>
246
247       <model type='virtio'/>
248
249       <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
             function='0x0'/>
250
251     </interface>
252
253     <interface type='vhostuser'>
254
255       <mac address='52:54:00:2a:32:74'/>
256
257       <source type='unix' path='/var/run/openvswitch/vhost-user3' mode=
             'client'/>
258
259       <model type='virtio'/>
260
261       <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
             function='0x0'/>
262
263     </interface>
264
265     <interface type='vhostuser'>
266
267       <mac address='52:54:00:2a:32:84'/>
268
269       <source type='unix' path='/var/run/openvswitch/vhost-user4' mode=
             'client'/>
270
271      <model type='virtio'/>
272
273       <address type='pci' domain='0x0000' bus='0x00' slot='0x09'
             function='0x0'/>
```



```
274
275      </interface>
276
277      <serial type='pty'>
278
279        <target port='0'/>
280
281      </serial>
282
283      <console type='pty'>
284
285        <target type='serial' port='0'/>
286
287      </console>
288
289      <input type='mouse' bus='ps2'/>
290
291      <input type='keyboard' bus='ps2'/>
292
293      <graphics type='vnc' port='-1' autoport='yes'>
294
295        <listen type='address'/>
296
297      </graphics>
298
299      <video>
300
301        <model type='cirrus' vram='16384' heads='1' primary='yes'/>
302
303        <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
             function='0x0'/>
304
305      </video>
306
307      <memballoon model='virtio'>
308
309        <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
             function='0x0'/>
310
311      </memballoon>
312
313    </devices>
314
315  </domain
316  <!--NeedCopy-->
```


Points à noter

Dans le fichier XML, la hugepage taille doit être de 1 Go, comme indiqué dans le fichier exemple.

```
<memoryBacking>

    <hugepages>

      <page size='1048576' unit='KiB'/>

    </hugepages>
<!--NeedCopy-->
```

En outre, dans le fichier exemple, vhost-user1 est le port vhost utilisateur lié à ovs-br0.

```
<interface type='vhostuser'>

      <mac address='52:54:00:55:55:56'/>

      <source type='unix' path='/var/run/openvswitch/vhost-user1' mode=
         'client'/>

      <model type='virtio'/>

      <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
         function='0x0'/>

    </interface>
<!--NeedCopy-->
```

Pour afficher l'instance Citrix ADC VPX, commencez à utiliser la virsh commande.

Citrix ADC VPX sur AWS

August 20, 2021

Vous pouvez lancer une instance Citrix ADC VPX sur Amazon Web Services (AWS). L'appliance Citrix ADC VPX est disponible en tant qu'image machine Amazon (AMI) sur le marché AWS. Une instance Citrix ADC VPX sur AWS vous permet d'utiliser les fonctionnalités de cloud computing AWS et d'utiliser les

fonctionnalités d'équilibrage de charge et de gestion du trafic Citrix ADC pour leurs besoins professionnels. L'instance VPX prend en charge toutes les fonctionnalités de gestion du trafic d'une appliance Citrix ADC physique et peut être déployée en tant qu'instances autonomes ou en paires HA. Pour plus d'informations sur les fonctionnalités de VPX, consultez la fiche technique VPX.

Mise en route

Avant de commencer à utiliser votre déploiement VPX, vous devez être familier avec les informations suivantes :

- Terminologie AWS
- Matrice de prise en charge AWS-VPX
- Limitations et directives d'utilisation
- Conditions préalables
- Fonctionnement d'une instance Citrix ADC VPX sur AWS

Deploy a Citrix ADC VPX instance on AWS

Dans AWS, les types de déploiement suivants sont pris en charge pour les instances VPX :

- Autonome
- Haute disponibilité (Acitve-Passif)
  - Haute disponibilité dans la même zone
  - Haute disponibilité dans différentes zones grâce à Elastic IP
  - Haute disponibilité dans différentes zones à l'aide de Private IP
- GSLB Active-Actif
- Mise à l'échelle automatique (Active-Active) à l'aide d'ADM

Déploiements hybrides

- Déployer Citrix ADC dans AWS Outpost
- Déployer Citrix ADC dans VMC dans AWS

Système de licences

Une instance Citrix ADC VPX sur AWS nécessite une licence. Les options de licence suivantes sont disponibles pour les instances Citrix ADC VPX exécutées sur AWS :

- Gratuit (illimité)
- Toutes les heures
- Annuel

- BYOL
- Essai gratuit (toutes les offres d'abonnement Citrix ADC VPX-AWS pendant 21 jours gratuits sur AWS Marketplace.)

Automatisation

- Citrix ADM : Déploiement intelligent
- Démarrage rapide AWS : Citrix ADC VPX pour applications Web sur AWS
- CFT GitHub : modèles et scripts Citrix ADC pour le déploiement AWS
- GitHub Ansible : modèles et scripts Citrix ADC pour le déploiement AWS
- GitHub Terraform : modèles et scripts Citrix ADC pour le déploiement AWS
- Bibliothèque de signatures AWS (PL) : Citrix ADC VPX

Blogs

- Comment Citrix ADC sur AWS aide les clients à fournir des applications en toute sécurité
- Fourniture d'applications dans le cloud hybride avec Citrix ADC et AWS
- Citrix est un partenaire de compétences réseau AWS
- Citrix ADC : Toujours prêt pour les clouds publics
- Évolutivité ou évolutivité avec facilité dans les nuages publics via Citrix ADC
- Citrix élargit le choix de déploiement ADC avec AWS Outposts
- Utilisation de Citrix ADC avec le routage d'entrée Amazon VPC
- Citrix offre choix, performances et déploiement simplifié dans AWS
- La sécurité du Citrix Web App Firewall — désormais disponible sur AWS Marketplace
- Comment Aria Systems utilise Citrix Web App Firewall sur AWS

Vidéos

- Simplification des déploiements Citrix ADC dans le cloud public via ADM
- Provisioning et configuration de Citrix ADC VPX dans AWS à l'aide de scripts terraform prêts à l'emploi
- Déployer Citrix ADC HA dans AWS à l'aide du modèle CloudFormation
- Déployer Citrix ADC HA dans les zones de disponibilité à l'aide d'AWS QuickStart

- Comment déployer Citrix ADC dans AWS
- Mise à l'échelle automatique Citrix ADC à l'aide d'ADM
- Citrix ADC prenant en charge la mise à l'échelle automatique des serveurs back-end dans AWS ou AWS Autoscaling groupe

Études de cas client

- Solution technologique - Xenit AB
- Une meilleure façon de faire des affaires avec Citrix et AWS cloud — Aria
- Découvrez l'avantage Citrix ADC et AWS
- Rain for Rent - Témoignage client

Solutions

- Déploiement d'une plateforme de publicité numérique sur AWS avec Citrix ADC
- Amélioration de l'analyse des flux de clics dans AWS à l'aide de Citrix ADC

Assistance

- Ouvrir un dossier de support
- Pour connaître l'offre d'abonnement Citrix ADC, voir Dépannage d'une instance VPX sur AWS. Pour déposer un dossier de support, recherchez votre numéro de compte AWS et votre code PIN de support, puis appelez le support Citrix.
- Pour l'offre sous licence client Citrix ADC ou BYOL, assurez-vous que vous disposez du contrat de support et de maintenance valide. Si vous n'avez pas d'accord, contactez votre représentant Citrix.

Références supplémentaires

- Webinaire AWS à la demande - Citrix ADC sur AWS
- Guides de déploiement pour Citrix ADC VPX sur AWS
- Création d'une image machine Amazon VPX (AMI) dans la région SC2S/Secret
- Citrix ADC sur AWS
- Conception de référence validée Citrix ADC et AWS
- Fiche technique Citrix ADC VPX
- Citrix ADC dans AWS Marketplace

- Citrix ADC fait partie des solutions partenaires réseau AWS (équilibreurs de charge)
- Citrix ADC pour le cloud VMware sur AWS
- Questions fréquentes sur AWS

Terminologie AWS

August 20, 2021

Cette section décrit la liste des termes et expressions AWS couramment utilisés. Pour plus d'informations, consultez AWS Glossary.

Terme	Définition
Image machine Amazon (AMI)	Image de machine, qui fournit les informations nécessaires au lancement d'une instance, qui est un serveur virtuel dans le cloud.
Elastic Block Store	Fournit des volumes de stockage en blocs persistants à utiliser avec des instances Amazon EC2 dans le cloud AWS.
Service de stockage simple (S3)	Stockage pour Internet. Il est conçu pour faciliter l'informatique à l'échelle du Web pour les développeurs.
Elastic Compute Cloud (EC2)	Service Web qui fournit une capacité de calcul sécurisée et redimensionnable dans le cloud. Il est conçu pour faciliter l'informatique en nuage à l'échelle du Web pour les développeurs.
Équilibrage de charge élastique (ELB)	Répartit le trafic d'application entrant sur plusieurs instances EC2, dans plusieurs zones de disponibilité. Cela augmente la tolérance aux pannes de vos applications.
Interface réseau élastique (ENI)	Interface réseau virtuelle que vous pouvez attacher à une instance dans un Virtual Private Cloud (VPC).

Terme	Définition
Adresse IP élastique (EIP)	Adresse IPv4 publique statique que vous avez allouée dans Amazon EC2 ou Amazon VPC, puis attachée à une instance. Les adresses IP Elastic sont associées à votre compte, et non à une instance spécifique. Ils sont élastiques car vous pouvez facilement les allouer, les attacher, les détacher et les libérer au fur et à mesure que vos besoins changent.
Type d'instance	Amazon EC2 propose un large choix de types d'instance optimisés pour s'adapter à différents cas d'utilisation. Les types d'instance comprennent diverses combinaisons de CPU, de mémoire, de stockage et de capacité réseau et vous offrent la flexibilité nécessaire pour choisir la combinaison appropriée de ressources pour vos applications.
Identity and Access Management (IAM)	Identité AWS avec des stratégies d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire dans AWS. Vous pouvez utiliser un rôle IAM pour permettre aux applications exécutées sur une instance EC2 d'accéder en toute sécurité à vos ressources AWS. Le rôle IAM est requis pour déployer des instances VPX dans une configuration haute disponibilité.
Passerelle Internet	Connecte un réseau à Internet. Vous pouvez acheminer le trafic pour les adresses IP en dehors de votre VPC vers la Gateway Internet.
Paire de clés	Ensemble d'informations d'identification de sécurité que vous utilisez pour prouver votre identité par voie électronique. Une paire de clés se compose d'une clé privée et d'une clé publique.

Terme	Définition
Tables de routage	Ensemble de règles de routage qui contrôle le trafic quittant tout sous-réseau associé à la table de routage. Vous pouvez associer plusieurs sous-réseaux à une seule table de routage, mais un sous-réseau ne peut être associé qu'à une seule table de routage à la fois.
Groupes de sécurité	Ensemble nommé de connexions réseau entrantes autorisées pour une instance.
Sous-réseaux	Segment de la plage d'adresses IP d'un VPC auquel les instances EC2 peuvent être attachées. Vous pouvez créer des sous-réseaux pour regrouper des instances en fonction des besoins opérationnels et de sécurité.
Virtual Private Cloud (VPC)	Service Web permettant de Provisioning une section logiquement isolée du cloud AWS dans laquelle vous pouvez lancer des ressources AWS dans un réseau virtuel que vous définissez.
Mise à l'échelle automatique	Service Web permettant de lancer ou de mettre fin à des instances Amazon EC2 automatiquement en fonction de stratégies, de calendriers et de vérifications de l'état définies par l'utilisateur.
CloudFormation	Service d'écriture ou de modification de modèles qui créent et suppriment ensemble des ressources AWS associées en tant qu'unité.

Matrice de prise en charge VPX-AWS

August 20, 2021

Les tableaux suivants répertorient le modèle VPX pris en charge et les régions, les types d'instance et les services AWS.

Tableau 1 : Modèles VPX pris en charge sur AWS

Modèle VPX pris en charge
Citrix ADC VPX Standard/Advance/Premium Edition - 200 Mbps
Citrix ADC VPX Standard/Advance/Premium Edition - 1000 Mbps
Citrix ADC VPX Standard/Advance/Premium Edition - 3 Gbit/s
Citrix ADC VPX Standard/Advance/Premium Edition - 5 Gbit/s
Citrix ADC VPX Standard/Avancé/Premium - 10 Mbps
Citrix ADC VPX Express - 20 Mbps
Citrix ADC VPX - Licence client
Citrix ADC (anciennement NetScaler) VPX FIPS - Licence client

Tableau : 2 régions AWS prises en charge

Régions AWS prises en charge
Région de l’Ouest des États-Unis (Oregon)
Région Ouest des États-Unis (Californie du Nord)
Région de l’Est des États-Unis (Ohio)
Région USA Est (Virginie du Nord)
Région Asie-Pacifique (Mumbai)
Région Asie-Pacifique (Séoul)
Région du Canada (Centre)
Région Asie-Pacifique (Singapour)
Région Asie-Pacifique (Sydney)
Région Asie-Pacifique (Tokyo)
Région Asie-Pacifique (Hong Kong)
Région du Canada (Centre)
Chine (Beijing) Région
Chine (Ningxia) région
Région UE (Francfort)
Région UE (Irlande)
Région UE (Londres)

Régions AWS prises en charge
Région UE (Paris)
Région UE (Milan)
Région Amérique du Sud (São Paulo)
Région AWS GovCloud (États-Unis-Est)
Région AWS GovCloud (US-Ouest)
Région AWS Top Secret (C2S)
Région Moyen-Orient (Bahreïn)
Afrique (Le Cap)
C2S

Tableau 3 : Types d'instance AWS pris en charge

Types d'instance AWS pris en charge
T2.medium, T2.large, T2.x Large, T2.2x Large
M3. Large, M3.x Large, M3,2 x Large
C4. Large, C4.large, C4,2 x grand, C4,4 x grand, C4,8 x grand
M4. Large, M4.large, M4,2 x grand, M4,4 x grand, M4,10 x grand
M5. Large, M5.x grand, M5,2 x grand, M5,4 x grand, M5,12 x grand, M5,24 x grand
C5.large, C5.x grand, C5,2 x grand, C5,4 x grand, C5,9 x grand, C5,18 x grand, C5,24 x grand
C5n.Grand, C5N.x grand, C5N.2x grand, C5N.4 x grand, C5N.9 x grand, C5N.18 x grand
D2.x grand, D2,2x grand, D2,4 x grand, D2,8x grand

Tableau 4 : Services AWS pris en charge

Services AWS pris en charge
EC2 : Lance les instances ADC.
Lambda : appelle les API NITRO Citrix ADC VPX VPX lors du provisionnement des instances Citrix ADC VPX à partir de CFT.
Routage d'entrée VPC et VPC : VPC crée des réseaux isolés dans lesquels ADC peut être lancé. Le routage d'entrée VPC est utilisé dans la solution d'équilibrage de charge du pare-feu.

Services AWS pris en charge
Route53 : distribue le trafic sur tous les nœuds ADC VPX de la solution Citrix ADC Autoscale.
ELB : distribue le trafic sur tous les nœuds ADC VPX de la solution Citrix ADC Autoscale.
Cloudwatch : surveille les performances et les paramètres système pour l'instance Citrix ADC VPX.
AWS Autoscaling : utilisé pour la mise à l'échelle automatique des serveurs back-end.
Formation de cloud : les modèles CloudFormation sont utilisés pour déployer des instances Citrix ADC VPX.
Simple Queue Service (SQS) : Surveille les événements à l'échelle et à la baisse dans la mise à l'échelle automatique du back-end.
Simple Notification Service (SNS) : Surveille les événements à l'échelle et à la baisse dans la mise à l'échelle automatique du back-end.
Gestion des identités et des accès (IAM) : permet d'accéder aux services et ressources AWS.
Outposts AWS : Provisionnez les instances Citrix ADC VPX dans AWS Outposts.

Pour une bande passante plus élevée, Citrix recommande les types d'instance suivants :

Type d'instance	Bande passante	Mise en réseau améliorée (SR-IOV)
M4.10x large	3 Gbit/s et 5 Gbit/s	Oui
C4.8x large	3 Gbit/s et 5 Gbit/s	Oui
C5.18x large/M5.18xlarge	25 Gbit/s	ENA
C5N.18 x grand	30 Gbit/s	ENA

Limitations et directives d'utilisation

August 20, 2021

Les limitations et instructions d'utilisation suivantes s'appliquent lors du déploiement d'une instance Citrix ADC VPX sur AWS :

- Avant de commencer, lisez la section Terminologie AWS dans Déployer une instance Citrix ADC VPX sur AWS.

- La fonctionnalité de clustering n'est pas prise en charge pour VPX.
- Pour que la configuration haute disponibilité fonctionne efficacement, associez un périphérique NAT dédié à l'interface de gestion ou associez EIP à NSIP. Pour plus d'informations sur NAT, dans la documentation AWS, consultez Instances NAT.
- Le trafic de données et le trafic de gestion doivent être séparés par les ENIs appartenant à différents sous-réseaux.
- Seule l'adresse NSIP doit être présente sur l'ENI de gestion.
- Si une instance NAT est utilisée pour la sécurité au lieu d'affecter un EIP au NSIP, des modifications appropriées de routage au niveau du VPC sont requises. Pour obtenir des instructions sur la modification du routage au niveau du VPC, dans la documentation AWS, voir Scénario 2 : VPC with Public and Private Subnets.
- Une instance VPX peut être déplacée d'un type d'instance EC2 à un autre (par exemple, de m3.large à m3.xlarge).
- Pour les options de stockage pour VPX sur AWS, Citrix recommande EBS, car il est durable et les données sont disponibles même après leur détachement de l'instance.
- L'ajout dynamique d'ENI à VPX n'est pas pris en charge. Redémarrez l'instance VPX pour appliquer la mise à jour. Citrix vous recommande d'arrêter l'instance autonome ou HA, d'attacher la nouvelle ENI, puis de redémarrer l'instance.
- Vous pouvez attribuer plusieurs adresses IP à un ENI. Le nombre maximal d'adresses IP par ENI est déterminé par le type d'instance EC2, voir la section « Adresses IP par interface réseau par type d'instance » dans Elastic Network Interfaces. Vous devez allouer les adresses IP dans AWS avant de les affecter à des ENI. Pour plus d'informations, voir Interfaces réseau Elastic.
- Citrix vous recommande d'éviter d'utiliser les commandes enable et disable interface sur les interfaces Citrix ADC VPX.
- Citrix ADC `set ha node \<NODE\_ID\> -haStatus STAYPRIMARY` et les commandes `set ha node \<NODE\_ID\> -haStatus STAYSECONDARY` sont désactivés par défaut.
- IPv6 n'est pas pris en charge pour VPX.
- En raison des limitations AWS, ces fonctionnalités ne sont pas prises en charge :
  - Gratuitous ARP (GARP)
  - Mode L2
  - VLAN taggé
  - Routage dynamique
  - MAC virtuel
- Pour que RNAT fonctionne, assurez-vous que la **vérification source/destination** est désactivée. Pour plus d'informations, voir « Modification de la vérification source/destination » dans

Elastic Network Interfaces.

- Dans un déploiement Citrix ADC VPX sur AWS, dans certaines régions AWS, l'infrastructure AWS peut ne pas être en mesure de résoudre les appels d'API AWS. Cela se produit si les appels API sont émis via une interface non gestion sur l'instance Citrix ADC VPX.
  Comme solution de contournement, limitez les appels d'API à l'interface de gestion uniquement. Pour ce faire, créez un NSVLAN sur l'instance VPX et liez l'interface de gestion au NSVLAN à l'aide de la commande appropriée.
  Par exemple :
  ```
  set ns config -nsvlan <vlan id> -ifnum 1/1 -tagged NO
  save config
  ```
  Redémarrez l'instance VPX à l'invite. Pour plus d'informations sur la configuration `nsvlan`, reportez-vous à la section Configuration de NSVLAN.
- Dans la console AWS, l'utilisation du vCPU affichée pour une instance VPX sous l'onglet **Surveillance** peut être élevée (jusqu'à 100 %), même lorsque l'utilisation réelle est beaucoup plus faible. Pour voir l'utilisation réelle du vCPU, accédez à **Afficher toutes les mesures CloudWatch**. Pour plus d'informations, voir Surveillance de vos instances à l'aide d'Amazon CloudWatch.

Conditions préalables

August 20, 2021

Avant de tenter de créer une instance VPX dans AWS, assurez-vous que vous disposez des éléments suivants :

- **Un compte AWS** : pour lancer une AMI Citrix ADC VPX dans un Cloud privé virtuel (VPC) Amazon Web Services (AWS). Vous pouvez créer gratuitement un compte AWS sur www.aws.amazon.com.
- **Un compte d'utilisateur AWS Identity and Access Management (IAM)** : pour contrôler en toute sécurité l'accès aux services et ressources AWS pour vos utilisateurs. Pour plus d'informations sur la création d'un compte utilisateur IAM, consultez la rubrique Création d'utilisateurs IAM (Console).

Un rôle IAM est obligatoire pour les déploiements autonomes et haute disponibilité. Le rôle IAM doit disposer des privilèges suivants :

```
1 ec2:DescribeInstances
2 ec2:DescribeNetworkInterfaces
3 ec2:DetachNetworkInterface
4 ec2:AttachNetworkInterface
5 ec2:StartInstances
```



```
ec2:StopInstances
ec2:RebootInstances
ec2:DescribeAddresses
ec2:AssociateAddress
ec2:DisassociateAddress
ec2:AssignPrivateIpAddresses
ec2:UnAssignPrivateIpAddresses
autoscaling:*
sns:CreateTopic
sns:DeleteTopic
sns:ListTopics
sns:Subscribe
sqs:CreateQueue
sqs:ListQueues
sqs:DeleteMessage
sqs:GetQueueAttributes
sqs:SetQueueAttributes
iam:SimulatePrincipalPolicy
iam:GetRole
<!--NeedCopy-->
```

Si vous utilisez le modèle Citrix CloudFormation, le rôle IAM est automatiquement créé. Le modèle ne permet pas de sélectionner un rôle IAM déjà créé.

> Remarque
>
> Lorsque vous ouvrez une session sur l'instance VPX via l'interface graphique, une invite pour configurer les privilèges requis pour le rôle IAM s'affiche. Ignorez l'invite si vous avez déjà configuré les privilèges.

- **CLI AWS** : Pour utiliser toutes les fonctionnalités fournies par AWS Management Console à partir de votre programme terminal. Pour plus d'informations, consultez le guide de l'utilisateur de l'AWS CLI. Vous avez également besoin de l'interface de ligne de commande AWS pour changer le type d'interface réseau en SR-IOV.
- **Elastic Network Adapter (ENA)** : pour le type d'instance compatible avec le pilote ENA, la version du microprogramme doit être 13.0 et supérieure.

Fonctionnement d'une instance Citrix ADC VPX sur AWS

January 21, 2021

L'instance Citrix ADC VPX est disponible en tant qu'AMI sur AWS Marketplace et peut être lancée en tant qu'instance EC2 au sein d'un VPC AWS. L'instance AMI Citrix ADC VPX nécessite au moins 2 processeurs

virtuels et 2 Go de mémoire. Une instance EC2 lancée dans un VPC AWS peut également fournir les multiples interfaces, plusieurs adresses IP par interface et les adresses IP publiques et privées nécessaires à la configuration VPX. Chaque instance VPX nécessite au moins trois sous-réseaux IP :

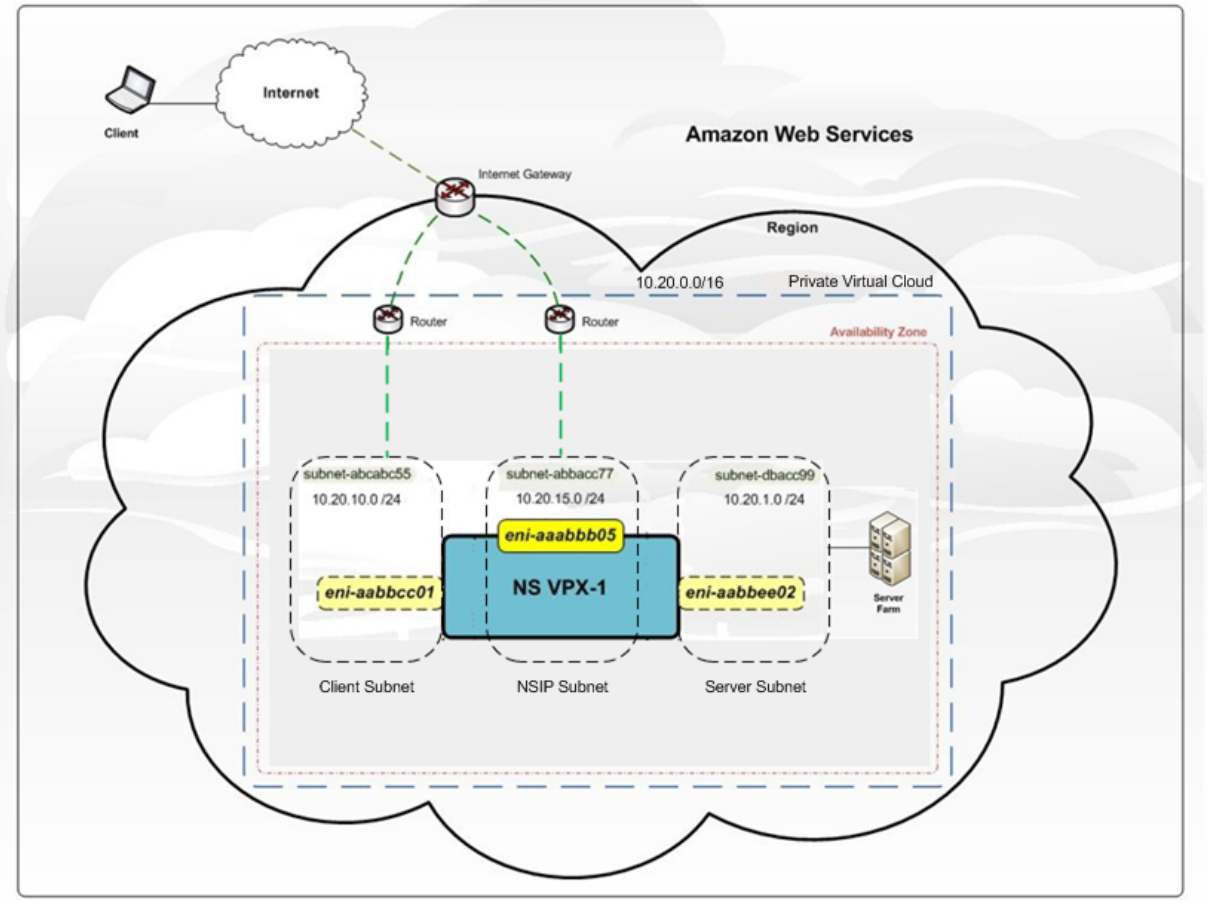
- Un sous-réseau de gestion
- Un sous-réseau orienté client (VIP)
- Un sous-réseau orienté vers le back-end (SNIP, MIP, etc.)

Citrix recommande trois interfaces réseau pour une instance VPX standard sur l'installation AWS.

AWS rend actuellement la fonctionnalité multi-IP disponible uniquement pour les instances exécutées au sein d'un VPC AWS. Une instance VPX dans un VPC peut être utilisée pour équilibrer la charge des serveurs exécutant dans des instances EC2. Un VPC Amazon vous permet de créer et de contrôler un environnement de réseau virtuel, y compris votre propre plage d'adresses IP, sous-réseaux, tables de routage et passerelles réseau.

Remarque : Par défaut, vous pouvez créer jusqu'à 5 instances VPC par région AWS pour chaque compte AWS. Vous pouvez demander des limites de VPC plus élevées en envoyant le formulaire de demande d'Amazon http://aws.amazon.com/contact-us/vpc-request.

Figure 1. Exemple de déploiement d'instance Citrix ADC VPX sur l'architecture AWS



La figure 1 illustre une topologie simple d'un VPC AWS avec un déploiement
Citrix ADC VPX. Le VPC AWS dispose de :

1. Une passerelle Internet unique pour acheminer le trafic entrant et sortant du VPC.
2. Connectivité réseau entre la passerelle Internet et Internet.
3. Trois sous-réseaux, un pour la gestion, le client et le serveur.
4. Connectivité réseau entre la passerelle Internet et les deux sous-réseaux (gestion et client).
5. Instance autonome Citrix ADC VPX déployée au sein du VPC. L'instance VPX a trois ENI, un attaché à chaque sous-réseau.

Déployer une instance autonome de Citrix ADC VPX sur AWS

August 20, 2021

Vous pouvez déployer une instance autonome Citrix ADC VPX sur AWS à l'aide des options suivantes :

- console Web AWS
- Modèle CloudFormation créé par Citrix
- CLI AWS

Cette rubrique décrit la procédure de déploiement d'une instance Citrix ADC VPX sur AWS.

Avant de commencer votre déploiement, lisez les rubriques suivantes :

- Conditions préalables
- Consignes de limitation et d'utilisation

Déployer une instance Citrix ADC VPX sur AWS à l'aide de la console Web AWS

Vous pouvez déployer une instance Citrix ADC VPX sur AWS via la console Web AWS. Le processus de déploiement comprend les étapes suivantes :

1. Créer une paire de clés
2. Créer un Virtual Private Cloud (VPC)
3. Ajouter d'autres sous-réseaux
4. Créer des groupes de sécurité et des règles de sécurité
5. Ajouter des tables de routage
6. Créer une passerelle Internet
7. Créer une instance Citrix ADC VPX
8. Créer et attacher plus d'interfaces réseau
9. Attacher des adresses IP élastiques à la carte réseau de gestion
10. Se connecter à l'instance VPX

Étape 1 : Créer une paire de clés.

Amazon EC2 utilise une paire de clés pour chiffrer et déchiffrer les informations d'ouverture de session. Pour vous connecter à votre instance, vous devez créer une paire de clés, spécifier le nom de la paire de clés lorsque vous lancez l'instance et fournir la clé privée lorsque vous vous connectez à l'instance.

Lorsque vous consultez et lancez une instance à l'aide de l'assistant AWS Launch Instance, vous êtes invité à utiliser une paire de clés existante ou à créer une nouvelle paire de clés. Pour plus d'informations sur la création d'une paire de clés, consultez Paires de clés Amazon EC2.

Étape 2 : Créer un VPC.

Une instance de VPC Citrix ADC est déployée dans un VPC AWS. Un VPC vous permet de définir le réseau virtuel dédié à votre compte AWS. Pour plus d'informations sur AWS VPC, voir Démarrage avec Amazon VPC.

Lors de la création d'un VPC pour votre instance Citrix ADC VPX, gardez à l'esprit les points suivants.

- Utilisez l'option VPC avec un seul sous-réseau public uniquement pour créer un VPC AWS dans une zone de disponibilité AWS.
- Citrix vous recommande de créer au moins **trois sous-réseaux**, des types suivants :
  - Un sous-réseau pour le trafic de gestion. Vous placez l'IP de gestion (NSIP) sur ce sous-réseau. Par défaut, l'interface réseau élastique (ENI) eth0 est utilisé pour la gestion IP.
  - Un ou plusieurs sous-réseaux pour le trafic d'accès client (User-to-Citrix ADC VPX), via lequel les clients se connectent à une ou plusieurs adresses IP virtuelles (VIP) affectées à des serveurs virtuels d'équilibrage de charge Citrix ADC.
  - Un ou plusieurs sous-réseaux pour le trafic d'accès serveur (VPX vers serveur), via lequel vos serveurs se connectent à des adresses SNIP de sous-réseau appartenant à VPX. Pour plus d'informations sur l'équilibrage de charge et les serveurs virtuels, les adresses IP virtuelles (VIP) et les adresses IP de sous-réseau (SNIP) Citrix ADC, voir :
  - Tous les sous-réseaux doivent se trouver dans la même zone de disponibilité.

Étape 3 : Ajouter des sous-réseaux.

Lorsque vous avez utilisé l'assistant VPC, un seul sous-réseau a été créé. Selon vos besoins, vous pouvez créer d'autres sous-réseaux. Pour plus d'informations sur la création d'autres sous-réseaux, voir Ajout d'un sous-réseau à votre VPC.

Étape 4 : Créer des groupes de sécurité et des règles de sécurité.

Pour contrôler le trafic entrant et sortant, créez des groupes de sécurité et ajoutez des règles aux groupes. Pour plus d'informations sur la création de groupes et l'ajout de règles, voir Groupes de sécurité pour votre VPC.

Pour les instances Citrix ADC VPX, l'assistant EC2 fournit des groupes de sécurité par défaut, générés par AWS Marketplace et basés sur les paramètres recommandés par Citrix. Toutefois, vous pouvez créer davantage de groupes de sécurité en fonction de vos besoins.

> **Remarque**
>
> Port 22, 80, 443 à ouvrir sur le groupe de sécurité pour l'accès SSH, HTTP et HTTPS respectivement.

Étape 5 : Ajouter des tables de routage.

La table Routes contient un ensemble de règles, appelées routes, qui sont utilisées pour déterminer où le trafic réseau est dirigé. Chaque sous-réseau de votre VPC doit être associé à une table de routage. Pour plus d'informations sur la création d'une table de routage, consultez Tables de routage.

Étape 6 : Créer une Gateway Internet.

Une Gateway Internet a deux objectifs : fournir une cible dans vos tables de routage VPC pour le trafic routable sur Internet et effectuer la traduction d'adresses réseau (NAT) pour les instances qui ont reçu des adresses IPv4 publiques.

Créez une Gateway Internet pour le trafic Internet. Pour plus d'informations sur la création d'une passerelle Internet, reportez-vous à la section Attachement d'une passerelle Internet.

Étape 7 : Créez une instance Citrix ADC VPX à l'aide du service AWS EC2.

Pour créer une instance Citrix ADC VPX à l'aide du service AWS EC2, procédez comme suit.

1. Dans le tableau de bord AWS, accédez à **Calcul > EC2 > Launch Instance > AWS Marketplace**.

   Avant de cliquer sur **Launch Instance**, vérifiez que votre région est correcte en cochant la note qui apparaît sous **Launch Instance**.

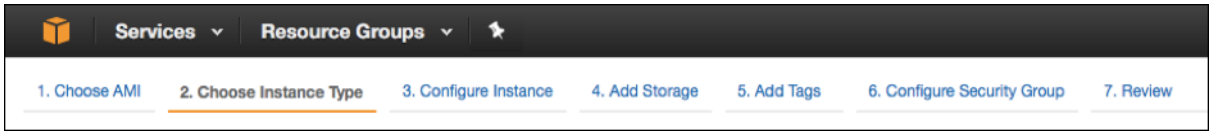
   

2. Dans la barre Rechercher AWS Marketplace, recherchez avec le mot-clé Citrix ADC VPX.
3. Sélectionnez la version à déployer, puis cliquez sur **Sélectionner**. Pour la version Citrix ADC VPX, vous disposez des options suivantes :

   - Une version sous licence
   - Appliance Citrix ADC VPX Express (Il s'agit d'une appliance virtuelle gratuite, disponible à partir de Citrix ADC 12.0 56.20.)
   - Apportez votre propre appareil

L'assistant de lancement d'instance démarre. Suivez l'assistant pour créer une instance. L'Assistant vous invite à :

- Choisir le type d'instance
- Configurer l'instance
- Ajouter du stockage
- Ajouter des balises
- Configurer le groupe de sécurité
- Vérifier



Étape 8 : Créer et attacher plus d'interfaces réseau.

Créez deux interfaces réseau supplémentaires pour VIP et SNIP. Pour plus d'informations sur la création d'autres interfaces réseau, reportez-vous à la section Création d'une interface réseau .

Après avoir créé les interfaces réseau, vous devez les attacher à l'instance VPX. Avant de joindre l'interface, arrêtez l'instance VPX, connectez l'interface et mettez l'instance sous tension. Pour plus d'informations sur la connexion d'interfaces réseau, consultez la section Attachement d'une interface réseau lors du lancement d'une instance .

Étape 9 : Allouer et associer des IP élastiques.

Si vous affectez une adresse IP publique à une instance EC2, elle reste affectée uniquement jusqu'à ce que l'instance soit arrêtée. Après cela, l'adresse est libérée dans le pool. Lorsque vous redémarrez l'instance, une nouvelle adresse IP publique est attribuée.

En revanche, une adresse IP élastique (EIP) reste affectée jusqu'à ce que l'adresse soit dissociée d'une instance.

Allouer et associer une IP élastique pour la carte réseau de gestion. Pour plus d'informations sur l'allocation et l'association d'adresses IP élastiques, consultez les rubriques suivantes :

- Allocation d'une adresse IP élastique
- Associer une adresse IP élastique à une instance en cours d'exécution

Ces étapes complètent la procédure de création d'une instance Citrix ADC VPX sur AWS. Cela peut prendre quelques minutes avant que l'instance soit prête. Vérifiez que votre instance a réussi ses vérifications d'état. Vous pouvez afficher ces informations dans la colonne **Vérifications d'état** de la page Instances.

Étape 10 : Connectez-vous à l'instance VPX.

Après avoir créé l'instance VPX, vous connectez l'instance à l'aide de l'interface graphique et d'un client SSH.

- GUI

Voici les informations d'identification d'administrateur par défaut pour accéder à une instance Citrix ADC VPX

Nom d'utilisateur : `nsroot`

Mot de passe : le mot de passe par défaut du compte racine ns est défini sur AWS Instance-ID de l'instance Citrix ADC VPX. Lors de votre première ouverture de session, vous êtes invité à modifier le mot de passe pour des raisons de sécurité. Après avoir modifié le mot de passe, vous devez enregistrer la configuration. Si la configuration n'est pas enregistrée et que l'instance redémarre, vous devez ouvrir une session avec le mot de passe par défaut. Modifiez à nouveau le mot de passe à l'invite.

- Client SSH

Dans la console de gestion AWS, sélectionnez l'instance Citrix ADC VPX et cliquez sur **Connexion**. Suivez les instructions données sur la page **Se connecter à votre instance** .

Pour plus d'informations sur le déploiement d'une instance autonome Citrix ADC VPX sur AWS à l'aide de la console Web AWS, consultez :

- Scénario : instance autonome
- Comment configurer une instance Citrix NetScaler VPX sur AWS à l'aide du modèle Citrix CloudFormation

Configurer une instance Citrix ADC VPX à l'aide du modèle Citrix CloudFormation

Vous pouvez utiliser le modèle CloudFormation fourni par Citrix pour automatiser le lancement d'instance VPX. Le modèle fournit des fonctionnalités permettant de lancer une seule instance Citrix ADC VPX ou de créer un environnement de haute disponibilité avec une paire d'instances Citrix ADC VPX.

Vous pouvez lancer le modèle depuis AWS Marketplace ou GitHub.

Le modèle CloudFormation nécessite un environnement VPC existant et lance une instance VPX avec trois interfaces réseau élastiques (ENI). Avant de démarrer le modèle CloudFormation, assurez-vous de remplir les conditions suivantes :

- Un cloud privé virtuel (VPC) AWS
- Trois sous-réseaux au sein du VPC : un pour la gestion, un pour le trafic client et un pour les serveurs back-end
- Une paire de clés EC2 pour activer l'accès SSH à l'instance
- Un groupe de sécurité avec les ports UDP 3003, TCP 3009—3010, HTTP, SSH ouverts

Consultez la section « Déployer une instance Citrix ADC VPX sur AWS à l'aide de la console Web AWS » ou la documentation AWS pour plus d'informations sur la façon de remplir les conditions préalables.

Regardez cette vidéo pour savoir comment configurer et lancer une instance autonome Citrix ADC VPX à l'aide du modèle Citrix CloudFormation disponible sur AWS Marketplace.

En outre, vous configurez et lancez une instance autonome Citrix ADC VPX Express à l'aide du modèle Citrix CloudFormation disponible dans GitHub :

https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/

Un rôle IAM n'est pas obligatoire pour un déploiement autonome. Toutefois, Citrix vous recommande de créer et d'attacher un rôle IAM avec les privilèges requis à l'instance, pour les besoins futurs. Le rôle IAM garantit que l'instance autonome est facilement convertie en nœud haute disponibilité avec SR-IOV, si nécessaire.

Pour plus d'informations sur les privilèges requis, consultez Configuration des instances Citrix ADC VPX pour utiliser l'interface réseau SR-IOV.

> Remarque
> Si vous déployez une instance Citrix ADC VPX sur AWS à l'aide de la console Web AWS, le service CloudWatch est activé par défaut. Si vous déployez une instance Citrix ADC VPX à l'aide du modèle Citrix CloudFormation, l'option par défaut est « Oui ». Si vous souhaitez désactiver le service CloudWatch, sélectionnez « Non ». Pour plus d'informations, voir Surveillance de vos instances à l'aide d'Amazon CloudWatch.

Configurer une instance Citrix ADC VPX à l'aide de l'interface de ligne de commande AWS

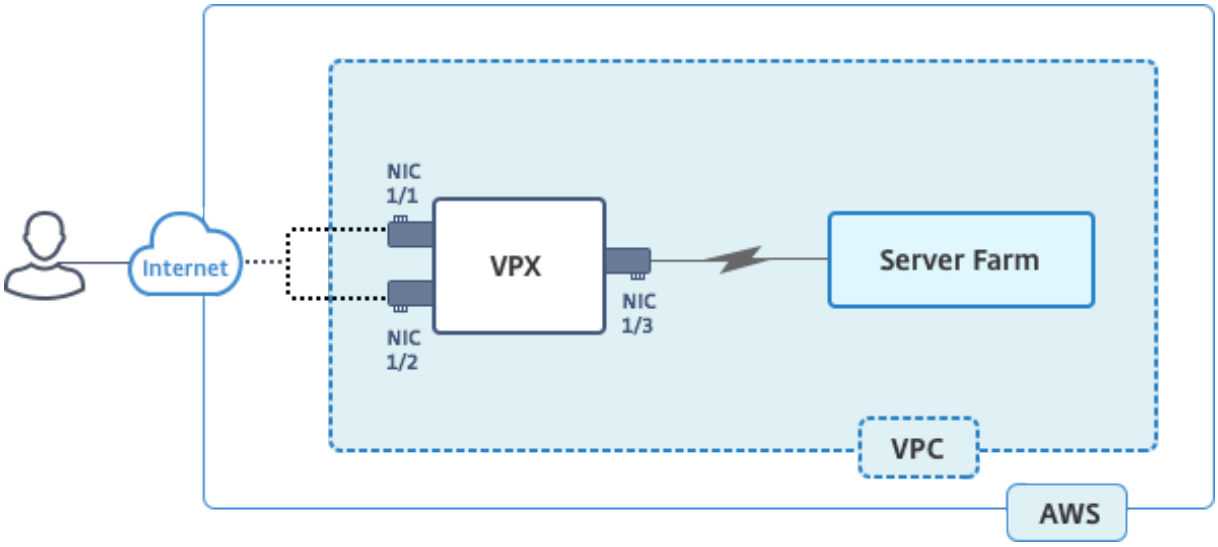
Vous pouvez utiliser l'interface de ligne de commande AWS pour lancer des instances. Pour plus d'informations, consultez la documentation de l'interface de ligne de commande AWS.

Scénario : instance autonome

August 20, 2021

Ce scénario illustre comment déployer une instance EC2 autonome Citrix ADC VPX dans AWS à l'aide de l'interface graphique AWS. Créez une instance VPX autonome avec trois cartes réseau. L'instance, qui est configurée en tant que serveur virtuel d'équilibrage de charge, communique avec les serveurs back-end (la batterie de serveurs). Pour cette configuration, configurez les routes de communication requises entre l'instance et les serveurs dorsaux, et entre l'instance et les hôtes externes sur Internet public.

Pour plus d'informations sur la procédure de déploiement d'une instance VPX, voir Déployer une instance autonome Citrix ADC VPX sur AWS.

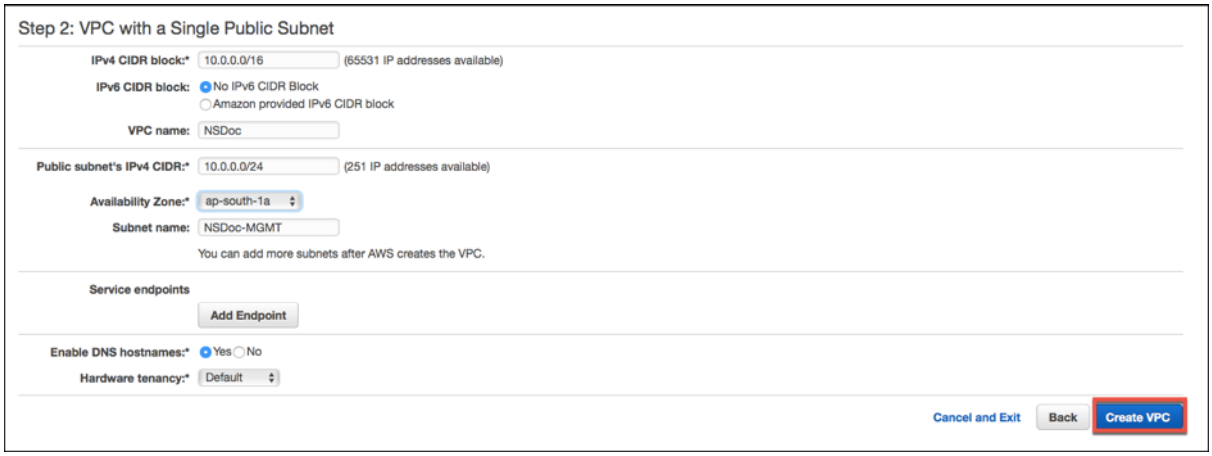


Créez trois cartes réseau. Chaque carte réseau peut être configurée avec une paire d'adresses IP (publiques et privées). Les cartes réseau servent les objectifs suivants.

CARTE RÉSEAU	Objectif	Associé à
eth0	Sert le trafic de gestion (NSIP)	Une adresse IP publique et une adresse IP privée
eth1	Sert le trafic côté client (VIP)	Une adresse IP publique et une adresse IP privée
eth2	Communication avec les serveurs back-end (SNIP)	Une adresse IP publique (adresse IP privée non obligatoire)

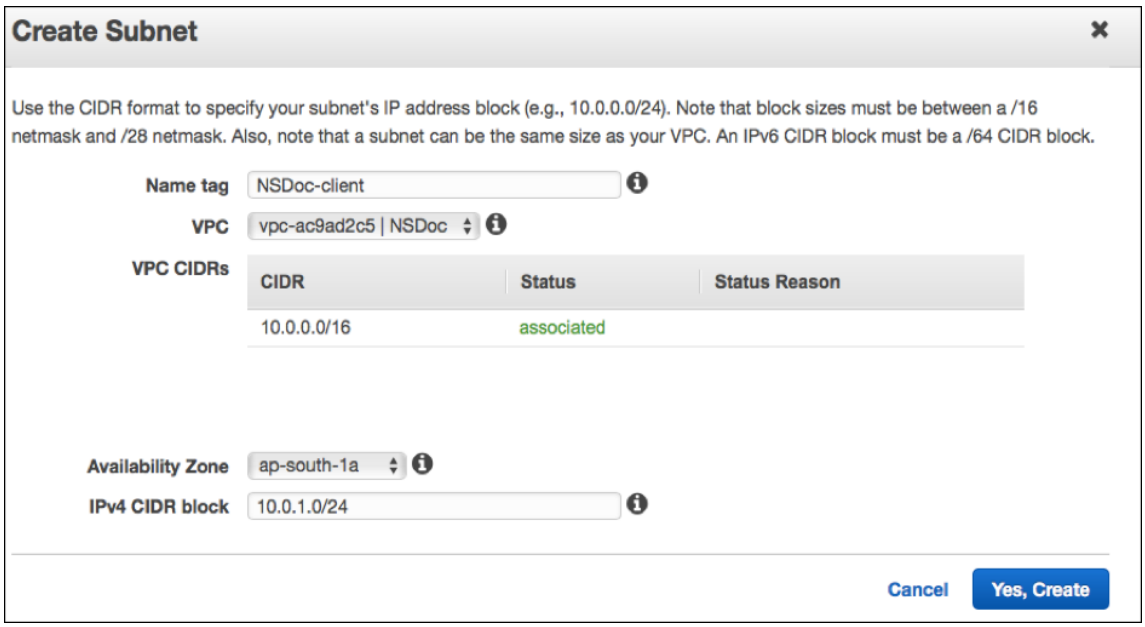
Étape 1 : Créer un VPC.

1. Connectez-vous à la console Web AWS et accédez à **Mise en réseau et diffusion de contenu** > **VPC** . Cliquez sur **Démarrer l'Assistant VPC**.
2. Sélectionnez **VPC avec un seul sous-réseau public**, puis cliquez sur **Sélectionner**.
3. Définissez le bloc CIDR IP sur 10.0.0.0/16, pour ce scénario.
4. Donnez un nom pour le VPC.
5. Définissez le sous-réseau public sur 10.0.0.0/24. (Ceci est le réseau de gestion).
6. Sélectionnez une zone de disponibilité.
7. Donnez un nom au sous-réseau.
8. Cliquez sur Créer un **VPC**.

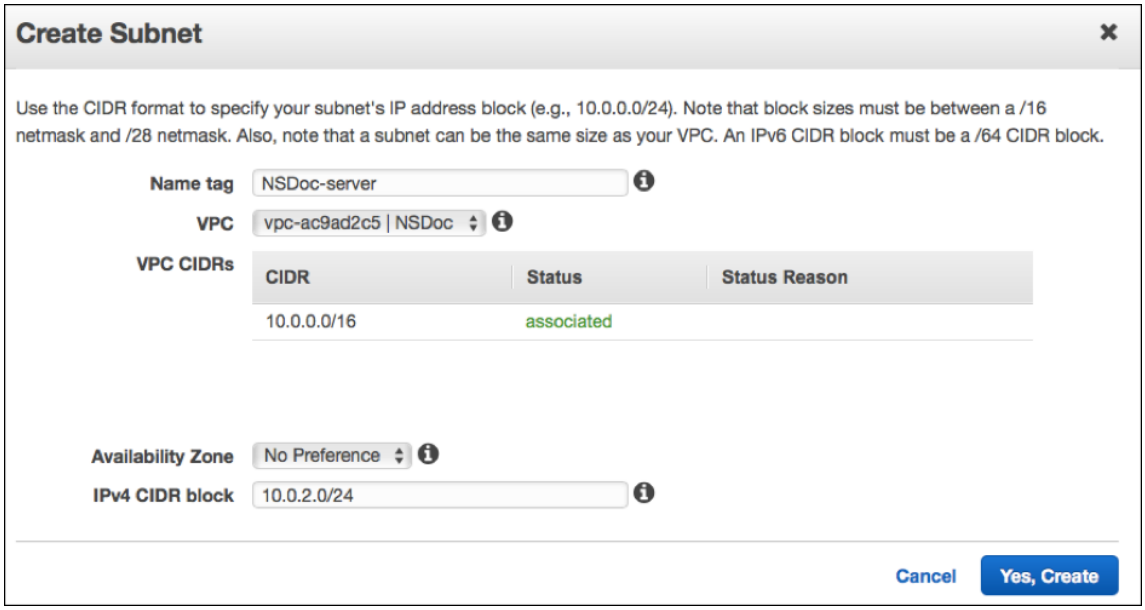


Étape 2 : Créer des sous-réseaux supplémentaires.

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Sous-réseaux, Créer un sous-réseau après avoir saisi les détails suivants.
   - Nom tag : indiquez un nom pour votre sous-réseau.
   - VPC : choisissez le VPC pour lequel vous créez le sous-réseau.
   - Zone de disponibilité : Choisissez la zone de disponibilité dans laquelle vous avez créé le VPC à l'étape 1.
   - Bloc CIDR IPv4 : spécifiez un bloc CIDR IPv4 pour votre sous-réseau. Pour ce scénario, choisissez 10.0.1.0/24.

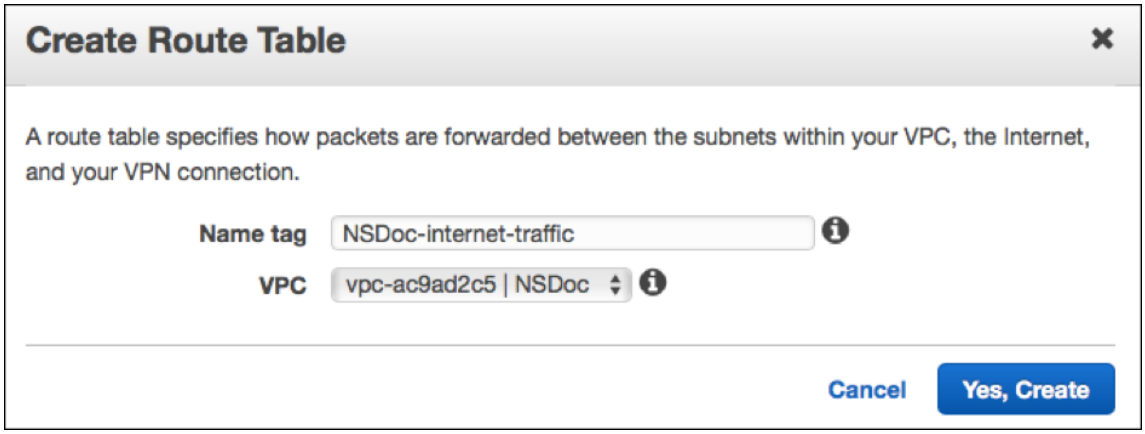


3. Répétez les étapes pour créer un sous-réseau supplémentaire pour les serveurs back-end.



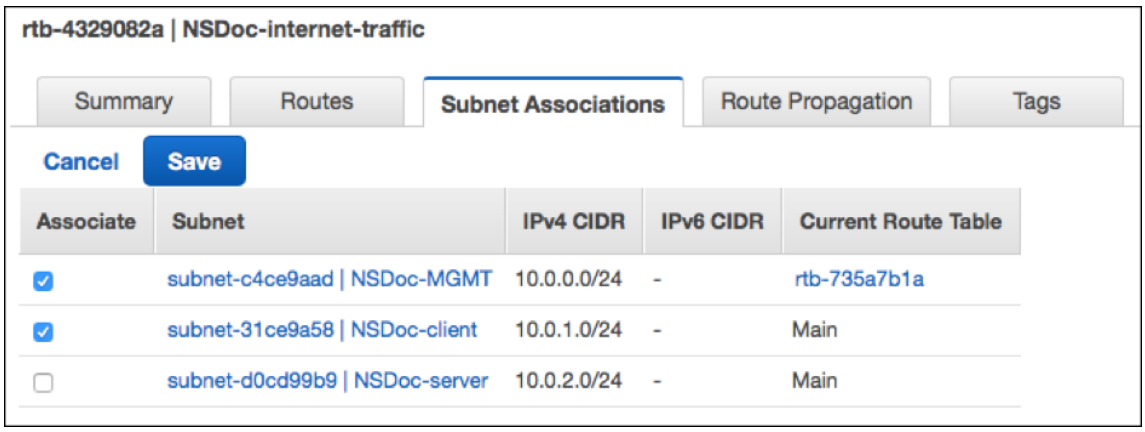
Étape 3 : Créer une table de routage.

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez **Tables de routage** > **Créer une table de routage.**
3. Dans la fenêtre Créer une table de routage, ajoutez un nom et sélectionnez le VPC que vous avez créé à l'étape 1.
4. Cliquez sur **Yes, Create**.



   La table de routage est affectée à tous les sous-réseaux que vous avez créés pour ce VPC, de sorte que le routage du trafic à partir d'une instance d'un sous-réseau peut atteindre une instance d'un autre sous-réseau.

5. Cliquez sur Associations de sous-réseau, puis sur Modifier.
6. Cliquez sur le sous-réseau de gestion et client, puis cliquez sur Enregistrer. Cela crée une table de routage pour le trafic Internet uniquement.



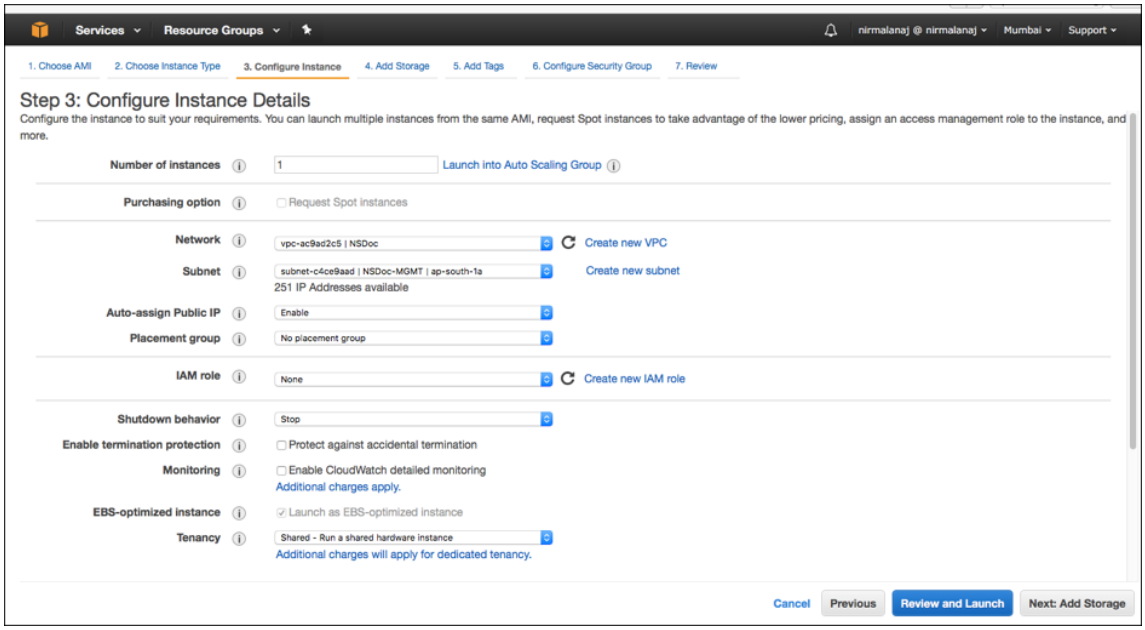
7. Cliquez sur **Itinéraires > Modifier > Ajouter un autre itinéraire**.
8. Dans le champ Destination, ajoutez 0.0.0.0/0 et cliquez sur le champ Cible pour sélectionner igw- <xxxx> la passerelle Internet créée automatiquement par l'Assistant VPC.
9. Cliquez sur Enregistrer.

10. Suivez les étapes pour créer une table de routage pour le trafic côté serveur.

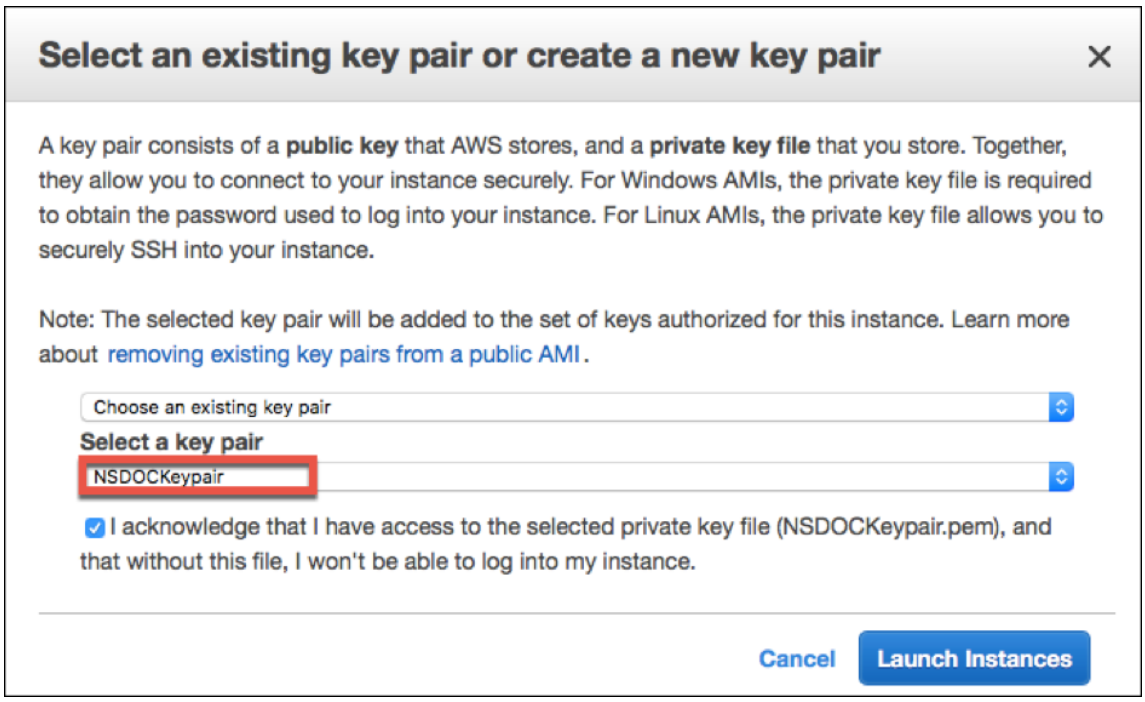
Étape 4 : Créer une instance Citrix ADC VPX.

1. Ouvrez une session sur AWS Management Console et cliquez sur **EC2** sous **Calcul** .
2. Cliquez sur AWS Marketplace. Dans la barre de recherche AWS Marketplace, tapez Citrix ADC VPX et appuyez sur Entrée. Les éditions Citrix ADC VPX disponibles sont affichées.
3. Cliquez sur **Sélectionner** pour choisir l'édition Citrix ADC VPX souhaitée. L'assistant d'instance EC2 démarre.
4. Dans la page **Choisir un type d'instance**, sélectionnez **m4. Xlarge** (recommandé) et cliquez sur **Suivant : Configurer les détails de l'instance**.
5. Dans la page Configurer les détails de l'instance, sélectionnez les éléments suivants, puis cliquez sur Suivant : Ajouter un stockage.

- Nombre d'instances : 1
- Réseau : VPC créé à l'étape 1
- Sous-réseau : sous-réseau de gestion
- Affectation automatique de l'adresse IP publique : Activer



6. Dans la page Ajouter un stockage, sélectionnez l'option par défaut, puis cliquez sur Suivant : Ajouter des balises.
7. Dans la page Ajouter des balises, ajoutez un nom pour l'instance, puis cliquez sur Suivant : Configurer le groupe de sécurité.
8. Dans la page Configurer le groupe de sécurité, sélectionnez l'option par défaut (générée par AWS Marketplace et basée sur les paramètres recommandés par Citrix Systems), puis cliquez sur **Réviser et lancer > Lancer**.
9. Vous êtes invité à sélectionner une paire de clés existante ou à créer et une nouvelle paire de clés. Dans la liste déroulante Sélectionner une paire de clés, sélectionnez la paire de clés que vous avez créée comme condition préalable (voir la section Prérequis).
10. Cochez la case pour accuser réception de la paire de clés et cliquez sur Lancer les instances.



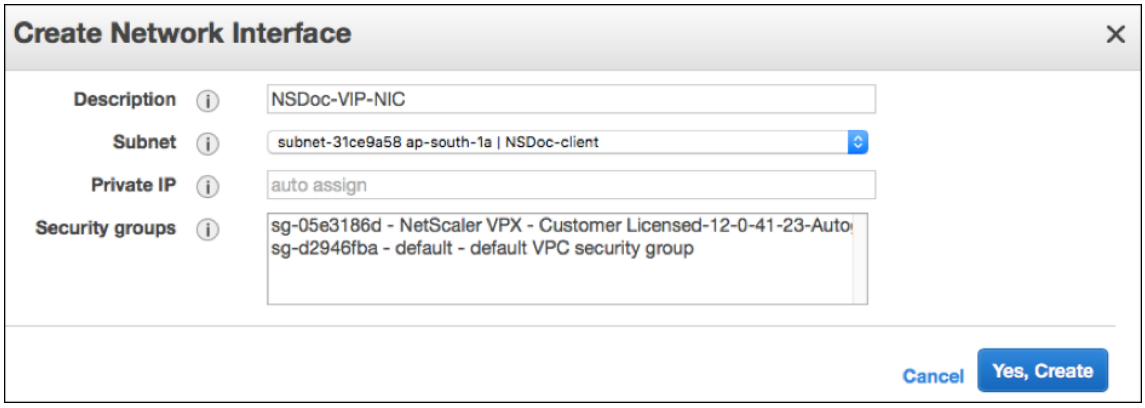
L'assistant de lancement d'instance affiche l'état de lancement et l'instance apparaît dans la liste des instances lorsqu'elle est entièrement lancée.

L'instance de vérification, accédez à la console AWS, cliquez sur EC2 > Instances en cours d'exécution. Sélectionnez l'instance et ajoutez un nom. Assurez-vous que l'état de l'instance est en cours d'exécution et que les vérifications d'état sont terminées.

Étape 5 : Créer et attacher plus d'interfaces réseau.

Lorsque vous avez créé le VPC, une seule interface réseau lui est associée. Maintenant, ajoutez deux interfaces réseau supplémentaires au VPC, pour le VIP et SNIP.

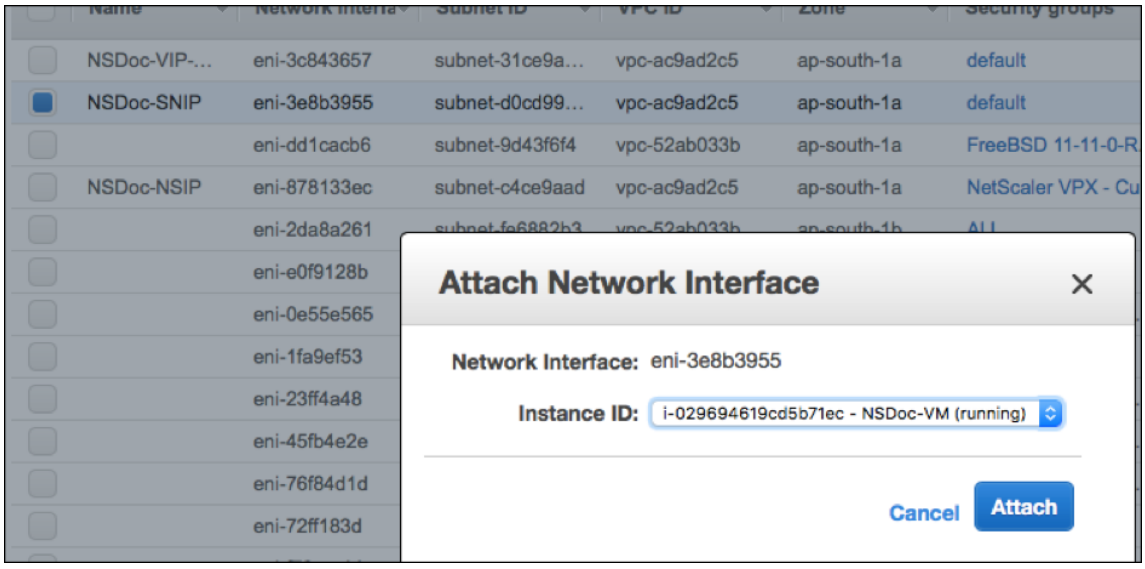
1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Interfaces réseau.
3. Choisissez Créer une interface réseau.
4. Pour Description, entrez un nom descriptif.
5. Pour Sous-réseau, sélectionnez le sous-réseau que vous avez créé précédemment pour le VIP.
6. Pour Private IP, laissez l'option par défaut.
7. Pour Groupes de sécurité, sélectionnez le groupe.
8. Cliquez sur **Yes, Create**.



9. Une fois l'interface réseau créée, ajoutez un nom à l'interface.
10. Répétez les étapes pour créer une interface réseau pour le trafic côté serveur.

Attachez les interfaces réseau :

1. Dans le volet de navigation, choisissez Interfaces réseau.
2. Sélectionnez l'interface réseau et choisissez Attach.
3. Dans la boîte de dialogue Attach Network Interface (Attach Network Interface), sélectionnez l'instance et choisissez Attach (Attach Network Interface).



Étape 6 : Fixez une adresse IP élastique au NSIP.

1. Depuis la console de gestion AWS, accédez à **NETWORK & SECURITY > IP Elastic**.
2. Vérifiez la disponibilité EIP gratuit à joindre. Si aucun, cliquez sur **Allouer une nouvelle adresse**.
3. Sélectionnez l'adresse IP nouvellement allouée et choisissez **Actions > Associer l'adresse**.
4. Cliquez sur le bouton radio **Interface réseau** .

5. Dans la liste déroulante Interface réseau, sélectionnez la carte réseau de gestion.
6. Dans le menu déroulant **IP privée**, sélectionnez l'adresse IP générée par AWS.
7. Activez la case à cocher **Réassociation** .
8. Cliquez sur **Associer**.

Accéder à l'instance VPX :

Après avoir configuré une instance Citrix ADC VPX autonome avec trois cartes réseau, ouvrez une session sur l'instance VPX pour terminer la configuration côté ADC Citrix. Utilisation des options suivantes :

- GUI : saisissez l'adresse IP publique de la carte réseau de gestion dans le navigateur. Ouvrez une session en utilisant `nsroot` comme nom d'utilisateur et l'ID d'instance (i-0c1ffe1d987817522) comme mot de passe.

> Remarque
>
> Lors de votre première ouverture de session, vous êtes invité à modifier le mot de passe pour des raisons de sécurité. Après avoir modifié le mot de passe, vous devez enregistrer la configuration. Si la configuration n'est pas enregistrée et que l'instance redémarre, vous devez ouvrir une session avec le mot de passe par défaut. Modifiez à nouveau le mot de passe à l'invite et enregistrez la configuration.

- SSH : Ouvrez un client SSH et tapez :

```
ssh -i \<location of your private key\> ns root@\<public DNS of the instance
\>
```

Pour rechercher le DNS public, cliquez sur l'instance, puis cliquez sur **Connecter**.

Informations connexes :

- Pour configurer les adresses IP appartenant à Citrix ADC (NSIP, VIP et SNIP), reportez-vous à la section Configuration des adresses IP appartenant à Citrix ADC.

- Vous avez configuré une version BYOL de l'appliance Citrix ADC VPX. Pour plus d'informations, consultez le Guide de licences VPX à l'adresse http://support.citrix.com/article/CTX122426

Télécharger une licence Citrix ADC VPX

August 20, 2021

Après le lancement de l'instance sous licence Citrix ADC VPX-Customer à partir du marché AWS, une licence est requise. Pour plus d'informations sur les licences VPX, reportez-vous à la section Présentation des licences.

Vous devez :

1. Utilisez le portail de licences du site Web Citrix pour générer une licence valide.
2. Télécharger la licence sur l'instance.

S'il s'agit d'une instance de marketplace **payante**, vous n'avez pas besoin d'installer une licence. Le jeu de fonctionnalités et les performances corrects s'activent automatiquement.

Si vous utilisez une instance Citrix ADC VPX avec un numéro de modèle supérieur à VPX 5000, le débit réseau peut ne pas être le même que celui spécifié par la licence de l'instance. Toutefois, d'autres fonctionnalités, telles que le débit SSL et les transactions SSL par seconde, peuvent s'améliorer.

La bande passante réseau de 5 Gbit/s est observée dans le type d' `c4.8xlarge` instance.

Comment migrer l'abonnement AWS vers BYOL

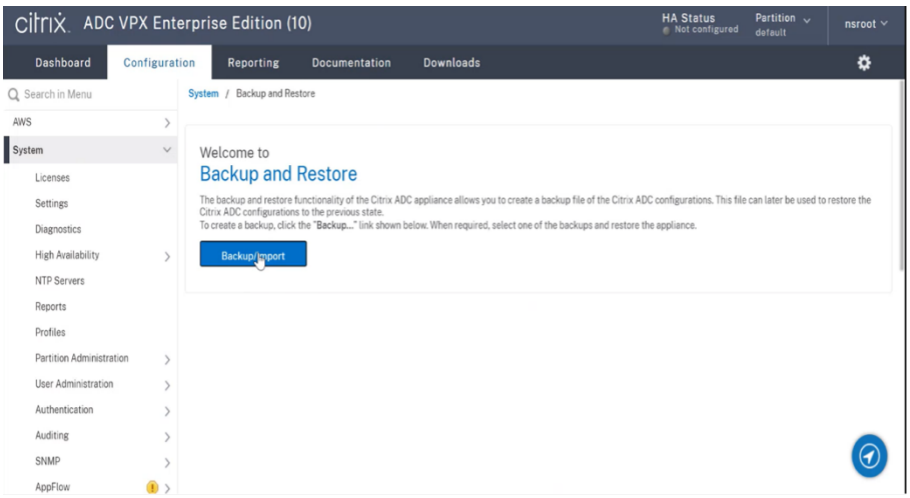
Cette section décrit la procédure de migration de l'abonnement AWS vers Bring your own license (BYOL), et inversement.

Procédez comme suit pour migrer un abonnement AWS vers BYOL :

> Remarque
>
> Les **étapes 2** et **3** sont effectuées sur l'instance Citrix ADC VPX, et toutes les autres étapes sont effectuées sur le portail AWS.

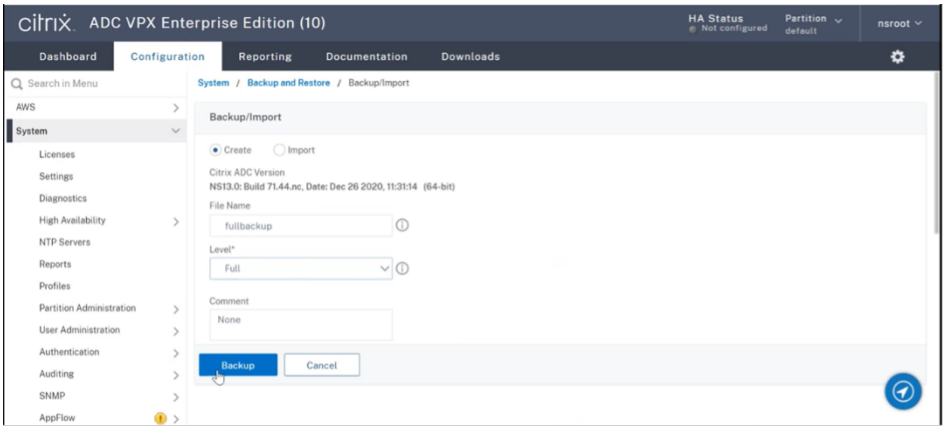
1. Créez une instance BYOL EC2 à l'aide de Citrix ADC VPX - Licence client dans la même zone de disponibilité que l'ancienne instance EC2 qui possède le même groupe de sécurité, le même rôle IAM et le même sous-réseau. La nouvelle instance EC2 ne doit avoir qu'une seule interface ENI.
2. Pour sauvegarder les données de l'ancienne instance EC2 à l'aide de l'interface graphique Citrix ADC, procédez comme suit.
    a) Accédez à **Système > Sauvegarde et restauration**.

b) Dans la page **Bienvenue**, cliquez sur **Sauvegarde/Importation** pour démarrer le processus.

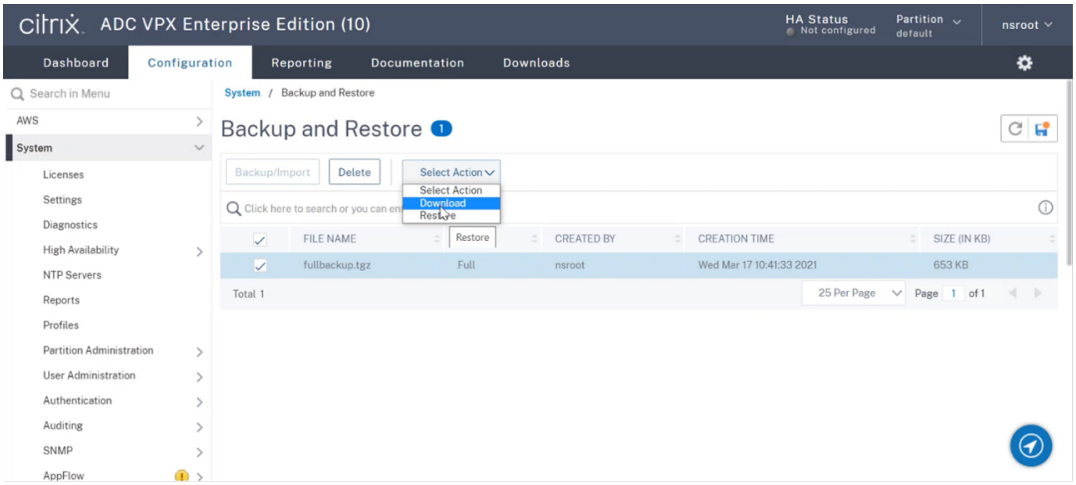


c) Dans la page **Sauvegarde/Importation**, renseignez les informations suivantes :

- **Nom** : nom du fichier de sauvegarde.
- **Niveau** : sélectionnez le niveau de sauvegarde **complet**.
- **Commentaire** : fournissez une brève description de la sauvegarde.



d) Cliquez sur **Sauvegarde**. Une fois la sauvegarde terminée, vous pouvez sélectionner le fichier et le télécharger sur votre machine locale.

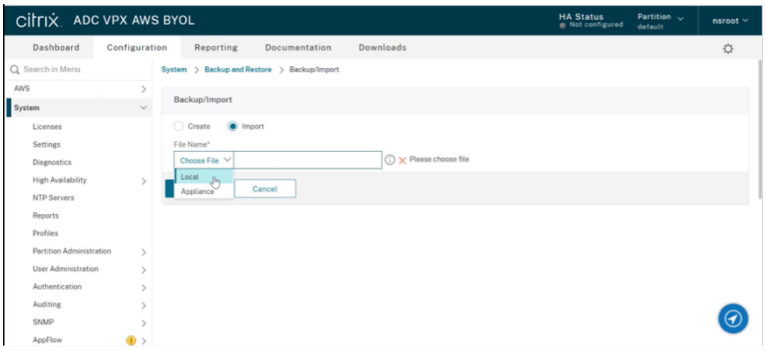


3. Pour restaurer les données de la nouvelle instance EC2 à l'aide de l'interface graphique Citrix ADC, procédez comme suit :

   a) Accédez à **Système > Sauvegarde et restauration**.

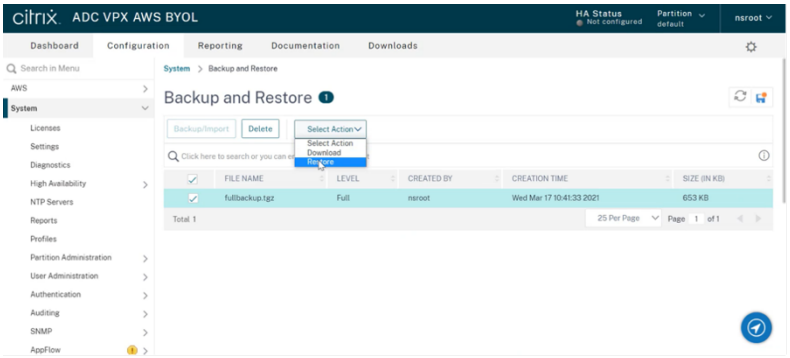
   b) Cliquez sur **Sauvegarde/Importer** pour démarrer le processus.

   c) Sélectionnez l'option **Importer** et téléchargez le fichier de sauvegarde.

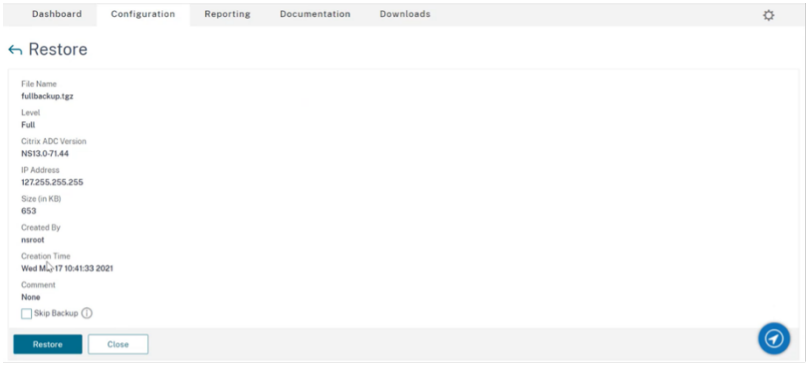


   d) Sélectionnez le fichier.

   e) **Dans le menu déroulant Sélectionner une action**, sélectionnez **Restaurer**.



   f) Sur la page **Restaurer**, vérifiez les détails du fichier, puis cliquez sur **Restaurer**.



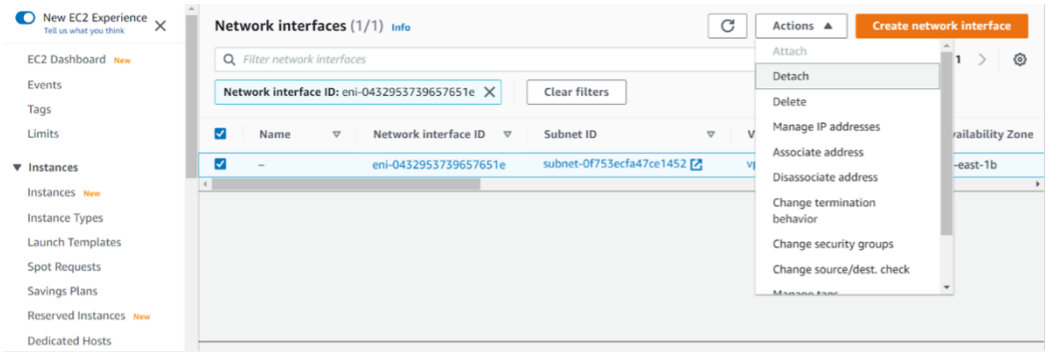
g) Après la restauration, redémarrez l'instance EC2.

4. Déplacez toutes les interfaces (à l'exception de l'interface de gestion à laquelle l'adresse NSIP est liée) de l'ancienne instance EC2 vers la nouvelle instance EC2. Pour déplacer une interface réseau d'une instance EC2 à une autre, procédez comme suit :

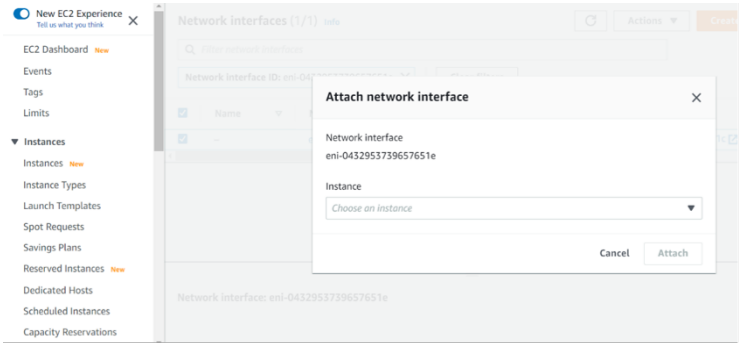
   a) Dans le **portail AWS**, arrêtez les anciennes et nouvelles instances EC2.

   b) Accédez à **Interfaces réseau**et sélectionnez l'interface réseau attachée à l'ancienne instance EC2.

   c) Détachez l'instance EC2 en cliquant sur **Actions > Détacher**.



   d) Connectez l'interface réseau à la nouvelle instance EC2 en cliquant sur **Actions > Attacher**. Entrez le nom de l'instance EC2 auquel l'interface réseau doit être connectée.



   e) Faites les **étapes 1** à **4** pour toutes les autres interfaces connectées. Assurez-vous de suivre la séquence et de conserver l'ordre de l'interface. C'est-à-dire, détachez d'abord l'interface

2 et attachez-la, puis détachez l'interface 3 et attachez-la, etc.

5. Vous ne pouvez pas détacher l'interface de gestion d'une ancienne instance EC2. Déplacez donc toutes les adresses IP secondaires (le cas échéant) de l'interface de gestion (interface réseau principale) de l'ancienne instance EC2 vers la nouvelle instance EC2. Pour déplacer une adresse IP d'une interface à une autre, procédez comme suit :

   a) Dans le **portail AWS**, assurez-vous que les anciennes et nouvelles instances EC2 sont à l'état **Stop** .

   b) Accédez à **Interfaces réseau**et sélectionnez l'interface réseau de gestion attachée à l'ancienne instance EC2.

   c) Cliquez sur **Actions > Gérer l'adresse IP**et notez toutes les adresses IP secondaires attribuées (le cas échéant).

   d) Accédez à l'interface réseau de gestion ou à l'interface principale de la nouvelle instance EC2.

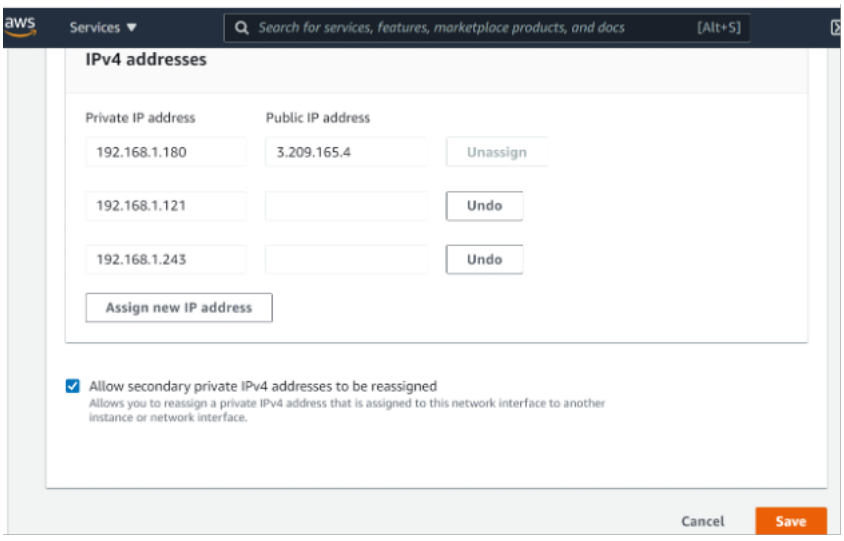
   e) Cliquez sur **Actions > Gérer les adresses IP**.

   f) Sous **Adresses IPv4**, cliquez sur **Attribuer une nouvelle adresse IP**.

   g) Saisissez les adresses IP indiquées à l' **étape 3**.

   h) Activez la case à cocher **Autoriser la réaffectation des adresses IP privées secondaires** .

   i) Cliquez sur **Enregistrer**.



6. Démarrez la nouvelle instance EC2 et vérifiez la configuration. Une fois que toute la configuration est déplacée, vous pouvez supprimer ou conserver l'ancienne instance EC2 selon vos besoins.

7. Si une adresse EIP est attachée à l'adresse NSIP de l'ancienne instance EC2, déplacez l'adresse NSIP de l'ancienne instance vers la nouvelle adresse NSIP de l'instance.
8. Si vous souhaitez revenir à l'ancienne instance, suivez les mêmes étapes de la manière opposée entre l'ancienne et la nouvelle instance.
9. Une fois que vous passez d'une instance d'abonnement à une instance BYOL, une licence est requise. Pour installer une licence, procédez comme suit :
    - Utilisez le portail de licences sur le site Web Citrix pour générer une licence valide.
    - Télécharger la licence sur l'instance. Pour plus d'informations, voir VPX ADC - Installer une nouvelle licence.

> Remarque
>
> Lorsque vous déplacez une instance BYOL vers une instance d'abonnement (instance de marché payante), vous n'avez pas besoin d'installer la licence. Le jeu de fonctionnalités et les performances corrects sont automatiquement activés.

Limitations

L'interface de gestion ne peut pas être déplacée vers la nouvelle instance EC2. Citrix vous recommande donc de configurer manuellement l'interface de gestion. Pour plus d'informations, reportez-vous à l' **étape 5** de la procédure précédente. Une nouvelle instance EC2 est créée avec le réplica exact de l'ancienne instance EC2, mais seule l'adresse NSIP possède une nouvelle adresse IP.

Serveurs d'équilibrage de charge dans différentes zones de disponibilité

August 20, 2021

Une instance VPX peut être utilisée pour équilibrer la charge des serveurs s'exécutant dans la même zone de disponibilité, ou dans :

- Une zone de disponibilité différente (AZ) dans le même VPC AWS
- Une autre région AWS
- AWS EC2 dans un VPC

Pour permettre à une instance VPX d'équilibrer la charge des serveurs s'exécutant en dehors du VPC AWS dans lequel se trouve l'instance
VPX, configurez l'instance pour qu'elle utilise les EIP pour acheminer le trafic via la Gateway Internet, comme suit :

1. Configurez un SNIP sur l'instance Citrix ADC VPX à l'aide de l'interface de ligne de commande Citrix ADC ou de l'interface graphique.

2. Activez l'acheminement du trafic hors de l'AZ en créant un sous-réseau public pour le trafic côté serveur.
3. Ajoutez une route de Gateway Internet à la table de routage, à l'aide de la console AWS GUI.
4. Associez la table de routage que vous avez mise à jour au sous-réseau côté serveur.
5. Associez un EIP à l'adresse IP privée côté serveur qui est mappée à une adresse SNIP Citrix ADC.

Fonctionnement de la haute disponibilité sur AWS

August 20, 2021

Vous pouvez configurer deux instances Citrix ADC VPX sur AWS en tant que paire actif-passif haute disponibilité (HA). Lorsque vous configurez une instance en tant que nœud principal et l'autre en tant que nœud secondaire, le nœud principal accepte les connexions et gère les serveurs. Le nœud secondaire surveille le principal. Si, pour une raison quelconque, le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

Dans AWS, les types de déploiement suivants sont pris en charge pour les instances VPX :

- Haute disponibilité dans la même zone
- Haute disponibilité dans différentes zones

> **Remarque**
>
> Pour que la haute disponibilité fonctionne, assurez-vous que les instances Citrix ADC VPX sont associées à des rôles IAM et attribuées avec l'adresse EIP (Elastic IP) au NSIP. Vous n'avez pas besoin d'affecter un EIP sur NSIP si le NSIP peut atteindre Internet via l'instance NAT.

Haute disponibilité dans les mêmes zones

Dans un déploiement haute disponibilité dans les mêmes zones, les deux instances VPX doivent avoir des configurations réseau similaires.

Suivez ces deux règles :

Article 1. Toute carte réseau sur une instance VPX doit se trouver dans le même sous-réseau que la carte réseau correspondante dans l'autre VPX. Les deux instances doivent avoir :

- Interface de gestion sur le même sous-réseau (appelé sous-réseau de gestion)
- Interface client sur le même sous-réseau (appelé sous-réseau client)
- Interface serveur sur le même sous-réseau (appelé sous-réseau serveur)

Article 2. La séquence de carte réseau de gestion, de carte réseau client et de carte réseau serveur sur les deux instances doit être la même.
Par exemple, le scénario suivant n'est pas pris en charge.

Instance VPX 1

NIC 0 :
carte réseau de gestion 1 :
carte réseau client 2 : serveur

Instance VPX 2

NIC 0 : gestion

Carte réseau 1 : serveur

Carte réseau 2 : client

Dans ce scénario, la carte réseau 1 de l'instance 1 est dans le sous-réseau client tandis que la carte réseau 1 de l'instance 2 est dans le sous-réseau du serveur. Pour que HA fonctionne, la carte réseau 1 des deux instances doit être soit dans le sous-réseau client, soit dans le sous-réseau du serveur.

À partir de 13.0 41.xx, la haute disponibilité peut être obtenue en migrant des adresses IP privées secondaires attachées aux cartes réseau (cartes réseau client et côté serveur) du nœud HA principal vers le nœud HA secondaire après le basculement. Dans ce déploiement :

- Les deux instances VPX ont le même nombre de cartes réseau et de mappage de sous-réseau selon l'énumération de carte réseau.
- Chaque carte réseau VPX possède une adresse IP privée supplémentaire, à l'exception de la première carte réseau, qui correspond à l'adresse IP de gestion. L'adresse IP privée supplémentaire apparaît comme l'adresse IP privée principale dans la console Web AWS. Dans notre document, nous désignons cette adresse IP supplémentaire comme adresse IP fictive).
- Les adresses IP factices ne doivent pas être configurées sur l'instance de Citrix ADC en tant que VIP et SNIP.
- D'autres adresses IP privées secondaires doivent être créées, selon les besoins, et configurées en tant que VIP et SNIP.
- Lors du basculement, le nouveau nœud principal recherche les SNIP et les VIP configurés et les déplace des cartes réseau attachées à la précédente principale vers les cartes réseau correspondantes sur la nouvelle interface principale.
- Les instances de Citrix ADC nécessitent des autorisations IAM pour que HA fonctionne. Ajoutez les privilèges IAM suivants à la stratégie IAM ajoutée à chaque instance.

```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeNetworkInterfaces"
"ec2:AssignPrivateIpAddresses"
```


> Remarque : n'`unassignPrivateIpAddress` est pas obligatoire.

Cette méthode est plus rapide que la méthode héritée. Dans l'ancienne méthode, HA dépend de la migration des interfaces réseau élastiques AWS du nœud principal vers le nœud secondaire.

Pour une méthode héritée, les stratégies suivantes sont requises :

```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeAddresses"
"ec2:AssociateAddress"
"ec2:DisassociateAddress"
```

Pour plus d'informations, voir Déployer une paire haute disponibilité sur AWS.

Haute disponibilité dans différentes zones

Vous pouvez configurer deux instances Citrix ADC VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes, en tant que paire actif-passif haute disponibilité en mode INC (Independent Network Configuration). Lors du basculement, l'EIP (Elastic IP) du VIP de l'instance principale migre vers le secondaire, qui prend le relais en tant que nouveau principal. Dans le processus de basculement, l'API AWS :

- Vérifie les serveurs virtuels qui y sont `IPSets` connectés.
- Recherche l'adresse IP qui a une adresse IP publique associée, à partir des deux adresses IP sur lesquelles le serveur virtuel écoute. Une qui est directement connectée au serveur virtuel et une qui est connectée via le jeu d'adresses IP.
- Réassocie l'IP publique (EIP) à l'IP privée appartenant au nouveau VIP principal.

Pour les HA dans différentes zones, les stratégies suivantes sont requises :

```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeAddresses"
"ec2:AssociateAddress"
"ec2:DisassociateAddress"
```

Pour plus d'informations, consultez la section Haute disponibilité dans les zones de disponibilité AWS.

Avant de commencer votre déploiement

Avant de commencer un déploiement HA sur AWS, lisez le document suivant :

- Conditions préalables
- Limitations et directives d'utilisation

- Deploy a Citrix ADC VPX instance on AWS
- Haute disponibilité

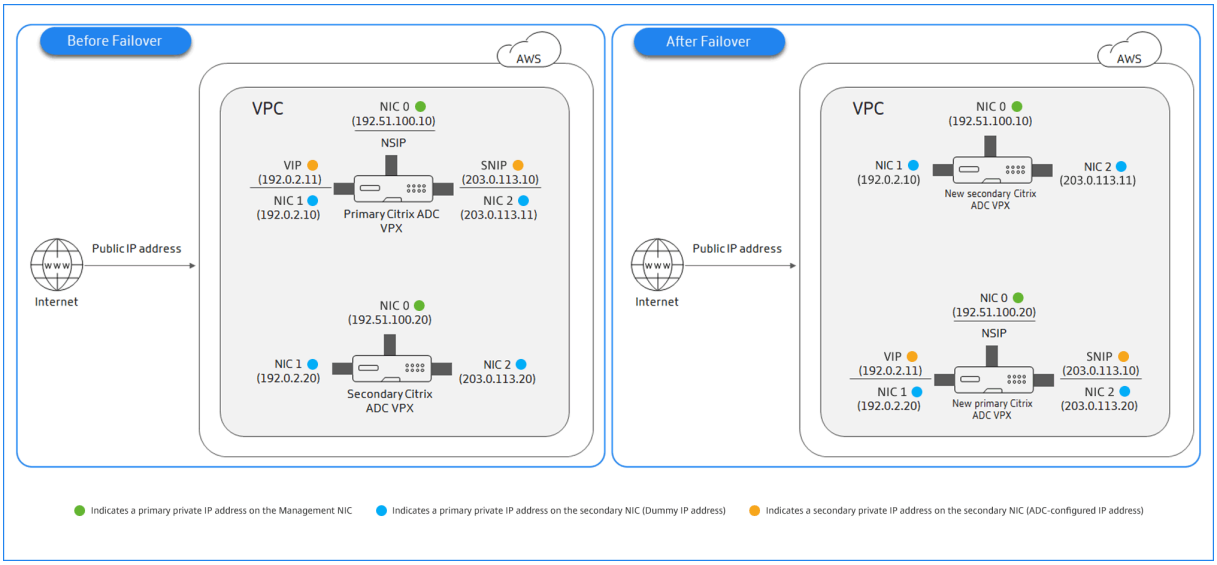
Déployer une paire haute disponibilité sur AWS

August 20, 2021

Vous pouvez configurer deux instances Citrix ADC VPX sur AWS en tant que paire haute disponibilité (HA), dans la même zone AWS où les deux instances VPX se trouvent sur le même sous-réseau. La HA est obtenue en migrant les adresses IP privées secondaires attachées aux cartes réseau (cartes réseau côté client et serveur) du nœud HA principal vers le nœud HA secondaire après le basculement. Toutes les adresses IP Elastic associées aux adresses IP privées secondaires sont également migrées.

L'illustration suivante un scénario de basculement HA à l'aide de la migration d'adresses IP privées secondaires.

Figure 1. Une paire Citrix ADC VPX HA sur AWS, utilisant la migration IP privée



Avant de démarrer votre document, lisez les documents suivants :

- Conditions préalables
- Limitations et directives d'utilisation
- Deploy a Citrix ADC VPX instance on AWS
- Haute disponibilité

Comment déployer une paire HA VPX dans la même zone

Voici le résumé des étapes pour déployer une paire HA VPX dans la même zone :

1. Créez deux instances VPX sur AWS, chacune avec trois cartes réseau
2. Attribuer une adresse IP privée secondaire AWS à VIP et SNIP du nœud principal
3. Configurer VIP et SNIP sur le nœud principal à l'aide d'adresses IP privées secondaires AWS
4. Configurer HA sur les deux nœuds

Étape 1. Créez deux instances VPX (nœuds primaires et secondaires) à l'aide du même VPC, chacune avec trois cartes réseau (Ethernet 0, Ethernet 1, Ethernet 2)

Suivez les étapes décrites dans la section Déployer une instance Citrix ADC VPX sur AWS à l'aide de la console Web AWS.

Étape 2. Sur le nœud principal, attribuez des adresses IP privées secondaires pour Ethernet 1 (IP client ou VIP) et Ethernet 2 (IP du serveur principal ou SNIP)

La console AWS affecte automatiquement les adresses IP privées principales aux cartes réseau configurées. Attribuez plus d'adresses IP privées à VIP et SNIP, connues sous le nom d'adresses IP privées secondaires.

Pour affecter une adresse IPv4 privée secondaire à une interface réseau, procédez comme suit :

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Interfaces réseau, puis sélectionnez l'interface réseau attachée à l'instance.
3. Choisissez Actions, Gérer les adresses IP.
4. Sous Adresses IPv4, choisissez Attribuer une nouvelle adresse IP.
5. Entrez une adresse IPv4 spécifique qui se trouve dans la plage de sous-réseau de l'instance, ou laissez le champ vide pour laisser Amazon sélectionner une adresse IP pour vous.
6. (Facultatif) Choisissez Autoriser la réaffectation pour autoriser la réaffectation de l'adresse IP privée secondaire si elle est déjà affectée à une autre interface réseau.
7. Choisissez Oui, Mettre à jour.

Sous la description de l'instance, les adresses IP privées secondaires attribuées apparaissent.

Étape 3. Configurer VIP et SNIP sur le nœud principal, à l'aide d'adresses IP privées secondaires

Accédez au nœud principal à l'aide de SSH. Ouvrez un client ssh et tapez :

```
ssh -i <location of your private key> nsroot@<public DNS of the
   instance>
<!--NeedCopy-->
```

Ensuite, configurez VIP et SNIP.

Pour VIP, tapez :


```
add ns ip <IPAddress> <netmask> -type <type>
<!--NeedCopy-->
```

Pour SNIP, tapez :

```
add ns ip <IPAddress> <netmask> -type SNIP
<!--NeedCopy-->
```

Tapez`save config` pour enregistrer.

Pour afficher les adresses IP configurées, tapez la commande suivante :

```
show ns ip
<!--NeedCopy-->
```

Pour plus d'informations, consultez les rubriques suivantes :

- Configuration et gestion des adresses IP virtuelles (VIP)
- Configuration de l'adresse NSIP

Étape 4 : Configurer HA sur les deux instances

Sur le nœud principal, ouvrez un client Shell et tapez la commande suivante :

```
add ha node <id> <private IP address of the management NIC of the
   secondary node>
<!--NeedCopy-->
```

Sur le nœud secondaire, tapez la commande suivante :

```
add ha node <id> < private IP address of the management NIC of the
   primary node >
<!--NeedCopy-->
```

Tapez`save config` pour enregistrer la configuration.

Pour afficher les nœuds HA configurés, tapez`show ha node`.

Lors du basculement, les adresses IP privées secondaires configurées en tant que VIP et SNIP sur le nœud principal précédent sont migrées vers le nouveau nœud principal.

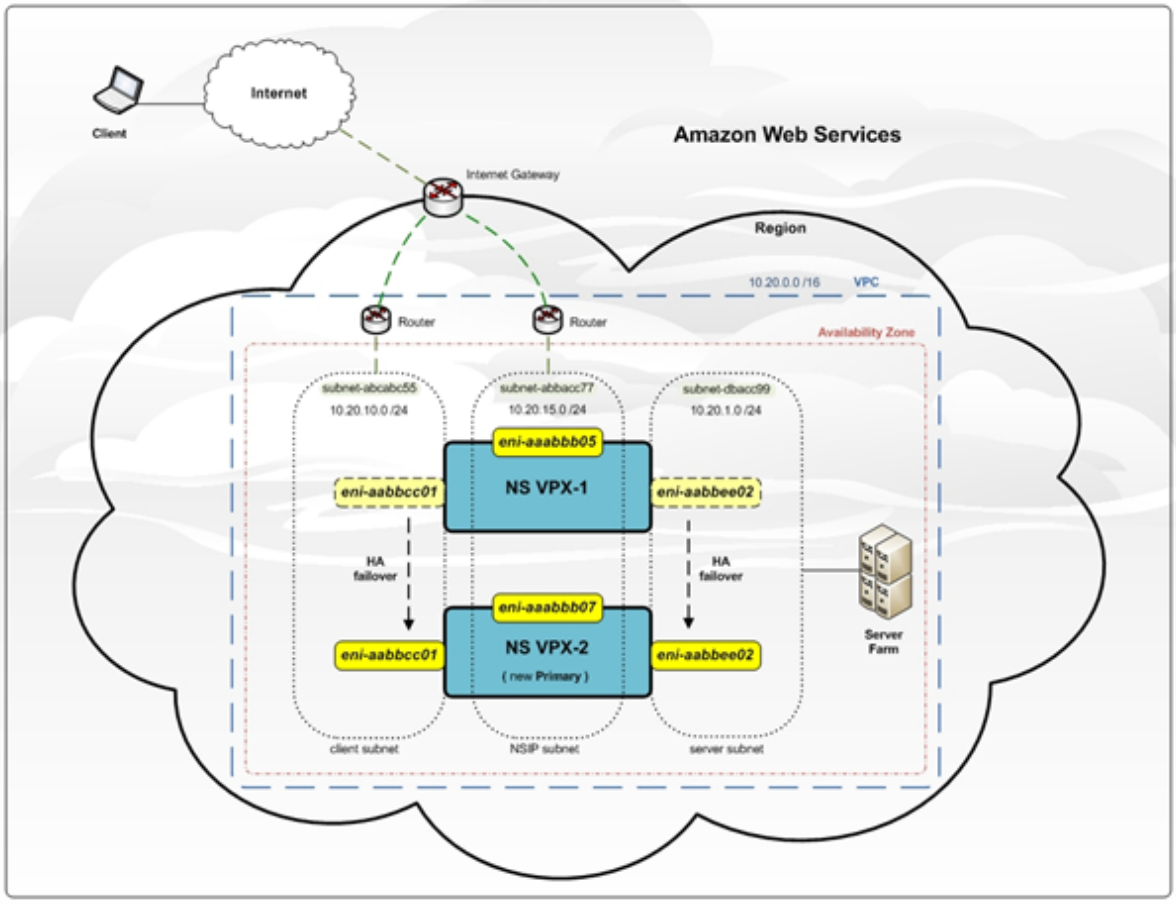
Pour forcer un basculement sur un nœud, tapez`force HA`basculement.

Méthode héritée pour le déploiement d'une paire HA VPX

Avant la publication 13.0 41.x, HA dans la même zone a été réalisée via la migration AWS Elastic Network Interface (ENI). Cependant, cette méthode est lentement obsolète.

La figure suivante illustre un exemple d'architecture de déploiement HA pour les instances Citrix ADC VPX sur AWS.

Figure 1. Une paire Citrix ADC VPX HA sur AWS, à l'aide de la migration ENI



Vous pouvez déployer deux instances VPX sur AWS en tant que paire HA à l'aide de l'une des options suivantes :

- Créez manuellement les instances avec le rôle IAM à l'aide d'AWS Management Console, puis configurez HA dessus.
- Ou automatisez le déploiement de haute disponibilité à l'aide du modèle Citrix CloudFormation.

Le modèle CloudFormation réduit considérablement le nombre d'étapes impliquées pour créer une paire HA et crée automatiquement un rôle IAM. Cette section explique comment déployer une paire Citrix ADC VPX HA (actif-passif) à l'aide du modèle Citrix CloudFormation.

Gardez à l'esprit les points suivants lors du déploiement de deux instances Citrix ADC VPX en tant que paire HA.

Points à noter

- HA sur AWS exige que le nœud principal dispose d'au moins deux ENI (l'un pour la gestion et l'autre pour le trafic de données) et que le nœud secondaire dispose d'un ENI de gestion. Toutefois, pour des raisons de sécurité, créez trois ENI sur le nœud principal, car cette configuration vous permet de séparer le réseau privé et public (recommandé).
- Le nœud secondaire a toujours une interface ENI (pour la gestion) et le nœud principal peut avoir jusqu'à quatre ENI.
- Les adresses NSIP pour chaque instance VPX dans une paire haute disponibilité doivent être configurées sur l'ENI par défaut de l'instance.
- Amazon n'autorise aucun paquet de diffusion/multidiffusion dans AWS. Par conséquent, dans une configuration HA, les ENI de plan de données sont migrés de l'instance principale vers l'instance VPX secondaire lorsque l'instance VPX principale échoue.
- Étant donné que l'ENI par défaut (gestion) ne peut pas être déplacé vers une autre instance VPX, n'utilisez pas l'ENI par défaut pour le trafic client et serveur (trafic de plan de données).
- Le message AWSCONFIG IOCTL NSAPI_HOTPLUG_INTF succès sortie 0 dans le /var/log/ns.log indique que les deux ENI de données ont été attachés avec succès à l'instance secondaire (la nouvelle instance principale).
- Le basculement sur incident peut prendre jusqu'à 20 secondes en raison du mécanisme ENI de détachement/d'attachement AWS.
- Lors du basculement, l'instance défaillante redémarre toujours.
- Les paquets de pulsations sont reçus uniquement sur l'interface de gestion.
- Le fichier de configuration des instances VPX principale et secondaire est synchronisé, y compris le`nsroot` mot de passe. Le`nsroot` mot de passe du nœud secondaire est défini sur celui du nœud principal après la synchronisation de la configuration HA.
- Pour avoir accès aux serveurs API AWS, soit l'instance VPX doit avoir une adresse IP publique attribuée, soit le routage doit être configuré correctement au niveau du sous-réseau VPC pointant vers la passerelle Internet du VPC.
- Les serveurs de noms et les serveurs DNS sont configurés au niveau du VPC à l'aide des options DHCP.
- Le modèle Citrix CloudFormation ne crée pas de configuration HA entre différentes zones de disponibilité.
- Le modèle Citrix CloudFormation ne crée pas de mode INC.
- Les messages de débogage AWS sont disponibles dans le fichier journal, /var/log/ns.log, sur l'instance VPX.

Déployer une paire haute disponibilité à l'aide du modèle Citrix CloudFormation

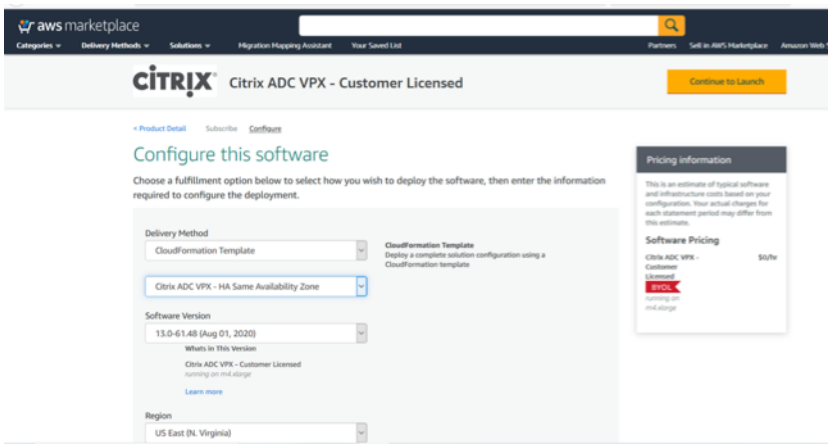
Avant de démarrer le modèle CloudFormation, assurez-vous de remplir les conditions suivantes :

- UN VPC
- Trois sous-réseaux dans le VPC
- Un groupe de sécurité avec les ports UDP 3003, TCP 3009—3010, HTTP, SSH ouverts
- Une paire de clés
- Créer une passerelle Internet
- Modifier les tables de routage pour les réseaux client et de gestion pour pointer vers la Gateway Internet

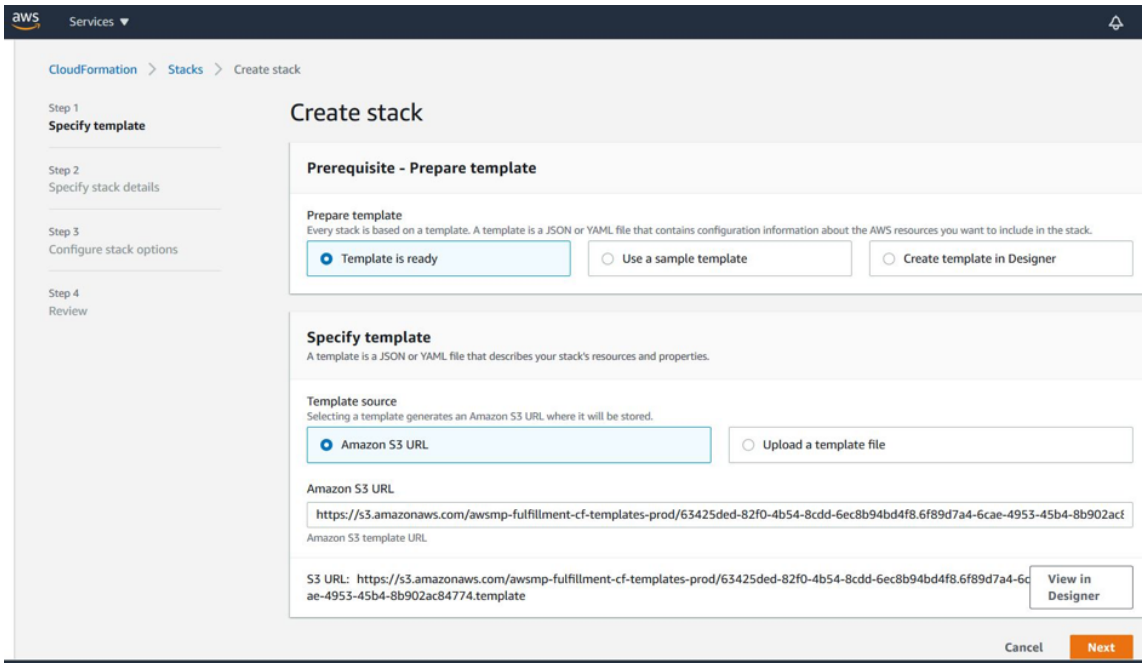
> **Remarque**
>
> Le modèle Citrix CloudFormation crée automatiquement un rôle IAM. Les rôles IAM existants n'apparaissent pas dans le modèle.

Pour lancer le modèle Citrix CloudFormation :

1. Connectez-vous à AWS Marketplace en utilisant vos informations d'identification AWS.
2. Dans le champ de recherche, saisissez **Citrix ADC VPX** pour rechercher l'AMI Citrix ADC, puis cliquez sur **OK**.
3. Sur la page de résultats de recherche, cliquez sur l'offre Citrix ADC VPX souhaitée.
4. Cliquez sur l'onglet **Tarification**, pour accéder à **Informations sur la tarification** .
5. Sélectionnez la région et l' **option de traitement** comme **Citrix ADC VPX — Licence client**.
6. Cliquez sur **Continuer pour vous abonner**.
7. Consultez les détails sur la page **S'abonner** et cliquez sur **Continuer vers la configuration**.
8. Sélectionnez **Méthode de livraison** comme **modèle CloudFormation**.
9. Sélectionnez le modèle CloudFormation requis.
10. Sélectionnez **Version et**région**du logiciel**, puis cliquez sur **Continuer vers le lancement**.



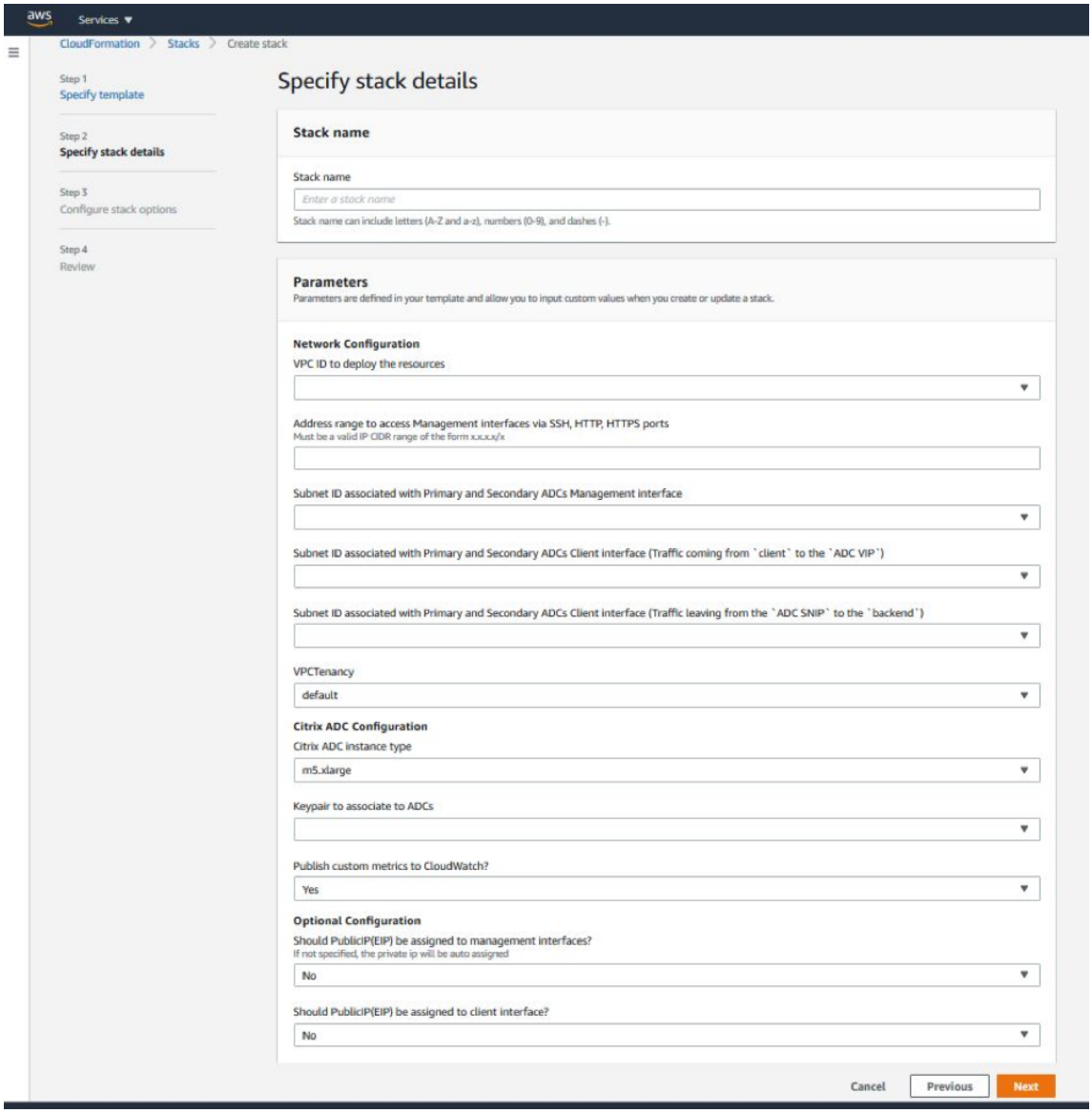
11. Sous **Choisir une action**, sélectionnez **Lancer CloudFormation**, puis cliquez sur **Lancer**.
12. La page **Créer une pile** apparaît, puis cliquez sur **Suivant**.



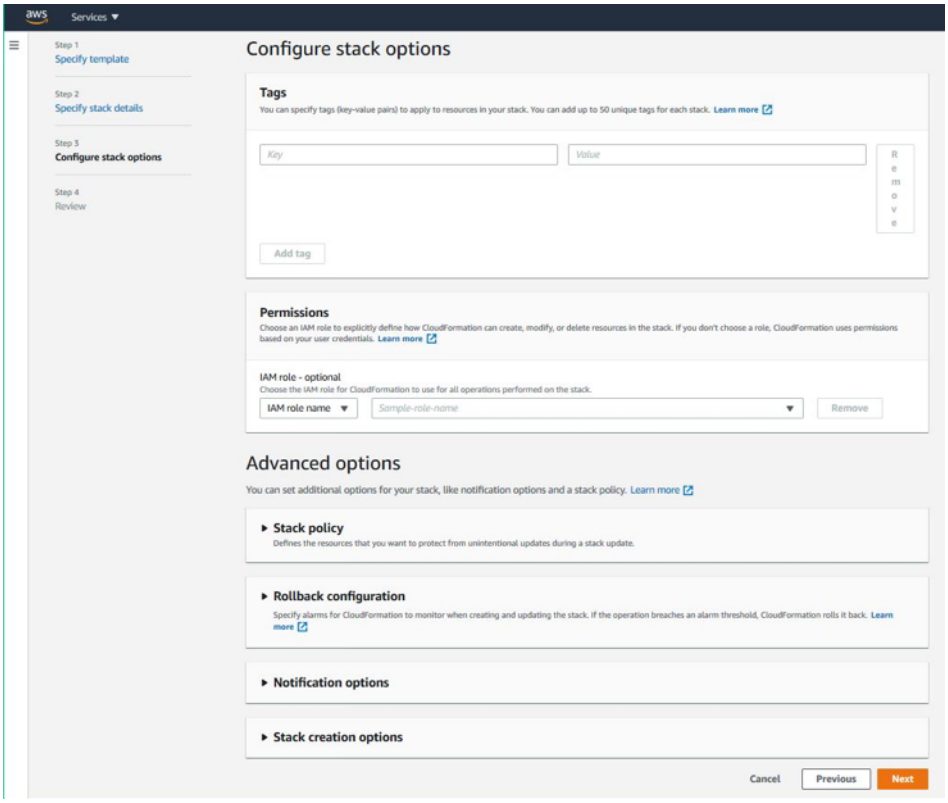
13. La page **Spécifier les détails de la pile** apparaît. Entrez les détails suivants.

    - Saisissez un **nom de pile**. Le nom doit contenir 25 caractères.
    - Sous **Configuration réseau**, effectuez les opérations suivantes :
        - Sélectionnez **Sous-réseau de gestion**, **Sous-réseau client**et **Sous-réseau de serveur**. Assurez-vous de sélectionner les sous-réseaux que vous avez créés dans le VPC que vous avez sélectionné sous ID VPC.
        - Ajoutez **l'adresse IP de gestion principale, l'adresseIP de gestion secondaire, l'adresse IP du client**et **l'adresse IP du serveur**. Les adresses IP doivent appartenir aux mêmes sous-réseaux des sous-réseaux respectifs. Vous pouvez également laisser le modèle attribuer automatiquement les adresses IP.
        - Sélectionnez **par défaut** pour **VPCTenancy**.
    - Sous **Configuration Citrix ADC**, effectuez les opérations suivantes :
        - Sélectionnez **m5.xlarge** pour le **type d'instance**.
        - Sélectionnez la paire de clés que vous avez déjà créée dans le menu de **Paire de clés**.
        - Par défaut, la fonction **Publier des mesures personnalisées sur CloudWatch ?** est définie sur **Oui**. Si vous souhaitez désactiver cette option, sélectionnez **Non**.
          Pour plus d'informations sur les mesures CloudWatch, voir Surveillance de vos instances à l'aide d'Amazon CloudWatch.
    - Sous **Configuration facultative**, effectuez les opérations suivantes :
        - Par défaut, le champ **PubliCIP (EIP) doit-il être affecté aux interfaces de gestion ?** est définie sur **Non**.

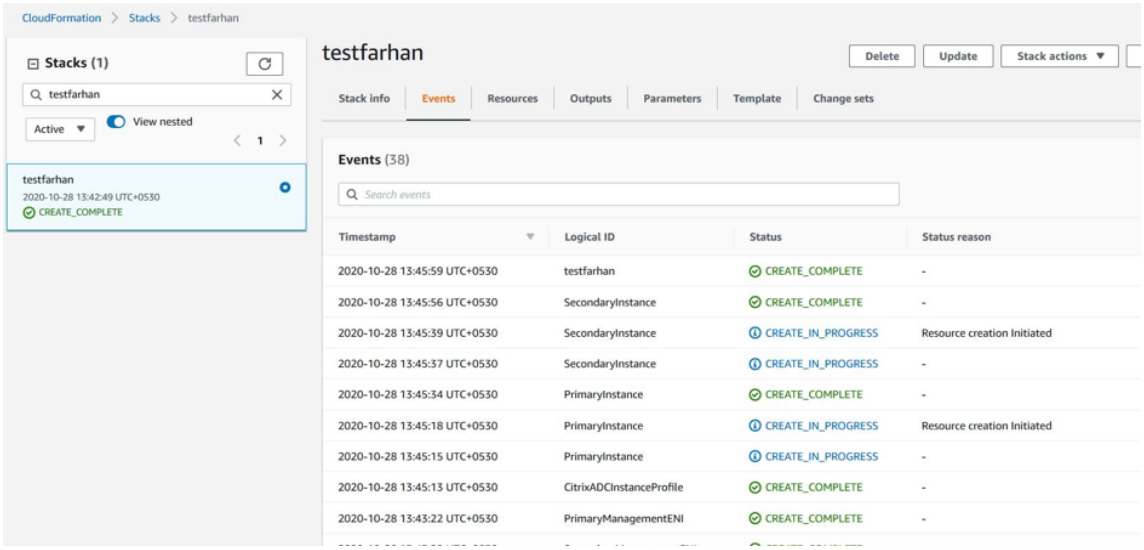
- Par défaut, la fonction **PubliCIP (EIP) doit-elle être affectée à l'interface client ?** est définie sur **Non**.



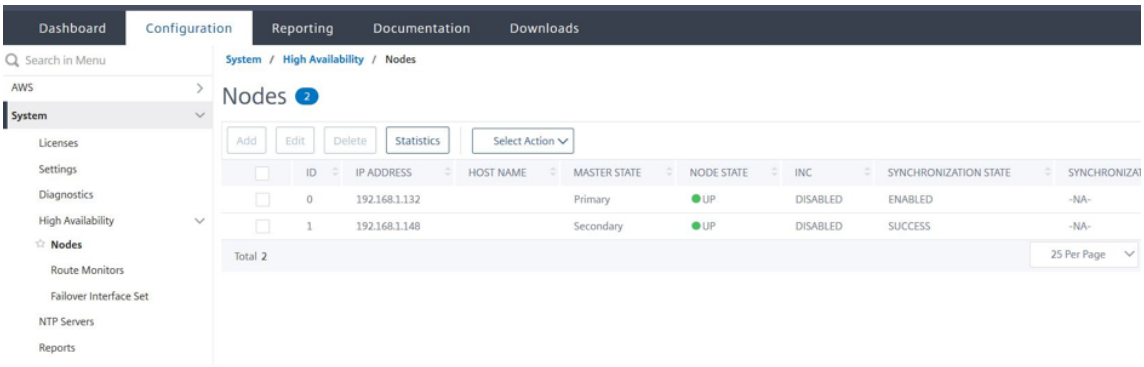
14. Cliquez sur **Suivant**.
15. La page **Configurer les options de la pile** apparaît. Il s'agit d'une page facultative.



16. Cliquez sur **Suivant**.
17. La page **Options** s'affiche. (Ceci est une page facultative.). Cliquez sur **Suivant**.
18. La page **Révision** s'affiche. Prenez quelques instants pour revoir les paramètres et apporter des modifications éventuelles, si nécessaire.
19. Sélectionnez la case **Je reconnais qu'AWS CloudFormation peut créer des ressources IAM.** , puis cliquez sur **Créer une pile**.
20. Le statut **CREATE-IN-PROGRESS** apparaît. Attendez que le statut soit **CREATE-COMPLETE**. Si le statut ne passe pas à **COMPLETE**, vérifiez la raison de l'échec dans l'onglet **Événements** et recréez l'instance avec les configurations appropriées.



21. Une fois qu'une ressource IAM est créée, accédez à **EC2 Management Console > Instances**. Vous trouvez deux instances VPX créées avec le rôle IAM. Les nœuds principaux et secondaires sont créés chacun avec trois adresses IP privées et trois interfaces réseau.
22. Ouvrez une session sur le nœud principal avec le nom d'utilisateur`nsroot` et l'ID d'instance comme mot de passe. Depuis l'interface graphique, accédez à **Système > Haute disponibilité > Nœuds**. Le Citrix ADC VPX est déjà configuré en paire HA par le modèle CloudFormation.
23. La paire Citrix ADC VPX HA apparaît.



Surveillez vos instances à l'aide d'Amazon CloudWatch

Vous pouvez utiliser le service Amazon CloudWatch pour surveiller un ensemble de mesures Citrix ADC VPX telles que l'utilisation du processeur et de la mémoire et le débit. CloudWatch surveille les ressources et les applications qui s'exécutent sur AWS, en temps réel. Vous pouvez accéder au tableau de bord Amazon CloudWatch à l'aide de la console AWS Management. Pour plus d'informations, consultez Amazon CloudWatch.

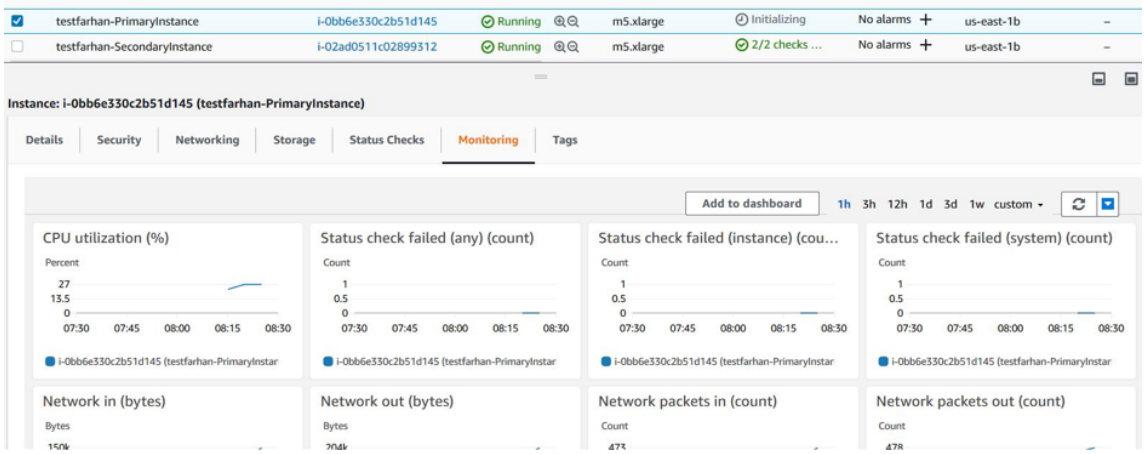
Points à noter

- Si vous déployez une instance Citrix ADC VPX sur AWS à l'aide de la console Web AWS, le service CloudWatch est activé par défaut.
- Si vous déployez une instance Citrix ADC VPX à l'aide du modèle Citrix CloudFormation, l'option par défaut est "Oui." Si vous souhaitez désactiver le service CloudWatch, sélectionnez "Non."
- Les mesures sont disponibles pour l'UC (gestion et utilisation de l'UC par paquets), la mémoire et le débit (entrants et sortants).

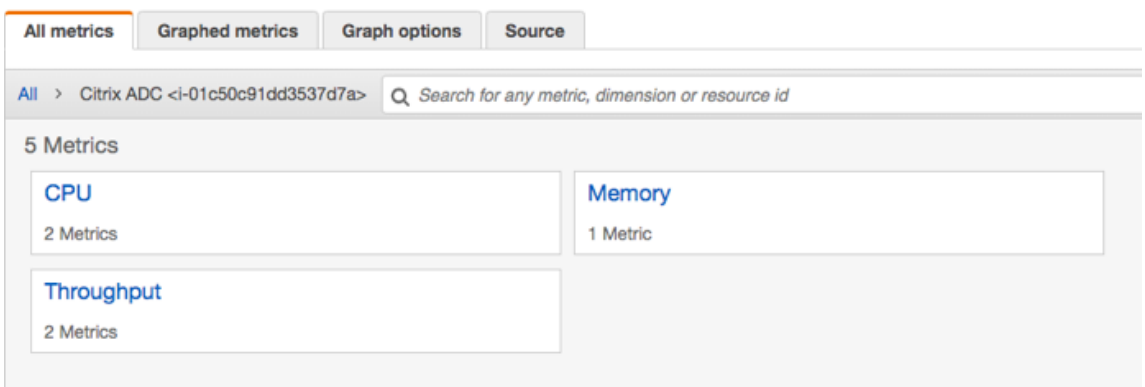
Comment afficher les statistiques CloudWatch

Pour afficher les mesures CloudWatch de votre instance, procédez comme suit :

1. Connectez-vous à **AWS Management Console > EC2 > Instances**.
2. Sélectionnez l'instance.
3. Cliquez sur **Surveillance**.
4. Cliquez sur **Afficher toutes les mesures CloudWatch**.

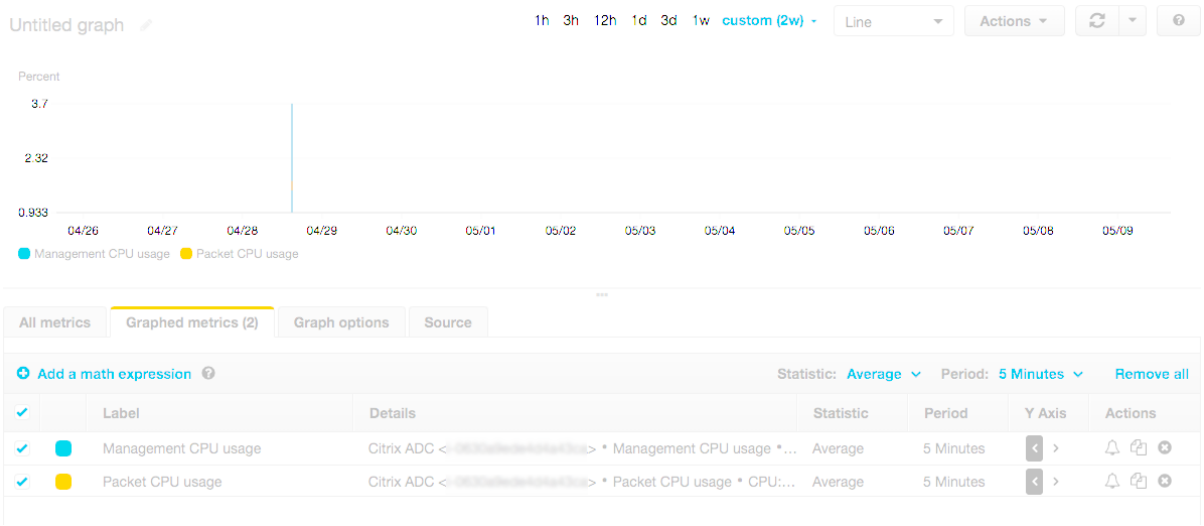


5. Sous Toutes les mesures, cliquez sur votre ID d'instance.



6. Cliquez sur les mesures que vous souhaitez afficher, définissez la durée (en minutes, heures, jours, semaines, mois).
7. Cliquez sur **Mesures graphiques** pour afficher les statistiques d'utilisation. Utilisez les **options Graph** pour personnaliser votre graphique.

Figure. Mesures graphiques pour l'utilisation de l'UC



Configuration de SR-IOV sur une configuration haute disponibilité

La prise en charge des interfaces SR-IOV dans une configuration haute disponibilité est disponible à partir de Citrix ADC version 12.0 57.19. Pour plus d'informations sur la configuration de SR-IOV, consultez Configuration des instances Citrix ADC VPX pour utiliser l'interface réseau SR-IOV.

Ressources connexes

Fonctionnement de la haute disponibilité sur AWS

Haute disponibilité dans toutes les zones de disponibilité AWS

August 20, 2021

Vous pouvez configurer deux instances Citrix ADC VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes, en tant que paire actif-passif haute disponibilité en mode INC (Independent Network Configuration). Si, pour une raison quelconque, le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité. Pour plus d'informations sur INC, voir Configuration de nœuds haute disponibilité dans différents sous-réseaux.

Points à noter

- Lisez les documents suivants avant de commencer votre déploiement :
  - Terminologie AWS
  - Conditions préalables
  - Limitations et directives d'utilisation
- La paire haute disponibilité VPX peut résider dans la même zone de disponibilité dans un sous-réseau différent ou dans deux zones de disponibilité AWS différentes.
- Citrix recommande d'utiliser différents sous-réseaux pour la gestion (NSIP), le trafic client (VIP) et le serveur principal (SNIP).
- La haute disponibilité doit être définie en mode INC (Independent Network Configuration) pour qu'un basculement fonctionne.
- Les deux instances doivent avoir le port 3003 ouvert pour le trafic UDP car il est utilisé pour les battements de cœur.
- Les sous-réseaux de gestion des deux nœuds doivent avoir accès à Internet ou au serveur API AWS via NAT interne afin que les autres API soient fonctionnelles.
- Le rôle IAM doit posséder l'autorisation E2 pour la migration IP publique ou Elastic IP (EIP) et les autorisations de table de routage EC2 pour la migration IP privée.

Vous pouvez déployer la haute disponibilité dans les zones de disponibilité AWS de la manière suivante :

- Utilisation d'adresses IP Elastic
- Utilisation d'adresses IP privées

Fonctionnement de la haute disponibilité dans les zones de disponibilité AWS

Lors du basculement, l'EIP du VIP de l'instance principale migre vers le secondaire, qui prend le relais en tant que nouveau principal. Dans le processus de basculement, l'API AWS

1. Vérifie les serveurs virtuels qui y sont `IPSets` connectés.
2. Recherche l'adresse IP qui a une adresse IP publique associée, à partir des deux adresses IP sur lesquelles le serveur virtuel écoute. Une qui est directement connectée au serveur virtuel et une qui est connectée via le jeu d'adresses IP.
3. Réassocie l'IP publique (EIP) à l'IP privée appartenant au nouveau VIP principal.

> **Remarque**
>
> Pour protéger votre réseau contre les attaques telles que le déni de service (DoS), lorsque vous utilisez un EIP, vous pouvez créer des groupes de sécurité dans AWS pour restreindre l'accès IP. Pour une haute disponibilité, vous pouvez passer d'EIP à une solution de déplacement IP privée selon vos déploiements.

Déployer une paire VPX haute disponibilité avec des adresses IP élastiques dans différentes zones AWS

October 5, 2021

Vous pouvez configurer deux instances Citrix ADC VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes à l'aide d'adresses IP élastiques en mode INC.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité. Pour plus d'informations sur INC, voir Configuration de nœuds haute disponibilité dans différents sous-réseaux.

Comment déployer une paire VPX haute disponibilité avec des adresses IP élastiques dans différentes zones AWS

Voici le résumé des étapes de déploiement d'une paire VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes.

1. Créez un cloud privé virtuel Amazon.
2. Déployez deux instances VPX dans deux zones de disponibilité différentes ou dans la même zone mais dans des sous-réseaux différents.
3. Configurer la haute disponibilité
   a) Configurez la haute disponibilité en mode INC dans les deux instances.
   b) Ajoutez un ensemble d'adresses IP dans les deux instances.
   c) Liez l'ensemble d'adresses IP dans les deux instances au VIP.
   d) Ajoutez un serveur virtuel dans l'instance principale.

Pour les étapes 1 et 2, utilisez la console AWS. Pour l'étape 3, utilisez l'interface utilisateur graphique Citrix ADC VPX ou l'interface de ligne de commande.

Étape 1. Créez un cloud privé virtuel (VPC) Amazon.

Étape 2. Déployez deux instances VPX dans deux zones de disponibilité différentes ou dans la même zone mais dans des sous-réseaux différents. Attachez un EIP au VIP du VPX principal.

Pour plus d'informations sur la façon de créer un VPC et de déployer une instance VPX sur AWS, voir Déployer une instance autonome Citrix ADC VPX sur AWS et Scenario : instance autonome

Étape 3. Configurer la haute disponibilité. Vous pouvez utiliser l'interface de ligne de commande Citrix ADC VPX ou l'interface graphique pour configurer la haute disponibilité.

Configurer la haute disponibilité à l'aide de l'interface de ligne de commande

1. Configurez la haute disponibilité en mode INC dans les deux instances.

Sur le nœud principal :

```
add ha node 1 <sec_ip> -inc ENABLED
```

Sur le nœud secondaire :

```
add ha node 1 <prim_ip> -inc ENABLED
```

<sec_ip> fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire

<prim_ip> fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal

2. Ajoutez le jeu d'adresses IP dans les deux instances.

   Tapez la commande suivante sur les deux instances.

   ```
   add ipset <ipsetname>
   ```

3. Liez l'IP définie à l'ensemble VIP sur les deux instances.

   Tapez la commande suivante sur les deux instances :

   ```
   add ns ip <secondary vip> <subnet> -type VIP
   ```

   ```
   bind ipset <ipsetname> <secondary VIP>
   ```

   > **Remarque**
   >
   > Vous pouvez lier l'IP définie au VIP principal ou au VIP secondaire. Toutefois, si vous liez l'IP définie au VIP principal, utilisez le VIP secondaire pour ajouter au serveur virtuel, et inversement.

4. Ajoutez un serveur virtuel sur l'instance principale.

   Exécutez la commande suivante :

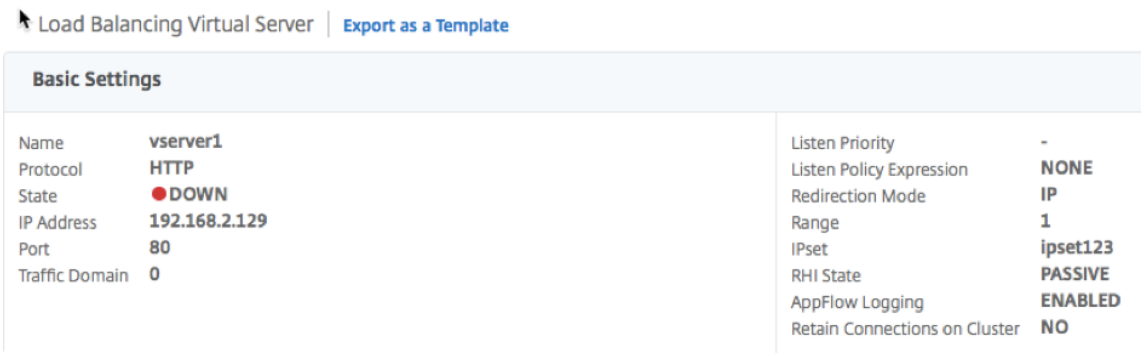
   ```
   add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port
   > -ipset \<ipset_name>
   ```

Configurer la haute disponibilité à l'aide de l'interface graphique

1. Configurer la haute disponibilité en mode INC sur les deux instances
2. Ouvrez une session sur le nœud principal avec le nom d'utilisateur`nsroot` et l'ID d'instance comme mot de passe.
3. Dans l'interface graphique, accédez à **Configuration** > **Système** > **Haute disponibilité**. Cliquez sur **Ajouter**.
4. Dans le champ **Adresse IP du nœud distant**, ajoutez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
5. Sélectionnez **Activer le mode NIC (Independent Network Configuration)** sur l'auto-nœud.

6. Sous **Informations d'identification de connexion au système distant**, ajoutez le nom d'utilisateur et le mot de passe du nœud secondaire et cliquez sur **Créer**.
7. Répétez les étapes du nœud secondaire.
8. Ajoutez un jeu IP et liez un jeu IP au jeu VIP sur les deux instances.
9. Depuis l'interface graphique, accédez à **Système** > **Réseau** > **IPs** > **Ajouter**.
10. Ajoutez les valeurs requises pour l'adresse IP, le masque de réseau, le type IP (IP virtuelle) et cliquez sur **Créer**.
11. Accédez à **Système** > **Réseau** > **Jeux d'adresses IP** > **Ajouter**. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
12. Dans la page IPv4, sélectionnez l'adresse IP virtuelle et cliquez sur **Insérer**. Cliquez sur **Créer** pour créer le jeu d'adresses IP.
13. Ajouter un serveur virtuel dans l'instance principale

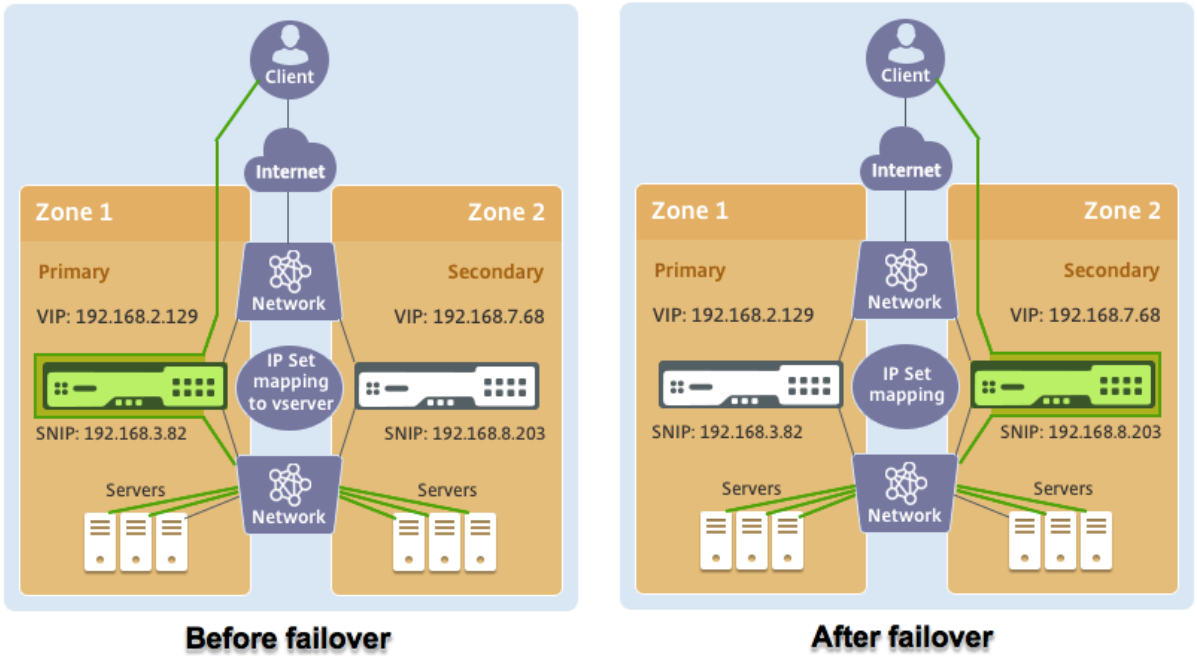
    Dans l'interface graphique, accédez à **Configuration** > **Gestion du trafic** > **Serveurs virtuels** > **Ajouter** .



Scénario

Dans ce scénario, un seul VPC est créé. Dans ce VPC, deux instances VPX sont créées dans deux zones de disponibilité. Chaque instance dispose de trois sous-réseaux : un pour la gestion, un pour le client et un pour le serveur principal. Un EIP est attaché au VIP du nœud principal.

Diagramme : Ce diagramme illustre la configuration de haute disponibilité de Citrix ADC VPX en mode INC, sur AWS



Pour ce scénario, utilisez CLI pour configurer la haute disponibilité.

1. Configurez la haute disponibilité en mode INC sur les deux instances.

   Tapez les commandes suivantes sur les nœuds primaire et secondaire.

   Sur le primaire :

   ```
   add ha node 1 192.168.6.82 -inc enabled
   ```

   Ici, 192.168.6.82 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire.

   Sur le secondaire :

   ```
   add ha node 1 192.168.1.108 -inc enabled
   ```

   Ici, 192.168.1.108 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal.

2. Ajouter un jeu d'adresses IP et lier le jeu d'adresses IP au VIP sur les deux instances

   Sur le primaire :

   ```
   add ipset ipset123
   ```

   ```
   add ns ip 192.168.7.68 255.255.255.0 -type VIP
   ```

   ```
   bindipset ipset123 192.168.7.68
   ```

   Au secondaire :

   ```
   add ipset ipset123
   ```



```
add ns ip 192.168.7.68 255.255.255.0 -type VIP

bind ipset ipset123 192.168.7.68
```

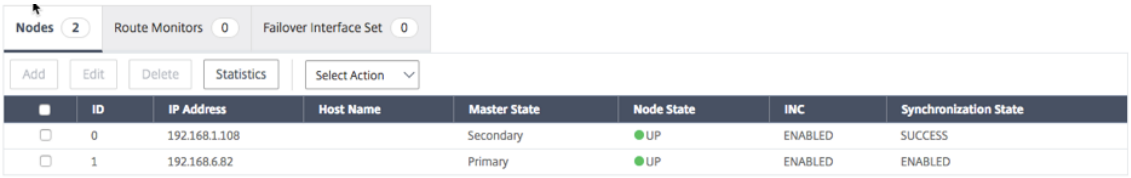
3. Ajoutez un serveur virtuel sur l'instance principale.

   La commande suivante :

   ```
   add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123
   ```

4. Enregistrez la configuration.

5. Après un basculement forcé, le secondaire devient le nouveau principal.



Déployez une paire VPX haute disponibilité avec des adresses IP privées dans différentes zones AWS

October 5, 2021

Vous pouvez configurer deux instances Citrix ADC VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes à l'aide d'adresses IP privées en mode INC. Cette solution peut être facilement intégrée à la paire haute disponibilité VPX multizone existante avec des adresses IP Elastic. Par conséquent, vous pouvez utiliser les deux solutions ensemble.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité. Pour plus d'informations sur INC, voir Configuration de nœuds haute disponibilité dans différents sous-réseaux.

> Remarque :
>
> Ce déploiement est pris en charge à partir de Citrix ADC version 13.0 version 67.39. Ce déploiement est compatible avec AWS Transit Gateway.

Conditions préalables

Assurez-vous que le rôle IAM associé à votre compte AWS dispose des autorisations IAM suivantes :

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
         }

    ]
 }


<!--NeedCopy-->
```

Comment déployer une paire VPX haute disponibilité avec des adresses IP privées dans différentes zones AWS

Voici un résumé des étapes de déploiement d'une paire VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes à l'aide d'adresses IP privées.

1. Créez un cloud privé virtuel Amazon.
2. Déployez deux instances VPX dans deux zones de disponibilité différentes.
3. Configurer la haute disponibilité
    a) Configurez la haute disponibilité en mode INC dans les deux instances.
    b) Ajoutez les tables de routage respectives dans le VPC qui pointe vers l'interface client.
    c) Ajoutez un serveur virtuel dans l'instance principale.

Pour les étapes 1 et 2, utilisez la console AWS. Pour l'étape 3, utilisez l'interface graphique Citrix ADC VPX ou l'interface de ligne de commande.

Étape 1. Créez un cloud privé virtuel (VPC) Amazon.

Étape 2. Déployez deux instances VPX dans deux zones de disponibilité différentes avec le même nombre d'interface réseau (ENI).

Pour plus d'informations sur la façon de créer un VPC et de déployer une instance VPX sur AWS, voir Déployer une instance autonome Citrix ADC VPX sur AWS et Scenario : instance autonome

Étape 3. Configurez les adresses VIP ADC en choisissant un sous-réseau qui ne chevauche pas les sous-réseaux Amazon VPC. Si votre VPC est 192.168.0.0/16, pour configurer les adresses VIP ADC, vous pouvez choisir n'importe quel sous-réseau parmi les plages d'adresses IP suivantes :

- 0.0.0.0 - 192.167.0.0
- 192.169.0.0 - 254.255.255.0

Dans cet exemple, le sous-réseau 10.10.10.0/24 choisi et créé des VIP dans ce sous-réseau. Vous pouvez choisir n'importe quel sous-réseau autre que le sous-réseau VPC (192.168.0.0/16).

Étape 4. Ajoutez une route qui pointe vers l'interface client (VIP) du nœud principal à partir de la table de routage du VPC.

À partir de l'interface de ligne de commande AWS, tapez la commande suivante :

```
1 aws ec2 create-route --route-table-id rtb-2272532 --destination-cidr-
     block 10.10.10.0/24 --gateway-id <eni-client-primary>
2 <!--NeedCopy-->
```

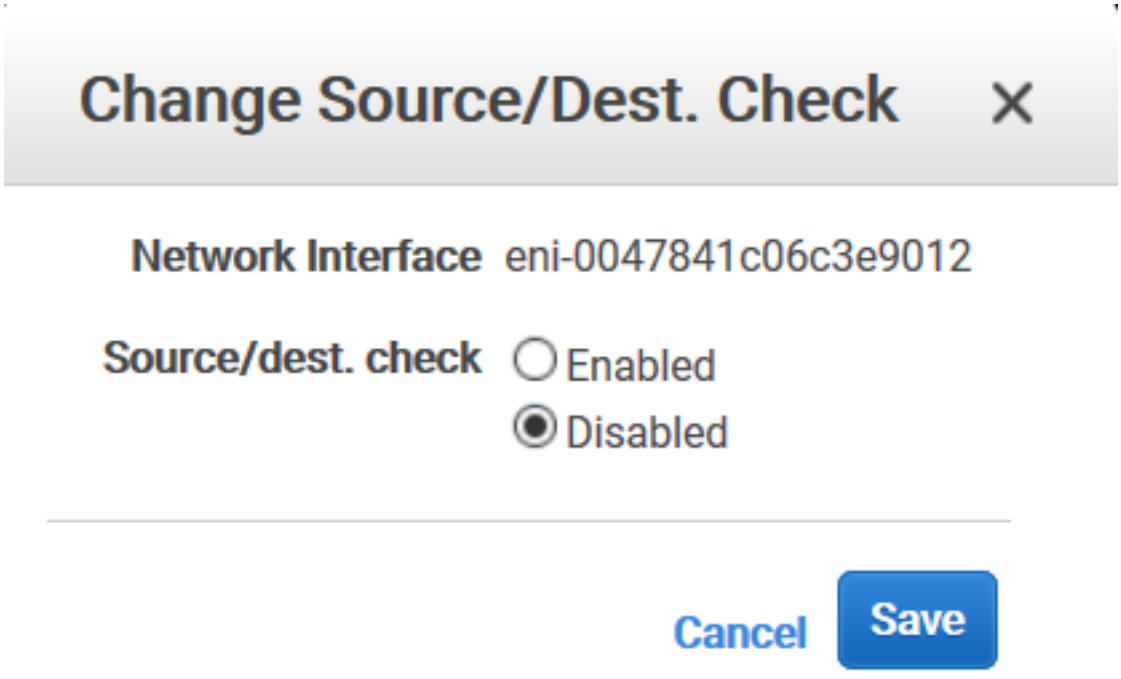
À partir de l'interface graphique AWS, effectuez les étapes suivantes pour ajouter un itinéraire :

1. Ouvrez la console Amazon EC2.
2. Dans le volet de navigation, choisissez **Tables de routage**et sélectionnez la table de routage.
3. Choisissez **Actions**, puis cliquez sur **Modifier les itinéraires**.
4. Pour ajouter un itinéraire, choisissez **Ajouter un itinéraire**. Pour **Destination**, entrez le bloc CIDR de destination, une adresse IP unique ou l'ID d'une liste de préfixes. Pour ID de passerelle, sélectionnez l'ENI d'une interface client du nœud principal.

> Remarque
>
> Vous devez désactiver la **vérification source/dest** sur l'ENI client de l'instance principale.

Pour désactiver la vérification source/destination d'une interface réseau à l'aide de la console, effectuez les opérations suivantes :

1. Ouvrez la console Amazon EC2.
2. Dans le volet de navigation, choisissez **Interfaces réseau**.
3. Sélectionnez l'interface réseau d'une interface client principale, puis choisissez **Actions**, puis cliquez sur **Modifier la source/Dest. Vérifie**.
4. Dans la boîte de dialogue, choisissez **Désactivé**, puis cliquez sur **Enregistrer**.



Étape 5. Configurez la haute disponibilité. Vous pouvez utiliser l'interface de ligne de commande Citrix ADC VPX ou l'interface graphique pour configurer la haute disponibilité.

Configuration de la haute disponibilité à l'aide de la CLI

1. Configurez la haute disponibilité en mode INC dans les deux instances.

   Sur le nœud principal :

   ```
   1 add ha node 1 <sec_ip> -inc ENABLED
   2 <!--NeedCopy-->
   ```

   Sur le nœud secondaire :

   ```
   1 add ha node 1 <prim_ip> -inc ENABLED
   2 <!--NeedCopy-->
   ```

   <sec_ip>fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire.

   <prim_ip>fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal.

2. Ajoutez un serveur virtuel sur l'instance principale. Vous devez l'ajouter à partir du sous-réseau choisi, par exemple 10.10.10.0/24.

   Exécutez la commande suivante :

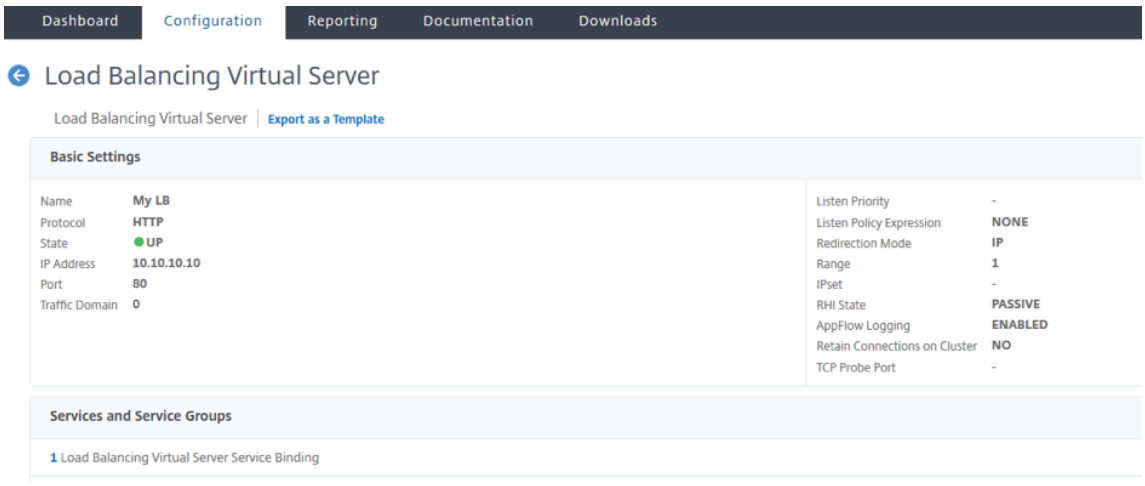
   ```
   1 add <server_type> vserver <vserver_name> <protocol> <primary_vip>
       <port>
   2 <!--NeedCopy-->
   ```

Configurer la haute disponibilité à l'aide de l'interface graphique

1. Configuration de la haute disponibilité en mode INC sur les deux instances
2. Ouvrez une session sur le nœud principal avec le nom d'utilisateur `nsroot` et l'ID d'instance comme mot de passe.
3. Accédez à **Configuration** > **Système** > **Haute disponibilité**, puis cliquez sur **Ajouter**.
4. Dans le champ **Adresse IP du nœud distant**, ajoutez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
5. Sélectionnez **Activer le mode NIC (Independent Network Configuration)** sur le nœud automatique.
6. Sous **Informations d'identification de connexion au système distant**, ajoutez le nom d'utilisateur et le mot de passe du nœud secondaire, puis cliquez sur **Créer**.

7. Répétez les étapes dans le nœud secondaire.
8. Ajouter un serveur virtuel dans l'instance principale

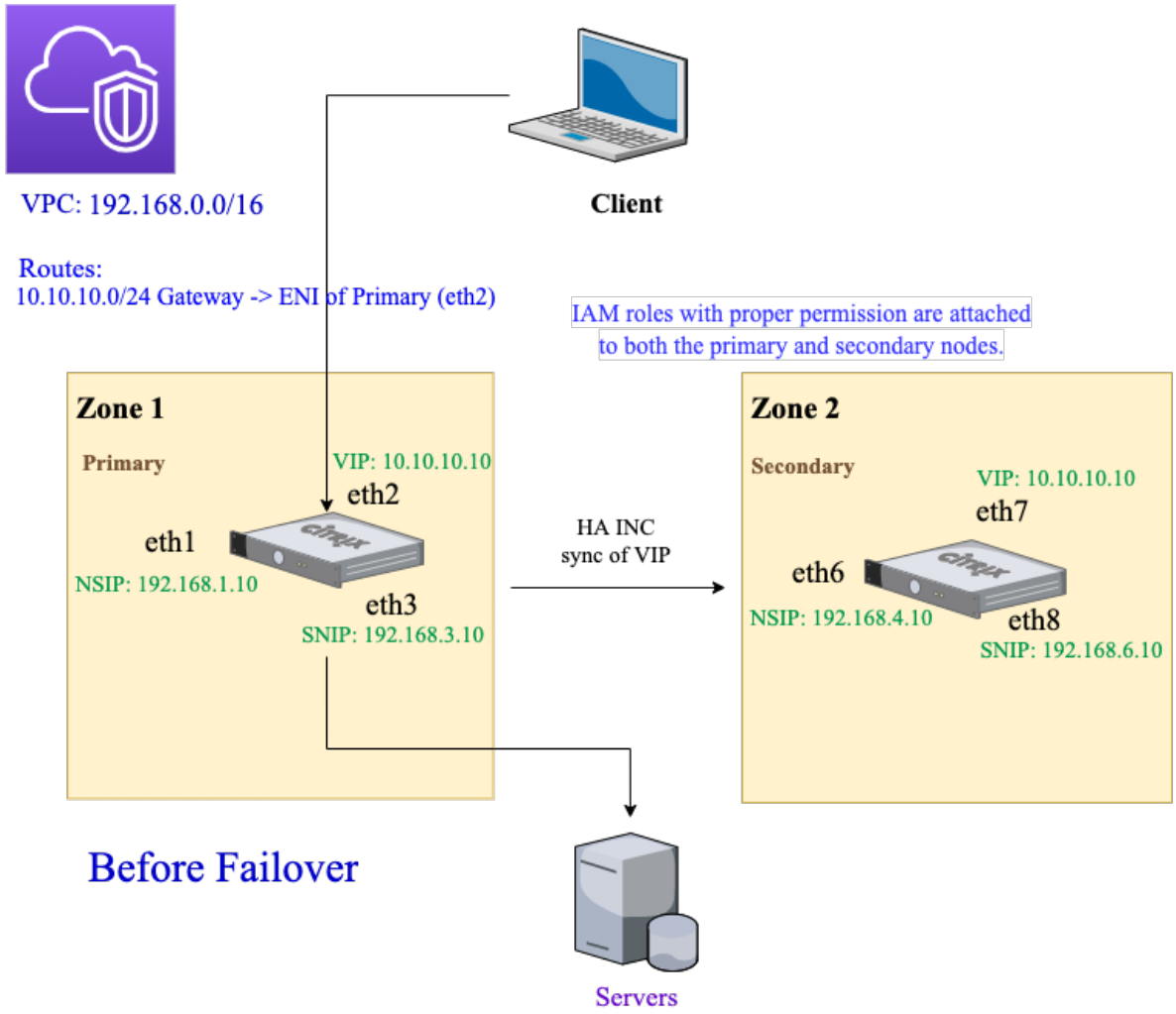
   Accédez à **Configuration** > **Gestion du trafic** > **Serveurs virtuels** > **Ajouter**.

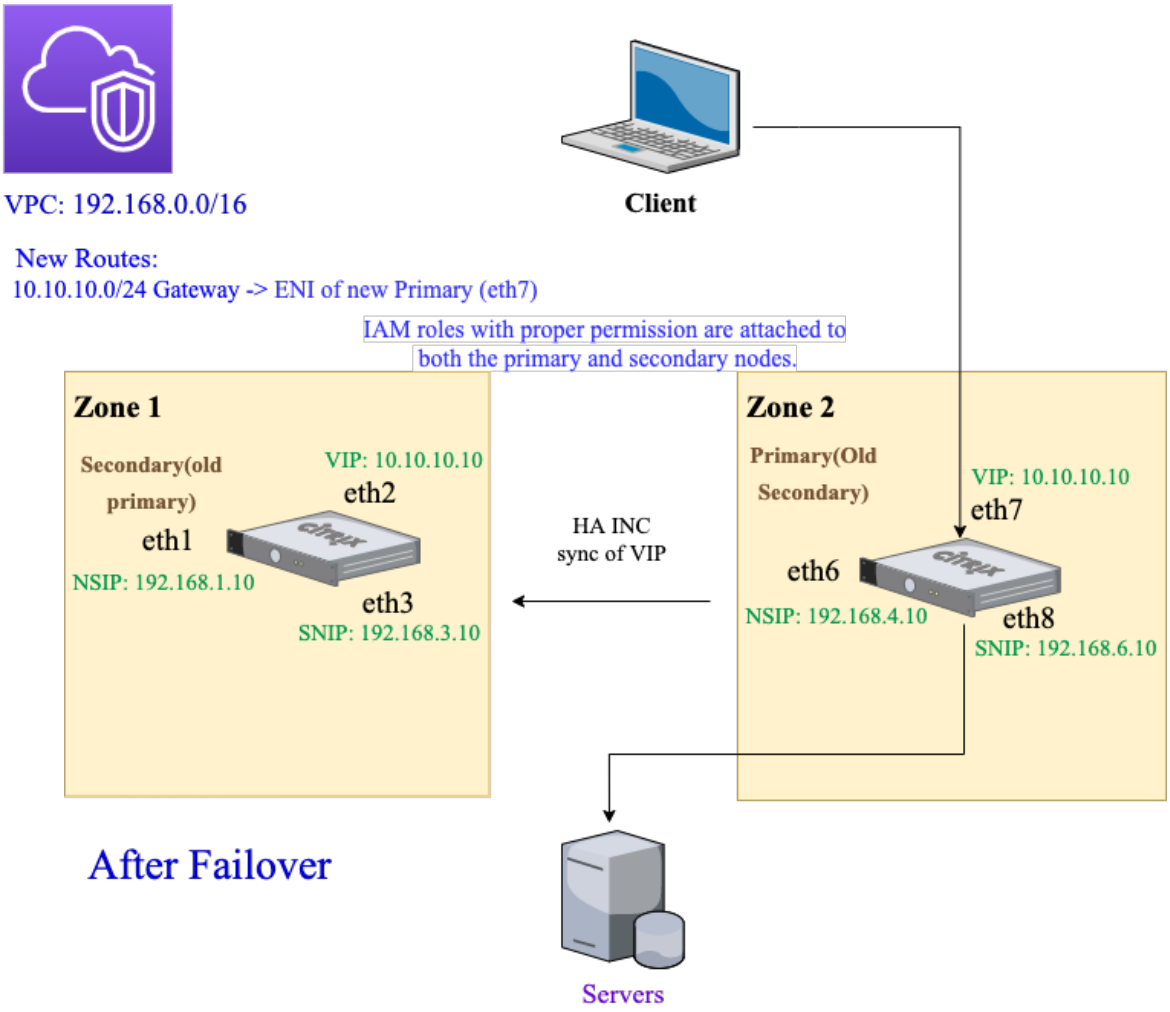


Scénario

Dans ce scénario, un seul VPC est créé. Dans ce VPC, deux instances VPX sont créées dans deux zones de disponibilité. Chaque instance comporte trois sous-réseaux : un pour la gestion, un pour le client et un pour le serveur principal.

Les diagrammes suivants illustrent la configuration haute disponibilité Citrix ADC VPX en mode INC, sur AWS. Le sous-réseau 10.10.10.10 personnalisé, qui ne fait pas partie du VPC, est utilisé comme VIP. Par conséquent, le sous-réseau 10.10.10.10 peut être utilisé dans toutes les zones de disponibilité.





Pour ce scénario, utilisez l'interface de ligne de commande pour configurer la haute disponibilité.

1. Configurez la haute disponibilité en mode INC sur les deux instances.

   Tapez les commandes suivantes sur les nœuds principal et secondaire.

   Sur le nœud principal :

   ```
   add ha node 1 192.168.4.10 -inc enabled
   <!--NeedCopy-->
   ```

   Ici, 192.168.4.10 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire.

   Sur le nœud secondaire :

   ```
   add ha node 1 192.168.1.10 -inc enabled
   <!--NeedCopy-->
   ```


Ici, 192.168.1.10 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal.

2. Ajoutez un serveur virtuel sur l'instance principale.

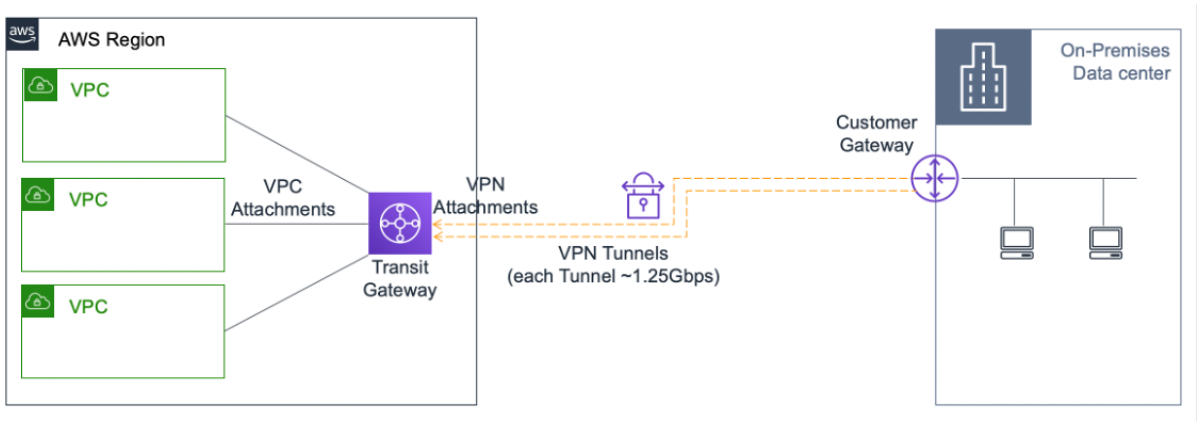
   Exécutez la commande suivante :

```
add lbvserver vserver1 http 10.10.10.10 80
<!--NeedCopy-->
```

3. Enregistrez la configuration.
4. Après un basculement forcé :
   - L'instance secondaire devient la nouvelle instance principale.
   - La route du VPC pointant vers l'ENI principale migre vers l'ENI du client secondaire.
   - Le trafic client reprend vers la nouvelle instance principale.

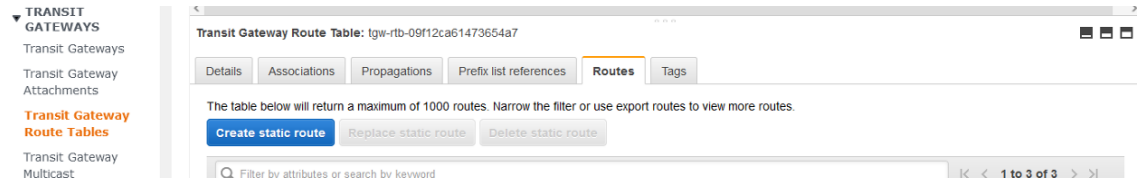
Configuration d'AWS Transit Gateway pour la solution IP privée HA

Vous avez besoin d'AWS Transit Gateway pour que le sous-réseau VIP privé soit routable au sein du réseau interne, sur les VPC AWS, les régions et les réseaux locaux. Le VPC doit se connecter à AWS Transit Gateway. Une route statique pour le sous-réseau VIP ou le pool IP à l'intérieur de la table de routage AWS Transit Gateway est créée et pointée vers le VPC.

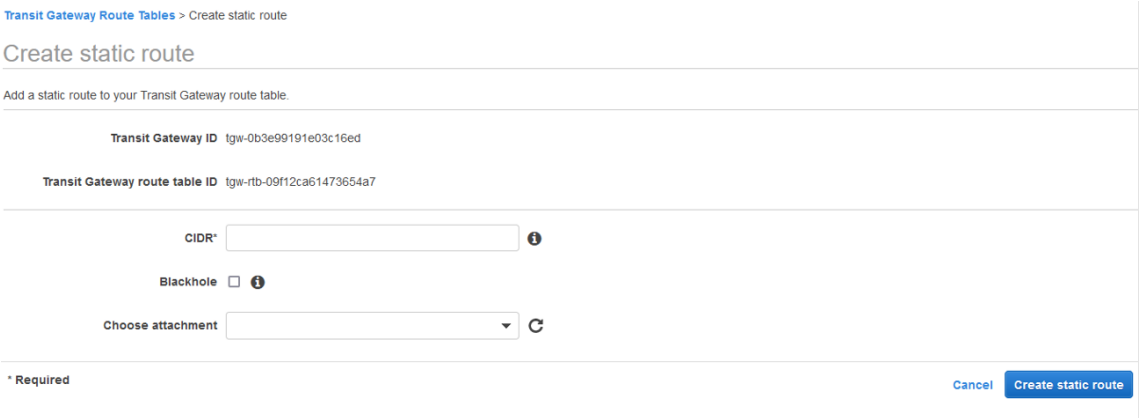


Pour configurer AWS Transit Gateway, procédez comme suit :

1. Ouvrez la console Amazon VPC.
2. Dans le volet de navigation, sélectionnez **Tables de routage Transit Gateway**.
3. Sélectionnez l'onglet **Itinéraires**, puis cliquez sur **Créer un itinéraire statique**.



4. Créez un itinéraire statique où le CIDR pointe vers votre sous-réseau VIPS privé et où les points joints pointent vers le VPC doté d'ADC VPX.



5. Cliquez sur **Créer un itinéraire statique**, puis choisissez **Fermer**.

Déployer une instance Citrix ADC VPX sur AWS Outposts

August 20, 2021

AWS Outposts est un pool de capacités de calcul et de stockage AWS déployé sur votre site. Outposts fournit une infrastructure et des services AWS dans votre emplacement local. AWS exploite, surveille et gère cette capacité dans le cadre d'une région AWS. Vous pouvez utiliser les mêmes instances Citrix ADC VPX, API AWS, outils et infrastructure sur site et dans le cloud AWS pour une expérience hybride cohérente.

Vous pouvez créer des sous-réseaux sur votre Outposts et les spécifier lorsque vous créez des ressources AWS telles que des instances EC2, des volumes EBS, des clusters ECS et des instances RDS. Les instances des sous-réseaux Outposts communiquent avec d'autres instances de la région AWS à l'aide d'adresses IP privées, toutes au sein du même Amazon Virtual Private Cloud (VPC).

Pour plus d'informations, consultez le guide de l'utilisateur AWS Outposts.

Fonctionnement de AWS Outposts

AWS Outposts est conçu pour fonctionner avec une connexion constante et cohérente entre vos avant-postes et une région AWS. Pour obtenir cette connexion à la région et aux charges de travail locales

de votre environnement local, vous devez connecter votre Outpost à votre réseau local. Votre réseau local doit fournir un accès WAN à la Région et à Internet. Internet doit également fournir un accès LAN ou WAN au réseau local où résident vos charges de travail ou applications locales.

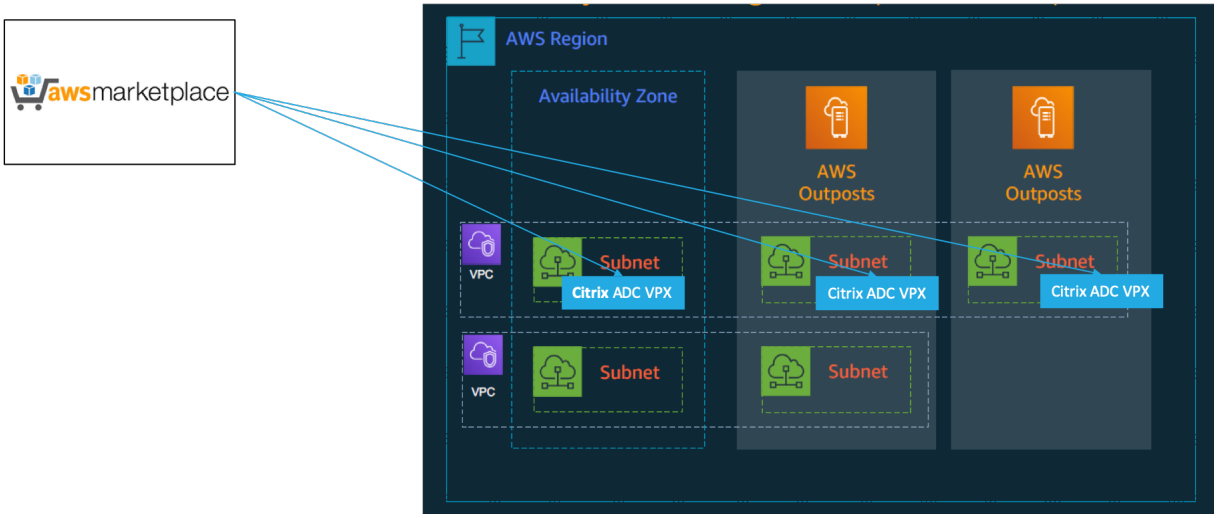
Conditions préalables

- Vous devez installer un AWS Outposts sur votre site.
- La capacité de calcul et de stockage de AWS Outposts doit être disponible pour une utilisation.

Pour plus d'informations sur la façon de passer une commande pour AWS Outposts, consultez la documentation AWS suivante :
https://aws.amazon.com/blogs/aws/aws-outposts-now-available-order-your-racks-today/

Déployer une instance Citrix ADC VPX sur AWS Outposts à l'aide de la console Web AWS

La figure suivante illustre un déploiement simple des instances Citrix ADC VPX sur Outposts. L'AMI Citrix ADC présente sur AWS Marketplace est également déployée dans les Outposts.



Connectez-vous à la console Web AWS et suivez les étapes suivantes pour déployer des instances ADC VPX EC2 sur vos AWS Outposts.

1. Créez une paire de clés.
2. Créez un Cloud privé virtuel (VPC).
3. Ajoutez d'autres sous-réseaux.
4. Créez des groupes de sécurité et des règles de sécurité.
5. Ajouter des tables de routage.
6. Créez une passerelle Internet.
7. Créez une instance VPX ADC à l'aide du service AWS EC2.
   Depuis le tableau de bord AWS, accédez à **Calculer > EC2 > Launch Instance > AWS Marketplace**.

8. Créez et connectez plus d'interfaces réseau.
9. Attachez des adresses IP élastiques à la carte réseau de gestion.
10. Connectez-vous à l'instance VPX.

Pour obtenir des instructions détaillées sur chacune des étapes, voir Déployer une instance Citrix ADC VPX sur AWS à l'aide de la console Web AWS.

Pour connaître la haute disponibilité dans le cadre du déploiement de la même zone de disponibilité, voir Déployer une paire haute disponibilité sur AWS.

Ajouter un service AWS Autoscaling back-end

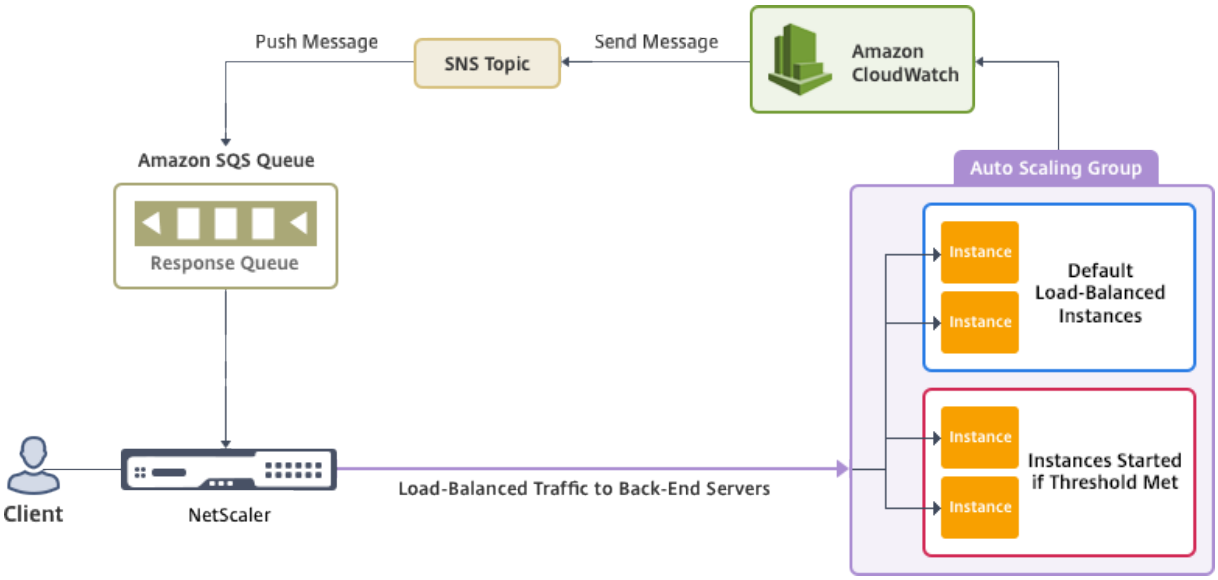
August 20, 2021

L'hébergement efficace des applications dans un cloud implique une gestion aisée et économique des ressources en fonction de la demande des applications. Pour répondre à la demande croissante, vous devez mettre à l'échelle les ressources réseau vers le haut. Que la demande diminue, vous devez réduire l'échelle pour éviter le coût inutile des ressources inutilisées. Pour minimiser le coût d'exécution de l'application en déployant seulement autant d'instances que nécessaire à un moment donné, vous devez constamment surveiller le trafic, la mémoire et l'utilisation du processeur, etc. Toutefois, la surveillance manuelle du trafic est fastidieuse. Pour que l'environnement d'application évolue de manière dynamique, vous devez automatiser les processus de surveillance du trafic et de mise à l'échelle des ressources lorsque cela est nécessaire.

Intégré au service AWS Auto Scaling, l'instance Citrix ADC VPX offre les avantages suivants :

- **Équilibrage et gestion de la charge** : configure automatiquement les serveurs pour qu'ils montent et descendent en puissance, en fonction de la demande. L'instance VPX détecte automatiquement les groupes de mise à l'échelle automatique dans le sous-réseau principal et permet à un utilisateur de sélectionner les groupes de mise à l'échelle automatique pour équilibrer la charge. Tout cela est fait en configurant automatiquement les adresses IP virtuelles et de sous-réseau sur l'instance VPX.
- **Haute disponibilité** : détecte les groupes de mise à l'échelle automatique qui couvrent plusieurs zones de disponibilité et serveurs d'équilibrage de charge.
- **Meilleure disponibilité du réseau** : l'instance VPX prend en charge :
  - Serveurs back-end sur différents VPC, à l'aide de l'appairage VPC
  - Serveurs back-end sur les mêmes groupes de placement
  - Serveurs back-end sur différentes zones de disponibilité
- **Fin de connexion gracieuse** : supprime les serveurs de mise à l'échelle automatique de manière gracieuse, évitant ainsi la perte de connexions clientes en cas d'activité de mise à l'échelle réduite, à l'aide de la fonction Délai d'expiration gracieux.

Diagramme : service AWS Autoscaling avec une instance Citrix ADC VPX



Ce diagramme illustre la compatibilité du service AWS Autoscaling avec une instance Citrix ADC VPX (serveur virtuel d'équilibrage de charge). Pour plus d'informations, consultez les rubriques AWS suivantes.

- Groupes de mise à l'échelle automatique
- CloudWatch
- Service de notification simple (SNS)
- Service de file d'attente simple (Amazon SQS)

Avant de commencer

Avant de commencer à utiliser Autoscaling avec votre instance Citrix ADC VPX, vous devez effectuer les tâches suivantes.

1. Lisez les rubriques suivantes :
   - Conditions préalables
   - Consignes de limitation et d'utilisation
2. Créez une instance Citrix ADC VPX sur AWS en fonction de vos besoins.
   - Pour plus d'informations sur la façon de créer une instance autonome Citrix ADC VPX, consultez Déployer une instance autonome Citrix ADC VPX sur AWS et Scenario : instance autonome
   - Pour plus d'informations sur le déploiement d'instances VPX en mode HA, voir Déployer une paire haute disponibilité sur AWS.

> **Remarque**
>
> Citrix recommande le modèle CloudFormation pour créer des instances Citrix ADC VPX sur AWS.
>
> Citrix vous recommande de créer trois interfaces : une pour la gestion (NSIP), une pour le serveur virtuel LB orienté client et une pour l'IP de sous-réseau (NSIP).

3. Créez un groupe AWS Autoscale. Si vous n'avez pas de configuration Autoscaling existante, vous devez :

   a) Créer une configuration de lancement

   b) Créer un groupe de mise à l'échelle automatique

   c) Vérifier le groupe Autoscaling

   Pour plus d'informations, consultez http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial.html.

4. Dans le groupe AWS Autoscale, vous devez spécifier au moins une stratégie d'échelle réduite. L'instance Citrix ADC VPX prend uniquement en charge la stratégie de mise à l'échelle Step. La stratégie de mise à l'échelle simple et la stratégie de mise à l'échelle du suivi cible ne sont pas prises en charge pour le groupe Mise à l'échelle

Ajouter le service AWS Autoscaling à une instance Citrix ADC VPX

Vous pouvez ajouter le service Autoscaling à une instance VPX en un seul clic à l'aide de l'interface graphique. Procédez comme suit pour ajouter le service Autoscaling à l'instance VPX :

1. Connectez-vous à l'instance VPX à l'aide de vos informations d'identification pour`nsroot`.
2. Lorsque vous ouvrez une session sur l'instance Citrix ADC VPX pour la première fois, la page de profil cloud par défaut s'affiche. Sélectionnez le groupe AWS Autoscaling dans le menu déroulant et cliquez sur **Créer** pour créer un profil cloud. Cliquez sur **Ignorer** si vous souhaitez créer le profil cloud ultérieurement.

   Points à garder à l'esprit lors de la création d'un profil cloud : par défaut, le modèle CloudFormation crée et attache le rôle IAM ci-dessous.

```
{

    "Version": "2012-10-17",

    "Statement": [

     {
```

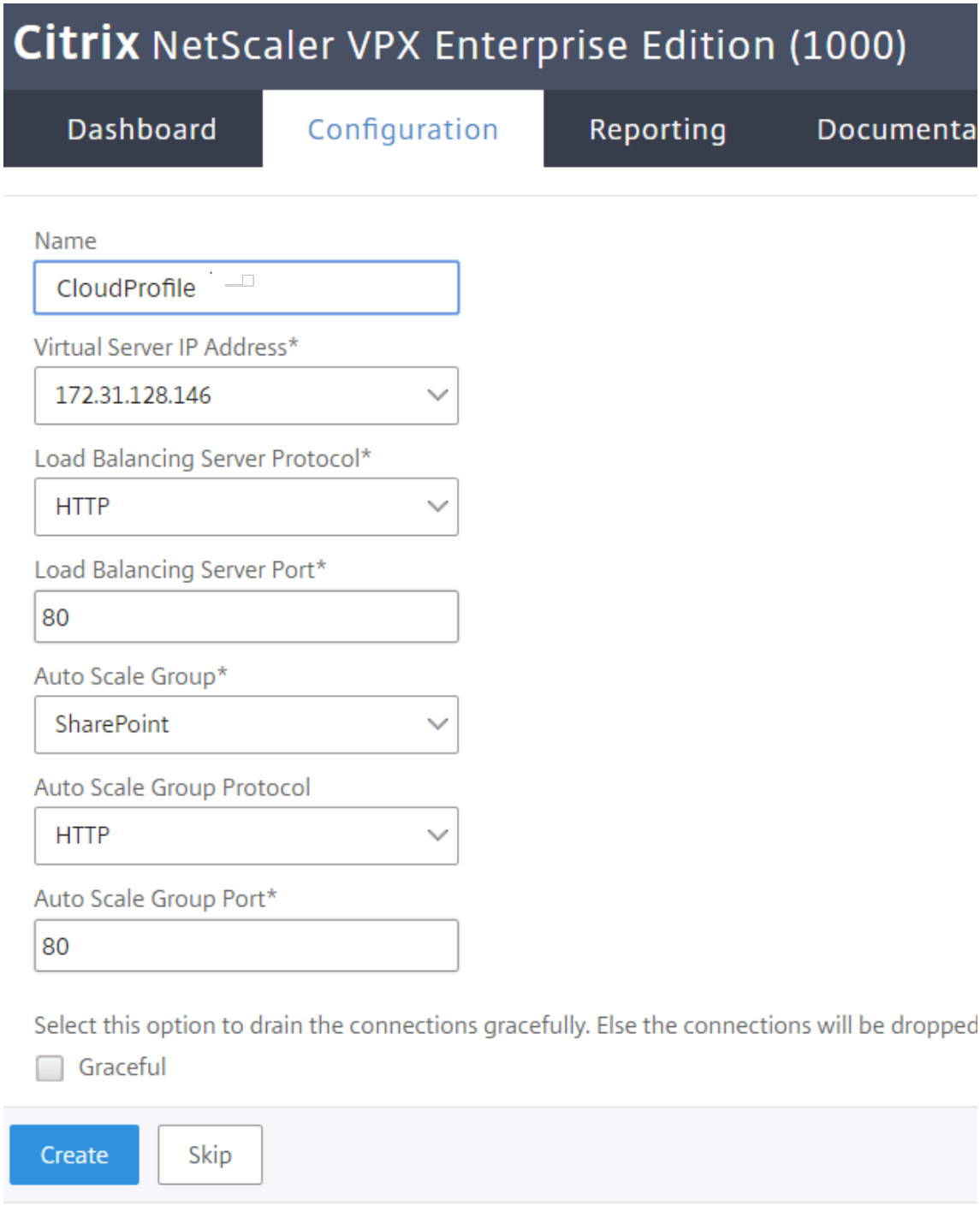


```
9
10
11              "Action": [
12
13                  "ec2:DescribeInstances",
14
15                  "ec2:DescribeNetworkInterfaces",
16
17                  "ec2:DetachNetworkInterface",
18
19                  "ec2:AttachNetworkInterface",
20
21                  "ec2:StartInstances",
22
23                  "ec2:StopInstances",
24
25                  "ec2:RebootInstances",
26
27                  "autoscaling:*",
28
29                  "sns:*",
30
31                  "sqs:*"
32
33                  “iam: SimulatePrincipalPolicy”
34
35                  “iam: GetRole”
36
37              ],
38
39              "Resource": "*",
40
41              "Effect": "Allow"
42
43          }
44
45
46      ]
47
48  }
49
50 <!--NeedCopy-->
```

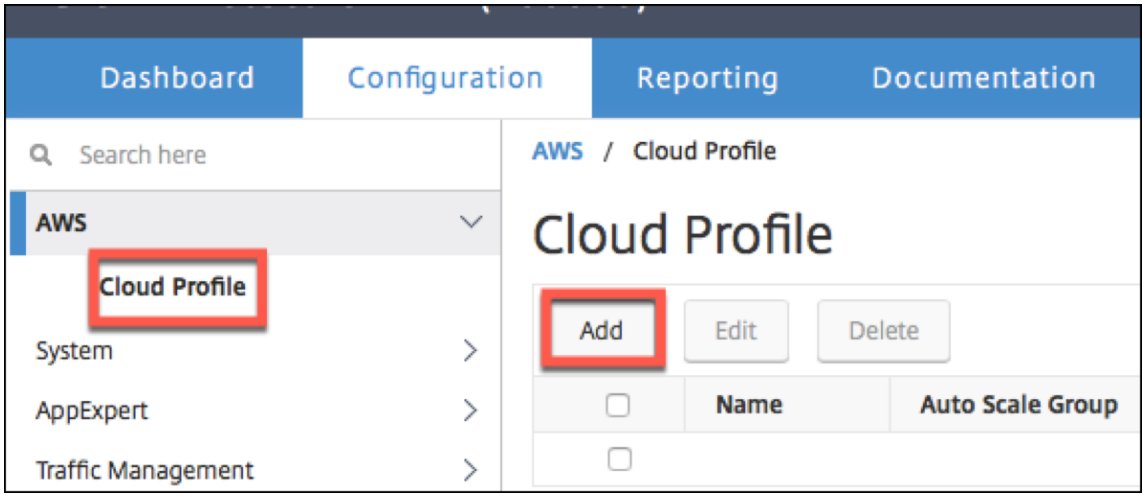
Assurez-vous que le rôle IAM d’une instance dispose des autorisations appropriées.

- L'adresse IP du serveur virtuel est automatiquement renseignée à partir de l'adresse IP libre disponible pour l'instance VPX. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html#ManageMultipleIP
- Le groupe Autoscale est prérempli à partir du groupe Autoscale configuré sur votre compte AWS. http://docs.aws.amazon.com/autoscaling/latest/userguide/AutoScalingGroup.html.
- Lors de la sélection du protocole et du port Autoscaling Group, assurez-vous que vos serveurs écoutent ces protocoles et ces ports et que vous liez le moniteur approprié dans le groupe de services. Par défaut, le moniteur TCP est utilisé.
- Pour le type de protocole SSL Autoscaling, après avoir créé le profil de nuage, le serveur virtuel d'équilibrage de charge ou le groupe de services est en panne en raison d'un certificat manquant. Vous pouvez lier manuellement le certificat au serveur virtuel ou au groupe de services.
- Sélectionnez l'option Délai d'expiration gracieux pour supprimer les serveurs de mise à l'échelle automatique. Si cette option n'est pas sélectionnée, le groupe Mise à l'échelle automatique est supprimé immédiatement après le chargement, ce qui peut entraîner une interruption de service pour les clients connectés existants. Sélectionner Graceful et donner un délai d'expiration signifie en cas de réduction de l'échelle. L'instance VPX ne supprime pas immédiatement le serveur mais marque l'un des serveurs pour une suppression gracieuse. Pendant cette période, l'instance n'autorise pas de nouvelles connexions à ce serveur. La connexion existante est servie jusqu'à ce que le délai d'expiration se produise, et après un délai d'expiration, l'instance VPX supprime le serveur.

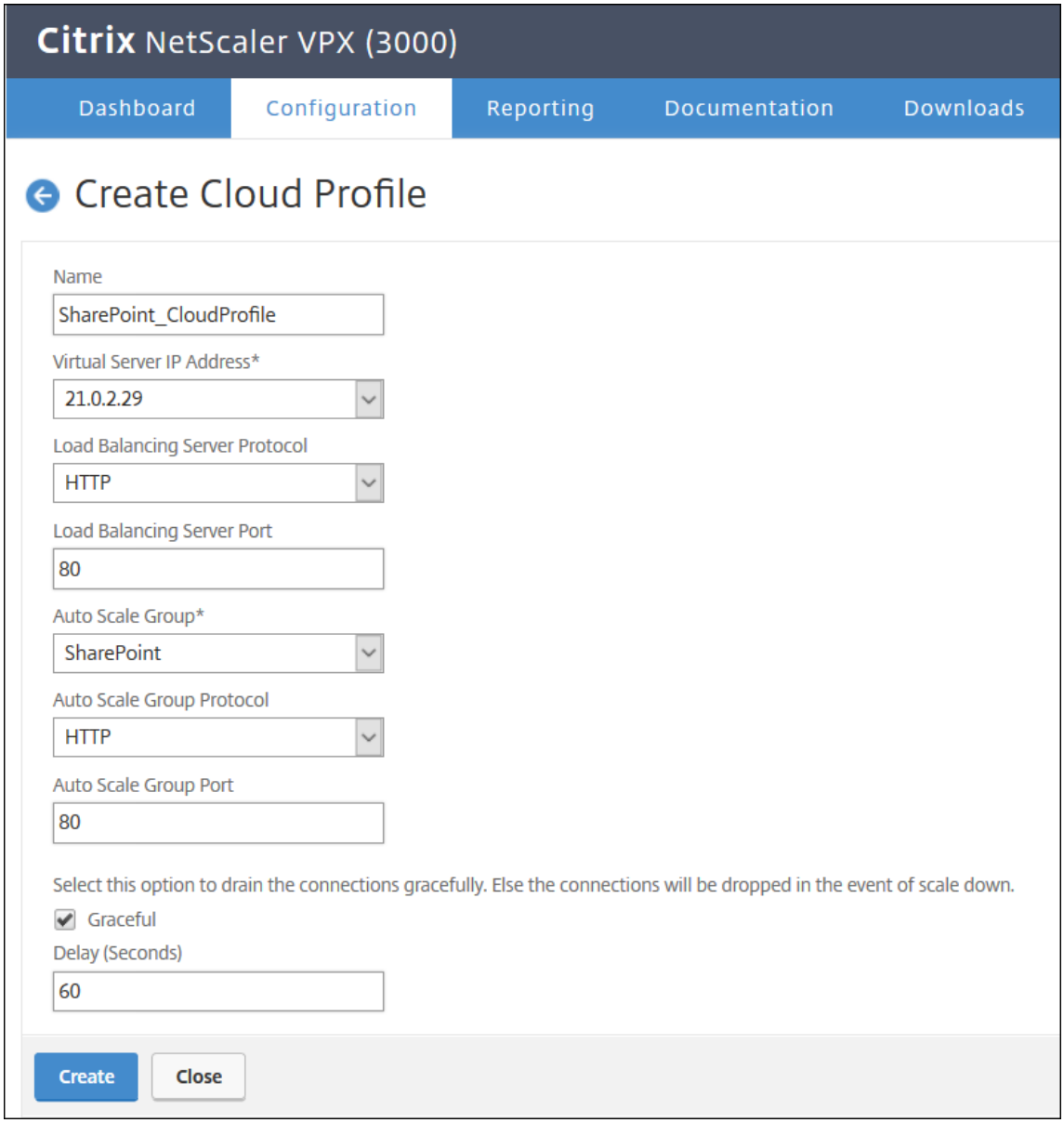
Figure : page Profil cloud par défaut



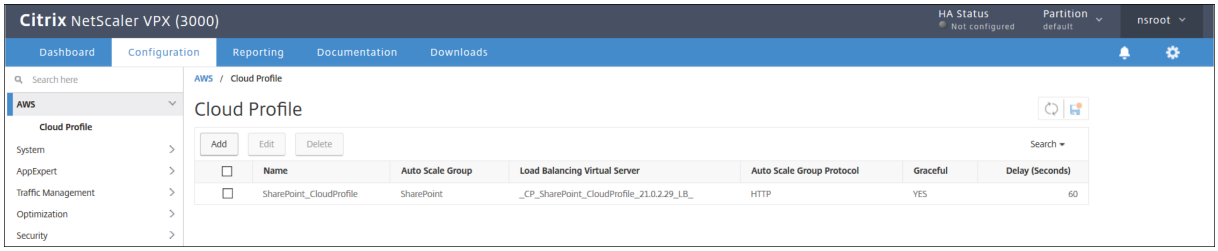
3. Après la première ouverture de session si vous souhaitez créer un profil cloud, dans l'interface graphique, accédez à **Système > AWS > Cloud Profile** et cliquez sur **Ajouter**.



La page de configuration **Créer un profil Cloud** s'affiche.



Cloud Profile crée un serveur virtuel d'équilibrage de charge Citrix ADC et un groupe de services dont les membres sont les serveurs du groupe Autoscaling. Vos serveurs back-end doivent être accessibles via le SNIP configuré sur l'instance VPX.



> **Remarque**
>
> Pour afficher les informations relatives à AutoScale dans la console AWS, accédez à **EC2** > **Tableau de bord** > **Auto Scaling** > **Auto Scaling Group** .

Configurer une instance Citrix ADC VPX pour utiliser l'interface réseau SR-IOV

August 20, 2021

> **Remarque**
>
> La prise en charge des interfaces SR-IOV dans une configuration haute disponibilité est disponible à partir de Citrix ADC version 12.0 57.19.

Une fois que vous avez créé une instance Citrix ADC VPX sur AWS, vous pouvez configurer l'appliance virtuelle pour qu'elle utilise les interfaces réseau SR-IOV, à l'aide de l'interface de ligne de commande AWS.

Dans tous les modèles Citrix ADC VPX, à l'exception des éditions Citrix ADC VPX AWS Marketplace 3G et 5G, SR-IOV n'est pas activé dans la configuration par défaut d'une interface réseau.

Avant de démarrer la configuration, lisez les rubriques suivantes :

- Conditions préalables
- Limitations et directives d'utilisation

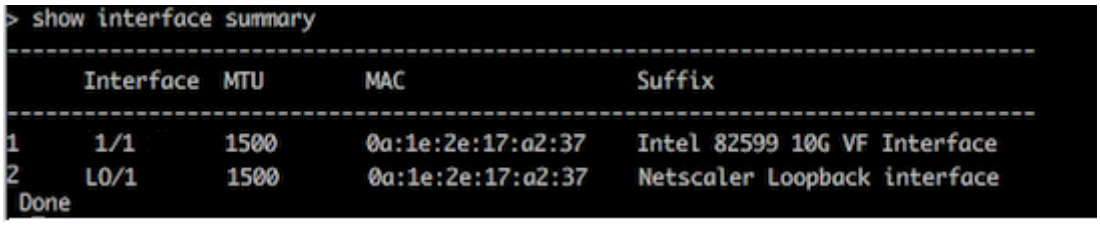
Cette section comprend les rubriques suivantes :

- Modifier le type d'interface en SR-IOV
- Configurer SR-IOV sur une configuration haute disponibilité

Modifier le type d'interface en SR-IOV

Vous pouvez exécuter la commande show interface summary pour vérifier la configuration par défaut d'une interface réseau.

Exemple 1 : La capture d'écran CLI suivante montre la configuration d'une interface réseau où SR-IOV est activé par défaut sur Citrix ADC VPX AWS Marketplace Editions de 3G et 5G.



Exemple 2 : La capture d'écran CLI suivante montre la configuration par défaut d'une interface réseau où SR-IOV n'est pas activée.

```
 Done
> sh int s
-------------------------------------------------------------------------------
      Interface  MTU        MAC                Suffix
-------------------------------------------------------------------------------
1     1/1        1500       12:fc:04:c5:d0:12  NetScaler Virtual Interface
2     LO/1       1500       12:fc:04:c5:d0:12  Netscaler Loopback interface
 Done
>
```

Pour plus d'informations sur la modification du type d'interface en SR-IOV, voir http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sriov-networking.html

Pour changer le type d'interface en SR-IOV

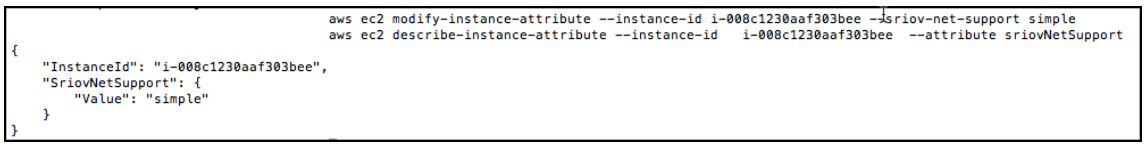
1. Arrêtez l'instance Citrix ADC VPX exécutée sur AWS.
2. Pour activer SR-IOV sur l'interface réseau, tapez la commande suivante dans l'interface de ligne de commande AWS.

   ```
   $ aws ec2 modify-instance-attribute --instance-id \<instance\\_id\> --sriov-net-support simple
   ```

3. Pour vérifier si SR-IOV a été activé, tapez la commande suivante dans l'interface de ligne de commande AWS.

   ```
   $ aws ec2 describe-instance-attribute --instance-id \<instance\\_id\> --attribute sriovNetSupport
   ```

   Exemple 3 : Le type d'interface réseau est passé à SR-IOV, à l'aide de l'interface de ligne de commande AWS.

   Si SR-IOV n'est pas activé, la valeur de SriovNetSupport est absente.

   Exemple 4 : Dans l'exemple suivant, la prise en charge SR-IOV n'est pas activée.


```
{
    "InstanceId": "i-0c3e84cfa65b04cc8",
    "SriovNetSupport": {}
}
```

4. Mettez l'instance VPX sous tension. Pour voir le statut modifié de l'interface réseau, tapez « show interface summary » dans l'interface de ligne de commande.

   Exemple 5 : La capture d'écran suivante montre les interfaces réseau avec SR-IOV activée. Les interfaces 10/1, 10/2, 10/3 sont activées SR-IOV.

```
> show interface summary
---------------------------------------------------------------------------
      Interface  MTU       MAC                Suffix
---------------------------------------------------------------------------
1     10/1       1500      0a:1e:2e:17:a2:37  Intel 82599 10G VF Interface
2     10/2       1500      0a:df:17:0a:fe:83  Intel 82599 10G VF Interface
3     10/3       1500      0a:de:5d:31:bf:c3  Intel 82599 10G VF Interface
4     LO/1       1500      0a:1e:2e:17:a2:37  Netscaler Loopback interface
 Done
```

Ces étapes complètent la procédure de configuration des instances VPX pour utiliser les interfaces réseau SR-IOV.

Configurer SR-IOV sur une configuration haute disponibilité

La haute disponibilité est prise en charge avec les interfaces SR-IOV à partir de Citrix ADC version 12.0 build 57.19.

Si la configuration de haute disponibilité a été déployée manuellement ou à l'aide du modèle Citrix CloudFormation pour Citrix ADC version 12.0 56.20 et inférieure, le rôle IAM associé à la configuration de haute disponibilité doit disposer des privilèges suivants :

- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DetachNetworkInterface
- ec2:AttachNetworkInterface
- ec2:StartInstances
- ec2:StopInstances
- ec2:RebootInstances
- autoscaling:*
- sns:*
- sqs:*
- IAM : Simuler la politique principale

- Je suis : Get Role

Par défaut, le modèle Citrix CloudFormation pour Citrix ADC version 12.0 57.19 ajoute automatiquement les privilèges requis au rôle IAM.

> **Remarque**
>
> Une configuration haute disponibilité avec interfaces SR-IOV prend environ 100 secondes d'arrêt.

Ressources connexes :

Pour plus d'informations sur les rôles IAM, consultez la documentation AWS.

Configurer une instance Citrix ADC VPX pour utiliser la mise en réseau améliorée avec AWS ENA

August 20, 2021

Après avoir créé une instance Citrix ADC VPX sur AWS, vous pouvez configurer l'appliance virtuelle pour qu'elle utilise la mise en réseau améliorée avec AWS Elastic Network Adapter (ENA), à l'aide d'AWS CLI.

Associé à AWS ENA, la mise en réseau améliorée offre une bande passante plus élevée, des performances PPS (paquet par seconde) plus élevées et des latences inter-instances toujours plus faibles.

Avant de démarrer la configuration, lisez les rubriques suivantes :

- Conditions préalables
- Limitations et directives d'utilisation

Les configurations HA suivantes sont prises en charge pour les instances compatibles ENA :

- Les adresses IP privées peuvent être déplacées dans la même zone de disponibilité.
- Les adresses IP élastiques peuvent être déplacées entre les zones de disponibilité.

Mettre à niveau une instance Citrix ADC VPX sur AWS

August 20, 2021

Vous pouvez mettre à niveau le type d'instance EC2, le débit, l'édition logicielle et le logiciel système d'un Citrix ADC VPX exécuté sur AWS. Pour certains types de mises à niveau, Citrix recommande d'utiliser la méthode de configuration haute disponibilité pour minimiser les temps d'arrêt.

> Remarque :
>
> - Le logiciel Citrix ADC version 10.1.e-124.1308.e ou ultérieure pour une AMI Citrix ADC VPX (y compris la licence utilitaire et la licence client) ne prend pas en charge les familles d'instances M1 et M2.
> - En raison des modifications apportées à la prise en charge des instances VPX, la rétrogradation de 10.1.e-124 ou une version ultérieure vers 10.1.123.x ou une version antérieure n'est pas prise en charge.
> - La plupart des mises à niveau ne nécessitent pas le lancement d'une nouvelle AMI, et la mise à niveau peut être effectuée sur l'instance actuelle de l'AMI Citrix ADC. Si vous souhaitez effectuer une mise à niveau vers une nouvelle instance AMI Citrix ADC, utilisez la méthode de configuration haute disponibilité.

Modifier le type d'instance EC2 d'une instance Citrix ADC VPX sur AWS

Si vos instances Citrix ADC VPX exécutent la version 10.1.e-124.1308.e ou ultérieure, vous pouvez modifier le type d'instance EC2 à partir de la console AWS comme suit :

1. Arrêtez l'instance VPX.
2. Modifiez le type d'instance EC2 à partir de la console AWS.
3. Démarrez l'instance.

Vous pouvez également utiliser la procédure ci-dessus pour modifier le type d'instance EC2 pour une version antérieure à 10.1.e-124.1308.e, sauf si vous souhaitez modifier le type d'instance en M3. Dans ce cas, vous devez d'abord suivre la procédure de mise à niveau standard de Citrix ADC, à l'adresse, pour mettre à niveau le logiciel Citrix ADC vers la version 10.1.e-124 ou une version ultérieure, puis suivre les étapes ci-dessus.

Mettre à niveau le débit ou l'édition logicielle d'une instance Citrix ADC VPX sur AWS

Pour mettre à niveau l'édition logicielle (par exemple, pour passer de l'édition Standard à Premium) ou le débit (par exemple, pour passer de 200 Mbps à 1000 Mbps), la méthode dépend de la licence de l'instance.

Utilisation d'une licence client (Bring-Your-Own-License)

Si vous utilisez une licence client, vous pouvez acheter et télécharger la nouvelle licence à partir du site Web Citrix, puis installer la licence sur l'instance VPX. Pour plus d'informations sur le téléchargement et l'installation d'une licence à partir du site Web Citrix, consultez le Guide des licences VPX.

Utilisation d'une licence d'utilitaire (licence d'utilitaire avec frais horaires)

AWS ne prend pas en charge les mises à niveau directes pour les instances payantes. Pour mettre à niveau l'édition logicielle ou le débit d'une instance Citrix ADC VPX payante, lancez une nouvelle AMI avec la licence et la capacité souhaitées et migrez l'ancienne configuration de l'instance vers la nouvelle instance. Pour ce faire, vous pouvez utiliser une configuration haute disponibilité Citrix ADC, comme décrit dans Mettre à niveau vers une nouvelle instance AMI Citrix ADC à l'aide d'une sous-section Configuration haute disponibilité Citrix ADC de cette page.

Mettre à niveau le logiciel système d'une instance Citrix ADC VPX sur AWS

Si vous devez mettre à niveau une instance VPX exécutant 10.1.e-124.1308.e ou une version ultérieure, suivez la procédure de mise à niveau standard de Citrix ADC lors de la mise à niveau et rétrogradez une appliance Citrix ADC.

Si vous devez mettre à niveau une instance VPX exécutant une version antérieure à 10.1.e-124.1308.e vers 10.1.e-124.1308.e ou une version ultérieure, mettez d'abord à niveau le logiciel système, puis modifiez le type d'instance en M3 comme suit :

1. Arrêtez l'instance VPX.
2. Modifiez le type d'instance EC2 à partir de la console AWS.
3. Démarrez l'instance.

Mise à niveau vers une nouvelle instance AMI Citrix ADC à l'aide d'une configuration Citrix ADC haute disponibilité

Pour utiliser la méthode haute disponibilité de mise à niveau vers une nouvelle instance AMI Citrix ADC, effectuez les tâches suivantes :

- Créez une nouvelle instance avec le type d'instance EC2 souhaité, l'édition logicielle, le débit ou la version logicielle à partir du marché AWS.
- Configurez la haute disponibilité entre l'ancienne instance (à mettre à niveau) et la nouvelle instance. Une fois la haute disponibilité configurée entre l'ancienne et la nouvelle instance, la configuration de l'ancienne instance est synchronisée avec la nouvelle instance.
- Forcer un basculement HA de l'ancienne instance vers la nouvelle instance. Par conséquent, la nouvelle instance devient principale et commence à recevoir du trafic.
- Arrêtez et reconfigurez ou supprimez l'ancienne instance d'AWS.

Prérequis et points à considérer

- Assurez-vous de comprendre le fonctionnement de la haute disponibilité entre deux instances Citrix ADC VPX sur AWS. Pour plus d'informations sur la configuration haute disponibilité entre deux instances Citrix ADC VPX sur AWS, voir Déployer une paire haute disponibilité sur AWS.

- Vous devez créer la nouvelle instance dans la même zone de disponibilité que l'ancienne instance, avec exactement le même groupe de sécurité et sous-réseau.
- La configuration de haute disponibilité nécessite des clés d'accès et secrètes associées au compte AWS Identity and Access Management (IAM) de l'utilisateur pour les deux instances. Si les informations de clé correctes ne sont pas utilisées lors de la création d'instances VPX, la configuration HA échoue. Pour plus d'informations sur la création d'un compte IAM pour une instance VPX, consultez Prérequis.
  - Vous devez utiliser la console EC2 pour créer la nouvelle instance. Vous ne pouvez pas utiliser le lancement d'AWS 1-Click, car il n'accepte pas les clés d'accès et les clés secrètes comme entrée.
  - La nouvelle instance ne doit avoir qu'une seule interface ENI.

Pour mettre à niveau une instance Citrix ADC VPX à l'aide d'une configuration haute disponibilité, procédez comme suit :

1. Configurez la haute disponibilité entre l'ancienne et la nouvelle instance. Pour configurer la haute disponibilité entre deux instances Citrix ADC VPX, à l'invite de commandes de chaque instance, tapez :

   - `add ha node <nodeID> <IPaddress of the node to be added>`
   - `save config`

   Exemple :

   À l'invite de commandes de l'ancienne instance, tapez :

   ```
   1 add ha node 30 192.0.2.30
   2 Done
   3 <!--NeedCopy-->
   ```

   À l'invite de commande de la nouvelle instance, tapez :

   ```
   1 add ha node 10 192.0.2.10
   2 Done
   3 <!--NeedCopy-->
   ```

   Tenez compte de ce qui suit :

   - Dans la configuration HA, l'ancienne instance est le nœud principal et la nouvelle instance est le nœud secondaire.
   - L'adresse IP NSIP n'est pas copiée de l'ancienne instance vers la nouvelle instance. Par conséquent, après la mise à niveau, votre nouvelle instance a une adresse IP de gestion différente de la précédente.
   - Le mot de passe du `nsroot` compte de la nouvelle instance est défini sur celui de l'ancienne instance après la synchronisation HA.

Pour plus d'informations sur la configuration haute disponibilité entre deux instances Citrix ADC VPX sur AWS, voir Déployer une paire haute disponibilité sur AWS.

2. Forcer un basculement HA. Pour forcer un basculement dans une configuration haute disponibilité, à l'invite de commandes de l'une ou l'autre des instances, tapez :

```
1 force HA failover
2 <!--NeedCopy-->
```

À la suite d'un basculement forcé, les ENI de l'ancienne instance sont migrés vers la nouvelle instance et le trafic circule à travers la nouvelle instance (le nouveau nœud principal). L'ancienne instance (le nouveau nœud secondaire) redémarre.

Si le message d'avertissement suivant s'affiche, tapez N pour annuler l'opération :

```
1 [WARNING]:Force Failover may cause configuration loss, peer health
      not optimum. Reason(s):
2 HA version mismatch
3 HA heartbeats not seen on some interfaces
4 Please confirm whether you want force-failover (Y/N)?
5 <!--NeedCopy-->
```

Le message d'avertissement s'affiche car le logiciel système des deux instances VPX n'est pas compatible HA. Par conséquent, la configuration de l'ancienne instance ne peut pas être synchronisée automatiquement avec la nouvelle instance lors d'un basculement forcé.

Voici la solution de contournement pour ce problème :

a) À l'invite du shell Citrix ADC de l'ancienne instance, tapez la commande suivante pour créer une sauvegarde du fichier de configuration (ns.conf) :

```
copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp
```

b) Supprimez la ligne suivante du fichier de configuration de sauvegarde (ns.conf.bkp) :

- `set ns config -IPAddress <IP> -netmask <MASK>`

Par exemple, `set ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0`

c) Copiez le fichier de configuration de sauvegarde de l'ancienne instance (ns.conf.bkp) dans le répertoire /nsconfig de la nouvelle instance.

d) À l'invite du shell Citrix ADC de la nouvelle instance, tapez la commande suivante pour charger le fichier de configuration de l'ancienne instance (ns.conf.bkp) sur la nouvelle instance :

- `batch -f /nsconfig/ns.conf.bkp`

e) Enregistrez la configuration sur la nouvelle instance.

- `save conifg`

f) À l'invite de commandes de l'un des nœuds, tapez la commande suivante pour forcer un basculement, puis tapez Y pour le message d'avertissement pour confirmer l'opération de basculement forcé :

- `force ha failover`

Exemple :

```
1          > force ha failover
2
3  WARNING]:Force Failover may cause configuration loss, peer health
       not optimum.
4          Reason(s):
5          HA version mismatch
6          HA heartbeats not seen on some interfaces
7          Please confirm whether you want force-failover (Y/N)? Y
8  <!--NeedCopy-->
```

3. Supprimez la configuration HA afin que les deux instances ne soient plus dans une configuration HA. Supprimez d'abord la configuration HA du nœud secondaire, puis supprimez la configuration HA du nœud principal.

   Pour supprimer une configuration HA entre deux instances Citrix ADC VPX, à l'invite de commandes de chaque instance, tapez :

   ```
   1      > remove ha node <nodeID>
   2      >  save config
   3  <!--NeedCopy-->
   ```

   Pour plus d'informations sur la configuration haute disponibilité entre deux instances VPX sur AWS, voir Déployer une paire haute disponibilité sur AWS.

   Exemple :

À l'invite de commandes de l'ancienne instance (nouveau nœud secondaire), tapez :

```
1          > remove ha node 30
2            Done
3          > save config
4            Done
5  <!--NeedCopy-->
```

À l'invite de commande de la nouvelle instance (nouveau nœud principal), tapez :


```
          > remove ha node 10
            Done
          > save config
            Done
<!--NeedCopy-->
```

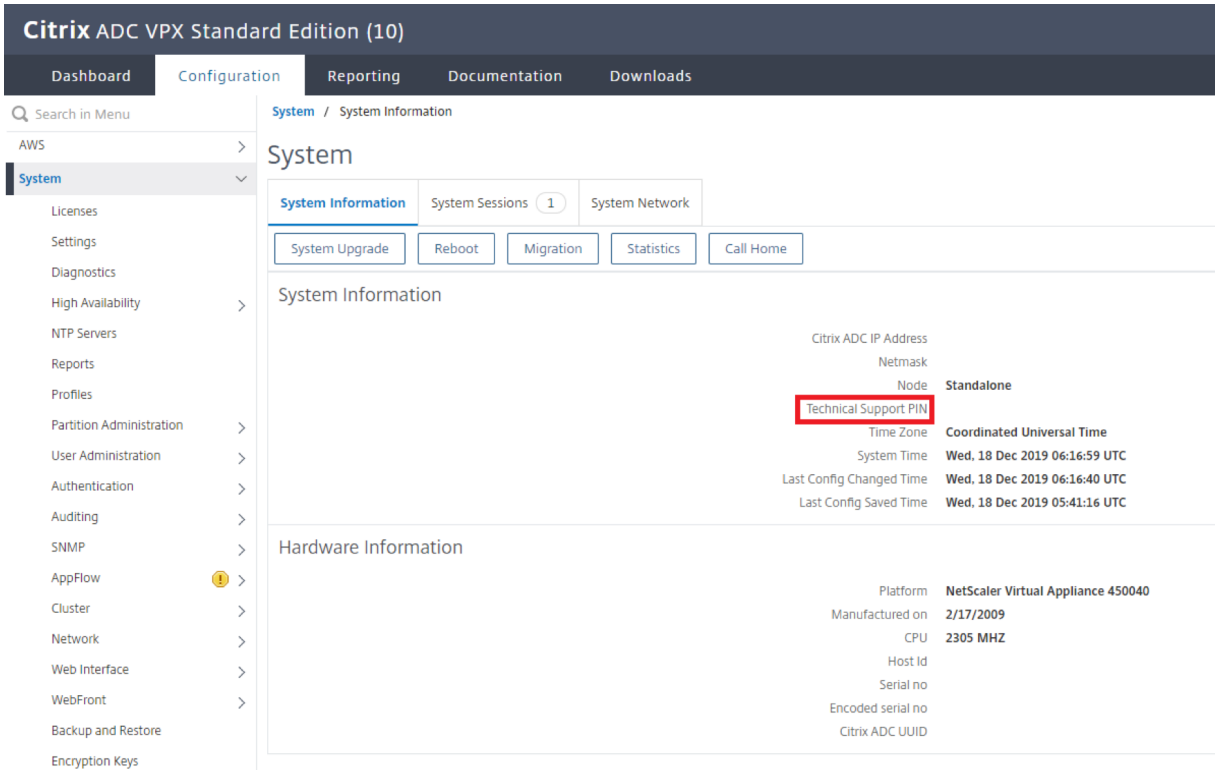
Dépannage d'une instance VPX sur AWS

August 20, 2021

Amazon ne fournit pas l'accès console à une instance Citrix ADC VPX. Pour résoudre les problèmes, vous devez utiliser l'interface graphique AWS pour afficher le journal d'activité. Vous ne pouvez déboguer que si le réseau est connecté. Pour afficher le journal système d'une instance, cliquez avec le bouton droit sur l'instance et sélectionnez Journal système.

Citrix prend en charge les instances Citrix ADC VPX sous licence AWS MarketPlace (licence utilitaire avec frais horaires) sur AWS. Pour déposer un dossier de support, recherchez votre numéro de compte AWS et votre code PIN de support, puis appelez le support Citrix. Vous serez également invité à indiquer votre nom et votre adresse e-mail. Pour trouver le code PIN de support, connectez-vous à l'interface graphique VPX et accédez à la page Système.

Voici un exemple de page système montrant le code PIN de support.



Questions fréquentes sur AWS

August 20, 2021

- **Une instance Citrix ADC VPX prend en charge les volumes chiffrés dans AWS ?**

  Le chiffrement et le déchiffrement se produisent au niveau de l'hyperviseur, et donc il fonctionne parfaitement avec n'importe quelle instance. Pour plus d'informations sur les volumes chiffrés, consultez le document AWS suivant :

  https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html

- **Quelle est la meilleure façon de provisionner l'instance Citrix ADC VPX sur AWS ?**

  Vous pouvez provisionner une instance Citrix ADC VPX sur AWS de l'une des manières suivantes :

  - Modèle AWS CloudFormation (CFT) dans AWS marketplace
  - Citrix ADM
  - Démarrages rapides AWS
  - CFT Citrix AWS dans GitHub
  - Scripts Citrix Terraform dans GitHub
  - Playbooks Citrix Ansible dans GitHub
  - Workflow de lancement AWS EC2

Vous pouvez choisir l'une des options répertoriées en fonction de l'outil d'automatisation que vous utilisez.

Pour plus d'informations sur les options, consultez Citrix ADC VPX on AWS.

- **Comment mettre à niveau l'instance Citrix ADC VPX dans AWS ?**

  Pour mettre à niveau l'instance Citrix ADC VPX dans AWS, vous pouvez mettre à niveau le logiciel système ou mettre à niveau vers une nouvelle Amazon Machine Image (AMI) Citrix ADC VPX en suivant la procédure de mise à niveau d'une instance Citrix ADC VPX sur AWS.

  La méthode recommandée pour mettre à niveau une instance Citrix ADC VPX consiste à utiliser le service ADM en suivant la procédure de la section Utiliser les tâches pour mettre à niveau des instances Citrix ADC.

- **Quel est le temps de basculement HA pour Citrix ADC VPX dans AWS ?**

  - Le basculement HA de Citrix ADC VPX dans la zone de disponibilité AWS prend environ 3 secondes.
  - Le basculement HA de Citrix ADC VPX sur les zones de disponibilité AWS prend environ 5 secondes.

- **Quel niveau de support est-il fourni aux clients d'abonnement Citrix ADC VPX Marketplace qui fournissent le code PIN du support technique ?**

  Par défaut, le service « Sélectionner pour le logiciel » est fourni aux clients qui fournissent le code PIN du support technique.

- **Dans la haute disponibilité dans différentes zones utilisant le déploiement Elastic IP, devons-nous créer plusieurs IPsets pour chaque application ?**

  Oui. S'il existe plusieurs applications avec plusieurs VIP mappés à plusieurs adresses IP, plusieurs IPsets sont nécessaires. Par conséquent, pendant le basculement HA, tous les mappages VIP principaux des EIP sont remplacés par des VIP secondaires (nouveaux VIP principaux).

- **Pourquoi le mode INC est-il activé en haute disponibilité dans différents déploiements de zones ?**

  Les paires HA dans toutes les zones de disponibilité se trouvent dans différents réseaux. Pour la synchronisation HA, la configuration réseau ne doit pas être synchronisée. Ceci est obtenu en activant le mode INC sur la paire HA.

- **Le nœud HA d'une zone de disponibilité peut-il communiquer avec les serveurs principaux d'une autre zone de disponibilité, à condition que ces zones de disponibilité se trouvent dans le même VPC ?**

  Oui, les sous-réseaux situés dans différentes zones de disponibilité du même VPC sont accessibles en ajoutant un itinéraire supplémentaire pointant vers le sous-réseau du serveur princi-

pal via SNIP. Par exemple, si le sous-réseau SNIP d'ADC dans AZ1 est 192.168.3.0/24 et que le sous-réseau de serveur principal dans AZ2 est 192.168.6.0/24, une route doit être ajoutée dans l'appliance Citrix ADC présente dans AZ1 sous la forme 192.168.6.0 255.255.255.0 192.168.3.1.

- **La haute disponibilité dans différentes zones utilisant Elastic IP et la haute disponibilité dans différentes zones utilisant des déploiements Private IP peut-elle fonctionner ensemble ?**

  Oui, les deux configurations peuvent être appliquées sur la même paire HA.

- **Dans Haute disponibilité dans différentes zones utilisant le déploiement Private IP, s'il existe plusieurs sous-réseaux avec plusieurs tables de routage dans un VPC, comment un nœud secondaire de la paire HA connaît-il la table de routage à vérifier pendant le basculement HA ?**

  Le nœud secondaire connaît les cartes réseau principales et effectue des recherches dans toutes les tables de routage d'un VPC.

- **Quelle est la taille de la `/var` partition lorsque vous utilisez l'image par défaut pour VPX sur AWS ? Comment augmenter l'espace disque ?**

  La taille du disque racine est limitée à 20 Go pour garder l'image disque petite.

  Si vous souhaitez augmenter l'espace `/var/core/` ou l'espace de `/var/crash/` répertoire, attachez un disque supplémentaire. Pour augmenter la `/var` taille, vous devez actuellement attacher un disque supplémentaire et créer un lien symbolique vers `/var`, après avoir copié le contenu critique sur le nouveau disque.

- **Combien de moteurs de paquets sont activés et alloués aux processeurs virtuels ?**

  Les moteurs de paquets (PE) sont limités par le nombre de processeurs virtuels sous licence. Les démons Citrix ADC ne sont épinglés à aucun processeur virtuel particulier et peuvent s'exécuter sur n'importe lequel des processeurs virtuels autres que PE. Selon AWS, le C5.9XLarge est une instance de 36 processeurs virtuels avec 72 Go de mémoire. Avec les licences regroupées, l'instance Citrix ADC VPX se déploie avec le nombre maximal de PE. Dans ce cas, 19 PE fonctionnent sur les cœurs 1 à 19. Toutefois, les processus de gestion ADC s'exécutent à partir des processeurs 20 à 31.

- **Comment décider de la bonne instance AWS pour ADC ?**

  1. Comprenez votre cas d'utilisation et vos exigences telles que le débit, le PPS, les exigences SSL et la taille moyenne des paquets.
  2. Choisissez l'offre ADC et les licences appropriées qui répondent à vos exigences, telles que les offres de bande passante VPX ou les licences basées sur des processeurs virtuels.
  3. En fonction de l'offre choisie, décidez de l'instance AWS.

  Exemple :

Une licence de 5 Gbit/s permet 5 moteurs de paquets de données. Par conséquent, l'exigence du processeur virtuel est de 6 (5+1 pour la gestion). Mais l'instance 6 vCPU n'est pas disponible. Un processeur virtuel 8 est donc suffisant pour atteindre ce débit à condition que vous choisissiez un réseau qui prend en charge la bande passante de 5 Gbps. Par exemple, vous devez choisir m5.2xlarge pour une licence de bande passante de 5 Gbps afin d'activer l'allocation PE maximale pour une licence de 5 Gbps. Mais si vous utilisez une licence vCPU qui n'est pas limitée par le débit, vous pouvez obtenir un débit de 5 Gbit/s à l'aide de l'instance m5.xlarge elle-même.

Instance Size	vCPU	Memory (GiB)	Instance Storage (GiB)	Network Bandwidth (Gbps)	EBS Bandwidth (Mbps)
m5.large	2	8	EBS-Only	Up to 10	Up to 4,750
m5.xlarge	4	16	EBS-Only	Up to 10	Up to 4,750
m5.2xlarge	8	32	EBS-Only	Up to 10	Up to 4,750
m5.4xlarge	16	64	EBS-Only	Up to 10	4,750

- **Le déploiement de trois sous-réseaux NIC et trois sous-réseaux est-il obligatoire pour ADC dans AWS** ?

  `Three NICs-three subnets` est le déploiement recommandé, où chacun est destiné à la gestion, au réseau client et serveur. Ce déploiement offre une meilleure isolation du trafic et des performances VPX. Deux sous-réseaux NIC, deux et un sous-réseau NIC-One sont les autres options disponibles. Citrix ne recommande pas plusieurs cartes réseau partageant un sous-réseau dans AWS, par exemple deux cartes réseau, un déploiement de sous-réseau. Parce que cela peut entraîner des problèmes de réseau tels que le routage asymétrique. Pour plus d'informations, voir Meilleures pratiques de configuration des interfaces réseau dans AWS.

Deploy a Citrix ADC VPX instance on Microsoft Azure

October 5, 2021

Lorsque vous déployez une instance Citrix ADC VPX sur Microsoft Azure Resource Manager (ARM), vous pouvez utiliser les deux ensembles de fonctionnalités suivants pour répondre aux besoins de votre entreprise :

- Fonctionnalités de cloud computing Azure
- Fonctionnalités d'équilibrage de charge et de gestion du trafic Citrix ADC

Vous pouvez déployer des instances Citrix ADC VPX sur ARM en tant qu'instances autonomes ou en tant que paires haute disponibilité en mode actif-veille.

Vous pouvez déployer une instance Citrix ADC VPX sur Microsoft Azure de deux manières :

- via la Place de marché Azure. Le boîtier virtuel Citrix ADC VPX est disponible en tant qu'image dans Microsoft Azure Marketplace.
- À l'aide du modèle json Citrix ADC Azure Resource Manager (ARM) disponible sur GitHub. Pour plus d'informations, consultez le référentiel GitHub pour les modèles de solutions Citrix NetScaler.

La pile Microsoft Azure est une plateforme intégrée de matériel et de logiciels qui fournit les services de cloud public Microsoft Azure dans un centre de données local pour permettre aux organisations de construire des clouds hybrides. Vous pouvez désormais déployer les instances Citrix ADC VPX sur la pile Microsoft Azure.

Conditions préalables

Vous avez besoin de connaissances préalables avant de déployer une instance Citrix VPX sur Azure.

- Familiarité avec la terminologie Azure et les détails du réseau. Pour plus d'informations, voir Terminologie Azure.
- Connaissance d'une appliance Citrix ADC. Pour obtenir des informations détaillées sur l'appliance Citrix ADC, consultez Citrix ADC.
- Connaissance de la mise en réseau Citrix ADC. Consultez la rubrique Mise en réseau .

Fonctionnement d'une instance Citrix ADC VPX sur Azure

Dans un déploiement sur site, une instance Citrix ADC VPX nécessite au moins trois adresses IP :

- Adresse IP de gestion, appelée adresse NSIP
- Adresse IP du sous-réseau (SNIP) pour communiquer avec la batterie de serveurs
- Adresse IP du serveur virtuel (VIP) pour accepter les demandes des clients

Pour plus d'informations, consultez Architecture réseau pour les instances Citrix ADC VPX sur Microsoft Azure.

> **Remarque**
>
> Les appliances virtuelles VPX peuvent être déployées sur n'importe quel type d'instance doté de deux cœurs Intel VT-X ou plus et de plus de 2 Go de mémoire. Pour plus d'informations sur la configuration système requise, consultez la fiche technique Citrix ADC VPX. Actuellement, l'instance Citrix ADC VPX ne prend en charge que les processeurs Intel.

Dans un déploiement Azure, vous pouvez provisionner une instance Citrix ADC VPX sur Azure de trois manières :

- Architecture multi-NIC Multi-IP
- Architecture multi-IP d'une carte réseau unique

- Carte d'interface réseau unique, IP unique

En fonction de vos besoins, vous pouvez utiliser n'importe lequel de ces types d'architecture pris en charge.

Architecture multi-NIC Multi-IP

Dans ce type de déploiement, plusieurs interfaces réseau (NIC) peuvent être attachées à une instance VPX. Toute carte réseau peut avoir une ou plusieurs configurations IP (adresses IP publiques et privées statiques ou dynamiques) qui lui sont attribuées.

Pour plus d'informations, consultez les cas d'utilisation suivants :

- Configurez une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau
- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell

> Remarque
>
> Pour éviter les déplacements MAC et les muets de l'interface sur les environnements Azure, Citrix vous recommande de créer un VLAN par interface de données (sans balise) de l'instance ADC VPX et de lier l'IP principale de la carte réseau dans Azure. Pour plus d'informations, consultez l'article CTX224626 .

Architecture multi-IP d'une carte réseau unique

Dans ce type de déploiement, une interface réseau (NIC) associée à plusieurs configurations IP - adresses IP publiques et privées statiques ou dynamiques qui lui sont attribuées.
Pour plus d'informations, consultez les cas d'utilisation suivants :

- Configuration de plusieurs adresses IP pour une instance autonome Citrix ADC VPX
- Configurez plusieurs adresses IP pour une instance autonome Citrix ADC VPX à l'aide des commandes PowerShell

Carte d'interface réseau unique, IP unique

Dans ce type de déploiement, une interface réseau (NIC) associée à une seule adresse IP, qui est utilisée pour exécuter les fonctions NSIP, SNIP et VIP.

Pour plus d'informations, consultez le cas d'utilisation suivant :

- Configurer une instance autonome Citrix ADC VPX

> **Remarque**
>
> Le mode IP unique est disponible uniquement dans les déploiements Azure. Ce mode n'est pas disponible pour une instance Citrix ADC VPX sur votre site, sur AWS ou dans un autre type de déploiement.

Licence Citrix ADC VPX

Une instance Citrix ADC VPX sur Azure nécessite une licence. Les options de licence suivantes sont disponibles pour les instances Citrix ADC VPX exécutées sur Azure.

- **Licences par abonnement** : les appliances Citrix ADC VPX sont disponibles en tant qu'instances payantes sur Azure Marketplace. Les licences par abonnement sont une option de paiement à l'utilisation. Les utilisateurs sont facturés à l'heure. Les modèles et types de licence VPX suivants sont disponibles sur la Azure Marketplace.

Modèle VPX	Type de licence	Instance recommandée
VPX10	Standard, Avancé, Premium	Standard_D2s_v4
VPX200	Standard, Avancé, Premium	Standard_D2s_v4
VPX1000*	Standard, Avancé, Premium	Standard_D4s_v4
VPX3000*	Standard, Avancé, Premium	Standard_D8s_v4
VPX5000*	Standard, Avancé, Premium	Standard_D8s_v4

> * : Du modèle VPX 1000 au VPX 5000, vous devez activer la mise en réseau accélérée sur les instances Citrix ADC VPX pour obtenir les performances souhaitées.

Citrix fournit une assistance technique pour les instances de licence basées sur un abonnement. Pour déposer un dossier de support, reportez-vous à la section Prise en charge de Citrix ADC on Azure — Licence d'abonnement à prix horaire.

- **Apportez votre propre licence (BYOL)** : si vous apportez votre propre licence (BYOL), consultez le Guide de licences VPX à l'adresse http://support.citrix.com/article/CTX122426. Vous devez :
  - Utilisez le portail de licences du site Web Citrix pour générer une licence valide.
  - Télécharger la licence sur l'instance.

Modèle VPX	Type de licence	Instance recommandée
VPX10	Standard, Avancé, Premium	Standard_D2s_v4
VPX200	Standard, Avancé, Premium	Standard_D2s_v4

Modèle VPX	Type de licence	Instance recommandée
VPX1000*	Standard, Avancé, Premium	Standard_D4s_v4
VPX3000*	Standard, Avancé, Premium	Standard_D8s_v4
VPX5000*	Standard, Avancé, Premium	Standard_D8s_v4
VPX8000*	Standard, Avancé, Premium	Standard_D8s_v4
VPX10000*	Standard, Avancé, Premium	Standard_D16s_v4

> * : Des modèles VPX 1000 à VPX 10000, vous devez activer la mise en réseau accélérée sur les instances Citrix ADC VPX pour obtenir les performances souhaitées.

- Licences d'**enregistrement et de départ Citrix ADC VPX : pour plus d'informations, consultez Licences**d' enregistrement et de départ Citrix ADC VPX.

> **Remarque**
>
> Dans un environnement Azure Stack, **BYOL** est la seule option de licence disponible.

À partir de NetScaler version 12.0 56.20, VPX Express pour les déploiements locaux et cloud ne nécessite pas de fichier de licence. Pour plus d'informations sur Citrix ADC VPX Express, consultez la section « Licence Citrix ADC VPX Express » de la présentation des licences Citrix ADC.

> **Remarque**
>
> Quelle que soit la licence horaire par abonnement achetée sur la Place de marché Azure, dans de rares cas, l'instance Citrix ADC VPX déployée sur Azure peut présenter une licence Citrix ADC par défaut. Cela est dû à des problèmes avec Azure Instance Metadata Service (IMDS).
>
> Redémarrez à chaud avant d'apporter une modification de configuration sur l'instance Citrix ADC VPX, pour activer la licence Citrix ADC VPX appropriée.

Limitations

L'exécution de la solution d'équilibrage de charge Citrix ADC VPX sur ARM impose les limitations suivantes :

- L'architecture Azure ne prend pas en charge les fonctionnalités NetScaler suivantes :
  - IPv6
  - ARP gratuit (GARP)
  - Mode L2
  - VLAN balisé
  - Routage dynamique

  - MAC virtuel
  - USIP
  - Trames Jumbo
  - Mise en cluster

  > Remarque
  >
  > Avec la fonctionnalité Autoscale de Citrix Application Delivery Management (ADM) (déploiement cloud), les instances ADC prennent en charge le clustering sur toutes les licences. Pour plus d'informations, consultez la section Mise à l'échelle automatique de Citrix ADC VPX dans Microsoft Azure à l'aide de Citrix ADM.

- Si vous vous attendez à devoir arrêter et désallouer temporairement la machine virtuelle Citrix ADC VPX à tout moment, attribuez une adresse IP interne statique lors de la création de la machine virtuelle. Si vous n'attribuez pas d'adresse IP interne statique, Azure peut attribuer à la machine virtuelle une adresse IP différente chaque fois qu'elle redémarre, et la machine virtuelle risque de devenir inaccessible.
- Dans un déploiement Azure, seuls les modèles Citrix ADC VPX suivants sont pris en charge : VPX 10, VPX 200, VPX 1000 et VPX 3000. Pour plus d'informations, consultez la fiche technique Citrix ADC VPX.

  Si vous utilisez une instance Citrix ADC VPX avec un numéro de modèle supérieur à VPX 3000, le débit réseau peut ne pas être le même que celui spécifié par la licence de l'instance. Cependant, d'autres fonctionnalités telles que le débit SSL et les transactions SSL par seconde peuvent s'améliorer.
- L'« ID de déploiement » généré par Azure lors du Provisioning de machine virtuelle n'est pas visible pour l'utilisateur dans ARM. Vous ne pouvez pas utiliser l'ID de déploiement pour déployer l'appliance Citrix ADC VPX sur ARM.
- L'instance Citrix ADC VPX prend en charge un débit de 20 Mo/s et des fonctionnalités d'édition standard lorsqu'elle est initialisée.
- Les instances Citrix ADC VPX sur Azure avec mise en réseau accélérée activée offrent de meilleures performances. La mise en réseau accélérée Azure est prise en charge sur les instances Citrix ADC VPX à partir de la version 13.0 build 76.x. Pour activer la mise en réseau accélérée sur ADC VPX, Citrix vous recommande d'utiliser un type d'instance Azure prenant en charge la mise en réseau accélérée.
- Pour un déploiement XenApp et XenDesktop, un serveur virtuel VPN sur une instance VPX peut être configuré dans les modes suivants :

  - Mode de base, où le paramètre du serveur virtuel `ICAOnly` VPN est défini sur ON. Le mode de base fonctionne entièrement sur une instance Citrix ADC VPX sans licence.

- Mode SmartAccess, où le paramètre du serveur virtuel `ICAOnly` VPN est défini sur OFF. Le mode SmartAccess ne fonctionne que pour cinq utilisateurs de session Citrix ADC AAA sur une instance Citrix ADC VPX sans licence.

> **Remarque**
>
> Pour configurer la fonctionnalité SmartControl, vous devez appliquer une licence Premium à l'instance Citrix ADC VPX.

Terminologie Azure

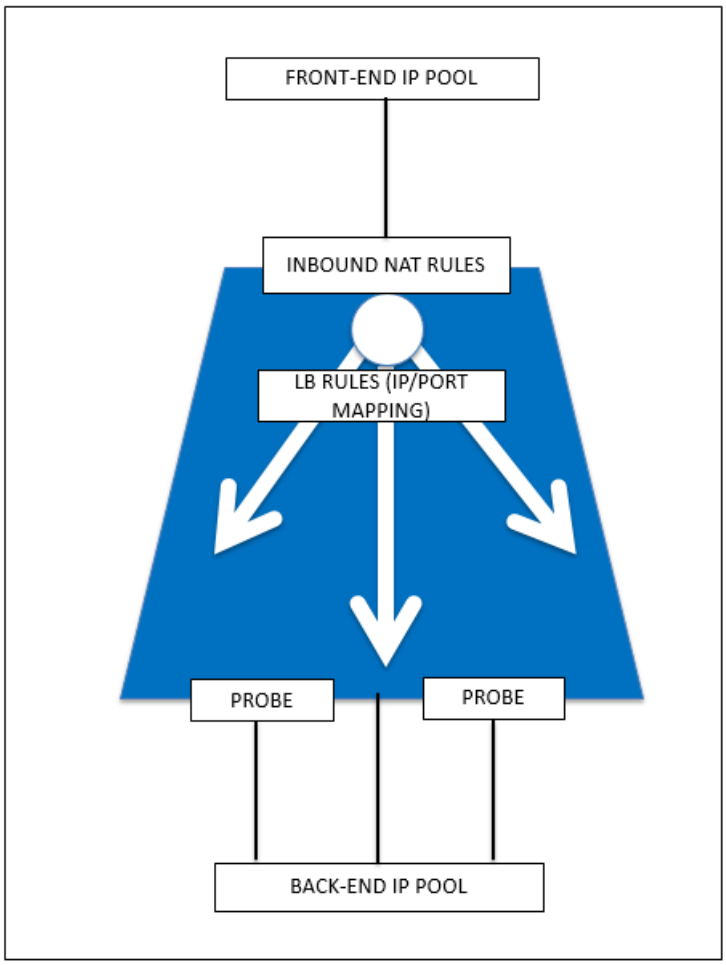
August 20, 2021

Certains des termes Azure utilisés dans la documentation Azure Citrix ADC VPX Azure sont répertoriés ci-dessous.

1. Azure Load Balancer — L'équilibreur de charge Azure est une ressource qui distribue le trafic entrant entre les ordinateurs d'un réseau. Le trafic est distribué entre les machines virtuelles définies dans un jeu d'équilibrage de charge. Un équilibreur de charge peut être externe ou connecté à Internet, ou il peut être interne.
2. Azure Resource Manager (ARM) — ARM est le nouveau cadre de gestion des services dans Azure. Azure Load Balancer est géré à l'aide d'API et d'outils ARM.
3. Pool d'adresses back-end : il s'agit d'adresses IP associées à la carte réseau (NIC) de la machine virtuelle vers laquelle la charge sera distribuée.
4. BLOB - Binary Large Object — Tout objet binaire tel qu'un fichier ou une image qui peut être stocké dans le stockage Azure.
5. Configuration IP front-end : un équilibreur de charge Azure peut inclure une ou plusieurs adresses IP front-end, également appelées adresses IP virtuelles (VIP). Ces adresses IP servent d'entrée pour le trafic.
6. IP publique de niveau instance (ILPIP) : un ILPIP est une adresse IP publique que vous pouvez attribuer directement à votre machine virtuelle ou instance de rôle, plutôt qu'au service cloud dans lequel réside votre machine virtuelle ou votre instance de rôle. Cela ne remplace pas le VIP (IP virtuelle) attribué à votre service cloud. Il s'agit plutôt d'une adresse IP supplémentaire que vous pouvez utiliser pour vous connecter directement à votre machine virtuelle ou instance de rôle.

   Note : Dans le passé, unILPIP était appelé PIP, qui signifie PI publique.
7. Règles NAT entrantes : contient des règles qui mappent un port public sur l'équilibreur de charge vers un port pour une machine virtuelle spécifique dans le pool d'adresses back-end.

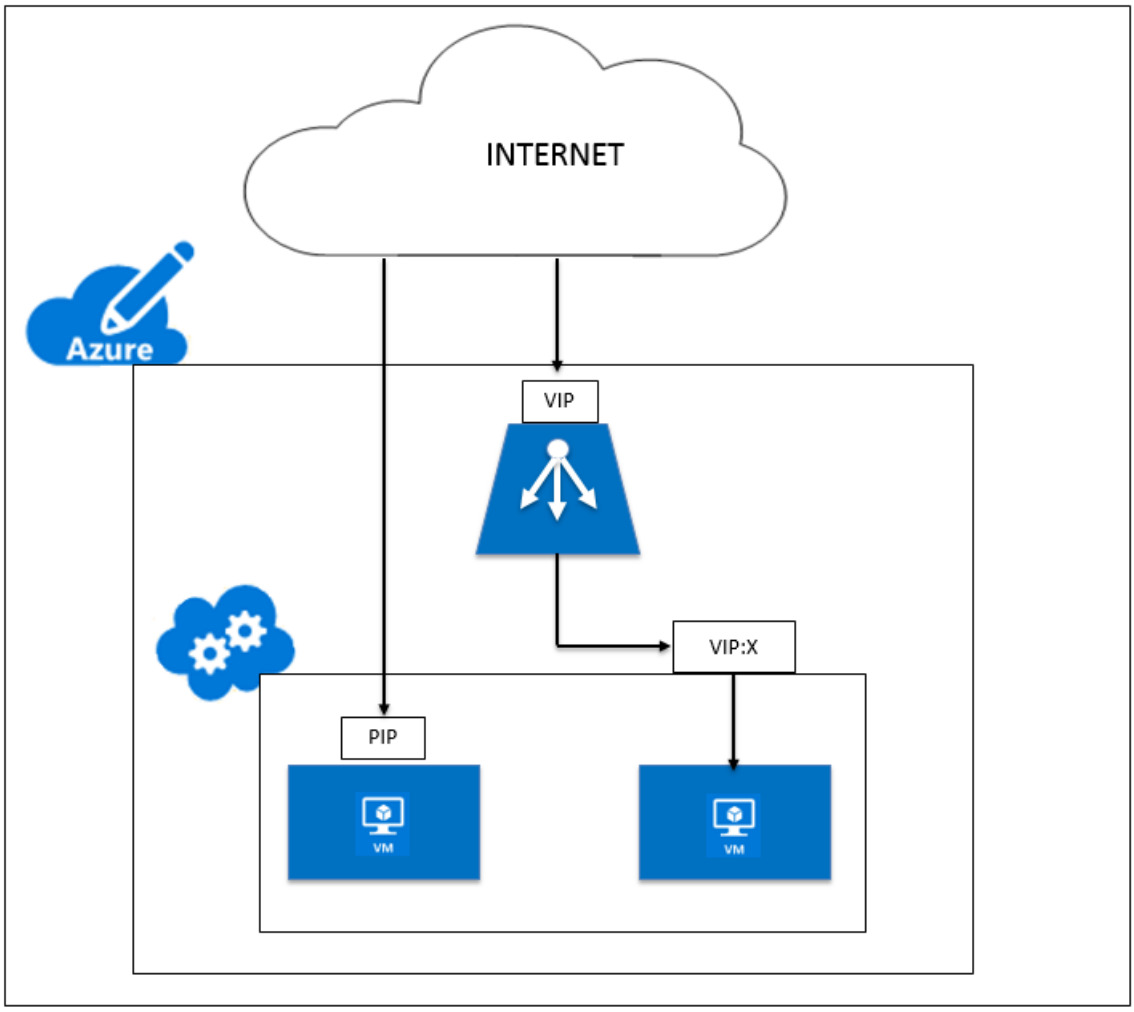
8. IP-Config - Il peut être défini comme une paire d'adresses IP (IP publique et IP privée) associée à une carte réseau individuelle. Dans une configuration IP, l'adresse IP publique peut être NULL. Chaque carte réseau peut être associée à plusieurs configurations IP, qui peuvent atteindre 255.
9. Règles d'équilibrage de charge : propriété de règle qui mappe une combinaison IP et port frontaux donnée à un ensemble d'adresses IP et de combinaisons de ports back-end. Avec une définition unique d'une ressource d'équilibrage de charge, vous pouvez définir plusieurs règles d'équilibrage de charge, chaque règle reflétant une combinaison d'une adresse IP et d'un port frontaux et d'une adresse IP et d'un port back-end associés à des machines virtuelles.



10. Groupe de sécurité réseau : contient une liste de règles de liste de contrôle d'accès (ACL) qui autorisent ou refusent le trafic réseau vers vos instances de machine virtuelle dans un réseau virtuel. Les NSG peuvent être associés à des sous-réseaux ou à des instances de machine virtuelle individuelles au sein de ce sous-réseau. Lorsqu'un groupe de sécurité réseau est associé à un sous-réseau, les règles ACL s'appliquent à toutes les instances de machines virtuelles de ce sous-réseau. En outre, le trafic vers une machine virtuelle individuelle peut être restreint davantage en associant un groupe de sécurité réseau directement à cette machine virtuelle.

11. Adresses IP privées — Utilisées pour la communication au sein d'un réseau virtuel Azure et de votre réseau local lorsque vous utilisez une Gateway VPN pour étendre votre réseau à Azure. Les adresses IP privées permettent aux ressources Azure de communiquer avec d'autres ressources dans un réseau virtuel ou un réseau local via une Gateway VPN ou un circuit ExpressRoute, sans utiliser d'adresse IP accessible par Internet. Dans le modèle de déploiement Azure Resource Manager, une adresse IP privée est associée aux types de ressources Azure suivants : machines virtuelles, équilibreurs de charge internes (ILB) et passerelles d'application.
12. Sondes : contient des sondes d'intégrité utilisées pour vérifier la disponibilité des instances de machines virtuelles dans le pool d'adresses back-end. Si une machine virtuelle particulière ne répond pas aux sondes d'intégrité pendant un certain temps, elle est retirée du service de trafic. Les sondes vous permettent de suivre l'état des instances virtuelles. Si une sonde d'intégrité échoue, l'instance virtuelle est automatiquement retirée de la rotation.
13. Adresses IP publiques (PIP) : PIP est utilisé pour la communication avec Internet, y compris les services publics Azure et est associé aux machines virtuelles, aux équilibreurs de charge connectés à Internet, aux passerelles VPN et aux passerelles d'application.
14. Région - Zone au sein d'une géographie qui ne franchit pas les frontières nationales et qui contient un ou plusieurs centres de données. Les tarifs, les services régionaux et les types d'offres sont exposés au niveau régional. Une région est généralement jumelée à une autre région, qui peut se trouver à plusieurs centaines de miles, pour former une paire régionale. Les paires régionales peuvent servir de mécanisme pour la reprise après sinistre et les scénarios de haute disponibilité. Aussi appelé généralement lieu.
15. Groupe de ressources : un conteneur dans le Gestionnaire de ressources contient les ressources associées pour une application. Le groupe de ressources peut inclure toutes les ressources d'une application, ou uniquement les ressources regroupées logiquement.
16. Compte de stockage : un compte de stockage Azure vous donne accès aux services blob, file d'attente, table et fichiers Azure dans Azure Storage. Votre compte de stockage fournit l'espace de noms unique pour vos objets de données de stockage Azure.
17. Machine virtuelle : implémentation logicielle d'un ordinateur physique qui exécute un système d'exploitation. Plusieurs machines virtuelles peuvent s'exécuter simultanément sur le même matériel. Dans Azure, les machines virtuelles sont disponibles dans une variété de tailles.
18. Réseau virtuel - Un réseau virtuel Azure est une représentation de votre propre réseau dans le cloud. Il s'agit d'un isolement logique du cloud Azure dédié à votre abonnement. Vous pouvez contrôler entièrement les blocs d'adresses IP, les paramètres DNS, les stratégies de sécurité et les tables de routage au sein de ce réseau. Vous pouvez également segmenter davantage votre réseau virtuel en sous-réseaux et lancer des machines virtuelles Azure IaaS et des services cloud (instances de rôle PaaS). En outre, vous pouvez connecter le réseau virtuel à votre réseau local à l'aide de l'une des options de connectivité disponibles dans Azure. Essentiellement, vous

pouvez étendre votre réseau à Azure, avec un contrôle complet sur les blocs d'adresses IP avec l'avantage d'Azure à l'échelle de l'entreprise.



Architecture réseau pour les instances Citrix ADC VPX sur Microsoft Azure

August 20, 2021

Dans Azure Resource Manager (ARM), une machine virtuelle Citrix ADC VPX réside dans un réseau virtuel. Une interface réseau unique peut être créée dans un sous-réseau donné du réseau virtuel et peut être attachée à l'instance VPX. Vous pouvez filtrer le trafic réseau vers et depuis une instance VPX dans un réseau virtuel Azure avec un groupe de sécurité réseau. Un groupe de sécurité réseau contient des règles de sécurité qui autorisent ou refusent le trafic réseau entrant vers ou le trafic réseau sortant à partir d'une instance VPX. Pour plus d'informations, voir Groupes de sécurité.

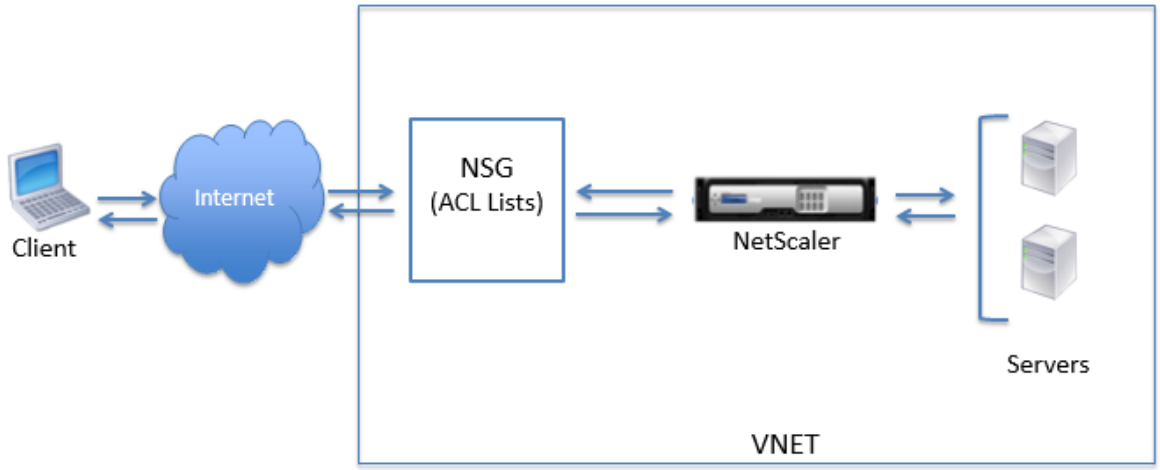
Le groupe de sécurité réseau filtre les demandes vers l'instance Citrix ADC VPX et l'instance VPX les envoie aux serveurs. La réponse d'un serveur suit le même chemin à l'envers. Le groupe de sécurité réseau peut être configuré pour filtrer une seule VM VPX ou, avec des sous-réseaux et des réseaux virtuels, peut filtrer le trafic lors du déploiement de plusieurs instances VPX.

La carte réseau contient des détails de configuration réseau tels que le réseau virtuel, les sous-réseaux, l'adresse IP interne et l'adresse IP publique.

Sur ARM, il est bon de connaître les adresses IP suivantes qui sont utilisées pour accéder aux machines virtuelles déployées avec une seule carte réseau et une seule adresse IP :

- L'adresse IP publique (PIP) est l'adresse IP connectée à Internet configurée directement sur la carte réseau virtuelle de la machine virtuelle NetScaler. Cela vous permet d'accéder directement à une machine virtuelle à partir du réseau externe.
- L'adresse IP Citrix ADC (également appelée NSIP) est l'adresse IP interne configurée sur la machine virtuelle. Il n'est pas routable.
- L'adresse IP virtuelle (VIP) est configurée à l'aide du NSIP et d'un numéro de port. Les clients accèdent aux services NetScaler via l'adresse PIP et lorsque la demande atteint la carte réseau de la machine virtuelle NetScaler VPX ou de l'équilibreur de charge Azure, le VIP est traduit en IP interne (NSIP) et en numéro de port interne.
- L'adresse IP interne est l'adresse IP interne privée de la machine virtuelle à partir du pool d'espace d'adressage du réseau virtuel. Cette adresse IP ne peut pas être atteinte à partir du réseau externe. Cette adresse IP est dynamique par défaut, sauf si vous la définissez sur statique. Le trafic d'Internet est acheminé vers cette adresse selon les règles créées sur le groupe de sécurité réseau. Le groupe de sécurité réseau s'intègre à la carte réseau pour envoyer de manière sélective le bon type de trafic vers le bon port de la carte réseau, qui dépend des services configurés sur la machine virtuelle.

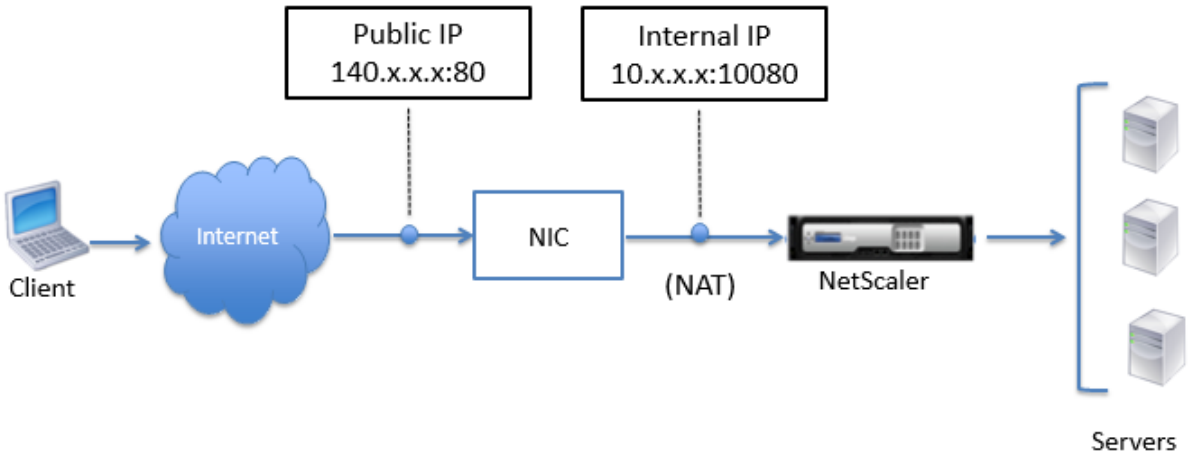
La figure suivante montre comment le trafic circule d'un client vers un serveur via une instance NetScaler VPX provisionnée dans ARM.



Flux de trafic via la traduction d'adresses réseau

Vous pouvez également demander une adresse IP publique (PIP) pour votre instance Citrix ADC VPX (niveau instance). Si vous utilisez ce PIP direct au niveau de la machine virtuelle, vous n'avez pas besoin de définir des règles entrantes et sortantes pour intercepter le trafic réseau. La demande entrante d'Internet est reçue directement sur la machine virtuelle. Azure effectue la traduction d'adresses réseau (NAT) et transfère le trafic à l'adresse IP interne de l'instance VPX.

La figure suivante montre comment Azure effectue la traduction d'adresses réseau pour mapper l'adresse IP interne NetScaler.



Dans cet exemple, l'adresse IP publique attribuée au groupe de sécurité réseau est 140.x.x.x et l'adresse IP interne est 10.x.x.x. Lorsque les règles entrantes et sortantes sont définies, le port HTTP public 80 est défini comme le port sur lequel les requêtes client sont reçues, et un port privé correspondant, 10080, est défini comme le port sur lequel l'instance Citrix ADC VPX écoute. La demande du client est reçue sur l'adresse IP publique (140.x.x). Azure effectue la traduction d'adresse réseau pour mapper le PIP à l'adresse IP interne 10.x.x.x sur le port 10080, et transmet la demande du client.

> **Remarque**
>
> Les machines virtuelles Citrix ADC VPX en haute disponibilité sont contrôlées par des équilibreurs de charge externes ou internes dont les règles entrantes sont définies pour contrôler le trafic d'équilibrage de charge. Le trafic externe est d'abord intercepté par ces équilibreurs de charge et le trafic est détourné selon les règles d'équilibrage de charge configurées, qui ont des pools back-end, des règles NAT et des sondes d'intégrité définies sur les équilibreurs de charge.

Instructions relatives à l'utilisation des ports

Vous pouvez configurer davantage de règles entrantes et sortantes dans un groupe de sécurité réseau lors de la création de l'instance Citrix ADC VPX ou après le provisionnement de la machine virtuelle. Chaque règle entrante et sortante est associée à un port public et à un port privé.

Avant de configurer les règles de groupe de sécurité réseau, notez les instructions suivantes concernant les numéros de port que vous pouvez utiliser :

1. L'instance Citrix ADC VPX réserve les ports suivants. Vous ne pouvez pas les définir en tant que ports privés lors de l'utilisation de l'adresse IP publique pour les demandes provenant d'Internet.

   Ports 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

   Toutefois, si vous souhaitez que les services Internet tels que le VIP utilisent un port standard (par exemple, le port 443), vous devez créer un mappage de ports à l'aide du groupe de sécurité réseau. Le port standard est ensuite mappé à un autre port configuré sur NetScaler pour ce service VIP.

   Par exemple, un service VIP peut s'exécuter sur le port 8443 sur l'instance VPX mais être mappé sur le port public 443. Ainsi, lorsque l'utilisateur accède au port 443 via l'IP publique, la requête est dirigée vers le port privé 8443.

2. L'adresse IP publique ne prend pas en charge les protocoles dans lesquels le mappage de ports est ouvert dynamiquement, tels que FTP passif ou ALG.
3. La haute disponibilité ne fonctionne pas pour le trafic qui utilise une adresse IP publique (PIP) associée à une instance VPX, au lieu d'un PIP configuré sur l'équilibreur de charge Azure.

> **Remarque**
>
> Dans Azure Resource Manager, une instance Citrix ADC VPX est associée à deux adresses IP : une adresse IP publique (PIP) et une adresse IP interne. Pendant que le trafic externe se connecte au PIP, l'adresse IP interne ou le NSIP n'est pas routable. Pour configurer VIP dans VPX, utilisez l'adresse IP interne et l'un des ports libres disponibles. N'utilisez pas le PIP pour configurer VIP.

Configurer une instance autonome Citrix ADC VPX

August 20, 2021

Vous pouvez provisionner une seule instance Citrix ADC VPX dans le portail ARM (Azure Resource Manager) en mode autonome en créant la machine virtuelle et en configurant d'autres ressources.

Avant de commencer

Assurez-vous que vous disposez des éléments suivants :

- Un compte d'utilisateur Microsoft Azure
- Accès au Gestionnaire de ressources Microsoft Azure
- Kit de développement logiciel (SDK) Microsoft Azure
- Microsoft Azure PowerShell

Sur la page Microsoft Azure Portal, connectez-vous au portail Azure Resource Manager en fournissant votre nom d'utilisateur et votre mot de passe.

> **Remarque**
>
> Dans le portail ARM, le fait de cliquer sur une option dans un volet ouvre un nouveau volet vers la droite. Naviguez d'un volet à l'autre pour configurer votre appareil.

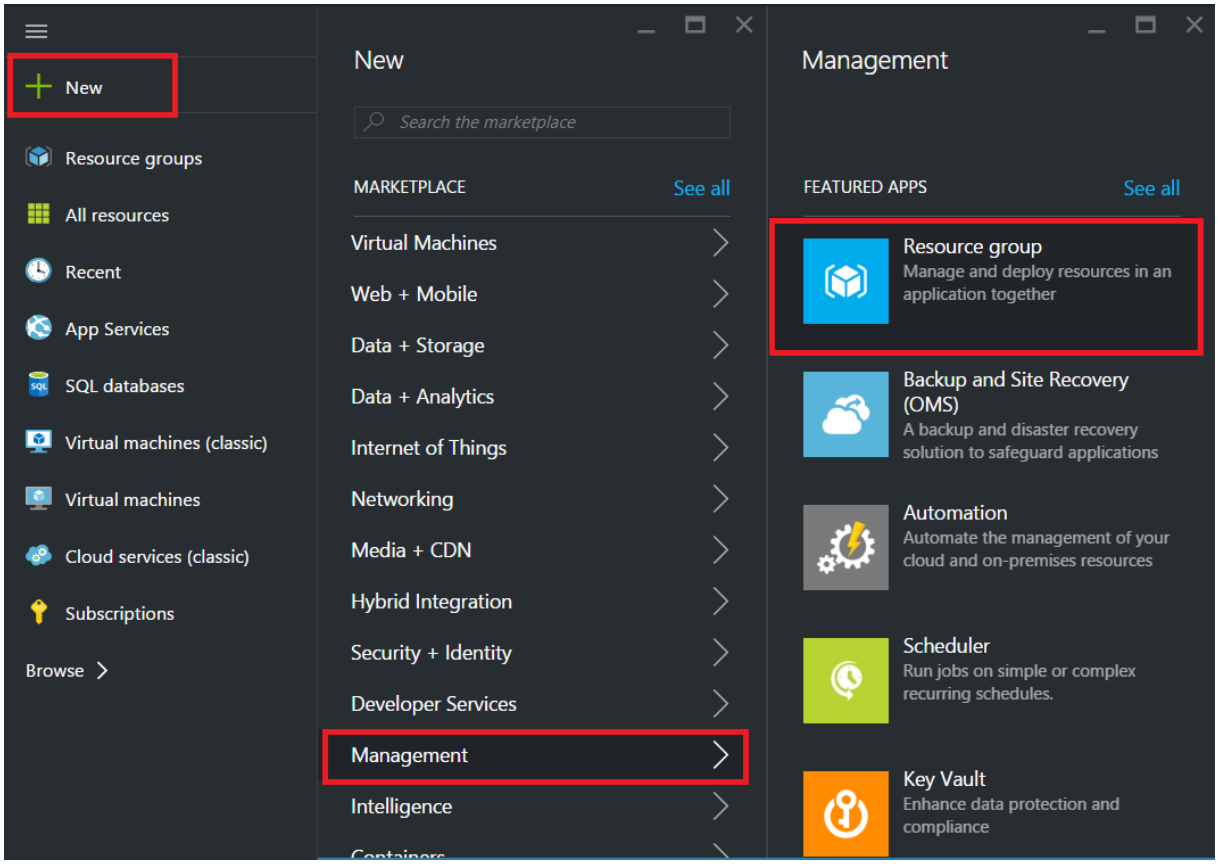
Résumé des étapes de configuration

1. Configurer un groupe de ressources
2. Configurer un groupe de sécurité réseau
3. Configurer le réseau virtuel et ses sous-réseaux
4. Configurer un compte de stockage
5. Configurer un jeu de disponibilité
6. Configurez une instance Citrix ADC VPX.

Configurer un groupe de ressources

Créez un nouveau groupe de ressources qui est un conteneur pour toutes vos ressources. Utilisez le groupe de ressources pour déployer, gérer et surveiller vos ressources en tant que groupe.

1. Cliquez sur **Nouveau** > **Gestion** > **Groupe de ressources** .
2. Dans le volet **Groupe de ressources**, entrez les détails suivants :
   - Nom du groupe de ressources
   - Emplacement du groupe de ressources
3. Cliquez sur **Créer**.

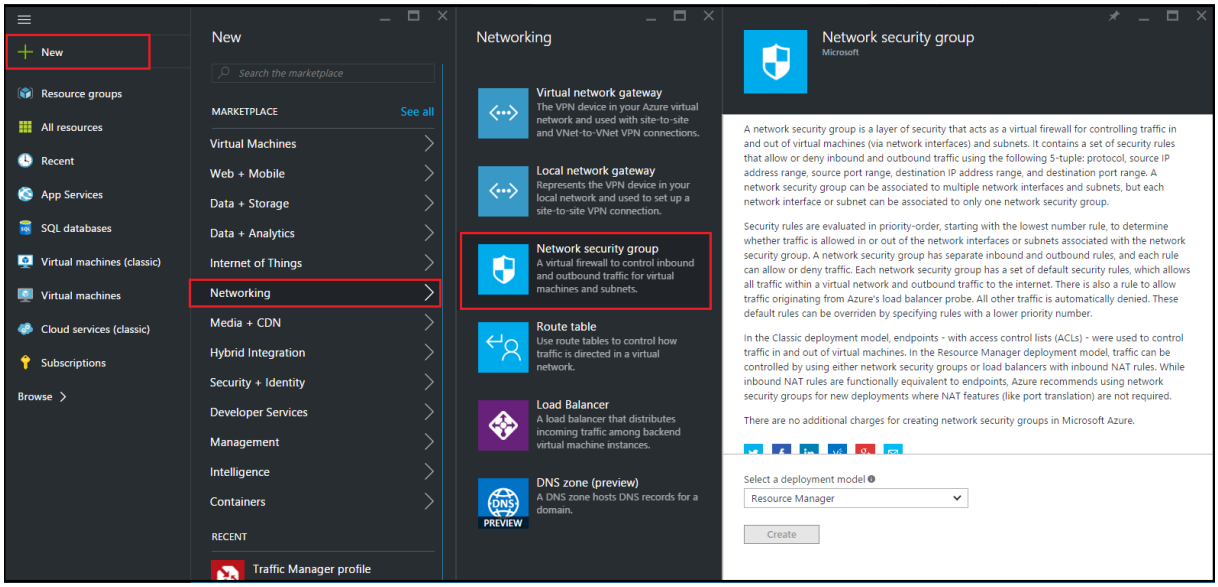


Configurer un groupe de sécurité réseau

Créez un groupe de sécurité réseau pour affecter des règles entrantes et sortantes pour contrôler le trafic entrant et sortant au sein du réseau virtuel. Le groupe de sécurité réseau vous permet de définir des règles de sécurité pour une seule machine virtuelle et de définir des règles de sécurité pour un sous-réseau virtuel.

1. Cliquez sur **Nouveau** > **Mise enréseau > Groupe de sécurité réseau** .
2. Dans le volet **Créer un groupe de sécurité réseau**, entrez les détails suivants, puis cliquez sur **Créer**.
    - Nom : saisissez un nom pour le groupe de sécurité
    - Groupe de ressources : sélectionnez le groupe de ressources dans la liste déroulante

> **Remarque**
>
> Vérifiez que vous avez sélectionné l'emplacement correct. La liste des ressources qui apparaissent dans la liste déroulante est différente selon les emplacements.

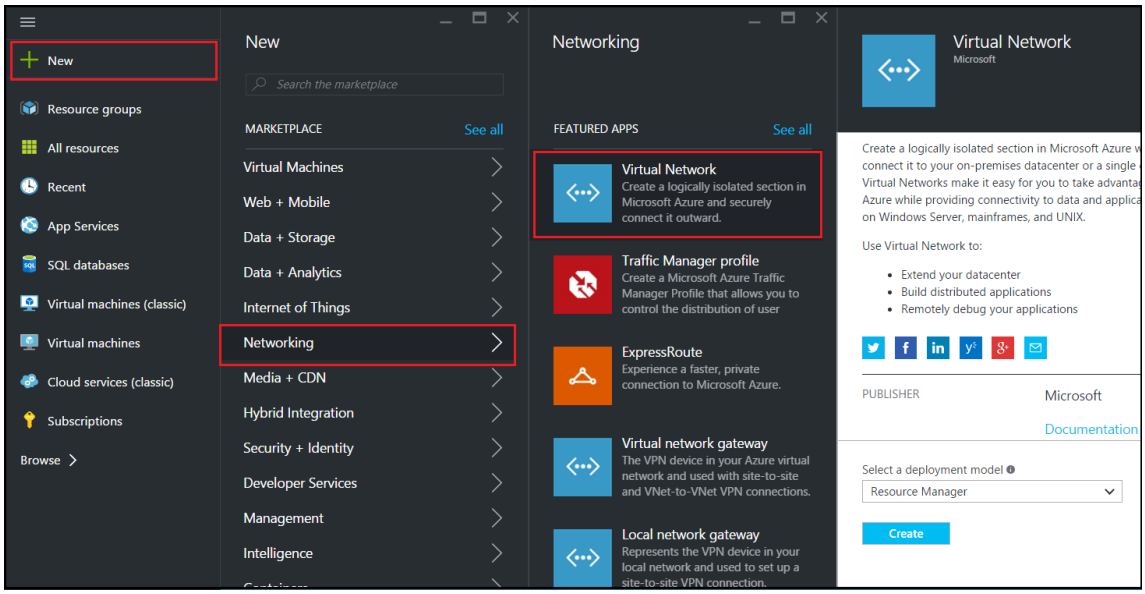


Configurer un réseau virtuel et des sous-réseaux

Les réseaux virtuels dans ARM fournissent une couche de sécurité et d'isolement à vos services. Les machines virtuelles et les services qui font partie d'un même réseau virtuel peuvent accéder les uns aux autres.

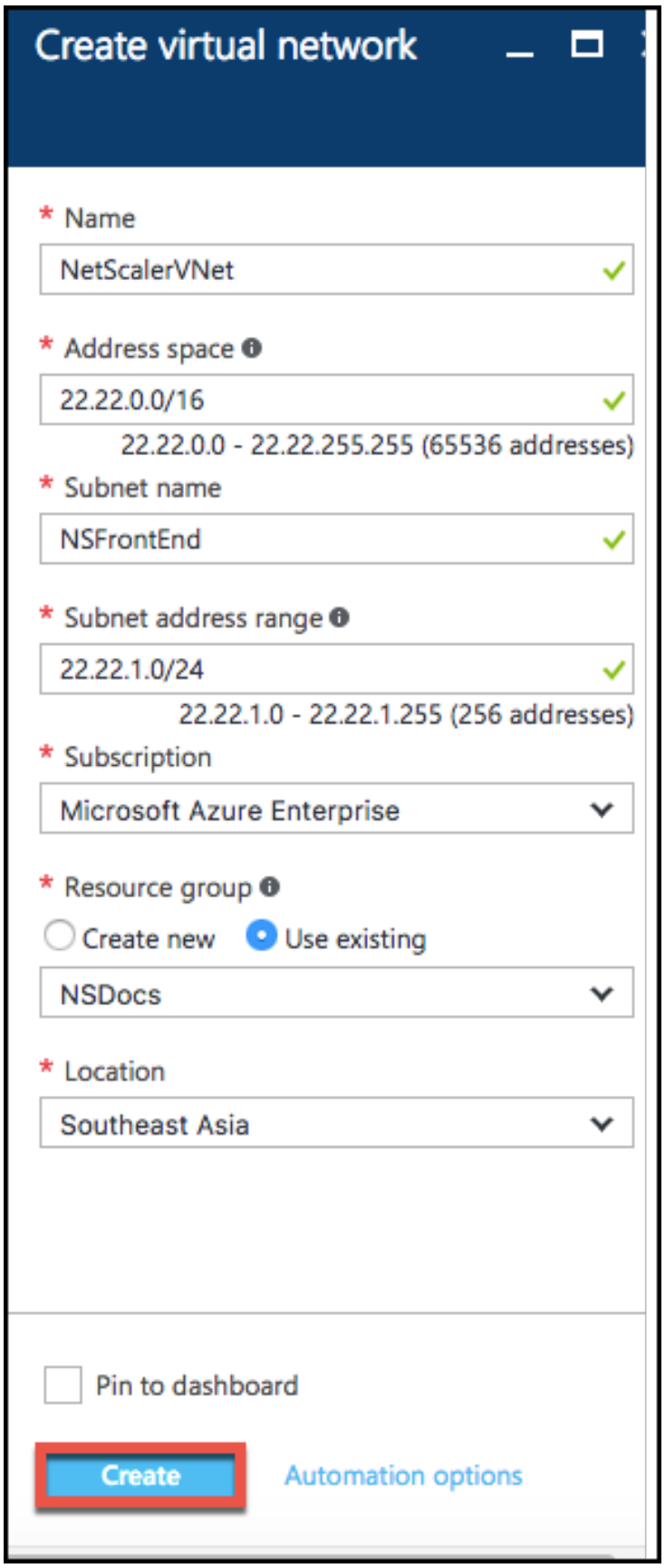
Pour ces étapes pour créer un réseau virtuel et des sous-réseaux.

1. Cliquez sur **Nouveau** > **Mise en réseau** > **Réseau virtuel** .
2. Dans le volet **Réseau virtuel**, assurez-vous que le mode de déploiement est **Gestionnaire de ressources** et cliquez sur **Créer**.



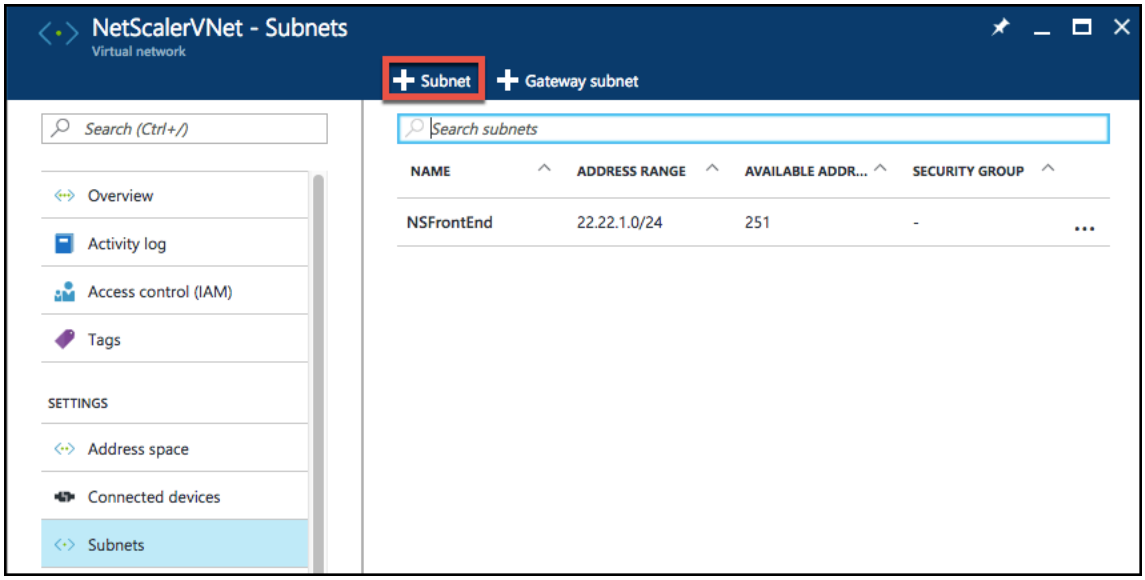
3. Dans le volet **Créer un réseau virtuel**, entrez les valeurs suivantes, puis cliquez sur **Créer** .

- Nom du réseau virtuel
- Espace d'adressage - tapez le bloc d'adresse IP réservé pour le réseau virtuel
- Sous-réseau - tapez le nom du premier sous-réseau (vous créez le second sous-réseau plus tard dans cette étape)
- Plage d'adresses de sous-réseau - tapez le bloc d'adresse IP réservé du sous-réseau
- Groupe de ressources : sélectionnez le groupe de ressources créé précédemment dans la liste déroulante

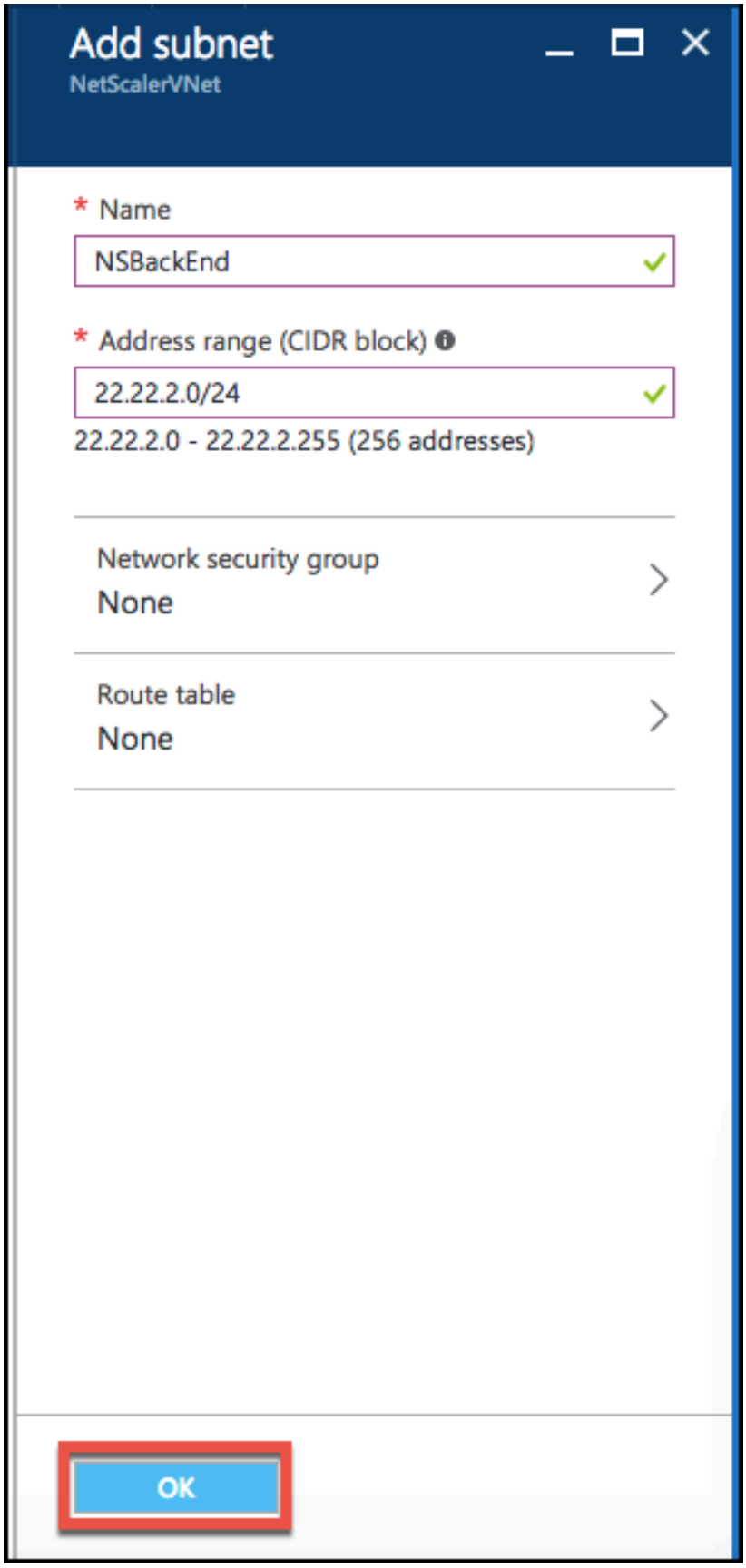


Configurer le deuxième sous-réseau

1. Sélectionnez le réseau virtuel nouvellement créé dans le volet **Toutes les ressources** et dans le volet **Paramètres**, cliquez sur **Sous-réseaux** .



2. Cliquez sur **+ Sous-réseau** et créez le second sous-réseau en entrant les détails suivants.
   - Nom du deuxième sous-réseau
   - Plage d'adresses - tapez le bloc d'adresse IP réservé du deuxième sous-réseau
   - Groupe de sécurité réseau : sélectionnez le groupe de sécurité réseau dans la liste déroulante.
3. Cliquez sur **Créer**.

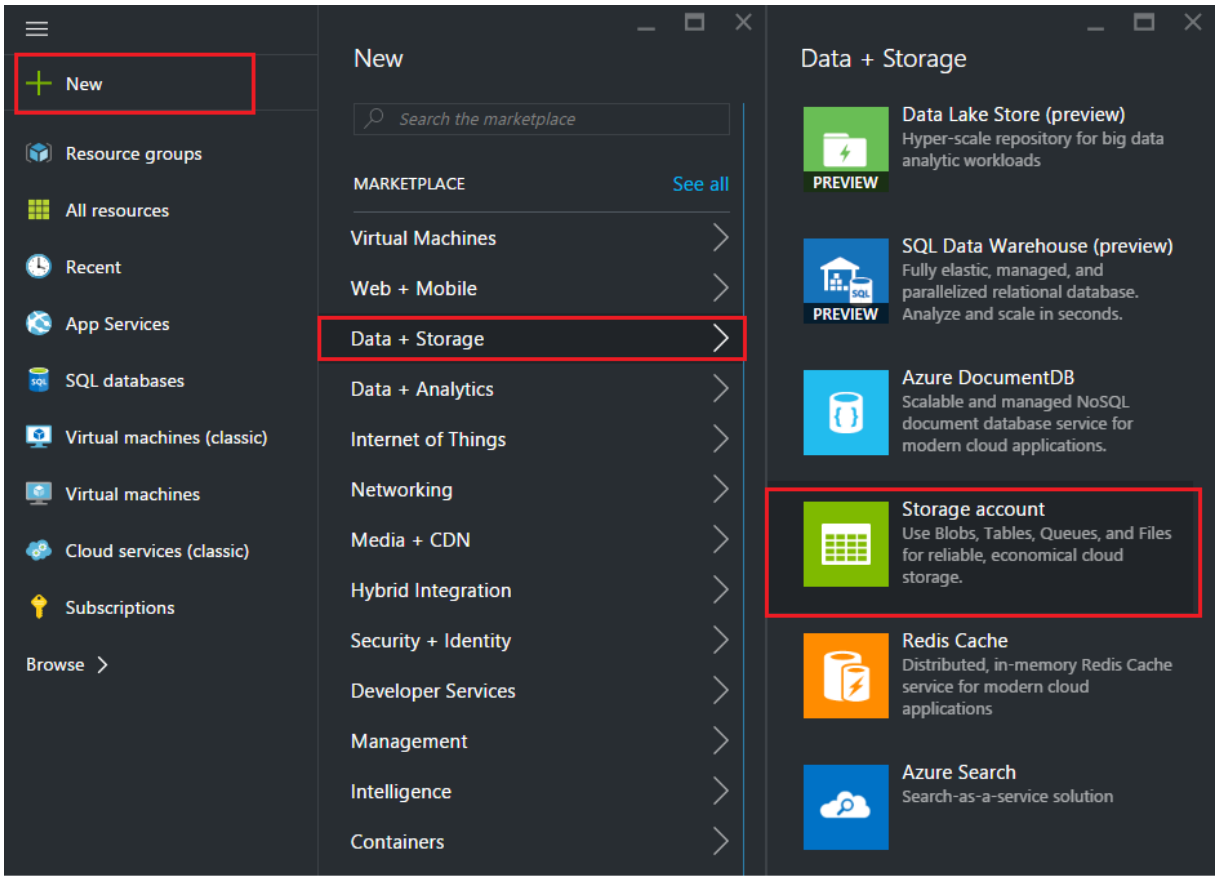


Configurer un compte de stockage

Le stockage de l'infrastructure ARM IaaS inclut tous les services où nous pouvons stocker des données sous forme de blobs, de tables, de files d'attente et de fichiers. Vous pouvez également créer des applications à l'aide de ces formes de données de stockage dans ARM.

Créez un compte de stockage pour stocker toutes vos données.

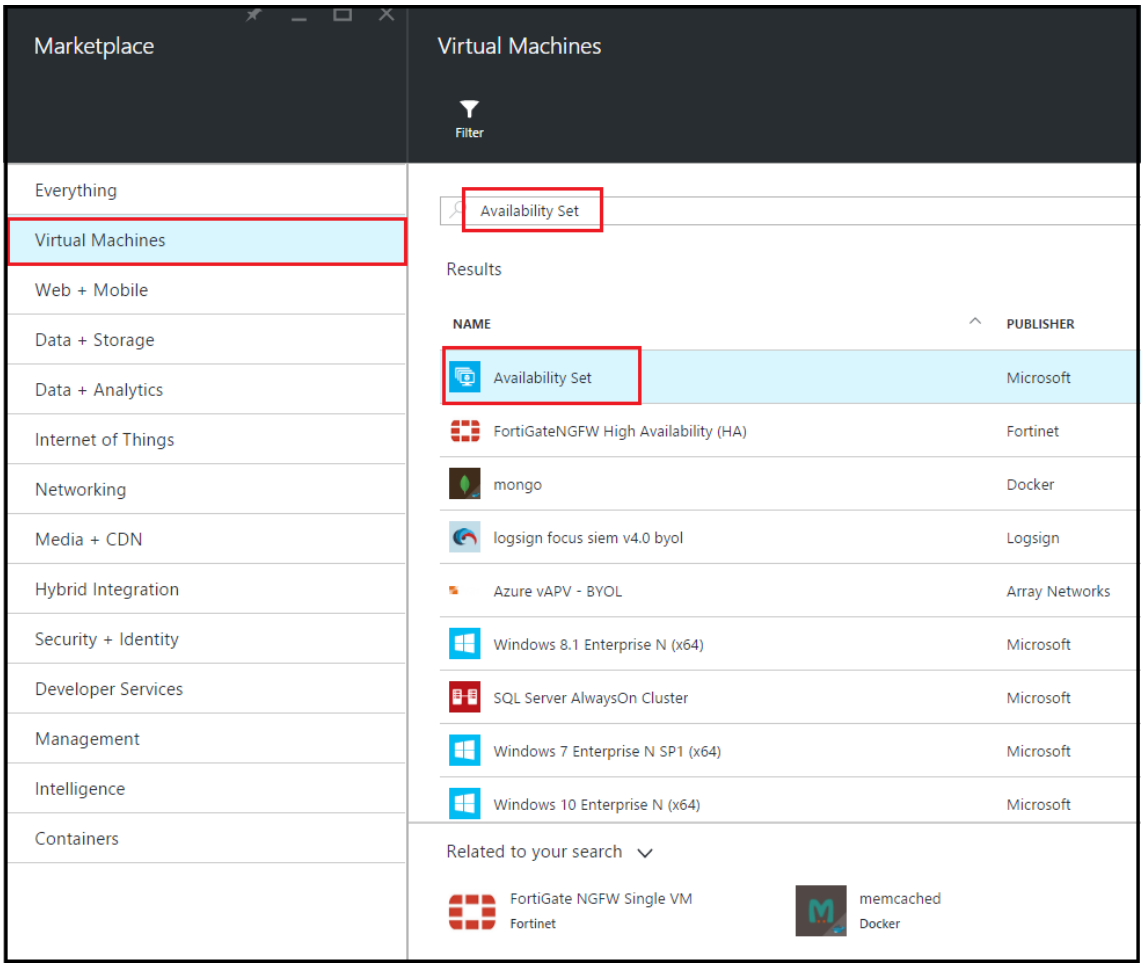
1. Cliquez sur **+Nouveau** > **Données + Stockage** > **Compte de stockage** .
2. Dans le volet **Créer un compte de stockage**, entrez les détails suivants :
    - Nom du compte
    - Mode de déploiement - assurez-vous de sélectionner **Gestionnaire de ressources**
    - Type de compte - sélectionnez **Usage général** dans la liste déroulante
    - Réplication : sélectionnez **Stockage redondant localement** dans la liste déroulante
    - Groupe de ressources : sélectionnez le groupe de ressources nouvellement créé dans la liste déroulante
3. Cliquez sur **Créer**.



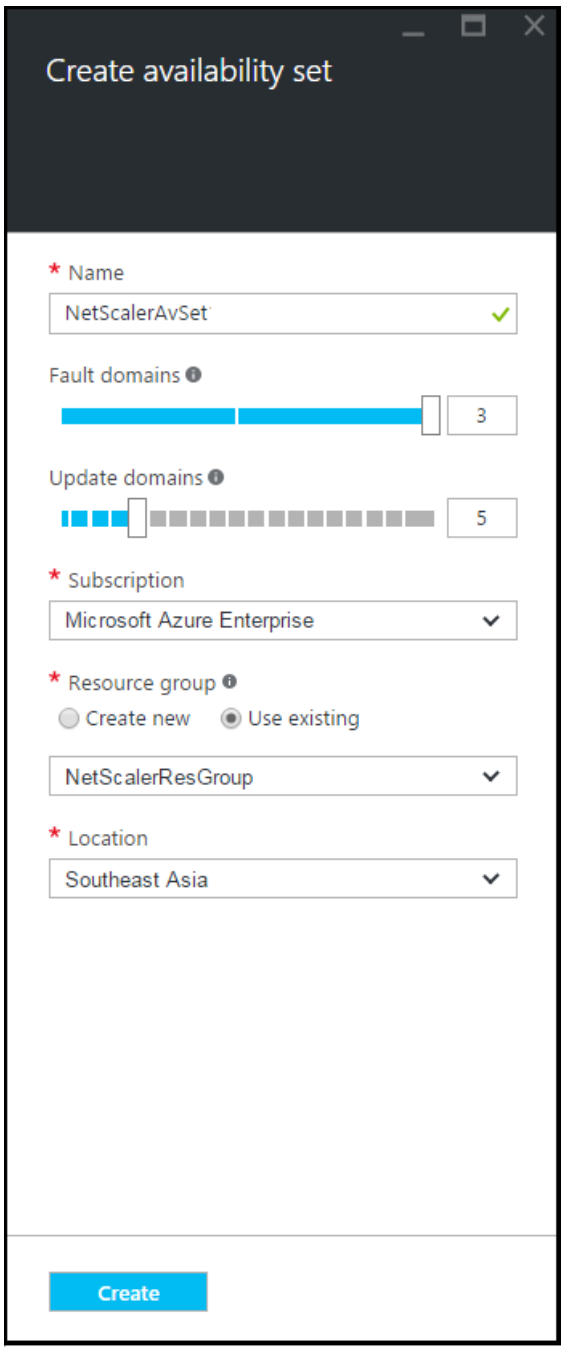
Configurer un jeu de disponibilité

Un jeu de disponibilité garantit qu'au moins une machine virtuelle est maintenue en fonctionnement en cas de maintenance planifiée ou non planifiée. Deux machines virtuelles ou plus sous le même « jeu de disponibilité » sont placées sur différents domaines de panne pour obtenir des services redondants.

1. Cliquez sur **+Nouveau**.
2. Cliquez sur **Voir tout** dans le volet MARKETPLACE et cliquez sur **Machines virtuelles**.
3. Recherchez le jeu de disponibilité, puis sélectionnez Entité de **jeu de disponibilité** dans la liste affichée.



4. Cliquez sur **Créer et,** dans le volet **Créer un jeu de disponibilité**, entrez les détails suivants :
   - Nom de l'ensemble
   - Groupe de ressources : sélectionnez le groupe de ressources nouvellement créé dans la liste déroulante
5. Cliquez sur **Créer**.



Configurer une instance Citrix ADC VPX

Créez une instance de Citrix ADC VPX dans le réseau virtuel. Obtenez l'image Citrix ADC VPX à partir de la Place de marché Azure, puis utilisez le portail Azure Resource Manager pour créer une instance Citrix ADC VPX.

Avant de commencer à créer l'instance Citrix ADC VPX, assurez-vous que vous avez créé un réseau virtuel avec les sous-réseaux requis dans lesquels l'instance réside. Vous pouvez créer des réseaux

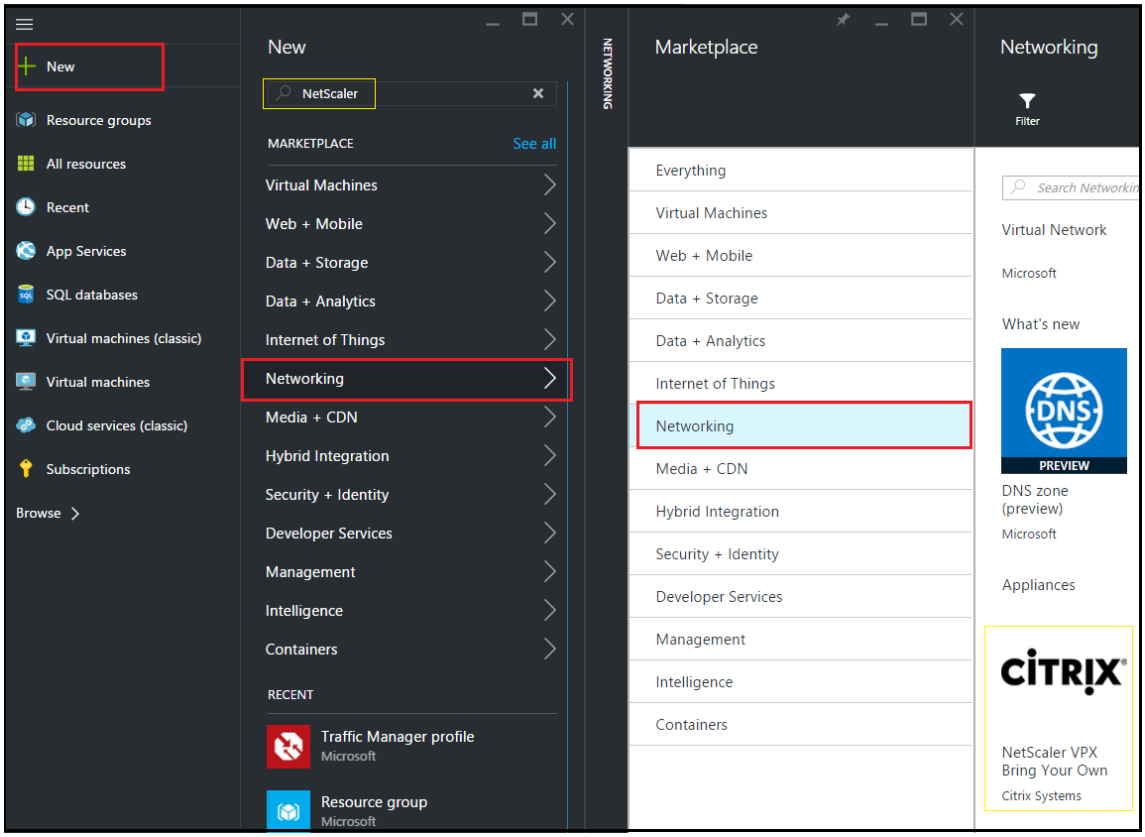
virtuels pendant le provisioning de machines virtuelles, mais sans la possibilité de créer différents sous-réseaux. Pour plus d'informations sur la création de réseaux virtuels, reportez-vous à la sectionhttp://azure.microsoft.com/en-us/documentation/articles/create-virtual-network/.

Vous pouvez également configurer le serveur DNS et la connectivité VPN qui permet à une machine virtuelle d'accéder aux ressources Internet.

> **Remarque**
>
> Citrix vous recommande de créer un groupe de ressources, un groupe de sécurité réseau, un réseau virtuel et d'autres entités avant de provisionner la VM Citrix ADC VPX, afin que les informations réseau soient disponibles pendant le Provisioning.

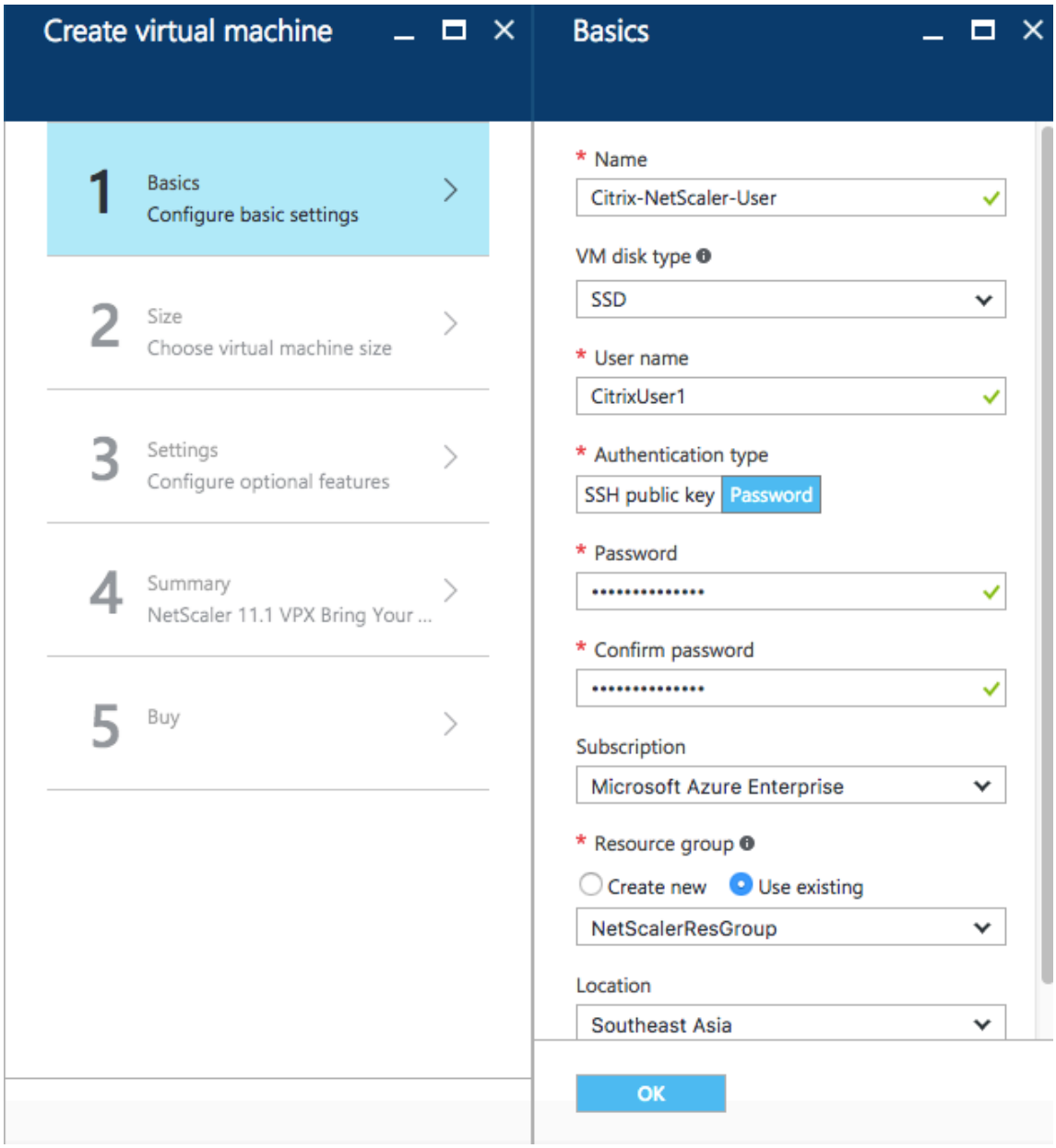
1. Cliquez sur **+Nouveau** > **Mise en réseau** .
2. Cliquez sur **Voir tout** et dans le volet Mise en réseau, cliquez sur **Citrix ADC 13.0**.
3. Sélectionnez **Citrix ADC 13.0 VPX Bring Your Own License** dans la liste des plans logiciels.

   Pour trouver rapidement une entité sur le portail ARM, vous pouvez également taper le nom de l'entité dans la zone de recherche Marketplace Azure et appuyer sur <Enter>. Tapez NetScaler dans la zone de recherche pour rechercher les images Citrix NetScaler.



> **Remarque**
>
> Assurez-vous de sélectionner la dernière image. Votre image Citrix NetScaler peut avoir le numéro de version dans le nom.

4. Sur la page **Citrix ADC VPX Bring Your Own License**, dans la liste déroulante, sélectionnez **Gestionnaire de ressources** et cliquez sur **Créer** .



5. Dans le volet **Créer une machine virtuelle**, spécifiez les valeurs requises dans chaque section pour créer une machine virtuelle. Cliquez sur **OK** dans chaque section pour enregistrer votre configuration.

Base :

- Nom : spécifiez un nom pour l'instance Citrix ADC VPX
- Type de disque de machine virtuelle - sélectionnez SSD (valeur par défaut) ou HDD dans le menu déroulant
- Nom d'utilisateur et mot de passe : spécifiez un nom d'utilisateur et un mot de passe pour accéder aux ressources du groupe de ressources que vous avez créé
- Type d'authentification - sélectionnez SSH Public Key ou Mot de passe
- Groupe de ressources : sélectionnez le groupe de ressources que vous avez créé dans la liste déroulante

Vous pouvez créer un groupe de ressources ici, mais Citrix vous recommande de créer un groupe de ressources à partir de groupes de ressources dans Azure Resource Manager, puis de sélectionner le groupe dans la liste déroulante.

> **Remarque**
>
> Dans un environnement de pile Azure, en plus des paramètres de base, spécifiez les paramètres suivants :
>
> - Domaine de pile Azure
> - Locataire de pile Azure (facultatif)
> - Client Azure (facultatif)
> - Secret client Azure (facultatif)

Taille :

Selon le type de disque de la machine virtuelle, le SDD ou le disque dur, que vous avez sélectionné dans Paramètres de base, les tailles de disque sont affichées.

- Sélectionnez une taille de disque en fonction de vos besoins et cliquez sur **Sélectionner**.

Paramètres :

- Sélectionnez le type de disque par défaut (Standard)
- Compte de stockage - sélectionnez le compte de stockage
- Réseau virtuel - sélectionnez le réseau virtuel
- Sous-réseau - définir l'adresse du sous-réseau
- Adresse IP publique - sélectionnez le type d'attribution d'adresse IP
- Groupe de sécurité réseau : sélectionnez le groupe de sécurité que vous avez créé. Assurez-vous que les règles entrantes et sortantes sont configurées dans le groupe de sécurité.
- Jeu de disponibilité - sélectionnez le jeu de disponibilité dans la boîte de menu déroulant

Résumé :

Les paramètres de configuration sont validés et la page Résumé affiche le résultat de la validation. Si la validation échoue, la page Résumé affiche la raison de l'échec. Retournez à la section particulière et apportez les modifications nécessaires. Si la validation réussit, cliquez sur **OK**.

Acheter :

Consultez les détails de l'offre et les conditions légales sur la page Achat, puis cliquez sur **Achat**.

Pour un déploiement à haute disponibilité, créez deux instances indépendantes de Citrix ADC VPX dans le même jeu de disponibilité et dans le même groupe de ressources pour les déployer dans une configuration active en veille.

Configurer plusieurs adresses IP pour une instance autonome Citrix ADC VPX

August 20, 2021

Cette section explique comment configurer une instance Citrix ADC VPX autonome avec plusieurs adresses IP, dans le Azure Resource Manager (ARM). Une ou plusieurs cartes réseau peuvent être attachées à l'instance VPX, et chaque carte réseau peut avoir une ou plusieurs adresses IP publiques et privées statiques ou dynamiques qui lui sont attribuées. Vous pouvez attribuer plusieurs adresses IP en tant que NSIP, VIP, SNIP, etc.

Pour plus d'informations, consultez la documentation Azure Attribuer plusieurs adresses IP à des machines virtuelles à l'aide du portail Azure.

Si vous souhaitez utiliser des commandes PowerShell, reportez-vous à la section Configuration de plusieurs adresses IP pour une instance Citrix ADC VPX en mode autonome à l'aide des commandes PowerShell.

Cas d'utilisation

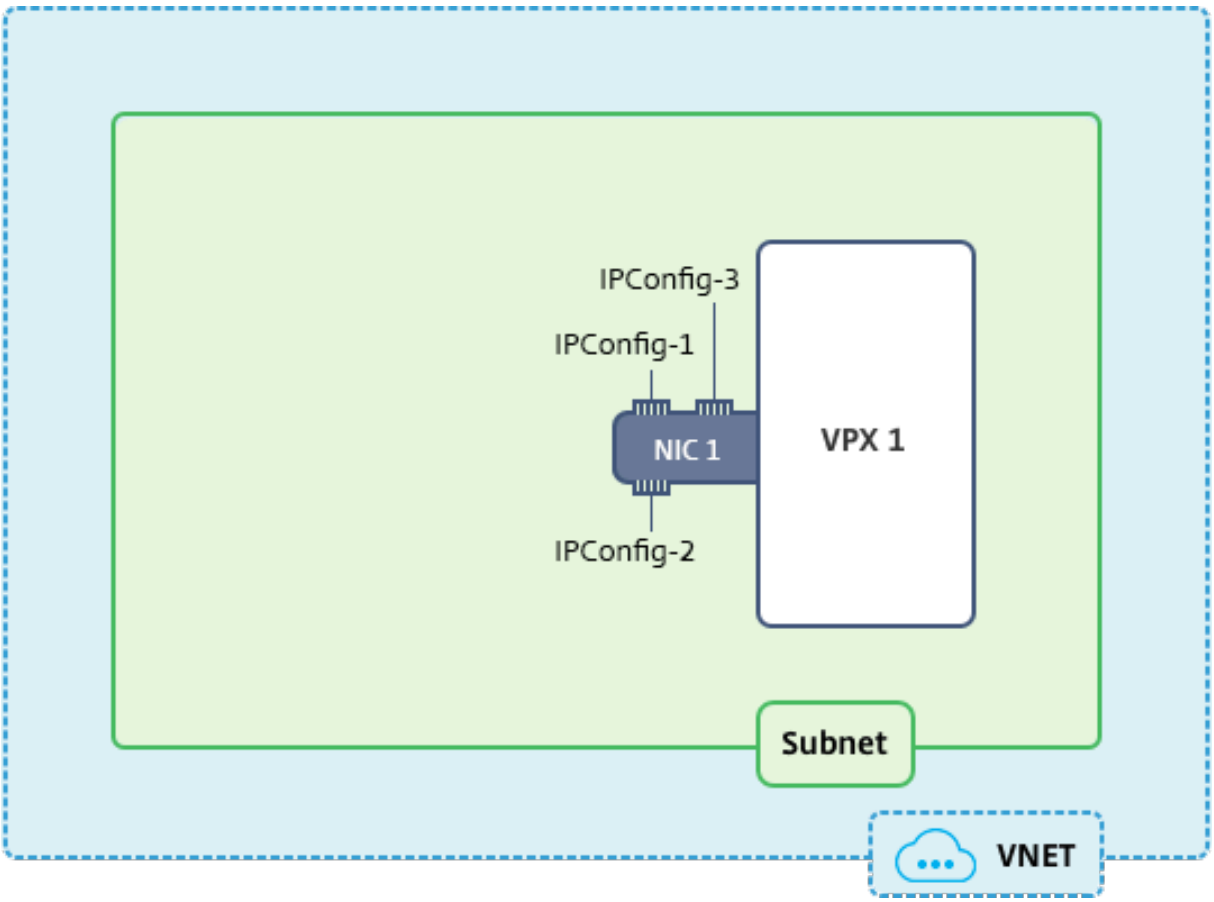
Dans ce cas d'utilisation, une appliance Citrix ADC VPX autonome est configurée avec une seule carte réseau connectée à un réseau virtuel (VNET). La carte réseau est associée à trois configurations IP (ipconfig), chaque serveur ayant une fonction différente, comme le montre le tableau.

Configuration IP	Associé à	Objectif
ipconfig1	Adresse IP publique statique ; adresse IP privée statique	Sert le trafic de gestion
ipconfig2	Adresse IP publique statique ; adresse privée statique	Sert le trafic côté client
ipconfig3	Adresse IP privée statique	Communication avec les serveurs back-end

> **Remarque**
>
> `IPConfig-3` n'est associé à aucune adresse IP publique.

Diagramme : Topologie

Voici la représentation visuelle du cas d'utilisation.



> **Remarque**
>
> Dans un déploiement Azure Citrix ADC VPX multi-NIC et multi-IP, l'adresse IP privée associée à la (première) principale (première) `IPConfig` carte réseau principale (première) est automatiquement ajoutée en tant que NSIP de gestion de l'appliance. Les adresses IP privées restantes associées `IPConfigs` doivent être ajoutées dans l'instance VPX en tant que VIP ou SNIP à l'aide de la `add ns ip` commande, selon vos besoins.

Avant de commencer

Avant de commencer, créez une instance VPX en suivant les étapes indiquées sur ce lien :

Configurer une instance autonome Citrix ADC VPX

Dans ce cas d'utilisation, l'instance VPX NSDoc0330vm est créée.

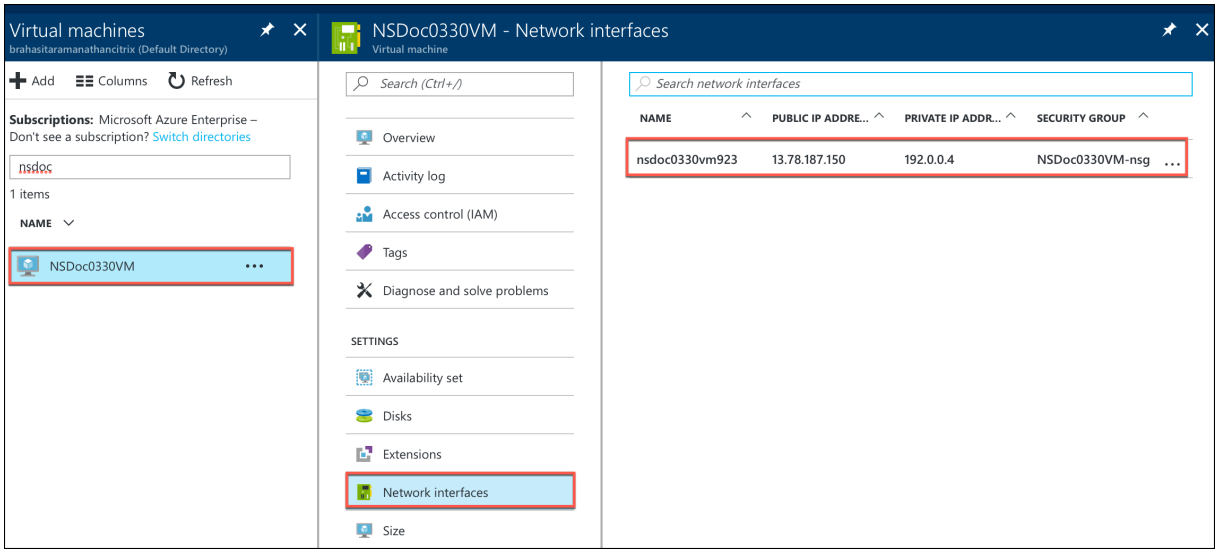
Procédure permettant de configurer plusieurs adresses IP pour une instance Citrix ADC VPX en mode autonome.

Pour configurer plusieurs adresses IP pour un dispositif Citrix ADC VPX en mode autonome :

1. Ajouter des adresses IP à la machine virtuelle
2. Configurer les adresses IP appartenant à Citrix ADC

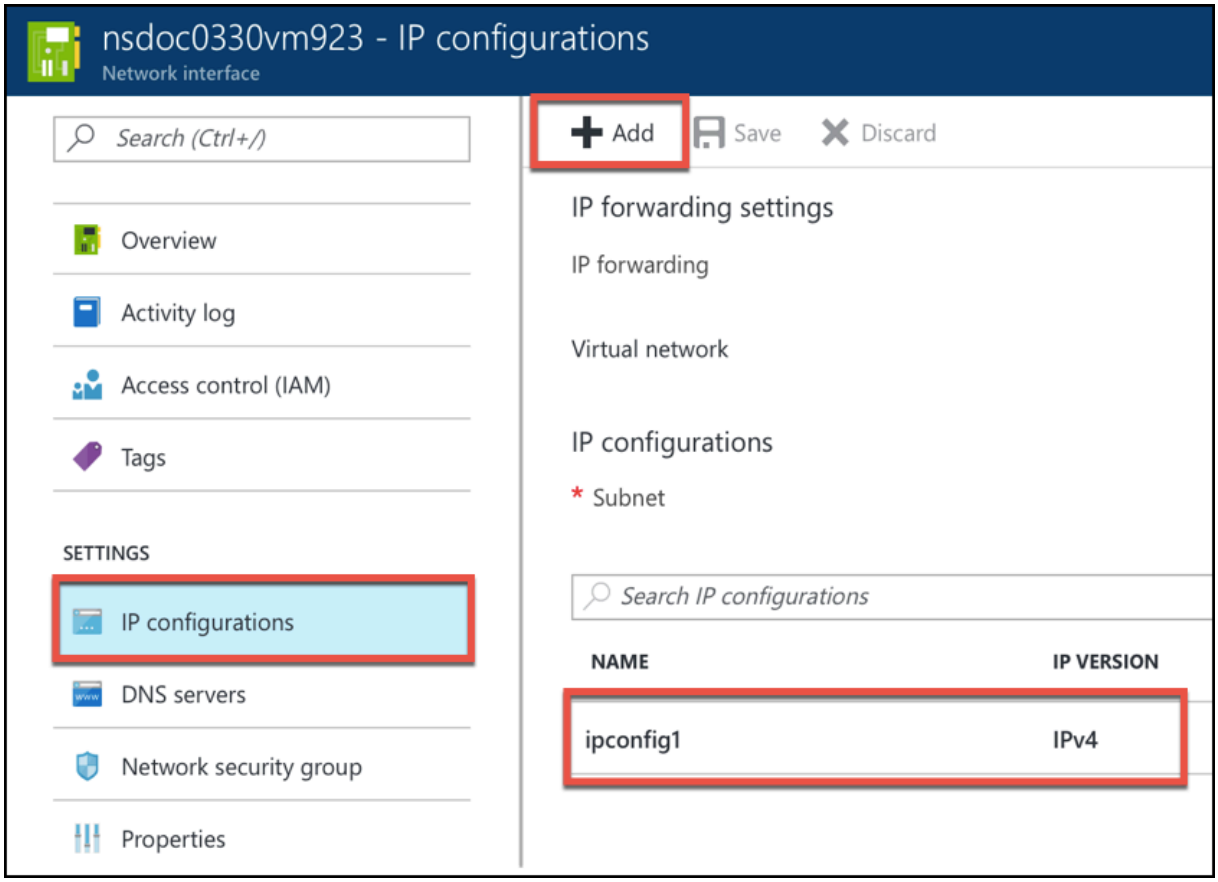
Étape 1 : Ajouter des adresses IP à la machine virtuelle

1. Dans le portail, cliquez sur **Autres services > tapez machines virtuelles** dans la zone de filtre, puis cliquez sur **Machines virtuelles** .
2. Dans la lame **Machines virtuelles**, cliquez sur la machine virtuelle à laquelle vous souhaitez ajouter des adresses IP. Cliquez sur **Interfaces réseau** dans la lame de machine virtuelle qui apparaît, puis sélectionnez l'interface réseau.



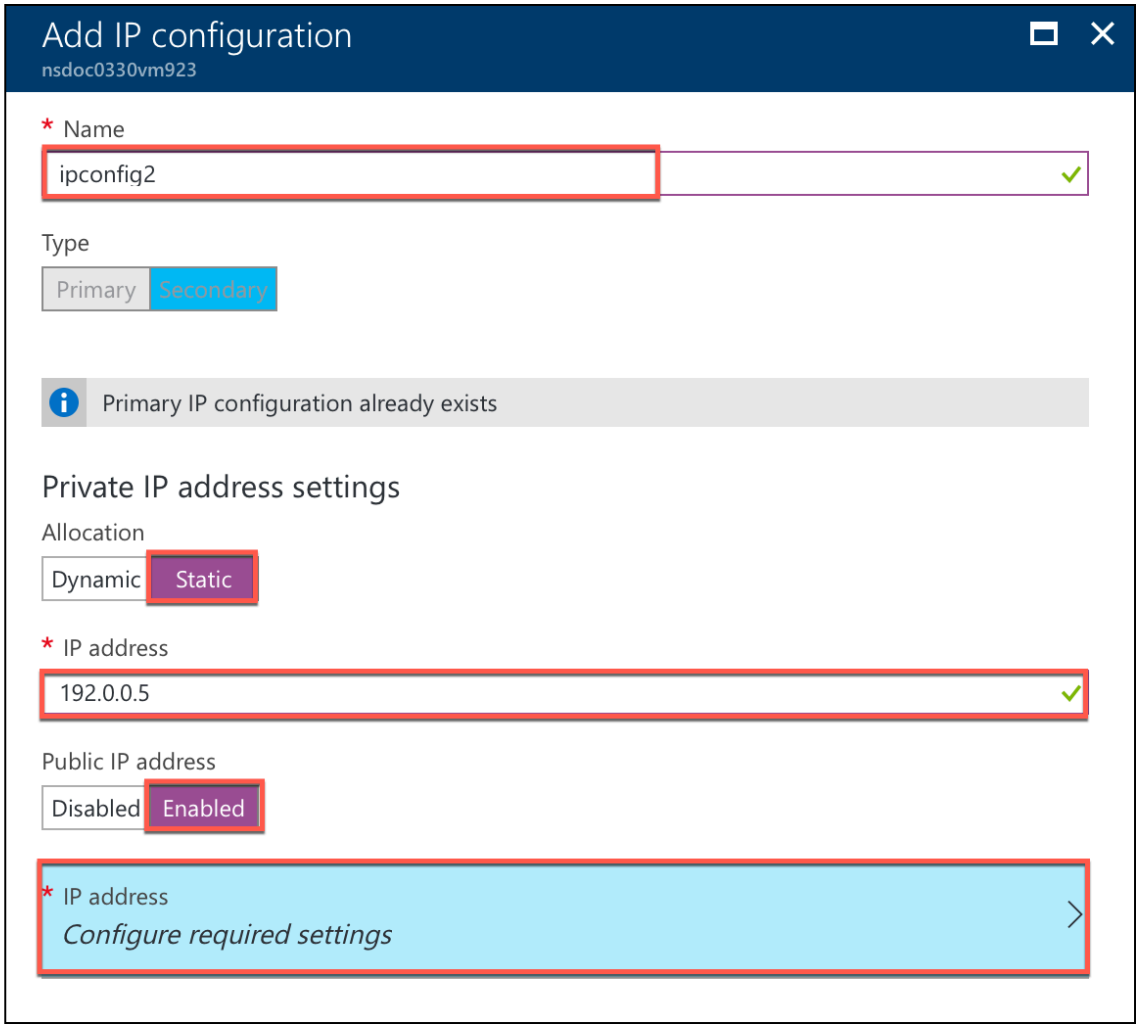
Dans la lame qui apparaît pour la carte réseau sélectionnée, cliquez sur **Configurations IP**. La configuration IP existante qui a été affectée lors de la création de la machine virtuelle, **ipconfig1**, s'affiche. Dans ce cas d'utilisation, assurez-vous que les adresses IP associées à ipconfig1 sont statiques. Ensuite, créez deux configurations IP supplémentaires : ipconfig2 (VIP) et ipconfig3 (SNIP).

Pour en créer plus `ipconfigs`, créez **Ajouter**.



Dans la fenêtre **Ajouter une configuration IP**, entrez un **nom**, spécifiez la méthode d'allocation comme **statique**, entrez une adresse IP (192.0.0.5 pour ce cas d'utilisation) et activez **l'adresse IP publique** .

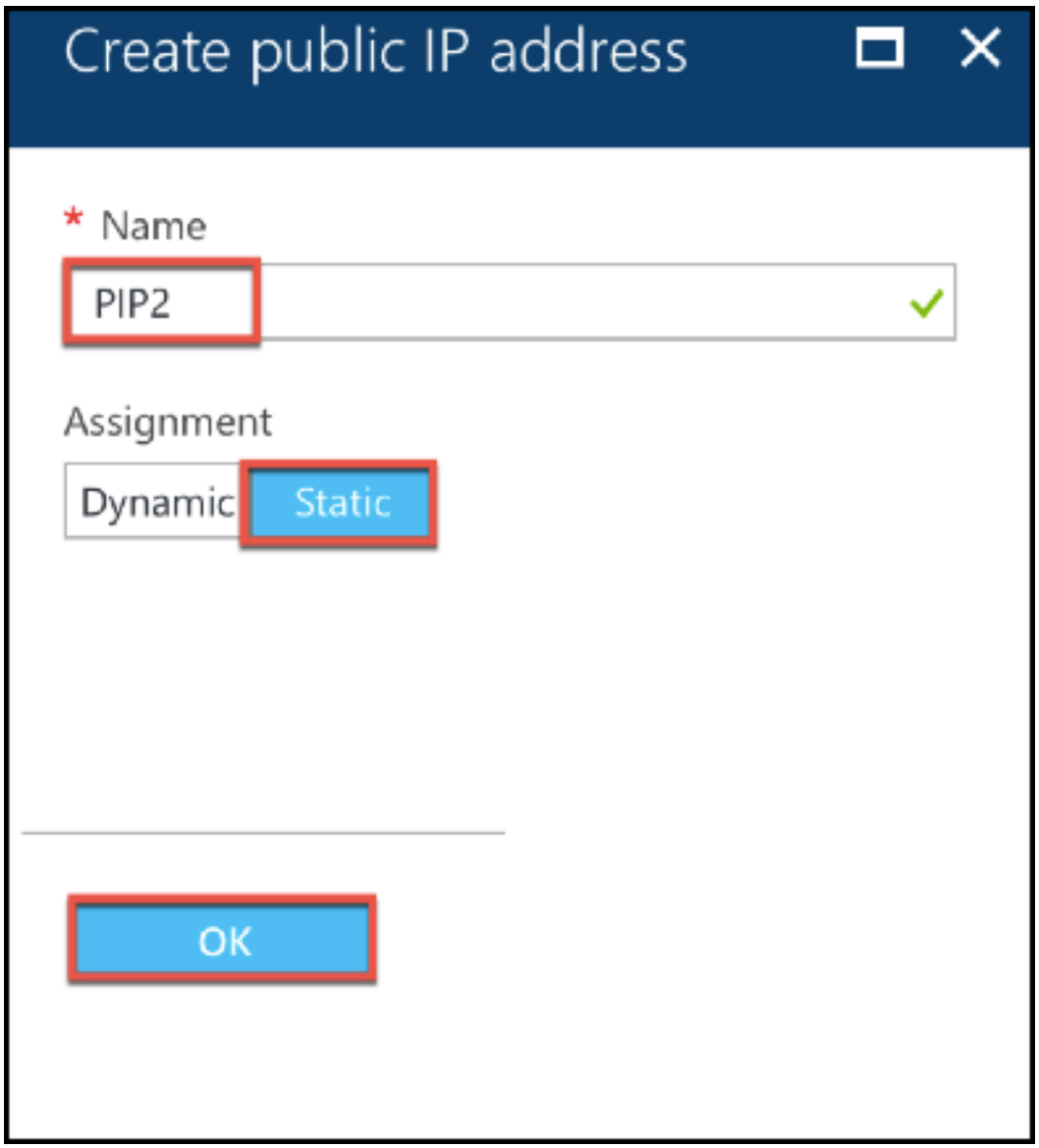
> **Remarque**
>
> Avant d'ajouter une adresse IP privée statique, vérifiez la disponibilité de l'adresse IP et assurez-vous que l'adresse IP appartient au même sous-réseau auquel la carte réseau est attachée.



Ensuite, cliquez sur **Configurer les paramètres requis** pour créer une adresse IP publique statique pour ipconfig2.

Par défaut, les adresses IP publiques sont dynamiques. Pour vous assurer que la machine virtuelle utilise toujours la même adresse IP publique, créez une adresse IP publique statique.

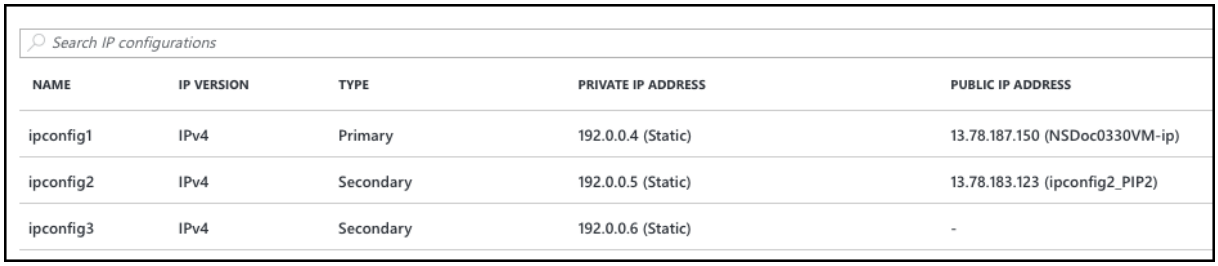
Dans la lame Créer une adresse IP publique, ajoutez un nom, sous Attribution, cliquez sur **Statique**. Puis cliquez sur **OK**.



Remarque

Même lorsque vous définissez la méthode d'allocation sur statique, vous ne pouvez pas spécifier l'adresse IP réelle affectée à la ressource IP publique. Au lieu de cela, il est alloué à partir d'un pool d'adresses IP disponibles dans l'emplacement Azure dans lequel la ressource est créée.

Suivez les étapes pour ajouter une configuration IP supplémentaire pour ipconfig3. La propriété intellectuelle publique n'est pas obligatoire.



Étape 2 : Configurer les adresses IP appartenant à Citrix ADC

Configurez les adresses IP appartenant à Citrix ADC à l'aide de l'interface graphique ou de la commande`add ns ip`. Pour plus d'informations, consultez Configuration des adresses IP appartenant à Citrix ADC.

Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau

August 20, 2021

Dans un déploiement Microsoft Azure, une configuration haute disponibilité de deux instances Citrix ADC VPX est réalisée à l'aide de l'équilibreur de charge Azure (ALB). Pour ce faire, vous pouvez configurer une sonde de santé sur ALB, qui surveille chaque instance VPX en envoyant une sonde de santé toutes les 5 secondes aux instances principales et secondaires.

Dans cette configuration, seul le nœud principal répond aux sondes de santé et le nœud secondaire ne le fait pas. Une fois que le principal envoie la réponse à la sonde d'intégrité, l'ALB commence à envoyer le trafic de données à l'instance. Si l'instance principale manque deux sondes d'intégrité consécutives, ALB ne redirige pas le trafic vers cette instance. Lors du basculement, la nouvelle base commence à répondre aux sondes d'intégrité et l'ALB redirige le trafic vers elle. Le temps de basculement standard VPX haute disponibilité est de trois secondes. Le temps total de basculement que peut prendre le changement de trafic peut être de 13 secondes maximum.

Vous pouvez déployer une paire d'instances Citrix ADC VPX avec plusieurs cartes réseau dans une configuration de haute disponibilité (HA) actif-passif sur Azure. Chaque carte réseau peut contenir plusieurs adresses IP.

Les options suivantes sont disponibles pour un déploiement multicarte haute disponibilité :

- Haute disponibilité à l'aide du jeu de disponibilité Azure
- Haute disponibilité à l'aide des zones de disponibilité Azure

Pour plus d'informations sur Azure Availability Set et Availability Zones, consultez la documentation Azure Gérer la disponibilité des machines virtuelles Linux.

Haute disponibilité en utilisant le jeu de disponibilité

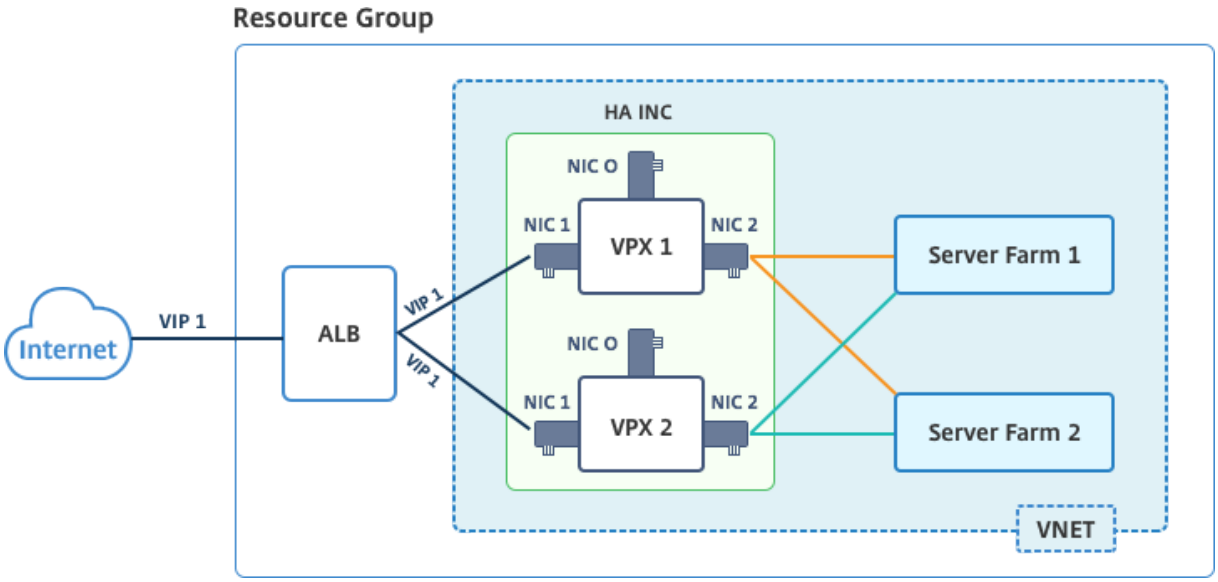
Une configuration haute disponibilité utilisant un jeu de disponibilité doit répondre aux exigences suivantes :

- Configuration de réseau indépendant HA (Independent Network Configuration)
- L'équilibrage de charge Azure (ALB) en mode retour direct du serveur (DSR)

Tout le trafic passe par le nœud principal. Le nœud secondaire reste en mode veille jusqu'à ce que le nœud principal tombe en panne.

> **Remarque**
>
> Pour qu'un déploiement haute disponibilité Citrix VPX sur le cloud Azure fonctionne, vous avez besoin d'une IP publique flottante (PIP) qui peut être déplacée entre les deux nœuds VPX. L'équilibrage de charge Azure (ALB) fournit ce PIP flottant, qui est déplacé automatiquement vers le deuxième nœud en cas de basculement.

Diagramme : Exemple d'architecture de déploiement haute disponibilité, à l'aide du jeu de disponibilité Azure



Dans un déploiement actif-passif, les adresses IP publiques frontales (PIP) ALB sont ajoutées en tant qu'adresses VIP dans chaque nœud VPX. Dans la configuration HA-INC, les adresses VIP sont flottantes et les adresses SNIP sont spécifiques à l'instance.

Vous pouvez déployer une paire VPX en mode haute disponibilité actif-passif de deux façons à l'aide de :

- **Modèle de haute disponibilité standard Citrix ADC VPX** : utilisez cette option pour configurer une paire HA avec l'option par défaut de trois sous-réseaux et six cartes réseau.
- **Commandes Windows PowerShell** : utilisez cette option pour configurer une paire HA en fonction des besoins de votre sous-réseau et de votre carte réseau.

Cette rubrique décrit comment déployer une paire VPX dans une configuration HA actif-passif à l'aide du modèle Citrix. Si vous souhaitez utiliser des commandes PowerShell, reportez-vous à la section Configuration d'une configuration HA avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell.

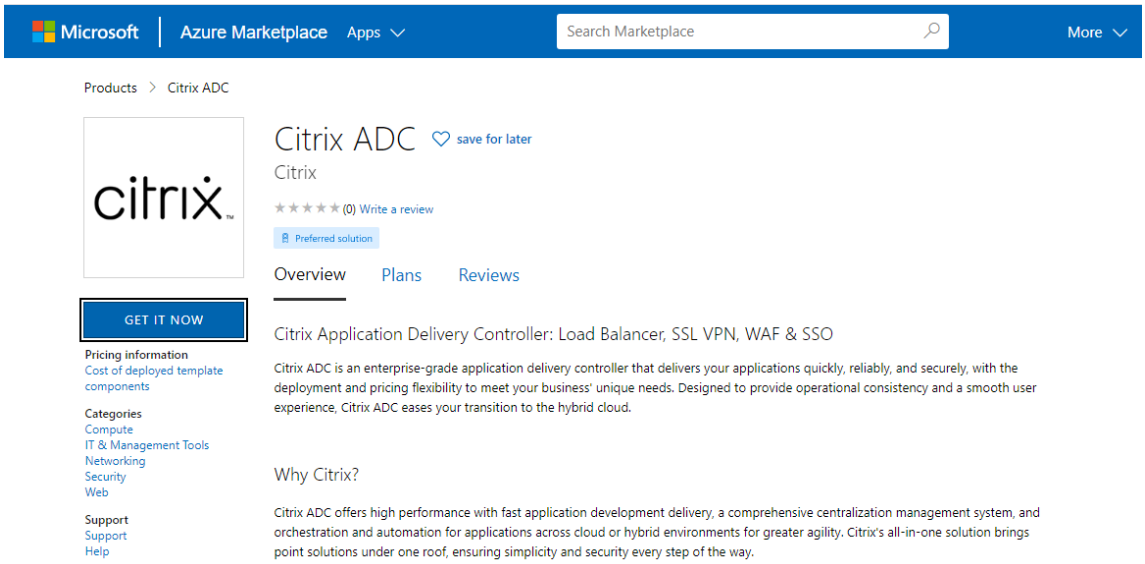
Configurer les nœuds HA-INC à l'aide du modèle de haute disponibilité Citrix

Vous pouvez déployer rapidement et efficacement une paire d'instances VPX en mode HA-INC à l'aide du modèle standard. Le modèle crée deux nœuds, avec trois sous-réseaux et six cartes réseau. Les sous-réseaux sont destinés au trafic de gestion, client et côté serveur, et chaque sous-réseau dispose de deux cartes réseau pour les deux instances VPX.

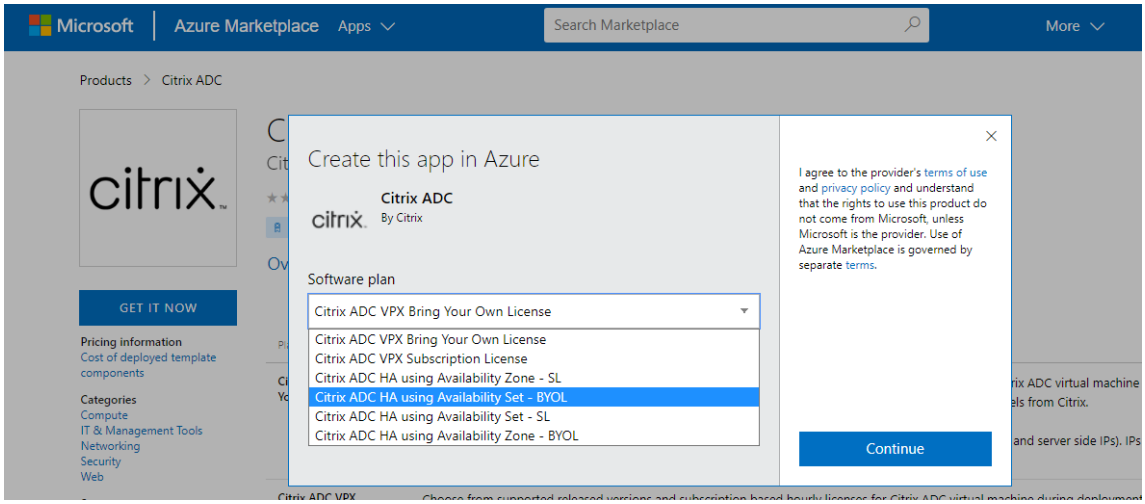
Vous pouvez obtenir le modèle Citrix ADC HA Pair sur Azure Marketplace.

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité, à l'aide des jeux de disponibilité Azure.

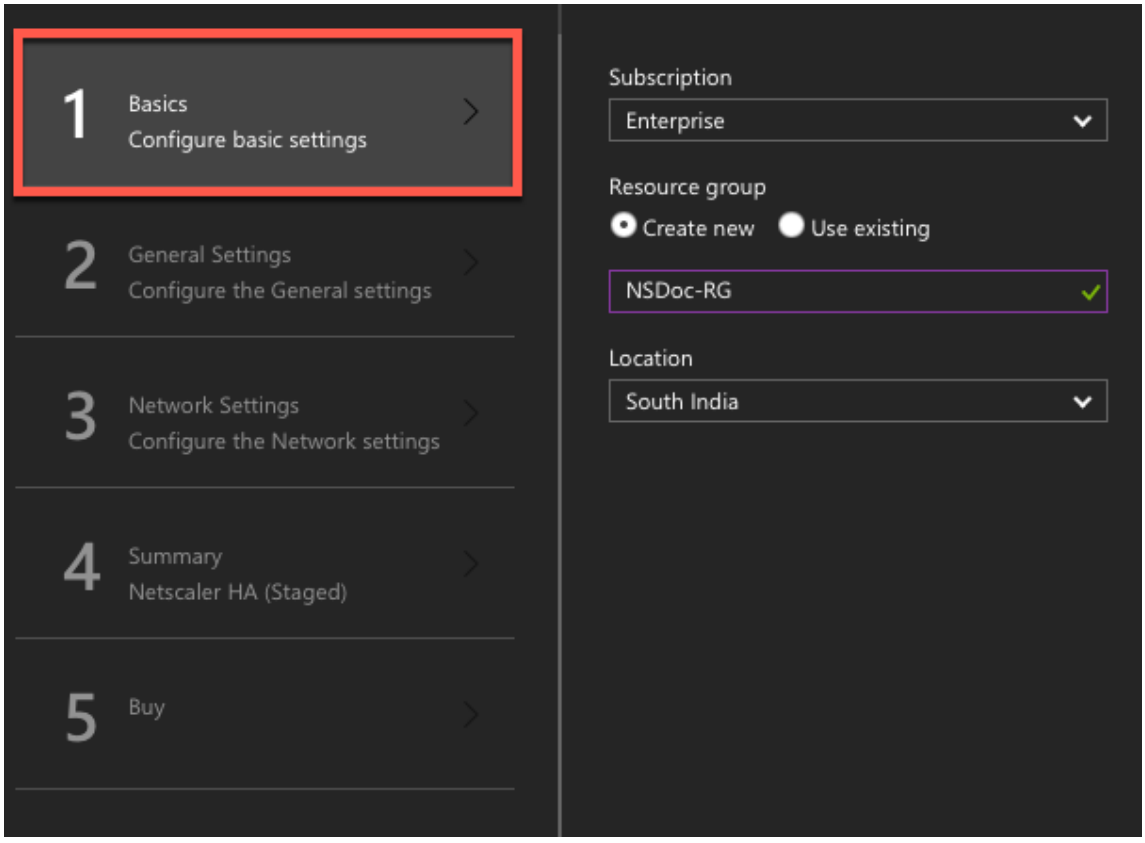
1. Sur la Place de marché Azure, recherchez **Citrix ADC**.



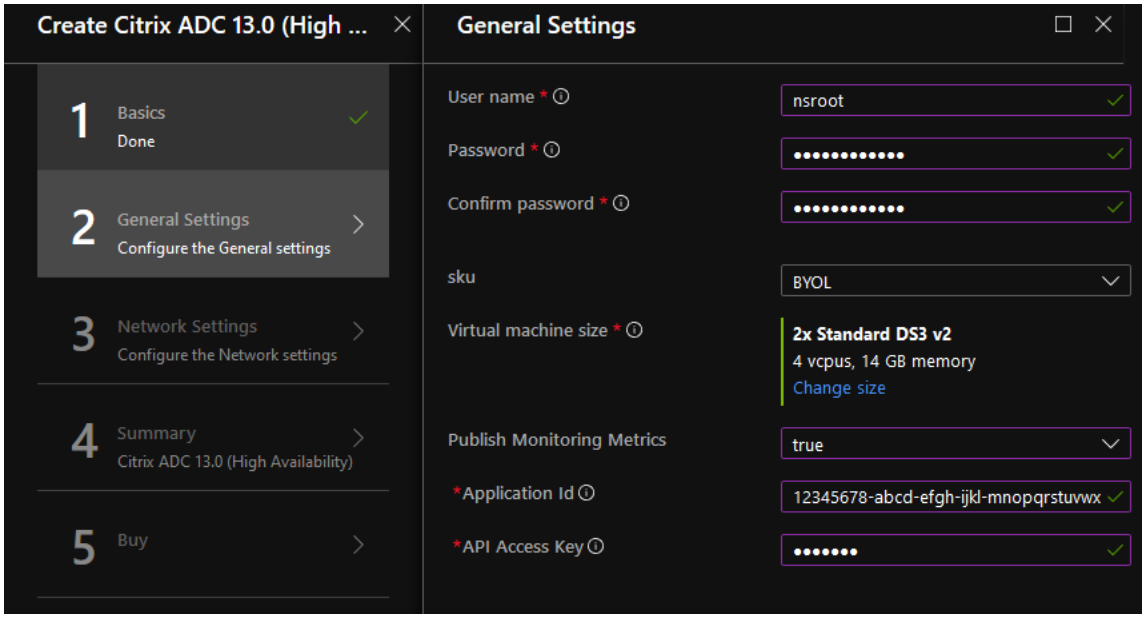
2. Cliquez sur **GET IT NOW**.
3. Sélectionnez le déploiement HA requis ainsi que la licence, puis cliquez sur **Continuer**.



4. La page **Bases** s'affiche. Créez un groupe de ressources et sélectionnez **OK**.

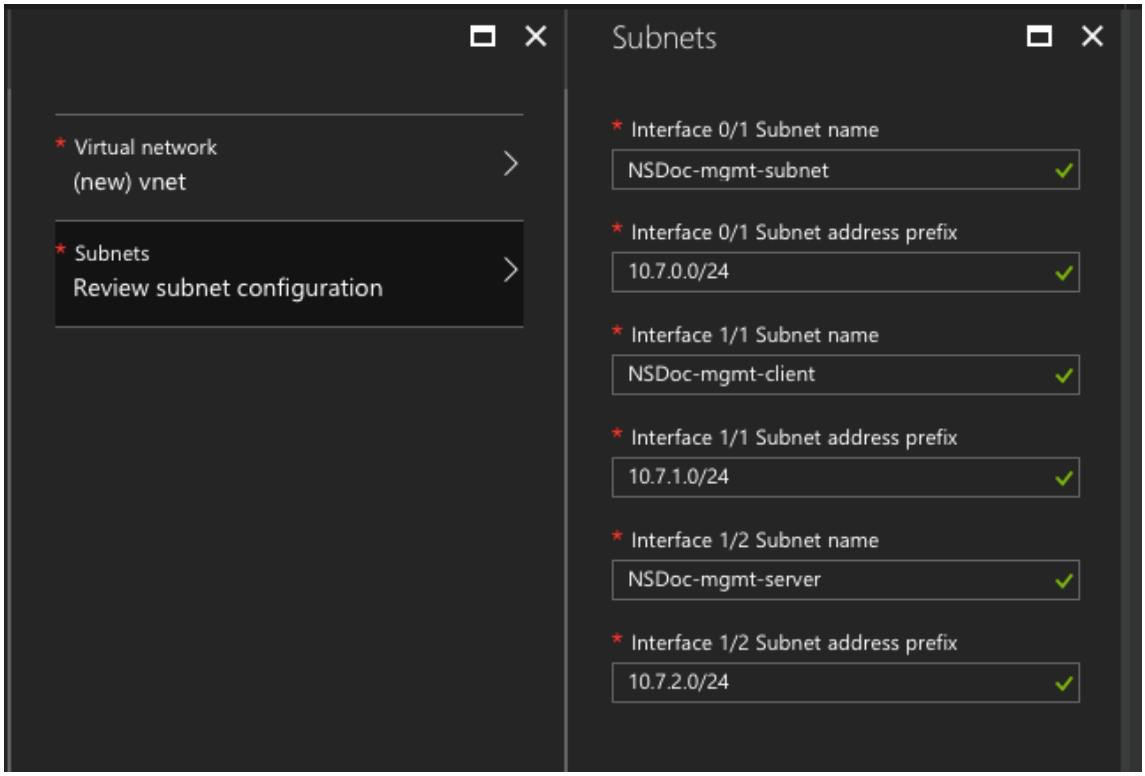


5. La page **Paramètres généraux** s'affiche. Tapez les détails et sélectionnez **OK**.



> Remarque :
>
> Par défaut, l'option **Mesures de surveillance de publication** est définie sur **false**. Si vous souhaitez activer cette option, sélectionnez **true**.
> Créez une application Azure Active Directory (ADD) et un principal de service pouvant accéder aux ressources. Attribuez un rôle de contributeur à l'application AAD nouvellement créée. Pour plus d'informations, voir Utiliser le portail pour créer une application Azure Active Directory et un principal de service pouvant accéder aux ressources.

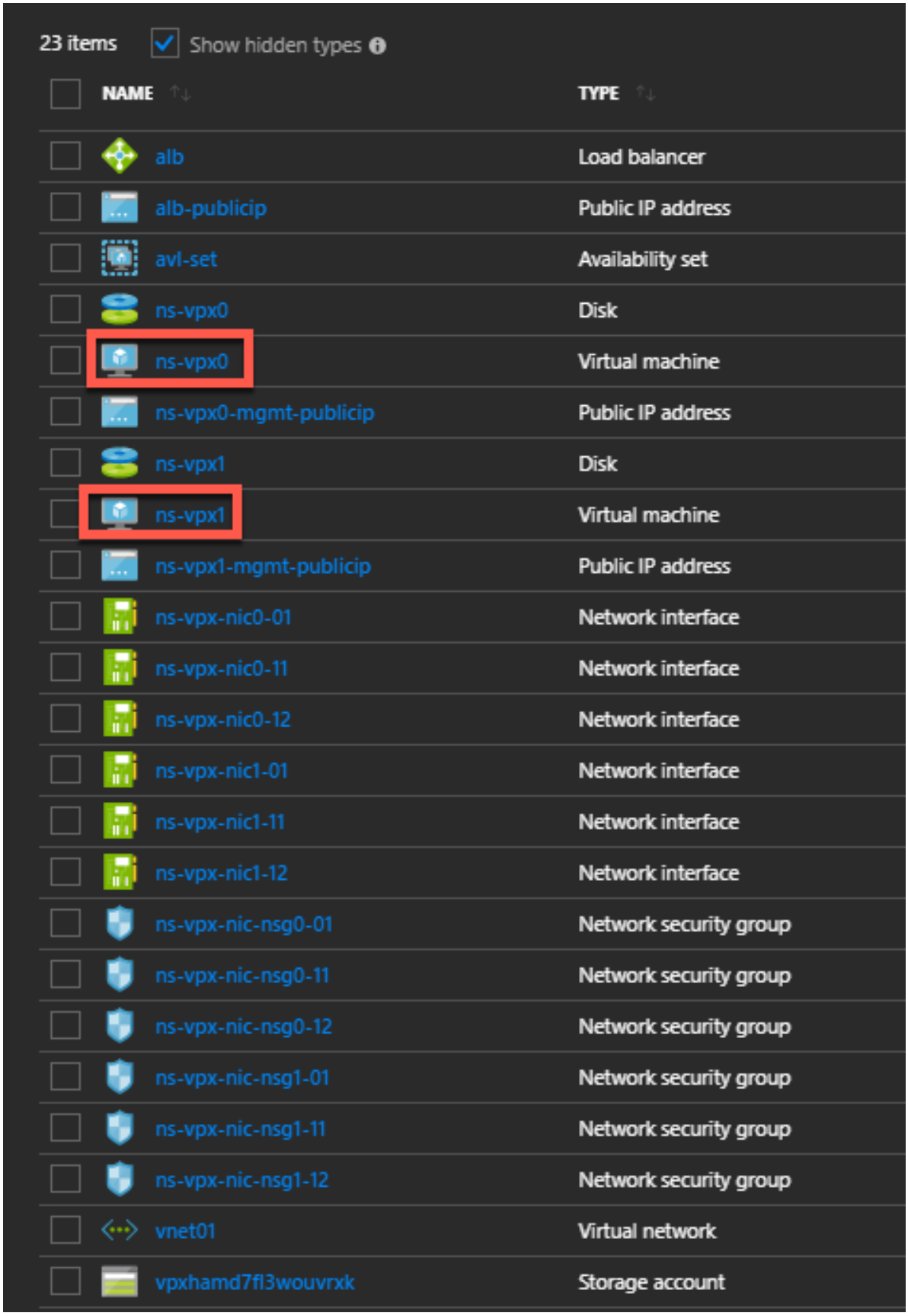
6. La page **Paramètres réseau** s'affiche. Vérifiez les configurations du réseau virtuel et du sous-réseau, modifiez les paramètres requis et sélectionnez **OK**.



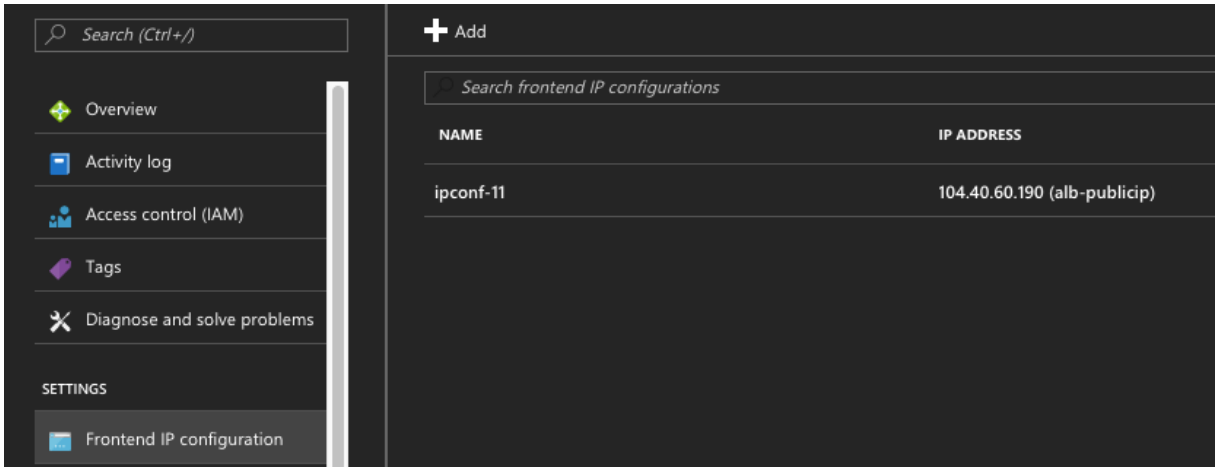
7. La page **Résumé** s'affiche. Vérifiez la configuration et modifiez en conséquence. Sélectionnez **OK** pour confirmer.
8. La page **Acheter** apparaît. Sélectionnez **Achat** pour terminer le déploiement.

Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois terminé, sélectionnez le **groupe de ressources** sur le portail Azure pour afficher les détails de configuration, tels que les règles LB, les pools dorsaux et les sondes de santé. La paire haute disponibilité apparaît sous la forme ns-vpx0 et ns-vpx1.

Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.



Ensuite, vous devez configurer le serveur virtuel d'équilibrage de charge avec l' **adresse IP publique (PIP) de l'ALB**, sur le nœud principal. Pour rechercher le PIP ALB, sélectionnez ALB > **Configuration IP frontend**.



Reportez-vous à la section **Ressources** pour plus d'informations sur la configuration du serveur virtuel d'équilibrage de charge.

Ressources :

Les liens suivants fournissent des informations supplémentaires relatives au déploiement HA et à la configuration du serveur virtuel :

- Configuration des nœuds haute disponibilité dans différents sous-réseaux
- Configurer l'équilibrage de charge de base

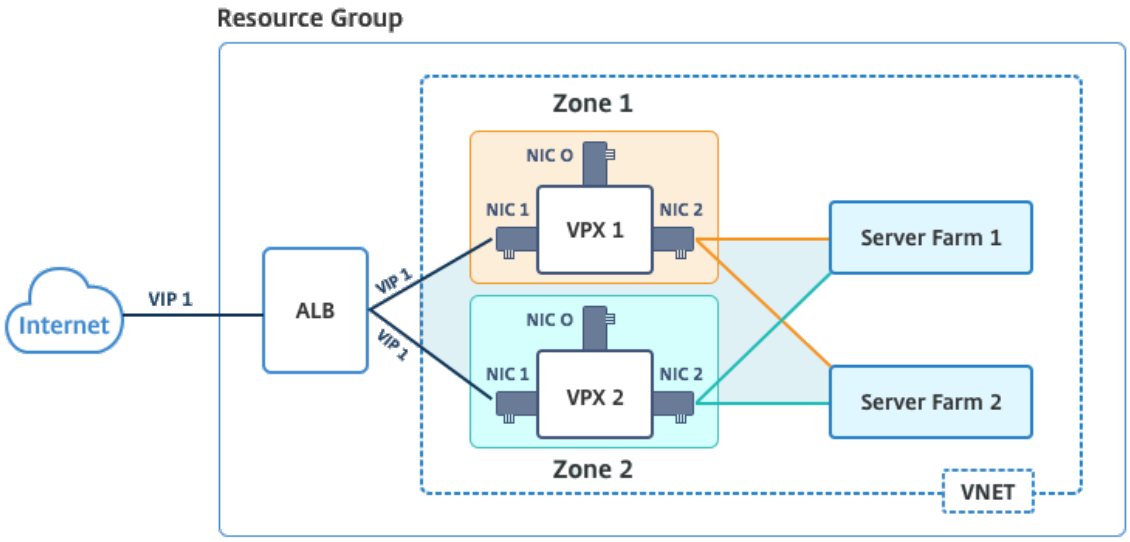
Ressources connexes :

- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell
- Configuration de GSLB sur un déploiement HA actif de secours sur Azure

Haute disponibilité à l'aide des zones de disponibilité

Les zones de disponibilité Azure sont des emplacements isolés de pannes dans une région Azure, fournissant une alimentation, un refroidissement et une mise en réseau redondantes et augmentant la résilience. Seules les régions Azure spécifiques prennent en charge les zones de disponibilité. Pour plus d'informations, consultez la documentation Azure [Qu'est-ce que les zones de disponibilité dans Azure ?

Diagramme : Exemple d'architecture de déploiement haute disponibilité, à l'aide de zones de disponibilité Azure



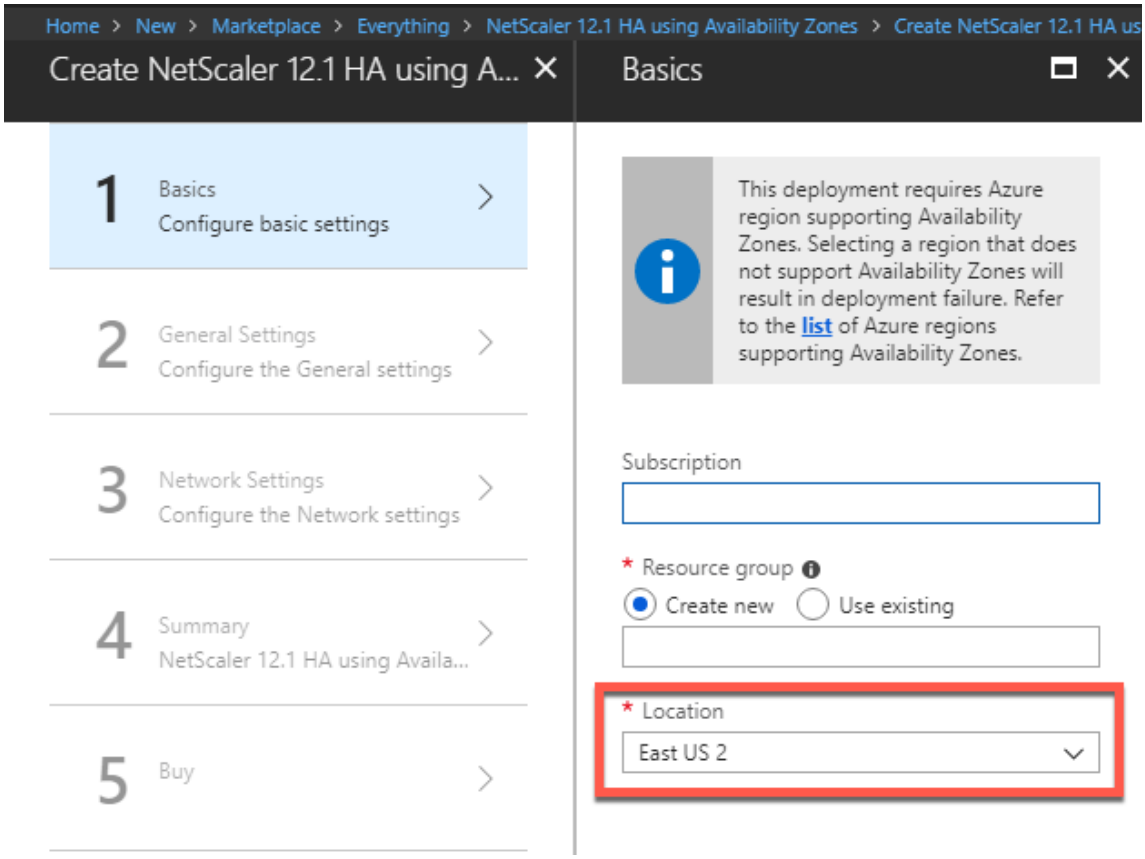
Vous pouvez déployer une paire VPX en mode haute disponibilité à l'aide du modèle appelé « NetScaler 13.0 HA using Availability Zones », disponible dans Azure Marketplace.

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité, à l'aide des zones de disponibilité Azure.

1. À partir de la Place de marché Azure, sélectionnez et lancez le modèle de solution Citrix.

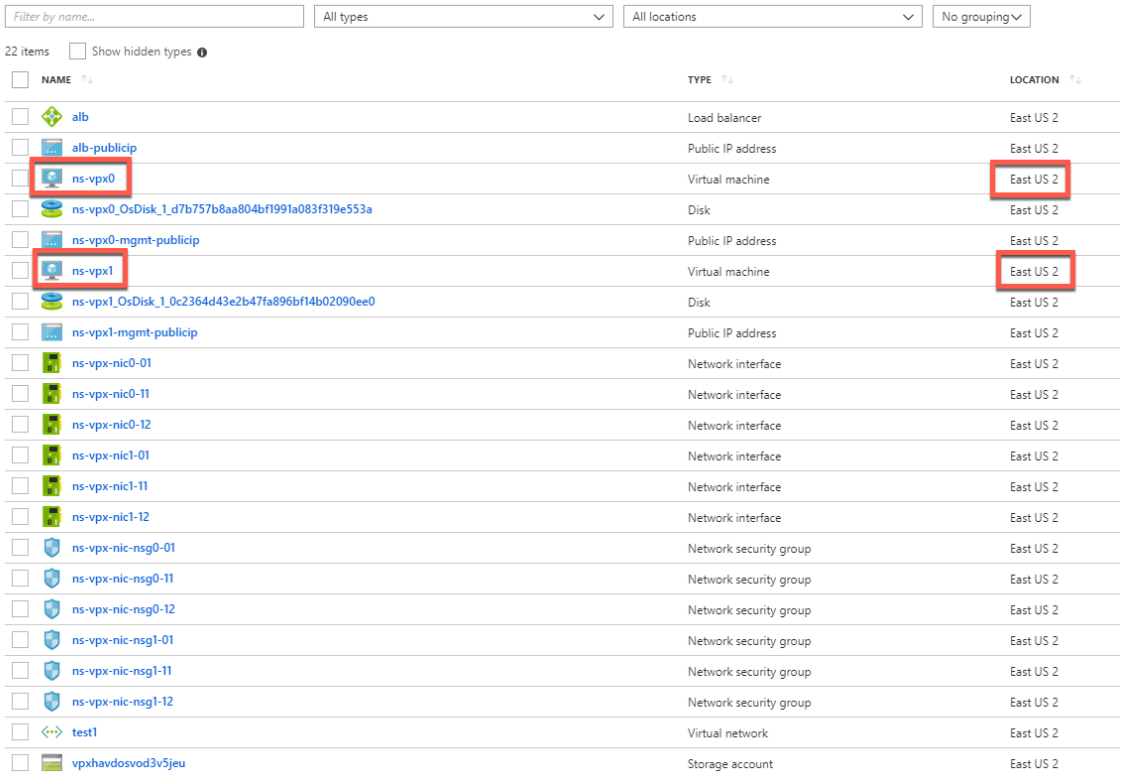
2. Assurez-vous que le type de déploiement est Gestionnaire de ressources et sélectionnez **Créer**.
3. La page **Bases** s'affiche. Entrez les détails et cliquez sur **OK**.

> Remarque : Assurez-vous de sélectionner une région Azure qui prend en charge les zones de disponibilité. Pour plus d'informations sur les régions prenant en charge les zones de disponibilité, consultez la documentation Azure Qu'est-ce que les zones de disponibilité dans Azure ?



4. La page **Paramètres généraux** s'affiche. Tapez les détails et sélectionnez **OK**.
5. La page **Paramètres réseau** s'affiche. Vérifiez les configurations du réseau virtuel et du sous-réseau, modifiez les paramètres requis et sélectionnez **OK**.
6. La page **Résumé** s'affiche. Vérifiez la configuration et modifiez en conséquence. Sélectionnez **OK** pour confirmer.
7. La page **Acheter** apparaît. Sélectionnez **Achat** pour terminer le déploiement.

   Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois terminé, sélectionnez le **groupe de ressources** pour afficher les détails de configuration, tels que les règles de LB, les pools back-end, les analyses de santé, etc., dans le portail Azure. La paire haute disponibilité apparaît sous la forme ns-vpx0 et ns-vpx1. En outre, vous pouvez voir l'emplacement sous la colonne **Emplacement** .



Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.

Surveillez vos instances à l'aide de mesures dans Azure Monitor

Vous pouvez utiliser des mesures dans la plate-forme de données Azure Monitor pour surveiller un ensemble de ressources Citrix ADC VPX telles que le processeur, l'utilisation de la mémoire et le débit. Le service Metrics surveille les ressources Citrix ADC VPX qui s'exécutent sur Azure, en temps réel. Vous pouvez utiliser l' **Explorateur de mesures** pour accéder aux données collectées. Pour plus d'informations, reportez-vous à la section Présentation des mesures Azure Monitor.

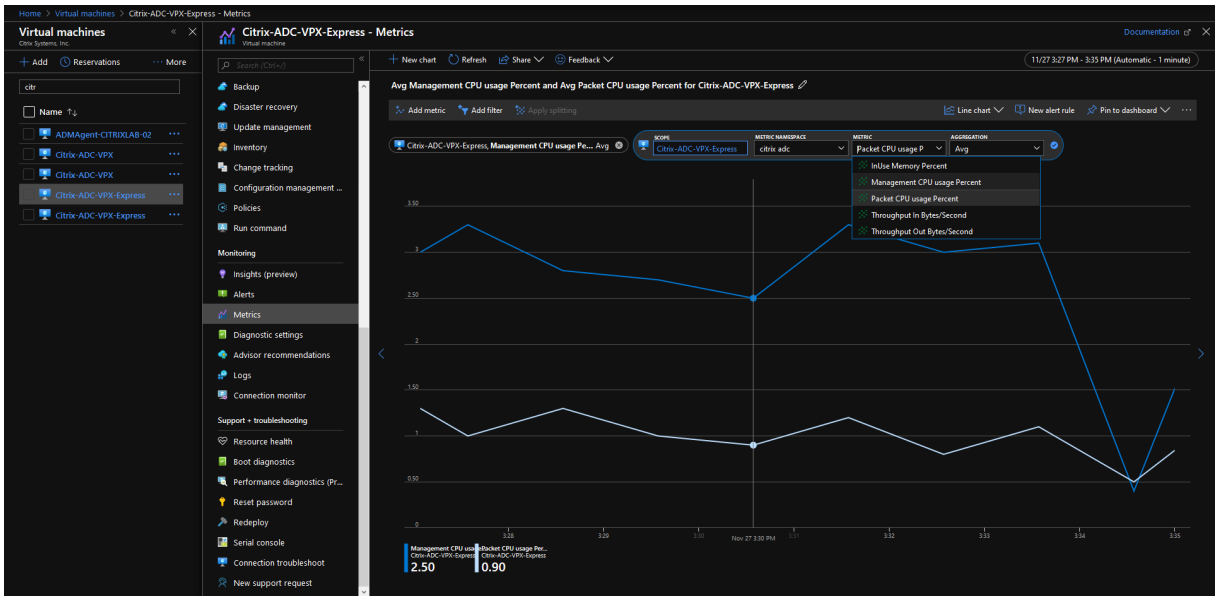
Points à noter

- Si vous déployez une instance Citrix ADC VPX sur Azure à l'aide de l'offre Place de marché Azure, le service Metrics est désactivé par défaut.
- Le service Metrics n'est pas pris en charge dans Azure CLI.
- Les mesures sont disponibles pour l'UC (gestion et utilisation de l'UC par paquets), la mémoire et le débit (entrants et sortants).

Comment afficher les mesures dans Azure Monitor

Pour afficher les mesures dans Azure Monitor pour votre instance, effectuez les opérations suivantes :

1. Connectez-vous à **Azure Portal > Machines virtuelles**.
2. Sélectionnez la machine virtuelle qui est le nœud principal.
3. Dans la section **Surveillance**, cliquez sur **Mesures**.
4. Dans le menu déroulant **Espace de noms de mesure**, cliquez sur **Citrix ADC**.
5. Sous **Toutes les mesures** dans le menu déroulant **Mesures**, cliquez sur les mesures que vous souhaitez afficher.
6. Cliquez sur **Ajouter une mesure** pour afficher une autre mesure sur le même graphique. Utilisez les options Graphique pour personnaliser votre graphique.



Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell

August 20, 2021

Vous pouvez déployer une paire d'instances Citrix ADC VPX avec plusieurs cartes réseau dans une configuration de haute disponibilité (HA) actif-passif sur Azure. Chaque carte réseau peut contenir plusieurs adresses IP.

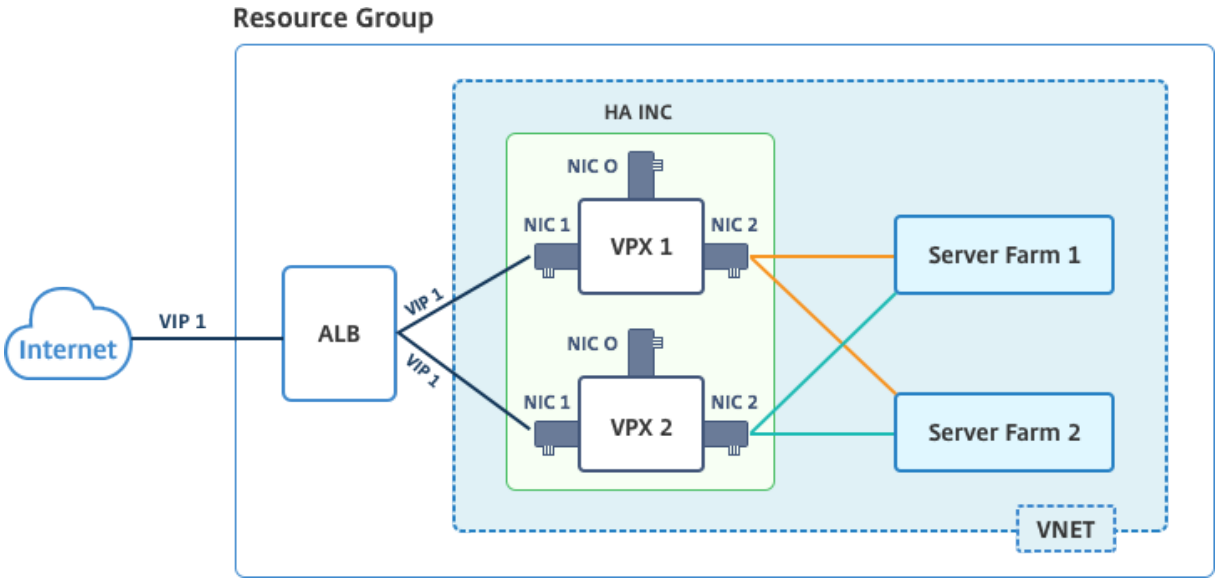
Un déploiement actif-passif nécessite :

- Configuration de réseau indépendant HA (Independent Network Configuration)
- L'équilibrage de charge Azure (ALB) en mode retour direct du serveur (DSR)

Tout le trafic passe par le nœud principal. Le nœud secondaire reste en mode veille jusqu'à ce que le nœud principal tombe en panne.

> **Remarque**
>
> Pour qu'un déploiement haute disponibilité Citrix ADC VPX fonctionne sur un cloud Azure, vous avez besoin d'une IP publique flottante (PIP) pouvant être déplacée entre les deux nœuds haute disponibilité. L'équilibrage de charge Azure (ALB) fournit ce PIP flottant, qui est déplacé automatiquement vers le deuxième nœud en cas de basculement.

Schéma : Exemple d'architecture de déploiement actif-passif



Dans un déploiement actif-passif, les adresses IP publiques flottantes (PIP) ALB sont ajoutées en tant qu'adresses VIP dans chaque nœud VPX. Dans la configuration HA-INC, les adresses VIP sont flottantes et les adresses SNIP sont spécifiques à l'instance.

ALB surveille chaque instance VPX en envoyant une sonde de santé toutes les 5 secondes et redirige le trafic vers cette instance uniquement qui envoie la réponse des sondes de santé à intervalles réguliers. Ainsi, dans une configuration HA, le nœud principal répond aux sondes d'intégrité et le nœud secondaire ne le fait pas. Si les instances principales manquent deux sondes de santé consécutives, ALB ne redirige pas le trafic vers cette instance. Lors du basculement, la nouvelle base commence à répondre aux sondes d'intégrité et l'ALB redirige le trafic vers elle. Le temps de basculement standard VPX haute disponibilité est de trois secondes. Le temps de basculement total qui peut prendre pour la commutation de trafic peut être de 13 secondes maximum.

Vous pouvez déployer une paire VPX dans une configuration HA actif-passif de deux façons à l'aide de :

- **Modèle de haute disponibilité Citrix ADC VPX Standard** : utilisez cette option pour configurer une paire HA avec l'option par défaut de trois sous-réseaux et six cartes réseau.
- **Commandes Windows PowerShell** : utilisez cette option pour configurer une paire HA en fonc-

tion des besoins de votre sous-réseau et de votre carte réseau.

Cette rubrique décrit comment déployer une paire VPX dans une configuration HA active-passive à l'aide des commandes PowerShell. Si vous souhaitez utiliser le modèle Citrix ADC VPX Standard HA, reportez-vous à la section Configuration d'une configuration HA avec plusieurs adresses IP et cartes réseau.

Configurer les nœuds HA-INC à l'aide des commandes PowerShell

Scénario : déploiement PowerShell HA-INC

Dans ce scénario, vous déployez une paire Citrix ADC VPX à l'aide de la topologie donnée dans la table. Chaque instance VPX contient trois cartes réseau, chaque carte réseau étant déployée dans un sous-réseau différent. Une configuration IP est attribuée à chaque carte réseau.

ALB	VPX1	VPX2
ALB est associé à l'IP publique 3 (pip3)	L'adresse IP de gestion est configurée avec IPConfig1, qui inclut une adresse IP publique (pip1) et une adresse IP privée (12.5.2.24) ; nic1 ; Mgmtsubnet=12.5.2.0/24	L'adresse IP de gestion est configurée avec IPConfig5, qui inclut une adresse IP publique (pip3) et une adresse IP privée (12.5.2.26) ; nic4 ; Mgmtsubnet=12.5.2.0/24
Les règles LB et le port configurés sont HTTP (80), SSL (443), sonde d'intégrité (9000)	L'adresse IP côté client est configurée avec IPConfig3, qui inclut une adresse IP privée (12.5.1.27) ; nic2 ; FrontendSubet=12.5.1.0/24	L'adresse IP côté client est configurée avec IPConfig7, qui inclut une adresse IP privée (12.5.1.28) ; nic5 ; FrontendSubet=12.5.1.0/24
-	L'adresse IP côté serveur est configurée avec IPConfig4, qui inclut une adresse IP privée (12.5.3.24) ; nic3 ; BackEndSubnet=12.5.3.0/24	L'adresse IP côté serveur est configurée avec IPConfig8, qui inclut une adresse IP privée (12.5.3.28) ; nic6 ; BackEndSubnet=12.5.3.0/24
-	Les règles et les ports pour NSG sont SSH (22), HTTP (80), HTTPS (443)	-

Paramètres des paramètres

Les paramètres suivants sont utilisés dans ce scénario.

$locName= “South east Asia”

$rgName = “MulitIP-MultiNIC-RG”

$nicName1= “VM1-NIC1”

$nicName2 = “VM1-NIC2”

$nicName3= “VM1-NIC3”

$nicName4 = “VM2-NIC1”

$nicName5= “VM2-NIC2”

$nicName6 = “VM2-NIC3”

$vNetName = “Azure-MultiIP-ALB-vnet”

$vNetAddressRange= “12.5.0.0/16”

$frontEndSubnetName= “frontEndSubnet”

$frontEndSubnetRange= “12.5.1.0/24”

$mgmtSubnetName= “mgmtSubnet”

$mgmtSubnetRange= “12.5.2.0/24”

$backEndSubnetName = “backEndSubnet”

$backEndSubnetRange = “12.5.3.0/24”

$prmStorageAccountName = “multiipmultinicbstorage”

$avSetName = “multiple-avSet”

$vmSize= “Standard_DS4_V2”

$publisher = « Citrix »

$offer = “netscalervpx-120”

$sku = “netscalerbyol”

$version=”latest”

$pubIPName1=”VPX1MGMT”

$pubIPName2=”VPX2MGMT”

$pubIPName3=”ALBPIP”

$domName1=”vpx1dns”

$domName2=”vpx2dns”

$domName3=”vpxalbdns”

$vmNamePrefix=”VPXMultiIPALB”

$osDiskSuffix1=”osmultiipalbdiskdb1”

$osDiskSuffix2=”osmultiipalbdiskdb2”

$lbName= “MultiIPALB”

$frontEndConfigName1= “FrontEndIP”

$backendPoolName1= “BackendPoolHttp”

$lbRuleName1= “LBRuleHttp”

$healthProbeName= “HealthProbe”

$nsgName=”NSG-MultiIP-ALB”

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

Pour terminer le déploiement, procédez comme suit à l’aide des commandes PowerShell :

1. Créer un groupe de ressources, un compte de stockage et un jeu de disponibilité
2. Créer un groupe de sécurité réseau et ajouter des règles
3. Créer un réseau virtuel et trois sous-réseaux
4. Créer des adresses IP publiques
5. Créer des configurations IP pour VPX1
6. Créer des configurations IP pour VPX2
7. Créer des cartes réseau pour VPX1
8. Créer des cartes réseau pour VPX2
9. Créer VPX1
10. Créer VPX2
11. Créer ALB

Créez un groupe de ressources, un compte de stockage et un jeu de disponibilité.

```
1 New-AzureRmResourceGroup -Name $rgName -Location $locName
2
3
4 $prmStorageAccount=New-AzureRMStorageAccount -Name
     $prmStorageAccountName -ResourceGroupName $rgName -Type Standard_LRS
      -Location $locName
5
```



```
6
7 $avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
     $rgName -Location $locName
```

Créez un groupe de sécurité réseau et ajoutez des règles.

```
1 $rule1 = New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -
     Description "Allow HTTP" -Access Allow -Protocol Tcp -Direction
     Inbound -Priority 101
2
3
4 -SourceAddressPrefix Internet -SourcePortRange * -
     DestinationAddressPrefix * -DestinationPortRange 80
5
6
7 $rule2 = New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -
     Description "Allow HTTPS" -Access Allow -Protocol Tcp -Direction
     Inbound -Priority 110
8
9
10 -SourceAddressPrefix Internet -SourcePortRange * -
     DestinationAddressPrefix * -DestinationPortRange 443
11
12
13 $rule3 = New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
     Description "Allow SSH" -Access Allow -Protocol Tcp -Direction
     Inbound -Priority 120
14
15
16 -SourceAddressPrefix Internet -SourcePortRange * -
     DestinationAddressPrefix * -DestinationPortRange 22
17
18
19 $nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
     Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
```

Créez un réseau virtuel et trois sous-réseaux.

```
1 $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
     $frontEndSubnetName -AddressPrefix $frontEndSubnetRange (this
     parameter value should be as per your requirement)
2
3
4 $mgmtSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name $mgmtSubnetName
      -AddressPrefix $mgmtSubnetRange
```



```
5
6
7  $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       $backEndSubnetName -AddressPrefix $backEndSubnetRange
8
9
10 $vnet =New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
       $rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet
       $frontendSubnet,$backendSubnet, $mgmtSubnet
11
12
13 $subnetName ="frontEndSubnet"
14
15
16 $subnet1=$vnet.Subnets|?{
17  $_.Name -eq $subnetName }
18
19
20
21 $subnetName="backEndSubnet"
22
23
24 $subnet2=$vnet.Subnets|?{
25  $_.Name -eq $subnetName }
26
27
28
29 $subnetName="mgmtSubnet"
30
31
32 $subnet3=$vnet.Subnets|?{
33  $_.Name -eq $subnetName }
```

Créez des adresses IP publiques.

```
1  $pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
       $rgName -DomainNameLabel $domName1 -Location $locName -
       AllocationMethod Dynamic
2
3  $pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
       $rgName -DomainNameLabel $domName2 -Location $locName -
       AllocationMethod Dynamic
4
5  $pip3=New-AzureRmPublicIpAddress -Name $pubIPName3 -ResourceGroupName
       $rgName -DomainNameLabel $domName3 -Location $locName -
```



```
    AllocationMethod Dynamic
```

Créez des configurations IP pour VPX1.

```
$IpConfigName1 = "IPConfig1"


$IPAddress = "12.5.2.24"


$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip1
    -Primary


$IPConfigName3="IPConfig-3"


$IPAddress="12.5.1.27"


$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary


$IPConfigName4 = "IPConfig-4"


$IPAddress = "12.5.3.24"


$IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
    Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Créez des configurations IP pour VPX2.

```
$IpConfigName5 = "IPConfig5"


$IPAddress="12.5.2.26"


$IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip2
    -Primary
```



```
8
9
10 $IPConfigName7="IPConfig-7"
11
12
13 $IPAddress="12.5.1.28"
14
15
16 $IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
       Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19 $IPConfigName8="IPConfig-8"
20
21
22 $IPAddress="12.5.3.28"
23
24
25 $IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8 -
       Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Créez des cartes réseau pour VPX1.

```
1 $nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig1 -
      NetworkSecurityGroupId $nsg.Id
2
3
4 $nic2=New-AzureRmNetworkInterface -Name $nicName2 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig3 -
      NetworkSecurityGroupId $nsg.Id
5
6
7 $nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig4 -
      NetworkSecurityGroupId $nsg.Id
```

Créez des cartes réseau pour VPX2.

```
1 $nic4=New-AzureRmNetworkInterface -Name $nicName4 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig5 -
      NetworkSecurityGroupId $nsg.Id
2
3
4 $nic5=New-AzureRmNetworkInterface -Name $nicName5 -ResourceGroupName
```



```
    $rgName -Location $locName -IpConfiguration $IpConfig7 -
    NetworkSecurityGroupId $nsg.Id
5
6
7 $nic6=New-AzureRmNetworkInterface -Name $nicName6 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig8 -
    NetworkSecurityGroupId $nsg.Id
```

Créez VPX1.

Cette étape comprend les sous-étapes suivantes :

- Créer un objet de configuration VM
- Définir les informations d'identification, le système d'exploitation et l'image
- Ajouter des cartes réseau
- Spécifier le disque du système d'exploitation et créer une machine virtuelle

```
1  $suffixNumber = 1
2
3  $vmName=$vmNamePrefix + $suffixNumber
4
5  $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
       AvailabilitySetId $avSet.Id
6
7  $cred=Get-Credential -Message "Type the name and password for VPX
       login."
8
9  $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
       ComputerName $vmName -Credential $cred
10
11 $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
       $publisher -Offer $offer -Skus $sku -Version $version
12
13 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.
       Id -Primary
14
15 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.
       Id
16
17 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.
       Id
18
19 $osDiskName=$vmName + "-" + $osDiskSuffix1
20
```



```
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/" + $osDiskName + ".vhd"

$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri $osVhdUri -CreateOption fromImage

Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -Name $sku

New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location $locName
```

Créez VPX2.

```
```
$suffixNumber=2

$vmName=$vmNamePrefix + $suffixNumber

$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avSet.Id

$cred=Get-Credential -Message "Type the name and password for VPX login."

$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName $vmName -Credential $cred

$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher -Offer $offer -Skus $sku -Version $version

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic4.Id -Primary

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id
```

 
```

```
27
28
29 $osDiskName=$vmName + "-" + $osDiskSuffix2
30
31
32 $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/"
       + $osDiskName + ".vhd"
33
34
35 $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
      $osVhdUri -CreateOption fromImage
36
37
38 Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
      Name $sku
39
40
41 New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
      $locName
42 <!--NeedCopy--> ```
```

Pour afficher les adresses IP privées et publiques affectées aux cartes réseau, tapez les commandes suivantes :

```
1 ```
2 $nic1.IPConfig
3
4
5 $nic2.IPConfig
6
7
8 $nic3.IPConfig
9
10
11 $nic4.IPConfig
12
13
14 $nic5.IPConfig
15
16
17 $nic6.IPConfig
18 <!--NeedCopy--> ```
```

Créer un équilibrage de charge Azure (ALB).

Cette étape comprend les sous-étapes suivantes :

- Création d'une configuration IP frontale
- Créer une sonde de santé
- Créer un pool d'adresses back-end
- Créer des règles d'équilibrage de charge (HTTP et SSL)
- Créer un ALB avec la configuration IP frontale, le pool d'adresses backend et la règle LB
- Associer la configuration IP à des pools dorsaux

```
$frontEndIP1=New-AzureRmLoadBalancerFrontendIpConfig -Name $frontEndConfigName1
 -PublicIpAddress $pip3

$healthProbe=New-AzureRmLoadBalancerProbeConfig -Name $healthProbeName
-Protocol Tcp -Port 9000 -IntervalInSeconds 5 -ProbeCount 2

$beAddressPool1=New-AzureRmLoadBalancerBackendAddressPoolConfig -Name
$backendPoolName1

$lbRule1=New-AzureRmLoadBalancerRuleConfig -Name $lbRuleName1 -FrontendIpConfigur
 $frontEndIP1 -BackendAddressPool $beAddressPool1 -Probe $healthProbe -
Protocol Tcp -FrontendPort 80 -BackendPort 80 -EnableFloatingIP

$lb=New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name $lbName -
Location $locName -FrontendIpConfiguration $frontEndIP1 -LoadBalancingRule
 $lbRule1 -BackendAddressPool $beAddressPool1 -Probe $healthProbe

$nic2.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.
BackendAddressPools[0])

$nic5.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.
BackendAddressPools[0])

$lb=$lb |Set-AzureRmLoadBalancer

$nic2=$nic2 | Set-AzureRmNetworkInterface

$nic5=$nic5 | Set-AzureRmNetworkInterface
```

Après avoir déployé avec succès la paire Citrix ADC VPX, connectez-vous à chaque instance VPX pour configurer HA-INC et les adresses SNIP et VIP.

1. Tapez la commande suivante pour ajouter des nœuds HA.

   ```
   add ha node 1 PeerNodeNSIP -inc Enabled
   ```

2. Ajouter des adresses IP privées de cartes réseau côté client en tant que SNIP pour VPX1 (NIC2) et VPX2 (NIC5)


```
add nsip privateIPofNIC2 255.255.255.0 -type SNIP
add nsip privateIPofNIC5 255.255.255.0 -type SNIP
```

3. Ajoutez un serveur virtuel d'équilibrage de charge sur le nœud principal avec l'adresse IP frontale (IP publique) d'ALB.

```
add lb virtual server v1 HTTP FrontEndIPofALB 80
```

Ressources connexes :

Configuration de GSLB sur un déploiement HA actif de secours sur Azure

Configurer une instance Citrix ADC VPX pour utiliser la mise en réseau accélérée Azure

August 20, 2021

La mise en réseau accélérée permet la carte réseau (VF) à fonction virtuelle (SR-IOV) de virtualisation d'E/S à racine unique sur une machine virtuelle, ce qui améliore les performances réseau. Vous pouvez utiliser cette fonctionnalité avec des charges de travail lourdes qui doivent envoyer ou recevoir des données à un débit supérieur avec un streaming fiable et une utilisation réduite du processeur. Lorsqu'une carte réseau est activée avec une mise en réseau accélérée, Azure associe l'interface para virtualisée (PV) existante de la carte réseau à une interface VF SR-IOV. La prise en charge de l'interface SR-IOV VF permet et améliore le débit de l'instance Citrix ADC VPX.

La mise en réseau accélérée offre les avantages suivants :

- Latence inférieure
- Performances supérieures des paquets par seconde (pps)
- Débit amélioré
- gigue réduite
- Utilisation réduite du processeur

> Remarque
>
> La mise en réseau accélérée Azure est prise en charge sur les instances Citrix ADC VPX à partir de la version 13.0 build 76.29.

Conditions préalables

- Assurez-vous que la taille de votre machine virtuelle correspond aux exigences relatives à la mise en réseau accélérée Azure.
- Arrêtez les machines virtuelles (individuelles ou dans un jeu de disponibilité) avant d'activer la mise en réseau accélérée sur n'importe quelle carte réseau.

Limitations

La mise en réseau accélérée peut être activée uniquement sur certains types d'instances. Pour plus d'informations, voir Types d'instances pris en charge.

cartes réseau prises en charge pour une mise en réseau accélérée

Azure fournit des cartes réseau Mellanox ConnectX3 et ConnectX4 en mode SR-IOV pour une mise en réseau accélérée.

Lorsque la mise en réseau accélérée est activée sur une interface Citrix ADC VPX, Azure associe l'interface ConnectX3 ou ConnectX4 à l'interface PV existante d'une appliance Citrix ADC VPX.

Pour plus d'informations sur l'activation d'une mise en réseau accélérée avant d'attacher une interface à une machine virtuelle, voir Créer une interface réseau avec une mise en réseau accélérée.

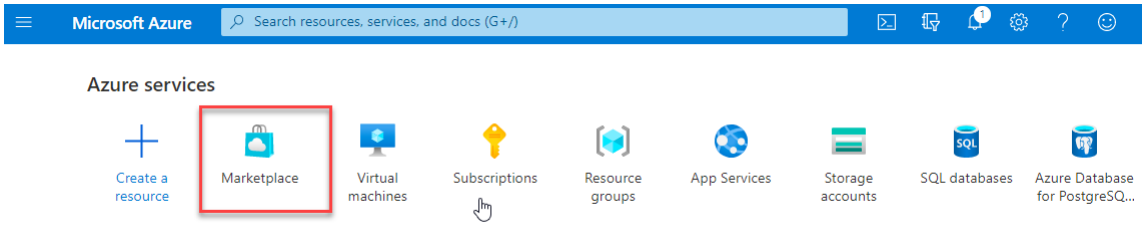
Pour plus d'informations sur l'activation d'une mise en réseau accélérée sur une interface existante sur une machine virtuelle, voir Activer les interfaces existantes sur une machine virtuelle.

Comment activer la mise en réseau accélérée sur une instance Citrix ADC VPX à l'aide de la console Azure

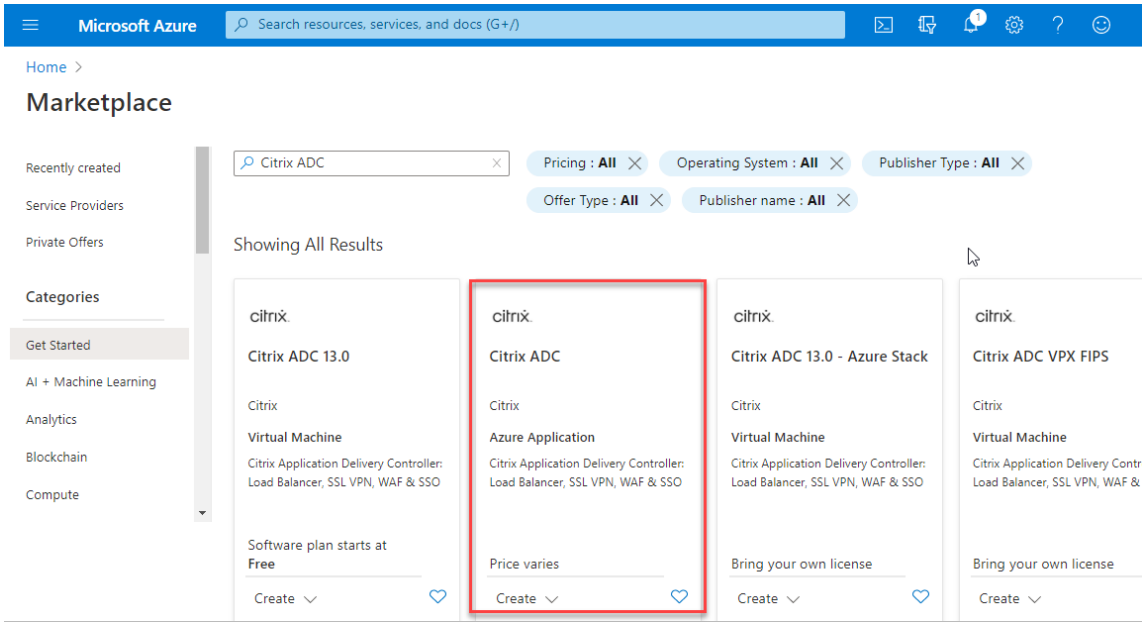
Vous pouvez activer la mise en réseau accélérée sur une interface spécifique à l'aide de la console Azure ou d'Azure PowerShell.

Procédez comme suit pour activer la mise en réseau accélérée à l'aide de jeux de disponibilité ou de zones de disponibilité Azure.

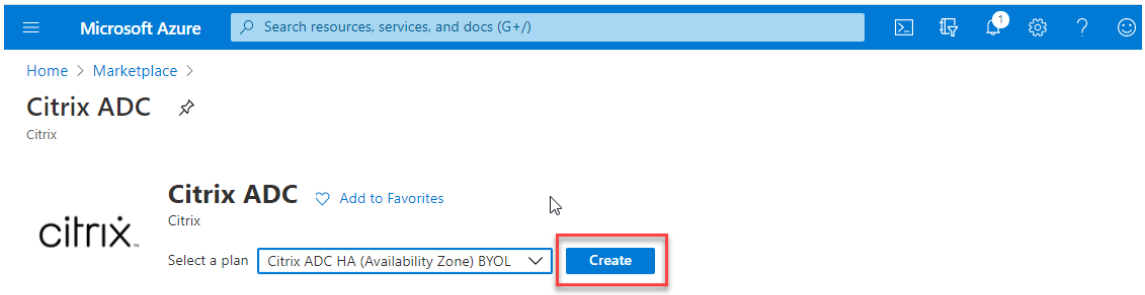
1. Connectez-vous au portail Azureet accédez à **Azure Marketplace**.



2. Depuis **Azure Marketplace**, recherchez **Citrix ADC**.

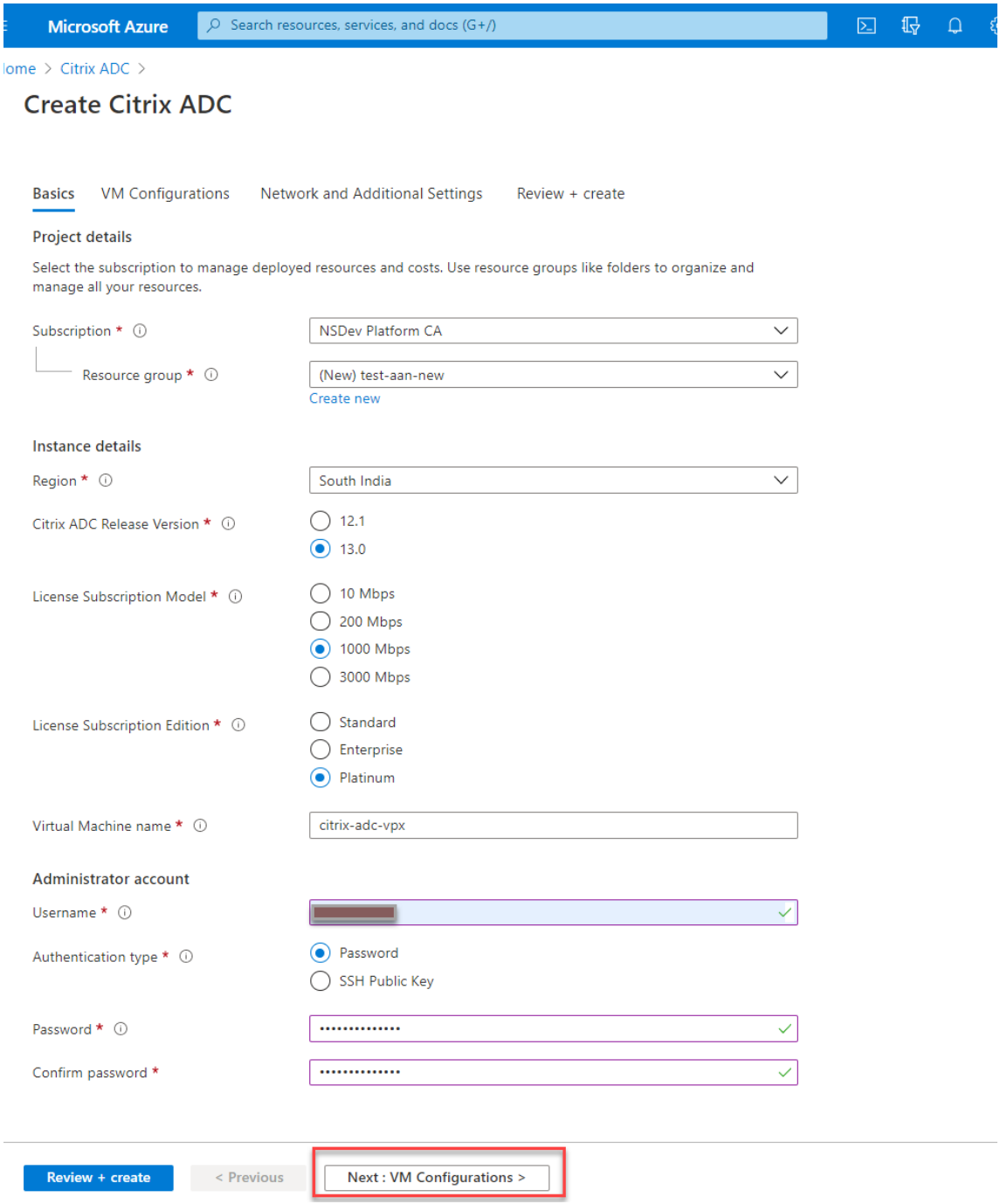


3. Sélectionnez un plan Citrix ADC non FIPS avec une licence, puis cliquez sur **Créer**.



La page **Créer Citrix ADC** apparaît.

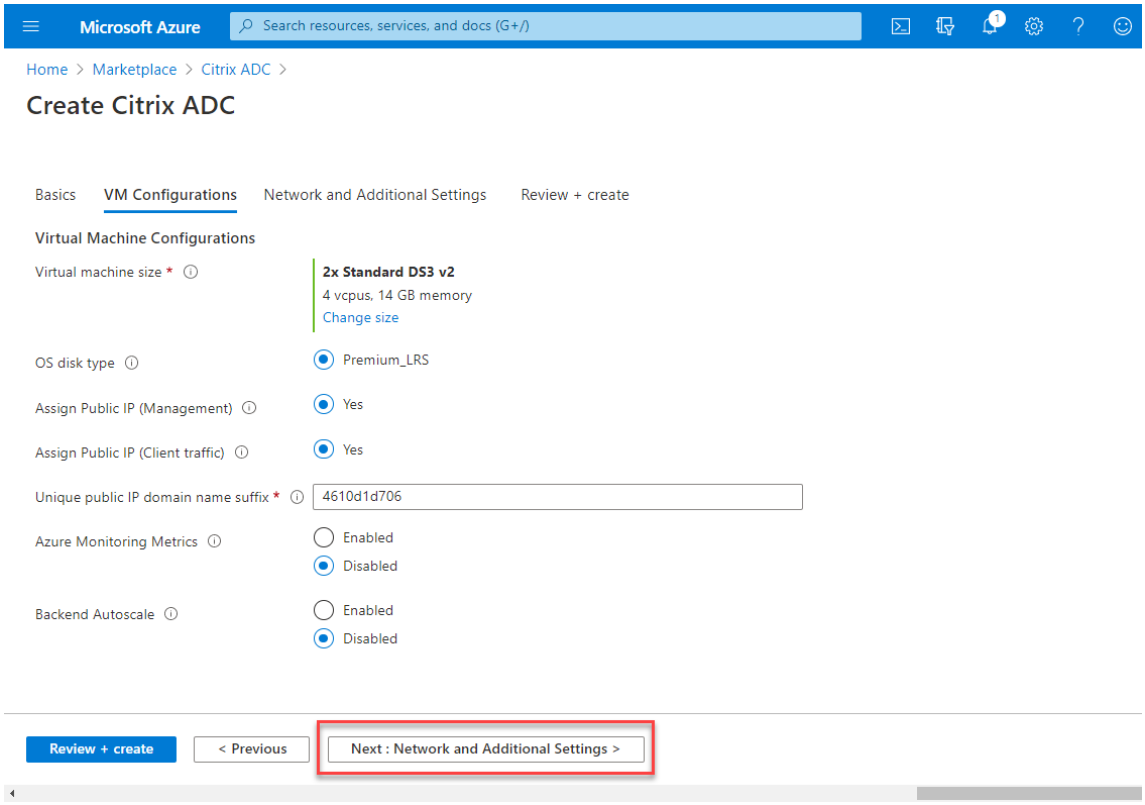
4. Dans l'onglet Notions de **base**, créez un groupe de ressources. Sous l'onglet **Paramètres**, saisissez les détails des champs Région, Nom d'utilisateur Admin, Mot de passe administrateur, type de licence (SKU VM) et d'autres champs.



5. Cliquez sur **Suivant : Configurations de machines virtuelles**.

   Sur la page **Configurations de machines virtuelles**, effectuez les opérations suivantes :

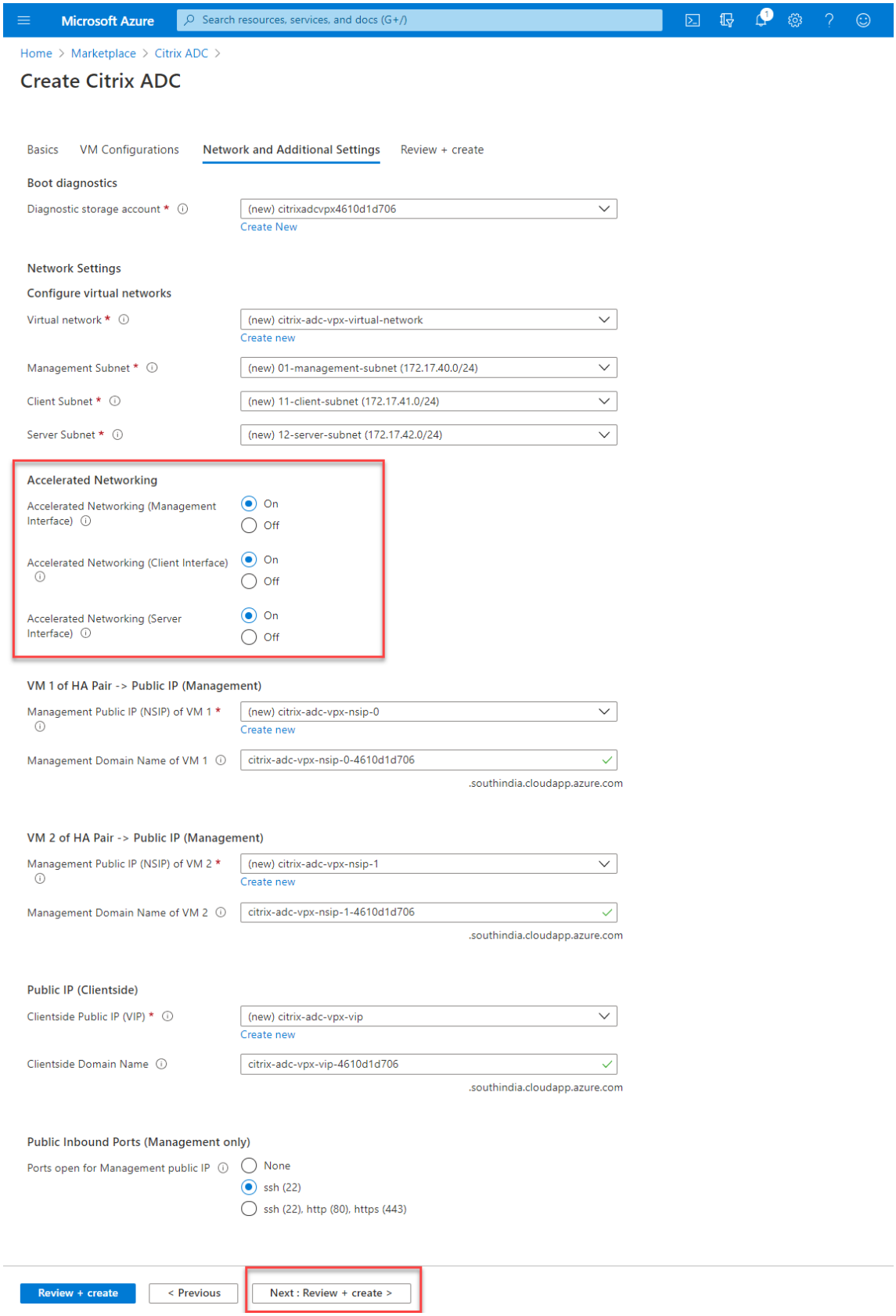
   a) Configurez le suffixe du nom de domaine IP public.
   b) Activez ou désactivez **Azure Monitoring Metrics**.
   c) Activez ou désactivez **Backend Autoscale**.



6. Cliquez sur **Suivant : Paramètres réseau et supplémentaires**.

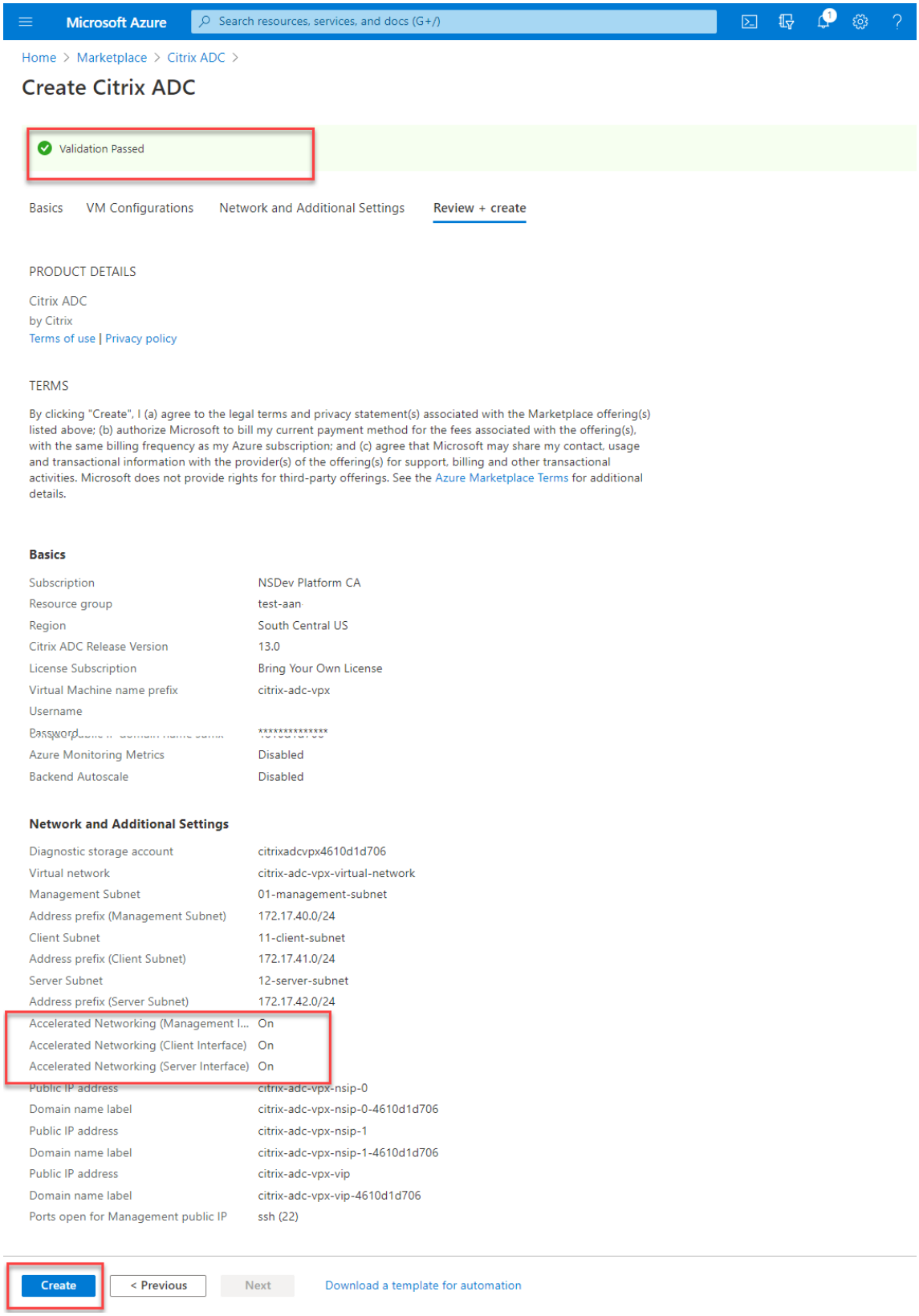
   Sur la page **Network and Additional Settings**, créez un compte de diagnostic de démarrage et configurez les paramètres réseau.

   Dans la section **Accelerated Networking**, vous avez la possibilité d'activer ou de désactiver la mise en réseau accélérée séparément pour l'interface de gestion, l'interface client et l'interface serveur.



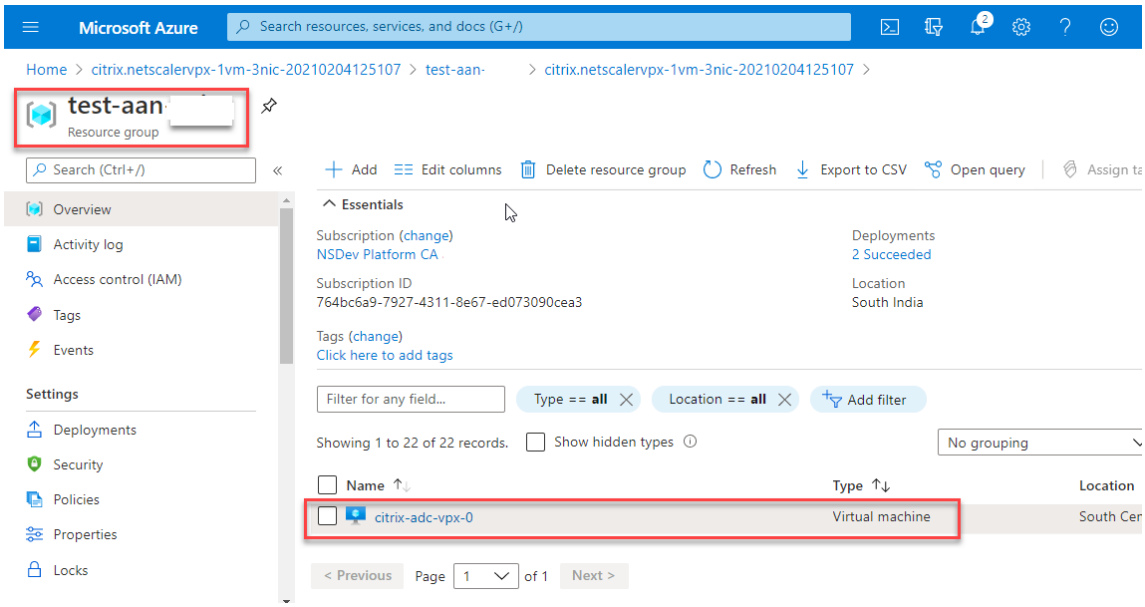
7. Cliquez sur **Next: Review + create >**.

   Une fois la validation réussie, passez en revue les paramètres de base, les configurations de machines virtuelles, le réseau et les paramètres supplémentaires, puis cliquez sur **Créer**. La création du groupe de ressources Azure avec les configurations requises peut prendre un certain temps.

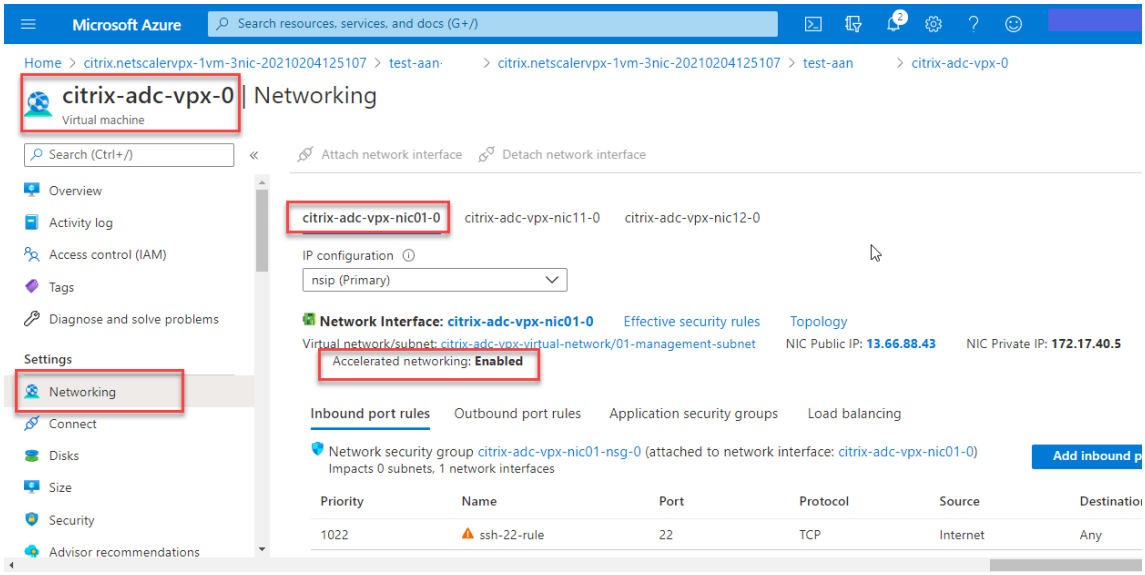


8. Une fois le déploiement terminé, sélectionnez le **groupe de ressources** pour voir les détails de

la configuration.



9. Pour vérifier les configurations Accelerated Networking, sélectionnez **Machine virtuelle > Mise en réseau**. L'état Accelerated Networking s'affiche sous la forme **Activé** ou **Désactivé** pour chaque carte réseau.



Activer la mise en réseau accélérée avec Azure PowerShell

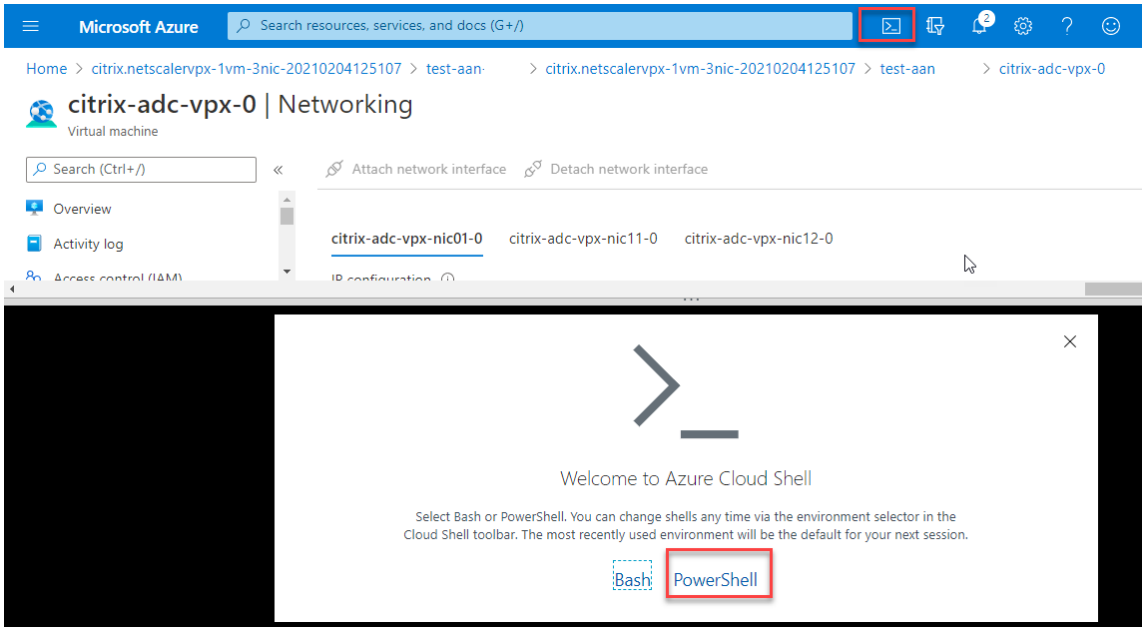
Si vous devez activer la mise en réseau accélérée après la création de la machine virtuelle, vous pouvez le faire à l'aide d'Azure PowerShell.

> Remarque :
>
> Assurez-vous d'arrêter la machine virtuelle avant d'activer Accelerated Networking à l'aide d'Azure PowerShell.

Effectuez les étapes suivantes pour activer la mise en réseau accélérée à l'aide d'Azure PowerShell.

1. Accédez au **portail Azure**, cliquez sur l'icône **PowerShell** dans le coin supérieur droit.

   > Remarque :
   >
   > Si vous êtes en mode Bash, passez au mode PowerShell.



2. À l'invite de commandes, exécutez la commande suivante :

```
az network nic update --name <nic-name> --accelerated-networking [true | false] --resource-group <resourcegroup-name>
<!--NeedCopy-->
```

   Le paramètre de mise en réseau accéléré accepte l'une des valeurs suivantes :

   - **Vrai :** active la mise en réseau accélérée sur la carte réseau spécifiée.
   - **Faux :** désactive la mise en réseau accélérée sur la carte réseau spécifiée.

   Pour activer la mise en réseau accélérée sur une carte réseau spécifique :

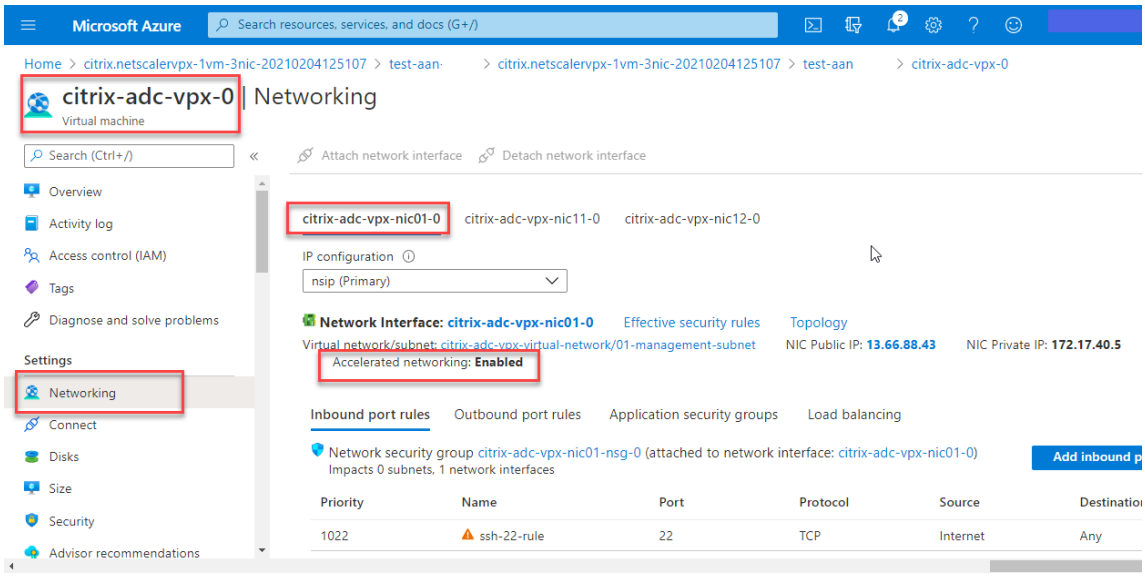
```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking true --resource-group rsgp1-aan
<!--NeedCopy-->
```

   Pour désactiver la mise en réseau accélérée sur une carte réseau spécifique :

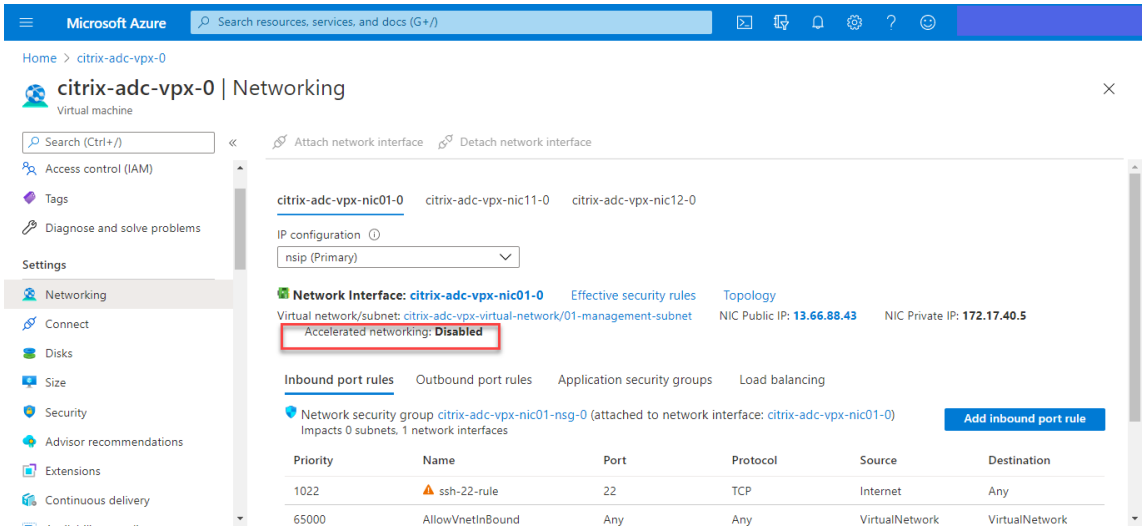

```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking false --resource-group rsgp1-aan
<!--NeedCopy-->
```

3. Pour vérifier l'état Accelerated Networking une fois le déploiement terminé, accédez à **VM > Mise en réseau**.

   Dans l'exemple suivant, vous pouvez voir que la mise en réseau accélérée est **activée**.



   Dans l'exemple suivant, vous pouvez voir que la mise en réseau accélérée est **désactivée**.



Pour vérifier l'accélération de la mise en réseau sur une interface à l'aide de FreeBSD Shell de Citrix ADC

Vous pouvez vous connecter au shell FreeBSD de Citrix ADC et exécuter les commandes suivantes pour vérifier l'état accéléré de la mise en réseau.

Exemple de carte réseau ConnectX3 :

L'exemple suivant montre la sortie de la commande « ifconfig » de la carte réseau Mellanox ConnectX3. Le « 50/n » indique les interfaces VF des cartes réseau Mellanox ConnectX3. 0/1 et 1/1 indiquent les interfaces PV de l'instance Citrix ADC VPX. Vous pouvez observer que l'interface PV (1/1) et l'interface VF CX3 (50/1) ont les mêmes adresses MAC (00:22:48:1 c : 99:3 e). Cela indique que les deux interfaces sont regroupées ensemble.

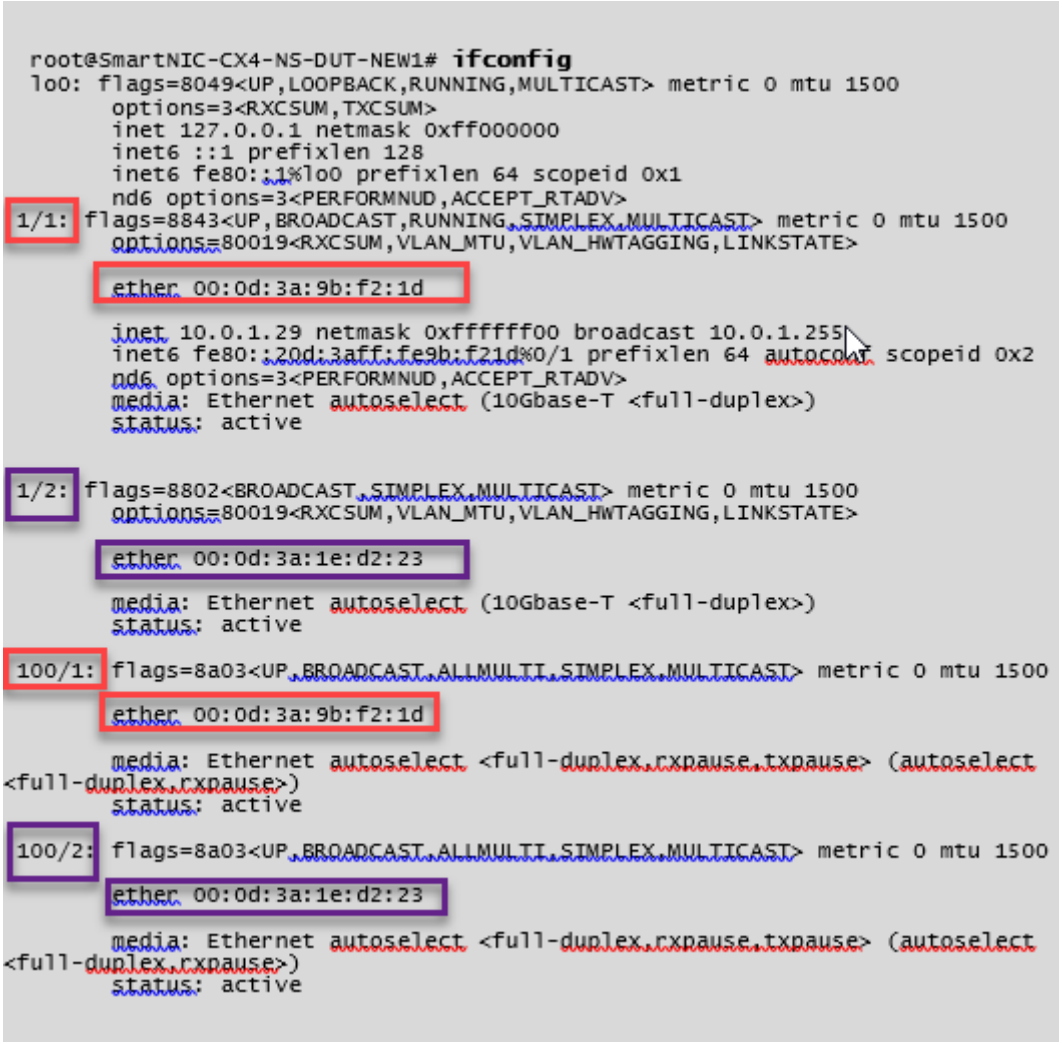

```
root@nvr-us-cx3# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
0/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:0d:3a:98:71:be
        inet 172.16.27.11 netmask 0xffffff00 broadcast 172.16.27.255
        inet6 fe80::20d:3aff:fe98:71be%0/1 prefixlen 64 autoconf scopeid 0x2
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
1/1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
50/1: flags=8842<BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500

options=900b8<VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,VLAN_HWFILTER,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (<unknown subtype>)
        status: active
```

Exemple de carte réseau ConnectX4 :

L'exemple suivant montre la sortie de la commande « ifconfig » de la carte réseau Mellanox ConnectX4. Le « 100/n » indique les interfaces VF des cartes réseau Mellanox ConnectX4. 0/1, 1/1 et 1/2 indique les interfaces PV de l'instance Citrix ADC VPX.

Vous pouvez observer que les interfaces PV (1/1) et CX4 VF (100/1) ont les mêmes adresses MAC (00:0 d:3a:9b:f 2:1 d). Cela indique que les deux interfaces sont regroupées ensemble. De même, l'interface PV (1/2) et l'interface VF CX4 (100/2) ont les mêmes adresses MAC (00:0 d:3a:1e:d 2:23).



Pour vérifier l'accélération de la mise en réseau sur une interface à l'aide d'ADC CLI

Exemple de carte réseau ConnectX3 :

La sortie de commande show interface suivante indique que l'interface PV 1/1 est fournie avec la fonction virtuelle 50/1, qui est une carte réseau VF SR-IOV. Les adresses MAC des cartes réseau 1/1 et 50/1 sont les mêmes. Une fois la mise en réseau accélérée activée, les données de l'interface 1/1 sont envoyées via le chemin de données de l'interface 50/1, qui est une interface ConnectX3. Vous pouvez voir que la sortie « show interface » de l'interface photovoltaïque (1/1) pointe vers le VF (50/1). De même, la sortie « show interface » de l'interface VF (50/1) pointe vers l'interface photovoltaïque (1/1).


```
> show interface 1/1

        Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 50/1 Datapath 50/1) #1
        flags=0xe060 <ENABLED, UP, UP, HEARTBEAT, 802.1q>
        MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m07s
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.

Done

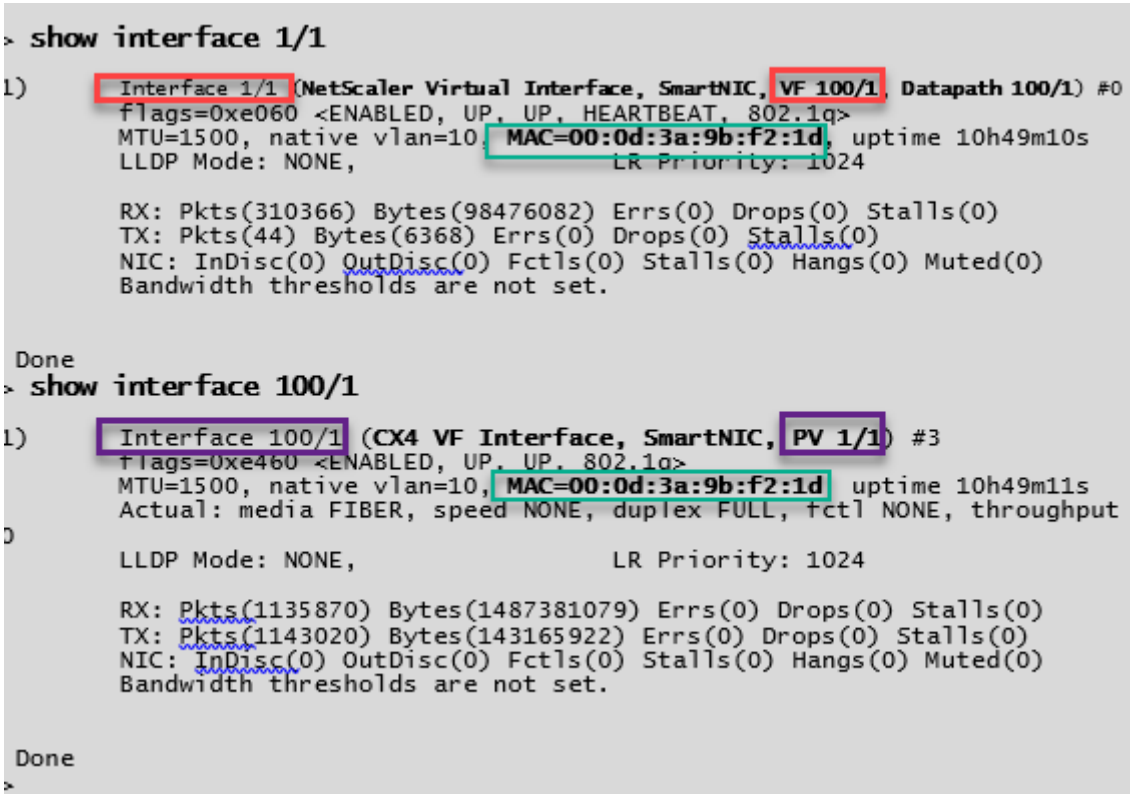
> show interface 50/1

      Interface 50/1 (CX3 VF Interface, SmartNIC, PV 1/1) #2
        flags=0xe460 <ENABLED, UP, UP, 802.1q>
        MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m08s
        Actual: media NONE, speed 50000, duplex FULL, fctl NONE, throughput 50000
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
```

Exemple de carte réseau ConnectX4 :

La sortie de commande show interface suivante indique que l'interface PV 1/1 est fournie avec la fonction virtuelle 100/1, qui est une carte réseau VF SR-IOV. Les adresses MAC des cartes réseau 1/1 et 100/1 sont les mêmes. Une fois la mise en réseau accélérée activée, les données de l'interface 1/1 sont envoyées via le chemin de données de l'interface 100/1, qui est une interface ConnectX4. Vous pouvez voir que la sortie « show interface » de l'interface photovoltaïque (1/1) pointe vers le VF (100/1). De même, la sortie « show interface » de l'interface VF (100/1) pointe vers l'interface photovoltaïque (1/1).



Points à noter dans Citrix ADC

- L'interface photovoltaïque est considérée comme l'interface principale ou principale pour toutes les opérations nécessaires. Les configurations doivent être effectuées uniquement sur des interfaces photovoltaïques.
- Toutes les opérations « set » sur une interface VF sont bloquées à l'exception des opérations suivantes :
  - interface d'activation
  - interface de désactivation
  - interface de réinitialisation
  - statistiques claires

  > Remarque :
  >
  > Citrix recommande de ne pas effectuer d'opérations sur l'interface VF.
- Vous pouvez vérifier la liaison de l'interface PV avec l'interface VF à l'aide de la `show interface` commande.

Configurer un VLAN sur une interface PV

Lorsqu'une interface PV est liée à un VLAN, l'interface VF accélérée associée est également liée au même VLAN que l'interface PV. Dans cet exemple, l'interface PV (1/1) est liée au VLAN (20). L'interface VF (100/1) fournie avec l'interface PV (1/1) est également liée au VLAN 20.

Exemple :

1. Créez un VLAN.

```
add vlan 20
<!--NeedCopy-->
```

2. Liez un VLAN à l'interface PV.

```
bind vlan 20  - ifnum 1/1

show vlan

1)  VLAN ID: 1
    Link-local IPv6 addr: fe80::20d:3aff:fe9b:f21d/64
    Interfaces : LO/1

2)  VLAN ID: 10     VLAN Alias Name:
    Interfaces : 0/1 100/1
    IPs : 10.0.1.29  Mask: 255.255.255.0

3)  VLAN ID: 20     VLAN Alias Name:
    Interfaces :  1/1 100/2

<!--NeedCopy-->
```

> Remarque
>
> L'opération de liaison VLAN n'est pas autorisée sur une interface VF accélérée.

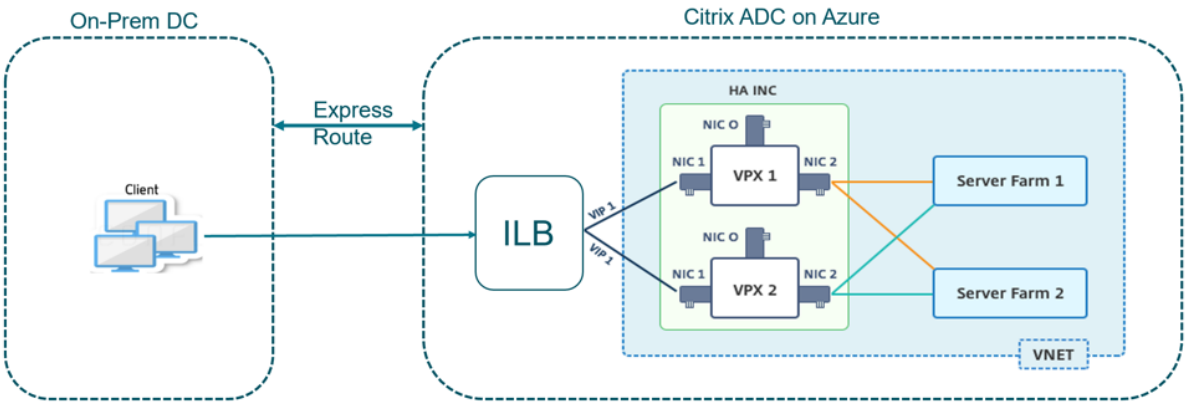
```
bind vlan 1 -ifnum 100/1
ERROR: Operation not permitted
<!--NeedCopy-->
```

Configurer les nœuds HA-INC à l'aide du modèle de haute disponibilité Citrix avec Azure ILB

August 20, 2021

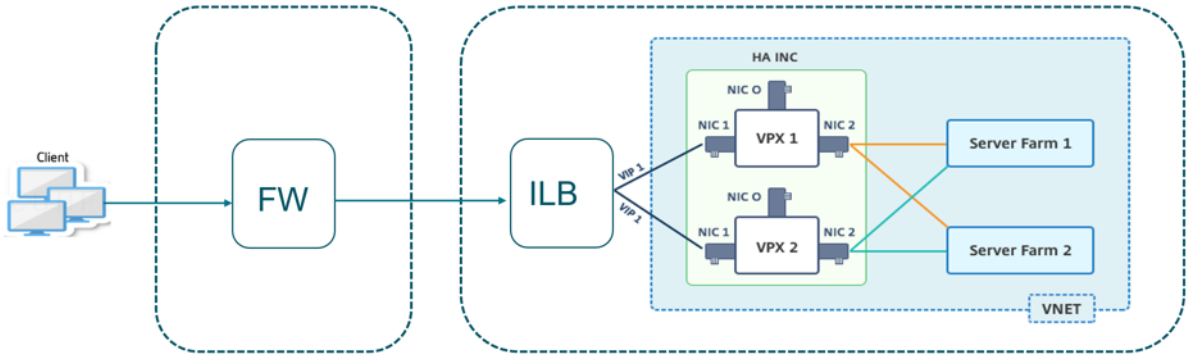
Vous pouvez déployer rapidement et efficacement une paire d'instances VPX en mode HA-INC en utilisant le modèle standard pour les applications intranet. L'équilibrage de charge interne (ILB) Azure utilise une adresse IP interne ou privée pour le front end, comme illustré à la figure 1. Le modèle crée deux nœuds, avec trois sous-réseaux et six cartes réseau. Les sous-réseaux sont destinés à la gestion, au client et au trafic côté serveur, chaque sous-réseau appartenant à une carte réseau différente sur chaque périphérique.

Figure 1 : paire Citrix ADC HA pour les clients d'un réseau interne



Vous pouvez également utiliser ce déploiement lorsque la paire Citrix ADC HA est derrière un pare-feu, comme illustré à la Figure 2. L'adresse IP publique appartient au pare-feu et est NAT à l'adresse IP frontale de l'ILB.

Figure 2 : paire Citrix ADC HA avec pare-feu ayant une adresse IP publique

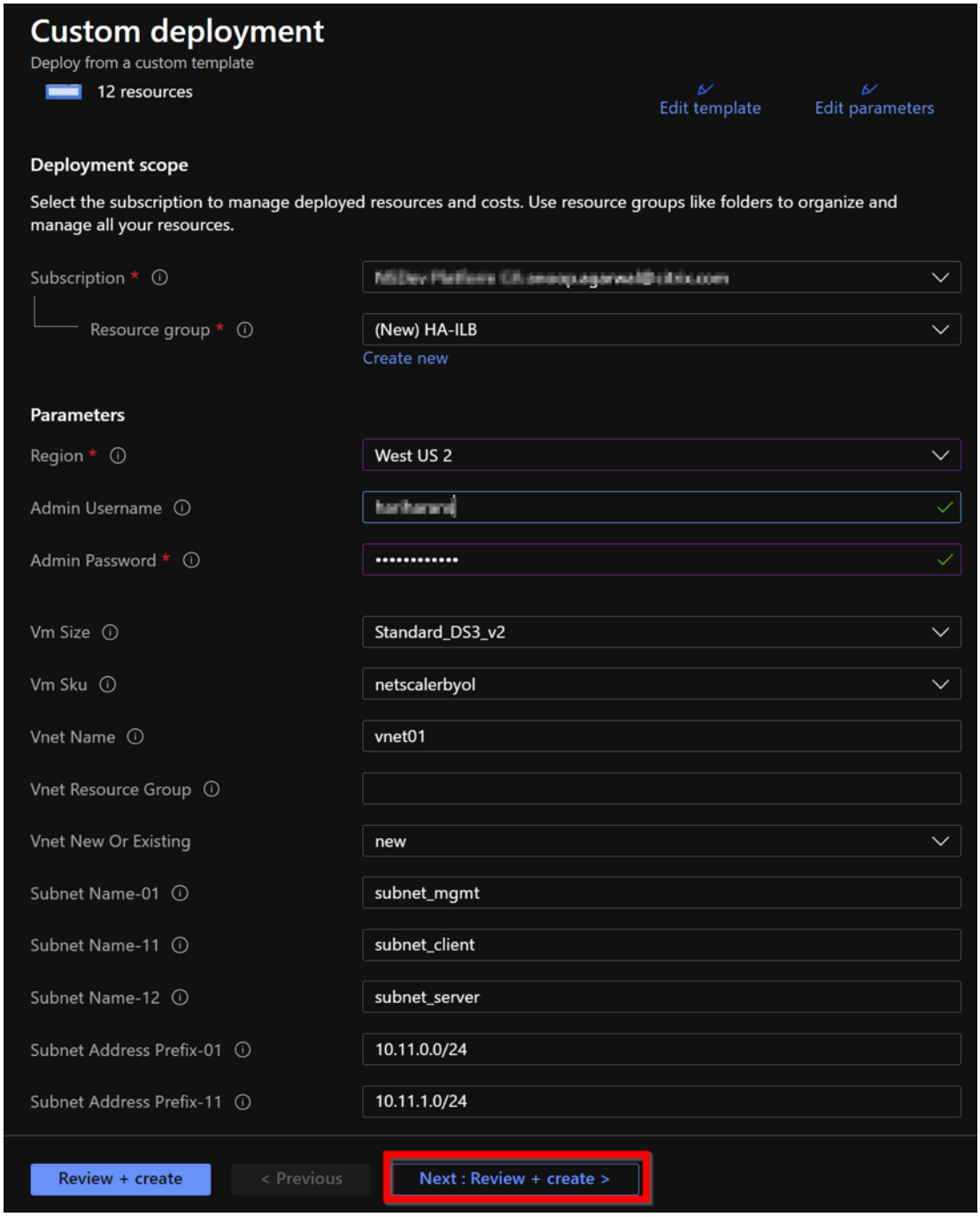


Vous pouvez obtenir le modèle de paire Citrix ADC HA pour les applications intranet sur le portail Azure.

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité à l'aide des jeux de disponibilité Azure.

1. À partir du portail Azure, accédez à la page **Déploiement personnalisé**.
2. La page **Bases** s'affiche. Créez un groupe de ressources. Sous l'onglet **Paramètres**, entrez les

détails de la région, du nom d'utilisateur administrateur, du mot de passe administrateur, du type de licence (`VM sku`) et d'autres champs.

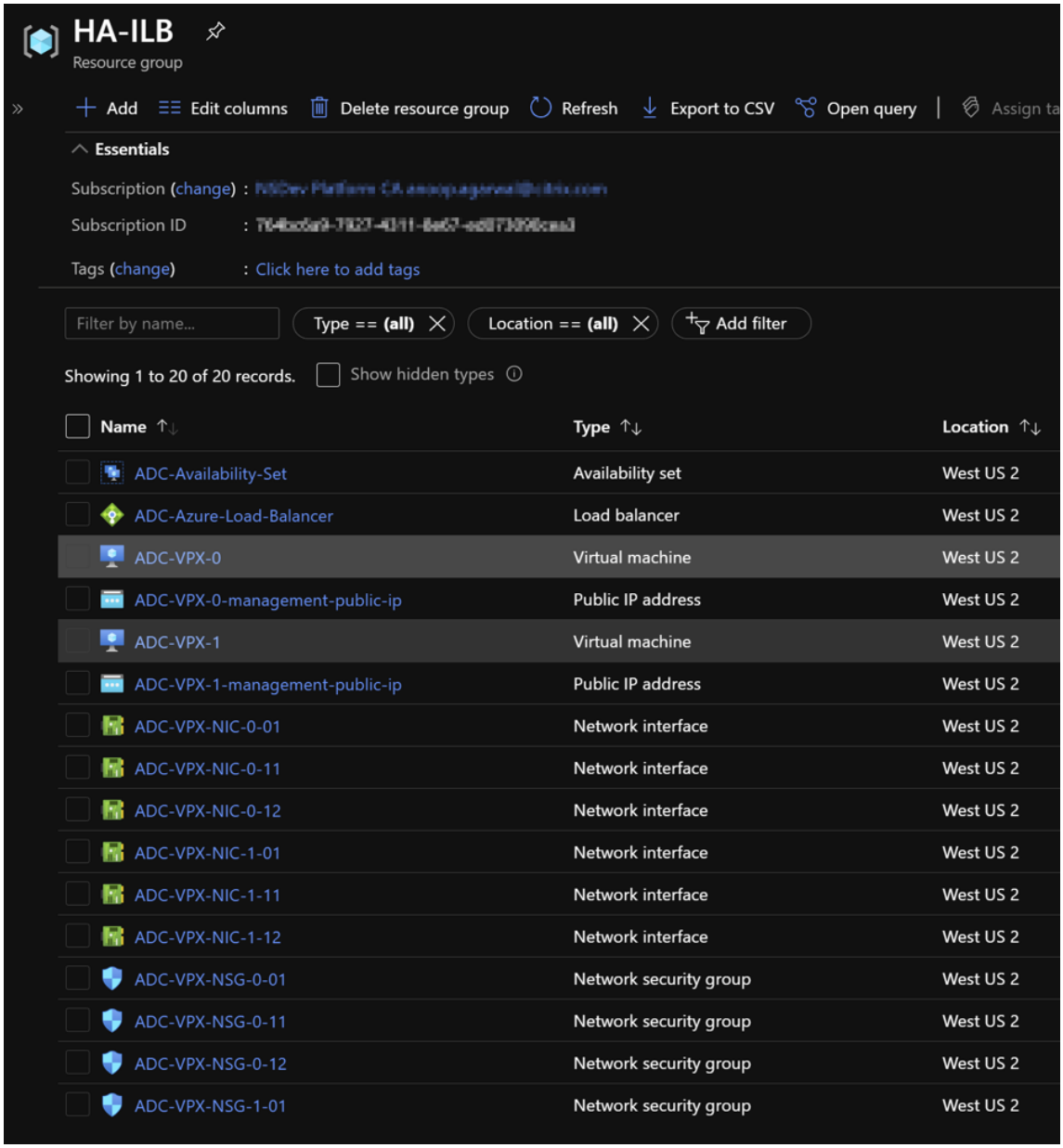


3. Cliquez sur **Next : Review + create >**.

   Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois terminé, sélectionnez le groupe de ressources dans le portail Azure pour afficher les détails de configuration, tels que les règles de LB, les pools back-end, les sondes d'intégrité. La paire haute disponibilité apparaît sous la forme ADC-VPX-0 et ADC-VPX-1.

Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.

Une fois la configuration requise terminée, les ressources suivantes sont créées.



4. Vous devez vous connecter aux nœuds **ADC-VPX-0** et **ADC-VPX-1** pour valider la configuration suivante :

   - Les adresses NSIP pour les deux nœuds doivent se trouver dans le sous-réseau de gestion.
   - Sur les nœuds principal (ADC-VPX-0) et secondaire (ADC-VPX-1), vous devez voir deux adresses SNIP. Un SNIP (sous-réseau client) est utilisé pour répondre aux sondes ILB et l'autre SNIP (sous-réseau serveur) est utilisé pour la communication du serveur back-end.

> Remarque
>
> En mode HA-INC, l'adresse SNIP des machines virtuelles ADC-VPX-0 et ADC-VPX-1 est différente dans le même sous-réseau, contrairement au déploiement ADC HA local classique où les deux sont identiques.
> Pour prendre en charge les déploiements lorsque le SNIP de la paire VPX se trouve dans des sous-réseaux différents ou chaque fois que le VIP ne se trouve pas dans le même sous-réseau qu'un SNIP, vous devez soit activer le transfert basé sur Mac (MBF), soit ajouter une route hôte statique pour chaque VIP à chaque nœud VPX.

Sur le nœud principal (ADC-VPX-0)

```
> sh ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      10.11.0.5        0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      10.11.1.5        0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      10.11.3.4        0               SNIP             Active   Enabled  Enabled  NA       Enabled
 Done
>
>
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.5 (ADC-VPX-0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:20:26 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.4
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

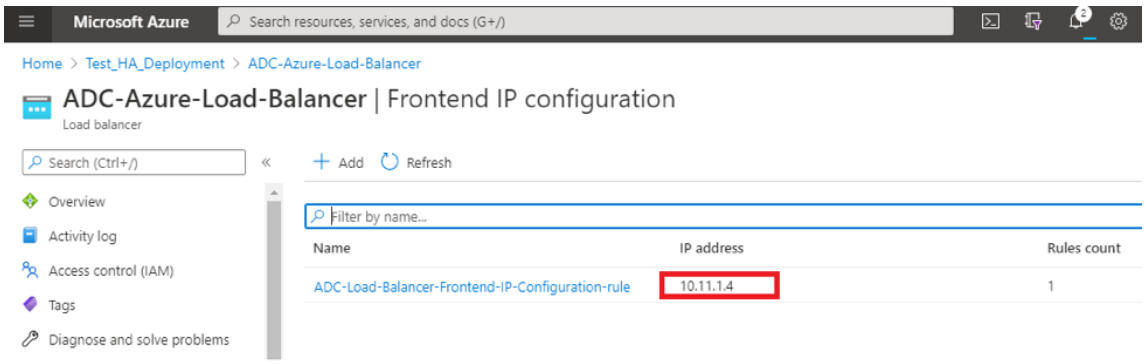

Sur le nœud secondaire (ADC-VPX-1)

```
> sh ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -----
1)      10.11.0.4        0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      10.11.1.6        0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      10.11.3.5        0               SNIP             Active   Enabled  Enabled  NA       Enabled
 Done
>
>
```

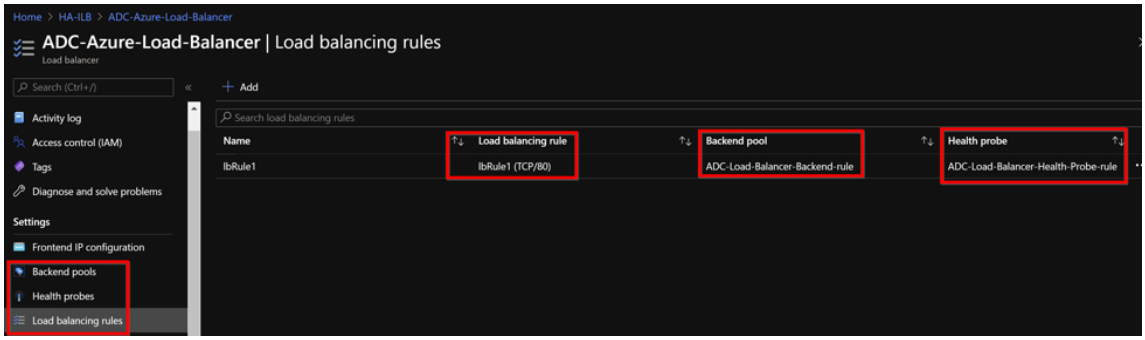
```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.4 (ADC-VPX-1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:24:18 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.5
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

5. Une fois que les nœuds principal et secondaire sont UP et que l' état de synchronisation est **SUCCESS**, vous devez configurer le serveur virtuel d'équilibrage de charge ou le serveur virtuel de passerelle sur le nœud principal (ADC-VPX-0) avec l'adresse IP flottante privée (FIP) de l'équilibreur de charge Azure ADC. Pour plus d'informations, consultez la section Exemple de configuration .

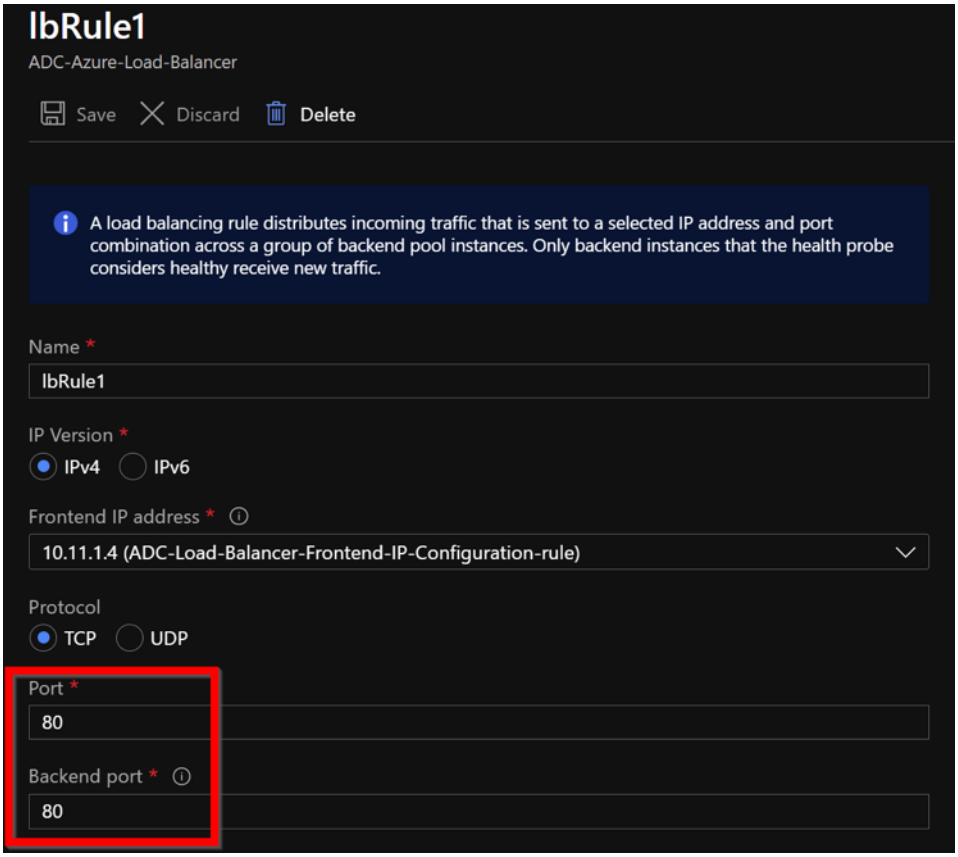
6. Pour rechercher l'adresse IP privée de l'équilibreur de charge ADC Azure, accédez au **portail Azure > AdC Azure Load Balancer > Configuration IP frontend**.



7. Dans la page de configuration d' **Azure Load Balancer**, le déploiement de modèles ARM permet de créer la règle de la LB, les pools back-end et les sondes d'intégrité.

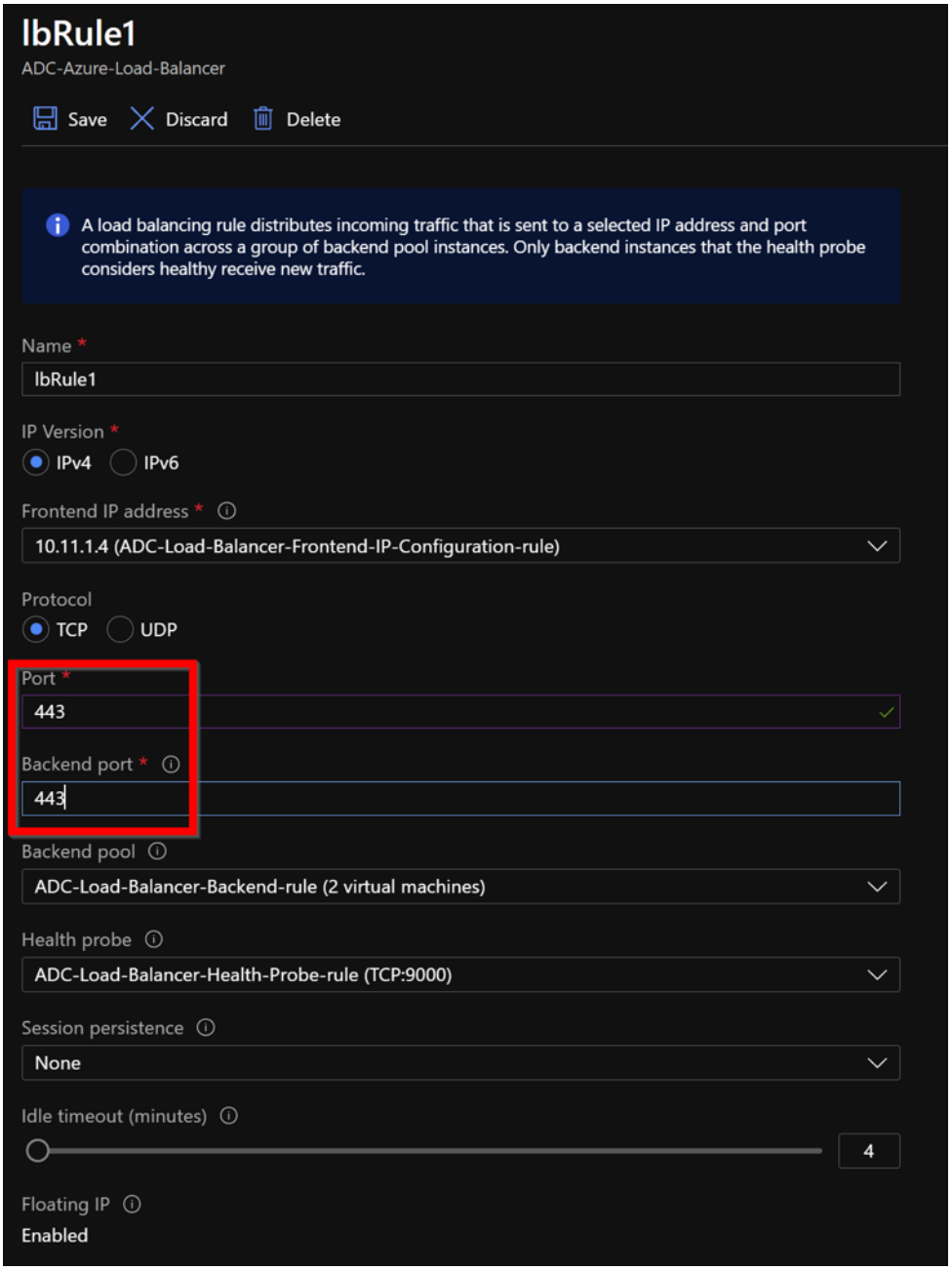


   - La règle LB (LBrule1) utilise le port 80, par défaut.



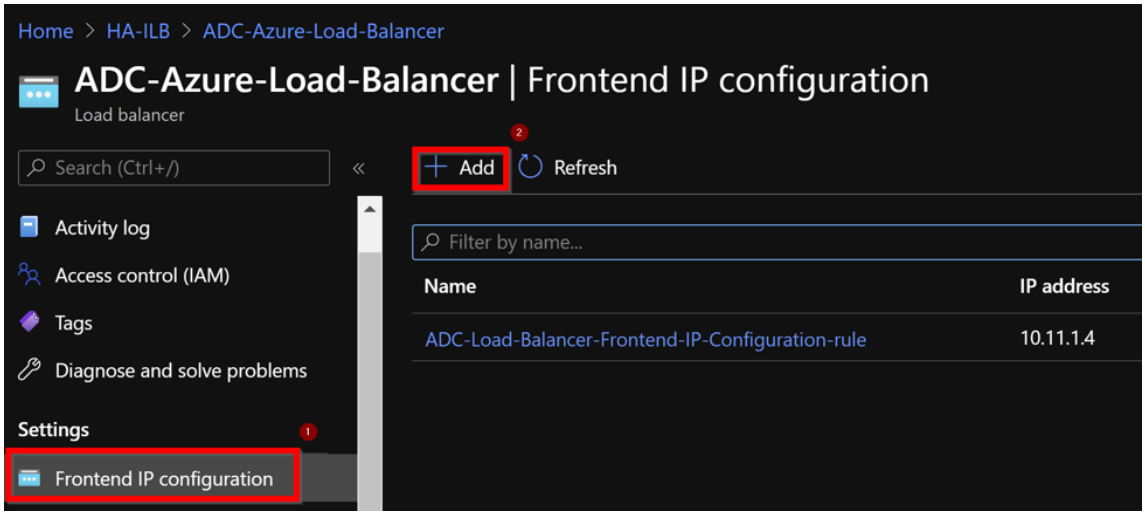
- Modifiez la règle pour utiliser le port 443 et enregistrez les modifications.

> Remarque
>
> Pour une sécurité accrue, Citrix vous recommande d'utiliser le port SSL 443 pour le serveur virtuel LB ou le serveur virtuel de passerelle.

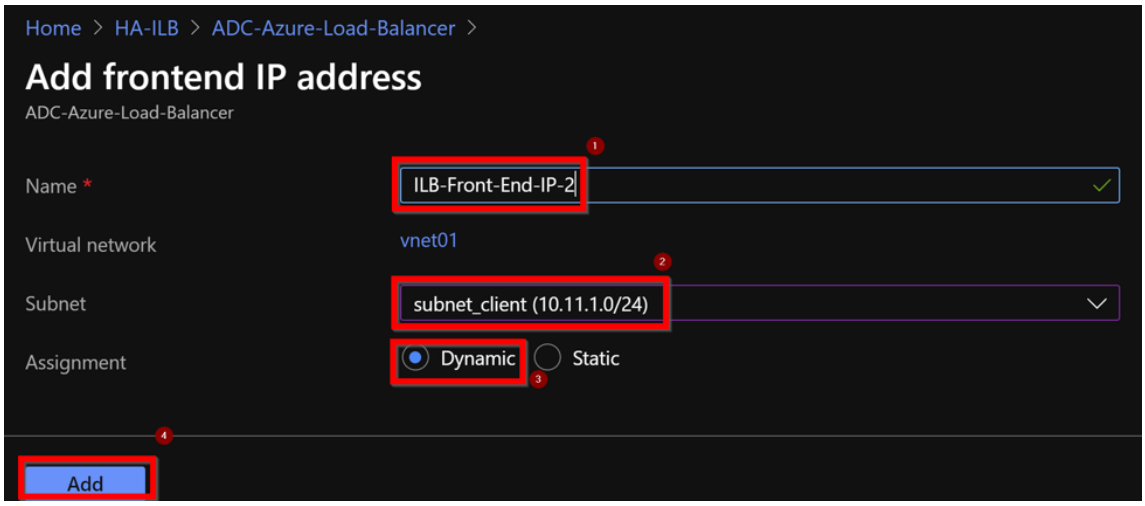


Pour ajouter d'autres adresses VIP sur ADC, effectuez les opérations suivantes :

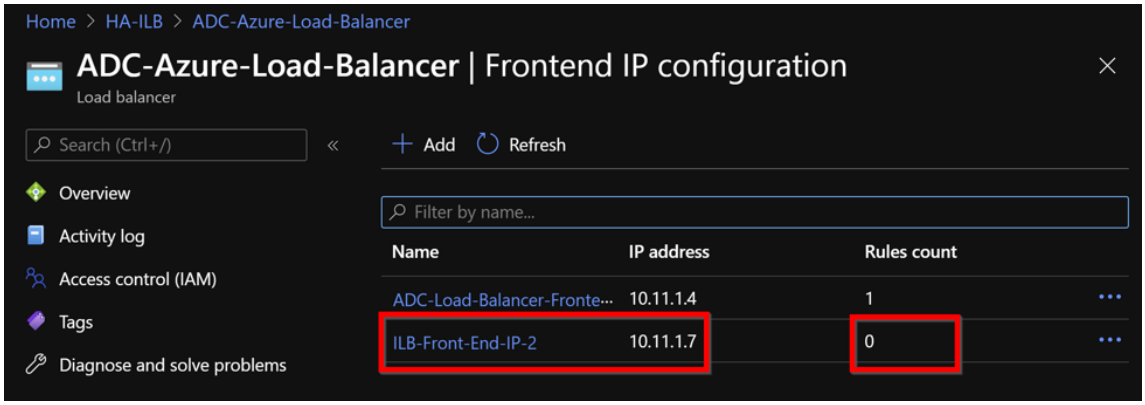
1. Accédez à **Azure Load Balancer > Configuration IP frontend**, puis cliquez sur **Ajouter** pour créer une adresse IP d'équilibrage de charge interne.



2. Dans la page **Ajouter une adresse IP frontale**, entrez un nom, choisissez le sous-réseau client, attribuez une adresse IP dynamique ou statique, puis cliquez sur **Ajouter**.

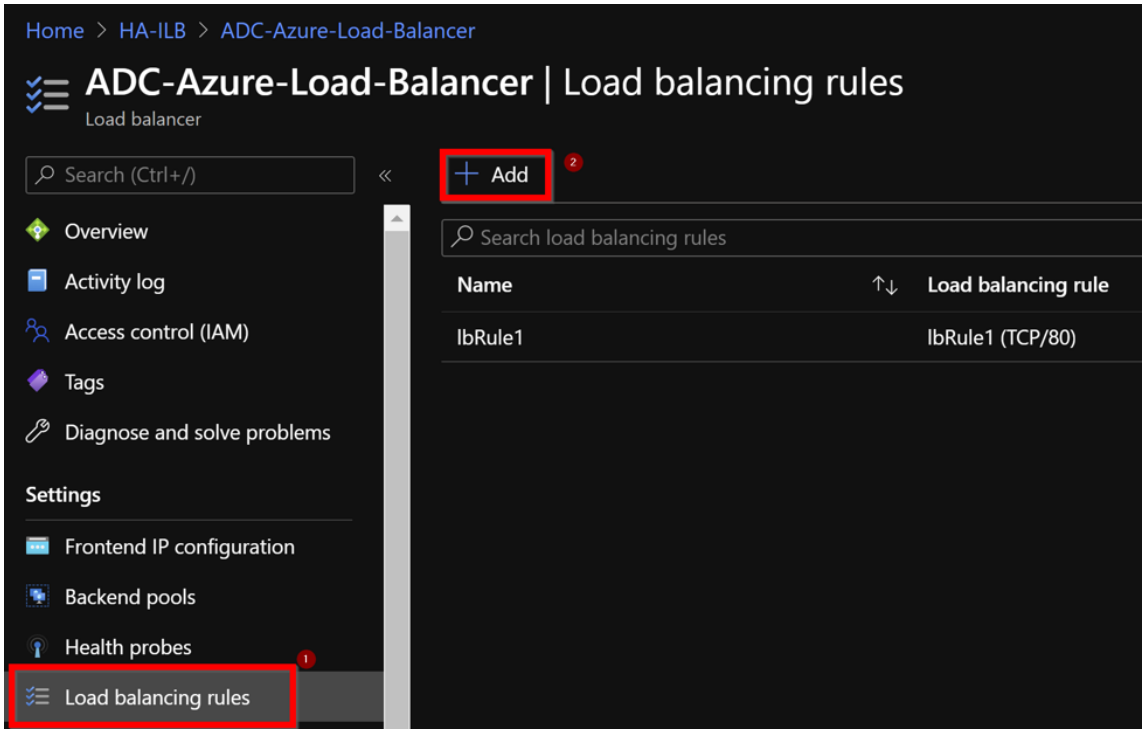


3. L'adresse IP frontale est créée mais aucune règle de LB n'est associée. Créez une nouvelle règle d'équilibrage de charge et associez-la à l'adresse IP frontale.

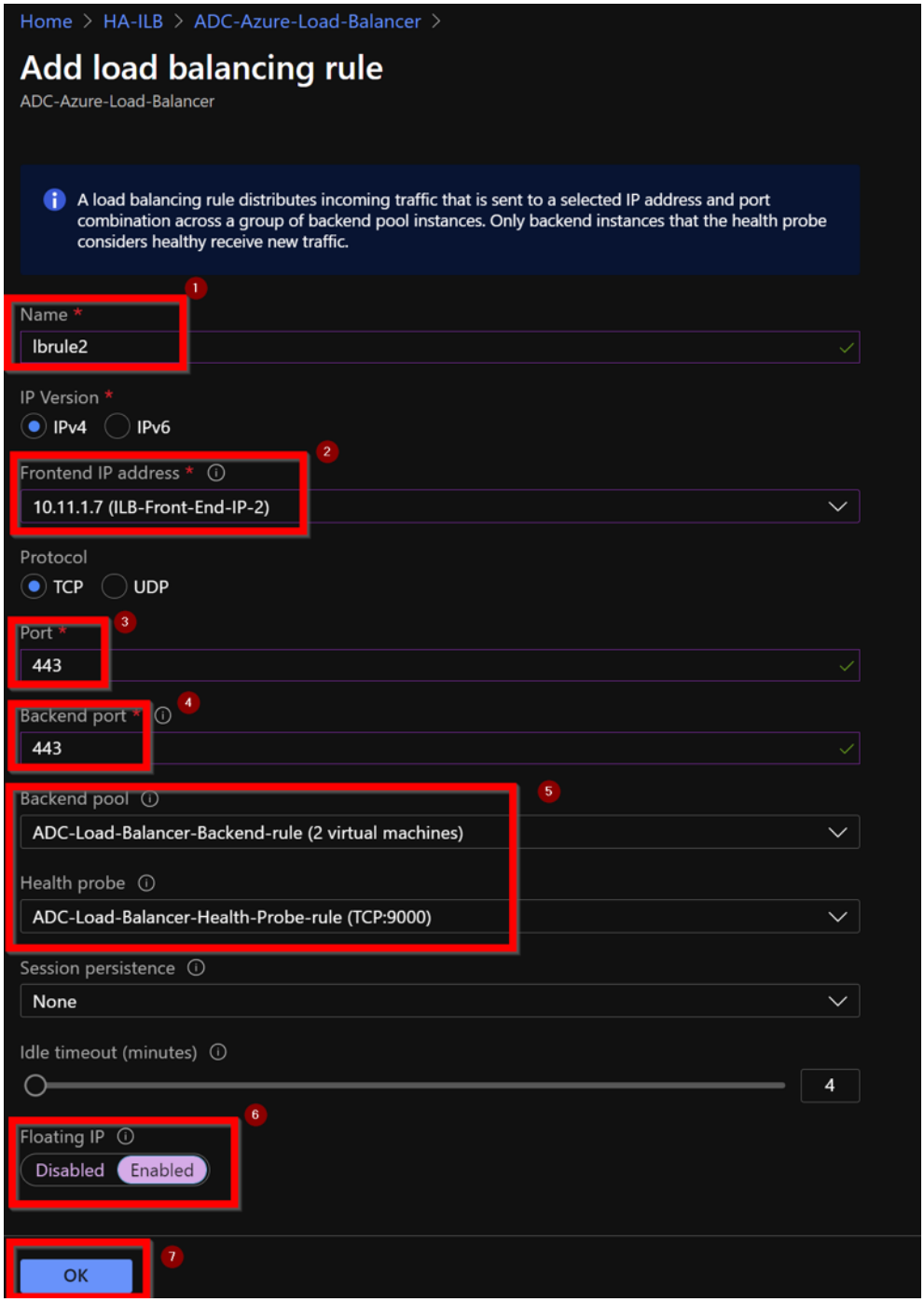


4. Dans la page **Équilibreur de charge Azure**, sélectionnez **Règles d'équilibrage de charge**, puis

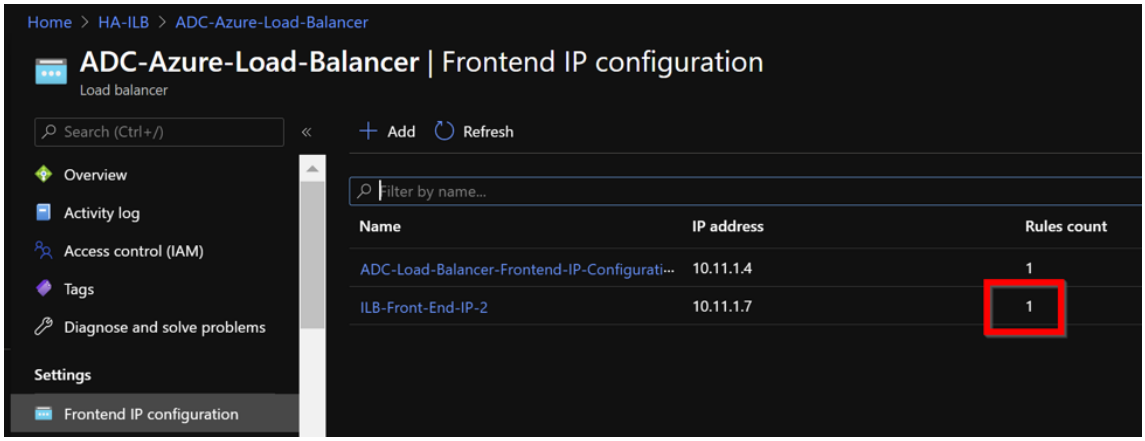
cliquez sur **Ajouter**.



5. Créez une nouvelle règle de LB en choisissant la nouvelle adresse IP frontale et le port. Le champ**IP flottant** doit être défini sur **Activé**.



6. Maintenant, la **configuration IP frontend** affiche la règle LB qui est appliquée.



Exemple de configuration

Pour configurer un serveur virtuel VPN de passerelle et un serveur virtuel d'équilibrage de charge, exécutez les commandes suivantes sur le nœud principal (ADC-VPX-0). La configuration se synchronise automatiquement avec le nœud secondaire (ADC-VPX-1).

Exemple de configuration de passerelle

```
enable feature aaa LB SSL SSLVPN
enable ns mode MBF
add vpn vserver vpn_ssl SSL 10.11.1.4 443
add ssl certKey ckp -cert wild-cgwsanity.cer -key wild-cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
<!--NeedCopy-->
```

Exemple de configuration d'équilibrage de charge

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 10.11.1.7 443
bind ssl vserver lb_vs1 -certkeyName ckp
<!--NeedCopy-->
```

Vous pouvez désormais accéder au serveur virtuel d'équilibrage de charge ou VPN à l'aide du nom de domaine complet (FQDN) associé à l'adresse IP interne d'ILB.

Reportez-vous à la section **Ressources** pour plus d'informations sur la configuration du serveur virtuel d'équilibrage de charge.

Ressources :

Les liens suivants fournissent des informations supplémentaires relatives au déploiement HA et à la configuration du serveur virtuel :

- Configuration des nœuds haute disponibilité dans différents sous-réseaux
- Configurer l'équilibrage de charge de base

Ressources connexes :

- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell
- Configuration de GSLB sur un déploiement HA actif de secours sur Azure

Configurer les nœuds HA-INC à l'aide du modèle haute disponibilité Citrix pour les applications connectées à Internet

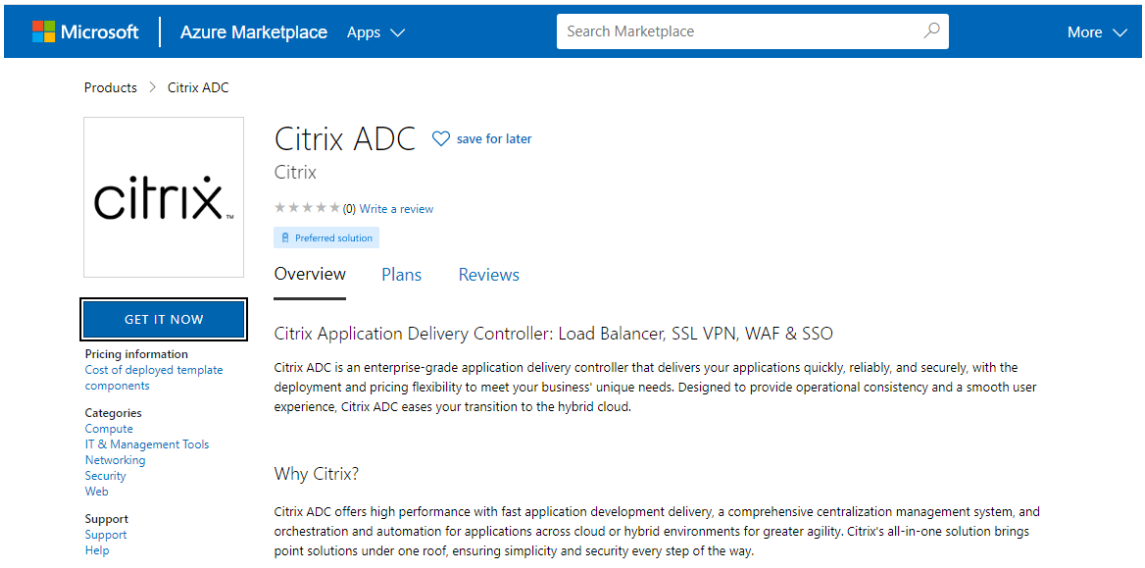
August 20, 2021

Vous pouvez déployer rapidement et efficacement une paire d'instances VPX en mode HA-INC à l'aide du modèle standard pour les applications connectées à Internet. L'équilibrage de charge Azure (ALB) utilise une adresse IP publique pour le front end. Le modèle crée deux nœuds, avec trois sous-réseaux et six cartes réseau. Les sous-réseaux sont destinés à la gestion, au client et au trafic côté serveur. Chaque sous-réseau possède deux cartes réseau pour les deux instances VPX.

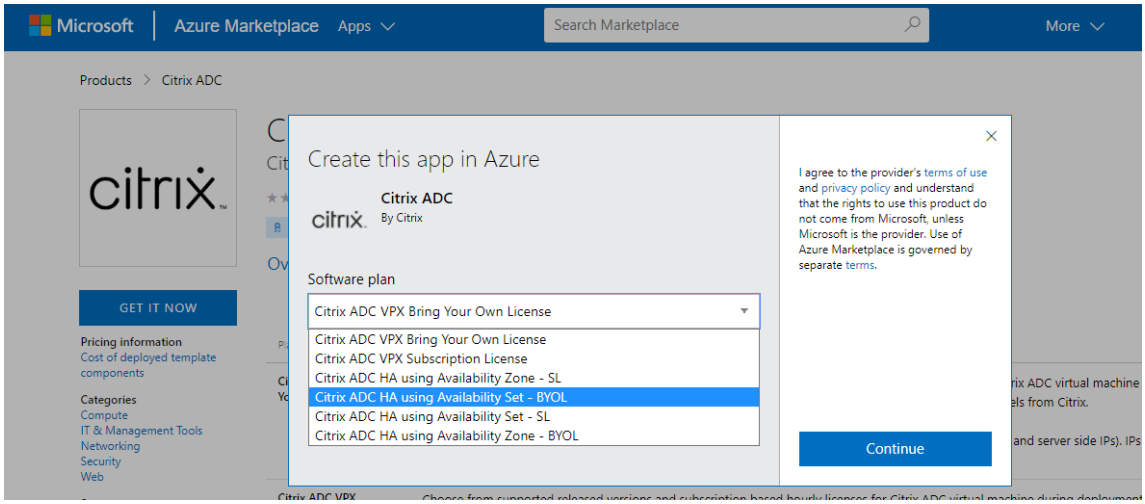
Vous pouvez obtenir le modèle de paire Citrix ADC HA pour les applications connectées à Internet sur Azure Marketplace.

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité à l'aide de jeux de disponibilité Azure ou d'une zone de disponibilité.

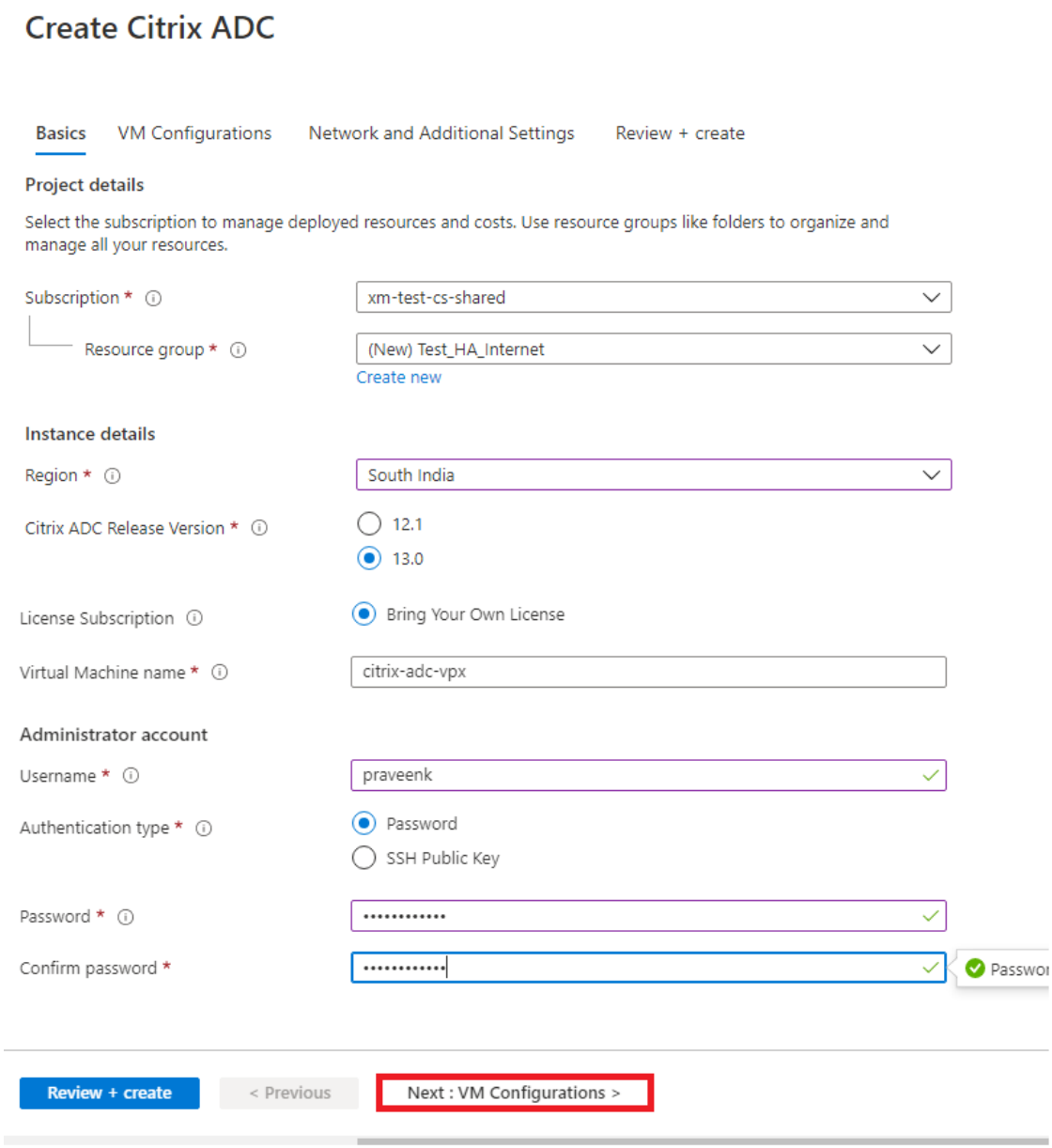
1. Sur la Place de marché Azure, recherchez **Citrix ADC**.
2. Cliquez sur **GET IT NOW**.



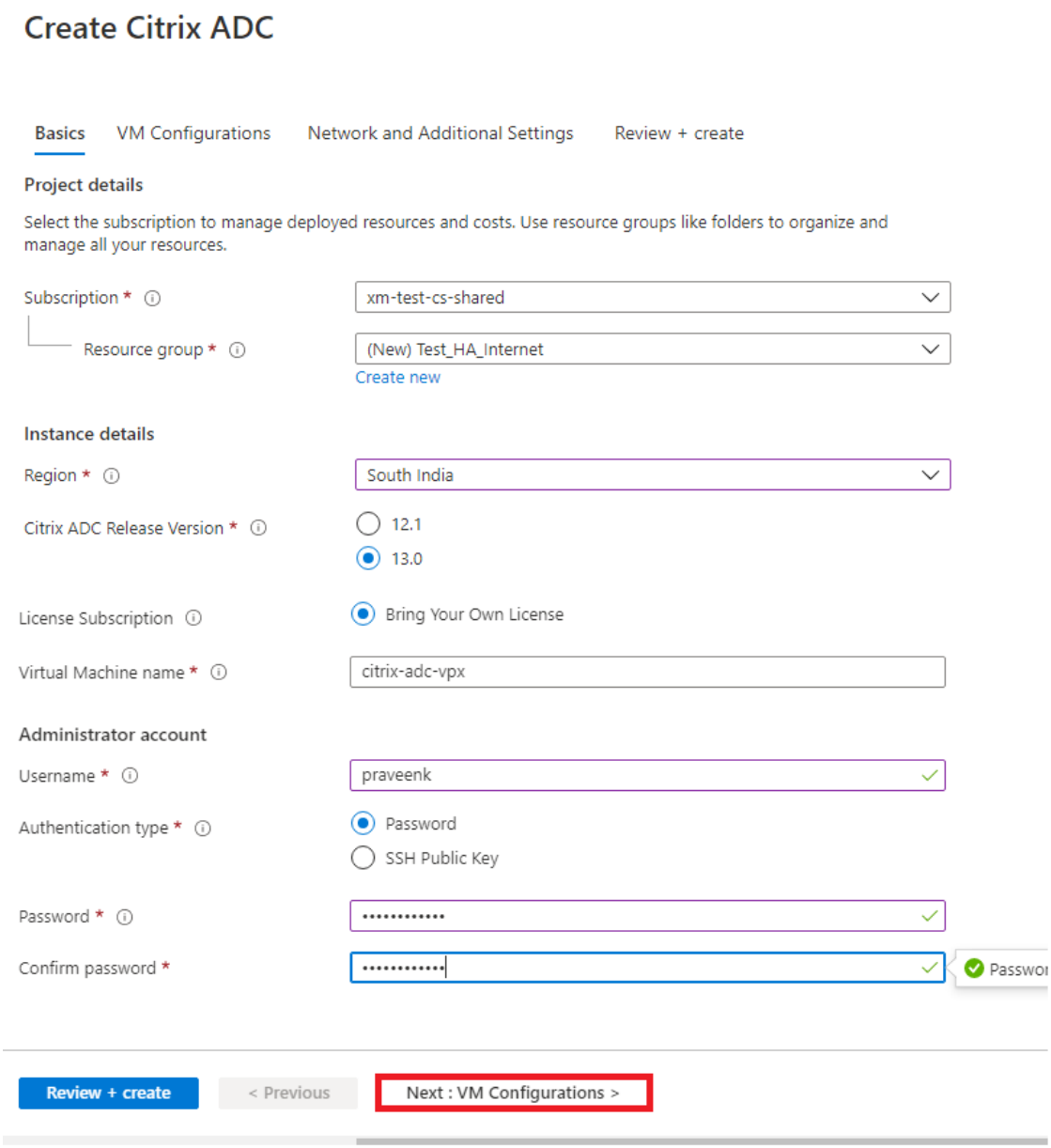
3. Sélectionnez le déploiement HA requis ainsi que la licence, puis cliquez sur **Continuer**.



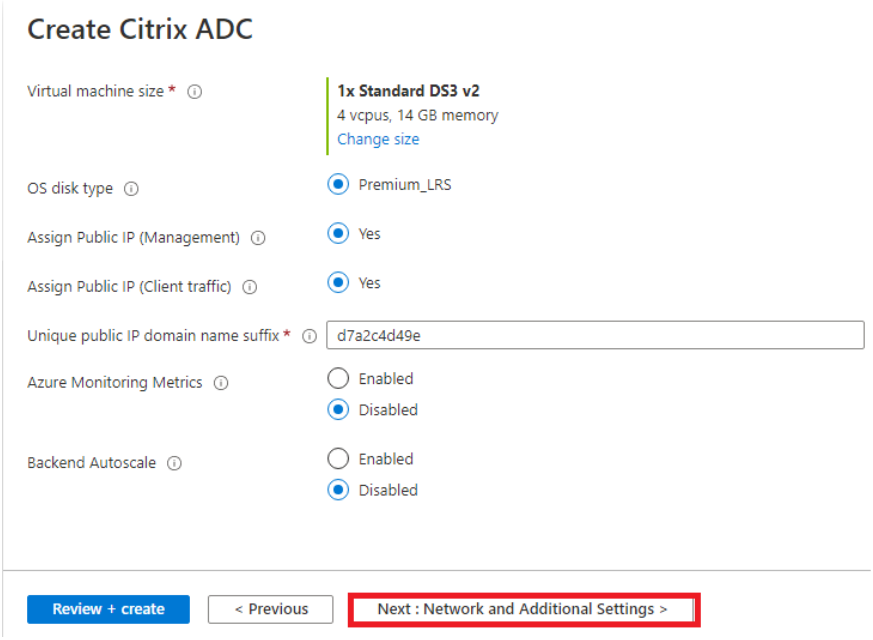
4. La page **Bases** s'affiche. Créez un groupe de ressources. Sous l'onglet **Paramètres**, saisissez les détails des champs Région, Nom d'utilisateur Admin, Mot de passe administrateur, type de licence (SKU VM) et d'autres champs.



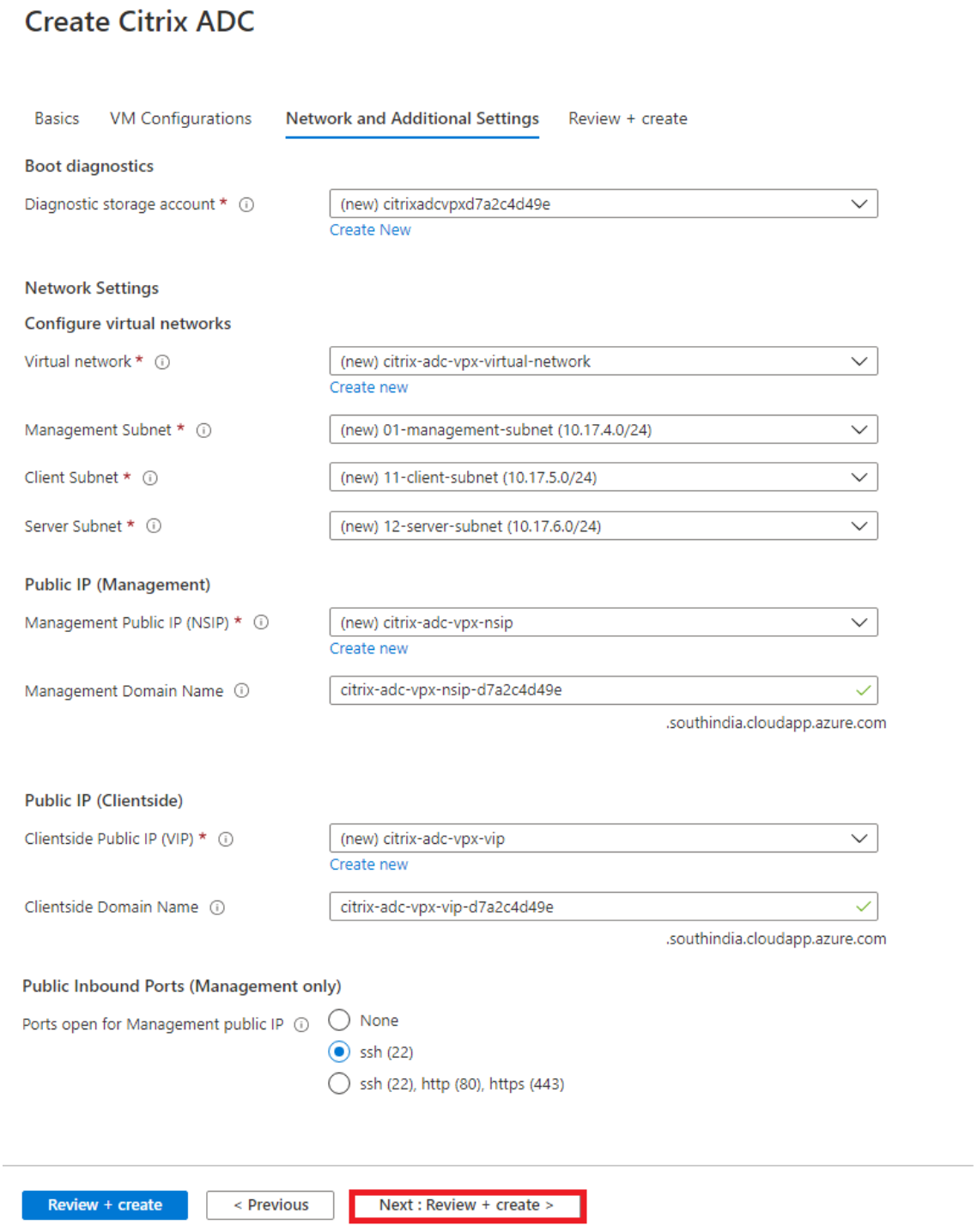
5. Cliquez sur **Suivant : Configurations de machines virtuelles**.



6. Sur la page **Configurations de machines virtuelles**, effectuez les opérations suivantes :
   - Configurer le suffixe du nom de domaine IP public
   - Activer ou désactiver les **mesures Azure Monitoring**
   - Activer ou désactiver la mise à l' **échelle automatique du backend**
7. Cliquez sur **Suivant : Paramètres réseau et paramètres supplémentaires**



8. Sur la page **Paramètres réseau et paramètres supplémentaires**, créez un compte de diagnostic de démarrage et configurez les paramètres réseau.

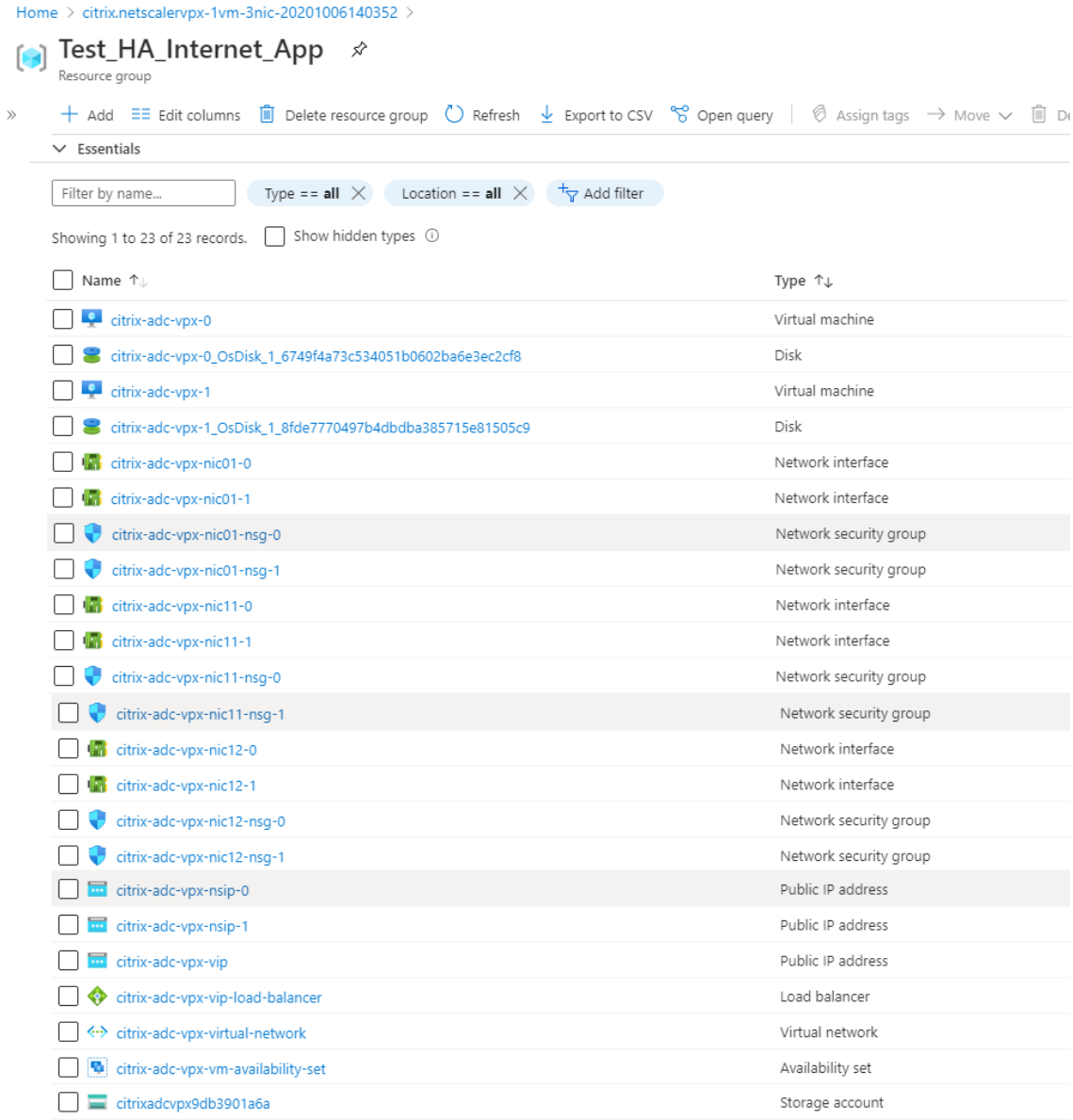


9. Cliquez sur **Next: Review + create >**.
10. Vérifiez les paramètres de base, la configuration de la machine virtuelle, le réseau et les paramètres supplémentaires, puis cliquez sur **Créer**.

Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois terminé, sélectionnez le groupe de ressources dans le portail Azure pour afficher les détails de configuration, tels que les règles de LB, les pools back-end et les sondes d'intégrité. La paire haute disponibilité apparaît comme **citrix-adc-vpx-0** et **citrix-adc-vpx-1**.

Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.

Une fois la configuration requise terminée, les ressources suivantes sont créées.



11. Vous devez vous connecter aux nœuds **citrix-adc-vpx-0** et **citrix-adc-vpx-1** pour valider la configuration suivante :

    - Les adresses NSIP pour les deux nœuds doivent se trouver dans le sous-réseau de gestion.

- Sur les nœuds principal (citrix-adc-vpx-0) et secondaire (citrix-adc-vpx-1), vous devez voir deux adresses SNIP. Un SNIP (sous-réseau client) est utilisé pour répondre aux sondes ALB et l'autre SNIP (sous-réseau serveur) est utilisé pour la communication du serveur principal.

> Remarque
>
> En mode HA-INC, les adresses SNIP des machines virtuelles citrix-adc-vpx-0 et citrix-adc-vpx-1 sont différentes, contrairement au déploiement ADC haute disponibilité local classique où les deux sont identiques.

Sur le nœud principal (citrix-adc-vpx-0)

```
> sh ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.18.0.4        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.4 (ns-vpx0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:34:21 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.5
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
```

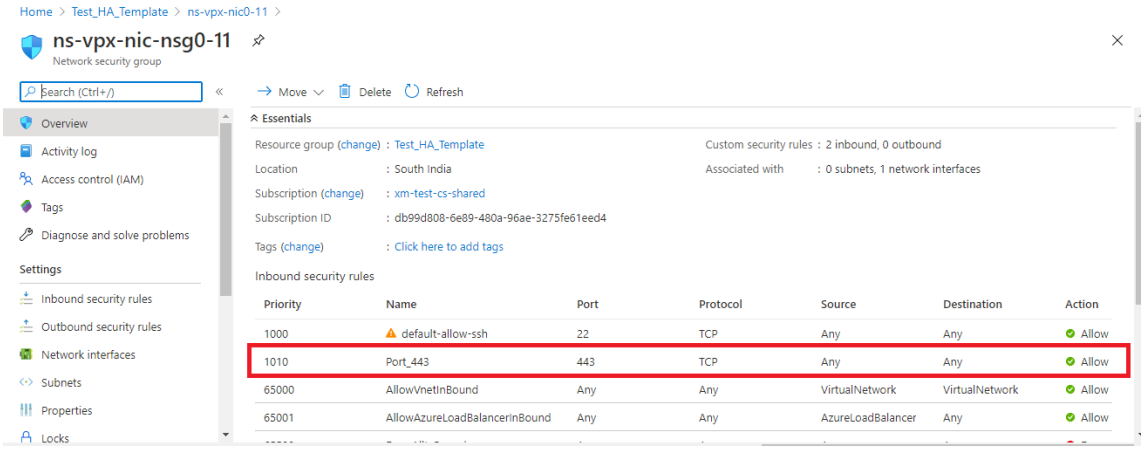
Sur le nœud secondaire (citrix-adc-vpx-1)

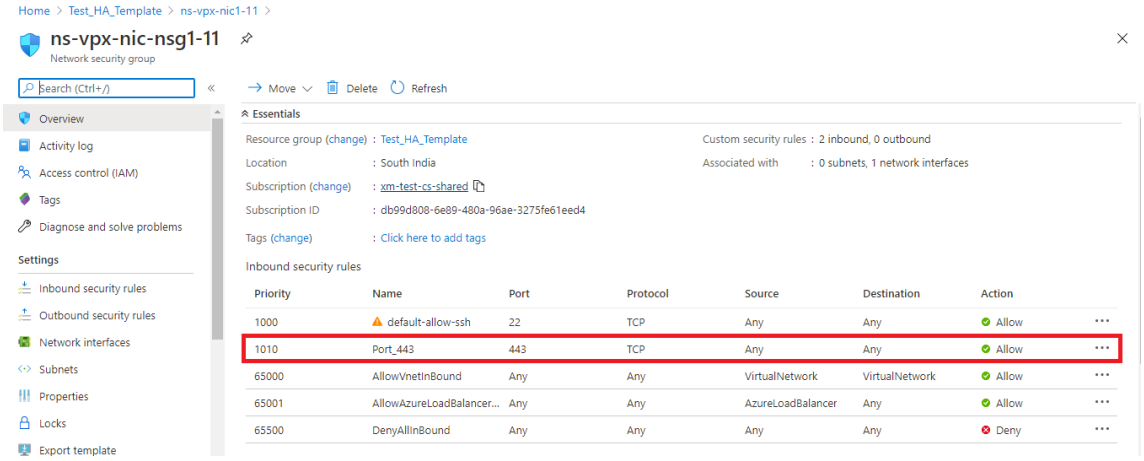

```
> show ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.18.0.5        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.5 (ns-vpx1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:23:51 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.4
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

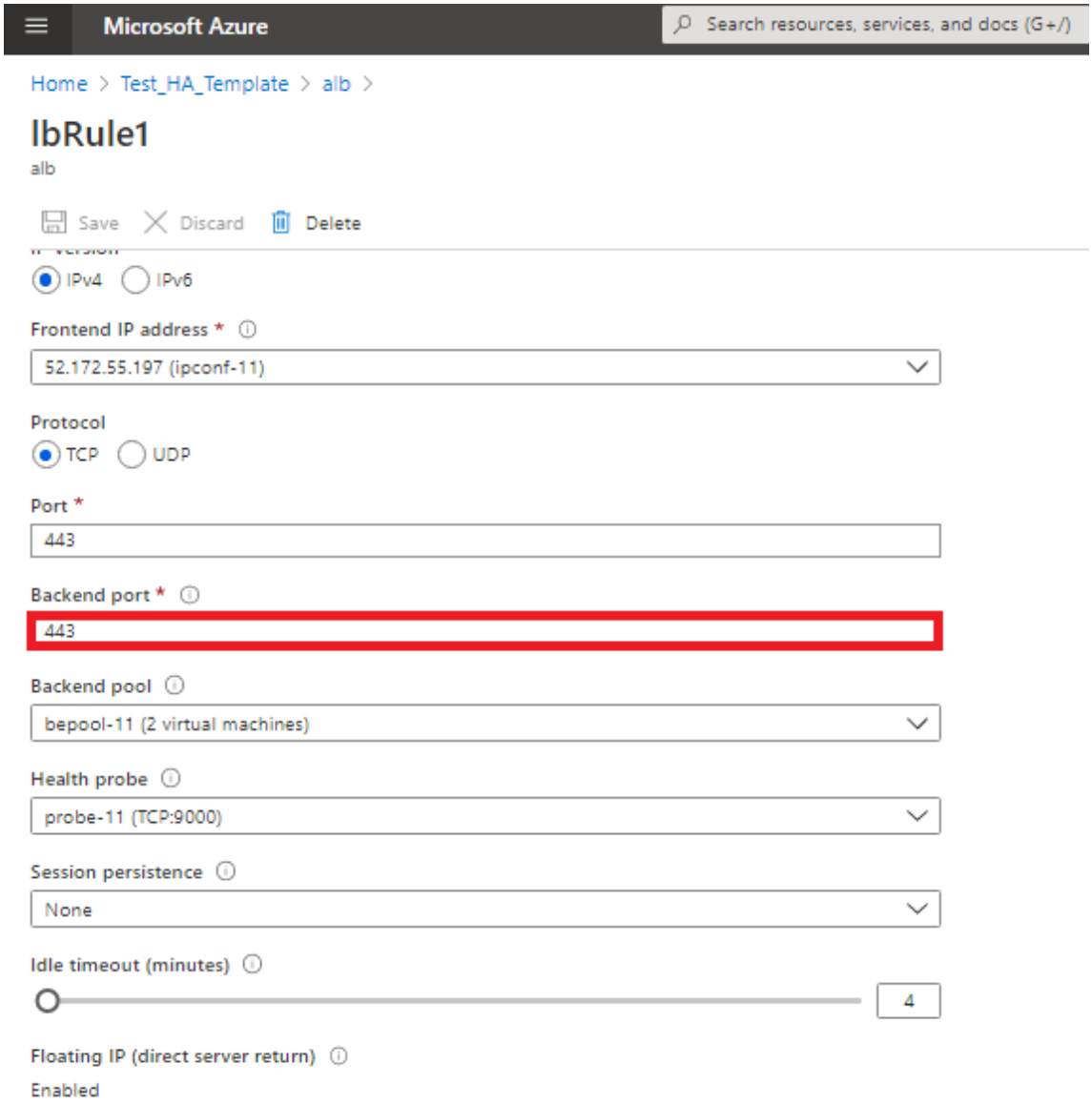
12. Une fois que les nœuds principal et secondaire sont UP et que l'état Synchronisation est **SUCCESS**, vous devez configurer le serveur virtuel d'équilibrage de charge ou le serveur virtuel de passerelle sur le nœud principal (citrix-adc-vpx-0) avec l'adresse IP publique du serveur virtuel ALB. Pour plus d'informations, consultez la section Exemple de configuration .
13. Pour rechercher l'adresse IP publique du serveur virtuel ALB, accédez au **portail Azure > Équilibreur de charge Azure > Configuration IP frontend**.

14. Ajoutez la règle de sécurité entrante pour le port 443 du serveur virtuel sur le groupe de sécurité réseau des deux interfaces clientes.

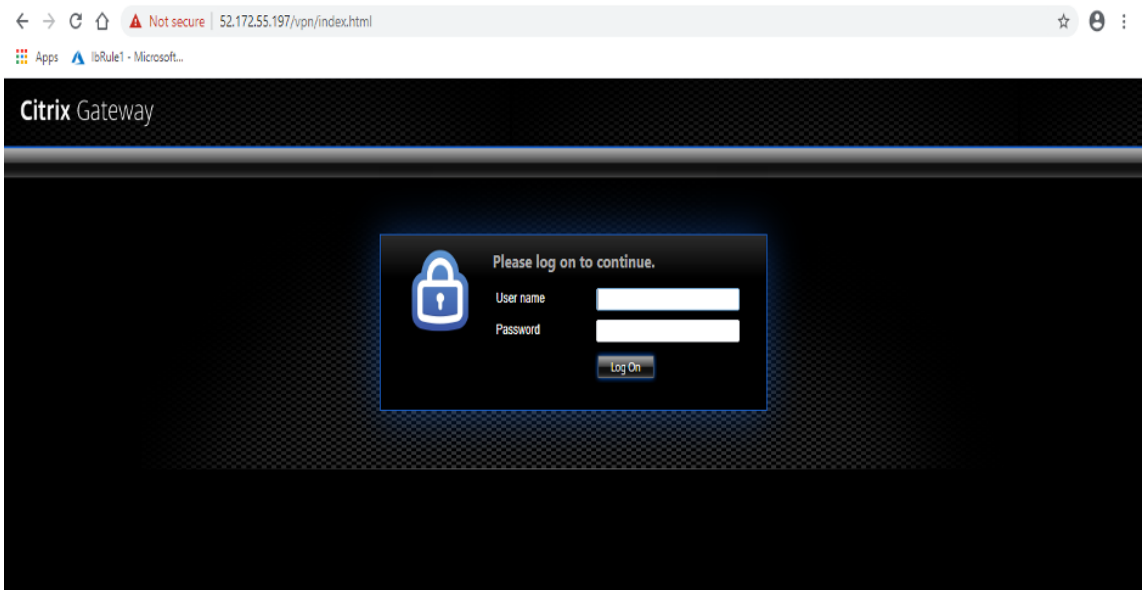




15. Configurez le port ALB auquel vous souhaitez accéder et créez une règle de sécurité entrante pour le port spécifié. Le port principal est votre port serveur virtuel d'équilibrage de charge ou le port du serveur virtuel VPN.



16. Vous pouvez désormais accéder au serveur virtuel d'équilibrage de charge ou au serveur virtuel VPN en utilisant le nom de domaine complet associé à l'adresse IP publique ALB.



Exemple de configuration

Pour configurer un serveur virtuel VPN de passerelle et un serveur virtuel d'équilibrage de charge, exécutez les commandes suivantes sur le nœud principal (ADC-VPX-0). La configuration se synchronise automatiquement avec le nœud secondaire (ADC-VPX-1).

Exemple de configuration de passerelle

```
enable feature aaa LB SSL SSLVPN
add ip 52.172.55.197 255.255.255.0 -type VIP
add vpn vserver vpn_ssl SSL 52.172.55.197 443
add ssl certKey ckp -cert cgwsanity.cer -key cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
<!--NeedCopy-->
```

Exemple de configuration d'équilibrage de charge

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 52.172.55.197 443
bind ssl vserver lb_vs1 -certkeyName ckp
<!--NeedCopy-->
```

Vous pouvez désormais accéder au serveur virtuel d'équilibrage de charge ou VPN à l'aide du nom de domaine complet (FQDN) associé à l'adresse IP interne d'ILB.

Reportez-vous à la section **Ressources** pour plus d'informations sur la configuration du serveur virtuel d'équilibrage de charge.

Ressources :

Les liens suivants fournissent des informations supplémentaires relatives au déploiement HA et à la configuration du serveur virtuel :

- Créer des serveurs virtuels
- Configurer l'équilibrage de charge de base

Configurer une configuration haute disponibilité avec des équilibreurs de charge externes et internes Azure simultanément

August 20, 2021

La paire haute disponibilité sur Azure prend en charge simultanément les équilibreurs de charge externes et internes.

Vous disposez des deux options suivantes pour configurer une paire haute disponibilité à l'aide d'équilibreurs de charge externes et internes Azure :

- Utilisation de deux serveurs virtuels LB sur l'appliance Citrix ADC.
- Utilisation d'un serveur virtuel LB et d'un ensemble d'adresses IP. Le serveur virtuel LB unique sert le trafic vers plusieurs adresses IP définies par l'IPSet.

Effectuez les étapes suivantes pour configurer une paire haute disponibilité sur Azure en utilisant simultanément les équilibreurs de charge externes et internes :

Pour les étapes 1 et 2, utilisez le portail Azure. Pour les étapes 3 et 4, utilisez l'interface graphique Citrix ADC VPX ou l'interface de ligne de commande.

Étape 1. Configurez un équilibreur de charge Azure, soit un équilibreur de charge externe, soit un équilibreur de charge interne.

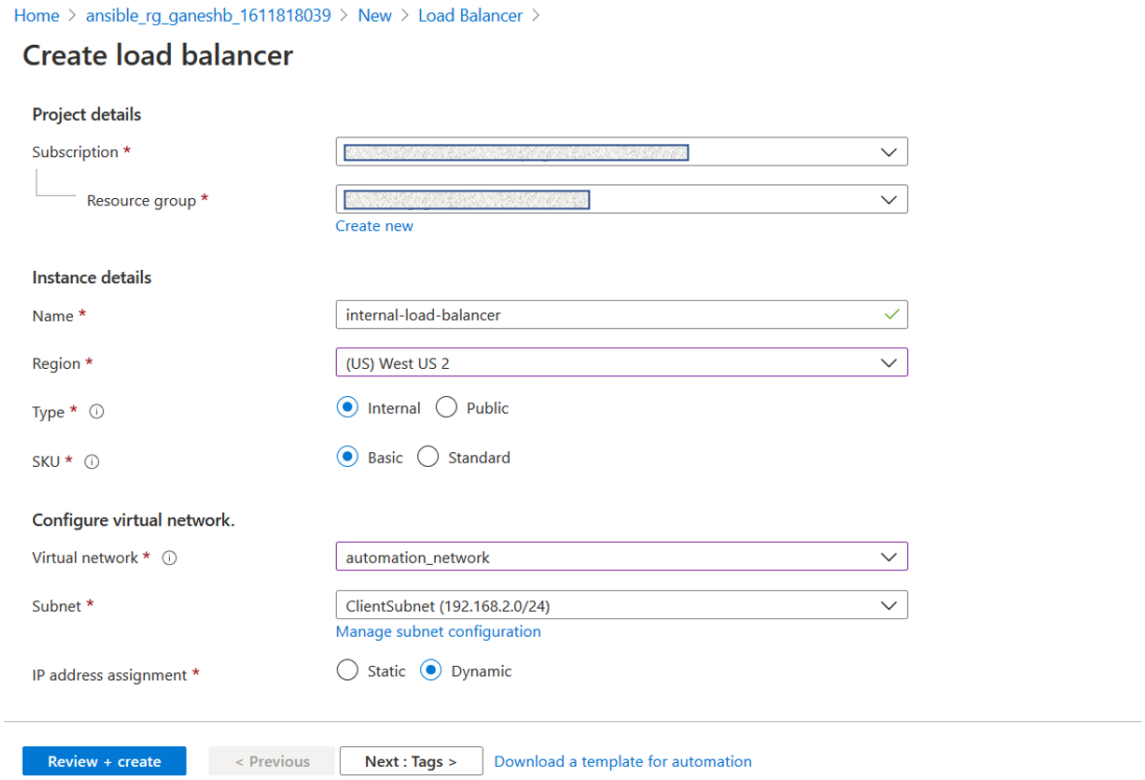
Pour plus d'informations sur la configuration de la configuration haute disponibilité avec des équilibreurs de charge externes Azure, voir Configurer une configuration haute disponibilité avec plusieurs adresses IP et carte réseau.

Pour plus d'informations sur la configuration de la configuration haute disponibilité avec les équilibreurs de charge internes Azure, consultez Configurer les nœuds HA-INC à l'aide du modèle Citrix haute disponibilité avec Azure ILB.

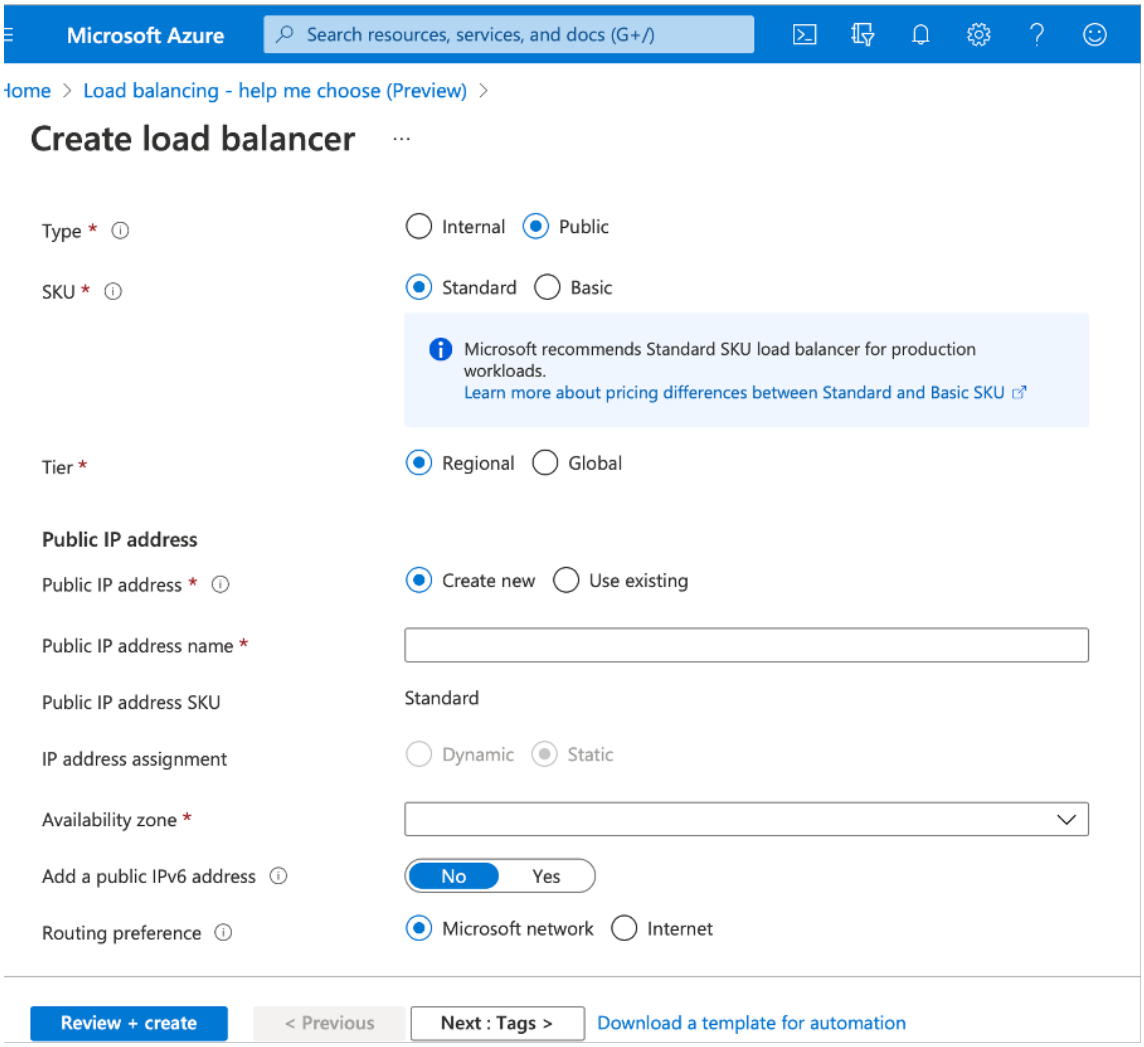
Étape 2. Créez un équilibreur de charge supplémentaire (ILB) dans votre groupe de ressources. À l'étape 1, si vous avez créé un équilibreur de charge externe, vous créez maintenant un équilibreur de charge interne et inversement.

- Pour créer un équilibreur de charge interne, choisissez le type d'équilibreur de charge comme **Interne**. Pour le champ **Sous-réseau**, vous devez choisir votre sous-réseau client Citrix ADC.

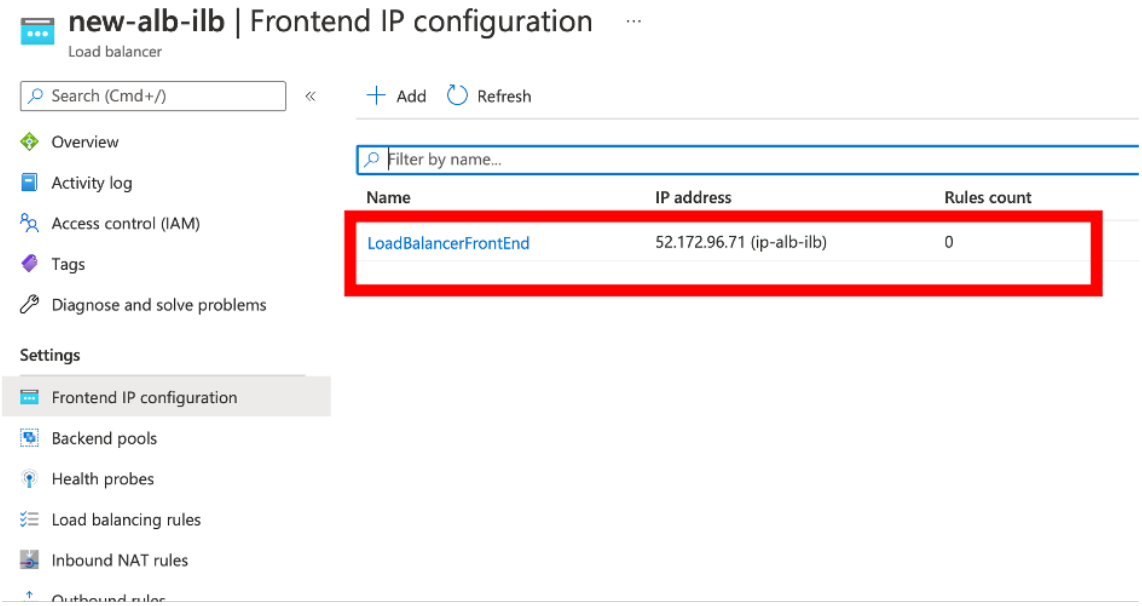
Vous pouvez choisir de fournir une adresse IP statique dans ce sous-réseau, à condition qu'il n'y ait pas de conflit. Sinon, choisissez l'adresse IP dynamique.



- Pour créer un équilibreur de charge externe, choisissez le type d'équilibreur de charge comme étant **Public** et créez l'adresse IP publique ici.



1. Après avoir créé Azure Load Balancer, accédez à la **configuration IP frontend** et notez l'adresse IP affichée ici. Vous devez utiliser cette adresse IP lors de la création du serveur virtuel d'équilibrage de charge ADC, comme à l'étape 3.



2. Dans la page de **configuration Azure Load Balancer**, le déploiement du modèle ARM aide à créer la règle LB, les pools dorsaux et les sondes de santé.
3. Ajoutez les cartes réseau client de la paire haute disponibilité au pool principal de l'ILB.
4. Créer une sonde de santé (TCP, port 9000)
5. Créez deux règles d'équilibrage de charge :
   - Une règle LB pour le trafic HTTP (cas d'utilisation de l'application Web) sur le port 80. La règle doit également utiliser le port principal 80. Sélectionnez le pool de backend créé et la sonde de santé. L'adresse IP flottante doit être activée.
   - Une autre règle LB pour le trafic HTTPS ou CVAD sur le port 443. Le processus est le même que le trafic HTTP.

Étape 3. Sur le nœud principal de l'appliance Citrix ADC, créez un serveur virtuel d'équilibrage de charge pour ILB.

1. Ajoutez un serveur virtuel d'équilibrage de charge.

```
1 add lb vserver <name> <serviceType> [<ILB Frontend IP address>] [<
     port>]
2 <!--NeedCopy-->
```

Exemple :

```
1 add lb vserver vserver_name HTTP 52.172.96.71 80
2 <!--NeedCopy-->
```


> Remarque :
>
> Utilisez l'adresse IP frontale de l'équilibreur de charge, associée à l'équilibreur de charge supplémentaire que vous créez à l'étape 2.

2. Liez un service à un serveur virtuel d'équilibrage de charge.

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour plus d'informations, voir Configurer l'équilibrage de charge de base.

Étape 4 : Au lieu de l'étape 3, vous pouvez créer un serveur virtuel d'équilibrage de charge pour ILB à l'aide d'IPsets.

1. Ajoutez une adresse IP de type IP de serveur virtuel (VIP).

```
add nsip <ILB Frontend IP address> -type <type>
<!--NeedCopy-->
```

Exemple :

```
add nsip 52.172.96.71 -type vip
<!--NeedCopy-->
```

2. Ajoutez un IPSet sur les nœuds principaux et secondaires.

```
add ipset <name>
<!--NeedCopy-->
```

Exemple :

```
add ipset ipset1
<!--NeedCopy-->
```

3. Liez les adresses IP au jeu d'adresses IP.

```
bind ipset <name> <ILB Frontend IP address>
<!--NeedCopy-->
```

Exemple :


```
bind ipset ipset1 52.172.96.71
<!--NeedCopy-->
```

4. Définissez le serveur virtuel LB existant pour qu'il utilise IPSet.

```
set lb vserver <vserver name> -ipset <ipset name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vserver_name -ipset ipset1
<!--NeedCopy-->
```

Pour plus d'informations, voir Configurer un serveur virtuel multi-IP.

Installer une instance Citrix ADC VPX sur Azure VMware Solution

August 20, 2021

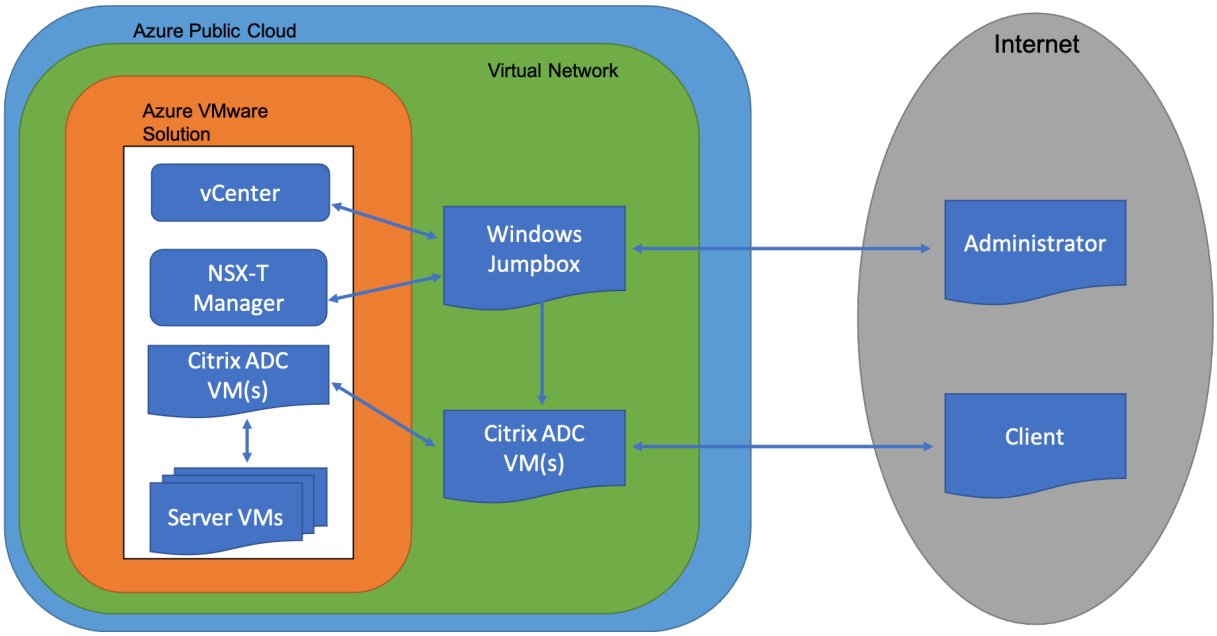
La solution Azure VMware (AVS) vous fournit des clouds privés contenant des clusters vSphere, construits à partir d'une infrastructure Azure dédiée. Le déploiement initial minimum est de trois hôtes, mais des hôtes supplémentaires peuvent être ajoutés un à la fois, jusqu'à 16 hôtes maximum par cluster. Tous les clouds privés provisionnés sont dotés de vCenter Server, vSAN, vSphere et NSX-T.

VMware Cloud (VMC) on Azure vous permet de créer des centres de données définis par logiciel (SDDC) dans le cloud sur Azure avec le nombre d'hôtes ESX que vous souhaitez. Le VMC sur Azure prend en charge les déploiements Citrix ADC VPX. VMC fournit une interface utilisateur identique à vCenter sur site. Il fonctionne de la même manière que les déploiements Citrix ADC VPX basés sur ESX.

Le diagramme suivant montre la solution Azure VMware sur le cloud public Azure à laquelle un administrateur ou un client peut accéder via Internet. Un administrateur peut créer, gérer et configurer des machines virtuelles de charge de travail ou de serveur à l'aide de la solution Azure VMware. L'administrateur peut accéder au vCenter Web et au gestionnaire NSX-T de l'AVS à partir d'une boîte de dialogue Windows. Vous pouvez créer les instances Citrix ADC VPX (paire autonome ou haute disponibilité) et les machines virtuelles de serveur dans Azure VMware Solution à l'aide de vCenter, et gérer la mise en réseau correspondante à l'aide de NSX-T Manager. L'instance Citrix ADC VPX sur AVS fonctionne de la même manière que le cluster d'hôtes VMware sur site. AVS est géré à partir d'une Jumpbox Windows créée sur le même réseau virtuel.

Un client ne peut accéder au service AVS qu'en se connectant au VIP d'ADC. Une autre instance Citrix ADC VPX en dehors de la solution Azure VMware, mais dans le même réseau virtuel Azure, aide à ajouter

le VIP de l'instance Citrix ADC VPX dans Azure VMware Solution en tant que service. Selon les besoins, vous pouvez configurer l'instance Citrix ADC VPX pour fournir un service sur Internet.



Conditions préalables

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Pour plus d'informations sur la solution Azure VMware et ses conditions préalables, consultez la documentation de la solution Azure VMware.
- Pour plus d'informations sur le déploiement de la solution Azure VMware, voir Déployer un cloud privé Azure VMware Solution.
- Pour plus d'informations sur la création d'une machine virtuelle Windows Jump Box pour accéder à la solution Azure VMware et la gérer, consultez Access an Azure VMware Solution Private Cloud.
- Dans la machine virtuelle Jump Box Windows, téléchargez les fichiers de configuration de l'appliance Citrix ADC VPX.
- Créez des segments réseau NSX-T appropriés sur VMware SDDC auxquels les machines virtuelles se connectent. Pour plus d'informations, voir Ajouter un segment réseau dans Azure VMware Solution.
- Obtenir des fichiers de licence VPX.
- Les machines virtuelles (VM) créées ou migrées vers le cloud privé Azure VMware Solution doivent être attachées à un segment réseau.

Configuration matérielle du cloud VMware

Le tableau suivant répertorie les ressources informatiques virtuelles que le SDDC VMware doit fournir pour chaque appliance virtuelle VPX nCore.

Tableau 1. Ressources de calcul virtuel minimales requises pour exécuter une instance Citrix ADC VPX

Composant	Exigences
Mémoire	2 Go
Processeur virtuel	2
Interfaces réseau virtuelles	Dans VMware SDDC, vous pouvez installer un maximum de 10 interfaces réseau virtuelles si le matériel VPX est mis à niveau vers la version 7 ou supérieure.
Espace disque	20 Go

> Remarque
>
> Ceci s'ajoute à toutes les exigences de disque pour l'Hypervisor.

Pour une utilisation en production de l'appliance virtuelle VPX, l'allocation complète de mémoire doit être réservée.

Configuration système requise pour OVF Tool 1.0

OVF Tool est une application cliente qui peut s'exécuter sur les systèmes Windows et Linux. Le tableau suivant décrit la configuration système requise pour l'installation de l'outil OVF.

Tableau 2. Configuration système requise pour l'installation d'outils OVF

Composant	Exigences
Système d'exploitation	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « OVF Tool User Guide » à l'adressehttp://kb.vmware.com/.
UC	750 MHz minimum, 1 GHz ou plus rapide recommandé
RAM	1 Go minimum, 2 Go recommandés
CARTE RÉSEAU	Carte réseau 100 Mbit/s ou plus rapide

Pour plus d'informations sur l'installation d'OVF, recherchez le fichier PDF « OVF Tool User Guide » à l'adressehttp://kb.vmware.com/.

Téléchargement des fichiers d'installation Citrix ADC VPX

Le package d'installation d'instance Citrix ADC VPX pour VMware ESX respecte la norme de format OVF (Open Virtual Machine). Vous pouvez télécharger les fichiers à partir du site Web Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l' adresse http://www.citrix.com. Cliquez sur le **lien Nouveaux utilisateurs**et suivez les instructions pour créer un compte Citrix.

Une fois connecté, naviguez dans le chemin suivant à partir de la page d'accueil Citrix :

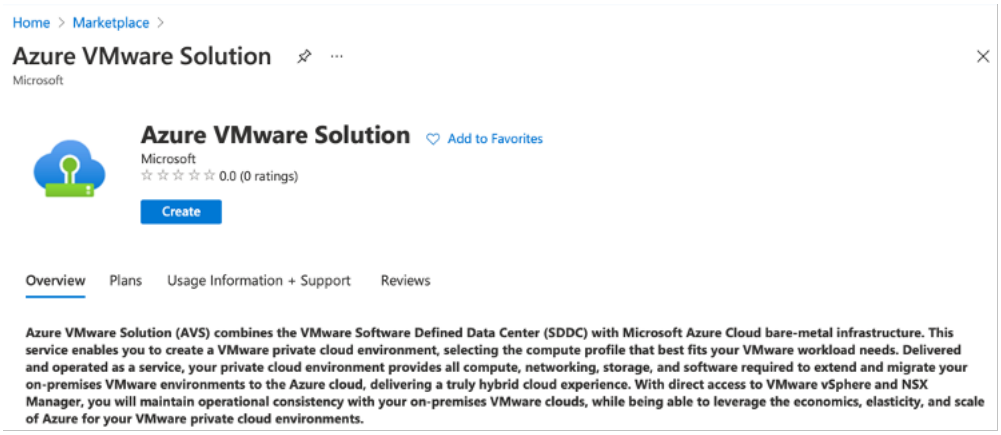
Citrix.com > **Téléchargements > Citrix ADC > Appliances virtuelles**.

Copiez les fichiers suivants sur une station de travail sur le même réseau que le serveur ESX. Copiez les trois fichiers dans le même dossier.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (par exemple, NSVPX-ESX-13.0-79.64-Disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (par exemple, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (par exemple, NSVPX-ESX-13.0-79.64.mf)

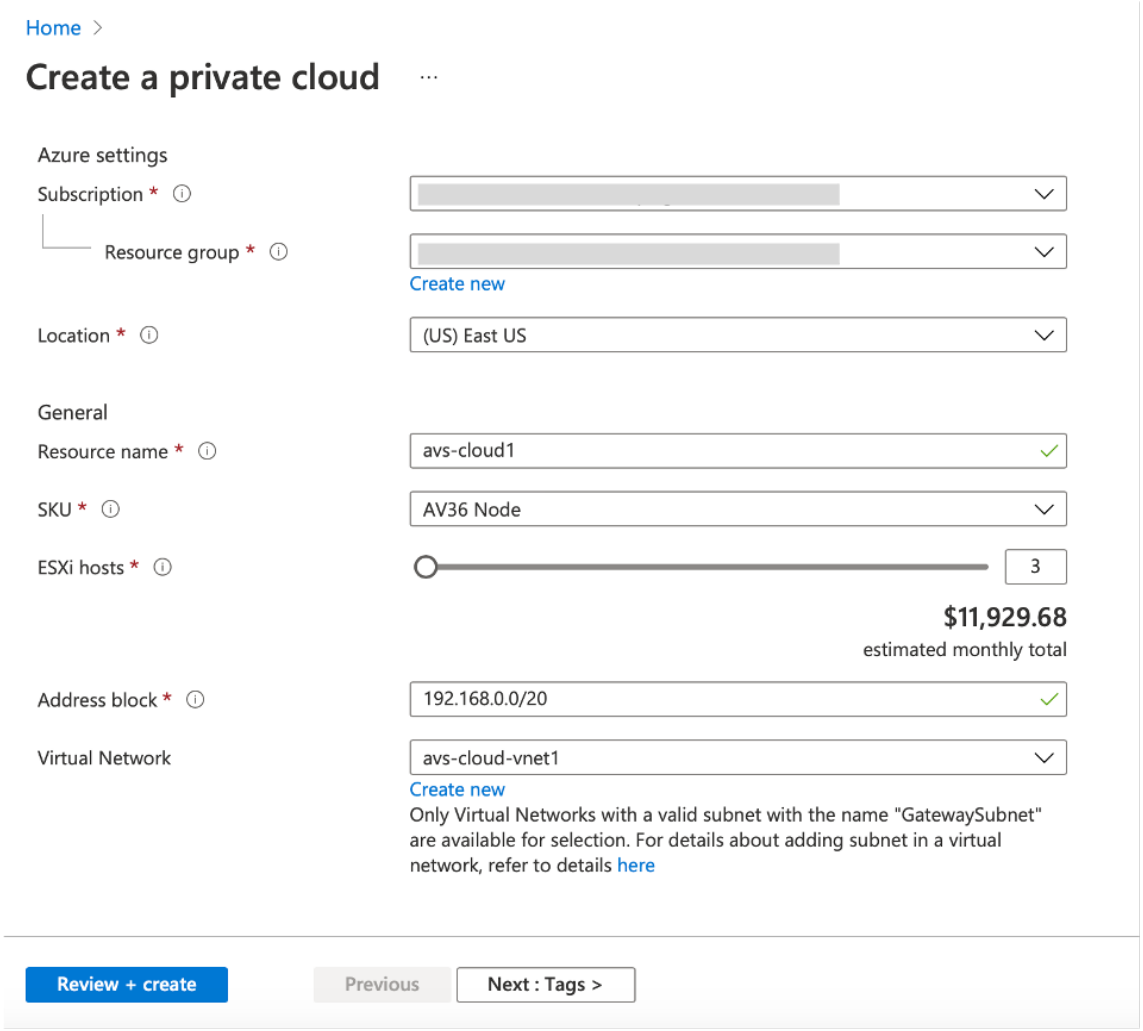
Déploiement de la solution Azure VMware

1. Connectez-vous à votre portail Microsoft Azureet accédez à **Azure Marketplace**.
2. Depuis **Azure Marketplace**, recherchez la **solution Azure VMware** et cliquez sur **Créer**.

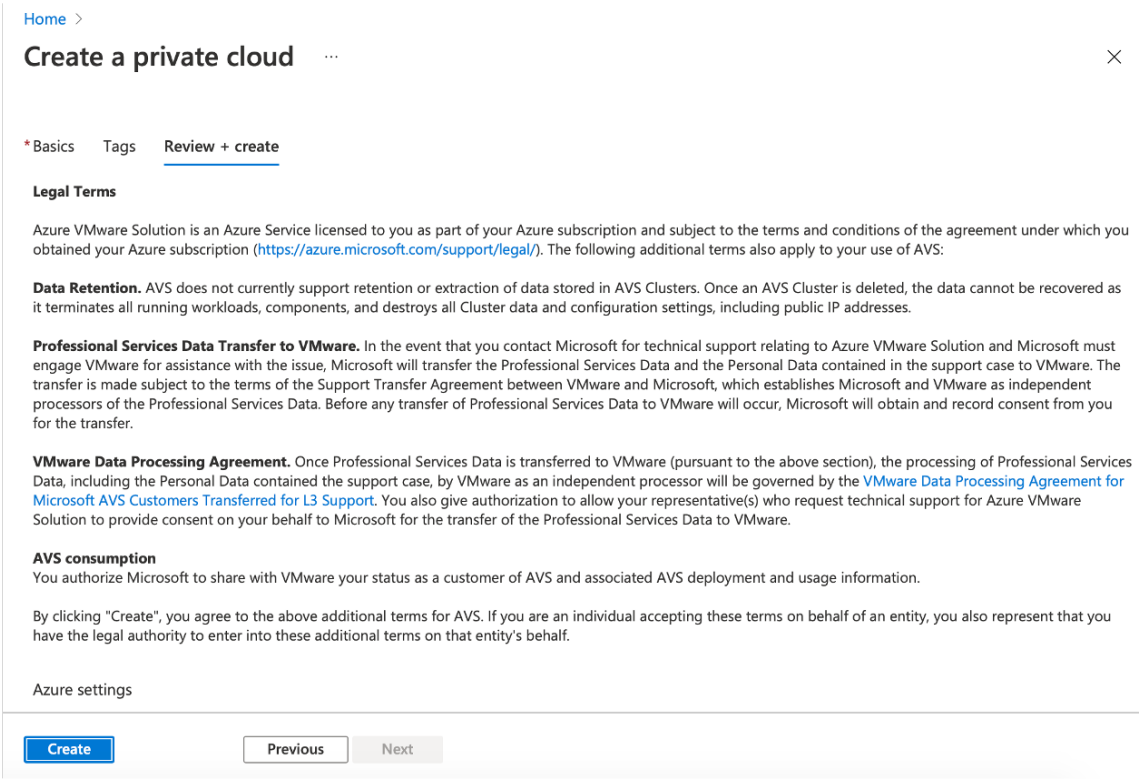


3. Sur la page **Créer un cloud privé**, entrez les informations suivantes :
   - Sélectionnez au moins 3 hôtes ESXi pour créer le cluster par défaut de votre cloud privé.
   - Pour le champ **Bloc d'adresse**, utilisez l'espace d'adressage **/22** .

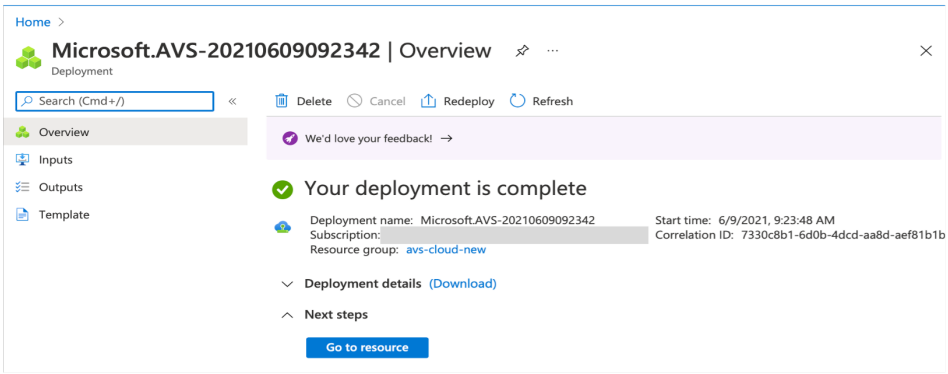
- Pour le **réseau virtuel**, assurez-vous que la plage CIDR ne chevauche aucun de vos sous-réseaux locaux ou autres sous-réseaux Azure (réseaux virtuels) ou avec le sous-réseau de passerelle.
- Le sous-réseau Gateway est utilisé pour exprimer le routage de la connexion avec le cloud privé.



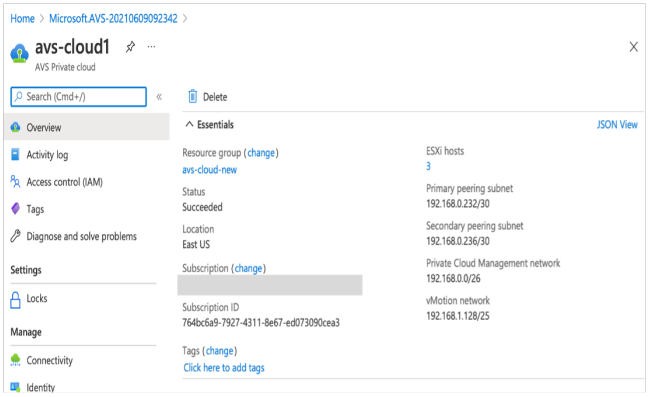
4. Cliquez sur **Réviser + Créer**.
5. Passez en revue les paramètres. Si vous devez modifier des paramètres, cliquez sur **Précédent**.



6. Cliquez sur **Créer**. Le processus de provisionnement du cloud privé démarre. Le provisionnement du cloud privé peut prendre jusqu'à deux heures.



7. Cliquez sur **Aller à la ressource**pour vérifier le cloud privé créé.



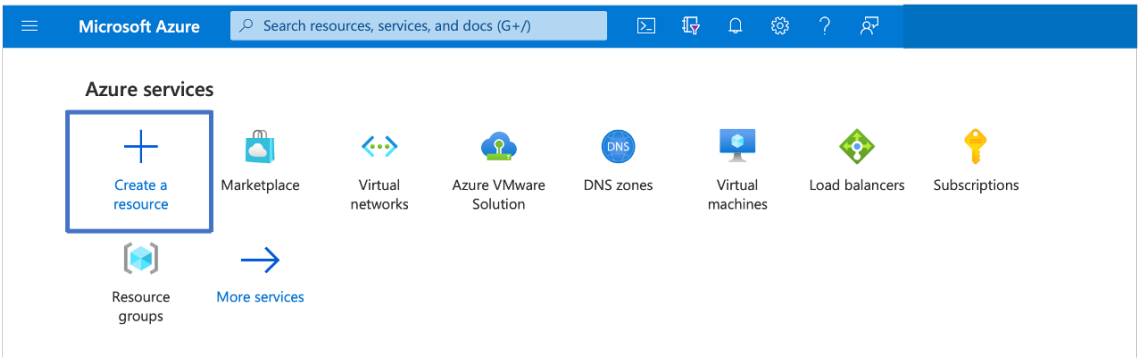
> Remarque
>
> Pour accéder à cette ressource, vous devez disposer d'une machine virtuelle sous Windows qui agit comme une boîte de dialogue Jump.

Connexion à une machine virtuelle Azure exécutant Windows

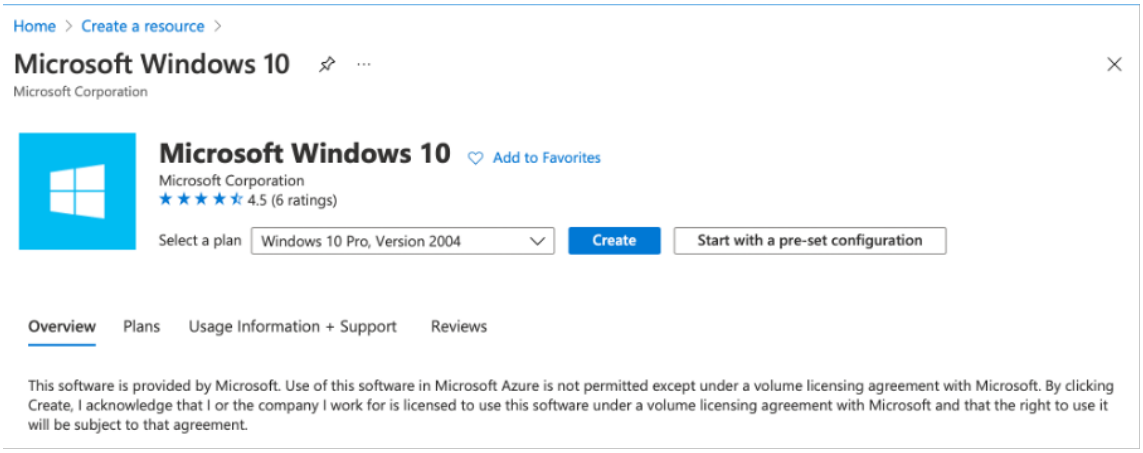
Cette procédure explique comment utiliser le portail Azure pour déployer une machine virtuelle (VM) dans Azure qui exécute Windows Server 2019. Pour voir votre machine virtuelle en action, vous devez ensuite effectuer un RDP sur la machine virtuelle et installer le serveur Web IIS.

Pour accéder au cloud privé que vous avez créé, vous devez créer un Jump Box Windows au sein du même réseau virtuel.

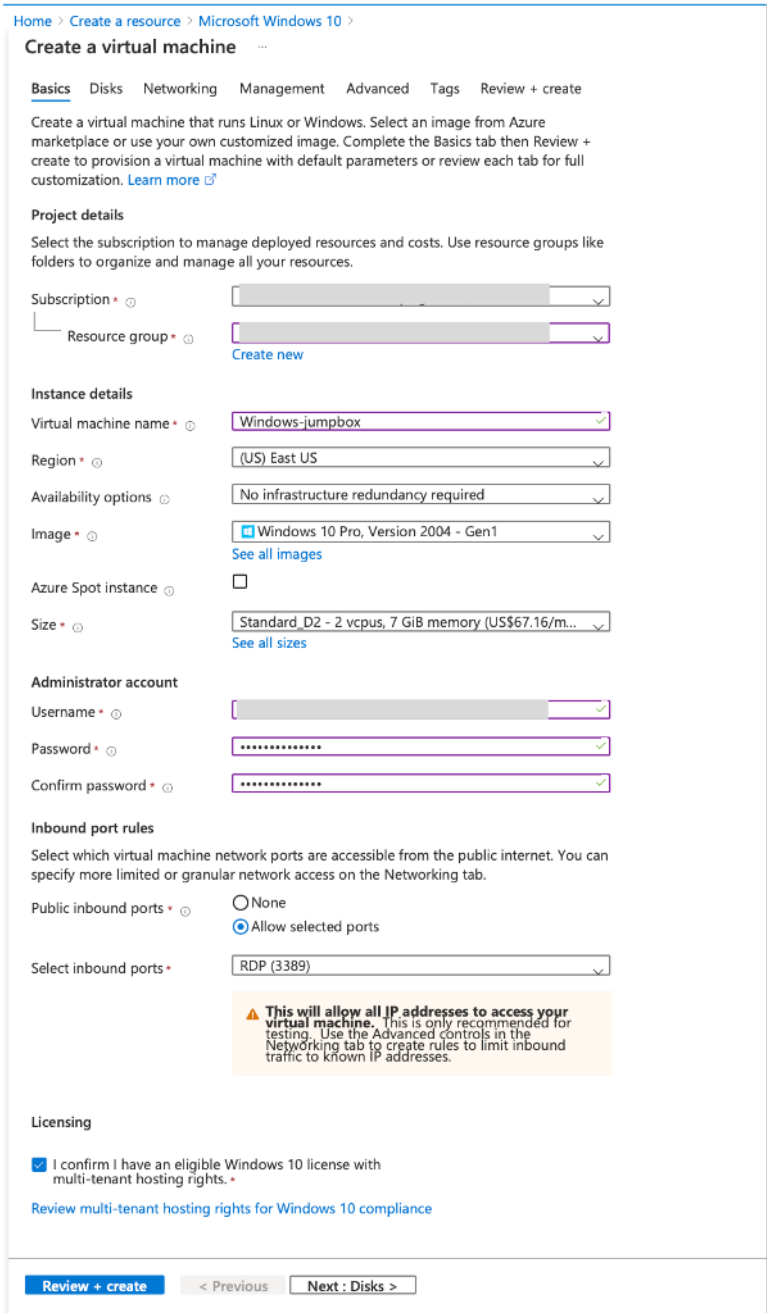
1. Accédez au **portail Azure**, puis cliquez sur **Créer une ressource**.



2. Recherchez **Microsoft Windows 10**, puis cliquez sur **Créer**.



3. Créez une machine virtuelle (VM) qui exécute Windows Server 2019. La page **Créer une machine virtuelle** apparaît. Saisissez tous les détails dans l'onglet **Principes** de base, puis cochez la case **Licences** . Laissez les valeurs par défaut restantes, puis cliquez **sur le bouton Réviser + créer** au bas de la page.



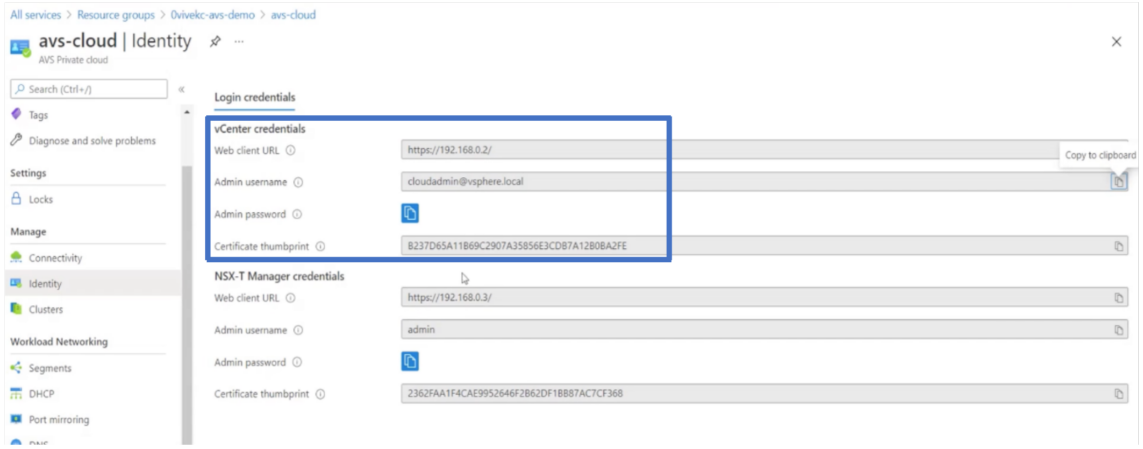
4. Une fois la validation exécutée, cliquez sur le bouton **Créer** en bas de la page.
5. Une fois le déploiement terminé, sélectionnez **Aller à la ressource**.
6. Accédez à la machine virtuelle Windows que vous avez créée. Utilisez l'adresse IP publique de la machine virtuelle Windows et connectez-vous à l'aide de RDP.

   Utilisez le bouton **Connexion** du portail Azure pour démarrer une session Bureau à distance (RDP) à partir d'un poste de travail Windows. Vous vous connectez d'abord à la machine virtuelle, puis vous vous connectez.

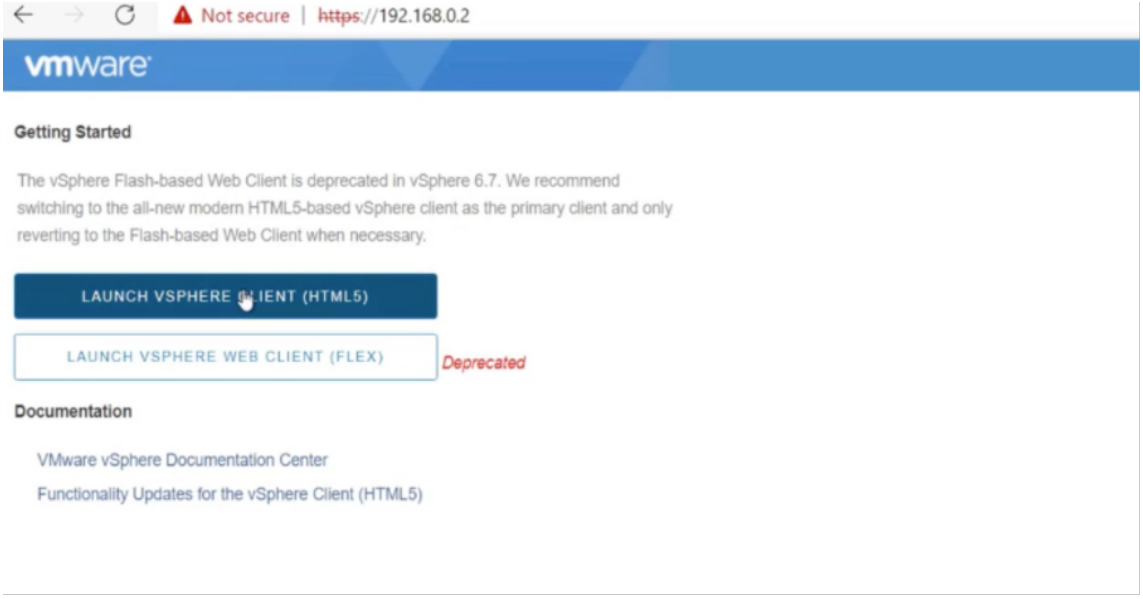
Pour vous connecter à une machine virtuelle Windows à partir d'un Mac, vous devez installer un client RDP pour Mac tel que Microsoft Remote Desktop. Pour plus d'informations, voir Comment se connecter et se connecter à une machine virtuelle Azure exécutant Windows.

Accédez à votre portail Private Cloud vCenter

1. Dans votre cloud privé Azure VMware Solution, sous **Gérer**, sélectionnez **Identité**. Notez les informations d'identification de vCenter.

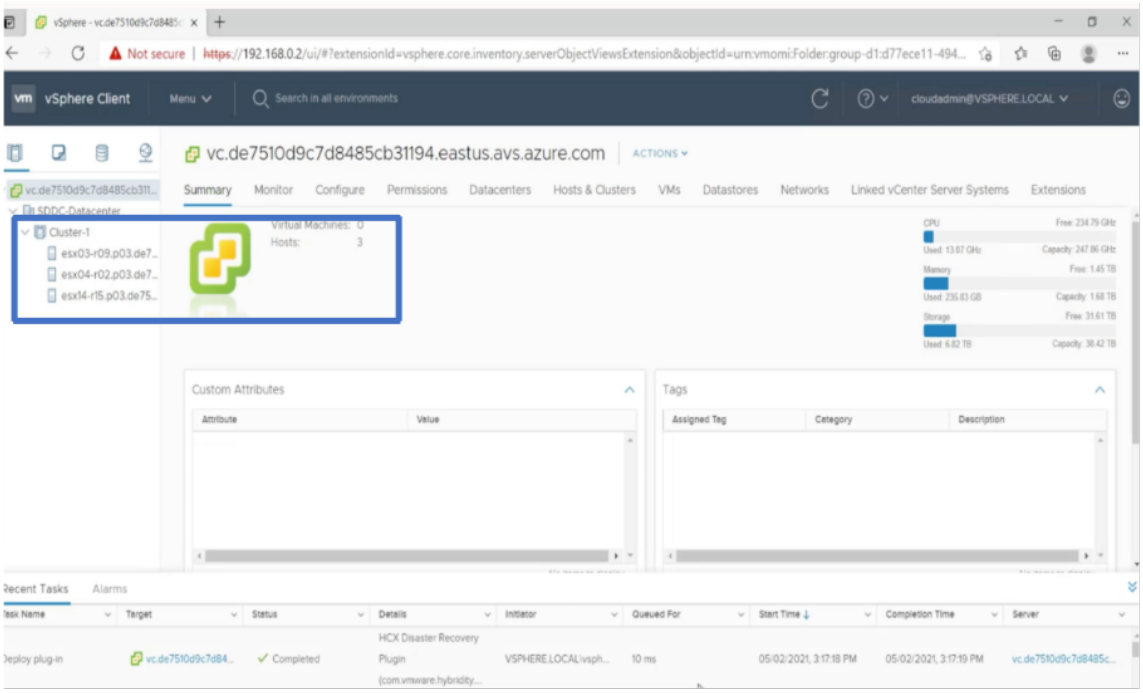


2. Lancez vSphere client en saisissant l'URL du client Web vCenter.



3. Connectez-vous à VMware vSphere à l'aide des informations d'identification vCenter de votre cloud privé Azure VMware Solution.

4. Dans vSphere Client, vous pouvez vérifier les hôtes ESXi que vous avez créés dans le portail Azure.



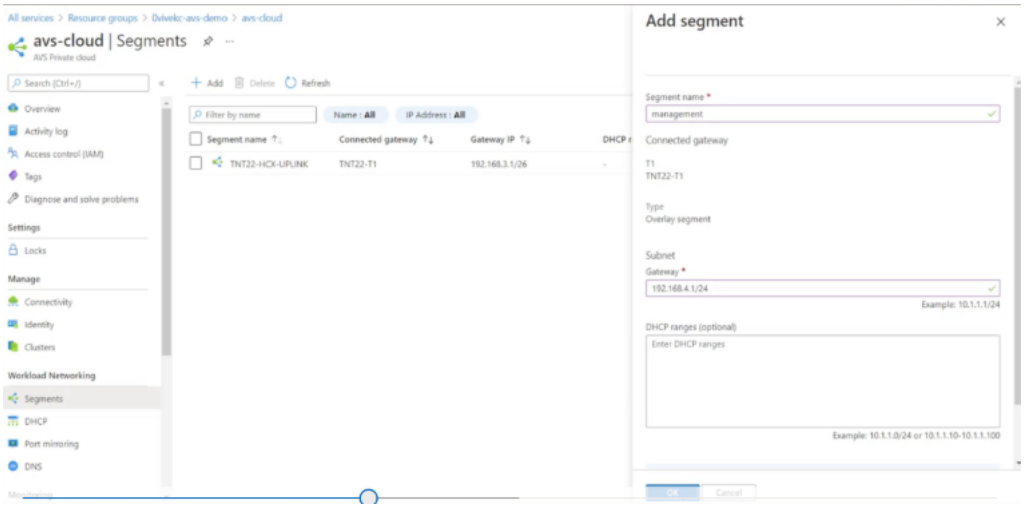
Pour plus d'informations, voir Accès à votre portail Private Cloud vCenter.

Création d'un segment NSX-T dans le portail Azure

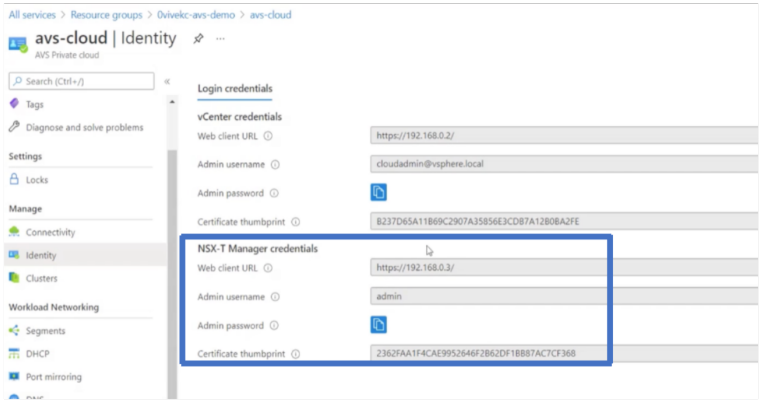
Vous pouvez créer et configurer un segment NSX-T à partir de la console Azure VMware Solution dans le portail Azure. Ces segments sont connectés à la passerelle de niveau 1 par défaut, et les charges

de travail de ces segments sont connectées Est-Ouest et Nord-Sud. Une fois que vous avez créé le segment, il s'affiche dans NSX-T Manager et vCenter.

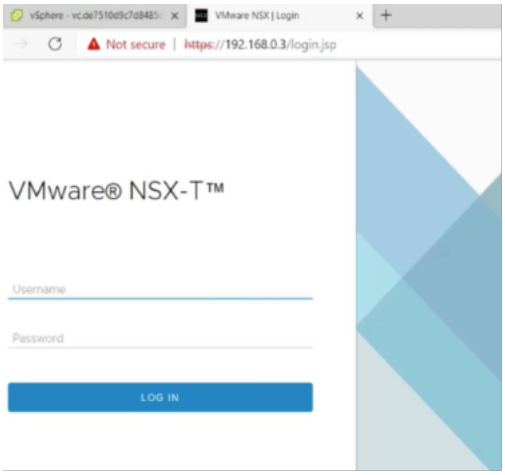
1. Dans votre cloud privé Azure VMware Solution, sous **Workload Networking**, sélectionnez **Segments > Ajouter**. Fournissez les détails du nouveau segment logique et sélectionnez **OK**. Vous pouvez créer trois segments distincts pour les interfaces Client, Management et Server.



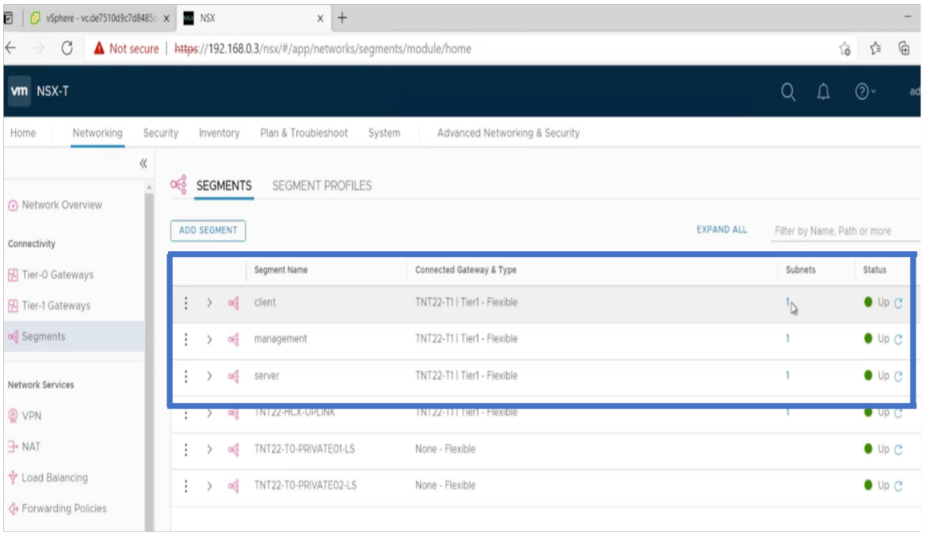
2. Dans votre cloud privé Azure VMware Solution, sous **Gérer**, sélectionnez **Identité**. Notez les informations d'identification NSX-T Manager.



3. Lancez VMware NSX-T Manager en saisissant l'URL du client Web NSX-T.



4. Dans le gestionnaire NSX-T, sous **Mise en réseau > Segments**, vous pouvez voir tous les segments que vous avez créés. Vous pouvez également vérifier les sous-réseaux.



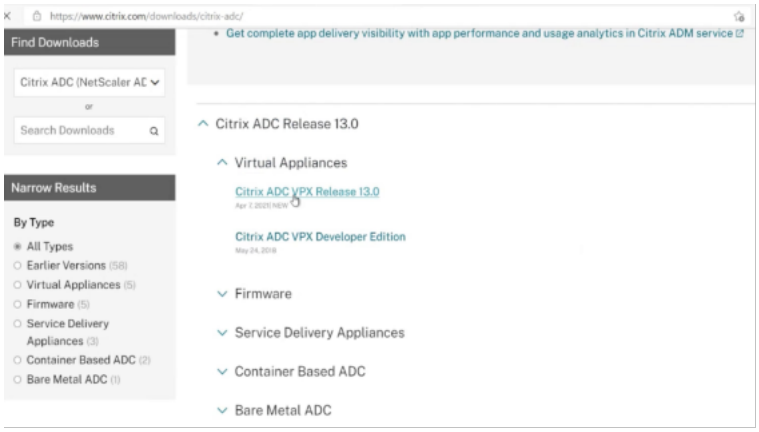
Pour plus d'informations, voir Créer un segment NSX-T dans le portail Azure.

Installer une instance Citrix ADC VPX sur le cloud VMware

Après avoir installé et configuré VMware Software-Defined Data Center (SDDC), vous pouvez utiliser le SDDC pour installer des appliances virtuelles sur le cloud VMware. Le nombre d'appliances virtuelles que vous pouvez installer dépend de la quantité de mémoire disponible sur le SDDC.

Pour installer des instances Citrix ADC VPX sur VMware Cloud, effectuez ces étapes dans Windows Jumpbox VM :

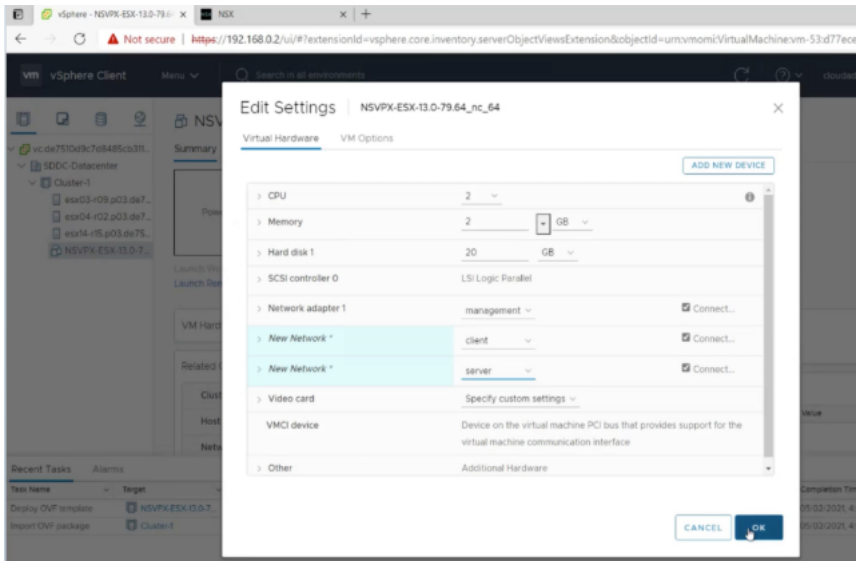
1. Téléchargez les fichiers de configuration de l'instance Citrix ADC VPX pour l'hôte ESXi depuis le site Citrix Downloads.



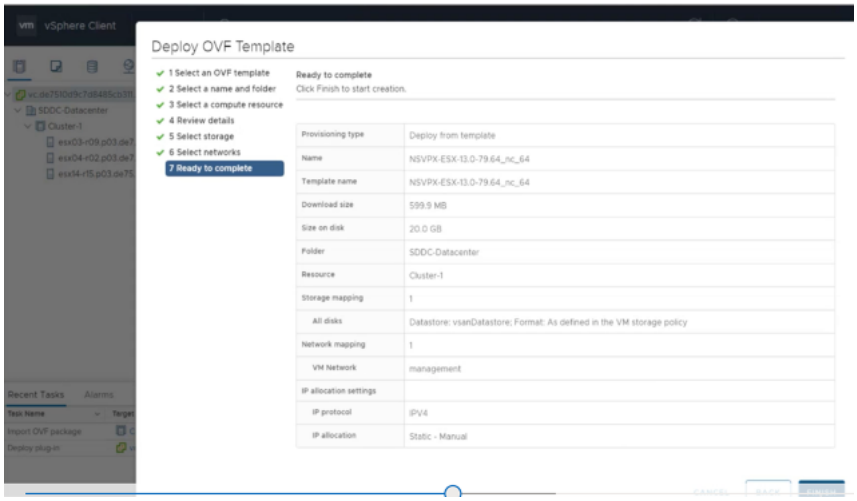
2. Ouvrez le SDDC VMware dans la Jumpbox Windows.
3. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur, puis cliquez sur **Connexion**.
4. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.
5. Dans la boîte de dialogue **Déployer un modèle OVF**, dans le champ **Déployer à partir d'un fichier**, accédez à l'emplacement où vous avez enregistré les fichiers d'installation de l'instance Citrix ADC VPX, sélectionnez le fichier .ovf, puis cliquez sur **Suivant**.

> REMARQUE
>
> Par défaut, l'instance Citrix ADC VPX utilise des interfaces réseau E1000. Pour déployer ADC avec l'interface VMXNET3, modifiez l'OVF pour utiliser l'interface VMXNET3 au lieu de l'E1000. La disponibilité de l'interface VMXNET3 est limitée par l'infrastructure Azure et peut ne pas être disponible dans Azure VMware Solution.

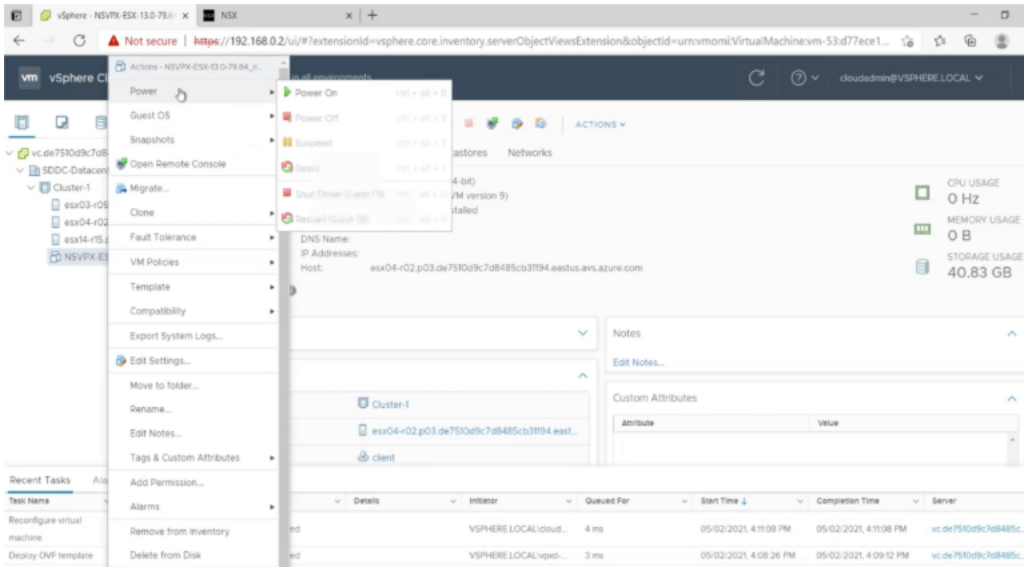
6. Mappez les réseaux affichés dans le modèle OVF de l'appliance virtuelle aux réseaux que vous avez configurés sur VMware SDDC. Cliquez sur **OK**.



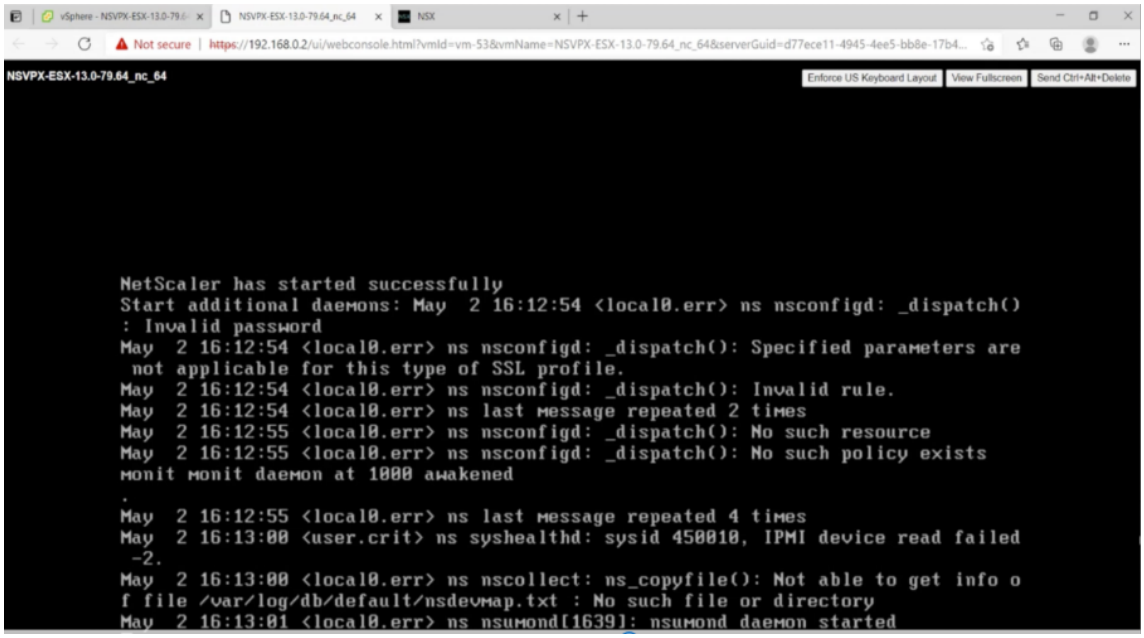
7. Cliquez sur **Terminer** pour commencer l'installation d'une appliance virtuelle sur VMware SDDC.



8. Vous êtes maintenant prêt à démarrer l'instance Citrix ADC VPX. Dans le volet de navigation, sélectionnez l'instance Citrix ADC VPX que vous avez installée et, dans le menu contextuel, sélectionnez **Mettez sous tension**. Cliquez sur l'onglet **Console** pour émuler un port de console.



9. Vous êtes maintenant connecté à la machine virtuelle Citrix ADC à partir de vSphere Client.



10. Pour accéder à l'appliance Citrix ADC à l'aide des clés SSH, tapez la commande suivante dans l'interface de ligne de commande :

```
ssh nsroot@<management IP address>
<!--NeedCopy-->
```

Exemple :

```
ssh nsroot@192.168.4.5
<!--NeedCopy-->
```

11. Vous pouvez vérifier la configuration ADC à l'aide de la `show ns ip` commande.

    ! [Vérifier à l'aide `show nsip` de la commande] (/en-us/citrix-adc/media/avs-show-nsip.png)

Ajouter des paramètres Azure Autoscale

August 20, 2021

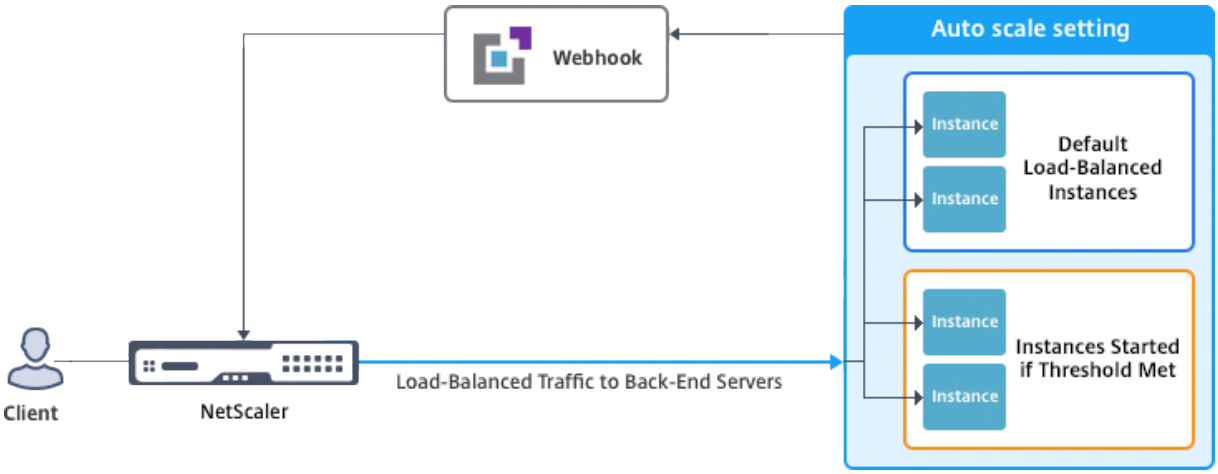
L'hébergement efficace des applications dans un cloud implique une gestion aisée et économique des ressources en fonction de la demande des applications. Pour répondre à la demande croissante, vous devez mettre à l'échelle les ressources réseau vers le haut. Que la demande diminue, vous devez réduire l'échelle pour éviter le coût inutile des ressources inactives. Pour minimiser le coût d'exécution de l'application, vous devez constamment surveiller le trafic, la mémoire et l'utilisation du processeur, etc. Toutefois, la surveillance manuelle du trafic est fastidieuse. Pour que

l'environnement d'application évolue de manière dynamique, vous devez automatiser les processus de surveillance du trafic et de mise à l'échelle des ressources lorsque cela est nécessaire.

Vous pouvez utiliser Autoscale avec des jeux d'échelle de machines virtuelles Azure (VMSS) pour le déploiement autonome et haute disponibilité VPX Multi-IP sur Azure.

Intégré aux jeux d'échelle de machines virtuelles Azure (VMSS) et à la fonctionnalité Autoscale, l'instance Citrix ADC VPX offre les avantages suivants :

- Équilibrage et gestion de la charge : configure automatiquement les serveurs pour qu'ils montent et descendent en puissance, en fonction de la demande. L'instance VPX détecte automatiquement le paramètre VMSS Autoscale dans le sous-réseau principal du même groupe de ressources que l'instance VPX et permet à l'utilisateur de sélectionner le paramètre VMSS Autoscale pour équilibrer la charge. Tout cela est fait en configurant automatiquement les adresses IP virtuelles et de sous-réseau Citrix ADC sur l'instance VPX.
- Haute disponibilité : détecte les groupes Autoscale dans le même groupe de ressources et serveurs d'équilibrage de charge.
- Meilleure disponibilité du réseau : l'instance VPX prend en charge les serveurs back-end sur différents réseaux virtuels (VNET).



Pour plus d'informations, consultez la rubrique Azure suivante

- Documentation sur les jeux d'échelle de machine virtuelle
- Présentation d'Autoscale dans les machines virtuelles Microsoft Azure, les services cloud et les applications Web

Avant de commencer

1. Lisez les instructions d'utilisation relatives à Azure. Pour plus d'informations, voir Déployer une instance Citrix ADC VPX sur Microsoft Azure.
2. Créez une ou plusieurs instances Citrix ADC VPX avec trois interfaces réseau sur Azure en fonction de vos besoins (déploiement autonome ou haute disponibilité).

3. Ouvrez le port TCP 9001 sur le groupe de sécurité réseau de l'interface 0/1 de l'instance VPX. L'instance VPX utilise ce port pour recevoir la notification de mise à l'échelle et de mise à l'échelle.
4. Créez un jeu d'échelle de machine virtuelle Azure (VMSS) dans le même groupe de ressources. Si vous n'avez pas de configuration VMSS existante, effectuez les tâches suivantes :

   a) Créer un VMSS

   b) Activer Autoscale sur VMSS

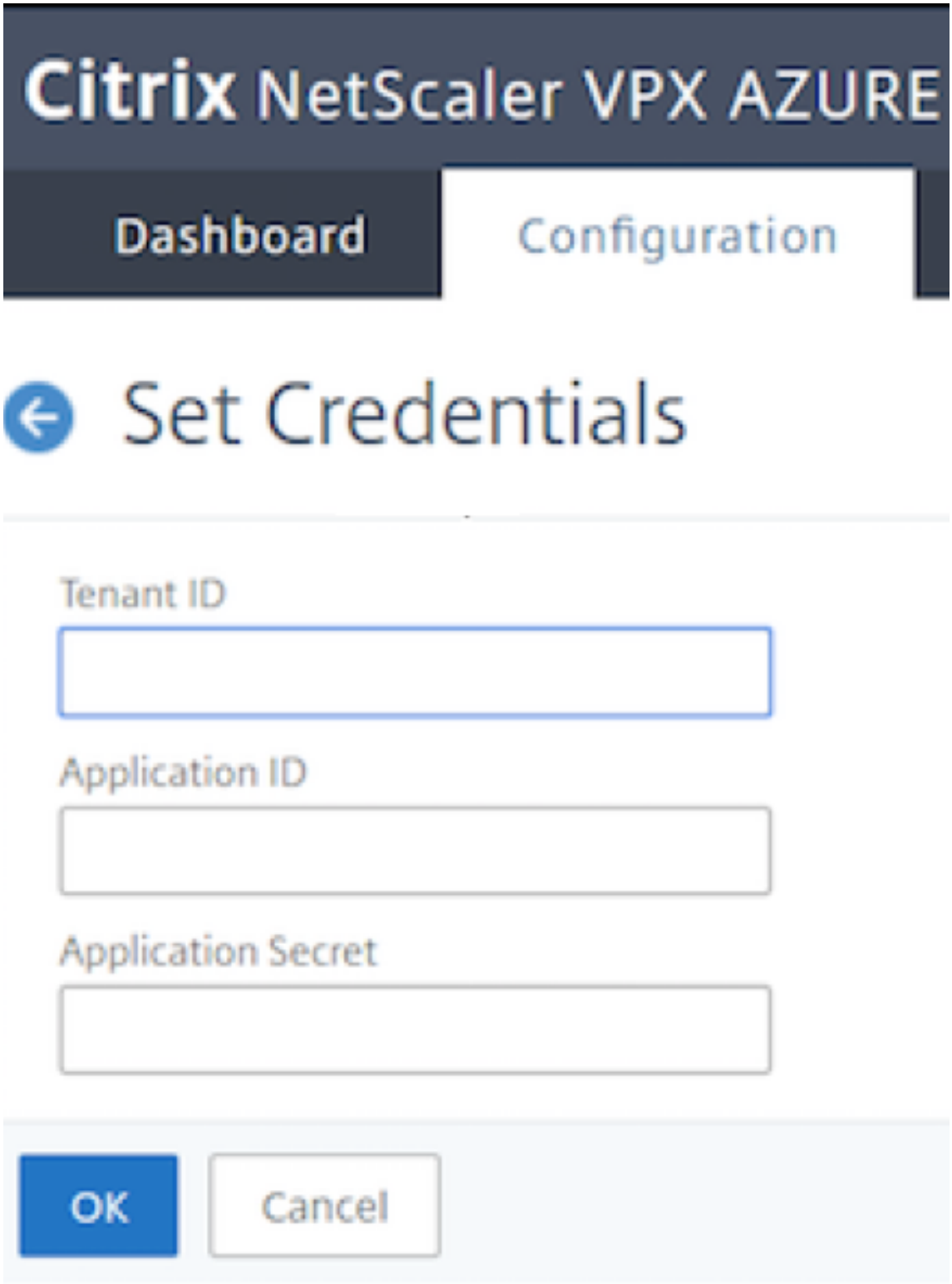
   c) Créer une stratégie évolutive et évolutive dans le paramètre VMSS Autoscale

   Pour plus d'informations, voir Vue d'ensemble des jeux d'échelle de machines virtuelles Azure Autoscale with Azure.
5. Créez une application Azure Active Directory (ADD) et un principal de service pouvant accéder aux ressources. Attribuez un rôle de contributeur à l'application AAD nouvellement créée. Pour plus d'informations, voir Utiliser le portail pour créer une application Azure Active Directory et un principal de service pouvant accéder aux ressources.

Ajouter VMSS à une instance Citrix ADC VPX

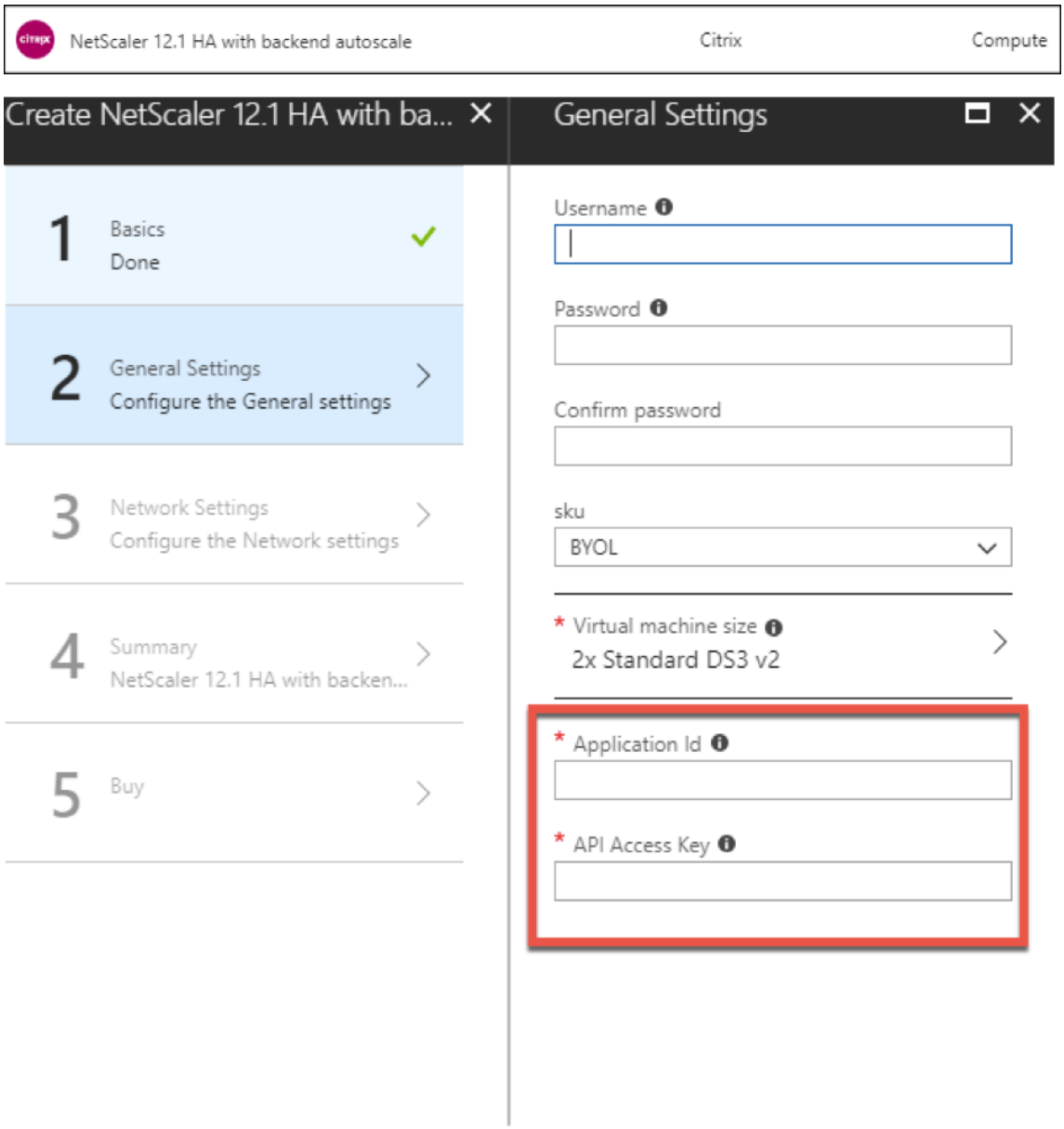
Vous pouvez ajouter le paramètre Autoscale à une instance VPX en un seul clic à l'aide de l'interface graphique. Procédez comme suit pour ajouter le paramètre Autoscale à l'instance VPX :

1. Ouvrez une session sur l'instance VPX.
2. Lorsque vous ouvrez une session sur l'instance Citrix ADC VPX pour la première fois, la page Définir les informations d'identification s'affiche. Ajoutez les informations d'identification Azure requises pour que la fonctionnalité Autoscale fonctionne.



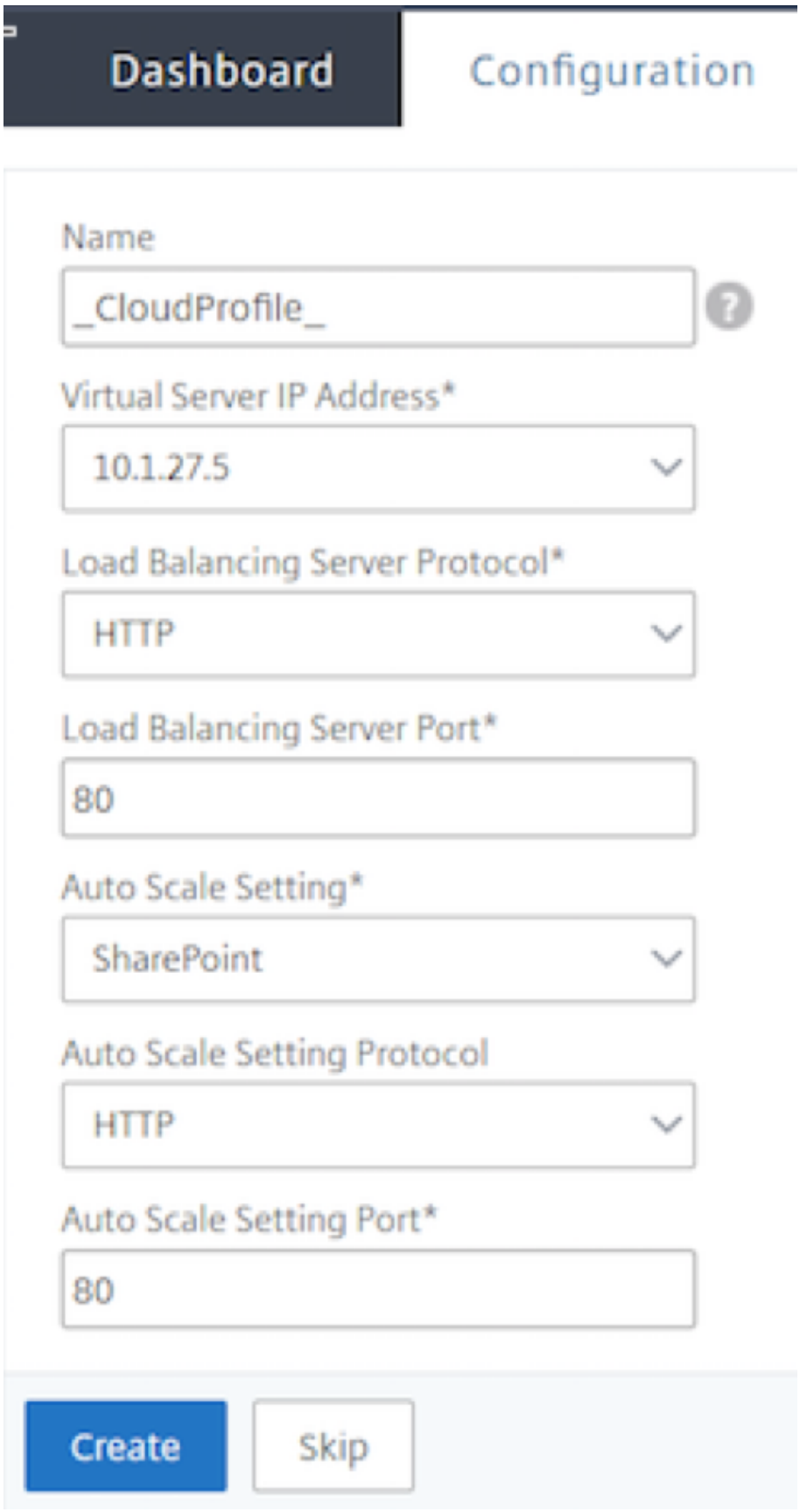
La page Définir les informations d'identification s'affiche uniquement lorsque l'ID d'application et la clé d'accès API ne sont pas définis ou que l'ID d'application et les clés d'accès API corrects (identiques au secret de l'application) ne sont pas définis dans le portail Azure.

Lorsque vous déployez l'offre « NetScaler 12.1 HA avec Autoscale principal » depuis Azure Marketplace, le portail Azure demande les informations d'identification principale du service Azure (ID d'application et clé d'accès API).



Pour plus d'informations sur la création d'un ID d'application, reportez-vous à la section Ajout d'une application et pour créer une clé d'accès ou un secret d'application, voir Configurer une application cliente pour accéder aux API Web.

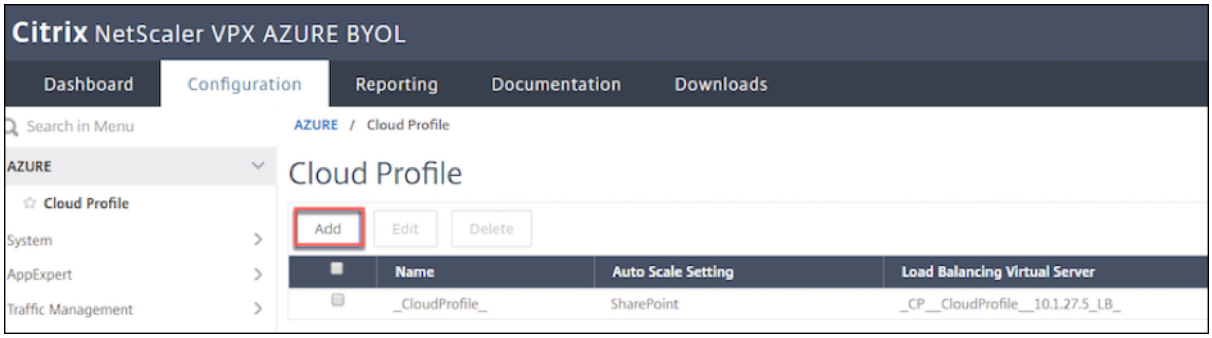
3. Dans la page de profil de nuage par défaut, entrez les détails, comme illustré dans l'exemple suivant, puis cliquez sur Créer.



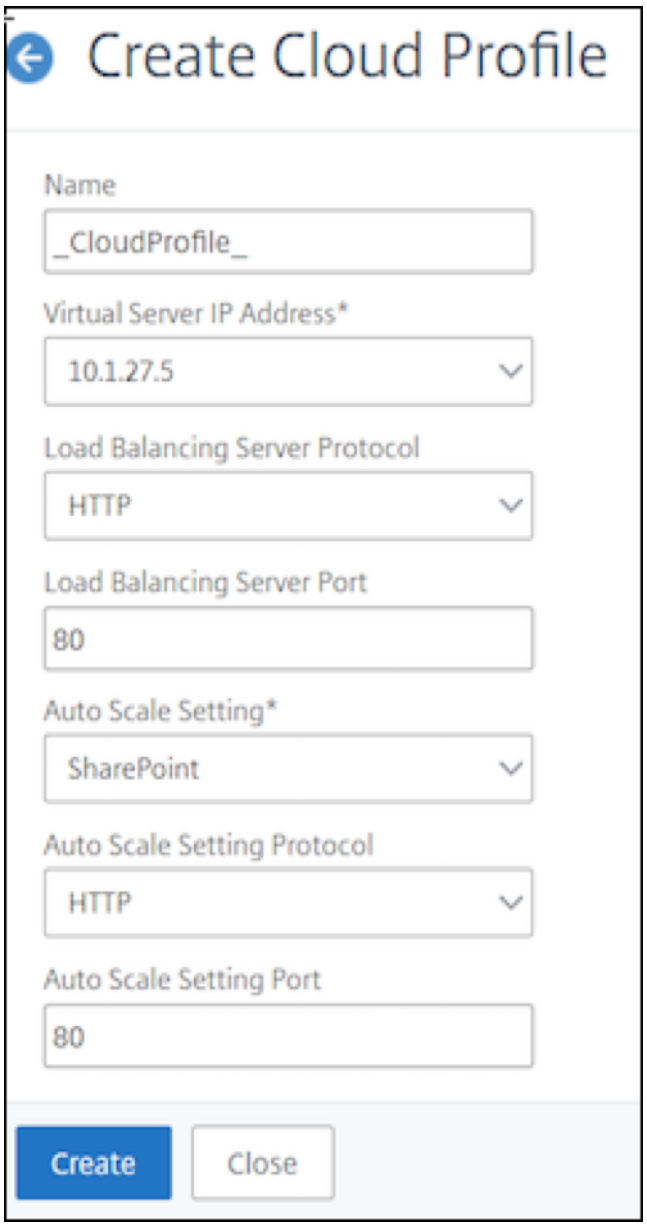
Points à garder à l'esprit lors de la création d'un profil cloud

- L'adresse IP du serveur virtuel est renseignée automatiquement à partir de l'adresse IP libre disponible pour l'instance VPX. Pour plus d'informations, voir Attribuer plusieurs adresses IP à des machines virtuelles à l'aide du portail Azure.
- Le paramètre Autoscale est prérempli à partir du paramètre VMSS Autoscale configuré dans le groupe de ressources actuel de votre compte Azure. Pour plus d'informations, voir Vue d'ensemble des jeux d'échelle de machines virtuelles Azure Autoscale with Azure.
- Lors de la sélection du protocole et du port Auto Scaling Group, assurez-vous que vos serveurs écoutent ces protocoles et ces ports et que vous liez le moniteur approprié dans le groupe de services. Par défaut, le moniteur TCP est utilisé.
- Pour le type de protocole SSL Autos Scaling, une fois que vous avez créé le profil de nuage, le serveur virtuel d'équilibrage de charge ou le groupe de services sera arrêté en raison d'un certificat manquant. Vous pouvez lier manuellement le certificat au serveur virtuel ou au groupe de services.

Après la première ouverture de session, si vous souhaitez créer un profil cloud, accédez à Système > Azure > Profil Cloud, puis cliquez sur Ajouter.



La page de configuration Créer un profil Cloud s'affiche.



Cloud Profile crée un serveur virtuel Citrix ADC d'équilibrage de charge (LB) (serveur virtuel) et un groupe de services avec des membres (serveurs) comme serveurs du groupe Auto Scaling. Vos serveurs back-end doivent être accessibles via le SNIP configuré sur l'instance VPX.

Pour afficher les informations relatives à la mise à l'échelle automatique dans le portail Azure, accédez à Tous les services > Jeu d'échelle de machine virtuelle > Sélectionner un jeu d'échelle de machine virtuelle > Mise à l'échelle.

Balises Azure pour le déploiement Citrix ADC VPX

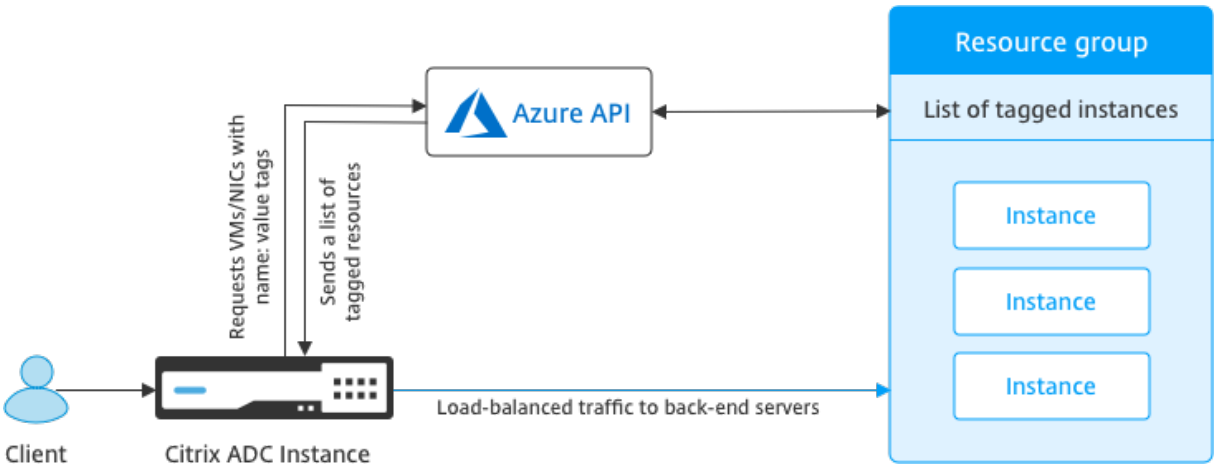
August 20, 2021

Dans le portail cloud Azure, vous pouvez baliser les ressources avec un nom : paire de valeurs (comme Dept : Finance) pour catégoriser et afficher les ressources entre les groupes de ressources et, au sein du portail, sur tous les abonnements. Le balisage est utile lorsque vous avez besoin d'organiser des ressources pour la facturation, la gestion ou l'automatisation.

Fonctionnement de la balise Azure pour le déploiement VPX

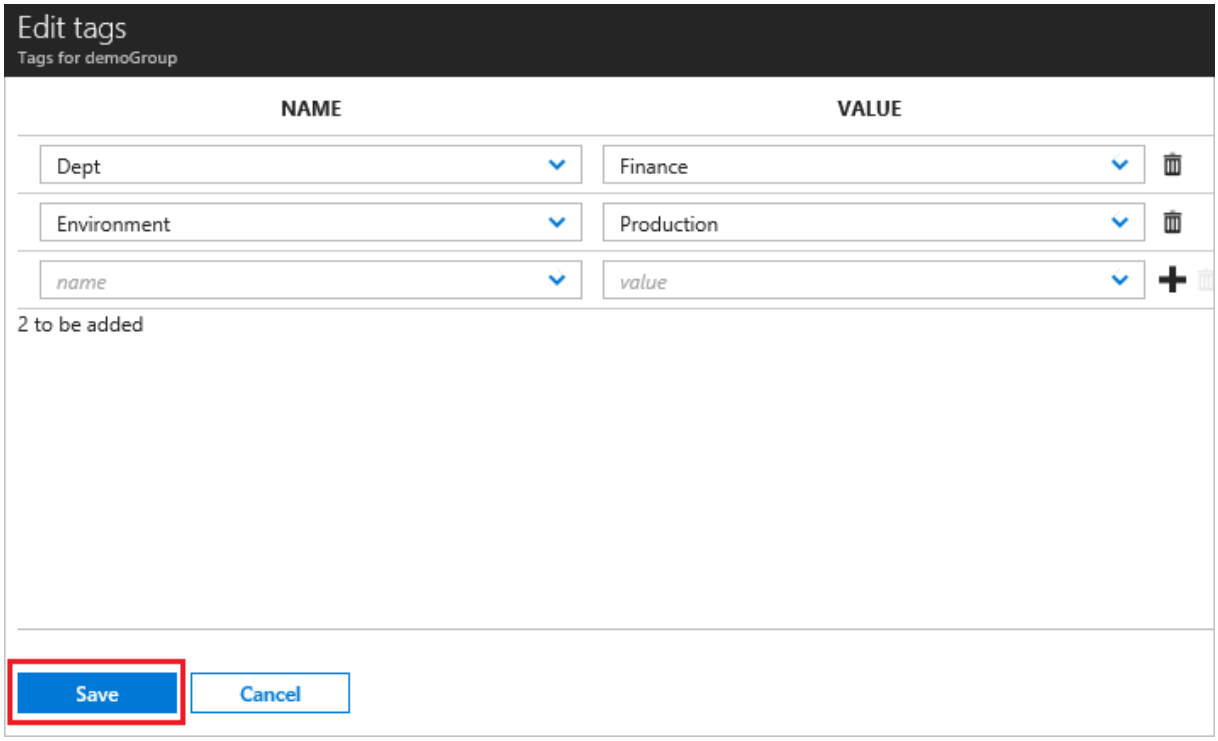
Pour les instances autonomes et haute disponibilité Citrix ADC VPX déployées sur Azure Cloud, vous pouvez désormais créer des groupes de services d'équilibrage de charge associés à une balise Azure. L'instance VPX surveille constamment les machines virtuelles Azure (serveurs back-end) et les interfaces réseau (NIC), ou les deux, avec la balise respective et met à jour le groupe de services en conséquence.

L'instance VPX crée le groupe de services qui équilibre la charge des serveurs back-end à l'aide de balises. L'instance interroge l'API Azure pour toutes les ressources qui sont balisées avec un nom de balise et une valeur de balise particuliers. En fonction de la période d'interrogation assignée (60 secondes par défaut), l'instance VPX interroge périodiquement l'API Azure et récupère les ressources disponibles avec le nom de balise et les valeurs de balise affectées dans l'interface graphique VPX. Chaque fois qu'une machine virtuelle ou une carte réseau avec la balise appropriée est ajoutée ou supprimée, ADC détecte la modification correspondante et ajoute ou supprime automatiquement l'adresse IP de la machine virtuelle ou de la carte réseau du groupe de services.



Avant de commencer

Avant de créer des groupes de services d'équilibrage de charge Citrix ADC, ajoutez une balise aux serveurs dans Azure. Vous pouvez affecter la balise à la machine virtuelle ou à la carte réseau.



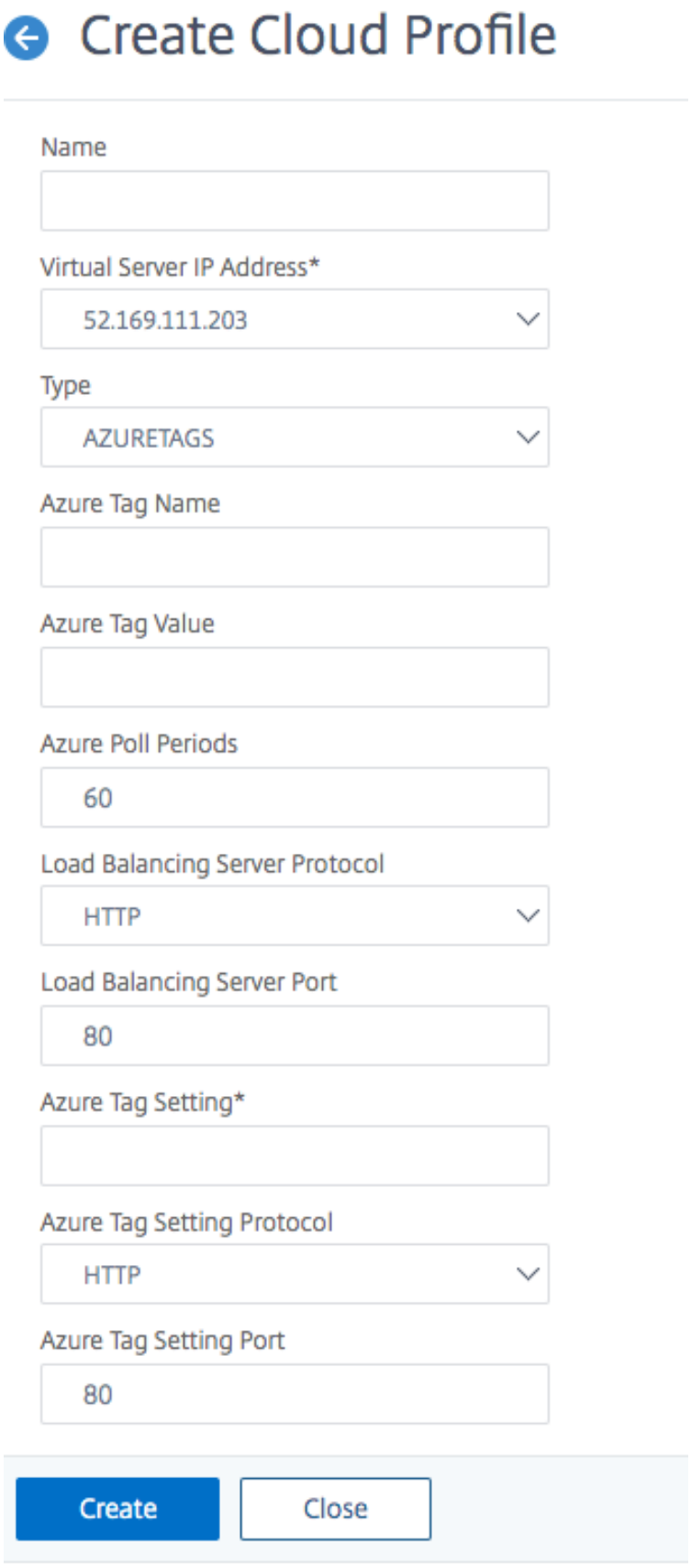
Pour plus d'informations sur l'ajout de balises Azure, consultez le document Microsoft Utiliser des balises pour organiser vos ressources Azure.

> Remarque Les commandes de l'interface de ligne de commande
> ADC pour ajouter des paramètres de balise Azure prennent en charge les noms de balise et les valeurs de balise qui commencent uniquement par des chiffres ou des alphabets et non par d'autres caractères du clavier.

Comment ajouter des paramètres de balise Azure à l'aide de l'interface graphique VPX

Vous pouvez ajouter le profil de nuage de balises Azure à une instance VPX à l'aide de l'interface graphique VPX afin que l'instance puisse équilibrer la charge des serveurs back-end à l'aide de la balise spécifiée. Procédez comme suit :

1. Dans l'interface graphique VPX, accédez à **Configuration > Azure > Cloud Profile**.
2. Cliquez sur Ajouter pour créer un profil cloud. La fenêtre de profil du nuage s'ouvre.



1. Entrez des valeurs pour les champs suivants :
   - Nom : Ajouter un nom pour votre profil
   - Adresse IP du serveur virtuel : l'adresse IP du serveur virtuel est renseignée automatiquement à partir de l'adresse IP libre disponible pour l'instance VPX. Pour plus d'informations, voir Attribuer plusieurs adresses IP à des machines virtuelles à l'aide du portail Azure.
   - Type : Dans le menu, sélectionnez AZURETAGS.
   - Nom de balise Azure : entrez le nom que vous avez attribué aux machines virtuelles ou aux cartes réseau dans le portail Azure.
   - Valeur de balise Azure : entrez la valeur que vous avez attribuée aux machines virtuelles ou aux cartes réseau dans le portail Azure.
   - Périodes d'interrogation Azure : par défaut, la période d'interrogation est de 60 secondes, soit la valeur minimale. Vous pouvez le modifier en fonction de vos besoins.
   - Protocole serveur d'équilibrage de charge : sélectionnez le protocole que votre équilibreur de charge écoute.
   - Port du serveur d'équilibrage de charge : sélectionnez le port sur lequel votre équilibreur de charge écoute.
   - Paramètre de balise Azure : nom du groupe de services qui sera créé pour ce profil cloud.
   - Azure Tag Setting Protocol : sélectionnez le protocole sur lequel vos serveurs back-end écoutent.
   - Port de réglage de balise Azure : sélectionnez le port sur lequel vos serveurs back-end écoutent.
2. Cliquez sur **Créer**.

Un serveur virtuel d'équilibrage de charge et un groupe de services sont créés pour les machines virtuelles ou cartes réseau balisées. Pour afficher le serveur virtuel d'équilibrage de charge, à partir de l'interface graphique VPX, accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

Comment ajouter des paramètres de balise Azure à l'aide de la CLI VPX

Tapez la commande suivante sur Citrix ADC CLI pour créer un profil cloud pour les balises Azure.

```
1 add cloud profile `<profile name>` -type azuretags -vServerName `<
    vserver name>` -serviceType HTTP -IPAddress `<vserver IP address>` -
    port 80 -serviceGroupName `<service group name>` -
    boundServiceGroupSvcType HTTP -vsvrbindsvcport 80 -azureTagName `<
    Azure tag specified on Azure portal>` -azureTagValue `<Azure value
    specified on the Azure portal>` -azurePollPeriod 60
2
3 <!--NeedCopy-->
```


> Important
> Vous devez enregistrer toutes les configurations ; sinon, les configurations sont perdues après le redémarrage de l'instance. Tapez `save config`.

Exemple 1 : Voici un exemple de commande pour un profil cloud pour le trafic HTTP de tous les VM-S/NIC Azure marqués avec la paire « MyTagname/MyTagValue » :

```
1 add cloud profile MyTagCloudProfile -type azuretags -vServerName
     MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80 -
     serviceGroupName MyTagsServiceGroup -boundServiceGroupSvcType HTTP -
     vsvrbindsvcport 80 -azureTagName myTagName -azureTagValue myTagValue
      -azurePollPeriod 60
2 Done
3 <!--NeedCopy-->
```

Pour afficher le profil de nuage, tapez `show cloudprofile`.

Exemple 2 : la commande CLI suivante imprime des informations sur le profil de nuage nouvellement ajouté dans l'exemple 1.

```
1 show cloudprofile
2 1)    Name:  MyTagCloudProfile Type:  azuretags         VServerName:
     MyTagVServer ServiceType:  HTTP       IPAddress:  52.178.209.133
     Port:  80               ServiceGroupName:  MyTagsServiceGroup
     BoundServiceGroupSvcType:  HTTP
3       Vsvrbindsvcport:  80     AzureTagName:  myTagName AzureTagValue:
          myTagValue AzurePollPeriod:  60     GraceFul:  NO
         Delay:  60
4 <!--NeedCopy-->
```

Pour supprimer un profil cloud, tapez profil cloud rm <`cloud profile name`>

Exemple 3 : La commande suivante supprime le profil de nuage créé dans l'exemple 1.

```
1 > rm cloudprofile MyTagCloudProfile
2   Done
3 <!--NeedCopy-->
```

Résolution des problèmes

Problème : Dans de très rares cas, la commande CLI « profil cloud rm » peut ne pas supprimer le groupe de services et les serveurs associés au profil cloud supprimé. Cela se produit lorsque la commande est émise secondes avant l'expiration de la période d'interrogation du profil de nuage en cours de suppression.

Solution : supprimez manuellement les groupes de services restants en entrant la commande CLI suivante pour chacun des groupes de services restants :

```
#> rm servicegroup <serviceGroupName>

<!--NeedCopy-->
```

Supprimez également chacun des serveurs restants en entrant la commande CLI suivante pour chacun des serveurs restants :

```
#> rm server <name>
<!--NeedCopy-->
```

Problème : Si vous ajoutez un paramètre de balise Azure à une instance VPX à l'aide de l'interface de ligne de commande, le processus rain_tags continue de s'exécuter sur un nœud de paire HA après un redémarrage chaud.

Solution : Terminer manuellement le processus sur le nœud secondaire après un redémarrage à chaud. À partir de l'interface de ligne de commande du nœud HA secondaire, sortez de l'invite de commandes :

```
#> shell

<!--NeedCopy-->
```

Utilisez la commande suivante pour tuer le processus rain_tags :

```
# PID=`ps -aux | grep rain_tags | awk '{
 print $2 }
 '`; kill -9 $PID

<!--NeedCopy-->
```

Problème : les serveurs back-end peuvent ne pas être accessibles et signalés comme DOWN par l'instance VPX, bien qu'ils soient en bonne santé.
Solution : Assurez-vous que l'instance VPX peut atteindre l'adresse IP balisée correspondant au serveur principal. Pour une carte réseau balisée, il s'agit de l'adresse IP de la carte réseau ; alors que pour une machine virtuelle balisée, il s'agit de l'adresse IP principale de la machine virtuelle. Si la VM/NIC réside sur un autre réseau virtuel Azure, assurez-vous que l'appairage de VNet est activé.

Configurer GSLB sur les instances Citrix ADC VPX

August 20, 2021

Les appliances Citrix ADC configurées pour l'équilibrage de charge des serveurs globaux (GSLB) assurent la reprise après sinistre et la disponibilité continue des applications en protégeant contre les points de défaillance d'un réseau étendu. GSLB peut équilibrer la charge entre les centres de données en dirigeant les demandes des clients vers le centre de données le plus proche ou le plus performant, ou vers les centres de données survivants en cas de panne.

Cette section décrit comment activer GSLB sur des instances VPX sur deux sites dans un environnement Microsoft Azure, à l'aide des commandes Windows PowerShell.

> **Remarque**
>
> Pour plus d'informations sur GSLB, consultez Global Server Load Balancing.

Vous pouvez configurer GSLB sur une instance Citrix ADC VPX sur Azure, en deux étapes :

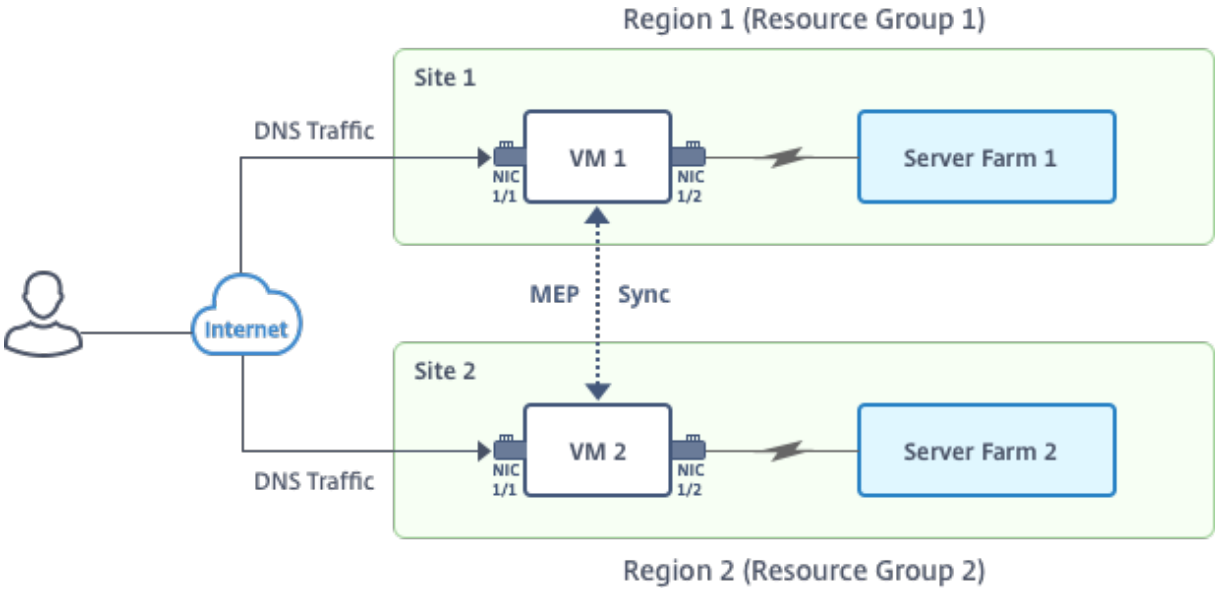
1. Créez une instance VPX avec plusieurs cartes réseau et plusieurs adresses IP, sur chaque site.
2. Activez GSLB sur les instances VPX.

> **Remarque**
>
> Pour plus d'informations sur la configuration de plusieurs cartes réseau et adresses IP, voir : Configurer plusieurs adresses IP pour une instance Citrix ADC VPX en mode autonome à l'aide des commandes PowerShell.

Scénario

Ce scénario comprend deux sites : le site 1 et le site 2. Chaque site dispose d'une machine virtuelle (VM1 et VM2) configurée avec plusieurs cartes réseau, plusieurs adresses IP et GSLB.

figure. Mise en place de la GSLB sur deux sites - le site 1 et le site 2.



Dans ce scénario, chaque machine virtuelle dispose de trois cartes réseau - NIC 0/1, 1/1 et 1/2. Chaque carte réseau peut avoir plusieurs adresses IP privées et publiques. Les cartes réseau sont configurées aux fins suivantes.

- Carte réseau 0/1 : pour servir le trafic de gestion
- Carte réseau 1/1 : pour servir le trafic côté client
- NIC 1/2 : pour communiquer avec les serveurs back-end

Pour plus d'informations sur les adresses IP configurées sur chaque carte réseau dans ce scénario, reportez-vous à la section Détails de la configuration IP .

Paramètres

Voici des exemples de paramètres de paramètres pour ce scénario dans ce document. Vous pouvez utiliser différents paramètres si vous le souhaitez.

```
$location="West Central US"

$vnetName="NSVPX-vnet"

$RGName="multiIP-RG"

$prmStorageAccountName="multiipstorageaccnt"

$avSetName="MultiIP-avset"

$vmSize="Standard_DS3_V2"
<!--NeedCopy-->
```

Remarque : La configuration minimale requise pour une instance VPX est de 2 processeurs virtuels et de 2 Go de RAM.

```
$publisher="citrix"

$offer="netscalervpx111"

$sku="netscalerbyol"

$version="latest"

$vmNamePrefix="MultiIPVPX"

$nicNamePrefix="MultiipVPX"

$osDiskSuffix="osdiskdb"
```



```
14
15 $numberOfVMs=1
16
17 $ipAddressPrefix="10.0.0."
18
19 $ipAddressPrefix1="10.0.1."
20
21 $ipAddressPrefix2="10.0.2."
22
23 $pubIPName1="MultiIP-pip1"
24
25 $pubIPName2="MultiIP-pip2"
26
27 $IpConfigName1="IPConfig1"
28
29 $IPConfigName2="IPConfig-2"
30
31 $IPConfigName3="IPConfig-3"
32
33 $IPConfigName4="IPConfig-4"
34
35 $frontendSubnetName="default"
36
37 $backendSubnetName1="subnet_1"
38
39 $backendSubnetName2="subnet_2"
40
41 $suffixNumber=10
42 <!--NeedCopy-->
```

Créer une machine virtuelle

Suivez les étapes 1 à 10 pour créer VM1 avec plusieurs cartes réseau et plusieurs adresses IP, à l'aide des commandes PowerShell :

1. Créer un groupe de ressources
2. Créer un compte de stockage
3. Créer un jeu de disponibilité
4. Créer un réseau virtuel
5. Créer une adresse IP publique
6. Créer des cartes réseau

7. Créer un objet de configuration VM
8. Obtenir les informations d'identification et définir les propriétés du SE pour la machine virtuelle
9. Ajouter des cartes réseau
10. Spécifier le disque du système d'exploitation et créer une machine virtuelle

Après avoir terminé toutes les étapes et commandes pour créer VM1, répétez ces étapes pour créer VM2 avec des paramètres spécifiques.

Créer un groupe de ressources

```
New-AzureRMResourceGroup -Name $RGName -Location $location
<!--NeedCopy-->
```

Créer un compte de stockage

```
$prmStorageAccount=New-AzureRMStorageAccount -Name
    $prmStorageAccountName -ResourceGroupName $RGName -Type Standard_LRS
     -Location $location
<!--NeedCopy-->
```

Créer un jeu de disponibilité

```
$avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
    $RGName -Location $location
<!--NeedCopy-->
```

Créer un réseau virtuel

1. Ajouter des sous-réseaux.

```
$subnet1=New-AzureRmVirtualNetworkSubnetConfig -Name
    $frontendSubnetName -AddressPrefix "10.0.0.0/24"
$subnet2=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName1 -AddressPrefix "10.0.1.0/24"
$subnet3=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName2 -AddressPrefix "10.0.2.0/24"
<!--NeedCopy-->
```

2. Ajouter un objet réseau virtuel.


```
$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
    $RGName -Location $location -AddressPrefix 10.0.0.0/16 -Subnet
    $subnet1, $subnet2, $subnet3
<!--NeedCopy-->
```

3. Récupérer les sous-réseaux.

```
$frontendSubnet=$vnet.Subnets|?{
 $\_.Name -eq $frontendSubnetName }

$backendSubnet1=$vnet.Subnets|?{
 $\_.Name -eq $backendSubnetName1 }

$backendSubnet2=$vnet.Subnets|?{
 $_.Name -eq $backendSubnetName2 }

<!--NeedCopy-->
```

Créer une adresse IP publique

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
<!--NeedCopy-->
```

Créer des cartes réseau

Créer une carte réseau 0/1

```
$nic1Name=$nicNamePrefix + $suffixNumber + "-Mgmnt"
$ipAddress1=$ipAddressPrefix + $suffixNumber
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    SubnetId $frontendSubnet.Id -PublicIpAddress $pip1 -PrivateIpAddress
     $ipAddress1 -Primary
$nic1=New-AzureRMNetworkInterface -Name $nic1Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig1
<!--NeedCopy-->
```

Créer une carte réseau 1/1

```
$nic2Name $nicNamePrefix + $suffixNumber + "-frontend"
```



```
$ipAddress2=$ipAddressPrefix1 + ($suffixNumber)
$ipAddress3=$ipAddressPrefix1 + ($suffixNumber + 1)
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    PublicIpAddress $pip2 -SubnetId $backendSubnet1.Id  -
    PrivateIpAddress $ipAddress2  -Primary
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    SubnetId $backendSubnet1.Id  -PrivateIpAddress $ipAddress3
nic2=New-AzureRMNetworkInterface -Name $nic2Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig2, $IpConfig3
<!--NeedCopy-->
```

Créer une carte réseau 1/2

```
$nic3Name=$nicNamePrefix + $suffixNumber + "-backend"
$ipAddress4=$ipAddressPrefix2 + ($suffixNumber)
$IPConfig4=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
    SubnetId $backendSubnet2.Id -PrivateIpAddress $ipAddress4 -Primary
$nic3=New-AzureRMNetworkInterface -Name $nic3Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig4
<!--NeedCopy-->
```

Créer un objet de configuration VM

```
$vmName=$vmNamePrefix
$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avSet.Id
<!--NeedCopy-->
```

Obtenir les informations d'identification et définir les propriétés du système d'exploitation

```
$cred=Get-Credential -Message "Type the name and password for VPX login
    ."
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
    ComputerName $vmName -Credential $cred
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
    $publisher -Offer $offer -Skus $sku -Version $version
<!--NeedCopy-->
```

Ajouter des cartes réseau


```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
    Primary
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id
<!--NeedCopy-->
```

Spécifier le disque du système d'exploitation et créer une machine virtuelle

```
$osDiskName=$vmName + "-" + $osDiskSuffix
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/"
     +$osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
    $osVhdUri -CreateOption fromImage
Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
    Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $RGName -Location
    $location
<!--NeedCopy-->
```

> **Remarque**
>
> Répétez les étapes 1 à 10 répertoriées dans « Créer des machines virtuelles multi-cartes réseau à l'aide des commandes PowerShell » pour créer VM2 avec des paramètres spécifiques à VM2.

Détails de la configuration IP

Les adresses IP suivantes sont utilisées.

Tableau 1. Adresses IP utilisées dans VM1

CARTE RÉSEAU	IP privée	IP publique (PIP)	Description
0/1	10.0.0.10	PIP1	Configuration en tant que NSIP (IP de gestion)
1/1	10.0.1.10	PIP2	Configuration en tant qu'IP du site SNIP/GSLB

CARTE RÉSEAU	IP privée	IP publique (PIP)	Description
-	10.0.1.11	-	Configurez comme IP du serveur LB. La propriété intellectuelle publique n'est pas obligatoire
12	10.0.2.10	-	Configuration en tant que SNIP pour l'envoi de sondes de moniteur aux services ; une IP publique n'est pas obligatoire

Tableau 2. Adresses IP utilisées dans VM2

CARTE RÉSEAU	IP interne	IP publique (PIP)	Description
0/1	20.0.0.10	PIP4	Configuration en tant que NSIP (IP de gestion)
1/1	20.0.1.10	PIP5	Configuration en tant qu'IP du site SNIP/GSLB
-	20.0.1.11	-	Configurez comme IP du serveur LB. La propriété intellectuelle publique n'est pas obligatoire
12	20.0.2.10	-	Configuration en tant que SNIP pour l'envoi de sondes de moniteur aux services ; une IP publique n'est pas obligatoire

Voici des exemples de configurations pour ce scénario, montrant les adresses IP et les configurations LB initiales telles que créées via l'interface de ligne de commande Citrix ADC VPX pour VM1 et VM2.

Voici un exemple de configuration sur VM1.

```
add ns ip 10.0.1.10 255.255.255.0 -mgmtAccess ENABLED
Add nsip 10.0.2.10 255.255.255.0
add service svc1 10.0.1.10 ADNS 53
add lb vserver v1 HTTP 10.0.1.11 80
add service s1 10.0.2.120 http 80
Add service s2 10.0.2.121 http 80
Bind lb vs v1 s[1-2]
<!--NeedCopy-->
```

Voici un exemple de configuration sur VM2.

```
add ns ip 20.0.1.10 255.255.255.0  -mgmtAccess ENABLED
Add nsip 20.0.2.10 255.255.255.0
add service svc1 20.0.1.10 ADNS 53
add lb vserver v1 HTTP 20.0.1.11 80
Add service s1 20.0.2.90 http 80
Add service s2 20.0.2.91 http 80
Bind lb vs v1 s[1-2]
<!--NeedCopy-->
```

Configurer les sites GSLB et d'autres paramètres

Effectuez les tâches décrites dans la rubrique suivante pour configurer les deux sites GSLB et les autres paramètres nécessaires :

Équilibrage de charge globale des serveurs

Pour plus d'informations, consultez cet article de support :https://support.citrix.com/article/CTX110348

Voici un exemple de configuration GSLB sur VM1 et VM2.

```
enable ns feature LB GSLB
add gslb site site1 10.0.1.10 -publicIP PIP2
add gslb site site2 20.0.1.10 -publicIP PIP5
add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP PIP3
    -publicPort 80 -siteName site1
add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP PIP6
    -publicPort 80 -siteName site2
add gslb vserver gslb_http_vip1 HTTP
bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
```



```
8 bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
9 bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
10 <!--NeedCopy-->
```

Vous avez configuré GSLB sur des instances Citrix ADC VPX exécutées sur Azure.

Pour plus d'informations sur la façon de configurer GSLB sur les instances Citrix ADC VPX, cliquez sur l'image suivante pour regarder la vidéo sur Configuration de Citrix ADC GSLB dans Microsoft Azure.

Configurer GSLB sur une configuration haute disponibilité active en veille

August 20, 2021

Vous pouvez configurer l'équilibrage de charge du serveur global (GSLB) sur un déploiement HA actif en veille sur Azure en trois étapes :

1. Créez une paire HA VPX sur chaque site GSLB. Consultez Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau pour plus d'informations sur la création d'une paire HA.
2. Configurez l'équilibreur de charge Azure (ALB) avec l'adresse IP frontale et les règles pour autoriser le trafic GSLB et DNS.

   Cette étape comporte les sous-étapes suivantes. Consultez le scénario de cette section pour connaître les commandes PowerShell utilisées pour effectuer ces sous-étapes.

   a. Créez un site frontal `IPconfig` pour GSLB.

   b. Créez un pool d'adresses back-end avec l'adresse IP de la carte réseau 1/1 des nœuds en HA.

   c. Créez des règles d'équilibrage de charge pour les éléments suivants :

   ```
   1 TCP/3011 - gslb communication
   2 TCP/3010 - gslb communication
   3 UDP/53 - DNS communication
   ```

   d. Associer le pool d'adresses back-end aux règles LB créées à l'étape c.

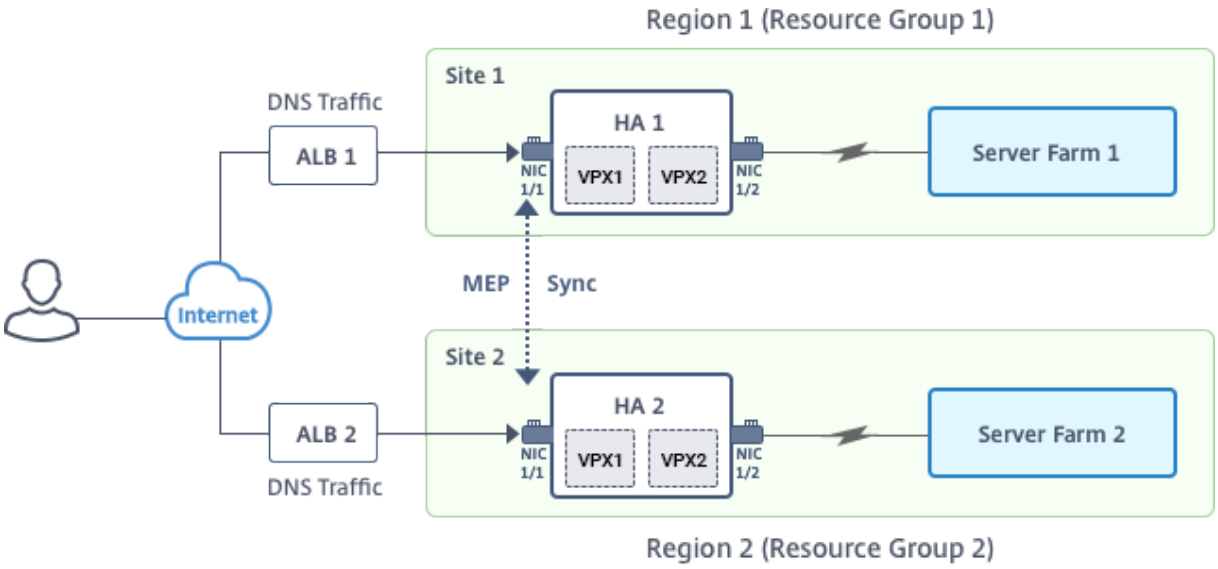
e. Mettez à jour le groupe de sécurité réseau de la carte réseau 1/1 des nœuds de la paire HA pour autoriser le trafic des ports TCP 3010, TCP 3011 et UDP 53.

3. Activez GSLB sur chaque paire HA.

Scénario

Ce scénario comprend deux sites : le site 1 et le site 2. Chaque site dispose d'une paire HA (HA1 et HA2) configurée avec plusieurs cartes réseau, plusieurs adresses IP et GSLB.

Figure : GLSB sur un déploiement HA active-Standy sur Azure



Dans ce scénario, chaque machine virtuelle dispose de trois cartes réseau - NIC 0/1, 1/1 et 1/2. Les cartes réseau sont configurées aux fins suivantes.

Carte réseau 0/1 : pour servir le trafic de gestion

Carte réseau 1/1 : pour servir le trafic côté client

NIC 1/2 : pour communiquer avec les serveurs back-end

Paramètres des paramètres

Voici des exemples de paramètres de paramètres pour l'ALB. Vous pouvez utiliser différents paramètres si vous le souhaitez.

```
$locName="South east Asia"

$rgName="MulitIP-MultiNIC-RG"

$pubIPName4="PIPFORGSLB1"
```



```
6
7  $domName4="vpxgslbdns"
8
9  $lbName="MultiIPALB"
10
11 $frontEndConfigName2="FrontEndIP2"
12
13 $backendPoolName1="BackendPoolHttp"
14
15 $lbRuleName2="LBRuleGSLB1"
16
17 $lbRuleName3="LBRuleGSLB2"
18
19 $lbRuleName4="LBRuleDNS"
20
21 $healthProbeName="HealthProbe"
```

Configurer ALB avec l'adresse IP frontale et les règles pour autoriser le trafic GSLB et DNS

Étape 1. **Créer une adresse IP publique pour l'adresse IP du site GSLB**

```
1 $pip4=New-AzureRmPublicIpAddress -Name $pubIPName4 -ResourceGroupName
      $rgName -DomainNameLabel $domName4 -Location $locName -
      AllocationMethod Dynamic
2
3
4 Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName | Add-
      AzureRmLoadBalancerFrontendIpConfig -Name $frontEndConfigName2 -
      PublicIpAddress $pip4 | Set-AzureRmLoadBalancer
```

Étape 2. **Créez des règles LB et mettez à jour l'ALB existant**.

```
1 $alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName
2
3
4 $frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
      LoadBalancer $alb -Name $frontEndConfigName2
5
6
7 $backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -
      LoadBalancer $alb -Name $backendPoolName1
8
9
```



```
$healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -
    Name $healthProbeName


$alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName2 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Tcp" -FrontendPort 3011 -BackendPort
    3011 -Probe $healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer


$alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName3 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Tcp" -FrontendPort 3010 -BackendPort
    3010 -Probe $healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer


$alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName4 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Udp" -FrontendPort 53 -BackendPort 53
    -Probe $healthprobe -EnableFloatingIP  | Set-AzureRmLoadBalancer
```

Activer GSLB sur chaque paire haute disponibilité

Vous disposez désormais de deux adresses IP frontales pour chaque ALB : ALB 1 et ALB 2. Une adresse IP est pour le serveur virtuel LB et l'autre pour l'IP du site GSLB.

HA 1 possède les adresses IP frontales suivantes :

- FrontendiPopalB1 (pour serveur virtuel LB)
- PIPFORGSLB1 (GSLB IP)

HA 2 possède les adresses IP frontales suivantes :

- FrontendiPopalB2 (pour serveur virtuel LB)
- PIPFORGSLB2 (GSLB IP)

Les commandes suivantes sont utilisées pour ce scénario.

```
enable ns feature LB GSLB

add service dnssvc PIPFORGSLB1 ADNS 53

add gslb site site1 PIPFORGSLB1 -publicIP PIPFORGSLB1

```



```
7  add gslb site site2 PIPFORGSLB2 -publicIP PIPFORGSLB2
8
9  add gslb service site1_gslb_http_svc1 FrontEndIPofALB1 HTTP 80 -
       publicIP FrontEndIPofALB1 -publicPort 80 -siteName site1
10
11 add gslb service site2_gslb_http_svc1 FrontEndIPofALB2 HTTP 80 -
       publicIP FrontEndIPofALB2 -publicPort 80 -siteName site2
12
13 add gslb vserver gslb_http_vip1 HTTP
14
15 bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
16
17 bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
18
19 bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

Ressources connexes :

Configurer GSLB sur les instances Citrix ADC VPX

Équilibrage de charge globale des serveurs

Configuration de l'adresse IP intranet des pools d'adresses pour une appliance Citrix Gateway

October 5, 2021

Dans certains cas, les utilisateurs qui se connectent au plug-in Citrix Gateway ont besoin d'une adresse IP unique pour une appliance Citrix ADC Gateway. Lorsque vous activez les pools d'adresses (également appelés pools d'adresses IP) pour un groupe, l'appliance Citrix Gateway peut attribuer un alias d'adresse IP unique à chaque utilisateur. Vous configurez des pools d'adresses à l'aide d'adresses IP intranet (IIP).

Vous pouvez configurer des pools d'adresses sur une appliance Citrix Gateway déployée sur Azure en suivant cette procédure en deux étapes :

- Enregistrement des adresses IP privées utilisées dans le pool d'adresses, dans Azure
- Configuration des pools d'adresses dans l'appliance Citrix Gateway

Enregistrer une adresse IP privée dans le portail Azure

Dans Azure, vous pouvez déployer une instance Citrix ADC VPX avec plusieurs adresses IP. Vous pouvez ajouter des adresses IP à une instance VPX de deux manières :

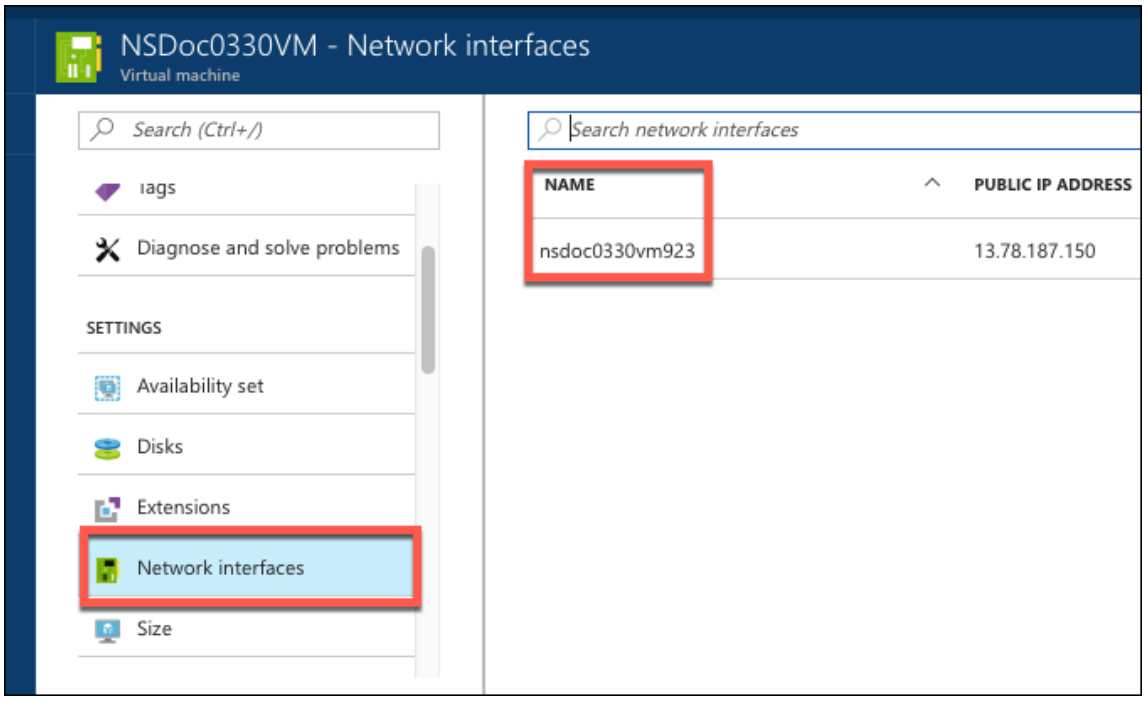
a. Lors du Provisioning d'une instance VPX

Pour plus d'informations sur la façon d'ajouter plusieurs adresses IP lors du provisionnement d'une instance VPX, consultez Configurer plusieurs adresses IP pour une instance autonome Citrix ADC. Pour ajouter des adresses IP à l'aide de commandes PowerShell lors du provisionnement d'une instance VPX, consultez Configurer plusieurs adresses IP pour une instance Citrix ADC VPX en mode autonome à l'aide de commandes PowerShell.

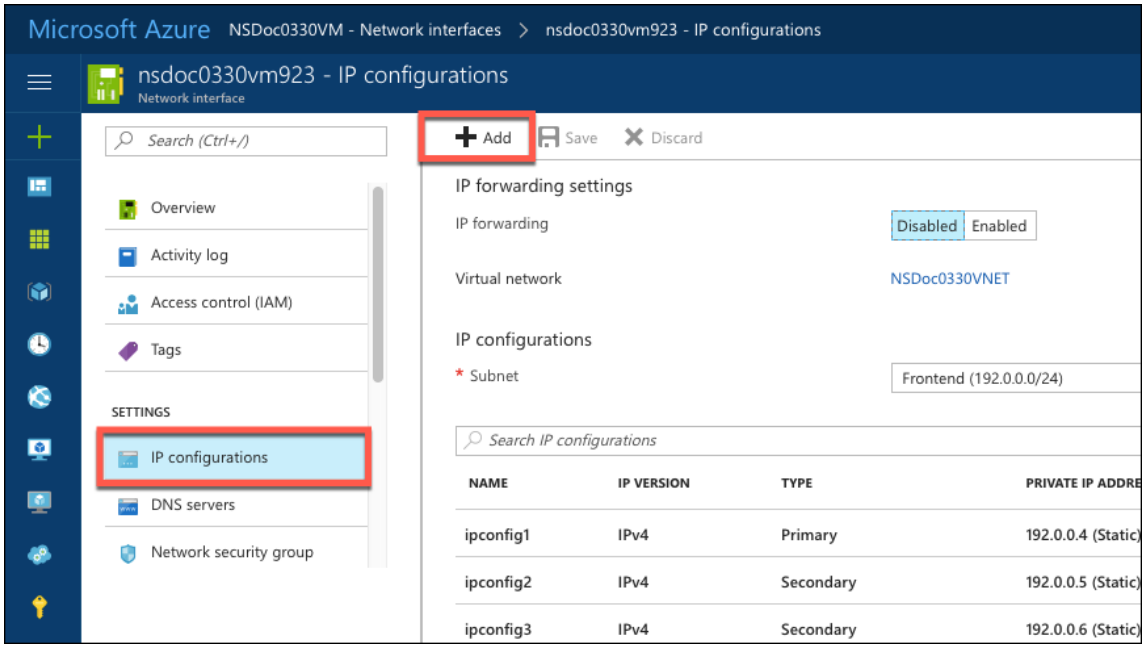
b. Après avoir Provisioning une instance VPX

Après avoir provisionné une instance VPX, suivez ces étapes pour enregistrer une adresse IP privée dans le portail Azure, que vous configurez en tant que pool d'adresses dans le dispositif Citrix Gateway.

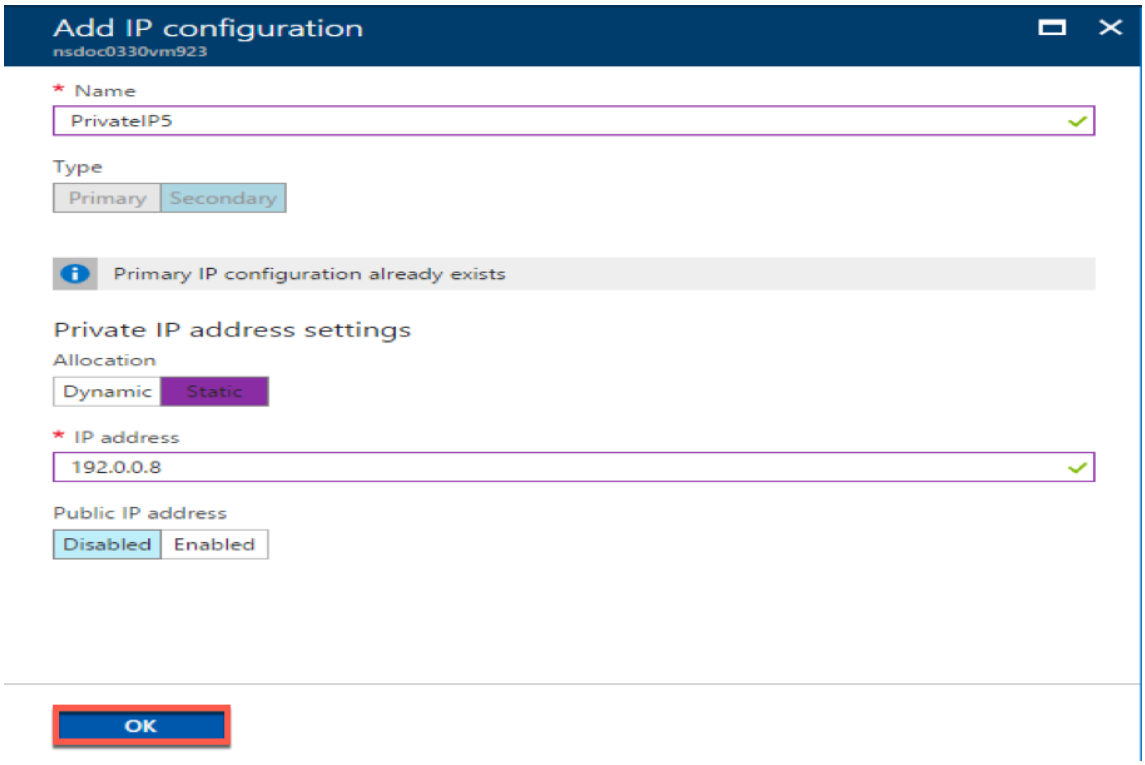
1. Dans Azure Resource Manager (ARM), accédez à l'instance Citrix ADC VPX déjà créée > **Interfaces réseau**. Choisissez l'interface réseau qui est liée à un sous-réseau auquel appartient l'IIP que vous souhaitez enregistrer.



2. Cliquez sur **Configurations IP**, puis sur **Ajouter**.



3. Fournissez les détails requis comme indiqué dans l'exemple ci-dessous et cliquez sur **OK**.



Configurer les pools d'adresses dans l'appliance Citrix Gateway

Pour plus d'informations sur la configuration des pools d'adresses sur Citrix Gateway, consultez cette section Configuration des pools d'adresses.

Limitation : Vous ne pouvez pas lier une plage d'adresses IP à des utilisateurs. Chaque adresse IIP utilisée dans un pool d'adresses doit être enregistrée.

Configurer plusieurs adresses IP pour une instance autonome Citrix ADC VPX à l'aide des commandes PowerShell

September 8, 2021

Dans un environnement Azure, une appliance virtuelle Citrix ADC VPX peut être déployée avec plusieurs cartes réseau. Chaque carte réseau peut comporter plusieurs adresses IP. Cette section explique comment déployer une instance Citrix ADC VPX avec une seule carte réseau et plusieurs adresses IP, à l'aide des commandes PowerShell. Vous pouvez utiliser le même script pour le déploiement multi-cartes réseau et multi-IP.

> **Remarque**
>
> Dans ce document, IP-Config fait référence à une paire d'adresses IP, IP publique et IP privée, associées à une carte réseau individuelle. Pour plus d'informations, consultez la section Terminologie Azure .

Cas d'utilisation

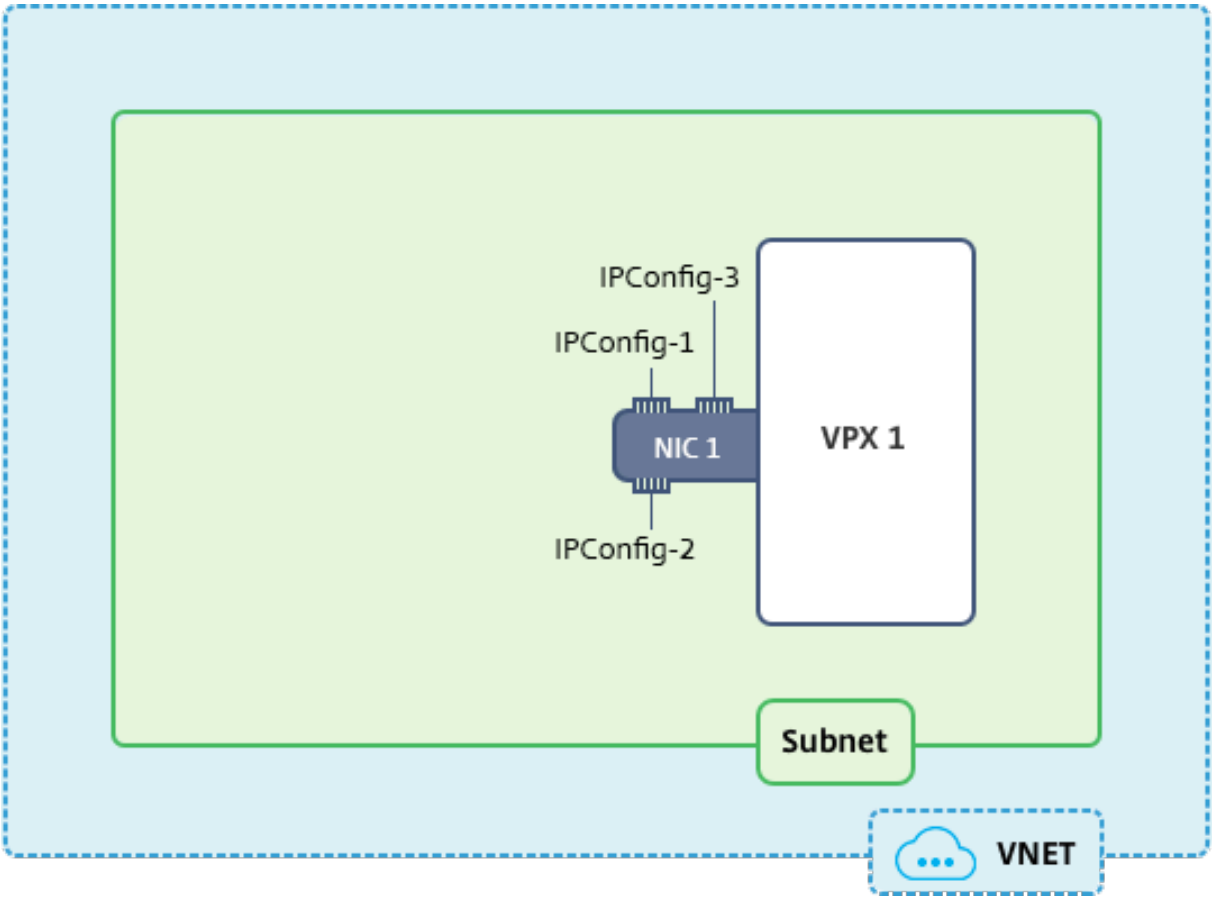
Dans ce cas d'utilisation, une seule carte réseau est connectée à un réseau virtuel (VNET). La carte réseau est associée à trois configurations IP, comme indiqué dans le tableau suivant.

Configuration IP	Associé à
IPConfig-1	Adresse IP publique statique ; adresse IP privée statique
IPConfig-2	Adresse IP publique statique ; adresse privée statique
IPConfig-3	Adresse IP privée statique

> **Remarque**
>
> IPConfig-3 n'est associé à aucune adresse IP publique.

Diagramme : Topologie

Voici la représentation visuelle du cas d'utilisation.



> **Remarque**
>
> Dans un déploiement Azure Citrix ADC VPX multi-NIC et multi-IP, l'adresse IP privée associée à la (première) `IPConfig` de la carte réseau principale (première) est automatiquement ajoutée en tant qu'adresse NSIP de gestion de l'appliance. Les adresses IP privées restantes associées `IPConfigs` doivent être ajoutées dans l'instance VPX en tant que VIP ou SNIP à l'aide de la `add ns ip` commande, comme déterminé par vos besoins.

Voici le résumé des étapes requises pour configurer plusieurs adresses IP pour un dispositif virtuel Citrix ADC VPX en mode autonome :

1. Créer un groupe de ressources
2. Créer un compte de stockage
3. Créer un jeu de disponibilité
4. Créer un groupe de services réseau
5. Créer un réseau virtuel
6. Créer une adresse IP publique
7. Attribuer une configuration IP
8. Créer une carte réseau
9. Créer une instance Citrix ADC VPX

10. Vérifier les configurations de carte réseau
11. Vérifier les configurations côté VPX

Script

Paramètres

Voici des exemples de paramètres pour le cas d'utilisation dans ce document. Vous pouvez utiliser différents paramètres si vous le souhaitez.

$locName="westcentralus"

$rgName="AZURE-MultiIP »

$nicName1="VM1-NIC1"

$VNetName="Azure-MultiIP VNet »

$vNetAddressRange="11.6.0.0/16"

$FRONTendSubnetName="FrontendSubnet »

$frontEndSubnetRange="11.6.1.0/24"

$PRMStorageAccountName="Stockage multi-IP »

$avSetName="multiip-avSet"

$VMSize="Standard_DS4_v2" (Ce paramètre crée une machine virtuelle comportant jusqu'à quatre cartes réseau.)

Remarque : La configuration minimale requise pour une instance VPX est de 2 processeurs virtuels et de 2 Go de RAM.

$publisher = « Citrix »

$offer="netscalervpx110-6531" (Vous pouvez utiliser différentes offres.)

$sku="netscalerbyol » (Selon votre offre, le SKU peut être différent.)

$version="dernière »

$pubIPName1="PIP1"

$pubIPName2="PIP2"

$domName1="multiipvpx1"

$domName2="multiipvpx2"

$VMNamePrefix="VPXMultiIP »

$osDiskSuffix="osmultiipalbdiskdb1"

Informations relatives au groupe de sécurité réseau (NSG) :

$NSGName=”NSG-MultiIP »

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

$IpConfigName1=”IPConfig1”

$IPConfigName2=”IPConfig-2”

$IPConfigName3=”IPConfig-3”

1. Créer un groupe de ressources

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. Créer un compte de stockage

```
$prmStorageAccount = New-AzureRMStorageAccount -Name $prmStorageAccountName
 -ResourceGroupName $rgName -Type Standard_LRS -Location $locName
```

3. Créer un jeu de disponibilité

```
$avSet = New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
$rgName -Location $locName
```

4. Créer un groupe de sécurité réseau

1. Ajoutez des règles. Vous devez ajouter une règle au groupe de sécurité réseau pour n’importe quel port desservant le trafic.

   ```
   $rule1=New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -Description
    "Allow HTTP"-Access Allow -Protocol Tcp -Direction Inbound -Priority
   101 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
    * -DestinationPortRange 80
   $rule2=New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -Description
    "Allow HTTPS"-Access Allow -Protocol Tcp -Direction Inbound -Priority
   110 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
    * -DestinationPortRange 443
   ```



```
$rule3=New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -Description
 "Allow SSH"-Access Allow -Protocol Tcp -Direction Inbound -Priority
120 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
 * -DestinationPortRange 22
```

2. Créez un objet de groupe de sécurité réseau.

```
$nsg=New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
```

5. Créer un réseau virtuel

1. Ajoutez des sous-réseaux.

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name $frontEndSubnetName
 -AddressPrefix $frontEndSubnetRange
```

2. Ajoutez un objet réseau virtuel.

```
$vnet=New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
$rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet
$frontendSubnet
```

3. Récupérez des sous-réseaux.

```
$subnetName="frontEndSubnet"
$subnet1=$vnet.Subnets|?{ $_.Name -eq $subnetName }
```

6. Créer une adresse IP publique

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
$rgName -DomainNameLabel $domName1 -Location $locName -AllocationMethod
Static
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
$rgName -DomainNameLabel $domName2 -Location $locName -AllocationMethod
Static
```

> **Remarque**
>
> Vérifiez la disponibilité des noms de domaine avant de les utiliser.
>
> La méthode d'allocation des adresses IP peut être dynamique ou statique.

7. Attribuer une configuration IP

Dans ce cas d'utilisation, tenez compte des points suivants avant d'attribuer des adresses IP :

- IPConfig-1 appartient au sous-net1 de VPX1.
- IPConfig-2 appartient au sous-réseau 1 du VPX1.
- IPConfig-3 appartient au sous-réseau 1 de VPX1.

> **Remarque**
>
> Lorsque vous affectez plusieurs configurations IP à une carte réseau, une configuration doit être affectée comme principale.

```
$IPAddress1="11.6.1.27"
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress $pip1
     -Primary
$IPAddress2="11.6.1.28"
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress2 -PublicIpAddress $pip2
$IPAddress3="11.6.1.29"
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress3 -Primary
```

Utilisez une adresse IP valide qui répond aux exigences de votre sous-réseau et vérifiez sa disponibilité.

8. Créer une carte réseau

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig1,$IpConfig2,$IPConfig3
 -NetworkSecurityGroupId $nsg.Id
```

9 Créer une instance Citrix ADC VPX

1. Initialisez les variables.

   ```
   $suffixNumber = 1
   $vmName = $vmNamePrefix + $suffixNumber
   ```

2. Créez un objet de configuration VM.

   ```
   $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
    $avSet.Id
   ```

3. Définissez les informations d'identification, le SE et l'image.

   ```
   $cred=Get-Credential -Message "Type the name and password for VPX login
   ."
   ```



```
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName
 $vmName -Credential $cred
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher
 -Offer $offer -Skus $sku -Version $version
```

4. Ajoutez une carte réseau.

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
Primary
```

> **Remarque**
>
> Dans un déploiement VPX multi-NIC, une carte réseau doit être principale. Par conséquent, « -Primary » doit être ajouté lors de l'ajout de cette carte réseau à l'instance VPX.

5. Spécifiez le disque du système d'exploitation et créez une machine virtuelle.

```
$osDiskName=$vmName + "-"+ $osDiskSuffix1
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString()+ "vhds/"+
 $osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
$osVhdUri -CreateOption fromImage
Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
$locName
```

10. Vérifier les configurations de carte réseau

Une fois l'instance VPX démarrée, vous pouvez vérifier les adresses IP allouées à `IPConfigs` la carte réseau VPX à l'aide de la commande suivante.

```
$nic.IPConfig
```

11. Vérifier les configurations côté VPX

Lorsque l'instance Citrix ADC VPX démarre, une adresse IP privée associée à la carte réseau principale `IPconfig` de la carte réseau principale est ajoutée en tant qu'adresse NSIP. Les adresses IP privées restantes doivent être ajoutées en tant qu'adresses VIP ou SNIP, selon vos besoins. Utilisez la commande suivante.

```
add nsip <Private IPAddress><netmask> -type VIP/SNIP
```

Vous avez maintenant configuré plusieurs adresses IP pour une instance Citrix ADC VPX en mode autonome.

Scripts PowerShell supplémentaires pour le déploiement Azure

August 20, 2021

Cette section fournit les applets de commande PowerShell avec lesquels vous pouvez effectuer les configurations suivantes dans Azure PowerShell :

- Provisionner une instance autonome Citrix ADC VPX
- Provisionner une paire Citrix ADC VPX dans une configuration haute disponibilité avec un équilibreur de charge externe Azure
- Provisionner une paire Citrix ADC VPX dans une configuration haute disponibilité avec l'équilibreur de charge interne Azure

Consultez également les rubriques suivantes pour les configurations que vous pouvez effectuer à l'aide des commandes PowerShell :

- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell
- Configurer GSLB sur les instances Citrix ADC VPX
- Configurer GSLB sur une configuration haute disponibilité active de secours NetScaler
- Configurer plusieurs adresses IP pour une instance Citrix ADC VPX en mode autonome à l'aide des commandes PowerShell
- Configurer plusieurs VIP Azure pour une instance VPX autonome

Provisionner une instance autonome Citrix ADC VPX

1. **Créer un groupe de ressources**

   Le groupe de ressources peut inclure toutes les ressources de la solution, ou uniquement les ressources que vous souhaitez gérer en tant que groupe. L'emplacement spécifié ici est l'emplacement par défaut des ressources de ce groupe de ressources. Assurez-vous que toutes les commandes permettant de créer un équilibreur de charge utilisent le même groupe de ressources.

   ```
   $rgName="<resource group name>"
   $locName="<location name, such as West US>
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Par exemple :

   ```
   $rgName = "ARM-VPX"
   $locName = "West US"
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   <!--NeedCopy-->
   ```


2. **Créer un compte de stockage**

   Choisissez un nom unique pour votre compte de stockage qui ne contient que des lettres et des chiffres minuscules.

   ```
   $saName="<storage account name>"
   $saType="<storage account type>", specify one: Standard_LRS, Standard_GRS, Standard_RAGRS, or Premium_LRS
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName
   ```

   Par exemple :

   ```
   $saName="vpxstorage"
   $saType="Standard_LRS"
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
       -Type $saType -Location $locName
   <!--NeedCopy-->
   ```

3. **Créer un jeu de disponibilité**

   Le jeu de disponibilité permet de garder vos machines virtuelles disponibles pendant les temps d'arrêt, par exemple pendant la maintenance. Un équilibreur de charge configuré avec un jeu de disponibilité garantit que votre application est toujours disponible.

   ```
   $avName="<availability set name>"

   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName
   ```

4. **Créer un réseau virtuel**

   Ajoutez un nouveau réseau virtuel avec au moins un sous-réseau, si le sous-réseau n'a pas été créé précédemment.

   ```
   $FrontendAddressPrefix="10.0.1.0/24"
   $BackendAddressPrefix="10.0.2.0/24"
   $vnetAddressPrefix="10.0.0.0/16"
   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet
    -AddressPrefix $FrontendAddressPrefix
   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet
    -AddressPrefix $BackendAddressPrefix
   New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet $frontendSubnet
   ,$backendSubnet
   ```

   Par exemple :


```
1 $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
     frontendSubnet -AddressPrefix $FrontendAddressPrefix
2
3 $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
     backendSubnet -AddressPrefix $BackendAddressPrefix
4
5 New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName
      -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet
     $frontendSubnet,$backendSubnet
6 <!--NeedCopy-->
```

5. **Créer une carte réseau**

   Créez une carte réseau et associez la carte réseau à l'instance Citrix ADC VPX. Le sous-réseau frontal créé dans la procédure ci-dessus est indexé à 0 et le sous-réseau arrière est indexé à 1. Créez maintenant une carte réseau de l'une des trois façons suivantes :

   a) *Carte réseau avec adresse IP publique*

   ```
   $nicName="<name of the NIC of the VM>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
   $rgName -Location $locName -AllocationMethod Dynamic

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
   $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
   PublicIpAddressId $pip.Id
   ```

   b) *Carte réseau avec étiquette IP publique et DNS*

   ```
   $nicName="<name of the NIC of the VM>"

   $domName="<domain name label>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
   $rgName -DomainNameLabel $domName -Location $locName -AllocationMethod
   Dynamic
   ```

   Avant d'assigner $domName, vérifiez qu'il est disponible ou non en utilisant la commande :

   ```
   Test-AzureRmDnsAvailability -DomainQualifiedName $domName -Location
   $locName

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
   $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
   PublicIpAddressId $pip.Id
   ```

   Par exemple :


```
$nicName="frontendNIC"

$domName="vpxazure"

$pip = New-AzureRmPublicIpAddress -Name $nicName -
    ResourceGroupName $rgName -DomainNameLabel $domName -Location
    $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -SubnetId $vnet.
    Subnets[0].Id -PublicIpAddressId $pip.Id
<!--NeedCopy-->
```

c) *Carte réseau avec adresse publique dynamique et adresse IP privée statique*

Assurez-vous que l'adresse IP privée (statique) que vous ajoutez à la machine virtuelle doit correspondre à celle du sous-réseau spécifié.

```
$nicName="<name of the NIC of the VM>"

$staticIP="<available static IP address on the subnet>"

$pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
$rgName -Location $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
$rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
PublicIpAddressId $pip.Id -PrivateIpAddress $staticIP
```

6. **Créer un objet virtuel**

```
$vmName="<VM name>"

$vmSize="<VM size string>"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName

$vm=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
 $avset.Id
```

7. **Obtenir l'image Citrix ADC VPX**

```
$pubName="<Image publisher name>"

$offerName="<Image offer name>"

$skuName="<Image SKU name>"
```



```
$cred=Get-Credential -Message "Type the name and password of the local administrator account."
```

Fournissez vos informations d'identification utilisées pour vous connecter à VPX

```
$vm=Set-AzureRmVMOperatingSystem -VM $vm -Linux -ComputerName $vmName -Credential $cred -Verbose
```

```
$vm=Set-AzureRmVMSourceImage -VM $vm -PublisherName $pubName -Offer $offerName -Skus $skuName -Version "latest"
```

```
$vm=Add-AzureRmVMNetworkInterface -VM $vm -Id $nic.Id
```

Par exemple :

```
$pubName="citrix"
```

La commande suivante est utilisée pour afficher toutes les offres de Citrix :

```
Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName |
    Select Offer

$offerName="netscalervpx110-6531"
<!--NeedCopy-->
```

La commande suivante permet de connaître le SKU proposé par l'éditeur pour un nom d'offre spécifique :

```
Get-AzureRMVMImageSku -Location $locName -Publisher $pubName -Offer $offerName | Select Skus
```

8. **Créer une machine virtuelle**

```
$diskName="<name identifier for the disk in Azure storage, such as OSDisk>"
```

Par exemple :

```
$diskName="dynamic"

$pubName="citrix"

$offerName="netscalervpx110-6531"

$skuName="netscalerbyol"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName

```



```
$osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/"
    + $diskName  + ".vhd"

$vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri $osDiskUri
     -CreateOption fromImage
<!--NeedCopy-->
```

Lorsque vous créez une machine virtuelle à partir d'images présentes sur le site de vente, utilisez la commande suivante pour spécifier le plan de machine virtuelle :

```
Set-AzureRmVMPlan -VM $vm -Publisher $pubName -Product $offerName -Name
 $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

Provisionner une paire Citrix ADC VPX dans une configuration haute disponibilité avec un équilibreur de charge externe Azure

Connectez-vous à AzureRmAccount à l'aide de vos informations d'identification utilisateur Azure.

1. **Créer un groupe de ressources**

   L'emplacement spécifié ici est l'emplacement par défaut des ressources de ce groupe de ressources. Assurez-vous que toutes les commandes utilisées pour créer un équilibreur de charge utilisent le même groupe de ressources.

   ```
   $rgName="<resource group name>"

   $locName="<location name, such as West US>"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Par exemple :

   ```
   $rgName = "ARM-LB-NS"

   $locName = "West US"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   <!--NeedCopy-->
   ```

2. **Créer un compte de stockage**

   Choisissez un nom unique pour votre compte de stockage qui ne contient que des lettres et des chiffres minuscules.

   ```
   $saName="<storage account name>"
   ```


`$saType="<storage account type>"`, specify one: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS`, or `Premium_LRS`

```
New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -
Type $saType -Location $locName
```

Par exemple :

```
$saName="vpxstorage"

$saType="Standard_LRS"

New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
    -Type $saType -Location $locName
<!--NeedCopy-->
```

3. **Créer un jeu de disponibilité**

   Un équilibreur de charge configuré avec un jeu de disponibilité garantit que votre application est toujours disponible.

   `$avName="<availability set name>"`

   ```
   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -
   Location $locName
   ```

4. **Créer un réseau virtuel**

   Ajoutez un nouveau réseau virtuel avec au moins un sous-réseau, si le sous-réseau n'a pas été créé précédemment.

   ```
   $vnetName = "LBVnet"

   $FrontendAddressPrefix="10.0.1.0/24"

   $BackendAddressPrefix="10.0.2.0/24"

   $vnetAddressPrefix="10.0.0.0/16"

   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       frontendSubnet -AddressPrefix $FrontendAddressPrefix

   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       backendSubnet -AddressPrefix $BackendAddressPrefix

   $vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
        $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -
       Subnet $frontendSubnet,$backendSubnet
   ```



```
<!--NeedCopy-->
```

Remarque : Choisissez la valeur du paramètre AddressPrefix en fonction de votre besoin.

Affectez des sous-réseaux frontaux et back-end au réseau virtuel que vous avez créé précédemment au cours de cette étape.

Si le sous-réseau frontal est le premier élément du réseau virtuel de tableau, SubnetID doit être $VNet.Subnets [0] .Id.

Si le sous-réseau frontal est le deuxième élément du tableau, l'ID de sous-réseau doit être $VNet.Subnets [1] .Id, etc.

5. **Configurer l'adresse IP frontale et créer un pool d'adresses back-end**

   Configurez une adresse IP frontale pour le trafic réseau d'équilibrage de charge entrant et créez un pool d'adresses back-end pour recevoir le trafic équilibré de charge.

```
$pubName="PublicIp1"

$publicIP1 = New-AzureRmPublicIpAddress -Name $pubName -
    ResourceGroupName $rgName -Location $locName -AllocationMethod
    Static -DomainNameLabel nsvpx
<!--NeedCopy-->
```

   Remarque : Vérifiez la disponibilité de la valeur pour DomainNameLabel.

```
$FIPName = "ELBFIP"

$frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig -Name
    $FIPName -PublicIpAddress $publicIP1

$BEPool = "LB-backend-Pool"

$beaddresspool1= New-AzureRmLoadBalancerBackendAddressPoolConfig -
    Name $BEPool
<!--NeedCopy-->
```

6. **Créer une sonde de santé**

   Créez une sonde de santé TCP avec le port 9000 et l'intervalle 5 secondes.

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name
    HealthProbe -Protocol Tcp -Port 9000 -IntervalInSeconds 5 -
    ProbeCount 2
<!--NeedCopy-->
```


7. **Créer une règle d'équilibrage de charge**

   Créez une règle de LB pour chaque service que vous répartirez la charge.

   Par exemple :

   Vous pouvez utiliser l'exemple suivant pour équilibrer la charge service HTTP.

```
$lbrule1 = New-AzureRmLoadBalancerRuleConfig -Name "HTTP-LB" -
    FrontendIpConfiguration $frontendIP1 -BackendAddressPool
    $beAddressPool1 -Probe $healthProbe -Protocol Tcp -FrontendPort
     80 -BackendPort 80
<!--NeedCopy-->
```

8. **Créer des règles NAT entrantes**

   Créez des règles NAT pour les services dont vous n'êtes pas l'équilibrage de charge.

   Par exemple, lors de la création d'un accès SSH à une instance Citrix ADC VPX.

   Remarque : Le triplet Protocol-FrontEndPort-BackendPort ne doit pas être le même pour deux règles NAT.

```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name SSH1     -FrontendIpConfiguration $frontendIP1 -Protocol
    TCP -FrontendPort 22 -BackendPort 22

$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name SSH2 -FrontendIpConfiguration $frontendIP1 -Protocol TCP -
    FrontendPort 10022 -BackendPort 22
<!--NeedCopy-->
```

9. **Créer une entité d'équilibrage de charge**

   Créez l'équilibreur de charge en ajoutant tous les objets (règles NAT, règles d'équilibrage de charge, configurations de sonde) ensemble.

```
$lbName="ELB"

$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name
    $lbName -Location $locName -InboundNatRule $inboundNATRule1,
    $inboundNATRule2 -FrontendIpConfiguration $frontendIP1 -
    LoadBalancingRule $lbrule1 -BackendAddressPool $beAddressPool1
    -Probe $healthProbe
<!--NeedCopy-->
```

10. **Créer une carte réseau**

    Créez deux cartes réseau et associez chaque carte réseau à chaque instance VPX

a) NIC1 avec VPX1

Par exemple :

```
$nicName="NIC1"

$lbName="ELB"

$bePoolIndex=0

* Rule indexes starts from 0.

$natRuleIndex=0

$subnetIndex=0

* Frontend subnet index

$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
   $rgName

$nic1=New-AzureRmNetworkInterface -Name $nicName -
   ResourceGroupName $rgName -Location $locName -Subnet $vnet.
   Subnets[$subnetIndex] -LoadBalancerBackendAddressPool $lb.
   BackendAddressPools[$bePoolIndex] -LoadBalancerInboundNatRule
   $lb.InboundNatRules[$natRuleIndex]
<!--NeedCopy-->
```

b) NIC2 avec VPX2

Par exemple :

```
$nicName="NIC2"

$lbName="ELB"

$bePoolIndex=0

$natRuleIndex=1

* Second Inbound NAT (SSH) rule we need to use

`$subnetIndex=0

* Frontend subnet index

```



```
$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName

$nic2=New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -Subnet $vnet.
    Subnets[$subnetIndex] -LoadBalancerBackendAddressPool $lb.
    BackendAddressPools[$bePoolIndex] -LoadBalancerInboundNatRule
    $lb.InboundNatRules[$natRuleIndex]
<!--NeedCopy-->
```

11. **Créer des instances Citrix ADC VPX**

    Créez deux instances Citrix ADC VPX dans le cadre du même groupe de ressources et du même jeu de disponibilité, puis attachez-les à l'équilibreur de charge externe.

    a) Instance Citrix ADC VPX 1

    Par exemple :

```
$vmName="VPX1"

$vmSize="Standard_A3"

$pubName="citrix"

$offerName="netscalervpx110-6531"

$skuName="netscalerbyol"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
    $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be used
    to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id

```



```
$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/
    " + $diskName  + ".vhd"

$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
     -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm1
<!--NeedCopy-->
```

b) Instance Citrix ADC VPX 2

Par exemple :

```
$vmName="VPX2"

$vmSize="Standard_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
     $rgName

$vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message " Type Credentials which will be
    used to login to VPX instance "

$vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id

$diskName="dynamic"

```



```
$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds2/
    " + $diskName  + ".vhd"

$vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
     -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm2
<!--NeedCopy-->
```

12. **Configurer les machines virtuelles**

    Lorsque les deux instances Citrix ADC VPX démarrent, connectez-vous aux deux instances Citrix ADC VPX à l'aide du protocole SSH pour configurer les machines virtuelles.

    a) Active-Active : exécutez le même ensemble de commandes de configuration sur la ligne de commande des instances Citrix ADC VPX.

    b) Active-Passif : Exécutez cette commande sur la ligne de commande des instances Citrix ADC VPX.

    ```
    add ha node ##nodeID <nsip of other Citrix ADC VPX>
    ```

    En mode actif-passif, exécutez uniquement les commandes de configuration sur le nœud principal.

Provisionner une paire Citrix ADC VPX dans une configuration haute disponibilité avec l'équilibreur de charge interne Azure

Connectez-vous à AzureRmAccount à l'aide de vos informations d'identification utilisateur Azure.

1. **Créer un groupe de ressources**

   L'emplacement spécifié ici est l'emplacement par défaut des ressources de ce groupe de ressources. Assurez-vous que toutes les commandes permettant de créer un équilibreur de charge utilisent le même groupe de ressources.

   ```
   $rgName="\<resource group name\>"

   $locName="\<location name, such as West US\>"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```


Par exemple :

```
$rgName = "ARM-LB-NS"

$locName = "West US"

New-AzureRmResourceGroup -Name $rgName -Location $locName
<!--NeedCopy-->
```

2. **Créer un compte de stockage**

   Choisissez un nom unique pour votre compte de stockage qui ne contient que des lettres et des chiffres minuscules.

   `$saName="<storage account name>"`

   `$saType="<storage account type>"`, specify one: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS`, or `Premium_LRS`

   `New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName`

   Par exemple :

   ```
   $saName="vpxstorage"

   $saType="Standard_LRS"

   New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
       -Type $saType -Location $locName
   <!--NeedCopy-->
   ```

3. **Créer un jeu de disponibilité**

   Un équilibreur de charge configuré avec un jeu de disponibilité garantit que votre application est toujours disponible.

   `$avName="<availability set name>"`

   `New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName`

4. **Créer un réseau virtuel**

   Ajoutez un nouveau réseau virtuel avec au moins un sous-réseau, si le sous-réseau n'a pas été créé précédemment.

   ```
   $vnetName = "LBVnet"

   ```



```
$vnetAddressPrefix="10.0.0.0/16"

$FrontendAddressPrefix="10.0.1.0/24"

$BackendAddressPrefix="10.0.2.0/24"

$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
    $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -
   Subnet $frontendSubnet,$backendSubnet`

$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
   frontendSubnet -AddressPrefix $FrontendAddressPrefix

$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
   backendSubnet -AddressPrefix $BackendAddressPrefix
<!--NeedCopy-->
```

Remarque : Choisissez la valeur du paramètre AddressPrefix en fonction de votre besoin.

Affectez des sous-réseaux frontaux et back-end au réseau virtuel que vous avez créé précédemment au cours de cette étape.

Si le sous-réseau frontal est le premier élément du réseau virtuel de tableau, SubnetID doit être $VNet.Subnets [0] .Id.

Si le sous-réseau frontal est le deuxième élément du tableau, l'ID de sous-réseau doit être $VNet.Subnets [1] .Id, etc.

5. **Créer un pool d'adresses backend**

```
$beaddresspool= New-AzureRmLoadBalancerBackendAddressPoolConfig -Name "
LB-backend"
```

6. **Créer des règles NAT**

Créez des règles NAT pour les services dont vous n'êtes pas l'équilibrage de charge.

```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
   Name "Inboundnatrule1" -FrontendIpConfiguration $frontendIP -
   Protocol TCP -FrontendPort 3441 -BackendPort 3389

$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
   Name "RDP2" -FrontendIpConfiguration $frontendIP -Protocol TCP
   -FrontendPort 3442 -BackendPort 3389
<!--NeedCopy-->
```

Utilisez les ports frontaux et back-end selon vos besoins.

7. **Créer une sonde de santé**

   Créez une sonde de santé TCP avec le port 9000 et l'intervalle 5 secondes.

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name "
    HealthProbe"  " -Protocol tcp -Port 9000 -IntervalInSeconds 5 -
    ProbeCount 2
<!--NeedCopy-->
```

8. **Créer une règle d'équilibrage de charge**

   Créez une règle de LB pour chaque service que vous répartirez la charge.

   Par exemple :

   Vous pouvez utiliser l'exemple suivant pour équilibrer la charge service HTTP.

```
$lbrule = New-AzureRmLoadBalancerRuleConfig -Name "lbrule1" -
    FrontendIpConfiguration $frontendIP -BackendAddressPool
    $beAddressPool -Probe $healthProbe -Protocol Tcp -FrontendPort
    80 -BackendPort 80
<!--NeedCopy-->
```

   Utilisez les ports frontaux et back-end selon vos besoins.

9. **Créer une entité d'équilibrage de charge**

   Créez l'équilibreur de charge en ajoutant tous les objets (règles NAT, règles d'équilibrage de charge, configurations de sonde) ensemble.

```
$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgname -Name
    "InternalLB" -Location $locName -FrontendIpConfiguration
    $frontendIP -InboundNatRule $inboundNATRule1,$inboundNatRule2 -
    LoadBalancingRule $lbrule -BackendAddressPool $beAddressPool -
    Probe $healthProbe
<!--NeedCopy-->
```

10. **Créer une carte réseau**

    Créez deux cartes réseau et associez chaque carte réseau à chaque instance Citrix ADC VPX

```
$backendnic1= New-AzureRmNetworkInterface -ResourceGroupName
    $rgName -Name lb-nic1-be -Location $locName -PrivateIpAddress
    10.0.2.6 -Subnet $backendSubnet -LoadBalancerBackendAddressPool
     $nrplb.BackendAddressPools[0] -LoadBalancerInboundNatRule
    $nrplb.InboundNatRules[0]
<!--NeedCopy-->
```


Cette carte réseau est pour Citrix ADC VPX 1. L'IP privée doit se trouver dans le même sous-réseau que celui du sous-réseau ajouté.

```
$backendnic2= New-AzureRmNetworkInterface -ResourceGroupName
    $rgName -Name lb-nic2-be -Location $locName -PrivateIpAddress
    10.0.2.7 -Subnet $backendSubnet -LoadBalancerBackendAddressPool
     $nrplb.BackendAddressPools[0] -LoadBalancerInboundNatRule
    $nrplb.InboundNatRules[1].
<!--NeedCopy-->
```

Cette carte réseau est destinée à Citrix ADC VPX 2.Le paramètre `Private IPAddress` peut avoir n'importe quelle adresse IP privée selon vos besoins.

11. **Créer des instances Citrix ADC VPX**

    Créez deux instances VPX faisant partie du même groupe de ressources et du même jeu de disponibilité, puis attachez-les à l'équilibreur de charge interne.

    a) Instance Citrix ADC VPX 1

    Par exemple :

```
$vmName="VPX1"

$vmSize="Standard_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
     $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be used
     to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName
```



```
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/
      " + $diskName  + ".vhd"
22
23 $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
      $osDiskUri1 -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
       -Name $skuName
26
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
      $vm1
28 <!--NeedCopy-->
```

b) Instance Citrix ADC VPX 2

Par exemple :

```
1  $vmName="VPX2"
2
3  $vmSize="Standard_A3"
4
5  $avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
       $rgName
6
7  $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
      AvailabilitySetId $avset.Id
8
9  $cred=Get-Credential -Message " Type Credentials which will be
      used to login to VPX instance "
10
11 $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
      $vmName -Credential $cred -Verbose
12
13 $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
      Offer $offerName -Skus $skuName -Version "latest"
14
15 $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $backendnic2.Id
16
17 $diskName="dynamic"
18
19 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
      Name $saName
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds2/
```



```
      " + $diskName  + ".vhd"
22
23 $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
      $osDiskUri1 -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
       -Name $skuName
26
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
      $vm2
28 <!--NeedCopy-->
```

12. **Configurer les machines virtuelles**

    Lorsque les deux instances Citrix ADC VPX démarrent, connectez-vous aux deux instances Citrix ADC VPX à l'aide du protocole SSH pour configurer les machines virtuelles.

    a) Active-Active : exécutez le même ensemble de commandes de configuration sur la ligne de commande des instances Citrix ADC VPX.

    b) Active-Passif : Exécutez cette commande sur la ligne de commande des instances Citrix ADC VPX.

    ```
    add ha node ##nodeID <nsip of other Citrix ADC VPX>
    ```

    En mode actif-passif, exécutez uniquement les commandes de configuration sur le nœud principal.

Questions fréquentes sur Azure

August 20, 2021

- **La procédure de mise à niveau de l'instance Citrix ADC VPX installée à partir de la Place de marché Azure est-elle différente de la procédure de mise à niveau locale ?**

  Non. Vous pouvez mettre à niveau votre instance Citrix ADC VPX dans le cloud Microsoft Azure vers Citrix ADC VPX version 11.1 ou ultérieure, à l'aide des procédures de mise à niveau standard Citrix ADC VPX. Vous pouvez effectuer une mise à niveau à l'aide de procédures GUI ou CLI. Pour toute nouvelle installation, utilisez l'image Citrix ADC VPX pour le cloud Microsoft Azure.

  Pour télécharger les versions de mise à niveau Citrix ADC VPX, accédez à **Téléchargements Citrix** > **Firmware Citrix ADC**.

- **Comment corriger les mouvements MAC et les muets d'interface observés sur les instances Citrix ADC VPX hébergées sur Azure ?**

Dans un environnement Azure Multi-NIC, par défaut, toutes les interfaces de données peuvent afficher des mouvements MAC et des muettes d'interface. Pour éviter les déplacements MAC et les muets de l'interface sur les environnements Azure, Citrix vous recommande de créer un VLAN par interface de données (sans balise) de l'instance ADC VPX et de lier l'adresse IP principale de la carte réseau dans Azure.

Pour plus d'informations, consultez l'article CTX224626 .

Déployer une instance Citrix ADC VPX sur Google Cloud Platform

September 8, 2021

Vous pouvez déployer une instance Citrix ADC VPX sur Google Cloud Platform (GCP). Une instance VPX dans GCP vous permet de tirer parti des fonctionnalités de cloud computing GCP et d'utiliser les fonctionnalités d'équilibrage de charge et de gestion du trafic Citrix pour vos besoins professionnels. Vous pouvez déployer des instances VPX dans GCP en tant qu'instances autonomes. Les configurations à carte unique et à plusieurs cartes réseau sont prises en charge.

Fonctionnalités prises en charge

Une instance VPX exécutée dans GCP prend en charge les fonctionnalités suivantes :

- Équilibrage de charge
- Proxy ICA
- Commutation de contenu
- Authentification, autorisation et audit
- Réécrire
- Répondeur
- Proxy RDP
- nFactor
- LDAP
- VPN (CVPN/Full)
- GSLB

Limitation

- IPv6 n'est pas pris en charge.

Configuration matérielle requise

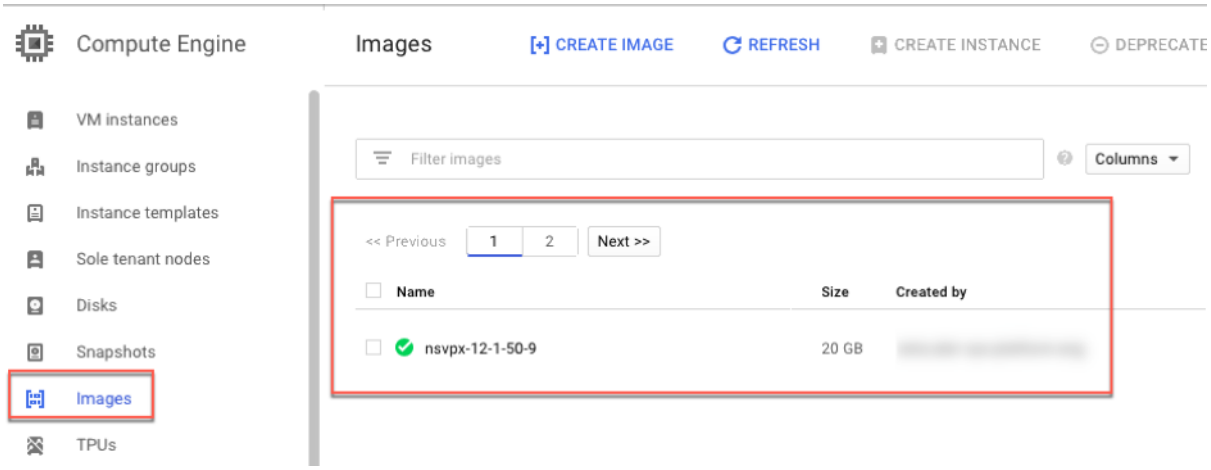
L'instance VPX dans GCP doit comporter au moins 2 processeurs virtuels et 4 Go de RAM.

Conditions préalables

1. Installez l'utilitaire « gcloud » sur votre appareil. Vous pouvez trouver l'utilitaire en cliquant sur ce lien : https://cloud.google.com/sdk/install
2. Téléchargez l'image NSVPX-GCP à partir du site de téléchargement Citrix.
3. Chargez le fichier (par exemple, NSVPX-GCP-12.1-50.9_NC_64.tar.gz) dans un compartiment de stockage sur Google en suivant les étapes indiquées à l'adresse https://cloud.google.com/storage/docs/uploading-objects.
4. Exécutez la commande suivante sur l'utilitaire gcloud pour créer une image.

```
gcloud compute images create <IMAGE_NAME> --source-uri=gs://<
    STORAGE_BUCKET_NAME>/<FILE_NAME>.tar.gz --guest-os-features=
    MULTI_IP_SUBNET
<!--NeedCopy-->
```

La création de l'image peut prendre un certain temps. Une fois l'image créée, elle apparaît sous **Compute** > **Compute Engine** dans la console GCP.



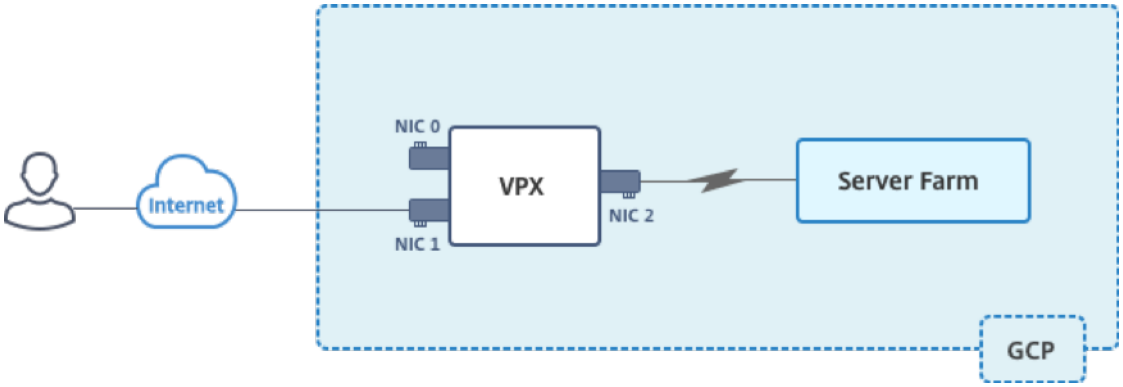
Points à noter

Prenez en compte les points spécifiques à GCP suivants avant de commencer votre déploiement.

- Après avoir créé l'instance, vous ne pouvez ni ajouter ni supprimer d'interfaces réseau.
- Pour un déploiement multi-NIC, créez des réseaux VPC distincts pour chaque carte réseau. Une carte réseau ne peut être associée qu'à un seul réseau.
- Pour une instance de carte réseau unique, la console GCP crée un réseau par défaut.
- Au moins 4 processeurs virtuels sont nécessaires pour une instance comportant plus de deux interfaces réseau.
- Si le transfert IP est requis, vous devez activer le transfert IP lors de la création de l'instance et de la configuration de la carte réseau.

Scénario : déployer une instance VPX autonome multi-cartes réseau et multi-IP

Ce scénario illustre comment déployer une instance autonome Citrix VPX dans GCP. Dans ce scénario, vous créez une instance VPX autonome avec plusieurs cartes réseau. L'instance communique avec les serveurs principaux (la batterie de serveurs).



Créez trois cartes réseau pour répondre aux objectifs suivants.

CARTE RÉSEAU	Objectif	Associé au réseau VPC
NIC 0	Dessert le trafic de gestion (Citrix ADC IP)	Réseau de gestion
CARTE RÉSEAU 1	Sert le trafic côté client (VIP)	Réseau client
NIC 2	Communication avec les serveurs back-end (SNIP)	Réseau de serveurs back-end

Configurez également les routes de communication requises entre l'instance et les serveurs principaux, ainsi qu'entre l'instance et les hôtes externes sur l'Internet public.

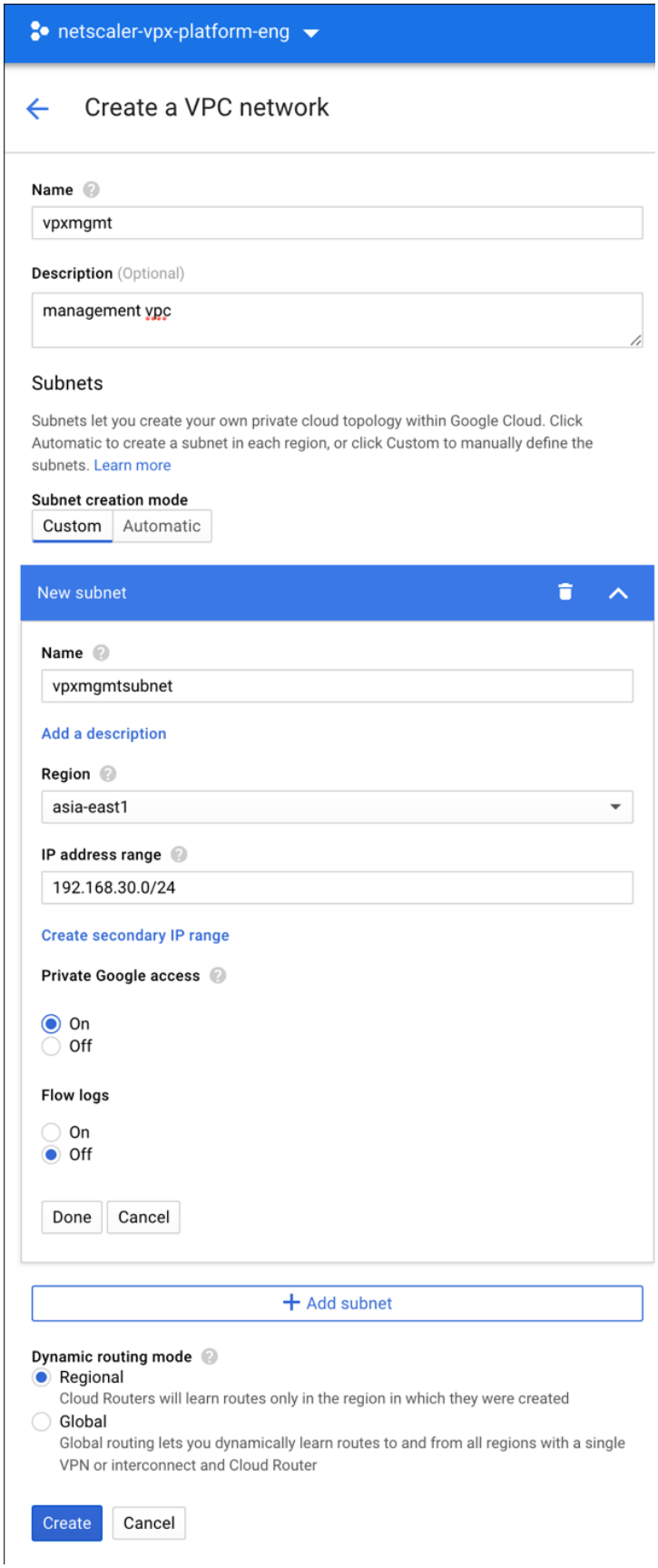
Résumé des étapes de déploiement

1. Créez trois réseaux VPC pour trois cartes réseau différentes.
2. Création de règles de pare-feu pour les ports 22, 80 et 443
3. Créer une instance avec trois cartes réseau

Remarque : créez une instance dans la même région que celle où vous avez créé les réseaux VPC.

Étape 1. Créez des réseaux VPC.

Créez trois réseaux VPC associés à la carte réseau de gestion, à la carte réseau client et à la carte réseau du serveur. Pour créer un réseau VPC, connectez-vous à **Google Console > Réseau > Réseau VPC > Créer un réseau VPC**. Remplissez les champs requis, comme indiqué dans la capture d'écran, puis cliquez sur **Créer**.

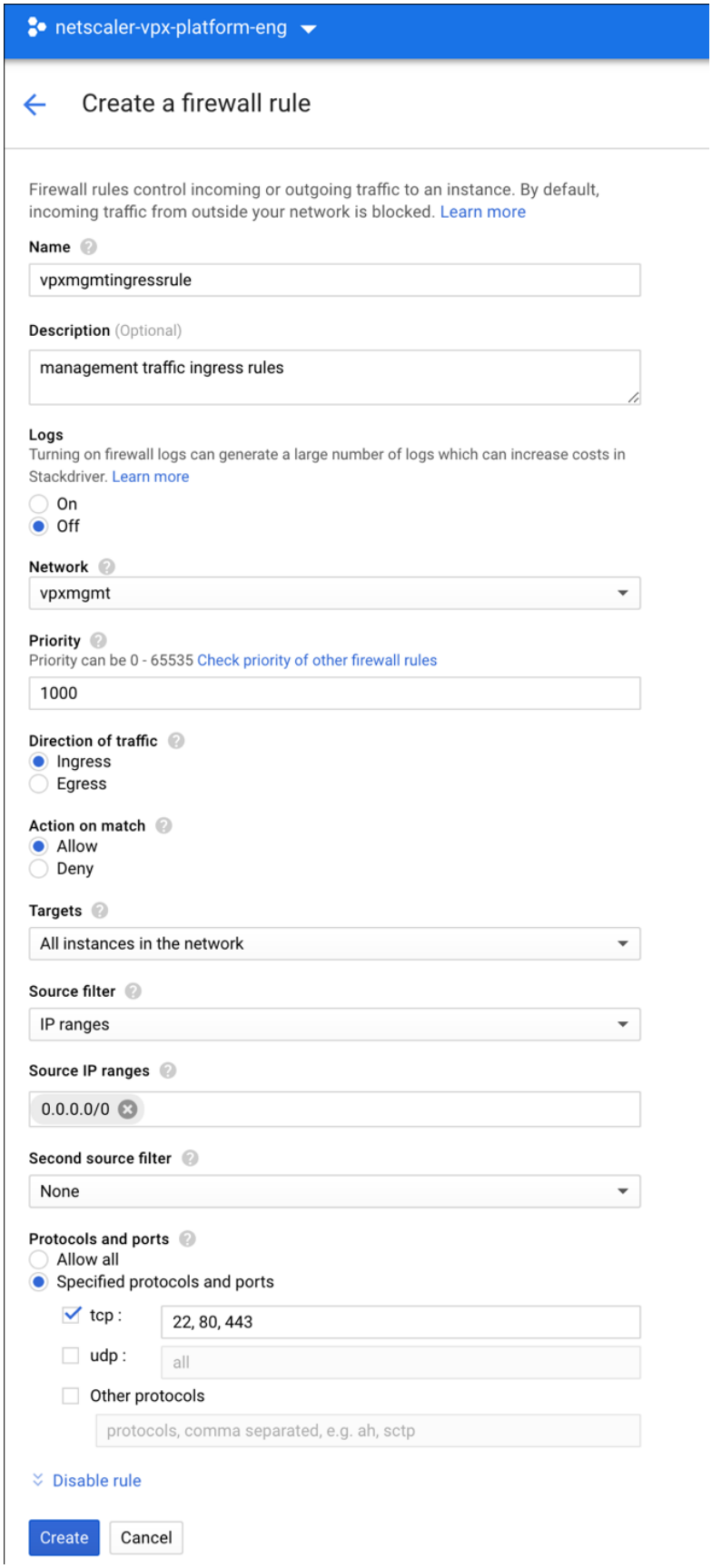


De même, créez des réseaux VPC pour les cartes réseau client et côté serveur.

Remarque : Les trois réseaux VPC doivent se trouver dans la même région, ce qui est asia-east1 dans ce scénario.

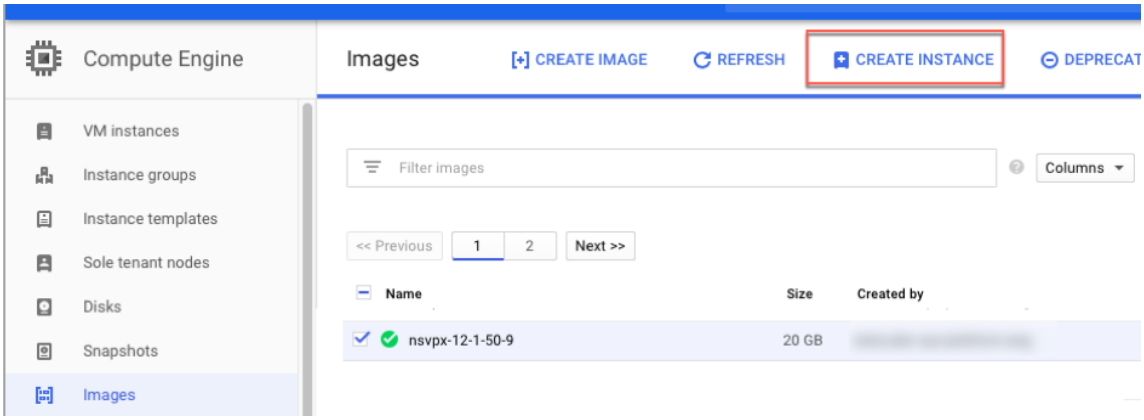
Étape 2. Créez des règles de pare-feu pour les ports 22, 80 et 443.

Créez des règles pour SSH (port 22), HTTP (port 80) et HTTPS (port 443) pour chaque réseau VPC. Pour plus d'informations sur les règles de pare-feu, voir Vue d' ensemble des règles de pare-feu.



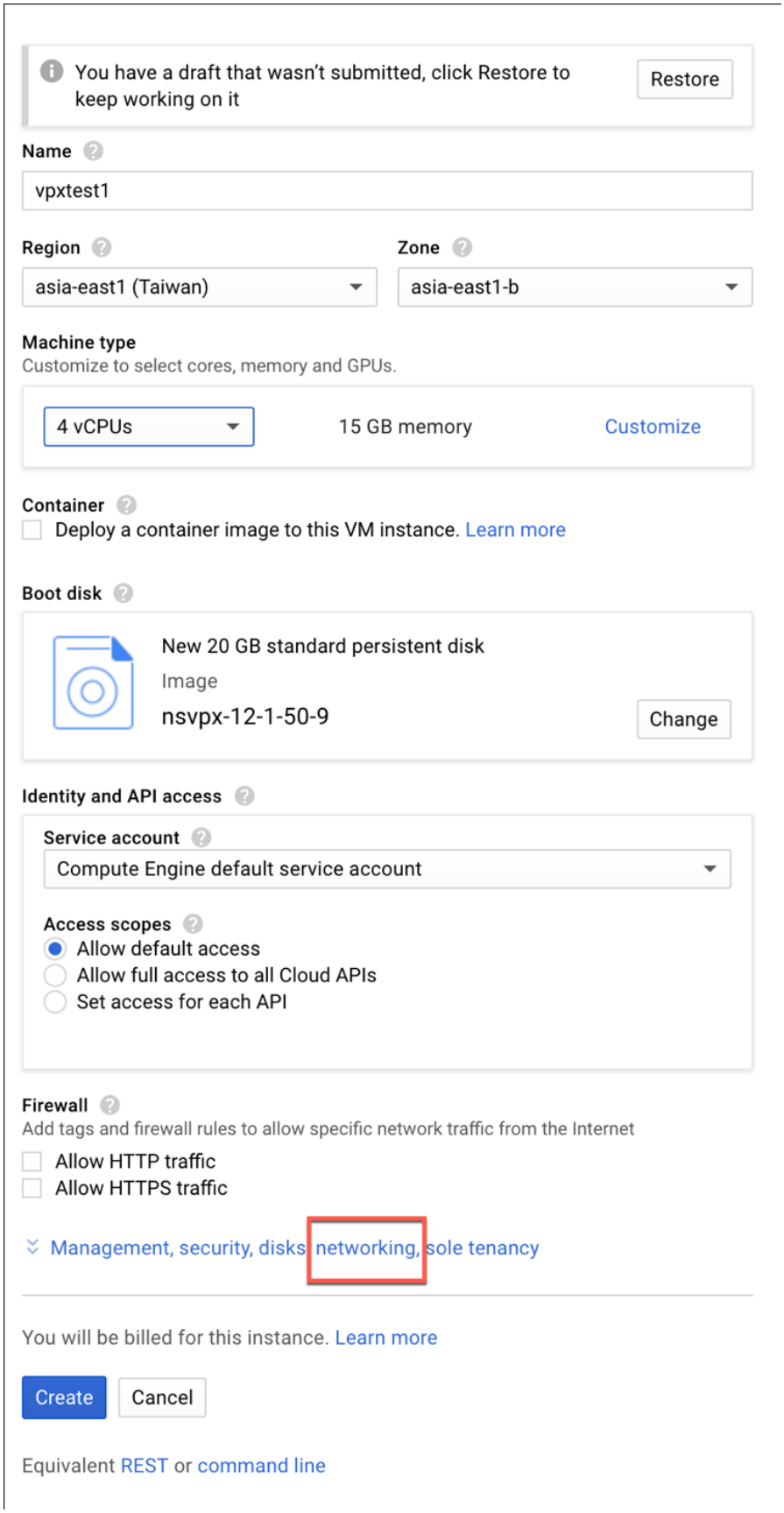
Étape 3. Créez l'instance VPX.

1. Connectez-vous à la console GCP.
2. Sous **Compute**, survolez Compute Engine et sélectionnez **Images**.
3. Sélectionnez l'image, puis cliquez sur **Créer une instance**.

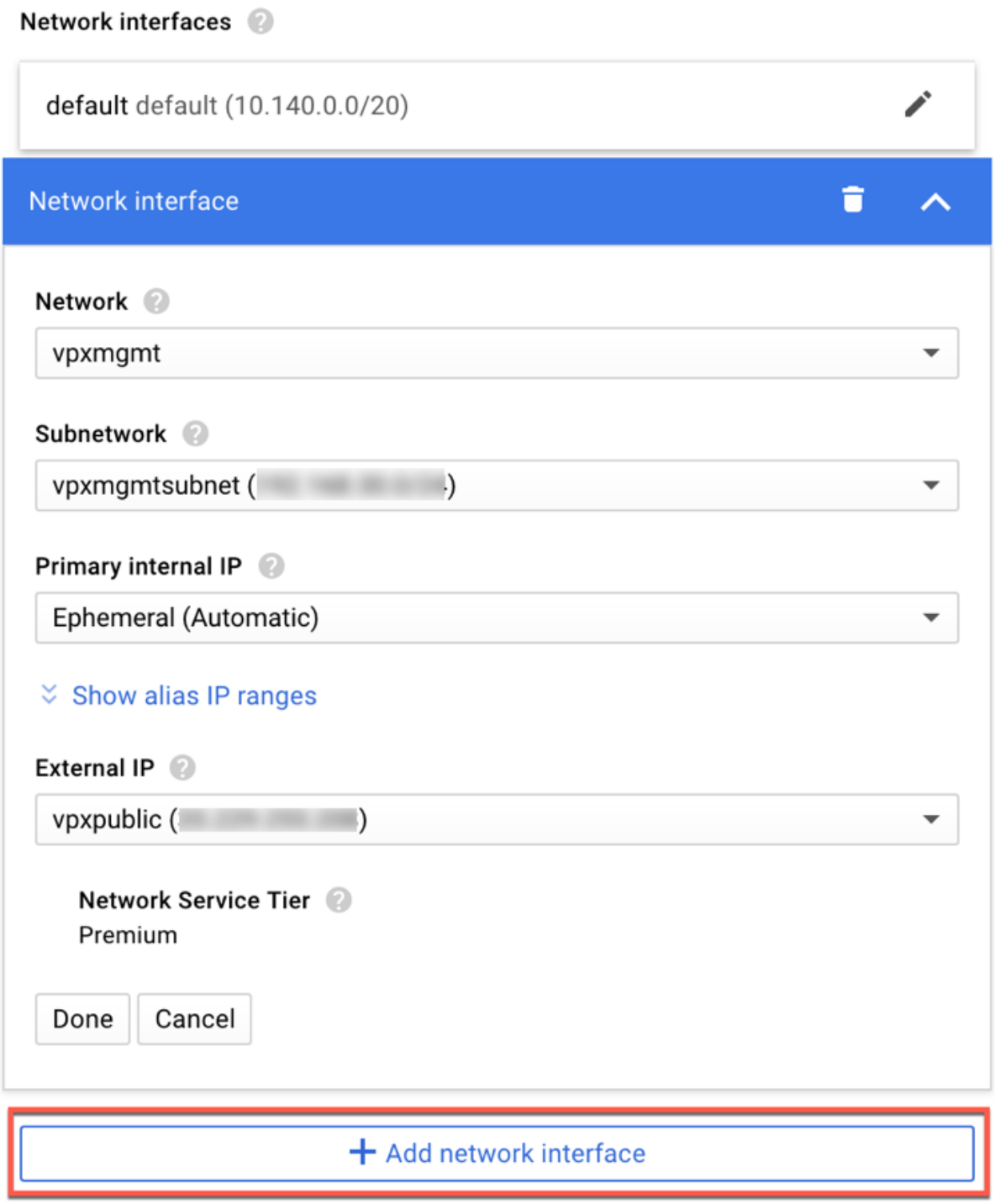


4. Sélectionnez une instance avec 4 processeurs virtuels pour prendre en charge plusieurs cartes réseau.
5. Cliquez sur l'option réseau dans Gestion, sécurité, disques, mise en réseau, location unique pour ajouter les cartes réseau supplémentaires.

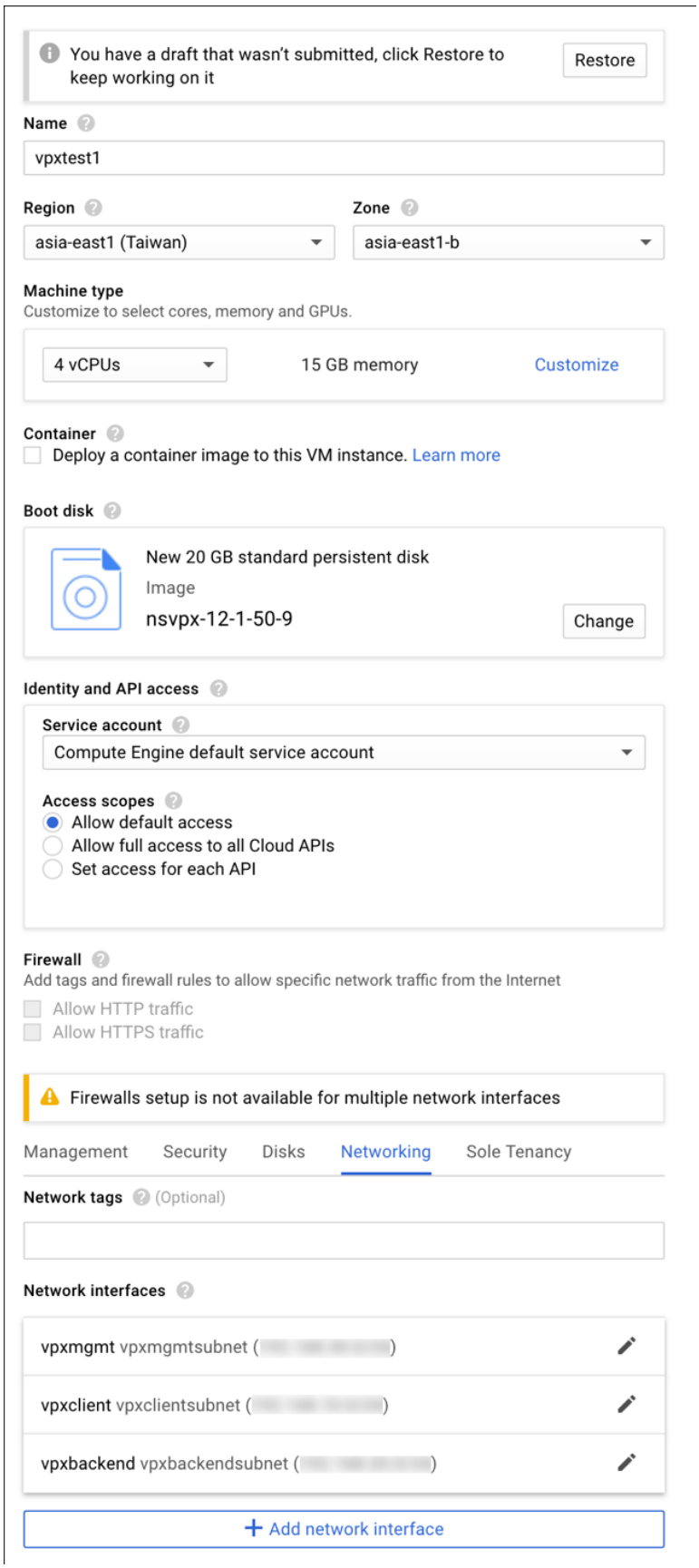
   Remarque : L'image de conteneur n'est pas prise en charge sur les instances VPX sur GCP.



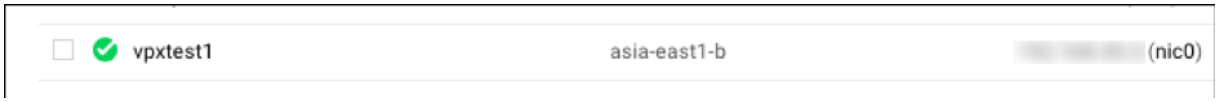
6. Sous **Interfaces réseau**, cliquez sur l'icône Modifier pour modifier la carte réseau par défaut. Cette carte réseau est la carte réseau de gestion.
7. Dans la fenêtre **Interfaces réseau**, sous **Réseau**, sélectionnez le réseau VPC que vous avez créé pour la carte réseau de gestion.
8. Pour la carte réseau de gestion, créez une adresse IP externe statique. Dans la liste IP externe, cliquez sur **Créer une adresse IP**.
9. Dans la fenêtre **Réserver une nouvelle adresse IP statique**, ajoutez un nom et une description, puis cliquez sur **Réserver**.
10. Cliquez sur **Ajouter une interface réseau** pour créer des cartes réseau pour un trafic client et côté serveur.



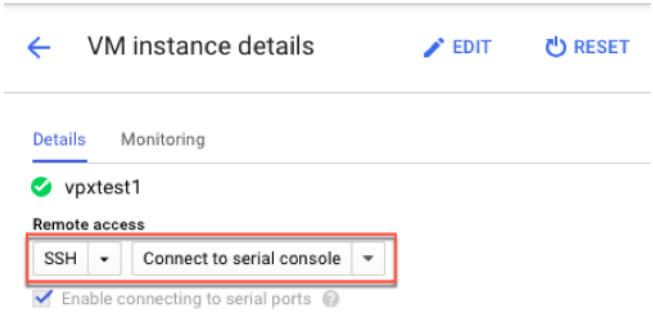
Une fois que vous avez créé toutes les cartes réseau, cliquez sur **Créer** pour créer l'instance VPX.



L'instance apparaît sous **Instances de VM**.

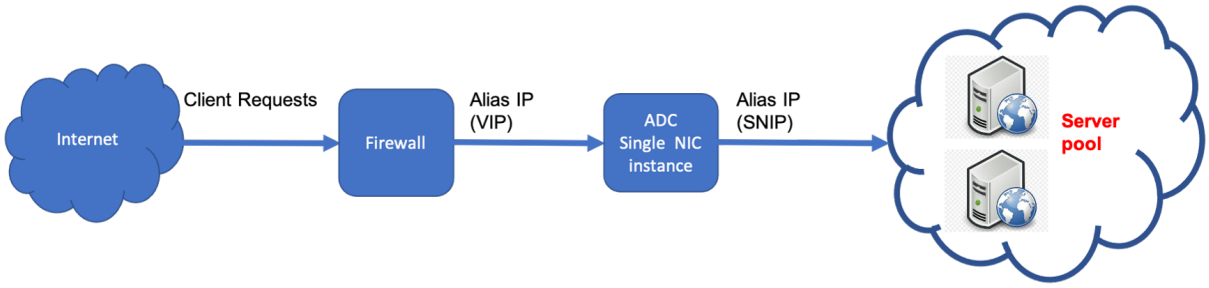


Utilisez le SSH GCP ou la console série pour configurer et gérer l'instance VPX.



Scénario : déployer une instance VPX autonome à carte réseau unique

Ce scénario illustre comment déployer une instance autonome Citrix VPX avec une carte réseau unique dans GCP. Les adresses IP de l'alias sont utilisées pour réaliser ce déploiement.



Créez une carte réseau unique (NIC0) pour répondre aux objectifs suivants :

- Gérez le trafic de gestion (Citrix ADC IP) dans le réseau de gestion.
- Gérez le trafic côté client (VIP) dans le réseau client.
- Communiquez avec les serveurs dorsaux (SNIP) du réseau de serveurs back-end.

Configurez les routes de communication requises entre les éléments suivants :

- Instance et serveurs back-end.
- Instance et les hôtes externes sur Internet public.

Résumé des étapes de déploiement

1. Créez un réseau VPC pour NIC0.
2. Créez des règles de pare-feu pour les ports 22, 80 et 443.

3. Créez une instance avec une seule carte réseau.
4. Ajoutez des adresses IP alias à VPX.
5. Ajoutez VIP et SNIP sur VPX.
6. Ajoutez un serveur virtuel d'équilibrage de charge.
7. Ajoutez un service ou un groupe de services sur l'instance.
8. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur l'instance.

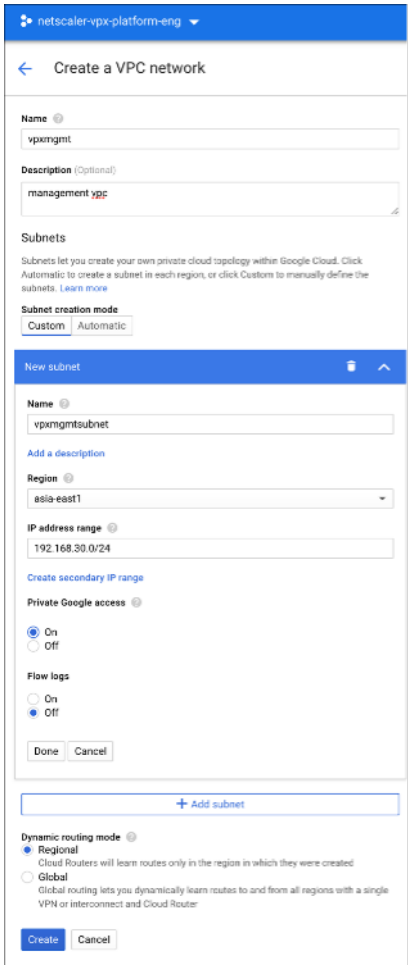
> **Remarque** :
>
> Créez une instance dans la même région que celle où vous avez créé les réseaux VPC.

Étape 1. Créez un réseau VPC.

Créez un réseau VPC à associer à NIC0.

Pour créer un réseau VPC, procédez comme suit :

1. Connectez-vous à la **console GCP > Réseau > Réseau VPC > Créer un réseau VPC**
2. Remplissez les champs requis, puis cliquez sur **Créer**.



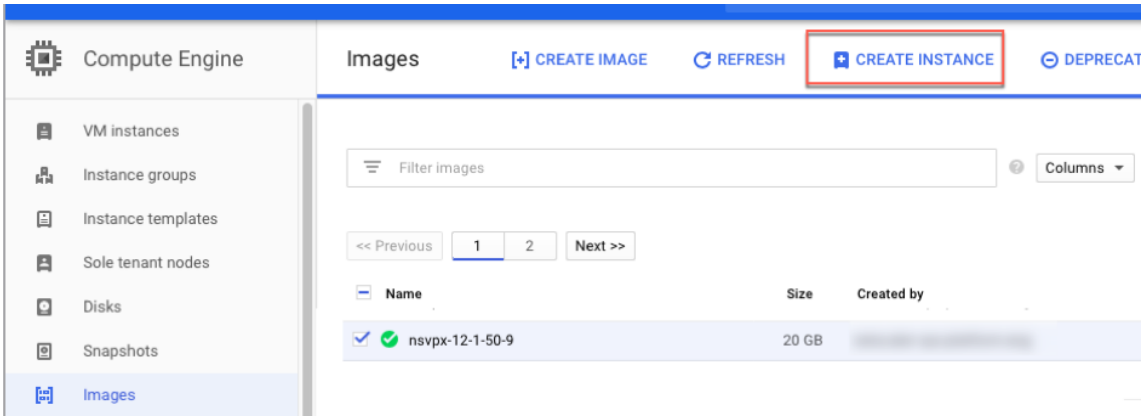
Étape 2. Créez des règles de pare-feu pour les ports 22, 80 et 443.

Créez des règles pour SSH (port 22), HTTP (port 80) et HTTPS (port 443) pour le réseau VPC. Pour plus d'informations sur les règles de pare-feu, voir Vue d' ensemble des règles de pare-feu.

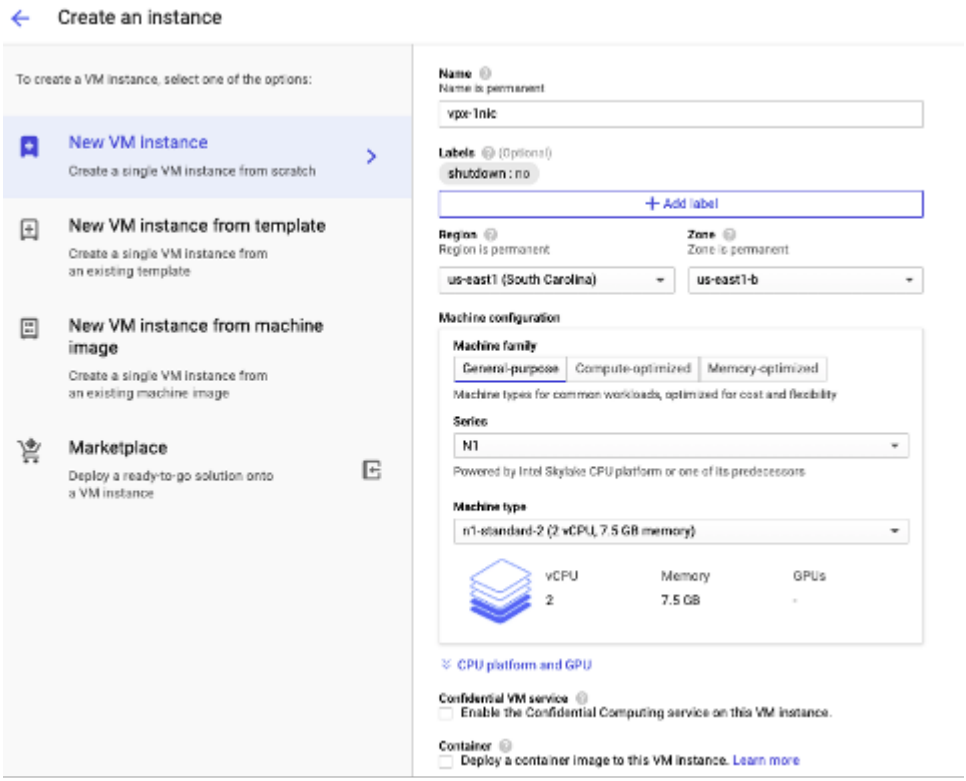
Étape 3. Créez une instance avec une carte réseau unique.

Pour créer une instance avec une carte réseau unique, procédez comme suit :

1. Connectez-vous à la **console GCP**.
2. Sous **Compute**, survolez **Compute Engine**et sélectionnez **Images**.
3. Sélectionnez l'image, puis cliquez sur **Créer une instance**.



4. Sélectionnez un type d'instance avec deux processeurs virtuels (configuration minimale requise pour ADC).



5. Cliquez sur l'onglet **Mise en réseau** dans la fenêtre **Gestion, sécurité, disques, réseau** .
6. Sous **Interfaces réseau**, cliquez sur l'icône **Modifier** pour modifier la carte réseau par défaut.
7. Dans la fenêtre **Interfaces réseau**, sous **Réseau**, sélectionnez le réseau VPC que vous avez créé.
8. Vous pouvez créer une adresse IP externe statique. Sous **Adresses IP externes**, cliquez sur **Créer une adresse IP**.
9. Dans la fenêtre **Réserver une adresse statique**, ajoutez un nom et une description, puis cliquez sur **Réserver**.

10. Cliquez sur **Créer** pour créer l'instance VPX.
    La nouvelle instance apparaît sous Instances de VM.

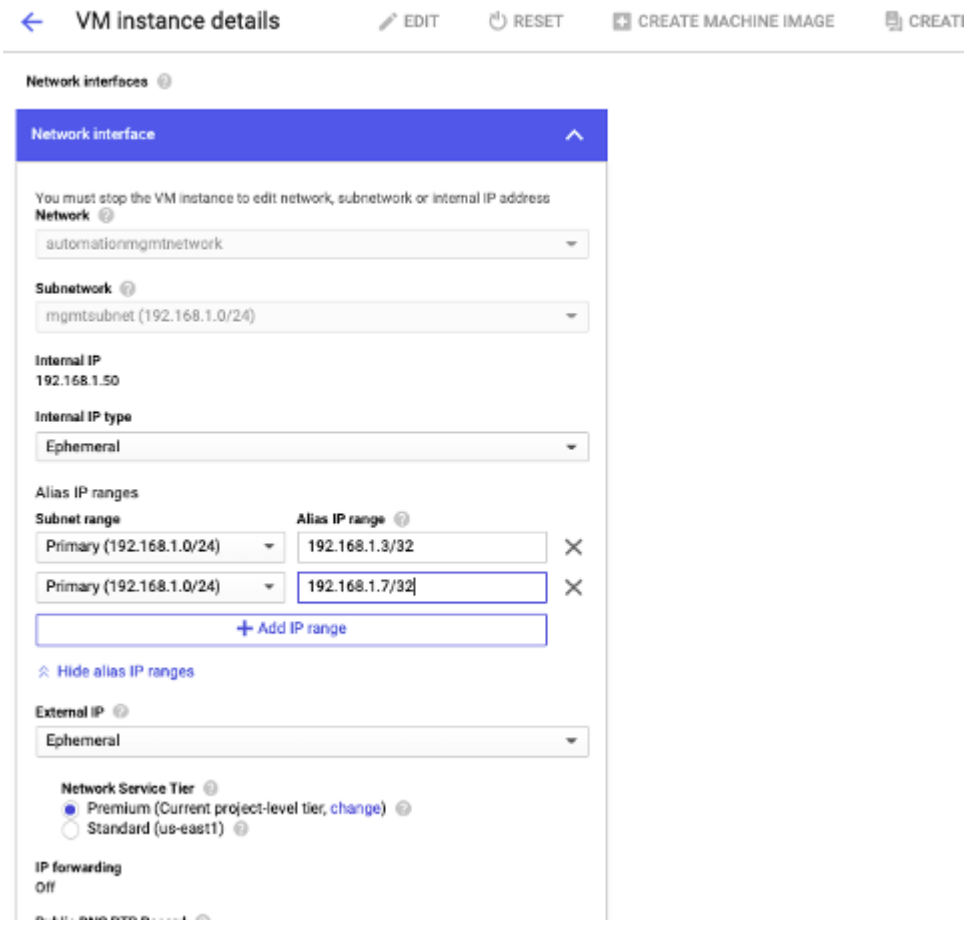
Étape 4. Ajoutez des adresses IP alias à l'instance VPX.

Attribuez deux adresses IP alias à l'instance VPX à utiliser comme adresses VIP et SNIP.

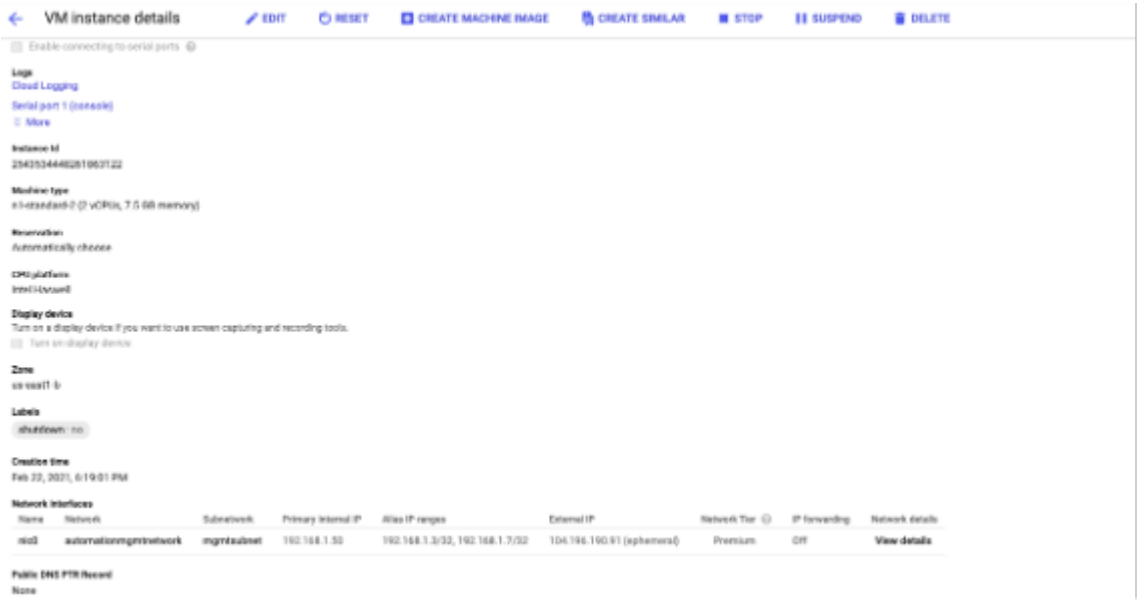
> **Remarque :**
>
> N'utilisez pas l'adresse IP interne principale de l'instance VPX pour configurer le VIP ou le SNIP.

Pour créer une adresse IP d'alias, procédez comme suit :

1. Accédez à l'instance de machine virtuelle et cliquez sur **Modifier**.
2. Dans la fenêtre **Interface réseau**, modifiez l'interface NIC0.
3. Dans le champ **Plage IP Alias**, entrez les adresses IP de l'alias.



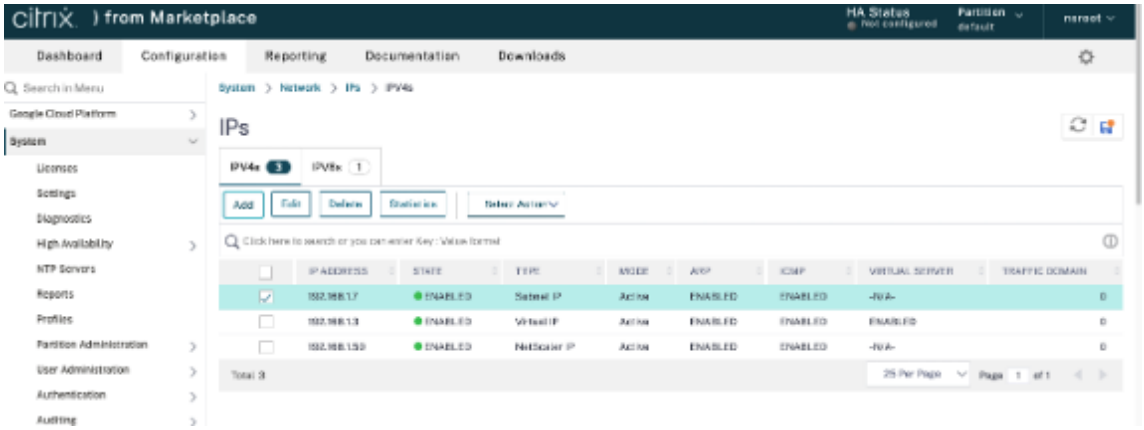
4. Cliquez sur **Terminé**, puis sur **Enregistrer**.
5. Vérifiez les adresses IP de l'alias dans la page de **détails de l'instance de machine virtuelle** .



Étape 5. Ajoutez VIP et SNIP sur l'instance VPX.

Sur l'instance VPX, ajoutez l'adresse IP de l'alias client et l'adresse IP de l'alias du serveur.

1. Sur l'interface graphique Citrix ADC, accédez à **Système > Réseau > IP > IPv4**, puis cliquez sur **Ajouter**.

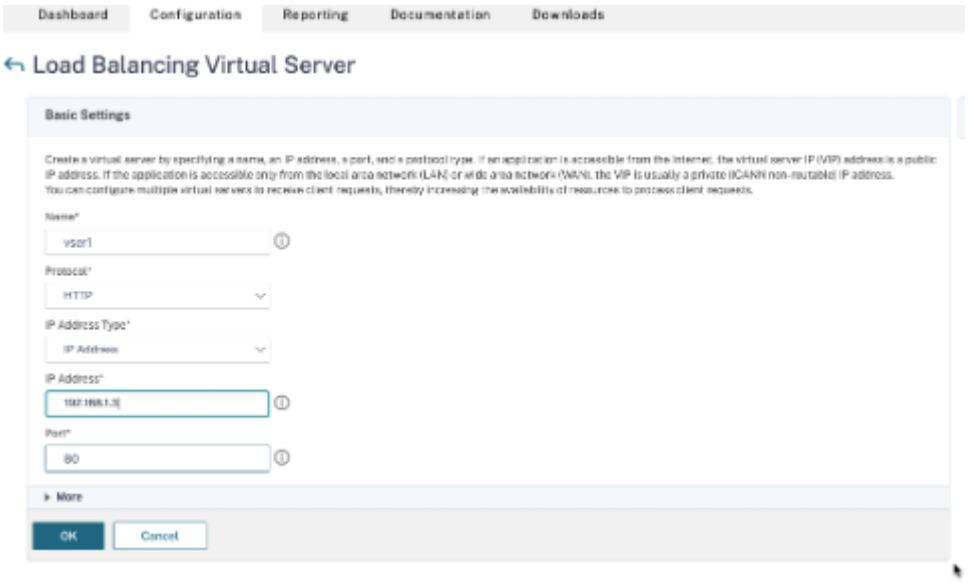


2. Pour créer une adresse IP (VIP) alias client :
   - Saisissez l'adresse IP et le masque de réseau client-alias configurés pour le sous-réseau VPC dans l'instance de machine virtuelle.
   - Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
   - Cliquez sur **Créer**.
3. Pour créer une adresse IP d'alias de serveur (SNIP) :
   - Saisissez l'adresse IP et le masque de réseau alias de serveur configurés pour le sous-réseau VPC dans l'instance de machine virtuelle.
   - Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.

- Cliquez sur **Créer**.

Étape 6. Ajoutez un serveur virtuel d'équilibrage de charge.

1. Sur l'interface graphique Citrix ADC, accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis cliquez sur **Ajouter**.
2. Ajoutez les valeurs requises pour Nom, Protocole, Type d'adresse IP (adresse IP), Adresse IP (adresse IP de l'alias client) et Port.
3. Cliquez sur **OK** pour créer le serveur virtuel d'équilibrage de charge.



Étape 7. Ajoutez un service ou un groupe de services sur l'instance VPX.

1. Depuis l'interface graphique Citrix ADC, accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services**, puis cliquez sur **Ajouter**.
2. Ajoutez les valeurs requises pour le nom du service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 8. Liez le groupe de services/services au serveur virtuel d'équilibrage de charge sur l'instance.

1. Depuis l'interface graphique, accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 6**, puis cliquez sur **Modifier**.
3. Dans la fenêtre **Groupes de services et de services**, cliquez sur **Liaison de service Virtual Server sans équilibrage de charge**.
4. Sélectionnez le service configuré à l' **étape 7**, puis cliquez sur **Lier**.

Points à noter après avoir déployé l'instance VPX sur GCP

- Connectez-vous au VPX avec le nom d'utilisateur `nsroot` et l'ID d'instance comme mot de passe. À l'invite, modifiez le mot de passe et enregistrez la configuration.
- Pour collecter un ensemble de support technique, exécutez la commande `shell /netscaler/showtech_cloud.pl` plutôt que la commande habituelle `show techsupport`.
- Après avoir supprimé une machine virtuelle Citrix ADC de la console GCP, supprimez également l'instance cible interne Citrix ADC associée. Pour ce faire, accédez à gcloud CLI et tapez la commande suivante :

```
1 gcloud compute -q  target-instances delete <instance-name>-
     adcinternal --zone <zone>
2 <!--NeedCopy-->
```

> Remarque : `<instance-name>-adcinternal` est le nom de l'instance cible qui doit être supprimée.

Licences Citrix ADC VPX

Une instance Citrix ADC VPX sur GCP nécessite une licence. Les options de licence suivantes sont disponibles pour les instances Citrix ADC VPX exécutées sur GCP.

- **Licences basées sur un abonnement** : les appliances Citrix ADC VPX sont disponibles en tant qu'instances payantes sur le marché GCP. Les licences par abonnement sont une option de paiement à l'utilisation. Les utilisateurs sont facturés à l'heure. Les modèles VPX et les éditions de licences suivants sont disponibles sur le marché GCP.

  |Modèle VPX|Éditions de licences|
  |—|—|
  |VPX10| Standard, Avancé, Premium|
  | |

- **Apportez votre propre licence (BYOL)** : si vous apportez votre propre licence (BYOL), consultez le Guide de licences VPX à l'adresse http://support.citrix.com/article/CTX122426. Vous devez :
  - Utilisez le portail de licences sur le site Web Citrix pour générer une licence valide.
  - Télécharger la licence sur l'instance.
- Licences d'**enregistrement et de départ Citrix ADC VPX : pour plus d'informations, consultez Licences**d' enregistrement et de départ Citrix ADC VPX.

VPX Express pour les déploiements sur site et dans le cloud ne nécessite pas de fichier de licence. Pour plus d'informations sur Citrix ADC VPX Express, consultez la section « Licence Citrix ADC VPX Express » de la présentation des licences Citrix ADC.

Modèles GDM pour déployer une instance Citrix ADC VPX

Vous pouvez utiliser un modèle Citrix ADC VPX Google Deployment Manager (GDM) pour déployer une instance VPX sur GCP. Pour plus de détails, consultez Modèles Citrix ADC GDM.

Images du marché Citrix ADC

Vous pouvez utiliser les images des modèles GDM pour faire apparaître l'appliance Citrix ADC.

Le tableau suivant répertorie les images disponibles sur le marché GCP.

Libérer	Nom de l'image	Emplacement de l'image
13.0	citrix-adc-vpx-1000-advanced-13-0-61-48	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-advanced-13-0-61-48
13.0	citrix-adc-vpx-1000-advanced-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-advanced-13-0-latest
13.0	citrix-adc-vpx-1000-premium-13-0-61-48	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-premium-13-0-61-48
13.0	citrix-adc-vpx-1000-premium-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-premium-13-0-latest
13.0	citrix-adc-vpx-1000-standard-13-0-61-48	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-standard-13-0-61-48
13.0	citrix-adc-vpx-1000-standard-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-standard-13-0-latest

Libérer	Nom de l'image	Emplacement de l'image
13.0	citrix-adc-vpx-5000-enterprise-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-enterprise-13-0-58-32
13.0	citrix-adc-vpx-5000-enterprise-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-enterprise-13-0-latest
13.0	citrix-adc-vpx-5000-platinum-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-13-0-58-32
13.0	citrix-adc-vpx-5000-platinum-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-13-0-latest
13.0	citrix-adc-vpx-5000-standard-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-standard-13-0–58-32
13.0	citrix-adc-vpx-5000-standard-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-standard-13-0-latest
13.0	citrix-adc-vpx-3000-enterprise-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-enterprise-13-0-58-32
13.0	citrix-adc-vpx-3000-enterprise-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-enterprise-13-0-latest
13.0	citrix-adc-vpx-3000-platinum-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-platinum-13-0-58-32

Libérer	Nom de l'image	Emplacement de l'image
13.0	citrix-adc-vpx-3000-platinum-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-platinum-13-0-latest
13.0	citrix-adc-vpx-3000-standard-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-standard-13-0–58-32
13.0	citrix-adc-vpx-3000-standard-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-standard-13-0-latest
13.0	citrix-adc-vpx-200-enterprise-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-13-0-58-32
13.0	citrix-adc-vpx-200-enterprise-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-13-0-latest
13.0	citrix-adc-vpx-200-platinum-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-200-platinum-13-0-58-32
13.0	citrix-adc-vpx-200-platinum-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-200-platinum-13-0-latest
13.0	citrix-adc-vpx-200-standard-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-200-standard-13-0–58-32
13.0	citrix-adc-vpx-200-standard-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-200-standard-13-0-latest

Libérer	Nom de l'image	Emplacement de l'image
13.0	citrix-adc-vpx-10-enterprise-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-10-enterprise-13-0-58-32
13.0	citrix-adc-vpx-10-enterprise-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-10-enterprise-13-0-latest
13.0	citrix-adc-vpx-10-platinum-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-10-platinum-13-0-58-32
13.0	citrix-adc-vpx-10-platinum-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-10-platinum-13-0-latest
13.0	citrix-adc-vpx-10-standard-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-10-standard-13-0-58-32
13.0	citrix-adc-vpx-10-standard-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-10-standard-13-0-latest
13.0	citrix-adc-vpx-express-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-express-13-0-58-32
13.0	citrix-adc-vpx-express-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-express-13-0-latest
13.0	citrix-adc-vpx-byol-13-0-58-32	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-13-0-58-32

Libérer	Nom de l'image	Emplacement de l'image
13.0	citrix-adc-vpx-byol-13-0-latest	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-13-0-latest

Ressources

- Création d'instances avec plusieurs interfaces réseau
- Création et démarrage d'une instance de machine virtuelle

Informations connexes

- Déployer une paire haute disponibilité VPX sur Google Cloud Platform

Déployer une paire haute disponibilité VPX sur Google Cloud Platform

August 20, 2021

Vous pouvez configurer deux instances Citrix ADC VPX sur Google Cloud Platform (GCP) en tant que paire actif-passif haute disponibilité (HA). Lorsque vous configurez une instance en tant que nœud principal et l'autre en tant que nœud secondaire, le nœud principal accepte les connexions et gère les serveurs. Le nœud secondaire surveille le principal. Si pour une raison quelconque, si le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

Pour plus d'informations sur HA, voir Haute disponibilité.

Les nœuds doivent se trouver dans la même région ; cependant, ils peuvent se trouver soit dans la même zone, soit dans des zones différentes. Pour plus d'informations, voir Régions et zones.

Chaque instance VPX nécessite au moins trois sous-réseaux IP (réseaux Google VPC) :

- Un sous-réseau de gestion
- Un sous-réseau orienté client (VIP)
- Un sous-réseau orienté vers le back-end (SNIP, MIP, etc.)

Citrix recommande trois interfaces réseau pour une instance VPX standard.

Vous pouvez déployer une paire VPX haute disponibilité en utilisant les méthodes suivantes :

- Utilisation d'une adresse IP statique externe
- Utilisation d'une adresse IP privée

Modèles GDM pour déployer une paire haute disponibilité VPX sur GCP

Vous pouvez utiliser un modèle Citrix ADC Google Deployment Manager (GDM) pour déployer une paire VPX haute disponibilité sur GCP. Pour plus de détails, consultez Modèles Citrix ADC GDM.

Prise en charge des règles de transfert pour la paire haute disponibilité VPX sur GCP

Vous pouvez déployer une paire VPX haute disponibilité sur le GCP à l'aide de règles de transfert.

Pour plus d'informations sur les règles de transfert, voir Vue d'ensemble des règles de transfert.

Conditions préalables

- Les règles de transfert doivent se trouver dans la même région que les instances VPX.
- Les instances cibles doivent se trouver dans la même zone que l'instance VPX.
- Le nombre d'instances cibles pour les nœuds principal et secondaire doit correspondre.

Exemple :

Vous avez une paire haute disponibilité dans la `us-east1` région avec VPX principal dans la `us-east1-b` zone et VPX secondaire dans la `us-east1-c` zone. Une règle de transfert est configurée pour le VPX principal avec l'instance cible dans la `us-east1-b` zone. Configurez une instance cible pour VPX secondaire dans la `us-east1-c` zone pour mettre à jour la règle de transfert lors du basculement.

Limitations

Seules les règles de transfert configurées avec des instances cibles en back-end sont prises en charge dans le déploiement haute disponibilité VPX.

Déployer une paire haute disponibilité VPX avec une adresse IP statique externe sur Google Cloud Platform

October 5, 2021

Vous pouvez déployer une paire haute disponibilité VPX sur GCP à l'aide d'une adresse IP statique externe. L'adresse IP du client du nœud principal doit être liée à une adresse IP statique externe. Lors du basculement, l'adresse IP statique externe est déplacée vers le nœud secondaire pour que le trafic reprenne.

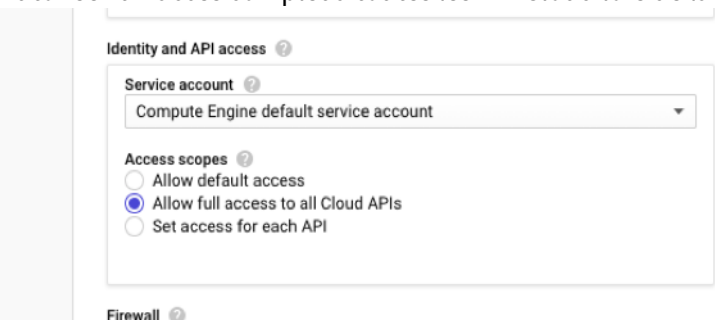
Une adresse IP externe statique est une adresse IP externe qui est réservée à votre projet jusqu'à ce que vous décidiez de la publier. Si vous utilisez une adresse IP pour accéder à un service, vous pouvez

réserver cette adresse IP afin que seul votre projet puisse l'utiliser. Pour plus d'informations, voir Réserver une adresse IP externe statique.

Pour plus d'informations sur HA, voir Haute disponibilité.

Avant de commencer

- Lisez la section Limitation, configuration matérielle requise, Points à noter mentionnés dans Déployer une instance Citrix ADC VPX sur Google Cloud Platform. Ces informations s'appliquent également aux déploiements HA.
- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Autorisez un accès complet à toutes les API Cloud lors de la création des instances.



- Assurez-vous que le rôle IAM associé à votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.addresses.use",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata"
"compute.instances.addAccessConfig",
"compute.instances.deleteAccessConfig",
"compute.instances.get",
"Compute.instances.list",
"compute.networks.useExternalIp",
"compute.subnetworks.useExternalIp",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
]
<!--NeedCopy-->
```


- Si vous avez configuré des adresses IP d'alias sur une interface autre que l'interface de gestion, assurez-vous que votre compte de service GCP dispose des autorisations IAM supplémentaires suivantes :

```
"compute.instances.updateNetworkInterface"
<!--NeedCopy-->
```

- Si vous avez configuré des règles de transfert GCP sur le nœud principal, lisez les limitations et exigences mentionnées dans Prise en charge des règles de transfert pour la paire haute disponibilité VPX sur GCP pour les mettre à jour vers le nouveau serveur principal lors du basculement.

Comment déployer une paire VPX HA sur Google Cloud Platform

Voici un résumé des étapes de déploiement HA :

1. Créez des réseaux VPC dans la même région. Par exemple, Asie-Est.
2. Créez deux instances VPX (nœuds principal et secondaire) sur la même région. Ils peuvent se trouver dans la même zone ou dans des zones différentes. Par exemple, l'Asie orientale 1a et l'Asie orientale Ib.
3. Configurez les paramètres HA sur les deux instances à l'aide de l'interface utilisateur graphique Citrix ADC ou des commandes CLI ADC.

Étape 1. Créer des réseaux VPC

Créez des réseaux VPC en fonction de vos besoins. Citrix vous recommande de créer trois réseaux VPC à associer à une carte réseau de gestion, une carte réseau client et une carte réseau de serveur.

Pour créer un réseau VPC, procédez comme suit :

1. Ouvrez une session sur la **console Google > Mise en réseau > Réseau VPC > Créer un réseau VPC**.
2. Remplissez les champs requis, puis cliquez sur **Créer**.

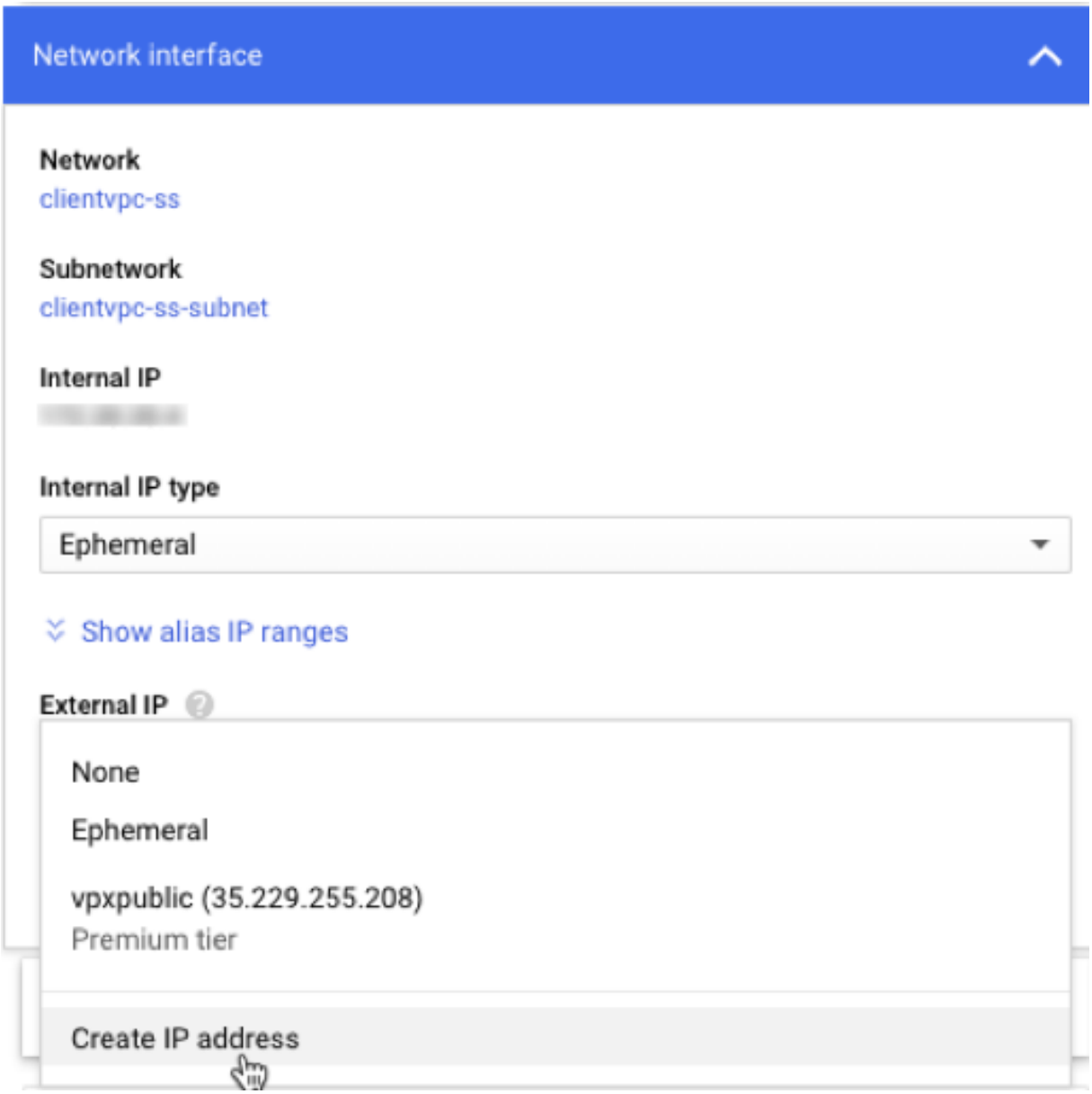
Pour plus d'informations, consultez la section **Créer des réseaux VPC** dans Déployer une instance Citrix ADC VPX sur Google Cloud Platform.

Étape 2. Créer deux instances VPX

Créez deux instances VPX en suivant les étapes indiquées dans Scénario : déployer une instance VPX autonome multi-cartes réseau et multi-IP.

> **Important**
>
> Attribuez une adresse IP externe statique à l'adresse IP du client (VIP) du nœud principal. Vous

> pouvez utiliser une adresse IP réservée existante ou en créer une nouvelle. Pour créer une adresse IP externe statique, accédez à **Interface réseau > IP externe**, cliquez sur **Créer une adresse IP**.



Après le basculement, lorsque l'ancien principal devient le nouveau secondaire, l'adresse IP externe statique se déplace de l'ancien principal et est attachée au nouveau principal. Pour plus d'informations, consultez le document Google Cloud Reserving a Static External IP Address.

Une fois que vous avez configuré les instances VPX, vous pouvez configurer les adresses VIP et SNIP. Pour plus d'informations, consultez Configuration des adresses IP appartenant à Citrix ADC.

Étape 3. Configurer la haute disponibilité

Après avoir créé les instances sur Google Cloud Platform, vous pouvez configurer HA à l'aide de l'interface graphique Citrix ADC pour CLI.

Configurer HA à l'aide de l'interface graphique

Étape 1. Configurez la haute disponibilité en mode INC sur les deux instances.

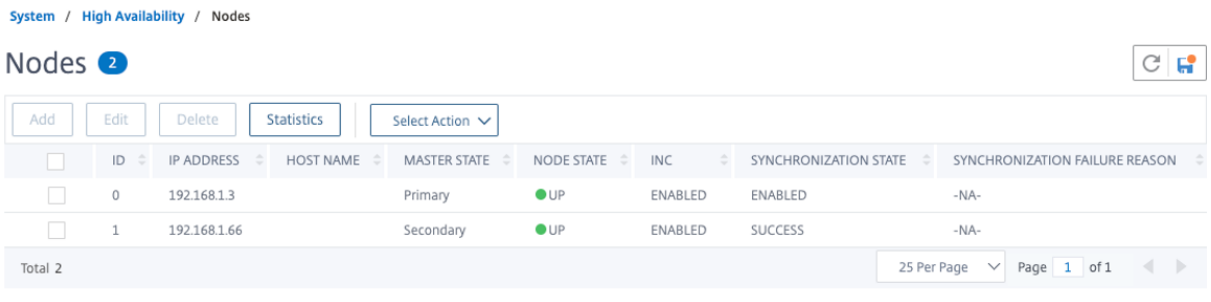
Sur le **nœud principal**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.

Sur le **nœud secondaire**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud principal.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.

Avant d'aller plus loin, assurez-vous que l'état de synchronisation du nœud secondaire s'affiche comme **SUCCÈS** dans la page **Nœuds** .



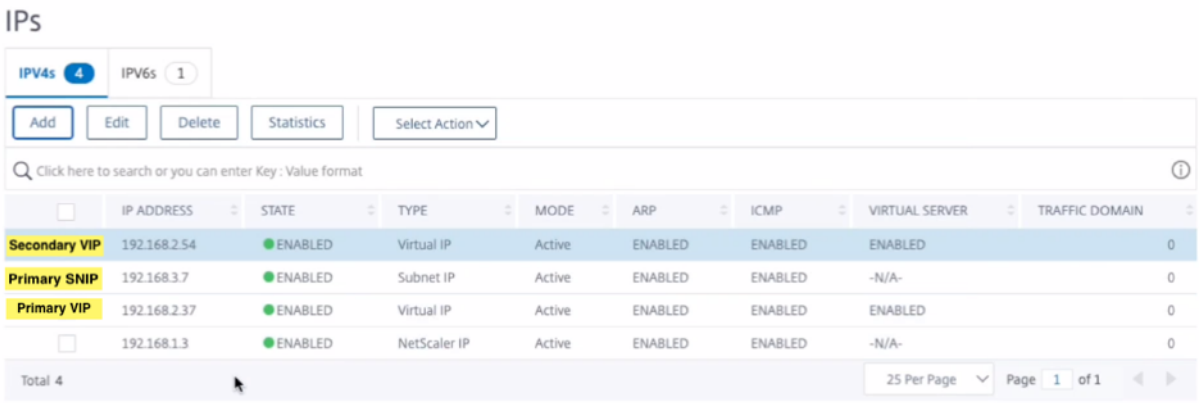
> **Remarque**
>
> Maintenant, le nœud secondaire a les mêmes informations d'identification d'ouverture de ses-

> sion que le nœud principal.

Étape 2. Ajoutez une adresse IP virtuelle et une adresse IP de sous-réseau sur les deux nœuds.

Sur le **nœud principal**, effectuez les opérations suivantes :

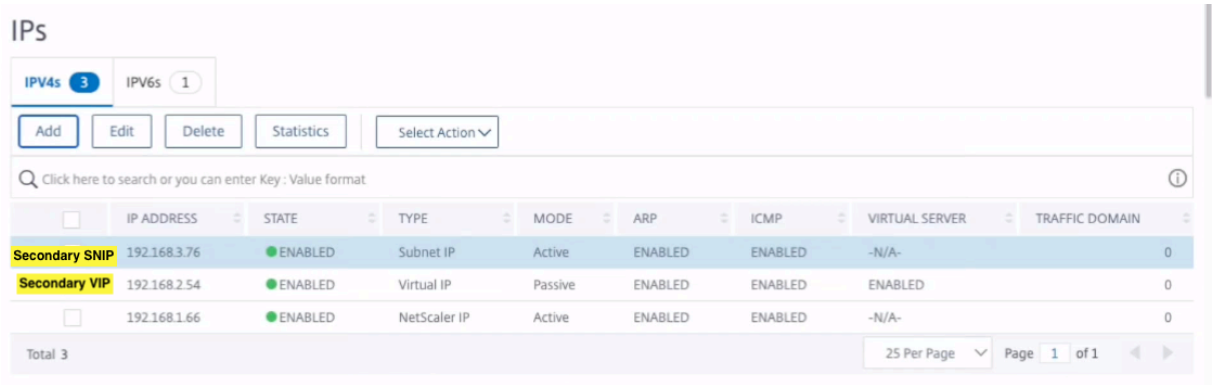
1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Ajoutez une adresse VIP principale en procédant comme suit :
   a) Entrez l'adresse IP interne de l'interface orientée client de l'instance principale et du masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
   b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
   c) Cliquez sur **Create**.
3. Ajoutez une adresse SNIP principale en procédant comme suit :
   a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance principale et du masque de réseau configurés pour le sous-réseau du serveur dans l'instance principale.
   b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
   c) Cliquez sur **Create**.
4. Ajoutez une adresse VIP secondaire en procédant comme suit :
   a) Entrez l'adresse IP interne de l'interface orientée client de l'instance secondaire et du masque réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
   b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
   c) Cliquez sur **Create**.



Sur le **nœud secondaire**, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Ajoutez une adresse VIP secondaire en procédant comme suit :
   a) Entrez l'adresse IP interne de l'interface orientée client de l'instance secondaire et du masque réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
   b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
3. Ajoutez une adresse SNIP secondaire en procédant comme suit :

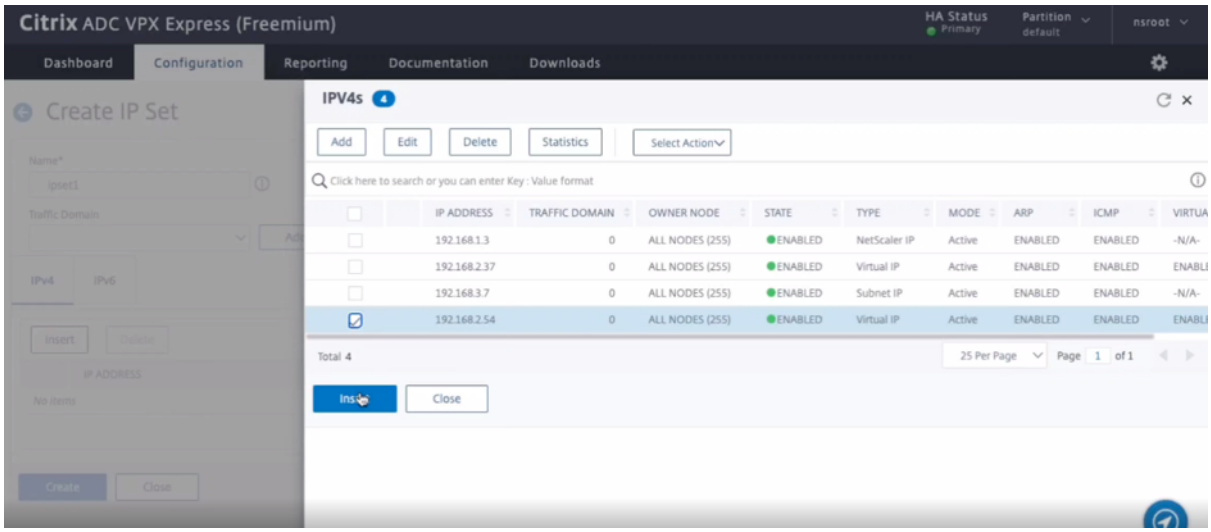
a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance secondaire et du masque de réseau configurés pour le sous-réseau du serveur dans l'instance secondaire.
b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
c) Cliquez sur **Create**.



Étape 3. Ajoutez un ensemble d'adresses IP et liez le jeu d'adresses IP au VIP secondaire sur les deux instances.

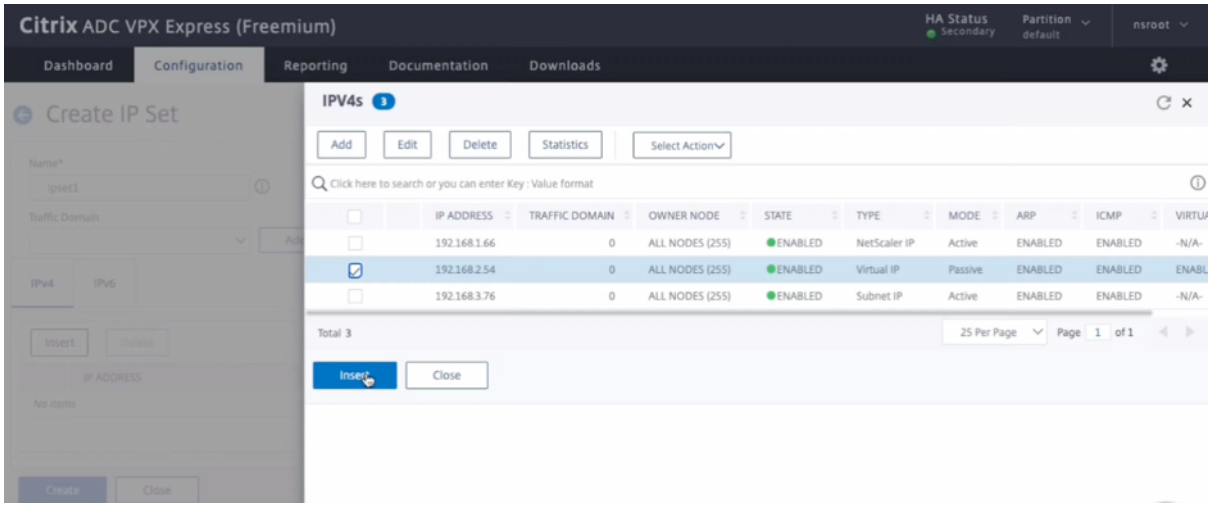
Sur le **nœud principal**, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > Jeux d'adresses IP > Ajouter**.
2. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
3. Sur la page **IPv4**, sélectionnez l'IP virtuelle (VIP secondaire) et cliquez sur **Insérer**.
4. Cliquez sur **Créer** pour créer le jeu d'adresses IP.



Sur le **nœud secondaire**, effectuez les opérations suivantes :

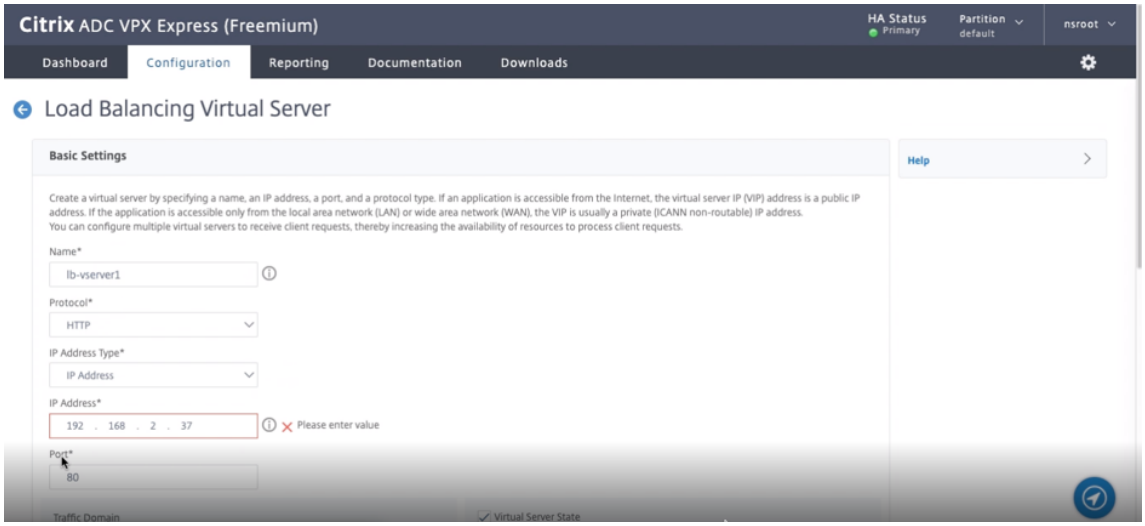
1. Accédez à **Système > Réseau > Jeux d'adresses IP > Ajouter**.
2. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
3. Sur la page **IPv4**, sélectionnez l'IP virtuelle (VIP secondaire) et cliquez sur **Insérer**.
4. Cliquez sur **Créer** pour créer le jeu d'adresses IP.



> **Remarque**
>
> Le nom du jeu d'adresses IP doit être identique sur les deux instances.

Étape 4. Ajoutez un serveur virtuel d'équilibrage de charge sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.
2. Ajoutez les valeurs requises pour le nom, le protocole, le type d'adresse IP (adresse IP), l'adresse IP (VIP principale) et le port.



3. Cliquez sur **Plus**. Accédez à **Paramètres du jeu d'adresses IP de plage IP**, sélectionnez **IPset** dans le menu déroulant et indiquez l'IPSet créé à l' **étape 3**.
4. Cliquez sur **OK** pour créer le serveur virtuel d'équilibrage de charge.

Étape 5. Ajoutez un service ou un groupe de services sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.

2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 6. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 4**, puis cliquez sur **Modifier**.
3. Dans l'onglet **Groupes de services et de services**, cliquez sur **Liaison de service Virtual Server sans équilibrage de charge**.
4. Sélectionnez le service configuré à l' **étape 5**, puis cliquez sur **Lier**.

Enregistrez la configuration. Après un basculement forcé, le secondaire devient le nouveau principal. L'adresse IP statique externe de l'ancienne VIP principale passe au nouveau VIP secondaire.

Configuration de la haute disponibilité à l'aide de l'interface

Étape 1. Configurez la haute disponibilité en mode INC dans les deux instances.

Sur le nœud principal, tapez la commande suivante.

```
add ha node 1 <sec_ip> -inc ENABLED
<!--NeedCopy-->
```

Sur le nœud secondaire, tapez la commande suivante.

```
add ha node 1 <prim_ip> -inc ENABLED
<!--NeedCopy-->
```

`sec_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud secondaire.

`prim_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud principal.

Étape 2. Ajoutez des IP virtuelles et des adresses IP de sous-réseau sur les deux nœuds.

Sur le nœud principal, tapez la commande suivante.

```
add ns ip <primary_vip> <subnet> -type VIP

add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <primary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

`primary_vip` fait référence à l'adresse IP interne de l'interface orientée client de l'instance principale.

`secondary_vip` fait référence à l'adresse IP interne de l'interface orientée client de l'instance secondaire.

`primary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance principale.

Sur le nœud secondaire, tapez la commande suivante.

```
1 add ns ip <secondary_vip> <subnet> -type VIP
2
3 add ns ip <secondary_snip> <subnet> -type SNIP
4 <!--NeedCopy-->
```

`secondary_vip` fait référence à l'adresse IP interne de l'interface orientée client de l'instance secondaire.

`secondary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance secondaire.

Étape 3. Ajoutez un ensemble d'adresses IP et liez le jeu d'adresses IP à une adresse VIP secondaire sur les deux instances.

Sur le nœud principal, tapez la commande suivante :

```
1 add ipset <ipsetname>
2 bind ipset <ipsetname> <secondary VIP>
3 <!--NeedCopy-->
```

Sur le nœud secondaire, tapez la commande suivante :

```
1 add ipset <ipsetname>
2 bind ipset <ipsetname> <secondary VIP>
3 <!--NeedCopy-->
```

> **Remarque**
>
> Le nom du jeu d'adresses IP doit être identique sur les deux instances.

Étape 4. Ajoutez un serveur virtuel sur l'instance principale.

Exécutez la commande suivante :

```
1 add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port
     > -ipset <ipset_name>
2 <!--NeedCopy-->
```

Étape 5. Ajoutez un service ou un groupe de services sur l'instance principale.

Exécutez la commande suivante :


```
add service <service_name> <service_ip_address> <protocol> <port>
<!--NeedCopy-->
```

Étape 6. Liez le groupe de services/services au serveur virtuel d'équilibrage de charge sur l'instance principale.

Exécutez la commande suivante :

```
bind <server_type> vserver <vserver_name> <service_name>
<!--NeedCopy-->
```

> *Remarque* :
>
> Pour enregistrer votre configuration, tapez la commande `save config`. Sinon, les configurations sont perdues après le redémarrage des instances.

Étape 7. Vérifiez la configuration.

Assurez-vous que l'adresse IP externe attachée à la carte réseau client principale se déplace vers la secondaire lors d'un basculement.

1. Effectuez une requête cURL à l'adresse IP externe et assurez-vous qu'elle est accessible.
2. Sur l'instance principale, effectuez un basculement :

   Depuis l'interface graphique, accédez à **Configuration > Système > Haute disponibilité > Action > Forcer le basculement**.

   À partir de l'interface de ligne de commande, tapez la commande suivante :

   ```
   force ha failover -f
   <!--NeedCopy-->
   ```

   Sur la console GCP, accédez à l'instance secondaire. L'adresse IP externe doit avoir été déplacée vers la carte réseau client de secondaire après basculement.
3. Émettez une requête cURL à l'adresse IP externe et assurez-vous qu'elle est à nouveau accessible.

Déployer une paire VPX haute disponibilité avec une adresse IP privée sur Google Cloud Platform

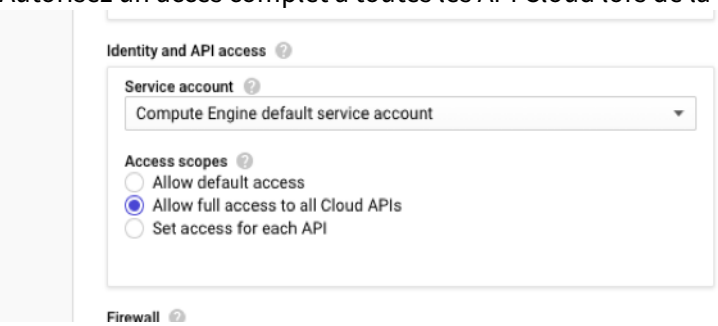
October 5, 2021

Vous pouvez déployer une paire VPX haute disponibilité sur GCP à l'aide d'une adresse IP privée. L'adresse IP du client (VIP) doit être configurée en tant qu'adresse IP alias sur le nœud principal. Lors du basculement, l'adresse IP du client est déplacée vers le nœud secondaire, pour que le trafic reprenne.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité.

Avant de commencer

- Lisez la section Limitation, configuration matérielle requise, Points à noter mentionnés dans Déployer une instance Citrix ADC VPX sur Google Cloud Platform. Ces informations s'appliquent également aux déploiements haute disponibilité.
- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Autorisez un accès complet à toutes les API Cloud lors de la création des instances.



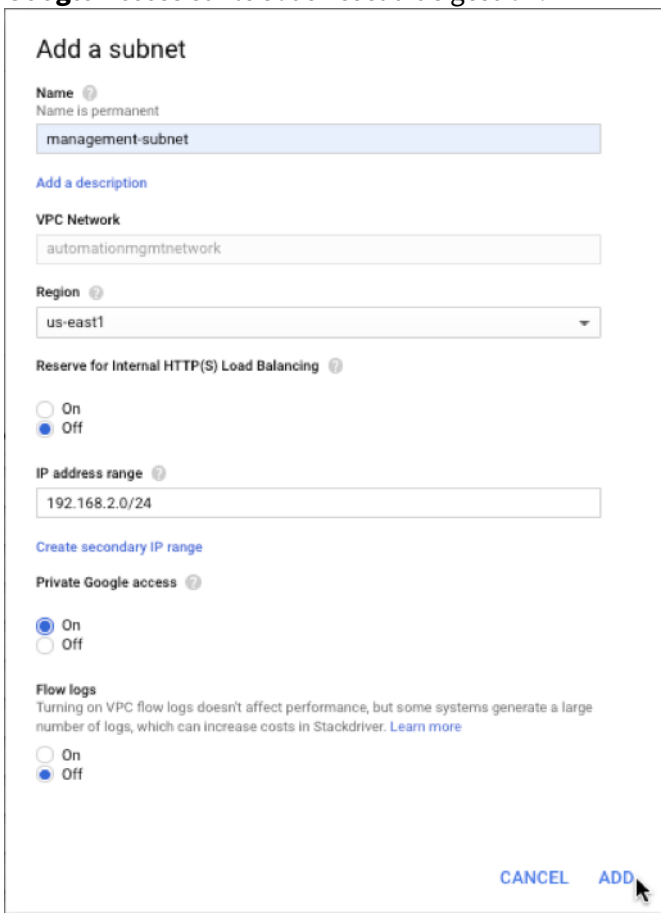
- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata",
"compute.instances.get",
"compute.instances.list",
"compute.instances.updateNetworkInterface",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
]
<!--NeedCopy-->
```

- Si vous avez configuré des adresses IP externes sur une interface autre que l'interface de gestion, assurez-vous que votre compte de service GCP dispose des autorisations IAM supplémentaires suivantes :


```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.addresses.use"
"compute.instances.addAccessConfig",
"compute.instances.deleteAccessConfig",
"compute.networks.useExternalIp",
"compute.subnetworks.useExternalIp",
]
<!--NeedCopy-->
```

- Si vos machines virtuelles ne disposent pas d'un accès Internet, vous devez activer **Private Google Access** sur le sous-réseau de gestion.



- Si vous avez configuré des règles de transfert GCP sur le nœud principal, lisez les limitations et exigences mentionnées dans Prise en charge des règles de transfert pour la paire haute disponibilité VPX sur GCP pour les mettre à jour vers le nouveau serveur principal lors du basculement.

Comment déployer une paire haute disponibilité VPX sur Google Cloud Platform

Voici un résumé des étapes de déploiement haute disponibilité :

1. Créez des réseaux VPC dans la même région. Par exemple, Asie-Est.
2. Créez deux instances VPX (nœuds principal et secondaire) sur la même région. Ils peuvent se trouver dans la même zone ou dans des zones différentes. Par exemple, l'Asie orientale 1a et l'Asie orientale Ib.
3. Configurez les paramètres de haute disponibilité sur les deux instances à l'aide de l'interface graphique Citrix ADC ou des commandes CLI ADC.

Étape 1. Créer des réseaux VPC

Créez des réseaux VPC en fonction de vos besoins. Citrix vous recommande de créer trois réseaux VPC à associer à une carte réseau de gestion, une carte réseau client et une carte réseau de serveur.

Pour créer un réseau VPC, procédez comme suit :

1. Ouvrez une session sur la **console Google > Mise en réseau > Réseau VPC > Créer un réseau VPC**.
2. Remplissez les champs requis, puis cliquez sur **Créer**.

Pour plus d'informations, consultez la section **Créer des réseaux VPC** dans Déployer une instance Citrix ADC VPX sur Google Cloud Platform.

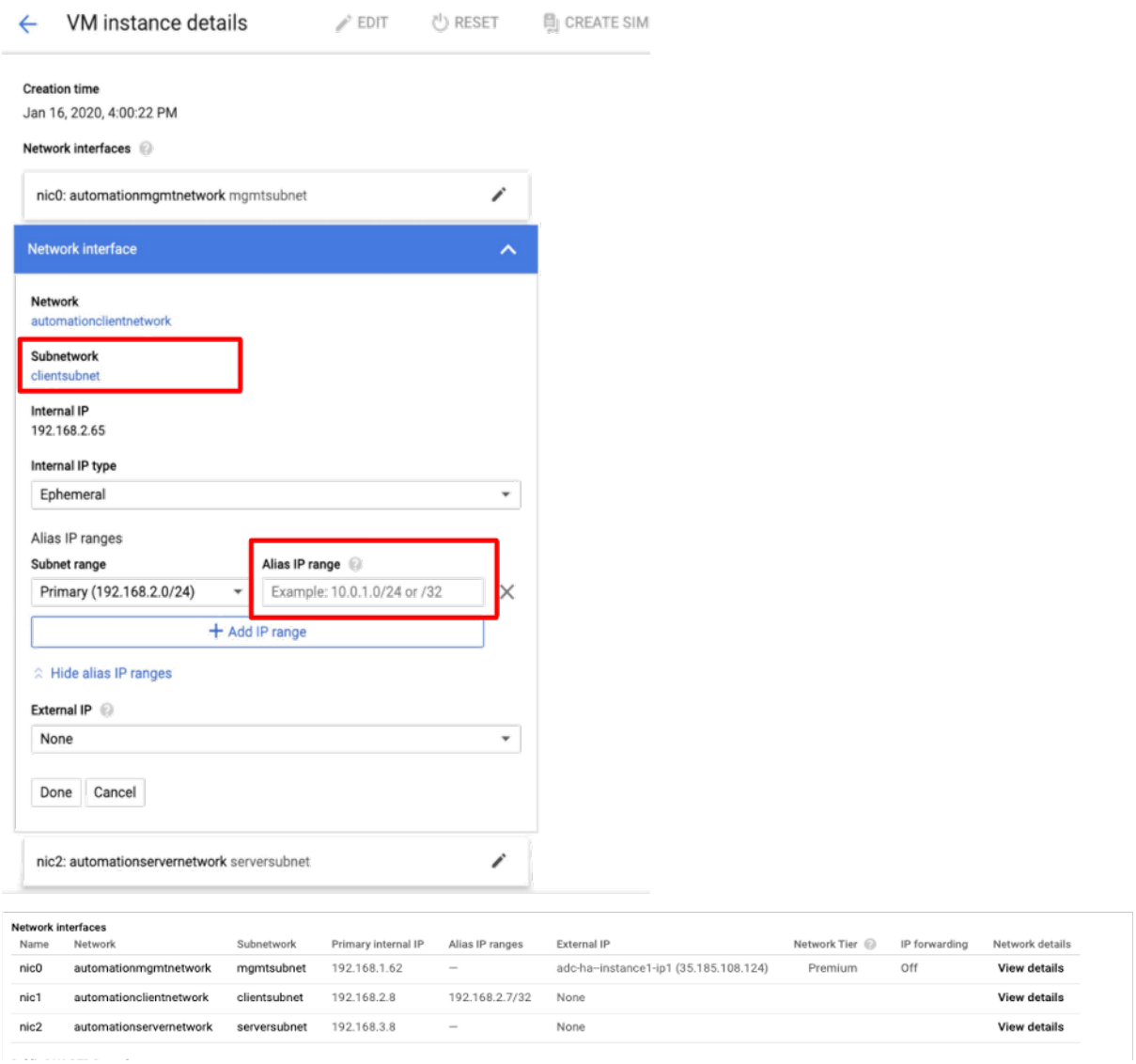
Étape 2. Créer deux instances VPX

Créez deux instances VPX en suivant les étapes indiquées dans Scénario : déployer une instance VPX autonome multi-cartes réseau et multi-IP.

> **Important :**
>
> Attribuez une adresse IP d'alias client au nœud principal. N'utilisez pas l'adresse IP interne de l'instance VPX pour configurer le VIP.

Pour créer une adresse IP d'alias client, procédez comme suit :

1. Accédez à l'instance de machine virtuelle et cliquez sur **Modifier**.
2. Dans la fenêtre **Interface réseau**, modifiez l'interface client.
3. Dans le champ **Plage d'adresses IP d'alias**, saisissez l'adresse IP de l'alias du client.



Après le basculement, lorsque l'ancien principal devient le nouveau secondaire, les adresses IP de l'alias se déplacent de l'ancien principal et sont attachées au nouveau principal.

Une fois que vous avez configuré les instances VPX, vous pouvez configurer les adresses IP virtuelles (VIP) et SNIP (Subnet IP). Pour plus d'informations, consultez Configuration des adresses IP appartenant à Citrix ADC.

Étape 3. Configurer la haute disponibilité

Après avoir créé les instances sur Google Cloud Platform, vous pouvez configurer la haute disponibilité à l'aide de l'interface graphique ou de l'interface de ligne de commande Citrix ADC.

Configurer la haute disponibilité à l'aide de l'interface graphique

Étape 1. Configurez la haute disponibilité en mode INC Enabled sur les deux nœuds.

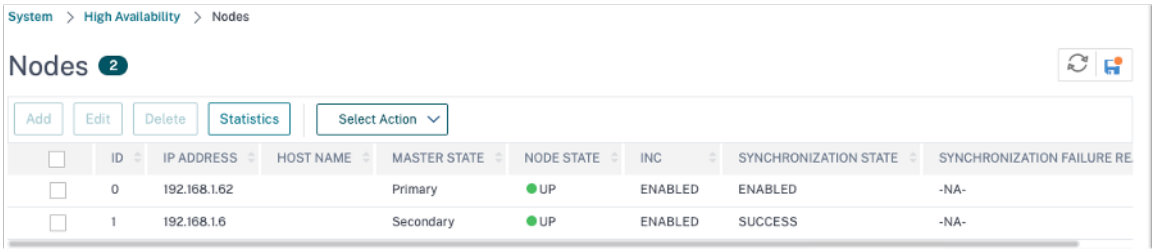
Sur le **nœud principal**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.

Sur le **nœud secondaire**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud principal.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.

Avant d'aller plus loin, assurez-vous que l'état de synchronisation du nœud secondaire s'affiche comme **SUCCÈS** dans la page **Nœuds** .



> **Remarque**
>
> Maintenant, le nœud secondaire a les mêmes informations d'identification d'ouverture de session que le nœud principal.

Étape 2. Ajoutez une adresse IP virtuelle et une adresse IP de sous-réseau sur les deux nœuds.

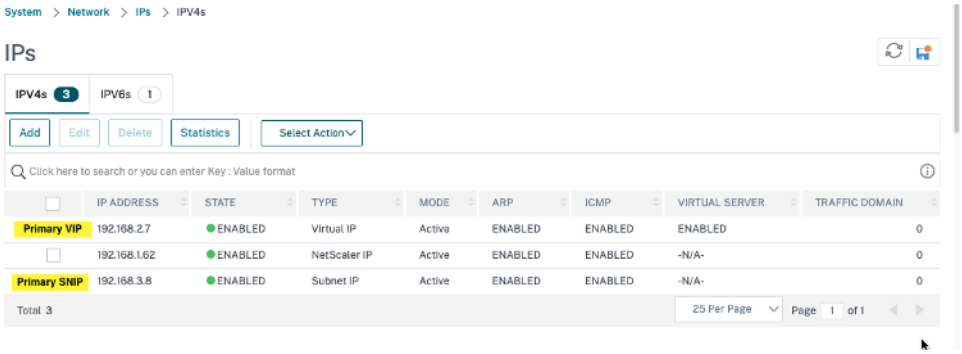
Sur le nœud principal, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Pour créer une adresse IP (VIP) alias client :

a) Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
c) Cliquez sur **Create**.

3. Pour créer une adresse IP du serveur (SNIP) :

a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance principale et du masque de réseau configurés pour le sous-réseau du serveur.
b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
c) Cliquez sur **Create**.



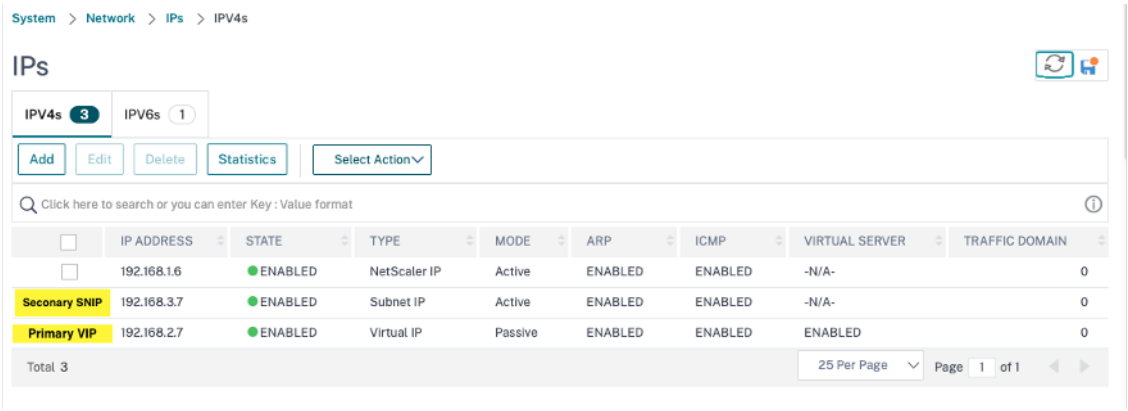
Sur le nœud secondaire, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Pour créer une adresse IP (VIP) alias client :

a) Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client sur l'instance de machine virtuelle principale.
b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
c) Cliquez sur **Create**.

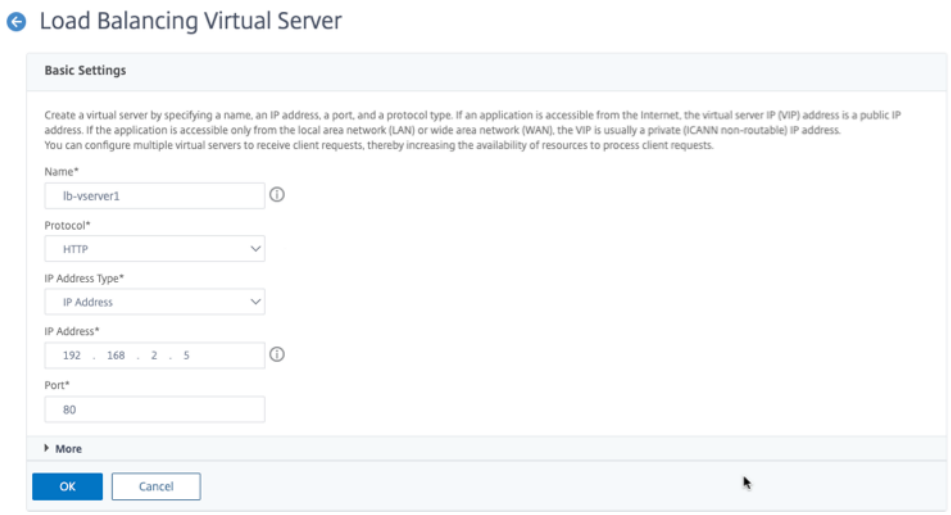
3. Pour créer une adresse IP du serveur (SNIP) :

a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance secondaire et du masque de réseau configurés pour le sous-réseau du serveur.
b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
c) Cliquez sur **Create**.



Étape 3. Ajoutez un serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.
2. Ajoutez les valeurs requises pour Nom, Protocole, Type d'adresse IP (adresse IP), Adresse IP (adresse IP de l'alias principal du client) et Port, puis cliquez sur **OK**.



Étape 4. Ajoutez un service ou un groupe de services sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 5. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 3**, puis cliquez sur **Modifier**.

3. Dans l'onglet **Groupes de services et de services**, cliquez sur **Liaison de service Virtual Server sans équilibrage de charge**.
4. Sélectionnez le service configuré à l' **étape 4**, puis cliquez sur **Lier**.

Étape 5. Enregistrez la configuration.

Après un basculement forcé, le secondaire devient le nouveau principal. L'adresse IP de l'alias client (VIP) et l'adresse IP de l'alias de serveur (SNIP) de l'ancien serveur principal sont déplacées vers la nouvelle adresse principale.

Configuration de la haute disponibilité à l'aide de la CLI

Étape 1. Configurez la haute disponibilité en mode **INC Désactivé** dans les deux instances à l'aide de l'interface de ligne de commande Citrix ADC.

Sur le nœud principal, tapez la commande suivante.

```
1 add ha node 1 <sec_ip> -inc ENABLED
2 <!--NeedCopy-->
```

Sur le nœud secondaire, tapez la commande suivante.

```
1 add ha node 1 <prim_ip> -inc ENABLED
2 <!--NeedCopy-->
```

Le `sec_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud secondaire.

Le `prim_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud principal.

Étape 2. Ajoutez VIP et SNIP sur les deux nœuds.

Tapez les commandes suivantes sur le nœud principal :

```
1 add ns ip <primary_client_alias_ip> <subnet> -type VIP
2
3 <!--NeedCopy-->
```

> **Remarque :**
>
> Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.

```
1 add ns ip <primary_snip> <subnet> -type SNIP
2 <!--NeedCopy-->
```

Le `primary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance principale.

Tapez les commandes suivantes sur le nœud secondaire :

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
<!--NeedCopy-->
```

> Remarque
>
> Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client sur l'instance de machine virtuelle principale.

```
add ns ip <secondary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

Le `secondary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance secondaire.

> **Remarque :**
>
> Entrez l'adresse IP et le masque de réseau configurés pour le sous-réseau du serveur dans l'instance de machine virtuelle.

Étape 3. Ajoutez un serveur virtuel sur le nœud principal.

Exécutez la commande suivante :

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
<!--NeedCopy-->
```

Étape 4. Ajoutez un service ou un groupe de services sur le nœud principal.

Exécutez la commande suivante :

```
add service <service_name> <service_ip_address> <protocol> <port>
<!--NeedCopy-->
```

Étape 5. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

Exécutez la commande suivante :

```
bind <server_type> vserver <vserver_name> <service_name>
<!--NeedCopy-->
```

> **Remarque :**

> Pour enregistrer votre configuration, tapez la commande `save config`. Sinon, les configurations sont perdues après le redémarrage des instances.

Ajouter un service de mise à l'échelle automatique GCP back-end

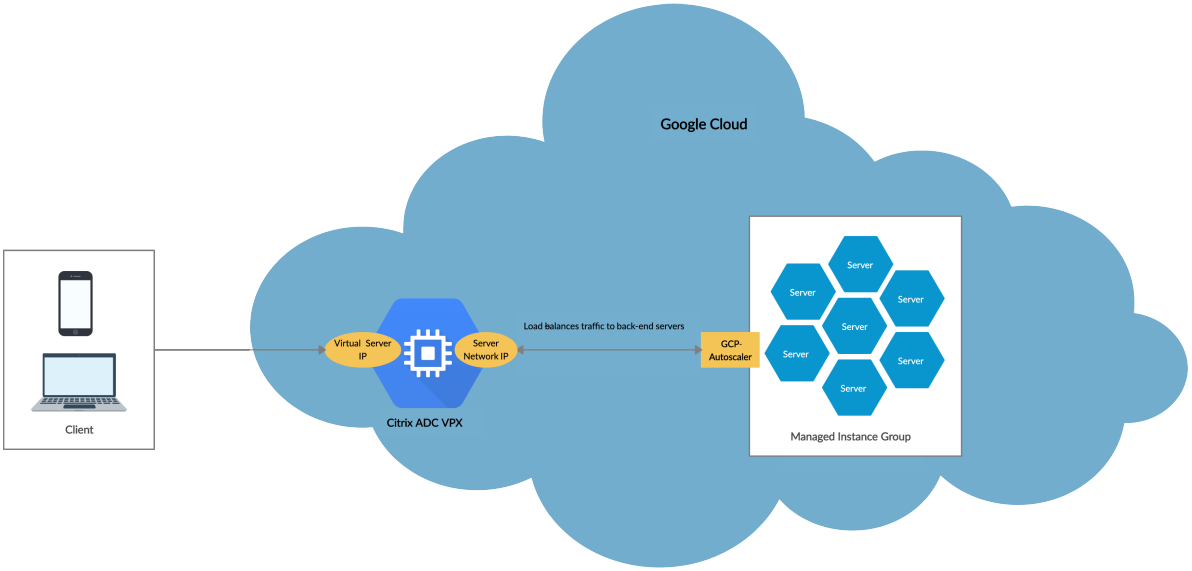
August 20, 2021

L'hébergement efficace des applications dans un cloud nécessite une gestion simple et économique des ressources, en fonction de la demande des applications. Pour répondre à la demande croissante, vous devez faire évoluer les ressources réseau à la hausse. Lorsque la demande diminue, vous devez réduire l'échelle pour éviter le coût inutile des ressources sous-utilisées. Pour minimiser le coût d'exécution de l'application, vous devez constamment surveiller le trafic, la mémoire et l'utilisation du processeur, etc. Toutefois, la surveillance manuelle du trafic est fastidieuse. Pour que l'environnement d'application évolue de manière dynamique, vous devez automatiser les processus de surveillance du trafic et de mise à l'échelle des ressources lorsque cela est nécessaire.

Intégré au service GCP Autoscaling, l'instance Citrix ADC VPX offre les avantages suivants :

- **Équilibrage et gestion de la charge** : configure automatiquement les serveurs pour qu'ils montent et descendent en puissance, en fonction de la demande. L'instance VPX détecte automatiquement les groupes d'instances gérées dans le sous-réseau principal et vous permet de sélectionner les groupes d'instances gérées pour équilibrer la charge. Les adresses IP virtuelles et de sous-réseau sont automatiquement configurées sur l'instance VPX.
- **Haute disponibilité** : détecte les groupes d'instances gérées qui couvrent plusieurs zones et serveurs d'équilibrage de charge.
- **Meilleure disponibilité du réseau** : l'instance VPX prend en charge :
  - Serveurs back-end sur les mêmes groupes de placement
  - Serveurs back-end sur différentes zones

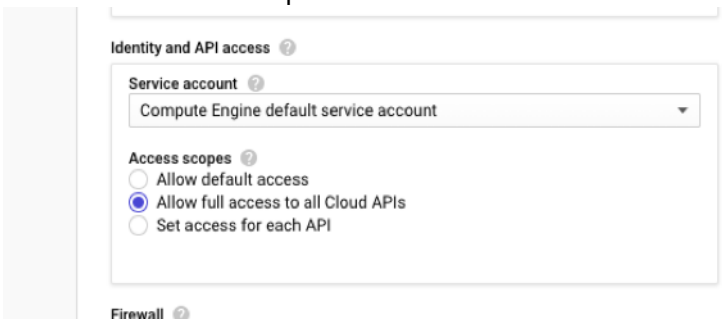
Ce diagramme illustre le fonctionnement du service GCP Autoscaling dans une instance Citrix ADC VPX agissant comme serveur virtuel d'équilibrage de charge.



Avant de commencer

Avant de commencer à utiliser Autoscaling avec votre instance Citrix ADC VPX, vous devez effectuer les tâches suivantes.

- Créez une instance Citrix ADC VPX sur GCP en fonction de vos besoins.
  - Pour plus d'informations sur la création d'une instance Citrix ADC VPX, voir Déployer une instance Citrix ADC VPX sur Google Cloud Platform.
  - Pour plus d'informations sur le déploiement d'instances VPX en mode HA, voir Déployer une paire haute disponibilité VPX sur Google Cloud Platform.
- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Autorisez un accès complet à toutes les API Cloud lors de la création des instances.



- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.instances.get",
```



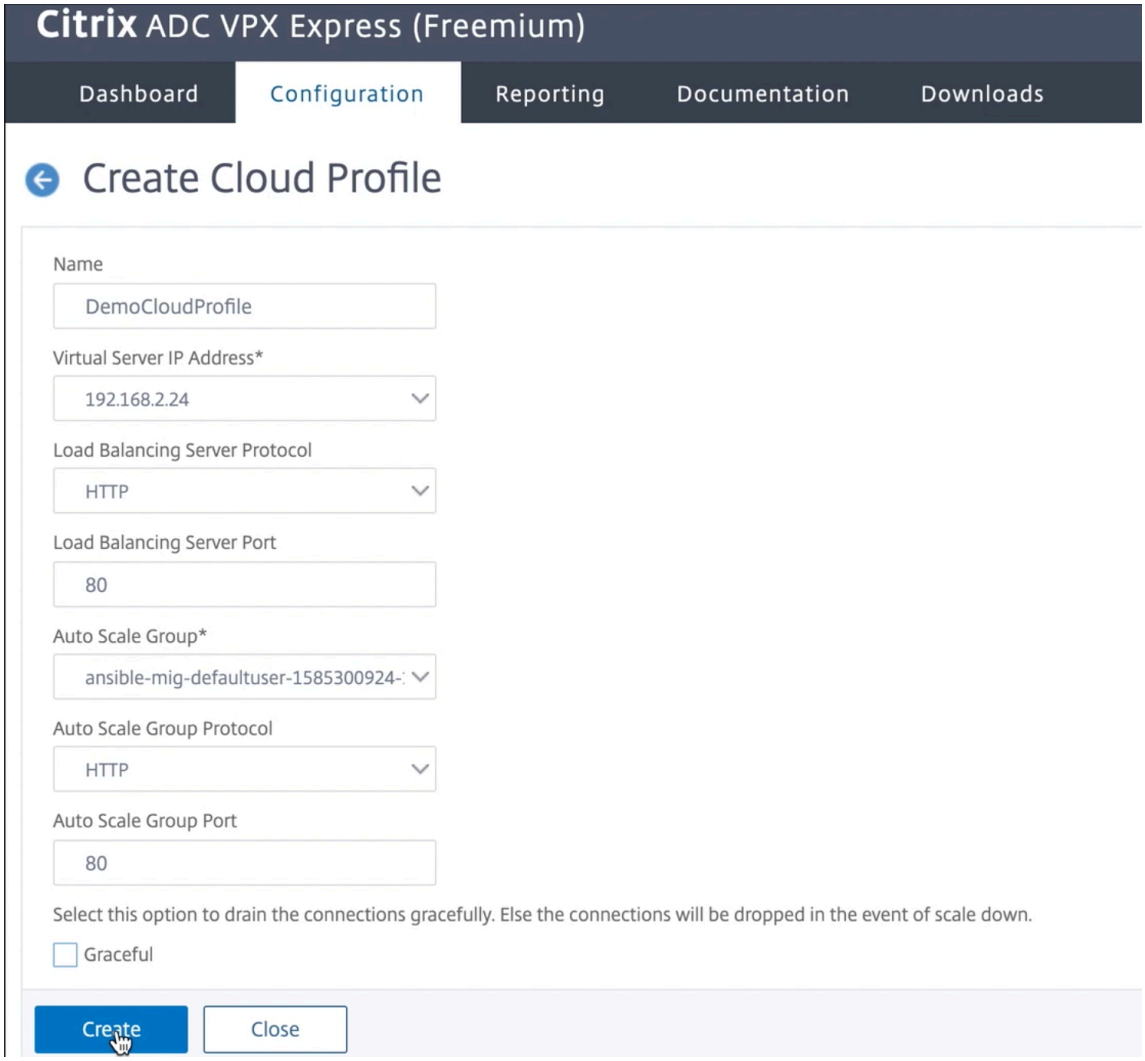
```
4   "compute.zones.list",
5   "compute.instanceGroupManagers.list",
6   "compute.instanceGroupManagers.get"
7   ]
8   <!--NeedCopy-->
```

- Pour configurer la mise à l'échelle automatique, assurez-vous que les éléments suivants sont configurés :
  - Modèle d'instance
  - Groupe d'instances gérées
  - Stratégie de mise à l'échelle automatique

Ajouter le service GCP Autoscaling à une instance Citrix ADC VPX

Vous pouvez ajouter le service Autoscaling à une instance VPX en un seul clic à l'aide de l'interface graphique. Procédez comme suit pour ajouter le service Autoscaling à l'instance VPX :

1. Connectez-vous à l'instance VPX à l'aide de vos informations d'identification pour`nsroot`.
2. Lorsque vous ouvrez une session sur l'instance Citrix ADC VPX pour la première fois, la page de profil cloud par défaut s'affiche. Sélectionnez le groupe d'instances gérées GCP dans le menu déroulant et cliquez sur **Créer** pour créer un profil cloud.

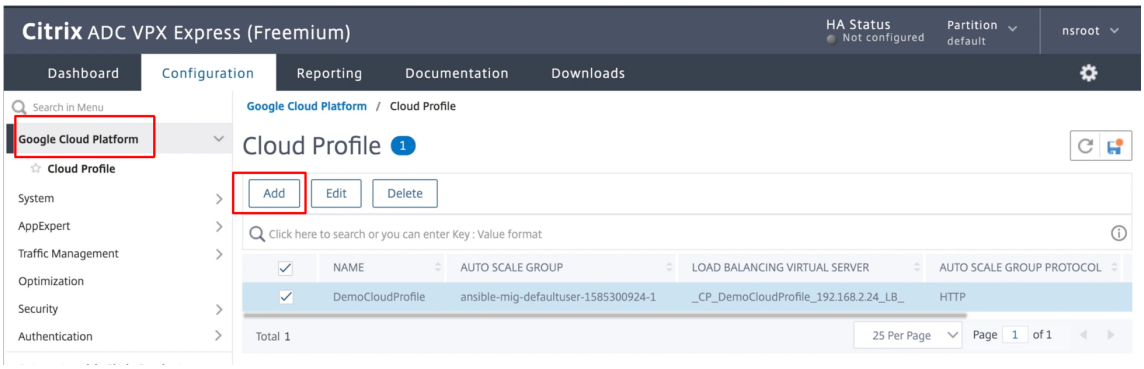


- Le champ **Adresse IP du serveur virtuel** est automatiquement renseigné à partir de toutes les adresses IP associées aux instances.
- Le **groupe Autoscale** est prérempli à partir du groupe d'instances géré configuré sur votre compte GCP.
- Lorsque vous sélectionnez le **protocole de groupe de mise** à l'**échelle automatique et le port de groupe**de mise à l'échelle automatique, assurez-vous que vos serveurs écoutent le protocole et les ports configurés. Liez le moniteur correct dans le groupe de services. Par défaut, le moniteur TCP est utilisé.
- Désactivez la case à cocher **Graceful** car elle n'est pas prise en charge.

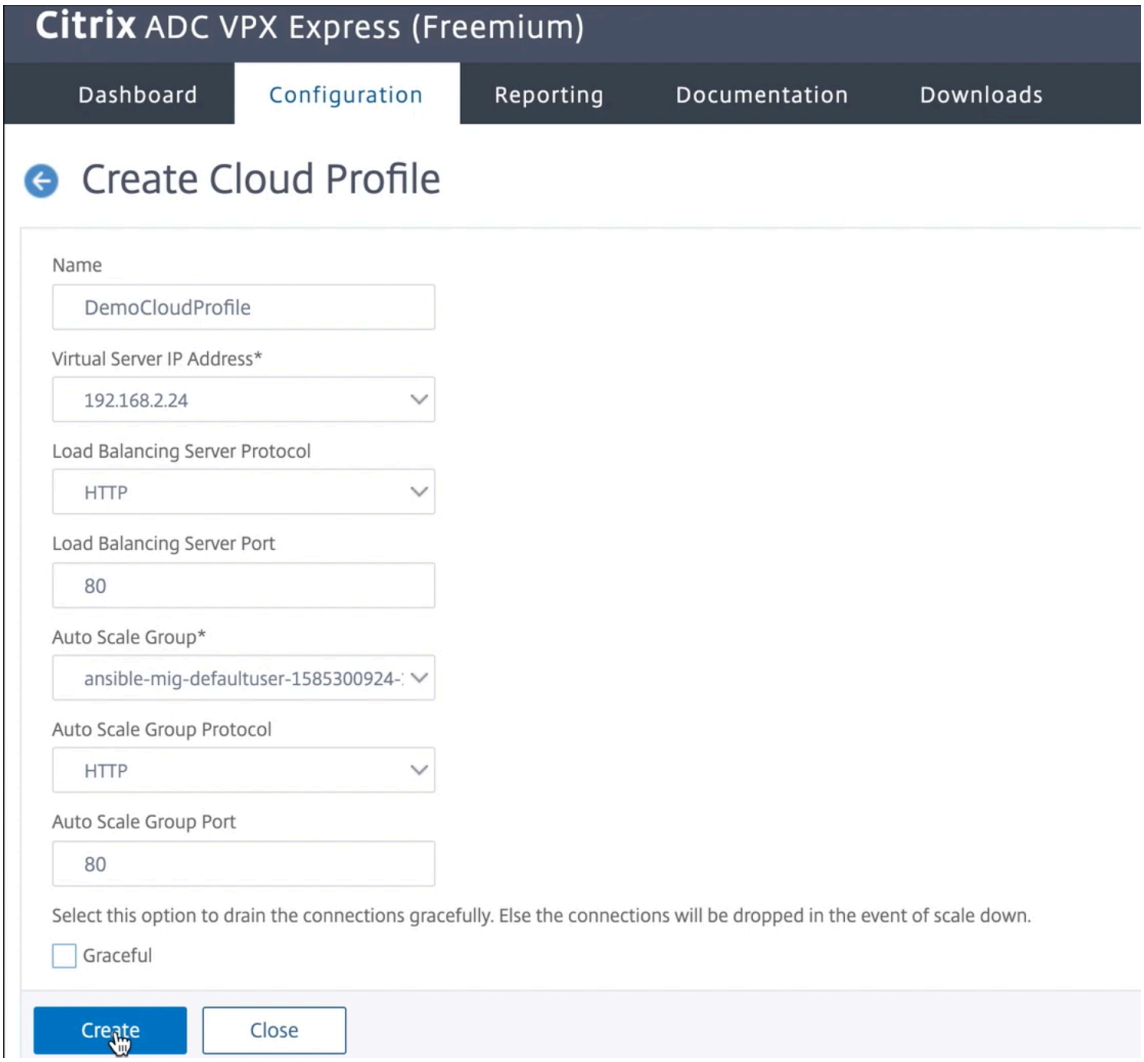
> Remarque :
>
> Pour le protocole SSL de type Autoscaling, après avoir créé le profil Cloud, le serveur virtuel d'équilibrage de charge ou le groupe de services est en panne en raison d'un certificat manquant. Vous pouvez lier manuellement le certificat au serveur virtuel ou au groupe de ser-

vices.

3. Après la première ouverture de session si vous souhaitez créer un profil Cloud, dans l'interface graphique, accédez à **Système > Google Cloud Platform > Profil Cloud** et cliquez sur **Ajouter**.

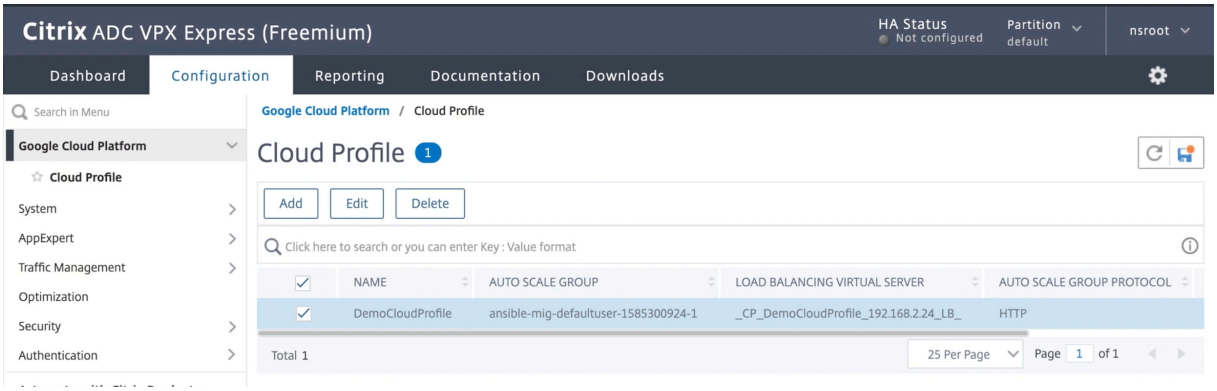


La page de configuration **Créer un profil Cloud** s'affiche.



Cloud Profile crée un serveur virtuel d'équilibrage de charge Citrix ADC et un groupe de ser-

vices dont les membres sont les serveurs du groupe d'instances gérées. Vos serveurs back-end doivent être accessibles via le SNIP configuré sur l'instance VPX.



Prise en charge de la mise à l'échelle VIP pour l'instance Citrix ADC VPX sur GCP

October 5, 2021

Une appliance Citrix ADC réside entre les clients et les serveurs, de sorte que les demandes des clients et les réponses du serveur passent par elle. Dans une installation classique, les serveurs virtuels configurés sur l'appliance fournissent des points de connexion que les clients utilisent pour accéder aux applications derrière l'appliance. Le nombre d'adresses IP virtuelles (VIP) publiques nécessaires pour un déploiement varie au cas par cas.

L'architecture GCP limite chaque interface de l'instance à connecter à un VPC différent. Un VPC sur GCP est un ensemble de sous-réseaux, et chaque sous-réseau peut s'étendent sur plusieurs zones d'une région. De plus, GCP impose la limitation suivante :

- Il existe un mappage 1:1 du nombre d'adresses IP publiques au nombre de cartes réseau. Une seule adresse IP publique peut être attribuée à une carte réseau.
- Un maximum de 8 cartes réseau peuvent être attachées à un type d'instance de capacité supérieure.

Par exemple, une instance n1-standard-2 ne peut avoir que 2 cartes réseau, et les VIP publics pouvant être ajoutés sont limités à 2. Pour plus d'informations, consultez Quotas de ressources VPC.

Pour obtenir des échelles plus élevées des adresses IP virtuelles publiques sur une instance Citrix ADC VPX, vous pouvez configurer les adresses VIP dans le cadre des métadonnées de l'instance. L'instance VPX ADC utilise en interne les règles de transfert fournies par le GCP pour réaliser la mise à l'échelle VIP. L'instance VPX ADC fournit également une haute disponibilité aux VIP configurés.
Une fois que vous avez configuré les adresses VIP dans le cadre des métadonnées, vous pouvez configurer un serveur virtuel LB à l'aide de la même adresse IP que celle utilisée pour créer les règles de

transfert. Ainsi, nous pouvons utiliser des règles de transfert pour atténuer les limitations que nous avons à l'échelle w.r.t dans l'utilisation des adresses VIP publiques sur une instance ADC VPX sur GCP.

Pour plus d'informations sur les règles de transfert, voir Vue d'ensemble des règles de transfert.

Pour plus d'informations sur HA, voir Haute disponibilité.

Points à noter

- Google facture des frais supplémentaires pour chaque règle de transfert d'adresse IP virtuelle. Le coût réel dépend du nombre d'entrées créées. Le coût associé est disponible dans les documents de tarification de Google.
- Les règles de transfert ne s'appliquent qu'aux VIP publics. Vous pouvez utiliser des adresses IP d'alias lorsque le déploiement a besoin d'adresses IP privées en tant que VIP.
- Vous pouvez créer des règles de transfert uniquement pour les protocoles qui nécessitent le serveur virtuel LB. Les VIP peuvent être créés, mis à jour ou supprimés à la volée. Vous pouvez également ajouter un nouveau serveur virtuel d'équilibrage de charge avec la même adresse VIP, mais avec un protocole différent.

Avant de commencer

- L'instance Citrix ADC VPX doit être déployée sur GCP.
- L'adresse IP externe doit être réservée. Pour plus d'informations, voir Réservation d'une adresse IP externe statique.
- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.instances.use",
"compute.subnetworks.use",
"compute.targetInstances.create"
"compute.targetInstances.get"
"compute.targetInstances.use",
]

<!--NeedCopy-->
```


- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Si vous utilisez la mise à l'échelle VIP sur une instance VPX autonome, assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.instances.use",
"compute.subnetworks.use",
"compute.targetInstances.create",
"compute.targetInstances.list",
"compute.targetInstances.use",
]
<!--NeedCopy-->
```

- Si vous utilisez la mise à l'échelle VIP en mode haute disponibilité, assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_IAM_PERMS = [
"compute.addresses.get",
"compute.addresses.list",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.use",
"compute.instances.get",
"compute.instances.list",
"compute.instances.setMetadata",
"compute.subnetworks.use",
"compute.targetInstances.create",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.zones.list",
]
<!--NeedCopy-->
```


> Remarque :
>
> En mode haute disponibilité, si votre compte de service n'a pas de rôle de propriétaire ou d'éditeur, vous devez ajouter le **rôle d'utilisateur du compte de service** à votre compte de service.

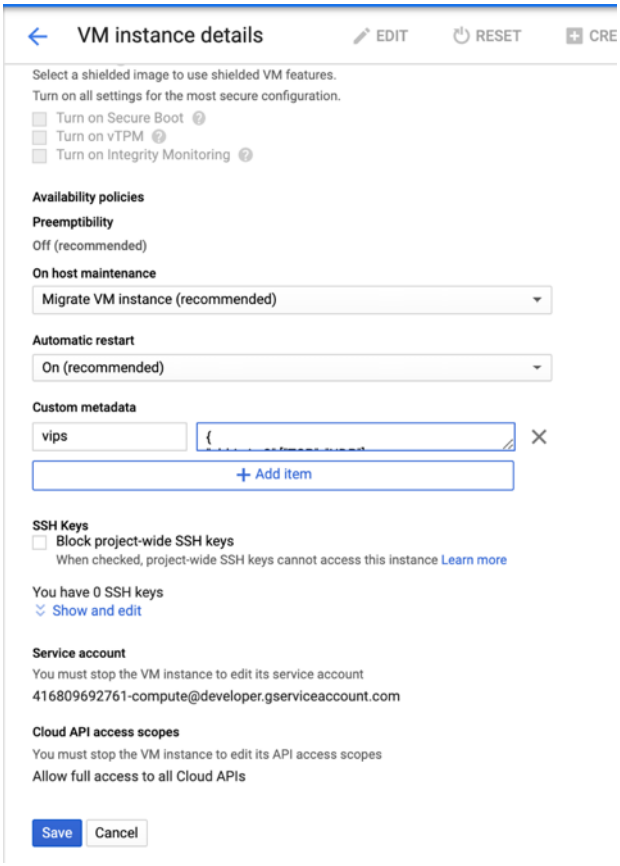
Configurer les adresses IP externes pour la mise à l'échelle VIP sur l'instance Citrix ADC VPX

1. Dans la console Google Cloud, accédez à la page **Instances de machine virtuelle** .
2. Créez une nouvelle instance de machine virtuelle ou utilisez une instance existante.
3. Cliquez sur le nom de l'instance. Sur la page des **détails de l'instance de machine virtuelle**, cliquez sur **Modifier**.
4. Mettez à jour les **métadonnées personnalisées** en saisissant ce qui suit :
   - Clé = VIP
   - Valeur = Fournir une valeur au format JSON suivant :

     {
     « Nom de l'adresse IP réservée externe » : [liste des protocoles],
     }

   GCP prend en charge les protocoles suivants :

   - AH
   - ESP
   - ICMP
   - SCT
   - TCP
   - UDP



Pour plus d'informations, voir Métadonnées personnalisées.

Exemple de métadonnées personnalisées :

{
"external-ip1-name":["TCP", "UDP"],
"external-ip2-name":["ICMP", "AH"]
}

Dans cet exemple, l'instance ADC VPX crée en interne une règle de transfert pour chaque paire IP, protocole. Les entrées de métadonnées sont mappées aux règles de transfert. Cet exemple vous aide à comprendre le nombre de règles de transfert créées pour une entrée de métadonnées.

Quatre règles de transfert sont créées comme suit :

a) nom-ip1-externe et TCP
b) nom-ip1-externe et UDP
c) nom-ip2 externe et ICMP
d) nom-ip2 externe et AH

> Remarque :
>
> En mode HA, vous devez ajouter des métadonnées personnalisées uniquement sur

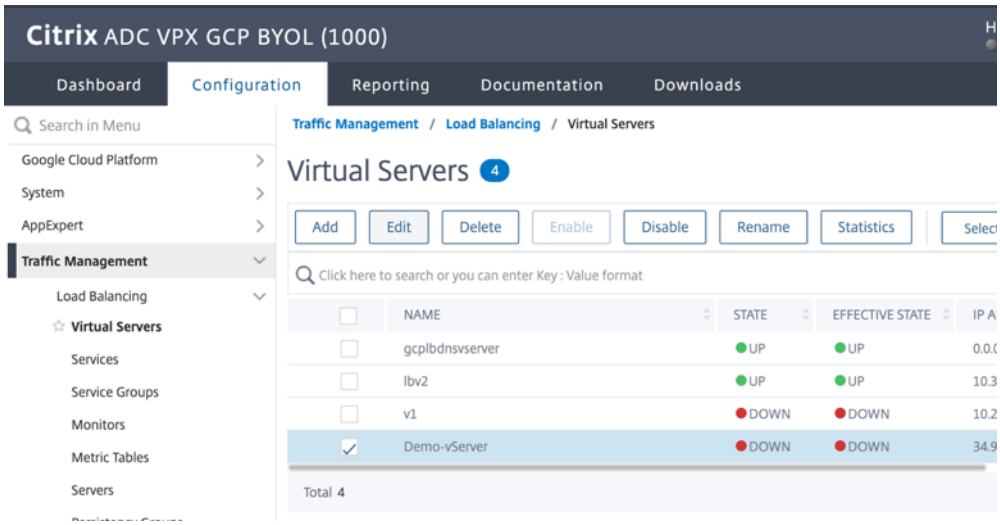
> l'instance principale. En cas de basculement, les métadonnées personnalisées sont synchronisées avec le nouveau serveur principal.

5. Cliquez sur **Enregistrer**.

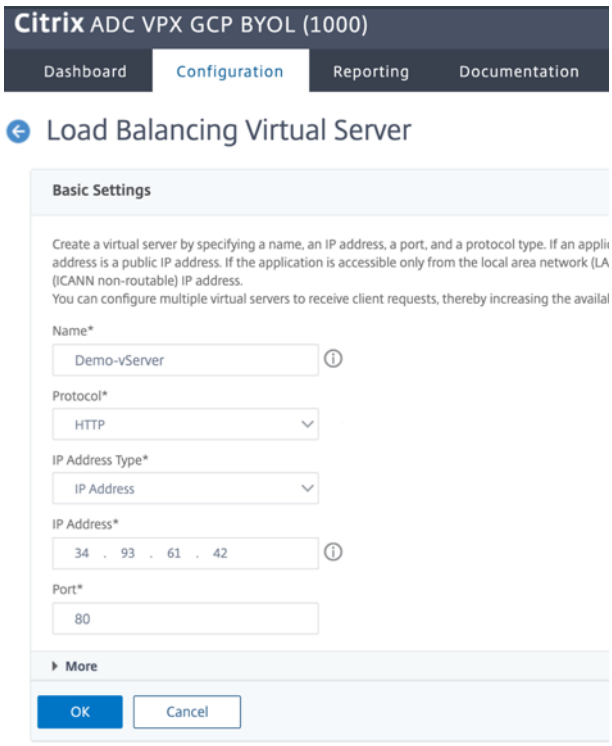
Configuration d'un serveur virtuel d'équilibrage de charge avec une adresse IP externe sur une instance Citrix ADC VPX

Étape 1. Ajoutez un serveur virtuel d'équilibrage de charge.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.

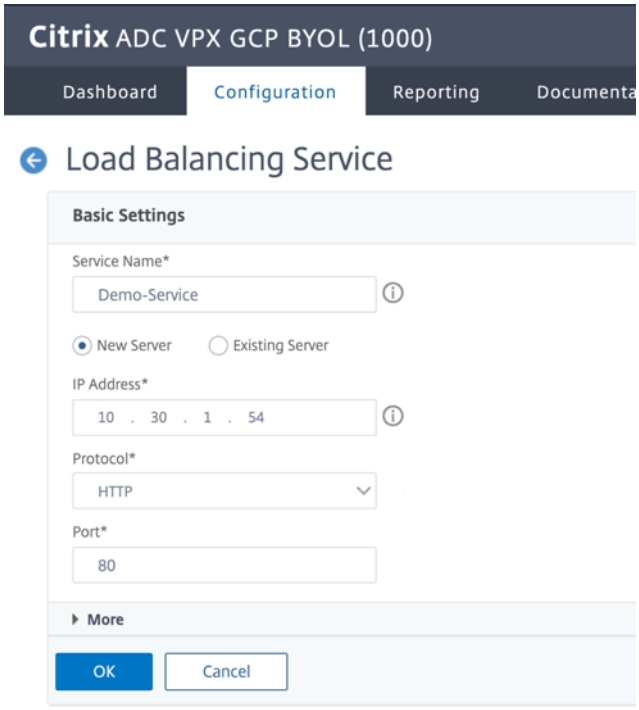


2. Ajoutez les valeurs requises pour le nom, le protocole, le type d'adresse IP (adresse IP), l'adresse IP (adresse IP externe de la règle de transfert ajoutée en tant que VIP sur ADC) et le port, puis cliquez sur **OK**.



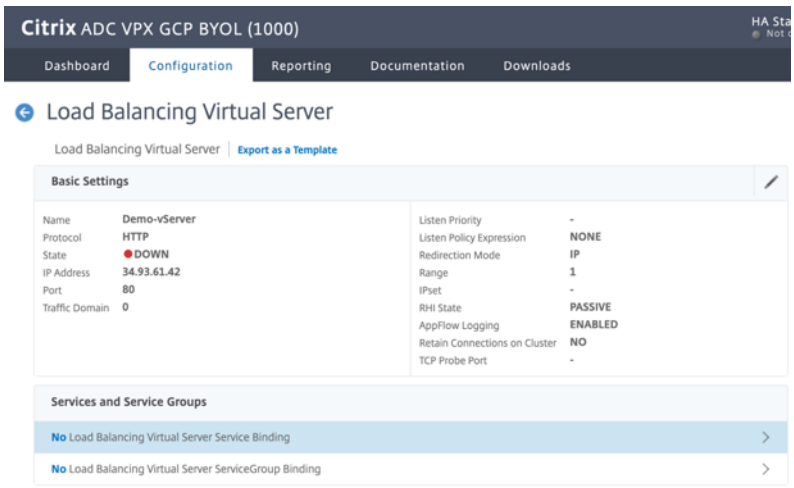
Étape 2. Ajoutez un service ou un groupe de services.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

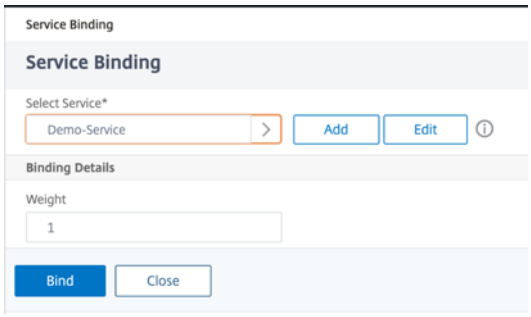


Étape 3. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 1**, puis cliquez sur **Modifier**.
3. Dans la page **Groupes de services et de services**, cliquez sur **Liaison de service de serveur virtuel sans équilibrage de charge**.



4. Sélectionnez le service configuré à l' **étape 3**, puis cliquez sur **Lier**.



5. Enregistrez la configuration.

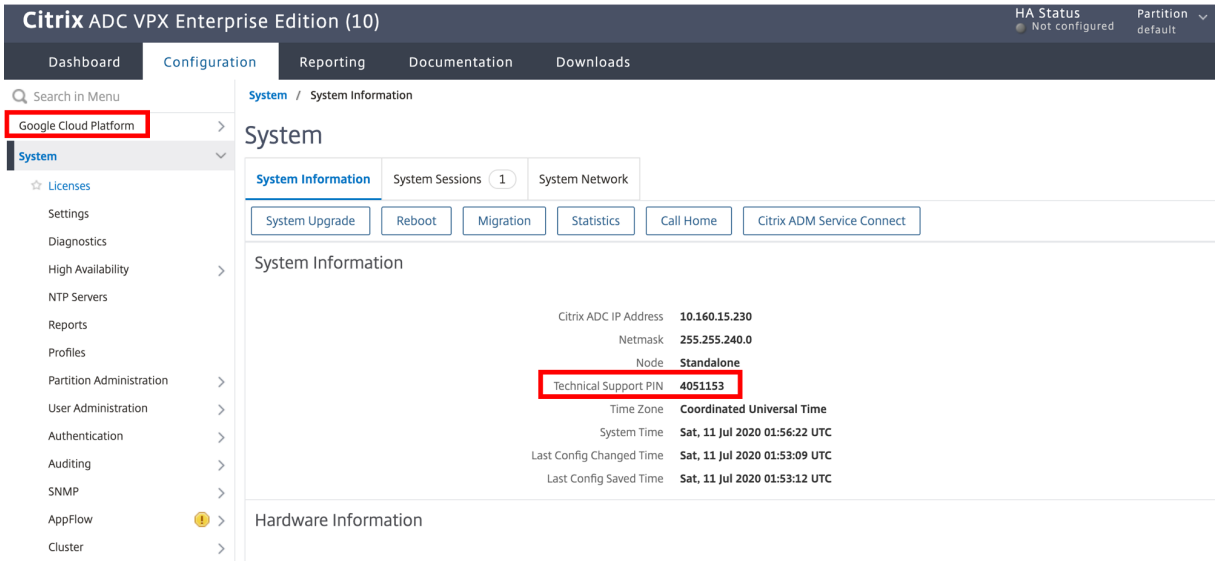
Résoudre les problèmes d'une instance VPX sur GCP

August 20, 2021

Google Cloud Platform (GCP) fournit un accès console à une instance Citrix ADC VPX. Vous ne pouvez déboguer que si le réseau est connecté. Pour afficher le journal système d'une instance, accédez à la console et vérifiez **les fichiers journaux système**.

Citrix prend en charge les instances Citrix ADC VPX basées sur des frais (licence utilitaire avec frais horaires) sur GCP. Pour déposer un dossier de support technique, recherchez votre numéro de compte GCP et code PIN de support, puis appelez le support technique Citrix. Il vous est demandé de fournir votre nom et votre adresse e-mail. Pour trouver le code PIN de support, connectez-vous à l'interface graphique VPX et accédez à la page **Système**.

Voici un exemple de page système montrant le code PIN de support.



Trames jumbo sur les instances Citrix ADC VPX

August 20, 2021

Les appliances Citrix ADC VPX prennent en charge la réception et la transmission de trames jumbo contenant jusqu'à 9216 octets de données IP. Les trames Jumbo peuvent transférer des fichiers volumineux plus efficacement qu'il n'est possible avec la taille standard de MTU IP de 1500 octets.

Une appliance Citrix ADC peut utiliser des trames jumbo dans les scénarios de déploiement suivants :

- Jumbo à Jumbo. L'appliance reçoit les données sous forme de trames jumbo et les envoie sous forme de trames jumbo.
- Non Jumbo à Jumbo. L'appliance reçoit les données sous forme de trames régulières et les envoie sous forme de trames jumbo.
- Jumbo à non-Jumbo. L'appliance reçoit les données sous forme de trames jumbo et les envoie en tant que trames régulières.

Pour plus d'informations, voirConfiguration de la prise en charge des trames Jumbo sur une appliance Citrix ADC.

La prise en charge des trames jumbo est disponible sur les appliances Citrix ADC VPX s'exécutant sur les plates-formes de virtualisation suivantes :

- VMware ESX
- Plateforme Linux-KVM
- Citrix XenServer
- Amazon Web Services (AWS)

Les cadres jumbo sur les appareils VPX fonctionnent de la même manière que les cadres jumbo sur les appareils MPX. Pour plus d'informations sur les trames Jumbo et leurs cas d'utilisation, voir Configuration des trames Jumbo sur les appliances MPX. Les cas d'utilisation des trames jumbo sur les appareils MPX s'appliquent également aux appareils VPX.

Configurer des trames jumbo pour une instance VPX exécutée sur VMware ESX

Effectuez les tâches suivantes pour configurer des trames jumbo sur une appliance Citrix ADC VPX exécutée sur le serveur VMware ESX :

1. Définissez la MTU de l'interface ou du canal de l'appliance VPX sur une valeur comprise entre 1501—9000. Utilisez l'interface de ligne de commande ou l'interface graphique pour définir la taille du MTU. Les appliances Citrix ADC VPX exécutées sur VMware ESX prennent en charge la réception et la transmission de trames jumbo contenant jusqu'à 9000 octets seulement de données IP.
2. Définissez la même taille MTU sur les interfaces physiques correspondantes du serveur VMware ESX à l'aide de ses applications de gestion. Pour plus d'informations sur la définition de la taille du MTU sur les interfaces physiques de VMware ESX, voir http://vmware.com/.

Configurer des trames jumbo pour une instance VPX exécutée sur un serveur Linux-KVM

Effectuez les tâches suivantes pour configurer les trames jumbo sur une appliance Citrix ADC VPX s'exécutant sur un serveur Linux-KVM :

1. Définissez la MTU de l'interface ou du canal de l'appliance VPX sur une valeur comprise entre 1501 et 9216. Utilisez l'interface de ligne de commande ou l'interface graphique graphique Citrix ADC VPX pour définir la taille MTU.
2. Définissez la même taille MTU sur les interfaces physiques correspondantes d'un serveur Linux-KVM à l'aide de ses applications de gestion. Pour plus d'informations sur la définition de la taille MTU sur les interfaces physiques de Linux-KVM, reportez-vous à la section http://www.linux-kvm.org/.

Configurer des trames jumbo pour une instance VPX exécutée sur Citrix XenServer

Effectuez les tâches suivantes pour configurer des trames jumbo sur une appliance Citrix ADC VPX exécutée sur Citrix XenServer :

1. Connectez-vous au XenServer à l'aide de XenCenter.
2. Arrêtez toutes les instances VPX qui utilisent les réseaux pour lesquels le MTU doit être modifié.
3. Sous l'onglet **Mise en réseau**, sélectionnez le réseau - réseau 0/1/2.
4. Sélectionnez **Propriétés** et modifiez MTU.

Après avoir configuré les trames jumbo sur XenServer, vous pouvez configurer les trames jumbo sur l'appliance ADC. Pour plus d'informations, voirConfiguration de la prise en charge des trames Jumbo sur une appliance Citrix ADC.

Configurer des trames jumbo pour une instance VPX exécutée sur AWS

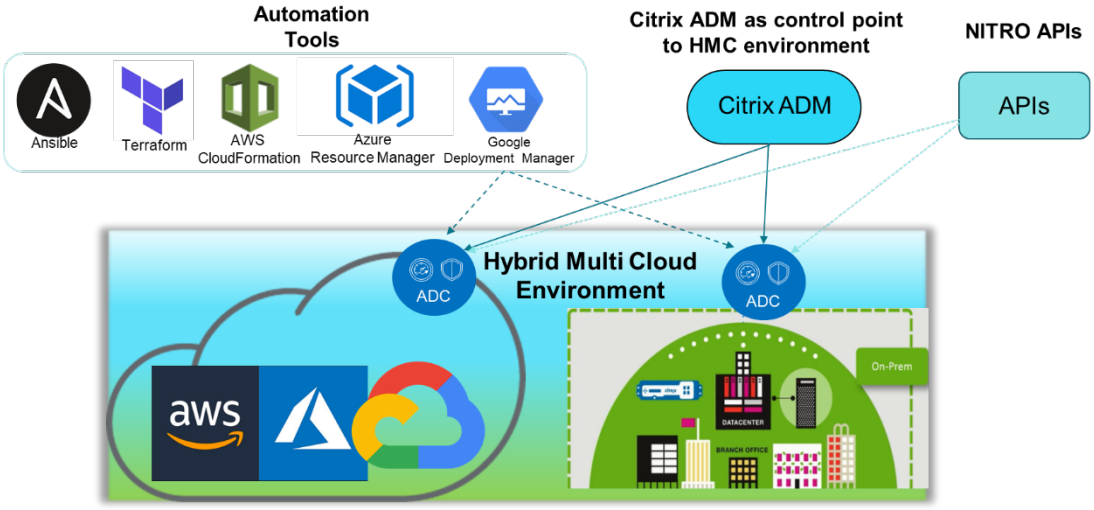
La configuration au niveau de l'hôte n'est pas requise pour VPX sur Azure. Pour configurer les trames Jumbo sur VPX, suivez les étapes décrites dans Configuration de la prise en charge des trames Jumbo sur une appliance Citrix ADC.

Automatisez le déploiement et les configurations de Citrix ADC

August 20, 2021

Citrix ADC fournit plusieurs outils pour automatiser vos déploiements et configurations ADC. Ce document fournit un bref résumé des divers outils d'automatisation et des références à diverses ressources d'automatisation que vous pouvez utiliser pour gérer les configurations ADC.

L'illustration suivante donne une vue d'ensemble de l'automatisation Citrix ADC dans un environnement multicloud hybride (HMC).



Automatisez Citrix ADC à l'aide de Citrix ADM

Citrix ADM agit comme point de contrôle d'automatisation pour votre infrastructure ADC distribuée. Citrix ADM fournit un ensemble complet de fonctionnalités d'automatisation, du provisionnement des appliances ADC à la mise à niveau. Voici les principales fonctionnalités d'automatisation d'ADM :

- Provisionnement d'instances Citrix ADC VPX sur AWS
- Provisionnement des instances Citrix ADC VPX sur Azure
- StyleBooks
- Travaux de configuration
- Audit de configuration
- Mises à niveau ADC
- Gestion des certificats SSL
- Intégrations - Intégrations [GitHub](/fr-fr/citrix-application-delivery-management-service/stylebooks/impor and-synchronizing-stylebooks-from-github-repository.html), [ServiceNow](/fr-fr/citrix-application-delivery-management-service/setting-up/integrate-itsm-adapter-citrix-adm-servicenow.html), notifications d'événements

Blogs et vidéos Citrix ADM sur l'automatisation

- Migrations d'applications avec StyleBooks
- Intégrer les configurations CAN avec CI/CD à l'aide de ADM StyleBooks
- Simplification des déploiements Citrix ADC dans le cloud public via ADM
- 10 façons dont le service Citrix ADM prend en charge les mises à niveau Citrix ADC plus faciles

Citrix ADM fournit également des API pour ses différentes fonctionnalités qui intègrent Citrix ADM et Citrix ADC dans le cadre de l'automatisation informatique globale. Pour plus d'informations, consultez API Citrix ADM Service.

Automatiser Citrix ADC à l'aide de Terraform

Terraform est un outil qui prend l'infrastructure comme approche de code pour provisionner et gérer le cloud, l'infrastructure ou le service. Les ressources terraform Citrix ADC sont disponibles dans GitHub pour une utilisation. Reportez-vous à GitHub pour la documentation détaillée et l'utilisation.

- Modules Citrix ADC Terraform pour configurer ADC pour divers cas d'utilisation tels que Load Balancing et GSLB
- Scripts de cloud Terraform pour déployer ADC dans AWS
- Scripts de cloud Terraform pour déployer ADC dans Azure

Vidéos sur Terraform pour l'automatisation ADC

- Automatiser vos déploiements Citrix ADC avec Terraform
- Provisionner et configurer ADC dans la configuration HA dans AWS à l'aide de Terraform

Automatiser Citrix ADC à l'aide de Ansible

Ansible est un outil open source de provisionnement logiciel, de gestion de la configuration et de déploiement d'applications permettant l'infrastructure en tant que code. Les modules Ansible Citrix ADC et les exemples de playbooks peuvent être trouvés dans GitHub pour une utilisation. Reportez-vous à GitHub pour la documentation détaillée et l'utilisation.

- Modules ansibles pour configurer ADC
- Automatiser ADC avec Ansible-whitepaper
- Modules ansibles pour ADM

Citrix est un partenaire certifié Ansible Automation. Les utilisateurs disposant d'un abonnement Red Hat Ansible Automation Platform peuvent accéder aux collections Citrix ADC à partir de Red Hat Automation Hub.

Blogs d'automatisation Terraform et Ansible

- Terraform et Ansible Automation pour la livraison et la sécurité des applications

Modèles de cloud public pour les déploiements ADC

Les modèles de cloud public simplifient le provisionnement de vos déploiements dans les clouds publics. Différents modèles Citrix ADC sont disponibles pour différents environnements. Pour plus d'informations sur l'utilisation, reportez-vous aux référentiels GitHub respectifs.

CFT AWS :

- CFT pour provisionner Citrix ADC VPX sur AWS

Modèles Azure Resource Manager (ARM) :

- Modèles ARM pour provisionner Citrix ADC VPX sur Azure

Modèles Google Cloud Deployment Manager (GDM) :

- Modèles GDM pour provisionner Citrix ADC VPX sur Google

Vidéos sur les modèles

- Déployer Citrix ADC HA dans AWS à l'aide du modèle CloudFormation
- Déployer Citrix ADC HA dans les zones de disponibilité à l'aide d'AWS QuickStart
- Déploiement Citrix ADC HA dans GCP à l'aide de modèles GDM

Démarrages rapides AWS

- Démarrage rapide Citrix WAF
- Démarrage rapide AWS pour Citrix ADC VPX pour applications Web sur AWS

API NITRO

Le protocole Citrix ADC NITRO vous permet de configurer et de surveiller par programme l'appliance Citrix ADC à l'aide des interfaces REST (Representational State Transfer). Par conséquent, les applications NITRO peuvent être développées dans n'importe quel langage de programmation. Pour les applications qui doivent être développées en Java, .NET ou Python, les API NITRO sont exposées via des bibliothèques pertinentes qui sont emballées sous forme de kits de développement logiciel (SDK) distincts.

- Documentation de l'API NITRO
- Référence de l'API Citrix ADC
- Exemple de configuration de cas d'utilisation ADC à l'aide de l'API NITRO

FAQ

October 5, 2021

La section suivante vous aide à classer les questions fréquentes en fonction de Citrix Application Delivery Controller (ADC) VPX.

- Fonctionnalité et fonctionnalité
- Cryptage

- Prix et emballage
- Citrix ADC VPX Express
- Hyperviseur
- Planification ou dimensionnement des capacités
- Configuration système requise
- Autres FAQ techniques

Fonctionnalité et fonctionnalité

Qu'est-ce que Citrix ADC VPX ?

Citrix ADC VPX est une appliance ADC virtuelle qui peut être hébergée sur un hyperviseur installé sur des serveurs standard.

Est-ce que Citrix ADC VPX inclut toutes les fonctionnalités d'optimisation des applications Web en tant qu'appliances ADC ?

Oui. Citrix ADC VPX inclut l'équilibrage de charge, la gestion du trafic, l'accélération des applications, la sécurité des applications (y compris Citrix ADC Gateway et Citrix Application Firewall) et les fonctionnalités de déchargement. Pour obtenir un aperçu complet de la fonctionnalité et des fonctionnalités de Citrix ADC, consultez la section Livraison d'applications à votre manière.

Existe-t-il des limitations avec Citrix Application Firewall lors de son utilisation sur Citrix ADC VPX ?

Citrix Application Firewall sur Citrix ADC VPX offre les mêmes protections de sécurité que sur les appliances Citrix ADC. Les performances ou le débit de Citrix Application Firewall varient selon la plateforme.

Existe-t-il des différences entre Citrix ADC Gateway sur Citrix ADC VPX et Citrix ADC Gateway sur les appliances Citrix ADC ?

Sur le plan fonctionnel, ils sont identiques. Citrix ADC Gateway sur Citrix ADC VPX prend en charge toutes les fonctionnalités de Citrix ADC Gateway disponibles dans la version 9.1 du logiciel Citrix ADC. Toutefois, comme les appliances Citrix ADC fournissent du matériel d'accélération SSL dédié, elles offrent une évolutivité VPN SSL supérieure à celle d'une instance Citrix ADC VPX.

Outre la différence évidente de pouvoir s'exécuter sur un hyperviseur, en quoi Citrix ADC VPX diffère-t-il des appliances physiques Citrix ADC ?

Il existe deux principaux domaines dans lesquels les clients constatent des différences de comportement. La première est que Citrix ADC VPX ne peut pas offrir les mêmes performances que la plupart des appliances Citrix ADC. La seconde est que si les appliances Citrix ADC intègrent sa propre fonctionnalité de mise en réseau L2, Citrix ADC VPX s'appuie sur l'hyperviseur pour ses services de mise en réseau de niveau 2. En règle générale, il ne limite pas la façon dont Citrix ADC VPX peut être déployé. Certaines fonctionnalités L2 peuvent être configurées sur une appliance Citrix ADC physique qui doivent être configurées sur l'hyperviseur sous-jacent.

Comment Citrix ADC VPX joue-t-il un rôle sur le marché de la mise à disposition d'applications ?

Citrix ADC VPX change la donne sur le marché de la mise à disposition d'applications de la manière suivante :

- En rendant une appliance Citrix ADC encore plus abordable, Citrix ADC VPX permet à toute organisation informatique de déployer une appliance Citrix ADC. Il ne s'agit pas uniquement de leurs applications Web les plus critiques, mais également de toutes leurs applications Web.
- Citrix ADC VPX permet aux clients de faire converger davantage la mise en réseau et la virtualisation au sein de leurs centres de données. Citrix ADC VPX ne peut pas uniquement être utilisé pour optimiser les applications Web hébergées sur des serveurs virtualisés. Il permet également à la livraison d'applications Web elle-même de devenir un service virtualisé qui peut être facilement et rapidement déployé n'importe où. Les organisations informatiques utilisent les processus standard du centre de données pour des tâches telles que le provisionnement, l'automatisation et la rétrofacturation pour l'infrastructure de distribution d'applications Web.
- Citrix ADC VPX ouvre de nouvelles architectures de déploiement qui ne sont pas pratiques si seules des appliances physiques sont utilisées. Les appliances Citrix ADC VPX et Citrix ADC MPX peuvent être utilisées de base, adaptées aux besoins individuels de chaque application respective pour gérer des actions exigeantes en processeurs telles que la compression et l'inspection du pare-feu d'application. À la périphérie du centre de données, les appliances Citrix ADC MPX gèrent des tâches à volume élevé à l'échelle du réseau telles que la distribution initiale du trafic, le chiffrement ou le déchiffrement SSL, la prévention des attaques par déni de service (DoS) et l'équilibrage de charge global. Le jumelage des appliances Citrix ADC MPX hautes performances à l'appliance virtuelle Citrix ADC VPX facile à déployer apporte une flexibilité et des capacités de personnalisation inégalées aux environnements modernes de datacenter à grande échelle tout en réduisant les coûts globaux des datacenters.

Comment Citrix ADC VPX s'intègre-t-il dans notre stratégie de centre de livraison Citrix ?

Avec la disponibilité de Citrix ADC VPX, l'ensemble de l'offre Citrix Delivery Centers est disponible sous forme d'offre virtualisée. L'ensemble du centre de mise à disposition Citrix bénéficie des puissantes fonctionnalités de gestion, de provisionnement, de surveillance et de création de rapports disponibles dans Citrix XenCenter. Cela peut être déployé rapidement dans presque n'importe quel environnement et géré de manière centralisée depuis n'importe où. Grâce à une infrastructure intégrée et virtualisée de distribution d'applications, les entreprises peuvent fournir des postes de travail, des applications client-serveur et des applications Web.

Cryptage

Citrix ADC VPX prend-il en charge le déchargement SSL ?

Oui. Cependant, Citrix ADC VPX effectue tous les traitements SSL dans le logiciel, de sorte que Citrix ADC VPX n'offre pas les mêmes performances SSL que les appliances Citrix ADC. Citrix ADC VPX peut prendre en charge jusqu'à 750 nouvelles transactions SSL par seconde.

Les cartes SSL tierces installées sur le serveur hébergeant Citrix ADC VPX accélèrent-elles le cryptage ou le déchiffrement SSL ?

Non. La prise en charge des cartes SSL tierces ne peut pas associer Citrix ADC VPX à des implémentations matérielles spécifiques. Cela réduit considérablement la capacité d'une organisation à héberger de manière flexible Citrix ADC VPX n'importe où dans le centre de données. Les appliances Citrix ADC MPX doivent être utilisées lorsqu'un débit SSL supérieur à celui fourni par Citrix ADC VPX est requis.

Citrix ADC VPX prend-il en charge les mêmes chiffrements de chiffrement que les appliances Citrix ADC physiques ?

VPX prend en charge tous les chiffrements de chiffrement en tant qu'appliances Citrix ADC physiques, à l'exception de l'ECDSA.

Quel est le débit de transactions SSL de Citrix ADC VPX ?

Consultez la fiche technique Citrix ADC VPX pour plus d'informations sur le débit des transactions SSL.

Prix et emballage

Comment est emballé Citrix ADC VPX ?

La sélection Citrix ADC VPX est similaire à celle des appliances Citrix ADC. Tout d'abord, le client sélectionne l'édition Citrix ADC en fonction de ses exigences de fonctionnalité. Ensuite, le client sélectionne

le niveau de bande passante Citrix ADC VPX spécifique en fonction de ses besoins en matière de débit. Citrix ADC VPX est disponible dans les éditions Standard, Advanced et Premium. Citrix ADC VPX offre de 10 Mbps (VPX 10) à 100 Gbit/s (VPX 100G). Vous trouverez plus de détails dans la fiche technique Citrix ADC VPX.

Le prix de Citrix ADC VPX est-il le même pour tous les hyperviseurs ?

Oui.

Les mêmes SKU Citrix ADC sont-ils utilisés pour VPX sur tous les hyperviseurs ?

Oui.

Une licence Citrix ADC VPX peut-elle être déplacée d'un hyperviseur à un autre (par exemple de VMware vers Hyper-V) ?

Oui. Les licences Citrix ADC VPX sont indépendantes de l'hyperviseur sous-jacent. Si vous décidez de déplacer la machine virtuelle Citrix ADC VPX d'un hyperviseur vers un autre, vous n'avez pas besoin d'obtenir une nouvelle licence. Toutefois, il se peut que vous deviez réhéberger la licence Citrix ADC VPX existante.

Les instances Citrix ADC VPX peuvent-elles être mises à niveau ?

Oui. Les limites de débit et l'édition de la famille Citrix ADC peuvent être mises à niveau. Les SKU de mise à niveau pour les deux types de mise à niveau sont disponibles.

Si je souhaite déployer Citrix ADC VPX dans une paire haute disponibilité, de combien de licences ai-je besoin ?

Comme pour les appliances physiques Citrix ADC, une configuration haute disponibilité Citrix ADC nécessite deux instances actives. Par conséquent, le client doit acheter deux licences.

Citrix ADC VPX Express et essai gratuit de 90 jours

Est-ce que Citrix ADC VPX Express inclut toutes les fonctionnalités standard de Citrix ADC ? Est-ce qu'il inclut Citrix ADC Gateway et l'équilibrage de charge pour l'interface Web Citrix Virtual Apps (anciennement XenApp) et le courtier XML ?

Oui. Citrix ADC VPX Express inclut la fonctionnalité Citrix ADC Standard complète. À partir de la version 12.0—56.20 de Citrix ADC, Citrix a modifié le comportement de VPX Express.

Est-ce que Citrix ADC VPX Express inclut toutes les fonctionnalités standard de Citrix ADC ? Est-ce qu'il inclut Citrix ADC Gateway et l'équilibrage de charge pour l'interface Web Citrix Virtual Apps et le courtier XML ?

À partir de la version 12.0—56.20 de Citrix ADC, VPX Express offre l'ensemble des fonctionnalités Citrix ADC Standard Edition, à l'exception de la fonctionnalité Gateway. Avant la version 12.0—56.20, VPX Express inclut toutes les fonctionnalités de l'édition standard.

Est-ce que Citrix ADC VPX Express nécessite une licence ?

Avec la nouvelle version Citrix ADC VPX Express (12.0—56.20 et suivantes), VPX Express est gratuit et ne nécessite aucun fichier de licence à installer et est livré sans engagement. Si vous possédez déjà une licence VPX Express, le comportement VPX Express précédent est conservé. Si le *fichier de licence* VPX Express est supprimé et que les versions 12.0—56.20 et suivantes sont utilisées, le nouveau comportement VPX Express prend effet.

La licence Citrix ADC VPX Express expire ?

Avec le nouveau VPX Express, non. Il n'y a pas de licence ni de date d'expiration. Si vous possédez déjà une licence VPX Express, celle-ci expire un an après le téléchargement.

Est-ce que Citrix ADC VPX Express inclut les cinq licences simultanées Citrix ADC Gateway gratuites ?

Oui, si vous possédez une licence VPX Express.

Y a-t-il une limite au nombre de Citrix ADC VPX Express qu'un client peut télécharger ?

Cinq.

Citrix ADC VPX Express prend-il en charge les mêmes chiffrements de chiffrement que les appliances Citrix ADC MPX ?

Pour une disponibilité générale, tous les mêmes chiffrements à chiffrement fort pris en charge sur les appliances Citrix ADC sont disponibles sur Citrix ADC VPX et Citrix ADC VPX Express. Il est soumis aux mêmes réglementations en matière d'importation ou d'exportation.

Puis-je déposer des demandes de support technique pour Citrix ADC VPX Express ?

Non. Une licence Citrix ADC VPX commerciale telle que VPX-10, VPX-200, VPX-1000, VPX-3000 est nécessaire pour déposer des demandes de support technique. Toutefois, les utilisateurs de Citrix ADC VPX

Express sont libres d'utiliser à la fois le centre de connaissances Citrix ADC VPX et de demander de l'aide à la communauté via les forums de discussion Z.

Citrix ADC VPX Express peut-il être mis à niveau vers une version commerciale ?

Oui. Il suffit d'acheter la licence Citrix ADC VPX de détail dont vous avez besoin, puis d'appliquer la licence correspondante à l'instance Citrix ADC VPX Express.

Hyperviseur

Quelles sont les versions de VMware prises en charge par Citrix ADC VPX ?

Citrix ADC VPX prend en charge VMware ESX et ESXi pour les versions 3.5 ou ultérieures. Pour plus d'informations, consultez la matrice de support et les directives d'utilisation.

Pour VMware, combien d'interfaces réseau virtuelles pouvez-vous allouer à un VPX ?

Vous pouvez allouer jusqu'à 10 interfaces réseau virtuelles à un Citrix ADC VPX.

Depuis vSphere, comment pouvons-nous accéder à la ligne de commande Citrix ADC VPX ?

Le client VMware vSphere fournit un accès intégré à la ligne de commande Citrix ADC VPX via un onglet de console. En outre, vous pouvez utiliser n'importe quel client SSH ou Telnet pour accéder à la ligne de commande. Vous pouvez utiliser l'adresse NSIP du Citrix ADC VPX dans le client SSH ou Telnet.

Comment accéder à l'interface graphique Citrix ADC VPX ?

Pour accéder à l'interface graphique Citrix ADC VPX, tapez le NSIP du Citrix ADC VPX, par exemple, `http://NSIP address` dans le champ d'adresse de n'importe quel navigateur.

Deux instances Citrix ADC VPX installées sur le même VMware ESX peuvent-elles être configurées dans une configuration haute disponibilité ?

Oui, mais ce n'est pas recommandé. Une panne matérielle affecterait les deux instances Citrix ADC VPX.

Deux instances Citrix ADC VPX exécutées sur deux systèmes VMware ESX différents peuvent-elles être configurées dans une configuration haute disponibilité ?

Oui. Il est recommandé dans une configuration haute disponibilité.

Pour VMware, les événements liés à l'interface sont-ils pris en charge sur Citrix ADC VPX ?

Non. Les événements liés à l'interface ne sont pas pris en charge.

Pour VMware, les VLAN balisés sont-ils pris en charge sur Citrix ADC VPX ?

Oui. Les VLAN étiquetés Citrix ADC sont pris en charge sur Citrix ADC VPX à partir des versions 11.0 et supérieures. Pour plus d'informations, consultez la documentation Citrix.

Pour VMware, l'agrégation de liens et le LACP sont-ils pris en charge sur Citrix ADC VPX ?

Non. L'agrégation de liens et LACP ne sont pas pris en charge pour Citrix ADC VPX. L'agrégation de liens doit être configurée au niveau VMware.

Comment accéder à la documentation Citrix ADC VPX ?

La documentation est disponible à partir de l'interface graphique Citrix ADC VPX. Une fois connecté, sélectionnez l'onglet **Documentation** .

Planification ou dimensionnement des capacités

Quelles sont les performances auxquelles je peux m'attendre avec Citrix ADC VPX ?

Citrix ADC VPX offre de bonnes performances. Consultez la fiche technique Citrix ADC VPX pour connaître un niveau de performance spécifique atteignable à l'aide de Citrix ADC VPX.

Étant donné que la puissance du processeur du serveur varie, comment pouvons-nous estimer les performances maximales d'une instance Citrix ADC ?

L'utilisation d'un processeur plus rapide peut entraîner des performances supérieures (jusqu'au maximum autorisé par la licence), tandis que l'utilisation d'un processeur plus lent peut certainement limiter les performances.

La bande passante ou le débit de Citrix ADC VPX sont-ils limités pour le trafic entrant uniquement, ou pour le trafic entrant et sortant ?

Les limites de bande passante Citrix ADC VPX sont appliquées pour le trafic entrant vers Citrix ADC uniquement, qu'il s'agisse du trafic de demande ou de réponse. Il indique qu'un Citrix ADC VPX-1000 (par exemple) peut traiter simultanément 1 Gbit/s de trafic entrant et 1 Gbit/s de trafic sortant. Le trafic entrant et sortant n'est pas le même que le trafic de demande et de réponse. Pour Citrix ADC, le trafic provenant des points de terminaison (trafic de requête) et le trafic provenant des serveurs d'origine (trafic de réponse) est « entrant » (c'est-à-dire qu'il arrive dans Citrix ADC).

Plusieurs instances de Citrix ADC VPX peuvent-elles être exécutées sur le même serveur ?

Oui. Toutefois, assurez-vous que le serveur physique dispose d'une capacité de processeur et d'E/S suffisante pour prendre en charge la charge de travail totale exécutée sur l'hôte, sinon les performances de Citrix ADC VPX peuvent être affectées.

Si plusieurs instances de Citrix ADC VPX sont exécutées sur un serveur physique, quelle est la configuration matérielle minimale requise par instance Citrix ADC VPX ?

Chaque instance Citrix ADC VPX doit se voir allouer 2 Go de RAM physique, 20 Go d'espace disque et 2 vCPU.

Puis-je héberger Citrix ADC VPX et d'autres applications sur le même serveur ?

Oui. Par exemple, Citrix ADC VPX, Citrix Virtual Apps Web Interface et Citrix Virtual Apps XML Broker peuvent tous être virtualisés et peuvent s'exécuter sur le même serveur. Pour des performances optimales, assurez-vous que l'hôte physique dispose d'une capacité de processeur et d'E/S suffisante pour prendre en charge toutes les charges de travail en cours d'exécution.

L'ajout de cœurs de processeur à une seule instance Citrix ADC VPX augmentera-t-il les performances de cette instance ?

Selon la licence, une instance Citrix ADC VPX peut utiliser jusqu'à 4 vCPU aujourd'hui. L'ajout d'un processeur supplémentaire à une instance Citrix ADC VPX pouvant utiliser davantage de processeurs augmente les performances.

Pourquoi Citrix ADC VPX semble consommer plus de 90 % du processeur même s'il est inactif ?

Il s'agit d'un comportement normal et les appliances Citrix ADC présentent le même comportement. Pour voir l'étendue réelle de l'utilisation du processeur Citrix ADC VPX, utilisez la commande stat CPU dans l'interface de ligne de commande Citrix ADC ou affichez l'utilisation du processeur Citrix ADC VPX à partir de l'interface graphique Citrix ADC. Le moteur de traitement des paquets Citrix ADC est toujours « à la recherche de travail », même s'il n'y a pas de travail à faire. Par conséquent, il fait tout pour prendre le contrôle de la CPU et ne pas le libérer. Sur un serveur installé avec Citrix ADC VPX et rien d'autre, cela donne l'impression (du point de vue de l'hyperviseur) que Citrix ADC VPX consomme l'intégralité du processeur. En examinant l'utilisation du processeur depuis « à l'intérieur de Citrix ADC » (à l'aide de l'interface de ligne de commande ou de l'interface graphique), vous pouvez obtenir une image de la capacité CPU Citrix ADC VPX utilisée.

Configuration système requise

Quelle est la configuration matérielle minimale requise pour Citrix ADC VPX ?

Consultez la fiche technique Citrix ADC VPX pour connaître sa configuration système requise.

Citrix ADC VPX nécessite :

- Configuration requise du processeur : serveur double cœur avec Intel VT-x.
- Mémoire disponible : 2 Go de RAM (4 Go si VPX fonctionne sur le firmware 13.0), disque dur de 20 Go.
- Hyperviseur : Citrix Hypervisor 5.6 ou version ultérieure ; VMware ESX/ESXi 3.5 ou version ultérieure, Windows Server 2008 R2 avec Hyper-V.
- Connectivité : 100 Mbps minimum. 1 Gbps recommandé.
- Une carte réseau compatible avec l'hyperviseur.

> **Remarque**
>
> À partir de la version 13.1 de Citrix ADC, l'instance Citrix ADC VPX sur l'hyperviseur VMware ESXi prend en charge les processeurs AMD.

Qu'est-ce qu'Intel VT-x ?

Ces fonctionnalités, parfois appelées « assistance matérielle » ou « assistance à la virtualisation », interceptent les instructions du processeur sensibles ou privilégiées exécutées par le système d'exploitation invité vers l'hyperviseur. Cela simplifie l'hébergement des OS invités (BSD pour un Citrix ADC VPX) sur l'hyperviseur.

Quelle est la commune de VT-x ?

Pratiquement, tous les serveurs livrés au cours des deux dernières années peuvent prendre en charge VT-x. De nombreux serveurs sont livrés avec l'aide à la virtualisation désactivée dans le BIOS. Avant de supposer que vous ne pouvez pas exécuter Citrix ADC VPX, vérifiez si vous devez modifier ce paramètre sur le serveur.

Existe-t-il une liste de compatibilité matérielle (HCL) pour Citrix ADC VPX ?

Tant que le serveur prend en charge Intel VT-x, Citrix ADC VPX doit s'exécuter sur n'importe quel serveur compatible avec l'hyperviseur sous-jacent. Consultez la HCL de l'hyperviseur pour obtenir une liste complète des plates-formes prises en charge.

Sur quelle version du système d'exploitation Citrix ADC est basé Citrix ADC VPX ?

Citrix ADC VPX est basé sur Citrix ADC 9.1 ou versions ultérieures.

Comme Citrix ADC VPX fonctionne sous BSD, peut-il être exécuté en mode natif sur un serveur sur lequel BSD Unix est installé ?

Non. Citrix ADC VPX nécessite l'exécution de l'hyperviseur. La prise en charge détaillée des hyperviseurs se trouve dans la fiche technique Citrix ADC VPX.

Autres FAQ techniques

L'agrégation de liens sur un serveur physique avec plusieurs cartes réseau fonctionne-t-elle ?

LACP n'est pas pris en charge. Pour Citrix Hypervisor, l'agrégation de liens statiques est prise en charge et est limitée à quatre canaux et sept interfaces virtuelles. Pour VMware, l'agrégation de liens statiques n'est pas prise en charge dans Citrix ADC VPX, mais peut être configurée au niveau de VMware.

Le transfert basé sur MAC (MBF) est-il pris en charge sur VPX ? Y a-t-il un changement par rapport à l'implémentation de l'appliance Citrix ADC ?

MBF est pris en charge et se comporte de la même manière qu'avec l'appliance Citrix ADC. L'hyperviseur bascule essentiellement tous les paquets reçus de Citrix ADC VPX vers l'extérieur et inversement.

Comment se déroule le processus de mise à niveau Citrix ADC VPX ?

Les mises à niveau sont effectuées de la même manière que pour les appliances Citrix ADC : téléchargez un fichier noyau et utilisez install ns ou l'utilitaire de mise à niveau dans l'interface graphique.

Comment sont alloués la mémoire flash et l'espace disque ? Pouvons-nous le changer ?

/flash = 965M
/var = 14G
Un minimum de 2 Go de mémoire doit être alloué à chaque instance Citrix ADC VPX. L'image disque Citrix ADC VPX a été dimensionnée à 20 Go à des fins de maintenance, telles que l'espace pour la prise et le stockage de vidages de mémoire allant jusqu'à 4 Go, ainsi que les fichiers journaux et traces. Bien qu'il soit possible de générer une image disque plus petite, il n'est pas prévu de le faire actuellement. /flash et /var sont tous deux dans la même image disque. Ils sont conservés sous forme de systèmes de fichiers distincts à des fins de compatibilité.
Pour obtenir des recommandations détaillées sur l'allocation de mémoire, reportez-vous à la fiche technique Citrix ADC VPX.

Que pouvons-nous espérer considérer la numérotation de build NetScaler VPX et l'interopérabilité avec d'autres versions ?

La numérotation de version de Citrix ADC VPX est similaire à celle de la version 9.1. Cl (classique) et 9.1. Version de Nc (nCore), par exemple 9.1_97.3.vpx, 9.1_97.3.nc et 9.1_97.3.cl.

Le Citrix ADC VPX peut-il faire partie d'une configuration haute disponibilité avec une appliance Citrix ADC ?

Configuration non prise en charge.

Toutes les interfaces visibles dans Citrix ADC VPX sont-elles directement liées au nombre d'interfaces sur l'hyperviseur ?

Non. Vous pouvez ajouter jusqu'à sept interfaces (10 pour VMware) via l'utilitaire de configuration Citrix ADC VPX avec une seule carte réseau physique sur l'hyperviseur.

Est-ce que Citrix Hypervisor XenMotion ou VMware VMotion ou Hyper-V Live Migration peut être utilisé pour déplacer des instances actives de Citrix ADC VPX ?

Citrix ADC VPX ne prend pas en charge la migration en direct XenMotion ou Hyper-V. VMotion est pris en charge à partir de la version 12.1 de Citrix ADC. Pour plus d'informations, consultez Notes de publication.

Présentation du système de licences

October 5, 2021

Citrix propose un large éventail d'éditions de produits et de modèles de licences pour les appliances MPX et VPX, afin de répondre aux besoins de votre entreprise.

Pour que l'appliance Citrix ADC fonctionne correctement, elle doit posséder l'une des licences Citrix ADC Family Edition. La gamme de produits ADC comprend trois éditions familiales :

- Édition Standard
- Édition Advanced
- Édition Premium

Pour plus d'informations, consultez la fiche technique Citrix ADC.

Après avoir sélectionné l'édition Citrix ADC, vous pouvez sélectionner l'une des offres de licences MPX et VPX. Sur la base de critères tels que perpétuel et abonnement (abonnement annuel et horaire), vCPU et bande passante, sur site et dans le cloud, etc.

Licences Citrix ADC VPX

Les licences suivantes sont spécifiques à VPX.

Licence Citrix ADC VPX Express

À partir de Citrix ADC version 12.0 56.20, VPX Express pour les déploiements sur site et dans le cloud ne nécessite pas de fichier de licence et est livré avec les fonctionnalités suivantes :

- Bande passante 20 Mbps
- Toutes les fonctionnalités de licence standard ADC, à l'exception de Citrix Gateway et des défenses L4 et L7
- 250 sessions SSL maximum
- Débit SSL de 20 Mbps

Vous pouvez mettre à niveau la licence VPX Express vers les deux options suivantes :

1. Une licence Citrix ADC VPX autonome
2. Licence Citrix ADC Pooled Capacity pour les instances VPX. Pour plus d'informations, consultez Citrix ADC Pooled Capacity.

> **Important**
>
> Le clustering est disponible dans l'édition Standard pour le cloud public VPX et dans la licence VPX Express.

Licence de capacité groupée Citrix ADC VPX

Vous pouvez utiliser Citrix Application Delivery Management (ADM) pour créer un cadre de licence comprenant une bande passante et un pool d'instances communs. Pour obtenir des informations complètes, reportez-vous à la section Capacité groupée Citrix ADC.

Ressources connexes

Système de licences Citrix

Comment allouer des licences Citrix ADC VPX

Licence VPX sur le cloud

Le déploiement VPX est pris en charge sur des fournisseurs de cloud public tels qu'Azure, AWS et Google. Pour plus d'informations, consultez les documents suivants :

- Licence VPX-Azure

- Licence VPX-AWS
- Licence VPX-GCP

Attribuer et appliquer une licence

October 5, 2021

Dans l'interface graphique Citrix MPX et VPX ADC, vous pouvez utiliser votre numéro de série matériel (HSN) ou votre code d'accès de licence pour allouer vos licences. Si une licence est déjà présente sur votre ordinateur local, vous pouvez également la télécharger sur la solution matérielle-logicielle.

Pour toutes les autres fonctionnalités, telles que le retour ou la réallocation de votre licence, vous devez utiliser le portail de licences. Le cas échéant, vous pouvez toujours utiliser le portail de licences pour l'allocation de licences. Pour plus d'informations, voir Utiliser la gestion des licences dans My Account sur citrix.com.

Guide de gestion des licences Citrix

Le guide de licences Citrix couvre également des informations sur l'installation de licences dans une appliance Citrix ADC et l'installation de licences dans d'autres produits Citrix. Pour plus d'informations, consultez Citrix Licensing Guide.

Conditions préalables

> **Remarque**
>
> Achetez des licences distinctes pour chaque appliance dans une paire haute disponibilité. Assurez-vous que les mêmes types de licences sont installés sur les deux appliances. Par exemple, si vous achetez une licence Premium pour une appliance, vous devez acheter une autre licence Premium pour l'autre appliance.

Pour utiliser le numéro de série du matériel ou le code d'accès de licence pour allouer vos licences :

- Vous devez être en mesure d'accéder aux domaines publics via la solution matérielle-logicielle. Par exemple, la solution matérielle-logicielle doit pouvoir accéder à www.citrix.com. Le logiciel d'allocation de licence accède en interne au portail de licences Citrix pour votre licence. Pour accéder à un domaine public :
  - Utilisez un serveur proxy ou configurez un serveur DNS.
  - Configurez une adresse IP Citrix ADC (NSIP) ou une adresse IP de sous-réseau (SNIP) sur votre appliance Citrix ADC.

- Votre licence doit être liée à votre matériel ou vous devez disposer d'un code d'accès à la licence valide. Citrix envoie votre code d'accès à la licence par e-mail lorsque vous achetez une licence.

Attribuer une licence à l'aide de l'interface graphique

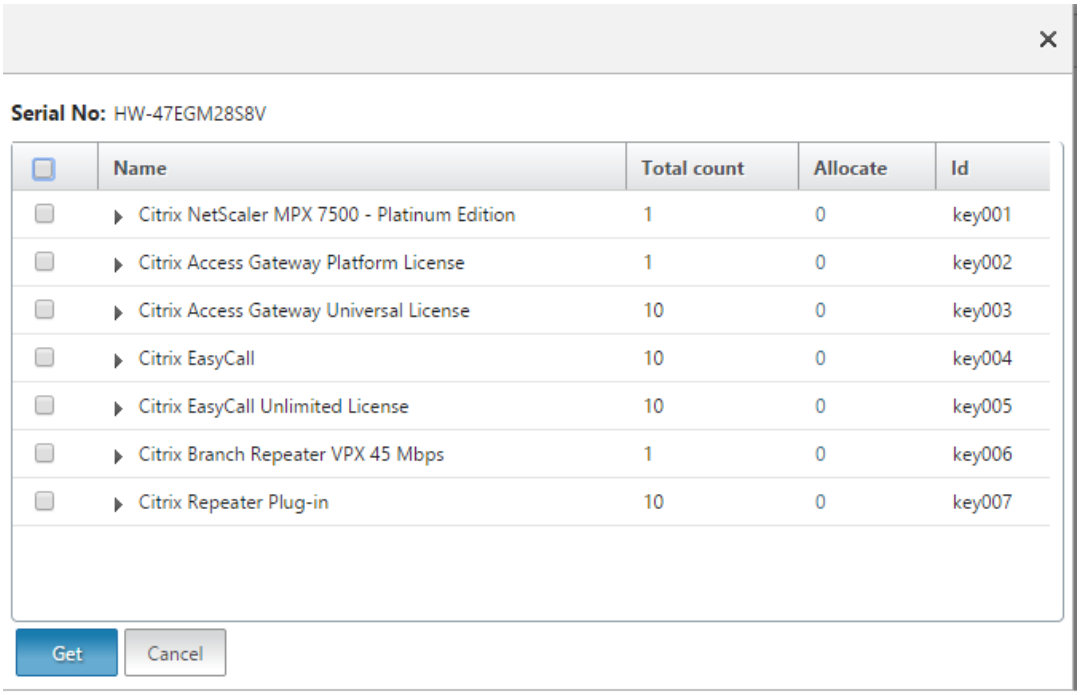
Si votre licence est déjà liée à votre matériel, le processus d'attribution des licences peut utiliser le numéro de série du matériel. Sinon, vous devez entrer le code d'accès à la licence.

Vous pouvez allouer partiellement des licences selon les besoins de votre déploiement. Par exemple, si votre fichier de licences contient 10 licences, mais que vos besoins actuels ne concernent que six licences, vous pouvez allouer six licences maintenant et en attribuer d'autres ultérieurement. Vous ne pouvez pas allouer plus de licences que le nombre total de licences présentes dans votre fichier de licences.

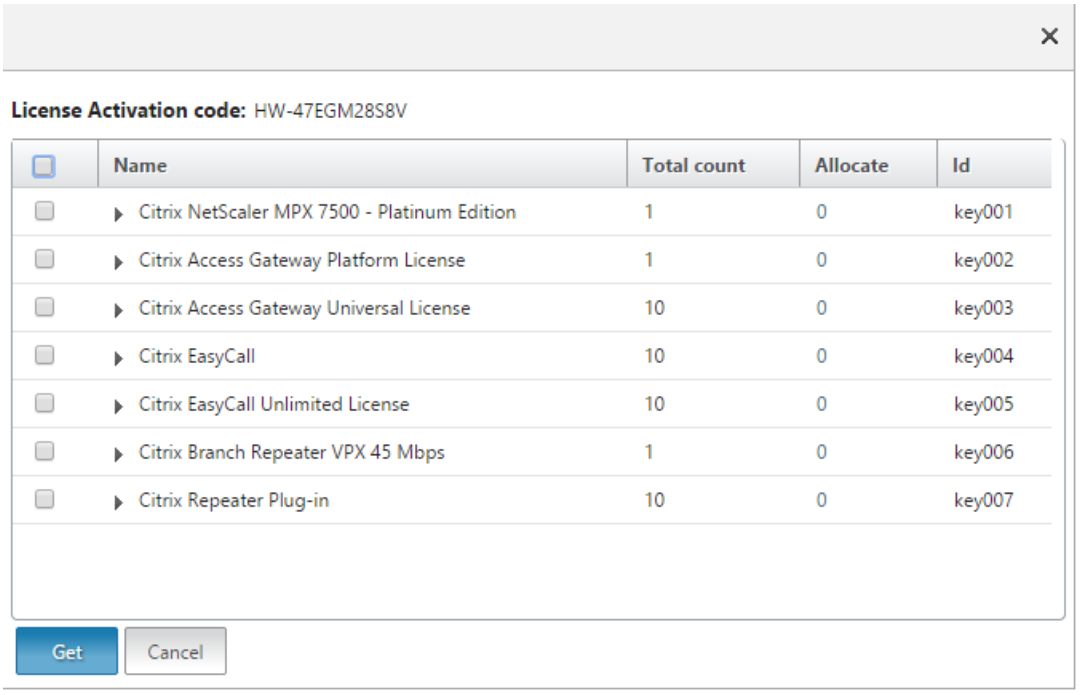
Pour attribuer votre licence

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix ADC (par exemple, `http://192.168.100.1`).
2. Dans Nom d'utilisateur et Mot de passe, tapez les informations d'identification de l'administrateur.
3. Sous l'onglet **Configuration**, accédez à **Système > Licences**.
4. Dans le volet d'informations, cliquez sur **Gérer les licences**, cliquez sur **Ajouter une nouvelle licence**, puis sélectionnez l'une des options suivantes :
   - **Utiliser le numéro de série** : Le logiciel récupère en interne le numéro de série de votre solution matérielle-logicielle et utilise ce numéro pour afficher vos licences.
   - **Utiliser le code d'accès à**la licence : Citrix envoie par e-mail le code d'accès à la licence que vous avez achetée. Entrez le code d'accès à la licence dans la zone de texte.

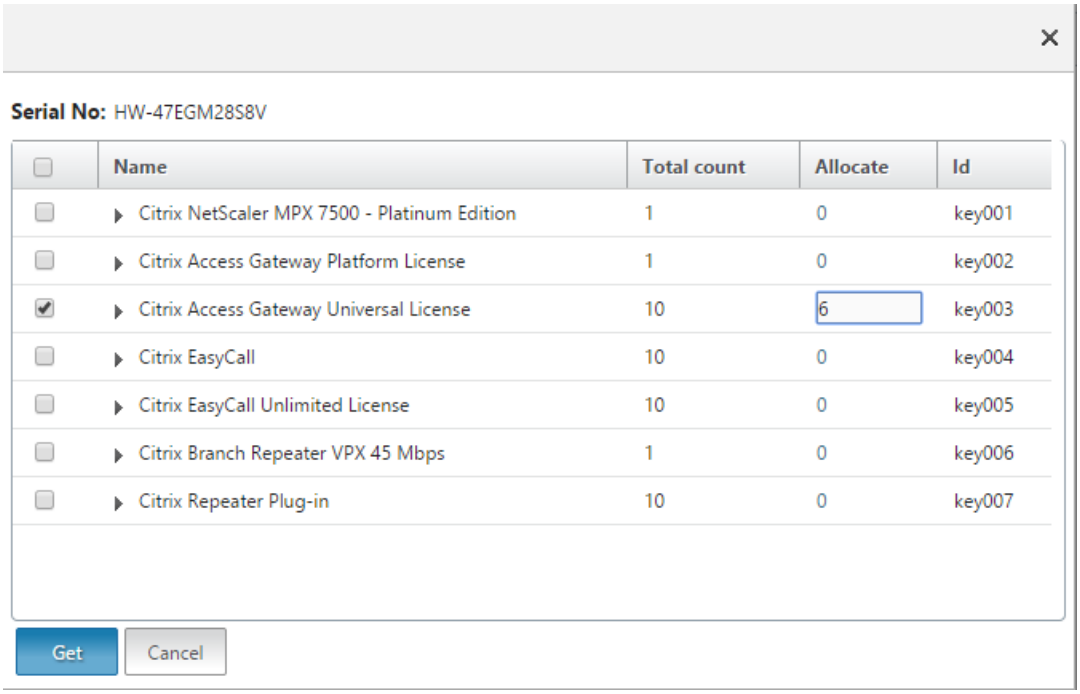
     Si vous ne souhaitez pas configurer la connectivité Internet sur l'appliance Citrix ADC, vous pouvez utiliser un serveur proxy. Activez la case à cocher **Connect through Proxy Server** et spécifiez l'adresse IP et le port de votre serveur proxy.
5. Cliquez sur **Obtenir licences**. Selon l'option sélectionnée, l'une des boîtes de dialogue suivantes s'affiche.
   - La boîte de dialogue suivante s'affiche si vous avez sélectionné Numéro de série matériel.



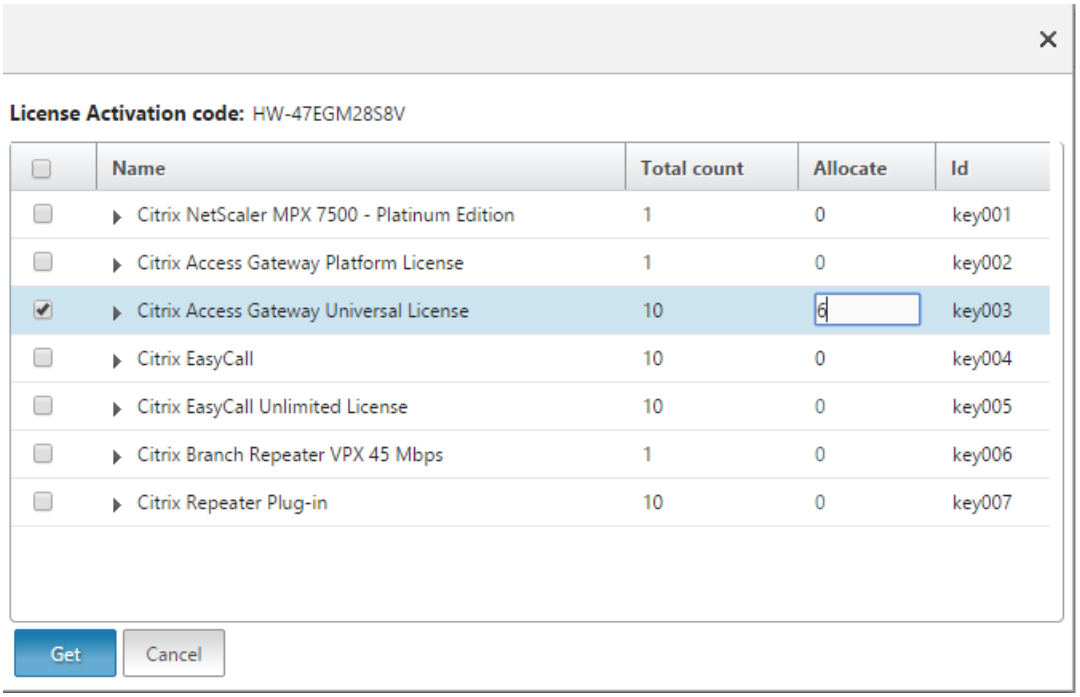
- La boîte de dialogue suivante apparaît si vous avez sélectionné un code d'accès à la licence.



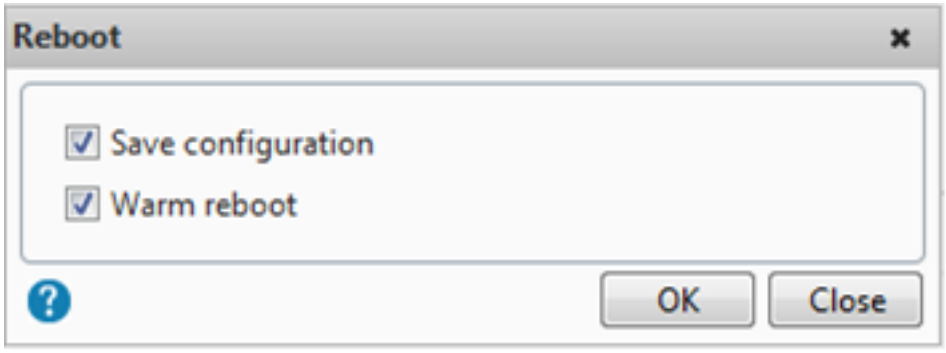
6. Sélectionnez le fichier de licences que vous souhaitez utiliser pour allouer vos licences.
7. Dans la colonne **Allocate**, saisissez le nombre de licences à allouer. Cliquez ensuite sur **Obtenir**.
   - Si vous avez sélectionné **Numéro de série matériel**, saisissez le nombre de licences, comme indiqué dans la capture d'écran suivante.



- Si vous avez sélectionné le **code d'accès aux licences**, saisissez le nombre de licences, comme indiqué dans la capture d'écran suivante.



8. Cliquez sur Redémarrer pour que la licence soit appliquée.
9. Dans la boîte de dialogue de redémarrage, cliquez sur **OK** pour poursuivre les modifications, ou cliquez sur **Fermer** pour annuler les modifications.



Installer une licence

Si vous avez téléchargé votre fichier de licence sur votre ordinateur local en accédant au portail de licences, vous devez télécharger la licence sur l'appliance.

Pour installer un fichier de licence à l'aide de l'interface graphique

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix ADC (par exemple, `http://192.168.100.1`).
2. Dans Nom d'utilisateur et Mot de passe, tapez les informations d'identification de l'administrateur.
3. Dans l'onglet **Configuration**, accédez à Licences système.
4. Dans le volet d'informations, cliquez sur **Gérer les licences**.
5. Cliquez sur **Ajouter une nouvelle licence**, puis sélectionnez **Charger fichier de licences depuis un ordinateur local**.
6. Cliquez sur **Parcourir**. Accédez à l'emplacement des fichiers de licence, sélectionnez le fichier de licences, puis cliquez sur **Ouvrir**.
7. Cliquez sur Redémarrer pour appliquer la licence.
8. Dans la boîte de dialogue de redémarrage, cliquez sur **OK** pour poursuivre les modifications, ou cliquez sur **Fermer** pour annuler les modifications.

Pour installer les licences à l'aide de l'interface de ligne de commande

1. Ouvrez une **connexion SSH** à l'appliance ADC à l'aide d'un client SSH, tel que PuTTY.
2. Ouvrez une session sur l'appliance ADC à l'aide des informations d'identification de l'administrateur.
3. Passez à l'invite du shell, créez un sous-répertoire de licences dans le `nsconfig` répertoire, s'il n'existe pas, et copiez un ou plusieurs nouveaux fichiers de licences dans ce répertoire.

   Exemple

   ```
   1 login: nsroot
   ```



```
Password: nsroot
Last login: Mon Aug  4 03:37:27 2008 from 10.102.29.9
Done
> shell
Last login: Mon Aug  4 03:51:42 from 10.103.25.64
root@ns# mkdir /nsconfig/license
root@ns# cd /nsconfig/license
<!--NeedCopy-->
```

Copiez un ou plusieurs nouveaux fichiers de licence dans ce répertoire.

> **Remarque**
>
> L'appliance Citrix ADC ne demande pas d'option de redémarrage lorsque vous utilisez l'interface de ligne de commande pour installer les licences. Exécutez la commande reboot -w pour redémarrer à chaud le système ou exécutez la commande de redémarrage pour redémarrer le système normalement.

Vérifier les fonctionnalités sous licence

Avant d'utiliser une fonctionnalité, assurez-vous que votre licence prend en charge cette fonctionnalité.

Pour vérifier les fonctionnalités sous licence à l'aide de l'interface de ligne de commande

1. Ouvrez une **connexion SSH** à l'appliance ADC à l'aide d'un client SSH, tel que PuTTY.
2. Ouvrez une session sur l'appliance ADC à l'aide des informations d'identification de l'administrateur.
3. À l'invite de commandes, entrez la commande sh ns license pour afficher les fonctionnalités prises en charge par la licence.

   Exemple

```
sh ns license
        License status:
                            Web Logging: YES
                      Surge Protection: YES
                        .......

                        Responder: YES
 Done
<!--NeedCopy-->
```


Pour vérifier les fonctionnalités sous licence à l'aide de l'interface graphique

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance ADC, par exemple `http://192.168.100.1`.
2. Dans Nom d'utilisateur et Mot de passe, tapez les informations d'identification de l'administrateur.
3. Indiquez le nom d'utilisateur et le mot de passe, puis cliquez sur **Connexion**.
4. Dans le volet de navigation, développez **Système**, puis cliquez sur **Licences**. Une coche verte s'affiche en regard des fonctionnalités sous licence.

Activer ou désactiver une fonctionnalité

Lorsque vous utilisez l'appliance Citrix ADC pour la première fois, vous devez activer une fonctionnalité avant de pouvoir l'utiliser. Si vous configurez une fonctionnalité avant qu'elle ne soit activée, un message d'avertissement s'affiche. La configuration est enregistrée, mais elle ne s'applique qu'une fois la fonctionnalité activée.

Pour activer une fonctionnalité à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer une fonctionnalité et vérifier la configuration :

- fonctionnalité d'activation <FeatureName>
- Afficher la fonctionnalité

Exemple

```
enable feature lb cs
done
 >show feature

        Feature                       Acronym
           Status
        -------                       -------
           ------
 1)     Web Logging                   WL                    OFF
 2)     Surge Protection              SP                    ON
 3)     Load Balancing                LB                    ON
 4)     Content Switching             CS                    ON
 5)     Cache Redirection             CR                    ON
 .
 .
 .
 24)    NetScaler Push                push                  OFF
 Done
```



```
<!--NeedCopy-->
```

L'exemple montre comment activer l'équilibrage de charge (lb) et la commutation de contenu (cs).

Si la clé de licence n'est pas disponible pour une fonctionnalité particulière, le message d'erreur suivant s'affiche pour cette fonctionnalité :

ERREUR : fonctionnalités non concédées sous licence

Remarque : Pour activer une fonctionnalité facultative, vous devez disposer d'une licence spécifique à cette fonctionnalité. Par exemple, vous avez acheté et installé la licence Citrix NetScaler Advanced Edition. Toutefois, pour activer la fonctionnalité de mise en cache intégrée, vous devez acheter et installer la licence AppCache.

Pour désactiver une fonctionnalité à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour désactiver une fonctionnalité et vérifier la configuration :

- fonctionnalité de désactivation <FeatureName>
- Afficher la fonctionnalité

Exemple

L'exemple suivant montre comment désactiver l'équilibrage de charge (LB).

```
> disable feature lb
 Done
> show feature

        Feature                       Acronym
           Status
        -------                       -------
           ------
 1)     Web Logging                   WL                    OFF
 2)     Surge Protection              SP                    ON
 3)     Load Balancing                LB                    OFF
 4)     Content Switching             CS                    ON
 .
 .
 .
 24)    NetScaler Push                push                  OFF
 Done
>
<!--NeedCopy-->
```


Vérifier les informations d'expiration de la licence

Vous pouvez vérifier les informations d'expiration des licences Citrix ADC via l'interface graphique ou l'interface de ligne de commande.

Pour vérifier les informations d'expiration de licence Citrix ADC via l'interface graphique :

Accédez à **Configuration > Système > Licences**.

Une alerte graphique apparaît lorsque la date d'expiration de la licence ADC est inférieure ou égale à 30 jours.

Pour vérifier les informations d'expiration de la licence via l'interfacede ligne de commande :

Tapez la commande « show ns license ».

```
> sh license
    License status:

    Web Logging: YES
    Surge Protection: YES

    Web Logging: YES
    Surge Protection: YES

    ...

Days to expiry: 204

Done
```



```
15 >
16 <!--NeedCopy-->
```

Une fois la licence expirée, l'appliance Citrix ADC génère une alarme SNMP « NS_LICENSE_EXPIRY » et un événement d'expiration est enregistré dans une console.

À l'expiration de la licence, l'appliance Citrix ADC redémarre automatiquement pour révoquer la licence. Si une appliance Citrix ADC utilise des licences Citrix Service Provider (CSP), l'appliance ne redémarre pas automatiquement pour révoquer la licence. Toutefois, si l'utilisateur redémarre la solution matérielle-logicielle, elle redémarre sans licence.

Mise à niveau d'une licence

Vous pouvez mettre à niveau un dispositif Citrix ADC d'une édition familiale à une autre et d'une plage de capacité à une autre en achetant une licence de capacité supérieure.

Les mises à niveau sont de deux types :

- Mises à niveau de l'édition : Standard vers Advanced, Standard to Premium et Advanced to Premium. Les mises à niveau de l'édition doivent être à l'intérieur de la même bande passante.
- Mises à niveau de capacité : vous pouvez passer d'une capacité inférieure à une capacité supérieure, à la fois pour le vCPU et la bande passante. Les mises à niveau de capacité ne peuvent être effectuées que sur la même édition (Standard, Advanced ou Premium).

Si vous souhaitez mettre à niveau la capacité et l'édition, commencez par mettre à niveau la capacité, redémarrez l'appliance, puis mettez à niveau l'édition.

Exemple : Pour mettre à niveau une licence VPX 10 Mbps Standard Edition vers VPX 200 Mbps Premium Edition, la mise à niveau doit être effectuée en deux étapes.

- Mise à niveau VPX de 10 Mbps Standard Edition à 200 Mbps Standard Edition.
- Mise à niveau VPX de 200 Mbps Standard Edition à 200 Mbps Premium Edition.

> Remarque
>
> Vous pouvez utiliser Citrix Application Delivery Management (ADM) pour créer un cadre de licence comprenant une bande passante et un pool d'instances communs. Pour obtenir des informations complètes, reportez-vous à la section Capacité groupée Citrix ADC.

Ressources connexes

- Système de licences Citrix
- Comment allouer des licences Citrix ADC VPX

Gouvernance des données

August 20, 2021

Qu'est-ce que Citrix ADM service connect ?

La connexion du service ADM (Application Delivery Management) Citrix est une fonctionnalité permettant l'intégration transparente des instances Citrix ADC MPX, SDX et VPX, et des appliances Citrix Gateway sur le service Citrix ADM. Cette fonctionnalité permet à l'instance Citrix ADC ou à l'appliance Citrix Gateway automatiquement, de se connecter en toute sécurité au service Citrix ADM et de lui envoyer des données système, d'utilisation et de télémétrie. Sur la base de ces données, vous obtenez des informations et des recommandations pour votre infrastructure Citrix ADC sur le service Citrix ADM.

En utilisant la fonctionnalité de connexion du service Citrix ADM et en intégration de vos instances Citrix ADC ou des appliances Citrix Gateway au service Citrix ADM. Vous pouvez également gérer toutes vos ressources Citrix ADC et Citrix Gateway, que ce soit sur site ou dans le cloud. En outre, vous bénéficiez d'un accès à un ensemble riche de fonctionnalités de visibilité qui aident à identifier rapidement les problèmes de performances, l'utilisation élevée des ressources, les erreurs critiques, etc. Le service Citrix ADM offre un large éventail de fonctionnalités pour vos instances et applications Citrix ADC. Pour plus d'informations sur le service Citrix ADM, consultez Citrix Application Delivery Management Service.

> **Important**
>
> - L'appliance Citrix Gateway prend également en charge la fonctionnalité de connexion du service Citrix ADM. Pour plus de facilité, l'appliance Citrix Gateway n'est pas explicitement appelée dans les sections consécutives.

Qu'est-ce que le service Citrix ADM ?

Le service Citrix ADM est une solution basée sur le cloud qui vous aide à gérer, surveiller, orchestrer, automatiser et dépanner vos instances Citrix ADC. Il vous fournit également des informations analytiques et des recommandations basées sur l'apprentissage automatique sur les instances Citrix ADC et sur l'intégrité, les performances et la sécurité des applications. Pour plus d'informations, reportez-vous à la section Présentation du service Citrix ADM.

Comment la connexion du service Citrix ADM est-elle activée ?

La connexion du service Citrix ADM est activée par défaut, après avoir installé ou mis à niveau Citrix ADC ou Gateway vers la version 13.0 build 61.xx et supérieure.

Quelles données sont capturées à l'aide du service Citrix ADM connect ?

Les détails suivants sont capturés à l'aide de Citrix ADM service connect :

- **Détails Citrix ADC**
  - ID de série
  - Identifiant de série codé
  - ID d'hôte
  - UUID
  - Adresse IP de gestion
  - Nom d'hôte
  - Version
  - Type de construction
  - Créer
  - Type de licence
  - Hyperviseur
  - Type de déploiement (Standalone/HA)
  - Type de plate-forme
  - Description de la plateforme
  - ID système
  - Modes activés sur ADC
  - Fonctionnalités activées sur ADC
- **Informations sur la licence**
  - Fonctionnalités sous licence sur Citrix ADC
  - Numéro de licence
- **Principales mesures d'utilisation**
  - Date système heure
  - Pourcentage d'utilisation de l'UC
  - Pourcentage du processeur de gestion
  - Débit
  - Nouvelles sessions SSL
  - Débit de chiffrement SSL
  - Débit de déchiffrement SSL
  - Temps de disponibilité du système
- **Configuration**
  - fichier ns.conf

> **Remarque**
>
> Avant que le service Citrix ADM connect envoie le `ns.conf` fichier de l'appliance Citrix ADC au service Citrix ADM, il anonyme les mots de passe chiffrés ou hachés. Le service Citrix ADM connect vérifie les paramètres « -crypted » ou « -passcrypt » et remplace la valeur chiffrée ou hachée associée par 'XXXX'. Le service Citrix ADM se connecte ensuite encode et compresse le `ns.conf` fichier, puis l'envoie au point de terminaison du service Citrix ADM.

- **Détails des erreurs critiques**
  - Défaillances du disque dur
  - Défaillances de la carte SSL
  - Pannes d'alimentation (bloc d'alimentation)
  - Défaillance du lecteur flash
  - Redémarrage à chaud
  - Utilisation soutenue de la mémoire supérieure à 90 % ou fuite de mémoire
  - baisse soutenue de la limite de débit

Comment les données sont-elles utilisées ?

En collectant les données, Citrix peut vous fournir des informations détaillées et opportunes sur vos installations Citrix ADC, notamment :

- **Principales mesures**. Détails des principales mesures concernant le processeur, la mémoire, le débit, le débit SSL et mettent en évidence un comportement anormal sur les instances Citrix ADC.
- **Erreurs critiques**. Toutes les erreurs critiques qui ont pu se produire sur vos instances Citrix ADC.
- **Avis de déploiement**. Identifiez les instances Citrix ADC déployées en mode autonome, mais qui présentent un débit élevé et sont vulnérables à un point de défaillance unique.

Combien de temps les données collectées sont-elles conservées ?

Les données collectées ne sont pas conservées plus de 13 mois.

Si vous décidez de mettre fin à l'utilisation du service en désactivant la fonctionnalité de connexion du service Citrix ADM depuis Citrix ADC, toutes les données collectées précédemment sont supprimées après une période de 30 jours.

Où sont stockées les données et dans quelle mesure sont-elles sécurisées ?

Toutes les données collectées par le service Citrix ADM connect sont stockées dans l'une des trois régions, soit les États-Unis, l'Union européenne et l'Australie et la Nouvelle-Zélande (ANZ). Pour plus

d'informations, voir Considérations géographiques.

Les données sont stockées en toute sécurité avec une isolation stricte des locataires au niveau de la couche de base de données.

Comment désactiver Citrix ADM service connect ?

Si vous souhaitez désactiver la collecte de données via Citrix ADM Service Connect, consultez Comment activer et désactiver Citrix ADM Service Connect.

Présentation du service Citrix ADM connect pour les appliances Citrix ADC

August 20, 2021

Le service Citrix ADM est une solution basée sur le cloud qui vous aide à gérer, surveiller, orchestrer, automatiser et dépanner vos instances Citrix ADC. Il fournit également des informations analytiques et des recommandations basées sur l'apprentissage automatique pour la santé, les performances et la sécurité de vos applications. Pour plus d'informations, consultez Citrix Application Delivery Management Service.

La connexion du service ADM (Application Delivery Management) Citrix est une fonctionnalité permettant l'intégration transparente des instances Citrix ADC sur le service Citrix ADM. Cette fonctionnalité aide les instances Citrix ADC et le service Citrix ADM à fonctionner comme une solution holistique, offrant aux clients des avantages multiples.

La fonctionnalité de connexion du service ADM Citrix permet à l'instance Citrix ADC de se connecter automatiquement au service Citrix ADM et lui envoyer des données système, d'utilisation et de télémétrie. Sur la base de ces données, le service Citrix ADM vous fournit des informations et des recommandations sur votre infrastructure Citrix ADC et Gateway, comme les suivantes :

- Informations sur les conseils de sécurité mettant en évidence vos appliances ADC vulnérables.
- Mise à niveau des informations consultatives mettant en évidence les appliances ADC qui ont atteint ou sont sur le point d'atteindre la fin de la maintenance et la fin de vie.
- Identification rapide des problèmes de performances, de l'utilisation élevée des ressources et des erreurs critiques.

Pour exploiter la puissance du service Citrix ADM, vous pouvez choisir d'embarquer vos instances Citrix ADC au service Citrix ADM. Le processus d'intégration utilise ADM Service Connect et rend l'expérience fluide et plus rapide pour vous.

> **Points à noter**
>
> - La connexion du service Citrix ADM est désormais disponible sur les instances Citrix ADC MPX, SDX et VPX et sur les appliances Citrix Gateway.
> - L'initiative du service Citrix ADM qui utilise cette fonctionnalité de connexion au service Citrix ADM est l'intégration low touch basée sur ADM Service Connect. Pour plus d'informations, consultez la section Intégration basse pression des instances Citrix ADC à l'aide de Citrix ADM Service connect.

Pour plus d'informations, voir Gouvernance des données.

> **Important**
>
> Citrix ADM Service Connect ne parvient pas à collecter les données de la sonde et ne peut pas aider à intégrer l'appliance ADC au service ADM si les conditions suivantes sont remplies :
>
> - `NSinternal` le compte utilisateur est désactivé.
> - La clé publique SSH n'est pas configurée.
>
> Pour surmonter le scénario précédent, Citrix vous recommande de suivre l'une des opérations suivantes :
>
> - Activez le compte `internaluser` d'utilisateur à l'aide du `set ns param -internaluserlogin ENABLED`.
> - Configurez l'authentification par clé publique. Pour plus d'informations, voir Accès à une appliance Citrix ADC à l'aide de clés SSH et sans mot de passe.

Comment le service Citrix ADM se connecte-t-il au service Citrix ADM ?

Voici un flux de travail de haut niveau sur la façon dont la fonctionnalité de connexion du service Citrix ADM sur Citrix ADC interagit avec le service Citrix ADM.

1. La fonctionnalité de connexion du service ADM Citrix sur l'appliance Citrix ADC se connecte automatiquement au service Citrix ADM à l'aide d'une demande de sonde périodique.
2. Cette demande contient des données système, d'utilisation et de télémétrie, à l'aide desquelles le service Citrix ADM vous fournit des informations et des recommandations sur votre infrastructure Citrix ADC. Comme ; identification rapide des problèmes de performances, une utilisation élevée des ressources et des erreurs critiques.
3. Vous pouvez consulter les informations et les recommandations et décider d'embarquer vos instances ADC au service Citrix ADM pour commencer à gérer vos instances Citrix ADC.
4. Lorsque vous décidez d'intégrer, la fonctionnalité de connexion du service Citrix ADM aide à effectuer l'intégration en toute transparence.

Sur quelles versions de Citrix ADC est prise en charge par Citrix ADM service connect ?

La connexion du service Citrix ADM est prise en charge sur toutes les plates-formes Citrix ADC et tous les modèles d'appliance (MPX, VPX et SDX). À partir de Citrix ADC version 13.0 build 61.xx, Citrix ADM service connect est activée par défaut pour les appliances Citrix ADC.

Comment activer Citrix ADM service connect ?

Si vous êtes un client Citrix ADC existant et que vous effectuez une mise à niveau vers Citrix ADC version 13.0 build 61.xx, Citrix ADM service connect est activée par défaut dans le cadre du processus de mise à niveau.

Si vous êtes un nouveau client Citrix ADC, installant Citrix ADC version 13.0 build 61.xx, Citrix ADM service connect est activé par défaut dans le cadre du processus d'installation.

> **Remarque**
>
> Contrairement aux nouvelles appliances Citrix ADC, les appliances Citrix ADC existantes trouvent l'itinéraire via Citrix Insight Service (CIS) ou Call Home.

Comment activer et désactiver Citrix ADM service connect ?

Vous pouvez activer et désactiver la connexion du service Citrix ADM à partir des méthodes CLI, GUI ou API NITRO.

Utilisation de la CLI

Pour activer le service Citrix ADM se connecter à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set adm parameter -admserviceconnect ENABLED
```

Pour désactiver le service Citrix ADM se connecter à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set adm parameter -admserviceconnect DISABLED
```

> **Important**
>
> Si votre Citrix ADC est sur la version 13.0 build 61.xx, le nom du paramètre permettant d'activer ou de désactiver Citrix ADC Service Connect est « Connexion automatique ». « Par exemple, pour ac-

> tiver la connexion de service, utilisez la `set adm parameter - autoconnect ENABLED` commande.

Utilisation de l'interface graphique

Pour désactiver la connexion du service Citrix ADM à l'aide de l'interface graphique Citrix ADC

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix ADC (par exemple, http://192.0.2.10).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Système > Paramètres > Configurer les paramètres ADM**.
4. Dans la page **Configurer les paramètres ADM**, **désactivez la boîte de dialogue Activer la connexion au service Citrix ADM**, puis cliquez sur **OK**.

Utilisation de l'API NITRO

Vous pouvez désactiver Citrix ADM Service Connect à l'aide de la commande **NITRO** .

- Dans Citrix ADC version 13.0 build 61.xx, vous pouvez activer ou désactiver le service Citrix ADM connect à l'aide de la commande suivante :

  ```
  curl -X PUT -H "Content-Type:application/json"http://192.0.2.10/nitro/v1/config/admparameter> -d '{ "admparameter":{ "autoconnect":"enabled" } } ' -u nsroot:Test@1
  ```

- À partir de Citrix ADC version 13.0 build 64.xx, le nom du paramètre « connexion automatique » est renommé en `admserviceconnect`. Vous pouvez désactiver la connexion du service Citrix ADM à l'aide de la commande suivante :

  ```
  curl -X PUT -H "Content-Type:application/json" http://192.0.2.10/nitro/v1/config/admparameter -d '{ "admparameter":{ "admserviceconnect":"disabled" } } ' -u nsroot:Test@1
  ```

> **Remarque**
>
> Lors de l'intégration des instances Citrix ADC sur le service Citrix ADM, il se peut que vous rencontriez des problèmes. Vous pouvez résoudre les problèmes à l'aide de l'outil de diagnostic. Pour plus d'informations, voir Dépannage des problèmes à l'aide de l'outil de diagnostic.

Comportement de l'agent intégré Citrix ADM

À partir de Citrix ADC version 13.0 build 61.xx et supérieure, l'agent intégré Citrix ADM disponible sur les instances Citrix ADC communique avec le service ADM. Il communique sans qu'il soit nécessaire

d'initialiser manuellement l'instance ADC correspondante. Une fois la communication avec le service ADM établie, l'agent intégré reste permanent en effectuant une mise à niveau automatique vers la dernière version du logiciel régulièrement.

Auparavant, vous deviez initialiser l'agent intégré sur les instances ADC, à l'aide de `mastools` commandes, pour établir une communication avec le service ADM et pour des mises à niveau automatiques régulières.
Pour plus d'informations, voir Configurer l'agent intégré ADC pour gérer les instances.

Références

Pour plus d'informations sur Citrix ADM service connect, consultez les rubriques suivantes :

- Gouvernance des données : gouvernance des données.
- Service Citrix ADM : Citrix Application Delivery Management Service.

Mettre à niveau et rétrograder une appliance Citrix ADC

October 5, 2021

Citrix ADC 13.1 propose des fonctionnalités nouvelles et mises à jour avec des fonctionnalités accrues. Une liste complète des améliorations est répertoriée dans les notes de mise à jour accompagnant l'annonce de publication. Lisez les notes de mise à jour avant de mettre à niveau votre logiciel.

Cette section fournit des informations sur la **mise à niveau et la rétrogradation du microprogramme d'une appliance Citrix ADC** (MPX et VPX) à **l'aide de l'interface graphique ou de l'interface de ligne de commande Citrix ADC**.

Vous pouvez également **utiliser Citrix ADM pour mettre à niveau un dispositif Citrix ADC**. Pour plus d'informations, consultez :

- 10 façons dont le service Citrix ADM prend en charge les mises à niveau Citrix ADC simplifiées
- Utiliser le service Citrix ADM pour mettre à niveau les instances Citrix ADC
- Utiliser le logiciel Citrix ADM pour mettre à niveau des instances Citrix ADC

Pour plus d'informations sur **la mise à niveau d'une appliance Citrix ADC SDX**, reportez-vous à la sectionMise à niveau unique.

> **Remarque**
>
> À partir de Citrix ADC version 13.1, les fonctionnalités et fonctionnalités classiques obsolètes basées sur des stratégies sont supprimées de l'appliance Citrix ADC. Pour plus d'informations,

> consultez le tableau FAQ sur la dépréciation des stratégies classiques .

Avant de commencer

October 5, 2021

Avant de commencer le processus de mise à niveau ou de rétrogradation, assurez-vous de vérifier les points suivants :

- Temps alloué à la mise à niveau des appliances Citrix ADC. Suivez la procédure de contrôle des modifications de votre organisation. Allouez deux fois plus de temps pour effectuer les mises à niveau. Allouez suffisamment de temps pour mettre à niveau chaque appliance Citrix ADC.
- Évaluez le contrat de support de votre organisation. Documentez le numéro de série de l'appliance, le contrat de support et les détails des contacts du support technique Citrix ou du partenaire agréé Citrix.
- Le cadre de licences et les types de licences. Une mise à niveau d'une édition logicielle peut nécessiter de nouvelles licences, telles que :
  - mise à niveau de l'édition standard vers l'édition avancée, ou
  - l'édition standard à l'édition Premium, ou
  - l'édition avancée jusqu'à l'édition Premium.

  Les licences Citrix ADC existantes continuent de fonctionner lorsque vous effectuez une mise à niveau vers la version 13.1. Pour plus d'informations, voir Licences
- Vérifiez la présence de commandes, de paramètres et d'OID SNMP nouveaux et obsolètes.
- Vérifiez la matrice de compatibilité matérielle et logicielle Citrix ADC MPX.
- Si la page d'ouverture de session Citrix ADC Gateway est personnalisée, assurez-vous que le thème de l'interface utilisateur est défini sur défaut.
- Si vous mettez à niveau LOM, consultez la page Mise à niveau du microprogramme LOM.
- Téléchargez le microprogramme Citrix ADC à partir des téléchargements Citrix ADC. Pour obtenir les étapes détaillées de téléchargement du microprogramme Citrix ADC, reportez-vous à la section Télécharger un package de version Citrix ADC.
- Sauvegardez les fichiers. Effectuez une sauvegarde du fichier de configuration, du fichier de personnalisation, des certificats, des scripts de surveillance, des fichiers de licences, etc. manuellement ou reportez-vous à la documentation suivante pour la sauvegarde à l'aide de l'interface de ligne de commande Citrix ADC ou de l'interface graphique - Sauvegarde et restauration.
  - Reportez-vous à la liste suivante pour connaître les autres fichiers personnalisés courants à sauvegarder.

    * /nsconfig/monitors/*.pl
    * /nsconfig/rc.netscaler

  – Sauvegardez le dossier de personnalisation. C'est généralement sous /var/customizations . Un exemple de personnalisation est une page d'ouverture de session avec un logo. Après avoir copié le dossier de personnalisation, vous devez le supprimer de l'appliance Citrix ADC avant de mettre à niveau l'appliance. La mise à niveau avec personnalisation en place peut entraîner certains problèmes.

> **Important :**
> Citrix recommande vivement de passer en revue les procédures de sauvegarde ci-dessus. Disposez d'un plan d'action en cas d'échec de la mise à jour sur l'appliance Citrix ADC.

- Vérifiez qu'il y a suffisamment d'espace dans les répertoires /var et /flash pour l'appliance Citrix ADC avant d'effectuer une mise à niveau. Le fichier /var nécessite 5 Go d'espace libre (1 Go pour le bundle de mise à niveau + 4 Go pour le processus de mise à niveau)
  Le /flash nécessite suffisamment d'espace pour copier sur le nouveau noyau, qui diffère entre 140 Mo et 160 Mo environ, garantissant qu'il y a au moins 250 Mo d'espace libre disponible.
  Pour plus d'informations sur la suppression de l'espace disque dans /var, consultez Comment libérer de l'espace sur le répertoire /var pour la journalisation des problèmes avec une appliance Citrix ADC.
  Pour plus d'informations sur la suppression des espaces disque dans /flash, reportez-vous à la section https://support.citrix.com/article/CTX133587.
- Valider l'intégrité de l'appliance Citrix ADC. Si vous disposez d'une appliance matérielle Citrix ADC, Citrix vous recommande vivement fsck d'exécuter une vérification du disque et de valider l'intégrité du disque dur Citrix ADC. En cas d'erreur, réinitialisez le disque dur et répétez la commande de vérification du disque. Si le message d'erreur réapparaît, contactez le support Citrix pour examiner plus avant le problème.
  – Validez l'intégrité du disque dur à l'aide d'une commande fsck. Pour plus d'informations, voir CTX122845.
  – Validez l'intégrité d'une appliance Citrix ADC à l'aide des fichiers de bundles de diagnostic et en téléchargeant les journaux vers Citrix Insight Service à des fins d'analyse. Pour plus d'informations, voir Comment collecter un pack de support technique.
- Consultez la matrice de support Citrix ADC VPX et les directives d'utilisation.
- Consultez la section FAQ .
- Il est recommandé de mettre à niveau vers une version majeure à la fois. N'effectuez pas de mise à niveau directe vers la dernière version.

  Par exemple, si l'appliance Citrix ADC est sur la version 12.1 et que vous souhaitez effectuer une mise à niveau vers la version 13.1, vous devez d'abord mettre à niveau l'appliance vers la version 13.0, puis vers la version 13.1.

- Vérifiez les procédures de mise à niveau avec un environnement de test.

Pour plus d'informations sur les conditions préalables à la mise à niveau ou à la rétrogradation de l'appliance Citrix ADC, consultez les articles suivants :

- CTX220371 : doit lire les articles avant et après la mise à niveau de Citrix ADC

Considérations concernant la mise à niveau - Configuration de SNMP

January 21, 2021

Le paramètre de temporisation d'une alarme SNMP est une option interne qui n'a aucun impact sur la configuration de l'alarme.

Le paramètre Timeout peut apparaître dans les configurations d'alarme SNMP de la configuration en cours d'exécution (sh en cours d'exécution) et de la configuration enregistrée (ns.conf) même si vous n'avez apporté aucune modification à ces configurations d'alarme SNMP.

Au moment de la mise à niveau vers une version de version avec le correctif du problème de réglage du délai d'expiration, les configurations SNMP sont réinitialisées par erreur aux valeurs par défaut.

Les alarmes SNMP suivantes (si configurées) sont affectées lors d'une mise à niveau :

- APPFW-BUFFER-OVERFLOW
- APPFW-COOKIE
- APPFW-CSRF-TAG
- APPFW-DENY-URL
- APPFW-FIELD-CONSISTENCY
- APPFW-FIELD-FORMAT
- APPFW-POLICY-HIT
- APPFW-REFERER-HEADER
- APPFW-SAFE-COMMERCE
- APPFW-SAFE-OBJET
- APPFW-SQL
- APPFW-START-URL
- APPFW-VIOLATIONS-TYPE
- APPFW-XML-ATTACHMENT
- APPFW-XML-DOS
- APPFW-XML-SCHEMA-COMPILE
- APPFW-XML-SOAP-FAULT
- APPFW-XML-SQL
- APPFW-XML-VALIDATION
- APPFW-XML-WSI

- APPFW-XML-XSS
- APPFW-XSS
- CLUSTER-BACKPLANE-HB-MISSING
- CLUSTER-NODE-HEALTH
- CLUSTER-NODE-QUORUM
- CLUSTER-VERSION-MISMATCH
- COMPACT-FLASH-ERRORS
- CONFIG-CHANGE
- CONFIG-SAVE
- HA-BAD-SECONDARY-STATE
- HA-NO-HEARTBEATS
- HA-SYNC-FAILURE
- HA-VERSION-MISMATCH
- HARD-DISK-DRIVE-ERRORS
- HA-STATE-CHANGE
- HA-STICKY-PRIMARY
- PORT-ALLOC-FAILED
- SYNFLOOD

Ces configurations d'alarmes SNMP sont affectées lorsque vous mettez à niveau Citrix ADC vers les versions suivantes :

- Version 11.1 version 61.2 ou ultérieure
- Version 12.0 version 61.0 ou ultérieure
- Version 12.1 version 30.1 ou ultérieure
- Version 13.0 build 51.4 ou ultérieure

Exemple

Considérons un exemple d'alarme SNMP CLUSTER-NODE-HEALTH.

```
1 CLUSTER-NODE-HEALTH SNMP alarm is set up by using the Citrix ADC
     command line:
2
3 > set snmp alarm CLUSTER-NODE-HEALTH -time 111 -state DISABLED -
     severity Major
4
5 > save config
6 <!--NeedCopy-->
```

Cette configuration d'alarme SNMP apparaît dans le fichier de configuration enregistré (`ns.conf`) comme suit :


```
set snmp alarm CLUSTER-NODE-HEALTH -time 111 -state DISABLED -severity
    Major -timeout 86400

<!--NeedCopy-->
```

Lors d'une mise à niveau vers l'une des versions mentionnées ci-dessus, l'erreur suivante apparaît dans le fichier ns.log :

```
May 23 09:14:46 <local0.err> ns nsconfigd: __init_config_filter(): (
    null) line 0: No such argument [-timeout]>> set snmp alarm CLUSTER-
    NODE-HEALTH -time 111 -state DISABLED -severity Major -timeout
    86400.
<!--NeedCopy-->
```

Après la mise à niveau, les configurations d'alarme SNMP sont réinitialisées aux valeurs par défaut.

Solution

Utilisez l'une des résolutions suivantes :

- Avant la mise à niveau, supprimez le paramètre de délai d'expiration des configurations SNMP dans le fichier de configuration enregistré (ns.conf).
- Après la mise à niveau, reconfigurez les alarmes SNMP sans le paramètre timeout.

Télécharger un package Citrix ADC

August 20, 2021

Procédez comme suit pour télécharger un package de version Citrix ADC :

1. Ouvrez la page Téléchargements Citrix ADC dans un navigateur Web.
2. Sur la page Téléchargements Citrix ADC, développez la **version Citrix ADC** vers laquelle vous souhaitez mettre à jour.
3. Développez l'une des catégories appropriées, puis cliquez sur le lien de génération Citrix ADC. Par exemple, pour télécharger une version du firmware Citrix ADC, développez **Firmware**et cliquez sur la version Citrix ADC que vous souhaitez télécharger.
4. Sur la page de génération Citrix ADC sélectionnée, développez la section **Générer**, cliquez sur **Télécharger le fichier** pour télécharger le package de construction Citrix ADC.

> **Remarque :**
> La somme de contrôle est fournie pour vous assurer que vous correspondez au package de build téléchargé avec le package réel qui est hébergé sur le site Web. Checksum est une vérification importante pour vous assurer que vous avez les bits corrects.

Mettre à niveau une appliance autonome Citrix ADC

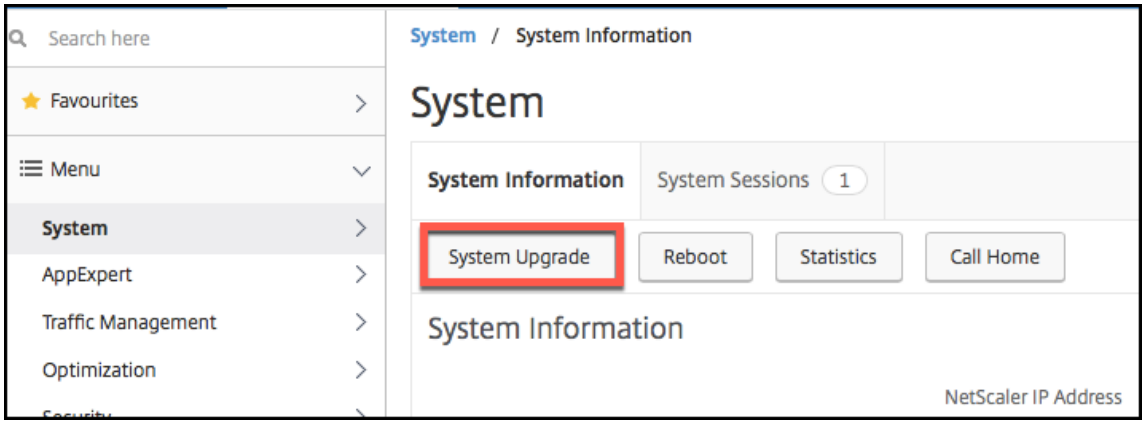
October 5, 2021

Avant de mettre à niveau le logiciel système, assurez-vous de lire la section Avant de commencer et de remplir les conditions préalables telles que la sauvegarde des fichiers nécessaires et le téléchargement du microprogramme Citrix ADC.

Mettre à niveau un dispositif autonome Citrix ADC à l'aide de l'interface graphique

Suivez ces étapes pour mettre à niveau un Citrix ADC autonome vers la version 13.1 à l'aide de l'interface graphique.

1. Dans un navigateur Web, tapez l'adresse IP du Citrix ADC, par exemple `http://10.102.29.50`.
2. Dans Nom d'utilisateur et mot de passe, tapez les informations d'identification de l'administrateur (nsroot/nsroot), puis cliquez **sur Connexion**.
3. Dans l'interface graphique, cliquez sur **Mise à niveau du système**.



4. Dans le menu **Choisir un fichier**, choisissez l'option appropriée : **Local** ou **Appliance**. Si vous souhaitez utiliser l'option Appliance, le microprogramme doit d'abord être téléchargé sur Citrix ADC. Vous pouvez utiliser n'importe quelle méthode de transfert de fichiers, telle que WinSCP, pour télécharger le microprogramme Citrix ADC sur l'appliance.
5. Sélectionnez le fichier approprié et cliquez sur **Mettre à niveau**.

6. Suivez les instructions pour mettre à niveau le logiciel.
7. Lorsque vous y êtes invité, sélectionnez **Redémarrer**.

Après la mise à niveau, fermez toutes les instances de navigateur et videz le cache de votre ordinateur avant d'accéder à la solution matérielle-logicielle.

Mettre à niveau un dispositif autonome Citrix ADC à l'aide de l'interface de ligne de commande

Suivez ces étapes pour mettre à niveau un Citrix ADC autonome vers la version 13.1 à l'aide de l'interface de ligne de commande :

Dans la procédure suivante, <release> et <releasenumber> représente la version de mise à niveau vers laquelle vous effectuez la mise à niveau et <targetbuildnumber> le numéro de version vers lequel vous effectuez la mise à niveau. La procédure inclut des étapes facultatives pour éviter de perdre les mises à jour qui sont poussées vers le répertoire /etc pendant la mise à niveau.

1. Utilisez un client SSH, tel que PuTTY, pour ouvrir une connexion SSH vers l'appliance.
2. Connectez-vous à l'appliance à l'aide des informations d'identification de l'administrateur. Enregistrez la configuration en cours d'exécution. À l'invite, tapez :

   ```
   save config
   ```

3. Passez à l'invite du shell en exécutant la commande suivante :

   ```
   shell
   ```

4. Créez une copie du fichier ns.conf. À l'invite shell, tapez :

   - `cd /nsconfig`
   - `cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber>`

   Vous devez sauvegarder le fichier de configuration sur un autre ordinateur.

5. (Facultatif) Si vous avez modifié certains des fichiers suivants dans le répertoire /etc et que vous les avez copiés dans /nsconfig pour conserver leur persistance, toutes les mises à jour qui sont poussées vers le répertoire /etc pendant la mise à niveau risquent d'être perdues :

   - ttys
   - resolv.conf
   - sshd_config
   - host.conf
   - newsyslog.conf
   - host.conf
   - httpd.conf
   - rc.conf

- syslog.conf
- crontab
- monitrc

Pour éviter de perdre ces mises à jour, créez un `/var/nsconfig_backup` répertoire et déplacez les fichiers personnalisés vers ce répertoire. En d'autres termes, déplacez tous les fichiers que vous avez modifiés dans le répertoire /etc et copiés dans /nsconfig en exécutant la commande suivante :

```
cp /nsconfig/<filename> /var/nsconfig_backup
```

Exemple :

```
cp /nsconfig/syslog.conf /var/nsconfig_backup
```

6. Créez un emplacement pour le package d'installation. À l'invite du shell, tapez :
   - `cd /var/nsinstall`
   - `cd <releasenumber>`

     > **Remarque :**
     >
     > Si le répertoire du numéro de version souhaité n'est pas présent, créez-en un à l'aide de la commande suivante :
     >
     > `mkdir <releasenumber>`
     >
     > **Exemple :**
     >
     > `mkdir 13.1`

   - `mkdir build_<targetbuildnumber>`
   - `cd build_<targetbuildnumber>`
7. Copiez le firmware Citrix ADC déjà téléchargé dans le répertoire de génération que vous avez créé à l'étape ci-dessus, à l'aide d'une méthode de transfert de fichiers telle que WinSCP. Consultez la section Avant de commencer pour plus d'informations sur le téléchargement du microprogramme Citrix ADC.
8. Extraire le contenu du package d'installation. Exemple :

   ```
   tar -xvzf build-13.1-37.2_nc_64.tgz
   ```

9. Exécutez le script installns pour installer la nouvelle version du logiciel système.

   ```
   ./installns
   ```

10. Lorsque vous y êtes invité, redémarrez Citrix ADC.
11. (Le cas échéant) Si vous avez créé une copie du fichier ns.conf dans la section Avant de commencer, procédez comme suit :

a) Comparez manuellement les fichiers dans /var/nsconfig_backup/etc et apportez les modifications appropriées dans /etc.
b) Pour conserver la persistance, déplacez les fichiers mis à jour /etc vers /nsconfig.
c) Redémarrez la solution matérielle-logicielle pour que les modifications soient prises en compte.

Voici un exemple de mise à niveau du firmware Citrix ADC.

```
login: nsroot

Password: nsroot

Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134

Done

> save config

> shell

Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134

root@NSnnn# cd /var/nsinstall

root@NSnnn# cd 13.1

root@NSnnn# mkdir build_43.1

root@NSnnn# cd build_43.1

root@NSnnn# ftp <FTP server IP address>

ftp> mget build-13.1-41.1_nc.tgz

ftp> bye

root@NSnnn# tar xzvf build-13.1-41.1_nc.tgz

root@NSnnn# ./installns

installns version (13.1-41.1) kernel (ns-13.1-41.1_nc.gz)

...

Copying ns-13.1-41.1_nc.gz to /flash/ns-13.1-41.1_nc.gz ...
```



```
38
39 ...
40
41 Installation has completed.
42
43 Reboot NOW? [Y/N] Y
```

Mettre à niveau un dispositif autonome Citrix ADC à l'aide de l'API NITRO

Pour utiliser l'API NITRO pour mettre à niveau ou rétrograder un Citrix ADC, consultez Automatiser la mise à niveau et la rétrogradation de Citrix ADC avec une seule API.

Vérifier l'état des entités sur l'appliance Citrix ADC après la mise à niveau

Une fois l'appliance Citrix ADC mise à niveau, vérifiez l'état des entités suivantes :

- Les serveurs virtuels sont en état UP
- Les moniteurs sont en état UP
- Les sites GSLB se synchronisent sans problème
- Tous les certificats sont présents sur l'appliance
- Toutes les licences sont présentes sur l'appliance

Vérifiez et installez la mise à jour logicielle Citrix ADC 13.1

Mettez à jour le logiciel Citrix ADC lorsqu'une mise à jour est disponible, pour de meilleures performances. Une mise à jour Citrix ADC peut inclure des améliorations de fonctionnalités, des correctifs de performances ou des améliorations. N'oubliez pas de lire les notes de publication pour voir quels correctifs et améliorations sont disponibles dans la mise à jour. Pour vérifier et installer une mise à jour logicielle, procédez comme suit.

1. Dans la page d'accueil de Citrix ADC, cliquez sur **Rechercher des mises à jour** dans le menu **nsroot** en haut à droite.
2. Dans la page **Dernières mises à jour logicielles système disponibles**, vérifiez la mise à jour logicielle disponible que vous pouvez installer.
3. Cliquez sur **Télécharger** pour télécharger le package d'installation à partir du site Web de téléchargement Citrix .
4. Après avoir téléchargé le package logiciel, installez la mise à jour via la procédure CLI ou GUI.

> **Remarque**
>
> Le lien **Vérifier la mise à jour** n'est accessible que si vous vous connectez à l'interface graphique via le protocole HTTP et non via le protocole HTTPS.

Ressources connexes

Les ressources suivantes fournissent des informations connexes sur la mise à niveau ou la rétrogradation d'une appliance Citrix ADC :

- Tutoriel vidéo - Comment mettre à niveau votre Citrix ADC à l'aide de l'interface de ligne de commande

Réversion d'une appliance autonome Citrix ADC

October 5, 2021

Vous pouvez passer à n'importe quelle version antérieure sur un Citrix ADC autonome à l'aide de l'interface de ligne de commande ou de l'interface graphique.

> **Remarque :**
>
> Une perte de configuration peut survenir lors d'une rétrogradation. Comparez les configurations avant et après la rétrogradation, puis saisissez à nouveau manuellement les entrées manquantes.

Réversion d'une appliance Citrix ADC à l'aide de l'interface de ligne de commande

Suivez les étapes ci-dessous pour rétrograder une appliance autonome Citrix ADC exécutant la version 13.1 vers une version antérieure.

Dans cette procédure, <release> et <releasenumber> représente la version de mise à niveau vers laquelle vous êtes en train de rétrograder et <targetbuildnumber> représente le numéro de version vers lequel vous procédez à la rétrogradation.

1. Ouvrez une connexion SSH à Citrix ADC à l'aide d'un client SSH, tel que PuTTY.
2. Ouvrez une session sur Citrix ADC à l'aide des informations d'identification de l'administrateur. Enregistrez la configuration en cours d'exécution. À l'invite, tapez :

   enregistrer la configuration
3. Créez une copie du fichier ns.conf. À l'invite shell, tapez :

   a) `cd /nsconfig`
   b) `cp ns.conf ns.conf.NS<currentbuildnumber>`

   Vous devez sauvegarder une copie du fichier de configuration sur un autre ordinateur.
4. Copiez le <releasenumber>fichier de configuration (NS.Conf.ns<releasenumber>) dans ns.conf. À l'invite shell, tapez :


```
cp ns.conf.NS<releasenumber> ns.conf
<!--NeedCopy-->
```

> **Remarque :**
>
> ns.conf.NS<releasenumber> est le fichier de configuration de sauvegarde qui est automatiquement créé lorsque le logiciel système est mis à niveau de la version finale <releasenumber> vers la version actuelle.
>
> Il peut y avoir une perte de configuration lors d'une rétrogradation. Après le redémarrage de la solution matérielle-logicielle, comparez la configuration enregistrée à l'étape 3 avec la configuration en cours d'exécution et effectuez les ajustements nécessaires pour les fonctionnalités et entités configurées avant la mise à niveau vers le bas. Enregistrez la configuration en cours d'exécution après avoir effectué les modifications.
>
> **Important :**
>
> Si le routage est activé, effectuez l'étape 5. Sinon, passez directement à l'étape 6.

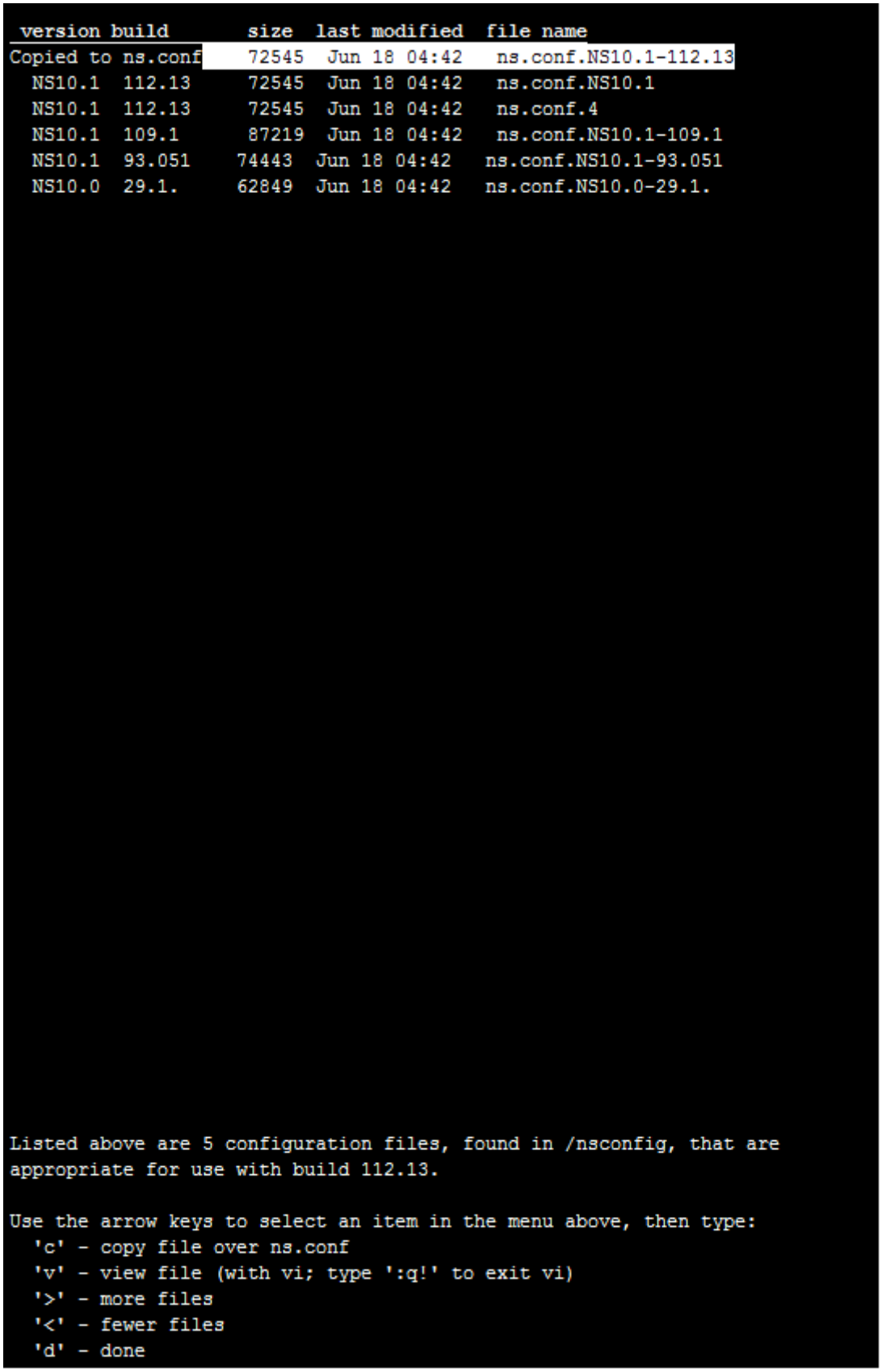
5. Si le routage est activé, le fichier Zebos.conf contient la configuration. À l'invite shell, tapez :

```
cd /nsconfig
cp ZebOS.conf ZebOS.conf.NS
cp ZebOS.conf.NS<targetreleasenumber> ZebOS.conf
<!--NeedCopy-->
```

6. Changez le /var/nsinstall/<releasenumber>nsinstallrépertoire ou créez-en un s'il n'existe pas.
7. Changez le build_<targetbuildnumber>répertoire ou créez-en un s'il n'existe pas.
8. Téléchargez ou copiez le package d'installation (build-<release>-<targetbuildnumber>.tgz) dans ce répertoire et extrayez le contenu du package d'installation.
9. Exécutez le installns script pour installer la nouvelle version du logiciel système. Le script met à jour le /etc répertoire.

   Si le fichier de configuration de la version vers laquelle vous procédez à la rétrogradation existe sur la solution matérielle-logicielle, vous êtes invité à charger cette configuration :

   Figure 1. Menu rétrograder s'il existe un fichier de configuration



Si l'espace disponible sur le lecteur flash est insuffisant pour installer la nouvelle version, Citrix ADC interrompt l'installation. Nettoyez manuellement le lecteur flash et redémarrez l'installation.

Exemple :

```
login: nsroot

Password: nsroot

Last login: Mon Apr 24 02:06:52 2017 from 10.102.29.9

Done

> save config

> shell

root@NSnnn# cp ns.conf.NS10.5 ns.conf

root@NSnnn# cd /var/nsinstall

root@NSnnn# mkdir 10.5nsinstall

root@NSnnn# cd 10.5nsinstall

root@NSnnn# mkdir build_57

root@NSnnn# cd build_57

root@NSnnn# ftp 10.102.1.1

ftp> mget build-10.5-57_nc.tgz

ftp> bye

root@NSnnn# tar -xzvf build-10.1-125_nc.tgz

root@NSnnn# ./installns

installns version (10.5-57) kernel (ns-10.5-57.gz)

...

...
```



```
40
41 ...
42
43 Copying ns-10.5-57.gz to /flash/ns-10.5-57_nc.gz ...
44
45 Changing /flash/boot/loader.conf for ns-10.5-57 ...
46
47
48
49 Installation has completed.
50
51
52
53 Reboot NOW? [Y/N] Y
54 <!--NeedCopy-->
```

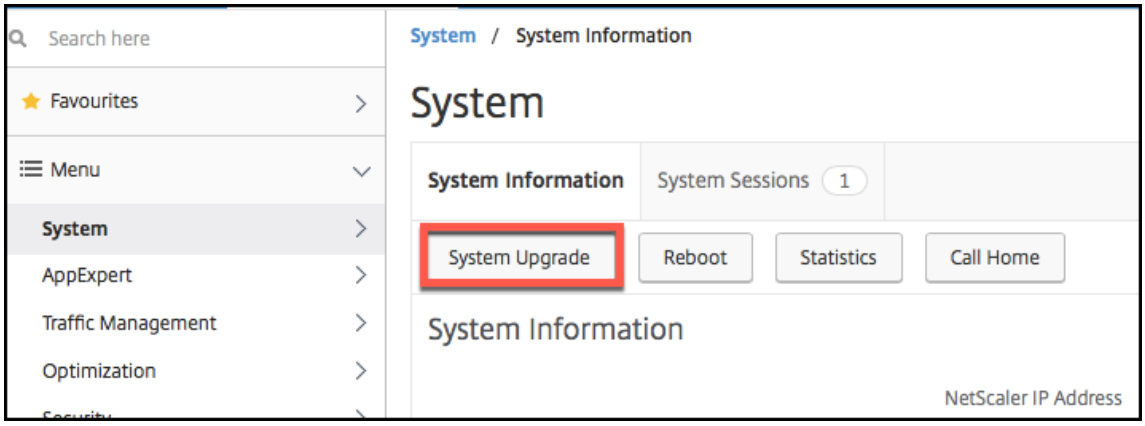
Réversion d'une appliance Citrix ADC à l'aide de l'interface graphique

Vous pouvez utiliser l'assistant de mise à niveau de l'interface graphique pour rétrograder un dispositif Citrix ADC exécutant la version 13.1 vers une version antérieure.

> **Remarques :**
>
> Vous ne pouvez pas rétrograder une appliance Citrix ADC exécutant la version 13.1 directement vers la version 10.5 ou antérieure à l'aide de l'interface graphique. Citrix recommande d'utiliser l'interface de ligne de commande pour la rétrogradation.
>
> Consultez le site Product Matrix pour plus d'informations sur le cycle de vie de la version Citrix ADC.
>
> Il est recommandé de passer à une version majeure à la fois.
>
> Par exemple, si l'appliance Citrix ADC est sur la version 13.1 et que vous souhaitez passer à la version 12.1, vous devez d'abord rétrograder l'appliance vers la version 13.0, puis vers la version 12.1.

Suivez les étapes ci-dessous pour rétrograder une appliance Citrix ADC exécutant la version 13.1 vers une version antérieure à l'aide de l'interface graphique.

1. Dans un navigateur Web, tapez l'adresse IP du Citrix ADC, par exemple `http://10.102.29.50`.
2. Dans Nom d'utilisateur et mot de passe, tapez les informations d'identification de l'administrateur, puis cliquez **sur Connexion**.
3. Dans l'interface graphique, cliquez sur **Mise à niveau du système**.



4. Dans le menu **Choisir un fichier**, choisissez l'option appropriée : **Local** ou **Appliance**. Si vous souhaitez utiliser l'option Appliance, le microprogramme doit d'abord être téléchargé sur Citrix ADC. Vous pouvez utiliser n'importe quelle méthode de transfert de fichiers, telle que WinSCP, pour télécharger le microprogramme Citrix ADC sur l'appliance.
5. Sélectionnez le fichier approprié et cliquez sur **Mettre à niveau**.
6. Suivez les instructions pour rétrograder le logiciel.
7. Lorsque vous y êtes invité, sélectionnez **Redémarrer**.

Après la mise à niveau, fermez toutes les instances de navigateur et effacez le cache de votre ordinateur avant d'accéder à la solution matérielle-logicielle.

Ressources connexes

Les ressources suivantes fournissent des informations connexes sur la mise à niveau ou la rétrogradation d'une appliance Citrix ADC :

- Tutoriel vidéo - Comment mettre à niveau votre Citrix ADC à l'aide de l'interface de ligne de commande

Mettre à niveau une paire haute disponibilité

August 20, 2021

Une des conditions requises pour les appliances Citrix ADC dans une configuration haute disponibilité consiste à installer la même version logicielle Citrix ADC sur les deux appliances de l'installation. Par conséquent, lorsque le logiciel d'une appliance est mis à niveau, assurez-vous que le logiciel est mis à niveau sur les deux appliances.

Vous pouvez suivre la même procédure pour mettre à niveau une appliance autonome ou chaque appliance dans une paire haute disponibilité, bien que des considérations supplémentaires s'appliquent à la mise à niveau d'une paire haute disponibilité.

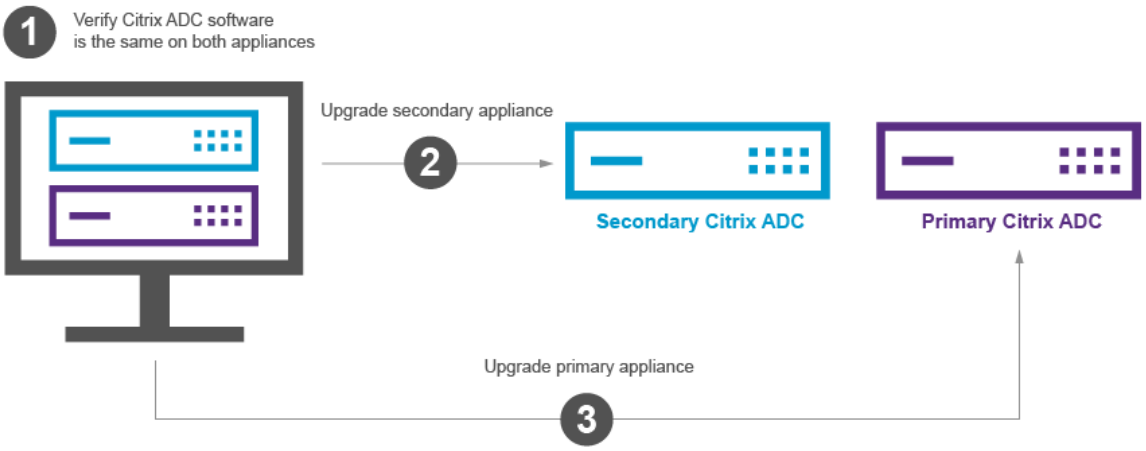
Avant de commencer une mise à niveau du microprogramme Citrix ADC sur une paire HA, lisez les conditions préalables mentionnées dans la section Avant de commencer . En outre, vous devez considérer quelques points spécifiques à l'HA.

Points à noter

- Mettez d'abord à niveau le nœud secondaire, puis le nœud principal. La mise à niveau du logiciel sur l'appliance secondaire avant l'appliance principale garantit que le processus de mise à niveau est terminé sans problème.
- Si les deux nœuds d'une installation de haute disponibilité (HA) exécutent différentes versions logicielles Citrix ADC, les fonctionnalités suivantes sont désactivées :
  - Synchronisation de configuration HA
  - Propagation des commandes HA
  - Synchronisation HA des informations des services d'états
  - Mise en miroir des connexions (basculement de connexion) des sessions
  - Synchronisation HA des informations sur les sessions de persistance
- Les fonctionnalités mentionnées ci-dessus sont désactivées, si les deux nœuds d'une configuration haute disponibilité (HA) exécutent différentes versions de la même version mais que les deux versions ont des versions HA internes différentes. Les fonctionnalités mentionnées ci-dessus fonctionnent bien si les deux nœuds d'une configuration haute disponibilité (HA) exécutent différentes versions de la même version, mais les deux versions ont les mêmes versions HA internes.

  Reportez-vous à la section Points à note des notes de mise à jour pour vérifier si la version HA interne a changé dans la version Citrix ADC.
- La synchronisation des fichiers dans le mode Tous de la commande Synchroniser les fichiers HA fonctionne correctement si les deux nœuds d'une configuration HA exécutent des versions logicielles Citrix ADC différentes, ou si les deux nœuds exécutent des versions différentes de la même version. Pour plus d'informations, consultez Synchronisation des fichiers de configuration dans la configuration haute disponibilité.

Figure. Mettre à niveau une paire haute disponibilité



Vous pouvez effectuer une mise à niveau à l'aide de l'interface de ligne de commande ou de l'interface graphique Citrix ADC.

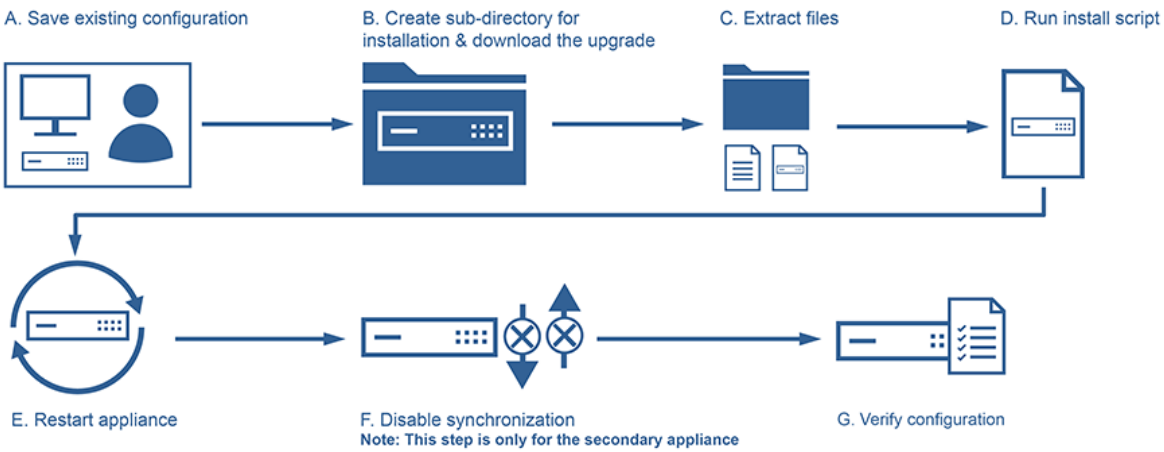
Mettre à niveau une paire haute disponibilité à l'aide de l'interface de ligne de commande

Le processus de mise à niveau comprend les étapes suivantes :

1. Mise à niveau du logiciel sur l'appliance secondaire
2. Mise à niveau du logiciel sur l'appliance principale
3. Synchroniser le matériel secondaire

Mise à niveau du logiciel sur l'appliance secondaire

L'illustration suivante illustre la procédure de mise à niveau du logiciel sur l'appliance secondaire :



1. Connectez-vous à l'appliance NetScaler secondaire à l'aide d'un utilitaire SSH, tel que PuTTY et

spécifiez l'IP NetScaler (NSIP). Utilisez les informations d'identification nsroot pour vous connecter à l'appliance.

2. À partir de l'interface de ligne de commande de l'appliance, tapez la commande suivante pour enregistrer la configuration existante : save config
3. Passez à l'invite du shell.

```
login as: username
Using keyboard-interactive authentication.
Password:
Last login: Wed Jun 24 14:59:16 2015 from 10.252.252.65
Done
> shell
Copyright (c) 1992-20

<!--NeedCopy-->
```

4. Exécutez la commande suivante pour passer au répertoire d'installation par défaut : # cd /var/nsinstall
5. Exécutez la commande suivante pour créer un sous-répertoire temporaire du répertoire nsinstall : **# mkdir x_xnsinstall**

> Remarque : Le texte x_x est utilisé pour nommer la version NetScaler pour les futures configurations. Par exemple, le répertoire des fichiers d'installation de NetScaler 9.3 us appelé 9_3nsinstall. N'utilisez pas de point (.) dans le nom du dossier, cela peut entraîner l'échec des mises à niveau.

6. Changez vers le répertoire **x_xnsinstall** .
7. Téléchargez le package d'installation et le bundle de documentation requis, tels que « ns-x.0-xx.x-doc.tgz », dans le répertoire temporaire créé à l'étape 4.

> **Remarque :**
>
> Certaines versions n'ont pas de paquet de documentation car il n'a pas besoin d'être installé.
>
> Cliquez sur l'onglet **Documentation** de l'interface graphique pour accéder à la documentation.

8. Avant d'exécuter le script d'installation, les fichiers doivent être extraits et placés sur l'appliance. Utilisez la commande suivante pour décompresser le bundle téléchargé à partir du site Web Citrix : **tar -zxvf ns-x.0-xx.x-doc.tgz**. Voici une explication rapide des paramètres utilisés.

   x : Extraire des fichiers

   v : Imprimez les noms de fichiers au fur et à mesure qu'ils sont extraits un par un

z : Le fichier est un fichier « gzippé »

f : Utilisez l'archive tar suivante pour l'opération

9. Exécutez la commande suivante pour installer le logiciel téléchargé : #. /installns

   > Remarque : si l'appliance ne dispose pas d'un espace disque suffisant pour installer les nouveaux fichiers du noyau, le processus d'installation effectue un nettoyage automatique du lecteur flash.

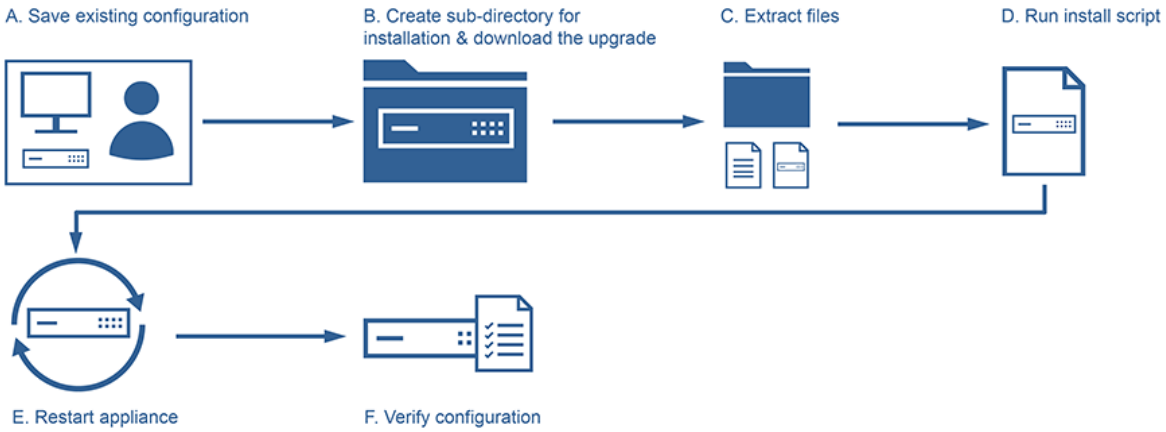
10. Une fois le processus d'installation terminé, le processus invite à redémarrer l'appliance. Appuyez sur y pour redémarrer l'appliance.
11. Connectez-vous à l'interface de ligne de commande de l'appliance à l'aide des informations d'identification nsroot.
12. Exécutez la commande suivante de pour afficher l'état de l'appliance NetScaler : **show ha node** La sortie de la commande précédente doit indiquer que l'appliance est un nœud secondaire et que la synchronisation est désactivée.
13. Exécutez la commande suivante pour effectuer un basculement forcé et une reprise en tant que appliance principale : **forcer le basculement sur incident**

Voici un exemple de configuration dans le nouveau nœud principal.

```
login: nsroot
Password: nsroot
Last login: Monday Apr  17 08:37:26 2017 from 10.102.29.9
Done
show ha node
        2 nodes:
1)      Node ID:      0
        IP:        10.0.4.2
        Node State: UP
        Master State: Primary
        ...
        Sync State: AUTO DISABLED
        Propagation: AUTO DISABLED
        ...
Done
<!--NeedCopy-->
```

Mise à niveau du logiciel sur l'appliance principale

L'illustration suivante illustre la procédure de mise à niveau du logiciel sur l'appliance principale :



> Remarque : après avoir terminé la procédure « Mise à niveau du logiciel sur l'appliance secondaire », l'appliance principale d'origine est désormais une appliance secondaire.

1. Connectez-vous à l'appliance NetScaler secondaire à l'aide d'un utilitaire SSH, tel que PuTY. Utilisez les informations d'identification nsroot pour vous connecter à l'appliance. Suivez les mêmes étapes que celles mentionnées dans la section ci-dessus pour terminer le processus d'installation. Nous devons suivre les mêmes étapes que celles mentionnées à l'étape 2 à l'étape 9 de la section précédente (Mise à niveau du logiciel de l'appliance secondaire)
2. Une fois le processus d'installation terminé, le processus invite à redémarrer l'appliance. Appuyez sur y pour redémarrer l'appliance.
3. Connectez-vous à l'interface de ligne de commande de l'appliance à l'aide des informations d'identification nsroot.
4. Exécutez la commande suivante pour afficher l'état de l'appliance NetScaler : **show ha node**. La sortie de la commande précédente doit indiquer que l'appliance est un nœud secondaire et que l'état du nœud est marqué comme UP.
5. Exécutez la commande suivante pour effectuer un basculement forcé afin de vous assurer que l'appliance est une appliance principale : **forcer le basculement sur incident**
6. Vérifiez que l'appliance est une appliance principale.

   Voici un exemple de configuration du nouveau nœud principal et du nouveau nœud secondaire.

```
1 show ha node
2     Node ID:      0
3     IP:   10.0.4.11
4     Node State: UP
5     Master State: Primary
6     ...
7     ...
8     INC State: DISABLED
```



```
    Sync State: ENABLED
    Propagation: ENABLED
    Enabled Interfaces : 1/1
    Disabled Interfaces : None
    HA MON ON Interfaces : 1/1
    ...
    ...
    Local node information
    Critical Interfaces: 1/1
Done

Show ha node
    Node ID:      0
    IP:   10.0.4.2
    Node State: UP
    Master State: Secondary
    ..
    ..
    INC State: DISABLED
    Sync State: SUCCESS
    Propagation: ENABLED
    Enabled Interfaces : 1/1
    Disabled Interfaces : None
    HA MON ON Interfaces : 1/1
    . .
    . .
    Local node information:
    Critical Interfaces: 1/1
Done
<!--NeedCopy-->
```

Mettre à niveau une paire haute disponibilité à l'aide de l'interface graphique

Procédez comme suit pour mettre à niveau une paire Citrix ADC dans une configuration haute disponibilité, à l'aide de l'interface graphique ADC. Prenons un exemple de configuration haute disponibilité des appliances Citrix ADC CITRIX-ADC-A (primaire) et CITRIX-ADC-B (secondaire).

1. **Mettez à niveau le nœud secondaire**. Connectez-vous à l'interface graphique du nœud secondaire à l'aide des informations d'identification de l'administrateur et effectuez la mise à niveau comme décrit dans Mettre à niveau une appliance autonome Citrix ADC à l'aide de l'interface graphique.
2. **Forcer le basculement**. Effectuez un basculement forcé sur le nœud secondaire à l'aide de l'interface graphique, comme décrit à la section Forcer un nœud à basculer.

Après l'opération de basculement, le nœud secondaire prend le relais en tant que principal et le nœud principal devient le nouveau nœud secondaire. Après l'opération de basculement dans l'exemple d'installation HA :

- CITRIX-ADC-B devient la nouvelle
- CITRIX-ADC-A devient le nouveau secondaire

3. **Mettez à niveau le nœud principal d'origine (nouveau nœud secondaire)**. Connectez-vous à la nouvelle interface graphique du nœud secondaire (CITRIX-ADC-A) et effectuez la mise à niveau comme décrit dans Mettre à niveau une appliance autonome Citrix ADC à l'aide de l'interface graphique.
4. **Forcer le basculement**. Effectuez un basculement forcé sur le nouveau nœud secondaire (CITRIX-ADC-A) à l'aide de l'interface graphique, comme décrit dans la section Forcer un nœud à basculer.

   Après cette deuxième opération de basculement, l'état des deux nœuds revient au même état qu'avant le démarrage de l'opération de mise à niveau HA. Après l'opération de basculement dans l'exemple d'installation HA :

   - CITRIX-ADC-A devient primaire
   - CITRIX-ADC-B devient secondaire
5. **Vérifiez le processus de mise à niveau**. Connectez-vous à l'interface graphique des deux nœuds. Accédez à **Système > Haute disponibilité**, sur la page de détails, vérifiez l'état HA des deux nœuds. Vérifiez également les détails de la version mise à niveau affichés dans le volet supérieur de l'interface graphique.

Ressources connexes

Les ressources suivantes fournissent des informations relatives à la mise à niveau d'une configuration haute disponibilité Citrix ADC :

- Tutoriel vidéo - Comment mettre à niveau votre paire Citrix ADC HA à l'aide de l'interface graphique

Prise en charge de la mise à niveau logicielle en service pour une haute disponibilité pour effectuer une mise à niveau zéro temps d'arrêt

August 20, 2021

Au cours d'un processus de mise à niveau régulier dans une configuration haute disponibilité, les deux nœuds exécutent des versions logicielles différentes. Ces deux versions peuvent avoir le même

numéro de version interne haute disponibilité ou différent.

Si les deux versions ont des numéros de version haute disponibilité différents, le basculement de connexion (même s'il est activé) pour les connexions de données existantes n'est pas pris en charge. En d'autres termes, toutes les connexions de données existantes sont perdues, ce qui entraîne des temps d'arrêt.

Pour résoudre ce problème, dans Service Software Upgrade (ISSU) peut être utilisé pour les configurations haute disponibilité. ISSU introduit une fonctionnalité de migration, qui remplace l'étape de l'opération de basculement forcé dans le processus de mise à niveau. La fonctionnalité de migration prend soin de respecter les connexions existantes et inclut l'opération de basculement forcé.

Une fois l'opération de migration effectuée, le nouveau nœud principal reçoit toujours le trafic (demande et réponse) lié aux connexions existantes mais les dirige vers l'ancien nœud principal. L'ancien nœud principal traite le trafic de données, puis les envoie directement à la destination.

Comment fonctionne le système ISU amélioré

Le processus de mise à niveau standard dans une configuration haute disponibilité comprend les étapes séquentielles suivantes :

1. **Mettez à niveau le nœud secondaire**. Cette étape inclut la mise à niveau logicielle du nœud secondaire et le redémarrage du nœud.
2. **Forcer le basculement sur incident**. L'exécution du basculement forcé rend le nœud secondaire mis à niveau vers le nœud principal et le nœud principal vers le nœud secondaire.
3. **Mettez à niveau le nouveau nœud secondaire**. Cette étape inclut la mise à niveau logicielle du nouveau nœud secondaire et le redémarrage du nœud.

Pendant la période comprise entre l'étape 1 et l'étape 3, les deux nœuds exécutent des versions logicielles différentes. Ces deux versions peuvent avoir les mêmes versions internes de haute disponibilité ou différentes.

Si les deux versions ont des numéros de version haute disponibilité différents, le basculement de connexion (même s'il est activé) pour les connexions de données existantes n'est pas pris en charge. En d'autres termes, toutes les connexions de données existantes sont perdues, ce qui entraîne des temps d'arrêt.

Le processus de mise à niveau de ISSU dans une configuration haute disponibilité comprend les étapes suivantes :

1. **Mettez à niveau le nœud secondaire**. Cette étape inclut la mise à niveau logicielle du nœud secondaire et le redémarrage du nœud.
2. **opération de migration ISSU**. L'étape inclut l'opération de basculement forcé et prend en charge les connexions existantes. Après avoir effectué l'opération de migration, le nouveau

nœud principal reçoit toujours le trafic (demande et réponse) lié aux connexions existantes mais les dirige vers l'ancien nœud principal via le VLAN SYNC configuré dans le tunnel GRE. L'ancien nœud principal traite le trafic de données, puis les envoie directement à la destination. L'opération de migration ISSU est terminée lorsque toutes les connexions existantes sont fermées.

3. **Mettez à niveau le nouveau nœud secondaire**. Cette étape inclut la mise à niveau logicielle du nouveau nœud secondaire et le redémarrage du nœud.

Avant de commencer

Avant de commencer à exécuter le processus ISSU dans une configuration haute disponibilité, suivez les conditions préalables et limitations suivantes :

- Assurez-vous que le VLAN SYNC est configuré sur les deux nœuds de la configuration haute disponibilité. Pour plus d'informations, voir Restriction du trafic de synchronisation haute disponibilité à un VLAN.
- ISSU n'est pas pris en charge dans le cloud Microsoft Azure car Microsoft Azure ne prend pas en charge le tunnel GRE.
- La propagation et la synchronisation de la configuration haute disponibilité ne fonctionnent pas pendant ISSU.
- ISSU n'est pas pris en charge pour la configuration de haute disponibilité IPv6.
- ISSU n'est pas pris en charge pour les sessions suivantes :
  - Cadres Jumbo
  - Sessions IPv6
  - NAT à grande échelle (LSN)

Étapes de configuration

ISSU inclut une fonctionnalité de migration, qui remplace l'opération de basculement forcé dans le processus de mise à niveau régulier d'une configuration haute disponibilité. La fonctionnalité de migration prend soin de respecter les connexions existantes et inclut l'opération de basculement forcé.

Au cours du processus ISSU d'une configuration haute disponibilité, vous exécutez l'opération de migration juste après la mise à niveau du nœud secondaire. Vous pouvez effectuer l'opération de migration à partir de l'un des deux nœuds.

Procédure CLI

Pour effectuer l'opération de migration haute disponibilité à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
start ns migration
<!--NeedCopy-->
```

Procédure GUI

Pour effectuer l'opération de migration haute disponibilité à l'aide de l'interface graphique :

Accédez à **Système**, cliquez sur onglet **Informations système**, cliquez sur **onglet Migration**, puis cliquez sur **Démarrer la migration**.

Afficher les statistiques ISSU

Vous pouvez consulter les statistiques ISSU pour surveiller le processus ISSU en cours dans une configuration haute disponibilité. Les statistiques ISSUE affichent les informations suivantes :

- État actuel de l'opération de migration de ISSU
- Heure de début de l'opération de migration ISSU
- Heure de fin de l'opération de migration ISSU
- Heure de début de l'opération de restauration ISSU

Vous pouvez afficher les statistiques ISSUE sur l'un des nœuds HA à l'aide de l'interface de ligne de commande ou de l'interface graphique.

Procédure CLI

Pour afficher les statistiques ISSU à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
show ns migration
<!--NeedCopy-->
```

Procédure GUI

Pour afficher les statistiques ISSU à l'aide de l'interface graphique :

Accédez à **Système**, cliquez sur l'onglet **Informations système**, sur **onglet Migration**, puis sur **Afficher la migration**.

Annulation du processus ISSU

Les configurations haute disponibilité (HA) prennent désormais en charge la restauration du processus ISSU (In Service Software Upgrade). La fonction d'annulation ISSU est utile si vous constatez que la configuration HA pendant l'opération de migration ISSU n'est pas stable ou ne fonctionne pas à un niveau optimal comme prévu.

La restauration ISSU est applicable lorsque l'opération de migration ISSU est en cours. L'annulation ISSU ne fonctionne pas si l'opération de migration ISSU est déjà terminée. En d'autres termes, vous devez exécuter l'opération d'annulation ISSU lorsque l'opération de migration ISSU est en cours.

L'annulation ISSU fonctionne différemment en fonction de l'état de l'opération de migration ISSU lorsque l'opération ISSU est déclenchée :

- **Le basculement forcé n'a pas encore eu lieu pendant l'opération de migration ISSU**. La restauration ISSU arrête l'opération de migration ISSU et supprime toutes les données internes liées à la migration ISSU stockées dans les deux nœuds. Le nœud principal actuel reste en tant que nœud principal et continue de traiter le trafic de données lié aux connexions existantes et nouvelles.
- **Le basculement forcé s'est produit lors de l'opération de migration ISSU**. Si le basculement de haute disponibilité s'est produit pendant l'opération de migration ISSU, le nouveau nœud principal (par exemple N1) traite le trafic lié aux nouvelles connexions. L'ancien nœud principal (nouveau nœud secondaire, disons qu'il s'agit de N2) traite le trafic lié aux anciennes connexions (connexions existantes avant l'opération de migration ISSU).

  La restauration ISSU arrête l'opération de migration ISSU et déclenche un basculement forcé. Le nouveau nœud principal (N2) commence maintenant à traiter le trafic lié aux nouvelles connexions. Le nouveau nœud principal (N2) continue également de traiter le trafic lié aux anciennes connexions (connexions existantes établies avant l'opération de migration ISSU). En d'autres termes, les connexions existantes établies avant l'opération de migration ISSU ne sont pas perdues.

  Le nouveau nœud secondaire (N1) supprime toutes les connexions existantes (nouvelles connexions créées lors de l'opération de migration ISSU) et ne traite aucun trafic. En d'autres termes, toutes les connexions existantes qui ont été établies après le basculement forcé de l'opération de migration ISSU sont perdues à jamais.

Étapes de configuration

Vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique Citrix ADC pour effectuer l'opération d'annulation de ISSU.

Procédure CLI

Pour effectuer l'opération de restauration ISSU à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
stop ns migration
<!--NeedCopy-->
```

Procédure GUI

Pour effectuer l'opération de restauration ISSU à l'aide de l'interface graphique :

Accédez à **Système**, cliquez sur onglet **Informations système**, cliquez sur **onglet Migration**, puis cliquez sur **Arrêter la migration**.

interruptions SNMP pour le processus de mise à niveau logicielle en service

Le processus ISSU (In Service Software Upgrade) pour une configuration haute disponibilité prend en charge les messages d'interruption SNMP suivants au début et à la fin de l'opération de migration ISSU.

Interruption SNMP	Description
migrationStarted	Cette interruption SNMP est générée et envoyée aux écouteurs SNMP configurés au démarrage de l'opération de migration ISSU.
migrationComplete	Cette interruption SNMP est générée et envoyée aux écouteurs SNMP configurés lorsque l'opération de migration ISSU est terminée.

Le nœud principal (avant le début du processus ISSU) génère toujours ces deux interruptions SNMP et les envoie aux écouteurs SNMP configurés.

Aucune alarme SNMP n'est associée aux interruptions SNMP ISSU. En d'autres termes, ces interruptions sont générées indépendamment de toute alarme SNMP. Il suffit de configurer les écouteurs SNMP d'interruption.

Pour plus d'informations sur la configuration des écouteurs d'interruptions SNMP, consultez les interruptions SNMP sur Citrix ADC.

Rétrograder une paire haute disponibilité

August 20, 2021

Vous pouvez passer à n'importe quelle version sur une paire haute disponibilité à l'aide de l'interface de ligne de commande. L'interface graphique ne prend pas en charge le processus de rétrogradation.

Pour rétrograder le logiciel système sur une paire Citrix ADC dans une paire haute disponibilité, vous devez d'abord rétrograder le logiciel sur le nœud secondaire, puis sur le nœud principal. Pour obtenir des instructions sur la rétrogradation de chaque nœud séparément, reportez-vous à la section Déclassement d'une appliance autonome Citrix ADC.

> **Important**
>
> Une perte de configuration peut se produire lors de la rétrogradation. Vous devez comparer les configurations avant et après la rétrogradation, puis saisir manuellement les entrées manquantes.

Résolution des problèmes liés aux processus d'installation, de mise à niveau et de rétrogradation

October 5, 2021

Si la solution matérielle-logicielle ne fonctionne pas comme prévu une fois le processus d'installation, de mise à niveau ou de mise à niveau antérieure terminé, la première chose à faire est de rechercher les causes les plus courantes du problème.

Ressources pour le dépannage

Pour obtenir de meilleurs résultats, utilisez les ressources suivantes pour résoudre un problème lié à l'installation, à la mise à niveau ou à la rétrogradation d'un Citrix ADC :

- Les fichiers de configuration de la solution matérielle-logicielle. Dans le cas d'une paire haute disponibilité, les fichiers de configuration des deux solutions matérielles-logicielles.
- Les fichiers suivants de la ou des solutions matérielle-logicielles :
  - Les fichiers newnslog pertinents.
  - Le fichier ns.log.
  - Le fichier de messages.
- Un diagramme de topologie du réseau.

Problèmes et résolutions

Voici les problèmes d'installation, de mise à niveau et de rétrogradation les plus courants, ainsi que des conseils pour les résoudre :

1. **Problème**

   La mise à niveau d'une appliance Citrix ADC MPX échoue en raison d'une incompatibilité matérielle et logicielle.

   Résolution

   Consultez la matrice de compatibilité matérielle et logicielle Citrix ADC MPX et vérifiez si la version logicielle est prise en charge sur le matériel Citrix ADC MPX.

2. **Problème**

   La mise à niveau d'un dispositif Citrix ADC VPX échoue en raison de l'incompatibilité de l'appliance Citrix ADC VPX et de l'hyperviseur.

   Résolution

   Consultez la matrice de compatibilité de l'appliance Citrix ADC VPX et de l'hyperviseur et vérifiez si le modèle d'appliance Citrix ADC VPX est pris en charge sur l'hyperviseur.

3. **Problème**

   La mise à niveau d'une appliance Citrix ADC échoue en raison d'erreurs matérielles.

   Résolution

   Valider l'intégrité de l'appliance Citrix ADC. Si vous disposez d'une appliance matérielle Citrix ADC, Citrix vous recommande `fsck` d'exécuter une vérification de disque et de valider l'intégrité du disque dur Citrix ADC.

   Pour plus d'informations, consultez Comment vérifier l'intégrité du système de fichiers d'une appliance Citrix ADC.

4. **Problème**

   La mise à niveau d'une appliance Citrix ADC à l'aide de l'interface graphique se bloque.

   Résolution

   Actualisez le navigateur pour vérifier si la mise à niveau progresse ou non.

5. **Problème**

   La mise à niveau d'une appliance Citrix ADC échoue en raison du manque d'espace dans le répertoire /var

   Résolution

Libérez de l'espace sur le répertoire /var. Pour plus d'informations, reportez-vous à la section Comment libérer de l'espace dans le répertoire /var.

6. **Problème**

   Le Citrix ADC n'est pas accessible après la mise à niveau du logiciel

   Cause

   Au cours du processus de mise à niveau du logiciel, si le fichier de configuration de la version et de la version existantes ne correspond pas au fichier de configuration de la version et de la version antérieures, l'appliance ne peut pas charger la configuration et l'adresse IP par défaut est attribuée à la solution matérielle-logicielle.

   Résolution

   - Vérifiez que la solution matérielle-logicielle est accessible depuis la console.
   - Vérifiez l'adresse NSIP et les routes sur la solution matérielle-logicielle.
     - Si l'adresse IP est passée à l'adresse IP 192.168.100.1 par défaut, modifiez l'adresse IP si nécessaire.
     - Vérifiez que la solution matérielle-logicielle est accessible.

7. **Problème**

   Au cours d'une mise à niveau, si j'exécute la commande de synchronisation, le message suivant apparaît :

   La commande a échoué sur le nœud secondaire, mais a réussi sur le nœud principal.

   Résolution

   N'exécutez aucune commande dépendante (set /unset /bind /unbind) lorsque la synchronisation haute disponibilité (HA) est en cours.

8. **Problème**

   Au cours d'un processus de mise à niveau, le trafic ne passe pas par le nouveau nœud principal lorsque vous exécutez la commande de basculement forcé.

   Résolution

   - Recherchez les problèmes liés à la topologie du réseau et aux configurations des commutateurs.
   - Exécutez la commande set L2Param -garpreply ENABLED pour activer la réponse GARP.
   - Essayez d'utiliser un MAC virtuel s'il n'est pas déjà utilisé.
   - Exécutez la commande sendarp —a depuis le nœud principal.

9. **Problème**

   Après la mise à niveau ou la rétrogradation d'une appliance Citrix ADC, la connexion à l'appliance échoue via SSH.

Résolution

Effectuez les opérations suivantes dans l'appliance Citrix ADC :

- Supprimez les clés d'hôte anciennes ou non sécurisées à l'adresse /nsconfig/ssh/ssh_host_*.
- Consultez la configuration SSHD personnalisée à l'adresse /nsconfig/sshd_config et vérifiez si elle est toujours pertinente et compatible. Renommez ou supprimez la configuration SSHD personnalisée en conséquence.
- Redémarrage à froid de l'appliance Citrix ADC

10. **Problème**

    Dans une paire HA, après avoir exécuté la commande Forcer le basculement HA, les périphériques continuent de redémarrer. Le périphérique secondaire n'apparaît pas après une mise à niveau.

    Résolution

    Vérifiez si le répertoire /var est plein. Si c'est le cas, supprimez les anciens fichiers d'installation. Exécutez la commande df —h pour afficher l'espace disque disponible.

11. **Problème**

    Après la mise à niveau d'une paire HA, l'un des nœuds est répertorié comme état UNKNOWN.

    Résolution

    - Vérifiez si les deux nœuds exécutent la même version. Si les versions ne sont pas identiques et que les nœuds HA ne correspondent pas à la version, certains champs sont affichés comme UNKNOWN lorsque vous exécutez la commande show ha node.
    - Vérifiez si la solution matérielle-logicielle secondaire est accessible.

12. **Problème**

    Après la mise à niveau de Citrix ADC, l'interface indique que la plupart des serveurs et services virtuels d'équilibrage de charge sont en PANNE.

    Résolution

    Vérifiez que l'adresse SNIP est active sur la solution matérielle-logicielle secondaire. Tapez également la commande show service pour voir si le service est en cours d'exécution.

13. **Problème**

    Après avoir effectué une mise à niveau, tous les serveurs virtuels sont en panne sur le dispositif secondaire.

    Résolution

    Activez l'état HA et la synchronisation HA en exécutant les commandes suivantes :

- définir le nœud hastate enable
- activer le mode hasync du nœud

La désactivation de l'HA n'est pas recommandée.

14. **Problème**

    Après avoir effectué une mise à niveau antérieure, Citrix ADC ne démarre pas correctement.

    Résolution

    Vérifiez si la licence correcte a été installée.

15. **Problème**

    Dans une paire HA, certaines fonctionnalités ne sont pas synchronisées après une mise à niveau.

    Résolution

    Exécutez la commande sync ha file misc pour synchroniser les fichiers de configuration du nœud principal vers le nœud secondaire.

16. **Problème**

    Au cours du redémarrage, le message d'erreur suivant s'affiche :

    Une ou plusieurs commandes dans ns.conf ont échoué. Que dois-je faire ?

    Résolution

    Assurez-vous qu'aucune commande du fichier ns.conf ne dépasse la limite de 255 octets. Dans les commandes qui créent des stratégies trop longues pour la limite de 255 octets, vous pouvez utiliser des jeux de modèles pour raccourcir les stratégies.

    Exemple :

    ```
    1 add cs policy p11 -rule 'HTTP.REQ.URL.ENDSWITH_ANY("
        ctx_file_extensions")'
    2 Done
    3 <!--NeedCopy-->
    ```

    ctx_file_extensions est un jeu de patset par défaut qui couvre un grand nombre d'extensions. En plus des jeux de motifs par défaut, vous pouvez créer des jeux de motifs définis par l'utilisateur. Ajoutez un patset en exécutant la commande suivante :

    ```
    1 add patset <name>
    2 <!--NeedCopy-->
    ```

    Remarque : Les patsets sont pris en charge uniquement dans la version 9.3 ou ultérieure.

17. **Problème**

Lors de la mise à niveau d'une appliance Citrix ADC VPX, on me dit de libérer de l'espace dans /var. Quels fichiers dois-je supprimer ?

Résolution

Supprimez les anciens fichiers d'installation du répertoire /var/tmp/. Supprimez également les fichiers indésirables de /flash.

18. **Problème**

    Il n'y a pas de connectivité à l'interface utilisateur graphique (GUI) lorsque vous exécutez la commande forcer le basculement HA sur le dispositif secondaire.

    Résolution

    Ouvrez une session sur l'appliance secondaire à l'aide de l'interface de ligne de commande et activez l'accès à l'interface graphique en exécutant la <IP>commande set ns ip -gui enabled.

19. **Problème**

    Après avoir effectué une mise à niveau, et lorsque je clique sur un lien de l'interface graphique qui doit charger une applet Java (Assistant de mise à niveau ou assistant de licence), le message d'erreur suivant apparaît : la version de l' **interface graphique ne correspond pas à la version du noyau. Fermez cette instance, videz le cache du plug-in Java et rouvrez-la**.

    Résolution

    - Ouvrez une session sur Citrix ADC à l'aide de l'interface graphique.
    - Accédez à Citrix ADC Gateway > Paramètres globaux.
    - Cliquez sur Modifier les paramètres globaux sous Paramètres.
    - Dans le volet d'informations, sous Expérience client, sélectionnez Par défaut dans la liste des thèmes de l'interface utilisateur.
    - Cliquez sur OK.

20. **Problème**

    Si la mise à niveau d'une appliance Citrix ADC a échoué pour une raison quelconque, comment restaurer l'appliance à l'aide des fichiers sauvegardés ?

    Résolution

    Si la mise à niveau échoue, restaurez l'appliance à la version précédente de l'appliance Citrix ADC à l'aide des fichiers sauvegardés. Pour plus d'informations, voir Sauvegarde et restauration d'une appliance Citrix ADC.

    Pour plus d'informations sur la sauvegarde et la restauration d'une configuration de cluster Citrix ADC, voir Sauvegarde et restauration d'une configuration de cluster.

21. **Problème**

Si des licences sont manquantes après l'échec de la mise à niveau d'une appliance Citrix ADC, comment résoudre le problème ?

Résolution

Si une licence est manquante ou si vous souhaitez réallouer les licences, reportez-vous à la rubrique Présentation des licencesci-dessous.

> **Remarque**
>
> Ces étapes de dépannage s'appliquent également aux problèmes de perte de configuration lors de la rétrogradation du logiciel sur plusieurs versions.
>
> Pour tout autre problème, consultez les notes de mise à jour, les articles du centre de connaissances et les FAQ.

FAQ

August 20, 2021

Pour obtenir des réponses aux questions que vous pourriez avoir sur la mise à niveau du microprogramme Citrix ADC, consultez la FAQ sur l'installation, la mise à niveau et la mise à niveau.

Solutions pour les fournisseurs de services de télécommunication

January 21, 2021

Les technologies de l'information et de la communication (TIC) ont pour but de rapprocher l'internaute des applications et des données. Les dernières technologies de datacenter ont permis à l'utilisateur, aux applications et aux données de se trouver n'importe où. Un utilisateur peut accéder aux applications et aux données depuis le bureau, depuis sa maison ou depuis un lieu tel qu'un aéroport. Les applications et les données peuvent être situées dans les locaux de l'entreprise, dans un cloud public ou privé, ou sur un hôte hybride. Le résultat n'a été qu'une augmentation de la productivité, mais aussi une réduction des coûts de propriété et d'entretien.

Le service fournit l'infrastructure de base nécessaire pour transporter les applications et les données de l'utilisateur sur le réseau. Étant donné que l'infrastructure de base dessert des millions d'abonnés et qu'une grande variété d'applications et de données, les exigences en matière d'évolutivité et de prise en charge des protocoles sont très élevées. L'infrastructure centrale gère deux grands types de trafic : le plan de données et le plan de contrôle. Chacun de ces avions a ses propres exigences d'échelle et de support de protocole.

Le plan de données est la partie de l'infrastructure centrale qui transporte les applications utilisateur et les données de bout en bout, c'est-à-dire entre l'équipement de l'utilisateur final et le serveur d'applications. Le nombre d'utilisateurs accédant aux applications et aux données se chiffre à des milliers de millions, de sorte que les exigences en matière de débit et d'adressage IP sont très élevées. Chaque utilisateur du réseau doit être identifiable de manière unique. Ce n'est qu'alors que le fournisseur de services peut contrôler le trafic, surveiller l'utilisation du réseau, fournir des services spécifiques à l'utilisateur et consigner correctement les informations. De nombreux périphériques clients et serveurs d'applications d'aujourd'hui prennent en charge IPv6 en mode natif. L'infrastructure de base doit non seulement prendre en charge un mélange de clients et de serveurs IPv4 et IPv6, mais aussi fournir les technologies de communication croisée entre IPv4 et IPv6. Enfin, un fournisseur de services est mesuré par la qualité du service (directement liée à l'expérience de l'utilisateur final) et la disponibilité du service sans interruption. Le plan de données doit être suffisamment résilient pour fournir à la fois qualité et disponibilité.

L'infrastructure du plan de contrôle gère le trafic utilisateur et maintient les services d'exploitation de l'entreprise et du réseau. Les protocoles les plus importants qui s'exécutent dans ce plan sont Diameter, Rayon et SMPP. Le Diameter est un protocole de base sur lequel plusieurs autres protocoles spécifiques à la fonction ont été développés. Par exemple :

- Interface Gx entre la fonction d'application des politiques et des frais (PCEF) et la fonction de règlement et de facturation (PCRF)
- Interface Gy entre le système de chargement en ligne (OCS) et la passerelle réseau de données de paquets Cisco (PGW) /Policy and Charging Enforcement Function (PCEF)

Le volume du trafic du plan de contrôle est directement proportionnel à l'activité de l'utilisateur. Pour gérer le trafic du plan de contrôle, les fournisseurs de services utilisent plusieurs fonctionnalités ADC, telles que l'équilibrage de charge et la commutation de contenu. Ils ont besoin d'un contrôle à grain fin du trafic des avions de contrôle, ce qui équivaut à la complexité du trafic des avions de données.

Les fournisseurs de services doivent respecter des ententes de niveau de service (SLA) exigeantes et sont examinés de près par les organismes de réglementation pour s'assurer de leur conformité. Le respect des exigences tout en gérant les données et le trafic des avions de contrôle nécessite un fournisseur de services pour maintenir son infrastructure agile, dans les limites du budget, facilement évolutive et flexible. En tant qu'ADC les plus puissants et les plus avancés du marché aujourd'hui, les produits Citrix ADC s'adaptent naturellement à l'environnement des fournisseurs de services.

NAT à grande échelle

January 21, 2021

> **Remarque**
>
> Cette fonctionnalité est disponible avec une licence Citrix ADC Advanced ou Premium Edition.

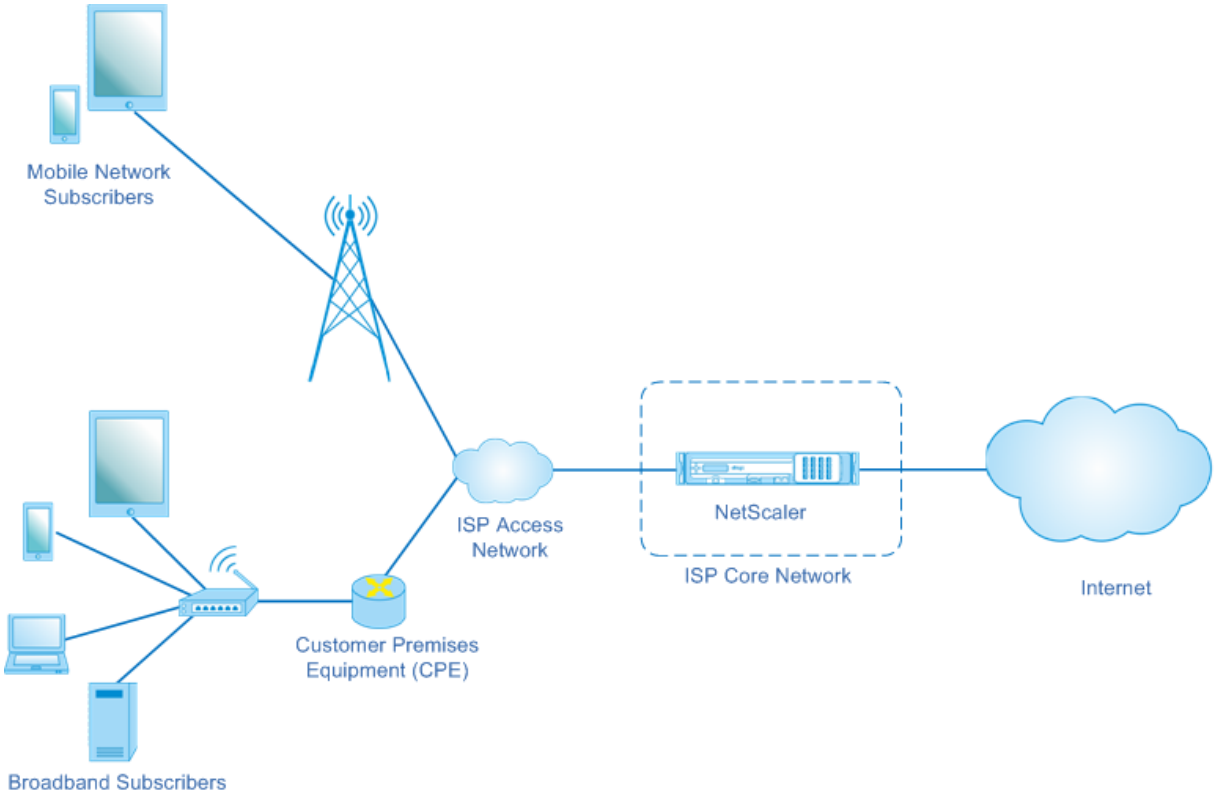
La croissance phénoménale d'Internet a entraîné une pénurie d'adresses IPv4 publiques. Large Scale NAT (LSN/CGNAT) fournit une solution à ce problème, maximisant l'utilisation des adresses IPv4 publiques disponibles en partageant quelques adresses IPv4 publiques parmi un grand nombre d'utilisateurs d'Internet.

LSN traduit les adresses IPv4 privées en adresses IPv4 publiques. Il inclut des méthodes de traduction d'adresse réseau et de port pour agréger de nombreuses adresses IP privées en moins d'adresses IPv4 publiques. LSN est conçu pour gérer NAT à grande échelle. La fonctionnalité Citrix ADC LSN est très utile pour les fournisseurs d'accès Internet (FAI) et les entreprises fournissant des millions de traductions pour prendre en charge un grand nombre d'utilisateurs (abonnés) et à un débit très élevé.

Architecture LSN

L'architecture LSN d'un fournisseur de services Internet utilisant les produits Citrix se compose d'abonnés (utilisateurs d'Internet) dans des espaces d'adressage privés accédant à Internet via une appliance Citrix ADC déployée dans le réseau central du fournisseur de services Internet. Les abonnés sont connectés au FAI par l'intermédiaire du réseau d'accès du FAI. Habituellement, les abonnés à des fins commerciales d'Internet sont directement connectés au réseau d'accès du FSI. Pour desservir ces abonnés, il n'y a qu'un seul niveau de NAT (NAT44).

Toutefois, les abonnés non commerciaux sont généralement derrière l'équipement local du client (CPE), comme les routeurs et les modems, qui implémente également NAT. Ces deux niveaux de NAT créent le modèle NAT444. Le déploiement d'une appliance Citrix ADC dans le réseau central d'un fournisseur de services Internet pour la fonctionnalité LSN est transparent pour les abonnés et ne nécessite aucune modification de configuration pour les abonnés ou les CPE.



Large Scale NAT

L'appliance Citrix ADC reçoit tous les paquets d'abonnés destinés à Internet. L'appliance est configurée avec un pool d'adresses IP NAT prédéfinies à utiliser pour LSN. L'appliance Citrix ADC utilise sa fonctionnalité LSN pour traduire l'adresse IP source (privée) et le port du paquet vers l'adresse IP NAT (publique) et le port NAT, puis envoie le paquet à sa destination sur Internet. L'appliance conserve un enregistrement de toutes les sessions actives qui utilisent la fonction LSN. Ces sessions sont appelées sessions LSN. L'appliance Citrix ADC gère également les mappages entre l'adresse IP et le port de l'abonné, et l'adresse IP NAT et le port, pour chaque session. Ces mappings sont appelés mappings LSN. À partir des sessions LSN et des mappages LSN, l'appliance Citrix ADC reconnaît un paquet de réponse (reçu d'Internet) appartenant à une session particulière. L'appliance convertit l'adresse IP de destination et le port du paquet de réponse de l'adresse IP NAT:port vers l'adresse IP de l'abonné : port, et envoie le paquet traduit à l'abonné.

Fonctionnalités LSN prises en charge sur l'appliance Citrix ADC

Voici quelques-unes des fonctionnalités LSN prises en charge sur l'appliance Citrix ADC :

Affectation des ressources NAT

L'appliance Citrix ADC alloue des adresses IP et des ports NAT, à partir de son pool de ressources NAT prédéfini, aux abonnés afin de traduire leurs paquets pour transmission vers des hôtes externes (In-

ternet). L'appliance Citrix ADC prend en charge les types suivants d'adresse IP NAT et d'allocation de port pour les abonnés :

- **Déterministe.** L'appliance Citrix ADC alloue une adresse IP NAT et un bloc de ports à chaque abonné. L'appliance alloue séquentiellement des ressources NAT à ces abonnés. Elle attribue le premier bloc de ports sur l'adresse IP NAT de début à l'adresse IP de l'abonné de début. La plage suivante de ports est attribuée à l'abonné suivant, et ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné suivant. À ce stade, le premier bloc de port sur l'adresse NAT suivante est affecté à l'abonné, et ainsi de suite.

  L'appliance Citrix ADC consigne l'adresse IP NAT allouée et le bloc de port pour un abonné. Pour une connexion, un abonné peut être identifié uniquement par son adresse IP NAT mappée et son bloc de port. Pour cette raison, l'appliance Citrix ADC ne consigne aucune session LSN créée ou supprimée. Si l'ensemble du bloc de ports est utilisé, l'appliance Citrix ADC supprime toute nouvelle connexion de l'abonné.

- **Dynamique.** L'appliance Citrix ADC alloue une adresse IP NAT aléatoire et un port du pool NAT LSN pour la connexion d'un abonné. Lorsque l'allocation de bloc de ports est activée dans la configuration, l'appliance alloue une adresse IP NAT aléatoire et un bloc de ports pour un abonné lorsqu'elle initie une connexion pour la première fois. L'appliance Citrix ADC alloue ensuite cette adresse IP NAT et l'un des ports du bloc alloué à chaque connexion ultérieure de cet abonné. Si l'ensemble du bloc de ports est utilisé, l'appliance alloue un nouveau bloc de ports aléatoire à l'abonné lorsqu'elle initie une nouvelle connexion. Un des ports du nouveau bloc de ports est alloué pour la nouvelle connexion.

Pool d'adresses IP

Les options d'allocation de ressources NAT suivantes sont disponibles pour les sessions suivantes d'un abonné qui a reçu une adresse IP NAT aléatoire et un port pour une session existante.

- **Couplé.** L'appliance Citrix ADC alloue la même adresse IP NAT pour toutes les sessions associées au même abonné. Lorsqu'aucun autre port n'est disponible pour cette adresse, l'appliance supprime les nouvelles connexions de l'abonné. Cette option est nécessaire pour le bon fonctionnement de certaines applications nécessitant la création de plusieurs sessions sur la même adresse IP source (par exemple dans les applications peer-to-peer qui utilisent le protocole RTP ou RTCP.
- **Aléatoire.** L'appliance Citrix ADC alloue des adresses IP NAT aléatoires, à partir du pool, pour différentes sessions associées au même abonné.

Réutilisation des mappages LSN

L'appliance Citrix ADC peut réutiliser un mappage LSN existant pour les nouvelles connexions provenant de la même adresse IP et du même port d'abonné. La fonctionnalité Citrix ADC LSN prend

en charge les types suivants de réutilisation du mappage LSN :

1. **Indépendant du point de terminaison.** L'appliance Citrix ADC réutilise le mappage LSN pour les paquets suivants envoyés à partir de la même adresse IP d'abonné et du même port (x:x) vers n'importe quelle adresse IP et port externes. Ce type de réutilisation du mapping LSN est utile pour le bon fonctionnement des applications VOIP et peer-to-peer.
2. **Dépendante de l'adresse.** L'appliance Citrix ADC réutilise le mappage LSN pour les paquets suivants envoyés à partir de la même adresse IP d'abonné et du même port (x:x) vers la même adresse IP externe (Y), quel que soit le port externe.
3. **Dépendante du port d'adresse.** L'appliance Citrix ADC réutilise le mappage LSN pour les paquets suivants envoyés à partir de la même adresse IP interne et du même port (x:x) vers la même adresse IP externe et le même port (Y:y) lorsque le mappage est toujours actif.

Filtrage LSN

L'appliance Citrix ADC peut filtrer les paquets des hôtes externes en fonction des sessions LSN actives et des mappages LSN. Prenons un exemple de mappage LSN qui inclut le mappage de l'abonné IP:Port (x:x), NAT IP:Port (n:n) et de l'hôte externe IP:Port (Y:y). La fonctionnalité Citrix ADC LSN prend en charge les types de filtrage suivants :

1. **Indépendant du point de terminaison.** L'appliance Citrix ADC filtre uniquement les paquets qui ne sont pas destinés à NAT IP:Port (n:n), qui représente l'abonné IP:Port (x:x), indépendamment de l'adresse IP de l'hôte externe et de la source du port (z:z). L'appliance Citrix ADC transfère tous les paquets destinés à X:x. En d'autres termes, l'envoi de paquets de l'abonné à n'importe quelle adresse IP externe est suffisant pour autoriser les paquets de n'importe quel hôte externe à l'abonné. Ce type de filtrage est utile pour le bon fonctionnement des applications VoIP et peer-to-peer.
2. **Dépendante de l'adresse.** L'appliance Citrix ADC filtre les paquets qui ne sont pas destinés à NAT IP:Port (n:n), qui représente l'abonné IP:Port (X:x). En outre, l'appliance filtre les paquets de l'adresse IP de l'hôte externe et du port (Y:y) destinés à n:n si l'abonné n'a pas déjà envoyé de paquets à Y:AnyPort (indépendant du port externe). En d'autres termes, la réception de paquets à partir d'un hôte externe spécifique nécessite que l'abonné envoie d'abord des paquets à l'adresse IP de cet hôte externe spécifique.
3. **Dépendante du port d'adresse.** L'appliance Citrix ADC filtre les paquets qui ne sont pas destinés à NAT IP:Port (n:n), qui représente l'abonné IP:Port (X:x). En outre, l'appliance filtre les paquets de l'adresse IP de l'hôte externe et du port (Y:y) destinés à n:n si l'abonné n'a pas déjà envoyé de paquets à Y:y. En d'autres termes, la réception de paquets à partir d'un hôte externe spécifique nécessite que l'abonné envoie d'abord des paquets à cette adresse IP externe et au port spécifiques.

Quotas

L'appliance Citrix ADC peut limiter le nombre de ports et de sessions NAT pour chaque abonné afin d'assurer une répartition équitable des ressources entre les abonnés. L'appliance Citrix ADC peut également limiter le nombre de sessions d'un groupe d'abonnés afin d'assurer une répartition équitable des ressources entre les différents groupes d'abonnés.

- **Quota de port.** L'appliance Citrix ADC peut limiter les ports NAT LSN à utiliser à la fois par chaque abonné pour un protocole spécifié. Par exemple, vous pouvez limiter chaque abonné à un maximum de 500 ports NAT TCP. Lorsque les mappages NAT LSN pour un abonné atteignent la limite, l'appliance Citrix ADC n'alloue pas de ports NAT supplémentaires du protocole spécifié à cet abonné.
- **Limite de session d'abonné.** Le nombre de sessions simultanées pour un abonné peut être supérieur au quota de port. L'appliance Citrix ADC peut limiter les sessions LSN autorisées pour chaque abonné pour un protocole spécifié. Lorsque le nombre de sessions LSN atteint la limite pour un abonné, l'appliance Citrix ADC ne permet pas à l'abonné d'ouvrir des sessions supplémentaires du protocole spécifié.
- **Limite de session de groupe.** L'appliance Citrix ADC peut limiter le nombre total de sessions LSN autorisées pour un groupe d'abonnés pour un protocole spécifié. Lorsque le nombre total de sessions LSN atteint la limite d'un groupe pour un protocole spécifié, l'appliance Citrix ADC n'autorise aucun abonné du groupe à ouvrir des sessions supplémentaires du protocole spécifié. Par exemple, Vous limitez un groupe à un maximum de 10000 sessions UDP. Lorsque le nombre total de sessions UDP pour ce groupe atteint 10000, l'appliance Citrix ADC n'autorise aucun abonné du groupe à ouvrir des sessions UDP supplémentaires.

Passerelles de couche d'application

Pour certains protocoles de couche Application, les adresses IP et les numéros de port de protocole sont également communiqués dans la charge utile du paquet. Application Layer Gateway for a protocol analyse la charge utile du paquet et effectue les modifications nécessaires pour s'assurer que le protocole continue de fonctionner sur LSN.

L'appliance Citrix ADC prend en charge ALG pour les protocoles suivants :

- FTP
- ICMP
- TFTP
- PPTP
- SIP
- RTSP

Support en épingle à cheveux

L'appliance Citrix ADC prend en charge la communication entre les abonnés ou les hôtes internes à l'aide d'adresses IP NAT. Ce type de communication entre deux abonnés utilisant des adresses IP NAT est appelé flux en épingle à cheveux. Le flux en épingle à cheveux est activé par défaut et vous ne pouvez pas le désactiver.

Points à considérer avant de configurer LSN

January 21, 2021

Tenez compte des points suivants avant de configurer LSN sur une appliance Citrix ADC :

- Assurez-vous de bien comprendre les différents composants du NAT à grande échelle, décrits dans les RFC 6888, 5382, 5508 et 4787.
- Le mappage indépendant des points de terminaison (EIM) et le filtrage indépendant des points de terminaison (EIF) sont désactivés par défaut. Ces options doivent être activées pour le bon fonctionnement des applications VoIP et peer-to-peer (P2P).
- **Journalisation LSN** : Voici les points de considération pour l'enregistrement des informations LSN :
  - Citrix recommande de consigner les informations LSN sur des serveurs de journaux externes plutôt que sur l'appliance Citrix ADC. La journalisation sur des serveurs externes facilite les performances optimales lorsque l'appliance crée un grand nombre d'entrées de journal LSN (par ordre de millions).
  - Citrix recommande l'utilisation de SYSLOG sur TCP, ou NSLOG. Par défaut, SYSLOG utilise UDP et NSLOG utilise uniquement TCP pour transférer les informations de journal vers les serveurs de journaux. TCP est plus fiable que UDP pour le transfert de données complètes.
  - Les limitations suivantes s'appliquent à SYSLOG sur TCP :
    * La solution Syslog sur TCP ne fournit pas l'authentification, la vérification de l'intégrité et la confidentialité.
    * L'appliance Citrix ADC s'appuie sur le protocole TCP pour confirmer la remise des messages SYSLOG aux serveurs de journaux externes.
- **Haute disponibilité** : Voici les points à considérer pour la haute disponibilité des appliances Citrix ADC pour LSN :
  - Citrix recommande de configurer la fonctionnalité LSN dans un déploiement haute disponibilité de deux appliances Citrix ADC pour un fonctionnement continu et continu de toutes les sessions LSN.
  - Dans un déploiement à haute disponibilité, Citrix recommande :
    * Définition du paramètre VLAN SYNC pour dédier un VLAN à toutes les communications liées à la haute disponibilité.

        * Synchronisation de la clé RSS symétrique du nœud principal vers le nœud secondaire pour la synchronisation avec état d'un grand nombre de mappages et de sessions LSN.
        * Liaison du sous-réseau des adresses IP LSN à un VLAN pour éviter l'inondation des diffusions GARP sur tous les VLAN après un basculement.
    - Dans un déploiement à haute disponibilité des appliances Citrix ADC, les sessions associées à ALG ne sont pas mises en miroir avec l'appliance secondaire.
- **Application Layer Gateways (ALG)** : Voici les points de considération associés aux ALG sur une appliance Citrix ADC :
    - Les éléments suivants ne sont pas pris en charge pour SIP ALG :
        * Adresses IP de multidiffusion
        * SDP chiffré
        * Messages SIP sur TLS
        * Traduction de nom complet dans les messages SIP
        * Authentification des messages SIP
        * Domaines de trafic, partitions d'administration et clusters ADC Citrix.
        * Messages SIP avec corps en plusieurs parties.
    - Les éléments suivants ne sont pas pris en charge pour RTSP ALG :
        * Sessions RTSP multidiffusion
        * Session RTSP via UDP
        * Domaines de trafic ADC Citrix, partitions d'administration et clusters Citrix ADC
    - L'appliance Citrix ADC ne prend pas en charge ALG pour le protocole IPSec.
- Si vous désactivez la fonctionnalité LSN lorsque certaines sessions LSN existent sur l'appliance Citrix ADC, ces sessions continuent d'exister pendant la durée de l'intervalle de temporisation configuré.
- LSN a préséance sur RNAT. Si un paquet d'un abonné LSN spécifié correspond également à une règle RNAT, le paquet est traduit selon la configuration LSN.
- Le transfert des paquets liés uniquement aux sessions LSN est basé sur la table de routage de l'appliance Citrix ADC.
- Contrairement aux adresses IP de sous-réseau, la sélection d'une adresse IP NAT LSN pour la connexion d'un abonné n'est pas basée sur l'entrée de routage de l'adresse IP de destination.
- Pour les paquets entrants, les mappages LSN statiques ont priorité sur les mappages LSN dynamiques.
- Pour les paquets sortants, les profils d'application LSN ont priorité sur le mappage statique.
- Lorsqu'un grand nombre de sessions LSN (> 1 million) existent sur l'appliance Citrix ADC, Citrix recommande d'afficher les sessions LSN sélectionnées au lieu de toutes. Dans l'interface de ligne de commande ou l'utilitaire de configuration, utilisez les paramètres de sélection pour afficher l'opération de session LSN.
- Pour réduire la quantité de mémoire active allouée à la fonctionnalité LSN, vous devez redé-

marrer l'appliance Citrix ADC après avoir modifié le paramètre de mémoire configurée. Sans un redémarrage chaud, vous ne pouvez augmenter que la quantité de mémoire active.

Étapes de configuration de LSN

August 20, 2021

La configuration de LSN sur une appliance Citrix ADC comporte les tâches suivantes :

1. **Définissez les paramètres LSN globaux.** Les paramètres globaux incluent la quantité de mémoire Citrix ADC réservée à la fonctionnalité LSN et la synchronisation des sessions LSN dans une configuration haute disponibilité.
2. **Créez une entité client LSN et liez-y les abonnés.** Une entité client LSN est un ensemble d'abonnés sur le trafic desquels vous souhaitez que l'appliance Citrix ADC exécute LSN. L'entité client inclut des adresses IPv4 et des règles ACL étendues pour identifier les abonnés. Un client LSN peut être lié à un seul groupe LSN. L'interface de ligne de commande comporte deux commandes pour créer une entité client LSN et lier un abonné à l'entité client LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.
3. **Créez un pool LSN et liez des adresses IP NAT à celui-ci.** Un pool LSN définit un pool d'adresses IP NAT à utiliser par l'appliance Citrix ADC pour exécuter LSN. Des paramètres sont affectés au pool, tels que l'allocation de bloc de port et le type NAT (déterministe ou dynamique). Un pool de LSN lié à un groupe de LSN s'applique à tous les abonnés d'une entité cliente de LSN liée au même groupe. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés ensemble. Plusieurs pools LSN peuvent être liés à un groupe LSN. Pour NAT dynamique, un pool LSN peut être lié à plusieurs groupes LSN. Pour NAT déterministe, les pools liés à un groupe LSN ne peuvent pas être liés à d'autres groupes LSN. L'interface de ligne de commande comporte deux commandes permettant de créer un pool LSN et de lier les adresses IP NAT au pool LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.
4. **(Facultatif) Créez un profil de transport LSN pour un protocole spécifié.** Un profil de transport LSN définit divers délais d'expiration et limites, tels que les sessions LSN maximales et l'utilisation maximale des ports, qu'un abonné peut avoir pour un protocole donné. Vous liez un profil de transport LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil de transport LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP est lié à un groupe LSN lors de sa création. Ce profil est appelé profil de transport par défaut. Un profil de transport LSN que vous liez à un groupe LSN remplace le profil de transport LSN par défaut pour ce protocole.
5. **(Facultatif) Créez un profil d'application LSN pour un protocole spécifié et liez un ensem-**

ble de ports de destination à celui-ci. Un profil d'application LSN définit les contrôles de mappage LSN et de filtrage LSN d'un groupe pour un protocole donné et pour un ensemble de ports de destination. Pour un ensemble de ports de destination, vous liez un profil LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil d'application LSN lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil d'application LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP pour tous les ports de destination est lié à un groupe LSN lors de sa création. Ce profil est appelé profil d'application par défaut. Lorsque vous liez un profil d'application LSN, avec un ensemble de ports de destination spécifié, à un groupe LSN, le profil lié remplace le profil d'application LSN par défaut pour ce protocole sur cet ensemble de ports de destination. L'interface de ligne de commande comporte deux commandes pour créer un profil d'application LSN et lier un ensemble de ports de destination au profil d'application LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.

6. **Créez un groupe LSN et liez des pools LSN, des profils de transport LSN (facultatif) et des profils d'application LSN (facultatif) au groupe LSN.** Un groupe LSN est une entité composée d'un client LSN, d'un ou de plusieurs pools LSN, d'un ou de plusieurs profils de transport LSN et d'un ou de plusieurs profils d'application LSN. Des paramètres sont attribués à un groupe, tels que la taille du bloc de port et la journalisation des sessions LSN. Les paramètres s'appliquent à tous les abonnés d'un client LSN lié au groupe LSN. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés ensemble. Plusieurs pools LSN peuvent être liés à un groupe LSN. Pour NAT dynamique, un pool LSN peut être lié à plusieurs groupes LSN. Pour NAT déterministe, les pools liés à un groupe LSN ne peuvent pas être liés à d'autres groupes LSN. Une seule entité client LSN peut être liée à un groupe LSN, et une entité client LSN liée à un groupe LSN ne peut pas être liée à d'autres groupes LSN. L'interface de ligne de commande comporte deux commandes pour créer un groupe LSN et lier des pools LSN, des profils de transport LSN, des profils d'application LSN au groupe LSN. L'utilitaire de configuration combine ces deux opérations dans un seul écran.

Le tableau suivant répertorie le nombre maximal d'entités LSN différentes et de liaisons pouvant être créées sur une appliance Citrix ADC. Ces limites sont également soumises à la mémoire disponible sur l'appliance Citrix ADC.

Entités et liaisons LSN	Limite
Clients LSN	1024
Piscines LSN	128
Groupes LSN	1024
Réseaux d'abonnés pouvant être liés à un client LSN	64

Entités et liaisons LSN	Limite
ACL étendues pouvant être liées à un client LSN	1024
Adresses IP NAT dans un pool	4096
Pools LSN pouvant être liés à un groupe LSN	8
Groupes LSN pouvant utiliser le même pool LSN	16
Profils de transport LSN pouvant être liés à un groupe LSN	3 (un pour chacun pour les protocoles TCP, UDP et ICMP)
Groupes LSN pouvant utiliser le même profil de transport LSN	8
Profils d'application LSN pouvant être liés à un groupe LSN	64
Groupes LSN pouvant utiliser le même profil d'application LSN	8
Plage de ports pouvant être liée à un profil d'application LSN	8

Configuration à l'aide de l'interface de ligne de commande

Pour créer un client LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn client <clientname>

show lsn client
<!--NeedCopy-->
```

Pour lier une adresse réseau ou une règle ACL à un client LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn client <clientname> ((-network <ip_addr> [-netmask <netmask>]
    [-td<positive_integer>]) | -aclname <string>)

show lsn client
<!--NeedCopy-->
```


Pour créer un pool LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn pool <poolname> [-nattype ( DYNAMIC | DETERMINISTIC )] [-
    portblockallocation ( ENABLED | DISABLED )] [-portrealloctimeout <
    secs>] [-maxPortReallocTmq <positive_integer>]

show lsn pool
<!--NeedCopy-->
```

Pour lier une plage d'adresses IP à un pool LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

Remarque : Pour supprimer les adresses IP LSN d'un pool LSN, utilisez la commande unbind lsn pool.

Pour créer un profil de transport LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```

Pour créer un profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )] [-td <positive_integer>]

show lsn appsprofile
```



```
<!--NeedCopy-->
```

Pour lier une plage de ports de protocole d'application à un profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

Pour créer un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC |
    DETERMINISTIC )] [-portblocksize <positive_integer>] [-logging (
    ENABLED | DISABLED )] [-sessionLogging ( ENABLED | DISABLED )][-
    sessionSync (ENABLED | DISABLED )] [-snmptraplimit <positive_integer
    >] [-ftp ( ENABLED | DISABLED )]

show lsn group
<!--NeedCopy-->
```

Pour lier des profils LSN et des pools LSN à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -appsprofilename <string>)

show lsn group
<!--NeedCopy-->
```

Configuration à l'aide de l'utilitaire de configuration

Pour configurer un client LSN et lier une adresse réseau IPv4 ou une règle ACL à l'aide de l'utilitaire de configuration

Accédez à **Système** > **NAT à grande échelle** > **Clients**, puis ajoutez un client, puis liez une adresse réseau IPv4 ou une règle ACL au client.

Pour configurer un pool LSN et lier des adresses IP NAT à l'aide de l'utilitaire de configuration

Accédez à **Système > NAT à grande échelle** > **Pools**, puis ajoutez un pool, puis liez une adresse IP NAT ou une plage d'adresses IP NAT au pool.

Pour configurer un profil de transport LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Système > NAT à grande échelle > Profils**.
2. Dans le volet d'informations, cliquez sur l'onglet **Transport**, puis ajoutez un profil de transport.

Pour configurer un profil d'application LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Système > NAT à grande échelle > Profils**.
2. Dans le volet d'informations, cliquez sur onglet **Application**, puis ajoutez un profil d'application.

Pour configurer un groupe LSN et lier un client LSN, des pools, des profils de transport et des profils d'application à l'aide de l'utilitaire de configuration

Accédez à **Système > NAT à grande échelle > Groupes**, puis ajoutez un groupe, puis liez un client LSN, des pools, des profils de transport et des profils d'application au groupe.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- ajouter le client lsn
  - clientname

    Nom de l'entité client LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le client LSN créé. La condition suivante s'applique uniquement à l'interface de ligne de commande : si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "lsn client1" ou 'lsn client1').

    Il s'agit d'un argument obligatoire. Longueur maximale : 127

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- lier le client lsn
  - clientname

Nom de l'entité client LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le client LSN créé. La condition suivante s'applique uniquement à l'interface de ligne de commande : si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "lsn client1" ou 'lsn client1').

Il s'agit d'un argument obligatoire. Longueur maximale : 127

- network

  Adresse (s) IPv4 du (des) abonné (s) LSN ou réseau (s) d'abonné (s) sur le trafic duquel vous souhaitez que l'appliance Citrix ADC effectue un NAT à grande échelle.

- netmask

  Masque de sous-réseau pour l'adresse IPv4 spécifiée dans le paramètre Network.

  Valeur par défaut : 255.255.255.255

- td

  ID du domaine de trafic sur lequel appartient cet abonné ou le réseau d'abonné (tel que spécifié par le paramètre réseau).

  Si vous ne spécifiez pas d'ID, l'abonné ou le réseau d'abonnés fait partie du domaine de trafic par défaut.

  Valeur par défaut : 0

  Valeur minimale : 0

  Valeur maximale : 4094

- aclname

  Nom(s) de toute ACL étendue configurée (s) dont l'action est ALLOW. La condition spécifiée dans la règle ACL étendue identifie le trafic provenant d'un abonné LSN pour lequel l'appliance Citrix ADC doit effectuer un NAT à grande échelle. Longueur maximale : 127

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- add lsn pool
  - poolname

    Nom du pool LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un

trait d'union (-). Impossible de modifier une fois le pool LSN créé. La condition suivante s'applique uniquement à l'interface de ligne de commande : si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "lsn pool1" ou "lsn pool1").

Il s'agit d'un argument obligatoire. Longueur maximale : 127

– Nattype

Type d'adresse IP NAT et d'allocation de port (à partir des pools LSN liés à un groupe LSN) pour les abonnés (de l'entité client LSN liée au groupe LSN) :

Les options disponibles fonctionnent comme suit :

* **Déterministe** : alloue une adresse IP NAT et un bloc de ports à chaque abonné (du client LSN lié au groupe LSN). L'appliance Citrix ADC alloue séquentiellement des ressources NAT à ces abonnés. L'appliance Citrix ADC affecte le premier bloc de ports (taille de bloc déterminée par le paramètre de taille de bloc de port du groupe LSN) sur l'adresse IP NAT de début à l'adresse IP de l'abonné de début. La plage suivante de ports est attribuée à l'abonné suivant, et ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné suivant. Dans ce cas, le premier bloc de port sur l'adresse NAT suivante est utilisé pour l'abonné, et ainsi de suite. Étant donné que chaque abonné reçoit désormais une adresse IP NAT déterministe et un bloc de ports, un abonné peut être identifié sans aucune journalisation. Pour une connexion, un abonné peut être identifié uniquement en fonction de l'adresse IP et du port NAT, ainsi que de l'adresse IP et du port de destination.

* **Dynamique** : alloue une adresse IP NAT aléatoire et un port du pool NAT LSN pour une connexion d'abonnés. Si l'allocation de bloc de port est activée (dans le pool LSN) et qu'une taille de bloc de port est spécifiée (dans le groupe LSN), l'appliance Citrix ADC alloue une adresse IP NAT aléatoire et un bloc de ports pour un abonné lorsqu'il initie une connexion pour la première fois. L'appliance alloue cette adresse IP NAT et un port (à partir du bloc de ports alloué) pour différentes connexions de cet abonné. Si tous les ports sont alloués (pour différentes connexions d'abonnés) à partir du bloc de ports alloué aux abonnés, l'appliance alloue un nouveau bloc de ports aléatoire à l'abonné. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés ensemble. Plusieurs pools LSN peuvent être liés à un groupe LSN.

  Valeurs possibles : DYNAMIC, DETERMINISTIC

  Valeur par défaut : DYNAMIC

– portblockallocation

Allouer un bloc de port NAT aléatoire, à partir du pool de ports NAT disponible d'une adresse IP NAT, pour chaque abonné lorsque l'allocation NAT est définie comme NAT dynamique. Pour toute connexion initiée à partir d'un abonné, l'appliance Citrix ADC alloue un port NAT à partir du bloc de port NAT alloué aux abonnés pour créer la session LSN.

Vous devez définir la taille du bloc de port dans le groupe LSN lié. Pour un abonné, si tous les ports sont alloués à partir du bloc de ports alloué aux abonnés, l'appliance Citrix ADC alloue un nouveau bloc de ports aléatoire à l'abonné.

Pour NAT déterministe, ce paramètre est activé par défaut et vous ne pouvez pas le désactiver.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

- portrealloctimeout

  Temps d'attente, en secondes, entre la délocalisation des ports NAT LSN (lorsqu'un mappage LSN est supprimé) et leur réaffectation pour une nouvelle session LSN. Ce paramètre est nécessaire pour éviter les collisions entre les anciennes et nouvelles mappages et sessions. Il garantit que toutes les sessions établies sont interrompues au lieu de rediriger vers un autre abonné. Ceci n'est pas applicable aux ports utilisés dans :

  * NAT déterministe
  * Filtrage dépendant de l'adresse et filtrage dépendant du port d'adresse
  * NAT dynamique avec allocation de bloc de port

  Dans ces cas, les ports sont immédiatement réaffectés.

  Valeur par défaut : 0

  Valeur maximale : 600

- maxPortReallocTmq

  Nombre maximal de ports pour lesquels le délai d'expiration de réaffectation des ports s'applique à chaque adresse IP NAT. En d'autres termes, la taille maximale de la file d'attente de port désalloué pour laquelle le délai d'expiration de réaffectation s'applique à chaque adresse IP NAT.

  Lorsque la taille de la file d'attente est pleine, le prochain port désalloué est immédiatement réalloué pour une nouvelle session LSN.

  Valeur par défaut : 65536

  Valeur maximale : 65536

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- bind lsn pool
  - poolname

    Nom du pool LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le pool LSN créé. La condition suivante s'applique uniquement à l'interface de ligne de commande : si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "lsn pool1" ou "lsn pool1").

    Il s'agit d'un argument obligatoire. Longueur maximale : 127
  - lsnip

    Adresse IPv4 ou plage d'adresses IPv4 à utiliser comme adresse IP NAT pour LSN.

    Une fois le pool créé, ces adresses IPv4 sont ajoutées à l'appliance Citrix ADC en tant qu'adresse IP appartenant à Citrix ADC de type LSN. Une adresse IP LSN associée à un pool LSN ne peut pas être partagée avec d'autres pools LSN. Les adresses IP spécifiées pour ce paramètre ne doivent pas exister déjà sur l'appliance Citrix ADC en tant qu'adresse IP appartenant à Citrix ADC. Dans l'interface de ligne de commande, séparez la plage par un trait d'union. Par exemple : 10.102.29.30-10.102.29.189. Vous pouvez ultérieurement supprimer une partie ou toutes les adresses IP LSN du pool et ajouter des adresses IP au pool LSN.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- ajouter un profil de transport lsn
  - transportprofilename

    Nom du profil de transport LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le profil de transport LSN créé. L'exigence suivante s'applique uniquement à l'interface de ligne de commande : si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « lsn transport profile1" ou « lsn transport profile1').

    Il s'agit d'un argument obligatoire. Longueur maximale : 127
  - transportprotocol

Protocole pour lequel définir les paramètres du profil de transport LSN.

Il s'agit d'un argument obligatoire.

Valeurs possibles : TCP, UDP, ICMP

- sessiontimeout

  Délai d'expiration, en secondes, pour une session LSN inactive. Si une session LSN est inactive pendant une durée supérieure à cette valeur, l'appliance Citrix ADC supprime la session.

  Ce délai d'expiration ne s'applique pas à une session TCP LSN lorsqu'un message FIN ou RST est reçu de l'un des points de terminaison.

  Valeur par défaut : 120

  Valeur minimale : 60

- finrsttimeout

  Délai d'expiration, en secondes, pour une session TCP LSN après réception d'un message FIN ou RST de l'un des points de terminaison.

  Si une session LSN TCP est inactive (une fois que l'appliance Citrix ADC reçoit un message FIN ou RST) pendant une durée supérieure à cette valeur, l'appliance Citrix ADC supprime la session.

  Étant donné que la fonctionnalité LSN de l'appliance Citrix ADC ne conserve pas les informations d'état des sessions LSN TCP, ce délai d'attente permet la transmission des messages FIN ou RST et ACK à partir de l'autre point de terminaison afin que les deux points de terminaison puissent correctement fermer la connexion.

  Valeur par défaut : 30

- portquota

  Nombre maximal de ports NAT LSN à utiliser à la fois par chaque abonné pour le protocole spécifié. Par exemple, chaque abonné peut être limité à un maximum de 500 ports NAT TCP. Lorsque les mappages NAT LSN pour un abonné atteignent la limite, l'appliance Citrix ADC n'alloue pas de ports NAT supplémentaires pour cet abonné.

  Valeur par défaut : 0

  Valeur minimale : 0

  Valeur maximale : 65535

- sessionquota

  Nombre maximal de sessions LSN simultanées autorisées pour chaque abonné pour le protocole spécifié. Lorsque le nombre de sessions LSN atteint la limite pour un abonné, l'appliance Citrix ADC ne permet pas à l'abonné d'ouvrir des sessions supplémentaires.

Valeur par défaut : 0

Valeur minimale : 0

Valeur maximale : 65535

- portpreserveparity

  Activer la parité de port entre un port d'abonné et son port NAT LSN mappé. Par exemple, si un abonné initie une connexion à partir d'un port numéroté impair, l'appliance Citrix ADC alloue un port NAT LSN numéroté impair pour cette connexion. Vous devez définir ce paramètre pour le bon fonctionnement des protocoles qui exigent que le port source soit numéroté pair ou impair, par exemple, dans les applications peer-to-peer qui utilisent le protocole RTP ou RTCP.

  Valeurs possibles : ENABLED, DISABLED

  Valeur par défaut : DISABLED

- portpreserverange

  Si un abonné initie une connexion à partir d'un port connu (0-1023), allouez un port NAT à partir de la plage de ports connue (0-1023) pour cette connexion. Par exemple, si un abonné initie une connexion à partir du port 80, l'appliance Citrix ADC peut allouer le port 100 en tant que port NAT pour cette connexion.

  Ce paramètre s'applique à NAT dynamique sans allocation de bloc de port. Elle s'applique également au NAT déterministe si la plage de ports allouée inclut des ports connus.

  Lorsque tous les ports connus de toutes les adresses IP NAT disponibles sont utilisés dans différentes connexions d'abonnés (sessions LSN) et qu'un abonné initie une connexion à partir d'un port bien connu, l'appliance Citrix ADC supprime cette connexion.

  Valeurs possibles : ENABLED, DISABLED

  Valeur par défaut : DISABLED

- syncheck

  Déposez silencieusement tous les paquets non-SYN pour les connexions pour lesquelles aucune session LSN-NAT n'est présente sur l'appliance Citrix ADC.

  Si vous désactivez ce paramètre, l'appliance Citrix ADC accepte tous les paquets non SYN et crée une nouvelle entrée de session LSN pour cette connexion.

  Voici quelques raisons pour lesquelles l'appliance Citrix ADC reçoit de tels paquets :

  * Une session LSN pour une connexion existait, mais l'appliance Citrix ADC a supprimé cette session car la session LSN était inactive pendant un temps qui dépassait le délai d'expiration de session configuré.
  * Ces paquets peuvent faire partie d'une attaque DoS.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- add lsn appsprofile
  - appsprofilename

    Nom du profil d'application LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le profil d'application LSN créé. L'exigence suivante s'applique uniquement à l'interface de ligne de commande : si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "lsn application profile1" ou 'lsn application profile1').

    Il s'agit d'un argument obligatoire. Longueur maximale : 127

  - transportprotocol

    Nom du protocole pour lequel les paramètres de ce profil d'application LSN s'appliquent.

    Il s'agit d'un argument obligatoire.

    Valeurs possibles : TCP, UDP, ICMP

  - ippooling

    Options d'allocation d'adresses IP NAT pour les sessions associées au même abonné.

    Les options disponibles fonctionnent comme suit :

    * **Paired** : l'appliance Citrix ADC alloue la même adresse IP NAT pour toutes les sessions associées au même abonné. Lorsque tous les ports d'une adresse IP NAT sont utilisés dans des sessions LSN (pour le même ou plusieurs abonnés), l'appliance Citrix ADC supprime toute nouvelle connexion de l'abonné.
    * **Random** : l'appliance Citrix ADC alloue des adresses IP NAT aléatoires, à partir du pool, pour différentes sessions associées au même abonné.

    Ce paramètre s'applique uniquement à l'allocation NAT dynamique.

    Valeurs possibles : PAIRED, RANDOM

    Valeur par défaut : RANDOM

  - mapping

    Type de mappage LSN à appliquer aux paquets suivants provenant de la même adresse IP et du même port d'abonné.

Prenons un exemple de mappage LSN qui inclut le mappage de l'abonné IP:Port (x:x), NAT IP:Port (n:n) et de l'hôte externe IP:Port (Y:y).

Les options disponibles fonctionnent comme suit :

* **ENDPOINT-INDEPENDENT**—Réutilisez le mappage LSN pour les paquets suivants envoyés à partir de la même adresse IP d'abonné et du même port (X:x) vers n'importe quelle adresse IP et port externes.
* **ADDRESS-DEPENDENT**—Réutilisez le mappage LSN pour les paquets suivants envoyés à partir de la même adresse IP d'abonné et du même port (X:x) vers la même adresse IP externe (Y), quel que soit le port externe.
* **ADDRESS-PORT-DEPENDENT**—Réutilisez le mappage LSN pour les paquets suivants envoyés à partir de la même adresse IP interne et du même port (x:x) vers la même adresse IP externe et le même port (Y:y) lorsque le mappage est toujours actif.

Valeurs possibles : ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT

Valeur par défaut : ADDRESS-PORT-DEPENDENT

– filtrage

Type de filtre à appliquer aux paquets provenant d'hôtes externes.

Prenons un exemple de mappage LSN qui inclut le mappage de l'abonné IP:Port (x:x), NAT IP:Port (n:n) et de l'hôte externe IP:Port (Y:y).

Les options disponibles fonctionnent comme suit :

* **ENDPOINT INDEPENDENT**—Filtre uniquement les paquets qui ne sont pas destinés à l'adresse IP de l'abonné et au port x:x, indépendamment de l'adresse IP de l'hôte externe et de la source du port (z:z). L'appliance Citrix ADC transfère tous les paquets destinés à X:x. En d'autres termes, l'envoi de paquets de l'abonné à n'importe quelle adresse IP externe est suffisant pour autoriser les paquets de n'importe quel hôte externe à l'abonné.
* **ADDRESS DEPENDENT**—Filtre les paquets non destinés à l'adresse IP de l'abonné et au port X:x. En outre, l'appliance filtre les paquets de Y:y destinés à l'abonné (X:x) si le client n'a pas déjà envoyé de paquets à Y:AnyPort (indépendant du port externe). En d'autres termes, la réception de paquets à partir d'un hôte externe spécifique nécessite que l'abonné envoie d'abord des paquets à l'adresse IP de cet hôte externe spécifique.
* **ADDRESS PORT DEPENDENT** (valeur par défaut) : filtre les paquets qui ne sont pas destinés à l'adresse IP de l'abonné et au port (X:x). En outre, l'appliance Citrix ADC filtre les paquets de Y:y destinés à l'abonné (x:x) si l'abonné n'a pas déjà envoyé de paquets à Y:y. En d'autres termes, la réception de paquets à partir d'un hôte externe

spécifique nécessite que l'abonné envoie d'abord les paquets à cette adresse IP externe et au port.

Valeurs possibles : ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT

Valeur par défaut : ADDRESS-PORT-DEPENDENT

- tcpproxy

  Activez le proxy TCP, qui permet à l'appliance Citrix ADC d'optimiser le trafic TCP à l'aide des fonctionnalités de couche 4.

  Valeurs possibles : ENABLED, DISABLED

  Valeur par défaut : DISABLED

- td

  ID du domaine de trafic via lequel l'appliance Citrix ADC envoie le trafic sortant après l'exécution du LSN.

  Si vous ne spécifiez pas d'ID, l'appliance envoie le trafic sortant via le domaine de trafic par défaut, dont l'ID est 0.

  Valeur par défaut : 65535

  Valeur maximale : 65535

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- profil de bind lsn appsprofile
  - appsprofilename

    Nom du profil d'application LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le profil d'application LSN créé. L'exigence suivante s'applique uniquement à l'interface de ligne de commande : si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "lsn application profile1" ou 'lsn application profile1').

    Il s'agit d'un argument obligatoire. Longueur maximale : 127

  - lsnport

    Numéros de port ou plage de numéros de port à comparer avec le port de destination du paquet entrant d'un abonné. Lorsque le port de destination est mis en correspondance, le profil d'application LSN est appliqué pour la session LSN. Séparer une plage de ports par un trait d'union. Par exemple, 40-90.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- ajouter le groupe lsn
  - groupname

    Nom du groupe LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le groupe LSN créé. L'exigence suivante s'applique uniquement à l'interface de ligne de commande : si le nom comporte un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "lsn group1" ou "lsn group1").

    Il s'agit d'un argument obligatoire. Longueur maximale : 127
  - clientname

    Nom de l'entité client LSN à associer au groupe LSN. Vous pouvez associer une seule entité client LSN à un groupe LSN. Vous ne pouvez pas supprimer cette association ou le remplacer par une autre entité client LSN une fois le groupe LSN créé.

    Il s'agit d'un argument obligatoire. Longueur maximale : 127
  - Nattype

    Type d'adresse IP NAT et d'allocation de port (à partir des pools LSN liés) pour les abonnés :

    Les options disponibles fonctionnent comme suit :

    * **Déterministe** : alloue une adresse IP NAT et un bloc de ports à chaque abonné (du client LSN lié au groupe LSN). L'appliance Citrix ADC alloue séquentiellement des ressources NAT à ces abonnés. L'appliance Citrix ADC affecte le premier bloc de ports (taille de bloc déterminée par le paramètre de taille de bloc de port du groupe LSN) sur l'adresse IP NAT de début à l'adresse IP de l'abonné de début. La plage suivante de ports est attribuée à l'abonné suivant, et ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné suivant. Dans ce cas, le premier bloc de port sur l'adresse NAT suivante est utilisé pour l'abonné, et ainsi de suite. Étant donné que chaque abonné reçoit désormais une adresse IP NAT déterministe et un bloc de ports, un abonné peut être identifié sans aucune journalisation. Pour une connexion, un abonné peut être identifié uniquement en fonction de l'adresse IP et du port NAT, ainsi que de l'adresse IP et du port de destination.
    * **Dynamique** : alloue une adresse IP NAT aléatoire et un port du pool NAT LSN pour la connexion d'un abonné. Si l'allocation de bloc de port est activée (dans le pool LSN) et qu'une taille de bloc de port est spécifiée (dans le groupe LSN), l'appliance Citrix ADC alloue une adresse IP NAT aléatoire et un bloc de ports pour un abonné lorsqu'il

initie une connexion pour la première fois. L'appliance alloue cette adresse IP NAT et un port (à partir du bloc de ports alloué) pour différentes connexions de cet abonné. Si tous les ports sont alloués (pour différentes connexions d'abonnés) à partir du bloc de ports alloué aux abonnés, l'appliance alloue un nouveau bloc de ports aléatoire à l'abonné.

Valeurs possibles : DYNAMIC, DETERMINISTIC

Valeur par défaut : DYNAMIC

- portblocksize

  Taille du bloc de port NAT à allouer pour chaque abonné.

  Pour définir ce paramètre pour NAT dynamique, vous devez activer le paramètre d'allocation de bloc de port dans le pool LSN lié. Pour NAT déterministe, le paramètre d'allocation de bloc de port est toujours activé et vous ne pouvez pas le désactiver.

  Dans NAT dynamique, l'appliance Citrix ADC alloue un bloc de port NAT aléatoire, à partir du pool de ports NAT disponible d'une adresse IP NAT, pour chaque abonné. Pour un abonné, si tous les ports sont alloués à partir du bloc de ports alloué aux abonnés, l'appliance alloue un nouveau bloc de ports aléatoire à l'abonné.

- journalisation

  Entrées de mappage de journaux et sessions créées ou supprimées pour ce groupe LSN. L'appliance Citrix ADC consigne les sessions LSN pour ce groupe LSN uniquement lorsque les paramètres de journalisation et de journalisation de session sont activés.

  L'appliance utilise son infrastructure de journal syslog et d'audit existants pour consigner les informations LSN. Vous devez activer la journalisation LSN de niveau global en activant le paramètre LSN dans l'action NSLOG associée et les entités d'action SYLOG. Lorsque le paramètre Journalisation est activé, l'appliance Citrix ADC génère des messages de journal liés aux mappages LSN et aux sessions LSN de ce groupe LSN. L'appliance envoie ensuite ces messages de journal aux serveurs associés à l'action NSLOG et aux entités d'actions SYSLOG.

  Un message de journal pour une entrée de mappage LSN contient les informations suivantes :

  * Adresse NSIP de l'appliance Citrix ADC
  * Horodatage
  * Type d'entrée (MAPPING ou SESSION)
  * Indique si l'entrée de mappage LSN est créée ou supprimée
  * Adresse IP, port et ID de domaine de trafic de l'abonné
  * Adresse IP NAT et port
  * Nom du protocole

* L'adresse IP de destination, le port et l'ID de domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison
  - Seule l'adresse IP de destination (et non le port) est enregistrée pour le mappage dépendant de l'adresse
  - L'adresse IP et le port de destination sont enregistrés pour le mappage dépendants du port d'adresse

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

– sessionLogging

Journaliser les sessions créées ou supprimées pour le groupe LSN. L'appliance Citrix ADC consigne les sessions LSN pour ce groupe LSN uniquement lorsque les paramètres de journalisation et de journalisation de session sont activés.

Un message de journal pour une session LSN contient les informations suivantes :

* Adresse NSIP de l'appliance Citrix ADC
* Horodatage
* Type d'entrée (MAPPING ou SESSION)
* Indique si la session LSN est créée ou supprimée
* Adresse IP, port et ID de domaine de trafic de l'abonné
* Adresse IP NAT et port
* Nom du protocole
* Adresse IP de destination, port et ID de domaine de trafic

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

– sessionSync

Dans un déploiement haute disponibilité (HA), synchronisez les informations de toutes les sessions LSN associées à ce groupe LSN avec le nœud secondaire. Après un basculement, les connexions TCP établies et les flux de paquets UDP sont maintenus actifs et repris sur le nœud secondaire (nouveau principal).

Pour que ce paramètre fonctionne, vous devez activer le paramètre de synchronisation de session globale.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

- snmptraplimit

  Nombre maximal de messages d'interruption SNMP pouvant être générés pour le groupe LSN en une minute.

  Valeur par défaut : 100

  Valeur minimale : 0

  Valeur maximale : 10000

- ftp

  Activez Application Layer Gateway (ALG) pour le protocole FTP. Pour certains protocoles de couche d'application, les adresses IP et les numéros de port de protocole sont généralement communiqués dans la charge utile des paquets. Lorsqu'elle agit en tant qu'ALG, l'appliance modifie la charge utile des paquets pour s'assurer que le protocole continue de fonctionner sur LSN.

  Remarque : l'appliance Citrix ADC inclut également les protocoles ALG pour ICMP et TFTP. ALG pour le protocole ICMP est activé par défaut et aucune disposition ne permet de le désactiver. ALG pour le protocole TFTP est désactivé par défaut. ALG est activé automatiquement pour un groupe LSN lorsque vous liez un profil d'application UDP LSN, avec mappage indépendant du point de terminaison, filtrage indépendant du point de terminaison et port de destination 69 (port connu pour TFTP), au groupe LSN.

  Valeurs possibles : ENABLED, DISABLED

  Valeur par défaut : ENABLED

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- groupe de liaison lsn
  - groupname

    Nom du groupe LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le groupe LSN créé. L'exigence suivante s'applique uniquement à l'interface de ligne de commande : si le nom comporte un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "lsn group1" ou "lsn group1").

    Il s'agit d'un argument obligatoire. Longueur maximale : 127

  - poolname

Nom du pool LSN à lier au groupe LSN spécifié. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés ensemble. Plusieurs pools LSN peuvent être liés à un groupe LSN.

Pour NAT déterministe, les pools liés à un groupe LSN ne peuvent pas être liés à d'autres groupes LSN. Pour NAT dynamique, les pools liés à un groupe LSN peuvent être liés à plusieurs groupes LSN. Longueur maximale : 127

- transportprofilename

  Nom du profil de transport LSN à lier au groupe LSN spécifié. Liez un profil pour chaque protocole pour lequel vous souhaitez spécifier des paramètres.

  Par défaut, un profil de transport LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP est lié à un groupe LSN lors de sa création. Ce profil est appelé transport par défaut.

  Un profil de transport LSN que vous liez à un groupe LSN remplace le profil de transport LSN par défaut pour ce protocole. Longueur maximale : 127

- appsprofilename

  Nom du profil d'application LSN à lier au groupe LSN spécifié. Pour chaque ensemble de ports de destination, liez un profil pour chaque protocole pour lequel vous souhaitez spécifier des paramètres.

  Par défaut, un profil d'application LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP pour tous les ports de destination est lié à un groupe LSN lors de sa création. Ce profil est appelé profil d'application par défaut.

  Lorsque vous liez un profil d'application LSN, avec un ensemble de ports de destination spécifié, à un groupe LSN, le profil lié remplace le profil d'application LSN par défaut pour ce protocole sur cet ensemble de ports de destination. Longueur maximale : 127

Exemples de configurations LSN

January 21, 2021

Voici des exemples de configuration de LSN via l'interface de ligne de commande.

Créez une configuration LSN simple avec un réseau abonné unique, une adresse IP NAT LSN unique et des paramètres par défaut :

```
1 add lsn client LSN-CLIENT-1
2
3 Done
```



```
4
5  bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-1
10
11 Done
12
13 bind lsn pool LSN-POOL-1 203.0.113.3
14
15 Done
16
17 add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1
18
19 Done
20
21 bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
22
23 Done
24 <!--NeedCopy-->
```

Créez une configuration LSN avec une liste ACL étendue pour identifier les abonnés LSN :

```
1  add ns acl LSN-ACL-2 ALLOW -srcIP 192.0.2.10-192.0.2.20
2
3  Done
4
5  apply acls
6
7  Done
8
9  add lsn client LSN-CLIENT-2
10
11 Done
12
13 bind lsn client LSN-CLIENT-2  - aclname LSN-ACL-2
14
15 Done
16
17 add lsn pool LSN-POOL-2
18
19 Done
20
21 bind lsn pool LSN-POOL-2 203.0.113.5-203.0.113.10
```



```
22
23 Done
24
25 add lsn group LSN-GROUP-2 -clientname LSN-CLIENT-2
26
27 Done
28
29 bind lsn group LSN-GROUP-2 -poolname LSN-POOL-2
30
31 Done
32 <!--NeedCopy-->
```

Créez une configuration LSN avec mappage indépendant du point de terminaison pour le protocole HTTP (port 80) et mappage dépendant du port d'adresse pour le protocole SSH (port 22). En outre, limitez chaque abonné à utiliser un maximum de 1000 ports NAT pour le protocole TCP et 100 ports NAT pour le protocole UDP. Restreindre chaque abonné à avoir un maximum de 2000 sessions simultanées pour le protocole TCP. Restreindre le groupe pour qu'il dispose d'un maximum de 30000 sessions simultanées pour le protocole TCP :

```
1  add lsn client LSN-CLIENT-3
2
3  Done
4
5  bind lsn client LSN-CLIENT-3 -network 192.0.3.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-3
10
11 Done
12
13 bind lsn pool LSN-POOL-3 203.0.113.11
14
15 Done
16
17 add lsn group LSN-GROUP-3 -clientname LSN-CLIENT-3
18
19 Done
20
21 bind lsn group LSN-GROUP-3 -poolname LSN-POOL-3
22
23 Done
24
25 add lsn appsprofile LSN-APPS-HTTPPROFILE-3 TCP -mapping ENDPOINT-
```



```
    INDEPENDENT

Done

bind lsn appsprofile LSN-APPS-HTTPPROFILE-3 80

Done

bind lsn group LSN-GROUP-3 -applicationprofilename LSN-APPS-HTTPPROFILE
    -3

Done

add lsn appsprofile LSN-APPS-SSHPROFILE-3 TCP -mapping ADDRESS-PORT-
    DEPENDENT

Done

bind lsn appsprofile LSN-APPS-SSHPROFILE-3 22

Done

bind lsn group LSN-GROUP-3 -applicationprofilename LSN-APPS-SSHPROFILE
    -3

Done

add lsn transportprofile LSN-TRANS-PROFILE-TCP-3 TCP -portquota 1000 -
    sessionquota 2000 -groupSessionLimit 30000

Done

bind lsn group LSN-GROUP-3 -transportprofilename LSN-TRANS-PROFILE-TCP
    -3

Done

add lsn transportprofile LSN-TRANS-PROFILE-UDP-3 UDP -portquota 100

Done

bind lsn group LSN-GROUP-3 -transportprofilename LSN-TRANS-PROFILE-UDP
    -3

Done
```



```
<!--NeedCopy-->
```

Créez une configuration LSN pour un grand nombre d'abonnés :

```
add lsn client LSN-CLIENT-4

Done

bind lsn client LSN-CLIENT-4 -network 192.0.4.0 -netmask 255.255.255.0

Done

bind lsn client LSN-CLIENT-4 -network 192.0.5.0 -netmask 255.255.255.0

Done

bind lsn client LSN-CLIENT-4 -network 192.0.6.0 -netmask 255.255.255.0

Done

bind lsn client LSN-CLIENT-4 -network 192.0.7.0 -netmask 255.255.255.0

Done

bind lsn client LSN-CLIENT-4 -network 192.0.8.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-4

Done

bind lsn pool LSN-POOL-4 203.0.113.30-203.0.113.40

Done

bind lsn pool LSN-POOL-4 203.0.113.45-203.0.113.50

Done

bind lsn pool LSN-POOL-4 203.0.113.55-203.0.113.60

Done

add lsn group LSN-GROUP-4 -clientname LSN-CLIENT-4
```



```
42
43 Done
44
45 bind lsn group LSN-GROUP-4 -poolname LSN-POOL-4
46
47 Done
48
49 add lsn appsprofile LSN-APPS-WELLKNOWNPROFILE-4 TCP -mapping ENDPOINT-
      INDEPENDENT
50
51 Done
52
53 bind lsn appsprofile LSN-APPS-WELLKNOWN-PORTS-PROFILE-4 1- 1023
54
55 Done
56
57 bind lsn group LSN-GROUP-4 -applicationprofilename LSN-APPS-WELLKNOWN-
      PORTS-PROFILE-4
58
59 Done
60 <!--NeedCopy-->
```

Créez une configuration LSN avec le partage des ressources NAT entre plusieurs groupes LSN. Dans cet exemple, le pool LSN LSN-POOL-5 est partagé avec les groupes LSN LSN-GROUP-5 et LSN-GROUP-6 :

```
1  add lsn client LSN-CLIENT-5
2
3  Done
4
5  bind lsn client LSN-CLIENT-5 -network 192.0.15.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-5
10
11 Done
12
13 bind lsn pool LSN-POOL-5 203.0.113.12-203.0.113.14
14
15 Done
16
17 add lsn group LSN-GROUP-5 -clientname LSN-CLIENT-5
18
19 Done
```



```
20
21 bind lsn group LSN-GROUP-5 -poolname LSN-POOL-5
22
23 Done
24
25 add lsn client LSN-CLIENT-6
26
27 Done
28
29 bind lsn client LSN-CLIENT-6 -network 192.0.16.0 -netmask 255.255.255.0
30
31 Done
32
33 add lsn pool LSN-POOL-6
34
35 Done
36
37 bind lsn pool LSN-POOL-6 203.0.113.15-203.0.113.18
38
39 Done
40
41 add lsn group LSN-GROUP-6 -clientname LSN-CLIENT-6
42
43 Done
44
45 bind lsn group LSN-GROUP-6 -poolname LSN-POOL-6
46
47 Done
48
49 bind lsn group LSN-GROUP-6 -poolname LSN-POOL-5
50
51 Done
52 <!--NeedCopy-->
```

Créez une configuration LSN avec une allocation de ressources NAT déterministe :

```
1 add lsn client LSN-CLIENT-7
2
3 Done
4
5 bind lsn client LSN-CLIENT-7 -network 192.0.17.0 -netmask 255.255.255.0
6
7 Done
8
9 add lsn pool LSN-POOL-7 -nattype DETERMINISTIC
```



```
10
11 Done
12
13 bind lsn pool LSN-POOL-7 203.0.113.19-203.0.113.23
14
15 Done
16
17 add lsn group LSN-GROUP-7 -clientname LSN-CLIENT-7 -nattype
      DETERMINISTIC -portblocksize 1024
18
19 Done
20
21 bind lsn group LSN-GROUP-7 -poolname LSN-POOL-7
22
23 Done
24 <!--NeedCopy-->
```

Créez une configuration LSN avec plusieurs réseaux d'abonnés ayant la même adresse réseau mais chaque réseau appartenant à un domaine de trafic différent. En outre, limitez le trafic sortant lié au protocole HTTP (port 80), en l'envoyant via un domaine de trafic particulier (td 5) :

```
1  add lsn client LSN-CLIENT-8
2
3  Done
4
5  bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
       -td 1
6
7  Done
8
9  bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
       -td 2
10
11 Done
12
13 bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
       -td 3
14
15 Done
16
17 add lsn pool LSN-POOL-8
18
19 Done
```



```
20
21 bind lsn pool LSN-POOL-8 203.0.113.80-203.0.113.86
22
23 Done
24
25 add lsn group LSN-GROUP-8 -clientname LSN-CLIENT-8
26
27 Done
28
29 bind lsn group LSN-GROUP-8 -poolname LSN-POOL-8
30
31 Done
32
33 add lsn appsprofile LSN-APPS-HTTP-PROFILE-8 TCP -td 5
34
35 Done
36
37 bind lsn appsprofile LSN-APPS-HTTP-PROFILE-8 80
38
39 Done
40
41 bind lsn group LSN-GROUP-8 -applicationprofilename LSN-APPS-HTTP-
      PROFILE-8
42
43 Done
44 <!--NeedCopy-->
```

Créez une configuration LSN qui limite le trafic sortant d'un protocole spécifique (TCP), en l'envoyant via un domaine de trafic particulier (td 5). Avec le filtrage indépendant du point de terminaison, recevez le trafic entrant lié à ce protocole (TCP) sur n'importe quel domaine de trafic :

```
1  add lsn client LSN-CLIENT-9
2
3  Done
4
5  bind lsn client LSN-CLIENT-9 -network 192.0.9.0 -netmask 255.255.255.0
      -td 1
6
7  Done
8
9  add lsn pool LSN-POOL-9
10
11 Done
```



```
12
13 bind lsn pool LSN-POOL-9 203.0.113.90
14
15 Done
16
17 add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9
18
19 Done
20
21 bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9
22
23 Done
24
25 add lsn appsprofile LSN-APPS-PROFILE-9 TCP -filtering ENDPOINT-
      INDEPENDENT -td 5
26
27 Done
28
29 bind lsn group LSN-GROUP-9 -approfile LSN-APPS-PROFILE-9
30
31 Done
32 <!--NeedCopy-->
```

Créez une configuration LSN qui limite le trafic HTTP sortant (port 80), en l'envoyant via un domaine de trafic particulier (td 10). Avec le filtrage dépendant de l'adresse, recevez le trafic entrant lié à ce protocole (HTTP) sur le domaine de trafic spécifié (td 10) :

```
1  add lsn client LSN-CLIENT-10
2
3  Done
4
5  bind lsn client LSN-CLIENT-10 -network 192.0.10.0 -netmask
      255.255.255.0 -td 1
6
7  Done
8
9  add lsn pool LSN-POOL-10
10
11 Done
12
13 bind lsn pool LSN-POOL-10 203.0.113.100
14
15 Done
16
17 add lsn group LSN-GROUP-10 -clientname LSN-CLIENT-10
```



```
18
19 Done
20
21 bind lsn group LSN-GROUP-10 -poolname LSN-POOL-10
22
23 Done
24
25 add lsn appsprofile LSN-APPS-PROFILE-10 TCP -mapping ENDPOINT -
      INDEPENDENT -filtering ADDRESS-DEPENDENT -td 10
26
27 Done
28
29 bind lsn appsprofile LSN-APPS-PROFILE-10 80
30
31 Done
32
33 bind lsn group LSN-GROUP-10 -approfile LSN-APPS-PROFILE-10
34
35 Done
36 <!--NeedCopy-->
```

Configuration des mappages LSN statiques

January 21, 2021

L'appliance Citrix ADC prend en charge la création manuelle d'un mappage LSN un-à-un entre une adresse IP abonné : port et une adresse IP NAT : port. Les mappages LSN statiques sont utiles dans les cas où vous voulez vous assurer que les connexions initiées à une adresse IP NAT : port sont mappées à l'adresse IP de l'abonné : port. Par exemple, les serveurs Web situés dans le réseau interne.

Pour créer un mappage LSN statique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lsn static <name> <transportprotocol> <subscrIP> <subscrPort> [-td
     <positive_integer>] [<natIP> [<natPort>]] [-destIP <ip_addr> [-dsttd
      <positive_integer>]]
2 -  show lsn static
3 <!--NeedCopy-->
```


Pour créer un mappage LSN statique à l'aide de l'utilitaire de configuration

Accédez à Système > NAT à grande échelle > Statique, puis ajoutez un nouveau mappage statique.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

ajouter le nom statique lsn

Nom de l'entrée de mappage statique LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le groupe LSN créé. La condition suivante s'applique uniquement à l'interface de ligne de commande : si le nom comporte un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « lsn static1" ou « lsn static1'). Il s'agit d'un argument obligatoire. Longueur maximale : 127

transportprotocol

Protocole pour l'entrée de mappage LSN. Il s'agit d'un argument obligatoire. Valeurs possibles : TCP, UDP, ICMP

subscrIP

Adresse IPv4 d'un abonné LSN pour l'entrée de mappage LSN. Il s'agit d'un argument obligatoire.

subscrPort

Port de l'abonné LSN pour l'entrée de mappage LSN. Il s'agit d'un argument obligatoire. Valeur maximale : 65535

td

ID du domaine de trafic auquel appartient l'abonné. Si vous ne spécifiez pas d'ID, l'abonné est supposé faire partie du domaine de trafic par défaut. Valeur par défaut : 0, Valeur minimale : 0, Valeur maximale : 4094

natIP

Adresse IPv4, déjà existante sur l'appliance Citrix ADC en tant que type LSN, à utiliser comme adresse IP NAT pour cette entrée de mappage.

natPort

Port NAT pour cette entrée de mappage LSN.

destIP

Adresse IP de destination pour l'entrée de mappage LSN.

dsttd

ID du domaine de trafic par lequel l'adresse IP de destination de cette entrée de mappage LSN est accessible depuis l'appliance Citrix ADC. Si vous ne spécifiez pas d'ID, l'adresse IP de destination est supposée être accessible via le domaine de trafic par défaut, qui a un ID de 0. Valeur par défaut : 0, Valeur minimale : 0, Valeur maximale : 4094

Mappings statiques des ports génériques

Une entrée de mappage statique est généralement un mappage LSN un-à-un entre une adresse IP abonné : port et une adresse IP NAT : port. Une entrée de mappage LSN statique un-à-un expose seulement un port de l'abonné à Internet.

Certaines situations peuvent nécessiter l'exposition de tous les ports (64 Ko) d'un abonné à Internet (par exemple, un serveur hébergé sur un réseau interne et exécutant un service différent sur chaque port). Pour rendre ces services internes accessibles via Internet, vous devez exposer tous les ports du serveur à Internet.

Une façon de répondre à cette exigence consiste à ajouter 64K entrées de mappage statiques un-à-un, une entrée de mappage pour chaque port. La création d'entrées 64K est très lourde et une tâche importante. En outre, ce grand nombre d'entrées de configuration peut entraîner des problèmes de performances dans l'appliance Citrix ADC.

Une autre méthode simple consiste à utiliser des ports génériques dans une entrée de mappage statique. Vous avez juste besoin de créer une entrée de mappage statique avec les paramètres de port NAT et de port d'abonné définis sur le caractère générique (*), et le paramètre de protocole défini sur ALL, pour exposer tous les ports d'un abonné à Internet. Pour les connexions entrantes ou sortantes d'un abonné correspondant à une entrée de mappage statique générique, le port de l'abonné ne change pas après l'opération NAT.

Lorsqu'une connexion initiée par un abonné à Internet correspond à une entrée de mappage statique générique, l'appliance Citrix ADC attribue un port NAT portant le même numéro que le port d'abonné à partir duquel la connexion est initiée. De même, un hôte Internet est connecté au port d'un abonné en se connectant au port NAT qui a le même numéro que le port de l'abonné.

Configuration de l'appliance Citrix ADC pour fournir l'accès à tous les ports d'un abonné IPv4

Pour configurer l'appliance Citrix ADC pour qu'elle donne accès à tous les ports d'un abonné IPv4, créez un mappage statique générique avec les paramètres obligatoires suivants :

- Protocol=ALL
- Port de l'abonné = *
- Port NAT = *

Dans un mapping statique générique, contrairement à un mapping statique un-à-un, la définition du paramètre IP NAT est obligatoire. En outre, l'adresse IP NAT attribuée à un mapping statique générique ne peut pas être utilisée pour d'autres abonnés.

Pour créer un mapping statique générique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn static <name> ALL <subscrIP> *  <natIP> * [-td <
   positive_integer>] [-destIP <ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```

Exemple de configuration

Dans l'exemple de configuration suivant d'un mapping statique générique, tous les ports d'un abonné dont l'adresse IP est 192.0.2.10 sont rendus accessibles via NAT IP 203.0.11.33.

Exemple de configuration :

```
add lsn static NAT44-WILDCARD-STATIC-1 ALL  192.0.2.10 * 203.0.113.33 *

Done
<!--NeedCopy-->
```

Configuration des passerelles de couche d'application

January 21, 2021

Pour certains protocoles de couche Application, les adresses IP et les numéros de port de protocole sont également communiqués dans la charge utile du paquet. Application Layer Gateway for a protocol analyse la charge utile du paquet et effectue les modifications nécessaires pour s'assurer que le protocole continue de fonctionner sur LSN.

L'appliance Citrix ADC prend en charge ALG pour les protocoles suivants :

- FTP
- ICMP
- TFTP
- PPTP
- SIP
- RTSP

Passerelle de couche d'application pour les protocoles FTP, ICMP et TFTP

January 21, 2021

Vous pouvez activer ou désactiver ALG pour le protocole FTP pour une configuration LSN en activant ou en désactivant l'option FTP du groupe LSN de la configuration LSN.

ALG pour le protocole ICMP est activé par défaut et aucune disposition ne permet de le désactiver.

ALG pour le protocole TFTP est désactivé par défaut. TFTP ALG est activé automatiquement pour une configuration LSN lorsque vous liez un profil d'application UDP LSN, avec mappage indépendant du point de terminaison, filtrage indépendant du point de terminaison et port de destination 69 (port connu pour TFTP), au groupe LSN.

Exemple de configuration LSN pour FTP ALG :
Dans l'exemple de configuration LSN suivant, ALG FTP est activé pour les abonnés dont l'adresse IP est comprise entre 192.0.2.30-192.0.2.100.

```
1  add ns acl LSN-ACL-1 ALLOW -srcIP 192.0.2.30-192.0.2.100
2
3  Done
4
5  apply acls
6
7  Done
8
9  add lsn client LSN-CLIENT-1
10
11 Done
12
13 bind lsn client LSN-CLIENT-1  -aclname LSN-ACL
14
15 Done
```



```
16
17 add lsn pool LSN-POOL-1
18
19 Done
20
21 bind lsn pool LSN-POOL-1 203.0.113.10
22
23 Done
24
25 add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  -FTP ENABLED
26
27 Done
28
29 bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
30
31 Done
32 <!--NeedCopy-->
```

Exemple de configuration LSN pour TFTP ALG :

Dans l'exemple de configuration LSN suivant, le mappage indépendant du point de terminaison et le filtrage indépendant du point de terminaison sont activés pour le protocole TFTP (port UDP 69). L'appliance Citrix ADC active automatiquement TFTP ALG pour cette configuration LSN.

```
1  add lsn client LSN-CLIENT-2
2
3  Done
4
5  bind lsn client LSN-CLIENT-2 -network 198.51.100.0 -netmask
       255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-2
10
11 Done
12
13 bind lsn pool LSN-POOL-2 203.0.113.10-203.0.113.11
14
15 Done
16
17 add lsn group LSN-GROUP-2 -clientname LSN-CLIENT-2
18
19 Done
20
```



```
21 bind lsn group LSN-GROUP-2 -poolname pool1 LSN-POOL-2
22
23 Done
24
25 add lsn appsprofile LSNAPPSPROFILE-TFTP-2 UDP -mapping ENDPOINT-
      INDEPENDENT  - filtering  ENDPOINT-INDEPENDENT
26
27 Done
28
29 bind lsn appsprofile LSNAPPSPROFILE-TFTP-2 69
30
31 Done
32
33 bind lsn group LSN-GROUP-1 -applicationprofilename LSNAPPSPROFILE-TFTP
      -2
34
35 Done
36 <!--NeedCopy-->
```

Passerelle de couche d'application pour le protocole PPTP

August 20, 2021

L'appliance Citrix ADC prend en charge les passerelles de couche d'application (ALG) pour le protocole PPTP (Point-to-Point Tunneling Protocol).

PPTP est un protocole réseau qui permet le transfert sécurisé de données d'un client distant vers un serveur d'entreprise en créant un tunnel entre les réseaux de données TCP/IP. PPTP encapsule les paquets PPP dans des paquets IP pour transmission sur Internet. PPTP établit un tunnel pour chaque paire de serveurs réseau PPTP (PNS) -PPTP Access Concentrator (PAC). Une fois le tunnel configuré, l'encapsulation de routage générique améliorée (GRE) est utilisée pour échanger des paquets PPP. Un ID d'appel dans l'en-tête GRE indique la session à laquelle appartient un paquet PPP particulier.

L'appliance Citrix ADC reconnaît les paquets PPTP qui arrivent sur le port TCP par défaut, 1723. L'appliance analyse les paquets de contrôle PPTP, traduit l'ID d'appel et attribue une adresse IP NAT. Pour la communication de données bidirectionnelle entre le client et le serveur, l'appliance Citrix ADC crée une entrée de session LSN basée sur l'ID d'appel du serveur, et une session LSN basée sur l'ID d'appel du client. L'appliance analyse ensuite les paquets de données GRE et traduit les ID d'appel sur la base des deux entrées de session LSN.

Pour le protocole PPTP, l'appliance Citrix ADC inclut également le paramètre de délai d'expiration pour les sessions LSN PPTP inactives. Si une session LSN PPTP est inactive pendant une durée supérieure

au paramètre de délai d'expiration, l'appliance Citrix ADC supprime la session.

Limitations :

Voici les limites de PPTP ALG sur une appliance Citrix ADC :

- PPTP ALG n'est pas pris en charge pour le flux LSN en épingle à cheveux.
- PPTP ALG n'est pas pris en charge pour fonctionner avec une configuration RNAT.
- PPTP ALG n'est pas pris en charge dans les clusters Citrix ADC.

Configuration de PPTP ALG

La configuration de PPTP ALG sur l'appliance Citrix ADC comporte les tâches suivantes :

- Créez une configuration LSN et activez PPTP ALG dessus. Dans une configuration LSN, le groupe LSN inclut le paramètre ALG PPTP. Pour obtenir des instructions sur la création d'une configuration LSN, voir Étapes de configuration pour LSN.
- (Facultatif) Définissez le délai global pour les sessions LSN PPTP inactives.

Pour activer PPTP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn group <groupname> -clientname <string> [-pptp ( ENABLED |
   DISABLED )]

show lsn group
<!--NeedCopy-->
```

Pour définir le délai global pour les sessions LSN PPTP inactives à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set appAlgParam -pptpGreIdleTimeout <positive_integer>

show appAlgParam
<!--NeedCopy-->
```

Exemple :

Dans l'exemple de configuration LSN suivant, PPTP ALG est activé pour les abonnés du réseau 192.0.2.0/24.

Également le délai d'expiration de session PPTP LSN inactif est réglé à 200 secondes.


```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  -pptp ENABLED

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done

set appAlgParam -pptpGreIdleTimeout 200

Done
<!--NeedCopy-->
```

Passerelle de couche d'application pour le protocole SIP

August 20, 2021

L'utilisation de NAT à grande échelle (LSN) avec le protocole SIP (Session Initiation Protocol) est compliquée, car les messages SIP contiennent des adresses IP dans les en-têtes SIP ainsi que dans le corps SIP. Lorsque LSN est utilisé avec SIP, les en-têtes SIP contiennent des informations sur l'appelant et le récepteur, et le périphérique traduit ces informations pour les masquer du réseau externe. Le corps SIP contient les informations SDP (Session Description Protocol), qui comprennent les adresses IP et les numéros de port pour la transmission du média.

SIP ALG adhère aux RFC suivants :

- RFC 3261
- RFC 3581
- RFC 4566
- RFC 4475

> **Remarque**
>
> SIP ALG est pris en charge dans une appliance autonome Citrix ADC, dans une configuration de haute disponibilité Citrix ADC, ainsi que dans une configuration de cluster Citrix ADC.

Fonctionnement de SIP ALG

La manière dont la traduction des adresses IP est effectuée dépend du type et de la direction du message. Un message peut être l'un des éléments suivants :

- Demande entrante
- Réponse sortante
- Demande sortante
- Réponse entrante

Pour un message sortant, l'adresse IP privée et le numéro de port du client SIP sont remplacés par l'adresse IP publique et le numéro de port appartenant à Citrix ADC, appelés l'adresse IP du *pool LSN et le numéro de port*, spécifiés lors de la configuration LSN. Pour un message entrant, l'adresse IP du pool LSN et le numéro de port sont remplacés par l'adresse privée du client. Si le message contient des adresses IP publiques, le Citrix ADC SIP ALG les conserve. En outre, un sténopé est créé sur le :

- L'adresse IP du pool LSN et le port au nom du client privé, de sorte que les messages qui arrivent à cette adresse IP et port du réseau public soient traités comme des messages SIP.
- Adresse IP publique et port pour le compte des clients publics, de sorte que les messages qui arrivent à cette adresse IP et port du réseau privé soient traités comme des messages SIP.

Lorsqu'un message SIP est envoyé sur le réseau, la passerelle SIP Application Layer Gateway (ALG) recueille des informations à partir du message et traduit les adresses IP des en-têtes suivants en adresses IP de pool LSN :

- Via
- Contactez
- Itinéraire
- Record-Route

Dans l'exemple de message de demande SIP suivant, LSN remplace les adresses IP dans les champs d'en-tête pour les masquer du réseau externe.

```
1 INVITE adam@10.102.185.156 SIP/2.0 Via: SIP/2.0/UDP 192.170.1.161:62914
      From: eve@10.120.210.3 To: adam@10.102.185.156 Call-ID: a12abcde@10
```



```
      .120.210.3 Contact: adam@10.102.185.156 Route: <sip:netscreen@10
      .150.20.3:5060> Record-Route: <sip:netscreen@10.150.20.3:5060>
2 <!--NeedCopy-->
```

Lorsqu'un message contenant des informations SDP arrive, l'ALG SIP recueille des informations à partir du message et traduit les adresses IP dans les champs suivants en adresses IP de pool LSN et numéros de port :

- c= (informations de connexion)

  Ce champ peut apparaître au niveau de la session ou du média. Il apparaît au format suivant :

  c=<network-type><address-type><connection-address>

  Si l'adresse IP de destination est une adresse IP monodiffusion, l'ALG SIP crée des trous d'épingle à l'aide de l'adresse IP et des numéros de port spécifiés dans le champ m=.

- m= (annonce de presse)

  Ce champ apparaît au niveau du média et contient la description du média. Il apparaît au format suivant :

  m=<media><port><transport><fmt list>

- a=(information about the media field)

  Ce champ peut apparaître au niveau de la session ou du média, dans le format suivant :

  a =<attribute>

  a =<attribute>:<value>

L'extrait suivant d'un exemple de section SDP montre les champs qui sont traduits pour l'allocation de ressources.

o=user 2344234 55234434 IN IP4 10.150.20.3

c=IN IP4 10.150.20.3

m=audio 43249 RTP/AVP 0

Le tableau suivant montre comment la charge utile SIP est traduite.

Demande entrante (du public au privé)	par :	Aucune
	De :	Aucune
	Call-ID :	Aucune
	Via :	Aucune

	URI de requête :	Remplacer l’adresse IP du pool LSN par une adresse IP privée
	Contact :	Aucune
	Record-Route	Aucune
	Itinéraire :	Aucune
Réponse sortante (du privé au public)	par :	Aucune
	De :	Aucune
	Call-ID :	Aucune
	Via :	Aucune
	URI de requête :	Remplacer l’adresse IP privée par l’adresse IP du pool LSN
	Contact :	Remplacer l’adresse IP privée par l’adresse IP du pool LSN
	Record-Route	Aucune
	Itinéraire :	Aucune
Demande sortante (du privé au public)	par :	Aucune
	De :	Aucune
	Call-ID :	Aucune
	Via :	Remplacer l’adresse IP privée par l’adresse IP du pool LSN
	URI de requête :	Aucune
	Contact :	Remplacer l’adresse IP privée par l’adresse IP du pool LSN
	Record-Route	Aucune
	Itinéraire :	Aucune
Réponse entrante (du public au privé)	par :	Aucune
	De :	Aucune

	Call-ID :	Aucune
	Via :	Remplacer l'adresse IP du pool LSN par une adresse IP privée
	URI de requête :	Aucune
	Contact :	Conserver l'adresse IP publique, le cas échéant
	Record-Route	Aucune
	Itinéraire :	Aucune

Limites de SIP ALG

Un ALG SIP présente les limitations suivantes :

- Seule la charge utile SDP est prise en charge.
- Les éléments suivants ne sont pas pris en charge :
  - Adresses IP de multidiffusion
  - SDP chiffré
  - SIP TLS
  - Traduction de FQDN
  - Authentification de la couche SIP
  - TD/partitionnement
  - Corps en plusieurs parties
  - Messages SIP sur le réseau IPv6
  - Réassemblage de lignes

Clients SIP et serveurs proxy testés

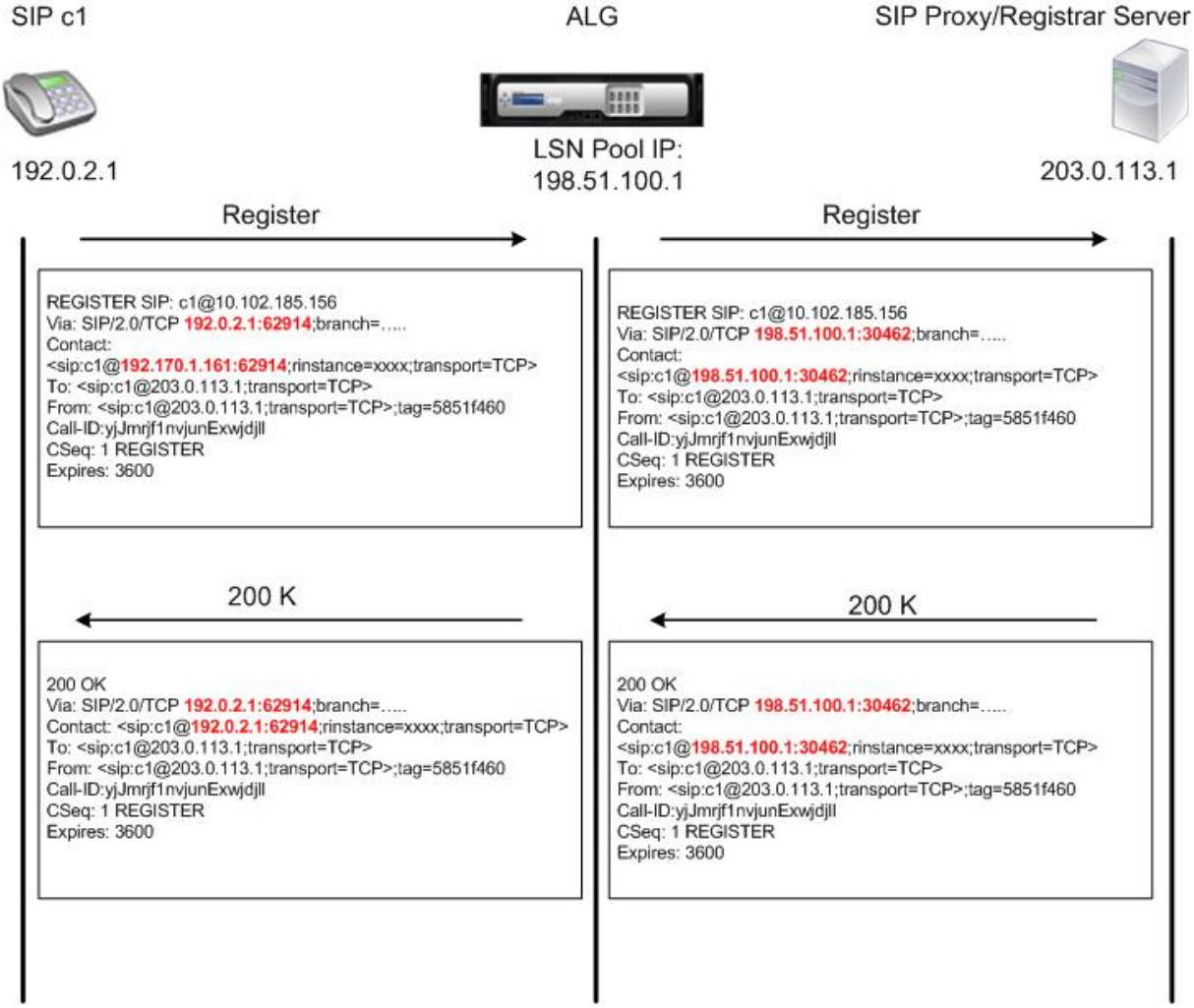
Les clients SIP et le serveur proxy suivants ont été testés avec SIP ALG :

- **Clients SIP :** X-Lite, Zoiper, Ekiga. Avaya
- **Serveur proxy :** OpenSIPS

Scénario SIP LSN : Proxy SIP en dehors du réseau privé (réseau public)

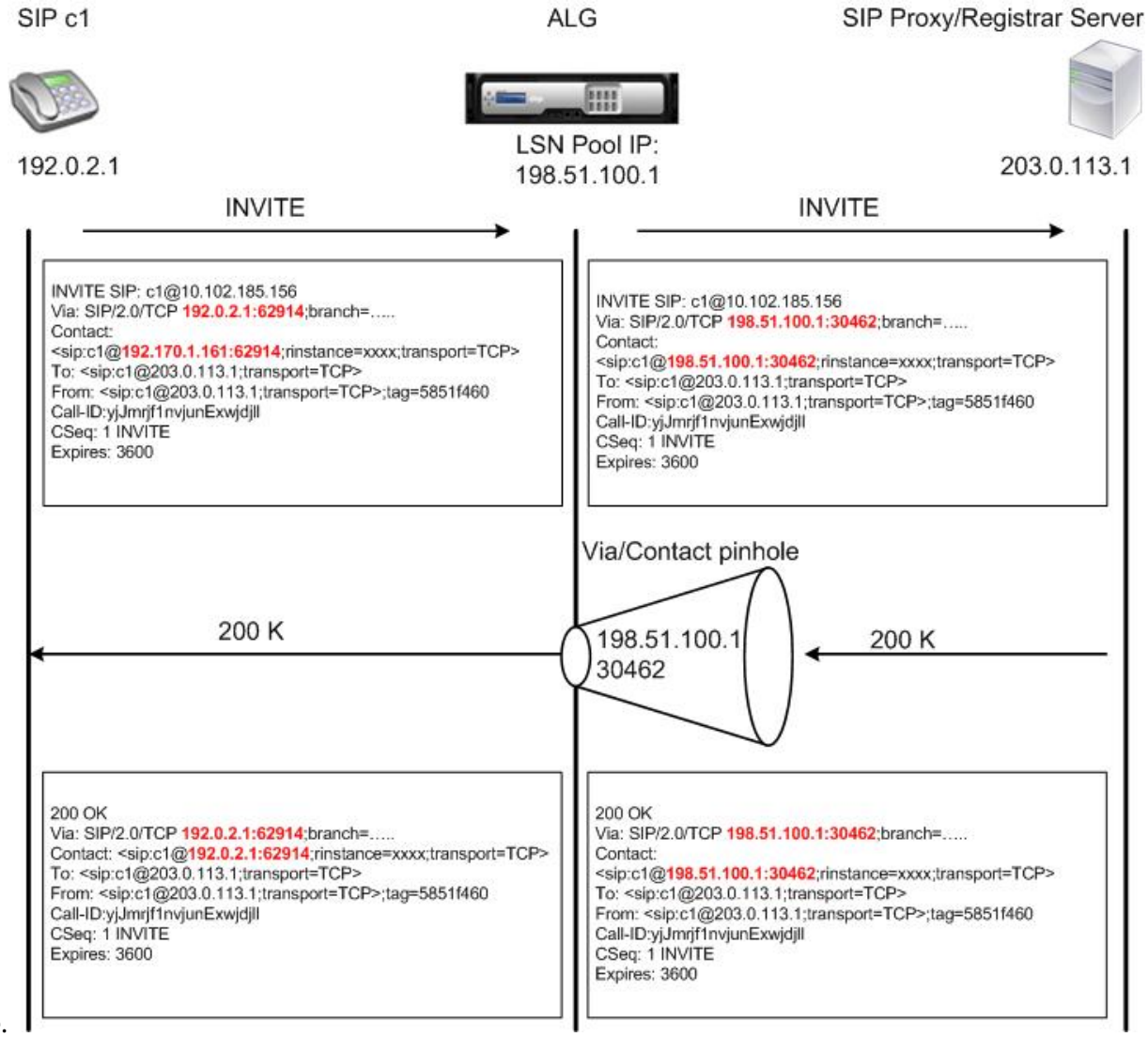
Enregistrement du client SIP

Pour un appel SIP typique, le client SIP doit s'inscrire auprès du bureau d'enregistrement SIP en composant une demande REGISTER et en l'envoyant au bureau d'enregistrement SIP. L'ALG SIP de l'appliance Citrix ADC intercepte la demande, remplace l'adresse IP et le numéro de port de la demande par l'adresse IP du pool LSN et le numéro de port fournis dans la configuration LSN, puis transmet la demande au bureau d'enregistrement SIP. L'ALG SIP ouvre ensuite un trou d'épingle dans la configuration de Citrix ADC pour permettre une communication SIP supplémentaire entre le client SIP et le bureau d'enregistrement SIP. Le bureau d'enregistrement SIP envoie une réponse 200 OK au client SIP via l'adresse IP du pool LSN et le numéro de port. L'appliance Citrix ADC capture cette réponse dans le trou d'épingle et l'ALG SIP remplace l'en-tête SIP, en remplaçant les champs SIP Contact, Via, Route et Record-Route d'origine dans le message. Le SIP ALG transmet ensuite le message au client SIP. La figure suivante montre comment SIP ALG utilise LSN dans un flux d'enregistrement d'appels SIP.



Appels sortants

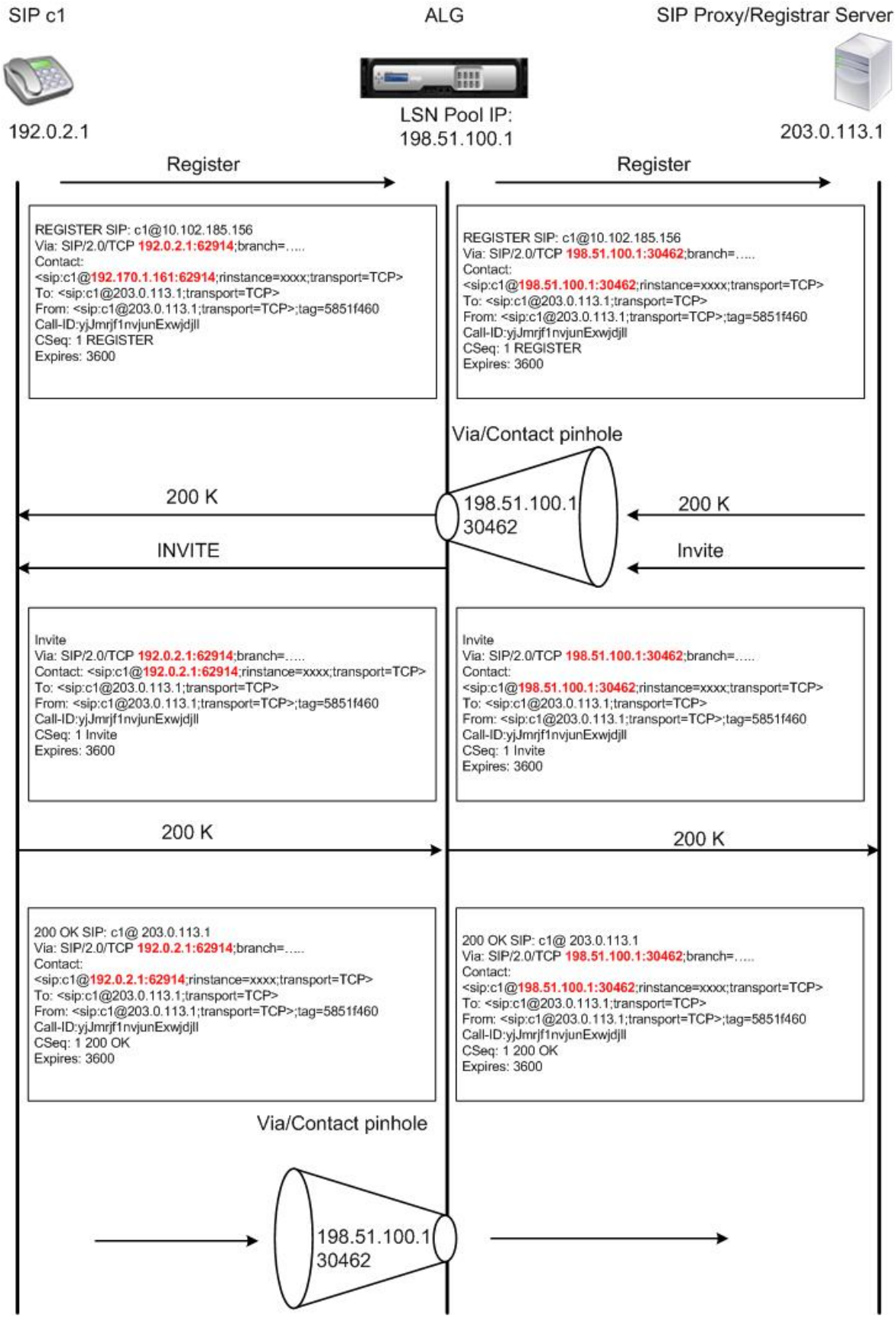
Un appel SIP est lancé avec un message SIP INVITE envoyé de l'interne au réseau externe. L'ALG SIP effectue NAT sur les adresses IP et les numéros de port dans les champs d'en-tête SIP Via, Contact, Route et Record-Route, en les remplaçant par l'adresse IP du pool LSN et le numéro de port. LSN stocke ces mappages pour les messages SIP suivants dans l'appel SIP. L'ALG SIP ouvre ensuite des trous d'épingles séparés dans la configuration de Citrix ADC pour autoriser SIP et les supports via l'appliance Citrix ADC sur les ports affectés dynamiquement spécifiés dans les en-têtes SDP et SIP. Lorsqu'un message 200 OK arrive à Citrix ADC, il est capturé par l'un des trous d'épingle créés. L'ALG SIP remplace l'en-tête SIP, restaure les champs SIP Contact, Via, Route et Record-Route d'origine, puis transfère le message au client SIP interne.



Appels entrants

Un appel entrant SIP est lancé avec un message SIP INVITE du client externe vers le réseau interne. Le bureau d'enregistrement SIP transmet le message INVITE au client SIP du réseau interne, en utilisant le trou d'épingle créé lors de l'inscription du client SIP interne auprès du bureau d'enregistrement SIP.

L'ALG SIP effectue NAT sur les adresses IP LSN et les numéros de port dans les champs d'en-tête SIP Via, Contact, Route et Record-Route SIP, en les traduisant en adresse IP et numéro de port du client SIP interne, et transmet la demande au client SIP. Lorsque le message de réponse 200 OK envoyé par le client SIP interne arrive à l'appliance Citrix ADC, l'ALG SIP effectue NAT sur les adresses IP et les numéros de port dans les champs d'en-tête SIP Via, Contact, Route et Record-Route, en les traduisant vers l'adresse IP du pool LSN et le numéro de port, transmet la réponse au bureau d'enregistrement SIP, puis ouvre un sténopé dans le sens sortant pour une communication SIP



ultérieure.

Terminaison d'appel

Le message BYE met fin à un appel. Lorsque le périphérique reçoit un message BYE, il traduit les champs d'en-tête dans le message comme il le fait pour tout autre message. Mais comme un message BYE doit être accusé de réception par le récepteur avec un 200 OK, l'ALG retarde le déchirement de l'appel pendant 15 secondes pour laisser le temps de transmission du 200 OK.

Appel entre clients du même réseau

Lorsque le client A et le client B du même réseau lancent un appel, les messages SIP sont acheminés via le proxy SIP dans le réseau externe. L'ALG SIP traite l'INVITE à partir du client A comme un appel sortant normal. Puisque le client B se trouve dans le même réseau, le proxy SIP renvoie INIVITE à l'appliance Citrix ADC. L'ALG SIP examine le message INIVITE, détermine qu'il contient l'adresse IP NAT du client A et remplace cette adresse par l'adresse IP privée du client A avant d'envoyer le message au client B. Une fois l'appel établi entre les clients, Citrix ADC n'est pas impliqué dans la transmission des médias entre les clients.

Plus de scénarios SIP LSN : Proxy SIP à l'intérieur du réseau privé

Si vous souhaitez héberger le serveur proxy SIP dans le réseau privé, Citrix vous recommande d'effectuer l'une des opérations suivantes :

- Configurez un mappage LSN statique pour le proxy SIP privé. Pour plus d'informations, reportez-vous à la section Configuration de cartes LSN statiques. Assurez-vous que le port NAT est le même que celui configuré dans le profil ALG SIP.
- Configurez le serveur proxy SIP à l'intérieur d'une zone démilitarisée (DMZ).

Figure 1. Enregistrement des appels SIP

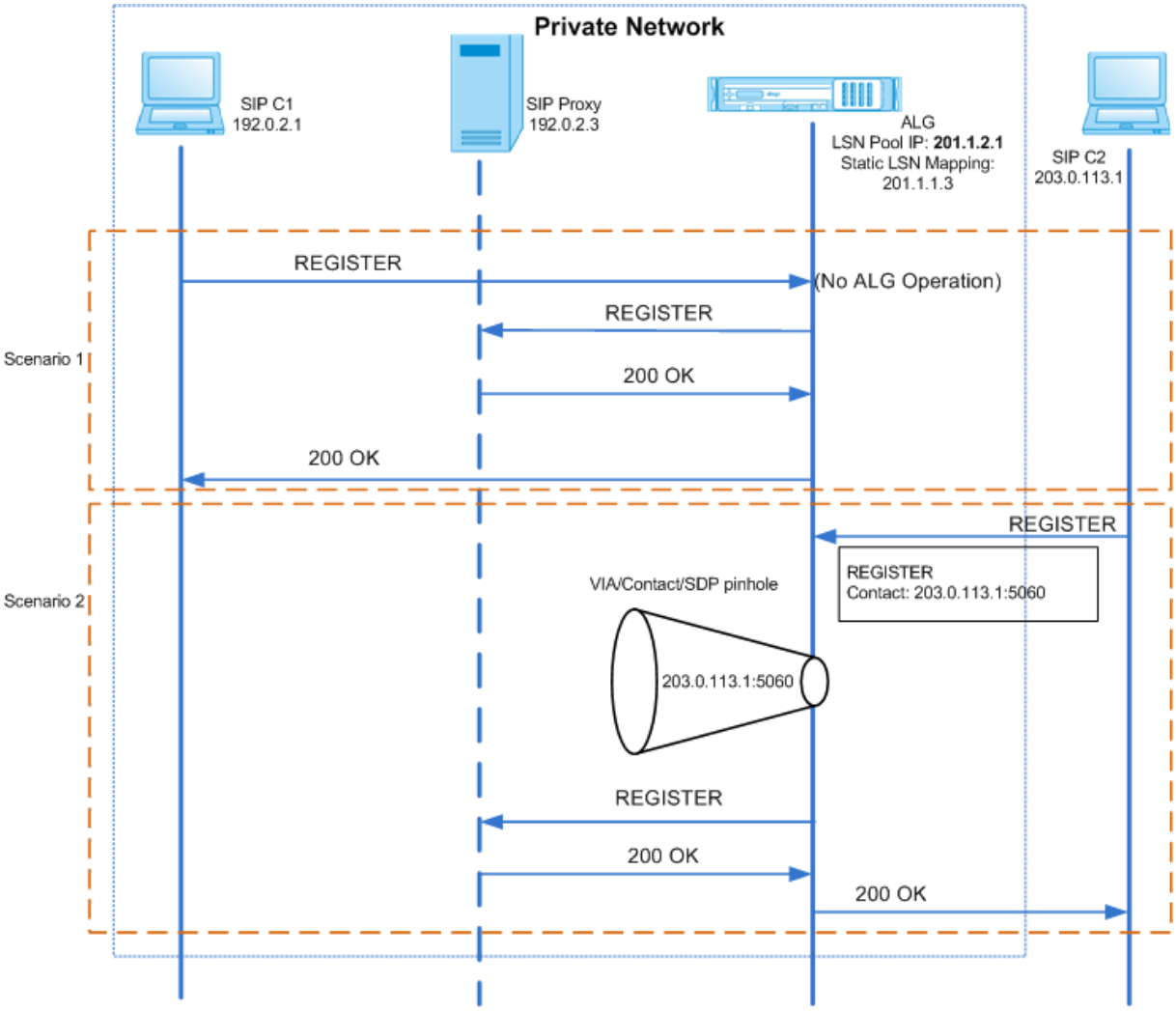
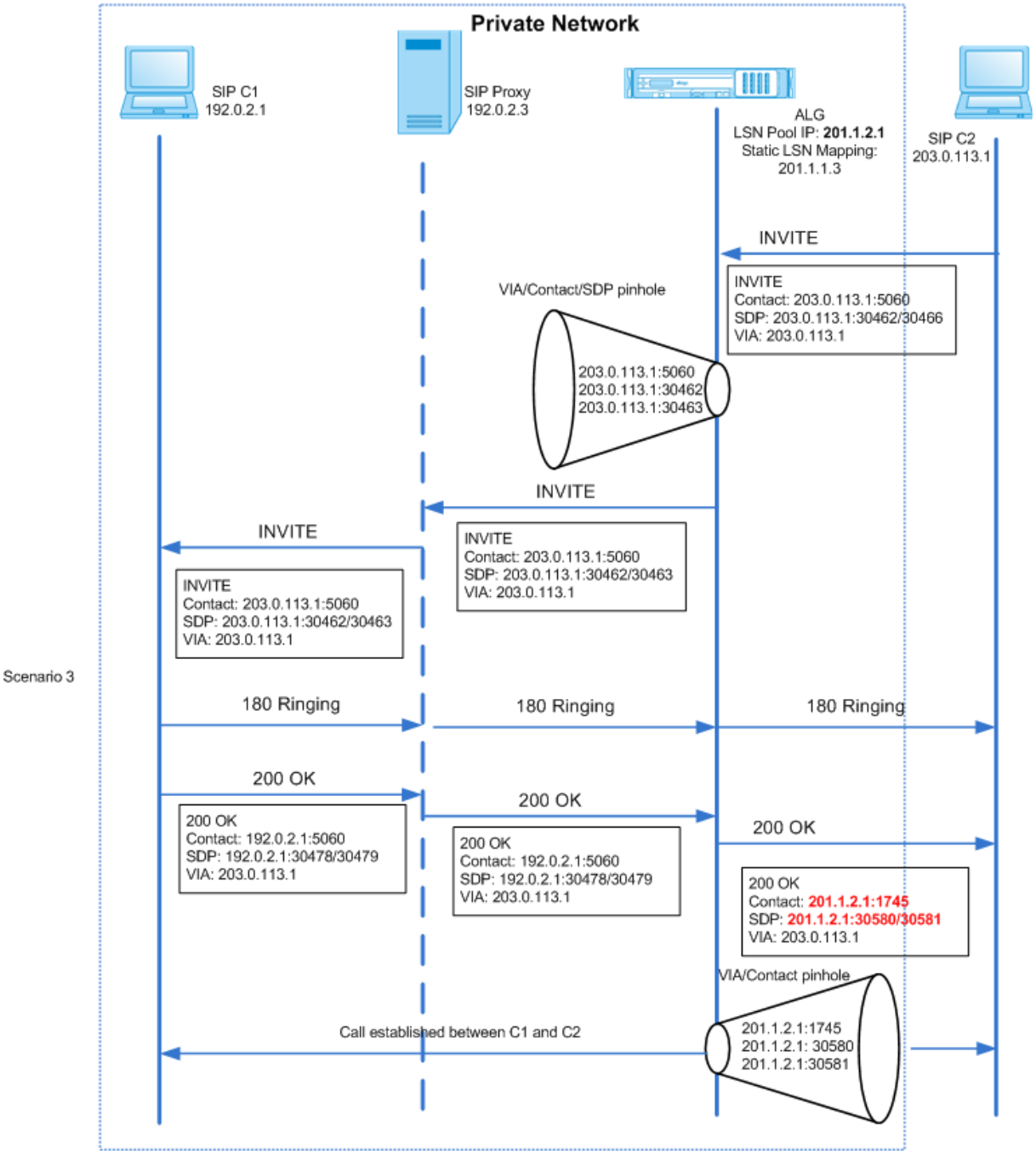


Figure 2. Flux d'appels entrants SIP



Les figures 1 et 2 présentent les scénarios suivants :

- Scénario 1 : Le client SIP du réseau privé s'enregistre auprès du serveur proxy SIP dans le même réseau. Les opérations ALG ne sont pas effectuées, car le client SIP et le serveur proxy SIP sont dans le même réseau.
- Scénario 2 : le client SIP dans le réseau public s'enregistre auprès du serveur proxy SIP dans le réseau privé. Le message REGISTER du client SIP public est envoyé à l'appliance Citrix ADC à l'aide du mappage LSN statique configuré sur l'appliance, et l'appliance crée un trou d'épingle

pour d'autres opérations SIP.

- Scénario 3 — SIP Flux d'appels entrants. Un appel entrant SIP est lancé avec un message SIP INVITE de l'externe vers le réseau interne. L'appliance Citrix ADC reçoit le message INVITE du client SIP C2, qui se trouve dans le réseau externe, via les mappages LSN statiques configurés sur l'appliance Citrix ADC.
  L'appliance crée un trou d'épingle et transmet le message INVITE au proxy SIP. Le proxy SIP transmet ensuite le message INVITE au client SIP C1 dans le réseau interne. Le client SIP C1 envoie ensuite 180 et 200 messages OK au proxy SIP, qui, à son tour, transfère le message au client SIP C2 via l'appliance Citrix ADC.
  Lorsque le message de réponse 200 OK envoyé par le client SIP interne C1 arrive à Citrix ADC, l'ALG SIP effectue NAT sur les adresses IP et les numéros de port dans les champs d'en-tête SIP Via, Contact, Route et Record-Route et dans les champs SDP, en les remplaçant par l'adresse IP du pool LSN et le numéro de port . Le SIP ALG transmet ensuite le message de réponse au client SIP C2 et ouvre un trou d'épingle dans le sens sortant pour une communication SIP ultérieure.

Prise en charge des journaux d'audit

Vous pouvez consigner les informations ALG dans le cadre de la journalisation LSN en activant ALG dans la configuration de journalisation d'audit LSN. Pour plus d'informations sur la journalisation LSN, consultez Logging and Monitoring LSN. Un message de journal pour une entrée ALG dans le journal LSN contient les informations suivantes :

- Horodatage
- Type de message SIP (par exemple, demande SIP)
- Adresse IP source et port du client SIP
- Adresse IP de destination et port du proxy SIP
- Adresse IP NAT et port
- Méthode SIP
- Numéro de séquence
- Indique si le client SIP est enregistré ou non
- Nom d'utilisateur et domaine de l'appelant
- Nom d'utilisateur et domaine du récepteur

Exemple de journal d'audit :

Requête :

```
1 07/19/2013:09:49:19 GMT Informational 0-PPE-0 : default ALG
    ALG_SIP_INFO_PACKET_EVENT 169 0 : Infomsg: "SIP request" - Group: g2
     - Call_ID: NTY0YjYwMTJmYjNhNDU5ZjlhMmQxOTM5ZTE3Zjc3NjM. - Transport
    : TCP - Source_IP: 192.169.1.165 - Source_port: 57952 -
    Destination_IP: 10.102.185.156 - Destination_port: 5060 - Natted_IP:
     10.102.185.191 - Natted_port: 10313 - Method: REGISTER -
```



```
    Sequence_Number: 3060 - Register: YES - Content_Type: -
    Caller_user_name: 156_pvt_1 - Callee_user_name: 156_pvt_1 -
    Caller_domain_name: - Callee_domain_name: -
<!--NeedCopy-->
```

Réponse :

```
07/19/2013:09:49:19 GMT Informational 0-PPE-0 : default ALG
    ALG_SIP_INFO_PACKET_EVENT 170 0 : Infomsg: "SIP response" - Group:
    g2 - Call_ID: NTY0YjYwMTJmYjNhNDU5ZjlhMmQxOTM5ZTE3Zjc3NjM. -
    Transport: TCP - Response_code 200 - Source_IP: 10.102.185.156 -
    Source_port: 5060 - Destination_IP: 192.169.1.165 - Destination_port
    : 57952 - Natted_IP: 10.102.185.191 - Natted_port: 10313 -
    Sequence_Number: 3060 - Content_Type: - Caller_user_name: 156_pvt_1
    - Callee_user_name: 156_pvt_1 - Caller_domain_name: -
    Callee_domain_name: -
<!--NeedCopy-->
```

Configuration de SIP ALG

Vous devez configurer le SIP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration de LSN, voir Étapes de configuration pour LSN. Lors de la configuration de LSN, assurez-vous que vous :

- Définissez les paramètres suivants lors de l'ajout du profil d'application LSN :
  - IP Pooling = PAIRED
  - Address and Port Mapping = ENDPOINT-INDEPENDENT
  - Filtering = ENDPOINT-INDEPENDENT

Important : Pour que le SIP ALG fonctionne, une configuration NAT de cône complet est obligatoire.

Exemple :

```
add lsn appsprofile app_tcp TCP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT
<!--NeedCopy-->
```

- Créez un profil ALG SIP et assurez-vous de définir la plage de ports source ou la plage de ports de destination.

Exemple :

```
add lsn sipalgprofile sipalgprofile_tcp -sipsrcportrange 1-65535 -
    sipdstportrange 5060 -openViaPinhole ENABLED -openRecordRoutePinhole
     ENABLED  - sipTransportProtocol TCP
```



```
<!--NeedCopy-->
```

- Définir SIP ALG = ENABLED, lors de la création du groupe LSN.

Exemple :

```
add lsn group g1 -clientname c1 -sipalg ENABLED
<!--NeedCopy-->
```

- Liez le profil ALG SIP au groupe LSN.

Exemple de configuration ALG SIP :

L'exemple de configuration suivant montre comment créer une configuration LSN simple avec un réseau abonné unique, une adresse IP NAT LSN unique, un paramètre spécifique SIP ALG et configurer SIP ALG :

```
add lsn pool p1

Done

bind lsn pool p1 10.102.185.190

Done

add lsn client c1

Done

bind lsn client c1 -network 192.170.1.0 -netmask 255.255.255.0

Done

add lsn appsprofile app_tcp TCP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done

add lsn appsprofile app_udp UDP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done

bind lsn appsprofile app_tcp 1-65535

Done
```



```
28
29 bind lsn appsprofile app_udp 1-65535
30
31 Done
32
33 add lsn sipalgprofile sipalgprofile_tcp -sipdstportrange 5060 -
      openViaPinhole ENABLED -openRecordRoutePinhole ENABLED  -
      sipTransportProtocol TCP
34
35 Done
36
37 add lsn sipalgprofile sipalgprofile_udp -sipdstportrange 5060 -
      openViaPinhole ENABLED -openRecordRoutePinhole ENABLED -
      sipTransportProtocol UDP
38
39 Done
40
41 add lsn group g1 -clientname c1 -sipalg ENABLED
42
43 Done
44
45 bind lsn group g1 -poolname p1
46
47 Done
48
49 bind lsn group g1 -appsprofilename app_tcp
50
51 Done
52
53 bind lsn group g1 -appsprofilename app_udp
54
55 Done
56
57 bind lsn group g1 -sipalgprofilename sipalgprofile_tcp
58
59 Done
60
61 bind lsn group g1 -sipalgprofilename sipalgprofile_udp
62
63 Done
64 <!--NeedCopy-->
```


Passerelle de couche d'application pour le protocole RTSP

August 20, 2021

Le protocole RTSP (Real Time Streaming Protocol) est un protocole au niveau de l'application pour le transfert de données multimédia en temps réel. Utilisé pour établir et contrôler des sessions multimédias entre les points de fin, RTSP est un protocole de canal de contrôle entre le client multimédia et le serveur multimédia. La communication typique est entre un client et un serveur multimédia de streaming.

La diffusion de médias à partir d'un réseau privé vers un réseau public nécessite la traduction des adresses IP et des numéros de port sur le réseau. La fonctionnalité Citrix ADC comprend une passerelle de couche d'application (ALG) pour RTSP, qui peut être utilisée avec le NAT à grande échelle (LSN) pour analyser le flux de médias et apporter les modifications nécessaires pour garantir que le protocole continue de fonctionner sur le réseau.

La manière dont la traduction d'adresses IP est effectuée dépend du type et de la direction du message, ainsi que du type de support pris en charge par le déploiement client-serveur. Les messages sont traduits comme suit :

- Demande sortante : adresse IP privée vers une adresse IP publique appartenant à Citrix ADC appelée adresse IP de pool LSN.
- Réponse entrante : adresse IP du pool LSN vers adresse IP privée.
- Demande entrante : aucune traduction.
- Réponse sortante : adresse IP privée à l'adresse IP du pool LSN.

> **Remarque**
>
> RTSP ALG est pris en charge dans une appliance autonome Citrix ADC, dans une configuration de haute disponibilité Citrix ADC, ainsi que dans une configuration de cluster Citrix ADC.

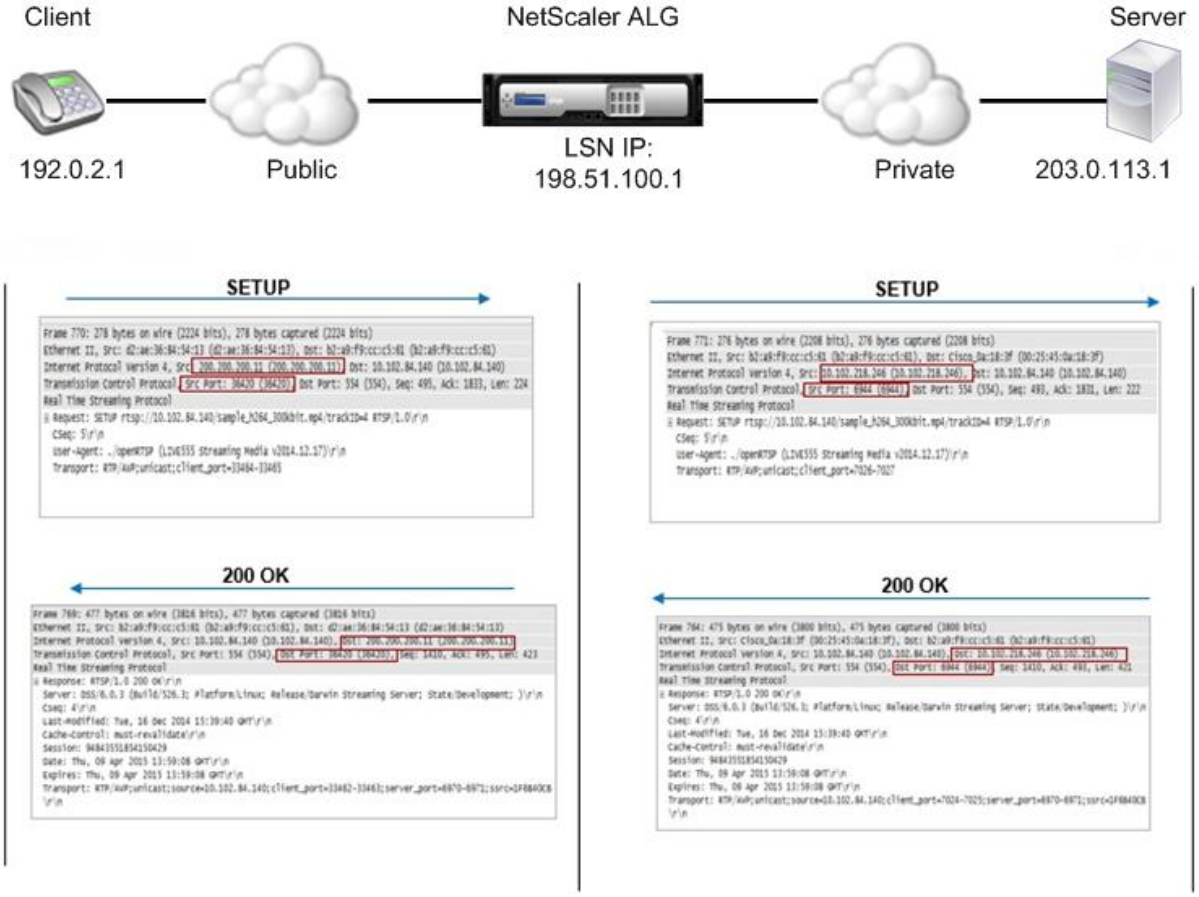
Limites de l'ALG RTSP

Le RTSP ALG ne prend pas en charge les éléments suivants :

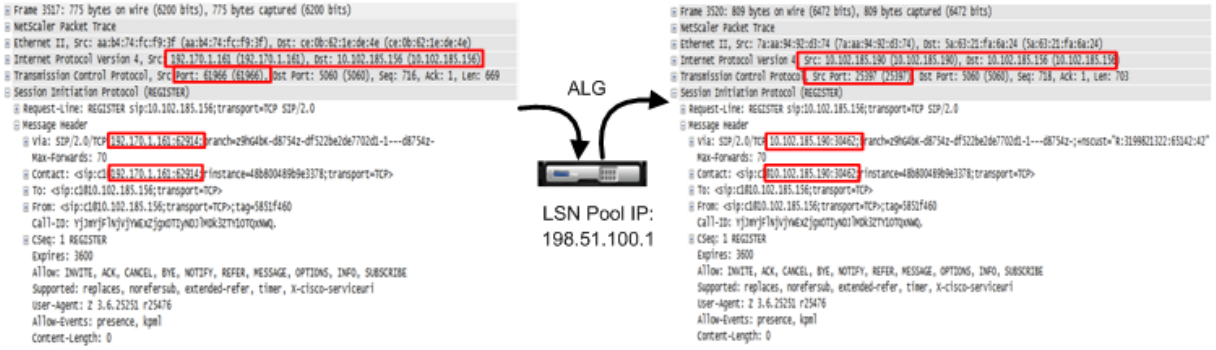
- Sessions RTSP multidiffusion
- Session RTSP via UDP
- Partitionnement TD/Admin
- Authentification RSTP
- Tunneling HTTP

Scénario RTSP et LSN

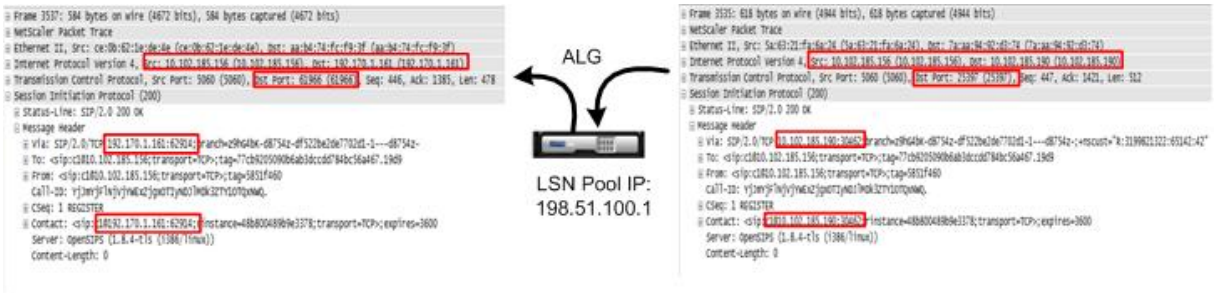
La figure suivante illustre un flux de demande RTSP SETUP. En règle générale, une requête SETUP spécifie comment un flux multimédia unique doit être transporté. La demande contient l'URL du flux de médias et un spécificateur de transport. Ce spécificateur inclut généralement un port local pour la réception de données RTP (audio ou vidéo), et un autre pour la réception de données RTCP (méta-informations). La réponse du serveur confirme généralement les paramètres choisis et remplit les parties manquantes, telles que les ports choisis par le serveur. Chaque flux multimédia doit être configuré à l'aide de la commande SETUP avant qu'une demande de lecture agrégée puisse être envoyée.



Dans une communication RTSP typique, le client média du réseau public envoie une demande SETUP au serveur de médias du réseau privé. RSTP ALG intercepte la demande et, dans le flux multimédia, remplace l'adresse IP publique et le numéro de port par l'adresse IP du pool LSN et le numéro de port LSN. La figure suivante illustre la traduction effectuée par une appliance Citrix ADC dans le flux de médias pour une demande sortante :



Le serveur de médias du réseau privé utilise l'adresse IP du pool LSN et le numéro de port LSN pour envoyer une réponse 200 OK au client multimédia dans le réseau public. Le Citrix ADC RTSP ALG intercepte la réponse et remplace l'adresse IP du pool LSN et le numéro de port LSN par l'adresse IP publique et le numéro de port du client multimédia. La figure suivante illustre la traduction effectuée par une appliance Citrix ADC dans le flux de médias pour une réponse entrante :



Configuration de RTSP ALG

Configurez RTSP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration de LSN, voir Étapes de configuration pour LSN. Lors de la configuration de LSN, assurez-vous que vous :

- Définissez le **type NAT** comme DETERMINISTIC ou DYNAMIC lors de l'ajout du pool LSN.
- Définissez les paramètres suivants lors de l'ajout du profil d'application LSN :
  - IP Pooling = PAIRED
  - Address and Port Mapping = ENDPOINT-INDEPENDENT
  - Filtering = ENDPOINT-INDEPENDENT
- Créer un profil ALG RTSP et lier le profil ALG RTSP au groupe LSN

Exemple de configuration ALG RTSP :

L'exemple de configuration suivant montre comment créer une configuration LSN simple avec un réseau abonné unique, une adresse IP NAT LSN unique et des paramètres ALG RTSP :

```
1 enable ns feature WL SP LB CS LSN
2
```



```
Done

add lsn pool pool1 -nattype DETERMINISTIC

Done

bind lsn pool pool1 10.102.218.246

Done

add lsn client client1

Done

bind lsn client client1 -network 200.200.200.11 -netmask 255.255.255.0

Done

add lsn appsprofile app1 TCP -ippooling PAIRED -mapping ENDPOINT-
   INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done

add lsn appsprofile app2 UDP -ippooling PAIRED -mapping ENDPOINT-
   INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done

bind lsn appsprofile app1 1-65535

Done

bind lsn appsprofile app2 1-65535

Done

add lsn rtspalgprofile rtspalgprofiledefault -rtspIdleTimeout 1000 -
   rtspportrange 554

Done

add lsn group group1 -clientname client1 -nattype DETERMINISTIC -
   portblocksize 512 -rtspalg ENABLED

Done
```



```
44
45 bind lsn group group1 -poolname pool1
46
47 Done
48
49 bind lsn group group1 -appsprofilename app1
50
51 Done
52
53 bind lsn group group1 -appsprofilename app2
54
55 Done
56
57 bind lsn group group1 -rtspalgprofilename rtspalgprofiledefault
58
59 Done
60 <!--NeedCopy-->
```

Passerelle de couche d'application pour le protocole IPSec

August 20, 2021

Si la communication entre deux périphériques réseau (par exemple, client et serveur) utilise le protocole IPSec, le trafic IKE (qui est via UDP) utilise des champs de port, mais pas le trafic ESP (Encapsulating Security Payload). Si un périphérique NAT sur le chemin attribue la même adresse IP NAT (mais des ports différents) à deux clients ou plus à la même destination, le périphérique NAT n'est pas en mesure de distinguer et d'acheminer correctement le trafic ESP de retour ne contient pas d'informations de port. Par conséquent, le trafic IPsec ESP échoue sur le périphérique NAT.

Les points de terminaison IPSec compatibles NAT-Traversal (NAT-T) détectent la présence d'un périphérique NAT intermédiaire pendant la phase 1 IKE et basculent vers le port UDP 4500 pour tout le trafic IKE et ESP ultérieur (encapsulant ESP dans UDP). Sans prise en charge NAT-T sur les points de terminaison IPsec homologues, le trafic ESP protégé IPsec est transmis sans encapsulation UDP. Par conséquent, le trafic IPsec ESP échoue sur le périphérique NAT.

L'appliance Citrix ADC prend en charge la fonctionnalité ALG (Application Layer Gateway) IPsec pour les configurations NAT à grande échelle. L'ALG IPsec traite le trafic ESP IPsec et gère les informations de session de sorte que le trafic n'échoue pas lorsque les points de terminaison IPSec ne prennent pas en charge NAT-T (encapsulation UDP du trafic ESP).

Fonctionnement d'IPSec ALG

Un ALG IPsec surveille le trafic IKE entre un client et le serveur et n'autorise qu'un seul échange de messages IKE phase 2 entre le client et le serveur à un moment donné.

Une fois que les paquets ESP bidirectionnels sont reçus pour un flux particulier, l'ALG IPSec crée une session NAT pour ce flux particulier afin que le trafic ESP ultérieur puisse circuler en douceur. Le trafic ESP est identifié par les SPI (Security Parameters Indexes), qui sont uniques pour un flux et pour chaque direction. Un ALG IPsec utilise des SPI ESP à la place des ports source et destination pour effectuer des NAT à grande échelle.

Si une porte ne reçoit pas de trafic, elle expire. Après l'expiration des deux portes, un autre échange IKE phase 2 est autorisé.

Délais d'expiration IPsec ALG

IPSec ALG sur une appliance Citrix ADC comporte trois paramètres de délai d'expiration :

- Délai d'**expiration de la porte ESP**. Durée maximale pendant laquelle l'appliance Citrix ADC bloque une porte ALG IPSec pour un client particulier sur une adresse IP NAT spécifique pour un serveur donné si aucun trafic ESP bidirectionnel n'est échangé entre le client et le serveur.
- Délai d'**expiration de la session IKE**. Durée maximale pendant laquelle l'appliance Citrix ADC conserve les informations de session IKE avant de les supprimer s'il n'y a pas de trafic IKE pour cette session.
- Délai d'**expiration de la session ESP**. Durée maximale pendant laquelle l'appliance Citrix ADC conserve les informations de session ESP avant de les supprimer s'il n'y a pas de trafic ESP pour cette session.

Points à considérer avant de configurer IPSec ALG

Avant de commencer à configurer IPSec ALG, tenez compte des points suivants :

- Vous devez comprendre les différents composants du protocole IPSec.
- IPSec ALG n'est pas pris en charge pour les configurations DS-Lite et Large échelle NAT64.
- IPSec ALG n'est pas pris en charge pour le flux LSN en épingle à cheveux.
- IPSec ALG ne fonctionne pas avec les configurations RNAT.
- IPSec ALG n'est pas pris en charge dans les clusters Citrix ADC.

Étapes de configuration

La configuration d'IPSec ALG pour NAT44 à grande échelle sur une appliance Citrix ADC comporte les tâches suivantes :

- **Créez un profil d'application LSN et liez-le à la configuration LSN.** Définissez les paramètres suivants lors de la configuration d'un profil d'application :
  - Protocol=UDP
  - IP Pooling = PAIRED
  - Port=500

Liez le profil d'application au groupe LSN d'une configuration LSN. Pour obtenir des instructions sur la création d'une configuration LSN, voir Étapes de configuration pour LSN.

- **Créez un profil IPSec ALG**. Un profil IPsec inclut divers délais d'expiration IPsec, tels que le délai d'expiration de session IKE, le délai d'expiration de session ESP et le délai d'expiration de la porte ESP. Vous liez un profil ALG IPsec à un groupe LSN. Un profil IPSec ALG possède les paramètres par défaut suivants :
  - Délai d'expiration de la session IKE = 60 minutes
  - Délai d'expiration de session ESP = 60 minutes
  - Délai d'expiration de la porte ESP = 30 secondes
- **Liez le profil ALG IPsec à la configuration LSN**. ALG IPsec est activé pour une configuration LSN lorsque vous liez un profil ALG IPSec à la configuration LSN. Liez le profil ALG IPsec à la configuration LSN en définissant le paramètre de profil ALG IPsec sur le nom du profil créé dans le groupe LSN. Un profil ALG IPsec peut être lié à plusieurs groupes LSN, mais un groupe LSN ne peut avoir qu'un seul profil ALG IPsec.

Pour créer un profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn appsprofile <appsprofilename> UDP -ippooling PAIRED

show lsn appsprofile
<!--NeedCopy-->
```

Pour lier le port de destination au profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```


Pour lier un profil d'application LSN à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname> -appsprofilename <string>

show lsn group
<!--NeedCopy-->
```

Pour créer un profil ALG IPSec à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ipsecalg profile <name> [-ikeSessionTimeout <positive_integer>] [-
    espSessionTimeout <positive_integer>] [-espGateTimeout <
    positive_integer>] [-connfailover ( ENABLED | DISABLED)

show ipsecalg profile <name>
<!--NeedCopy-->
```

Pour lier un profil ALG IPSec à une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname> -poolname <string> - ipsecAlgProfile <string
    >

show lsn group <name>
<!--NeedCopy-->
```

Pour créer un profil d'application LSN et le lier à une configuration LSN à l'aide de l'interface graphique

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur l'onglet **Application**, ajoutez un profil d'application LSN et liez-le à un groupe LSN.

Pour créer un profil ALG IPSec à l'aide de l'interface graphique**

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur l'onglet **ALG IPSEC**, puis ajoutez un profil ALG IPSec.

Pour lier un profil ALG IPsec à une configuration LSN à l'aide de l'interface graphique****

1. Accédez à **Système** > **NAT à grande échelle** > **Groupe LSN**, ouvrez le groupe LSN.
2. Dans **Paramètres avancés**, cliquez sur **+ Profil ALG IPSEC**pour lier le profil ALG IPSec créé au groupe LSN.

Exemple de configuration

Dans l'exemple de configuration NAT44 à grande échelle suivant, IPSec ALG est activé pour les abonnés du réseau 192.0.2.0/24. Le profil IPSec ALG IPSECALGPROFILE-1 avec divers paramètres de délai d'expiration IPsec est créé et est lié au groupe LSN LSN Group -1.

Exemple de configuration :

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.9

Done

add lsn appsprofile LSN-APPSPROFILE-1 UDP -ippooling PAIRED

Done

bind lsn appsprofile LSN-APPSPROFILE-1 500

Done

add ipsecalg profile  IPSECALGPROFILE-1 -ikeSessionTimeout 45  -
   espSessionTimeout 40  - espGateTimeout 20 -connfailover ENABLED

Done

bind lsn group LSN-GROUP-1 -appsprofilename LSN-APPSPROFILE-1

```



```
Done

bind lsn group LSN-GROUP-1 -poolname LSN-POOL-1

Done

bind lsn group LSN-GROUP-1 - ipsecAlgProfile IPSECALGPROFILE-1

Done
<!--NeedCopy-->
```

Journalisation et surveillance LSN

October 4, 2021

Vous pouvez consigner les informations LSN pour diagnostiquer, résoudre les problèmes et respecter les exigences légales. Vous pouvez surveiller les performances de la fonction LSN en utilisant les compteurs statistiques LSN et en affichant les sessions LSN actuelles.

Journalisation LSN

La consignation des informations sur les LSN est l'une des fonctions importantes requises par les FSI pour satisfaire aux exigences légales et pour identifier la source du trafic à tout moment.

Une appliance Citrix ADC enregistre les entrées de mappage LSN et les sessions LSN créées ou supprimées pour chaque groupe LSN. Vous pouvez contrôler la journalisation des informations LSN pour un groupe LSN en utilisant les paramètres de journalisation et de journalisation de session du groupe LSN. Il s'agit de paramètres au niveau du groupe et sont désactivés par défaut. L'appliance Citrix ADC consigne les sessions LSN pour un groupe LSN uniquement lorsque les paramètres de journalisation et de journalisation de session sont activés.

Le tableau suivant affiche le comportement de journalisation d'un groupe LSN pour différents paramètres de journalisation et de journalisation de session.

Journalisation	Journalisation de session	Comportement de journalisation
Activé	Activé	Consigne les entrées de mappage LSN ainsi que les sessions LSN.

Journalisation	Journalisation de session	Comportement de journalisation
Activé	Désactivé	Consigne les entrées de mappage LSN mais pas les sessions LSN.
Désactivé	Activé	Ne consigne ni les entrées de mappage ni les sessions LSN.

Un message de journal pour une entrée de mappage LSN contient les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal provient
- Horodatage
- Type d'entrée (MAPPING)
- Indique si l'entrée de mappage LSN a été créée ou supprimée
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP NAT et port
- Nom du protocole
- L'adresse IP de destination, le port et l'ID de domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
  - Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
  - L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse.

Un message de journal pour une session LSN contient les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal provient
- Horodatage
- Type d'entrée (SESSION)
- Indique si la session LSN est créée ou supprimée
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP NAT et port
- Nom du protocole
- Adresse IP de destination, port et ID de domaine de trafic

L'appliance utilise son infrastructure de journal syslog et d'audit existants pour consigner les informations LSN. Vous devez activer la journalisation LSN de niveau global en activant le paramètre LSN dans

l'action NSLOG associée et les entités d'action SYLOG. Lorsque le paramètre Journalisation est activé, l'appliance Citrix ADC génère des messages de journal liés aux mappages LSN et aux sessions LSN de ce groupe LSN. L'appliance envoie ensuite ces messages de journal aux serveurs associés à l'action NSLOG et aux entités d'action SYSLOG.

Pour la journalisation des informations LSN, Citrix recommande :

- Journalisation des informations LSN sur les serveurs de journaux externes plutôt que sur l'appliance Citrix ADC. La journalisation sur des serveurs externes facilite les performances optimales lorsque l'appliance crée de grandes quantités d'entrées de journal LSN (par ordre de millions).
- Utilisation de SYSLOG sur TCP, ou NSLOG. Par défaut, SYSLOG utilise UDP et NSLOG utilise uniquement TCP pour transférer les informations de journal vers les serveurs de journaux. TCP est plus fiable que UDP pour le transfert de données complètes.

  Remarque :

  - Les SYSLOG générés sur l'appliance Citrix ADC sont envoyés dynamiquement aux serveurs de journaux externes.
  - Lors de l'utilisation de SYSLOG sur TCP, si la connexion TCP est interrompue ou si le serveur SYSLOG est occupé, les appliances Citrix ADC stockent les journaux dans la mémoire tampon et envoient les données une fois la connexion active.

Pour plus d'informations sur la configuration de la journalisation, voir Journalisation des audits.

La configuration de la journalisation LSN comporte les tâches suivantes :

- **Configuration de l'appliance Citrix ADC pour la journalisation.** Cette tâche implique la création et la définition de diverses entités et paramètres de l'appliance Citrix ADC :
  - **Créez une configuration de journalisation d'audit SYSLOG ou NSLOG**. La création d'une configuration de journalisation d'audit implique les tâches suivantes :
    * Créez une action d'audit NSLOG ou SYSLOG et activez le paramètre LSN. Les actions d'audit spécifient les adresses IP des serveurs de journaux.
    * Créez une stratégie d'audit SYSLOG ou NSLOG et liez l'action d'audit à la stratégie d'audit. Les actions d'audit spécifient les adresses IP des serveurs de journaux. Le cas échéant, vous pouvez définir la méthode de transport pour les messages de journal envoyés aux serveurs de journaux externes. Par défaut, UDP est sélectionné, vous pouvez définir la méthode de transport comme TCP pour un mécanisme de transport fiable.Liez la stratégie d'audit au système global.
    * Créez une stratégie d'audit SYSLOG ou NSLOG et liez l'action d'audit à la stratégie d'audit.
    * Liez la stratégie d'audit au système global.
      Remarque : Pour une configuration de journalisation d'audit existante, activez simplement le paramètre LSN pour la journalisation des informations LSN dans le serveur

spécifié par l'action d'audit.

- **Activer les paramètres de journalisation et de journalisation de session.** Activez les paramètres de journalisation et de journalisation de session lorsque vous ajoutez des groupes LSN ou après avoir créé les groupes. L'appliance Citrix ADC génère des messages de journal liés à ces groupes LSN et les envoie au serveur des actions d'audit pour lesquelles le paramètre LSN est activé.

- **Configuration des serveurs de journaux.** Cette tâche implique l'installation de packages SYSLOG ou NSLOG sur les serveurs souhaités. Cette tâche implique également de spécifier l'adresse NSIP de l'appliance Citrix ADC dans le fichier de configuration de SYSLOG ou NSLOG. La spécification de l'adresse NSIP permet au serveur d'identifier les informations de journal envoyées par l'appliance Citrix ADC pour les stocker dans un fichier journal.

Pour plus d'informations sur la configuration de la journalisation, voir Journalisation des audits.

Configuration SYSLOG à l'aide de l'interface de ligne de commande

Pour créer une action serveur SYSLOG pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel
    <logLevel>... [-transport (TCP)] [-lsn ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Pour créer une stratégie de serveur SYSLOG pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add audit syslogPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Pour lier une stratégie de serveur SYSLOG au système global pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind system global [<policyName> [-priority <positive_integer>]]
<!--NeedCopy-->
```


Configuration SYSLOG à l'aide de l'utilitaire de configuration

Pour configurer une action serveur SYSLOG pour la journalisation LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Systèmes** > **Audit** > **Syslog** et, sous l'onglet Serveurs, ajoutez un nouveau serveur d'audit ou modifiez un serveur existant.
2. Pour activer la journalisation LSN, sélectionnez l'option **Journalisation NAT à grande échelle**.
3. (Facultatif) Pour activer SYSLOG sur TCP, sélectionnez l'option **Journalisation TCP** .

Pour configurer une stratégie de serveur SYSLOG pour la journalisation LSN à l'aide de l'utilitaire de configuration

Accédez à **Systèmes** > **Audit** > **Syslog** et, sous l'onglet **Stratégies**, ajoutez une nouvelle stratégie ou modifiez une stratégie existante.

Pour lier une stratégie de serveur SYSLOG au système global pour la journalisation LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Systèmes** > **Audit** > **Syslog** .
2. Sous l'onglet **Stratégies**, dans la liste **Action**, cliquez sur **Liaisons globales** pour lier les stratégies globales d'audit.

Configuration de NSLOG à l'aide de l'interface de ligne de commande

Pour créer une action serveur NSLOG pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel
     <logLevel> ... [-lsn ( ENABLED | DISABLED )]
2 <!--NeedCopy-->
```

Pour créer une stratégie de serveur NSLOG pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add audit nslogPolicy <name> <rule> <action>
2 <!--NeedCopy-->
```


Pour lier une stratégie de serveur NSLOG au système global pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind system global [<policyName>]
<!--NeedCopy-->
```

Configuration de NSLOG à l'aide de l'utilitaire de configuration

Pour configurer une action de serveur NSLOG pour la journalisation LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Systèmes** > **Audit** > **Nslog** et, sous l'onglet **Serveurs**, ajoutez un nouveau serveur d'audit ou modifiez un serveur existant.
2. Pour activer la journalisation LSN, sélectionnez l'option **Journalisation NAT à grande échelle**.

Pour configurer une stratégie de serveur NSLOG pour la journalisation LSN à l'aide de l'utilitaire de configuration

Accédez à **Systèmes** > **Audit** > **Nslog** et, sous l'onglet **Stratégies**, ajoutez une nouvelle stratégie ou modifiez une stratégie existante.

Pour lier une stratégie de serveur NSLOG au système global pour la journalisation LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Systèmes** > **Audit** > **Nslog** .
2. Sous l'onglet **Stratégies**, dans la liste **Action**, cliquez sur **Liaisons globales** pour lier les stratégies globales d'audit.

Exemple

La configuration suivante spécifie deux serveurs SYSLOG et deux serveurs NSLOG pour stocker les entrées de journal, y compris les journaux LSN. La journalisation LSN est configurée pour les groupes LSN LSN-GROUP-2 et LSN-GROUP-3.

L'appliance Citrix ADC génère des messages de journal liés aux mappages LSN et aux sessions LSN de ces groupes LSN et les envoie aux serveurs de journaux spécifiés.

```
add audit syslogAction SYS-ACTION-1 198.51.101.10 -logLevel ALL -lsn
    ENABLED
Done
add audit syslogPolicy SYSLOG-POLICY-1 ns_true SYS-ACTION-1
```



```
4  Done
5  bind system global SYSLOG-POLICY-1
6  Done
7
8  add audit syslogAction SYS-ACTION-2 198.51.101.20 -logLevel ALL -lsn
       ENABLED
9  Done
10 add audit syslogPolicy SYSLOG-POLICY-2 ns_true SYS-ACTION-2
11 Done
12 bind system global SYSLOG-POLICY-2
13 Done
14
15 add audit nslogAction NSLOG-ACTION-1 198.51.101.30 -logLevel ALL -lsn
       ENABLED
16 Done
17 add audit nslogPolicy NSLOG-POLICY-1 ns_true NSLOG-ACTION-1
18 Done
19 bind system global NSLOG-POLICY-1
20 Done
21 add audit nslogAction NSLOG-ACTION-2 198.51.101.40 -logLevel ALL -lsn
       ENABLED
22 Done
23 add audit nslogPolicy NSLOG-POLICY-2 ns_true NSLOG-ACTION-2
24 Done
25 bind system global NSLOG-POLICY-2
26 Done
27
28 add lsn group LSN-GROUP-3 -clientname LSN-CLIENT-2  - logging ENABLED  -
       sessionLogging ENABLED
29 Done
30 set lsn group LSN-GROUP-2   - logging ENABLED  - sessionLogging ENABLED
31 Done
32 <!--NeedCopy-->
```

La configuration suivante spécifie la configuration SYSLOG pour l'envoi de messages de journal au serveur SYSLOG externe 192.0.2.10 à l'aide de TCP.

```
1  add audit syslogAction SYS-ACTION-1 192.0.2.10 -logLevel ALL -transport
       TCP
2  Done
3
4  add audit syslogPolicy SYSLOG-POLICY-1 ns_true SYS-ACTION-1
5  Done
6
7  bind system global SYSLOG-POLICY-1
```



```
8 Done
9 <!--NeedCopy-->
```

Le tableau suivant affiche des exemples d'entrées de journal LSN de chaque type stocké sur les serveurs de journaux configurés. Ces entrées de journal LSN sont générées par une appliance Citrix ADC dont l'adresse NSIP est 10.102.37.115.

Type d'entrée du journal LSN	Exemple d'entrée de journal
Création de session LSN	Local4.Informational 10.102.37.115 08/05/2014:09:59:48 GMT 0-PPE-0 : LSN LSN_SESSION 2581750 : SESSION CREATED Client IP:Port:TD 192.0.2.10: 15136:0, NatIP:NatPort 203.0.113.6: 6234, Destination IP:Port:TD 198.51.100.9: 80:0, Protocol: TCP
Suppression de session LSN	Local4.Informational 10.102.37.115 08/05/2014:10:05:12 GMT 0-PPE-0 : LSN LSN_SESSION 3871790 : SESSION DELETED Client IP:Port:TD 192.0.2.11: 15130:0, NatIP:NatPort 203.0.113.6: 7887, Destination IP:Port:TD 198.51.101.2:80:0, Protocol: TCP
Création de mappage LSN	Local4.Informational 10.102.37.115 08/05/2014:09:59:47 GMT 0-PPE-0 : LSN LSN_MAPPING 2581580 : EIM CREATED Client IP:Port 192.0.2.15: 14567, NatIP:NatPort 203.0.113.5: 8214, Protocol: TCP
Suppression de mappage LSN	Local4.Informational 10.102.37.115 08/05/2014:10:05:12 GMT 0-PPE-0 : LSN LSN_MAPPING 3871700 : EIM DELETED Client IP:Port 192.0.3.15: 14565, NatIP:NatPort 203.0.113.11: 8217, Protocol: TCP

Journalisation minimale

Les configurations LSN déterministes et les configurations LSN dynamiques avec bloc de port réduisent considérablement le volume du journal LSN. Pour ces deux types de configuration, l'appliance Citrix ADC alloue une adresse IP NAT et un bloc de ports à un abonné. L'appliance Citrix ADC génère un message de journal pour un bloc de port au moment de l'allocation à un abonné. L'appliance Citrix ADC génère également un message de journal lorsqu'une adresse IP NAT et un bloc

de port sont libérés. Pour une connexion, un abonné peut être identifié uniquement par son adresse IP NAT mappée et son bloc de port. Pour cette raison, l'appliance Citrix ADC ne consigne aucune session LSN créée ou supprimée. De plus, l'appliance ne consigne aucune entrée de mappage créée pour une session ni lorsque l'entrée de mappage est supprimée.

La fonction de journalisation minimale pour les configurations LSN déterministes et les configurations LSN dynamiques avec bloc de port est activée par défaut et aucune disposition ne permet de le désactiver. En d'autres termes, l'appliance Citrix ADC effectue automatiquement une journalisation minimale pour les configurations LSN déterministes et les configurations LSN dynamiques avec bloc de port. Aucune option n'est disponible pour désactiver cette fonctionnalité. L'appliance envoie les messages de journal à tous les serveurs de journaux configurés.

Un message de journal pour chaque bloc de port contient les informations suivantes :

- Adresse NSIP de l'appliance Citrix ADC
- Horodatage
- Type d'entrée DETERMINISTIC ou PORTBLOCK
- Indique si un bloc de port est alloué ou libéré
- Adresse IP de l'abonné et adresse IP NAT assignée et bloc de port
- Nom du protocole

Journalisation minimale pour la configuration de LSN déterministe

Prenons un exemple de configuration de LSN déterministe simple pour quatre abonnés ayant les adresses IP 192.0.17.1, 192.0.17.2, 192.0.17.3 et 192.0.17.4.

Dans cette configuration LSN, la taille du bloc de port est définie sur 32768 et le pool d'adresses IP NAT LSN a des adresses IP dans la plage 203.0.113.19-203.0.113.23.

```
1  add lsn client LSN-CLIENT-7
2  Done
3  bind lsn client LSN-CLIENT-7 -network 192.0.17.0 -netmask
       255.255.255.253
4  Done
5  add lsn pool LSN-POOL-7 -nattype DETERMINISTIC
6  Done
7  bind lsn pool LSN-POOL-7 203.0.113.19-203.0.113.23
8  Done
9  add lsn group LSN-GROUP-7 -clientname LSN-CLIENT-7 -nattype
       DETERMINISTIC -portblocksize 32768
10 Done
11 bind lsn group LSN-GROUP-7 -poolname LSN-POOL-7
12 Done
13 <!--NeedCopy-->
```


L'appliance Citrix ADC préalloue séquentiellement, à partir du pool d'adresses IP NAT LSN et en fonction de la taille de bloc de port définie, une adresse IP NAT LSN et un bloc de ports à chaque abonné. Il affecte le premier bloc de ports (1024-33791) sur l'adresse IP NAT de début (203.0.113.19) à l'adresse IP de l'abonné débutant (192.0.17.1). La plage suivante de ports est attribuée à l'abonné suivant, et ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné suivant. À ce stade, le premier bloc de port sur l'adresse IP NAT suivante est attribué à l'abonné, et ainsi de suite. L'appliance enregistre l'adresse IP NAT et le bloc de ports alloués à chaque abonné.

L'appliance Citrix ADC ne consigne aucune session LSN créée ou supprimée pour ces abonnés. L'appliance génère les messages de journal suivants pour la configuration LSN.

```
1) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201453 0 :  Dtrstc ALLOC Client 12.0.0.241,
   NatInfo 50.0.0.2:59904 to 60415
2) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201454 0 :  Dtrstc ALLOC Client 12.0.0.242,
   NatInfo 50.0.0.2:60416 to 60927
3) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201455 0 :  Dtrstc ALLOC Client 12.0.0.243,
   NatInfo 50.0.0.2:60928 to 61439
4) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201455 0 :  Dtrstc ALLOC Client 12.0.0.243,
   NatInfo 50.0.0.2:60928 to 61439
<!--NeedCopy-->
```

Lorsque vous supprimez la configuration LSN, l'adresse IP NAT allouée et le bloc de ports sont libérés de chaque abonné. L'appliance consigne l'adresse IP NAT et le bloc de ports libérés de chaque abonné. L'appliance génère les messages de journal suivants pour chaque abonné lorsque vous supprimez la configuration LSN.

```
1) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201706 0 :  Dtrstc FREE Client 12.0.0.238,
   NatInfo 50.0.0.2:58368 to 58879
2) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201707 0 :  Dtrstc FREE Client 12.0.0.239,
   NatInfo 50.0.0.2:58880 to 59391
3) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201708 0 :  Dtrstc FREE Client 12.0.0.240,
   NatInfo 50.0.0.2:59392 to 59903
<!--NeedCopy-->
```


Journalisation minimale pour la configuration LSN dynamique avec bloc de port

Considérons un exemple d'une configuration LSN dynamique simple avec bloc de port pour tout abonné dans le réseau 192.0.2.0/24. Dans cette configuration LSN, la taille du bloc de port est définie sur 1024 et le pool d'adresses IP NAT LSN a des adresses IP dans la plage 203.0.113.3-203.0.113.4.

```
set lsn parameter -memLimit 4000
Done
add lsn client LSN-CLIENT-1
Done
bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
Done
add lsn pool LSN-POOL-1
Done
bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.4
Done
add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1 -portblocksize 1024
Done
bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
Done
<!--NeedCopy-->
```

L'appliance Citrix ADC alloue une adresse IP NAT aléatoire et un bloc de ports, à partir du pool d'adresses IP NAT LSN et sur la base de la taille de bloc de port définie, pour un abonné lorsqu'il lance une session pour la première fois. Citrix ADC consigne l'adresse IP NAT et le bloc de ports alloués à cet abonné. L'appliance ne consigne aucune session LSN créée ou supprimée pour cet abonné. Si tous les ports sont alloués (pour les sessions d'abonnés différents) à partir du bloc de ports alloué à l'abonné, l'appliance alloue une nouvelle adresse IP NAT aléatoire et un nouveau bloc de ports pour l'abonné pour les sessions supplémentaires. Citrix ADC enregistre chaque adresse IP NAT et chaque bloc de port alloué à un abonné.

L'appliance génère le message de journal suivant lorsque l'abonné, ayant l'adresse IP 192.0.2.1, lance une session. Le message de journal indique que l'appliance a alloué l'adresse IP NAT 203.0.113.3 et le bloc de port 1024-2047 à l'abonné.

```
03/23/2015:00:07:12 GMT  Informational 0-PPE-3 : default LSN
   LSN_PORTBLOCK 106725793 0 :  Portblock ALLOC Client 12.0.2.72,
   NatInfo 203.0.113.3:1024 to 2047, Proto:TCP
<!--NeedCopy-->
```

Une fois qu'il n'y a plus de sessions qui utilisent l'adresse IP NAT allouée et l'un des ports dans le bloc de port alloué, l'adresse IP NAT allouée et le bloc de ports sont libérés de l'abonné. Le Citrix ADC enregistre que l'adresse IP NAT et le bloc de ports sont libérés de l'abonné. L'appliance génère les messages de journal suivants pour l'abonné, avec l'adresse IP 192.0.2.1, lorsqu'il ne reste plus de

sessions utilisant l'adresse IP NAT allouée (203.0.113.3) et un port du bloc de port alloué (1024-2047). Le message de journal indique que l'adresse IP NAT et le bloc de port sont libérés de l'abonné.

```
1 03/23/2015:00:11:09 GMT Informational 0-PPE-3 : default LSN
     LSN_PORTBLOCK 106814342 0 :  Portblock FREE Client 12.0.3.122,
     NatInfo 203.0.113.3: 1024 to 2047, Proto:TC
2 <!--NeedCopy-->
```

Serveurs SYSLOG d'équilibrage de charge

L'appliance Citrix ADC envoie ses événements et messages SYSLOG à tous les serveurs de journaux externes configurés. Cela entraîne le stockage des messages redondants et rend la surveillance difficile pour les administrateurs système. Pour résoudre ce problème, l'appliance Citrix ADC propose des algorithmes d'équilibrage de charge qui peuvent équilibrer la charge des messages SYSLOG parmi les serveurs de journaux externes pour une meilleure maintenance et des performances. Les algorithmes d'équilibrage de charge pris en charge incluent RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets et AuditlogHash.

Équilibrage de charge des serveurs SYSLOG à l'aide de l'interface de ligne de commande

Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

```
1 add service <name>(<IP> | <serverName>) <serviceType (SYSLOGTCP |
     SYSLOGUDP)> <port>
2 <!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGTCP, et la méthode d'équilibrage de charge AUDITLOGHASH.

```
1 add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
     <AUDITLOGHASH>]
2 <!--NeedCopy-->
```

Liez le service au serveur virtuel d'équilibrage de charge.

```
1 Bind lb vserver <name> <serviceName>
2 <!--NeedCopy-->
```

Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge qui a SYSLOGTCP ou SYSLOGUDP comme type de service.

```
1 add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
      <logLevel>]
```



```
2 <!--NeedCopy-->
```

Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

```
1 add syslogpolicy <name> <rule> <action>
2 <!--NeedCopy-->
```

Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.

```
1 bind system global <policyName>
2 <!--NeedCopy-->
```

Équilibrage de charge des serveurs SYSLOG à l'aide de l'utilitaire de configuration

1. Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

   Accédez à Gestion du trafic > Services, cliquez sur Ajouter et sélectionnez SYLOGTCP ou SYSLOGUDP comme protocole.

2. Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGTCP, et la méthode d'équilibrage de charge AUDITLOGHASH.

   Accédez à Gestion du trafic > Serveurs virtuels, cliquez sur Ajouter et sélectionnez SYLOGTCP ou SYSLOGUDP comme protocole.

3. Liez le service au serveur virtuel d'équilibrage de charge au service.

   Liez le service au serveur virtuel d'équilibrage de charge.

   Accédez à Gestion du trafic > Serveurs virtuels, sélectionnez un serveur virtuel, puis sélectionnez AUDITLOGHASH dans la méthode d'équilibrage de la charge.

4. Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge qui a SYSLOGTCP ou SYSLOGUDP comme type de service.

   Accédez à Système > Audit, cliquez sur Serveurs et ajoutez un serveur en sélectionnant LB Vserver option Inservers.

5. Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

   Accédez à Système > Syslog, cliquez sur Stratégies et ajoutez une stratégie SYSLOG.

6. Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.

   Accédez à Système > Syslog, sélectionnez une stratégie SYSLOG et cliquez sur Action, puis cliquez sur Liaisons globales et liez la stratégie à système global.

Exemple :

La configuration suivante spécifie l'équilibre de charge des messages SYSLOG entre les serveurs de journaux externes en utilisant la méthode AUDITLOGHASH comme méthode d'équilibrage de charge. L'appliance Citrix ADC génère des événements et des messages SYSLOG équilibrés entre les services, service1, service2 et service 3.

```
add service service1 192.0.2.10 SYSLOGUDP 514
Done

add service service2 192.0.2.11 SYSLOGUDP 514
Done

add service service3 192.0.2.11 SYSLOGUDP 514
Done

add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH
Done

bind lb vserver lbvserver1 service1
Done

bind lb vserver lbvserver1 service2
Done

bind lb vserver lbvserver1 service3
Done

add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All
Done

add syslogpolicy syspol1 ns_true sysaction1
Done

bind system global syspol1
Done
<!--NeedCopy-->
```

Journalisation des informations d'en-tête HTTP

L'appliance Citrix ADC peut désormais consigner les informations d'en-tête de requête d'une connexion HTTP qui utilise la fonctionnalité LSN de Citrix ADC. Les informations d'en-tête suivantes d'un paquet de requête HTTP peuvent être enregistrées :

- URL à laquelle la requête HTTP est destinée.
- Méthode HTTP spécifiée dans la requête HTTP.

- Version HTTP utilisée dans la requête HTTP.
- Adresse IP de l'abonné qui a envoyé la requête HTTP.

Les journaux d'en-tête HTTP peuvent être utilisés par les FAI pour voir les tendances liées au protocole HTTP parmi un ensemble d'abonnés. Par exemple, un FAI peut utiliser cette fonctionnalité pour trouver les sites Web les plus populaires parmi un ensemble d'abonnés.

Un profil de journal d'en-tête HTTP est un ensemble d'attributs d'en-tête HTTP (par exemple, URL et méthode HTTP) qui peuvent être activés ou désactivés pour la journalisation. Le profil de journal d'en-tête HTTP est alors lié à un groupe LSN. L'appliance Citrix ADC consigne ensuite les attributs d'en-tête HTTP, qui sont activés dans le profil de journal d'en-tête HTTP lié pour la journalisation, de toutes les requêtes HTTP liées au groupe LSN. L'appliance envoie ensuite les messages de journal aux serveurs de journaux configurés.

Un profil de journal d'en-tête HTTP peut être lié à plusieurs groupes LSN, mais un groupe LSN ne peut avoir qu'un seul profil de journal d'en-tête HTTP.

Pour créer un profil de journal d'en-tête HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
    DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
    ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

show lsn httphdrlogprofile
<!--NeedCopy-->
```

Pour lier un profil de journal d'en-tête HTTP à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```

Exemple

Dans l'exemple suivant d'une configuration LSN, le profil de journal d'en-tête HTTP HTTP-header-log-1 est lié au groupe LSN LSN-GROUP-1. Le profil de journal a tous les attributs HTTP (URL, méthode HTTP, version HTTP et adresse IP HOST) activés pour la journalisation afin que tous ces attributs soient

enregistrés pour toutes les requêtes HTTP des abonnés (dans le réseau 192.0.2.0/24) liés au groupe LSN.

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1
Done

set lsn parameter -memLimit 4000
Done

add lsn client LSN-CLIENT-1
Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
Done

add lsn pool LSN-POOL-1
Done

bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.4
Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1 -portblocksize 1024
Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
Done

bind lsn group  LSN-GROUP-1  -httphdrlogprofilename HTTP-HEADER-LOG-1
Done
<!--NeedCopy-->
```

Citrix ADC génère le message de journal d'en-tête HTTP suivant lorsque l'un des abonnés appartenant à l'exemple de configuration LSN envoie une requête HTTP.

Le message de journal nous indique qu'un client ayant l'adresse IP 192.0.2.33 envoie une requête HTTP à l'URL example.com en utilisant la méthode HTTP GET et HTTP version 1.1.

```
03/19/2015:16:24:04 GMT  Informational 0-PPE-1 : default LSN Message 59
     0 :  "LSN Client IP:TD 10.102.37.118:0 URL: example.com Host:
    192.0.2.33 Version: HTTP1.1 Method: GET"
<!--NeedCopy-->
```


Journalisation des informations MSISDN

Un numéro d'annuaire d'abonné intégré de station mobile (MSISDN) est un numéro de téléphone qui identifie de façon unique un abonné sur plusieurs réseaux mobiles. Le MSISDN est associé à un code de pays et à un code de destination national identifiant l'opérateur de l'abonné.

Vous pouvez configurer une appliance Citrix ADC pour inclure MSISDN dans les entrées de journal LSN pour les abonnés des réseaux mobiles. La présence de MSISDN dans les journaux LSN aide l'administrateur à retracer plus rapidement et plus précisément un abonné mobile qui a enfreint une politique ou une loi, ou dont les informations sont requises par les agences d'interception légales.

Les exemples d'entrées de journal LSN suivants incluent des informations MSISDN pour une connexion à partir d'un abonné mobile dans une configuration LSN. Les entrées de journal montrent qu'un abonné mobile dont MSISDN est E 164:5556543210 a été connecté à la destination IP: Port 23.0.0. 1:80 via le NAT IP: Port 203.0.113. 3:45195.

Type d'entrée du journal	Exemple d'entrée de journal
Création de session LSN	Oct 14 15:37:30 10.102.37.77 10/14/2015:10:08:14 GMT 0-PPE-6 : default LSN LSN_SESSION 25012 0 : SESSION CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP
Création de mappage LSN	Oct 14 15:37:30 10.102.37.77 10/14/2015:10:08:14 GMT 0-PPE-6 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP
Suppression de session LSN	Oct 14 15:40:30 10.102.37.77 10/14/2015:10:11:14 GMT 0-PPE-6 : default LSN LSN_SESSION 25012 0 : SESSION CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP

Type d'entrée du journal	Exemple d'entrée de journal
Mappage LSN	Oct 14 15:40:30 10.102.37.77 10/14/2015:10:11:14 GMT 0-PPE-6 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP

Effectuez les tâches suivantes pour inclure des informations MSISDN dans les journaux LSN

- **Créez un profil de journal LSN**. Un profil de journal LSN inclut le paramètre ID d'abonné du journal, qui spécifie s'il faut ou non inclure les informations MSISDN dans les journaux LSN d'une configuration LSN. Activez le paramètre ID d'abonné du journal lors de la création du profil de journal LSN.
- **Liez le profil de journal LSN à un groupe LSN d'une configuration LSN**. Liez le profil de journal LSN créé à un groupe LSN d'une configuration LSN en définissant le paramètre nom de profil de journal sur le nom de profil de journal LSN créé. Pour obtenir des instructions sur la configuration du NAT à grande échelle, consultez Étapes de configuration pour LSN.

Pour créer un profil de journal LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn logprofile <logprofilename -logSubscriberID ( ENABLED |
   DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Pour lier un profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```


Exemple de configuration :

Dans cet exemple de configuration LSN, le paramètre ID d'abonné du journal LSN est activé dans le profil de journal LSN. Le profil est lié au groupe LSN LSN-GROUP-9. Les informations MSISDN sont incluses dans la session LSN et les journaux de mappage LSN pour les connexions des abonnés mobiles (dans le réseau 192.0.2.0/24).

```
add lsn logprofile  LOG-PROFILE-MSISDN-9   -logSubscriberID ENABLED

Done
add lsn client LSN-CLIENT-9

Done
bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0

Done
add lsn pool LSN-POOL-9

Done
bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4

Done
add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

Done
bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done
bind lsn group  LSN-GROUP-9  -logprofilename LOG-PROFILE-MSISDN-9

Done
<!--NeedCopy-->
```

Affichage des sessions LSN actuelles

Vous pouvez afficher les sessions LSN actuelles pour détecter les sessions LSN indésirables ou inefficaces sur l'appliance Citrix ADC. Vous pouvez afficher toutes ou certaines sessions LSN sur la base des paramètres de sélection.

Remarque : lorsqu'il existe plus d'un million de sessions LSN sur l'appliance Citrix ADC, Citrix recommande d'afficher les sessions LSN sélectionnées au lieu de toutes à l'aide des paramètres de sélection.

Configuration à l'aide de l'interface de ligne de commande

Pour afficher toutes les sessions LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show lsn session
<!--NeedCopy-->
```

Pour afficher des sessions LSN sélectives à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show lsn session [-clientname <string>] [-network <ip_addr> [-netmask <
    netmask>] [-td <positive_integer>]] [-natIP <ip_addr> [-natPort <
    port>]]
<!--NeedCopy-->
```

Exemple

Pour afficher toutes les sessions LSN existantes sur un Citrix ADC

```
> show lsn session
        SubscrIP            SubscrPort      SubscrTD            DstIP                   DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.10          15136           0           198.51.100.9            80          0       203.0.113.6     6234            TCP     OUT
2.      192.0.2.11          15130           0           198.51.101.2            80          0       203.0.113.6     7887            TCP     OUT
3.      192.0.2.12          16136           0           198.51.100.3            80          0       203.0.113.6     9807            TCP     OUT
4.      192.0.2.13          18148           0           198.51.101.6            80          0       203.0.113.6     4657            TCP     OUT
5.      192.0.2.14          13560           0           198.51.101.7            80          0       203.0.113.7     9341            TCP     OUT
6.      192.0.2.15          14567           0           198.51.100.8            80          0       203.0.113.5     8214            TCP     OUT
7.      192.0.2.15          16890           0           198.51.101.1            80          0       203.0.113.5     8214            TCP     OUT
8.      192.0.2.16          12345           0           198.51.102.9            80          0       203.0.113.5     1678            TCP     OUT
9.      192.0.2.19          19876           0           198.51.103.8            80          0       203.0.113.5     1567            TCP     OUT
10.     192.0.2.20          10989           0           198.51.104.19           80          0       203.0.113.11    1343            TCP     OUT
11.     192.0.3.13          18149           0           198.51.101.61           80          0       203.0.113.11    4653            TCP     OUT
12.     192.0.3.14          13510           0           198.51.101.74           80          0       203.0.113.11    9344            TCP     OUT
13.     192.0.3.15          14565           0           198.51.100.82           80          0       203.0.113.11    8217            TCP     OUT
14.     192.0.3.15          16899           0           198.51.101.12           80          0       203.0.113.11    8219            TCP     OUT
15.     192.0.3.16          12343           0           198.51.102.99           80          0       203.0.113.11    1673            TCP     OUT

Done
```

Pour afficher toutes les sessions LSN liées à une entité client LSN LSN-CLIENT-2

```
> show lsn session -clientname LSN-CLIENT-2
        SubscrIP            SubscrPort      SubscrTD            DstIP                   DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.10          15136           0           198.51.100.9            80          0       203.0.113.6     6ß234           TCP     OUT
2.      192.0.2.11          15130           0           198.51.101.2            80          0       203.0.113.6     7887            TCP     OUT
3.      192.0.2.12          16136           0           198.51.100.3            80          0       203.0.113.6     9807            TCP     OUT
4.      192.0.2.13          18148           0           198.51.101.6            80          0       203.0.113.6     4657            TCP     OUT
5.      192.0.2.14          13560           0           198.51.101.7            80          0       203.0.113.7     9341            TCP     OUT
6.      192.0.2.15          14567           0           198.51.100.8            80          0       203.0.113.5     8214            TCP     OUT
7.      192.0.2.15          16890           0           198.51.101.1            80          0       203.0.113.5     8214            TCP     OUT
8.      192.0.2.16          12345           0           198.51.102.9            80          0       203.0.113.5     1678            TCP     OUT
9.      192.0.2.19          19876           0           198.51.103.8            80          0       203.0.113.5     1567            TCP     OUT
10.     192.0.2.20          10989           0           198.51.104.19           80          0       203.0.113.11    1343            TCP     OUT

Done
```

Pour afficher toutes les sessions LSN qui utilisent 203.0.113.5 comme adresse IP NAT


```
> show lsn session –natIP 203.0.113.5
SubscrIP               SubscrPort      SubscrTD        DstIP                 DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.15             14567           0               198.51.100.8           80              0       203.0.113.5     8214            TCP     OUT
2.      192.0.2.15             16890           0               198.51.101.1           80              0       203.0.113.5     8214            TCP     OUT
3.      192.0.2.16             12345           0               198.51.102.9           80              0       203.0.113.5     1678            TCP     OUT
4.      192.0.2.19             19876           0               198.51.103.8           80              0       203.0.113.5     1567            TCP     OUT
Done
```

Configuration à l'aide de l'utilitaire de configuration

Pour afficher toutes les sessions LSN sélectionnées ou toutes les sessions LSN à l'aide de l'utilitaire de configuration

1. Accédez à Système > NAT à grande échelle > Sessions, puis cliquez sur l'onglet NAT44.
2. Pour afficher les sessions LSN sur la base des paramètres de sélection, cliquez sur Rechercher.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- afficher la session lsn
  - clientname

    Nom de l'entité client LSN. Longueur maximale : 127
  - network

    Adresse IP ou adresse réseau du ou des abonnés.
  - netmask

    Masque de sous-réseau pour l'adresse IP spécifiée par le paramètre réseau.

    Valeur par défaut : 255.255.255.255
  - td

    ID de domaine de trafic de l'entité client LSN.

    Valeur par défaut : 0

    Valeur minimale : 0

    Valeur maximale : 4094
  - natIP

    Adresse IP NAT mappée utilisée dans les sessions LSN.

Affichage des statistiques LSN

Vous pouvez afficher des statistiques relatives à la fonction LSN pour évaluer les performances de la fonction LSN ou pour résoudre les problèmes. Vous pouvez afficher un résumé des statistiques de la

fonction LSN ou d'un groupe LSN particulier. Les compteurs statistiques reflètent les événements survenus depuis le dernier redémarrage de l'appliance Citrix ADC. Tous ces compteurs sont réinitialisés à 0 lorsque l'appliance Citrix ADC est redémarrée.

Pour afficher toutes les statistiques LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat lsn
<!--NeedCopy-->
```

Pour afficher les statistiques d'un groupe LSN spécifié à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat lsn group [<groupname>]
<!--NeedCopy-->
```

Exemple

```
> stat lsn

Large Scale NAT statistics
                                                    Rate(/s)
                                                       Total
LSN TCP Received Packets                              0
   40
LSN TCP Received Bytes                                0
   3026
LSN TCP Transmitted Packets                           0
   40
LSN TCP Transmitted Bytes                             0
   3026
LSN TCP Dropped Packets                               0
                        0
LSN TCP Current Sessions                              0
                        0
LSN UDP Received Packets                              0
                        0
LSN UDP Received Bytes                                0
                        0
```



```
13 LSN UDP Transmitted Packets                          0
                         0
14 LSN UDP Transmitted Bytes                            0
                         0
15 LSN UDP Dropped Packets                              0
                         0
16 LSN UDP Current Sessions                             0
                         0
17 LSN ICMP Received Packets                            0
    982
18 LSN ICMP Received Bytes                              0
    96236
19 LSN ICMP Transmitted Packets                         0
                         0
20 LSN ICMP Transmitted Bytes                           0
                         0
21 LSN ICMP Dropped Packets                             0
    982
22 LSN ICMP Current Sessions                            0
                         0
23 LSN Subscribers                                      0
                         1
24
25 Done
26
27 > stat lsn group LSN-GROUP-1
28
29 LSN Group Statistics
30                                                 Rate (/s)
                                                      Total
31 TCP Translated Pkts                                  0
    40
32 TCP Translated Bytes                                 0
    3026
33 TCP Dropped Pkts                                     0
                         0
34 TCP Current Sessions                                 0
                         0
35 UDP Translated Pkts                                  0
                         0
36 UDP Translated Bytes                                 0
                         0
37 UDP Dropped Pkts                                     0
                         0
38 UDP Current Sessions                                 0
```



```
                          0
39 ICMP Translated Pkts                              0
                          0
40 ICMP Translated Bytes                             0
                          0
41 ICMP Dropped Pkts                                 0
                          0
42 ICMP Current Sessions                             0
                          0
43 Current Subscribers                               0
                          1
44
45 Done
46 <!--NeedCopy-->
```

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- stat groupe lsn
  - groupname

    Nom du groupe LSN. Longueur maximale : 127
  - détail

    Spécifie la sortie détaillée (y compris plus de statistiques). La sortie peut être assez volumineuse. Sans cet argument, la sortie n'affichera qu'un résumé.
  - fullValues

    Spécifie que les nombres et les chaînes doivent être affichés dans leur forme complète. Sans cette option, les longues chaînes sont raccourcies et les grands nombres sont abrégés.
  - ntimes

    Le nombre de fois, par intervalles de sept secondes, les statistiques doivent être affichées.

    Valeur par défaut : 1
  - logFile

    Nom du fichier journal à utiliser en entrée.
  - clearstats

    Effacer les statistiques/compteurs

    Valeurs possibles : basic, full

Journalisation compacte

L'enregistrement des informations sur les LSN est l'une des fonctions importantes dont ont besoin les FSI pour satisfaire aux exigences légales et être en mesure d'identifier la source du trafic à tout moment. Cela se traduit par un volume énorme de données de journal, ce qui oblige les fournisseurs de services Internet à faire d'importants investissements pour maintenir l'infrastructure de journalisation.

La journalisation compacte est une technique permettant de réduire la taille du journal en utilisant une modification notationnelle impliquant des codes courts pour les noms d'événements et de protocoles. Par exemple, C pour le client, SC pour la session créée et T pour TCP. La journalisation compacte entraîne une réduction moyenne de 40% de la taille des journaux.

Les exemples suivants d'entrées du journal de création de mappage NAT44 montrent l'avantage de la journalisation compacte.

Default logging format	02/02/2016:01: GMT Informational 0-PPE-2 : default LSN LSN_ADDRPOR 85 0 : A&PDM CREATED Clien- tIP:Port:TD1.1.1 Destina- tionIP:Port:TD2 Protocol: TCP				
Compact logging format	02/02/2016:01:14:57 GMT Info 0-PE2:default LSN 87 0:A&PDMC	C 1.1.1.1:6500:0	N- 8.8.8.9:51066	D-2.2.2.2:80:0	T

Étapes de configuration

Effectuez les tâches suivantes pour consigner les informations LSN au format compact :

- **Créez un profil de journal LSN.** Un profil de journal LSN inclut le paramètre Log Compact, qui spécifie s'il faut ou non enregistrer les informations au format compact pour une configuration

LSN.

- **Liez le profil de journal LSN à un groupe LSN d'une configuration LSN.** Liez le profil de journal LSN créé à un groupe LSN d'une configuration LSN en définissant le paramètre Log Profile Name sur le nom de profil de journal LSN créé. Toutes les sessions et mappages de ce groupe LSN sont enregistrés au format compact.

Pour créer un profil de journal LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn logprofile <logprofilename> -logCompact (ENABLED|DISABLED)

show lsn logprofile
<!--NeedCopy-->
```

Pour lier un profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname> -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Exemple de configuration :

```
add lsn logprofile  LOG-PROFILE-COMPACT-9 -logCompact ENABLED

Done
add lsn client LSN-CLIENT-9
Done
bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0
Done
add lsn pool LSN-POOL-9
Done
bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4
Done
add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9
Done
bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9
Done
bind lsn group  LSN-GROUP-9  - logProfileName LOG-PROFILE-COMPACT-9
```



```
17 Done
18 <!--NeedCopy-->
```

Journalisation IPFIX

L'appliance Citrix ADC prend en charge l'envoi d'informations sur les événements LSN au format IPFIX (Internet Protocol Flow Information Export) vers l'ensemble configuré de collecteurs IPFIX. L'appliance utilise la fonctionnalité AppFlow existante pour envoyer des événements LSN au format IPFIX aux collecteurs IPFIX.

La journalisation basée sur IPFIX est disponible pour les événements NAT44 à grande échelle suivants :

- Création ou suppression d'une session LSN.
- Création ou suppression d'une entrée de mappage LSN.
- Allocation ou désallocation de blocs de ports dans le contexte d'un NAT déterministe.
- Allocation ou désallocation de blocs de ports dans le contexte de NAT dynamique.
- Chaque fois que le quota de session d'abonné est dépassé.

Points à considérer avant de configurer la journalisation IPFIX

Avant de commencer à configurer IPSec ALG, tenez compte des points suivants :

- Vous devez configurer la fonctionnalité AppFlow et les collecteurs IPFIX sur l'appliance Citrix ADC. Pour obtenir des instructions, voir Configuration de la rubrique de fonctionnalité AppFlow.

Étapes de configuration

Effectuez les tâches suivantes pour consigner les informations LSN au format IPFIX :

- **Activez la journalisation LSN dans la configuration AppFlow**. Activez le paramètre de journalisation LSN dans le cadre de la configuration AppFlow.
- **Créez un profil de journal LSN**. Un profil de journal LSN inclut le paramètre IPFIX qui active ou désactive les informations de journal au format IPFIX.
- **Liez le profil de journal LSN à un groupe LSN d'une configuration LSN**. Liez le profil de journal LSN à un ou plusieurs groupes LSN. Les événements liés au groupe LSN lié seront enregistrés au format IPFIX.

Pour activer la journalisation LSN dans la configuration AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set appflow param -lsnLogging ( ENABLED | DISABLED )

show appflow param
<!--NeedCopy-->
```

Pour créer un profil de journal LSN à l'aide du Cliat, l'invite de commande

À l'invite de commandes, tapez :

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Pour créer un profil de journal LSN à l'aide de l'interface graphique

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur onglet **Journal**, puis ajoutez un profil de journal.

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface graphique

1. Accédez à **Système** > **NAT à grande échelle** > **Groupe LSN,** ouvrez le groupe **LSN**.
2. Dans **Paramètres avancés,** cliquez sur **+ Profil du journal** pour lier le profil journal créé au groupe LSN.

Délai d'inactivité TCP SYN

August 20, 2021

Le délai d'inactivité SYN est le délai d'expiration pour établir des connexions TCP qui utilisent LSN sur l'appliance Citrix ADC. Si une session TCP n'est pas établie dans le délai d'expiration configuré, Citrix ADC supprime la session. Le délai d'inactivité SYN est utile pour fournir une protection contre les attaques d'inondation SYN. Dans une configuration LSN, l'entité de groupe LSN inclut le paramètre de délai d'inactivité SYN.

Exemple :

Dans l'exemple de configuration LSN suivant, le délai d'inactivité SYN est défini sur 30 secondes pour les connexions TCP liées aux abonnés du réseau 192.0.2.0/24.

```
1  add lsn client LSN-CLIENT-1
2
3  Done
4
5  bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-1
10
11 Done
12
13 bind lsn pool LSN-POOL-1 203.0.113.3
14
15 Done
16
17 add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  - synidletimeout 30
18
19 Done
20
21 bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
22
23 Done
24 <!--NeedCopy-->
```

Remplacer la configuration LSN avec la configuration d'équilibrage de charge

January 21, 2021

Par défaut, une configuration LSN a priorité sur toute configuration d'équilibrage de charge. Pour

remplacer la configuration de réseau à grande échelle (LSN) par la configuration d'équilibrage de charge pour le trafic correspondant aux deux configurations, créez un profil net avec le paramètre Override LSN activé et liez ce profil au serveur virtuel de la configuration d'équilibrage de charge. Les paramètres USNIP ou USIP de la configuration d'équilibrage de charge sont appliqués au trafic, au lieu d'appliquer l'adresse IP LSN de la configuration LSN.

Cette option est utile dans un déploiement LSN qui inclut des appliances Citrix ADC et des services à valeur ajoutée, tels que des dispositifs de pare-feu et d'optimisation. Dans ce type de déploiement, le trafic entrant sur l'appliance Citrix ADC est requis pour passer par ces services à valeur ajoutée avant qu'une configuration LSN sur l'appliance ne soit appliquée au trafic. Pour que l'appliance Citrix ADC envoie le trafic entrant à un service à valeur ajoutée, une configuration d'équilibrage de charge est créée et le remplacement du LSN est activé sur l'appliance. La configuration d'équilibrage de charge inclut des services à valeur ajoutée, représentés en tant que services d'équilibrage de charge, liés à un serveur virtuel de type Y. Le serveur virtuel est configuré avec des stratégies d'écoute pour identifier le trafic à envoyer au service à valeur ajoutée.

Pour activer le remplacement lsn dans un profil net à l'aide de l'interface de ligne de commande

Pour activer override lsn lors de l'ajout d'un profil net, à l'invite de commandes, tapez

```
add netProfile <name> -overrideLsn ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Pour activer override lsn lors de l'ajout d'un profil net, à l'invite de commandes, tapez

```
set netProfile <name> -overrideLsn ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Pour activer le remplacement lsn dans un profil net à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **Profils réseau**.
2. Définissez le paramètre **Override LSN** lors de l'ajout ou de la modification de profils réseau.

Dans l'exemple de configuration suivant, le profil net NETPROFILE-OVERRIDELSN-1 a écrasé l'option LSN activée et est lié à l'équilibrage de charge du serveur virtuel LBVS-1.

Exemple de configuration :


```
add netprofile NETPROFILE-OVERRIDELSN-1 -overrideLsn ENABLED

Done

set lb vserver LBVS-1 -netprofile NETPROFILE-OVERRIDELSN-1

Done
<!--NeedCopy-->
```

Suppression des sessions LSN

August 20, 2021

Vous pouvez supprimer toutes les sessions LSN indésirables ou inefficaces de l'appliance Citrix ADC. L'appliance libère immédiatement les ressources (telles que l'adresse IP NAT, le port et la mémoire) allouées à ces sessions, ce qui rend les ressources disponibles pour les nouvelles sessions. L'appliance supprime également tous les paquets suivants liés à ces sessions supprimées. Vous pouvez supprimer toutes les sessions LSN ou sélectionnées de l'appliance Citrix ADC.

Pour effacer toutes les sessions LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
flush lsn session

show lsn session
<!--NeedCopy-->
```

Pour effacer les sessions LSN sélectives à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
flush lsn session [-clientname <string>] [-network <ip_addr> [-netmask
    <netmask>] [-td <positive_integer>]] [-natIP <ip_addr> [-natPort <
    port>]]

show lsn session
<!--NeedCopy-->
```


Exemple

Effacer toutes les sessions LSN existantes sur un Citrix ADC

```
1 flush lsn session
2
3 Done
4 <!--NeedCopy-->
```

Effacer toutes les sessions LSN liées à l'entité client LSN-CLIENT-1

```
1 flush lsn session -clientname LSN-CLIENT-1
2
3 Done
4 <!--NeedCopy-->
```

Effacer toutes les sessions LSN liées à un réseau d'abonnés (192.0.2.0) de l'entité client LSN LSN-CLIENT-2 appartenant au domaine de trafic 100

```
1 flush lsn session -clientname LSN-CLIENT-2 -network 192.0.2.0 -
     netmask 255.255.255.0 -td 100
2
3 Done
4 <!--NeedCopy-->
```

Pour effacer toutes les sessions LSN à l'aide de l'utilitaire de configuration

Accédez à Système > NAT à grande échelle > Sessions, puis cliquez sur Vider les sessions.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- vider la session lsn
  - clientname

    Nom de l'entité client LSN. Longueur maximale : 127
  - network

    Adresse IP ou adresse réseau du ou des abonnés.
  - netmask

    Masque de sous-réseau pour l'adresse IP spécifiée par le paramètre réseau.

    Valeur par défaut : 255.255.255.255

- td

  ID de domaine de trafic de l'entité client LSN.

  Valeur par défaut : 0

  Valeur minimale : 0

  Valeur maximale : 4094

- natIP

  Adresse IP NAT mappée utilisée dans les sessions LSN.

- natPort

  Port NAT mappé utilisé dans les sessions LSN.

Serveurs SYSLOG d'équilibrage de charge

August 20, 2021

L'appliance Citrix ADC envoie ses événements et messages SYSLOG à tous les serveurs de journaux externes configurés. Cela entraîne le stockage des messages redondants et rend la surveillance difficile pour les administrateurs système. Pour résoudre ce problème, l'appliance Citrix ADC propose des algorithmes d'équilibrage de charge qui peuvent équilibrer la charge des messages SYSLOG parmi les serveurs de journaux externes pour une meilleure maintenance et des performances. Les algorithmes d'équilibrage de charge pris en charge incluent RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets et AuditlogHash.

Équilibrage de charge des serveurs SYSLOG à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

```
1 add service <name>(<IP> | <serverName>) <serviceType (SYSLOGTCP |
     SYSLOGUDP)> <port>
2 <!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGTCP, et la méthode d'équilibrage de charge AUDITLOGHASH.

```
1 add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
     <AUDITLOGHASH>]
2 <!--NeedCopy-->
```

Liez le service au serveur virtuel d'équilibrage de charge.


```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

1. Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge qui a SYSLOGTCP ou SYSLOGUDP comme type de service.

```
add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
    <logLevel>]
<!--NeedCopy-->
```

Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

```
add syslogpolicy <name> <rule> <action>
<!--NeedCopy-->
```

Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.

```
bind system global <policyName>
<!--NeedCopy-->
```

Équilibrage de charge des serveurs SYSLOG à l'aide de l'utilitaire de configuration

1. Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

   Accédez à Gestion du trafic > Services, cliquez sur Ajouter et sélectionnez SYLOGTCP ou SYSLOGUDP comme protocole.

2. Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGTCP, et la méthode d'équilibrage de charge AUDITLOGHASH.

   Accédez à Gestion du trafic > Serveurs virtuels, cliquez sur Ajouter et sélectionnez SYLOGTCP ou SYSLOGUDP comme protocole.

3. Liez le service au serveur virtuel d'équilibrage de charge au service.

   Liez le service au serveur virtuel d'équilibrage de charge.

   Accédez à Gestion du trafic > Serveurs virtuels, sélectionnez un serveur virtuel, puis sélectionnez AUDITLOGHASH dans la méthode d'équilibrage de la charge.

4. Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge qui a SYSLOGTCP ou SYSLOGUDP comme type de service.

   Accédez à Système > Audit, cliquez sur Serveurs et ajoutez un serveur en sélectionnant LB Vserver option Inservers.

5. Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

   Accédez à Système > Syslog, cliquez sur Stratégies et ajoutez une stratégie SYSLOG.

6. Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.

   Accédez à Système > Syslog, sélectionnez une stratégie SYSLOG et cliquez sur Action, puis cliquez sur Liaisons globales et liez la stratégie à système global.

Exemple :

La configuration suivante spécifie l'équilibre de charge des messages SYSLOG entre les serveurs de journaux externes en utilisant la méthode AUDITLOGHASH comme méthode d'équilibrage de charge. L'appliance Citrix ADC génère des événements et des messages SYSLOG équilibrés entre les services, service1, service2 et service 3.

```
add service service1 192.0.2.10 SYSLOGUDP 514

add service service2 192.0.2.11 SYSLOGUDP 514

add service service3 192.0.2.11 SYSLOGUDP 514

add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH

bind lb vserver lbvserver1 service1

bind lb vserver lbvserver1 service2

bind lb vserver lbvserver1 service3

add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All

add syslogpolicy syspol1 ns_true sysaction1

bind system global syspol1
<!--NeedCopy-->
```

Limitations :

L'appliance Citrix ADC ne prend pas en charge un serveur virtuel d'équilibrage de charge externe équilibrant la charge du serveur virtuel équilibrant les messages SYSLOG entre les serveurs de journaux.

Protocole de contrôle de port

January 21, 2021

Les appliances Citrix ADC prennent désormais en charge le protocole PCP (Port Control Protocol) pour NAT à grande échelle (LSN). Bon nombre des applications abonnées d'un fournisseur de services Internet doivent être accessibles à partir d'Internet (par exemple, des appareils Internet des objets (IOT), comme une caméra IP qui assure la surveillance sur Internet). Une façon de répondre à cette exigence est de créer des mappings NAT (LSN) statiques à grande échelle. Mais pour un très grand nombre d'abonnés, la création de mappings NAT LSN statiques n'est pas une solution réalisable.

Port Control Protocol (PCP) permet à un abonné de demander des mappages NAT LSN spécifiques pour lui-même et/ou pour d'autres périphériques tiers. Le périphérique NAT à grande échelle crée un mapping LSN et l'envoie à l'abonné. L'abonné envoie aux périphériques distants sur Internet l'adresse IP NAT : port NAT auquel ils peuvent se connecter à l'abonné.

Les applications envoient généralement des messages keep-alive fréquents au périphérique NAT à grande échelle afin que leurs mappages LSN ne s'écoule pas. PCP aide à réduire la fréquence de ces messages Keep-alive en permettant aux applications d'apprendre les paramètres de délai d'expiration des mappages LSN. Cela permet de réduire la consommation de bande passante sur le réseau d'accès du FAI et la consommation de batterie sur les appareils mobiles.

PCP est un modèle client-serveur qui fonctionne sur le protocole de transport UDP. Une appliance Citrix ADC implémente le composant serveur PCP et est conforme à la RFC 6887.

Étapes de configuration

Effectuez les tâches suivantes pour configurer PCP :

- (Facultatif) Créez un profil PCP. Un profil PCP inclut des paramètres pour les paramètres associés à PCP (par exemple, pour écouter les requêtes de mappage et PCP homologue). Un profil PCP peut être lié à un serveur PCP. Un profil PCP lié à un serveur PCP applique tous ses paramètres au serveur PCP. Un profil PCP peut être lié à plusieurs serveurs PCP. Par défaut, un profil PCP avec les paramètres par défaut est lié à tous les serveurs PCP. Un profil PCP que vous liez à un serveur PCP remplace les paramètres de profil PCP par défaut pour ce serveur. Un profil PCP par défaut possède les paramètres suivants :
  - Mappage : activé
  - Peer : activé
  - Durée de vie minimale du mapping : 120 secondes
  - Durée de vie maximale : 86400 secondes
  - Nombre d'annonces : 10
  - Tiers : désactivé
- Créez un serveur PCP et liez un profil PCP à celui-ci. Créez un serveur PCP sur l'appliance Citrix ADC pour écouter les requêtes PCP et les messages des abonnés. Une adresse IP de sous-réseau (SNIP) doit être attribuée à un serveur PCP pour y accéder. Par défaut, un serveur PCP écoute sur le port 5351.

- Liez le serveur PCP à un groupe LSN d'une configuration LSN. Liez le serveur PCP créé à un groupe LSN d'une configuration LSN en définissant le paramètre Serveur PCP pour spécifier le serveur PCP créé. Le serveur PCP créé est accessible uniquement par les abonnés de ce groupe LSN.

> **Remarque**
>
> Un serveur PCP pour une configuration NAT à grande échelle ne répond pas aux demandes des abonnés identifiés à partir des règles ACL.

Pour créer un profil PCP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

Pour créer un serveur PCP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Exemple de configuration pour NAT44

Dans l'exemple de configuration suivant, le serveur PCP PCP-SERVER-9, avec les paramètres PCP par défaut, est lié au groupe LSN LSN-GROUP-9. PCP-SERVER-9 sert les demandes PCP des abonnés dans le réseau 192.0.2.0/24.

Exemple de configuration :

```
add pcp server PCP-SERVER-9 192.0.3.9

Done

```



```
add lsn client LSN-CLIENT-9

Done

bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-9

Done

bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4

Done

add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

Done

bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done

bind lsn group  LSN-GROUP-9  -pcpServer PCP-SERVER-9

Done
<!--NeedCopy-->
```

LSN44 dans une configuration de cluster

January 21, 2021

Les configurations NAT44 à grande échelle sont prises en charge sur une configuration de cluster Citrix ADC.

Un cluster CITRIX ADC est un groupe d'appliances Citrix ADC configurées et gérées en tant que système unique. Un cluster Citrix ADC offre évolutivité et disponibilité. Chaque appliance Citrix ADC dans une configuration de cluster agit comme une entité LSN indépendante et est gérée comme un système unique.

La configuration LSN dans une configuration de cluster est identique à celle d'une appliance autonome, sauf qu'un pool spécifique d'adresses IP LSN appartient à un seul nœud à la fois. En d'autres

termes, une entité de pool IP LSN est configurée en tant qu'entité spotted dans un nœud particulier. Tous les nœuds d'une configuration de cluster peuvent avoir une entité de pool IP LSN spécifique. Pour vous assurer que les paquets liés à une session LSN sont reçus sur le même nœud de cluster qui a effectué l'opération NAT, la direction du backplane basé sur la stratégie (PBS) est configurée. PBS dirige les paquets associés reçus d'une session LSN vers le même nœud de cluster.

Exemple de configuration :

```
1  add lsn client LSN-CLIENT-1
2
3  Done
4
5  bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-1
10
11 Done
12
13 bind lsn pool LSN-POOL-1 -ownerNode 1 203.0.113.3
14
15 Done
16
17 bind lsn pool LSN-POOL-1 -ownerNode 2 203.0.113.3
18
19 Done
20
21 add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1
22
23 Done
24
25 bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
26
27 Done
28
29 add ns acl b1 ALLOW -srcIP = 192.0.2.0-192.0.2.255 -type DFD -dfdhash
      SIP
30
31
32 Done
33
34 apply ns acls -type DFD
35
36 Done
```



```
37 <!--NeedCopy-->
```

Dual-Stack Lite

January 21, 2021

En raison de la pénurie d'adresses IPv4 et des avantages d'IPv6 par rapport à IPv4, de nombreux fournisseurs de services Internet ont commencé à passer à l'infrastructure IPv6. Mais pendant la transition, les FSI doivent continuer à prendre en charge IPv4 avec IPv6, car la plupart de l'Internet public utilise toujours uniquement IPv4, et de nombreux abonnés ne prennent pas en charge IPv6.

Dual Stack Lite (DS-Lite) est une solution de transition IPv6 pour les FAI disposant d'une infrastructure IPv6 pour connecter leurs abonnés IPv4 à Internet. DS-Lite utilise le tunnel IPv4-in-IPv6 pour envoyer au FAI le paquet IPv4 d'un abonné via un tunnel sur le réseau d'accès IPv6. Le paquet IPv6 est décapsulé pour récupérer le paquet IPv4 de l'abonné et est ensuite envoyé à Internet après la traduction d'adresse et de port NAT et d'autres traitements liés au LSN. Les paquets de réponse traversent le même chemin d'accès à l'abonné.

L'appliance Citrix ADC implémente le composant AFTR d'un déploiement DS-Lite et est conforme à la RFC 6333.

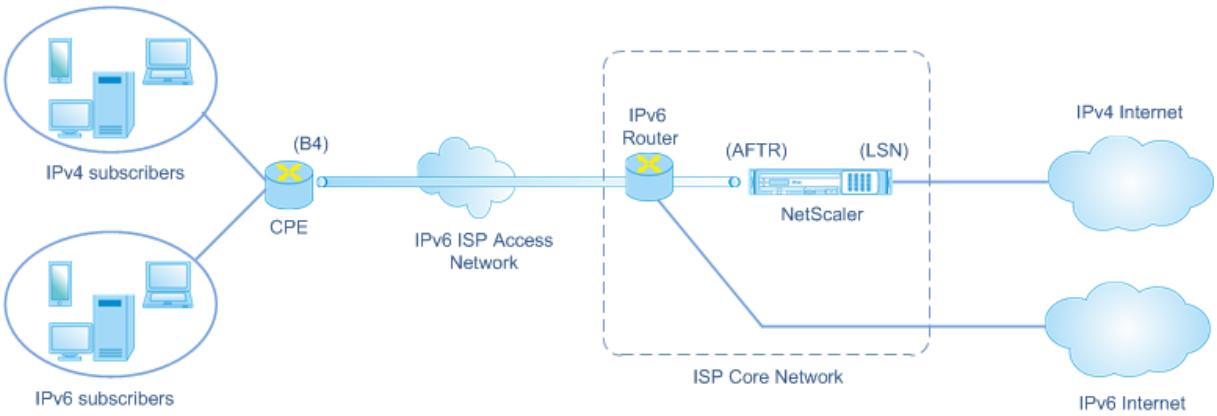
Architecture

L'architecture Dual-Stack Lite pour un fournisseur de services Internet comprend les composants suivants :

- **Basic Bridging Large (B4).** B4 (Basic Bridging Broadband) est un périphérique ou un composant qui réside dans les locaux de l'abonné. Généralement, B4 est un composant dans les périphériques CPE dans les locaux de l'abonné. Les abonnés IPv4 sont connectés au réseau d'accès ISP uniquement IPv6 via le périphérique CPE contenant le composant B4. La fonction principale du B4 est d'initier un tunnel IPv6 entre B4 et un routeur de transition de famille d'adresses (AFTR) afin d'envoyer ou de recevoir des paquets de requête IPv4 d'abonné ou de réponse via le tunnel. B4 inclut une adresse IPv6 connue sous le nom d'adresse du point de terminaison du tunnel B4. B4 utilise cette adresse pour envoyer des paquets IPv6 à AFTR et recevoir des paquets d'AFTR.
- **Routeur de transition de famille d'adresses (AFTR).** AFTR est un dispositif ou un composant résidant dans le réseau central du FSI. AFTR met fin au tunnel IPv6 à partir du périphérique B4. En d'autres termes, le tunnel IPv6 est formé entre B4 dans le local de l'abonné et AFTR dans le réseau central du fournisseur de services Internet. AFTR décapsule les paquets IPv6 reçus de B4 pour récupérer les paquets IPv4 d'origine des abonnés. AFTR envoie les paquets IPv4 au

périphérique ou au composant LSN. LSN achemine les paquets IPv4 vers leur destination après avoir effectué la traduction d'adresse et de port NAT (NAT 44) et d'autres traitements liés au LSN. AFTR inclut une adresse IPv6 connue sous le nom d'adresse du point de terminaison du tunnel AFTR. AFTR utilise cette adresse pour envoyer des paquets IPv6 vers B4 et recevoir des paquets IPv6 de B4. L'appliance Citrix ADC implémente le composant AFTR.

- **Logiciel.** Le tunnel IPv6 créé entre B4 et AFTR est appelé un logiciel.



L'architecture DS-Lite d'un fournisseur de services Internet utilisant une appliance Citrix ADC se compose d'abonnés dans des espaces d'adressage privés accédant à Internet via une appliance Citrix ADC déployée dans le réseau central du fournisseur de services Internet. Les abonnés IPv4 sont connectés à un périphérique CPE qui inclut la fonctionnalité DS-Lite B4. Le périphérique CPE est connecté au réseau central du fournisseur de services Internet via le réseau d'accès IPv6 uniquement du fournisseur de services Internet. L'appliance Citrix ADC contient les fonctionnalités DS-Lite AFTR et LSN.

Les abonnés IPv4 connectés au périphérique CPE se voient attribuer des adresses IPv4 privées manuellement ou via un serveur DHCP s'exécutant sur le périphérique CPE. Sur le périphérique CPE, l'adresse du point de terminaison du tunnel AFTR est spécifiée manuellement ou via DHCPv6. La configuration des périphériques CPE est spécifique au fournisseur et ne relève donc pas de la présente documentation.

À la réception d'un paquet de requête provenant d'un abonné IPv4 et destiné à un emplacement sur Internet, le composant B4 du périphérique CPE encapsule le paquet IPv4 dans un paquet IPv6 et l'envoie à l'appliance Citrix ADC dans le réseau central du fournisseur de services Internet. La fonctionnalité AFTR de l'appliance Citrix ADC décapsule le paquet IPv6 pour récupérer le paquet IPv4 d'origine de l'abonné. La fonctionnalité LSN de l'appliance Citrix ADC traduit l'adresse IP source et le port du paquet IPv4 en une adresse IP NAT et un port NAT sélectionnés dans le pool NAT configuré, puis envoie le paquet à sa destination sur Internet.

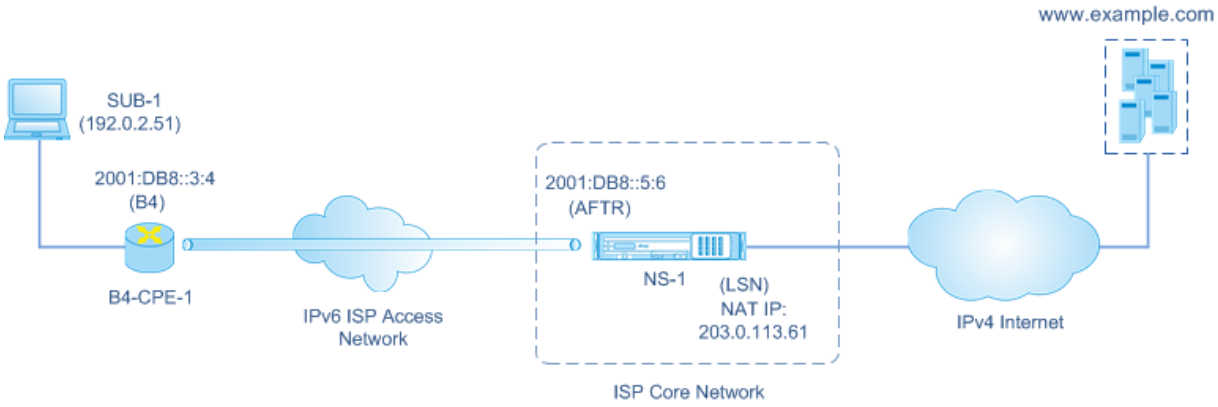
L'appliance conserve un enregistrement de toutes les sessions actives qui utilisent les fonctionnalités AFTR et LSN. Ces sessions sont appelées sessions DS-Lite. L'appliance Citrix ADC gère également les mappages entre l'adresse IPv6 B4, l'adresse et le port IPv4 de l'abonné, et l'adresse et le port NAT IPv4, pour chaque session DS-Lite. Ces mappages sont appelés mappings LSN DS-Lite. À partir des entrées

de session DS-Lite et des entrées de mappage DS-Lite LSN, l'appliance Citrix ADC reconnaît un paquet de réponse (reçu d'Internet) comme appartenant à une session DS-Lite particulière.

Lorsque l'appliance Citrix ADC reçoit un paquet de réponse appartenant à une session DS-Lite particulière, la fonctionnalité LSN de l'appliance traduit l'adresse IP de destination et le port du paquet de réponse de l'adresse IP et du port NAT vers l'adresse IP et le port de l'abonné, la fonctionnalité AFTR encapsule le dans un paquet IPv6 et l'envoie au périphérique CPE. La fonctionnalité B4 du périphérique CPE décapsule le paquet IPv6 pour récupérer le paquet de réponse IPv4, puis envoie le paquet IPv4 à l'abonné.

Exemple

Prenons un exemple de déploiement DS-Lite composé de Citrix ADC NS-1 dans le réseau central d'un fournisseur de services Internet, d'un périphérique CPE B4-CPE-1 dans un local d'abonné et d'un seul abonné IPv4 SUB-1. B4-CPE-1 prend en charge la fonctionnalité B4 de la fonction DS-Lite.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Entité	Nom	Détails
Adresse IPv4 de l'abonné SUB-1		192.0.2.51
Adresse IPv6 du point de terminaison logiciel sur le périphérique B4 (B4-CPE-1)		2001:DB8::3:4
Adresse IPv6 du point de terminaison logiciel sur le périphérique AFTR (NS-1)		2001:DB8::5:6

Paramètres de l'appliance Citrix ADC NS-1 :

Entité	Nom	Détails
Client LSN	LSN-DSLITE-CLIENT-1	Network6 (Identification du trafic à partir de périphériques B4) = 2001:DB8::3:0/100
Piscine LSN	LSN-DSLITE-POOL-1	IP LSN (IP NAT) = 203.0.113.61 - 203.0.113.70
Profil IPv6	LSN-DSLITE-PROFILE-1	Type = DS-LITE ; adresse IPv6 (adresse IPv6 AFTR) = une adresse IPv6 appartenant à Citrix ADC de type SNIP6 = 2001:DB8::5:6
Groupe LSN	LSN-DSLITE-GROUP-1	Client LSN = LSN-DSLITE-CLIENT-1 ; pool LSN = LSN-DSLITE-POOL-1 ; profil IPv6 = LSN-DSLITE-PROFILE-1

Voici le flux de trafic dans cet exemple :

1. L'abonné IPv4 SUB-1 envoie une requête à (`http://www.example.com/`). Le paquet IPv4 a :
   - Adresse IP source = 192.0.2.51
   - Port source = 2552
   - Adresse IP de destination = 198.51.100.250
   - Port de destination = 80
2. À la réception du paquet de requête IPv4, B4-CPE-1 l'encapsule dans la charge utile d'un paquet IPv6, puis envoie le paquet IPv6 à NS-1. Le paquet IPv6 a :
   - Adresse IP source = 2001:DB8::3:4
   - Adresse IP de destination = 2001:DB8::5:6
3. Lorsque NS-1 reçoit le paquet IPv6, le module AFTR décapsule le paquet en supprimant les en-têtes IPv6. Le paquet résultant est le paquet de requête IPv4 d'origine de SUB-1.
4. Le module LSN de NS-1 traduit l'adresse IP source et le port du paquet en une adresse IP NAT et un port NAT sélectionnés dans le pool NAT configuré. Le paquet IPv4 traduit a :
   - Adresse IP source = 203.0.113.61
   - Port source = 3002
   - Adresse IP de destination = 198.51.100.250

- Port de destination = 80

5. Le module LSN crée également un mappage LSN et une entrée de session pour cette session DS Lite. Le mappage comprend les informations suivantes :
   - Adresse IP source du paquet IPv6 (adresse IPv6 de B4-CPE-1) = 2001:DB8::3:4
   - Adresse IP source du paquet IPv4 (adresse IPv4 de SUB-1) = 192.0.2.51
   - Port source du paquet IPv4 = 2552
   - Adresse IP NAT = 203.0.113.61
   - Port NAT = 3002
6. NS-1 envoie le paquet IPv4 obtenu à sa destination sur Internet.
7. Le serveur de www.example.com traite le paquet de requête et envoie un paquet de réponse. Le paquet de réponse IPv4 a :
   - Adresse IP source = 198.51.100.250
   - Port source = 80
   - Adresse IP de destination = 203.0.113.61
   - Port de destination = 3002
8. Lors de la réception du paquet IPv4, NS-1 examine le mappage LSN et les entrées de session et constate que le paquet de réponse IPv4 appartient à une session DS Lite. Le module LSN de NS-1 traduit l'adresse IP de destination et le port. Le paquet IPv4 a maintenant :
   - Adresse IP source = 198.51.100.250
   - Port source = 80
   - Adresse IP de destination = 192.0.2.51
   - Port de destination = 2552
9. Le module AFTR de NS-1 encapsule le paquet IPv4 dans un paquet IPv6, puis envoie le paquet IPv6 à B4-CPE-1. Le paquet IPv6 a :
   - Adresse IP source = 2001:DB8::5:6
   - Adresse IP de destination = 2001:DB8::3:4
10. À la réception du paquet, B4-CPE-1 supprime l'encapsulation du paquet IPv6 en supprimant les en-têtes IPv6, puis envoie le paquet IPv4 obtenu au CL-1.

Points à considérer avant de configurer DS-Lite

August 20, 2021

Tenez compte des points suivants avant de configurer DS-Lite sur un appliance Citrix ADC :

1. Vous devez comprendre les différents composants de DS-Lite, décrits dans la RFC 6333.

2. Une configuration DS-Lite sur une appliance Citrix ADC utilise les jeux de commandes LSN. Dans une configuration DS-Lite, l'entité client LSN spécifie l'adresse IPv6 ou l'adresse réseau IPv6 ou les règles ACL6 pour identifier le trafic à partir du périphérique B4. Une configuration DS-Lite inclut également un profil IPv6, qui spécifie le composant AFTR d'adresse IPv6 sur une appliance Citrix ADC. Pour plus d'informations sur la fonctionnalité LSN Citrix ADC, consultez NAT à grande échelle.
3. Pour une configuration DS-Lite, l'appliance Citrix ADC prend en charge LSN pour les paquets IPv4 appartenant à l'un des protocoles suivants uniquement. L'appliance Citrix ADC supprime les paquets IPv4 appartenant à d'autres protocoles :
    - TCP
    - UDP
    - ICMP
4. L'appliance Citrix ADC prend en charge les ALG DS-Lite suivantes :
    - ICMP
    - FTP
    - TFTP
    - Protocole d'initiation de session (SIP)
    - Protocole de streaming en temps réel (RTSP)

Configuration de DS-Lite

August 20, 2021

Une configuration DS-Lite sur une appliance Citrix ADC utilise les jeux de commandes LSN. Dans une configuration DS-Lite, l'entité client LSN spécifie l'adresse IPv6 ou l'adresse réseau IPv6 ou les règles ACL6 pour identifier le trafic à partir du périphérique B4. Pour plus d'informations sur la fonctionnalité Citrix ADC LSN, consultez NAT à grande échelle. Une configuration DS-Lite inclut également un profil IPv6, qui spécifie l'adresse IPv6 (de type SNIP6) du composant DS-Lite AFTR sur une appliance Citrix ADC.

La configuration de DS-Lite sur une appliance Citrix ADC comporte les tâches suivantes :

- **Définissez les paramètres LSN globaux**. Les paramètres globaux incluent la quantité de mémoire Citrix ADC réservée à la fonctionnalité LSN et la synchronisation des sessions LSN dans une configuration haute disponibilité.
- **Créez une entité client LSN pour identifier le trafic à partir de périphériques B4 CPE**. L'entité client LSN fait référence à un ensemble de périphériques DS-Lite B4. L'entité client inclut des adresses IPv6 ou des adresses réseau IPv6 ou des règles ACL6 pour identifier le trafic

provenant de ces périphériques B4. Un client LSN peut être lié à un seul groupe LSN. L'interface de ligne de commande comporte deux commandes pour créer une entité client LSN et lier un abonné à l'entité client LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.

- **Créez un pool LSN et liez des adresses IP NAT à celui-ci**. Un pool LSN définit un pool d'adresses IP NAT à utiliser par l'appliance Citrix ADC pour exécuter LSN. L'interface de ligne de commande comporte deux commandes permettant de créer un pool LSN et de lier les adresses IP NAT au pool LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.
- **Créez un profil LSN IP6.** Un profil LSN IP6 définit l'adresse IPv6 du composant AFTR DS-Lite sur l'appliance Citrix ADC. L'adresse IPv6 doit être l'une des adresses IPv6 appartenant à Citrix ADC de type SNIP6.
- **(Facultatif) Créez un profil de transport LSN pour un protocole spécifié**. Un profil de transport LSN définit divers délais d'expiration et limites, tels que les sessions LSN maximales et l'utilisation maximale des ports qu'un abonné peut avoir pour un protocole donné. Vous liez un profil de transport LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil de transport LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP est lié à un groupe LSN lors de sa création. Ce profil est appelé profil de transport par défaut. Un profil de transport LSN que vous liez à un groupe LSN remplace le profil de transport LSN par défaut pour ce protocole.
- **(Facultatif) Créez un profil d'application LSN pour un protocole spécifié et liez un ensemble de ports de destination à celui-ci**. Un profil d'application LSN définit les contrôles de mappage LSN et de filtrage LSN d'un groupe pour un protocole donné et pour un ensemble de ports de destination. Pour un ensemble de ports de destination, vous liez un profil LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil d'application LSN lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil d'application LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP pour tous les ports de destination est lié à un groupe LSN lors de sa création. Ce profil est appelé profil d'application par défaut. Lorsque vous liez un profil d'application LSN, avec un ensemble de ports de destination spécifié, à un groupe LSN, le profil lié remplace le profil d'application LSN par défaut pour ce protocole sur cet ensemble de ports de destination. L'interface de ligne de commande comporte deux commandes pour créer un profil d'application LSN et lier un ensemble de ports de destination au profil d'application LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.
- **Créez un groupe LSN et liez des pools LSN, un profil IPv6 LSN, des profils de transport LSN (facultatif) et (facultatif) des profils d'application LSN au groupe LSN**. Un groupe LSN est une entité composée d'un client LSN, d'un profil IPv6 LSN, de pools LSN, de profils de transport LSN et de profils d'application LSN. Des paramètres sont attribués à un groupe, tels que la taille

du bloc de port et la journalisation des sessions LSN. Les paramètres s'appliquent à tous les abonnés d'un client LSN lié au groupe LSN. Un seul profil LSN IPv6 peut être lié à un groupe LSN, et un profil LSN IPv6 lié à un groupe LSN ne peut pas être lié à d'autres groupes LSN. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés ensemble. Plusieurs pools LSN peuvent être liés à un groupe LSN. Une seule entité client LSN peut être liée à un groupe LSN, et une entité client LSN liée à un groupe LSN ne peut pas être liée à d'autres groupes LSN. L'interface de ligne de commande comporte deux commandes pour créer un groupe LSN et lier des pools LSN, des profils de transport LSN et des profils d'application LSN au groupe LSN. L'utilitaire de configuration combine ces deux opérations dans un seul écran.

Configuration à l'aide de la ligne de commande

Pour créer un client LSN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
add lsn client <clientname>

show lsn client
<!--NeedCopy-->
```

Pour lier un réseau IPv6 ou une règle ACL6 à un client LSN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
bind lsn client <clientname> (-network6 <ipv6_addr|*>| -acl6name <
   string>)

show lsn client
<!--NeedCopy-->
```

Pour créer un pool LSN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
add lsn pool <poolname> [-nattype ( DYNAMIC )] [-portblockallocation (
   ENABLED | DISABLED )] [-portrealloctimeout <secs>] [-
   maxPortReallocTmq <positive_integer>]

show lsn pool
<!--NeedCopy-->
```

Pour lier une plage d'adresses IP à un pool LSN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :


```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

Remarque : Pour supprimer des adresses IP LSN d'un pool LSN, utilisez la commande unbind lsn pool.

Pour configurer un profil LSN IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
add lsn ip6profile <name>  -type DS-Lite  -network6 < ipv6_addr|*s >

show lsn ip6profile
<!--NeedCopy-->
```

Pour créer un profil de transport LSN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```

Pour créer un profil d'application LSN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )] [-td <positive_integer>]

show lsn appsprofile
<!--NeedCopy-->
```

Pour lier une plage de ports de protocole d'application à un profil d'application LSN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :


```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

Pour créer un groupe LSN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC )]
    [-portblocksize <positive_integer>] [-logging (ENABLED | DISABLED )]
     [-sessionLogging ( ENABLED | DISABLED )][-sessionSync ( ENABLED |
    DISABLED )] [-snmptraplimit<positive_integer>] [-ftp ( ENABLED |
    DISABLED )] [-pptp ( ENABLED |DISABLED )] [-sipalg ( ENABLED |
    DISABLED )] [-rtspalg ( ENABLED |DISABLED )] [-ip6profile <string>]

show lsn group
<!--NeedCopy-->
```

Pour lier des profils de protocole LSN et des pools LSN à un groupe LSN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -httphdrlogprofilename <string> | -appsprofilename <
    string> | -sipalgprofilename <string> | rtspalgprofilename <string>)

show lsn group
<!--NeedCopy-->
```

Configuration à l'aide de l'utilitaire de configuration

Pour configurer un client LSN et lier une adresse réseau IPv6 ou une règle ACL6 à l'aide de l'utilitaire de configuration :

Accédez à **Système** > **NAT à grande échelle** > **Clients**, puis ajoutez un client, puis liez une adresse réseau IPv6 ou une règle ACL6 au client.

Pour configurer un pool LSN et lier des adresses IP NAT à l'aide de l'utilitaire de configuration :

Accédez à **Système** > **NAT à grande échelle** > **Pools**, puis ajoutez un pool, puis liez une adresse IP NAT ou une plage d'adresses IP NAT au pool.

Pour configurer un profil LSN IPv6 à l'aide de l'utilitaire de configuration :

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur l'onglet **IPv6** et attribuez une adresse IPv6 à DS-lite AFTR.

Pour configurer un profil de transport LSN à l'aide de l'utilitaire de configuration :

1. Accédez à **Système** > **NAT à grande échelle** > **Profils**.
2. Dans le volet d'informations, cliquez sur **Transport**, puis ajoutez un profil de transport.

Pour configurer un profil d'application LSN à l'aide de l'utilitaire de configuration :

1. Accédez à **Système** > **NAT à grande échelle** > **Profils**.
2. Dans le volet d'informations, cliquez sur **Application**, puis ajoutez un profil d'application.

Pour configurer un groupe LSN et lier un client LSN, un profil IPv6 LSN, des pools, des profils de transport et des profils d'application à l'aide de l'utilitaire de configuration :

Accédez à **Système** > **NAT à grande échelle** > **Groupes**, puis ajoutez un groupe, puis liez un client LSN, un profil IPv6 LSN, des pools, des profils de transport et des profils d'application au groupe.

```
> add lsn client LSN-DSLITE-CLIENT-1
Done
> bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100
Done
> add lsn pool LSN-DSLITE-POOL-1
Done
> bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
Done
> add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
   DB8::5:6
Done
> add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1
Done
> add lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
Done
```

Journalisation et surveillance de DS-Lite

Vous pouvez consigner les informations DS-Lite pour diagnostiquer ou résoudre les problèmes et répondre aux exigences légales. L'appliance Citrix ADC prend en charge toutes les fonctionnalités de journalisation LSN pour la journalisation des informations DS-Lite. Pour configurer la journalisation DS-Lite, utilisez les procédures de configuration de la journalisation LSN, décrites dans Logging and Monitoring LSN.

Un message de journal pour une entrée de mappage DS-Lite LSN contient les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal est source
- Horodatage
- Type d'entrée (MAPPING)
- Indique si l'entrée de mappage DS-Lite LSN a été créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP NAT et port
- Nom du protocole
- L'adresse IP de destination, le port et l'ID de domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
  - Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
  - L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse.

Un message de journal pour une session DS-Lite contient les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal est source
- Horodatage
- Type d'entrée (SESSION)
- Indique si la session DS-Lite est créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP NAT et port
- Nom du protocole
- Adresse IP de destination, port et ID de domaine de trafic

Le tableau suivant présente des exemples d'entrées de journal DS-Lite de chaque type stocké sur les serveurs de journaux configurés. Ces entrées de journal sont générées par une appliance Citrix ADC dont l'adresse NSIP est 10.102.37.115.Vous pouvez consigner des informations DS-Lite pour diagnostiquer ou résoudre des problèmes et répondre aux exigences légales. L'appliance Citrix ADC prend en charge toutes les fonctionnalités de journalisation LSN pour la journalisation des informations DS-Lite. Pour configurer la journalisation DS-Lite, utilisez les procédures de configuration de la journalisation LSN, décrites dans Logging and Monitoring LSN.

Un message de journal pour une entrée de mappage DS-Lite LSN contient les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le mes-

sage de journal est source
- Horodatage
- Type d'entrée (MAPPING)
- Indique si l'entrée de mappage DS-Lite LSN a été créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP NAT et port
- Nom du protocole
- L'adresse IP de destination, le port et l'ID de domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
  - Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
  - L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse.

Un message de journal pour une session DS-Lite contient les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal est source
- Horodatage
- Type d'entrée (SESSION)
- Indique si la session DS-Lite est créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP NAT et port
- Nom du protocole
- Adresse IP de destination, port et ID de domaine de trafic

Le tableau suivant présente des exemples d'entrées de journal DS-Lite de chaque type stocké sur les serveurs de journaux configurés. Ces entrées de journal sont générées par une appliance Citrix ADC dont l'adresse NSIP est 10.102.37.115.

Type d'entrée du journal LSN	Exemple d'entrée de journal

Création de session DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:35:38 GMT 0-PPE-1 : default LSN LSN_SESSION 37647607 0 : SESSION CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol:TCP
Suppression de session DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:38:22 GMT 0-PPE-1 : default LSN LSN_SESSION 37647617 0 : SESSION DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol: TCP
Création de mappage DS-Lite LSN	Local4.Informational 10.102.37.115 08/14/2015:13:35:39 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647610 0 : EIM CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP
Suppression du mappage DS-Lite LSN	Local4.Informational 10.102.37.115 08/14/2015:13:38:25 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647618 0 : EIM DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP

Affichage des sessions DS-Lite actuelles

Vous pouvez afficher les sessions DS-Lite actuelles pour détecter les sessions indésirables ou inefficaces sur l'appliance Citrix ADC. Vous pouvez afficher toutes les sessions DS-Lite ou certaines, sur la base des paramètres de sélection.

Configuration à l'aide de l'interface de ligne de commande

Pour afficher toutes les sessions DS-Lite à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
show lsn session  - nattype DS-Lite
<!--NeedCopy-->
```

Pour afficher les sessions DS-Lite sélectionnées à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
show lsn session  - nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Exemple :

L'exemple de sortie suivant affiche toutes les sessions DS-Lite existantes sur une appliance Citrix ADC :

```
show lsn session  - nattype DS-Lite
  B4-Address SubscrIP SubscrPort SubscrTD DstIP DstPort DstTD NatIP
     NatPort Proto Dir

1.  2001:DB8::3:4 192.0.2.51 2552 0 198.51.100.250 80 0 203.0.113.61
    3002 TCP OUT

2.  2001:DB8::3:4 192.0.2.51 3551 0 198.51.100.300 80 0 203.0.113.61
    52862 TCP OUT

3.  2001:DB8::3:4 192.0.2.100 4556 0 198.51.100.250 0 0 203.0.113.61
    48116 ICMP OUT

4.  2001: DB8::190 192.0.2.150 3881 0 198.51.100.199 80 0 203.0.113.69
    48305 TCP OUT

Done
<!--NeedCopy-->
```

Configuration à l'aide de l'utilitaire de configuration

Pour afficher toutes les sessions DS-Lite ou sélectionnées à l'aide de l'utilitaire de configuration

1. **Accédez à Système** > **NAT à grande échelle** > **Sessions**, puis cliquez sur l'onglet **DS-lite**.
2. Pour afficher les sessions DS-Lite sur la base des paramètres de sélection, cliquez sur **Rechercher**.

Effacement des sessions DS-Lite

Vous pouvez supprimer toutes les sessions DS-Lite indésirables ou inefficaces de l'appliance Citrix ADC. L'appliance libère immédiatement les ressources (telles que l'adresse IP NAT, le port et la mémoire) allouées pour ces sessions, ce qui rend les ressources disponibles pour les nouvelles sessions. L'appliance supprime également tous les paquets suivants liés à ces sessions supprimées. Vous pouvez supprimer toutes les sessions DS-Lite ou sélectionnées de l'appliance Citrix ADC.

Pour effacer toutes les sessions DS-Lite à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
flush lsn session -nattype DS-Lite
show lsn session -nattype DS-Lite
```

Pour effacer les sessions DS-Lite sélectionnées à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
flush lsn session  - nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]

show lsn session  - nattype DS-Lite
<!--NeedCopy-->
```

Pour effacer toutes les sessions DS-Lite ou sélectionnées à l'aide de l'utilitaire de configuration :

1. Accédez à **Système** > **NAT à grande échelle** > **Sessions**, puis cliquez sur l'onglet **DS-Lite** .
2. Cliquez sur **Vider les sessions**.

Configuration de cartes statiques DS-Lite

August 20, 2021

L'appliance Citrix ADC prend en charge la création manuelle de mappages LSN DS-Lite, qui contiennent le mappage entre les informations suivantes :

- Adresse IP et port de l'abonné, et adresse IPv6 du périphérique ou du composant B4
- Adresse IP NAT et port

Les mappages LSN DS-Lite statiques sont utiles dans les cas où vous souhaitez vous assurer que les connexions initiées à une adresse IP NAT et à un port correspondent à l'adresse IP de l'abonné et au port via le périphérique B4 spécifié (par exemple, les serveurs Web situés dans le réseau interne).

Remarque : Cette fonctionnalité est prise en charge dans la version 11.0 build 64.x et les versions ultérieures.

Pour créer un mappage LSN statique DS-Lite à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort> [-td
    <positive_integer>] [-network6 <B4_ADDR>] [<natIP> [<natPort>]] [-
    destIP<ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```

Descriptions des paramètres

add lsn static

- nom

Nom de l'entrée de mappage statique LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le groupe LSN créé. La condition suivante s'applique uniquement à l'interface de ligne de commande : si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "ds-lite lsn static1" ou 'ds-lite lsn static1'). Il s'agit d'un argument obligatoire. Longueur maximale : 127

- transportprotocol

Protocole pour l'entrée de mappage DS-Lite LSN.

- subscrIP

Adresse IPv4 d'un abonné pour l'entrée de mappage DS-Lite LSN.

- subscrPort

Port de l'abonné pour l'entrée de mappage DS-Lite LSN.

- Network6

Adresse IPv6 du périphérique ou du composant B4.

- td

ID du domaine de trafic auquel appartient le périphérique B4. L'adresse IPv6 du périphérique B4 est spécifiée dans le paramètre network6. Si vous ne spécifiez pas d'ID, le périphérique B4 est supposé faire partie du domaine de trafic par défaut.

- natIP

Adresse IPv4, déjà existante sur l'appliance Citrix ADC en tant que type LSN, à utiliser comme adresse IP NAT pour cette entrée de mappage.

- natPort

Port NAT pour cette entrée de mappage LSN DS-Lite.

- destIP

Adresse IP de destination pour l'entrée de mappage DS-Lite LSN.

- dsttd

ID du domaine de trafic par lequel l'adresse IP de destination de cette entrée de mappage DS-Lite LSN est accessible depuis l'appliance Citrix ADC. Si vous ne spécifiez pas d'ID, l'adresse IP de destination est supposée être accessible via le domaine de trafic par défaut, qui a un ID de 0.

Pour créer un mappage LSN statique DS-Lite à l'aide de l'utilitaire de configuration

Accédez à Système > NAT à grande échelle > Statique et ajoutez un nouveau mappage LSN statique DS-Lite.

Configuration de l'allocation NAT déterministe pour DS-Lite

January 21, 2021

L'allocation NAT déterministe pour les déploiements LSN DS-Lite est un type d'allocation de ressources NAT dans lequel l'appliance Citrix ADC préalloue, à partir du pool IP NAT LSN et en fonction de la taille de bloc de port spécifiée, une adresse IP NAT LSN et un bloc de ports à chaque abonné (abonné derrière le périphérique B4).

Remarque : Cette fonctionnalité est prise en charge dans la version 11.0 build 64.x et les versions ultérieures.

L'appliance alloue séquentiellement des ressources NAT à ces abonnés. Elle attribue le premier bloc de ports sur l'adresse IP NAT de début à l'adresse IP de l'abonné de début. La plage suivante de ports est attribuée à l'abonné suivant, et ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné suivant. À ce stade, le premier bloc de port sur l'adresse NAT suivante est affecté à l'abonné, et ainsi de suite.

L'appliance Citrix ADC consigne l'adresse IP NAT allouée et le bloc de port pour un abonné. Pour une connexion, un abonné peut être identifié uniquement par son adresse IP NAT mappée et son bloc de

port. Pour cette raison, l'appliance Citrix ADC ne consigne pas la création ou la suppression d'une session LSN.

Un abonné DS-Lite ne peut avoir qu'un seul bloc de port déterministe. Si l'ensemble du bloc de ports est utilisé, l'appliance Citrix ADC supprime toute nouvelle connexion de l'abonné.

Exemple : DS-Lite déterministe

Dans cet exemple, une configuration DS-Lite déterministe inclut quatre abonnés avec les adresses IP 192.0.17.5, 192.0.17.6, 192.0.17.7 et 192.0.17.8. Ces abonnés ipv4 sont derrière un périphérique B4 ayant l'adresse IPv6 2001:DB8::3:4. Dans cette configuration, la taille du bloc de port est définie sur 20480 et le pool d'adresses IP NAT LSN a des adresses IP dans la plage 203.0.113.41-203.0.113.42.

L'appliance Citrix ADC préalloue séquentiellement, à partir du pool d'adresses IP NAT LSN et en fonction de la taille de bloc de port définie, une adresse IP NAT LSN et un bloc de ports à chaque abonné. Il affecte le premier bloc de ports (1024-21503) sur l'adresse IP NAT de début (203.0.113.41) à l'adresse IP de l'abonné débutant (192.0.17.5). La plage suivante de ports est attribuée à l'abonné suivant, et ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné suivant. À ce stade, le premier bloc de port sur l'adresse IP NAT suivante est attribué à l'abonné, et ainsi de suite. Citrix ADC consigne l'adresse IP NAT et le bloc de ports alloués à chaque abonné.

L'appliance Citrix ADC ne consigne aucune session LSN créée ou supprimée pour ces abonnés.

Le tableau suivant répertorie l'adresse IP NAT et les blocs de ports alloués à chaque abonné dans cet exemple :

Adresse IP de l'abonné	Adresse IP NAT allouée	Bloc de ports alloué	Adresse IPv6 de B4
192.0.17.5	203.0.113.41	1024 - 21503	2001:DB8::3:4
192.0.17.6	203.0.113.41	21504 - 41983	2001:DB8::3:4
192.0.17.7	203.0.113.41	41984 - 62463	2001:DB8::3:4
192.0.17.8	203.0.113.42	1024 - 21503	2001:DB8::3:4

Étapes de configuration

Vous devez configurer NAT déterministe dans le cadre de la configuration DS-Lite. Pour obtenir des instructions sur la configuration de DS-Lite, reportez-vous à la section Configuration de DS-Lite.

Lors de la configuration de DS-Lite, assurez-vous que vous :

- Définissez le paramètre Type NAT sur Deterministic lors de l'ajout du pool LSN et du groupe LSN.
- Définissez le paramètre de taille de bloc de port souhaité lors de l'ajout du groupe LSN, sauf si vous pouvez accepter la valeur par défaut.

Points à prendre en considération avant de configurer le DS-Lite déterministe

Tenez compte des points suivants avant de configurer DS-Lite déterministe :

- L'adresse IP complète de chaque abonné doit être spécifiée dans une commande distincte add lsn client, en définissant les paramètres Réseau et Masque réseau. (Définissez le masque de réseau sur 255.255.255.255.) L'adresse IPv4 du périphérique B4 spécifié dans le paramètre Network6 doit également être complète (préfixe /128). En d'autres termes, le paramètre Network et Network6 n'accepte pas les adresses autres que le masque /32 bits et le préfixe /128, respectivement.
- L'appliance Citrix ADC supprime les connexions des abonnés qui ne sont pas spécifiés dans une configuration DS-Lite déterministe, mais qui se trouvent derrière les périphériques B4 spécifiés dans une configuration DS-Lite déterministe.
- L'appliance Citrix ADC reconnaît les abonnés ayant la même adresse IPv4 que les abonnés différents s'ils se trouvent derrière des périphériques B4 différents. Une combinaison de l'adresse IPv4 de l'abonné et du périphérique B4 définit un abonné unique dans l'entité client LSN d'une configuration DS-Lite.

Exemple de configuration déterministe DS-Lite :

La configuration suivante utilise les paramètres répertoriés dans la section Exemple : DS-Lite déterministe.

```
1  add lsn client LSN-DSLITE-CLIENT-10
2
3  Done
4  bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.5 -netmask
       255.255.255.255 -network6 2001:DB8::3:4/128
5
6  Done
7  bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.6 -netmask
       255.255.255.255 -network6 2001:DB8::3:4/128
8
9  Done
10 bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.7 -netmask
       255.255.255.255 -network6 2001:DB8::3:4/128
11
12 Done
13 bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.8 -netmask
       255.255.255.255 -network6 2001:DB8::3:4/128
```



```
14
15 Done
16 add lsn pool LSN-DSLITE-POOL-10 -nattype DETERMINISTIC
17
18 Done
19 bind lsn pool LSN-DSLITE-POOL-10  203.0.113.41-203.0.113.42
20
21 Done
22 add lsn ip6profile LSN-DSLITE-PROFILE-10 -type DS-Lite -network6 2001:
      DB8::5:6
23
24 Done
25 add lsn group LSN-DSLITE-GROUP-10 -clientname LSN-DSLITE-CLIENT-10 -
      nattype DETERMINISTIC -portblocksize 20480 -ip6profile LSN-DSLITE-
      PROFILE-10
26
27 Done
28 bind lsn group LSN-DSLITE-GROUP-10 -poolname LSN-DSLITE-POOL-10
29
30 Done
31 <!--NeedCopy-->
```

Configuration des passerelles de couche d'application pour DS-Lite

January 21, 2021

Pour certains protocoles de couche d'application, les adresses IP et les numéros de port de protocole sont également communiqués dans la charge utile du paquet. Application Layer Gateway (AGL) pour un protocole analyse la charge utile du paquet et effectue les modifications nécessaires pour s'assurer que le protocole continue de fonctionner sur DS-Lite.

L'appliance Citrix ADC prend en charge ALG pour les protocoles suivants pour DS-Lite :

- FTP
- ICMP
- TFTP
- SIP
- RTSP

Passerelle de couche d'application pour les protocoles FTP, ICMP et TFTP

January 21, 2021

Vous pouvez activer ou désactiver ALG pour le protocole FTP pour une configuration DS-Lite en activant ou en désactivant l'option ALG FTP du groupe LSN de la configuration.

ALG pour le protocole ICMP est activé par défaut et aucune disposition ne permet de le désactiver.

ALG pour le protocole TFTP est désactivé par défaut. TFTP ALG est activé automatiquement pour une configuration DS-Lite lorsque vous liez un profil d'application UDP LSN, avec mappage indépendant du point de terminaison, filtrage indépendant du point de terminaison et port de destination 69 (port connu pour TFTP), au groupe LSN.

Passerelle de couche d'application pour le protocole SIP

August 20, 2021

L'utilisation de DS-Lite avec protocole SIP (Session Initiation Protocol) est compliquée, car les messages SIP contiennent des adresses IP dans les en-têtes SIP ainsi que dans le corps SIP. Lorsque LSN est utilisé avec SIP, les en-têtes SIP contiennent des informations sur l'appelant et le récepteur, et le périphérique traduit ces informations pour les masquer du réseau externe. Le corps SIP contient les informations SDP (Session Description Protocol), qui comprennent les adresses IP et les numéros de port pour la transmission du média. SIP ALG pour DS-Lite est conforme aux RFC 3261, RFC 3581, RFC 4566 et RFC 4475.

> **Remarque**
>
> SIP ALG est pris en charge dans une appliance autonome Citrix ADC, dans une configuration de haute disponibilité Citrix ADC, ainsi que dans une configuration de cluster Citrix ADC.

Limites de SIP ALG

SIP ALG pour DS-Lite présente les limitations suivantes :

- Seule la charge utile SDP est prise en charge.
- Les éléments suivants ne sont pas pris en charge :
  - Adresses IP de multidiffusion
  - SDP chiffré
  - SIP TLS
  - Traduction de FQDN

- Authentification de la couche SIP
- Partitions d'administration
- Corps en plusieurs parties
- Réassemblage de lignes

Configuration de SIP ALG

Vous devez configurer le SIP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration de LSN, reportez-vous à la section Configuration de DS-Lite. Lors de la configuration de LSN, assurez-vous que vous :

- Définissez les paramètres suivants lors de l'ajout d'un profil d'application LSN :
  - IP Pooling = PAIRED
  - Address and Port Mapping = ENDPOINT-INDEPENDENT
  - Filtering = ENDPOINT-INDEPENDENT
- Créez un profil ALG SIP et assurez-vous de définir la plage de ports source ou la plage de ports de destination. Liez le profil ALG SIP au groupe LSN
- Activer SIP ALG dans le groupe LSN

Pour activer SIP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn group <groupname> -clientname <string>[-sipalg ( ENABLED |
    DISABLED )]

show lsn group<groupname>
<!--NeedCopy-->
```

Pour activer SIP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn sipalgprofile<sipalgprofilename>[-dataSessionIdleTimeout<
    positive_integer>][-sipSessionTimeout<positive_integer>][-
    registrationTimeout<positive_integer>][-sipsrcportrange<port[-port
    ]>][-sipdstportrange<port[-port]>][-openRegisterPinhole ( ENABLED |
    DISABLED )][-openContactPinhole ( ENABLED | DISABLED )][-
    openViaPinhole ( ENABLED | DISABLED )][-openRecordRoutePinhole (
    ENABLED | DISABLED )]-sipTransportProtocol ( TCP | UDP )[-
    openRoutePinhole ( ENABLED | DISABLED )][-rport ( ENABLED | DISABLED
     )]
```



```
2
3 show lsn sipalgprofile<sipalgprofilename>
4 <!--NeedCopy-->
```

Exemple de configuration

L'exemple de configuration DS-Lite suivant, SIP ALG est activé pour le trafic TCP à partir de périphériques B4 dans le réseau 2001:DB8::3:0/96.

```
1 add lsn client LSN-DSLITE-CLIENT-1
2 Done
3 bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/96
4 Done
5 add lsn pool LSN-DSLITE-POOL-1
6 Done
7 bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
8 Done
9 add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
     DB8::5:6
10 Done
11 add lsn appsprofile LSN-DSLITE-APPS-PROFILE-1 TCP -ippooling PAIRED -
     mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
12 Done
13 add lsn sipalgprofile SIPALGPROFILE-1  -sipdstportrange 5060 -
     sipTransportProtocol TCP
14 Done
15 add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
     portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1 -sipalg ENABLED
16 Done
17 bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
18 Done
19 bind lsn group LSN-DSLITE-GROUP-1 -appsprofilename LSN-DSLITE-APPS-
     PROFILE-1
20 Done
21 bind lsn group LSN-DSLITE-GROUP-1 -sipalgprofilename SIPALGPROFILE-1
22 Done
23 <!--NeedCopy-->
```

Passerelle de couche d'application pour le protocole RTSP

August 20, 2021

Le protocole RTSP (Real Time Streaming Protocol) est un protocole au niveau de l'application pour le transfert de données multimédia en temps réel. Utilisé pour établir et contrôler des sessions multimédias entre les points de fin, RTSP est un protocole de canal de contrôle entre le client multimédia et le serveur multimédia. La communication typique est entre un client et un serveur multimédia de streaming.

La diffusion de médias à partir d'un réseau privé vers un réseau public nécessite la traduction des adresses IP et des numéros de port sur le réseau. La fonctionnalité Citrix ADC comprend une passerelle de couche d'application (ALG) pour RTSP, qui peut être utilisée avec le NAT à grande échelle (LSN) pour analyser le flux de médias et apporter les modifications nécessaires pour garantir que le protocole continue de fonctionner sur le réseau.

La manière dont la traduction d'adresses IP est effectuée dépend du type et de la direction du message, ainsi que du type de support pris en charge par le déploiement client-serveur. Les messages sont traduits comme suit :

- Demande sortante : adresse IP privée vers une adresse IP publique appartenant à Citrix ADC appelée adresse IP LSN.
- Réponse entrante : adresse IP LSN vers adresse IP privée.
- Demande entrante : aucune traduction.
- Réponse sortante : adresse IP privée à l'adresse IP du pool LSN.

> **Remarque**
>
> RTSP ALG est pris en charge dans une appliance autonome Citrix ADC, dans une configuration de haute disponibilité Citrix ADC, ainsi que dans une configuration de cluster Citrix ADC.

Limites de l'ALG RTSP

Le RTSP ALG ne prend pas en charge les éléments suivants :

- Sessions RTSP multidiffusion
- Session RTSP via UDP
- Partitions d'administration
- Authentification RTSP
- Tunneling HTTP

Configuration de RTSP ALG

Configurez RTSP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration de LSN, reportez-vous à la section Configuration de DS-Lite. Lors de la configuration de LSN, assurez-vous que vous :

- Définissez les paramètres suivants lors de l'ajout d'un profil d'application LSN :

  - IP Pooling = PAIRED
  - Address and Port Mapping = ENDPOINT-INDEPENDENT
  - Filtering = ENDPOINT-INDEPENDENT
- Activer RTSP ALG dans le groupe LSN
- Créer un profil ALG RTSP et lier le profil ALG RTSP au groupe LSN

Pour activer RTSP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn group <groupname> -clientname <string> [-rtspalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

Pour activer RTSP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn rtspalgprofile <rtspalgprofilename> [-rtspIdleTimeout <
    positive_integer>] -rtspportrange <port[-port]> [-
    rtspTransportProtocol (TCP|UDP)]

show lsn rtspalgprofile <rtspalgprofilename>
<!--NeedCopy-->
```

Exemple de configuration ALG RTSP

L'exemple de configuration DS-Lite suivant, RTSP ALG est activé pour le trafic TCP à partir de périphériques B4 dans le réseau 2001:DB8::4:0/96.

Exemple de configuration ALG RTSP :

```
add lsn client LSN-DSLITE-CLIENT-5
Done
bind lsn client LSN-DSLITE-CLIENT-5 -network6 2001:DB8::4:0/96
Done
add lsn pool LSN-DSLITE-POOL-5
Done
bind lsn pool LSN-DSLITE-POOL-5 203.0.113.61 - 203.0.113.70
Done
```



```
add lsn ip6profile LSN-DSLITE-PROFILE-5 -type DS-Lite -network6 2001:
   DB8::5:6
Done
add lsn appsprofile LSN-DSLITE-APPS-PROFILE-5 TCP -ippooling PAIRED -
   mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn rtspalgprofile RTSPALGPROFILE-5 -rtspIdleTimeout 1000 -
   rtspportrange 554
Done
add lsn group LSN-DSLITE-GROUP-5 -clientname LSN-DSLITE-CLIENT-5 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-5 -rtspalg ENABLED
Done
bind lsn group LSN-DSLITE-GROUP-5 -poolname LSN-DSLITE-POOL-5
Done
bind lsn group LSN-DSLITE-GROUP-5 -appsprofilename LSN-DSLITE-APPS-
   PROFILE-5
Done
bind lsn group LSN-DSLITE-GROUP-5 -rtspalgprofilename RTSPALGPROFILE-5
Done
<!--NeedCopy-->
```

Journalisation et surveillance de DS-Lite

August 20, 2021

Vous pouvez consigner les informations DS-Lite pour diagnostiquer ou résoudre les problèmes et répondre aux exigences légales. L'appliance Citrix ADC prend en charge toutes les fonctionnalités de journalisation LSN pour la journalisation des informations DS-Lite. Pour configurer la journalisation DS-Lite, utilisez les procédures de configuration de la journalisation LSN, décrites dans Logging and Monitoring LSN.

Un message de journal pour une entrée de mappage DS-Lite LSN contient les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal est source
- Horodatage
- Type d'entrée (MAPPING)
- Indique si l'entrée de mappage DS-Lite LSN a été créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP NAT et port

- Nom du protocole
- L'adresse IP de destination, le port et l'ID de domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
  - Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
  - L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse.

Un message de journal pour une session DS-Lite contient les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal est source
- Horodatage
- Type d'entrée (SESSION)
- Indique si la session DS-Lite est créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP NAT et port
- Nom du protocole
- Adresse IP de destination, port et ID de domaine de trafic

Le tableau suivant présente des exemples d'entrées de journal DS-Lite de chaque type stocké sur les serveurs de journaux configurés. Ces entrées de journal sont générées par une appliance Citrix ADC dont l'adresse NSIP est 10.102.37.115.Vous pouvez consigner des informations DS-Lite pour diagnostiquer ou résoudre des problèmes et répondre aux exigences légales. L'appliance Citrix ADC prend en charge toutes les fonctionnalités de journalisation LSN pour la journalisation des informations DS-Lite. Pour configurer la journalisation DS-Lite, utilisez les procédures de configuration de la journalisation LSN, décrites dans Logging and Monitoring LSN.

Un message de journal pour une entrée de mappage DS-Lite LSN contient les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal est source
- Horodatage
- Type d'entrée (MAPPING)
- Indique si l'entrée de mappage DS-Lite LSN a été créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP NAT et port
- Nom du protocole

- L'adresse IP de destination, le port et l'ID de domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
  - Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
  - L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse.

Un message de journal pour une session DS-Lite contient les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal est source
- Horodatage
- Type d'entrée (SESSION)
- Indique si la session DS-Lite est créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP NAT et port
- Nom du protocole
- Adresse IP de destination, port et ID de domaine de trafic

Le tableau suivant présente des exemples d'entrées de journal DS-Lite de chaque type stocké sur les serveurs de journaux configurés. Ces entrées de journal sont générées par une appliance Citrix ADC dont l'adresse NSIP est 10.102.37.115.

Type d'entrée du journal LSN	Exemple d'entrée de journal
Création de session DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:35:38 GMT 0-PPE-1 : default LSN LSN_SESSION 37647607 0 : SESSION CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol:TCP

Suppression de session DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:38:22 GMT 0-PPE-1 : default LSN LSN_SESSION 37647617 0 : SESSION DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol: TCP
Création de mappage DS-Lite LSN	Local4.Informational 10.102.37.115 08/14/2015:13:35:39 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647610 0 : EIM CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP
Suppression du mappage DS-Lite LSN	Local4.Informational 10.102.37.115 08/14/2015:13:38:25 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647618 0 : EIM DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP

Affichage des sessions DS-Lite actuelles

Vous pouvez afficher les sessions DS-Lite actuelles pour détecter les sessions indésirables ou inefficaces sur l'appliance Citrix ADC. Vous pouvez afficher toutes les sessions DS-Lite ou certaines, sur la base des paramètres de sélection.

Pour afficher toutes les sessions DS-Lite à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 show lsn session -nattype DS-Lite
2 <!--NeedCopy-->
```

Pour afficher les sessions DS-Lite sélectionnées à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
show lsn session  -nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

L'exemple de sortie suivant affiche toutes les sessions DS-Lite existantes sur une appliance Citrix ADC :

> show lsn session –nattype DS-Lite

```
  B4-Address SubscrIP SubscrPort SubscrTD DstIP DstPort DstTD NatIP
     NatPort Proto Dir

1. 2001:DB8::3:4 192.0.2.51 2552 0 198.51.100.250 80 0 203.0.113.61
    3002 TCP OUT

2. 2001:DB8::3:4 192.0.2.51 3551 0 198.51.100.300 80 0 203.0.113.61
    52862 TCP OUT

3. 2001:DB8::3:4 192.0.2.100 4556 0 198.51.100.250 0 0 203.0.113.61
    48116 ICMP OUT

4. 2001: DB8::190 192.0.2.150 3881 0 198.51.100.199 80 0 203.0.113.69
    48305 TCP OUT
Done
<!--NeedCopy-->
```

Configuration à l'aide de l'utilitaire de configuration

Pour afficher toutes les sessions DS-Lite ou sélectionnées à l'aide de l'utilitaire de configuration

1. **Accédez à Système** > **NAT à grande échelle** > **Sessions**, puis cliquez sur l'onglet **DS-lite**.
2. Pour afficher les sessions DS-Lite sur la base des paramètres de sélection, cliquez sur **Rechercher**.

Effacement des sessions DS-Lite

Vous pouvez supprimer toutes les sessions DS-Lite indésirables ou inefficaces de l'appliance Citrix ADC. L'appliance libère immédiatement les ressources (telles que l'adresse IP NAT, le port et la mémoire) allouées pour ces sessions, ce qui rend les ressources disponibles pour les nouvelles sessions. L'appliance supprime également tous les paquets suivants liés à ces sessions supprimées. Vous pouvez supprimer toutes les sessions DS-Lite ou sélectionnées de l'appliance Citrix ADC.

Pour effacer toutes les sessions DS-Lite à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
flush lsn session -nattype DS-Lite

show lsn session -nattype DS-Lite
<!--NeedCopy-->
```

Pour effacer les sessions DS-Lite sélectionnées à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
flush lsn session -nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]

show lsn session -nattype DS-Lite
<!--NeedCopy-->
```

Pour effacer toutes les sessions DS-Lite ou sélectionnées à l'aide de l'utilitaire de configuration

1. Accédez à **Système** > **NAT à grande échelle** > **Sessions**, puis cliquez sur l'onglet **DS-Lite** .
2. Cliquez sur **Vider les sessions**.

Journalisation des informations d'en-tête HTTP

L'appliance Citrix ADC peut consigner les informations d'en-tête de requête d'une connexion HTTP qui utilise la fonctionnalité DS-Lite. Les informations d'en-tête suivantes d'un paquet de requête HTTP peuvent être enregistrées :

- URL à laquelle la requête HTTP est destinée
- Méthode HTTP spécifiée dans la requête HTTP
- Version HTTP utilisée dans la requête HTTP
- Adresse IPv4 de l'abonné qui a envoyé la requête HTTP

Les journaux d'en-tête HTTP peuvent être utilisés par les FAI pour voir les tendances liées au protocole HTTP parmi un ensemble d'abonnés. Par exemple, un FAI peut utiliser cette fonctionnalité pour trouver le site Web le plus populaire parmi un ensemble d'abonnés.

Étapes de configuration

Effectuez les tâches suivantes pour configurer l'appliance Citrix ADC pour consigner les informations d'en-tête HTTP :

- **Créez un profil de journal d'en-tête HTTP**. Un profil de journal d'en-tête HTTP est un ensemble d'attributs d'en-tête HTTP (par exemple, URL et méthode HTTP) qui peuvent être activés ou désactivés pour la journalisation.
- **Liez l'en-tête HTTP à un groupe LSN d'une configuration LSN DS-Lite**. Liez le profil du journal des en-têtes HTTP à un groupe LSN d'une configuration LSN en définissant le paramètre nom du profil du journal des en-têtes HTTP sur le nom du profil du journal des en-têtes HTTP créé. L'appliance Citrix ADC consigne ensuite les informations d'en-tête HTTP de toutes les requêtes HTTP liées au groupe LSN. Un profil de journal d'en-tête HTTP peut être lié à plusieurs groupes LSN, mais un groupe LSN ne peut avoir qu'un seul profil de journal d'en-tête HTTP.

Pour créer un profil de journal d'en-tête HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
     DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
     ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]
2
3 show lsn httphdrlogprofile
4 <!--NeedCopy-->
```

Pour lier un profil de journal d'en-tête HTTP à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 bind lsn group <groupname> -httphdrlogprofilename <string>
2
3 show lsn group <groupname>
4 <!--NeedCopy-->
```

Exemple de configuration

Dans la configuration LSN DS-Lite suivante, le profil de journal d'en-tête HTTP HTTP-header-log-1 est lié au groupe LSN LSN-DSLITE-GROUP-1. Le profil de journal a tous les attributs HTTP (URL, méthode HTTP, version HTTP et adresse IP HOST) activés pour la journalisation, de sorte que tous

ces attributs sont enregistrés pour toutes les requêtes HTTP des périphériques B4 (dans le réseau 2001:DB8:5001::/96).

Exemple de configuration :

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1

Done

add lsn client LSN-DSLITE-CLIENT-1

Done

bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100

Done

add lsn pool LSN-DSLITE-POOL-1

Done

bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70

Done

add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
   DB8::5:6

Done

add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1

Done

bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1

Done

bind lsn group LSN-DSLITE-GROUP-1 -httphdrlogprofilename HTTP-HEADER-
   LOG-1

Done
<!--NeedCopy-->
```


Journalisation IPFIX

L'appliance Citrix ADC prend en charge l'envoi d'informations sur les événements LSN au format IPFIX (Internet Protocol Flow Information Export) vers l'ensemble configuré de collecteurs IPFIX. L'appliance utilise la fonctionnalité AppFlow existante pour envoyer des événements LSN au format IPFIX aux collecteurs IPFIX.

La journalisation basée sur IPFIX est disponible pour les événements DS_Lite suivants :

- Création ou suppression d'une session LSN.
- Création ou suppression d'une entrée de mappage LSN.
- Allocation ou désallocation de blocs de ports dans le contexte d'un NAT déterministe.
- Allocation ou désallocation de blocs de ports dans le contexte de NAT dynamique.
- Chaque fois que le quota de session d'abonné est dépassé.

Points à considérer avant de configurer la journalisation IPFIX

Avant de commencer à configurer IPSec ALG, tenez compte des points suivants :

- Vous devez configurer la fonctionnalité AppFlow et les collecteurs IPFIX sur l'appliance Citrix ADC. Pour obtenir des instructions, reportez-vous à la section Configuration de la fonctionnalité AppFlow.

Étapes de configuration

Effectuez les tâches suivantes pour consigner les informations LSN au format IPFIX :

- **Activez la journalisation LSN dans la configuration AppFlow**. Activez le paramètre de journalisation LSN dans le cadre de la configuration AppFlow.
- **Créez un profil de journal LSN**. Un profil de journal LSN inclut le paramètre IPFIX qui active ou désactive les informations de journal au format IPFIX.
- **Liez le profil de journal LSN à un groupe LSN d'une configuration LSN**. Liez le profil de journal LSN à un ou plusieurs groupes LSN. Les événements liés au groupe LSN lié seront enregistrés au format IPFIX.

Pour activer la journalisation LSN dans la configuration AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set appflow param -lsnLogging (ENABLED |DISABLED )

show appflow param
<!--NeedCopy-->
```


Pour créer un profil de journal LSN à l'aide de l'interface de ligne de commande, tapez

À l'invite de commandes, tapez :

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Pour créer un profil de journal LSN à l'aide de l'interface graphique

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur onglet **Journal**, puis ajoutez un profil de journal.

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface graphique

1. Accédez à **Système** > **NAT à grande échelle** > **Groupe LSN,** ouvrez le groupe **LSN**.
2. Dans **Paramètres avancés,** cliquez sur **+ Profil du journal** pour lier le profil journal créé au groupe LSN.

Protocole de contrôle de port pour DS-Lite

January 21, 2021

Les appliances Citrix ADC prennent désormais en charge le protocole PCP (Port Control Protocol) pour NAT à grande échelle (LSN). Bon nombre des applications abonnées d'un fournisseur de services Internet doivent être accessibles à partir d'Internet (par exemple, des appareils Internet des objets (IOT), comme une caméra IP qui assure la surveillance sur Internet). Une façon de répondre à cette exigence est de créer des mappings NAT (LSN) statiques à grande échelle. Mais pour un très grand nombre d'abonnés, la création de mappings NAT LSN statiques n'est pas une solution réalisable.

Port Control Protocol (PCP) permet à un abonné de demander des mappages NAT LSN spécifiques pour lui-même et/ou pour d'autres périphériques tiers. Le périphérique NAT à grande échelle crée un mapping LSN et l'envoie à l'abonné. L'abonné envoie aux périphériques distants sur Internet l'adresse IP NAT : port NAT auquel ils peuvent se connecter à l'abonné.

Les applications envoient généralement des messages keep-alive fréquents au périphérique NAT à grande échelle afin que leurs mappages LSN ne s'écoule pas. PCP aide à réduire la fréquence de ces messages Keep-alive en permettant aux applications d'apprendre les paramètres de délai d'expiration des mappages LSN. Cela permet de réduire la consommation de bande passante sur le réseau d'accès du FAI et la consommation de batterie sur les appareils mobiles.

PCP est un modèle client-serveur qui fonctionne sur le protocole de transport UDP. Une appliance Citrix ADC implémente le composant serveur PCP et est conforme à la RFC 6887.

Étapes de configuration

Effectuez les tâches suivantes pour configurer PCP :

- (Facultatif) Créez un profil PCP. Un profil PCP inclut des paramètres pour les paramètres associés à PCP (par exemple, pour écouter les requêtes de mappage et PCP homologue). Un profil PCP peut être lié à un serveur PCP. Un profil PCP lié à un serveur PCP applique tous ses paramètres au serveur PCP. Un profil PCP peut être lié à plusieurs serveurs PCP. Par défaut, un profil PCP avec les paramètres par défaut est lié à tous les serveurs PCP. Un profil PCP que vous liez à un serveur PCP remplace les paramètres de profil PCP par défaut pour ce serveur. Un profil PCP par défaut possède les paramètres suivants :
  - Mappage : activé
  - Peer : activé
  - Durée de vie minimale du mapping : 120 secondes
  - Durée de vie maximale : 86400 secondes
  - Nombre d'annonces : 10
  - Tiers : désactivé
- Créez un serveur PCP et liez un profil PCP à celui-ci. Créez un serveur PCP sur l'appliance Citrix ADC pour écouter les requêtes PCP et les messages des abonnés. Une adresse IP de sous-réseau (SNIP) doit être attribuée à un serveur PCP pour y accéder. Par défaut, un serveur PCP écoute sur le port 5351.
- Liez le serveur PCP à un groupe LSN d'une configuration LSN. Liez le serveur PCP créé à un groupe LSN d'une configuration LSN en définissant le paramètre Serveur PCP pour spécifier le serveur PCP créé. Le serveur PCP créé est accessible uniquement par les abonnés de ce groupe LSN.

  Remarque : Un serveur PCP pour une configuration NAT à grande échelle ne répond pas aux demandes des abonnés identifiés par les règles ACL.

Pour créer un profil PCP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

Pour créer un serveur PCP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Exemple de configuration pour DS-LITE

Dans l'exemple de configuration suivant, le serveur PCP PCP-SERVER-1, avec les paramètres PCP de PCP-DSLITE-PROFILE-1, est lié au groupe LSN LSN-DSLITE-GROUP-1. PCP-SERVER-9 sert les demandes PCP des abonnés IPv4 derrière les périphériques B4 du réseau 2001:DB8::3:0/100.

Exemple de configuration :

```
add pcp profile PCP-DSLITE-PROFILE-1 -minMapLife 300
Done
add pcp server PCP-DSLITE-SERVER-1 192.0.3.10  -pcpProfile PCP-DSLITE-
    PROFILE-1
Done
add lsn client LSN-DSLITE-CLIENT-1
Done
bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100
Done
add lsn pool LSN-DSLITE-POOL-1
Done
bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
Done
```



```
13 add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
      DB8::5:6
14 Done
15 add lsn group LSN-DSLITE-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
      ip6profile LSN-NAT64-PROFILE-1
16 Done
17 bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-NAT64-POOL-1
18 Done
19 bind lsn group LSN-DSLITE-GROUP-1 -poolname  PCP-NAT64-SERVER-1
20 Done
21 <!--NeedCopy-->
```

Large Scale NAT64

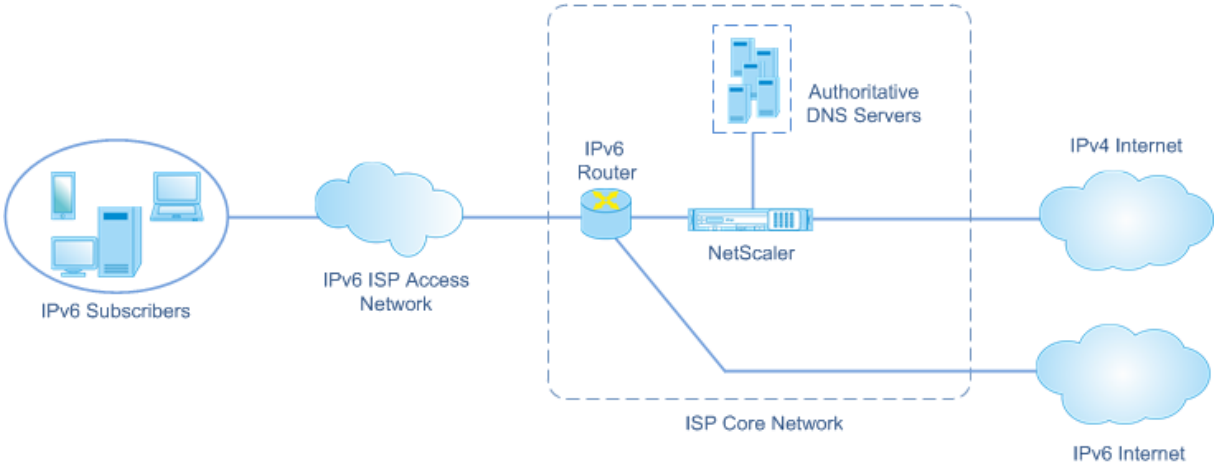
August 20, 2021

En raison de l'épuisement imminent des adresses IPv4, les FAI ont commencé à passer à l'infrastructure IPv6. Mais pendant la transition, les FAI doivent continuer à prendre en charge IPv4 avec IPv6, car la plupart de l'Internet public utilise encore IPv4. NAT64 à grande échelle est une solution de transition IPv6 permettant aux FAI disposant d'une infrastructure IPv6 de connecter leurs abonnés IPv6 uniquement à Internet IPv4. DNS64 est une solution permettant la découverte de domaines IPv4 uniquement par des clients IPv6 uniquement. Le DNS64 est utilisé avec NAT64 à grande échelle pour permettre une communication transparente entre les clients IPv6 uniquement et les serveurs IPv4 uniquement.

Une appliance Citrix ADC implémente NAT64 et DNS64 à grande échelle et est conforme aux RFC 6145, 6146, 6147, 6052, 3022, 2373, 2765 et 2464.

Architecture

L'architecture NAT64 d'un fournisseur de services Internet utilisant une appliance Citrix ADC consiste en des abonnés IPv6 accédant à Internet IPv4 via une appliance Citrix ADC déployée dans le réseau central du fournisseur de services Internet. Les abonnés IPv6 sont connectés au réseau central du FAI via le réseau d'accès IPv6 uniquement du FAI.



La fonctionnalité NAT64 à grande échelle d'une appliance Citrix ADC permet la communication entre les clients IPv6 et les serveurs IPv4 via la traduction de paquets IPv6 vers IPv4, et vice versa, tout en conservant les informations de session sur l'appliance Citrix ADC. La fonctionnalité Citrix ADC DNS64 représente les domaines IPv4 uniquement à IPv6- en synthétisant les enregistrements DNS AAAA pour les domaines IPv4 uniquement et en les envoyant aux abonnés.

NAT64 à grande échelle a deux composants principaux : le préfixe NAT64 et NAT IPv4 pool. DNS64 a un composant principal, le préfixe DNS64, qui a la même valeur que le préfixe NAT64.

Lors de la réception d'une demande AAAA d'un abonné IPv6 uniquement pour un nom de domaine hébergé sur un serveur Web IPv4 uniquement sur Internet, la fonctionnalité Citrix ADC DNS64 synthétise un enregistrement AAAA pour le nom de domaine et l'envoie à l'abonné. L'enregistrement AAAA est synthétisé en concaténant le préfixe DNS64 (qui est défini sur le préfixe NAT64) et l'adresse IPv4 réelle du nom de domaine.

L'abonné dispose désormais d'une adresse de destination IPv6 correspondant au nom de domaine souhaité. L'abonné envoie la demande à l'adresse IPv6 synthétisée. Lors de la réception de la demande IPv6, la fonctionnalité Citrix ADC NAT64 à grande échelle traduit le paquet de requête IPv6 en paquet de requête IPv4. NAT64 à grande échelle définit l'adresse de destination de la demande IPv4 sur l'adresse IPv4, qui est extraite de l'adresse de destination de la demande IPv6 en dépouillant le préfixe NAT64 de l'adresse IPv6. Le port de destination est conservé à partir de la demande IPv6. NAT64 à grande échelle définit également l'adresse IP source:port source du paquet IPv4 sur l'adresse IP NAT : port NAT sélectionné dans le pool NAT configuré.

L'appliance conserve un enregistrement de toutes les sessions actives qui utilisent la fonctionnalité NAT64 à grande échelle. Ces sessions sont appelées sessions NAT64 à grande échelle. L'appliance gère également les mappages entre l'adresse et le port IPv6 de l'abonné, et l'adresse et le port NAT IPv4, pour chaque session NAT64 à grande échelle. Ces mappings sont appelés mappings NAT64 à grande échelle. À partir des entrées de session NAT64 à grande échelle et des entrées de mappage NAT64 à grande échelle, l'appliance Citrix ADC reconnaît un paquet de réponse (reçu d'Internet) comme appartenant à une session NAT64 particulière.

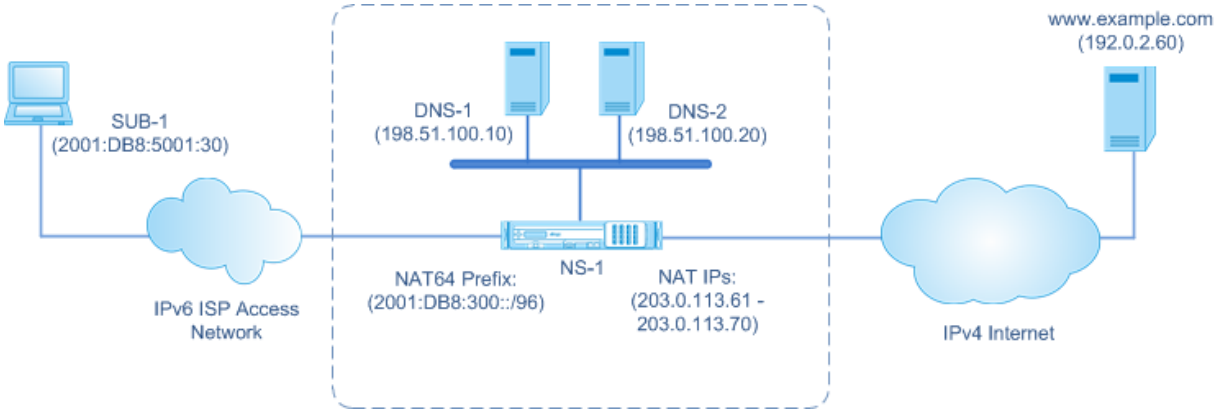
Lorsque l'appliance reçoit un paquet de réponse IPv4 appartenant à une session NAT64 particulière, elle utilise les informations stockées dans la session NAT64 pour traduire le paquet IPv4 en paquet IPv6, puis envoie le paquet de réponse IPv6 à l'abonné.

Exemple : Flux de trafic du déploiement NAT64 et DNS64

Prenons un exemple de déploiement à grande échelle NAT64 et DNS64 comprenant l'appliance Citrix ADC NS-1 et deux serveurs DNS locaux, DNS-1 et DNS-2, dans le réseau central d'un fournisseur de services Internet, et l'abonné IPv6 SUB-1. SUB-1 est connecté à NS-1 via le réseau d'accès IPv6 du FAI. NS-1 comprend des configurations NAT64 et DNS64 à grande échelle pour permettre la communication entre les hôtes SUB-1 de l'abonné IPv6 et IPv4 (internes et externes).

La configuration NAT64 à grande échelle comprend un préfixe NAT64 (2001:DB8:300::/96) et un pool NAT IPv4 pour la traduction des requêtes IPv6 en requêtes IPv4 et des réponses IPv4 aux réponses IPv6.

La configuration DNS64 inclut un serveur virtuel d'équilibrage de charge DNS LBVS-DNS64-1 (2001:DB8:9999::99) et un préfixe DNS64 (2001:DB8:300::/96). LBVS-DNS64-1 représente le serveur DNS local DNS-1 et DNS-2 aux abonnés du FAI. Le préfixe DNS64, qui a la même valeur que le préfixe NAT64, est utilisé pour synthétiser les enregistrements DNS AAAA à partir des enregistrements DNS A reçus des serveurs DNS DNS-1 et DNS-2. NS-1 répond avec un enregistrement AAAA synthétisé à SUB-1 pour une requête DNS pour résoudre un hôte IPv4.



Flux de trafic DNS64

Le trafic entre l'abonné IPv6 SUB-1 et le site`www.example.com`, qui réside sur un serveur Web IPv4 uniquement sur Internet, comme suit :

1. L'abonné IPv6 SUB-1 envoie une requête DNS AAAA`www.example.com` à son serveur DNS désigné (2001:DB8:9999::99).
2. Serveur virtuel d'équilibrage de charge DNS LBVS-DNS64-1 (2001:DB8:9999::99) sur l'appliance Citrix ADC NS1 reçoit la demande AAAA. L'algorithme d'équilibrage de charge de LBVS-DNS64-1

sélectionne le serveur DNS DNS-1 et lui transmet la requête AAAA.

3. DNS-1 renvoie un enregistrement vide ou un message d'erreur, car il n'y a pas d'enregistrement AAAA disponible pour`www.example.com`.
4. Étant donné que l'option DNS64 est activée sur LBVS-DNS64-1 et que la requête AAAA de CL1 correspond à la condition spécifiée dans DNS64-Policy-1, NS1 envoie une demande DNS A à DNS-1 pour l'adresse IPv4 de`www.example.com`.
5. DNS-1 répond avec l'enregistrement A de 192.0.2.60 pour`www.example.com`.
6. Le module DNS64 sur NS1 synthétise un enregistrement AAAA pour `www.example.com` en concaténant le préfixe DNS64 (2001:DB8:300::/96) associé à LBVS-DNS64-1, et l'adresse IPv4 (192.0.2.60) pour `www.example.com` = 2001:DB8:300::192.0.2.60
7. NS1 envoie l'enregistrement AAAA synthétisé au client IPv6 CL1. NS1 met également en cache l'enregistrement A dans sa mémoire. NS1 utilise l'enregistrement A mis en cache pour synthétiser les enregistrements AAAA pour les requêtes AAAA suivantes.

NAT64 Flux de trafic

1. L'abonné IPv6 SUB-1 envoie une requête à 2001:DB8:5001:30 `www.example.com`. Le paquet IPv6 a :
   - Adresse IP source = 2001:DB8:5001:30
   - Port source = 2552
   - Adresse IP de destination = 2001:DB8:300::192.0.2.60
   - Port de destination = 80
2. L'abonné IPv6 SUB-1 envoie une requête à 2001:DB8:5001:30 `www.example.com`. Le paquet IPv6 a :
   - Adresse IP source = 2001:DB8:5001:30
   - Port source = 2552
   - Adresse IP de destination = 2001:DB8:300::192.0.2.60
   - Port de destination = 80
3. Lorsque NS-1 reçoit le paquet IPv6, le module NAT64 à grande échelle crée un paquet de requête IPv4 traduit avec :
   - Adresse IP source = Une des adresses IPv4 disponibles dans le pool NAT configuré (203.0.113.61)
   - Port source = Un des ports disponibles avec l'adresse NAT IPv4 allouée (3002)
   - Adresse IP de destination = adresse IPv4 extraite de l'adresse de destination de la requête IPv6 en dénuant le préfixe NAT64 (2001:DB8:300::/96) de l'adresse IPv6 (192.0.2.60)
   - Port de destination = port de destination de la requête IPv6 (80)
4. Le module NAT64 à grande échelle crée également des entrées de mappage et de session pour

ce flux NAT64 à grande échelle. Les entrées de session et de mappage contiennent les informations suivantes :

- Adresse IP source du paquet IPv6 = 2001:DB 8:5001:30
- Port source du paquet IPv6 = 2552
- Adresse IP NAT = 203.0.113.61
- Port NAT = 3002
- NS-1 envoie le paquet IPv4 obtenu à sa destination sur Internet.

5. À la réception du paquet de requête, le serveur pour`www.example.com` traite le paquet et envoie un paquet de réponse à NS-1. Le paquet de réponse IPv4 a :

   - Adresse IP source = 192.0.2.60
   - Port source = 80
   - Adresse IP de destination = 203.0.113.61
   - Port de destination = 3002

6. Lors de la réception du paquet de réponse IPv4, NS-1 examine le mappage et les entrées de session NAT64 à grande échelle et trouve que le paquet de réponse IPv4 appartient à une session NAT64 à grande échelle. Le module NAT64 à grande échelle crée un paquet de réponse IPv6 traduit :

   - Adresse IP source = 2001:DB8:300::192.0.2.60
   - Port source = 80
   - Adresse IP de destination = 2001:DB 8:5001:30
   - Port de destination = 2552

7. NS-1 envoie la réponse IPv6 traduite au client SUB-1.

Fonctionnalités NAT64 à grande échelle prises en charge sur les appliances Citrix ADC

NAT64 à grande échelle sur une appliance Citrix ADC prend en charge le jeu de fonctionnalités LSN standard. Pour plus d'informations sur ces fonctionnalités LSN, voir Architecture LSN.

Voici quelques-unes des fonctionnalités NAT64 à grande échelle prises en charge sur les appliances Citrix ADC :

- ALG. Prise en charge de l'application Layer Gateway (ALG) pour les protocoles SIP, RTSP, FTP, ICMP et TFTP.
- NAT déterministique/fixe. Prise en charge de la pré-allocation de blocs de ports aux abonnés pour minimiser la journalisation.
- Cartographie. Prise en charge du mappage indépendant du point de terminaison (EIM), du mappage dépendant de l'adresse (ADM) et du mappage dépendant du port d'adresse (APDM).
- Filtrage. Prise en charge du filtrage indépendant des points de terminaison (EIF), du filtrage dépendant des adresses (ADF) et du filtrage dépendant des ports d'adresses (APDF).

- Quotas. Limites configurables du nombre de ports, de sessions par abonné et de sessions par groupe LSN.
- Mappage statique. Prise en charge de la définition manuelle d'une cartographie NAT64 à grande échelle.
- Épingle à cheveux Flow. Prise en charge de la communication entre les abonnés ou les hôtes internes à l'aide d'adresses IP NAT.
- 464XLAT connexions. Prise en charge de la communication entre les applications IPv4 uniquement sur les hôtes d'abonnés IPv6 et les hôtes IPv4 sur Internet via le réseau IPv6.
- Préfixes de longueur variable NAT64 et DNS64. L'appliance Citrix ADC prend en charge la définition de préfixes NAT64 et DNS64 de longueurs 32, 40, 48, 56, 64 et 96.
- Plusieurs préfixe NAT64 et DNS64. L'appliance Citrix ADC prend en charge plusieurs préfixes NAT64 et DNS64.
- Clients LSN. Prise en charge de la spécification ou de l'identification des abonnés pour NAT64 à grande échelle à l'aide de préfixes IPv6 et de règles ACL6 étendues.
- Journalisation. Support pour l'enregistrement des sessions NAT64 pour l'application de la loi. En outre, les éléments suivants sont également pris en charge pour la journalisation.
  - **SYSLOG fiable**. Prise en charge de l'envoi de messages SYSLOG via TCP à des serveurs de journaux externes pour un mécanisme de transport plus fiable.
  - **Équilibrage de charge des serveurs de journaux**. Prise en charge de l'équilibrage de charge des serveurs de journaux externes pour empêcher le stockage des messages de journaux redondants.
  - **Journalisation minimale**. Les configurations LSN déterministes ou les configurations LSN dynamique avec bloc de port réduisent considérablement le volume de journal NAT64 à grande échelle.
  - **Journalisation des informations MSISDN**. Prise en charge de l'inclusion des informations MSISDN des abonnés dans les journaux NAT64 à grande échelle afin d'identifier et de suivre l'activité des abonnés sur Internet.

Points à prendre en considération pour la configuration de Large Scale NAT64

January 21, 2021

Avant de commencer à configurer NAT64 et DNS64 à grande échelle, tenez compte des points suivants :

1. Assurez-vous de bien comprendre les différents composants du NAT64 à grande échelle, décrits dans les RFC.
2. L'appliance Citrix ADC prend en charge uniquement les ALG suivantes pour les NAT64 à grande échelle :

- FTP
- TFTP
- ICMP
- SIP
- RTSP

3. Dans une configuration haute disponibilité de deux appliances Citrix ADC, la synchronisation de session NAT64 volumineuse (mise en miroir de connexion) n'est pas prise en charge.

Configuration de DNS64

August 20, 2021

La création des entités requises pour la configuration NAT64 avec état sur l'appliance Citrix ADC implique les procédures suivantes :

- Ajouter des services DNS. Les services DNS sont des représentations logiques de serveurs DNS pour lesquels l'appliance Citrix ADC agit en tant que serveur proxy DNS. Pour plus d'informations sur la définition des paramètres facultatifs d'un service, voir Équilibrage de charge.
- Ajouter une action DNS64 et une stratégie DNS64, puis liez l'action DNS64 à la stratégie DNS64. Une stratégie DNS64 spécifie les conditions à mettre en correspondance avec le trafic pour le traitement DNS64 en fonction des paramètres de l'action DNS64 associée. L'action DNS64 spécifie le préfixe DNS64 obligatoire et les paramètres facultatifs de règle d'exclusion et de règle mappée.
- Créez un serveur virtuel d'équilibrage de charge DNS et liez les services DNS et la stratégie DNS64 à celui-ci. Le serveur virtuel d'équilibrage de charge DNS agit comme un serveur proxy DNS pour les serveurs DNS représentés par les services DNS liés. Le trafic arrivant sur le serveur virtuel est mis en correspondance avec la stratégie DNS64 liée pour le traitement DNS64. Pour plus d'informations sur la définition des paramètres facultatifs d'un serveur virtuel d'équilibrage de charge, voir Équilibrage de charge.

> **Remarque**
>
> L'interface de ligne de commande comporte des commandes distinctes pour ces deux tâches, mais l'interface graphique les combine dans une seule boîte de dialogue.

- Activer la mise en cache des enregistrements DNS. Activez le paramètre global de l'appliance Citrix ADC pour mettre en cache les enregistrements DNS, qui sont obtenus via des opérations de proxy DNS. Pour plus d'informations sur l'activation de la mise en cache des enregistrements DNS, consultez Activation de la mise en cache des enregistrements DNS.

Pour créer un service de type DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <name> <IP> <serviceType> <port> …
<!--NeedCopy-->
```

Pour créer une action DNS64 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add dns action64 <actionName> -Prefix <ipv6_addr|*> [-mappedRule <
    expression>] [-excludeRule <expression>]
<!--NeedCopy-->
```

Pour créer une stratégie DNS64 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add dns policy64 <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Pour créer un serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb vserver <name> DNS <IPAddress> <port> -dns64 (ENABLED | DISABLED
    ) [-bypassAAAA ( YES | NO)] …
<!--NeedCopy-->
```

Pour lier les services DNS et la stratégie DNS64 au serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb vserver <name> <serviceName> ...

bind lb vserver <name> -policyName <string> -priority <positive_integer
    > ...
<!--NeedCopy-->
```


Exemple de configuration :

```
add service SVC-DNS-1 203.0.113.50 DNS 53
Done
add service SVC-DNS-2 203.0.113.60 DNS 53
Done
add dns Action64 DNS64-Action-1 -Prefix 2001:DB8:300::/96
Done
add dns Policy64 DNS64-Policy-1 -rule "CLIENT.IPv6.SRC.IN_SUBNET(2001:
   DB8:5001::/64)" -action DNS64-Action-1
Done
add lb vserver LBVS-DNS64-1 DNS 2001:DB8:9999::99 53 -dns64 ENABLED
Done
bind lb vserver LBVS-DNS64-1 SVC-DNS-1
Done
bind lb vserver LBVS-DNS64-1 SVC-DNS-2
Done
bind lb vserver LBVS-DNS64-1 -policyname DNS64-Policy-1 -priority 2
Done
<!--NeedCopy-->
```

Configuration de Large Scale NAT64

August 20, 2021

Une configuration NAT64 à grande échelle sur une appliance Citrix ADC utilise les jeux de commandes LSN. Dans une configuration NAT64 à grande échelle, l'entité client LSN spécifie l'adresse IPv6 ou l'adresse réseau IPv6, ou les règles ACL6, pour identifier les abonnés IPv6. Une configuration NAT64 inclut également un profil IPv6, qui spécifie un préfixe NAT64.

La configuration de NAT64 sur une appliance Citrix ADC comporte les tâches suivantes :

- Définissez les paramètres LSN globaux. Les paramètres globaux incluent la quantité de mémoire Citrix ADC réservée à la fonctionnalité LSN et la synchronisation des sessions LSN dans une configuration haute disponibilité.
- Créez une entité client LSN pour identifier le trafic provenant d'abonnés IPv6. L'entité client LSN fait référence à un ensemble d'abonnés IPv6. L'entité client inclut des adresses IPv6 ou des préfixes réseau IPv6, ou des règles ACL6, pour identifier le trafic de ces abonnés. Un client LSN peut être lié à un seul groupe LSN. L'interface de ligne de commande comporte deux commandes pour créer une entité client LSN et lier un abonné à l'entité client LSN. L'interface graphique combine ces deux opérations sur un seul écran.

- Créez un pool LSN et liez des adresses IP NAT à celui-ci. Un pool LSN définit un pool d'adresses IP NAT à utiliser par l'appliance Citrix ADC pour exécuter NAT64 à grande échelle. L'interface de ligne de commande comporte deux commandes permettant de créer un pool LSN et de lier les adresses IP NAT au pool LSN. L'interface graphique combine ces deux opérations sur un seul écran.
- Créez un profil LSN IP6. Un profil LSN IP6 définit le préfixe NAT64 pour une configuration NAT64 à grande échelle.
- (Facultatif) Créez un profil de transport LSN pour un protocole spécifié. Un profil de transport LSN définit divers délais d'expiration et limites, tels que le maximum de sessions NAT64 à grande échelle et l'utilisation maximale des ports qu'un abonné peut avoir pour un protocole donné. Vous liez un profil de transport LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil de transport LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP est lié à un groupe LSN lors de sa création. Ce profil est appelé profil de transport par défaut. Un profil de transport LSN que vous liez à un groupe LSN remplace le profil de transport LSN par défaut pour ce protocole.
- (Facultatif) Créez un profil d'application LSN pour un protocole spécifié et liez un ensemble de ports de destination à celui-ci. Un profil d'application LSN définit les contrôles de mappage LSN et de filtrage LSN d'un groupe pour un protocole donné et pour un ensemble de ports de destination. Pour un ensemble de ports de destination, vous liez un profil LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil d'application LSN lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil d'application LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP pour tous les ports de destination est lié à un groupe LSN lors de sa création. Ce profil est appelé profil d'application par défaut. Lorsque vous liez un profil d'application LSN, avec un ensemble de ports de destination spécifié, à un groupe LSN, le profil lié remplace le profil d'application LSN par défaut pour ce protocole sur cet ensemble de ports de destination. L'interface de ligne de commande comporte deux commandes pour créer un profil d'application LSN et lier un ensemble de ports de destination au profil d'application LSN. L'interface graphique combine ces deux opérations sur un seul écran.
- Créez un groupe LSN et liez des pools LSN, un profil IPv6 LSN, des profils de transport LSN (facultatif) et (facultatif) des profils d'application LSN au groupe LSN. Un groupe LSN est une entité composée d'un client LSN, d'un profil IPv6 LSN, de pools LSN, de profils de transport LSN et de profils d'application LSN. Des paramètres sont attribués à un groupe, tels que la taille du bloc de port et la journalisation des sessions LSN. Les paramètres s'appliquent à tous les abonnés d'un client LSN lié au groupe LSN. Un seul profil LSN IPv6 peut être lié à un groupe LSN, et un profil LSN IPv6 lié à un groupe LSN ne peut pas être lié à d'autres groupes LSN. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés ensemble. Plusieurs pools LSN peuvent être liés à un groupe LSN. Une seule entité client LSN peut

être liée à un groupe LSN, et une entité client LSN liée à un groupe LSN ne peut pas être liée à d'autres groupes LSN. L'interface de ligne de commande comporte deux commandes pour créer un groupe LSN et lier des pools LSN, des profils de transport LSN et des profils d'application LSN au groupe LSN. L'interface graphique combine ces deux opérations dans un seul écran.

Configuration à l'aide de la ligne de commande

Vous pouvez créer différentes configurations à l'aide de l'interface de ligne de commande. Suivez les étapes ci-dessous.

Pour créer un client LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn client <clientname

show lsn client
<!--NeedCopy-->
```

Pour lier un réseau IPv6 ou une règle ACL6 à un client LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn client <clientname> (-network6 <ipv6_addr|*>| -acl6name <
   string>)

show lsn client
<!--NeedCopy-->
```

Pour créer un pool LAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn pool <poolname>

show lsn pool <poolname>
<!--NeedCopy-->
```


Pour lier des adresses IP NAT à un pool LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

> **Remarque**
>
> Pour supprimer des adresses IP NAT (adresses IP LSN) d'un pool LSN, utilisez la commande unbind lsn pool.

Pour configurer un profil LSN IPv6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn ip6profile <name>  -type NAT64 -natprefix <ipv6_addr|*>

show lsn ip6profile
<!--NeedCopy-->
```

Pour créer un profil de transport LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```

Pour créer un profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )]

```



```
show lsn appsprofile
<!--NeedCopy-->
```

Pour lier une plage de ports de protocole d'application à un profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

Pour créer un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC |
    DETERMINISTIC )] [-portblocksize <positive_integer>] [-logging(
    ENABLED | DISABLED )] [-sessionLogging ( ENABLED | DISABLED )][-
    sessionSync ( ENABLED | DISABLED )] [-snmptraplimit<positive_integer
    >] [-ftp ( ENABLED | DISABLED )] [-sipalg ( ENABLED | DISABLED )] [-
    rtspalg ( ENABLED |DISABLED )] [-ip6profile <string>]

show lsn group
<!--NeedCopy-->
```

Pour lier des profils de protocole LSN et des pools LSN à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -httphdrlogprofilename <string> | -appsprofilename <
    string> | -sipalgprofilename <string> | rtspalgprofilename <string>)

show lsn group
<!--NeedCopy-->
```

Exemple de configurations NAT64 à grande échelle

Voici quelques exemples de configurations de NAT64 à grande échelle :

Configuration simple à grande échelle NAT64 avec paramètres par défaut :

```
add lsn client LSN-NAT64-CLIENT-1

bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96

add lsn pool LSN-NAT64-POOL-1

bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70

add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96

add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1

bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1

<!--NeedCopy-->
```

Configuration simple à grande échelle NAT64 avec une règle ACL6 étendue pour identifier les abonnés :

```
add ns acl6 LSN-NAT64-ACL-2 ALLOW  - srcIPv6 = 2001:DB8:5002::20 - 2001:
    DB8:5002::200

apply acl6s

add lsn client LSN-NAT64-CLIENT-2

bind lsn client LSN-NAT64-CLIENT-2  - acl6name LSN-NAT64-ACL-2

add lsn pool LSN-NAT64-POOL-2

bind lsn pool LSN-NAT64-POOL-2 203.0.113.5-203.0.113.10

add lsn ip6profile LSN-NAT64-PROFILE-2 -type NAT64 -natprefix 2001:DB8
    :302::/96

add lsn group LSN-NAT64-GROUP-2 -clientname LSN-NAT64-CLIENT-2 -
    ip6profile LSN-NAT64-PROFILE-2

bind lsn group LSN-NAT64-GROUP-2 -poolname LSN-NAT64-POOL-2

<!--NeedCopy-->
```


Configuration NAT64 à grande échelle avec allocation déterministe des ressources NAT :

```
add lsn client LSN-NAT64-CLIENT-7

bind lsn client LSN-NAT64-CLIENT-7 -network6 2001:DB8:1002::7/128

add lsn pool LSN-NAT64-POOL-7 -nattype DETERMINISTIC

bind lsn pool LSN-NAT64-POOL-7 203.0.113.24-203.0.113.27

add lsn ip6profile LSN-NAT64-PROFILE-7 -type NAT64 -natprefix 2001:DB8
   :307::/96

add lsn group LSN-NAT64-GROUP-7 -clientname LSN-NAT64-CLIENT-7 -
   ip6profile LSN-NAT64-PROFILE-7 -nattype DETERMINISTIC -portblocksize
    256

bind lsn group LSN-NAT64-GROUP-7 -poolname LSN-POOL-7

<!--NeedCopy-->
```

Configuration des passerelles de couche d'application pour Large Scale NAT64

January 21, 2021

Pour certains protocoles de couche Application, les adresses IP et les numéros de port de protocole sont également communiqués dans la charge utile du paquet. Application Layer Gateway for a protocol analyse la charge utile du paquet et effectue les modifications nécessaires pour s'assurer que le protocole continue de fonctionner sur NAT64 à grande échelle.

L'appliance Citrix ADC prend en charge ALG pour les protocoles suivants pour NAT64 à grande échelle :

- FTP
- ICMP
- TFTP
- SIP
- RTSP

Passerelle de couche d'application pour les protocoles FTP, ICMP et TFTP

January 21, 2021

Vous pouvez activer ou désactiver ALG pour le protocole FTP pour une configuration NAT64 à grande échelle en activant ou en désactivant l'option ALG FTP du groupe LSN de la configuration.

ALG pour le protocole ICMP est activé par défaut et aucune disposition ne permet de le désactiver.

ALG pour le protocole TFTP est désactivé par défaut. TFTP ALG est activé automatiquement pour une configuration NAT64 à grande échelle lorsque vous liez un profil d'application UDP LSN, avec mappage indépendant du point de terminaison, filtrage indépendant du point de terminaison et port de destination 69 (port bien connu pour TFTP), au groupe LSN.

Passerelle de couche d'application pour le protocole SIP

January 21, 2021

L'utilisation de Large Scale NAT64 avec Session Initiation Protocol (SIP) est compliquée, car les messages SIP contiennent des adresses IP dans les en-têtes SIP ainsi que dans le corps SIP. Lorsque LSN est utilisé avec SIP, les en-têtes SIP contiennent des informations sur l'appelant et le récepteur, et le périphérique traduit ces informations pour les masquer du réseau externe. Le corps SIP contient les informations SDP (Session Description Protocol), qui comprennent les adresses IP et les numéros de port pour la transmission du média. SIP ALG pour grande échelle NAT64 est conforme aux RFC 3261, RFC 3581, RFC 4566 et RFC 4475.

> **Remarque**
>
> SIP ALG est pris en charge dans une appliance autonome Citrix ADC, dans une configuration de haute disponibilité Citrix ADC, ainsi que dans une configuration de cluster Citrix ADC.

Limites de SIP ALG

SIP ALG pour grande échelle NAT64 a les limitations suivantes :

- Seule la charge utile SDP est prise en charge.
- Les éléments suivants ne sont pas pris en charge :
  - Adresses IP de multidiffusion
  - SDP chiffré
  - SIP TLS

- Traduction de FQDN
- Authentification de la couche SIP
- Domaines de trafic
- Partitions d'administration
- Corps en plusieurs parties
- Réassemblage de lignes

Configuration de SIP ALG

Vous devez configurer le SIP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration de LSN, reportez-vous à Configuration Large Scale NAT64. Lors de la configuration de LSN, assurez-vous que vous :

- Définissez les paramètres suivants lors de l'ajout d'un profil d'application LSN :
  - IP Pooling = PAIRED
  - Address and Port Mapping = ENDPOINT-INDEPENDENT
  - Filtering = ENDPOINT-INDEPENDENT
- Créez un profil ALG SIP et assurez-vous de définir la plage de ports source ou la plage de ports de destination. Liez le profil ALG SIP au groupe LSN.
- Activez SIP ALG dans le groupe LSN.

Pour activer SIP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn group <groupname> -clientname <string> [-sipalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

Pour activer SIP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn sipalgprofile <sipalgprofilename>[-dataSessionIdleTimeout <
    positive_integer>][-sipSessionTimeout <positive_integer>] [-
    registrationTimeout <positive_integer>] [-sipsrcportrange <port[-
    port]>] [-sipdstportrange <port[-port]>] [-openRegisterPinhole (
    ENABLED | DISABLED )] [-openContactPinhole ( ENABLED | DISABLED )]
    [-openViaPinhole ( ENABLED | DISABLED )] [-openRecordRoutePinhole (
    ENABLED | DISABLED )]-sipTransportProtocol ( TCP | UDP ) [-
```



```
    openRoutePinhole ( ENABLED | DISABLED )] [-rport ( ENABLED |
    DISABLED )]
2
3 show lsn sipalgprofile <sipalgprofilename
4 <!--NeedCopy-->
```

Exemple de configuration

L'exemple suivant de configuration NAT64 à grande échelle, SIP ALG est activé pour le trafic TCP à partir de périphériques abonnés dans le réseau 2001:DB8:1003::/96.

```
1  add lsn client LSN-NAT64-CLIENT-9
2
3  Done
4  bind lsn client LSN-NAT64-CLIENT-9 -network6 2001:DB8:1002::/96
5
6  Done
7  add lsn pool LSN-NAT64-POOL-9
8
9  Done
10 bind lsn pool LSN-NAT64-POOL-9 203.0.113.90
11
12 Done
13 add lsn ip6profile LSN-NAT64-PROFILE-9 -type NAT64 -natprefix 2001:DB8
       :309::/96
14
15 Done
16 add lsn appsprofile LSN-NAT64-APPS-PROFILE-9 TCP -ippooling PAIRED -
       mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
17
18 Done
19 add lsn sipalgprofile SIPALGPROFILE-9  -sipdstportrange 5060  -
       sipTransportProtocol TCP
20
21 Done
22 add lsn group LSN-NAT64-GROUP-9 -clientnameLSN-NAT64-CLIENT-9 -
       ip6profile LSN-NAT64-PROFILE-7 -sipalg ENABLED
23
24 Done
25 bind lsn group LSN-NAT64-GROUP-9 -poolnameLSN-NAT64-POOL-9
26 Done
27 bind lsn group LSN-NAT64-GROUP-9 -appsprofilename LSN-NAT64-APPS-
       PROFILE-9
28 Done
```



```
29 bind lsn group LSN-NAT64-GROUP-9 -sipalgprofilename SIPALGPROFILE-9
30 Done
31 <!--NeedCopy-->
```

Passerelle de couche d'application pour le protocole RTSP

January 21, 2021

Le protocole RTSP (Real Time Streaming Protocol) est un protocole au niveau de l'application pour le transfert de données multimédia en temps réel. Utilisé pour établir et contrôler des sessions multimédias entre les points de fin, RTSP est un protocole de canal de contrôle entre le client multimédia et le serveur multimédia. La communication typique est entre un client et un serveur multimédia de streaming.

La diffusion de médias à partir d'un réseau privé vers un réseau public nécessite la traduction des adresses IP et des numéros de port sur le réseau. La fonctionnalité Citrix ADC comprend une passerelle de couche d'application (ALG) pour RTSP, qui peut être utilisée avec le NAT à grande échelle (LSN) pour analyser le flux de médias et apporter les modifications nécessaires pour garantir que le protocole continue de fonctionner sur le réseau.

La manière dont la traduction d'adresses IP est effectuée dépend du type et de la direction du message, ainsi que du type de support pris en charge par le déploiement client-serveur. Les messages sont traduits comme suit :

- Demande sortante : adresse IP privée vers une adresse IP publique appartenant à Citrix ADC appelée adresse IP LSN.
- Réponse entrante : adresse IP LSN vers adresse IP privée.
- Demande entrante : aucune traduction.
- Réponse sortante : adresse IP privée à l'adresse IP du pool LSN.

> **Remarque**
>
> RTSP ALG est pris en charge dans une appliance autonome Citrix ADC, dans une configuration de haute disponibilité Citrix ADC, ainsi que dans une configuration de cluster Citrix ADC.

Limites de l'ALG RTSP

Le RTSP ALG ne prend pas en charge les éléments suivants :

- Sessions RTSP multidiffusion
- Session RTSP via UDP
- Partitions d'administration

- Authentification RTSP
- Tunneling HTTP

Configuration de RTSP ALG

Configurez RTSP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration de LSN, reportez-vous à la section Configuration de la NAT64 à grande échelle. Lors de la configuration, assurez-vous que vous :

- Définissez les paramètres suivants lors de l'ajout d'un profil d'application LSN :
  - IP Pooling = PAIRED
  - Address and Port Mapping = ENDPOINT-INDEPENDENT
  - Filtering = ENDPOINT-INDEPENDENT
- Activer RTSP ALG dans le groupe LSN
- Créer un profil ALG RTSP et lier le profil ALG RTSP au groupe LSN

Pour activer RTSP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn group <groupname> -clientname <string> [-rtspalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

Pour activer RTSP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn rtspalgprofile <rtspalgprofilename> [-rtspIdleTimeout <
    positive_integer>] -rtspportrange <port[-port]> [-
    rtspTransportProtocol (TCP|UDP)]

show lsn rtspalgprofile <rtspalgprofilename>
<!--NeedCopy-->
```

Exemple de configuration ALG RTSP

L'exemple suivant de configuration NAT64 à grande échelle, RTSP ALG est activé pour le trafic TCP à partir de périphériques abonnés dans le réseau 2001:DB8:1002::/96.


```
add lsn client LSN-NAT64-CLIENT-9
Done
bind lsn client LSN-NAT64-CLIENT-9 -network6 2001:DB8:1002::/96
Done
add lsn pool LSN-NAT64-POOL-9
Done
bind lsn pool LSN-NAT64-POOL-9 203.0.113.90
Done
add lsn ip6profile LSN-NAT64-PROFILE-9 -type NAT64 -natprefix 2001:DB8
   :309::/96
Done
add lsn appsprofile LSN-NAT64-APPS-PROFILE-9 TCP -ippooling PAIRED -
   mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn rtspalgprofile RTSPALGPROFILE-9 -rtspIdleTimeout 1000 -
   rtspportrange 554
Done
add lsn group LSN-NAT64-GROUP-9 -clientname LSN-NAT64-CLIENT-9 -
   ip6profile LSN-NAT64-PROFILE-7 -rtspalg ENABLED
Done
bind lsn group LSN-NAT64-GROUP-9 -poolname LSN-NAT64-POOL-9
Done
bind lsn group LSN-NAT64-GROUP-9 -appsprofilename LSN-NAT64-APPS-
   PROFILE-9
Done
bind lsn group LSN-NAT64-GROUP-9  -rtspalgprofilename RTSPALGPROFILE-9
Done
<!--NeedCopy-->
```

Configuration de cartes statiques Large Scale NAT64

January 21, 2021

L'appliance Citrix ADC prend en charge la création manuelle de mappages NAT64, qui contiennent le mappage entre les informations suivantes :

- Adresse IP et port de l'abonné
- Adresse IP NAT et port

Les mappages NAT64 statiques à grande échelle sont utiles dans les cas où vous voulez vous assurer que les connexions IPv4 initiées à une adresse IP NAT:port sont traduites IPv6 et mappées à l'adresse IP de l'abonné : port (par exemple, les serveurs Web situés dans le réseau interne).

Pour créer un mappage NAT64 à grande échelle à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort>  [<
    natIP> [<natPort>]] [-destIP <ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```

Mappings de port génériques statiques à grande échelle NAT64

Une entrée de mappage statique à grande échelle NAT64 est généralement un mappage un-à-un entre une adresse IPv6 abonné : port et une adresse IPv4 NAT : port. Une entrée de mappage statique à grande échelle NAT64 n'expose qu'un seul port de l'adresse IP de l'abonné à Internet.

Certaines situations peuvent nécessiter l'exposition à Internet de tous les ports (64 Ko - limité au nombre maximal de ports d'une adresse IP NAT IPv4) d'une adresse IP d'abonné (par exemple, un serveur hébergé sur un réseau interne et exécutant un service différent sur chaque port). Pour rendre ces services internes accessibles via Internet, vous devez exposer tous les ports du serveur à Internet.

Une façon de répondre à cette exigence consiste à ajouter 64 000 entrées de mappage statiques un-à-un, une entrée de mappage pour chaque port. La création de ces entrées est très lourde et une tâche importante. En outre, ce grand nombre d'entrées de configuration peut entraîner des problèmes de performances dans l'appliance Citrix ADC.

Une méthode plus simple consiste à utiliser des ports génériques dans une entrée de mappage statique. Vous avez juste besoin de créer une entrée de mappage statique avec les paramètres de port NAT et de port d'abonné définis sur le caractère générique (*), et le paramètre de protocole défini sur ALL, pour exposer tous les ports d'une adresse IP d'abonné pour tous les protocoles à Internet.

Pour les connexions entrantes ou sortantes d'un abonné correspondant à une entrée de mappage statique générique, le port de l'abonné ne change pas après l'opération NAT. Lorsqu'une connexion initiée par un abonné à Internet correspond à une entrée de mappage statique générique, l'appliance Citrix ADC attribue un port NAT portant le même numéro que le port d'abonné à partir duquel la connexion est initiée. De même, un hôte Internet est connecté au port d'un abonné en se connectant au port NAT qui a le même numéro que le port de l'abonné.

Pour configurer l'appliance Citrix ADC de manière à permettre l'accès à tous les ports d'une adresse IPv6 d'abonné, créez un mappage statique générique avec les paramètres obligatoires suivants :

- Protocol=ALL
- Port de l'abonné = *
- Port NAT = *

Dans un mapping statique générique, contrairement à un mapping statique un-à-un, la définition du paramètre IP NAT est obligatoire. En outre, l'adresse IP NAT attribuée à un mapping statique générique ne peut pas être utilisée pour d'autres abonnés.

Pour créer un mapping statique générique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lsn static <name> ALL <subscrIP> *  <natIP> * [-td <
     positive_integer>] [-destIP <ip_addr>
2
3 show lsn static
4 <!--NeedCopy-->
```

Dans l'exemple de configuration suivant d'un mappage statique générique, tous les ports d'un abonné dont l'adresse IP est 2001:DB8:5001::3 sont rendus accessibles via NAT IP 203.0.11.33.

```
1 add lsn static NAT64-WILDCARD-STATIC-1 ALL 2001:DB8:5001::3 *
     203.0.113.33 *
2 Done
3 <!--NeedCopy-->
```

Exploitation et surveillance Large Scale NAT64

August 20, 2021

Vous pouvez consigner des informations NAT64 à grande échelle pour diagnostiquer et dépanner les problèmes et répondre aux exigences légales. Vous pouvez surveiller les performances du déploiement NAT64 à grande échelle en utilisant des compteurs statistiques et en affichant les sessions en cours associées.

Journalisation à grande échelle NAT64

La consignation de l'information NAT64 à grande échelle est nécessaire pour que les FSI satisfassent aux exigences légales et identifient la source du trafic à tout moment.

Un message de journal pour une entrée de mappage NAT64 à grande échelle comprend les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal provient
- Horodatage.
- Type d'entrée (MAPPING).

- Indique si l'entrée de mappage a été créée ou supprimée.
- Adresse IP, port et ID de domaine de trafic de l'abonné.
- Adresse IP NAT et port.
- Nom du protocole.
- L'adresse IP de destination, le port et l'ID de domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
  - Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
  - L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse.

Un message de journal pour une session NAT64 à grande échelle comprend les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal est source
- Horodatage
- Type d'entrée (SESSION)
- Indique si la session est créée ou supprimée
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP NAT et port
- Nom du protocole
- Adresse IP de destination, port et ID de domaine de trafic

Le tableau suivant présente des exemples d'entrées de journal NAT64 à grande échelle de chaque type stockées sur les serveurs de journaux configurés. Les entrées du journal montrent qu'un abonné dont l'adresse IPv6 est 2001:db8:5001::9 a été connecté à la destination IP:Port 23.0.0.1:80 via NAT IP:Port 203.0.113.63:45195 le 7 avril 2016, de 14:07:57 GMT à 14:10:59 GMT.

Type d'entrée du journal	Exemple d'entrée de journal
Création de session	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_SESSION 5532 0 : SESSION CREATED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Type d'entrée du journal	Exemple d'entrée de journal
Création de mappage	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_ADDR_MAPPING 5533 0 : ADM CREATED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:TD 23.0.0.1:80, Protocol: TCP
Suppression de session	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_SESSION 25012 0 : SESSION DELETED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP
Suppression de mappage	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM DELETED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Étapes de configuration

Vous pouvez configurer la journalisation des informations NAT64 à grande échelle pour une configuration NAT64 à grande échelle en définissant les paramètres de journalisation et de journalisation de session des groupes LSN. Il s'agit de paramètres au niveau du groupe et sont désactivés par défaut. L'appliance Citrix ADC enregistre les sessions NAT64 à grande échelle pour un groupe LSN uniquement lorsque les paramètres de journalisation et de journalisation de session sont activés.

Le tableau suivant affiche le comportement de journalisation d'un groupe LSN pour différents paramètres de journalisation et de journalisation de session.

Journalisation	Journalisation de session	Comportement de journalisation
Activé	Activé	Consigne les entrées de mappage LSN ainsi que les sessions LSN
Activé	Désactivé	Consigne les entrées de mappage LSN mais pas les sessions LSN

Journalisation	Journalisation de session	Comportement de journalisation
Désactivé	Activé	Journalise ni les entrées de mappage ni les sessions LSN

Pour enregistrer des informations NAT64 à grande échelle à l'aide de l'interface de ligne de commande

Pour définir les paramètres de journalisation et de journalisation de session lors de l'ajout d'un groupe LSN, à l'invite de commandes, tapez :

```
add lsn group <groupname> -clientname <string> [-logging (ENABLED|
    DISABLED)] [-sessionLogging (ENABLED|DISABLED)]

show lsn group
<!--NeedCopy-->
```

Pour définir les paramètres de journalisation et de journalisation de session pour un groupe LSN existant, à l'invite de commandes, tapez :

```
set lsn group <groupname> [-logging (ENABLED|DISABLED)] [-
    sessionLogging (ENABLED|DISABLED)]

show lsn group
<!--NeedCopy-->
```

Exemple de configuration

Dans cet exemple de configuration NAT64 à grande échelle, les paramètres de journalisation et de journalisation de session sont activés pour le groupe LSN LSN-NAT64-GROUP-1.

L'appliance Citrix ADC enregistre les informations de session NAT64 à grande échelle et de mappage pour les connexions des abonnés (dans le réseau 2001:DB8:5001::/96).

Exemple de configuration :

```
add lsn client LSN-NAT64-CLIENT-1 Done
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
```



```
7  bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
8  Done
9  add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
       :300::/96
10 Done
11 add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
       ip6profile LSN-NAT64-PROFILE-1  -logging ENABLED -sessionLogging
       ENABLED
12 Done
13 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
14 Done
15 <!--NeedCopy-->
```

Journalisation des informations MSISDN pour NAT64 à grande échelle

Un numéro d'annuaire d'abonné intégré de station mobile (MSISDN) est un numéro de téléphone qui identifie de façon unique un abonné sur plusieurs réseaux mobiles. Le MSISDN est associé à un code de pays et à un code de destination national identifiant l'opérateur de l'abonné.

Vous pouvez configurer une appliance Citrix ADC pour inclure MSISDN dans les entrées de journal LSN NAT64 à grande échelle pour les abonnés des réseaux mobiles. La présence de MSISDN dans les journaux des LSN facilite un suivi plus rapide et précis d'un abonné mobile qui a enfreint une politique ou une loi, ou dont l'information est requise par les agences d'interception légales.

Les exemples d'entrées de journal LSN suivants incluent des informations MSISDN pour une connexion à partir d'un abonné mobile dans une configuration LSN. Les entrées de journal montrent qu'un abonné mobile dont MSISDN est E 164:5556543210 et l'adresse IPv6 est 2001:db 8:5001::9 a été connecté à la destination IP:Port 23.0.0. 1:80 via le NAT IP:Port 203.0.113. 63:45195 le 7 avril 2016, de 14:07:57 GMT à 14:10:59 GMT.

Type d'entrée du journal	Exemple d'entrée de journal
Création de session	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_SESSION 5532 0 : SESSION CREATED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Type d'entrée du journal	Exemple d'entrée de journal
Création de mappage	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_ADDR_MAPPING 5533 0 : ADM CREATED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:TD 23.0.0.1:80, Protocol: TCP
Suppression de session	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_SESSION 25012 0 : SESSION DELETED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP
Suppression de mappage	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM DELETED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Étapes de configuration

Effectuez les tâches suivantes pour inclure des informations MSISDN dans les journaux LSN :

- **Créez un profil de journal LSN**. Un profil de journal LSN inclut le paramètre ID d'abonné du journal, qui spécifie s'il faut ou non inclure les informations MSISDN dans les journaux LSN d'une configuration LSN.
- Liez le profil de journal LSN à un groupe LSN d'une configuration LSN. Liez le profil de journal LSN créé à un groupe LSN d'une configuration LSN en définissant le paramètre de nom de profil de journal sur le nom de profil de journal LSN créé. Les informations MSISDN sont incluses dans tous les journaux LSN relatifs aux abonnés mobiles de ce groupe LSN.

Pour créer un profil de journal LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn logprofile <logprofilename> -logSubscriberID ( ENABLED |
    DISABLED )

```



```
show lsn logprofile
<!--NeedCopy-->
```

Pour lier un profil de journal LSN à un groupe LSN d'une configuration NAT64 LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Exemple de configuration

Dans cet exemple de configuration LSN NAT64, le paramètre ID d'abonné du journal est activé dans le profil de journal LSNLOG-PROFILE-MSISDN-1. LOG-PROFILE-MSISDN-1 est lié au groupe LSN LSN-NAT64-GROUP-1. Les informations MSISDN sont incluses dans la session LSN et les journaux de mappage LSN pour les connexions des abonnés mobiles (dans le réseau 2001:DB8:5001::/96).

```
add lsn logprofile  LOG-PROFILE-MSISDN-1  -logSubscriberID ENABLED
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96
Done
add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1 -logprofilename  LOG-PROFILE-MSISDN-1
Done
<!--NeedCopy-->
```


Journalisation compacte pour NAT à grande échelle

L'enregistrement des informations sur les LSN est l'une des fonctions importantes dont ont besoin les FSI pour satisfaire aux exigences légales et être en mesure d'identifier la source du trafic à tout moment. Cela se traduit par un volume énorme de données de journal, ce qui oblige les fournisseurs de services Internet à faire d'importants investissements pour maintenir l'infrastructure de journalisation.

La journalisation compacte est une technique permettant de réduire la taille du journal en utilisant une modification notationnelle impliquant des codes courts pour les noms d'événements et de protocoles. Par exemple, C pour le client, SC pour la session créée et T pour TCP. La journalisation compacte entraîne une réduction moyenne de 40% de la taille des journaux.

Étapes de configuration

Effectuez les tâches suivantes pour consigner les informations LSN au format compact :

1. Créez un profil de journal LSN. Un profil de journal LSN inclut le paramètre Log Compact, qui spécifie s'il faut ou non enregistrer les informations au format compact pour une configuration LSN.
2. Liez le profil de journal LSN à un groupe LSN d'une configuration LSN. Liez le profil de journal LSN créé à un groupe LSN d'une configuration LSN en définissant le paramètre Log Profile Name sur le nom de profil de journal LSN créé. Toutes les sessions et mappages de ce groupe LSN sont enregistrés au format compact.

Pour créer un profil de journal LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn logprofile <logprofilename> -logCompact (ENABLED|DISABLED)

show lsn logprofile
<!--NeedCopy-->
```

Pour lier un profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname> -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```


Exemple de configuration pour NAT64 :

```
add lsn logprofile  LOG-PROFILE-COMPACT-1 -logCompact ENABLED
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96
Done
add lsn group LSN-NAT64-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1  - logProfileName LOG-PROFILE-COMPACT-1
Done
<!--NeedCopy-->
```

Journalisation des informations d'en-tête HTTP

L'appliance Citrix ADC peut consigner les informations d'en-tête de requête d'une connexion HTTP qui utilise la fonctionnalité Citrix ADC NAT64 à grande échelle. Les informations d'en-tête suivantes d'un paquet de requête HTTP peuvent être enregistrées :

- URL à laquelle la requête HTTP est destinée
- Méthode HTTP spécifiée dans la requête HTTP
- Version HTTP utilisée dans la requête HTTP
- Adresse IPv6 de l'abonné qui a envoyé la requête HTTP

Les journaux d'en-tête HTTP peuvent être utilisés par les FAI pour voir les tendances liées au protocole HTTP parmi un ensemble d'abonnés. Par exemple, un FAI peut utiliser cette fonctionnalité pour trouver le site Web le plus populaire parmi un ensemble d'abonnés.

Étapes de configuration

Effectuez les tâches suivantes pour configurer l'appliance Citrix ADC pour consigner les informations d'en-tête HTTP :

- Créez un profil de journal d'en-tête HTTP. Un profil de journal d'en-tête HTTP est un ensemble d'attributs d'en-tête HTTP (par exemple, URL et méthode HTTP) qui peuvent être activés ou désactivés pour la journalisation.
- Liez l'en-tête HTTP à un groupe LSN d'une configuration NAT64 à grande échelle. Liez le profil du journal des en-têtes HTTP à un groupe LSN d'une configuration LSN en définissant le paramètre nom du profil du journal des en-têtes HTTP sur le nom du profil du journal des en-têtes HTTP créé. L'appliance Citrix ADC consigne ensuite les informations d'en-tête HTTP de toutes les requêtes HTTP liées au groupe LSN. Un profil de journal d'en-tête HTTP peut être lié à plusieurs groupes LSN, mais un groupe LSN ne peut avoir qu'un seul profil de journal d'en-tête HTTP.

Pour créer un profil de journal d'en-tête HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
    DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
    ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

show lsn httphdrlogprofile
<!--NeedCopy-->
```

Pour lier un profil de journal d'en-tête HTTP à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```

Exemple de configuration

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1
Done
add lsn client LSN-NAT64-CLIENT-1 Done
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
```



```
10 Done
11 add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
      :300::/96
12 Done
13 add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
      ip6profile LSN-NAT64-PROFILE-1
14 Done
15 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
16 Done
17 bind lsn group LSN-NAT64-GROUP-1 -httphdrlogprofilename HTTP-HEADER-LOG
      -1
18 Done
19 <!--NeedCopy-->
```

Affichage des sessions NAT64 à grande échelle actuelles

Vous pouvez afficher les sessions NAT64 à grande échelle actuelles afin de détecter les sessions indésirables ou inefficaces sur l'appliance Citrix ADC. Vous pouvez afficher toutes ou certaines sessions NAT64 à grande échelle sur la base des paramètres de sélection.

> **Remarque**
>
> Lorsqu'il existe plus d'un million de sessions NAT64 à grande échelle sur l'appliance Citrix ADC, Citrix recommande d'utiliser les paramètres de sélection pour afficher les sessions NAT64 à grande échelle sélectionnées au lieu de les afficher toutes.

Pour afficher toutes les sessions NAT64 à grande échelle à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 show lsn session  -nattype NAT64
2 <!--NeedCopy-->
```

Pour afficher des sessions NAT64 sélectives à grande échelle à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 show lsn session  -nattype NAT64 [-network6 <ipv6_addr|*>] [-clientname
      <string>] [-natIP <ip_addr> [-natPort <port>]]
2 <!--NeedCopy-->
```


Affichage des statistiques NAT64 à grande échelle

Vous pouvez afficher des statistiques relatives au module NAT64 à grande échelle, et évaluer ses performances ou résoudre les problèmes. Vous pouvez afficher un résumé des statistiques de toutes les configurations NAT64 à grande échelle ou d'une configuration NAT64 à grande échelle particulière. Les compteurs statistiques reflètent les événements survenus depuis le dernier redémarrage de l'appliance Citrix ADC. Tous ces compteurs sont réinitialisés à 0 lorsque l'appliance Citrix ADC est redémarrée.

Pour afficher les statistiques totales de NAT64 à grande échelle à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat lsn nat64
<!--NeedCopy-->
```

Pour afficher les statistiques d'une configuration NAT64 à grande échelle spécifiée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat lsn group <groupname>
<!--NeedCopy-->
```

Effacement des sessions NAT64 à grande échelle

Vous pouvez supprimer toutes les sessions NAT64 à grande échelle indésirables ou inefficaces de l'appliance Citrix ADC. L'appliance libère immédiatement les ressources (telles que l'adresse IP NAT, le port et la mémoire) allouées à ces sessions, ce qui rend les ressources disponibles pour les nouvelles sessions. L'appliance supprime également tous les paquets suivants liés à ces sessions supprimées. Vous pouvez supprimer toutes les sessions NAT64 à grande échelle ou sélectionnées de l'appliance Citrix ADC.

Pour effacer toutes les sessions NAT64 à grande échelle à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
flush lsn session -nattype NAT64

```



```
show lsn session -nattype NAT64
<!--NeedCopy-->
```

Pour effacer les sessions NAT64 sélectives à grande échelle à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
flush lsn session -nattype NAT64 [-network6 <ipv6_addr|*>] [-
   clientname <string>] [-natIP <ip_addr> [-natPort <port>]]

show lsn session -nattype NAT64 [-network6 <ipv6_addr|*>] [-clientname
    <string>] [-natIP <ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Exemple de configuration :

Effacer toutes les sessions NAT64 à grande échelle existantes sur une appliance Citrix ADC

```
flush lsn session  -nattype NAT64
Done
<!--NeedCopy-->
```

Effacer toutes les sessions NAT64 à grande échelle liées à l'entité cliente LSN-NAT64-CLIENT-1

```
flush lsn session -nattype NAT64 -clientname LSN-NAT64-CLIENT-1
Done
<!--NeedCopy-->
```

Effacer toutes les sessions NAT64 à grande échelle liées à un réseau d'abonnés (2001:DB8:5001::/96) de l'entité client LSN LSN-NAT64-CLIENT-2

```
flush lsn session -nattype NAT64 -network6 2001:DB8:5001::/96 -
   clientname LSN-NAT64-CLIENT-2
Done
<!--NeedCopy-->
```

Journalisation IPFIX

L'appliance Citrix ADC prend en charge l'envoi d'informations sur les événements LSN au format IPFIX (Internet Protocol Flow Information Export) vers l'ensemble configuré de collecteurs IPFIX. L'appliance utilise la fonctionnalité AppFlow existante pour envoyer des événements LSN au format IPFIX aux collecteurs IPFIX.

La journalisation basée sur IPFIX est disponible pour les événements liés à NAT64 suivants :

- Création ou suppression d'une session LSN.
- Création ou suppression d'une entrée de mappage LSN.
- Allocation ou désallocation de blocs de ports dans le contexte d'un NAT déterministe.
- Allocation ou désallocation de blocs de ports dans le contexte de NAT dynamique.
- Chaque fois que le quota de session d'abonné est dépassé.

Points à considérer avant de configurer la journalisation IPFIX

Avant de commencer à configurer IPSec ALG, tenez compte des points suivants :

- Vous devez configurer la fonctionnalité AppFlow et les collecteurs IPFIX sur l'appliance Citrix ADC. Pour obtenir des instructions, reportez-vous à la section Configuration de la fonctionnalité AppFlow.

Étapes de configuration

Effectuez les tâches suivantes pour consigner les informations LSN au format IPFIX :

- **Activez la journalisation LSN dans la configuration AppFlow**. Activez le paramètre de journalisation LSN dans le cadre de la configuration AppFlow.
- **Créez un profil de journal LSN**. Un profil de journal LSN inclut le paramètre IPFIX qui active ou désactive les informations de journal au format IPFIX.
- **Liez le profil de journal LSN à un groupe LSN d'une configuration LSN**. Liez le profil de journal LSN à un ou plusieurs groupes LSN. Les événements liés au groupe LSN lié seront enregistrés au format IPFIX.

Pour activer la journalisation LSN dans la configuration AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set appflow param -lsnLogging ( ENABLED | DISABLED )

show appflow param
<!--NeedCopy-->
```

Pour créer un profil de journal LSN à l'aide de l'interface de ligne de commande, tapez

À l'invite de commandes, tapez :


```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Pour créer un profil de journal LSN à l'aide de l'interface graphique

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur onglet **Journal**, puis ajoutez un profil de journal.

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface graphique

1. Accédez à **Système** > **NAT à grande échelle** > **Groupe LSN,** ouvrez le groupe **LSN**.
2. Dans **Paramètres avancés,** cliquez sur **+ Profil du journal** pour lier le profil journal créé au groupe LSN.

Protocole de contrôle de port pour Large Scale NAT64

January 21, 2021

Les appliances Citrix ADC prennent désormais en charge le protocole PCP (Port Control Protocol) pour NAT à grande échelle (LSN). Bon nombre des applications abonnées d'un fournisseur de services Internet doivent être accessibles à partir d'Internet (par exemple, des appareils Internet des objets (IOT), comme une caméra IP qui assure la surveillance sur Internet). Une façon de répondre à cette exigence est de créer des mappings NAT (LSN) statiques à grande échelle. Mais pour un très grand nombre d'abonnés, la création de mappings NAT LSN statiques n'est pas une solution réalisable.

Port Control Protocol (PCP) permet à un abonné de demander des mappages NAT LSN spécifiques pour lui-même et/ou pour d'autres périphériques tiers. Le périphérique NAT à grande échelle crée un

mapping LSN et l'envoie à l'abonné. L'abonné envoie aux périphériques distants sur Internet l'adresse IP NAT : port NAT auquel ils peuvent se connecter à l'abonné.

Les applications envoient généralement des messages keep-alive fréquents au périphérique NAT à grande échelle afin que leurs mappages LSN ne s'écoule pas. PCP aide à réduire la fréquence de ces messages Keep-alive en permettant aux applications d'apprendre les paramètres de délai d'expiration des mappages LSN. Cela permet de réduire la consommation de bande passante sur le réseau d'accès du FAI et la consommation de batterie sur les appareils mobiles.

PCP est un modèle client-serveur qui fonctionne sur le protocole de transport UDP. Une appliance Citrix ADC implémente le composant serveur PCP et est conforme à la RFC 6887.

Étapes de configuration

Effectuez les tâches suivantes pour configurer PCP :

- **(Facultatif) Créez un profil PCP**. Un profil PCP inclut des paramètres pour les paramètres associés à PCP (par exemple, pour écouter les requêtes de mappage et PCP homologue). Un profil PCP peut être lié à un serveur PCP. Un profil PCP lié à un serveur PCP applique tous ses paramètres au serveur PCP. Un profil PCP peut être lié à plusieurs serveurs PCP. Par défaut, un profil PCP avec les paramètres par défaut est lié à tous les serveurs PCP. Un profil PCP que vous liez à un serveur PCP remplace les paramètres de profil PCP par défaut pour ce serveur. Un profil PCP par défaut possède les paramètres suivants :
  - Mappage : activé
  - Peer : activé
  - Durée de vie minimale du mapping : 120 secondes
  - Durée de vie maximale : 86400 secondes
  - Nombre d'annonces : 10
  - Tiers : désactivé
- **Créez un serveur PCP et liez un profil PCP à celui-ci**. Créez un serveur PCP sur l'appliance Citrix ADC pour écouter les requêtes PCP et les messages des abonnés. Une adresse IP de sous-réseau (SNIP) ou (SNIP6) doit être attribuée à un serveur PCP pour y accéder. Par défaut, un serveur PCP écoute sur le port 5351.
- **Liez le serveur PCP à un groupe LSN d'une configuration LSN**. Liez le serveur PCP créé à un groupe LSN d'une configuration LSN en définissant le paramètre Serveur PCP pour spécifier le serveur PCP créé. Le serveur PCP créé est accessible uniquement par les abonnés de ce groupe LSN.

> **Remarque**
>
> Un serveur PCP pour une configuration NAT à grande échelle ne répond pas aux demandes des abonnés identifiés à partir des règles ACL.

Pour créer un profil PCP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

Pour créer un serveur PCP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Exemple de configuration pour NAT64

Dans l'exemple de configuration suivant, le serveur PCP PCP-SERVER-1, avec les paramètres PCP de PCP-PROFILE-1, est lié au groupe LSN LSN-NAT64-GROUP-1. PCP-SERVER-1 sert les demandes PCP des abonnés IPv6 dans le réseau 2001:DB8:5001::/96.

Exemple de configuration :

```
add pcp profile PCP-PROFILE-1 -minMapLife 400
Done
add pcp server PCP-SERVER-1 2001:DB8:6001::90  -pcpProfile PCP-PROFILE
    -1
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
```



```
13 add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
      :300::/96
14 Done
15 add lsn group LSN-NAT64-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
      ip6profile LSN-NAT64-PROFILE-1
16 Done
17 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
18 Done
19 bind lsn group LSN-NAT64-GROUP-1  - pcpServer PCP-NAT64-SERVER-1
20 Done
21 <!--NeedCopy-->
```

LSN64 dans une configuration de cluster

January 21, 2021

Les configurations NAT64 à grande échelle sont prises en charge sur une configuration de cluster Citrix ADC.

Un cluster CITRIX ADC est un groupe d'appliances Citrix ADC configurées et gérées en tant que système unique. Un cluster Citrix ADC offre évolutivité et disponibilité. Chaque appliance Citrix ADC dans une configuration de cluster agit comme une entité LSN indépendante et est gérée comme un système unique.

La configuration LSN dans une configuration de cluster est identique à celle d'une appliance autonome, à l'exception d'un pool spécifique d'adresses IP LSN appartenant à un seul nœud à la fois. En d'autres termes, une entité de pool IP LSN est configurée en tant qu'entité spotted dans un nœud particulier. Tous les nœuds d'une configuration de cluster peuvent avoir une entité de pool IP LSN spécifique. Pour vous assurer que les paquets liés à une session LSN sont reçus sur le même nœud de cluster qui a effectué l'opération NAT, la direction du backplane basé sur la stratégie (PBS) est configurée. PBS dirige les paquets associés reçus d'une session LSN vers le même nœud de cluster.

Exemple de configuration :

```
1 add lsn client LSN-NAT64-CLIENT-1
2
3 Done
4
5 bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
6
7 Done
8
9 add lsn pool LSN-NAT64-POOL-1
```



```
10
11 Done
12
13 bind lsn pool LSN-NAT64-POOL-1 -ownerNode 1  203.0.113.61 -
      203.0.113.70
14
15 Done
16
17 bind lsn pool LSN-NAT64-POOL-1 -ownerNode 2  203.0.113.101 -
      203.0.113.110
18
19 Done
20
21 add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
      :300::/96
22
23 Done
24
25 add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
      ip6profile LSN-NAT64-PROFILE-1
26
27 Done
28
29 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
30
31 Done
32
33 add ns acl6 NAT64-DFD ALLOW -srcIPv6 = 2001:DB8:5001:: -type DFD -
      dfdhash SIP -dfdprefix 64
34
35 Done
36
37 apply ns acls6 -type DFD
38
39 Done
40 <!--NeedCopy-->
```

Mappage d’adresse et de port à l’aide de la traduction

January 21, 2021

Mapping Address and Port using Translation (MAP-T) est une solution de transition IPv6 pour les FAI

disposant d'une infrastructure IPv6 pour connecter leurs abonnés IPv4 à l'Internet IPv4_.MAP-T est construite sur des technologies de traduction d'adresses IPv4 et IPv6 sans état. MAP-T est un mécanisme qui effectue une double traduction (IPv4 vers IPv6 et vice versa) sur les périphériques client (CE) et les routeurs frontière (dans le réseau central du fournisseur de services Internet).

Dans un déploiement MAP-T, le dispositif CE implémente une combinaison de traduction NAPT44 avec état et traduction NAT46 sans état. Le périphérique CE obtient NAT-IP et le bloc de port à utiliser pour la traduction via DHCPv6 ou toute autre méthode.

Lorsqu'un paquet IPv4 d'un périphérique abonné arrive au périphérique CE, le périphérique CE exécute NAPT44 et stocke les informations de liaison NAPT44. Après la traduction de NAT44, le paquet est soumis à la traduction de NAT46, puis transmis au périphérique de routeur frontalier (BR) situé dans le réseau central du fournisseur de services Internet. Le périphérique BR reçoit les paquets IPv6 du périphérique CE, extrait et valide l'IP NAT-IP et le bloc de port incorporé dans l'en-tête IPv6 et transfère le paquet IPv4 à l'Internet IPv4. Lorsque le BR reçoit le paquet IPv4 d'Internet, il traduit le paquet IPv4 en paquet IPv6 et envoie le paquet IPv6 au périphérique CE.

MAP-T est sans état sur un périphérique BR, il ne nécessite donc pas que le périphérique BR effectue NAT sur le trafic. Au lieu de cela, la fonctionnalité NAT est déléguée aux périphériques CE. Cette délégation et la fonctionnalité sans état dans les périphériques BR permettent au déploiement de BR d'évoluer proportionnellement au volume de trafic.

L'appliance Citrix ADC implémente la fonctionnalité BR d'une solution MAP-T comme décrit par la RFC 7599.

Configuration de MAP-T

La configuration de MAP-T sur une appliance Citrix ADC comporte les tâches suivantes :

- Ajouter une règle de mappage par défaut
- Ajouter une règle de mappage de base
- Liez une plage d'adresses NAT IPv4 de périphériques CE à une règle de mappage de base
- Ajouter un domaine de mappage et lier une règle de mappage de base et une règle de mappage par défaut au domaine

Pour ajouter une règle de mappage par défaut à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add MapDmr <name> -BRIpv6Prefix ( <ipv6_addr> | <*> )
2
3 show MapDmr <name>
4 <!--NeedCopy-->
```


Pour ajouter une règle de mappage de base à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add MapBmr <name> -RuleIpv6Prefix <ipv6_addr> | <*>  [-psidoffset <
    positive_integer>] [-EAbitLength <positive_integer>]  [-psidlength <
    positive_integer>]

show MapBmr <name>
<!--NeedCopy-->
```

Pour lier la plage d'adresses NAT IPv4 de périphériques CE à une règle de mappage de base à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind MapBmr <name> (-network <ip_addr>  [-netmask <netmask>])

show MapBmr <name>
<!--NeedCopy-->
```

Pour ajouter un domaine de mapping à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add MapDomain <name> -MapDmrName <string>

show MapDomain <name>
<!--NeedCopy-->
```

Pour lier une règle de mappage de base à un domaine de mappage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind MapDomain <name> -MapBmrName <string>

show MapDomain <name>
<!--NeedCopy-->
```


Exemple de configuration

```
add mapdmr DMR-1 -BRIpv6Prefix 2002:db8::/64

Done

add mapbmr BMR-1 -ruleIpv6Prefix 2002:db8:89ab::/48 -eAbitLength 16 -
    psidlength 8 -psidoffset 6

Done

bind mapbmr BMR-1 -network 192.0.1.0 -netmask 255.255.255.0

Done

add MapDomain MAP-DOMAIN-1 -mapdmrname DMR-1

Done

bind MapDomain MAP-DOMAIN-1 -mapbmrname BMR-1
Done
<!--NeedCopy-->
```

Gestion des abonnés à des opérateurs de téléphonie

August 20, 2021

Le nombre d'abonnés dans un réseau de télécommunications augmente à un rythme sans précédent, et leur gestion devient un défi pour les fournisseurs de services. Des appareils plus récents, plus rapides et plus intelligents placent une forte demande sur le réseau et les systèmes de gestion des abonnés. Il n'est plus possible d'offrir à chaque abonné la même norme de service, et il est impératif de traiter le trafic par abonné.

L'appliance Citrix ADC fournit l'intelligence pour profiler les abonnés en fonction de leurs informations stockées dans la fonction Policy and Charging Rules Function (PCRF). Lorsqu'un abonné mobile se connecte à Internet, la Gateway de paquets associe une adresse IP à l'abonné et transfère le paquet de données à l'appliance. L'appliance reçoit les informations de l'abonné dynamiquement ou vous pouvez configurer des abonnés statiques. Ces informations permettent à l'appliance d'appliquer ses fonctionnalités de gestion du trafic, telles que la commutation de contenu, la mise en cache intégrée, la réécriture et le répondeur, sur une base par abonné pour gérer le trafic.

Avant de configurer l'appliance Citrix ADC pour gérer les abonnés, vous devez allouer de la mémoire au

module qui stocke les sessions d'abonnés. Pour les abonnés dynamiques, vous devez configurer une interface via laquelle l'appliance reçoit les informations de session. Les abonnés statiques doivent se voir attribuer des ID et vous pouvez les associer à des stratégies.

Vous pouvez également effectuer les opérations suivantes :

- Application et gestion de la politique des abonnés.
- Configurez l'appliance pour identifier de manière unique un abonné en utilisant uniquement le préfixe IPv6 au lieu de l'adresse IPv6 complète.
- Utilisez des stratégies pour optimiser le trafic TCP pour les abonnés dynamiques et statiques. Ces stratégies associent différents profils TCP à différents types d'utilisateurs.
- Gérer les sessions inactives sur une appliance Citrix ADC.
- Activer la journalisation sur un serveur de journaux.
- Supprimer les sessions LSN pour les sessions d'abonné supprimées.

Allocation de mémoire pour le module de stockage de session de l'abonné

Chaque entrée de session d'abonné consomme 1 Ko de mémoire. Le stockage de 500 000 sessions d'abonnés à tout moment nécessite 500 Mo de mémoire. Cette valeur doit être ajoutée à la mémoire minimale requise, qui est affichée dans la sortie de la commande « show extendedmemoryparam ». Dans l'exemple suivant, la sortie est pour une instance Citrix ADC VPX avec 3 moteurs de paquets et 8 Go de mémoire.

Pour stocker 500 000 sessions d'abonnés sur cette appliance, la mémoire configurée doit être de 2058+500 Mo (500 000 x 1 Ko = 500 Mo).

> **Remarque**
>
> La mémoire configurée doit être en multiples de 2 Mo et ne doit pas dépasser la limite maximale d'utilisation de la mémoire. L'appliance doit être redémarrée pour que les modifications prennent effet.

Exemple

```
1 show extendedmemoryparam
2         Extended Memory Global Configuration. This memory is utilized by
              LSN and Subscriber Session Store Modules:
3          Active Memory Usage: 0 MBytes
4          Configured Memory Limit: 0 MBytes
5          Minimum Memory Required: 2058 MBytes
6          Maximum Memory Usage Limit: 2606 MBytes
7      Done
8      set extendedmemoryparam -memLimit 2558
9      Done
```



```
10      show extendedmemoryparam
11              Extended Memory Global Configuration. This memory is
                   utilized by LSN and Subscriber Session Store Modules:
12
13              Active Memory Usage: 2558 MBytes
14              Configured Memory Limit: 2558 MBytes
15              Minimum Memory Required: 2058 MBytes
16              Maximum Memory Usage Limit: 2606 MBytes
17      Done
18  <!--NeedCopy-->
```

Configurer une interface pour les abonnés dynamiques

L'appliance Citrix ADC reçoit dynamiquement les informations de l'abonné via l'un des types d'interface suivants :

- Interface GX
- Interface RADIUS
- Interface RADIUS et Gx

> **Remarque**
>
> - À partir de NetScaler version 12.0 build 57.19, l'interface Gx est prise en charge pour un déploiement de cluster. Pour plus d'informations, voir Interface Gx dans une topologie de cluster.
> - Dans une configuration HA, les sessions d'abonné sont continuellement synchronisées sur le nœud secondaire. En cas de basculement, les informations de l'abonné sont toujours disponibles sur le nœud secondaire.

Interface Gx

Une interface Gx (comme spécifié dans 3GPP 29.212) est une interface standard basée sur le protocole Diameter qui permet l'échange de règles de contrôle de stratégie et de facturation entre un PCRF et une entité PCEF (Policy and Charging Enforcement Function) dans un réseau de télécommunications.

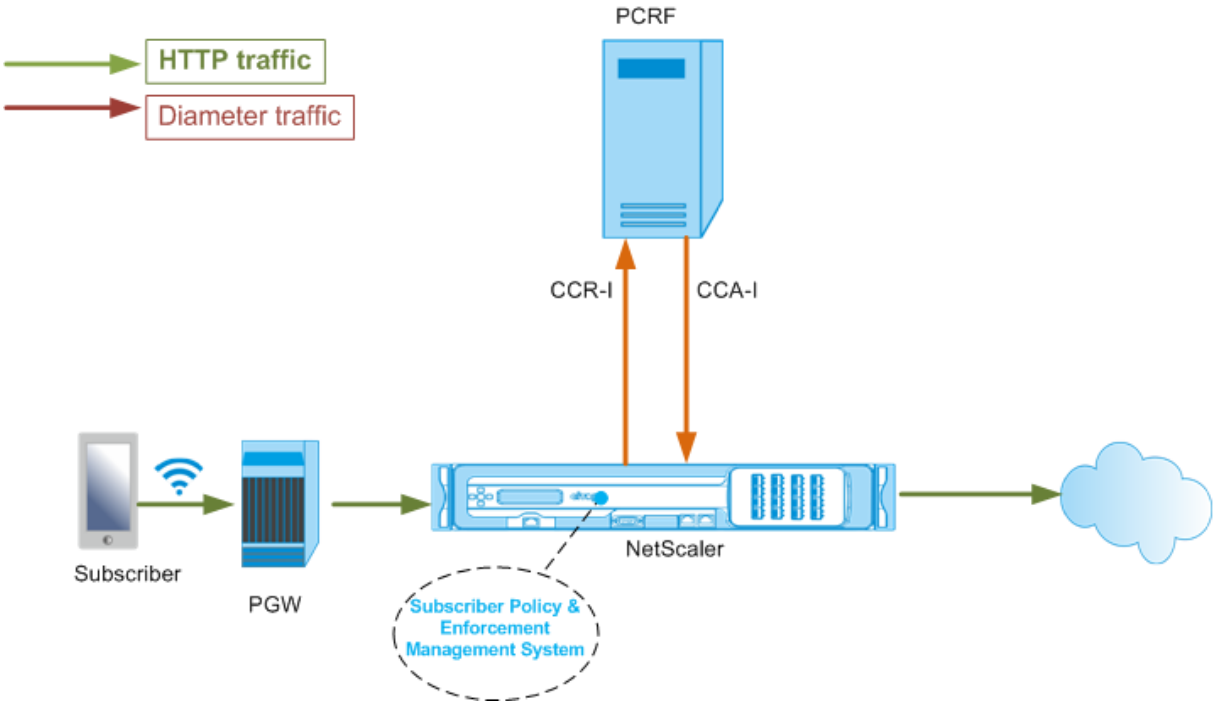
Lorsqu'une session IP-CAN est établie, la passerelle de paquets transmet l'ID d'abonné, tel que le MSISDN, et les informations d'adresse IP encadrée sur l'abonné au PCRF en tant que message de Diameter. Lorsque le paquet de données arrive à l'appliance à partir de la Gateway de paquets (PGW), l'appliance utilise l'adresse IP de l'abonné pour interroger le PCRF afin d'obtenir les informations de l'abonné. Ceci est également connu sous le nom de fonctionnalité PCEF secondaire.

Les règles PCC (Policy and Charging Control) reçues par l'appliance via l'interface Gx sont stockées sur l'appliance pendant la session de l'abonné, c'est-à-dire jusqu'à ce que le PCRF envoie un message RAR

(Re-Auth-Request) avec un AVP de Release-Cause ou que la session de l'abonné soit interrompue à partir de l'interface CLI ou du utilitaire de configuration. S'il existe des mises à jour pour un abonné existant, le PCRF envoie les mises à jour dans un message RAR. Une session d'abonné est lancée lorsqu'un abonné ouvre une session sur le réseau et s'arrête lorsque l'abonné se déconnecte.

> **Remarque** : si le serveur PCRF est en panne, l'appliance Citrix ADC crée des sessions négatives pour les demandes d'abonné Gx en attente ou entrantes. Lorsque le serveur PCRF est à nouveau en cours de sauvegarde, l'appliance Citrix ADC empêche une tempête de requêtes en attendant l'expiration des sessions négatives avant d'exécuter les demandes d'abonné spécifiques.

L'illustration suivante montre le flux de trafic de haut niveau. Il suppose que le trafic du plan de données est HTTP. L'appliance envoie une demande de contrôle de crédit (CCR) via une interface Gx au serveur PCRF et, dans la réponse de contrôle de crédit (CCA), reçoit les règles PCC et, éventuellement, d'autres informations, telles que le type de technologie d'accès radio (RAT), qui s'appliquent à l'abonné particulier. Les règles PCC incluent un ou plusieurs noms de stratégie (règle) et d'autres paramètres. L'appliance utilise ces informations pour récupérer les règles prédéfinies stockées sur l'appliance et pour diriger le flux de trafic. Il stocke également ces informations dans le système de gestion de la stratégie de l'abonné et de l'application pendant la session de l'abonné. Une fois la session d'abonné terminée, l'appliance rejette toutes les informations relatives à l'abonné.



L'exemple suivant montre les commandes de configuration d'une interface Gx. Les commandes sont en caractères gras.

Pour configurer une interface Gx, effectuez les tâches suivantes

Ajoutez un service DIAMETER pour chaque interface Gx. Par exemple :

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868

add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge DIAMETER non adressable et liez les services créés à l'étape 1 à ce serveur virtuel. Pour plusieurs services, spécifiez un PersistEnceType et le PersistAvPNO afin que des sessions spécifiques soient gérées par le même serveur PCRF. Par exemple :

```
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263

bind lb vserver vdiam pcrf-svc1

bind lb vserver vdiam pcrf-svc2
<!--NeedCopy-->
```

Configurez l'identité de Diameter et le domaine de domaine de Citrix ADC. Identité et domaine sont utilisés comme AVP Origin-Host et Origin-Realm dans les messages de Diameter envoyés par le client Gx. Par exemple :

```
set ns diameter  - identity netscaler.com  - realm com
<!--NeedCopy-->
```

Configurez l'interface Gx pour utiliser le serveur virtuel créé à l'étape 2 en tant que serveur virtuel PCRF. Spécifiez le domaine PCRF à utiliser comme AVP Destination-Realm dans les messages de Diameters envoyés par le client Gx. Par exemple :

```
set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf.com
<!--NeedCopy-->
```

Définissez le type d'interface de l'abonné sur GXOnly. Par exemple :

```
set subscriber param -interfaceType GxOnly
<!--NeedCopy-->
```

Pour afficher la configuration et l'état de l'interface Gx, tapez :

```
show subscriber gxinterface
<!--NeedCopy-->
```


Exemple

```
show subscriber gxinterface
    Gx Interface parameters:
        PCRF Vserver: vdiam (DOWN)
        Gx Client Identity...:  netscaler1.com
        Gx Client Realm ..........:  com
        PCRF Realm: epc.mnc030.mcc234.3gppnetwork.org
        Hold Packets On Subscriber Absence: YES
        CCR Request Timeout: 4 Seconds
        CCR Request Retry Attempts: 1
        Gx HealthCheck enabled: NO
        Gx HealthCheck TTL : 30 Seconds
        CER Request Timeout: 10 Seconds
        RevalidationTimeout: 30 Seconds
        NegativeTTL: 60 Seconds
        NegativeTTL Limited Success: NO
        Purge SDB on Gx Failure: YES
        ServicePath AVP code: 262099    ServicePath AVP VendorID: 3845
        PCRF Connection State: PCRF is not ready
    Done

<!--NeedCopy-->
```

ARGUMENTS

vServer

Nom du serveur virtuel d'équilibrage de charge ou de commutation de contenu vers lequel les connexions Gx sont établies. Le type de service du serveur virtuel doit être DIAMETER ou SSL_DIAMETER. Ce paramètre s'exclut mutuellement avec le paramètre de service. Par conséquent, vous ne pouvez pas définir à la fois le service et le serveur virtuel dans l'interface Gx.

Service

Nom du service DIAMETER ou SSL_DIAMETER correspondant au PCRF auquel la connexion Gx est établie. Ce paramètre est mutuellement exclusif avec le paramètre vserver. Par conséquent, vous ne pouvez pas définir à la fois le service et le serveur virtuel dans l'interface Gx.

pcrfRealm

Domaine de PCRF vers lequel le message doit être acheminé. Il s'agit du domaine utilisé dans Destination-Realm AVP par le client Citrix ADC Gx (en tant que nœud de Diameter).

holdOnSubscriberAbsence

Définissez la valeur Oui pour conserver les paquets jusqu'à ce que les informations de session de l'abonné soient récupérées à partir du serveur PCRF. S'il est défini sur Non, le profil d'abonné par défaut est appliqué jusqu'à ce que les informations de session d'abonné soient récupérées à partir du serveur PCRF. Si un profil d'abonné par défaut n'est pas configuré, un UNDEF est déclenché pour les expressions qui utilisent des attributs d'abonné.

requestTimeout

Délai, en secondes, pendant lequel la demande de CCR Gx doit être remplie. Si la demande ne se termine pas dans ce délai, la demande est retransmise pour le nombre de fois spécifié dans le paramètre RequestRetryAttents. Si la demande n'est pas terminée même après la retransmission, le profil d'abonné par défaut est appliqué à cet abonné. Si un profil d'abonné par défaut n'est pas configuré, un UNDEF est déclenché pour les expressions qui utilisent des attributs d'abonné. Zéro désactive le délai d'expiration. Valeur par défaut : 10

requestRetryAttempts

Spécifiez le nombre de fois qu'une demande doit être retransmise si la demande ne se termine pas dans la valeur spécifiée dans le paramètre RequestTimeout. Valeur par défaut : 3.

healthCheck

Définissez la valeur Oui pour activer la vérification de l'état en ligne de l'homologue Gx. Lorsqu'elle est activée, Citrix ADC envoie des paquets DWR au serveur PCRF. Lorsque la session Gx est inactive, le minuteur HealthCheck expire et les paquets DWR sont initiés pour vérifier si le serveur PCRF est actif. Valeur par défaut : Non.
Remarque : Ce paramètre est pris en charge dans Citrix ADC 12.1 build 51.xx et versions ultérieures.

healthCheckTTL

Durée en secondes définie pour la surveillance du chien de garde. Après l'expiration du délai de vérification de l'état, DWR est envoyé pour vérifier l'état du serveur PCRF. Tout message CCR, CCA, RAR ou RAA réinitialise la minuterie.
Valeur minimale : 6 secondes. Valeur par défaut : 30 secondes.
Remarque : Ce paramètre est pris en charge dans Citrix ADC 12.1 build 51.xx et versions ultérieures.

cerRequestTimeout

Durée en secondes définie pour la retransmission de la demande d'échange de capacités. Citrix ADC lance un nouveau message CER s'il ne reçoit pas de CEA du PCRF dans ce délai configuré.

Si aucune réponse n'est reçue du serveur PCRF, l'appliance tente d'envoyer le message CER 5 fois. S'il n'y a pas de réponse même après 5 messages CER, l'appliance ferme la connexion TCP et signale un échec. Si la valeur du délai d'expiration est définie sur 0, la fonction de vérification de l'état de l'application est désactivée.
Valeur minimale : 0 secondes. Valeur par défaut : 0 secondes.
Remarque : Ce paramètre est pris en charge dans Citrix ADC 12.1 build 51.xx et versions ultérieures.

revalidationTimeout

Temps, en secondes, après quoi la demande CCR-U Gx est envoyée après toute activité PCRF sur une session. Tout message RAR ou CCA réinitialise la minuterie. La valeur zéro désactive le délai d'attente d'inactivité.

negativeTTL

Temps, en secondes, après quoi la requête CCR-I Gx est envoyée pour les sessions qui n'ont pas été résolues par PCRF parce que le serveur est en panne ou qu'il n'y a pas de réponse ou qu'une réponse a échoué est reçue. Au lieu d'interroder constamment le serveur PCRF, un Negative-TTL empêche l'appliance de conserver une session non résolue. Pour les sessions négatives, l'appliance hérite des attributs du profil d'abonné par défaut, s'il en est configuré, et du message de comptabilisation RADIUS, s'il en est reçu. La valeur zéro désactive les sessions négatives. L'appliance n'installe pas de sessions négatives même si une session d'abonné n'a pas pu être récupérée. Valeur par défaut : 600

negativeTTLLimitedSuccess

Définissez la valeur Oui pour créer une session négative pour le code de réponse de succès partiel (2002). Si la valeur Non est définie, la session régulière est créée. Valeur par défaut : Non.

Ce paramètre est pris en charge dans Citrix ADC 12.1 build 49.xx et versions ultérieures.

purgeSDBonGxFailure

Définissez sur Oui pour vider la base de données abonné lorsque l'interface Gx échoue. L'échec de l'interface Gx inclut à la fois la surveillance DWR (si activée) et le HealthCheck réseau (si activée). Lorsque la valeur Oui est définie, toutes les sessions d'abonné sont effacées.
Valeur par défaut : Non.
Remarque : Ce paramètre est pris en charge dans Citrix ADC 12.1 build 51.xx et versions ultérieures.

servicePathAVP

Code AVP dans lequel PCRF envoie le chemin de service applicable à un abonné.

servicePathVendorid

ID fournisseur de l'AVP dans lequel PCRF envoie le chemin de service applicable à un abonné.

Pour configurer l'interface Gx à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.
2. Cliquez sur **Configurer les paramètres de l'abonné**.
3. Dans Type d'interface, sélectionnez **GXOnly**.
4. Spécifiez les valeurs pour tous les paramètres requis.
5. Cliquez sur **OK**.

Détecter les pannes de transport sur les connexions Gx établies

Remarque : Cette fonctionnalité est prise en charge dans Citrix ADC 12.1 build 51.xx et versions ultérieures.

Une appliance Citrix ADC peut être configurée pour détecter les défaillances de transport sur les connexions Gx établies à l'aide des messages DWR (Device Watchdog Request) et DWA (Device Watchdog answer).

Une fois qu'une session Gx est établie, une minuterie prédéfinie est déclenchée pour détecter si une session est inactive. Un message DWR est envoyé après l'expiration du délai d'inactivité. Le minuteur d'inactivité est réinitialisé chaque fois que l'appliance Citrix ADC reçoit un message sur une session Gx établie. La disponibilité du pair est confirmée en fonction du message DWA après l'envoi d'un message DWR.

- Si le DWA est reçu, la disponibilité d'un pair est confirmée et la minuterie de surveillance est réinitialisée.
- Si le DWA n'est pas reçu et que le minuteur de surveillance expire deux fois consécutivement, la session est considérée comme indisponible et indisponible. L'appliance ferme la session et tente d'établir une nouvelle session avec l'homologue Gx.

Lorsque le minuteur de surveillance expire deux fois sans réponse, l'appliance Citrix ADC considère la connexion Gx comme défectueuse et lance une fermeture de connexion. Une fois la connexion fermée, aucune autre demande de chien de garde n'est envoyée à l'homologue Gx. L'appliance Citrix ADC utilise la prochaine session Gx disponible pour toutes les demandes PCRF.

Pour détecter les défaillances de transport sur des connexions Gx établies à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set subscriber gxInterface [-vServer <string>] [-service <string>] [-
    healthCheck ( YES | NO )] [-healthCheckTTL<positive_integer>][-
    cerRequestTimeout <positive_integer>] [-purgeSDBonGxFailure ( YES |
    NO )]
<!--NeedCopy-->
```

Exemple :

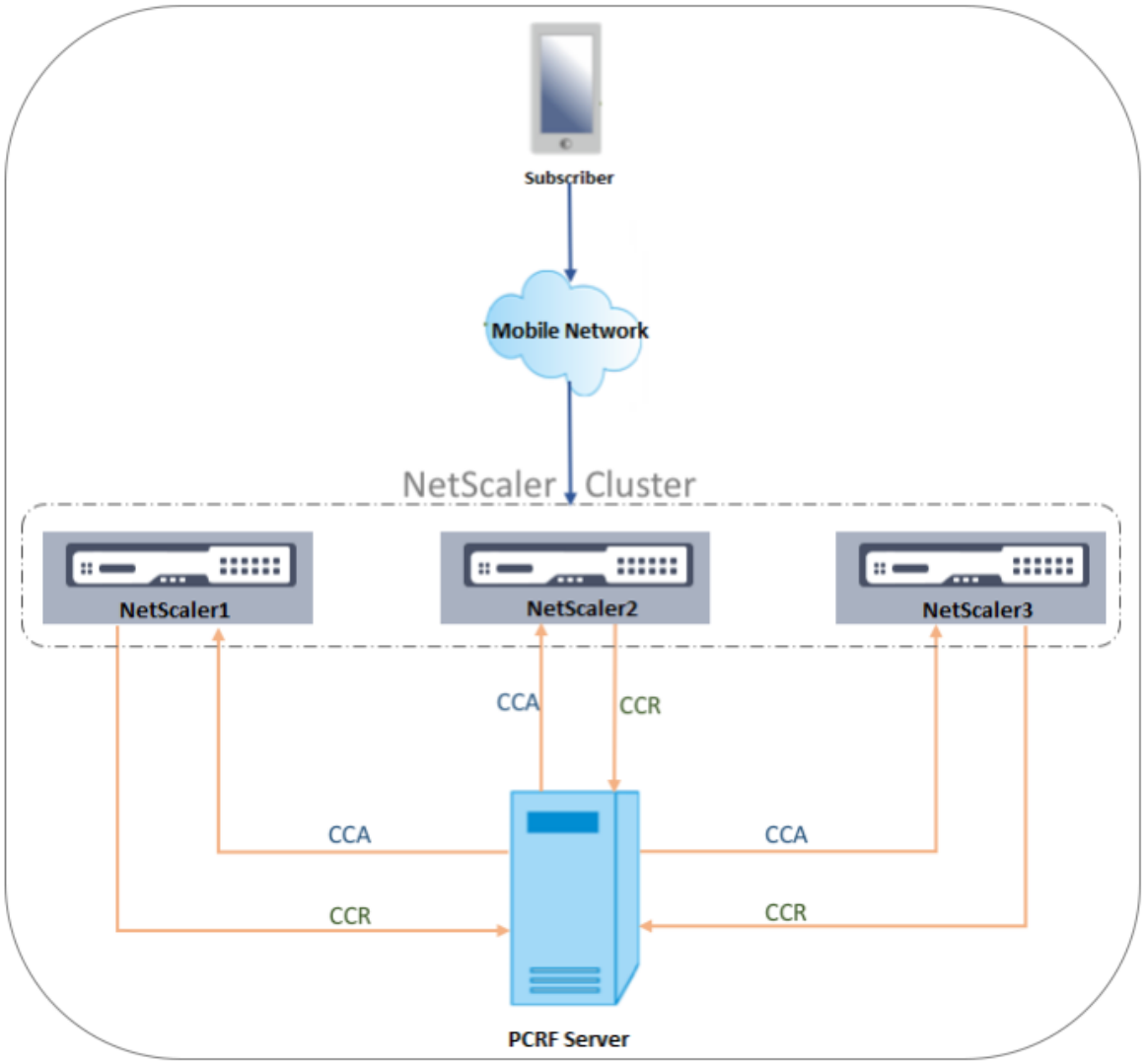
```
set subscriber gxInterface set subscriber gxInterface -vServer vdiam -
    healthCheck YES -healthCheckTTL 31 -cerRequestTimeout 15
    purgeSDBonGxFailure  YES
<!--NeedCopy-->
```

Pour détecter les défaillances de transport sur des connexions Gx établies à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.
2. Cliquez sur **Configurer les paramètres de l'abonné**.
3. Dans **Type d'interface**, sélectionnez **GXOnly**.
4. Spécifiez les valeurs de tous les paramètres requis.
5. Sélectionnez **Vérification de l'état** et spécifiez des valeurs pour **TTL de vérification de l'état** et **Délai d'expiration de la demande CER**.
6. Cliquez sur **OK**.

Interface Gx dans une topologie de cluster

L'appliance Citrix ADC prend en charge l'interface Gx dans une topologie de cluster.



Les nœuds Citrix ADC du cluster communiquent avec un serveur PCRF externe via l'interface Gx. Lorsqu'un nœud reçoit du trafic client, l'appliance effectue les opérations suivantes :

- Envoie une requête CCR-I au serveur PCRF pour récupérer les informations de l'abonné.
- Le serveur PCRF répond avec un CCR-A.
- Le nœud Citrix ADC stocke ensuite les informations d'abonné reçues dans son magasin d'abonné et applique les règles au trafic client.

Chaque nœud gère un magasin d'abonnés indépendant et les sessions d'abonnés ne sont pas synchronisées avec d'autres nœuds.

Conformément au protocole de base de diamètre RFC 6733, chaque homologue doit être configuré avec une identité de diamètre unique pour communiquer avec d'autres homologues sur le protocole de diamètre. Par conséquent, dans un déploiement de cluster, la configuration de l'identité de Diameter est spotted. Les paramètres de diamètre (identité, domaine, propagation de fermeture du serveur) pour chaque nœud peuvent être configurés individuellement à l'aide de l'interface graphique ou de

l'interface de ligne de commande.

Lorsqu'un nœud est ajouté à un cluster, il suppose les paramètres de Diameter par défaut (identity=netscaler.com, realm=com, serverClosePropogation=NO). Une fois les nœuds ajoutés, les paramètres de Diameter de chaque nœud doivent être configurés.

Pour configurer les paramètres de Diameter à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans le volet d'informations, cliquez sur **Modifier les paramètres de diamètre**.
3. Dans la page Paramètres de Diameter, sélectionnez le nœud Citrix ADC pour lequel vous souhaitez configurer les paramètres de Diameter, puis cliquez sur **Configurer**.
4. Dans la page Configurer les paramètres de diamètre, configurez l'identité de diamètre, le domaine de diamètre et la propagation de fermeture du serveur pour le nœud sélectionné.
5. Cliquez sur **OK**.

Pour configurer les paramètres de Diameter à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ns diameter [-identity <string>] [-ownerNode <positive_integer>]
<!--NeedCopy-->
```

ARGUMENTS

Identité

L'identité de Diameter est utilisée pour identifier un nœud de Diameter de manière unique. Avant de configurer la configuration du Diameter, l'appliance Citrix ADC (en tant que nœud de Diameter) doit se voir attribuer une identité de Diameter unique.

Par exemple, définissez ns diameter -identity netscaler.com -ownerNode 1. Ainsi, chaque fois que le système Citrix ADC doit utiliser l'identité dans les messages de diamètre, il utilise 'netscaler.com' comme AVP Origin-Host tel que défini dans RFC3588.

Longueur maximale : 255

OwnerNode

OwnerNode représente l'ID du nœud de cluster pour lequel l'ID de Diameter est défini. OwnerNode peut être configuré uniquement via CLIP.

Valeur minimale : 0

Valeur maximale : 31

Exemple :

set ns diameter -identity netscaler1.com -ownerNode 1

Remarque :

L'option OwnerNode est également ajoutée à la commande show ns diameter.

Exemple :

```
show diameter -ownerNode <0-31>
<!--NeedCopy-->
```

Lorsque la commande show ns diameter est exécutée, elle affiche les paramètres de Diameter d'un nœud donné.

Pour configurer une interface Gx pour le déploiement de cluster

Pour configurer une interface Gx, effectuez les tâches suivantes :

Ajoutez un service DIAMETER pour chaque interface Gx.

Exemple :

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868
add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge DIAMETER et liez les services créés à l'étape 1 à ce serveur virtuel.

Exemple :

```
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263

bind lb vserver vdiam pcrf-svc1

bind lb vserver vdiam pcrf-svc2
<!--NeedCopy-->
```

Configurez l'identité et le domaine de Diameter d'Citrix ADC sur tous les nœuds de cluster. Identité et domaine sont utilisés comme AVP Origin-Host et Origin-Realm dans les messages de Diameter envoyés par le client Gx.

Exemple :


```
set ns diameter -identity node0.netscaler.com -realm netscaler.com -
    ownerNode 0

set ns diameter -identity node1.netscaler.com -realm netscaler.com -
    ownerNode 1
<!--NeedCopy-->
```

Configurez l'interface Gx pour utiliser le serveur virtuel créé à l'étape 2 en tant que serveur virtuel PCRF et définissez également le domaine PCRF.

Exemple :

```
set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf.com

Set the subscriber interface type to GxOnly.
<!--NeedCopy-->
```

Exemple :

```
set subscriber param -interfaceType GxOnly
<!--NeedCopy-->
```

Pour afficher la configuration et l'état de l'interface Gx, tapez :

```
show subscriber gxinterface
<!--NeedCopy-->
```

Interface RADIUS

Avec une interface RADIUS, la Gateway de paquets transmet les informations de l'abonné dans un message de démarrage de la comptabilité RADIUS à l'appliance via l'interface RADIUS lorsqu'une session IP-CAN est établie. Un service de type RadiusListener traite les messages de comptabilité RADIUS. Ajoutez un secret partagé pour le client RADIUS. Si un secret partagé n'est pas configuré, le message RADIUS est supprimé en silence. L'exemple suivant montre les commandes de configuration d'une interface RADIUS. Les commandes sont en caractères gras.

Pour configurer une interface RADIUS, effectuez les tâches suivantes :

Créez un service d'écoute RADIUS à l'adresse SNIP où les messages RADIUS sont reçus. Par exemple :

```
add service srad1 192.0.0.206 RADIUSLISTENER 1813
<!--NeedCopy-->
```

Configurez l'interface RADIUS de l'abonné pour utiliser ce service. Par exemple :


```
set subscriber radiusInterface -listeningService srad1
<!--NeedCopy-->
```

Définissez le type d'interface de l'abonné sur RadiusOnly. Par exemple :

```
set subscriber param -interfaceType RadiusOnly
<!--NeedCopy-->
```

Ajoutez un client RADIUS spécifiant un sous-réseau et un secret partagé. Par exemple :

```
add radius client 192.0.2.0/24 -radkey client123
<!--NeedCopy-->
```

Un sous-réseau de 0.0.0.0/0 implique qu'il s'agit du secret partagé par défaut pour tous les clients. Pour afficher la configuration et l'état de l'interface RADIUS, tapez :

```
show subscriber radiusInterface
<!--NeedCopy-->
```

Paramètres de l'interface RADIUS :

Service d'écoute de rayon : srad1 (UP)

Terminé

Exemple :

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868

add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```

ARGUMENTS

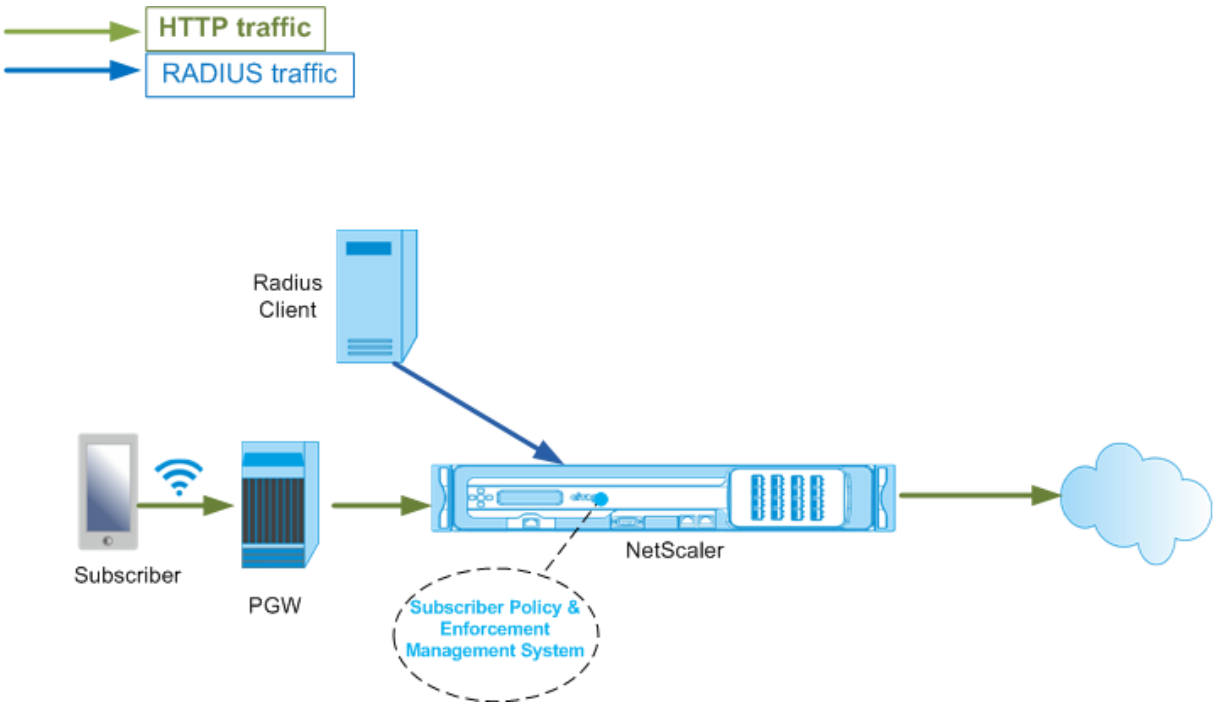
ListeningService

Nom du service d'écoute RADIUS qui traite les demandes de comptabilisation RADIUS.

svrState

État du service d'écoute RADIUS.

L'illustration suivante montre le flux de trafic de haut niveau.



Pour configurer l'interface RadiusOnly à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.
2. Cliquez sur **Configurer les paramètres de l'abonné**.
3. Dans Type d'interface, sélectionnez **RadiusOnly**.
4. Spécifiez les valeurs pour tous les paramètres requis.
5. Cliquez sur **OK**.

Interface RADIUS et Gx

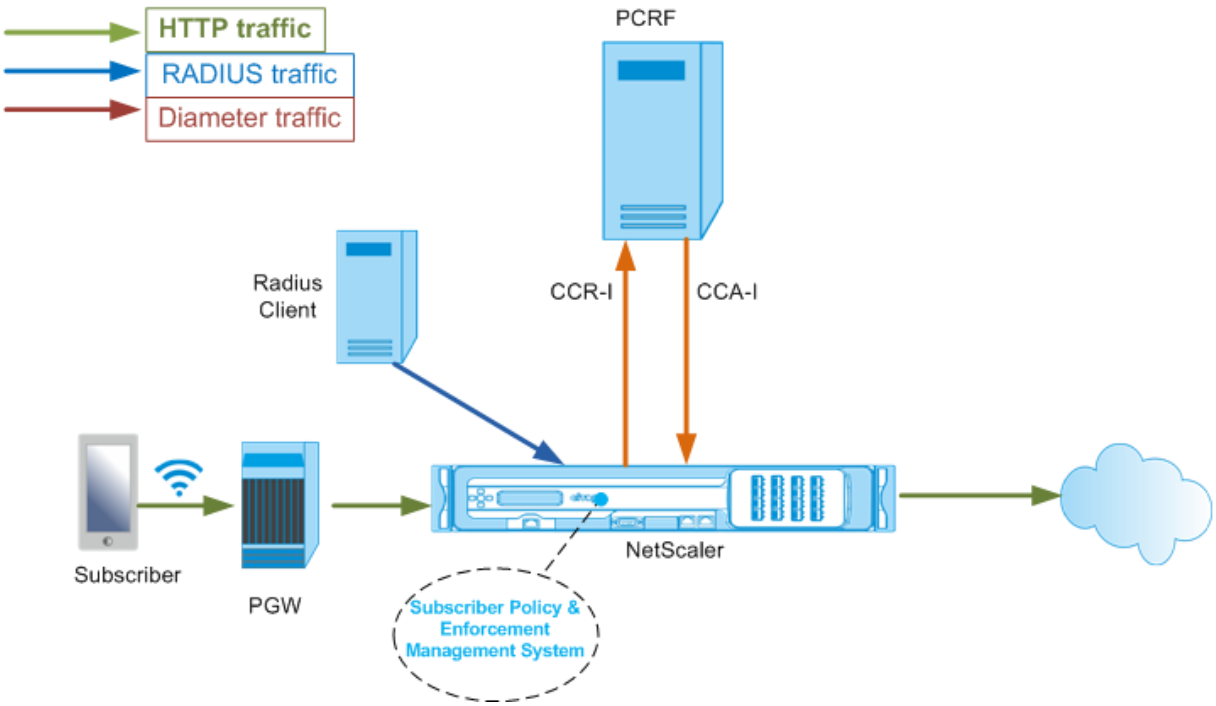
Avec une interface RADIUS et Gx, lorsqu'une session IP-CAN est établie, la Gateway de paquets transmet l'ID d'abonné, tel que le MSISDN, et les informations d'adresse IP encadrée concernant l'abonné à l'appliance via l'interface RADIUS. L'appliance utilise cet ID d'abonné pour interroger le PCRF sur l'interface Gx afin d'obtenir les informations de l'abonné. C'est ce qu'on appelle la fonctionnalité PCEF principale. L'exemple suivant montre les commandes de configuration d'une interface RADIUS et Gx.

```
1 set subscriber param -interfaceType RadiusandGx
2 add service pcrf-svc 203.0.113.1 DIAMETER 3868
3 add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
     persistAVPno 263
4 bind lb vserver vdiam pcrf-svc
5 set subscriber gxInterface -vServer vdiam -pcrfRealm testrealm1.net -
     holdOnSubscriberAbsence YES -revalidationTimeout 60 -negativeTTL 120
```



```
6 add service srad1 192.0.0.206 RADIUSLISTENER 1813    set subscriber
     radiusInterface -listeningService srad1
7 <!--NeedCopy-->
```

L'illustration suivante montre le flux de trafic de haut niveau.



Pour configurer l'interface RadiusAndGX à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.
2. Cliquez sur **Configurer les paramètres de l'abonné**.
3. Dans Type d'interface, sélectionnez **RadiusAndGX**.
4. Spécifiez les valeurs pour tous les paramètres requis.
5. Cliquez sur **OK**.

Configurer les abonnés statiques

Vous pouvez configurer manuellement les abonnés sur l'appliance Citrix ADC à l'aide de la ligne de commande ou de l'utilitaire de configuration. Vous créez des abonnés statiques en affectant un ID d'abonné unique et éventuellement en associant une stratégie à chaque abonné. Les exemples suivants montrent les commandes de configuration d'un abonné statique.

Dans les exemples suivants, **SubscriptionIdValue** spécifie le numéro de téléphone international et **SubscriptionIdType** (E164 dans cet exemple) spécifie le format général des numéros de téléphone internationaux.


```
1     add subscriber profile 203.0.113.6 -subscriberRules policy1 policy2
          -subscriptionIdType E164 -subscriptionIdvalue 98767543211
2     add subscriber profile 2002::a66:e8d3/64 -subscriberRules policy1
         policy3 -subscriptionIdtype E164 -subscriptionIdvalue
         98767543212
3     add subscriber profile 203.0.24.2 10 -subscriberRules policy2
         policy3 -subscriptionIdtype E164 -subscriptionIdvalue
         98767543213
4 <!--NeedCopy-->
```

Pour afficher les profils d'abonnés configurés, tapez :

```
show subscriber profile
```

```
1     > show subscriber profile
2
3     1)  Subscriber IP: 203.0.24.2 VLAN:10
4         Profile Attributes:
5                 Active Rules: policy2, policy3
6                 Subscriber Id Type: E164
7                 Subscriber Id Value: 98767543213
8     2)  Subscriber IP: 2002::/64
9         Profile Attributes:
10                Active Rules: policy1, policy3
11                Subscriber Id Type: E164
12                Subscriber Id Value: 98767543212
13    3)  Subscriber IP: 203.0.113.6
14        Profile Attributes:
15                Active Rules: policy1, policy2
16                Subscriber Id Type: E164
17                Subscriber Id Value: 98767543211
18
19     Done
20 <!--NeedCopy-->
```

Profil d'abonné par défaut

Un profil d'abonné par défaut est utilisé si l'adresse IP de l'abonné est introuvable dans le magasin de sessions de l'abonné sur l'appliance. Dans l'exemple suivant, un profil d'abonné par défaut est ajouté avec la stratégie de règle d'abonnement1.

```
1     > add subscriber profile * -subscriberRules policy1
2 <!--NeedCopy-->
```


Afficher et effacer les sessions d'abonnés

Utilisez la commande suivante pour afficher toutes les sessions d'abonnés statiques et dynamiques.

> show subscriber sessions

```
    > show subscriber sessions
    1)  Subscriber IP: 2002::/64
        Session Attributes:
                Active Rules: policy1, policy3
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543212
    2)  Subscriber IP: *
        Session Attributes:
                Active Rules: policy1
    3)  Subscriber IP: 203.0.24.2 VLAN:10
        Session Attributes:
                Active Rules: policy2, policy3
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543213
    4)  Subscriber IP: 203.0.113.6
        Session Attributes:
                Active Rules: policy1, policy2
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543211
    5)  Subscriber IP: 192.168.0.11
        Session Attributes:
                Idle TTL remaining: 361 Seconds
                Active Rules: policy1
                Subscriber Id Type: E164
                Subscriber Id Value: 1234567811
                Service Path: policy1
                AVP(44): 34 44 32 42 42 38 41 43  2D 30 30 30 30 30 30
                   31 31
                AVP(257): 00 01 C0 A8 0A 02
                PCRF-Host: host.pcrf.com
                AVP(280): 74 65 73 74 2E 63 6F 6D

    Done
<!--NeedCopy-->
```

Utilisez la commande suivante pour effacer une seule session ou le magasin de sessions complet. Si vous ne spécifiez pas d'adresse IP, le magasin de sessions complet de l'abonné est effacé.

```
clear subscriber sessions <ip>
<!--NeedCopy-->
```


Système de gestion et d'application de la politique d'abonné

L'appliance Citrix ADC utilise l'adresse IP de l'abonné comme clé du système de gestion et d'application de la stratégie de l'abonné.

Vous pouvez ajouter des expressions d'abonné pour lire les informations d'abonné disponibles dans le Système d'application et de gestion des stratégies d'abonné. Ces expressions peuvent être utilisées avec des règles de stratégie et des actions configurées pour les fonctionnalités de Citrix ADC, telles que la mise en cache intégrée, la réécriture, le répondeur et la commutation de contenu.

Les commandes suivantes sont un exemple d'ajout d'une action et d'une stratégie de répondeur basée sur l'abonné. La stratégie est évaluée à true si la valeur de la règle de l'abonné est « pol1 ».

```
1     add responder action error_msg respondwith '"HTTP/1.1 403 OKrnrn" +
          " You are  not authorized to access Internet"'
2     add responder policy no_internet_access "SUBSCRIBER.RULE_ACTIVE("
          pol1")" error_msg
3 <!--NeedCopy-->
```

L'exemple suivant montre les commandes pour ajouter une action de réécriture basée sur l'abonné et une stratégie. L'action insère un en-tête HTTP « X-Nokia-MSISDN » en utilisant la valeur de AVP (45) dans la session d'abonné.

```
1     > add rewrite action AddHDR-act insert_http_header X-Nokia-MSISDN "
          SUBSCRIBER.AVP(45).VALUE"
2     > add rewrite policy AddHDR-pol "HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.
          URL).EQUALS_ANY("patset-test")" AddHDR-act
3 <!--NeedCopy-->
```

Dans l'exemple suivant, deux stratégies sont configurées sur l'appliance. Lorsque l'appliance vérifie les informations de l'abonné et que la règle d'abonné est cache_enable, elle effectue la mise en cache. Si la règle d'abonné est cache_disable, l'appliance n'effectue pas de mise en cache.

```
1     > add cache policy nocachepol -rule "SUBSCRIBER.RULE_ACTIVE("
          cache_disable")" - action NOCACHE
2     > add cache policy cachepol -rule "SUBSCRIBER.RULE_ACTIVE("
          cache_enable")" - action CACHE -storeInGroup cg1
3 <!--NeedCopy-->
```

Pour obtenir la liste complète des expressions commençant par "SUBSCRIBER", consultez le Guide de configuration des stratégies.

> **Important**
>
> Le logiciel Citrix ADC version 12.1 prend en charge la méthode de recherche de clé IPANDVLAN

> lorsque l'interface de l'abonné est définie sur GxOnly. Pour plus de détails, reportez-vous à la section Méthode de recherche de clé d'adresse IP et d'ID VLAN

Sessions d'abonné basées sur le préfixe IPv6

Un utilisateur de télécommunications est identifié par le préfixe IPv6 plutôt que par l'adresse IPv6 complète. L'appliance Citrix ADC utilise désormais le préfixe au lieu de l'adresse IPv6 complète (/128) pour identifier un abonné dans la base de données (magasin d'abonnés). Pour communiquer avec le serveur PCRF (par exemple, dans un message CCR-I), l'appliance utilise désormais le préfixe AVP encadré IPv6 au lieu de l'adresse IPv6 complète. La longueur du préfixe par défaut est /64, mais vous pouvez configurer l'appliance pour qu'elle utilise une valeur différente.

Pour configurer le préfixe IPv6 à l'aide de la ligne de commande

```
set subscriber param [-ipv6PrefixLookupList <positive_integer> ...]
```

Le premier exemple de commande ci-dessous définit un seul préfixe et le second exemple définit plusieurs préfixes.

```
1     set subscriber param -ipv6PrefixLookupList 64
2     set subscriber param -ipv6PrefixLookupList 64 72 96
3 <!--NeedCopy-->
```

Pour configurer le préfixe IPv6 à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Configurer les paramètres d'abonné**et dans la **liste de recherche de préfixes IPv6**, spécifiez un ou plusieurs préfixes.

Adresse IP et méthode de recherche de clé d'ID VLAN

L'appliance Citrix ADC utilise l'adresse IP de l'abonné comme méthode de recherche de clé pour le système d'application et de gestion des stratégies d'abonné. Cette méthode n'est pas efficace si les adresses IP se chevauchent. Dans de tels cas, vous pouvez utiliser l'ID VLAN comme type de recherche d'abonné supplémentaire. La méthode de recherche de clé IPANDVLAN est prise en charge uniquement lorsque l'interface de l'abonné est définie sur GxOnly. Lorsque IPANDVLAN est configuré comme méthode de recherche, l'appliance Citrix ADC effectue les opérations suivantes :

- Inclut l'ID VLAN d'origine dans la requête Gx pour les abonnés IPv4.
- Inclut le VLAN AVP Gx dans toutes les réponses Gx. Toutefois, en cas de non-concordance de l'ID de VLAN, l'appliance ignore les réponses.

Par exemple, si l'appliance envoie un CCR-I avec gxSessionId-a:IPv4-b:vLAN-C et que la réponse contient gxSessionId-a:IPv4-b:vLAN-D, la réponse est supprimée et une entrée d'abonné par défaut est créée.

> **Remarque**
>
> - Les types d'interface RadiusAndGX et RadiusOnly ne peuvent pas être configurés avec le type de clé IPANDVLAN.
> - Si le trafic provient d'une adresse IPv6, l'appliance Citrix ADC utilise la méthode de recherche IP.

Pour configurer IP ou IPANDVLAN comme méthode de recherche de clé à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set subscriber param [-keytype ( IP | IPANDVLAN )] [-interfaceType <
   interfaceType>]
<!--NeedCopy-->
```

Exemple :

```
set subscriber param -keytype IPANDVLAN -interfaceType GxOnly

set subscriber param -keytype IP -interfaceType GxOnly
<!--NeedCopy-->
```

> **Remarque**
>
> Changer le paramètre keytype d'IP à IPANDVLAN et efface inversement toutes les données de l'abonné.

Paramètre VLAN

Le paramètre VLAN est également ajouté pour les commandes suivantes.

```
add subscriber profile <ip>@ [-vlan]

set subscriber profile <ip>@ [-vlan] [-subscriptionIdType  <
   subscriptionIdType>]

show subscriber profile [<ip>@] [-vlan]

rm subscriber profile <ip>@ [-vlan <positive_integer>]
<!--NeedCopy-->
```


Arguments

IP

Représente l'adresse IP de l'abonné. Il s'agit d'un argument obligatoire et ne peut pas être modifié après l'ajout du profil d'abonné.

VLAN

Représente le numéro de VLAN sur lequel se trouve l'abonné. Le numéro de VLAN ne peut pas être modifié après l'ajout du profil d'abonné.

Valeur minimale : 1

Valeur maximale : 4096

```
add subscriber profile 192.0.2.23 10

set subscriber profile 192.0.2.23 10 -subscriptionIdtype E164

show subscriber profile 192.0.2.23 10

rm subscriber profile 192.0.2.23 10

<!--NeedCopy-->
```

Pour configurer IP ou IPANDVLAN comme méthode de recherche de clé à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres.**
2. Cliquez sur **Configurer les paramètres de l'abonné.**
3. Dans **Type de clé**, sélectionnez **IP**ou **IPANDVLAN**selon vos besoins.
4. Terminez la configuration et cliquez sur **OK**.

Gestion des sessions inactives des sessions d'abonné dans un réseau de télécommunications

Le nettoyage de session d'abonné sur une appliance Citrix ADC est basé sur des événements de plan de contrôle, tels qu'un message d'arrêt de la comptabilité RADIUS, un message de Diameter RAR (version de session) ou une commande « effacer la session d'abonné ». Dans certains déploiements, les messages provenant d'un client RADIUS ou d'un serveur PCRF peuvent ne pas atteindre l'appliance. En outre, en cas de trafic intense, les messages peuvent être perdus. Une session d'abonné qui est

inactive pendant une longue période continue de consommer de la mémoire et des ressources IP sur l'appliance Citrix ADC. La fonction de gestion des sessions inactives fournit des temporisateurs configurables pour identifier les sessions inactives et nettoie ces sessions en fonction de l'action spécifiée.

Une session est considérée comme inactive si aucun trafic provenant de cet abonné n'est reçu sur le plan de données ou le plan de contrôle. Vous pouvez spécifier une action de mise à jour, terminer (informer PCRF, puis supprimer la session) ou supprimer (sans informer PCRF). L'action n'est effectuée qu'une fois que la session est inactive pendant la durée spécifiée dans le paramètre de délai d'attente d'inactivité.

Pour configurer le délai d'expiration de la session inactive et l'action associée à l'aide de la ligne de commande

```
set subscriber param [-idleTTL <positive_integer>] [-idleAction <
   idleAction>]
<!--NeedCopy-->
```

Exemples :

```
set subscriber param -idleTTL 3600 -idleAction ccrTerminate

set subscriber param -idleTTL 3600 -idleAction ccrUpdate

set subscriber param -idleTTL 3600 -idleAction delete
<!--NeedCopy-->
```

Pour désactiver le délai d'expiration de la session inactive, définissez le délai d'attente d'inactivité sur zéro.

set subscriber param –idleTTL 0

Pour configurer le délai d'expiration de la session inactive et l'action associée à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Configurer les paramètres de l'abonné** et spécifiez une action de temps **d'inactivité** et **d'inactivité**.

Enregistrement des événements de session d'abonné

Si vous activez la journalisation des abonnés, vous pouvez suivre les messages du plan de contrôle RADIUS et Gx spécifiques à un abonné et utiliser les données historiques pour analyser les activités

de l'abonné. Certains des attributs clés sont MSISDN et horodatage. Les attributs suivants sont également enregistrés :

- Événement de session (installation, mise à jour, suppression, erreur)
- Type de message Gx (CCR-I, CCR-U, CCR-T, RAR)
- Type de message de rayon (début, arrêt)
- IP de l'abonné
- Type d'ID d'abonné (MSISDN (E164), IMSI)
- Valeur d'ID d'abonné

En utilisant ces journaux, vous pouvez suivre les utilisateurs par adresse IP et, le cas échéant, MSISDN.

Vous pouvez activer la journalisation de session d'abonné sur un serveur syslog ou nslog local ou distant. L'exemple suivant montre comment activer la journalisation des abonnés sur un serveur syslog distant.

```
1      > add syslogAction sysact1 192.0.2.0 -loglevel EMERGENCY ALERT
          CRITICAL ERROR WARNING NOTICE INFORMATIONAL -subscriberlog
          enabled
2  <!--NeedCopy-->
```

À partir de ces journaux, vous pouvez en savoir plus sur toute activité liée à un utilisateur, comme l'heure à laquelle une session a été mise à jour, supprimée ou créée (installée). En outre, les messages d'erreur sont également enregistrés.

Exemples :

1. Les entrées de journal suivantes sont des exemples de création de session RadiusAndGX, de mise à jour de session et de suppression de session.

   > 09/30/2015:16:29:18 GMT Informational 0-PPE-0 : default SUBSCRIBER SESSION_EVENT 147 0 : Session Install, GX MsgType: CCR-I, RADIUS MsgType: Start, IP: 100.10.1.1, ID: E164 - 30000000001
   >
   > 09/30/2015:16:30:18 GMT Informational 0-PPE-0 : default SUBSCRIBER SESSION_EVENT 148 0 : Session Update, GX MsgType: CCR-U, IP: 100.10.1.1, ID: E164 - 30000000001
   >
   > 09/30/2015:17:27:56 GMT Informational 0-PPE-0 : default SUBSCRIBER SESSION_EVENT 185 0 : Session Delete, GX MsgType: CCR-T, RADIUS MsgType: Stop, IP: 100.10.1.1, ID: E164 - 30000000001

2. Les entrées de journal suivantes sont des exemples de messages d'échec, par exemple lorsqu'un abonné est introuvable sur le serveur PCRF et lorsque l'appliance ne peut pas se connecter au serveur PCRF.

> 09/30/2015:16:44:15 GMT Error 0-PPE-0 : default SUBSCRIBER SESSION_FAILURE 169 0 : Failure Reason: PCRF failure response, GX MsgType: CCR-I, IP: 100.10.1.1
>
> Sep 30 13:03:01 09/30/2015:16:49:08 GMT 0-PPE-0 : default SUBSCRIBER SESSION_FAILURE 176 0 : Failure Reason: Unable to connect to PCRF, GX MsgType: CCR-I, RADIUS MsgType: Start, IP: 100.10.1.1, ID: E164 - 30000000001#000#000#000#000#000#000#000#000#000#000#000#000#00

Résiliation de session LSN prenant en compte l'abonné

Dans les versions antérieures, si une session d'abonné est supprimée lorsqu'un message RADIUS Accounting STOP ou PCRF-RAR est reçu, ou à la suite de tout autre événement, tel que l'expiration de la TTL ou le vidage, les sessions LSN correspondantes de l'abonné ne sont supprimées qu'après le délai d'expiration du LSN configuré. Les sessions LSN qui sont maintenues ouvertes jusqu'à ce que ce délai expire continuent à consommer des ressources sur l'appliance.

À partir de la version 11.1, un nouveau paramètre (SubscrSessionRemoval) est ajouté. Si ce paramètre est activé et que les informations de l'abonné sont supprimées de la base de données de l'abonné, les sessions LSN correspondant à cet abonné sont également supprimées. Si ce paramètre est désactivé, les sessions d'abonné sont expirées comme spécifié par les paramètres de délai d'expiration du LSN.

Pour configurer la fin de session LSN sensible aux abonnés à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lsn parameter -subscrSessionRemoval (          DISABLED )
ENABLED
```

```
1      > set lsn parameter -subscrSessionRemoval ENABLED
2      Done
3      > sh lsn parameter
4                  LSN Global Configuration:
5
6                  Active Memory Usage: 0 MBytes
7                  Configured Memory Limit: 0 MBytes
8                  Maximum Memory Usage Limit: 912 MBytes
9                  Session synchronization: ENABLED
10                 Subscriber aware session removal: ENABLED
11 <!--NeedCopy-->
```


Pour configurer la fin de session LSN sensible à l'abonné à l'aide de l'interface graphique

1. Accédez à **Système** > **NAT à grande échelle** .
2. Dans **Mise en route**, cliquez sur **Définir le paramètre LSN**.
3. Définissez le **paramètre Suppression de session prenant en compte l'abonné**.

Résolution des problèmes

Si votre déploiement ne fonctionne pas comme prévu, utilisez les commandes suivantes pour résoudre les problèmes :

- show subscriber gxinterface
  Cette commande peut inclure les messages d'erreur suivants (présentés ici avec les réponses suggérées) :
  - Interface Gx non configurée-Utilisez la commande set subscriber param pour configurer le type d'interface correct.
  - PCRF non configurée-Configurez un serveur ou un service Diameter sur GXInterface-Utilisez la commande set subscriber gx interface pour affecter un serveur virtuel Diameter ou un service à cette interface.
  - PCRF n'est pas prêt à vérifier vserver/service correspondant pour plus de détails - Utilisez la commande show LB vserver ou show service pour vérifier l'état du service.
  - Citrix ADC attend le CEA de la négociation de la capacité PCRF entre le PCRF et Citrix ADC peut échouer. Cela pourrait être un état intermittent. Si elle persiste, vérifiez les paramètres DIAMETER sur votre serveur PCRF.
  - La mémoire n'est pas configurée pour stocker les sessions d'abonnés. Utilisez 'set extendedmemoryparam -memlimit <>'-Utilisez la commande set extendedmemoryparam pour configurer la mémoire étendue.
- show subscriber radiusinterface
  Si « Non configuré » est la sortie de cette commande, utilisez la commande set subscriber radiusinterface pour spécifier un service RadiusListener.

Si la journalisation des abonnés est activée, vous pouvez obtenir des informations plus détaillées à partir des fichiers journaux.

Orientation du trafic des abonnés

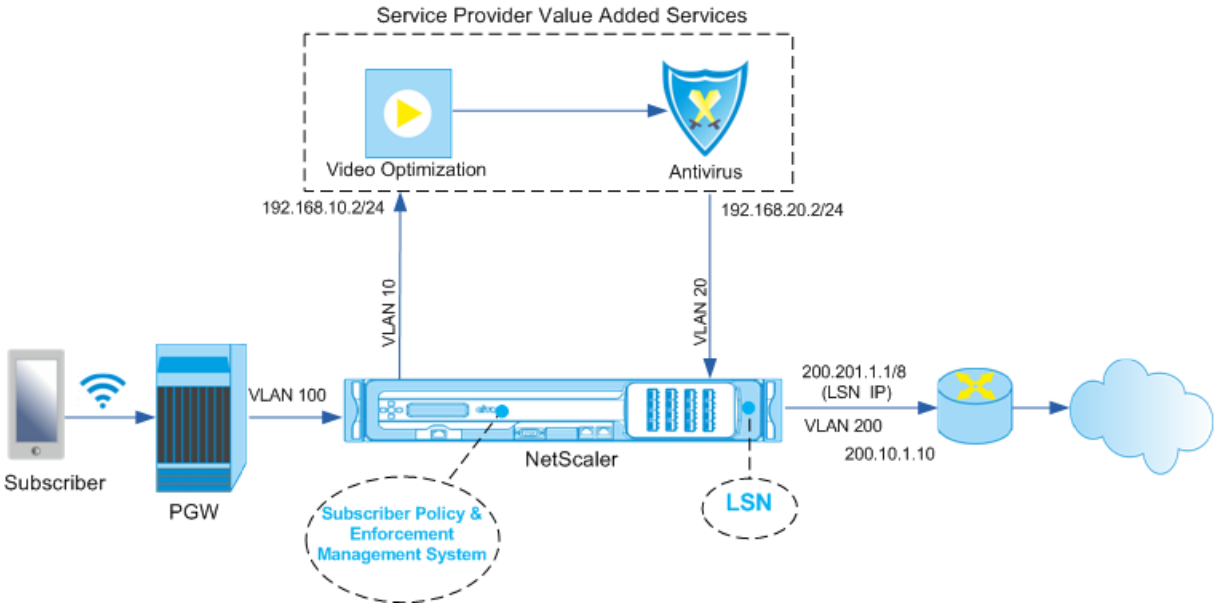
August 20, 2021

La direction de la circulation dirige le trafic des abonnés d'un point à l'autre. Lorsqu'un abonné se connecte au réseau, la Gateway de paquets associe une adresse IP à l'abonné et transfère le paquet de données à l'appliance Citrix ADC. L'appliance communique avec le serveur PCRF via l'interface Gx

pour obtenir les informations de stratégie. Selon les informations de stratégie, l'appliance effectue l'une des actions suivantes :

- Transférer le paquet de données à un autre ensemble de services (comme illustré dans l'illustration suivante).
- Lâchez le paquet.
- Effectuez uniquement le NAT à grande échelle (LSN), si le LSN est configuré sur l'appliance.

Les valeurs indiquées dans la figure suivante sont configurées dans la procédure CLI qui suit la figure. Un serveur virtuel de commutation de contenu sur l'appliance Citrix ADC dirige les demandes vers les services à valeur ajoutée ou les ignore, en fonction de la règle définie, puis envoie le paquet vers Internet après avoir effectué LSN.



Pour configurer la direction du trafic pour le déploiement ci-dessus à l'aide de l'interface de ligne de commande

Ajoutez les adresses SNIP de sous-réseau (SNIP) de l'appliance.

Exemple :

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 100.100.100.1 255.0.0.0 -type snip

add ns ip 200.200.200.1 255.0.0.0 -type snip

add ns ip 100.1.1.1 255.0.0.0 -type snip
```



```
10
11 add ns ip 200.201.1.1 255.0.0.0 -type snip
12 <!--NeedCopy-->
```

Ajoutez les VLAN. Les VLAN aident l'appliance à identifier la source du trafic. Liez les VLAN aux interfaces et aux adresses IP de sous-réseau.

Exemple :

```
1  add vlan 10
2
3  add vlan 20
4
5  add vlan 100
6
7  add vlan 200
8
9  bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1 255.255.255.0
10
11 bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1 255.255.255.0
12
13 bind vlan 100 -ifnum 1/2 -tagged -IPAddress 100.1.1.1 255.0.0.0
14
15 bind vlan 200 -ifnum 1/3 -tagged -IPAddress 200.1.1.1 255.0.0.0
16 <!--NeedCopy-->
```

Spécifiez le VLAN sur lequel le trafic d'abonnés arrive sur l'appliance. Spécifiez le chemin d'accès du service AVP qui indique à l'appliance où rechercher le nom du chemin d'accès du service dans la session d'abonné. Pour la fonctionnalité PCEF principale, spécifiez InterfaceType comme RadiusAndGX.

Exemple :

```
1  set ns param -servicePathIngressVLAN 100
2
3  set subscriber gxinterface -servicepathAVP 1001 1005 -
      servicepathVendorid 10415
4
5  set subscriber param -interfaceType RadiusAndGx
6  <!--NeedCopy-->
```

Configurez un service et un serveur virtuel de type Diameter et liez le service au serveur virtuel. Ensuite, spécifiez les paramètres de l'interface Gx du domaine PCRF et de l'abonné. Pour la fonctionnalité PCEF principale, configurez un service d'écoute RADIUS et une interface RADIUS.

Exemple :


```
add service sd1 10.102.232.200 DIAMETER 3868

add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263

bind lb vserver vdiam sd1

set ns diameter -identity netscaler.sc1.net -realm pcrf1.net

set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net -
    holdOnSubscriberAbsence YES -idleTTL 1200 -negativeTTL 120

add service srad1 10.102.232.236 RADIUSListener 1813

set subscriber radiusInterface -listeningService srad1
<!--NeedCopy-->
```

Ajoutez des fonctions de service pour associer un VAS à un VLAN d'entrée. Ajoutez un chemin de service pour définir la chaîne, c'est-à-dire spécifier le VAS auquel le paquet doit être envoyé et l'ordre dans lequel il doit aller dans ce VAS. Le nom du chemin d'accès du service est généralement envoyé par le PCRF. Toutefois, le chemin d'accès du service du profil d'abonné par défaut (*) s'applique si l'une des conditions suivantes est remplie :

- Le PCRF ne possède pas les informations sur l'abonné.
- Les informations sur l'abonné ne comprennent pas cet AVP.
- L'appliance ne peut pas interroger le PCRF. Par exemple, le service représentant le PCRF est DOWN.

Le chemin de service AVP qui contient ce nom doit déjà être configuré dans le cadre de la configuration globale. Liez la fonction de service au chemin d'accès du service. L'index de service spécifie l'ordre dans lequel le SAV est ajouté à la chaîne. Le nombre le plus élevé (255) indique le début de la chaîne.

Exemple :

```
add ns servicefunction SF1 -ingressVLAN 20

add ns servicepath pol1

bind ns servicepath pol1 -servicefunction SF1 -index 255

add subscriber profile * -subscriberrules default_path
<!--NeedCopy-->
```

Ajoutez la configuration LSN. Autrement dit, définissez le pool NAT et identifiez les clients pour

lesquels l'appliance doit exécuter LSN.

```
add lsn pool pool1

bind lsn pool pool1 200.201.1.1

add lsn client client1

bind lsn client client1 -network 100.0.0.0 -netmask 255.0.0.0

add lsn group group1 -clientname client1

bind lsn group group1 -poolname pool1
<!--NeedCopy-->
```

L'appliance exécute LSN par défaut. Pour remplacer LSN, vous devez créer un profil net avec le paramètre overridelsN activé et lier ce profil à tous les serveurs virtuels d'équilibrage de charge configurés pour les services à valeur ajoutée (vASs).

Exemple :

```
add netprofile np1

set netprofile np1 -overrideLsn ENABLED

set lb vserver vs1 -netprofile np1
<!--NeedCopy-->
```

Configurez le VAS sur l'appliance. Cela inclut la création des services et des serveurs virtuels, puis la liaison des services aux serveurs virtuels.

```
add service vas1 192.168.10.2 ANY 80 -usip YES

add service sint 200.10.1.10 ANY 80 -usip YES

add lb vserver vs1 ANY -m MAC -l2Conn ON

add lb vserver vint ANY -m MAC -l2Conn ON

bind lb vserver vs1 vas1

bind lb vserver vint sint
<!--NeedCopy-->
```

Ajoutez la configuration de commutation de contenu (CS). Cela inclut les serveurs virtuels, les straté-

gies et les actions associées. Le trafic arrive au serveur virtuel CS et est ensuite redirigé vers le serveur virtuel d'équilibrage de charge approprié. Définissez les expressions qui associent un serveur virtuel à une fonction de service.

Exemple :

```
add cs vserver cs1 ANY * 80 -l2Conn ON

add cs action csact1 -targetLBVserver vs1

add cs action csactint -targetLBVserver vint

add cs policy cspol1 -rule  SUBSCRIBER.SERVICEPATH.IS_NEXT("SF1") &&
   SYS.VSERVER("vs1").STATE.EQ(UP)" -action csact1

bind cs vserver cs1 -policyName cspol1 -priority 110

bind cs vserver cs1 -lbvserver vint
<!--NeedCopy-->
```

Pour configurer la direction de la circulation sur l'appliance à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **IP** et ajoutez les adresses IP du sous-réseau.
2. Accédez à Système > Réseau > **VLAN** et ajoutez des VLAN, liez les VLAN aux interfaces et aux adresses IP des sous-réseaux.
3. Accédez à **Gestion du trafic** > **Chaîne** de **service > Configurer le VLAN d'entrée du chemin** de service et spécifiez un VLAN d'entrée.
4. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres** > **Configurer les paramètres d'abonné** et spécifiez les éléments suivants :
   - Type d'interface : Spécifiez **RadiusAndGX**.
   - Configurez un serveur virtuel de Diameter, un domaine PCRF et les paramètres de l'interface GX de l'abonné.
   - Spécifiez les paramètres de l'interface RADIUS.
5. Accédez à **Gestion du trafic** > **Chaîne** de **service > Fonction** de service et ajoutez des fonctions de service pour associer un service à valeur ajoutée à un VLAN d'entrée.
6. Accédez à **Système** > **Réseau** > **NAT à grande échelle**. Cliquez sur **Pools** et ajoutez un pool. Cliquez sur **Clients** et ajoutez un client. Cliquez sur **Groupes**, ajoutez un groupe et spécifiez le client. Modifiez le groupe et liez le pool à ce groupe.
7. Accédez à **Système** > **Réseau** > **Profils** réseau et ajoutez un profil réseau. Sélectionnez **Remplacer LSN**. Le cas échéant, accédez à **Système** > **Réseau** > **Paramètres** > **Configurer les paramètres de couche 3** et vérifiez que **Remplacer LSN** n'est pas sélectionné.

8. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs** virtuels et configurez les serveurs virtuels et les services à valeur ajoutée sur l'appliance. Liez les services et le profil réseau au serveur virtuel.
9. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels** et configurez un serveur virtuel, une stratégie et une action. Spécifiez le serveur virtuel d'équilibrage de charge cible.

Pour configurer le chaînage des services sur l'appliance à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **IP** et ajoutez les adresses IP du sous-réseau.
2. Accédez à Système > Réseau > **VLAN** et ajoutez des VLAN, liez les VLAN aux interfaces et aux adresses IP des sous-réseaux.
3. Accédez à **Gestion du trafic** > **Chaîne** de **service > Configurer le VLAN d'entrée du chemin** de service et spécifiez un VLAN d'entrée.
4. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres** > **Configurer les paramètres d'abonné** et spécifiez les éléments suivants :
   - Type d'interface : Spécifiez **RadiusAndGX**.
   - Configurez un serveur virtuel de Diameter, un domaine PCRF et les paramètres de l'interface GX de l'abonné.
   - Spécifiez les paramètres de l'interface RADIUS.
5. Accédez à **Gestion du trafic** > **Chaîne** de **service > Fonction** de service et ajoutez des fonctions de service pour associer un service à valeur ajoutée à un VLAN d'entrée.
6. Accédez à **Système** > **Réseau** > **NAT à grande échelle**. Cliquez sur **Pools** et ajoutez un pool. Cliquez sur **Clients** et ajoutez un client. Cliquez sur **Groupes**, ajoutez un groupe et spécifiez le client. Modifiez le groupe et liez le pool à ce groupe.
7. Accédez à **Système** > **Réseau** > **Profils** réseau et ajoutez un profil réseau. Sélectionnez **Remplacer LSN**. Le cas échéant, accédez à **Système** > **Réseau** > **Paramètres** > **Configurer les paramètres de couche 3** et vérifiez que **Remplacer LSN** n'est pas sélectionné.
8. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs** virtuels et configurez les serveurs virtuels et les services à valeur ajoutée sur l'appliance. Liez les services et le profil réseau au serveur virtuel.
9. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels** et configurez un serveur virtuel, une stratégie et une action. Spécifiez le serveur virtuel d'équilibrage de charge cible.

Chaîne de service prenant en compte les abonnés

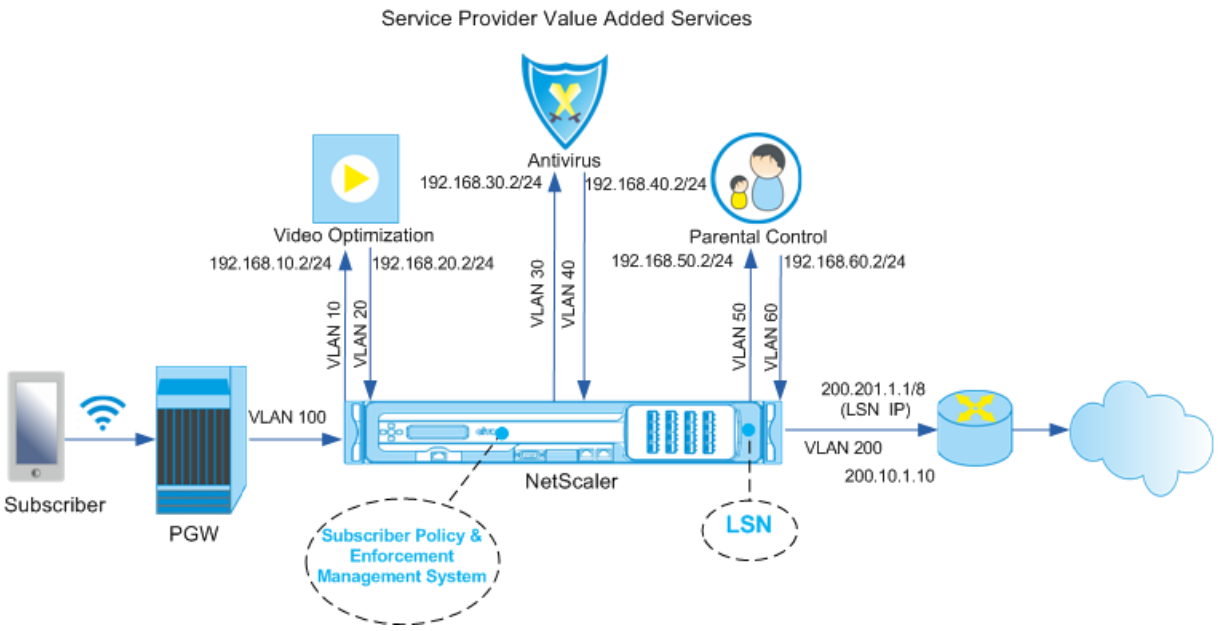
August 20, 2021

Avec l'augmentation considérable du trafic de données passant par les réseaux de télécommunications, il n'est plus possible pour les prestataires de services de diriger tout le trafic via tous les services à valeur ajoutée (SAV). Un fournisseur de services devrait être en mesure d'optimiser l'utilisation du SAV et de diriger intelligemment le trafic afin d'améliorer l'expérience utilisateur. Par exemple, l'optimisation vidéo n'est pas requise pour le trafic qui n'inclut pas de vidéo. De plus, si un abonné est connecté à un réseau 4G, le contenu peut être diffusé en continu en haute définition (HD), et l'optimisation vidéo peut ne pas être nécessaire. Cependant, l'optimisation vidéo améliore l'expérience pour un utilisateur dans un réseau 3G. De même, la mise en cache offre une expérience utilisateur plus rapide et meilleure et peut être activée en fonction de l'abonnement. Un autre exemple de SAV est le contrôle parental. Si les parents fournissent un combiné mobile à un enfant mineur, ils aimeraient avoir une sorte de contrôle sur les sites Web que leur enfant visite.

Pour faire ce qui précède et plus encore, les fournisseurs de services doivent être en mesure de fournir des services à valeur ajoutée par abonné. En d'autres termes, les entités du réseau des fournisseurs de services doivent être capables d'extraire les informations de l'abonné et de diriger intelligemment le paquet sur la base de ces informations.

Le chaînage des services détermine l'ensemble des services par lesquels le trafic d'un abonné doit passer avant d'accéder à Internet. Au lieu d'envoyer tout le trafic à tous les services, Citrix ADC achemine intelligemment toutes les demandes d'un abonné vers un ensemble spécifique de services sur la base de la stratégie définie pour cet abonné.

La figure suivante montre les entités impliquées dans le chaînage des services. Les valeurs affichées sont configurées dans la procédure qui suit la figure. Un serveur virtuel de commutation de contenu sur l'appliance Citrix ADC dirige les demandes vers les services à valeur ajoutée ou les ignore, en fonction de la règle définie, puis envoie le paquet vers Internet après avoir effectué LSN.



Pour configurer le chaînage de service pour le déploiement ci-dessus à l'aide de l'interface de ligne de commande

Ajoutez les adresses SNIP de sous-réseau (SNIP) de l'appliance.

Exemple :

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 192.168.30.1 255.255.255.0 -type snip

add ns ip 192.168.40.1 255.255.255.0 -type snip

add ns ip 192.168.50.1 255.255.255.0 -type snip

add ns ip 192.168.60.1 255.255.255.0 -type snip

add ns ip 100.1.1.1 255.0.0.0 -type snip

add ns ip 200.201.1.1 255.0.0.0 -type snip
<!--NeedCopy-->
```

Ajoutez les VLAN. Les VLAN aident l'appliance à identifier la source du trafic. Liez les VLAN aux interfaces et aux adresses IP de sous-réseau. Ajoutez un VLAN d'entrée et un VLAN de sortie pour chaque SAV.

Exemple :

```
add vlan 10

add vlan 20

add vlan 30

add vlan 40

add vlan 50

add vlan 60

add vlan 100

add vlan 200

bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.30.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.40.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.50.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.60.1 255.255.255.0

bind vlan 100 -ifnum 1/2 -tagged -IPAddress 100.1.1.1 255.0.0.0

bind vlan 200 -ifnum 1/3 -tagged -IPAddress 200.201.1.1 255.0.0.0
<!--NeedCopy-->
```

Spécifiez le VLAN sur lequel le trafic d'abonnés arrive sur l'appliance. Spécifiez le chemin d'accès du service AVP qui indique à l'appliance où rechercher le nom du chemin d'accès du service dans la session d'abonné. Pour la fonctionnalité PCEF principale, spécifiez InterfaceType comme RadiusAndGX.

Exemple :

```
set ns param -servicePathIngressVLAN 100

set subscriber gxinterface -servicepathAVP 1001 1005 -
    servicepathVendorid 10415
```



```
4
5 set subscriber param -interfaceType RadiusAndGx
6 <!--NeedCopy-->
```

Configurez un service et un serveur virtuel de type Diameter et liez le service au serveur virtuel. Ensuite, spécifiez les paramètres de l'interface Gx du domaine PCRF et de l'abonné. Pour la fonctionnalité PCEF principale, configurez un service d'écoute RADIUS et une interface RADIUS.

Exemple :

```
1 add service sd1 10.102.232.200 DIAMETER 3868
2
3 add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
     persistAVPno 263
4
5 bind lb vserver vdiam sd1
6
7 set ns diameter -identity netscaler.sc1.net -realm pcrf1.net
8
9 set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net -
     holdOnSubscriberAbsence YES -idleTTL 1200 -negativeTTL 120
10
11 add service srad1 10.102.232.236 RADIUSListener 1813
12
13 set subscriber radiusInterface -listeningService srad1
14 <!--NeedCopy-->
```

Ajoutez des fonctions de service pour associer un VAS à un VLAN d'entrée. Ajoutez un chemin de service pour définir la chaîne, c'est-à-dire spécifier le VAS auquel le paquet doit être envoyé et l'ordre dans lequel il doit aller dans ce VAS. Le nom du chemin d'accès du service est généralement envoyé par le PCRF. Toutefois, le chemin d'accès du service du profil d'abonné par défaut (*) s'applique si l'une des conditions suivantes est remplie :

- Le PCRF ne possède pas les informations sur l'abonné.
- Les informations sur l'abonné ne comprennent pas cet AVP.
- L'appliance ne peut pas interroger le PCRF. Par exemple, le service représentant le PCRF est DOWN.

Le chemin de service AVP qui contient ce nom doit être configuré dans le cadre de la configuration globale antérieure. Liez la fonction de service au chemin d'accès du service. L'index de service spécifie l'ordre dans lequel le SAV est ajouté à la chaîne. Le nombre le plus élevé (255) indique le début de la chaîne.

Exemple :


```
add ns servicefunction SF1 -ingressVLAN 20

add ns servicefunction SF2 -ingressVLAN 40

add ns servicefunction SF3 -ingressVLAN 60

add ns servicepath pol1

bind ns servicepath pol1 -servicefunction SF1 -index 255

bind ns servicepath pol1 -servicefunction SF2 -index 254

bind ns servicepath pol1 -servicefunction SF3 -index 253

add ns servicepath pol2

bind ns servicepath pol2 -servicefunction SF2 -index 255

add ns servicepath pol3

bind ns servicepath pol3 -servicefunction SF1 -index 255

add subscriber profile * -subscriberrules default_path
<!--NeedCopy-->
```

Ajoutez la configuration LSN. Autrement dit, définissez le pool NAT et identifiez les clients pour lesquels l'appliance doit exécuter LSN.

Exemple :

```
add lsn pool pool1

bind lsn pool pool1 200.201.1.1

add lsn client client1

bind lsn client client1 -network 100.0.0.0 -netmask 255.0.0.0

add lsn group group1 -clientname client1

bind lsn group group1 -poolname pool1
<!--NeedCopy-->
```

L'appliance exécute LSN par défaut. Pour remplacer LSN, vous devez créer un profil net avec le paramètre overridelsN activé et lier ce profil à tous les serveurs virtuels d'équilibrage de charge

configurés pour les services à valeur ajoutée (vASs).

Exemple :

```
add netprofile np1

set netprofile np1 -overrideLsn ENABLED

set lb vserver vs1 -netprofile np1
<!--NeedCopy-->
```

Configurez le VAS sur l'appliance. Cela inclut la création des services et des serveurs virtuels, puis la liaison des services aux serveurs virtuels.

Exemple :

```
add service vas1 192.168.10.2 ANY 80 -usip YES

add service vas2 192.168.30.2 ANY 80 -usip YES

add service vas3 192.168.50.2 ANY 80 -usip YES

add service sint 200.10.1.10 ANY 80 -usip YES

add lb vserver vs1 ANY -m MAC -l2Conn ON

add lb vserver vs2 ANY -m MAC -l2Conn ON

add lb vserver vs3 ANY -m MAC -l2Conn ON

add lb vserver vint ANY -m MAC -l2Conn ON

bind lb vserver vs1 vas1

bind lb vserver vs2 vas2

bind lb vserver vs3 vas3

bind lb vserver vint sint
<!--NeedCopy-->
```

Ajoutez la configuration de commutation de contenu (CS). Cela inclut les serveurs virtuels, les stratégies et les actions associées. Le trafic arrive au serveur virtuel CS et est ensuite redirigé vers le serveur virtuel d'équilibrage de charge approprié. Définissez les expressions qui associent un serveur virtuel à une fonction de service.

Exemple :

```
add cs vserver cs1 ANY * 80 -l2Conn ON

add cs action csact1 -targetLBVserver vs1

add cs action csact2 -targetLBVserver vs2

add cs action csact3 -targetLBVserver vs3

add cs action csactint -targetLBVserver vint

add cs policy cspol1 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF1") &&
   SYS.VSERVER("vs1").STATE.EQ(UP)" -action csact1

add cs policy cspol2 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF2") &&
   SYS.VSERVER("vs2").STATE.EQ(UP)" -action csact2

add cs policy cspol3 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF3") &&
   SYS.VSERVER("vs3").STATE.EQ(UP)" -action csact3

bind cs vserver cs1 -policyName cspol1 -priority 110

bind cs vserver cs1 -policyName cspol2 -priority 120

bind cs vserver cs1 -policyName cspol3 -priority 130

bind cs vserver cs1 -lbvserver vint
<!--NeedCopy-->
```

Pour configurer le chaînage des services sur l'appliance à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **IP** et ajoutez les adresses IP du sous-réseau.
2. Accédez à **Système** > **Réseau** > **VLAN** et ajoutez des VLAN, Liez les VLAN aux interfaces et aux adresses IP du sous-réseau.
3. Accédez à **Gestion du trafic** > **Chaîne** de **service > Configurer le VLAN d'entrée du chemin** de service et spécifiez un VLAN d'entrée.
4. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres** > **Configurer les paramètres d'abonné** et spécifiez les éléments suivants :
   - Type d'interface : Spécifiez **RadiusAndGX**.
   - Configurez un serveur virtuel de Diameter, un domaine PCRF et les paramètres de l'interface GX de l'abonné.

- Spécifiez les paramètres de l'interface RADIUS.

5. Accédez à **Gestion du trafic** > **Chaîne** de **service > Fonction** de service et ajoutez des fonctions de service pour associer un service à valeur ajoutée à un VLAN d'entrée.
6. Accédez à **Système** > **Réseau** > **NAT à grande échelle**. Cliquez sur **Pools** et ajoutez un pool. Cliquez sur **Clients** et ajoutez un client. Cliquez sur **Groupes**, ajoutez un groupe et spécifiez le client. Modifiez le groupe et liez le pool à ce groupe.
7. Accédez à **Système** > **Réseau** > **Profils** réseau et ajoutez un profil réseau. Sélectionnez **Remplacer LSN**. Le cas échéant, accédez à **Système** > **Réseau** > **Paramètres** > **Configurer les paramètres de couche 3** et vérifiez que **Remplacer LSN** n'est pas sélectionné.
8. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs** virtuels et configurez les serveurs virtuels et les services à valeur ajoutée sur l'appliance. Liez les services et le profil réseau au serveur virtuel.
9. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels** et configurez un serveur virtuel, une stratégie et une action. Spécifiez le serveur virtuel d'équilibrage de charge cible.

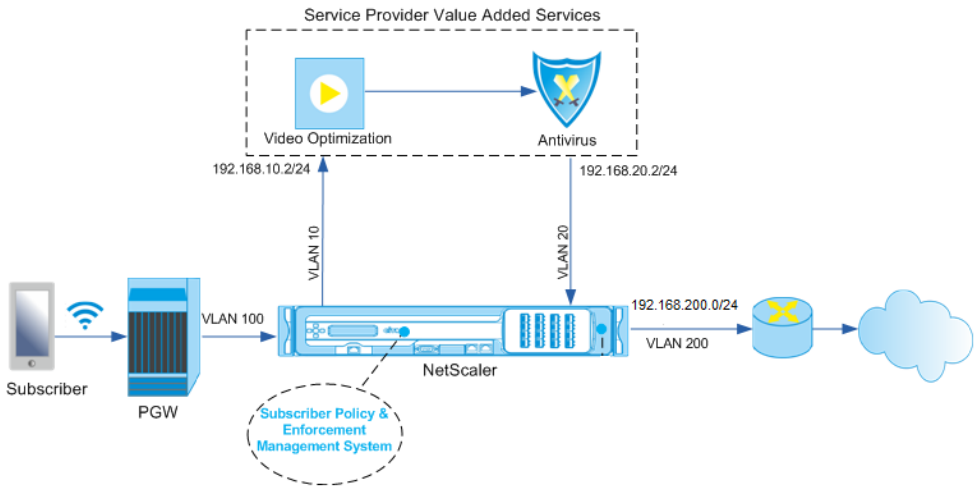
Orientation du trafic des abonnés avec optimisation TCP

January 21, 2021

La direction de la circulation dirige le trafic des abonnés d'un point à l'autre. Lorsqu'un abonné se connecte au réseau, la Gateway de paquets associe une adresse IP à l'abonné et transfère le paquet de données à l'appliance Citrix ADC. L'appliance communique avec le serveur PCRF via l'interface Gx pour obtenir les informations de stratégie de l'abonné. Selon les informations de stratégie, l'appliance effectue l'une des actions suivantes :

- Transférer le paquet de données à un autre ensemble de services (comme illustré dans l'illustration suivante).
- Effectuer uniquement l'optimisation TCP.

Les valeurs indiquées dans la figure suivante sont configurées dans la procédure CLI qui suit la figure. Un serveur virtuel de commutation de contenu sur l'appliance Citrix ADC dirige les demandes vers les services à valeur ajoutée ou les ignore et effectue l'optimisation TCP, en fonction de la règle définie, puis envoie le paquet vers Internet.



> **Remarque**
>
> La prise en charge de la configuration ci-dessous a été introduite dans la version 11.1 build 50.10.

Pour configurer la direction du trafic pour le déploiement ci-dessus à l'aide de l'interface de ligne de commande :

1. Ajoutez les adresses SNIP de sous-réseau (SNIP) de l'appliance.

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 192.168.100.1 255.255.255.0 -type snip

add ns ip 192.168.200.1 255.255.255.0 -type snip

add ns ip 10.102.232.236 255.255.255.0  - type snip
<!--NeedCopy-->
```

2. Ajoutez les VLAN. Les VLAN aident l'appliance à identifier la source du trafic. Liez les VLAN aux interfaces et aux adresses IP de sous-réseau.

```
add vlan 10

add vlan 20

add vlan 100

add vlan 200

```



```
add vlan 102

bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1
    255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1
    255.255.255.0

bind vlan 100 -ifnum 1/2 -tagged -IPAddress 192.168.100.1
    255.255.255.0

bind vlan 200 -ifnum 1/2 -tagged -IPAddress 192.168.200.1
    255.255.255.0

bind vlan 102  - ifnum 1/1  - tagged  - IPAddress 10.102.232.236
    255.255.255.0
<!--NeedCopy-->
```

3. Configurez un service et un serveur virtuel de type Diameter et liez le service au serveur virtuel. Spécifiez le domaine PCRF et les valeurs pour les paramètres de l'interface Gx de l'abonné. Spécifiez également le chemin d'accès du service AVP qui indique où l'appliance peut trouver le nom du chemin d'accès du service dans la session d'abonné. Pour la fonctionnalité PCEF principale, configurez un service d'écoute RADIUS et une interface RADIUS, puis spécifiez le type d'interface comme « RadiusAndGX ».

```
add service sd1 10.102.232.200 DIAMETER 3868

add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER
    -persistAVPno 263

bind lb vserver vdiam sd1

set ns diameter -identity netscaler.sc1.net -realm pcrf1.net

set extendedmemoryparam -memLimit 2558

set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net

set subscriber gxinterface -servicepathAVP 1001 1005 -
    servicepathVendorid 10415

add service srad1 10.102.232.236 RADIUSListener 1813

set subscriber radiusInterface -listeningService srad1
```



```
18
19 set subscriber param -interfaceType RadiusAndGx
20 <!--NeedCopy-->
```

4. Spécifiez un profil d'abonné par défaut (*) à appliquer si l'une des conditions suivantes est remplie :

   - Le PCRF ne possède pas les informations sur l'abonné.
   - Les informations de l'abonné n'incluent pas le chemin de service AVP.
   - L'appliance ne peut pas interroger le PCRF. Par exemple, le service représentant le PCRF est DOWN.

```
1 add subscriber profile * -subscriberrules default_path
2 <!--NeedCopy-->
```

5. Créez des profils TCP pour le chemin d'optimisation VAS et TCP, respectivement. Le trafic dirigé vers le VAS ne subira aucune optimisation TCP avant ou après avoir quitté le VAS. Par conséquent, le mode TCP du profil VAS doit être défini sur TRANSPARENT tandis que le mode TCP du profil TCPopt doit être défini sur ENDPOINT.

   add ns tcpProfile VAS –tcpMode TRANSPARENT

   add ns tcpProfile TCPOpt -WS ENABLED -SACK ENABLED -WSVal 8 -mss 1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -fack ENABLED -rstMaxAck enABLED -tcpmode ENDPOINT

6. Configurez l'équilibrage de charge pour les serveurs VAS. Créez un serveur virtuel non adressable de type TCP. Créez des services TCP avec les adresses IP des serveurs VAS et liez les services au serveur virtuel. Le serveur virtuel et les services utiliseront le profil TCP transparent créé pour le chemin du VAS :

```
1 add service vas1 192.168.10.2 TCP * -usip YES -useproxyport NO -
     TCPB NO -tcpProfileName VAS
2
3 add service vas2 192.168.10.3 TCP * -usip YES -useproxyport NO -
     TCPB NO -tcpProfileName VAS
4
5 add lb vserver vs1 TCP -m MAC -l2Conn ON  - tcpProfileName VAS
6
7 bind lb vserver vs1 vas1
8
9 bind lb vserver vs1 vas2
10 <!--NeedCopy-->
```


7. Ajoutez un serveur virtuel d'équilibrage de charge pour capturer le trafic de sortie du VAS. Ce vserver surveillera le VLAN de sortie du VAS et utilisera le profil TCP transparent :

```
add lb vserver vsint TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ(20)"
     -Listenpriority 30 -l2Conn ON -tcpProfileName VAS
<!--NeedCopy-->
```

8. Ajoutez un serveur virtuel d'optimisation TCP qui écoute tout trafic dans le VLAN côté sans fil et utilise le profil TCP de point de terminaison créé pour le chemin d'optimisation TCP :

```
add lb vserver vs-TcpOpt TCP * * -Listenpolicy "client.vlan.id.eq
   (100)" -Listenpriority 20 -l2Conn ON -tcpProfileName TCPOpt
<!--NeedCopy-->
```

9. Ajoutez la configuration de commutation de contenu (CS). Cela inclut les serveurs virtuels, les stratégies et les actions associées. Le serveur virtuel CS reçoit le trafic et le redirige vers le serveur virtuel d'équilibrage de charge approprié selon les stratégies CS définies. Créez un serveur virtuel CS TCP qui écoute tout trafic dans le VLAN côté sans fil avec la plus haute priorité et utilise le profil TCP du point de terminaison. Créez une stratégie CS évaluant TRUE lorsque « vas » est la règle d'abonné et spécifiez une action CS qui dirige le trafic vers VAS. Faites du serveur virtuel d'optimisation TCP le serveur LB par défaut. Tout trafic d'abonné avec une règle autre que « vas » passera par le serveur LB par défaut.

```
add cs vserver cs1 TCP * * -Listenpolicy "client.vlan.id.eq(100)"
     -Listenpriority 10 -l2Conn ON -tcpProfileName TCPOpt

add cs action csact1 -targetLBVserver vs1

add cs policy cspol1 -rule  SUBSCRIBER.RULE_ACTIVE("vas") && SYS.
   VSERVER("vs1").STATE.EQ(UP)" -action csact1

bind cs vserver cs1 -policyName cspol1

bind cs vserver cs1 -lbvserver vs-TcpOpt
<!--NeedCopy-->
```

10. Ajouter des routes statiques ou basées sur des stratégies à Internet. Le routage dynamique est également pris en charge dans cette configuration. L'exemple suivant utilise des itinéraires basés sur des stratégies :

```
add ns pbr pbr-vlan100-to-vlan200 ALLOW -nextHop 192.168.200.10 -
   vlan 100 -priority 10

```



```
add ns pbr pbr-vlan20-to-vlan200 ALLOW -nextHop 192.168.200.10 -
    vlan 20 -priority 11

apply ns pbrs
<!--NeedCopy-->
```

Remarque

- Les stratégies CS peuvent contenir des adresses IP et des numéros de port en plus des expressions d'abonné (par exemple, SUBSCRIBER.RULE_ACTIVE("vas") && && (CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443). Ils peuvent également contenir des expressions basées sur HTTP, par exemple, HTTP.REQ.HOSTNAME.DOMAIN.EQ("somedomain.com Dans ce cas, remplacez les entités TCP (vserver, service, etc.) par HTTP. La configuration du profil TCP reste la même.
- Ajoutez une configuration IPv6 (adresses, routes, PBR) pour prendre en charge les abonnés IPv6. Les applications clientes Happy Eyeballs fonctionneront sans problème pour les chemins d'optimisation VAS et TCP.
- Ajoutez des VLAN, des adresses IP, des PBR et des serveurs virtuels LB devant VAS (vs1, vs2, etc.) pour prendre en charge plusieurs flux d'abonnés. Modifiez les stratégies d'écoute de CS vserver « cs1" et LB vserver « vsint » pour inclure les VLAN supplémentaires.

Sélection de profil TCP basée sur des stratégies

January 21, 2021

Vous pouvez configurer l'appliance Citrix ADC pour effectuer l'optimisation TCP en fonction des attributs d'abonné. Par exemple, l'appliance peut sélectionner différents profils TCP au moment de l'exécution, en fonction du réseau auquel l'équipement utilisateur (UE) est connecté. Par conséquent, vous pouvez améliorer l'expérience d'un utilisateur mobile en définissant certains paramètres dans les profils TCP, puis en utilisant des stratégies pour sélectionner le profil approprié.

Créez des profils TCP distincts pour les abonnés qui se connectent via un réseau 4G et pour les utilisateurs qui se connectent via un autre réseau. Définissez une règle de stratégie sélectionnée sur la base d'un paramètre d'abonné, tel que RAT-Type. Dans les exemples suivants, si le type RAT est EUTRAN, un profil TCP prenant en charge une connexion plus rapide est sélectionné (exemple 1). Pour toutes les autres valeurs de type Rat, un profil TCP différent est sélectionné (exemple 2).

Remarque

L'AVP de type RAT (code AVP 1032) est de type Enuméré et sert à identifier la technologie d'accès radio qui dessert l'UE.

> La valeur « 1004” indique que le RAT est EUTRAN. (RFC 29.212).

Example1:

```
add ns tcpProfile tcp2 -WS ENABLED -SACK ENABLED -WSVal 8 -initialCwnd
    16 - oooQSize 15000 -slowStartIncr 1 -bufferSize 1000000 -flavor BIC
     - dynamicReceiveBuffering DISABLED -sendBuffsize 1000000 -dsack
    DISABLED -maxcwnd 4000000 -fack ENABLED -minRTO 500 -maxburst 15

add appqoe action appact2 -priority HIGH -tcpprofile tcp2

add appqoe policy apppol2 -rule "SUBSCRIBER.AVP(1032).VALUE.
    GET_UNSIGNED32(0, BIG_ENDIAN).EQ(1004)" -action appact2

bind cs vserver <name>  -policyname apppol2 -priority 20 -type request
<!--NeedCopy-->
```

Example2:

```
add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -initialCwnd
    16 - oooQSize 15000 -slowStartIncr 1 -bufferSize 150000 -flavor BIC
    - dynamicReceiveBuffering DISABLED -sendBuffsize 150000 -dsack
    DISABLED -maxcwnd 4000000 -fack ENABLED -minRTO 200 -maxburst 15

add appqoe action appact1 -priority HIGH -tcpprofile tcp1

add appqoe policy apppol1 -rule "SUBSCRIBER.AVP(1032).VALUE.
    GET_UNSIGNED32(0, BIG_ENDIAN).NE(1004)" -action appact1

bind cs vserver <name>  -policyname apppol1 -priority 10 -type request
<!--NeedCopy-->
```

Trafic de plan de contrôle d’équilibrage de charge basé sur les protocoles Diameter, SIP et SMPP

August 20, 2021

Avec l’augmentation du trafic du plan de contrôle, les serveurs peuvent devenir un goulot d’étranglement car le trafic n’est pas réparti de manière optimale entre les serveurs. Par conséquent, les messages doivent être équilibrés de charge. L’appliance Citrix ADC prend en charge l’équilibrage de charge de Diameter, SIP et SMPP.

SIP

Citrix ADC vous permet d'équilibrer la charge des messages SIP via UDP ou TCP (y compris TLS) vers un groupe de serveurs proxy. Citrix ADC fournit également la persistance et la méthode d'équilibrage de charge de hachage d'ID d'appel basée sur l'ID d'appel à l'aide de laquelle vous dirigez les paquets pour une session SIP particulière vers le même serveur SIP équilibré de charge.
Le langage d'expressions par défaut Citrix ADC contient un certain nombre d'expressions qui fonctionnent sur les connexions SIP (Session Initiation Protocol). Ces expressions sont destinées à être utilisées dans les stratégies pour le protocole SIP qui fonctionne sur une base demande/réponse. Ces expressions peuvent être utilisées dans les stratégies de commutation de contenu, de limitation de débit, de répondeur et de réécriture.

Pour plus d'informations, consultez la section Équilibrage de charge d'un groupe de serveurs SIP.

SMPP

Des millions de messages courts sont échangés quotidiennement entre des particuliers et des fournisseurs de services à valeur ajoutée, tels que les banques, les annonceurs et les services d'annuaire, à l'aide du protocole SMPP (Short Message peer to peer). Souvent, la remise des messages est retardée parce que les serveurs sont surchargés et que le trafic n'est pas réparti de manière optimale entre les serveurs.
l'appliance Citrix ADC fournit une distribution optimale des messages sur vos serveurs, évitant ainsi les mauvaises performances et les pannes. L'appliance Citrix ADC :

- Équilibre de charge des messages provenant du serveur et du client
- Surveille l'état des centres de messages
- Prise en charge de la commutation de contenu pour les centres de messages
- Gère les messages concaténés

Limitation : Les ID de message, provenant du centre de message, de plus de 59 octets, ne sont pas pris en charge. Si la longueur de l'ID de message renvoyée par le centre de messages est supérieure à 59 octets, les opérations auxiliaires échouent et l'appliance Citrix ADC répond par un message d'erreur.

Pour plus d'informations, voir Équilibrage de charge SMPP

Diameter

Diameter est un protocole de base avec plus de 50 protocoles (également appelés applications) construits sur lui. Par conséquent, le trafic de Diameter généré dans un réseau Telco est élevé. Pour maintenir de manière optimale ce trafic de Diameter, l'appliance Citrix ADC effectue l'équilibrage de charge, la commutation de contenu et agit en tant qu'agent relais. En outre, l'appliance offre des fonctionnalités de réécriture et de répondeur. L'appliance prend en charge la limitation de débit des messages de Diameter.

Pour plus d'informations, voir Configuration de l'équilibrage de charge de diamètre.

Fournir des services d'infrastructure DNS et de trafic, tels que l'équilibrage de charge, la mise en cache et la journalisation pour les fournisseurs de services de télécommunication

August 20, 2021

Les fournisseurs de services de télécommunication peuvent configurer l'appliance Citrix ADC pour qu'elle fonctionne comme un proxy DNS. La mise en cache des enregistrements DNS, qui est une fonction importante d'un proxy DNS, est activée par défaut sur l'appliance Citrix ADC. Cela permet à l'appliance Citrix ADC de fournir des réponses rapides pour les traductions répétées, améliorant ainsi l'expérience client et économise également la bande passante. Le cache les réponses des serveurs de noms DNS. Lorsque l'appliance reçoit une requête DNS, elle vérifie le domaine interrogé dans son cache. Si l'adresse du domaine interrogé est présente dans son cache, l'appliance Citrix ADC renvoie l'adresse correspondante au client. Sinon, il transfère la requête à un serveur de noms DNS qui vérifie la disponibilité de l'adresse et la renvoie à l'appliance Citrix ADC. L'appliance Citrix ADC renvoie ensuite l'adresse au client.

Pour les demandes d'un domaine qui a été mis en cache précédemment, l'appliance Citrix ADC sert l'enregistrement Adresse du domaine à partir du cache sans interroger le serveur DNS configuré et enregistre donc la bande passante.

À partir de la version 11.0, Citrix ADC enregistre également les demandes DNS qu'il reçoit ainsi que les réponses qu'il envoie au client. Les fournisseurs de services de télécommunication peuvent utiliser ce journal pour :

- Audit des réponses DNS au client
- Audit des clients DNS
- Détecter et empêcher les attaques DNS
- Résolution des problèmes

Pour plus d'informations, voir Système de noms de domaine.

Fournir une distribution de la charge d'abonné à l'aide de GSLB sur les réseaux de base d'un fournisseur de services de télécommunication

August 20, 2021

L'évolutivité, la haute disponibilité et les performances sont essentielles aux déploiements des fournisseurs de services. Bien que de nombreux fournisseurs de services y déploient une infrastructure à un seul emplacement ou à plusieurs emplacements, ces déploiements sont soumis à un certain nombre de limitations inhérentes, telles que :

- Si le site perd la connectivité à tout ou partie de l'Internet public, il sera inaccessible aux utilisateurs et aux clients, ce qui peut avoir un impact significatif sur l'entreprise.
- Les utilisateurs qui accèdent au site à partir d'emplacements géographiquement éloignés peuvent subir des retards importants et très variables, exacerbés par le grand nombre de voyages aller-retour dont HTTP a besoin pour transférer du contenu.

Le Global Server Load Balancing (GSLB) de l'appliance Citrix ADC permet de résoudre ces problèmes en répartissant le trafic entre les sites déployés dans plusieurs emplacements géographiques. En diffusant du contenu provenant de nombreux points différents sur Internet, GSLB atténue l'impact des goulots d'étranglement de la bande passante réseau et assure la robustesse en cas de panne réseau sur un site particulier. Les utilisateurs peuvent être automatiquement dirigés vers le site le plus proche ou le moins chargé au moment de la demande, ce qui minimise la probabilité de longs retards de téléchargement et/ou d'interruptions de service.

Vous pouvez utiliser l'équilibrage de charge du serveur global de l'appliance Citrix ADC pour :

- Récupération après sinistre ou haute disponibilité en configurant un centre de données actif en attente qui se compose d'un centre de données actif et d'un centre de données de secours. Lorsqu'un basculement survient à la suite d'un sinistre, le centre de données de secours devient opérationnel.
- Haute disponibilité et vitesse grâce à la configuration d'un centre de données actif composé de plusieurs centres de données actifs. Les demandes des clients sont équilibrées de charge entre les datacenters actifs.
- Diriger les demandes des clients vers le centre de données qui est le plus proche en distance géographique ou en distance réseau en configurant une configuration de proximité.
- Résolutions DNS complètes, GSLB traite les requêtes DNS des types A, AAAA et CNAME, et l'option de fonction DNS peut traiter les requêtes DNS de tous les autres types, tels que MX et PTR. En outre, si la résolution récursive est activée, l'appliance transmet les requêtes DNS pour les noms de domaine qui ne sont pas configurés sur l'appliance Citrix ADC.

Pour plus d'informations, voir Global Server Load Balancing.

Utilisation de la bande passante à l'aide de la fonctionnalité de redirection de cache

August 20, 2021

Le volume de trafic Web sur Internet est énorme et un pourcentage important de ce trafic est redondant. Plusieurs clients demandent à des serveurs Web le même contenu à plusieurs reprises, ce qui entraîne une utilisation inefficace de la bande passante. Pour supprimer le serveur Web d'origine du traitement de chaque requête, les fournisseurs de services Internet (FAI) peuvent utiliser la fonctionnalité de redirection de cache de l'appliance Citrix ADC et servir le contenu à partir d'un serveur de cache plutôt que du serveur d'origine. L'appliance Citrix ADC analyse les demandes entrantes, envoie des demandes de données mises en cache aux serveurs de cache et envoie des demandes non mises en cache et des requêtes HTTP dynamiques aux serveurs d'origine. La fonction de redirection du cache de Citrix ADC est basée sur des stratégies et, par défaut, les demandes correspondant à une stratégie sont envoyées au serveur d'origine et toutes les autres demandes sont envoyées à un serveur de cache. Vous pouvez combiner la commutation de contenu avec la redirection de cache pour mettre en cache du contenu sélectif et diffuser du contenu à partir de serveurs de cache spécifiques pour des types spécifiques de contenu demandé.

Pour plus d'informations, voir Redirection du cache.

Optimisation TCP de Citrix ADC

January 21, 2021

L'appliance Citrix ADC fournit des techniques et des capacités avancées de réglage et d'optimisation TCP qui sont bien adaptées aux réseaux 3.5 et 4G modernes, améliorant ainsi l'expérience utilisateur et les vitesses de téléchargement perçues.

La présente section porte sur des instructions détaillées concernant :

- Choix et insertion d'un modèle Citrix ADC T1000 Series approprié dans un réseau mobile pour l'optimisation TCP
- Instructions de configuration complètes liées non seulement à l'optimisation TCP, mais aussi à la configuration appropriée des couches 2 et 3 du périphérique T1

La section comprend les rubriques suivantes :

- Mise en route
- Réseau de gestion
- Système de licences
- Haute disponibilité
- Intégration Gi-LAN
- Configuration de l'optimisation TCP
- Optimisation des performances TCP à l'aide de TCP NILE
- Analyses et rapports
- Statistiques en temps réel

- SNMP
- Recettes techniques
- Instructions de dépannage
- Questions fréquemment posées

Mise en route

August 20, 2021

Matériel

Citrix fournit un large éventail de modèles Citrix ADC qui peuvent être lâchement basés sur deux facteurs :

- Capacité, qui va actuellement de centaines de Mbit/s pour l'appliance VPX bas de gamme à 160 Gbit/s pour l'appliance haut de gamme 25000 MPX
- Niveau Telco, avec la disponibilité de la série T1000 pour les datacenters Telco.

Votre représentant des ventes ou du support Citrix peut vous aider à sélectionner le matériel approprié pour vos besoins de démonstration, d'essai ou de production.

Le reste de cette section utilise un Citrix ADC T1200 comme matériel de référence. Notez que mettre de côté les différences superficielles liées au nombre et à la notation des interfaces disponibles (voir ⋆ en note) ou les limitations bien documentées de Citrix ADC VPX (voir ⋆ en note), les instructions doivent s'appliquer principalement verbatim quel que soit le modèle Citrix ADC sélectionné.

> **Remarque**
>
> ⋆ Par exemple, un modèle T1010 n'a que 12x1GbE généralement marqué 1/1-1/12 plutôt que la notation 10/x utilisée dans ce document.
>
> ⋆⋆ Une instance Citrix ADC VPX ne prend généralement pas en charge l'agrégation LACP ; elle peut également ne pas prendre en charge le balisage VLAN.

Configuration initiale

Via la console série

Une fois qu'un câble série est connecté, vous pouvez vous connecter à l'appliance Citrix ADC avec les informations d'identification suivantes :

- Nom d'utilisateur : nsroot
- Password: nsroot

Une fois connecté, configurez les détails de base de l'appliance Citrix ADC comme indiqué dans la capture d'écran ci-dessous.

Exemple :

```
set ns config  - IPAddress <ip_addr> -netmask <netmask>

saveconfig

reboot -warm
<!--NeedCopy-->
```

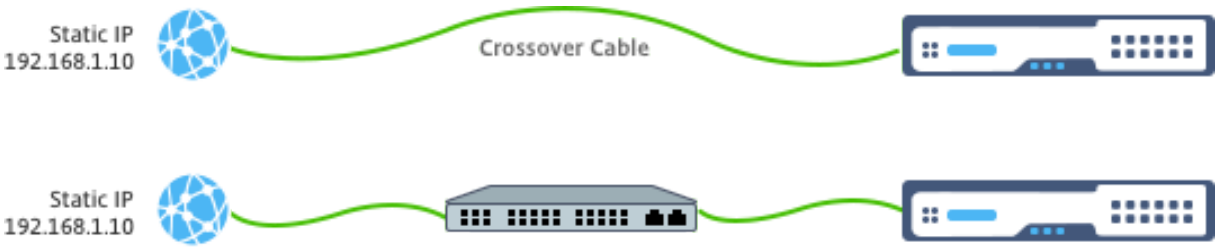
Après le redémarrage de l'appliance, vous pouvez utiliser SSH pour la configuration ultérieure des nœuds T1100.

Par LOM

Le port de gestion des lumières (LOM) situé sur le panneau avant de l'appliance Citrix ADC permet à l'opérateur de surveiller et de gérer à distance l'appliance indépendamment du système d'exploitation. L'opérateur peut modifier l'adresse IP, le cycle d'alimentation et effectuer un vidage de code en se connectant à l'appliance Citrix ADC via le port LOM.

L'adresse IP par défaut du port LOM est 192.168.1.3

figure. Configuration initiale du module LOM



Définissez une adresse IP statique sur votre ordinateur portable et branchez-la directement à l'interface LOM avec un câble croisé ou dans un commutateur dans le même domaine de diffusion que l'interface LOM.

Pour la configuration initiale, tapez l'adresse par défaut du port :http://192.168.1.3 dans un navigateur Web et modifiez l'adresse IP par défaut du port LOM.

Reportez-vous aux Guides de configuration pour plus de détails.

Logiciel

L'optimisation Citrix ADC TCP pour les réseaux mobiles est en constante évolution. Les fonctionnalités et les réglages décrits dans ce document nécessitent une version Citrix ADC Telco. Voici un exemple

montrant la version Citrix ADC Telco.

Exemple :

```
show ver

NetScaler NS11.0: Build 64.957.nc, Date: Aug 26 2016, 02:00:23
<!--NeedCopy-->
```

Si le T1000 n'a pas été livré avec la révision de version appropriée, contactez le support client Citrix ADC.

> **Important**
>
> Les deux appliances doivent avoir la même image logicielle.

Client SSH

Une appliance Citrix ADC peut être configurée à l'aide de l'interface de ligne de commande ou de l'interface graphique HTML5. Toutefois, cette section fournit uniquement des instructions basées sur l'interface utilisateur.

Bien que l'interface de ligne de commande soit accessible via la console série Citrix ADC, il est normalement recommandé d'utiliser un client SSH pour autoriser la configuration de Citrix ADC distante.

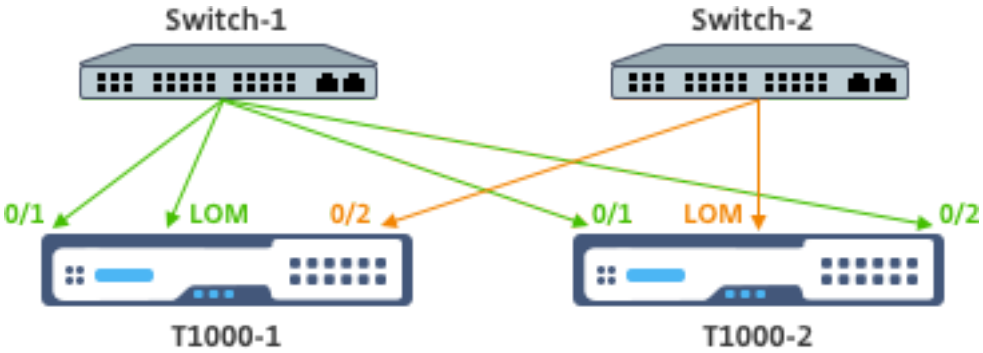
Réseau de gestion

August 20, 2021

Connectivité

La plupart des périphériques Citrix ADC offrent des ports OAM 1 GbE redondants, notés 0/1 et 0/2. Pour assurer la redondance en cas de défaillance d'un commutateur, vous devez connecter les ports pertinents à différents commutateurs en amont.

Un aperçu général de la connectivité recommandée est présenté dans le diagramme suivant :



Une fois que l'appliance Citrix ADC est connectée au réseau de gestion, les étapes de configuration suivantes peuvent être effectuées à distance à l'aide de la connectivité SSH ou Web à l'interface de ligne de commande et à l'interface graphique.

Routage

La commande add route peut être utilisée pour configurer toutes les routes appropriées au réseau de gestion. La Gateway pertinente doit être accessible sur le sous-réseau NSIP, comme indiqué ci-dessous.

Exemple :

```
1 add route <network>  <netmask>  <gateway>
2 <!--NeedCopy-->
```

Système de licences

August 20, 2021

Un fichier de licence valide doit être installé sur l'appliance Citrix ADC. La licence doit prendre en charge au moins autant de Gbit/s que le débit GI-LAN maximal attendu.

Les fichiers de licence doivent être copiés via un client SCP vers le /nsconfig/license de l'appliance, comme indiqué dans la capture d'écran ci-dessous.

Exemple :

```
1 shell ls /nsconfig/license/
2
3 CNS_V3000_SERVER_PLT_Retail.lic ssl
4 <!--NeedCopy-->
```


Faites un redémarrage à chaud pour appliquer la nouvelle licence, comme indiqué dans la capture d'écran ci-dessous.

Exemple :

```
reboot -warm

Are you sure you want to restart NetScaler (Y/N)? [N]:y

Done
<!--NeedCopy-->
```

Une fois le redémarrage terminé, vérifiez que la licence a été correctement appliquée, à l'aide de l'interface de ligne de commande show license.

Dans l'exemple ci-dessous, une licence Premium 3Gbps a été installée avec succès.

Exemple :

```
> show license

            License status:

                                    Web Logging: YES

                                            ...

                                Model Number ID: 3000

                                   License Type: Premium License

Done

<!--NeedCopy-->
```

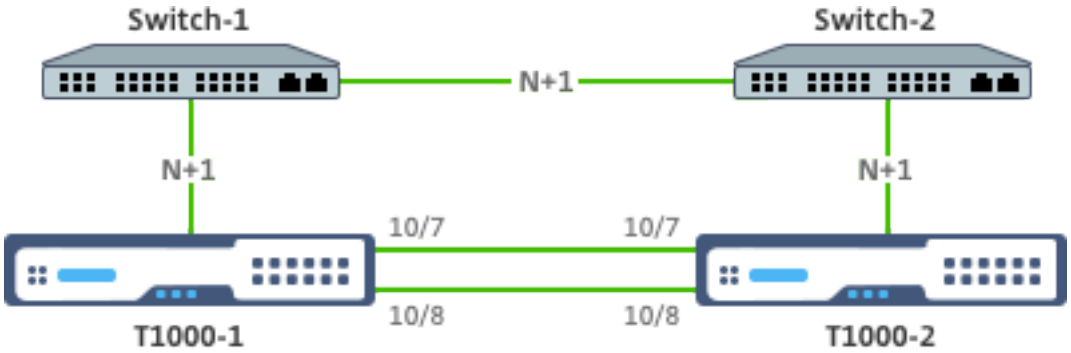
Haute disponibilité

August 20, 2021

La haute disponibilité (HA) fait référence au mode opérationnel actif de veille d'une paire de périphériques Citrix ADC. Chaque appareil a sa propre adresse IP de gestion dédiée. Toutes les autres adresses IP appartiennent au périphérique actif de la paire.

Connectivité

Bien qu'il existe plusieurs options de connectivité pour une paire Citrix ADC HA, la plus recommandée est illustrée dans le diagramme suivant :



Dans le diagramme ci-dessus, les liaisons rouges N+1 entre chaque T1000 et le commutateur respectif impliquent une redondance N+1, comme expliqué dans Connectivité. Par exemple, considérer un Gi-LAN 45 Gbit/s N=5 est une valeur appropriée, avec des canaux LACP 6x10GbE entre chaque commutateur et le T1000 respectif ainsi qu'entre les deux commutateurs.

Une paire de liens supplémentaire est recommandée entre la paire Citrix ADC, afin d'assurer l'isolation de communication HA à partir du réseau OAM.

Intégration Gi-LAN

August 20, 2021

En règle générale, une appliance Citrix ADC est insérée en tant que nœud Inline L3 distinct dans le Gi-LAN, de la même manière qu'un routeur L3.

Figure : Une représentation simple d'un Gi-LAN

Connectivité

Une connectivité physique de Citrix ADC aux commutateurs en amont est recommandée pour assurer une redondance suffisante. Par exemple, en supposant qu'une appliance Citrix ADC soit insérée dans

un LAN GI-LAN qui gère un total (liaison montant+liaison descendante) de 24 Gbps, la connectivité avec des interfaces 4x10GbE ou plus est recommandée. Cela permet effectivement une redondance N+1 en cas de panne de liaison.

Les ports pertinents du commutateur en amont doivent être configurés pour l'agrégation des ports LACP. La configuration pertinente sur Citrix ADC est décrite ci-dessous :

Configuration de la connectivité :

```
set interface 10/1 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/2 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/3 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/4 -tagall ON -lacpMode ACTIVE -lacpKey 1
<!--NeedCopy-->
```

Vous pouvez vérifier la fonctionnalité appropriée de LACP à l'aide de la commande « show interface » :

show interface:

```
sh interface LA/1

    1)      Interface LA/1 (802.3ad Link Aggregate) #39

             flags=0x4100c020 <ENABLED, UP, AGGREGATE, UP, HAMON, 802.1
                q>

             MTU=1500, native vlan=1, MAC=02:e0:ed:33:88:b0, uptime 340
                h11m56s

             Requested: media NONE, speed AUTO, duplex NONE, fctl NONE,

             throughput 0

             Actual: throughput 4000

             LLDP Mode: NONE,

             RX: Pkts(918446) Bytes(110087414) Errs(0) Drops(795989)
                Stalls(0)

             TX: Pkts(124113) Bytes(15255532) Errs(0) Drops(0) Stalls
                (0)

```



```
21              NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0)
                   Muted(0)
22
23              Bandwidth thresholds are not set.
24
25 Disable the remaining unused interfaces and turn off the monitor.
26
27 set interface 10/5  - haMonitor OFF
28 <!--NeedCopy-->
```

Commande :

```
1 set interface 10/24  - haMonitor OFF
2
3 disable interface 10/5
4
5 disable interface 10/24
6 <!--NeedCopy-->
```

La configuration des interfaces physiques n'est pas partagée entre les deux unités Citrix ADC. Par conséquent, les commandes ci-dessus doivent être exécutées sur les deux nœuds Citrix ADC en cas de déploiement d'une paire HA.

Configuration HA

Tous les autres paramètres de configuration sont partagés entre les nœuds Citrix ADC d'une paire HA. Par conséquent, la synchronisation HA doit être activée avant l'exécution d'autres commandes de configuration. La configuration de base HA implique les étapes suivantes :

1. Utilisation du même matériel, logiciel et licence Citrix ADC : les paires HA ne sont pas prises en charge entre différents modèles (T1100 et MPX21550) ou les mêmes modèles avec différents niveaux de firmware. Reportez-vous aux instructions appropriées sur la mise à niveau d'une paire HA existante - Mise à niveau vers la version 11.1.

2. Établir la paire HA.

Exemple :

```
1 netscaler-1> add HA node 1 <netscaler-2-NSIP>
2
3 netscaler-2> add HA node 1 <netscaler-1-NSIP>
4 <!--NeedCopy-->
```

3. Vérifiez l'établissement de paires HA exécutant la commande suivante dans l'un ou l'autre des

nœuds ; les deux nœuds doivent être visibles, l'un d'eux étant Primaire (actif), l'autre comme Secondaire (veille).

Exemple :

"'show HA node

```
4\. Activez le mode Failsafe et MaxFlips. Cela garantit qu'en cas de dé
   faillance d'un moniteur de routage sur les deux nœuds, au moins un
   nœud reste actif sans changement constant d'état actif/veille.

**Exemple :**
```

set HA node –failsafe ON

set HA node -maxFlips 3 -maxFlipTime 1200

```
5\. Enfin, activez la synchronisation HA sur les ports ADC intra-Citrix
    dédiés plutôt que sur le réseau OAM.

**Exemple :**
```

add vlan 4080 -aliasName syncVlan

set HA node -syncvlan 4080

```
> **Remarque**
>
> Le VLAN 4080 dans les commandes de l'exemple ci-dessus ne devrait pas
    être pris littéralement. Tout VLAN-ID non utilisé peut être réservé
   .

## Configuration de VLAN

Une fois les interfaces physiques configurées de maniére appropriée,
   vous pouvez configurer les VLAN GI-LAN appropriés. Par exemple,
   considérez un environnement GI-LAN plutôt simple avec une paire VLAN
    d'entrée et de sortie avec un identificateur VLAN 100/101
   respectivement.

Les commandes suivantes configurent les VLAN pertinents au-dessus du
   canal LACP créé à l'étape précédente.
```

add vlan 100
add vlan 101
bind vlan 100 –ifnum LA/1 –tagged
bind vlan 101 –ifnum LA/1 –tagged


```
## Configuration IPv4

En régle générale, une appliance Citrix ADC nécessite un SNIP par VLAN.
     L'exemple ci-dessous suppose que les réseaux décrits dans le
    diagramme d'intégration GI-LAN, donné au début de cette page, ont un
     masque de sous-réseau /24 :
```

add ns ip 192.168.1.254 255.255.255.0 –vserver DISABLED –mgmtAccess DISABLED
add ns ip 192.168.2.254 255.255.255.0 –vserver DISABLED –mgmtAccess DISABLED

```
Une fois les SNIP configurés, ils doivent être associés au VLAN
    approprié :
```

bind vlan 100 –IPAddress 192.168.1.254 255.255.255.0
bind vlan 101 –IPAddress 192.168.2.254 255.255.255.0

```
## Routage statique IPv4

L'exemple décrit dans la section [Réseau de gestion](/fr-fr/citrix-adc/
    current-release/citrix-adc-support-for-telecom-service-providers/
    NS_TCP_optimization/NS_TCP_opt_mgmt_network.html) n'appelle que
    quelques régles de routage statiques :

-  Une route statique 10.0.0.0/8 vers les clients via le routeur d'entr
    ée
-  Un itinéraire par défaut vers Internet via le routeur de sortie

**Exemple :**
```

add route 0.0.0.0 0.0.0.0 192.168.2.1
add route 10.0.0.0 255.0.0.0 192.168.1.1

```
## Routage basé sur des stratégies IPv4 (VLAN - VLAN)

Une appliance Citrix ADC permet un routage basé sur des régles plutôt
    que statique, les décisions de routage étant généralement prises en
    fonction de l'interface entrante et/ou du VLAN plutôt que de l'
    adresse IP de destination. Le routage basé sur des régles est une
    alternative pratique, dans le cas où la plage d'adresses IP source
    du client est soumise à des modifications périodiques, ou une consid
    ération obligatoire, dans le cas où l'adresse IP de destination d'un
     paquet ne suffit pas à elle seule pour prendre une décision de
    routage (c'est-à-dire en cas de chevauchement d'adresses IP client
    sur plusieurs VLAN).
```



```
4
5 **Exemple :**
```

add ns pbr fromWirelessToInternet ALLOW –nextHop 192.168.2.1 –vlan 100 –priority 10

Done

add ns pbr fromInternetToWireless ALLOW –nextHop 192.168.1.1 –vlan 200 –priority 20

Done

apply ns pbrs

```
1 ## Configuration IPv6
2
3 Les commandes suivantes attribuent IPv6 SNIP par vlan. L'exemple ci-
    dessous suppose que les réseaux décrits dans la figure : Une simple
    représentation d'un réseau GI-LAN dans cette page ont un masque de
    sous-réseau /64 :
4
5 **Commande :**
```

add ns ip6 fd00:192:168:1::254/64 -vServer DISABLED –mgmtAccess DISABLED
add ns ip6 fd00:192:168:2::254/64 -vServer DISABLED –mgmtAccess DISABLED
bind vlan 100 -IPAddress fd00:192:168:1::254/64
bind vlan 200 -IPAddress fd00:192:168:2::254/64

```
1 ## Routage IPv6
2
3 Une fois l'adressage IPv6 terminé, le routage statique IPv6 peut être
    configuré :
4
5 - Une route statique fd00:10::/64 vers les clients via le routeur d'
    entrée
6 - Un itinéraire par défaut vers Internet via le routeur de sortie
7
8 **Exemple :**
```

add route6 fd00:10::/64 fd00:192:168:1::1
add route6 ::/0 fd00:192:168:2::1

```
1 Ou à l'aide d'un routage basé sur des régles :
2
3 **Exemple :**
```

add ns pbr6 fromWirelessToInternetv6 ALLOW -vlan 100 -priority 10 -nextHop fd00:192:168:2::1

add ns pbr6 fromInternetToWirelessv6 ALLOW -vlan 200 -priority 20 -nextHop fd00:192:168:1::1

apply ns pbr6

```
## Redondance et basculement LACP

Dans le cas d'une configuration HA, il est recommandé de tirer parti de l'option de débit pour configurer un seuil bas pour le canal LACP. Par exemple, considérez un Gi-LAN 25 Gbps et un canal 4x10 GbE entre chaque appliance Citrix ADC de la paire HA et le commutateur en amont pour fournir une redondance de liaison N+1 :

**Exemple :**
```

set interface LA/1 –haMonitor ON –throughput 29000

```
En cas de panne de double liaison entre l'appliance principale et le commutateur en amont, le débit Gi-LAN maximal pouvant être pris en charge tomberait à 20 Gbit/s. Un seuil bas de 29 Gbit/s selon l'exemple ci-dessus entraînerait un événement de basculement de redondance vers l'appliance secondaire (qui n'a pas subi de dé faillances de liaison similaires), de sorte que le trafic Gi-LAN n'est pas affecté.

## Moniteurs de routage

En plus de la redondance LACP, les vérifications du moniteur de routage peuvent être configurées et associées à la configuration de la paire HA. Les vérifications du moniteur de routage peuvent être utiles pour détecter les défaillances entre l'appliance Citrix ADC et les routeurs de saut suivant, en particulier si ces routeurs ne sont pas directement connectés mais via un commutateur en amont.

Une configuration typique du moniteur de routage HA selon l'exemple de GI-LAN dans la section 2.5.1 est décrite ci-dessous :
```

add route 192.168.1.0 255.255.255.0 192.168.1.1 -msr ENABLED -monitor arp
add route 192.168.2.0 255.255.255.0 192.168.2.1 -msr ENABLED -monitor arp
bind HA node -routeMonitor 192.168.1.0 255.255.255.0
bind HA node -routeMonitor 192.168.2.0 255.255.255.0
‘‘‘

Configuration de l'optimisation TCP

August 20, 2021

Avant de configurer l'optimisation TCP, appliquez les paramètres de configuration de base suivants sur l'appliance Citrix ADC :

Configuration initiale :

```
enable ns feature LB IPv6PT
enable ns mode FR L3 USIP MBF Edge USNIP PMTUD
disable ns feature SP
disable ns mode TCPB
set lb parameter -preferDirectRoute NO
set lb parameter -vServerSpecificMac ENABLED
set l4param -l2ConnMethod Vlan
set rsskeytype -rsstype SYMMETRIC
set ns param -useproxyport DISABLED
<!--NeedCopy-->
```

> **Remarque**
>
> Redémarrez l'appliance Citrix ADC si vous modifiez le paramètre système rsskeytype.

Résiliation TCP

Pour que Citrix ADC T1 applique l'optimisation TCP, il doit d'abord mettre fin au trafic TCP entrant. À cette fin, un serveur TCP générique doit être créé et configuré pour intercepter le trafic entrant, puis le transférer au routeur Internet.

Environnement de routage statique ou dynamique

Pour les environnements avec routage statique ou dynamique en place, vserver peut compter sur les informations de la table de routage pour transférer les paquets vers le routeur Internet. Route par défaut doit pointer vers le routeur Internet et aussi les entrées de routage pour les sous-réseaux clients vers le routeur sans fil doivent être en place :

Exemple :

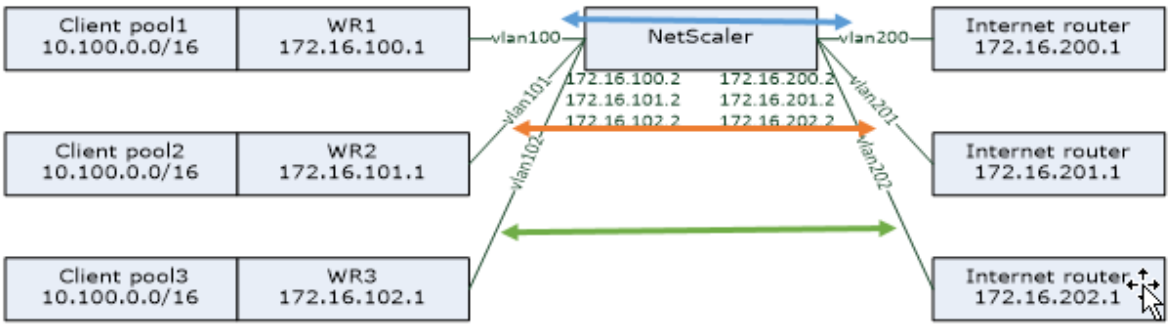
```
add lb vserver vsrv-wireless TCP * * -persistenceType NONE -
    Listenpolicy "CLIENT.VLAN.ID.EQ(100) && SYS.VSERVER("vsrv-wireless")
    .STATE.EQ(UP)" -m IP -cltTimeout 9000
add route 0.0.0.0 0.0.0.0 192.168.2.1
add route 10.0.0.0 255.0.0.0 192.168.1.1
```



```
<!--NeedCopy-->
```

Environnement VLAN à VLAN (PBR)

Il existe des environnements clients où le trafic d'abonnés est segmenté en plusieurs flux et doit être transféré à différents routeurs en fonction des paramètres de trafic entrant. Le routage basé sur la stratégie (PBR) peut être utilisé pour router des paquets en fonction des paramètres de paquets entrants, tels que VLAN, adresse MAC, interface, adresse IP source, port source, adresse IP de destination et port de destination.



Exemple :

```
add lb vserver vsrv-wireless TCP * * -m IP -l2Conn ON -listenpolicy "
    CLIENT.VLAN.ID.EQ(100) || CLIENT.VLAN.ID.EQ(101) || CLIENT.VLAN.ID.
    EQ(102)"

add ns pbr pbr-vlan100-to-vlan200 ALLOW -vlan 100 -nexthop 172.16.200.1

add ns pbr pbr-vlan101-to-vlan201 ALLOW -vlan 101 -nexthop 172.16.201.1

add ns pbr pbr-vlan102-to-vlan202 ALLOW -vlan 102 -nexthop 172.16.202.1
<!--NeedCopy-->
```

L'utilisation du routage basé sur des stratégies pour acheminer le trafic optimisé TCP est une nouvelle fonctionnalité ajoutée dans la version 11.1 50.10. Pour les versions précédentes, avoir plusieurs entités vserver « mode MAC » par VLAN est une solution alternative pour les environnements multi-VLAN. Chaque serveur vserver a un service lié représentant le routeur Internet pour le flux particulier.

Exemple :

```
add server internet_router_1 172.16.200.1

add server internet_router_2 172.16.201.1
```



```
4
5  add server internet_router_3 172.16.202.1
6
7  add service svc-internet-1 internet_router_1 TCP * -usip YES -
       useproxyport NO
8
9  add service svc-internet-2 internet_router_2 TCP * -usip YES -
       useproxyport NO
10
11 add service svc-internet-3 internet_router_3 TCP * -usip YES -
       useproxyport NO
12
13 bind service svc-internet-1 -monitorName arp
14
15 bind service svc-internet-2 -monitorName arp
16
17 bind service svc-internet-3 -monitorName arp
18
19 add lb vserver vsrv-wireless-1 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
       (100) && SYS.VSERVER("vsrv-wireless-1").STATE.EQ(UP)" -m MAC -l2Conn
        ON
20
21 add lb vserver vsrv-wireless-2 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
       (101) && SYS.VSERVER("vsrv-wireless-2").STATE.EQ(UP)" -m MAC -l2Conn
        ON
22
23 add lb vserver vsrv-wireless-3 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
       (102) && SYS.VSERVER("vsrv-wireless-3").STATE.EQ(UP)" -m MAC -l2Conn
        ON
24
25 bind lb vserver vsrv-wireless-1 svc-internet-1
26
27 bind lb vserver vsrv-wireless-2 svc-internet-2
28
29 bind lb vserver vsrv-wireless-3 svc-internet-3
30 <!--NeedCopy-->
```

Remarque :

Le mode vserver est MAC contrairement aux exemples précédents où il s'agit d'un mode IP. Ceci est nécessaire pour conserver les informations IP de destination lorsque nous avons des services liés à vserver. En outre, la configuration PBR supplémentaire doit acheminer le trafic non optimisé.

Optimisation TCP

La terminaison TCP Citrix ADC prête à l'emploi est configurée pour la fonctionnalité de transmission TCP. La transmission TCP signifie essentiellement que Citrix ADC T1 peut intercepter de manière transparente un flux TCP client-serveur mais ne conserve pas de tampons client-serveur distincts ou n'applique aucune technique d'optimisation.

Pour activer l'optimisation TCP, un profil TCP, nommé nstcpprofile, est utilisé pour spécifier les configurations TCP utilisées si aucune configuration TCP n'est fournie au niveau du service ou du serveur virtuel et qu'il doit être modifié comme suit :

Commande :

```
add ns tcpProfile nstcpprofile -WS ENABLED -SACK ENABLED -WSVal 8 -mss
    1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA
    ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -
    spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -
    fack ENABLED -rstMaxAck enABLED -tcpmode ENDPOINT
<!--NeedCopy-->
```

> **Remarque :**
>
> S'il n'y a pas de profil explicitement créé et lié à vserver et service, le profil nstcp_default_profile est lié par défaut.
>
> En cas de besoin de plusieurs profils TCP, des profils TCP supplémentaires peuvent être créés et associés au serveur virtuel approprié

Commande :

```
add ns tcpProfile custom_profile -WS ENABLED -SACK ENABLED -WSVal 8 -
    mss 1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA
    ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -
    spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -
    fack ENABLED -rstMaxAck enABLED -tcpmode ENDPOINT

set lb vserver vsrv-wireless -tcpProfileName custom_profile
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour les déploiements avec vserver -m MAC et service, le même profil doit être associé au service.

```
set service svc-internet -tcpProfileName custom_profile
<!--NeedCopy-->
```


Fonctionnalités d'optimisation TCP

La plupart des fonctionnalités d'optimisation TCP pertinentes d'une appliance Citrix ADC sont exposées via un profil TCP correspondant. Les paramètres CLI typiques qui doivent être pris en compte lors de la création d'un profil TCP sont les suivants :

1. **Fenêtre Scaling (WS)** : La mise à l'échelle de fenêtre TCP permet d'augmenter la taille de fenêtre de réception TCP au-delà de 65535 octets. Il aide à améliorer les performances TCP en général et en particulier dans les réseaux à large bande passante et à long retard. Il aide à réduire la latence et à améliorer le temps de réponse sur TCP.
2. **Accusé de réception sélectif (SACK)** : TCP SACK résout le problème de la perte de plusieurs paquets qui réduit la capacité globale de débit. Avec un accusé de réception sélectif, le destinataire peut informer l'expéditeur de tous les segments qui sont reçus avec succès, ce qui permet à l'expéditeur de ne retransmettre que les segments perdus. Cette technique permet à T1 d'améliorer le débit global et de réduire la latence de connexion.
3. **Facteur de mise à l'échelle de la fenêtre (WSVal)** : Facteur utilisé pour calculer la nouvelle taille de la fenêtre. Il doit être configuré avec une valeur élevée afin de permettre à la fenêtre annoncée par NS d'être au moins égale à la taille du tampon.
4. **Taille maximale du segment (MSS)** : MSS d'un seul segment TCP. Cette valeur dépend du paramètre MTU sur les routeurs intermédiaires et les clients finaux. Une valeur de 1460 correspond à une MTU de 1500.
5. **MaxBurst** : nombre maximal de segments TCP autorisés dans une rafale.
6. **Taille de la fenêtre de congestion initiale (InitialCwnd)** : La taille de la fenêtre de congestion initiale TCP détermine le nombre d'octets qui peuvent être en attente au début de la transaction. Il permet à T1 d'envoyer ces nombreux octets sans se soucier de la congestion sur le fil.
7. **Taille maximale de la file d'attente de paquets OOO (oooQSize)** : TCP maintient la file d'attente hors ordre pour conserver les paquets OOO dans la communication TCP. Ce paramètre affecte la mémoire système si la taille de la file d'attente est longue que les paquets doivent être conservés dans la mémoire d'exécution. Cela doit donc être maintenu à un niveau optimisé basé sur le type de caractéristiques de réseau et d'application.
8. **RTO minimum (MinRTO)** : Le délai d'expiration de retransmission TCP est calculé sur chaque ACK reçu en fonction de la logique d'implémentation interne. Le délai d'expiration de retransmission par défaut se produit à 1 seconde pour commencer et cela peut être modifié avec ce paramètre. Pour la seconde retransmission de ces paquets RTO sera calculé par N*2, puis N*4… N*8… continue jusqu'à la dernière tentative de retransmission.
9. **BufferSize/sendBuffSize** : ils font référence à la quantité maximale de données que le T1 peut recevoir du serveur et de la mémoire tampon en interne sans envoyer au client. Ils doivent être définis sur une valeur supérieure (au moins double) au produit de retard de bande passante du canal de transmission sous-jacent.
10. **saveur** : cela fait référence à l'algorithme de contrôle de la congestion TCP. Les valeurs valides sont Default, BIC, CUBIC, Westwood et Nile.

11. Mémoire**tampon de réception dynamique** : permet d'ajuster dynamiquement le tampon de réception en fonction des conditions de mémoire et de réseau. Il remplira le tampon autant qu'il est nécessaire pour garder le canal de téléchargement du client plein au lieu de remplir, en lisant à l'avance à partir du serveur, un tampon de taille fixe, tel que celui-ci est spécifié dans le profil TCP et généralement basé sur des critères tels que 2*BDP, pour une connexion. Citrix ADC T1 surveille les conditions réseau au client et estime combien il doit lire à l'avance à partir du serveur.
12. **Keep-Alive (KA)** : Envoyez périodiquement des sondes TCP keep-alive (KA) pour vérifier si l'homologue est toujours actif.
13. rstWindowAttenuate : Défense de TCP contre les attaques d'usurpation d'identité. Il répondra avec ACK correctif lorsqu'un numéro de séquence n'est pas valide.
14. **rstMaxAck** : Activer ou désactiver l'acceptation de RST qui est hors de la fenêtre tout en faisant écho au numéro de séquence ACK le plus élevé.
15. **spoofSynDrop** : suppression de paquets SYN non valides pour se protéger contre l'usurpation.
16. **Explicit Congestion Notification(ecn)** : Il envoie une notification de l'état de congestion réseau à l'expéditeur des données et prend des mesures correctives pour la congestion des données ou la corruption des données.
17. **Forward RTO-Recovery** : En cas de retransmissions fausses, les configurations de contrôle de congestion sont rétablies à leur état d'origine.
18. **TCP maximum congestion window (maxcwnd)** : taille de fenêtre de congestion maximale TCP configurable par l'utilisateur.
19. **Forward acknowledgment (FACK)** : Pour éviter la congestion TCP en mesurant explicitement le nombre total d'octets de données en attente dans le réseau et en aidant l'expéditeur (T1 ou un client) à contrôler la quantité de données injectées dans le réseau pendant les délais de retransmission.
20. **tcpmode** : modes d'optimisation TCP pour un profil spécifique. Il existe deux modes d'optimisation TCP - Transparent et Endpoint.

    - Point de terminaison. Dans ce mode, l'appliance gère les connexions client et serveur séparément.
    - Transparent. En mode transparent, les clients doivent accéder directement aux serveurs, sans serveur virtuel intermédiaire. Les adresses IP du serveur doivent être publiques car les clients doivent pouvoir y accéder. Dans l'exemple illustré dans la figure suivante, une appliance NetScaler est placée entre le client et le serveur, de sorte que le trafic doit passer par l'appliance.

Lâche silencieuse des connexions inactives

Dans un réseau de télécommunications, près de 50 % des connexions TCP d'une appliance Citrix ADC deviennent inactives et l'appliance envoie des paquets RST pour les fermer. Les paquets envoyés sur

des canaux radio activent ces canaux inutilement, provoquant un flot de messages qui, à leur tour, provoquent un flot de messages de rejet de service à l'appliance. Le profil TCP par défaut inclut désormais les paramètres DropHALFClosedConnonTimeout et DropestConnonTimeout, qui sont désactivés par défaut. Si vous les activez tous les deux, ni une connexion semi-fermée ni une connexion établie ne provoque l'envoi d'un paquet RST au client lorsque la connexion expire. L'appliance abandonne simplement la connexion.

```
set ns tcpProfile nstcpprofile  -DropHalfClosedConnOnTimeout ENABLED
set ns tcpProfile nstcpprofile  -DropEstConnOnTimeout ENABLED
<!--NeedCopy-->
```

Analyses et rapports

October 5, 2021

Le rapport de vitesse TCP est une fonctionnalité Citrix ADC qui extrait les statistiques de connexion TCP, comme mesure des performances de téléchargement et de téléchargement TCP. Elle est utilisée dans les rapports TCP Insight de Citrix Application Delivery Management (ADM). Pour ce faire, Citrix ADC surveille chaque connexion TCP, localise les rafales de paquets sur une base de délai d'inactivité et signale les mesures clés (telles que le nombre d'octets, le nombre d'octets retransmis et la durée) pour la rafale maximale identifiée. La fonctionnalité de rapport de vitesse TCP est activée par défaut, prend en charge les vServers TCP et HTTP et dépend de l'infrastructure de reporting AppFlow/ULFD.

Statistiques en temps réel

August 20, 2021

La commande stat peut être utilisée pour vérifier que l'optimisation TCP est correctement appliquée :

Commande :

```
> stat lb vserver vsrv-wireless
Virtual Server Summary
                      vsvrIP  port     Protocol        State   Health
                         actSvcs
vsrv...eless              *     0          TCP           UP      100
           1

            inactSvcs
vsrv...eless       0
```



```
8  Virtual Server Statistics
9                                                Rate (/s)
                                                    Total
10 Vserver hits                                          0
       10
11 Requests                                              0
                          0
12 Responses                                             0
                          0
13 Request bytes                                         0
       1580
14 Response bytes                                        0
       532594360
15 Total Packets rcvd                                    0
       216463
16 Total Packets sent                                    0
       369898
17 Current client connections                           --
                          0
18 Current Client Est connections                       --
                          0
19 Current server connections                           --
                          0
20 Requests in surge queue                              --
                          0
21 Requests in vserver's surgeQ                         --
                          0
22 Requests in service's surgeQs                        --
                          0
23 Spill Over Threshold                                 --
                          0
24 Spill Over Hits                                      --
                          0
25 Labeled Connection                                   --
                          0
26 Push Labeled Connection                              --
                          0
27 Deferred Request                                      0
                          0
28 Invalid Request/Response                             --
                          0
29 Invalid Request/Response Dropped                     --
                          0
30 Bound Service(s) Summary
31                          IP  port         Type        State     Hits
```



```
                                    Hits/s
32 svc-internet     192.168.2.2     0           TCP           UP       10
         0/s
33
34                  Req    Req/s      Rsp    Rsp/s Throughp ClntConn
                       SurgeQ
35 svc-internet       0      0/s        0      0/s        0        0
           0
36                   SvrConn   ReuseP  MaxConn ActvTran  SvrTTFB     Load
37 svc-internet         0        0        0        0        0        0
```

Les compteurs Total devraient constamment augmenter pour un système opérationnel. En outre, les compteurs de taux doivent être non nuls.

> **Remarque**
>
> La sortie précédente provient d'un système de laboratoire opérationnel mais inactif, expliquant le taux zéro.

SNMP

August 20, 2021

L'agent SNMP peut être interrogé pour obtenir des informations spécifiques au système à partir d'un périphérique distant (SNMP Manager). Sur la base de la requête, l'agent recherche l'identifiant d'objet égal (OID) dans la base d'informations de gestion (MIB) pour les données demandées et envoie les informations au gestionnaire SNMP. Voici les OID SNMP les plus utiles pour les déploiements de télécommunications :

Mémoire

- **resMemUsage (1.3.6.1.4.1.5951.4.1.1.41.2)**

Pourcentage d'utilisation de la mémoire sur Citrix ADC.

Processeur du moteur de paquets

- **resCpuUsage (1.3.6.1.4.1.5951.4.1.1.41.1)**

Pourcentage d'utilisation du processeur.

- **nsCPUTable (1.3.6.1.4.1.5951.4.1.1.41.6)**

Ce tableau contient des informations sur chaque processeur dans Citrix ADC.

Indexé sur : nsCPUname

- **nsCPUname (1.3.6.1.4.1.5951.4.1.1.41.6.1.1)**

Nom de la CPU.

- **nsCPUusage (1.3.6.1.4.1.5951.4.1.1.41.6.1.2)**

Pourcentage d'utilisation du processeur.

Débit

- **allNicTotRxMbits (1.3.6.1.4.1.5951.4.1.1.71.1)**

Nombre de mégabits reçus par l'appliance Citrix ADC.

- **allNicTotTxMbits (1.3.6.1.4.1.5951.4.1.1.71.2)**

Nombre de mégabits transmis par l'appliance Citrix ADC.

- **ipTotRxPkts (1.3.6.1.4.1.5951.4.1.1.43.25)**

Paquets IP reçus.

- **ipTotRxMbits (1.3.6.1.4.1.5951.4.1.1.43.27)**

Megabits de données IP reçues.

- **ipTotTxPkts (1.3.6.1.4.1.5951.4.1.1.43.28)**

Paquets IP transmis.

- **ipTotTxMbits (1.3.6.1.4.1.5951.4.1.1.43.30)**

Megabits de données IP transmises.

Connexions

Connexions actives :

- **tcpActiveServerConn (1.3.6.1.4.1.5951.4.1.1.46.8)**

Connexions à un serveur répondant actuellement aux demandes.

Nombre total de connexions :

- **tcpCurServerConn (1.3.6.1.4.1.5951.4.1.1.46.1)**

Connexions au serveur, y compris les connexions à l'état Ouverture, Établi et Fermeture.

- **tcpCurClientConn (1.3.6.1.4.1.5951.4.1.1.46.2)**

Connexions client, y compris les connexions dans l'état Ouverture, Établi et Fermeture.

Remarque : En raison de SYN-cookie, cela n'inclut pas le client dans l'état d'ouverture

- **tcpTotZombieCltConnFlushed (1.3.6.1.4.1.5951.4.1.1.46.26)**

Connexions client qui sont vidé parce que le client est inactif depuis un certain temps.

- **tcpTotZombieSvrConnFlushed (1.3.6.1.4.1.5951.4.1.1.46.27)**

Connexions serveur qui sont vidé car il n'y a pas eu de demandes client dans la file d'attente depuis un certain temps.

Erreurs

- **tcpErrSynGiveUp (1.3.6.1.4.1.5951.4.1.1.46.37)**

Tente d'établir une connexion sur Citrix ADC qui a expiré.

- **tcpErrRetransmitGiveUp (1.3.6.1.4.1.5951.4.1.1.46.60)**

Nombre de fois que Citrix ADC met fin à une connexion après avoir retransmis le paquet sept fois sur cette connexion. La retransmission se produit lorsque la fin de réception ne reconnaît pas le paquet.

- **ifInDiscards (1.3.6.1.2.1.2.2.1.13)**

Nombre de paquets entrants qui ont été choisis pour être ignorés même si aucune erreur n'a été détectée pour empêcher leur livraison vers un protocole de couche supérieure. Une raison possible pour rejeter un tel paquet pourrait être de libérer de l'espace tampon.

- **ifOutDiscards (1.3.6.1.2.1.2.2.1.19)**

Nombre de paquets sortants qui ont été choisis pour être ignorés même si aucune erreur n'a été détectée pour empêcher leur transmission. Une raison possible pour rejeter un tel paquet pourrait être de libérer de l'espace tampon.

- **ifErrTxOverflow (1.3.6.1.4.1.5951.4.1.1.54.1.36)**

Nombre de paquets qui ont traversé les files d'attente de débordement, lors de la transmission sur l'interface spécifiée, depuis le démarrage de l'appliance Citrix ADC ou l'effacement des statistiques de l'interface. Cela est incrémenté uniquement sur les ports congestionnés.

Connexions optimisées/contourner

- **tcpOptimizationEnabled (1.3.6.1.4.1.5951.4.1.1.46.131)**

Nombre total de connexions activées avec l'optimisation TCP.

- **tcpOptimizationBypassed (1.3.6.1.4.1.5951.4.1.1.46.132)**

Nombre total de connexions contournées l'optimisation TCP.

Recettes techniques

August 20, 2021

Les modèles Citrix ADC T1 fournissent des fonctionnalités avancées et un langage de configuration de stratégie puissant qui permettent d'évaluer la décision complexe en exécution.

Bien qu'il ne soit pas possible d'évaluer toutes les capacités potentiellement déverrouillées par le guide de configuration des fonctionnalités et des stratégies T1000, les récepteurs techniques envisagent la mise en œuvre de diverses exigences introduites par les opérateurs de télécommunications. N'hésitez pas à réutiliser les « recettes » telles qu'elles sont ou à vous adapter à votre environnement.

Limite de connexion par utilisateur

Le modèle Citrix ADC T1 peut être configuré pour limiter le nombre de connexions par adresse IP d'abonné unique. Avec la configuration ci-dessous, N connexions TCP simultanées par IP (CLIENT.IP.SRC) sont autorisées. Pour chaque tentative de connexion au-delà du seuil configuré, T1 envoie une RST. Pour un maximum de 2 connexions simultanées par utilisateur :

Commande :

```
add stream selector streamSel_usrlimit CLIENT.IP.SRC
add ns limitIdentifier limitId_usrlimit -threshold 2 -mode CONNECTION -
    selectorName streamSel_usrlimit
add responder policy respPol_usrlimit "SYS.CHECK_LIMIT("
    limitId_usrlimit")" RESET
bind lb vserver vsrv-wireless -policyName respPol_usrlimit -priority 1
    -gotoPriorityExpression END
<!--NeedCopy-->
```

Insertion/Suppression en douceur de Vserver

De nombreux opérateurs s'inquiètent de la perturbation des connexions TCP lorsque le modèle Citrix ADC T1 est activé en ligne pour l'optimisation TCP ou lorsqu'il est désactivé à des fins de maintenance. Pour éviter de rompre les connexions existantes lors de l'introduction de vserver, la configuration suivante doit être appliquée avant de configurer ou d'activer vserver pour l'optimisation TCP :

Commande :

```
add ns acl acl-ingress ALLOW  - vlan 100
add forwardingSession fwd-ingress  - aclname acl-ingress
apply ns acls
<!--NeedCopy-->
```


Les sessions de transfert sont efficaces en plus du routage (statique ou dynamique ou PBR) et créent des entrées de session pour le trafic routé (mode L3). Toute connexion existante est gérée par transfert de session en raison des sessions correspondantes, et lors de l'introduction de vserver, elle commence à capturer uniquement les nouvelles connexions TCP.

Les ACL peuvent être configurées pour capturer uniquement des ports spécifiques comme vserver, afin d'éviter de créer des sessions pour le trafic inutile, qui consomme de la mémoire. Une autre option consiste à supprimer une configuration spécifique après l'activation de vserver.

À des fins de maintenance, vserver doit être désactivé et son état apparaît comme OUT OF SERVICE. Lorsque cela se produit, le serveur vserver met immédiatement fin à toutes les connexions par défaut. Pour que vserver serve toujours les connexions existantes et ne pas accepter de nouvelles, la configuration suivante doit être appliquée :

Commande :

```
set lb vserver vsrv-wireless  - downStateFlush DISABLED
<!--NeedCopy-->
```

Les nouvelles connexions passent par la table de routage et les entrées de session correspondantes sont créées en raison de sessions de transfert.

Profilage TCP basé sur des règles

La sélection de profils TCP basée sur des règles permet aux opérateurs de configurer dynamiquement le profil TCP pour les clients provenant de différents domaines de trafic (c'est-à-dire 3G ou 4G). Certaines mesures QoS sont différentes pour ces domaines de trafic, et pour obtenir de meilleures performances, vous devez modifier dynamiquement certains paramètres TCP. Considérons un cas où les clients provenant de 3G et 4G ont atteint le même vserver et utilisent le même profil TCP, ce qui a un impact négatif sur les performances de certains clients. La fonctionnalité AppQoE peut classer ces clients et modifier dynamiquement le profil TCP sur vserver.

Exemple :

```
enable feature AppQoE

add ns tcpProfile nstcpprofile1 -WS ENABLED -SACK ENABLED -WSVal 8 -mss
     1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    slowStartIncr 1 -bufferSize 4000000 -flavor BIC -KA ENABLED -
    sendBuffsize 4000000 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -frto ENABLED -maxcwnd 1000000 -fack ENABLED -tcpmode
    ENDPOINT

add ns tcpProfile nstcpprofile2 -WS ENABLED -SACK ENABLED -WSVal 8 -mss
     1460 -maxBurst 15 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
```



```
    slowStartIncr 1 -bufferSize 128000 -flavor BIC -KA ENABLED -
    sendBuffsize 6000000 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -frto ENABLED -maxcwnd 64000 -fack ENABLED -tcpmode ENDPOINT
6
7 add appqoe action action_1 -priority HIGH -tcpprofile nstcpprofile1
8
9 add appqoe action action_2 -priority HIGH -tcpprofile nstcpprofile2
10
11 add appqoe policy appqoe_4G -rule "CLIENT.VLAN.ID.EQ(100)" -action
    action_1
12
13 add appqoe policy appqoe_3G -rule "CLIENT.VLAN.ID.EQ(200)" -action
    action_2
14
15 bind lb vserver vsrv-wireless -policyName appqoe_4G -priority 100
16
17 bind lb vserver vsrv-wireless -policyName appqoe_3G -priority 110
18 <!--NeedCopy-->
```

Le modèle Citrix ADC T1 est capable de recevoir les informations de l'abonné dynamiquement via l'interface Gx ou Radius ou Radius et Gx et d'appliquer un profil TCP différent par abonné.

Commande :

```
1 add appqoe action action_1 -priority HIGH -tcpprofile nstcpprofile1
2
3 add appqoe action action_2 -priority HIGH -tcpprofile nstcpprofile2
4
5 add appqoe policy appqoe_4G -rule "SUBSCRIBER.RULE_ACTIVE("3G")" -
    action action_1
6
7 add appqoe policy appqoe_3G -rule "SUBSCRIBER.RULE_ACTIVE("4G")" -
    action action_2
8 <!--NeedCopy-->
```

Pour l'intégration du modèle Citrix ADC T1 avec le réseau de plan de contrôle de l'opérateur, consultez Gestion des abonnés des télécommunications.

Capacité à monter en charge

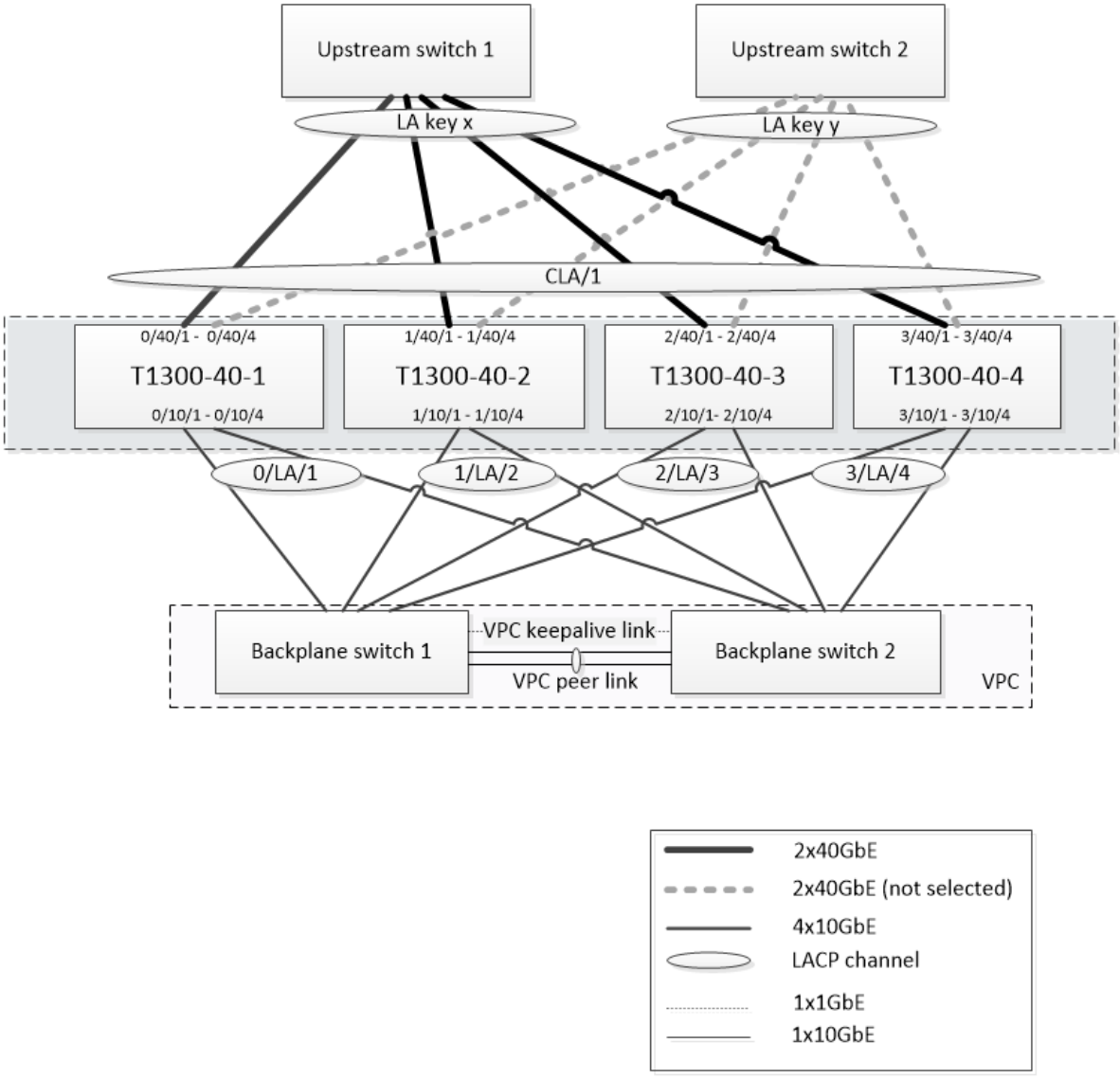
August 20, 2021

Étant donné que l'optimisation TCP nécessite beaucoup de ressources, une seule appliance Citrix ADC,

même une appliance haut de gamme, peut ne pas être en mesure de supporter des débits Gi-LAN élevés. Pour étendre la capacité de votre réseau, vous pouvez déployer des appliances Citrix ADC dans une formation de cluster N+1. Dans un déploiement de cluster, les appliances Citrix ADC fonctionnent ensemble en tant qu'image système unique. Le trafic client est distribué sur les nœuds de cluster à l'aide d'un périphérique de commutateur externe.

Topologie

La figure 1 est un exemple de cluster composé de quatre nœuds T1300-40G.



La configuration illustrée à la figure 1 possède les propriétés suivantes :

1. Tous les nœuds de cluster appartiennent au même réseau (également connu sous le nom de cluster L2).

2. Le trafic du plan de données et du backplane est géré par différents commutateurs.
3. En supposant que le débit Gi-LAN soit de 200 Gbit/s et qu'une appliance T1300-40G puisse supporter un débit de 80 Gbit/s, nous avons besoin de trois appliances T1300-40G. Pour assurer la redondance en cas de défaillance d'un nœud de cluster unique, nous déployons quatre appliances au total.
4. Chaque nœud recevra jusqu'à 67 Gbit/s de trafic (50 Gbit/s dans des conditions normales de fonctionnement et 67 Gbit/s en cas de défaillance d'un nœud de cluster unique), il a donc besoin de connexions 2x40 Gbit/s au commutateur en amont. Pour assurer la redondance en cas de panne du commutateur, nous déployons quelques commutateurs en amont et doublons le nombre de connexions.
5. Cluster Link Aggregation (CLAG) est utilisé pour distribuer le trafic entre les nœuds de cluster. Un seul CLAG gère à la fois le trafic client et serveur. La redondance des liens est activée sur le CLAG, de sorte qu'un seul « sous-canal » est sélectionné à un moment donné et gère le trafic. Si une liaison échoue ou si le débit tombe en dessous du seuil spécifié, l'autre sous-canal est sélectionné.
6. Le commutateur en amont effectue l'équilibrage symétrique de la charge du canal port (par exemple, l'algorithme source-dest-ip uniquement de Cisco IOS 7.0 (8) N1 (1)) afin que les flux de trafic avant et inverse soient gérés par le même nœud de cluster. Cette propriété est souhaitable car elle élimine la réorganisation des paquets, ce qui dégraderait les performances TCP.
7. Cinquante pour cent du trafic de données devrait être dirigé vers le backplane, ce qui signifie que chaque nœud dirigera jusqu'à 34 Gbit/s vers d'autres nœuds de cluster (25 Gbit/s dans des conditions normales d'exploitation et 34 Gbit/s en cas de défaillance d'un nœud de cluster unique). Ainsi, chaque nœud a besoin d'au moins 4x10G connexions au commutateur de backplane. Pour assurer la redondance en cas de panne du commutateur, nous déployons quelques commutateurs de backplane et doublons le nombre de connexions. La redondance de liaison n'est pas actuellement prise en charge pour le backplane, de sorte que Cisco VPC ou une technologie équivalente est souhaitée pour obtenir une redondance au niveau du commutateur.
8. La taille MTU des paquets dirigés est de 1578 octets, donc les commutateurs de backplane doivent prendre en charge un MTU supérieur à 1500 octets.

Remarque : La conception illustrée à la figure 1 s'applique également aux appareils T1120 et T1310. Pour T1310, nous utiliserions des interfaces 40GbE pour les connexions de backplane, car il manque de ports 10GbE.

Remarque : Bien que ce document utilise Cisco VPC à titre d'exemple, si vous travaillez avec des commutateurs non Cisco, des solutions équivalentes alternatives pourraient être utilisées, telles que le MLAG de Juniper.

Remarque : Bien que d'autres topologies telles que ECMP au lieu de CLAG soient possibles, elles ne sont pas actuellement prises en charge pour ce cas d'utilisation particulier.

Configuration de l'optimisation TCP dans un cluster Citrix ADC T1000

Une fois l'installation physique, la connectivité physique, l'installation logicielle et les licences terminées, vous pouvez procéder à la configuration réelle du cluster. Les configurations décrites ci-dessous s'appliquent au cluster représenté à la figure 1.

Remarque : Pour plus d'informations sur la configuration du cluster, voir Configuration d'un cluster Citrix ADC.

Supposons que les quatre nœuds T1300 de la figure 1 ont les adresses NSIP suivantes :

Quatre nœuds T1300 avec adresse NSIP :

```
T1300-40-1: 10.102.29.60
T1300-40-2: 10.102.29.70
T1300-40-3: 10.102.29.80
T1300-40-4: 10.102.29.90
```

Le cluster sera géré via l'adresse IP du cluster (CLIP), qui est supposée être 10.78.16.61.

Configuration du cluster

Pour commencer à configurer le cluster illustré à la figure 1, ouvrez une session sur la première appliance à ajouter au cluster (par exemple, T1300-40-1) et procédez comme suit.

1. À l'invite de commandes, entrez les commandes suivantes :

   Commande :

   ```
   > add cluster instance 1
   > add cluster node 0 10.102.29.60 -state ACTIVE
   > add ns ip 10.102.29.61 255.255.255.255 -type clip
   > enable cluster instance 1
   > save ns config
   > reboot -warm
   ```

2. Après le redémarrage de l'appliance, connectez-vous à l'adresse IP du cluster (CLIP) et ajoutez le reste des nœuds au cluster :

   Commande :

   ```
   > add cluster node 1 10.102.29.70 -state ACTIVE
   > add cluster node 2 10.102.29.80 -state ACTIVE
   > add cluster node 3 10.102.29.90 -state ACTIVE
   > save ns config
   ```


3. Connectez-vous à l'adresse NSIP de chacun des nœuds nouvellement ajoutés et rejoignez le cluster :

   Commande :

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot  - warm
```

4. Après le redémarrage des nœuds, procédez à la configuration du fond de panier. Sur l'adresse IP du cluster, entrez les commandes suivantes pour créer un canal LACP pour le lien de backplane de chaque nœud de cluster :

   Commande :

```
> set interface 0/10/[1-8]  - lacpkey 1  - lacpmode ACTIVE
> set interface 1/10/[1-8]  - lacpkey 2  - lacpmode ACTIVE
> set interface 2/10/[1-8]  - lacpkey 3  - lacpmode ACTIVE
> set interface 3/10/[1-8]  - lacpkey 4  - lacpmode ACTIVE
```

5. De même, configurez LA et VPC dynamiques sur les commutateurs de fond de panier. Assurez-vous que la MTU des interfaces de commutateur de backplane est d'au moins 1578 octets.

6. Vérifiez que les canaux sont opérationnels :

   Commande :

```
> show channel 0/LA/1
> show channel 1/LA/2
> show channel 2/LA/3
> show channel 3/LA/4
```

7. Configurez les interfaces de fond de panier du nœud de cluster.

   Commande :

```
> set cluster node 0 -backplane 0/LA/1
> set cluster node 1 -backplane 1/LA/2
> set cluster node 2 -backplane 2/LA/3
> set cluster node 3  - backplane 3/LA/4
```

8. Vérifiez l'état du cluster et vérifiez que le cluster est opérationnel :

```
> show cluster instance
> show cluster node
```

Pour plus d'informations sur la configuration du cluster, voir Configuration d'un cluster Citrix ADC.

Répartition du trafic entre les nœuds de cluster

Une fois que vous avez formé le cluster ADC CITRIX, déployez Cluster Link Aggregation (CLAG) pour distribuer le trafic entre les nœuds de cluster. Une liaison CLAG unique gérera à la fois le trafic client et serveur.

Sur l'adresse IP du cluster, exécutez les commandes suivantes pour créer le groupe CLAG (Cluster Link Agrégation) illustré à la Figure 1 :

Commande :

```
> set interface 0/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 1/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 2/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 3/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
```

Configurez l'agrégation de liens dynamiques sur les commutateurs externes.

Activez ensuite la redondance des liens comme suit :

Code :

```
> set channel CLA/1 -linkRedundancy ON -lrMinThroughput 240000
```

Enfin, vérifiez l'état de la chaîne en entrant :

Commande :

```
> show channel CLA/1
```

Le canal doit être UP et le débit réel devrait être 320000.

Pour plus d'informations sur l'agrégation des liens de cluster, consultez les rubriques suivantes :

- Agrégation de liens de cluster dynamique
- Lier la redondance dans un cluster avec LACP.

Parce que nous allons utiliser le transfert basé sur Mac (MBF), configurez un jeu de liens et le lier au groupe CLAG comme suit :

Commande :

```
> add linkset LS/1
> bind linkset LS/1 -ifnum CLA/1
```

Pour plus d'informations sur les jeux de liens, consultez les rubriques suivantes :

- Configuration des jeux de liens
- Utilisation du canal LA de cluster avec des jeux de liens

Configuration des adresses VLAN et IP

Nous utiliserons la configuration IP par bandes, ce qui signifie que les adresses IP sont actives sur tous les nœuds (paramètre par défaut). Voir Configurations rayées, partiellement rayées et tachetées pour plus d'informations sur cette rubrique.

1. Ajouter les SNIP d'entrée et de sortie :

   Commande :

```
> add ns ip 172.16.30.254 255.255.255.0 -type SNIP
> add ns ip 172.16.31.254 255.255.255.0 -type SNIP
> add ns ip6 fd00:172:16:30::254/112 -type SNIP
> add ns ip6 fd00:172:16:31::254/112 -type SNIP
```

2. Ajoutez les VLAN d'entrée et de sortie correspondants :

   Commande :

```
> add vlan 30 -aliasName wireless
> add vlan 31 -aliasName internet
```

3. Liez des VLAN avec des adresses IP et un jeu de liens :

   Commande :

```
> bind vlan 31 -ifnum LS/1 -tagged
> bind vlan 30 -ifnum LS/1 -tagged
> bind vlan 30 -IPAddress 172.16.30.254 255.255.255.0
> bind vlan 31 -IPAddress 172.16.31.254 255.255.255.0
> bind vlan 30 -IPAddress fd00:172:16:30::254/112
> bind vlan 31 -IPAddress fd00:172:16:31::254/112
```

Plus de VLAN d'entrée et de sortie peuvent être ajoutés si nécessaire.

Configuration de l'optimisation TCP

À ce stade, nous avons appliqué toutes les commandes spécifiques au cluster. Pour terminer la configuration, suivez les étapes décrites dans Configuration de l'optimisation TCP.

Configuration du routage dynamique

Un cluster Citrix ADC peut être intégré à l'environnement de routage dynamique du réseau du client. Voici un exemple de configuration de routage dynamique à l'aide du protocole de routage BGP (OSPF est également pris en charge).

1. À partir de l'adresse CLIP, activez BGP et le routage dynamique sur les adresses IP d'entrée et de sortie :

   Commande :

```
> enable ns feature bgp
> set ns ip 172.16.30.254  -dynamicRouting ENABLED
> set ns ip 172.16.31.254  -dynamicRouting ENABLED
```

2. Ouvrez vtysh et configurez BGP pour le côté sortie :

   Code :

```
> shell
root@ns# vtysh
ns# configure terminal
ns(config)# router bgp 65531
ns(config-router)# network 10.0.0.0/24
ns(config-router)# neighbor 172.16.31.100 remote-as 65530
ns(config-router)# neighbor 172.16.31.100 update-source
    172.16.31.254
ns(config-router)# exit
ns(config)# ns route-install propagate
ns(config)# ns route-install default
ns(config)# ns route-install bgp
ns(config)# exit
```

3. Configurez l'homologue BGP côté sortie pour annoncer la route par défaut vers le cluster Citrix ADC. Par exemple :

   Commande :

```
router bgp 65530
 bgp router-id 172.16.31.100
 network 0.0.0.0/0
 neighbor 172.16.31.254 remote-as 65531
```

4. Suivez les étapes similaires pour configurer le côté entrée.
5. À partir de vtysh, vérifiez que la configuration est propagée à tous les nœuds de cluster, en entrant :

   Commande :

```
ns# show running-config
```


6. Enfin, connectez-vous à l'adresse NSIP de chaque nœud de cluster et vérifiez les routes annoncées par le pair BGP :

   Commande :

```
1 > show route | grep BGP
```

Optimisation des performances TCP à l'aide de TCP Nile

August 20, 2021

TCP utilise les techniques d'optimisation et les stratégies (ou algorithmes) de contrôle de la congestion suivantes pour éviter la congestion du réseau dans la transmission des données.

Stratégies de lutte contre la congestion

Le protocole TCP (Transmission Control Protocol) a longtemps été utilisé pour établir et gérer les connexions Internet, gérer les erreurs de transmission et connecter facilement des applications Web avec des périphériques clients. Mais le trafic réseau est devenu plus difficile à contrôler, car la perte de paquets ne dépend pas seulement de la congestion dans le réseau, et la congestion ne provoque pas nécessairement la perte de paquets. Par conséquent, pour mesurer la congestion, un algorithme TCP doit se concentrer à la fois sur la perte de paquets et la bande passante.

Algorithme NILE

Citrix Systems a développé un nouvel algorithme de contrôle de la congestion-control, NILE, un algorithme d'optimisation TCP conçu pour les réseaux à grande vitesse tels que LTE, LTE avancé et 3G. Le Nil répond aux défis uniques causés par la décoloration, les pertes aléatoires ou congestives, les retransmissions des couches de liaison et l'agrégation des porteurs.

L'algorithme NILE :

- Base les estimations de latence en file d'attente sur des mesures de temps aller-retour.
- Utilise une fonction congestion-fenêtre-augmentation inversement proportionnelle à la latence de la file d'attente mesurée. Cette méthode permet d'approcher le point de congestion du réseau plus lentement que la méthode TCP standard, et réduit les pertes de paquets pendant la congestion.
- Peut distinguer entre perte aléatoire et perte basée sur la congestion sur le réseau en utilisant la latence estimée de la file d'attente.

Les fournisseurs de services de télécommunication peuvent utiliser l'algorithme NILE dans leur infrastructure TCP pour :

- Optimiser les réseaux mobiles et longue distance : l'algorithme NILE atteint un débit supérieur par rapport au TCP standard. Cette fonctionnalité est particulièrement importante pour les réseaux mobiles et longue distance.
- Diminution de la latence perçue par l'application et amélioration de l'expérience de l'abonné — L'algorithme du Nil utilise les informations de perte de paquets pour déterminer si la taille de la fenêtre de transmission doit être augmentée ou diminuée, et utilise les informations de retard de mise en file d'attente pour déterminer la taille de l'incrément ou du décrément. Ce paramètre dynamique de la taille de la fenêtre de transmission diminue la latence de l'application sur le réseau.

Pour configurer la prise en charge de NILE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
set ns tcpProfile <name> [-flavor NILE]
<!--NeedCopy-->
```

Configuration de la prise en charge de NILE à l'aide de l'utilitaire de configuration

1. Accédez à **Système** > **Profils** > **Profils TCP** et cliquez sur **Profils TCP** .
2. Dans la liste déroulante **TCP Flavor**, sélectionnez **NILE** .

Exemple :

```
set ns tcpProfile tcpprofile1 -flavor NILE
<!--NeedCopy-->
```

Algorithme de récupération de taux proportionnel (PRR)

Les mécanismes TCP Fast Recovery réduisent la latence web causée par les pertes de paquets. Le nouvel algorithme PRR (Proportional Rate Recovery) est un algorithme de récupération rapide qui évalue les données TCP lors d'une récupération de perte. Il est modelé après la réduction de la moitié de la vitesse, en utilisant la fraction appropriée à la fenêtre cible choisie par l'algorithme de contrôle de la congestion. Il minimise le réglage de la fenêtre, et la taille réelle de la fenêtre à la fin de la récupération est proche du seuil de démarrage lent (ssthresh).

TCP Ouverture rapide (TFO)

TCP Fast Open (TFO) est un mécanisme TCP qui permet un échange de données rapide et sûr entre un client et un serveur pendant la prise de main initiale de TCP. Cette fonctionnalité est disponible en tant qu'option TCP dans le profil TCP lié à un serveur virtuel d'une appliance Citrix ADC. TFO utilise

un cookie TCP Fast Open (un cookie de sécurité) que l'appliance Citrix ADC génère pour valider et authentifier le client initiant une connexion TFO au serveur virtuel. En utilisant le mécanisme TFO, vous pouvez réduire la latence réseau d'une application du temps nécessaire pour un aller-retour complet, ce qui réduit considérablement le retard subi dans les transferts TCP courts.

Fonctionnement de TFO

Lorsqu'un client tente d'établir une connexion TFO, il inclut un cookie TCP Fast Open avec le segment SYN initial pour s'authentifier. Si l'authentification réussit, le serveur virtuel de l'appliance Citrix ADC peut inclure des données dans le segment SYN-ACK même s'il n'a pas reçu le segment ACK final de la poignée de main à trois voies. Cela permet d'économiser jusqu'à un aller-retour complet par rapport à une connexion TCP normale, ce qui nécessite une poignée de main à trois voies avant d'échanger des données.

Un client et un serveur principal effectuent les étapes suivantes pour établir une connexion TFO et échanger des données en toute sécurité lors de la liaison TCP initiale.

1. Si le client ne dispose pas d'un cookie TCP Fast Open pour s'authentifier, il envoie une demande Fast Open Cookie dans le paquet SYN au serveur virtuel sur l'appliance Citrix ADC.
2. Si l'option TFO est activée dans le profil TCP lié au serveur virtuel, l'appliance génère un cookie (en chiffrant l'adresse IP du client sous une clé secrète) et répond au client avec un SYN-ACK qui inclut le cookie d'ouverture rapide généré dans un champ d'option TCP.
3. Le client met en cache le cookie pour les futures connexions TFO au même serveur virtuel sur l'appliance.
4. Lorsque le client tente d'établir une connexion TFO au même serveur virtuel, il envoie SYN qui inclut le cookie d'ouverture rapide mis en cache (en tant qu'option TCP) ainsi que des données HTTP.
5. L'appliance Citrix ADC valide le cookie et, si l'authentification réussit, le serveur accepte les données du paquet SYN et accuse réception de l'événement avec un SYN-ACK, un cookie TFO et une réponse HTTP.

Remarque : Si l'authentification du client échoue, le serveur supprime les données et reconnaît l'événement uniquement avec un SYN indiquant un délai d'expiration de session.

1. Côté serveur, si l'option TFO est activée dans un profil TCP lié à un service, l'appliance Citrix ADC détermine si le cookie TCP Fast Open est présent dans le service auquel il tente de se connecter.
2. Si le cookie TCP Fast Open n'est pas présent, l'appliance envoie une demande de cookie dans le paquet SYN.
3. Lorsque le serveur principal envoie le cookie, l'appliance stocke le cookie dans le cache d'informations du serveur.
4. Si l'appliance dispose déjà d'un cookie pour la paire IP de destination donnée, il remplace l'ancien cookie par le nouveau.

5. Si le cookie est disponible dans le cache d'informations du serveur lorsque le serveur virtuel tente de se reconnecter au même serveur principal en utilisant la même adresse SNIP, l'appliance combine les données du paquet SYN avec le cookie et les envoie au serveur principal.
6. Le serveur principal reconnaît l'événement avec des données et un SYN.

Remarque : si le serveur reconnaît l'événement avec uniquement un segment SYN, l'appliance Citrix ADC renoue immédiatement le paquet de données après avoir supprimé le segment SYN et les options TCP du paquet d'origine.

Configuration de TCP Fast Open

Pour utiliser la fonction TCP Fast Open (TFO), activez l'option TCP Fast Open dans le profil TCP approprié et définissez le paramètre TFO Cookie Timeout sur une valeur correspondant aux exigences de sécurité de ce profil.

Pour activer ou désactiver TFO à l'aide de la ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver TFO dans un profil nouveau ou existant.

Remarque : La valeur par défaut est DISABLED.

```
add tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
set tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
unset tcpprofile <TCP Profile Name> - tcpFastOpen
<!--NeedCopy-->
```

Exemples :

add tcpprofile Profile1 – tcpFastOpen
Set tcpprofile Profile1 – tcpFastOpen Enabled
unset tcpprofile Profile1 – tcpFastOpen

Pour définir la valeur du délai d'expiration du cookie TCP Fast Open à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set tcpparam  - tcpfastOpenCookieTimeout <Timeout Value>
<!--NeedCopy-->
```

Exemple :


```
set tcpprofile  - tcpfastOpenCookieTimeout 30secs
<!--NeedCopy-->
```

Pour configurer le TCP Fast Open à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Profils**, puis cliquez sur **Modifier** pour modifier un profil TCP.
2. Sur la page **Configurer le profil TCP**, activez la case à cocher **TCP Fast Open**.
3. Cliquez sur **OK**, puis sur **Terminé**.

Pour configurer la valeur de délai d'expiration TCP Fast Cookie à l'aide de l'interface graphique

Accédez à **Configuration** > **Système** > **Paramètres** > **Modifier les paramètres TCP**, puis la page **Configurer les paramètres TCP** pour définir la valeur de délai d'expiration du cookie TCP Fast Open.

TCP Hystart

Un nouveau paramètre de profil TCP, hystart, active l'algorithme Hystart, qui est un algorithme de démarrage lent qui détermine dynamiquement un point sûr auquel se terminer (ssthresh). Il permet une transition vers l'évitement de la congestion sans lourdes pertes de paquets. Ce nouveau paramètre est désactivé par défaut.

Si la congestion est détectée, Hystart entre dans une phase d'évitement de congestion. En l'activant, vous obtenez un meilleur débit dans les réseaux à grande vitesse avec une forte perte de paquets. Cet algorithme permet de maintenir une bande passante proche du maximum lors du traitement des transactions. Il peut donc améliorer le débit.

Configuration de TCP Hystart

Pour utiliser la fonction Hystart, activez l'option Hystart cubique dans le profil TCP approprié.

Pour configurer Hystart à l'aide de l'interface de ligne de commande (CLI)

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver Hystart dans un profil TCP nouveau ou existant.

```
add tcpprofile <profileName> -hystart ENABLED
set tcpprofile <profileName> -hystart ENABLED
unset tcprofile <profileName> -hystart
<!--NeedCopy-->
```


Exemples :

```
add tcpprofile Profile1 - tcpFastOpen
Set tcpprofile Profile1 - tcpFastOpen Enabled
unset tcpprofile Profile1 - tcpFastOpen
<!--NeedCopy-->
```

Pour configurer la prise en charge d'Hystart à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Profils** > et cliquez sur **Modifier** pour modifier un profil TCP.
2. Sur la page **Configurer le profil TCP**, activez la case à cocher **Hystart cubique**.
3. Cliquez sur **OK**, puis sur **Terminé**.

Techniques d'optimisation

TCP utilise les techniques et méthodes d'optimisation suivantes pour des contrôles de flux optimisés.

Sélection de profil TCP basée sur des stratégies

Aujourd'hui, le trafic réseau est plus diversifié et gourmand en bande passante que jamais. Avec l'augmentation du trafic, l'effet de la qualité de service (QoS) sur les performances TCP est significatif. Pour améliorer la qualité de service, vous pouvez désormais configurer des stratégies AppQoE avec différents profils TCP pour différentes classes de trafic réseau. La stratégie AppQoE classe le trafic d'un serveur virtuel pour associer un profil TCP optimisé pour un type de trafic particulier, tel que 3G, 4G, LAN ou WAN.

Pour utiliser cette fonctionnalité, créez une action de stratégie pour chaque profil TCP, associez une action aux stratégies AppQoE et associez les stratégies aux serveurs virtuels d'équilibrage de charge.

Configuration de la sélection de profils TCP basée sur des stratégies

La configuration de la sélection de profils TCP basée sur des stratégies consiste en les tâches suivantes :

- Activation d'AppQoE. Avant de configurer la fonctionnalité de profil TCP, vous devez activer la fonctionnalité AppQoE.
- Ajout d'une action AppQoE. Après avoir activé la fonctionnalité AppQoE, configurez une action AppQoE avec un profil TCP.
- Configuration de la sélection de profils TCP basée sur AppQoE. Pour implémenter la sélection de profil TCP pour différentes classes de trafic, vous devez configurer des stratégies AppQoE

avec lesquelles votre appliance Citrix ADC peut distinguer les connexions et lier l'action AppQoE correcte à chaque stratégie.

- Liaison de la stratégie AppQoE au serveur virtuel. Une fois que vous avez configuré les stratégies AppQoE, vous devez les lier à un ou plusieurs serveurs virtuels d'équilibrage de charge, de commutation de contenu ou de redirection de cache.

Configuration à l'aide de l'interface de ligne de commande

Pour activer AppQoE à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour activer la fonctionnalité et vérifier qu'elle est activée :

```
enable ns feature appqoe

show ns feature
<!--NeedCopy-->
```

Pour lier un profil TCP lors de la création d'une action AppQoE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande d'action AppQoE suivante avec l'option tcpprofiletobind.

Liaison d'un profil TCP :

```
add appqoe action <name> [-priority <priority>] [-respondWith ( ACS |
    NS ) [<CustomFile>] [-altContentSvcName <string>] [-altContentPath <
    string>] [-maxConn <positive_integer>] [-delay <usecs>]] [-polqDepth
     <positive_integer>] [-priqDepth <positive_integer>] [-
    dosTrigExpression <expression>] [-dosAction ( SimpleResponse |
    HICResponse )] [-tcpprofiletobind <string>]

show appqoe action
<!--NeedCopy-->
```

Pour configurer une stratégie AppQoE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add appqoe policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```


Pour lier une stratégie AppQoE à des serveurs virtuels d'équilibrage de charge, de redirection de cache ou de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind cs vserver cs1 -policyName <appqoe_policy_name> -priority <
    priority>
bind lb vserver <name> - policyName <appqoe_policy_name> -priority <
    priority>
bind cr vserver <name> -policyName <appqoe_policy_name> -priority <
    priority>
<!--NeedCopy-->
```

Exemple :

```
add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -nagle
    ENABLED -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 500 -
    slowStartIncr 1 -bufferSize 4194304 -flavor BIC -KA ENABLED -
    sendBuffsize 4194304 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -dsack enabled -frto ENABLED -maxcwnd 4000000 -fack ENABLED
    -tcpmode ENDPOINT

add appqoe action appact1 -priority HIGH -tcpprofile tcp1

add appqoe policy apppol1 -rule "client.ip.src.eq(10.102.71.31)" -
    action appact1

bind lb vserver lb2 -policyName apppol1 -priority 1 -
    gotoPriorityExpression END -type REQUEST

bind cs vserver cs1 -policyName apppol1 -priority 1 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Configuration du profilage TCP basé sur une stratégie à l'aide de l'interface graphique

Pour activer AppQoE à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans le volet d'informations, cliquez sur **Configurer les fonctionnalités avancées**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, activez la case à cocher **AppQoE** .
4. Cliquez sur **OK**.

Pour configurer la stratégie AppQoE à l'aide de l'interface graphique

1. Accédez à **App-Expert** > **AppQoE** > **Actions** .
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
3. Pour créer une action, cliquez sur **Ajouter**.
4. Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Modifier**.
5. Dans l'écran **Créer une action AppQoE** ou **Configurer une action AppQoE**, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres pour configurer l'action AppQoE » comme suit (un astérisque indique un paramètre requis) :
   a) Name—name
   b) Type d'action—respondWith
   c) Priorité—priority
   d) Profondeur de la file d'attente des stratégies—polqDepth
   e) Profondeur de file d'attente—priqDepth
   f) Action DOS—dosAction
6. Cliquez sur **Créer**.

Pour lier la stratégie AppQoE à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez un serveur, puis cliquez sur **Modifier**.
2. Dans la section **Stratégies** et cliquez sur (+) pour lier une stratégie AppQoE.
3. Dans le curseur **Stratégies**, procédez comme suit :
   a) Sélectionnez un type de stratégie comme AppQoE dans la liste déroulante.
   b) Sélectionnez un type de trafic dans la liste déroulante.
4. Dans la section **Liaison de la stratégie**, procédez comme suit :
   a) Cliquez sur **Nouveau** pour créer une stratégie AppQoE.
   b) Cliquez sur **Stratégie existante** pour sélectionner une stratégie AppQoE dans la liste déroulante.
5. Définissez la priorité de liaison et cliquez sur **Lier** à la stratégie au serveur virtuel.
6. Cliquez sur **Terminé**.

Génération de blocs SACK

Les performances TCP ralentissent lorsque plusieurs paquets sont perdus dans une fenêtre de données. Dans un tel scénario, un mécanisme d'accusé de réception sélectif (SACK) combiné à une

stratégie de retransmission sélective répétitive surmonte cette limite. Pour chaque paquet entrant en rupture de commande, vous devez générer un bloc SACK.

Si le paquet hors commande s'insère dans le bloc de file d'attente de réassemblage, insérez les informations de paquet dans le bloc et définissez les informations de bloc complètes comme SACK-0. Si un paquet hors commande ne rentre pas dans le bloc de réassemblage, envoyez le paquet sous la forme SACK-0 et répétez les blocs SACK précédents. Si un paquet hors commande est un doublon et que les informations de paquet sont définies comme SACK-0 alors D-SACK le bloc.

Note : Un paquet est considéré comme D-SACK s'il s'agit d'un paquet accusé de réception, ou d'un paquet hors commande qui est déjà reçu.

Révocation d'un client

Une appliance Citrix ADC peut gérer la révocation du client lors de la restauration basée sur SACK.

Vérification de la mémoire pour marquer end_point sur PCB ne tient pas compte de la mémoire totale disponible

Dans une appliance Citrix ADC, si le seuil d'utilisation de la mémoire est défini sur 75 % au lieu d'utiliser la mémoire totale disponible, les nouvelles connexions TCP contournent l'optimisation TCP.

Retransmissions inutiles en raison de blocs SACK manquants

Dans un mode non-endpoint, lorsque vous envoyez DUPACKS, si des blocs SACK sont manquants pour quelques paquets hors ordre, déclenche des retransmissions supplémentaires à partir du serveur.

SNMP pour le nombre de connexions contournées optimisation en raison d'une surcharge

Les identifiants SNMP suivants ont été ajoutés à une appliance Citrix ADC pour suivre le nombre de connexions contournées par l'optimisation TCP en raison d'une surcharge.

1. 1.3.6.1.4.1.5951.4.1.1.46.13 (TCPopTimizationEnabled). Pour suivre le nombre total de connexions activées avec l'optimisation TCP.
2. 1.3.6.1.4.1.5951.4.1.1.46.132 (TCPopTimizationBypassed). Pour suivre le nombre total de connexions contournées l'optimisation TCP.

Mémoire tampon de réception dynamique

Pour optimiser les performances TCP, une appliance Citrix ADC peut désormais ajuster dynamiquement la taille du tampon de réception TCP.

Instructions de dépannage

August 20, 2021

Support technique

Toutes les requêtes de dépannage et d'escalade nécessitent un ensemble récent de support technique Citrix ADC, qui capture la configuration actuelle, la version du microprogramme installée, les fichiers journaux, les cœurs en attente, etc.

Exemple :

```
show techsupport

showtechsupport data collector tool - $Revision: #5 $!
...
<!--NeedCopy-->
```

Toutes les données seront collectées sous

```
...
Archiving all the data into "/var/tmp/support/collector_P_192
   .168.121.117_18Jun2015_09_53.tar.gz" ....
Created a symbolic link for the archive with /var/tmp/support/support.
   tgz
/var/tmp/support/support.tgz  ---- points to ---> /var/tmp/support/
   collector_P_192.168.121.117_18Jun2015_09_53.tar.gz
<!--NeedCopy-->
```

Une fois qu'un bundle techsupport a été généré, il peut être copié à l'aide de SCP.

Des traces

Les problèmes d'optimisation TCP Citrix ADC nécessitent normalement des traces Citrix ADC pour dépanner correctement. Notez qu'il faut essayer de capturer des traces dans des conditions similaires, c'est-à-dire sur la même cellule, au même moment de la journée, en utilisant le même équipement utilisateur et l'application, et d'autres.

Les commandes start nstrace et stop nstrace peuvent être utilisées pour capturer des traces :

- Il est fortement recommandé d'utiliser le filtre approprié pour éviter de capturer des paquets superflus sur la trace. Par exemple, utilisez start nstrace -filter 'IP == 10.20.30.40' pour capturer uniquement les paquets envoyés ou reçus à partir de l'adresse IP 10.20.30.40, qui est l'adresse IP de l'équipement utilisateur.

- N'utilisez pas l'option -tcpdump, car elle supprime les en-têtes nstrace requis pour le débogage.

Analyse de trace

Une fois qu'une trace de Citrix ADC a été capturée, elle peut être affichée avec Wireshark 1.12 ou version ultérieure. Vérifiez que les traces capturées incluent les en-têtes Citrix ADC Packet Trace appropriés, comme indiqué dans la capture d'écran ci-dessous :

Les en-têtes de débogage supplémentaires sont également visibles dans l'illustration ci-dessous :

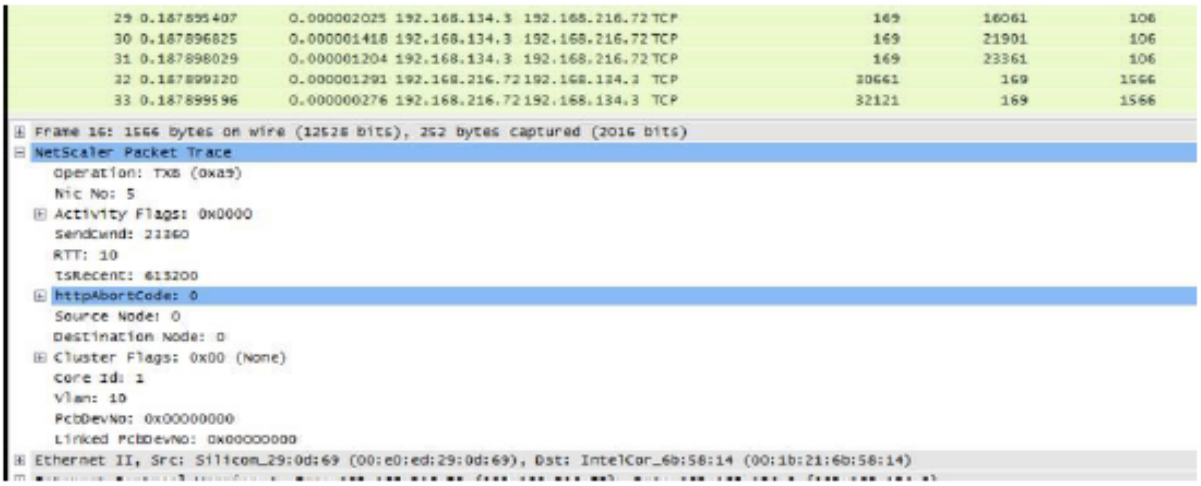


Table de connexion

Lorsque le problème est lié à l'optimisation TCP et qu'il peut être reproduit ou qu'il est en cours, il est préférable d'obtenir également la table de connexion lorsque le problème se produit à partir du nœud T1 principal.

Pour obtenir la table, vous devez basculer vers le shell BSD et exécuter la commande suivante :

```
1 shell
2 ...
3
4 nscli -U 127.0.0.1:nsroot:nsroot show connectiontable -detail full link
      > /var/tmp/contable.log
```



```
<!--NeedCopy-->
```

> **Remarque**
>
> La commande peut être exécutée plus longtemps et l'UC de gestion peut être stressée à ce moment-là (dépend du nombre d'entrées de table de connexion), mais elle n'affecte pas le service.

Questions fréquemment posées

August 20, 2021

Délais d' expiration

> **Important**
>
> Avant *d'utiliser un bouton nsapimgr*, consultez le support client Citrix.

Voici une liste des différents délais d'expiration de connexion inactives qui peuvent être définis sur les serveurs et services virtuels Citrix ADC T1. Le délai d'inactivité défini pour les connexions client ou serveur au niveau vserver ou service ne s'applique que pour les connexions en état TCP ESTABLISHED et sont inactives.

- Le paramètre cltTimeout du serveur virtuel d'équilibrage de charge spécifie le temps, en secondes, pendant lequel une connexion d'un client à un serveur virtuel d'équilibrage de charge doit être inactive, avant que l'appliance ferme la connexion.
- Le paramètre Service svrTimeout spécifie le temps, en secondes, pendant lequel une connexion entre l'appliance et un service ou un serveur doit être inactive, avant que l'appliance ferme la connexion.
- Le paramètre Service cltTimeout spécifie le temps en secondes pendant lequel une connexion d'un client à un service doit être inactive, avant que l'appliance ferme la connexion.

Lorsqu'un service est lié à un serveur virtuel d'équilibrage de charge, le CLTTimeout pour le serveur virtuel d'équilibrage de charge a priorité et le service CLTTimeout pour le service est ignoré.

En cas d'absence de service lié au serveur virtuel d'équilibrage de charge, le délai global d'inactivité, à savoir TCPServer, est utilisé pour les connexions côté serveur. Il peut être configuré comme suit :

Commande :

```
set ns timeout -tcpServer 9000
<!--NeedCopy-->
```

Les connexions dans un autre état ont des valeurs de délai d'expiration différentes :

- Délai d'inactivité des connexions à moitié ouvertes : 120 secondes (valeur codée en dur)
- Délai d'inactivité des connexions TIME_WAIT : 40 secondes (valeur codée en dur)
- Délai d'inactivité des connexions à moitié fermer. Par défaut, il est 10s et peut être configuré entre 1s et 600s à l'aide de l'extrait

Commande :

```
1  set ns timeout -halfclose 10
2  <!--NeedCopy-->
```

Lorsque le délai de demi-fermeture est déclenché, la connexion est déplacée à l'état zombie. Lorsque le délai d'expiration des zombies expire, le nettoyage zombie démarre et T1 envoie RST côté client et serveur pour une connexion donnée par défaut.

- Délai d'expiration zombie : intervalle auquel le processus de nettoyage zombie doit s'exécuter pour nettoyer les connexions TCP inactives. La valeur de délai d'expiration par défaut est 120s et peut être configurée entre 1s et 600s.

Commande :

```
1  set ns timeout -zombie 120
2  <!--NeedCopy-->
```

Tableau de la taille maximale des segments

Une appliance Citrix ADC T1 se défend contre les attaques d'inondation SYN en utilisant des cookies SYN au lieu de maintenir des connexions semi-ouvertes sur la pile de mémoire système. L'appliance envoie un cookie à chaque client qui demande une connexion TCP, mais elle ne conserve pas les états des connexions semi-ouvertes. Au lieu de cela, l'appliance alloue de la mémoire système pour une connexion uniquement à la réception du paquet ACK final ou, pour le trafic HTTP, à la réception d'une requête HTTP. Cela empêche les attaques SYN et permet aux communications TCP normales avec des clients légitimes de continuer sans interruption. Fonction spécifique est activée par défaut sans option à désactiver.

Cependant, il existe une mise en garde car les cookies SYN standard limitent les connexions à l'utilisation de seulement huit valeurs MSS (Maximum Segment Size). Si le MMS de connexion ne correspond à aucune valeur prédéfinie, il récupère la valeur inférieure suivante disponible à la fois côté client et serveur.

Les valeurs TCP Maximum Segment Size (MSS) prédéfinies sont les suivantes et peuvent être configurées via un nouveau bouton nsapimgr.

1460	1440	1330	1220	956	536	384	128

La nouvelle table MSS :

- Pas besoin de contenir la prise en charge Jumbo-Frame. Même si par défaut 8 valeurs sont réservées dans la table MSS pour les trames jumbo, les paramètres de la table peuvent être modifiés pour inclure uniquement les trames standard de taille Ethernet.
- Devrait avoir 16 valeurs
- Doit avoir des valeurs dans l'ordre décroissant
- Devrait inclure 128 comme dernière valeur

Si la nouvelle table MSS est valide, la table est stockée et les anciennes valeurs sont désactivées au moment de la rotation SYN-cookie. Sinon, la nouvelle table renvoie une erreur. Les modifications sont appliquées aux nouvelles connexions tandis que les connexions existantes conservent l'ancienne table MSS jusqu'à ce que les connexions expirent ou soient terminées.

Pour afficher la table MSS actuelle dans une appliance Citrix ADC, tapez la commande suivante.

Commande :

```
>shell

#nsapimgr -d mss_table
```

Exemple :

```
#nsapimgr -d mss_table

MSS table

{
 9176,9156,8192,7168,6144,4196,3072,2048,1460,1440,1330,1212,956,536,384,128
     }


Done.
```

Pour modifier la table mss, tapez la commande suivante :

Commande :

```
>shell

```



```
#nsapimgr -s mss_table=<16 comma seperated values>
```

Exemple :

```
#nsapimgr -ys mss_table
   =9176,9156,8192,7168,6144,4196,3072,2048,1460,1400,1330,1212,956,536,384,128


# nsapimgr -d mss_table

MSS table

{
 9176,9156,8192,7168,6144,4196,3072,2048,1460,1400,1330,1212,956,536,384,128
     }


Done.
```

Un exemple d'utilisation de valeurs standard Ethernet est illustré ci-dessous :

Exemple :

```
#nsapimgr -ys mss_table
   =1460,1440,1420,1400,1380,1360,1340,1320,1300,1280,1260,1212,956,536,384,128


# nsapimgr -d mss_table

MSS table

{
 1460,1440,1420,1400,1380,1360,1340,1320,1300,1280,1260,1212,956,536,384,128
     }


Done.
```

Pour rendre cette modification permanente même après le redémarrage de l'appliance Citrix ADC, incluez la commande `##nsapimgr -ys mss_table=<16 comma seperated values>` dans le fichier « /nsconfig/rc.netscaler ». Si le fichier « rc.netscaler » n'existe pas, créez-le sous le dossier « /nsconfig », puis ajoutez la commande.

Protection contre les surcharges de mémoire

Un moteur de traitement des paquets (PPE) Citrix ADC commence à contourner les connexions de l'optimisation TCP si la mémoire utilisée par cet EPI est supérieure à une valeur de filigrane élevée spécifiée. Si une utilisation de la mémoire PPE dépasse ~2,6 Go, elle commence à contourner *les nouvelles* connexions de l'optimisation. Les connexions existantes (celles déjà admises pour l'optimisation) continuent d'obtenir l'optimisation. Cette valeur de filigrane a été sélectionnée délibérément et n'est pas recommandée pour le réglage.

> **Remarque**
>
> Si vous pensez qu'il y a une bonne raison de modifier cette valeur de filigrane, contactez le support client.

Prise en charge des clients Happy Eyeballs

Si l'appliance Citrix ADC reçoit un SYN pour une destination dont l'état est inconnu, l'appliance vérifie d'abord l'accessibilité du serveur, puis reconnaît le client. Ce mécanisme de sondage permet aux clients disposant de deux piles IP de découvrir l'accessibilité des serveurs Internet à double pile. Si le client découvre que les accès IPv6 et IPv4 sont disponibles, il établit une connexion au serveur qui répond plus rapidement et réinitialise l'autre. Pour que la connexion de l'appliance Citrix ADC reçoive une réinitialisation, elle réinitialise la connexion côté serveur correspondante.

Remarque : cette fonctionnalité ne dispose pas de paramètres TCP configurables par l'utilisateur à désactiver/activer sur l'appliance Citrix ADC.

Pour plus d'informations sur la prise en charge de Happy Eyeballs, voir RFC 6555.

Optimisation de la vidéo Citrix ADC

January 21, 2021

L'appliance Citrix ADC fournit des techniques et des fonctionnalités d'optimisation pour optimiser le trafic vidéo ABR pour le trafic vidéo sur les réseaux mobiles. Cela améliore l'expérience utilisateur et réduit la consommation globale de bande passante réseau.

La section comprend les rubriques suivantes :

- Mise en route
- Système de licences
- Configuration de l'optimisation vidéo sur TCP
- Configuration de l'optimisation vidéo sur UDP

Mise en route

January 21, 2021

Les fichiers multimédias ont généré un trafic croissant sur les réseaux mobiles, et la migration vers des technologies de mise en réseau plus rapides a considérablement augmenté le volume du trafic vidéo crypté. La technologie traditionnelle de diffusion multimédia (Progressive Download) ne permet pas d'offrir une qualité d'expérience acceptable (QoE) à un taux de transmission élevé. Cela a conduit à l'introduction du protocole ABR (Adaptive Bit Rate). Il peut adapter le débit binaire de streaming à la bande passante réseau disponible et restreindre la qualité du streaming pour correspondre à la capacité du combiné recevant la vidéo. Cependant, le protocole ABR ne fonctionne pas aussi bien sur les réseaux mobiles qu'sur Internet. Les opérateurs mobiles doivent donc optimiser le trafic ABR.

Une appliance Citrix ADC dispose de capacités uniques pour détecter le trafic vidéo entrant et optimiser sélectivement les vidéos ABR.

Fonctionnement de l'optimisation vidéo Citrix ADC

Une appliance Citrix ADC peut identifier et optimiser le trafic ABR chiffré (y compris le trafic vidéo Facebook) sur TCP, et le trafic ABR YouTube sur QUIC. L'appliance possède les fonctionnalités suivantes :

1. Détecter les vidéos de téléchargement progressif (DP) sur HTTP.
2. Détecter et optimiser les vidéos ABR sur HTTP.
3. Détectez et optimisez les vidéos ABR sur HTTPS.
4. Détectez et optimisez les vidéos ABR YouTube sur QUIC.

En outre, l'appliance utilise les domaines de prise en charge suivants pour détecter le trafic vidéo via les protocoles TCP et QUIC.

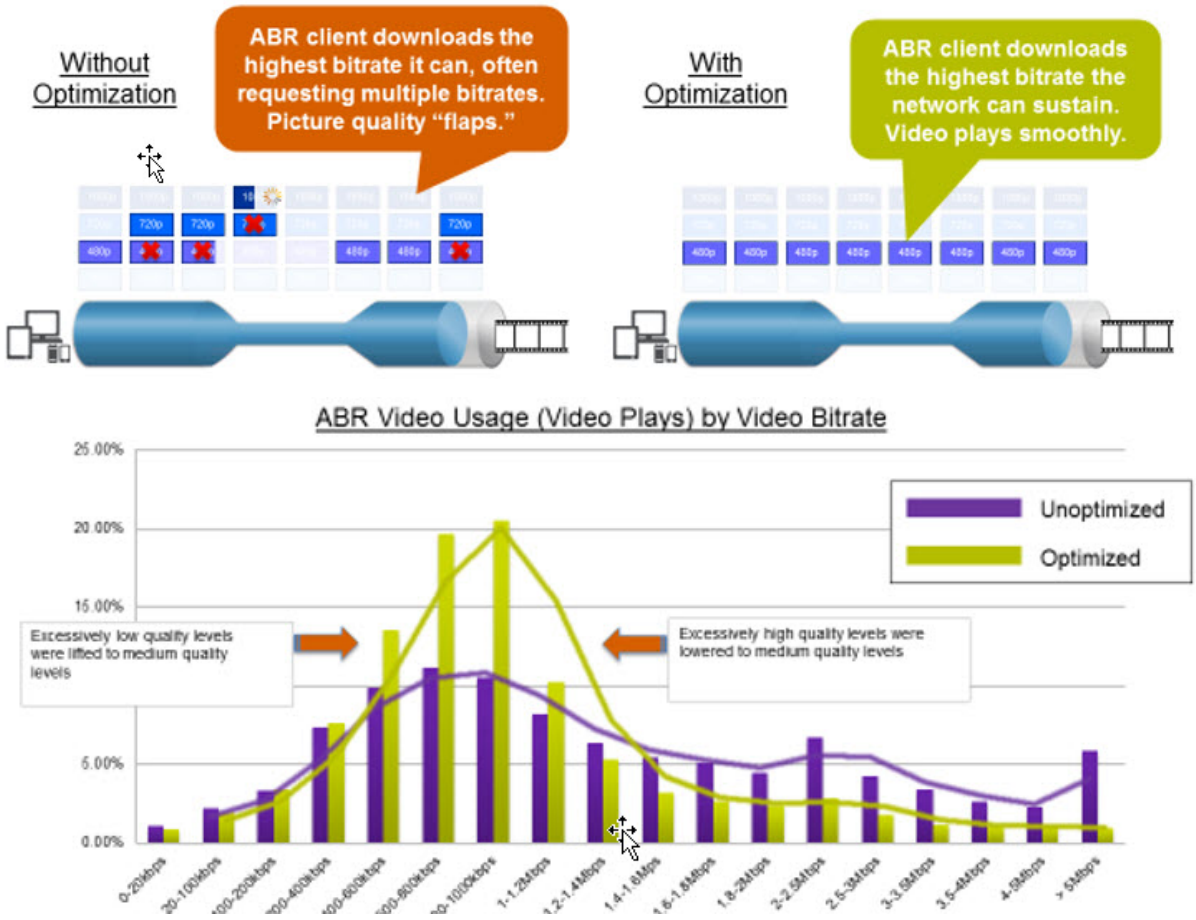
- Vidéos ABR non chiffrées sur TCP. L'appliance détecte tous les sites Web de streaming vidéo conformes aux normes. L'appliance détecte les sessions ABR en inspectant l'en-tête de charge utile vidéo de réponse, l'URL et les en-têtes HTTP.
- Vidéo ABR cryptée sur TCP. L'appliance détecte les sessions ABR à l'aide d'un algorithme générique et heuristique basé sur le domaine, l'en-tête SSL et les modèles de trafic. Grâce à cela, l'appliance dispose d'une prise en charge intégrée pour détecter les principaux sites Web vidéo, avec une précision de 95 %, et nous continuons d'ajouter la prise en charge des nouveaux types de vidéo. Citrix ADC dispose également d'un programme pour fournir une vérification supplémentaire pour les sites ABR chiffrés les plus importants pour une région ou un pays afin d'assurer la couverture du réseau.
- Vidéos ABR cryptées sur QUIC. L'appliance détecte les sessions ABR pour un fournisseur vidéo basé sur QUIC, tel que YouTube. L'algorithme de détection est basé sur une heuristique exploitant les en-têtes et le domaine QUIC. Citrix ADC continuera d'ajouter la prise en charge des

sites vidéo plus récents à l'aide de QUIC.

Avantages

L'optimisation du trafic vidéo ABR peut offrir les avantages suivants :

- Gérer le réseau pendant la congestion pendant les heures de pointe.
- Améliorez la cohérence de la lecture vidéo et réduisez le blocage vidéo.
- Activez de nouvelles offres de services vidéo (par exemple, les services vidéo Binge-on).
- Permettez aux clients de sélectionner la meilleure qualité vidéo durable.
- Fournir une expérience utilisateur cohérente à l'abonné.



Optimisation vidéo sur TCP

Optimisation Citrix ADC du trafic ABR sur TCP fonctionne comme suit :

1. Le trafic HTTP ou HTTPS que l'appliance reçoit via TCP est envoyé au serveur virtuel d'équilibrage de charge correspondant.

2. Les stratégies de détection intégrées liées au serveur virtuel combinées à d'autres algorithmes de détection propriétaires évaluent le trafic.
3. Les stratégies utilisent un ensemble de signatures de détection vidéo intégrées pour détecter le type de vidéo. La stratégie qui correspond au trafic applique une action qui classe le type de vidéo comme l'un des éléments suivants :
   a) PD en texte clair
   b) ABR en texte clair
   c) ABR chiffré
   d) Autre
4. Les stratégies d'optimisation liées au même serveur virtuel évaluent le trafic et déterminent le débit binaire d'optimisation à appliquer au trafic.
5. Le débit binaire d'optimisation est appliqué si le trafic est ABR en texte clair ou ABR chiffré.

Un fournisseur de services mobiles peut améliorer la qualité de l'expérience (QoE) en définissant la vitesse de téléchargement pour le trafic mobile 2G, 3G et 4G. Cela réduit les heures de démarrage de la vidéo ou les événements de mise en mémoire tampon. L'optimisation peut également réduire la quantité de bande passante réseau consommée par les sessions vidéo.

Les techniques d'optimisation comprennent le contrôle dynamique de rafale et l'échantillonnage aléatoire.

Contrôle dynamique de rafale

L'optimisation Citrix ADC ABR s'adapte dynamiquement aux conditions réseau changeantes. Il permet un taux de rafale initial de 1,3 fois le taux de stimulation configuré pendant 15 secondes. Le taux de rafale initial s'applique au début de chaque session vidéo ABR optimisée, même lorsque plusieurs sessions utilisent la même connexion TCP ou le même groupe de connexions TCP.

L'appliance prend également en charge les rafales de récupération dans le cas où le débit binaire pris en charge par le réseau tombe en dessous du taux de stimulation configuré. Par exemple, si le débit binaire effectif diminue à la 7ème seconde et se rétablit à la 15ème seconde de l'éclatement initial, l'appliance récupère la perte au cours du cycle de rafale suivant. Ce faisant, l'appliance optimise dynamiquement la bande passante réseau pour tous les abonnés afin que la qualité de la vidéo reste cohérente par pixel.

Remarque : Lorsqu'une rafale de récupération se produit au cours d'une rafale initiale, le débit binaire de stimulation ne doit pas dépasser les taux maximaux de récupération et de rafale initiale (vous ne devez pas ajouter le facteur de rafale de récupération en plus du facteur de rafale initiale). Sinon, il peut être si rapide que le lecteur multimédia passe à un mode de qualité supérieure. Toutefois, si nécessaire, vous pouvez prolonger la durée de l'éclatement initial pour compenser la bande passante inutilisée.

Échantillonnage aléatoire

Pour estimer les économies réalisées grâce à l'optimisation vidéo, l'appliance Citrix ADC implémente l'échantillonnage aléatoire. Avec cette technique, l'appliance sélectionne aléatoirement un pourcentage configurable du trafic vidéo détecté (le paramètre d'échantillonnage aléatoire est un nombre entier compris entre 0 et 100, donc moins de 1 % n'est pas possible). Ces transactions (et sessions) sélectionnées aléatoirement et non optimisées deviennent un groupe de référence, et elles sont identifiées dans les journaux de transactions (ainsi que d'autres caractéristiques, telles que la taille de l'octet et les champs de minuterie. Les caractéristiques des sessions optimisées sont également consignées, et le moteur de création de rapports compare les statistiques des groupes optimisés et de référence pour estimer les économies de l'optimisation (y compris les économies de l'optimisation ABR).

Optimisation vidéo sur UDP

Google a introduit un nouveau protocole de transport appelé QUIC. Le protocole QUIC de Google est très similaire à TCP+TLS+HTTP/2 et est implémenté sur UDP. Citrix ADC peut détecter les vidéos ABR YouTube diffusées sur le protocole QUIC et appliquer l'optimisation vidéo ABR de la même manière que ABR sur TCP.

Système de licences

August 20, 2021

La fonctionnalité d'optimisation vidéo fonctionne sur les plates-formes Telco avec l'achat d'une licence CBM de base et d'une licence CBM Premium. Pour d'autres plates-formes Citrix ADC, la fonctionnalité fonctionne avec l'achat d'une licence CNS Premium. Avant de configurer la fonction d'optimisation vidéo, votre appliance doit disposer d'une licence appropriée.

Prise en charge des licences pour les plates-formes Telco :

- **CBM_TXXX_SERVER_Retail.lic**
- **CBM_TPRE_Server_Retail.lic**
- **CNS_Webf_SServer_Retail.lic**

Où XXX est le débit, par exemple Citrix ADC T1000.

Prise en charge des licences pour d'autres plates-formes Citrix ADC :

- **CNS_XXX_Server_PLT_Retail.lic**

Où XXX est le débit.

Pour télécharger un fichier de licence Premium, procédez comme suit :

1. Un fichier de licence valide doit être installé sur l'appliance Citrix ADC. La licence doit prendre en charge au moins autant de Gbit/s que le débit GI-LAN maximal attendu.

   Les fichiers de licence doivent être copiés via un client SCP vers le /nsconfig/license de l'appliance, comme indiqué dans la capture d'écran ci-dessous.

```
> shell ls /nsconfig/license/
CNS_V3000_SERVER_PLT_Retail.lic ssl
<!--NeedCopy-->
```

2. Faites un redémarrage à chaud pour demander la nouvelle licence, comme indiqué dans la capture d'écran ci-dessous.

```
> reboot -warm
Are you sure you want to restart NetScaler (Y/N)? [N]:y
 Done
<!--NeedCopy-->
```

3. Une fois le redémarrage terminé, vérifiez que la licence a été correctement appliquée, à l'aide de l'interface de ligne de commande show license.

Dans l'exemple ci-dessous, une licence Premium avec édition Premium a été installée avec succès.

```
    > show license

                License status:

                                        Video Optimization: YES

                                                  ...

                                    Model Number ID: 110050

                                       License Type: Premium License
<!--NeedCopy-->
```

Configuration de l'optimisation vidéo sur TCP

October 5, 2021

> **Avertissement :**
>
> Dans le cadre de l'optimisation vidéo, la fonctionnalité de rythme vidéo est obsolète et sera sup-

> primée de l'appliance Citrix ADC dans les prochaines versions.

Pour optimiser le trafic vidéo sur TCP, commencez par activer la fonctionnalité d'optimisation vidéo. L'appliance active ensuite les stratégies de détection intégrées pour détecter le trafic vidéo entrant et identifier le type de vidéo. Les stratégies d'optimisation configurables par l'utilisateur pour chaque type de vidéo spécifient le débit binaire d'optimisation nécessaire à l'optimisation du trafic.

Configuration de l'optimisation vidéo sur TCP à l'aide de l'interface de ligne de commande

Pour configurer l'optimisation vidéo sur une appliance Citrix ADC, vous effectuez les tâches suivantes :

1. Activez la fonction d'optimisation vidéo.
2. Ajoutez des serveurs virtuels pour le trafic HTTP et HTTPS.
3. Liez toutes les stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge pour le trafic HTTP.
4. Liez toutes les stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge SSL Bridge pour le trafic HTTPS.
5. Ajoutez les stratégies d'optimisation souhaitées pour le trafic HTTP et HTTPS.
6. Liez les stratégies d'optimisation à un serveur virtuel d'équilibrage de charge pour le trafic HTTP.
7. Liez les stratégies d'optimisation à un serveur virtuel d'équilibrage de charge SSL Bridge pour le trafic HTTPS.

Activation de l'optimisation vidéo

Si vous souhaitez que l'appliance Citrix ADC détecte, optimise et signale le trafic vidéo, vous devez activer la fonctionnalité d'optimisation vidéo et définir l'optimisation sur ON. Après avoir activé la fonctionnalité, vous pouvez utiliser des stratégies de détection intégrées pour identifier le trafic vidéo entrant, et vous pouvez configurer des stratégies d'optimisation pour optimiser le trafic ABR chiffré. Pour optimiser le trafic vidéo ABR, vous devez configurer le débit binaire de téléchargement (également appelé *débit de rythme*).

Vous devez également activer la fonctionnalité d'équilibrage de charge, et si vous souhaitez utiliser l'optimisation vidéo pour le trafic HTTPS, vous devez activer la fonctionnalité SSL.

Pour activer la fonctionnalité d'optimisation vidéo

À l'invite de commandes, tapez la commande suivante :

```
1 enable ns feature VideoOptimization
2 <!--NeedCopy-->
```


> **Remarque**
>
> Si vous souhaitez surveiller les performances d'optimisation vidéo et les rapports d'informations vidéo, vous devez activer la fonctionnalité AppFlow, puis accéder à la fonctionnalité Video Analytics sur Citrix Application Delivery Management (ADM). Pour plus d'informations, consultez la documentation Video Insight .

Création de serveurs virtuels pour le trafic vidéo HTTP et HTTPS

Une appliance Citrix ADC utilise différents serveurs virtuels pour détecter et optimiser les différents types de trafic vidéo entrant. La solution matérielle-logicielle prend en charge les types de serveurs virtuels suivants pour le trafic TCP.

- **Serveur virtuel d'équilibrage de charge HTTP**. Pour détecter le trafic vidéo HTTP, la solution matérielle-logicielle utilise un serveur virtuel d'équilibrage de charge HTTP. Il gère les demandes vidéo HTTP que la solution matérielle-logicielle reçoit des clients.
- **Serveur virtuel d'équilibrage de charge SSL-Bridge**. Pour détecter le trafic vidéo chiffré, vous devez configurer un serveur virtuel de pont SSL sur l'appliance.

Pour ajouter un serveur virtuel d'équilibrage de charge HTTP pour détecter le trafic vidéo HTTP

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name> HTTP * 80 -persistenceType NONE
<!--NeedCopy-->
```

Exemple :

```
add lb vserver ProxyVserver-HTTP HTTP * 80 -persistenceType NONE -
   cltTimeout 120
<!--NeedCopy-->
```

Pour ajouter un serveur virtuel SSL Bridge pour détecter le trafic vidéo HTTPS

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name> SSL_BRIDGE * 443 -persistenceType NONE
<!--NeedCopy-->
```

Exemple :


```
add lb vserver ProxyVserver-SSL SSL_BRIDGE * 443 -persistenceType NONE
    -cltTimeout 180
<!--NeedCopy-->
```

Liaison des stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge HTTP

Pour détecter le trafic vidéo via une connexion HTTP, vous devez lier toutes les stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge. Vous devez lier les stratégies au traitement en temps de demande ou au traitement en temps de réponse, selon le type de stratégie.

> **Remarque :**
>
> La stratégie d'optimisation `ns_videoopt_http_body_detection` vidéo ne prend pas en charge la méthode de requête `CONNECT` HTTP.

Pour lier des stratégies de détection pour différents types de vidéo à un serveur virtuel d'équilibrage de charge HTTP

À l'invite de commandes, tapez la commande appropriée pour chaque type. Les commandes disponibles sont les suivantes :

```
bind lb vserver <name> -policyName ns_videoopt_http_abr_netflix -
    priority <integer> -type (REQUEST | RESPONSE)

bind lb vserver <name>   -policyName ns_videoopt_http_abr_netflix2 -
    priority <integer> -type (REQUEST | RESPONSE)

bind lb vserver <name>   -policyName ns_videoopt_http_abr_youtube -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver <name>    -policyName ns_videoopt_http_pd_youtube -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver <name>    -policyName ns_videoopt_http_pd_youtube2  -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver  <name>   -policyName ns_videoopt_http_pd_youtube3 -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver  <name>  -policyName ns_videoopt_http_abr_generic -
    priority <integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```


Exemple :

```
bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_netflix -priority 400  type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_netflix2 -priority 500 -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_youtube -priority 600  -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_pd_youtube -priority 800  -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_pd_youtube2 -priority 900 -type RESPONSE

bind lb vserver  ProxyVserver-HTTP   -policyName
    ns_videoopt_http_pd_youtube3 -priority 1000 -type REQUEST

bind lb vserver  ProxyVserver-HTTP   -policyName
    ns_videoopt_http_abr_generic -priority 1100 -type RESPONSE
<!--NeedCopy-->
```

Liaison de la stratégie de détection du contenu du corps HTTP au serveur virtuel d'équilibrage de charge

Pour détecter le trafic vidéo via HTTP, vous devez lier la stratégie de détection du contenu du corps au serveur virtuel d'équilibrage de charge. Vous pouvez utiliser la commande suivante :

```
bind lb vserver <name> -policyName ns_videoopt_http_body_detection -
    priority <integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver ProxyVserver-HTTP -policyName
    ns_videoopt_http_body_detection -priority 1500 -type REQUEST
<!--NeedCopy-->
```


Liaison de stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge SSL

Pour détecter le trafic vidéo via une connexion HTTPS, vous devez lier des stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge du pont SSL.

Pour lier une stratégie de détection à un serveur virtuel d'équilibrage de charge de pont SSL

À l'invite de commandes, tapez la commande appropriée pour chaque type. Les commandes disponibles sont les suivantes :

```
bind lb vserver <name> -policyName ns_videoopt_https_abr_netflix -
    priority <positive_integer> -type (REQUEST | RESPONSE)

bind lb vserver <name> -policyName ns_videoopt_https_abr_youtube -
    priority <positive_integer> -type (REQUEST | RESPONSE)

bind lb vserver <name> -policyName ns_videoopt_https_abr_generic -
    priority <positive_integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_netflix -priority 120 -type REQUEST

bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_youtube -priority 140 -type REQUEST

bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_generic -priority 150 -type REQUEST
<!--NeedCopy-->
```

Ajout de stratégies d'optimisation pour le rythme du trafic ABR

Pour optimiser le trafic ABR, vous devez configurer des stratégies d'optimisation et les actions associées. Vous liez ensuite les stratégies aux mêmes serveurs virtuels d'équilibrage de charge auxquels vous avez lié les stratégies de détection. Pour chaque stratégie, créez d'abord l'action, afin de pouvoir l'inclure lors de la création de la stratégie.

Pour ajouter une action d'optimisation

À l'invite de commandes, tapez :


```
add videooptimization pacingaction <action Name> -rate <integer> [-
    comment <string>]
<!--NeedCopy-->
```

Où le paramètre **rate** spécifie le débit en Kbps auquel envoyer le trafic (la fréquence de rythme).

Exemple :

```
add videooptimization pacingaction MyOptAct2000 -rate 2000
<!--NeedCopy-->
```

Pour ajouter une stratégie d'optimisation

À l'invite de commandes, tapez :

```
add videooptimization pacingpolicy <name> -rule <expression> -action <
    string>
<!--NeedCopy-->
```

Exemple :

```
add videooptimization pacingpolicy myOptPolicy2000 -rule TRUE -action
    MyOptAct2000
<!--NeedCopy-->
```

Liaison des stratégies d'optimisation à un serveur virtuel d'équilibrage de charge HTTP

Pour optimiser le trafic vidéo ABR via une connexion HTTP, vous devez lier les stratégies d'optimisation à un serveur virtuel d'équilibrage de charge auquel les stratégies de détection sont liées.

Pour lier une stratégie d'optimisation à un serveur virtuel d'équilibrage de charge

À l'invite de commandes, tapez la commande suivante :

```
bind lb vserver <name> -policyName <policy_name> -priority <
    positive_integer> -type  (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Exemple :


```
bind lb vserver ProxyVserver-HTTP -policyName myOptPolicy2000 -priority
    3400 -type  REQUEST
<!--NeedCopy-->
```

Liaison des stratégies d'optimisation aux serveurs virtuels SSL-Bridge

Pour optimiser le trafic vidéo ABR via une connexion HTTPS, vous devez lier les stratégies d'optimisation au serveur virtuel SSL Bridge auquel les stratégies de détection intégrées sont liées.

Pour lier une stratégie d'optimisation au serveur virtuel SSL Bridge afin de rythmer le trafic chiffré

À l'invite de commandes, tapez la commande suivante :

```
bind lb vserver <name> -policyName <policy_name> -priority <
    positive_integer> -type  (REQUEST |RESPONSE)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver ProxyVserver-SSL -policyName myOptPolicy2000 -priority
    3400 -type  REQUEST
<!--NeedCopy-->
```

Définition des paramètres de stimulation de l'optimisation vidéo

L'interface de ligne de commande vous permet de définir les paramètres de rythme d'optimisation vidéo, tels que le pourcentage d'échantillonnage aléatoire.

Pour définir le pourcentage d'échantillonnage aléatoire

À l'invite de commandes, tapez la commande suivante :

```
set videooptimization parameter - RandomSamplingPercentage <realNumber>
<!--NeedCopy-->
```

Où, un RealNumber est une valeur comprise entre 0,0 et 100,0.

Exemple :


```
set videooptimization parameter -RandomSamplingPercentage 50
<!--NeedCopy-->
```

Configuration de l'optimisation vidéo sur TCP à l'aide de l'interface graphique

L'interface graphique vous permet de :

- Activez la fonction d'optimisation vidéo.
- Créez un serveur virtuel d'équilibrage de charge HTTP.
- Créez un serveur virtuel d'équilibrage de charge SSL Bridge.
- Liez les stratégies de détection intégrées au serveur virtuel d'équilibrage de charge HTTP.
- Liez les stratégies de détection intégrées au serveur virtuel d'équilibrage de charge SSL Bridge.
- Créez une stratégie d'optimisation.
- Créez une action d'optimisation.
- Configuration du paramètre de rythme d'optimisation.
- Liez la stratégie d'optimisation au serveur virtuel d'équilibrage de charge pour le trafic HTTP.
- Liez la stratégie d'optimisation au serveur virtuel d'équilibrage de charge SSL-Bridge pour le trafic HTTPS.

Pour activer la fonctionnalité d'optimisation vidéo

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Sur la page **Paramètres**, cliquez sur le lien **Configurer les fonctionnalités avancées** .
3. Sur la page **Configurer les fonctionnalités avancées**, cochez la case **Optimisation vidéo** .
4. Cliquez sur **OK**, puis sur **Fermer**.

Pour créer un serveur virtuel d'équilibrage de charge pour le trafic HTTP

1. Connectez-vous à l'appliance Citrix ADC et accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Sur l'écran Serveur virtuel d'équilibrage de charge, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Sélectionnez le type de protocole HTTP
   c) **Type d'adresse IP**. Type d'adresse IP : IPv4 ou IPv6.
   d) **Adresse IP**. Adresse IPv4 ou IPv6 attribuée au serveur virtuel.
   e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez sur **OK** pour poursuivre la configuration d'autres paramètres facultatifs. Pour plus d'informations, voir Création d'un serveur virtuel.
5. Cliquez sur **Créer** et **Fermer**.

Pour créer un serveur virtuel d'équilibrage de charge pour le trafic HTTPS

1. Connectez-vous à l'appliance Citrix ADC et accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Sur l'écran **Serveur virtuel d'équilibrage de charge**, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Sélectionnez le type de protocole en tant que pont SSL.
   c) **Type d'adresse IP**. Type d'adresse IP : IPv4 ou IPv6.
   d) **Adresse IP**. Adresse IPv4 ou IPv6 attribuée au serveur virtuel.
   e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez sur **OK** pour poursuivre la configuration d'autres paramètres facultatifs. Pour plus d'informations, voir Création d'un serveur virtuel.
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour lier une stratégie de détection intégrée à un serveur virtuel d'équilibrage de charge

1. Connectez-vous à l'appliance Citrix ADC et accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet d'informations, sélectionnez le serveur virtuel d'équilibrage de charge et cliquez sur **Modifier**.
   a) Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
   b) Dans la section **Stratégies**, cliquez sur l'icône **+** pour accéder au curseur **Stratégies** .
   c) Dans la section **Stratégies**, définissez les paramètres suivants.
   d) Choisissez Policy. Sélectionnez une stratégie de détection d'optimisation vidéo dans la liste déroulante.
   e) Sélectionnez Type. Sélectionnez le type de stratégie en tant que demande.
   f) Cliquez sur **Continuer**.
3. Sélectionnez la stratégie de détection vidéo dans la liste, puis cliquez sur **Fermer**.

Pour lier une stratégie de détection intégrée à un serveur virtuel d'équilibrage de charge SSL Bridge

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet de détails, sélectionnez le serveur virtuel d'équilibrage de charge SSL-Bridge, puis cliquez sur **Modifier**.
3. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
4. Dans la section **Stratégies**, cliquez sur l'icône **+** pour accéder au curseur **Stratégies** .
5. Dans la section **Stratégies**, définissez les paramètres suivants.

a) Choisissez Policy. Sélectionnez la stratégie de détection de l'optimisation vidéo dans la liste déroulante.
b) Sélectionnez Type. Sélectionnez le type de stratégie en tant que demande.

6. Cliquez sur **Continuer**.
7. Sélectionnez la stratégie de détection vidéo dans la liste, puis cliquez sur **Fermer**.

Pour créer une action d'optimisation vidéo

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à **Configuration** > **Optimisation** > **Optimisation vidéo** > **Pacing** > **Actions**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Sur la page **Créer une action de rythme d'optimisation vidéo**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'action d'optimisation.
   b) **Taux d'optimisation ABR (Kbps).** Taux de rythme auquel envoyer le trafic vidéo ABR. Le débit par défaut pour l'optimisation ABR est de 1000 Kbps. La valeur minimale est 1 et la valeur maximale est 2147483647.
   c) **Commentaire**. Une brève description de l'action.
4. Cliquez sur **Créer** et **Fermer**.

Pour créer une stratégie d'optimisation vidéo

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à **Configuration** > **Optimisation** > **Optimisation vidéo** > **Pacing** > **Stratégies**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Sur la page **Créer une stratégie de rythme d'optimisation vidéo**, définissez les paramètres suivants.
   a) **Nom**. Nom de la stratégie d'optimisation
   b) **Expression**. Expressions régex personnalisées qui implémentent la stratégie.
   c) **Action**. Action d'optimisation associée à la stratégie pour gérer le trafic vidéo entrant.
   d) **Action du FNUD.** Événement non défini si la demande entrante ne correspond pas à la stratégie d'optimisation.
   e) **Commentaire**. Une brève description de la politique.
   f) **Action de journalisation.** Sélectionnez l'action du journal d'audit qui crée les messages de journal souhaités.
4. Cliquez sur **Créer**, puis cliquez sur **Fermer.**

Pour définir les paramètres de rythme d'optimisation vidéo

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à **Configuration** > **Optimisation** > **Optimisation vidéo.**
2. Dans la page **Optimisation vidéo**, cliquez sur **le lien Modifier les paramètres d'optimisation vidéo** .
3. Dans la page **Paramètres d'optimisation vidéo**, définissez le paramètre suivant.
   a) **Pourcentage d'échantillonnage aléatoire (%)**. Pourcentage de paquets sélectionnés pour un échantillonnage aléatoire.
4. Cliquez sur **OK** et sur **Fermer**.

Pour lier une stratégie d'optimisation vidéo à un serveur virtuel d'équilibrage de charge HTTP

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à **Configuration** > **Optimisation** > **Optimisation vidéo**.
2. Sur la page **Optimisation vidéo**, cliquez sur le lien **Video Optimization Pacing Policy Manager** .
3. Définissez les paramètres suivants.
   a) **Point de liaison**. Point auquel appliquer la stratégie d'optimisation pendant le traitement de la demande ou de la réponse.
   b) **Type de connexion**. Type de connexion Request ou Response.
   c) **Serveur virtuel**. Serveur virtuel d'équilibrage de charge auquel lier la stratégie.
   d) Cliquez sur **Continuer**.
4. Dans la section **Point de liaison**, effectuez l'une des opérations suivantes :
   a) Sélectionnez une stratégie dans la liste.
   b) Cliquez sur **Ajouter une liaison** pour accéder au curseur **Liaison des stratégies** .
      i. Sélectionnez une stratégie existante ou ajoutez-en une nouvelle.
      ii. Saisissez les détails de la liaison et cliquez sur **Liaison**.
5. Cliquez sur **Fermer**.

Pour lier une stratégie d'optimisation vidéo à un serveur virtuel d'équilibrage de charge SSL Bridge

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à **Configuration** > **Optimisation** > **Optimisationvidéo**.
2. Sur la page **Optimisation vidéo**, cliquez sur le lien **Video Optimization Pacing Policy Manager** .
3. Sur la page **Video Optimization Policy Manager**, définissez les paramètres suivants.
   a) Point de liaison. Point auquel appliquer la stratégie d'optimisation pendant le traitement de la demande/réponse.

b) Type de connexion. Type de connexion Request ou Response.
c) Serveur virtuel. Serveur virtuel d'équilibrage de charge SSL Bridge auquel lier la stratégie.

4. Cliquez sur **Continuer**.
5. Dans la section **Point de liaison**, effectuez l'une des opérations suivantes :
   a) Sélectionnez une liaison de stratégie dans la liste.
   b) Cliquez sur **Ajouter une liaison** pour accéder au curseur **Liaison des stratégies** .
      i. Sélectionnez une stratégie existante ou ajoutez-en une nouvelle.
      ii. Saisissez les détails de la liaison et cliquez sur **Liaison**.
6. Cliquez sur **Fermer**.

Configuration de l'optimisation vidéo sur UDP

August 20, 2021

Pour optimiser le trafic vidéo QUIC ABR via UDP, commencez par activer la fonction d'optimisation vidéo. Une fois la configuration terminée, l'appliance détecte le trafic vidéo ABR basé sur QUIC et applique le débit binaire d'optimisation configuré sur l'appliance.

Configuration de l'optimisation vidéo pour QUIC à l'aide de l'interface de ligne de commande

Pour configurer l'optimisation vidéo pour le trafic vidéo QUIC via UDP, vous devez effectuer les tâches suivantes :

1. Activer l'optimisation vidéo.
2. Créez un service QUIC.
3. Créez un serveur virtuel d'équilibrage de charge QUIC.
4. Liez le service Web QUIC au serveur virtuel d'équilibrage de chargement.
5. Créez une stratégie d'optimisation vidéo pour le rythme du trafic UDP basé sur QUIC.
6. Liez la stratégie d'optimisation à un serveur virtuel d'équilibrage de charge basé sur QUIC.

Activation de l'optimisation vidéo pour le trafic QUIC

Si vous souhaitez que l'appliance Citrix ADC détecte, optimise et signale le trafic vidéo, vous devez activer la fonctionnalité d'optimisation vidéo et activer l'optimisation.

> **Remarque**
>
> Si vous souhaitez utiliser l'optimisation vidéo pour le trafic QUIC, vous devez activer les fonctionnalités d'équilibrage de charge et d'AppFlow.

Pour activer l'optimisation vidéo

À l'invite de commandes, tapez la commande suivante :

```
enable ns feature VideoOptimization
<!--NeedCopy-->
```

Création d'un service pour le trafic QUIC

Une appliance Citrix ADC utilise un service QUIC pour que le serveur virtuel d'équilibrage de charge se connecte au routeur de sortie en mode de routage statique.

> **Remarque**
>
> Actuellement, le routage dynamique n'est pas pris en charge.

Pour créer un service Web d'équilibrage de charge pour le trafic vidéo QUIC

À l'invite de commandes, tapez :

```
add service <name> <router-IP> <serviceType> <port> -usip yes -
   useproxyport  [yes | no]
<!--NeedCopy-->
```

Exemple :

```
add service svc-quic 10.102.29.200 QUIC 443  - usip yes  - useproxyport
   no

where IP address is the internet router address.
<!--NeedCopy-->
```

Création d'un serveur virtuel d'équilibrage de charge pour le trafic QUIC

Une appliance Citrix ADC utilise un serveur virtuel d'équilibrage de charge pour détecter et optimiser le trafic vidéo QUIC via UDP.

Pour créer un serveur virtuel d'équilibrage de charge pour le trafic vidéo QUIC

À l'invite de commandes, tapez :

```
add lb vserver <name> <serviceType> <ip> <port> -m MAC
<!--NeedCopy-->
```


Exemple :

```
add lb vserver vs-quic QUIC * 443 -persistenceType NONE -m MAC -
    cltTimeout 120
<!--NeedCopy-->
```

Liaison d'un service Web QUIC au serveur virtuel d'équilibrage de charge

Après avoir créé les services Web et le serveur virtuel d'équilibrage de charge pour le trafic QUIC, vous devez lier les services au serveur virtuel.

Pour lier un service Web à un serveur virtuel d'équilibrage de charge pour le trafic vidéo QUIC

À l'invite de commandes, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver vs-quic svc-quic
<!--NeedCopy-->
```

Création d'une stratégie d'optimisation vidéo pour le trafic UDP basé sur QUIC

Pour optimiser le trafic UDP basé sur QUIC, vous devez configurer les stratégies de stimulation d'optimisation et ses actions. Vous devez ensuite lier les stratégies aux serveurs virtuels d'équilibrage de charge basés sur QUIC. Pour chaque stratégie, créez d'abord une action afin de pouvoir l'associer à la stratégie.

Pour ajouter une action d'optimisation

À l'invite de commandes, tapez :

```
add videooptimization pacingaction <action Name> -rate <integer> [-
    comment <string>]
<!--NeedCopy-->
```

Où, le paramètre **rate** spécifie le débit en Kbps auquel envoyer le trafic (le débit de rythme).

Exemple :


```
set videooptimization parameter -QUICPacingRate 1000
<!--NeedCopy-->
```

où 1000 représente le taux de rythme souhaité en Kbits/s.

Pour ajouter une stratégie d'optimisation

À l'invite de commandes, tapez :

```
add videooptimization pacingpolicy <name> -rule <expression> -action <
   string>
<!--NeedCopy-->
```

Exemple :

```
add videooptimization pacingpolicy myOptPolicy2000 -rule TRUE -action
   MyOptAct2000
<!--NeedCopy-->
```

Liaison de stratégies d'optimisation à un serveur virtuel d'équilibrage de charge QUIC

Pour optimiser le trafic vidéo QUIC sur une connexion UDP, vous devez lier les stratégies d'optimisation à un serveur virtuel d'équilibrage de charge QUIC.

Pour lier une stratégie d'optimisation à un serveur virtuel d'équilibrage de charge QUIC

À l'invite de commandes, tapez la commande suivante :

```
bind lb vserver <name> -policyName <policy_name> -priority <
   positive_integer> -type (REQUEST)
<!--NeedCopy-->
```

> **Remarque**
>
> Les stratégies de rythme doivent être liées à un serveur virtuel d'équilibrage de charge QUIC uniquement au moment de la demande.

Exemple :

```
bind lb vserver vs-quic -policyName myOptPolicy2000 -priority 3400 -
   type  REQUEST
<!--NeedCopy-->
```


Configuration de l'optimisation vidéo pour QUIC à l'aide de l'interface graphique

Pour configurer la fonctionnalité sur l'appliance via l'interface graphique, vous devez effectuer les tâches suivantes :

1. Activer l'optimisation vidéo
2. Configurer un serveur QUIC
3. Configurer le service QUIC
4. Configurer un serveur virtuel d'équilibrage de charge QUIC
5. Liez le service Web QUIC au serveur virtuel d'équilibrage de charge
6. Créer une stratégie d'optimisation.
7. Créer une action d'optimisation.
8. Configuration du paramètre de rythme d'optimisation.
9. Liez la stratégie d'optimisation pour équilibrer la charge serveur virtuel pour le trafic QUIC.

Pour activer l'optimisation vidéo

1. Connectez-vous à l'appliance Citrix ADC et accédez à **Système** > **Paramètres.**
2. Sur la page de détails, sélectionnez le lien **Configurer les fonctionnalités avancées** .
3. Dans la page **Configurer les fonctionnalités avancées**, activez la case à cocher **Optimisation vidéo**.

Pour créer un serveur QUIC

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs** .
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer un serveur**, définissez les paramètres suivants :
   a) Nom. Nom du serveur QUIC.
   b) Adresse IP. Adresse IP du serveur QUIC
   c) Domaine de trafic. Nom de domaine du serveur.
   d) Activation après la création. État initial du serveur.
   e) Commentaires. Brèves informations sur le serveur.
4. Cliquez sur **Créer**.

Pour créer un service QUIC

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à l'**écran**Gestion du trafic**>**Équilibrage de charge**> Services** .
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Service d'équilibrage de** charge, définissez les paramètres suivants :

a) **Nom du service**. Nom du service QUIC.
b) **Adresse IP**. Adresse IP attribuée au service QUIC.
c) **Protocole**. Sélectionnez le protocole comme QUIC.
d) **Port**. Numéro de port du service Web.

4. Cliquez sur **OK** pour continuer. Vous pouvez ensuite configurer d'autres paramètres facultatifs. Pour plus d'informations, voir Configuration des services.
5. Une fois que vous avez configuré les paramètres facultatifs, cliquez sur **OK** et **Fermer** .

Pour créer un serveur virtuel d'équilibrage de charge

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à l'écran **Gestion du trafic** > **Équilibrage de la charge** > **Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Serveur virtuel d'équilibrage** de charge, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Protocole utilisé par le service pour envoyer des demandes QUIC.
   c) Type d'adresse IP. Type d'adresse IP : IPv4 ou IPv6.
   d) **Adresse IP**. Adresse IP 4 ou IP6 attribuée au serveur virtuel.
   e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez sur OK pour poursuivre la configuration des autres paramètres facultatifs. Pour plus d'informations, voir Création d'un serveur virtuel.

Pour lier un serveur virtuel d'équilibrage de charge à un service QUIC

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis sélectionnez un serveur virtuel.
2. Cliquez sur **Services et groupes de services** pour accéder à l'écran **Liaison de service de serveur virtuel d'équilibrage** de charge.
3. Sélectionnez un service Web basé sur QUIC et cliquez sur **Lier**.
4. Cliquez sur **Terminé**.

Pour lier un serveur virtuel d'équilibrage de charge à un service QUIC

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis sélectionnez un serveur virtuel.
2. Cliquez sur **Services et groupes de services** pour accéder à l'écran **Liaison de service de serveur virtuel d'équilibrage**de charge.
3. Sélectionnez un service Web basé sur QUIC et cliquez sur **Lier**.
4. Cliquez sur **Terminé**.

Pour créer une action d'optimisation vidéo pour le trafic QUIC

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à **Configuration** > **Optimisation** > **Optimisation vidéo** > **Pacing** > **Actions**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer une action de stimulation d'optimisation vidéo**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'action d'optimisation.
   b) **Taux d'optimisation ABR (Kbps).** Vitesse de stimulation à laquelle envoyer le trafic vidéo ABR. Le débit par défaut pour l'optimisation ABR est de 1000 Kbps. La valeur minimale est 1 et la valeur maximale est 2147483647.
   c) **Commentaire**. Une brève description de l'action.
4. Cliquez sur **Créer** et **Fermer**.

Pour créer une stratégie d'optimisation vidéo pour le trafic QUIC

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à **Configuration** > **Optimisation** > **Optimisation vidéo** > **Pacing** > **Stratégies**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer une stratégie de stimulation d'optimisation vidéo**, définissez les paramètres suivants.
   a) Nom. Nom de la stratégie d'optimisation
   b) Expression. Expressions regrex personnalisées qui implémentent la stratégie.
   c) Action. Action d'optimisation associée à la stratégie pour gérer le trafic vidéo entrant.
   d) Mesures prises par le Fonds pour l'environnement. Événement non défini si la demande entrante ne correspond pas à la stratégie d'optimisation.
   e) Commentaire. Une brève description de la stratégie.
   f) Actions de journalisation. Sélectionnez l'action du journal d'audit qui crée les messages de journal souhaités.
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour lier une stratégie d'optimisation vidéo à un serveur virtuel d'équilibrage de charge QUIC

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à **Configuration** > **Optimisation** > **Optimisationvidéo**.
2. Sur la page **Optimisation vidéo**, cliquez sur le lien **Gestionnaire de stratégies d'optimisation vidéo**.
3. Dans la page **Gestionnaire de stratégies d'optimisation vidéo**, définissez les paramètres suivants.

a) Point de liaison. Point auquel appliquer la stratégie d'optimisation pendant le traitement des demandes. **Remarque** : Les stratégies de rythme doivent être liées à un serveur virtuel d'équilibrage de charge QUIC uniquement au moment de la demande.
b) Type de connexion. Type de connexion en tant que Demande ou Réponse.
c) Serveur virtuel. Serveur virtuel d'équilibrage de charge auquel lier la stratégie.

4. Cliquez sur **Continuer**.
5. Dans la section **Point de liaison**, effectuez l'une des opérations suivantes :
   a) Sélectionnez une stratégie dans la liste.
   b) Cliquez sur **Ajouter une liaison** pour accéder au curseur **Liaison de stratégies**.
      i. Sélectionnez une stratégie existante ou ajoutez une nouvelle stratégie.
      ii. Entrez les détails de la liaison et cliquez sur **Lier**.
6. Cliquez sur **Fermer**.

Filtrage d'URL de Citrix ADC

August 20, 2021

Le filtrage d'URL fournit un contrôle basé sur des règles des sites Web à l'aide des informations contenues dans les URL. Cette fonctionnalité permet aux administrateurs réseau de surveiller et de contrôler l'accès des utilisateurs aux sites Web malveillants sur les réseaux mobiles.

En tant qu'administrateur, vous pouvez configurer une stratégie de filtrage d'URL à l'aide de la fonction de catégorisation d'URL ou de la fonction de liste d'URL.

Liste d'URL. Contrôle l'accès aux sites Web et aux pages Web figurant sur la liste noire en bloquant l'accès aux URL figurant dans un ensemble d'URL importé dans l'appliance.

Catégorisation des URL. Contrôle l'accès aux sites Web et aux pages Web en filtrant le trafic sur la base d'une liste prédéfinie de catégories.

Liste d'URL

August 20, 2021

La fonctionnalité Liste d'URL vous permet de contrôler l'accès aux listes d'URL personnalisées (jusqu'à un million d'entrées). La fonctionnalité filtre les sites Web en appliquant une stratégie de filtrage d'URL liée à un serveur virtuel.

En tant qu'administrateur, vous devez importer la liste des URL dans l'appliance Citrix ADC. Cette liste importée est stockée en interne en tant que jeu de données de stratégie appelé *jeu d'URL*. L'appliance

applique ensuite un algorithme unique de correspondance rapide d'URL aux demandes d'URL entrantes. Si la demande d'URL entrante correspond à une entrée du jeu, l'appliance applique l'action de stratégie associée pour contrôler l'accès.

Types de liste d'URL

Chaque entrée d'un jeu d'URL peut inclure une URL et, éventuellement, ses métadonnées (catégorie d'URL, groupes de catégories ou toute autre donnée connexe). Pour les URL avec une métadonnées, l'appliance utilise une expression de stratégie qui évalue les métadonnées. Pour plus d'informations, voir Jeux d'URL.

Liste d'URL personnalisée. Vous pouvez créer un ensemble d'URL personnalisé comportant jusqu'à 1 000 000 entrées d'URL et l'importer en tant que fichier texte dans votre appliance. La liste peut contenir des URL avec ou sans métadonnées (ce qui pourrait ressembler à une catégorie d'URL). La plateforme CITRIX ADC détecte automatiquement si des métadonnées sont présentes. Il prend également en charge le stockage sécurisé des listes importées. Pour plus d'informations, voir Jeu d'URL.

Vous pouvez héberger la liste d'URL et configurer l'appliance Citrix ADC pour qu'elle mette à jour périodiquement la liste sans intervention manuelle. Une fois la liste d'URL mise à jour, l'appliance peut détecter automatiquement les métadonnées et les catégories à l'aide d'expressions de stratégie pour évaluer chaque URL entrante, puis appliquer des actions telles que autoriser, bloquer, rediriger ou notifier l'utilisateur.

Expressions de stratégie de liste d'URL

Le tableau suivant décrit les expressions de base que vous pouvez utiliser pour évaluer le trafic entrant. Une fois que vous avez importé une liste d'URL dans l'appliance, elle est appelée un *jeu d'URL*.

Expression.	Opération
`<URL expression>.URLSET_MATCHES_ANY (<URLSET>)`	Value TRUE si l'URL correspond exactement à n'importe quelle entrée du jeu d'URL.
`<URL expression>. GET_URLSET_METADATA(<URLSET>)`	L'expression GET_URLSET_METADATA() renvoie les métadonnées associées si l'URL correspond exactement à n'importe quel motif dans le jeu d'URL. Une chaîne vide est renvoyée s'il n'y a pas de correspondance.
`<URL expression>.GET_ URLSET_METADATA(<URLSET>).EQ(< METADATA>)`	Evalue à TRUE si les métadonnées correspondantes sont égales à `<METADATA>`.

Expression.	Opération
<URLexpression>.GET_URLSET_METADATA (<URLSET>).TYPECAST_LIST_T(',').GET (0).EQ(<CATEGORY>)	Value TRUE si les métadonnées correspondantes sont au début de la catégorie. Ce modèle peut être utilisé pour encoder des champs distincts dans les métadonnées, mais correspondre uniquement au champ 1st.
HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL)	Joigne les paramètres hôte et URL, qui peuvent ensuite être utilisés comme un <URL expression> pour la correspondance.

Actions de stratégie de liste d'URL

L'action d'application la plus courante pour les URL qui correspondent à une liste d'URL consiste à restreindre l'accès. Créez une stratégie de liste d'URL avec une expression et une action d'application de la liste d'URL souhaitées. L'utilisation du groupe de stratégies dépend du type de trafic entrant (HTTP ou HTTPS) et du serveur virtuel configuré sur l'appliance. Vous pouvez utiliser une stratégie de répondeur pour le trafic HTTP ou une stratégie d'optimisation vidéo pour le trafic HTTPS. Spécifiez les actions à appliquer aux URL qui correspondent aux expressions dans les stratégies. Le tableau suivant répertorie les actions disponibles.

Type d'action	Stratégie	Description
ALLOW	Répondeur	Autoriser la demande à accéder à l'URL cible.
REDIRECT	Répondeur	Redirigez la demande vers l'URL spécifiée comme cible.
DENY	Répondeur	Refuser la demande.
RESET	Responder, VideoOptimization	Réinitialisez la connexion.
DROP	Responder, VideoOptimization	Laisse tomber la connexion.

Conditions préalables

Pour configurer la fonctionnalité Liste d'URL, assurez-vous d'avoir configuré le serveur suivant.

Serveur DNS pour les demandes DNS

Vous devez configurer un serveur DNS si vous importez un jeu d'URL à partir d'une URL de nom d'hôte.

À l'invite de commandes, tapez :

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>) [-state (
    ENABLED | DISABLED )] [-type <type>] [-dnsProfileName <string>]
<!--NeedCopy-->
```

Exemple :

```
add dns nameServer 10.140.50.5
<!--NeedCopy-->
```

Importation d'une liste d'URL personnalisée

Pour importer un ensemble d'URL, reportez-vous à la rubrique Jeu d'URL .

Configuration d'une liste d'URL pour le trafic HTTP

L'appliance Citrix ADC prend en charge le trafic HTTP et HTTPS. Pour configurer un serveur virtuel d'équilibrage de charge pour le trafic HTTP et lier des stratégies de liste d'URL au serveur, procédez comme suit :

- Ajouter des actions de liste d'URL.
- Ajouter des stratégies de liste d'URL.
- Ajouter un serveur virtuel d'équilibrage de charge HTTP pour le trafic HTTP
- Liez les stratégies de liste d'URL au serveur virtuel d'équilibrage de charge HTTP pour le trafic HTTP

Pour ajouter une action de liste d'URL

À l'invite de commandes, tapez ce qui suit :

```
add responder action <name> <type> (<target> | <htmlpage>) [-comment <
    string>] [-responseStatusCode <positive_integer>] [-reasonPhrase <
    string>]
<!--NeedCopy-->
```

Pour ajouter un serveur virtuel d'équilibrage de charge HTTP pour le trafic HTTP

À l'invite de commandes, tapez ce qui suit :


```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT
    imeout <secs>]
<!--NeedCopy-->
```

Exemple :

```
add lb vserver vsrv-HTTP HTTP * 80 -persistenceType NONE -cltTimeout
    120
<!--NeedCopy-->
```

Pour lier la stratégie de liste d'URL au serveur virtuel d'équilibrage de charge HTTP

À l'invite de commandes, tapez ce qui suit :

```
bind lb vserver <vServerName> -policyName <string> [-priority <
    positive_integer>]
<!--NeedCopy-->
```

Configuration de la liste d'URL pour le trafic HTTPS

L'appliance Citrix ADC prend en charge le trafic HTTP et HTTPS. Pour configurer un serveur virtuel d'équilibrage de charge SSL pour le trafic HTTPS et lier les stratégies de liste d'URL au serveur, procédez comme suit :

- Ajouter des actions de liste d'URL.
- Ajouter des stratégies de liste d'URL.
- Ajouter un serveur virtuel d'équilibrage de charge SSL pour le trafic HTTP
- Liez les stratégies de liste d'URL au serveur virtuel d'équilibrage de charge SSL pour le trafic HTTP

Pour ajouter une stratégie de liste d'URL pour le trafic HTTPS

À l'invite de commandes, tapez :

```
add videooptimization detectionpolicy <name> -rule <expression> -action
     <string> [-undefAction <string>] [-comment <string>] [-logAction <
    string>]
<!--NeedCopy-->
```


Pour ajouter un serveur virtuel d'équilibrage de charge SSL pont

À l'invite de commandes, tapez :

```
1 add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT
     imeout <secs>]
2 <!--NeedCopy-->
```

Exemple :

```
1 add lb vserver vsrv-HTTPS SSL_BRIDGE * 443 -persistenceType NONE -
     cltTimeout 180
2 <!--NeedCopy-->
```

Pour lier la stratégie de liste d'URL avec l'équilibrage de charge du pont SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 bind lb vserver <vServerName> -policyName <string> [-priority <
     positive_integer>]
2 <!--NeedCopy-->
```

Configuration d'une liste d'URL à l'aide de l'interface graphique

L'interface graphique vous permet de :

- Importer une liste d'URL.
- Ajoutez une liste d'URL.
- Configurer les actions de liste d'URL.
- Configurez les stratégies de liste d'URL pour le trafic HTTP.
- Ajoutez un serveur virtuel d'équilibrage de charge HTTP pour le trafic HTTP.
- Ajoutez un serveur virtuel d'équilibrage de charge SSL pour le trafic HTTPS.
- Liez les stratégies de liste d'URL au serveur virtuel d'équilibrage de charge HTTP.
- Liez une stratégie de liste d'URL au serveur virtuel d'équilibrage de charge SSL Bridge.

Pour importer une liste d'URL

1. Dans le volet de navigation, développez **AppExpert** > **Jeux d'URL**.
2. Dans le volet d'informations, cliquez sur **Importer**.
3. Dans la page **Configurer le jeu d'URL**, définissez les paramètres suivants.
   a) **Nom**. Nom du jeu d'URL.

b) **URL**. Adresse Web de l'emplacement où accéder au jeu d'URL.
c) **Écraser**. Remplacer un jeu d'URL précédemment importé.
d) **Délimiteur**. Séquence de caractères qui délimite un enregistrement de fichier CSV.
e) **Séparateur de ligne**. Séparateur de ligne utilisé dans le fichier CSV. Une valeur de caractère unique est autorisée par exemple « /n ».
f) **Intervalle**. Intervalle en secondes, arrondi aux 15 minutes les plus proches, à laquelle l'URL définie est mise à jour.
g) **Ensemble privé.** Option pour empêcher l'exportation du jeu d'URL
h) **URL Canary**. URL interne permettant de vérifier si le contenu de l'ensemble d'URL doit rester confidentiel. La longueur maximale de l'URL est de 2047 caractères

4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour ajouter une liste d'URL

1. Dans le volet de navigation, développez **AppExpert** > **Jeux d'URL**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer un jeu d'URL**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'ensemble d'URL qui a été donné lors de son importation.
   b) **Commentaires**. Une brève description du jeu d'URL.
4. Cliquez sur **Créer**.

Pour configurer une action de liste d'URL

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à la page **de l'onglet Configuration** .
2. Dans le volet de menu, accédez à **AppExpert** > **Répondeur** > **Actions** .
3. Dans le volet d'informations, cliquez sur **Ajouter**.
4. Dans la page **Créer une action de répondeur**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'action de stratégie Liste d'URL.
   b) **Type**. Sélectionnez un type d'action.
   c) **Expression**. Utilisez l'éditeur d'expressions pour créer l'expression de stratégie.
   d) **Commentaires**. Une brève description sur l'action de stratégie.
5. Cliquez sur **Créer** et **Fermer**.

Pour configurer une stratégie de liste d'URL

1. Dans le volet de navigation, développez **AppExpert** > **Répondeur** > **Stratégies**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer une stratégie de répondeur**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'action de stratégie Liste d'URL.
   b) **Action** : Sélectionnez l'action Liste d'URL que vous préférez associer à la stratégie.

c) **Actions de journalisation**. Sélectionnez l'action du journal.
d) **AppFlow**. Sélectionnez une action AppFlow.
e) **Expression**. Utilisez l'éditeur d'expressions pour créer l'expression de stratégie.
f) **Commentaires**. Une brève description de la stratégie.

4. Cliquez sur **Créer** et **Fermer**.

Pour ajouter un serveur virtuel d'équilibrage de charge HTTP

1. Accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans l'écran **Serveur virtuel d'équilibrage** de charge, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Choisissez le type de protocole comme HTTP.
   c) **Type d'adresse IP**. Type adressable IP.
   d) **Adresse IP**. Adresse IP 4 ou IP6 attribuée au serveur virtuel.
   e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez sur **OK** pour poursuivre la configuration des autres paramètres facultatifs. Pour plus d'informations, voir Création d'un serveur virtuel.

Pour lier une stratégie de liste d'URL au serveur virtuel d'équilibrage de charge HTTP

1. Accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel d'équilibrage de charge et cliquez sur **Modifier**.
3. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
4. Dans la section **Stratégies**, cliquez sur l'icône **+** pour accéder au curseur **Stratégies**.
5. Dans la section **Stratégies**, définissez les paramètres suivants.
   a) Choisissez Stratégie. Sélectionnez une stratégie de catégorisation d'URL dans la liste déroulante.
   b) Choisissez Type. Sélectionnez le type de stratégie en tant que Demande.
6. Cliquez sur **Continuer**.
7. Dans la page Stratégies, sélectionnez la stratégie de liste d'URL dans la liste, puis cliquez sur **Sélectionner**.
8. Dans le curseur **Stratégies**, cliquez sur **Lier** et **fermer** .

Pour ajouter une stratégie de liste d'URL pour le trafic HTTPS

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à **Configuration** > **Optimisation** > **Optimisation vidéo** > **Détection**.
2. Dans la page **Détection**, cliquez sur le lien **Stratégies de détection d'optimisation vidéo**.

3. Sur la page **Stratégies de détection d'optimisation vidéo**, cliquez sur **Ajouter**.
4. Dans la page **Créer une stratégie de détection d'optimisation vidéo**, définissez les paramètres suivants.
   a) **Nom**. Nom de la stratégie d'optimisation
   b) **Expression**. Configurez la stratégie à l'aide d'expressions personnalisées.
   c) **Action** : Action d'optimisation associée à la stratégie pour gérer le trafic vidéo entrant.
   d) **Action de l'UNDEF**. Événement non défini si la demande entrante ne correspond pas à la stratégie d'optimisation.
   e) **Commentaire**. Une brève description de la stratégie.
   f) **Actions de journalisation**. Sélectionnez une action du journal d'audit qui spécifie l'action à effectuer pour les messages du journal.
5. Cliquez sur **Créer** et **Fermer**.

Pour ajouter un serveur virtuel d'équilibrage de charge SSL pour le trafic HTTPS

1. Accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans l'écran **Serveur virtuel d'équilibrage** de charge, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Sélectionnez le type de protocole comme pont SSL.
   c) **Type d'adresse IP**. Type d'adresse IP : IPv4 ou IPv6.
   d) **Adresse IP**. Adresse IPv4 ou IP6Vip attribuée au serveur virtuel.
   e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez sur **OK** pour poursuivre la configuration des autres paramètres facultatifs. Pour plus d'informations, consultez la rubrique « Création d'un serveur virtuel ».

Pour lier une stratégie de liste d'URL au serveur virtuel d'équilibrage de charge SSL Bridge

1. Accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet d'informations, sélectionnez le serveur virtuel d'équilibrage de charge SSL Bridge et cliquez sur **Modifier**.
3. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
4. Dans la section **Stratégies**, cliquez sur l'icône **+** pour accéder au curseur **Stratégies**.
5. Définissez les paramètres suivants.
   a) **Choisissez Stratégie.** Sélectionnez la stratégie de détection vidéo dans la liste déroulante.
   b) **Choisissez Type**. Sélectionnez le type de stratégie en tant que Demande.
6. Cliquez sur **Continuer**.
7. Sélectionnez la stratégie de détection vidéo dans la liste et cliquez sur **Fermer**.

Configuration de la messagerie du journal d'audit

La journalisation d'audit vous permet de consulter une condition ou une situation dans n'importe quelle phase du processus de liste d'URL. Lorsqu'une appliance Citrix ADC reçoit une URL entrante, si la stratégie du répondeur possède une expression de stratégie avancée de jeu d'URL, la fonctionnalité de journal d'audit collecte les informations d'ensemble d'URL dans l'URL et stocke les détails sous forme de message de journal pour toute cible autorisée par la journalisation d'audit.

Le message de journal contient les informations suivantes :

1. Horodatage.
2. Type de message de journal.
3. Les niveaux de journalisation prédéfinis (Critique, Erreur, Avis, Avertissement, Informations, Débogage, Alerte et Urgence).
4. Consigner les informations de message, telles que le nom du jeu d'URL, l'action de stratégie, l'URL.

Pour configurer la journalisation d'audit pour la fonctionnalité Liste d'URL, vous devez effectuer les tâches suivantes :

1. Activer le journal d'audit :
2. Action Créer un message journal d'audit.
3. Définissez la stratégie de répondeur de liste d'URL avec l'action de message Journal d'audit.

Pour plus d'informations, voir Journalisation des audits.

Sémantique de la liste d'URL

Le tableau suivant répertorie les modèles de correspondance d'URL et décrit comment les URL d'une liste d'URL sont mises en correspondance avec les URL de demande entrante. Par exemple, le modèle www.example.com/bar ne correspond qu'à une seule page sur www.example.com/bar. Pour faire correspondre toutes les pages dont l'URL commence par 'www.example.com/bar', vous devez ajouter un astérisque (*) à la fin de l'URL.

Sémantique	Modèle d'adresse URL	Correspondance	Incomparable
Correspondance de sous-domaines	domaine.com	domaine .com www.domain.com ; sub.one.domain.com	votredomaine.com ; wwwdomain.com
Correspondance d'URL, chemin exact	domain.com/example/bar/index.html	domain.com/exemple/bar/index.html ; www.domain.com/exemple/bar/index.html ; s.domaine.com/exemple/bar/index.html	www.domain.com/example/bar/index /bar/index.html/example/bar/index.html/

Sémantique	Modèle d'adresse URL	Correspondance	Incomparable
Correspondance d'URL, chemin exact	domain.com/example/l	domain.com/example/l www.domain.com/exar s.domain.com/example	wwwdomaincom/examp le/bar/index do-main.com/example/bar/index.html/
Correspondance d'URL, correspondance de sous-chemins	domain.com/exemple/bar/	domain.com/exemple/bar/; do-main.com/exemple/bar/index.html `www.domain.com/example/bar/index.html`; do-main.com/exemple/bar/index.html/one.jpg	www.domaincom/example/bar/index

Catégorisation d'URL

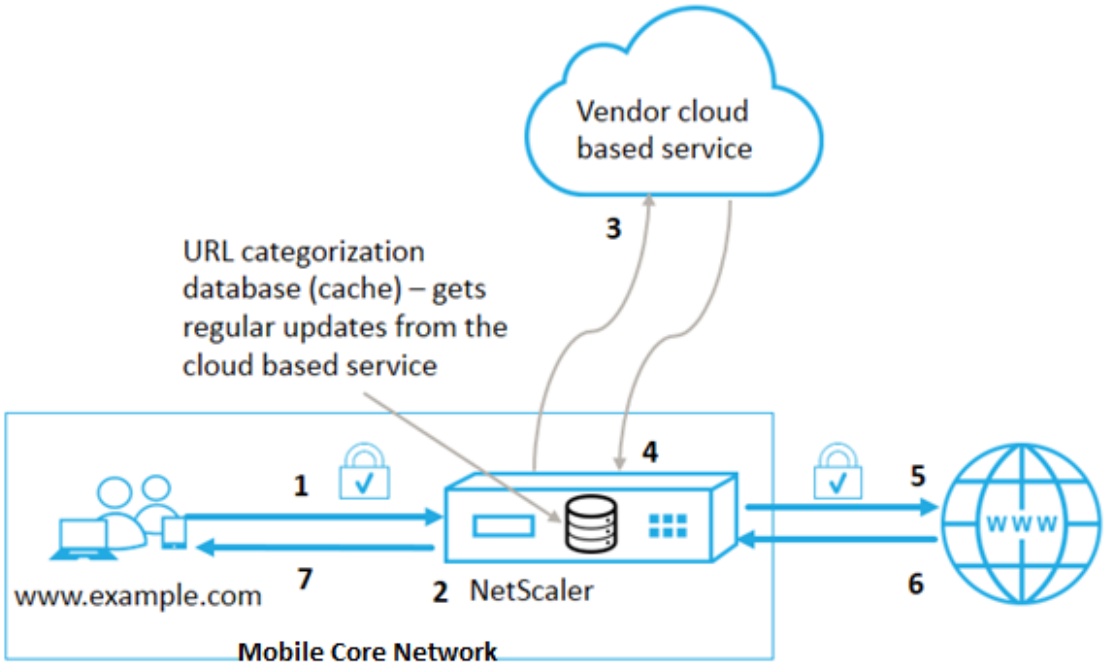
August 20, 2021

La catégorisation des URL limite l'accès des utilisateurs à des sites Web et à des catégories de sites Web spécifiques. En tant que service abonné en collaboration avec `NetSTAR`, la fonctionnalité permet aux clients d'entreprise de filtrer le trafic Web à l'aide d'une base de données de catégorisation commerciale. La `NetSTAR` base de données contient un grand nombre (milliards) d'URL classées en différentes catégories, telles que les réseaux sociaux, les jeux d'argent, le contenu pour adultes, les nouveaux médias et les achats. En plus de la catégorisation, chaque URL a un score de réputation tenu à jour en fonction du profil de risque historique du site. Nous pouvons utiliser `NetSTAR` les données pour filtrer le trafic en configurant des politiques avancées basées sur des catégories, des groupes de catégories (tels que Terrorisme, Drogues illégales) ou des scores de réputation de site.

Par exemple, vous pouvez bloquer l'accès à des sites dangereux, tels que les sites infectés par des logiciels malveillants, ou restreindre sélectivement l'accès au contenu pour adultes ou aux médias de divertissement en streaming.

Fonctionnement de la catégorisation d'URL

La figure suivante montre comment le service de filtrage d'URL Citrix ADC est intégré à une base de données de catégorisation d'URL commerciale et aux services cloud pour les mises à jour fréquentes.



Les composants interagissent comme suit :

1. Le client envoie une demande d'URL liée à Internet.
2. Une stratégie Citrix ADC tente d'évaluer la demande en termes de détails de catégorisation (catégorie, groupe de catégories et score de réputation de site, par exemple) extraits de la base de données de catégorisation d'URL. Si la base de données renvoie les détails de la catégorie, le processus passe à l'étape 5.
3. Si la base de données ne renvoie pas les détails de catégorisation, la demande est envoyée à un service de recherche basé sur un nuage géré par un fournisseur de catégorisation d'URL. Toutefois, l'appliance n'attend pas de réponse. Au lieu de cela, il marque l'URL comme Non classé et passe à l'étape 5. Toutefois, il continue de surveiller les commentaires des requêtes dans le nuage et l'utilise pour mettre à jour le cache afin que les futures demandes puissent bénéficier de la recherche dans le nuage.
4. L'appliance Citrix ADC reçoit les détails de la catégorie d'URL (catégorie, groupe de catégories et score de réputation) du service basé sur un nuage et les stocke dans le cache du nuage.
5. Si la stratégie autorise l'URL, la demande est envoyée au serveur d'origine. Sinon, l'appliance supprime ou redirige la demande, ou répond avec une page HTML personnalisée.
6. Le serveur d'origine répond avec les données demandées à l'appliance Citrix ADC.
7. L'appliance envoie la réponse au client.

Vous pouvez utiliser la fonctionnalité de filtrage d'URL pour détecter les sites qui enfreignent les mandats d'utilisation d'Internet sécurisés émis par le gouvernement et mettre en œuvre des stratégies pour bloquer ces sites. Sites qui hébergent du contenu pour adultes, des médias en streaming ou des

réseaux sociaux identifiés comme dangereux pour les enfants ou interdits comme illégaux.

Conditions préalables

La fonctionnalité fonctionne sur les plates-formes Telco avec l'achat d'une licence CBM de base et d'une licence CBM Premium et pour d'autres plates-formes Citrix ADC, la fonctionnalité fonctionne avec l'achat d'une licence CNS Premium.

Remarque : en plus d'une licence CBM Basic et d'une licence CBM Premium, l'appliance doit posséder une licence URL Threat Intelligence avec un service d'abonnement pendant 1 an ou 3 ans. Avant d'activer et de configurer la fonctionnalité, vous devez installer les licences suivantes :

Prise en charge des licences pour les plates-formes Telco :

- **CBM_TXXX_SERVER_Retail.lic**
- **CBM_TPRE_Server_Retail.lic**
- **CNS_Webf_SServer_Retail.lic**

Où XXX est le débit, par exemple Citrix ADC T1000.

Prise en charge des licences pour d'autres plates-formes Citrix ADC :

- **CNS_XXX_Server_PLT_Retail.lic**

Où XXX est le débit.

Expressions de stratégie de catégorisation d'URL

Le tableau suivant répertorie les différentes expressions de stratégie de catégorisation d'URL permettant d'identifier les URL entrantes et applique une action configurée.

Expression.	Opération
<text>. URL_CATEGORIZE (< min_reputation>, <max_reputation>)	Renvoie un objet URL_CATEGORY. Le score de réputation est un nombre de 1 à 4. Pour obtenir des objets, tous les scores de réputation utilisent 0,0 comme <min reputation> et <max_reputation>. En cas <min_reputation> est supérieur à 0, l'objet renvoyé ne contient pas de catégorie dont la réputation est inférieure à <min_reputation>. En cas <max_reputation> est supérieur à 0, l'objet renvoyé ne contient pas de catégorie dont la réputation est supérieure à <max_reputation>. Si la catégorie ne parvient pas à résoudre en temps opportun, la valeur undef est renvoyée.
<url_category>. CATEGORY	Renvoie la chaîne de catégorie de cet objet. Si l'URL n'a pas de catégorie, ou si l'URL est mal formée, la valeur renvoyée est "Uncategorized".
<url_category>. GROUP	Renvoie une chaîne identifiant le groupe de catégories de l'objet. Il s'agit d'un regroupement de catégories de niveau supérieur, ce qui est utile dans les opérations qui nécessitent des informations moins détaillées sur la catégorie d'URL. Si l'URL n'a pas de catégorie, ou si l'URL est mal formée, la valeur renvoyée est "Uncategorized".
<url_category>. REPUTATION	Renvoie le score de réputation sous la forme d'un nombre compris entre 1 et 4, où 4 indique la réputation la plus risquée. Si la catégorie est « Non classé », la valeur de réputation est 2.

Exemples d'expressions de stratégie

Stratégie	Expressions de stratégie
Stratégie pour sélectionner les demandes d'URL qui se trouvent dans la catégorie Moteur de recherche	add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGO CATEGORY.EQ("Search Engine")
Stratégie pour sélectionner les demandes d'URL qui se trouvent dans le groupe de catégorie Adulte	add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGO GROUP.EQ("Adult")'
Stratégie permettant de sélectionner les demandes d'URL du moteur de recherche avec un score de réputation égal à 4.	add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGO CATEGORY.EQ("Search Engine")'
Stratégie de sélection des demandes pour les URL de moteur de recherche et d'achat	add policy patset good_categories; bind policy good_categories "Search Engine"; bind policy good_categories "Shopping"; add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGO CATEGORY .EQUALS_ANY("good_categories")
Stratégie permettant de sélectionner les demandes d'URL du moteur de recherche avec un score de réputation égal à 4.	add responder policy p5 'CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(4,0). CATEGORY.EQ("Search Engine")

Actions de stratégie de catégorisation d'URL

Une stratégie de filtrage d'URL évalue le trafic pour identifier les demandes appartenant à une catégorie particulière. Le tableau suivant répertorie les actions que vous pouvez affecter à une stratégie de filtrage d'URL.

Action stratégique	Groupe de stratégies	Description
ALLOW	Répondeur	Autoriser la requête entrante à accéder à l'URL cible
REDIRECT	Répondeur	Redirigez la demande entrante vers l'URL spécifiée comme cible.
DENY	Répondeur	Refuser la demande entrante.
RESET	Responder, VideoOptimization	Réinitialiser la connexion.

Action stratégique	Groupe de stratégies	Description
DROP	Responder, VideoOptimization	Laisse tomber la connexion.

> **Remarque**
>
> Pour le trafic chiffré, la stratégie VideoOptimization inclut des actions qui implémentent les actions de filtrage d'URL.

Configuration de la catégorisation d'URL

Pour configurer la catégorisation d'URL, commencez par activer la fonction de filtrage d'URL. Vous devez ensuite configurer les limites de mémoire cache, la stratégie de catégorisation et les serveurs virtuels pour le trafic HTTP et HTTPS. Configuration de la catégorisation d'URL à l'aide de l'interface de ligne de commande.

Pour utiliser la catégorisation d'URL de configuration de l'interface de ligne de commande sur une appliance Citrix ADC, procédez comme suit :

- Configurez la catégorisation des URL.
  - Activez la fonction de filtrage d'URL.
  - Configurez la mémoire partagée pour limiter la mémoire cache.
  - Configurez les paramètres de catégorisation d'URL.
- Configurez la catégorisation d'URL pour le trafic HTTP.
  - Ajouter des actions de catégorisation d'URL.
  - Ajouter des stratégies de catégorisation d'URL.
  - Ajoutez un serveur virtuel d'équilibrage de charge pour le trafic HTTP.
  - Liez les stratégies de catégorisation d'URL au serveur virtuel d'équilibrage de charge.
- Configurez la catégorisation d'URL pour le trafic HTTPS.
  - Ajouter des stratégies de catégorisation d'URL.
  - Ajouter un serveur virtuel d'équilibrage de charge SSL Bridge.
  - Liez les stratégies de catégorisation d'URL au serveur virtuel d'équilibrage de charge.

Configuration de la catégorisation d'URL

Pour configurer la fonctionnalité, vous devez activer la fonction de catégorisation d'URL, configurer les paramètres de filtrage et définir la limite de mémoire partagée.

Pour activer la fonction de filtrage d'URL

À l'invite de commandes, tapez :


```
enable ns feature URLFiltering VideoOptimization Responder IC SSL AppFlow
```

Pour configurer la limite de mémoire partagée

À l'invite de commandes, tapez :

```
1 set cache parameter [-memLimit <megaBytes>]
2 <!--NeedCopy-->
```

Où MemLimit est la limite de mémoire pour la mise en cache.

Exemple :

```
set cache parameter -memLimit 10
```

Pour configurer les paramètres de catégorisation d'URL

À l'invite de commandes, tapez :

```
1 set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>]
     [-TimeOfDayToUpdateDB <HH:MM>]
2 <!--NeedCopy-->
```

***Exemple :**

```
set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
03:00
```

Configuration de la catégorisation d'URL pour le trafic HTTP

Pour configurer la fonction de catégorisation d'URL pour le trafic HTTP, vous devez configurer un serveur virtuel d'équilibrage de chargement, ajouter des stratégies de catégorisation d'URL et lier les stratégies au serveur virtuel. Ce faisant, le serveur virtuel reçoit le trafic HTTP et, en fonction de l'évaluation des stratégies, le système attribue une action de filtrage.

Pour ajouter une action de catégorisation d'URL pour le trafic HTTP

À l'invite de commandes, tapez :

```
add responder action <name> <type> (<target> | <htmlpage>)[-comment <string
>] [-responseStatusCode <positive_integer>] [-reasonPhrase <string>]
```

Exemple :


```
add responder action act_url_categorize respondwith "\"HTTP/1.1 200 OK\r\n\
r\n\" + HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY
 + \"\n\""
```

Pour ajouter une stratégie de catégorisation d'URL pour le trafic HTTP

À l'invite de commandes, tapez :

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
string>] [-logAction <string>] [-appflowAction <string>]
```

Exemple :

```
add responder policy pol_url_categorize_http "HTTP.REQ.HOSTNAME.APPEND(
HTTP.REQ.URL).URL_CATEGORIZE(0,0).GROUP.EQ(\"Adult\")|| HTTP.REQ.HOSTNAME.
APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).GROUP.EQ(\"Gambling\")"RESET
```

Pour ajouter un serveur virtuel d'équilibrage de charge HTTP

Si un serveur virtuel pour le trafic HTTP n'est pas déjà configuré, à l'invite de commandes, tapez :

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-clt Timeout
<secs>]
```

Exemple :

```
add lb vserver vsrv-HTTP HTTP * 80 -persistenceType NONE -cltTimeout 120
```

Pour lier une stratégie de catégorisation d'URL avec un serveur virtuel d'équilibrage de charge

À l'invite de commandes, tapez :

```
bind lb vserver <name> -policyName <string> [-priority <positive_integer>]
```

Exemple :

```
bind lb vserver vsrv-HTTP -policyName pol_url_categorize_http -priority 10
-gotoPriorityExpression END -type REQUEST
```

Configuration de la catégorisation d'URL pour le trafic HTTPS

Pour configurer la fonction de catégorisation d'URL pour le trafic HTTPS, vous devez configurer un serveur virtuel d'équilibrage de chargement SSL, ajouter des stratégies de catégorisation d'URL et lier les stratégies au serveur virtuel de pont SSL. Ce faisant, le serveur reçoit le trafic HTTPS et, en fonction de l'évaluation de la stratégie, le système attribue une action de filtrage.

Pour ajouter une stratégie de catégorisation d'URL pour le trafic HTTPS

À l'invite de commandes, tapez :

```
add videooptimization detectionpolicy <name> -rule <expression> -action <
string> [-undefAction <string>] [-comment <string>] [-logAction <string>]
```

Exemple :

```
add videooptimization detectionpolicy pol_url_categorize_https_block_adult -
rule "CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(0,0).CATEGORY.EQ("Adult")' -
action RESET
```

Pour ajouter un serveur virtuel d'équilibrage de charge SSL pont

À l'invite de commandes, tapez :

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT imeout
<secs>]
```

Exemple :

```
add lb vserver vsrv-HTTPS SSL_BRIDGE * 443 -persistenceType NONE -cltTimeout
 180
```

Pour lier une stratégie de catégorisation avec un serveur virtuel SSL Bridge

À l'invite de commandes, tapez :

```
bind lb vserver <name> -policyName <string> [-priority <positive_integer>]
```

Exemple :

```
bind lb vserver vsrv-HTTPS -policyName pol_url_categorize_https_block_adult
 -priority 20 -type REQUEST
```

Configuration de la catégorisation d'URL à l'aide de l'interface graphique

L'interface graphique vous permet de :

- Activez la fonction de catégorisation d'URL.
- Ajouter des actions de catégorisation d'URL pour le trafic HTTP.
- Ajouter des stratégies de catégorisation d'URL pour le trafic HTTP.
- Ajouter des stratégies de catégorisation d'URL pour le trafic HTTPS.
- Ajoutez un serveur virtuel d'équilibrage de charge pour le trafic HTTP.
- Ajoutez un serveur virtuel d'équilibrage de charge de pont SSL pour le trafic HTTPS.
- Liez les stratégies de catégorisation d'URL au serveur virtuel d'équilibrage de charge.

- Liez les stratégies de catégorisation d'URL au serveur virtuel d'équilibrage de charge SSL Bridge.
- Configurez la limite de mémoire partagée.
- Configurez les paramètres de catégorisation d'URL.

Pour activer la catégorisation d'URL

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres** .
2. Dans la page **Paramètres**, cliquez sur le lien **Configurer les fonctionnalités avancées** .
3. Dans la page **Configurer les fonctionnalités avancées**, activez la case à cocher **Filtrage d'URL** .
4. Cliquez sur **OK** et **Fermer**.

Pour ajouter une action de catégorisation d'URL

1. Dans le volet de navigation, développez **AppExpert** > **Répondeur** > **Action** .
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer une action de répondeur**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'action de stratégie de catégorisation d'URL.
   b) **Type**. Sélectionnez un type d'action.
   c) **Expression**. Utilisez l'éditeur d'expressions pour créer l'expression de stratégie.
   d) **Commentaires**. Une brève description de l'action de stratégie.
4. Cliquez sur **Créer** et **Fermer**.

Pour ajouter une stratégie de catégorisation d'URL pour le trafic HTTP

1. Dans le volet de navigation, développez **AppExpert** > **Répondeur** > **Stratégies**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer une stratégie de répondeur**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'action de stratégie de catégorisation d'URL.
   b) **Action** : Sélectionnez l'action de catégorisation d'URL que vous préférez associer à la stratégie.
   c) **Actions de journalisation**. Sélectionnez l'action du journal.
   d) **AppFlow**. Sélectionnez une action AppFlow.
   e) **Expression**. Utilisez l'éditeur d'expressions pour créer l'expression de stratégie.
   f) **Commentaires**. Une brève description sur l'action de stratégie.
4. Cliquez sur **Créer** et **Fermer**.

Pour ajouter une stratégie de catégorisation pour le trafic HTTPS

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à **Configuration** > **Optimisation** > **Optimisation vidéo** > **Détection**.
2. Dans la page **Détection**, cliquez sur le lien **Stratégies de détection d'optimisation vidéo**.
3. Dans la page Stratégies de détection d'optimisation vidéo, cliquez sur **Ajouter**.
4. Dans la page **Créer une stratégie de détection d'optimisation vidéo**, définissez les paramètres suivants.
   a) **Nom**. Nom de la stratégie d'optimisation
   b) **Expression**. Configurez la stratégie à l'aide d'expressions personnalisées.
   c) **Action** : Action d'optimisation associée à la stratégie pour gérer le trafic vidéo entrant.
   d) **Action de l'UNDEF**. Événement non défini si la demande entrante ne correspond pas à la stratégie d'optimisation.
   e) **Commentaire**. Une brève description de la stratégie.
   f) **Action de journalisation.** Sélectionnez une action du journal d'audit qui spécifie l'action à effectuer pour les messages du journal.
5. Cliquez sur **Créer** et **Fermer**.

Pour ajouter un serveur virtuel d'équilibrage de charge pour le trafic HTTP

1. Accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Serveur virtuel d'équilibrage** de charge, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Choisissez le type de protocole comme HTTP.
   c) **Type d'adresse IP.** IPv4 ou IPv6.
   d) **Adresse IP.** IPv4 ou IPv6, adresse VIP attribuée au serveur virtuel.
   e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez sur **OK** pour poursuivre la configuration des autres paramètres facultatifs.
5. Cliquez sur **Créer** et **Fermer**.

Pour ajouter un serveur virtuel d'équilibrage de charge SSL pont

1. Accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Serveur virtuel d'équilibrage** de charge, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Sélectionnez le type de protocole comme pont SSL.
   c) **Type d'adresse IP**. Type adressable IP.
   d) **Adresse IP**. Adresse IP 4 ou IP6 attribuée au serveur virtuel.

e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez **sur OK** pour continuer la configuration d'autres paramètres facultatifs.
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour lier une stratégie de catégorisation d'URL au serveur virtuel d'équilibrage de charge HTTP

1. Accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet d'informations, sélectionnez le serveur virtuel d'équilibrage de charge et cliquez sur **Modifier**.
3. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
4. Dans la section **Stratégies**, cliquez sur l'icône **+** pour accéder au curseur **Stratégies**.
5. Définissez les paramètres suivants.
   a) **Choisissez Policy**. Sélectionnez la stratégie de catégorisation d'URL dans la liste déroulante.
   b) **Choisissez Type**. Sélectionnez le type de stratégie en tant que Demande.
6. Cliquez sur **Continuer**.
7. Sélectionnez la stratégie de catégorisation d'URL dans la liste et cliquez sur **Fermer**.

Pour lier une stratégie de catégorisation au serveur virtuel d'équilibrage de charge SSL pont

1. Accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel d'équilibrage de charge SSL Bridge et cliquez sur **Modifier**.
3. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
4. Dans la section **Stratégies**, cliquez sur l'icône **+** pour accéder au curseur **Stratégies** .
5. Dans la section **Stratégies**, définissez les paramètres suivants.
   a) **Choisissez Policy**. Sélectionnez la stratégie de détection vidéo dans la liste déroulante.
   b) **Choisissez Type**. Sélectionnez le type de stratégie en tant que Demande.
6. Cliquez sur **Continuer**.
7. Sélectionnez la stratégie de détection vidéo dans la liste et cliquez sur **Fermer**.

Pour configurer la limite de mémoire partagée

1. Connectez-vous à l'appliance et accédez à **Optimisation** > **Mise en cache intégrée**.
2. Dans le volet d'informations, cliquez sur le lien **Modifier les paramètres du cache** .
3. Dans la page **Paramètres globaux du cache**, définissez les paramètres suivants.
   a) **Limite d'utilisation de la mémoire (Mo).**
   b) **Limite d'utilisation de la mémoire active**.
   c) **Via En-tête**.
   d) **Longueur maximale du corps du poste à mettre en cache**

e) **Action globale à résultat indéfini**
f) **Activer la persistance de l'objet HA**
g) **Vérifier la persistance de l'objet mis en cache**
h) **Pré-récupérés**

4. Cliquez sur **OK** et **Fermer**.

Pour configurer les paramètres de catégorisation d'URL

1. Connectez-vous à l'appliance et accédez à **Sécurité**.
2. Dans le volet d'informations, cliquez sur **Modifier le lien des paramètres de filtrage d'URL** .
3. Dans la page **Configuration des paramètres de filtrage d'URL**, définissez les paramètres suivants.
   a) Heures entre les mises à jour de base de données. Heures de filtrage d'URL entre les mises à jour de la base de données. Valeur minimale : 0 et Valeur maximale : 720.
   b) Heure de la journée pour mettre à jour la base de données. URL Filtrage heure de la journée pour mettre à jour la base de données.
4. Cliquez sur **OK** et sur **Fermer.**

Configuration de la messagerie du journal d'audit

Lorsqu'une appliance Citrix ADC reçoit une URL entrante, si la stratégie de répondeur possède une expression de filtrage d'URL, la fonctionnalité du journal d'audit collecte les informations de catégorisation et les affiche sous forme de messages de journal à tout serveur de journal d'audit cible configuré. Les informations sont consignées.

- Adresse IP source (adresse IP du client qui a fait la demande).
- Adresse IP de destination (adresse IP du serveur demandé).
- URL demandée contenant le schéma, l'hôte et le nom de domaine (`http://www.example.com`).
- Catégorie d'URL renvoyée par le cadre de filtrage d'URL.
- groupe de catégories d'URL renvoyé par le cadre de filtrage d'URL.
- Numéro de réputation d'URL renvoyé par le cadre de filtrage d'URL.
- Action du journal d'audit effectuée par la stratégie de catégorisation d'URL.

Pour configurer la journalisation d'audit pour la fonctionnalité Liste d'URL, vous devez effectuer les tâches suivantes :

1. Activer le journal d'audit :
2. Action Créer un message journal d'audit.
3. Définissez la stratégie de répondeur de liste d'URL avec l'action de message Journal d'audit.

Pour plus d'informations, consultez la rubrique Audit Logging .

Stockage des erreurs d'échec à l'aide de la messagerie SYSLOG

À n'importe quelle étape du processus de filtrage d'URL, en cas de défaillance au niveau du système, l'appliance Citrix ADC utilise le mécanisme du journal d'audit pour stocker les journaux dans le fichier ns.log. Les erreurs sont stockées sous forme de messages texte au format SYSLOG de sorte qu'un administrateur puisse les afficher plus tard dans un ordre chronologique d'occurrence d'événement. Ces journaux sont également envoyés à un serveur SYSLOG externe pour archivage. Pour plus d'informations, consultez l'article CTX229399.

Par exemple, si un échec se produit lorsque vous initialisez le SDK de filtrage d'URL, le message d'erreur est stocké dans le format de messagerie suivant.

3 oct 15 : 43:40 <local0.err> ns URLFiltering[1349] : Erreur lors de l'initialisation du SDK NetStar (erreur SDK = -1). (statut = 1).

L'appliance Citrix ADC stocke les messages d'erreur sous quatre catégories de défaillance différentes :

- Échec du téléchargement. Si une erreur se produit lorsque vous essayez de télécharger la base de données de catégorisation.
- Échec de l'intégration. Si une erreur se produit lorsque vous intégrez une mise à jour dans la base de données de catégorisation existante.
- Échec de l'initialisation. Si une erreur se produit lorsque vous initialisez la fonction de catégorisation d'URL, définissez des paramètres de catégorisation ou terminez un service de catégorisation.
- Échec de la récupération. Si une erreur se produit lorsque l'appliance récupère les détails de catégorisation de la demande.

Score de réputation d'URL

La fonction de catégorisation d'URL fournit un contrôle basé sur des stratégies pour restreindre les URL sur la liste rouge. Vous pouvez contrôler l'accès aux sites Web en fonction de la catégorie d'URL, du score de réputation ou de la catégorie d'URL et du score de réputation. Si un administrateur réseau surveille un utilisateur accédant à des sites Web à risque élevé, il peut utiliser une stratégie de répondeur liée au score de réputation d'URL pour bloquer ces sites Web à risque.

À la réception d'une demande d'URL entrante, l'appliance récupère la catégorie et le score de réputation de la base de données de catégorisation d'URL. En fonction du score de réputation renvoyé par la base de données, l'appliance attribue une cote de réputation aux sites Web. La valeur peut varier de 1 à 4, où 4 est le type de sites Web le plus risqué, comme indiqué dans le tableau suivant.

Classement de la réputation d'URL	Commentaire de réputation
1	Nettoyer le site.
2	Site inconnu.

Classement de la réputation d'URL	Commentaire de réputation
3	Potentiellement dangereux ou affilié à un site dangereux.
4	Site malveillant.

FAQ

August 20, 2021

Cette section fournit la FAQ sur les fonctionnalités suivantes de Citrix ADC

- Partition d'administration
- AppFlow
- Call Home
- Mise en cluster
- Gestion des connexions
- Commutation de contenu
- Débogage
- Matériel
- Haute disponibilité
- Mise en cache intégrée
- Installation, mise à niveau et rétrogradation
- Équilibrage de charge
- NetScaler GUI
- SSL

Partition d'administration

August 20, 2021

Où puis-je obtenir le fichier de configuration Citrix ADC pour une partition ?

Le fichier de configuration (*ns.conf*) de la partition par défaut est disponible dans le répertoire */nsconfig*. Pour les partitions d'administration, le fichier est disponible dans le répertoire */nsconfig/partitions/<partitionName>*.

Comment puis-je configurer la mise en cache intégrée dans une appliance Citrix ADC partitionnée ?

> **Remarque**
>
> La mise en cache intégrée dans les partitions d'administration est prise en charge à partir de NetScaler 11.0.

Pour configurer la mise en cache intégrée (IC) sur un Citrix ADC partitionné, après avoir défini la mémoire IC sur la partition par défaut, le superutilisateur peut configurer la mémoire IC sur chaque partition d'administration de telle sorte que la mémoire IC totale allouée à toutes les partitions d'administration ne dépasse pas la mémoire IC définie sur la partition par défaut. La mémoire qui n'est pas configurée pour les partitions d'administration reste disponible pour la partition par défaut.

Par exemple, si une appliance Citrix ADC avec deux partitions d'administration dispose de 10 Go de mémoire IC allouée à la partition par défaut et que l'allocation de mémoire IC pour les deux partitions d'administration est la suivante :

- Partition1 : 4 Go
- Partition2 : 3 Go

Ensuite, la partition par défaut a 10 - (4 + 3) = 3 Go de mémoire IC disponible pour l'utilisation.

> **Remarque**
>
> Si toute la mémoire CI est utilisée par les partitions d'administration, aucune mémoire CI n'est disponible pour la partition par défaut.

Quelle est la portée des paramètres L2 et L3 dans les partitions d'administration ?

> **Remarque**
>
> - Applicable à partir de NetScaler 11.0.
> - Pour que ARP fonctionne dans une partition autre que par défaut, vous devez activer le paramètre « ProxyARP » dans la commande « set l2param ».

Sur une appliance Citrix ADC partitionnée, l'étendue de la mise à jour des paramètres L2 et L3 est la suivante :

- Pour les paramètres L2 définis à l'aide de la commande « set L2Param », les paramètres suivants peuvent être mis à jour uniquement à partir de la partition par défaut, et leurs valeurs sont applicables à toutes les partitions d'administration :

  MaxBridgeCollision, BDGSetting, GarpOnVridintf, GarpReply, ProxyARP, ResetInterfaceOnHafailOver et skip_proxying_bsd_traffic.

  Les autres paramètres L2 peuvent être mis à jour dans des partitions d'administration spécifiques, et leurs valeurs sont locales à ces partitions.

- Pour les paramètres L3 définis à l'aide de la commande « set L3Param », tous les paramètres peuvent être mis à jour dans des partitions d'administration spécifiques, et leurs valeurs sont locales à ces partitions. De même, les valeurs mises à jour dans la partition par défaut ne s'appliquent qu'à la partition par défaut.

Comment activer le routage dynamique dans une partition d'administration ?

> **Remarque**
>
> Le routage dynamique dans les partitions d'administration est pris en charge à partir de NetScaler 11.0.

Alors que le routage dynamique (OSPF, RIP, BGP, ISIS, BGP+) est activé par défaut sur la partition par défaut, dans une partition admin, il doit être activé à l'aide de la commande suivante :

```
> set L3Param -dynamicRouting ENABLED
```

> **Remarque**
>
> Un maximum de 63 partitions peuvent exécuter le routage dynamique (62 partitions d'administration et 1 partition par défaut).

Lors de l'activation du routage dynamique sur une partition d'administration, un routeur virtuel (VR) est créé.

- Chaque VR conserve son propre vlan0 qui sera affiché sous la forme vlan0_ <partition-name>.
- Toutes les adresses IP non liées qui sont exposées à des ZEBO sont liées à vlan0.
- Le VR par défaut (de la partition par défaut) affiche tous les VR configurés.
- Le VR par défaut affiche les VLAN qui sont liés à ces VR (à l'exception des VLAN par défaut).

Où puis-je trouver les journaux d'une partition ?

Les journaux Citrix ADC ne sont pas spécifiques à la partition. Les entrées de journal de toutes les partitions doivent être stockées dans le répertoire */var/log/* .

Comment puis-je obtenir des journaux d'audit pour une partition d'administrateur ?

Dans un Citrix ADC partitionné, vous ne pouvez pas disposer de serveurs de journaux spécifiques pour une partition spécifique. Les serveurs définis à la partition par défaut sont applicables à toutes les partitions d'administration. Par conséquent, pour afficher les journaux d'audit d'une partition spécifique, vous devez utiliser la commande « afficher les messages d'audit ».

> **Remarque**
>
> Les utilisateurs d'une partition d'administrateur n'ont pas accès à l'interpréteur de commandes

> et ne peuvent donc pas accéder aux fichiers journaux.

Comment puis-je obtenir des journaux Web pour une partition d'administration ?

Vous pouvez obtenir les journaux Web pour une partition d'administration comme suit :

- **Pour NetScaler 11.0 et versions ultérieures**

  La fonctionnalité de journalisation Web doit être activée sur chacune des partitions qui nécessitent la journalisation Web. À l'aide du client Citrix ADC Web Logging (NSWL), Citrix ADC récupère les journaux Web de toutes les partitions auxquelles l'utilisateur est associé.

- **Pour les versions antérieures à NetScaler 11.0**

  Les journaux Web ne peuvent être obtenus que par `nsroot` et d'autres superutilisateurs. En outre, même si la journalisation Web est activée sur la partition par défaut, le client Citrix ADC Web Logging (NSWL) récupère les journaux Web pour toutes les partitions.

Pour afficher la partition de chaque entrée de journal, personnalisez le format de journal pour inclure l'option%p. Vous pouvez ensuite filtrer les journaux pour afficher les journaux d'une partition spécifique.

Comment puis-je obtenir la trace d'une partition d'administration ?

Vous pouvez obtenir la trace d'une partition d'administration comme suit :

- **Pour NetScaler 11.0 et versions ultérieures**

  Dans une appliance Citrix ADC partitionnée, l'opération `nstrace` peut être effectuée sur des partitions d'administration individuelles. Les fichiers de trace sont stockés dans le répertoire */var/partitions/<partitionName>/nstrace/*.

  Remarque : Vous ne pouvez pas obtenir la trace d'une partition d'administration à l'aide de l'interface graphique. Vous devez utiliser l'interface de ligne de commande.

- **Pour les versions antérieures à NetScaler 11.0**

  L'opération `nstrace` ne peut être effectuée que sur la partition par défaut. Par conséquent, les captures de paquets sont disponibles pour l'ensemble du système Citrix ADC. Pour obtenir des captures de paquets spécifiques à une partition, utilisez des filtres basés sur VLAN-ID.

Comment puis-je obtenir le pack de support technique spécifique à une partition d'administration ?

Pour obtenir le bundle de support technique pour une partition spécifique, vous devez exécuter la commande suivante à partir de la partition par défaut :


```
> show techsupport -scope partition -partitionname <string>
```

Remarque : Cette commande fournit également des informations spécifiques au système.

AppFlow

August 20, 2021

- **Quelle version de Citrix ADC prend en charge AppFlow ?**

  AppFlow est pris en charge sur les appliances Citrix ADC exécutant la version 9.3 et supérieure avec la version nCore.

- **Quel est le format utilisé par AppFlow pour transmettre des données ?**

  AppFlow transmet des informations au format IPFIX (Internet Protocol Flow Information Export), qui est un standard ouvert Internet Engineering Task Force (IETF) défini dans la RFC 5101. IPFIX (la version standardisée de NetFlow de Cisco) est largement utilisé pour surveiller les informations de flux réseau.

- **Que contiennent les enregistrements AppFlow ?**

  Les enregistrements AppFlow contiennent des informations standard NetFlow ou IPFIX, telles que les horodatages pour le début et la fin d'un flux, le nombre de paquets et le nombre d'octets. Les enregistrements AppFlow contiennent également des informations au niveau de l'application (telles que les URL HTTP, les méthodes de requête HTTP et les codes d'état de la réponse, le temps de réponse du serveur et la latence). Les enregistrements de flux IPFIX sont basés sur des modèles qui doivent être envoyés avant d'envoyer des enregistrements de flux.

- **Après une mise à niveau vers NetScaler Version 9.3 Build 48.6 Cl, pourquoi une tentative d'ouverture d'un serveur virtuel à partir de l'interface graphique entraîne le message d'erreur « La fonctionnalité AppFlow est uniquement disponible sur Citrix ADC Ncore » ?**

  AppFlow est pris en charge uniquement sur les appliances nCore. Lorsque vous ouvrez l'onglet Configuration du serveur virtuel, désactivez la case à cocher **AppFlow** .

- **Que contient l'ID de transaction dans un enregistrement AppFlow ?**

  Un ID de transaction est un numéro 32 bits non signé identifiant une transaction au niveau de l'application. Pour HTTP, une transaction correspond à une paire de requête et de réponse. Tous les enregistrements de flux qui correspondent à cette paire demande et réponse ont le même ID de transaction. Une transaction type comporte quatre enregistrements de flux. Si Citrix ADC génère la réponse par lui-même (à partir du cache intégré ou d'une stratégie de sécurité), il peut y avoir seulement deux enregistrements de flux pour la transaction.

- **Qu' est-ce qu'une action AppFlow ?**

  Une action AppFlow est un ensemble de collecteurs auxquels les enregistrements de flux sont envoyés si la stratégie AppFlow associée correspond.

- **Quelles commandes puis-je exécuter sur l'appliance Citrix ADC pour vérifier que l'action AppFlow est un succès ?**

  L'action Afficher AppFlow. Par exemple :

```
> show appflow action
1) Name: aFL-act-collector-1
  Collectors: collector-1
  Hits: 0
  Action Reference Count: 2
 2) Name: apfl-act-collector-2-and-3
  Collectors: collector-2, collecter-3
  Hits: 0
  Action Reference Count: 1
 3) Name: apfl-act-collector-1-and-3
  Collectors: collector-1, collecter-3
  Hits: 0
  Action Reference Count: 1
<!--NeedCopy-->
```

- **Qu' est-ce qu'un collecteur AppFlow ?**

Un collecteur reçoit les enregistrements de flux générés par l'appliance Citrix ADC. Pour pouvoir envoyer des enregistrements de flux, vous devez spécifier au moins un collecteur. Vous pouvez spécifier jusqu'à quatre. Vous pouvez supprimer les collecteurs inutilisés.

- **Quelle version Citrix ADC est requise pour utiliser AppFlow ?**

  Utilisez NetScaler version 9.3.49.5 ou supérieure, et rappelez-vous que AppFlow est disponible uniquement dans les versions nCore.

- **Quel protocole de transport AppFlow utilise-t-il ?**

  AppFlow utilise UDP comme protocole de transport.

- **Quels ports doivent être ouverts si j'ai un pare-feu dans le réseau ?**

  Port 4739. Il s'agit du port UDP par défaut utilisé par le collecteur AppFlow pour écouter des messages IPFIX. Si l'utilisateur modifie le port par défaut, ce port doit être ouvert sur le pare-feu.

- **Comment puis-je modifier le port par défaut utilisé par AppFlow ?**

  Lorsque vous ajoutez un collecteur AppFlow à l'aide de la commande add AppFlowCollector, vous pouvez spécifier le port à utiliser.


```
> add appflowCollector coll1 -IPAddress 10.102.29.251 -port 8000
 Done
<!--NeedCopy-->
```

- **A quoi sert le paramètre ClientTrafficOnly ?**

  Citrix ADC génère des enregistrements AppFlow uniquement pour le trafic côté client.

- **Combien de collecteurs peuvent être configurés à la fois ?**

  Vous pouvez configurer jusqu'à quatre collecteurs AppFlow à la fois sur l'appliance Citrix ADC. Notez que le nombre maximal de collecteurs pouvant être configurés sur une appliance Citrix ADC est de quatre.

Call Home

August 20, 2021

- **Qu' est-ce que Call Home sur une appliance Citrix ADC ?**

  Call Home surveille et notifie les événements critiques sur une appliance Citrix ADC. En activant Call Home, vous pouvez automatiser le processus de notification d'erreur. Vous évitez non seulement d'appeler le support Citrix, de lancer une demande de service et de charger des données système avant que le support Citrix puisse résoudre le problème, mais aussi d'identifier et de résoudre les problèmes avant qu'il ne se produise.

- **Call Home est-il activé par défaut sur une appliance Citrix ADC ?**

  Oui, Call Home est activé par défaut sur l'appliance. Si vous effectuez une mise à niveau vers le dernier logiciel à partir d'une version antérieure où Call Home a été désactivée par défaut, le processus de mise à niveau active automatiquement la fonctionnalité. Si vous décidez ultérieurement de le désactiver, le paramètre mis à jour est mémorisé pour toutes les mises à niveau ultérieures. Pour plus d'informations, voir Call Home.

- **Quelles sont les conditions préalables pour que Call Home fonctionne ?**

  Accès à une connexion Internet.

  Remarque : Si votre appliance Citrix ADC ne dispose pas d'une connectivité Internet, vous pouvez configurer un serveur proxy via lequel Citrix ADC peut générer des journaux système et les télécharger sur le serveur CIS (Citrix Technical Support Server).

- **Quels sont les avantages de l'utilisation de Call Home ?**

  - Surveillez les conditions d'erreur matérielle et logicielle.

  - Avertissez l'apparition d'événements critiques qui ont un impact sur votre réseau.
  - Envoyez des données de performances et des journaux système à Citrix à l'adresse suivante :
    * Analysez et améliorez la qualité des produits.
    * Fournissez des informations de dépannage en temps réel pour une identification proactive des problèmes et une résolution plus rapide des problèmes.

- **Quelle version du logiciel Citrix ADC prend en charge Call Home ?**

  Citrix ADC version 10.0 et ultérieure.

- **Quels modèles de plate-forme Citrix ADC prennent en charge Call Home ?**

  La fonction Call Home est activée par défaut sur toutes les plates-formes Citrix ADC et tous les modèles d'appliance (MPX, VPX et SDX).

  - Citrix ADC MPX : Tous les modèles MPX.
  - Citrix ADC VPX : Tous les modèles VPX. En outre, il est pris en charge sur les appliances VPX qui obtiennent leurs licences à partir de pools de licences externes ou centraux. Toutefois, la fonctionnalité reste la même que pour une appliance VPX standard.
  - Citrix ADC SDX : surveille le lecteur de disque et les puces SSL affectées pour détecter toute erreur ou défaillance. Toutefois, les instances VPX n'ont pas accès à l'unité d'alimentation (PSU) et leur état n'est donc pas surveillé. Dans une plate-forme SDX, vous pouvez configurer Call Home directement sur une instance individuelle ou via la SVM.

- **Dois-je configurer l'alarme SNMP pour Call Home pour notifier les conditions d'erreur ?**

  Non, vous n'avez pas besoin de configurer SNMP pour Call Home pour surveiller les conditions d'erreur, car les téléchargements SNMP et Call Home sont indépendants les uns des autres. Si vous souhaitez être averti chaque fois qu'une condition d'erreur se produit, vous pouvez configurer l'alarme SNMP CALLHOME-UPLOAD-EVENT pour générer une alerte SNMP chaque fois qu'un téléchargement Call Home se produit. L'alerte SNMP informe l'administrateur local des événements critiques.

- **Comment puis-je contacter un support technique ?**

  Pour tous les événements critiques liés au matériel, Call Home crée automatiquement une demande de service à Citrix. Pour d'autres erreurs, une fois que vous avez vérifié les journaux système, vous pouvez contacter l'équipe de support technique Citrix pour ouvrir une demande de service en vue d'une enquête plus approfondie. Pour plus d'informations, voir http://support.citrix.com/article/CTX200021.

- **Quelles sont les conditions d'erreur Call Home moniteur-t-il dans une appliance Citrix ADC ?**

  Call Home prend en charge la surveillance des événements suivants dans une appliance Citrix ADC :

  - Erreurs de lecteur flash compact
  - Erreurs de disque dur
  - Défaillance de l'unité d'alimentation
  - Échec de la carte SSL
  - Redémarrage à chaud
  - Anomalies de mémoire
  - Limite de taux baisse

- **Avez-vous besoin d'une licence distincte pour Call Home ?**

  Non, Call Home ne nécessite pas de licence distincte. Vous pouvez l'activer dans toutes les licences de plate-forme Citrix ADC.

- **Quelles données Call Home envoie-t-il au serveur de support Citrix et à quelle fréquence est-il envoyé ?**

  Call Home collecte et envoie deux types de données au CIS. Ils sont :

  - Informations système de base (exécution de Citrix ADC version, mode de déploiement (autonome, HA, cluster), détails matériels, etc.). Il est envoyé au moment de l'enregistrement Call Home et dans le cadre de battements cardiaques périodiques. Le rythme cardiaque est envoyé une fois tous les 30 jours, mais vous pouvez configurer cet intervalle entre 1 et 30 jours. Cependant, une valeur inférieure à 5 jours n'est pas recommandée, car les chargements fréquents ne sont généralement pas très utiles.
  - Une version abrégée de la condition `show tech support bundle` lorsqu'il y a une erreur. Il est envoyé lors de la première apparition d'une condition d'erreur particulière depuis le dernier démarrage de l'appliance. Autrement dit, une réoccurrence de la même condition d'erreur ne déclenche pas un autre chargement à moins que l'appliance ait été redémarrée après l'occurrence précédente.

- **Call Home peut-il générer et télécharger des journaux système via un serveur proxy ?**

  Oui. Si votre appliance Citrix ADC ne dispose pas de connectivité Internet directe, vous pouvez configurer un serveur proxy et charger les journaux système sur le serveur CIS (Citrix Technical Support Server).

- **Puis-je consulter les données de Call Home avant qu'elles ne soient envoyées à SIC ?**

  Malheureusement, vous ne pouvez pas consulter les Call Home avant d'être envoyées à SIC. Call Home ne collecte aucune autre donnée en plus des données que vous fournirez lorsque vous contactez l'équipe de support Citrix.

- **Dans quelle mesure les téléchargements Call Home sont-ils sécurisés et privés ?**

  Call Home assure la sécurité et la confidentialité des données de la manière suivante :

  - Utilise un canal SSL/TLS sécurisé pour transférer des données vers des serveurs Citrix.

- Les données téléchargées sont examinées uniquement par le personnel autorisé et ne sont pas partagées avec un tiers.

Mise en cluster

August 20, 2021

Cliquez ici pour consulter les questions fréquentes sur le clustering.

Gestion des connexions

August 20, 2021

- **Qu' est-ce qu'une connexion admin ?**

  Une connexion d'administration établit une connexion à l'adresse NSIP et permet aux administrateurs de configurer et de surveiller l'appliance Citrix ADC.

- **Quels sont les types de connexions admin ?**

  Il existe deux types de connexions d'administration :

  - Connexion SSH : les utilisateurs administrateurs utilisent un client SSH pour se connecter via l'adresse NSIP.
  - Connexion à l'API NITRO : les utilisateurs administrateurs utilisent les API NITRO pour automatiser le processus de connexion à l'appliance Citrix ADC.

> **Remarque**
>
> Les utilisateurs administrateurs peuvent également ouvrir une session via l'interface graphique pour se connecter, à l'aide d'un navigateur pour se connecter à l'adresse NSIP. L'interface graphique ouvre en interne une connexion d'API NITRO. Par conséquent, une session GUI équivaut à une connexion API NITRO, et les FAQ relatives à l'API NITRO s'appliquent à l'interface graphique.

- **Combien de connexions d'administration simultanées sont autorisées sur une appliance Citrix ADC ?**

  L'appliance autorise jusqu'à 20 connexions d'administration simultanées.

- **Quelles informations d'identification de connexion sont requises pour une ouverture de session admin ?**

  L'ouverture de session de l'administrateur nécessite un nom d'utilisateur et un mot de passe.

Remarque : Une clé d'authentification peut être utilisée à la place d'un mot de passe.

- **Quelles méthodes d'authentification externe un appliance Citrix ADC prend-il en charge ?**

  L'appliance prend en charge les méthodes d'authentification externes suivantes :

  - RADIUS
  - LDAP
  - TACACS

- **Qu' est-ce qu'un client ?**

  Un client est un appareil (ordinateur portable ou ordinateur de bureau) utilisé par l'utilisateur administrateur pour ouvrir une connexion administrateur.

- **Qu' est-ce qu'un jeton de session ?**

  Un jeton de session est un identifiant unique que l'appliance Citrix ADC émet à un client qui envoie une demande d'ouverture de session de l'API NITRO.

  - Les clients API peuvent réutiliser le jeton de session, s'il n'a pas expiré, pour les requêtes API ultérieures sur les nouvelles connexions TCP
  - Les clients de l'interface graphique ouvrent en interne des connexions à l'API NITRO et gardent le jeton de session actif pendant la session de l'interface graphique.

- **Qu' est-ce qu'une session active sur une appliance Citrix ADC ?**

  Une session CLI est considérée comme active si la session n'a pas expiré et dispose d'une connexion SSH ouverte avec une appliance Citrix ADC.

  Une session API NITRO est considérée comme active si le délai d'expiration du jeton de session n'a pas expiré sur l'appliance Citrix ADC.

- **Comment Citrix ADC applique-t-il la limite de connexion simultanée ?**

  Chaque fois que l'appliance Citrix ADC reçoit une demande de connexion d'administrateur (API SSH ou NITRO), elle vérifie le nombre de connexions d'administration ouvertes. Si le nombre est inférieur à 20, une nouvelle connexion est ouverte.

- **Quel compteur reflète le nombre de connexions d'administration sur une appliance Citrix ADC ?**

  Le compteur de connexion (nsconfigd_cur_clients) reflète le nombre de connexions actives. Ce compteur est incrémenté lorsqu'un client ouvre une nouvelle connexion à l'appliance et est décrémenté lorsqu'une connexion est fermée.

- **Quel compteur reflète le nombre de jetons actifs sur l'appliance Citrix ADC ?**

  Le compteur *configd_cur_tokens* reflète le nombre de jetons actifs sur l'appliance Citrix ADC.

- **Comment l'appliance Citrix ADC traite-t-elle les erreurs sur une connexion ?**

L'appliance Citrix ADC ferme immédiatement la connexion client (CLI, API et GUI) si elle rencontre des erreurs sur une connexion.

- **Une session CLI ou GUI sur une connexion à l'adresse de gestion compte-t-elle par rapport à la limite de connexion admin ?**

  Oui, toutes les connexions CLI et GUI sont des connexions TCP, et chaque connexion TCP à l'adresse de gestion compte par rapport à la limite de connexion administrateur.

- **Une session NITRO compte-t-elle par rapport à la limite de connexion admin ?**

  Une session NITRO compte sur la limite de connexion d'administrateur si une connexion TCP est ouverte à l'aide du jeton de session émis par l'appliance Citrix ADC.

- **Quel est le délai d'expiration par défaut pour les sessions API, GUI et CLI sur l'appliance Citrix ADC ?**

  Le tableau suivant répertorie le délai d'expiration par défaut pour les sessions API, GUI et CLI sur l'appliance Citrix ADC :

Versions de Citrix ADC	Délai d'expiration par défaut de la CLI (min)	Délai d'expiration par défaut de l'API (min)	Délai d'expiration par défaut de l'interface graphique (min)
NetScaler 9.3	Aucune	30 Minutes	30 Minutes
NetScaler 10.1	Aucune	30 Minutes	30 Minutes
NetScaler 10.5 à partir de	15 Minutes	30 Minutes	15 Minutes

- **Comment définir le délai d'expiration des sessions CLI sur une appliance Citrix ADC ?**

  Le délai d'expiration de la session CLI peut être configuré en exécutant la commande suivante à l'invite de l'interface de ligne de commande :

  ```
  set cli mode -timeout \<xx seconds>
  ```

- **Comment remplacer le délai d'expiration par défaut lors de l'utilisation de l'API NITRO ?**

  Vous pouvez remplacer le délai d'expiration par défaut pour une API NITRO en définissant la durée d'expiration dans le champ « timeout » de l'objet login. Si le délai d'expiration de session est défini sur zéro, le jeton de session a un délai d'expiration infini.

  Remarque : Un délai d'expiration infini n'est pas conseillé, car les sessions qui n'ont pas de délai d'expiration continuent à compter sur le nombre de connexions administrateur.

- **Que se passe-t-il si un compte d'utilisateur est supprimé de l'appliance Citrix ADC après la création d'une session d'administration ?**

Pour les utilisateurs internes du système, l'appliance Citrix ADC ferme la session CLI ou NITRO API existante.

Pour les utilisateurs du système externes, la session reste active jusqu'à son expiration.

- Les**clients API NITRO peuvent-ils utiliser un seul jeton de session pour ouvrir plusieurs connexions d'administration sur l'appliance Citrix ADC ?**

  Oui. Chaque connexion de ce type est comptée par rapport à la limite de connexion d'administrateur.

- **Si l'accès à la gestion est activé pour une adresse SNIP, les connexions administrateur à cette adresse compte-t-elle dans la limite du nombre de connexions administrateur ?**

  Oui, les connexions d'administrateur à l'adresse de gestion (SNIP) comptent dans la limite de connexion administrateur sur Citrix ADC.

- **Un administrateur Citrix ADC peut-il ouvrir une session sur l'appliance Citrix ADC une fois que la limite maximale de connexions est atteinte ?**

  Oui. Une autre connexion administrateur est autorisée une fois la limite maximale de connexion atteinte.

- Les**points de terminaison de l'API NITRO peuvent-ils ouvrir plusieurs connexions d'administration sur Citrix ADC l'appliance ?**

  Oui, les points de terminaison de l'API NITRO peuvent ouvrir plusieurs connexions d'administration et épuiser la limite de connexion d'administration simultanée sur une appliance Citrix ADC. Dans de telles situations, une connexion SSH/CLI supplémentaire est autorisée et l'administrateur peut forcer la fermeture des anciennes sessions API ou réduire la durée du délai d'expiration de la session pour les sessions API existantes.

- **Le même client peut-il ouvrir plusieurs sessions API sur une appliance Citrix ADC ?**

  Oui, un client peut ouvrir plusieurs sessions API en se connectant à plusieurs reprises. Par exemple, le client peut se reconnecter après un redémarrage.
  Remarque : les ouvertures de session client répétées sont comptabilisées par rapport à la limite de connexion admin sur l'appliance Citrix ADC.

- Les**clients API peuvent-ils utiliser toute la limite de jeton de session API ?**

  Oui, les clients API peuvent utiliser toute la limite de jeton de session API, fournie en se connectant de manière répétée sans utiliser un jeton émis précédemment.

  Remarque : Si le délai d'expiration de session d'un client est égal à zéro, le jeton est valide pour toujours. Les ouvertures de session répétées utilisant de nouveaux jetons de session peuvent être comptabilisées par rapport à la limite des jetons de session API.

- **Les sessions CLI sont-elles comptabilisées par rapport à la limite de jeton de session API ?**

Non, les sessions CLI ne sont pas comptées par rapport à la limite de jeton de session API.

- **Les utilisateurs d'administration peuvent-ils utiliser telnet pour ouvrir une session CLI ?**

  Non. Seul un client SSH peut ouvrir une session CLI.

- **Qu' est-ce que la limite de connexion et la limite de session API applicables aux différentes versions de Citrix ADC ?**

  Le tableau suivant répertorie les limites maximales de connexion admin simultanée et de session API active applicables aux différentes versions de Citrix ADC :

Versions de Citrix ADC	9.3	10.1 (Avant 130.x)	10.1 (Avant 130.10)	10.1 (De 130.10)
Nombre maximal de connexions d'administration simultanées	20	20	20	20
Nombre maximal de sessions API actives*	1 000	20	1 000	1 000

Remarque :

- Les sessions API sont considérées comme actives si elles n'ont pas expiré. Par exemple, si 500 sessions API ont été créées mais que 100 ont expiré, 400 sessions API sont actives.
- Une session API n'a pas besoin d'ouvrir une connexion TCP à l'appliance Citrix ADC.

Commutation de contenu

October 5, 2021

- **J'ai installé une appliance d'équilibrage de charge non Citrix ADC sur le réseau. Toutefois, je souhaite utiliser la fonctionnalité de commutation de contenu de l'appliance Citrix ADC pour diriger les demandes des clients vers l'appliance d'équilibrage de charge. Est-il possible d'utiliser la fonctionnalité de commutation de contenu de l'appliance Citrix ADC avec une appliance d'équilibrage de charge autre que Citrix ADC ?**

  Oui. Vous pouvez utiliser la fonctionnalité de commutation de contenu de l'appliance Citrix ADC avec la fonctionnalité d'équilibrage de charge de l'appliance Citrix ADC ou d'une appliance

d'équilibrage de charge non Citrix ADC. Toutefois, lorsque vous utilisez l'appliance d'équilibrage de charge non Citrix ADC, assurez-vous de créer un serveur virtuel d'équilibrage de charge sur l'appliance Citrix ADC et de le lier à l'appliance d'équilibrage de charge non Citrix ADC en tant que service.

- **En quoi un serveur virtuel de commutation de contenu diffère-t-il d'un serveur virtuel d'équilibrage de charge ?**

  Un serveur virtuel de commutation de contenu est uniquement capable d'envoyer les demandes des clients à d'autres serveurs virtuels. Il ne communique pas avec les serveurs.

  Un serveur virtuel d'équilibrage de charge équilibre la charge du client entre les serveurs et communique avec les serveurs. Il surveille la disponibilité du serveur et peut être utilisé pour appliquer différents algorithmes d'équilibrage de charge afin de répartir la charge du trafic.

  La commutation de contenu est une méthode utilisée pour diriger les demandes des clients pour des types spécifiques de contenu vers des serveurs ciblés au moyen de serveurs virtuels d'équilibrage de charge. Vous pouvez diriger les demandes des clients vers les serveurs les mieux adaptés pour les traiter. Il en résulte une réduction des frais généraux de traitement des demandes des clients sur les serveurs.

- **Je souhaite implémenter la fonctionnalité de commutation de contenu de l'appliance Citrix ADC pour diriger les demandes des clients. Quels types de demandes client puis-je adresser à l'aide de la fonction de changement de contenu ?**

  Vous pouvez diriger uniquement des demandes de clients HTTP, HTTPS, FTP, TCP, TCP sécurisé et RTSP à l'aide de la fonction de commutation de contenu. Pour diriger les demandes des clients HTTPS, vous devez configurer la fonctionnalité de déchargement SSL sur l'appliance.

- **Je souhaite créer des règles de commutation de contenu sur l'appliance Citrix ADC. Quels sont les différents éléments de la demande du client sur lesquels je peux créer une règle de changement de contenu ?**

  Vous pouvez créer les règles de changement de contenu en fonction des éléments suivants et de leurs valeurs dans la demande du client :

  - URL
  - jetons URL
  - version HTTP
  - En-têtes HTTP
  - Adresse IP source du client
  - Version client
  - Port TCP de destination

- **Je comprends que la fonctionnalité de commutation de contenu de l'appliance Citrix ADC contribue à améliorer les performances du réseau. Est-ce que c'est exact ?**

Oui. Vous pouvez diriger les demandes des clients vers les serveurs les mieux adaptés pour les traiter. Il en résulte une réduction de la surcharge de traitement des demandes des clients sur les serveurs.

- **Quelle fonctionnalité de l'appliance Citrix ADC dois-je configurer sur l'appliance Citrix ADC pour améliorer la gérabilité du site et le temps de réponse aux demandes des clients ?**

  Vous pouvez configurer la fonctionnalité de commutation de contenu de l'appliance Citrix ADC pour améliorer la gestion du site et le temps de réponse à la demande du client. Cette fonctionnalité vous permet de créer des groupes de contenu au sein du même nom de domaine et de la même adresse IP. Cette approche est flexible, contrairement à l'approche commune consistant à partitionner explicitement le contenu en différents noms de domaine et adresses IP, qui sont visibles par l'utilisateur.

  Plusieurs partitions divisant un site Web en différents noms de domaine et adresses IP forcent le navigateur à créer une connexion distincte pour chaque domaine qu'il trouve lors du rendu et de la récupération du contenu d'une page Web. Ces connexions WAN supplémentaires dégradent le temps de réponse de la page Web.

- **J'ai hébergé un site Web sur une batterie de serveurs Web. Quels sont les avantages de la fonctionnalité de commutation de contenu Citrix ADC pour ce type de configuration ?**

  La fonctionnalité de commutation de contenu offre les avantages suivants sur une appliance Citrix ADC dans un site basé sur une batterie de serveurs Web :

  - Gérez le contenu du site en créant un groupe de contenus au sein du même domaine et de la même adresse IP.
  - Améliorez le temps de réponse aux demandes des clients en utilisant le groupe de contenus au sein du même domaine et de la même adresse IP.
  - Évitez de recourir à la réplication complète du contenu entre les domaines.
  - Activez le partitionnement de contenu spécifique à l'application. Par exemple, vous pouvez diriger les demandes des clients vers un serveur qui gère uniquement le contenu dynamique ou uniquement le contenu statique, selon le cas.
  - Prend en charge le multi-hébergement de plusieurs domaines sur le même serveur et utilise la même adresse IP.
  - Réutilisez les connexions aux serveurs.

- **Je souhaite implémenter la fonctionnalité de commutation de contenu sur l'appliance Citrix ADC. Je souhaite diriger les demandes des clients vers les différents serveurs après avoir évalué les différents paramètres de chaque demande. Quelle approche dois-je suivre pour implémenter cette configuration lors de la configuration de la fonctionnalité de changement de contenu ?**

  Vous pouvez utiliser des expressions de stratégie pour créer des stratégies pour la fonctionnalité de changement de contenu. Une expression est une condition évaluée en comparant les quali-

ficatifs de la demande du client à un opérande à l'aide d'un opérateur. Vous pouvez utiliser les paramètres suivants de la demande du client pour créer une expression :

- **Method** : méthode de requête HTTP.
- **URL** : URL dans l'en-tête HTTP.
- **JETONS D'URL**- Jetons spéciaux dans l'URL.
- **VERSION : version**de la requête HTTP.
- **URL QUERY**- Contient le LEN de requête d'URL, le LEN d'URL et l'en-tête HTTP.
- **SOURCEIP** : adresse IP du client.

Voici la liste complète des opérateurs que vous pouvez utiliser pour créer une expression :

- == (égal à)
- ! = (pas égal à)
- EXISTE
- N'EXISTE PAS
- CONTIENT
- NE CONTIENT PAS
- GT (supérieur à)
- LT (inférieur à)

Vous pouvez également créer diverses règles, qui sont des agrégations logiques d'un ensemble d'expressions. Vous pouvez combiner plusieurs expressions pour créer des règles. Pour combiner des expressions, vous pouvez utiliser && (AND) et	opérateurs (OR). Vous pouvez également utiliser des parenthèses pour créer des règles imbriquées et complexes.

- **Je souhaite configurer une stratégie basée sur des règles ainsi qu'une stratégie basée sur une URL pour le même serveur virtuel de commutation de contenu. Est-il possible de créer les deux types de stratégies pour le même serveur virtuel de commutation de contenu ?**

  Oui. Vous pouvez créer les deux types de stratégies pour le même serveur virtuel de commutation de contenu. Toutefois, veillez à attribuer des priorités afin de définir une priorité appropriée pour les stratégies.

- **Je souhaite créer des stratégies de changement de contenu qui évaluent le nom de domaine, ainsi qu'un préfixe et un suffixe d'une URL, et dirigent les demandes des clients en conséquence. Quel type de stratégie de changement de contenu dois-je créer ?**

Vous pouvez créer une stratégie de domaine et d'URL exacte. Lorsque ce type de stratégie est évalué, l'appliance Citrix ADC sélectionne un groupe de contenus si le nom de domaine complet et l'URL de la demande du client correspondent à ceux configurés. La demande du client doit correspondre au nom de domaine configuré et correspondre exactement au préfixe et au suffixe de l'URL s'ils sont configurés.

- **Je souhaite créer des stratégies de changement de contenu qui évaluent le nom de domaine, ainsi qu'un préfixe et un suffixe partiels d'URL, et dirigent les demandes des clients en conséquence. Quel type de stratégie de changement de contenu dois-je créer ?**

  Vous pouvez créer une stratégie de domaine et d'URL générique pour le serveur virtuel de commutation de contenu. Lorsque ce type de stratégie est évalué, l'appliance Citrix ADC sélectionne un groupe de contenus si la demande correspond au nom de domaine complet et correspond partiellement au préfixe d'URL.

- **Qu'est-ce qu'une stratégie d'URL générique ?**

  Vous pouvez utiliser des caractères génériques pour évaluer des URL partielles dans les demandes des clients vers l'URL que vous avez configurée sur l'appliance Citrix ADC. Vous pouvez utiliser des caractères génériques dans les types de stratégies basées sur les URL suivants :

  - Préfixe uniquement. Par exemple, l'expression /sports/* correspond à toutes les URL disponibles sous l'URL /sports. De même, l'expression /sports* correspond à toutes les URL dont le préfixe est /sports.
  - Suffixe seulement. Par exemple, l'expression /*.jsp correspond à toutes les URL dont l'extension de nom de fichier est jsp.
  - Préfixe et suffixe. Par exemple, l'expression /sports/ *.jsp correspond à toutes les URL de l'URL /sports/ qui possèdent également l'extension de nom de fichier jsp. De même, l'expression /sports *.jsp correspond à toutes les URL avec un préfixe /sports * et une extension de nom de fichier de jsp.

- **Qu' est-ce qu'une politique de domaine et de règle ?**

  Lorsque vous créez une stratégie de domaine et de règle, la demande du client doit correspondre au domaine complet et à la règle configurée sur l'appliance Citrix ADC.

- **Quelle est la priorité par défaut définie pour l'évaluation des stratégies ?**

  Par défaut, les stratégies basées sur des règles sont évaluées en premier.

- **Si une partie du contenu est identique pour toutes les demandes du client, quel type de priorité dois-je utiliser pour évaluer les stratégies ?**

  Si une partie du contenu est identique pour tous les utilisateurs et qu'un contenu différent doit être diffusé sur la base d'attributs client, vous pouvez utiliser la priorité basée sur l'URL pour l'évaluation des stratégies.

- **Quelles syntaxes d'expression de stratégie sont prises en charge dans le changement de contenu ?**

  La commutation de contenu prend en charge deux types d'expressions de stratégie :

  - **Syntaxe classique :** la syntaxe classique de la commutation de contenu commence par le mot-clé REQ et est plus avancée que la stratégie Avancé. Les stratégies classiques ne peuvent pas être liées à une action. Par conséquent, le serveur virtuel d'équilibrage de charge cible peut être ajouté uniquement après avoir lié le serveur virtuel de commutation de contenu.
  - **Stratégie avancée :** la stratégie avancée commence généralement par le mot clé HTTP et est plus facile à configurer. Une action de serveur virtuel d'équilibrage de charge cible peut être liée à une stratégie avancée, et la stratégie peut être utilisée sur plusieurs serveurs virtuels de commutation de contenu.

- **Puis-je lier une stratégie de commutation de contenu unique à plusieurs serveurs virtuels ?**

  Oui. Vous pouvez lier une stratégie de commutation de contenu unique à plusieurs serveurs virtuels en utilisant des stratégies avec des actions définies. Les stratégies de commutation de contenu qui utilisent une action peuvent être liées à plusieurs serveurs virtuels de commutation de contenu, car le serveur virtuel d'équilibrage de charge cible n'est plus spécifié dans la stratégie de commutation de contenu. La possibilité de lier une seule stratégie à plusieurs serveurs virtuels de commutation de contenu permet de réduire davantage la taille de la configuration de commutation de contenu.

  Pour plus d'informations, consultez les articles du centre de connaissances et les rubriques de documentation Citrix suivants :

  - Voir CTX122918 - Comment lier la même stratégie de commutation de contenu à deux serveurs virtuels de commutation de contenu sur une appliance Citrix ADC.
  - Voir CTX122736 - Comment lier la même stratégie avancée à plusieurs serveurs virtuels de commutation de contenu à l'aide d'étiquettes de stratégie.
  - Configuration de la commutation de contenu de base.

- **Puis-je créer une stratégie basée sur l'action en utilisant des expressions classiques ?**

  Non. À partir de maintenant, Citrix ADC ne prend pas en charge les stratégies utilisant des expressions de syntaxe classiques avec des actions. Le serveur virtuel d'équilibrage de charge cible doit être ajouté lors de la liaison de la stratégie au lieu de la définir dans une action.

Débogage

January 21, 2021

- **Comment puis-je déterminer l'interface (CLI, GUI ou API) à travers laquelle une opération a été effectuée ?**

  Citrix ADC conserve le suivi des interfaces à travers lesquelles les opérations sont effectuées. Vous pouvez afficher ces informations dans syslogs (dans l'interface graphique, accédez à Configuration > Système > Audit > Messages d'audit > Messages Syslog) ou dans le fichier ns.log (situé dans le répertoire /var/log/).

  Par exemple, les opérations effectuées via l'API sont marquées comme "API CMD_EXECUTED."

Matériel

August 20, 2021

Cliquez ici pour consulter la FAQ sur le matériel MPX.

Haute disponibilité

August 20, 2021

- **Quels sont les différents ports utilisés pour échanger les informations relatives à la HA entre les nœuds d'une configuration HA ?**

  Dans une configuration HA, les deux nœuds utilisent les ports suivants pour échanger des informations relatives à HA :

  - UDP Port 3003, pour échanger des paquets de pulsations
  - Port 3010, pour la synchronisation et la propagation des commandes

- **Quelles configurations ne sont pas synchronisées ou propagées dans une configuration HA en mode INC ou non-INC ?**

  Les configurations implémentées avec les commandes suivantes ne sont ni propagées ni synchronisées avec le nœud secondaire :

  - Toutes les commandes de configuration HA spécifiques au nœud. Par exemple `add ha node`, `set ha node`, et `bind ha node`.
  - Toutes les commandes de configuration liées à l'interface. Par exemple, set interface et unset interface.
  - Toutes les commandes de configuration associées au canal. Par exemple, add channel, set channel et bind channel.

Pour plus d'informations sur la configuration HA en mode INC, consultez Configuration des nœuds haute disponibilité dans différents sous-réseaux.

- **Quelles configurations ne sont pas synchronisées ou propagées dans une configuration HA en mode INC ?**

  Les configurations suivantes ne sont ni synchronisées ni propagées. Chaque nœud a son propre.

  - MIP
  - SNIP
  - VLAN
  - Itinéraires (sauf les routes LLB)
  - Moniteurs de routage
  - Règles RNAT (sauf toute règle RNAT avec VIP comme IP NAT)
  - Configurations de routage dynamique.

- **Quelles sont les conditions qui déclenchent la synchronisation ?**

  La synchronisation est déclenchée par l'une des conditions suivantes :

  - Le numéro d'incarnation du nœud principal, reçu par le nœud secondaire, ne correspond pas à celui du nœud secondaire.
    Remarque : Les deux nœuds d'une configuration HA conservent un compteur appelé *numéro d'incarnation*, qui compte le nombre de configurations dans le fichier de configuration du nœud. Chaque nœud envoie son numéro d'incarnation à l'autre nœud dans les messages de pulsation. Le numéro d'incarnation n'est pas incrémenté pour les commandes suivantes :
    * Toutes les commandes associées à la configuration HA. Par exemple `add ha node`, `set ha node`, et `bind ha node`.
    * Toutes les commandes liées à l'interface. Par exemple, set interface et unset interface.
    * Toutes les commandes liées au canal. Par exemple, add channel, set channel et bind channel.
  - Le nœud secondaire apparaît après un redémarrage.
  - Le nœud principal devient secondaire après un basculement.

- **Une configuration ajoutée au nœud secondaire est-elle synchronisée sur le principal ?**

  Non, une configuration ajoutée au nœud secondaire n'est pas synchronisée avec le nœud principal.

- **Quelle pourrait être la raison pour laquelle les deux nœuds prétendent être les principaux dans une configuration HA ?**

  La raison la plus probable est que les nœuds primaire et secondaire sont tous les deux sains, mais que le secondaire ne reçoit pas les paquets de pulsations du primaire. Le problème peut être lié au réseau entre les nœuds.

- **Une configuration HA se heurte-t-elle à des problèmes si vous déployez les deux nœuds avec des paramètres d'horloge système différents ?**

  Différents paramètres d'horloge système sur les deux nœuds peuvent causer les problèmes suivants :

  - Les horodatages dans les entrées du fichier journal ne correspondent pas. Cette situation rend difficile l'analyse des entrées de journal pour tout problème.
  - Après un basculement, vous pouvez rencontrer des problèmes avec tout type de persistance basée sur les cookies pour l'équilibrage de charge. Une différence significative entre les temps peut faire expirer un cookie plus tôt que prévu, entraînant la fin de la session de persistance.
  - Des considérations similaires s'appliquent à toutes les décisions liées au temps sur les nœuds.

- **Quelles sont les conditions d'échec de la commande *force HA sync* ?**

  La synchronisation forcée échoue dans l'une des circonstances suivantes :

  - Vous forcez la synchronisation lorsque la synchronisation est déjà en cours.
  - Le nœud secondaire est désactivé.
  - La synchronisation HA est désactivée sur le nœud secondaire actuel.
  - La propagation HA est désactivée sur le nœud principal actuel et vous forcez la synchronisation à partir du nœud principal.

- **Quelles sont les conditions d'échec de la commande *synchroniser les fichiers HA* ?**

  La synchronisation des fichiers de configuration échoue si le nœud secondaire est désactivé.

- **Dans une configuration HA, si le nœud secondaire prend le relais en tant que principal, revient-il à l'état secondaire si le principal d'origine revient en ligne ?**

  Non. Une fois que le nœud secondaire prend le relais comme principal, il reste comme principal même si le nœud principal d'origine revient en ligne. Pour échanger le statut principal et secondaire des nœuds, exécutez la commande *force failover*.

- **Quelles sont les conditions d'échec de la commande *force basculement* ?**

  Un basculement forcé échoue dans l'une des circonstances suivantes :

  - Le nœud secondaire est désactivé.
  - Le nœud secondaire est configuré pour rester secondaire.
  - Le nœud principal est configuré pour rester principal.
  - L'état du nœud homologue est inconnu.

Mise en cache intégrée

August 20, 2021

Groupes de contenu

- **En quoi un groupe de contenu DEFAULT est-il différent des autres groupes de contenu ?**

  Le comportement du groupe de contenu DEFAULT est le même que n'importe quel autre groupe. Le seul attribut qui rend le groupe de contenu DEFAULT spécial est que si un objet est mis en cache et qu'aucun groupe de contenu n'a été créé. L'objet est mis en cache dans le groupe DEFAULT.

- **Quelle est l'option « Cache-control » du niveau du groupe de contenu ?**

  Vous pouvez envoyer n'importe quel en-tête de contrôle de cache au navigateur. Il existe une option de niveau groupe de contenu, -cacheControl, qui vous permet de spécifier l'en-tête de contrôle de cache que vous souhaitez insérer dans la réponse au navigateur.

- **Qu' est-ce que l'option « Minhit » au niveau du groupe de contenu ?**

  `Minhit` est une valeur entière spécifiant le nombre minimum de sélection dans une stratégie de cache avant la mise en cache de l'objet. Cette valeur est configurable au niveau du groupe de contenus. Voici la syntaxe pour configurer cette valeur à partir de l'interface de ligne de commande.

  ```
  add/set cache contentGroup \<Content_Group_Name> [-minHits \<Integer>]
  ```

- **Quelle est l'utilisation de l'option ExpireAtlastByte ?**

  L'option ExpireAtLastByte permet au cache intégré d'expirer l'objet lorsqu'il est téléchargé. Seules les demandes en attente sont alors servies à partir du cache. Toutes les nouvelles demandes sont envoyées au serveur. Ce paramètre est utile lorsque l'objet est fréquemment modifié, comme dans le cas des cotations boursières. Ce mécanisme d'expiration fonctionne avec la fonction Flash Cache. Pour configurer une option ExpireatLastByte, exécutez la commande suivante à partir de l'interface de ligne de commande :

  ```
  add cache contentGroup \<Group_Name> -expireAtLastByte YES
  ```

Stratégie de cache

- **Qu' est-ce qu'une stratégie de mise en cache ?**

  Les stratégies déterminent les transactions pouvant être mises en cache et celles qui ne le sont pas. En outre, les stratégies ajoutent ou remplacent le comportement de mise en cache HTTP

standard. Les stratégies déterminent une action, telle que CACHE ou NOCACHE, en fonction des caractéristiques spécifiques de la demande ou de la réponse. Si une réponse correspond aux règles de stratégie, l'objet de la réponse est ajouté au groupe de contenu configuré dans la stratégie. Si vous n'avez pas configuré de groupe de contenu, l'objet est ajouté au groupe de contenu DEFAULT.

- **Qu' est-ce qu'un accès à la stratégie ?**

  Une sélection se produit lorsqu'une demande ou une réponse correspond à une stratégie de cache.

- **Qu' est-ce qu'une erreur ?**

  Une erreur se produit lorsqu'une requête ou une réponse ne correspond à aucune stratégie de cache. Une erreur peut également se produire si la requête ou la réponse correspond à une stratégie de cache, mais un remplacement du comportement RFC empêche l'objet d'être stocké dans le cache.

- **J' ai configuré la fonctionnalité de mise en cache intégrée de l'appliance Citrix ADC. Lors de l'ajout de la stratégie suivante, un message d'erreur s'affiche. Y a-t-il une erreur dans la commande ?**

  ```
  add cache policy image_caching -rule exp1 | ns_ext_not_jpeg -action
  cache
  ```

  ```
  \> ERROR: No such command
  ```

  Dans la commande précédente, l'expression doit être comprise entre guillemets. Sans guillemets, l'opérateur est considéré comme l'opérateur de tuyauterie.

Mémoire requise

- **Quelles sont les commandes que je peux exécuter sur l'appliance Citrix ADC pour vérifier la mémoire allouée au cache ?**

  Pour afficher la mémoire allouée au cache dans l'appliance Citrix ADC, exécutez l'une des commandes suivantes à partir de l'interface de ligne de commande :

  - `show cache parameter`

    Dans la sortie, vérifiez la valeur du paramètre limite d'utilisation de la mémoire. This is the maximum memory allocated for cache.

  - `show cache \<Content_Group_Name>`

    Dans la sortie, vérifiez les valeurs des paramètres d'utilisation de la mémoire et de limite d'utilisation de la mémoire indiquant la mémoire utilisée et allouée pour le groupe de contenu individuel.

- **Mon appliance Citrix ADC dispose de 2 Go de mémoire. Existe-t-il une limite de mémoire recommandée pour le cache ?**

  Pour n'importe quel modèle de l'appliance Citrix ADC, vous pouvez allouer la moitié de la mémoire au cache. Cependant, Citrix recommande d'allouer un peu moins de la moitié de la mémoire, en raison de la dépendance de la mémoire interne. Vous pouvez exécuter la commande suivante pour allouer 1 Go de mémoire au cache :

  ```
  set cache parameter -memLimit 1024
  ```

- **Est-il possible d'allouer de la mémoire pour des groupes de contenu individuels ?**

  Oui. Même si vous allouez de la mémoire pour le cache intégré globalement en exécutant le paramètre set cache —memlimit <Integer>, vous pouvez allouer de la mémoire à des groupes de contenu individuels en exécutant la <Content_Group_Name> <Integer> commande set cache —memLimit. La mémoire maximale que vous pouvez allouer aux groupes de contenu (combinée) ne peut pas dépasser la mémoire allouée au cache intégré.

- **Quelle est la dépendance de la mémoire entre le cache intégré et le tampon TCP ?**

  Si l'appliance Citrix ADC dispose de 2 Go de mémoire, l'appliance réserve environ 800 Mo à 900 Mo de mémoire et le reste est alloué au système d'exploitation FreeBSD. Par conséquent, vous pouvez allouer jusqu'à 512 Mo de mémoire au cache intégré et le reste est alloué au tampon TCP.

- **Cela affecte-t-il le processus de mise en cache si je n'alloue pas de mémoire globale au cache intégré ?**

  Si vous n'allouez pas de mémoire au cache intégré, toutes les requêtes sont envoyées au serveur. Pour vous assurer que vous avez alloué de la mémoire au cache intégré, exécutez la commande show cache parameter. En fait, aucun objet n'est mis en cache si la mémoire globale est 0, elle doit donc être définie en premier.

Commandes de vérification

- **Quelles sont les options pour afficher les statistiques de cache ?**

  Vous pouvez utiliser l'une des options suivantes pour afficher les statistiques du cache :

  - `stat cache`

    Pour afficher le résumé des statistiques du cache.

  - `stat cache -detail`

    Pour afficher tous les détails des statistiques du cache.

- **Quelles sont les options pour afficher le contenu mis en cache ?**

Pour afficher le contenu mis en cache, vous pouvez exécuter la commande `show cache object`.

- **Quelle est la commande que je peux exécuter pour afficher les caractéristiques d'un objet stocké dans le cache ?**

  Si l'objet stocké dans le cache est, par exemple, GET //10.102.12.16:80/index.html, vous pouvez afficher les détails de l'objet en exécutant la commande suivante à partir de l'interface de ligne de commande de l'appliance :

  ```
  show cache object -url '/index.html'-host 10.102.3.96 -port 80
  ```

- **Est-il obligatoire de spécifier le nom du groupe en tant que paramètre pour afficher les objets paramétrés dans le cache ?**

  Oui. Il est obligatoire de spécifier le nom du groupe en tant que paramètre pour afficher les objets paramétrés dans le cache. Par exemple, considérez que vous avez ajouté les stratégies suivantes avec la même règle :

  ```
  1 add cache policy p2 -rule ns_url_path_cgibin -action CACHE -
      storeInGroup g1
  2 add cache policy p1 -rule ns_url_path_cgibin -action CACHE -
      storeInGroup g2
  3 <!--NeedCopy-->
  ```

  Dans ce cas, pour les demandes multiples, si la stratégie p1 est évaluée, son compteur de sélection est incrémenté et la stratégie stocke l'objet dans le groupe g1, qui comporte des paramètres de sélection. Par conséquent, vous devez exécuter la commande suivante pour afficher les objets du cache :

  ```
  show cache object -url "/cgi-bin/setCookie.pl"-host 10.102.18.152
  groupName g1
  ```

  De même, pour un autre ensemble de requêtes multiples, si la stratégie p2 est évaluée, son compteur de sélection est incrémenté et la stratégie stocke l'objet dans le groupe g2, qui n'a pas de paramètres de sélection. Par conséquent, vous devez exécuter la commande suivante pour afficher les objets du cache :

  ```
  show cache object -url "/cgi-bin/setCookie2.pl"-host 10.102.18.152
  ```

- **Je remarque qu'il y a des entrées vides dans la sortie de la commande nscachemgr. Quelles sont ces entrées ?**

  Tenez compte de l'exemple de sortie suivant de la `nscachemgr` commande. Les entrées vides de cette sortie sont surlignées en gras pour votre référence :

  ```
  1 root@ns# /netscaler/nscachemgr -a
  2 //10.102.3.89:80/image8.png
  ```



```
3   //10.102.3.97:80/staticdynamic.html
4   //10.102.3.97:80/
5   //10.102.3.89:80/image1.png
6   //10.102.3.89:80/file5.html
7   //10.102.3.96:80/
8   //10.102.3.97:80/bg_logo_segue.png
9   //10.102.3.89:80/file500.html
10  //10.102.3.92:80/
11  //10.102.3.96:80/cgi-bin/rfc/ccProxyReval.pl
12  Total URLs in IC = 10
13  <!--NeedCopy-->
```

Les entrées vides dans la sortie sont dues aux propriétés de mise en cache par défaut pour GET/HTTP/1.1.

Vidage des objets

- **Comment puis-je vider un objet sélectif du cache ?**

  Vous pouvez identifier un objet de manière unique par son URL complète. Pour vider un tel objet, vous pouvez effectuer l'une des tâches suivantes :

  - Vider le cache
  - Vider le groupe de contenus
  - Rincer l'objet spécifique

  Pour vider l'objet spécifique, vous devez spécifier les paramètres de requête. Vous spécifiez le paramètre InvalParam pour vider l'objet. Ce paramètre s'applique uniquement à une requête.

- **Est-ce qu'un changement dans la configuration du cache déclenche le vidage du cache ?**

  Oui. Lorsque vous passez à la configuration du cache, toutes les commandes SET cache videront intrinsèquement les groupes de contenu appropriés.

- **J'ai mis à jour les objets sur le serveur. Dois-je vider les objets mis en cache ?**

  Oui. Lorsque vous mettez à jour des objets sur le serveur, vous devez vider les objets mis en cache, ou au moins les objets et groupes de contenu pertinents. Le cache intégré n'est pas affecté par une mise à jour du serveur. Il continue à servir les objets mis en cache jusqu'à ce qu'ils expirent.

Cache Flash

- **Qu' est-ce que la fonctionnalité Flash Cache de l'appliance Citrix ADC ?**

Le phénomène des foules Flash se produit lorsque de nombreux clients accèdent au même contenu. Le résultat est une poussée soudaine du trafic vers le serveur. La fonctionnalité Flash Cache permet à l'appliance Citrix ADC d'améliorer les performances dans une telle situation en envoyant une seule requête au serveur. Toutes les autres demandes sont mises en file d'attente sur l'appliance et la réponse unique est servie aux demandes. Vous pouvez utiliser l'une des commandes suivantes pour activer la fonction Cache rapide :

- `add cache contentGroup \<Group_Name> -flashCache YES`
- `set cache contentGroup \<Group_Name> -flashCache YES`

- **Quelle est la limite pour les clients Flash Cache ?**

  Le nombre de clients Flash Cache dépend de la disponibilité des ressources sur l'appliance Citrix ADC.

Le comportement par défaut

- **L'appliance Citrix ADC reçoit-elle des objets de manière proactive à l'expiration ?**

  L'appliance Citrix ADC ne reçoit jamais d'objets de manière proactive à l'expiration. Cela est vrai même pour les objets négatifs. Le premier accès après expiration déclenche une requête au serveur.

- **Le cache intégré ajoute-t-il des clients à la file d'attente pour servir avant même qu'il ne commence à recevoir la réponse ?**

  Oui. Le cache intégré ajoute des clients à la file d'attente pour servir avant même qu'il ne commence à recevoir la réponse.

- **Quelle est la valeur par défaut de l'objet mis en cache Verify utilisant le paramètre de la configuration du cache ?**

  HOSTNAME_AND_IP est la valeur par défaut.

- **Le dispositif Citrix ADC crée-t-il des entrées de journal dans les fichiers journaux ?**

  Oui. L'appliance Citrix ADC crée des entrées de journal dans les fichiers journaux.

- **Les objets compressés sont-ils stockés dans le cache ?**

  Oui. Les objets compressés sont stockés dans le cache.

Interopérabilité avec d'autres fonctionnalités

- **Qu'advient-il des objets actuellement stockés dans le cache et auxquels on accède via le VPN SSL ?**

  Les objets stockés dans le cache et accessibles régulièrement sont servis en cache, sélectionnés lorsqu'ils sont accessibles via le VPN SSL.

- **Qu' advient-il des objets stockés dans le cache lorsqu'ils sont accessibles via SSL VPN et plus tard accessibles via une connexion régulière ?**

  Les objets stockés via l'accès VPN SSL sont servis de sélection lorsqu'ils sont accessibles via la connexion normale.

- **Lors de l'utilisation de la journalisation Web, comment différencier les entrées qui indiquent la réponse servie du cache de celles desservies par le serveur ?**

  Pour les réponses fournies à partir du cache intégré, le champ de journal du serveur contient la valeur IC. Pour les réponses envoyées à partir d'un serveur, le champ de journal du serveur contient la valeur envoyée par le serveur. Voici un exemple d'entrée de journal pour une transaction de mise en cache intégrée :

  ```
  "10.102.1.52 - "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 4.0; .NET
   CLR 1.0.3705)""GET /"200 0 "IC"10.102.1.45"
  ```

  Avec une demande client, la réponse consignée est celle envoyée au client et pas nécessairement celle envoyée par le serveur.

> **Remarque**
>
> Lors de l'utilisation de la journalisation Web, les réponses du cache intégré contiennent la valeur IC dans le champ journal du serveur. Le champ journal du serveur est présent dans le client NSWL avec le spécificateur de format « %o1 ».

Divers

- **Que voulez-vous dire par la configuration de relexpiry et absexpiry ?**

  En configurant `relexpiry` et `absexpiry`, cela signifie que vous remplacez l'en-tête indépendamment de ce qui apparaît dans l'en-tête. Vous pouvez configurer un paramètre d'expiration différent et le niveau du groupe de contenu. Avec `relexpiry`, l'expiration de l'en-tête est basée sur l'heure à laquelle l'objet est reçu par Citrix ADC. Avec `absexpiry`, l'expiration est basée sur l'heure configurée sur Citrix ADC. `Relexpiry` est configuré en secondes. `Absexpiry` est un moment de la journée.

- **Que voulez-vous dire par la configuration de weakpos et heuristic ?**

  Les `weakpos` et heuristiques sont comme des valeurs de secours. S'il y a un en-tête d'expiration, il n'est considéré que si le dernier en-tête modifié est présent. L'appliance Citrix ADC définit l'expiration en fonction du dernier en-tête modifié et du paramètre heuristique. Le calcul heuristique de l'expiration détermine la durée d'expiration en vérifiant l'en-tête de la dernière modification. Un certain pourcentage de la durée depuis la dernière modification de l'objet est utilisé comme délai d'expiration. heuristique d'un objet qui reste non modifié pendant des

périodes plus longues et qui est susceptible d'avoir des périodes d'expiration plus longues. –heurExpiryParam spécifie la valeur de pourcentage à utiliser dans ce calcul. Sinon, l'appliance utilise la valeur `weakpos`.

- **Que dois-je considérer avant de configurer la mise en cache dynamique ?**

  Si un paramètre est sous la forme nom-valeur et ne dispose pas de la requête URL complète, ou si l'appliance reçoit le paramètre dans un en-tête de cookie ou un corps POST, envisagez de configurer la mise en cache dynamique. Pour configurer la mise en cache dynamique, vous devez configurer le paramètre HitParams.

- **Comment le codage hexadécimal est-il pris en charge dans les noms de paramètres ?**

  Sur l'appliance Citrix ADC, le codage %HEXHEX est pris en charge dans les noms des paramètres. Dans les noms que vous spécifiez pour HitParams ou InvalParams, vous pouvez spécifier un nom qui contient%HEXHEX dans les noms. Par exemple, le nom, le nom%65 et n%61m%65 sont équivalents.

- **Quel est le processus de sélection d'un paramètre HitParam ?**

  Considérons l'extrait suivant d'un en-tête HTTP pour une requête POST :

```
POST /data2html.asp?param1=value1&param2=&param3&param4=value4
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, application/x-shockwave-flash, \*/\*
Referer: http://10.102.3.97/forms.html
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 10.102.3.97
Content-Length: 153
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDQGQGGRNY=NNLLKDADEENOAFLCCDGFGDMO
S1=This+text+is+only+text%2C+not+more+and+not+less%2C+%0D%0Ajust+
   text+to+be+itself%2C+namely+%22Text%22+to+be+posted+as+text
   +%28what+else...%29&B1=Submit
<!--NeedCopy-->
```

  Dans la requête précédente, vous pouvez utiliser S1 et B1, mis en surbrillance en gras pour votre référence, comme HitParams en fonction de vos besoins. En outre, si vous utilisez -matchCookies YES dans le groupe de contenu ASPSESSIONIDQGQGGRNY, vous pouvez également utiliser ces paramètres comme HitParams.

- **Qu' advient-il des clients en file d'attente si la réponse n'est pas mise en cache ?**

  Si la réponse n'est pas mise en cache, tous les clients de la file d'attente reçoivent la même réponse que le premier client reçoit.

- **Puis-je activer les fonctionnalités Poll à chaque fois (PET) et Flash Cache sur le même groupe de contenu ?**

  Non. Vous ne pouvez pas activer PET et Flash Cache sur le même groupe de contenu. Le cache intégré n'exécute pas la fonction AutoPet sur les groupes de contenu Flash Cache. La fonction PET garantit que le cache intégré ne sert pas un objet stocké sans consulter le serveur. Vous pouvez configurer explicitement PET pour un groupe de contenus.

- **Quand les entrées de journal sont-elles créées pour les clients en file d'attente ?**

  Les entrées de journal sont créées pour les clients mis en file d'attente peu de temps après que l'appliance a reçu l'en-tête de réponse. Les entrées de journal sont créées uniquement si l'en-tête de réponse ne rend pas l'objet non mis en cache.

- **Quelle est la signification des valeurs DNS, HOSTNAME et HOSTNAME_AND_IP de l'objet en cache Verify à l'aide du paramètre de configuration du cache ?**

  Les significations sont les suivantes :

  - `set cache parameter -verifyUsing HOSTNAME`

    La commande ignore l'adresse IP de destination.

  - `set cache parameter -verifyUsing HOSTNAME_AND_IP`

    La commande correspond à l'adresse IP de destination.

  - `set cache parameter -verifyUsing DNS`

    La commande utilise le serveur DNS.

- **J'ai défini weakNegRelExpiry sur 600, ce qui est 10 minutes. J'ai remarqué que les réponses 404 ne sont pas mises en cache. Quelle est la raison ?**

  Cela dépend complètement de votre configuration. Par défaut, 404 réponses sont mises en cache pendant 10 minutes. Si vous voulez que toutes les réponses 404 soient récupérées depuis le serveur, spécifiez —WeakNegrelExpiration 0. Vous pouvez affiner —weakNegrelExpiration à une valeur souhaitée, telle que supérieure ou inférieure pour obtenir les réponses 404 correctement mises en cache. Si vous avez configuré —absExpiration pour des réponses positives, il se peut que cela ne donne pas les résultats souhaités.

- **Lorsque l'utilisateur accède au site à l'aide du navigateur Mozilla Firefox, le contenu mis à jour est servi. Toutefois, lorsque l'utilisateur accède au site à l'aide du navigateur Microsoft Internet Explorer, le contenu obsolète est servi. Qu'elle peut en être la raison ?**

Le navigateur Microsoft Internet Explorer peut prendre le contenu de son cache local au lieu du cache intégré Citrix ADC. La raison peut être que le navigateur Microsoft Internet Explorer ne respecte pas l'en-tête lié à l'expiration dans la réponse.

Pour résoudre ce problème, vous pouvez désactiver le cache local d'Internet Explorer et effacer le contenu hors connexion. Après avoir effacé le contenu hors connexion, le navigateur doit afficher le contenu mis à jour.

- **Et si les résultats sont nuls ?**

  Vérifiez si l'heure du serveur et l'heure NS sont synchronisés. Et l'ensemble de limites WeakposrelExpiration doit supporter la différence de temps entre NS et serveur comme suit :

  ```
  root@ns180# date
  Tue May 15 18:53:52 IST 2012
  <!--NeedCopy-->
  ```

- **Pourquoi les stratégies obtiennent-elles des hits mais rien n'est mis en cache ?**

  Vérifiez que la mémoire est allouée au cache intégré et que l'allocation est supérieure à zéro.

- **Est-il possible de mettre à zéro les compteurs de cache ?**

  Il n'y a pas de ligne de commande ou d'option d'interface graphique pour définir les compteurs du cache à zéro, et le vidage du cache ne le fait pas non plus. Le redémarrage de la boîte définit automatiquement ces compteurs à zéro.

Installer, mettre à niveau et rétrograder

August 20, 2021

Installation et mise à niveau

Comment télécharger un package de construction de version Citrix ADC spécifique ?

Pour plus d'informations sur le téléchargement d'un package de génération de version Citrix ADC spécifique, consultez Télécharger un package de version Citrix ADC.

Comment mettre à niveau le logiciel système d'une appliance Citrix ADC ?

Pour plus d'informations sur la mise à niveau du logiciel système d'une appliance Citrix ADC, consultez Mettre à niveau une appliance autonome Citrix ADC.

Où puis-je trouver les notes de mise à jour pour une version Citrix ADC ?

Le document des notes de mise à jour pour une version Citrix ADC contient les éléments suivants pour la version de version :

- Améliorations
- Problèmes résolus
- Problèmes connus

Le document des notes de mise à jour pour une version Citrix ADC se trouve aux emplacements suivants :

- Page de téléchargement du micrologiciel Citrix ADC ou de l'appliance virtuelle d'une version spécifique.
- Page Notes de mise à jour de Citrix ADC sur le site Citrix Docs

Où puis-je trouver les mises à jour de sécurité pour les appliances Citrix ADC ?

L'équipe de sécurité Citrix publie régulièrement des bulletins de sécurité sur les vulnérabilités et expositions communes (CVE) pour tous les produits Citrix associés. Ces informations peuvent être trouvées dans le bulletin de sécurité Citrix. Vous pouvez également rechercher un CVE spécifique sur le site de support Citrix.

À quoi sert le fichier zebos.conf disponible dans une version de Citrix ADC ?

Une appliance Citrix ADC utilise ZEBOs comme suite de routage. Le fichier zebos.conf disponible dans une version Citrix ADC est le fichier de configuration pour ZEBOs.

Je veux changer le port SSH (22) sur l'appliance Citrix ADC vers un autre port. Est-il possible de modifier le port SSH de l'appliance ?

Oui. Vous pouvez modifier le port SSH de l'appliance Citrix ADC en modifiant le fichier sshd_config dans le répertoire /nsconfig. Si le fichier n'existe pas dans le répertoire /nsconfig, copiez-le à partir du répertoire /etc.

Dans le fichier sshd_config, modifiez l'entrée du port 22 à Port <Number>, où <Number> est le numéro de port cible. Si vous ne souhaitez pas redémarrer l'appliance et rendre les modifications effectives, mettez fin au `sshd` processus à l'aide de la commande kill, puis redémarrez le processus.

Le répertoire flash est manquant dans l'appliance Citrix ADC. Quelle procédure dois-je suivre pour monter le répertoire Flash ?

Pour monter le répertoire flash, procédez comme suit :

1. Démarrez l'appliance Citrix ADC en mode mono-utilisateur.

   Au démarrage de l'appliance, le message suivant s'affiche :

   Sélectionnez [Entrée] pour démarrer immédiatement ou n'importe quelle autre touche de l'invite de commandes. Démarrage [du noyau] en 10 secondes… » Sélectionnez un espace et l'invite suivante doit s'afficher :

   Tapez '?' pour une liste de commandes, 'help' pour une aide plus détaillée.

2. Entrez la commande suivante pour démarrer FreeBSD en mode mono-utilisateur :

   boot –s

   Après le démarrage de l'appliance, le message suivant s'affiche :

   Entrez le nom de chemin complet de shell ou RETURN pour /bin/sh :

3. Appuyez sur Entrée pour afficher l'invite #.

4. Exécutez la commande suivante pour monter le répertoire flash :

```
mount /dev/ad0s1a /flash

Note: If the preceding command displays an error message about
   permissions, run the following command to check the disk for
   consistency:

fsck /dev/ad0s1a

Run the mount command again to mount the flash directory.
```

5. Redémarrez l'appliance.

6. À partir de l'invite de shell, exécutez la commande suivante pour vérifier que le répertoire flash est monté :

```
df -kh
```

Je souhaite me connecter à l'appliance Citrix ADC sans entrer le mot de passe. Est-il possible de configurer SSH sur l'appliance pour permettre cela ?

Oui. Vous pouvez configurer SSH sur l'appliance Citrix ADC pour qu'elle se connecte sans mot de passe. Toutefois, vous devez fournir votre nom d'utilisateur. Pour configurer SSH pour se connecter sans mot de passe, procédez comme suit :

1. Exécutez la commande suivante pour générer les clés publiques et privées :

```
\# ssh-keygen -t rsa
```


2. Exécutez la commande suivante pour copier le fichier id_rsa.pub dans le répertoire .ssh de l'hôte distant sur lequel vous souhaitez vous connecter :

```
\# scp id_dsa.pub \<user>@\<remote_host>/.ssh/id_dsa.pub
```

3. Ouvrez une session sur l'hôte distant.
4. Changez dans le répertoire .ssh.
5. Exécutez les commandes suivantes pour ajouter la clé publique du client aux clés publiques connues :

```
\# cat id_dsa.pub >> authorized_keys2

\# chmod 640 authorized_keys2

\# rm id_dsa.pub
```

Quelle est la procédure de réinitialisation du BIOS de l'appliance Citrix ADC ? Dans quelles circonstances dois-je réinitialiser le BIOS ?

Pour réinitialiser le BIOS de l'appliance Citrix ADC, procédez comme suit :

1. Connectez-vous à l'appliance via le port série.
2. Démarrez l'appliance et appuyez sur Supprimer lorsque le processus de démarrage démarre.

   Appuyez sur Supprimer pendant le processus POST pour afficher les paramètres du BIOS de l'appliance.
3. Activez la page Quitter des paramètres du BIOS.
4. Sélectionnez l'option Charger les valeurs par défaut optimales. La boîte de message Charger les paramètres optimaux s'affiche.
5. Sélectionnez OK.
6. Apportez les modifications suivantes aux paramètres du BIOS dans les différents onglets :

   Tab
7. Activez la page Quitter des paramètres du BIOS.
8. Sélectionnez Enregistrer les modifications et Quitter.
9. Sélectionnez OK pour confirmer.
10. Vérifiez que l'appliance démarre correctement et que la console série affiche la sortie après le démarrage de l'appliance.

Vous devez réinitialiser le BIOS lorsque la console série ne répond pas. Cela se produit généralement après la mise à niveau de l'appliance et la console série désactivée. Toutefois, vous pouvez toujours accéder à l'appliance à l'aide de l'utilitaire telnet ou SSH.

Je dois rétablir les paramètre d'usine sur l'appliance Citrix ADC. Quelle procédure dois-je suivre ?

Pour réinitialiser l'appliance Citrix ADC aux valeurs par défaut, vous devez réinitialiser deux environnements : l'environnement d'application Citrix ADC et l'environnement FreeBSD de base.
Pour réinitialiser l'environnement d'application Citrix ADC de l'appliance aux valeurs par défaut, procédez comme suit :

1. Effectuez une sauvegarde du fichier /nsconfig/ns.conf.
2. Supprimez le fichier /nsconfig/ns.conf.
3. Redémarrez l'appliance. Pour réinitialiser l'environnement FreeBSD de l'appliance aux valeurs par défaut, procédez comme suit :
   a) Installez une nouvelle image de code Citrix ADC sur l'appliance. Cela remplace plusieurs fichiers de configuration de niveau FreeBSD par des valeurs par défaut.
   b) Supprimez tous les utilisateurs et groupes ajoutés à l'appliance, c'est-à-dire tous sauf les utilisateurs par défaut.
   c) Supprimez le fichier /etc/resolv.conf.
   d) Supprimez les entrées que vous avez ajoutées au fichier /etc/hosts.
   e) Si le fichier /etc/rc.netscaler existe, supprimez-le.
   f) Ouvrez le fichier /etc/nsperm_group_suser et assurez-vous que toutes les entrées IOCTL sont des entrées de commentaires.
   g) Ouvrez le fichier /etc/rc.conf et assurez-vous que l'entrée Syslogd_enable=no n'est pas modifiée en Syslogd_enable=yes.
   h) Ouvrez le fichier /etc/syslog.conf et assurez-vous qu'il n'y a pas d'entrée supplémentaire dans le fichier.
   i) Supprimez le contenu des fichiers /var/nslog, /var/nstrace et /var/crash.
   j) Si le processus syslog est activé sur l'appliance et qu'elle crée des fichiers journaux localement, supprimez le contenu des fichiers journaux répertoriés dans le fichier /etc/syslog.conf. Les fichiers sont créés dans le répertoire /var/log. Par exemple, si le processus syslog écrit des événements système dans le fichier /var/log/events et `sslvpn` accède aux événements dans le fichier /var/log/sslvpnevents, supprimez ces fichiers.

L'appliance affiche un message similaire au message « 21 juin 12 : 20 : 18 ns /flash/ns-10.0-47.15 : [1/2]dc0 : la carte réseau bloque la condition #663 : TX 10000/10000, RX 0, HF 0 » sur la console. Quelle est la signification de ce message ?

Le message se compose des éléments suivants (illustrés ici à titre d'exemples) :

- #663 : Nombre de fois que cette condition s'est produite sur l'appliance.
- TX 10000/10000 : nombre de paquets que l'appliance a tenté de transmettre et nombre de paquets transmis. Si les deux nombres sont identiques, comme dans cet exemple, la carte réseau a transmis tous les paquets que l'appliance a tenté de transmettre.
- RX 0 : Nombre de paquets reçus. Dans cet exemple, aucun paquet n'a été reçu.
- HF0 : Nombre de problèmes matériels signalés par la carte réseau. Dans cet exemple, la carte réseau n'a signalé aucun problème matériel.

Si l'appliance ne reçoit aucun paquet, elle signale une condition de blocage, car sur un réseau, il est peu probable qu'elle ne reçoive aucun paquet. Toutefois, si l'appliance est branchée sur l'interface, vous pouvez ignorer ce message d'erreur.

Après avoir mis à niveau la version Citrix ADC sur l'appliance, l'appliance affiche toujours la version antérieure. Quelle peut être la raison ?

L'appliance affiche le numéro de version du logiciel à partir du fichier /flash/boot/loader.conf. Si l'entrée du noyau de la version actuelle de Citrix ADC est manquante dans ce fichier, l'appliance affiche la dernière version de Citrix ADC pour laquelle l'entrée était disponible.
Pour résoudre ce problème, procédez comme suit :

1. Vérifiez que le fichier noyau existe dans le répertoire /nsconfig.
2. Vérifiez dans le fichier /flash/boot/loader.conf une entrée pour le noyau.

   (Vous pouvez vous attendre à ce que l'entrée du noyau de la release/build que vous avez installée soit absente du fichier.)
3. Ouvrez le fichier loader.conf dans un éditeur de texte, tel que l'éditeur vi, et mettez à jour l'entrée du noyau pour la nouvelle version.
4. Enregistrez, puis fermez le fichier.
5. Répétez les étapes 2 à 4 pour le fichier /flash/boot/loader.conf.local.
6. Mettez à jour l'entrée de sortie/build dans le fichier ns.conf.
7. Redémarrez l'appliance.

Depuis que j'ai mis à niveau la version Citrix ADC sur l'appliance, l'écran LCD situé sur le panneau avant de l'appliance affiche le message hors service ou n'affiche rien. Comment puis-je résoudre ce problème ?

Exécutez la commande suivante à partir de l'invite de shell de l'appliance :

```
1 /netscaler/nslcd -k
```


J'ai mis à jour la version/build de Citrix ADC. Toutefois, après le processus de mise à niveau, l'appliance ne parvient pas à démarrer. Puis-je rétrograder le logiciel de l'appliance vers la version précédente ?

Oui. Vous pouvez démarrer l'appliance avec le fichier noyau kernel.old. Lorsque vous redémarrez l'appliance, appuyez sur la touche F1 lorsque la console appliance affiche le message Appuyez sur F1. Tapez kernel.old et appuyez sur **Entrée**.

Après la mise à niveau de la version Citrix ADC sur l'appliance, j'ai accidentellement supprimé le fichier du noyau du répertoire /flash. Par conséquent, je ne suis pas en mesure de démarrer l'appareil. Existe-t-il une méthode pour démarrer l'appliance dans cette situation ?

Oui. Vous pouvez démarrer l'appliance à l'aide du fichier du noyau `kernel.GENERIC`, comme suit :

1. Lorsque vous redémarrez l'appliance, appuyez sur la touche F1 lorsque la console appliance affiche le message Appuyez sur F1.
2. Tapez le noyau. GENERIC et appuyez sur Entrée.
3. Connectez-vous en tant qu'utilisateur racine.
4. Réinstallez la version Citrix ADC.
5. Redémarrez l'appliance.

Après la mise à niveau du logiciel de l'appliance, je ne suis pas en mesure de me connecter à l'appliance et le message suivant s'affiche. J'ai essayé de résoudre ce problème en utilisant la procédure de récupération de mot de passe, mais je n'ai pas réussi. Qu'ai-je fait de mal ?

```
```
login: nsroot
Password:
connect: No such file or directory
nsnet_connect: No such file or directory
Login incorrect
<!--NeedCopy--> ```
```

Vous ne pouvez pas résoudre ce problème en utilisant la procédure de récupération de mot de passe. Citrix ADC version 12.1 ou ultérieure utilise le nouveau système de licences, basé sur le démon `Imgrd`, qui s'exécute pendant la procédure de démarrage. Pour que ce démon fonctionne correctement, le nom d'hôte de l'appliance Citrix ADC, qui est défini dans le fichier /nsconfig/rc.conf, doit être résolu par un serveur de noms à l'adresse NSIP. Vous pouvez également créer un fichier hosts dans le répertoire /nsconfig et ajouter l'entrée 127.0.0.1 <Host_Name> dans le fichier.

Assurez-vous également que vous avez copié les fichiers de licence dans le répertoire /nsconfig/license/.

 
```

Lors d'une mise à niveau d'une paire haute disponibilité, le message suivant apparaît à plusieurs reprises. Quelle peut être la raison ?

ns sshd[5035] : erreur : nom d'utilisateur ou mot de passe non valide
Ce message d'erreur s'affiche lorsque les appliances impliquées dans le couplage haute disponibilité ont une version Citrix ADC différente ou une version différente de la même version installée. Les appliances peuvent disposer d'une version différente si vous avez mis à niveau ou déclassé une appliance, mais pas l'autre.
Je souhaite modifier le masque de réseau de l'adresse NSIP sur une appliance Citrix ADC. Puis-je le faire sans provoquer d'interruption ?
La modification du masque de réseau de l'IP Citrix ADC peut entraîner une courte interruption. Assurez-vous de modifier le masque de réseau sur l'appliance secondaire, puis de rompre le couplage haute disponibilité. Vérifiez la fonctionnalité de l'appliance. Si tout fonctionne comme prévu, reconstruisez le couplage haute disponibilité.
Pour modifier le masque de réseau sur l'appliance, exécutez la 'config ns' commande à partir de l'invite CLI, puis choisissez la deuxième option dans le menu.
J'ai configuré une paire haute disponibilité d'appliances Citrix ADC. Après la mise à niveau de la version du logiciel d'une version préliminaire vers une version finale, j'ai remarqué que certaines configurations de l'appliance étaient manquantes. Puis-je récupérer les configurations perdues ?
Vous pouvez utiliser la procédure suivante pour restaurer la configuration :
1. Ouvrez une session sur la ligne de commande Citrix ADC de l'appliance principale.
2. Exécutez les commandes suivantes :
save config
shell
\#cp /nsconfig/ns.conf /nsconfig/ns.conf.bkup
The ns.conf.bkup file is a backup for the running configuration.
3. Mettez à niveau le logiciel des deux appliances vers la version finale.
4. Ouvrez une session sur la ligne de commande Citrix ADC de l'appliance principale.
L'appliance principale et la solution secondaire peuvent-elles avoir des versions distinctes ?
Il est recommandé d'utiliser la même version et le même numéro de build sur l'appliance principale et secondaire.
Les deux appliances d'une paire High Availability (HA) peuvent-elles être mises à niveau en même temps ?
Non. Dans une paire HA, mettez d'abord à niveau le nœud secondaire, puis mettez à niveau le nœud principal.
Pour plus de détails, reportez-vous [à la section Mise à niveau d'une paire haute disponibilité](/fr-fr/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-downgrade-HA-pair.html).
Citrix prend-il en charge les mises à niveau du microprogramme dans le cloud Amazon Web Services ?

Oui.

Puis-je mettre à niveau l'instance Citrix ADC indépendamment de la version SDX ?

Il n'est pas nécessaire de mettre à niveau la version SDX lorsque l'appliance Citrix ADC est mise à niveau. Cependant, certaines fonctionnalités peuvent ne pas fonctionner.

Puis-je utiliser le serveur FTP pour mettre à niveau l'appliance Citrix ADC ?

Non. Vous devez d'abord télécharger le micrologiciel à partir du site de téléchargement Citrix, l'enregistrer sur votre ordinateur local, puis mettre à niveau l'appliance.

La procédure de mise à niveau de l'appliance Citrix ADC avec des configurations GSLB diffère-t-elle d'une mise à niveau d'une appliance qui n'est pas impliquée dans GSLB ?

Non. La procédure de mise à niveau est similaire à la procédure de mise à niveau de base. La seule différence est que vous pouvez mettre à niveau les appliances autonomes ou HA sur différents sites de manière progressive.

Déclasser

J'ai reçu une appliance Citrix ADC sur laquelle la dernière version de Citrix ADC est installée. Cependant, je veux rétrograder la version du logiciel. Puis-je le faire ?

Non. Si vous tentez de rétrograder la version logicielle, il se peut que l'appliance ne fonctionne pas comme prévu, car le fichier ns.conf de la version ultérieure n'est peut-être pas compatible avec la version antérieure et que l'appliance peut restaurer les paramètres d'usine.

Lors de la rétrogradation de la version de Citrix ADC, j'ai suivi les instructions. Toutefois, l'appliance affiche le message suivant. Comment la procédure d'annulation est-elle exécutée sur une appliance Citrix ADC ?

root@LBCOL03B# ./installns
installns version (10.0-47.7) kernel (ns-10.0-47.7.gz)
Note:
Installation may pause for up to 3 minutes while data is written to the flash.
Caution:
Do not interrupt the installation process.
Doing so may cause the system to become unusable.
Installation will proceed in 5 seconds, CTRL-C to abort
No Valid Citrix ADC Version Detected
root@LBCOL03B#

La procédure d'annulation est similaire à la procédure de mise à niveau de base. Sélectionnez la version cible vers laquelle vous souhaitez revenir et effectuez la rétrogradation. Avant de revenir à une autre version, Citrix recommande de créer une copie de vos fichiers de configuration actuels. Pour rétrograder à partir d'une version, reportez-vous à la section [Dégradation d'une appliance autonome Citrix ADC](/fr-fr/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/downgrade-standalone-appliance.html).

Équilibrage de charge

August 20, 2021

- **Quelles sont les différentes stratégies d'équilibrage de charge que je peux créer sur l'appliance Citrix ADC ?**

  Vous pouvez créer les types de stratégies d'équilibrage de charge suivants sur l'appliance Citrix ADC :

  - Connexions moindres
  - Round Robin
  - Temps de réponse le plus faible
  - Bande passante minimale
  - Moins de paquets
  - hachage d'URL
  - Hachage de nom de domaine
  - Hachage de l'adresse IP source
  - Hachage de l'adresse IP de destination
  - IP source - Hachage IP de destination
  - Jeton
  - LRTM

- **Puis-je assurer la sécurité de la batterie de serveurs Web en implémentant l'équilibrage de charge à l'aide de l'appliance Citrix ADC ?**

  Oui. Vous pouvez assurer la sécurité de la batterie de serveurs Web en implémentant l'équilibrage de charge à l'aide de l'appliance Citrix ADC. L'appliance Citrix ADC vous permet d'implémenter les options suivantes de la fonctionnalité d'équilibrage de charge :

  - Masquage des adresses IP : vous permet d'installer les serveurs réels sur un espace d'adressage IP privé pour des raisons de sécurité et pour la conservation des adresses IP. Ce processus est transparent pour l'utilisateur final car l'appliance Citrix ADC accepte les demandes au nom du serveur. En mode de masquage d'adresses, l'appliance isole complètement les deux réseaux. Par conséquent, un client peut accéder à un service s'exécutant sur le sous-réseau privé, tel que FTP ou un serveur Telnet, via un autre VIP sur l'appliance pour ce service.
  - Mappage de ports : permet d'héberger les services TCP réels sur des ports non standard pour des raisons de sécurité. Ce processus est transparent pour l'utilisateur final car l'appliance Citrix ADC accepte les demandes au nom du serveur sur l'adresse IP et le numéro de port annoncés standard.

- **Quels sont les différents périphériques que je peux utiliser pour équilibrer la charge avec**

une appliance Citrix ADC ?

Vous pouvez équilibrer la charge des appareils suivants avec une appliance Citrix ADC :

- Batteries de serveurs
- Caches ou Proxies inversées
- Périphériques de pare-feu
- Systèmes de détection des intrusions
- Dispositifs de déchargement SSL
- Dispositifs de compression
- Serveurs d'inspection de contenu

- **Pourquoi devrais-je implémenter la fonction d'équilibrage de charge pour le site Web ?**

  Vous pouvez implémenter la fonctionnalité d'équilibrage de charge pour le site Web afin de tirer les avantages suivants :

  - Réduisez le temps de réponse : lorsque vous implémentez la fonction d'équilibrage de charge pour le site Web, l'un des principaux avantages est l'augmentation que vous pouvez attendre avec impatience dans le temps de chargement. Avec deux serveurs ou plus partageant la charge du trafic Web, chacun des serveurs exécute moins de charge de trafic qu'un seul serveur. Cela signifie qu'il y a plus de ressources disponibles pour répondre aux demandes des clients. Cela se traduit par un site Web plus rapide.
  - Redondance : La mise en œuvre de la fonction d'équilibrage de charge introduit un peu de redondance. Par exemple, si le site est équilibré sur trois serveurs et que l'un d'eux ne répond pas du tout, les deux autres peuvent continuer à fonctionner et les visiteurs du site ne remarquent même pas de temps d'arrêt. Toute solution d'équilibrage de charge cesse immédiatement d'envoyer du trafic vers le serveur principal qui n'est pas disponible.

- **Pourquoi dois-je désactiver l'option MBF (Mac Based Forwarding) pour Link Load Balancing (LLB) ?**

  - Si vous activez l'option MBF, l'appliance Citrix ADC considère que le trafic entrant en provenance du client et le trafic sortant vers le même client passent par le même routeur en amont. Toutefois, la fonctionnalité LLB nécessite que le meilleur chemin soit choisi pour le trafic de retour.
  - L'activation de l'option MBF rompt cette conception de topologie en envoyant le trafic sortant via le routeur qui a transféré le trafic client entrant.

- **Quels sont les différents types de persistance disponibles sur l'appliance Citrix ADC ?**

  L'appliance Citrix ADC prend en charge les types de persistance suivants :

  - IP source
  - Insert de cookie
  - ID de session SSL

- URL passif
- ID de serveur personnalisé
- Règle
- DESTIP

GUI

August 20, 2021

- **Lorsque j'utilise Firefox pour comparer deux configurations Citrix ADC, le navigateur semble geler ?**

  Firefox finira par afficher les différences dans les configurations, mais le processus prend beaucoup de temps s'il y a plus de 1000 différences. Utilisez Chrome pour une réponse plus rapide.

- **J' utilise un navigateur MAC Safari pour mettre à niveau un Citrix ADC. Dans l'assistant de mise à niveau, lorsque je clique sur le bouton Parcourir pour choisir le fichier de construction de l'appliance, la boîte de dialogue n'affiche aucun fichier ou dossier. En outre, lorsque je retourne au dossier racine, la boîte de dialogue affiche le dossier de niveau supérieur, mais je ne peux pas le parcourir. Que dois-je faire ?**

  Dans le navigateur Safari, cliquez sur l'icône Paramètres et accédez à Préférences > Sécurité > Gérer les paramètres du site Web > Java, puis modifiez la valeur du paramètre Lors de la visite d'autres sites Web sur Exécuter en mode non sécurisé.

- **Que dois-je faire avant d'accéder à l'interface graphique ?**

  Avant d'accéder à une nouvelle version du logiciel Citrix ADC :

  - Effacer le cache du navigateur, y compris les cookies.
  - Accéder à l'interface graphique en mode navigation privée du navigateur.
  - Accéder à l'interface graphique dans un autre navigateur.
  - Désactivez l'option « Utiliser l'accélération logicielle » dans la configuration et redémarrez le navigateur.
  - Accédez aux extensions Chrome :, désactivez la case « Activer » et redémarrez le navigateur Chrome.

- **Quel port dois-je ouvrir pour accéder à l'interface graphique en utilisant HTTP ou HTTPS ?**

  La liste suivante répertorie les numéros de port par défaut des services de gestion HTTP et HTTPS (GUI) dans les appliances Citrix ADC MPX, VPX et CPX :

  - Appliances Citrix ADC MPX et VPX : 80 (HTTP) et 443 (HTTPS)
  - Appliances Citrix ADC CPX : 9080 (HTTP) et 9443 (HTTPS)

En outre, vous pouvez configurer des ports pour les services de gestion HTTP et HTTPS autres que les ports 80 et 443. Pour plus d'informations, voir Configurer les ports de gestion HTTP et HTTPS.

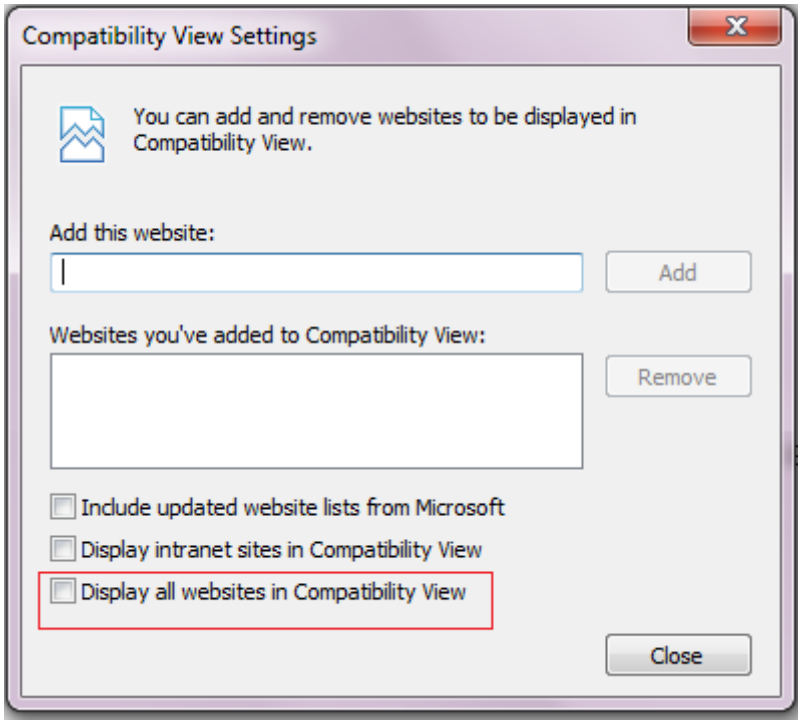
- **Avec quels navigateurs l'interface graphique est-elle compatible avec différents systèmes d'exploitation ?**

  Le tableau suivant répertorie les navigateurs compatibles pour NetScaler GUI version 12.0, 12.1 et 13.0 :

OS	Navigateur	Versions
Windows 7 et versions ultérieures	Internet Explorer	11, Edge, & versions ultérieures
Windows 7 et versions ultérieures	Mozilla Firefox	45 et versions ultérieures
Windows 7 et versions ultérieures	Chrome	60 et versions ultérieures
MAC	Mozilla Firefox	45 et versions ultérieures
MAC	Safari	10.1.1 et versions ultérieures

- **Lorsque j'accède à l'interface graphique à l'aide d'Internet Explorer version 8 ou 9, le navigateur affiche uniquement une barre grise en haut de l'écran. Que dois-je faire ?**

  Le navigateur peut être configuré en mode de compatibilité. Pour désactiver le mode de compatibilité, accédez à **Outils** > **Paramètres d'affichage de compatibilité** et désactivez la case à cocher **Afficher tous les sites Web dans l'affichage de compatibilité** .



- **Même après avoir désactivé le mode de compatibilité dans Internet Explorer version 8 ou 9, l'interface graphique n'apparaît pas. Que dois-je faire ?**

  Assurez-vous que le mode navigateur et le mode document du navigateur sont définis sur la même version. Pour afficher la configuration, appuyez sur F12. Définissez les valeurs sur Internet Explorer 8 ou Internet Explorer 9.

- **Une fois connecté à l'appliance Citrix ADC, la page apparaît vide. Que dois-je faire ?**

  Assurez-vous d'avoir désactivé le mode Protégé dans les paramètres de votre navigateur. Si cette option est activée, le script Java provoque l'affichage vide de l'écran de l'interface utilisateur Citrix ADC.

  Pour désactiver cette option :

  1. Dans les paramètres de votre navigateur Internet Explorer, accédez à **Options Internet**.
  2. Accédez à Paramètres **de l'onglet Sécurité**, cliquez sur Zone **Sites restreints** pour désactiver la case à cocher **Activer le mode protégé**.
  3. Cliquez sur **Appliquer** et **OK**.

- **Lorsque j'accède à l'interface graphique à l'aide d'Internet Explorer version 9, l'utilitaire affiche le message d'erreur suivant : « Vous n'êtes pas connecté. Veuillez vous connecter." Que dois-je faire ?**

  Assurez-vous que les cookies ne sont pas bloqués dans vos paramètres Internet Explorer. Accédez à **Outils** > **Options Internet** . Cliquez sur l'onglet **Confidentialité**, puis sous **Paramètres**, assurez-vous que le curseur est défini sur **Moyenne** ou toute valeur inférieure.

SSL

August 20, 2021

Cliquez ici pour consulter les questions fréquentes sur SSL.

Authentification, autorisation et audit du trafic des applications

October 5, 2021

De nombreuses entreprises limitent l'accès au site Web aux seuls utilisateurs valides et contrôlent le niveau d'accès autorisé à chaque utilisateur. La fonctionnalité d'authentification, d'autorisation et d'audit permet à un administrateur de site de gérer les contrôles d'accès avec l'appliance Citrix ADC au lieu de gérer ces contrôles séparément pour chaque application. L'authentification sur la solution matérielle-logicielle permet également de partager ces informations sur tous les sites Web du même domaine qui sont protégés par la solution matérielle-logicielle.

Pour utiliser l'authentification, l'autorisation et l'audit, vous devez configurer des serveurs virtuels d'authentification pour gérer le processus d'authentification et des serveurs virtuels de gestion du trafic pour gérer le trafic vers les applications Web nécessitant une authentification. Vous configurez également votre DNS pour attribuer des noms de noms de noms de niveau de qualité à chaque serveur virtuel. Après avoir configuré les serveurs virtuels, vous configurez un compte d'utilisateur pour chaque utilisateur qui s'authentifiera via l'appliance Citrix ADC, et vous pouvez éventuellement créer des groupes et attribuer des comptes d'utilisateurs aux groupes. Après avoir créé des comptes d'utilisateurs et des groupes, vous configurez des stratégies qui indiquent à la solution matérielle-logicielle comment authentifier les utilisateurs, quelles ressources autoriser les utilisateurs à accéder et comment consigner les sessions utilisateur. Pour mettre en œuvre les stratégies, vous liez chaque stratégie globalement, à un serveur virtuel spécifique ou aux comptes ou groupes d'utilisateurs appropriés. Après avoir configuré vos stratégies, vous personnalisez les sessions utilisateur en configurant les paramètres de session et en liant vos stratégies de session au serveur virtuel de gestion du trafic. Enfin, si votre intranet utilise des certificats clients, vous configurez la configuration du certificat client.

Pour comprendre le fonctionnement de l'authentification, de l'autorisation et de l'audit dans un environnement distribué, envisagez une organisation dotée d'un intranet auquel ses employés accèdent au bureau, à domicile et en déplacement. Le contenu de l'intranet est confidentiel et nécessite un accès sécurisé. Tout utilisateur souhaitant accéder à l'intranet doit disposer d'un nom d'utilisateur et d'un mot de passe valides. Pour répondre à ces exigences, l'ADC effectue les opérations suivantes :

- Redirige l'utilisateur vers la page de connexion s'il accède à l'intranet sans s'être connecté.

- Collecte les informations d'identification de l'utilisateur, les remet au serveur d'authentification et les met en cache dans un répertoire accessible via le protocole LDAP (Lightweight Directory Access Protocol). Pour plus d'informations, voir Déterminer les attributs dans votre annuaire LDAP.
- Vérifie que l'utilisateur est autorisé à accéder au contenu intranet spécifique avant de remettre la demande de l'utilisateur au serveur d'applications.
- Conserve un délai d'expiration de session après lequel les utilisateurs doivent s'authentifier à nouveau pour pouvoir accéder à nouveau à l'intranet. (Vous pouvez configurer le délai d'expiration.)
- Consigne l'accès de l'utilisateur, y compris les tentatives de connexion non valides, dans un journal d'audit.

types d'authentification pris en charge

- Stockage local
- LDAP
- RADIUS
- SAML
- TACACS+
- Authentification du certificat client (incluant l'authentification par carte à puce
- Web
- Une authentification avancée
- Authentification par formulaire
- Authentification basée sur 401
- OTP natif
- Notification Push
- Courriel OTP
- reCAPTCHA

Citrix Gateway prend également en charge RSA SecurID, Gemalto Protiva et SafeWord. Vous utilisez un serveur RADIUS pour configurer ces types d'authentification.

Avant de configurer l'authentification, l'autorisation et l'audit, vous devez connaître et comprendre comment configurer l'équilibrage de charge, la commutation de contenu et le protocole SSL sur l'appliance Citrix ADC.

Authentification sans autorisation

L'autorisation spécifie les ressources réseau auxquelles les utilisateurs ont accès lorsqu'ils ouvrent une session sur la solution matérielle-logicielle. Le paramètre par défaut de l'autorisation consiste à

refuser l'accès à toutes les ressources réseau. Citrix recommande d'utiliser le paramètre global par défaut, puis de créer des stratégies d'autorisation pour définir les ressources réseau auxquelles les utilisateurs peuvent accéder.

Vous configurez l'autorisation sur la solution matérielle-logicielle à l'aide d'une stratégie d'autorisation et d'expressions. Après avoir créé une stratégie d'autorisation, vous pouvez la lier aux utilisateurs ou aux groupes que vous avez configurés sur la solution matérielle-logicielle.

Vous pouvez configurer la solution matérielle-logicielle pour qu'elle utilise uniquement l'authentification, sans autorisation. Lorsque vous configurez l'authentification sans autorisation, la solution matérielle-logicielle n'effectue pas de vérification d'autorisation de groupe. Les stratégies que vous configurez pour l'utilisateur ou le groupe sont attribuées à l'utilisateur.

Activation de l'authentification, de l'autorisation et de l'audit

Pour utiliser la fonctionnalité d'authentification, d'autorisation et d'audit, vous devez l'activer. Vous pouvez configurer les entités d'authentification, d'autorisation et d'audit, telles que les serveurs virtuels d'authentification et de gestion du trafic, avant d'activer la fonctionnalité d'authentification, d'autorisation et d'audit, mais les entités ne fonctionnent pas tant que la fonctionnalité n'est pas activée.

Pour activer l'authentification, l'autorisation et l'audit à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer l'authentification, l'autorisation et l'audit et vérifier la configuration :

```
enable ns feature AAA
<!--NeedCopy-->
```

Pour activer l'authentification, l'autorisation et l'audit à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**.
2. Dans le volet d'informations, sous **Modes et fonctionnalités**, cliquez sur **Modifier les fonctionnalités de base**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités de base**, activez la case à cocher **Authentification, autorisation et audit** .
4. Cliquez sur **OK**.

Désactivation de l'authentification

Si votre déploiement ne nécessite pas d'authentification, vous pouvez le désactiver. Vous pouvez désactiver l'authentification pour chaque serveur virtuel qui ne nécessite pas d'authentification.

> **Important :**
>
> **Important :** Citrix recommande de désactiver l'authentification avec prudence. Si vous n'utilisez pas de serveur d'authentification externe, créez des utilisateurs et des groupes locaux pour permettre à la solution matérielle-logicielle d'authentifier les utilisateurs. La désactivation de l'authentification arrête l'utilisation des fonctionnalités d'authentification, d'autorisation et de comptabilité qui contrôlent et surveillent les connexions à l'appliance. Lorsque les utilisateurs saisissent une adresse Web pour se connecter à la solution matérielle-logicielle, la page d'ouverture de session n'apparaît pas.

Pour désactiver l'authentification

1. Accédez à **Configuration > Citrix Gateway > Virtual Servers**.
2. Dans le volet d'informations, cliquez sur un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Dans la page **Paramètres de base**, **désactivez la case à cocher Activer l'authentification** .

Fonctionnement de l'authentification, de l'autorisation et de l'audit

October 5, 2021

L'authentification, l'autorisation et l'audit assurent la sécurité d'un environnement Internet distribué en permettant à tout client disposant des informations d'identification appropriées de se connecter en toute sécurité à des serveurs d'applications protégés depuis n'importe où sur Internet. Cette fonctionnalité intègre les trois fonctions de sécurité que sont l'authentification, l'autorisation et l'audit. L'authentification permet à Citrix ADC de vérifier les informations d'identification du client, localement ou avec un serveur d'authentification tiers, et d'autoriser uniquement les utilisateurs approuvés à accéder aux serveurs protégés. L'autorisation permet à l'ADC de vérifier le contenu d'un serveur protégé auquel il autorise chaque utilisateur à accéder. L'audit permet à l'ADC de conserver un enregistrement de l'activité de chaque utilisateur sur un serveur protégé.

Pour comprendre le fonctionnement de l'authentification, de l'autorisation et de l'audit dans un environnement distribué, envisagez une organisation dotée d'un intranet auquel ses employés accèdent au bureau, à domicile et en déplacement. Le contenu de l'intranet est confidentiel et nécessite un accès sécurisé. Tout utilisateur souhaitant accéder à l'intranet doit disposer d'un nom d'utilisateur et d'un mot de passe valides. Pour répondre à ces exigences, l'ADC effectue les opérations suivantes :

- Redirige l'utilisateur vers la page de connexion s'il accède à l'intranet sans s'être connecté.

- Collecte les informations d'identification de l'utilisateur, les transmet au serveur d'authentification et les met en cache dans un répertoire accessible via LDAP. Pour plus d'informations, voir Déterminer les attributs dans votre annuaire LDAP.
- Vérifie que l'utilisateur est autorisé à accéder au contenu intranet spécifique avant de remettre la demande de l'utilisateur au serveur d'applications.
- Conserve un délai d'expiration de session après lequel les utilisateurs doivent s'authentifier à nouveau pour pouvoir accéder à nouveau à l'intranet. (Vous pouvez configurer le délai d'expiration.)
- Consigne l'accès de l'utilisateur, y compris les tentatives de connexion non valides, dans un journal d'audit.

Configuration des stratégies d'authentification, d'autorisation et d'audit

Après avoir configuré vos utilisateurs et groupes, vous configurez ensuite les stratégies d'authentification, les stratégies d'autorisation et les stratégies d'audit pour définir les utilisateurs autorisés à accéder à votre intranet, les ressources auxquelles chaque utilisateur ou groupe est autorisé à accéder, et le niveau d'authentification, d'autorisation et d'audit détaillé. sera conservé dans les journaux d'audit. Une stratégie d'authentification définit le type d'authentification à appliquer lorsqu'un utilisateur tente d'ouvrir une session. Si l'authentification externe est utilisée, la stratégie spécifie également le serveur d'authentification externe. Les stratégies d'autorisation spécifient les ressources réseau auxquelles les utilisateurs et les groupes peuvent accéder après leur ouverture de session. Les stratégies d'audit définissent le type et l'emplacement du journal d'audit.

Vous devez lier chaque stratégie pour la mettre en œuvre. Vous liez les stratégies d'authentification aux serveurs virtuels d'authentification, les stratégies d'autorisation à un ou plusieurs comptes ou groupes d'utilisateurs et les stratégies d'audit globalement et à un ou plusieurs comptes ou groupes d'utilisateurs.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel nombre entier positif. Dans le système d'exploitation Citrix ADC, les priorités de stratégie fonctionnent dans l'ordre inverse : plus le nombre est élevé, plus la priorité est faible. Par exemple, si vous avez trois stratégies avec des priorités de 10, 100 et 1000, la stratégie affectée d'une priorité de 10 est exécutée en premier, puis la stratégie attribuée une priorité de 100 et enfin la stratégie affectée d'un ordre de 1000. La fonctionnalité d'authentification, d'autorisation et d'audit implémente uniquement la première de chaque type de stratégie correspondant à une demande, et non les stratégies supplémentaires de ce type qu'une demande peut également correspondre. La priorité de stratégie est donc importante pour obtenir les résultats souhaités.

Vous pouvez vous laisser suffisamment d'espace pour ajouter d'autres stratégies dans n'importe quel ordre, tout en les définissant pour qu'elles soient évaluées dans l'ordre souhaité, en définissant des

priorités avec des intervalles de 50 ou 100 entre chaque stratégie lorsque vous liez les stratégies. Vous pouvez ensuite ajouter des stratégies supplémentaires à tout moment sans avoir à réaffecter la priorité d'une stratégie existante.

Pour plus d'informations sur les stratégies de liaison sur l'appliance Citrix ADC, consultez la documentation du produit Citrix ADC.

Configurer la stratégie No_Auth pour contourner certains trafic

Vous pouvez désormais configurer la stratégie No_Auth pour contourner certains trafics de l'authentification lorsque l'authentification basée sur 401 est activée sur le serveur virtuel de gestion du trafic. Pour ce type de trafic, vous devez lier une stratégie « No_Auth ».

Pour configurer la stratégie No_Auth afin de contourner certains trafics à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add authentication policy <name> -rule <expression> -action <string>
2 <!--NeedCopy-->
```

Exemple :

```
1 add authentication policy ldap -rule ldapAct1 -action No_Auth
2 <!--NeedCopy-->
```

Composants de base de la configuration d'authentification, d'autorisation et d'audit

August 20, 2021

Les composants de base de la configuration d'authentification, d'autorisation et d'audit sont les suivants :

- **Serveur virtuel d'** authentification - Toutes les demandes d'authentification sont redirigées par le serveur virtuel de gestion du trafic (équilibrage de charge ou changement de contenu) vers le serveur virtuel d'authentification. Ce serveur virtuel traite les stratégies d'authentification associées et donne donc accès à l'application. Pour plus de détails, voir Serveur virtuel d'authentification.
- **Profils d'** authentification - Un profil d'authentification spécifie le serveur virtuel d'authentification, l'hôte d'authentification, le domaine d'authentification et un niveau d'authentification.

Vous pouvez créer un ou plusieurs profils d'authentification pour spécifier différents paramètres d'authentification et lier ces profils d'authentification aux serveurs de gestion du trafic pertinents en fonction de vos besoins. Pour plus de détails, voir Profils d'authentification.

- **Stratégies d'authentification** : lorsque les utilisateurs ouvrent une session sur l'appliance Citrix ADC ou Citrix Gateway, ils sont authentifiés en fonction d'une stratégie que vous créez. Une stratégie d'authentification comprend une expression et une action. Les stratégies d'authentification utilisent des expressions Citrix ADC. Pour plus de détails, voir Stratégies d'authentification.
- **Stratégies d'autorisation** - Lorsque vous configurez une stratégie d'autorisation, vous pouvez la définir pour autoriser ou refuser l'accès aux ressources réseau du réseau interne. Pour plus de détails, voir Stratégies d'autorisation.
- **Utilisateurs et groupes :** - Après avoir configuré la configuration de base de l'authentification, de l'autorisation et de l'audit, vous créez des utilisateurs et des groupes. Vous devez d'abord créer un compte d'utilisateur pour chaque personne qui s'authentifiera via l'appliance Citrix ADC. Si vous utilisez l'authentification locale contrôlée par l'appliance Citrix ADC elle-même, vous créez des comptes d'utilisateur locaux et attribuez des mots de passe à chacun de ces comptes. Pour plus de détails, voir Utilisateurs et groupes.

Authentification serveur virtuel

October 5, 2021

Le serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu) redirige toutes les demandes d'authentification vers le serveur virtuel d'authentification. Ce serveur virtuel traite les stratégies d'authentification associées et donne donc accès à l'application.

Remarque : Vous ne pouvez pas lier les stratégies de gestion du trafic aux serveurs virtuels d'authentification, d'autorisation et d'audit.

Configurer le serveur virtuel d'authentification

Les étapes de configuration d'un serveur virtuel d'authentification sont les suivantes :

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit.

```
enable ns feature AAA
<!--NeedCopy-->
```

2. Configurez un serveur virtuel d'authentification. Il doit être de type SSL et assurez-vous de lier la paire de clés de certificat SSL au serveur virtuel.


```
add authentication vserver <name> SSL <ipaddress> <port>

bind ssl certkey <auth-vserver-name> <certkey>
<!--NeedCopy-->
```

3. Spécifiez le nom de domaine complet du domaine pour le serveur virtuel d'authentification.

```
set authentication vserver <name> -authenticationDomain <FQDN>
<!--NeedCopy-->
```

4. Associez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic concerné.

   Points à noter :

   - Le nom de domaine complet du serveur virtuel de gestion du trafic doit se trouver dans le même domaine que le nom de domaine complet du serveur virtuel d'authentification pour que le cookie de session de domaine fonctionne correctement. Sur le serveur virtuel de gestion du trafic :
     - Activez l'authentification.
     - Spécifiez le nom de domaine complet du serveur virtuel d'authentification en tant qu'hôte d'authentification du serveur virtuel de gestion du trafic.
     - [Facultatif] Spécifiez le domaine d'authentification sur le serveur virtuel de gestion du trafic.
     - Si vous ne configurez pas le domaine d'authentification, l'appliance affecte un nom de domaine complet constitué du nom de domaine complet du serveur virtuel d'authentification sans la partie nom d'hôte. Par exemple, si le nom de domaine du serveur virtuel d'authentification est **tm.xyz.bar.com**, l'appliance affecte **xyz.bar.com** comme domaine d'authentification.
       * Pour l'équilibrage de charge :

```
set lb vserver <name> -authentication ON -
   authenticationhost <FQDN> [-authenticationdomain <
   authdomain>]
<!--NeedCopy-->
```

       * Pour le changement de contenu :

```
set cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

   - Si vous devez définir un cookie à l'échelle du domaine pour un domaine d'authentification, vous devez activer le profil d'authentification sur un serveur virtuel d'équilibrage de charge.

5. Vérifiez que les deux serveurs virtuels sont actifs et configurés correctement.

```
show authentication vserver <name>
<!--NeedCopy-->
```

Pour configurer un serveur virtuel d'authentification à l'aide de l'interface graphique

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit.

   Accédez à **Système > Paramètres**, cliquez sur **Configurer les fonctionnalités de base**et activez **l'authentification, l'autorisation et l'audit**.

2. Configurez le serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**, puis configurez le cas échéant.

3. Configurez le serveur virtuel de gestion du trafic pour l'authentification.

   - **Pour l'équilibrage de charge :**

     Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis configurez le serveur virtuel selon vos besoins.

   - **Pour le changement de contenu :**

     Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis configurez le serveur virtuel selon vos besoins.

4. - Vérifiez la configuration de l'authentification.

     Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**, puis vérifiez les détails du serveur virtuel d'authentification correspondant.

Configurez le serveur virtuel d'authentification

Pour configurer l'authentification, l'autorisation et l'audit, configurez d'abord un serveur virtuel d'authentification pour gérer le trafic d'authentification. Ensuite, liez une paire de clés de certificat SSL au serveur virtuel pour lui permettre de gérer les connexions SSL.
Pour plus d'informations sur la configuration de SSL et la création d'une paire de clés de certificat, voir Certificats SSL.

Configurer un serveur virtuel d'authentification à l'aide de l'interface de ligne de commande

Pour configurer un serveur virtuel d'authentification et vérifier la configuration, à l'invite de commandes, tapez les commandes suivantes dans le même ordre :


```
add authentication vserver <name> ssl <ipaddress>

show authentication vserver <name>

bind ssl certkey <certkeyName>

show authentication vserver <name>

set authentication vserver <name>

show authentication vserver <name>
<!--NeedCopy-->
```

Exemple :

```
add authentication vserver Auth-Vserver-2 SSL 10.102.29.77 443 Done

show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: DOWN[Certkey not bound
    ] Client Idle Timeout: 180 sec Down state flush: DISABLED Disable
    Primary Vserver On Down : DISABLED Authentication : ON Current AAA
    Users: 0 Done

bind ssl certkey Auth-Vserver-2 Auth-Cert-1 Done

show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: UP Client Idle Timeout
    : 180 sec Down state flush: DISABLED Disable Primary Vserver On Down
     : DISABLED Authentication : ON Current AAA Users: 0 Done

set authentication vserver Auth-Vserver-2

show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: DOWN[Certkey not bound
    ] Client Idle Timeout: 180 sec Down state flush: DISABLED Disable
    Primary Vserver On Down : DISABLED Authentication : ON Current AAA
    Users: 0 Done
<!--NeedCopy-->
```

> **Remarque**
>
> Le paramètre Authentication Domain est obsolète. Utilisez le profil d'authentification pour définir des cookies à l'échelle du domaine.

Configuration d'un serveur virtuel d'authentification à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau serveur virtuel d'authentification, cliquez sur **Ajouter**.
   - Pour modifier un serveur virtuel d'authentification existant, sélectionnez le serveur virtuel, puis cliquez sur **Modifier**. La boîte de dialogue Configuration s'ouvre avec la zone Paramètres de base développée.
3. Spécifiez les valeurs des paramètres comme suit (un astérisque indique un paramètre obligatoire) :
   - Nom* : nom (ne peut pas être modifié pour un serveur virtuel créé précédemment)
   - Type d'adresse IP* : type d'adresse IP du serveur virtuel d'authentification
   - Adresse IP* : adresse IP du serveur virtuel d'authentification
   - PORT* : port TCP sur lequel le serveur virtuel accepte les connexions.
   - Failed login timeout : failedLoginTimeout (secondes autorisées avant l'échec de la connexion, et l'utilisateur doit recommencer le processus de connexion.)
   - Tentatives de connexion maximales : maxLoginAttempts (nombre de tentatives de connexion autorisées avant que l'utilisateur ne soit verrouillé)

   > **Remarque :**
   >
   > Le serveur virtuel d'authentification utilise uniquement le protocole SSL et le port 443. Ces options sont donc grisées. Toutes les options qui ne sont pas mentionnées peuvent être ignorées.
4. Cliquez sur **Continuer** pour afficher la zone Certificats.
5. Dans la zone **Certificats**, configurez tous les certificats SSL que vous souhaitez utiliser avec ce serveur virtuel.
   - Pour configurer un certificat d'autorité de certification, cliquez sur la flèche à droite de Certificat d'autorité de certification pour afficher la boîte de dialogue Clé de certificat d'autorité de certification, sélectionnez le certificat que vous souhaitez lier à ce serveur virtuel, puis cliquez sur **Enregistrer**.
   - Pour configurer un certificat de serveur, cliquez sur la flèche à droite de Certificat de serveur et suivez le même processus que pour le certificat d'autorité de certification.
6. Cliquez sur **Continuer** pour afficher la zone **Stratégies d'authentification avancées** .
7. Si vous souhaitez lier une stratégie d'authentification avancée au serveur virtuel, cliquez sur la flèche située à droite de la ligne pour afficher la boîte de dialogue **Stratégie d'authentification**, choisissez la stratégie à lier au serveur, définissez la priorité, puis cliquez sur **OK**.
8. Cliquez sur **Continuer** pour afficher la zone **Stratégies d'authentification de base** .

9. Si vous souhaitez créer une stratégie d'authentification de base et la lier au serveur virtuel, cliquez sur le signe plus pour afficher la boîte de dialogue **Stratégies**, puis suivez les invites pour configurer la stratégie et la lier à ce serveur virtuel.
10. Cliquez sur **Continuer** pour afficher la zone Serveurs virtuels 401.
11. Dans la zone Serveurs virtuels 401, configurez tous les serveurs virtuels d'équilibrage de charge ou de commutation de contenu que vous souhaitez lier à ce serveur virtuel.
    - Pour lier un serveur virtuel d'équilibrage de charge, cliquez sur la flèche située à droite du serveur virtuel d'équilibrage de charge pour afficher la boîte de dialogue Serveurs virtuels d'équilibrage de charge, puis suivez les instructions.
    - Pour lier un serveur virtuel de commutation de contenu, cliquez sur la flèche située à droite du serveur virtuel de commutation de contenu pour afficher la boîte de dialogue Serveurs virtuels de commutation de contenu et suivez le même processus que pour lier un serveur virtuel de base de données.
12. Si vous souhaitez créer ou configurer un groupe, dans la zone Groupes, cliquez sur la flèche pour afficher la boîte de dialogue Groupes, puis suivez les instructions.
13. Vérifiez vos paramètres et, lorsque vous avez terminé, cliquez sur **Terminé**. La boîte de dialogue se ferme. Si vous avez créé un nouveau serveur virtuel d'authentification, il apparaît désormais dans la liste de la fenêtre **Configuration** .

Serveur virtuel de gestion du trafic

Après avoir créé et configuré votre serveur virtuel d'authentification, vous devez ensuite créer ou configurer un serveur virtuel de gestion du trafic et y associer votre serveur virtuel d'authentification. Vous pouvez utiliser un serveur virtuel d'équilibrage de charge ou de commutation de contenu pour un serveur virtuel de gestion du trafic.
Pour plus d'informations sur la création et la configuration de l'un ou l'autre type de serveur virtuel, reportez-vous au *Guide Citrix Traffic Management* dans Traffic Management.

> **Remarque :**
>
> le nom de domaine complet du serveur virtuel de gestion du trafic doit se trouver dans le même domaine que le nom de domaine complet du serveur virtuel d'authentification pour que le cookie de session de domaine fonctionne correctement.

Vous configurez un serveur virtuel de gestion du trafic pour l'authentification, l'autorisation et l'audit en activant l'authentification, puis en attribuant le nom de domaine complet du serveur d'authentification au serveur virtuel de gestion du trafic. Vous pouvez également configurer le domaine d'authentification sur le serveur virtuel de gestion du trafic actuellement. Si vous ne configurez pas cette option, l'appliance Citrix ADC attribue au serveur virtuel de gestion du trafic un nom de domaine complet qui se compose du nom de domaine complet du serveur virtuel d'authentification

sans la partie du nom d'hôte. Par exemple, si le nom de domaine du serveur virtuel d'authentification est tm.xyz.bar.com, l'appliance affecte xyz.bar.com. comme domaine d'authentification.

Pour configurer un serveur virtuel de gestion du trafic à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'un des jeux de commandes suivants :

```
set lb vserver <name>  -authentication ON -authenticationhost <FQDN> [-authenticationdomain <authdomain>]
show lb vserver <name>
set cs vserver <name>  -authentication ON -authenticationhost <FQDN> [-authenticationdomain <authdomain>]
show cs vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vs-cont-sw -Authentication ON -AuthenticationHost mywiki.index.com Done

show lb vserver vs-cont-sw vs-cont-sw (0.0.0.0:0) - TCP Type: ADDRESS State: DOWN Last state change was at Wed Aug 19 10:03:15 2009 (+410 ms) Time since last state change: 5 days, 20:00:40.290 Effective State: DOWN Client Idle Timeout: 9000 sec Down state flush: ENABLED Disable Primary Vserver On Down : DISABLED No. of Bound Services : 0 (Total) 0 (Active) Configured Method: LEASTCONNECTION Mode: IP Persistence: NONE Connection Failover: DISABLED Authentication: ON Host: mywiki.index.com
Done
<!--NeedCopy-->
```

Pour configurer un serveur virtuel de gestion du trafic à l'aide de l'interface graphique

1. Dans le volet de navigation, effectuez l'une des opérations suivantes.
   - Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
   - Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**
   - Dans le volet d'informations, sélectionnez le serveur virtuel sur lequel vous souhaitez activer l'authentification, puis cliquez sur **Modifier**.
   - Dans la zone de texte Domaine, tapez le domaine d'authentification.
   - Dans le menu **Avancé** de droite, sélectionnez **Authentification**.

- Sélectionnez **Authentification basée sur un formulaire ou Authentificationbasée sur 401**, puis renseignez les informations d'authentification.
  - Pour Authentification basée sur un formulaire, entrez le nom de domaine complet de l'authentification (nom de domaine complet du serveur d'authentification), le serveur virtuel d'authentification (l'adresse IP du serveur virtuel d'authentification) et le profil d'authentification (le profil à utiliser pour l'authentification).
  - Pour l'authentification basée sur 401, entrez le serveur virtuel d'authentification et le profil d'authentification uniquement.
- Cliquez sur **OK**. Un message apparaît dans la barre d'état, indiquant que le serveur virtuel a été correctement configuré.

Prise en charge simplifiée du protocole de connexion pour l'authentification, l'autorisation et l'audit

Le protocole de connexion entre les serveurs virtuels d'authentification, d'autorisation et d'audit de gestion du trafic et les serveurs virtuels d'authentification, d'autorisation et d'audit est simplifié pour utiliser des mécanismes internes plutôt que d'envoyer les données chiffrées via des paramètres de requête. Cette fonctionnalité empêche la relecture des demandes.

Configurer le DNS

Pour que le cookie de session de domaine utilisé dans le processus d'authentification fonctionne correctement, vous devez configurer DNS pour affecter à la fois l'authentification et les serveurs virtuels de gestion du trafic aux FQDN dans le même domaine. Pour plus d'informations sur la configuration des enregistrements d'adresses DNS, voir Système de noms de domaine.

Vérifier l'authentification serveur virtuel

Après avoir configuré les serveurs virtuels d'authentification et de gestion du trafic et avant de créer des comptes d'utilisateurs, vous devez vérifier que les deux serveurs virtuels sont correctement configurés et qu'ils sont à l'état UP.

Configurer une authentification NoAuth à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
show authentication vserver <name>
<!--NeedCopy-->
```

Exemple :


```
show authentication vserver Auth-Vserver-2
Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT
State: UP
Client Idle Timeout: 180 sec
Down state flush: DISABLED
Disable Primary Vserver On Down : DISABLED
Authentication : ON
Current AAA Users: 0
Authentication Domain: myCompany.employee.com
Done
<!--NeedCopy-->
```

Configurer une authentification NoAuth à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix ADC AAA - Trafic des applications > Serveurs virtuels**.
   Remarque : Dans Citrix Gateway, accédez à **Citrix Gateway > Serveurs virtuels**.
2. Consultez les informations du volet **Serveurs virtuels AAA** pour vérifier que votre configuration est correcte et que votre serveur virtuel d'authentification accepte le trafic. Vous pouvez sélectionner un serveur virtuel spécifique pour afficher des informations détaillées dans le volet de détails.

Stratégies d'autorisation

August 20, 2021

Lorsque vous configurez une stratégie d'autorisation, vous pouvez la définir pour autoriser ou refuser l'accès aux ressources réseau dans le réseau interne. Par exemple, pour autoriser les utilisateurs à accéder au réseau 10.3.3.0, utilisez l'expression suivante :

CLIENT.IP.DST.IN_SUBNET(10.3.0.0/16)

Les stratégies d'autorisation sont appliquées aux utilisateurs et aux groupes. Une fois qu'un utilisateur est authentifié, Citrix Gateway effectue une vérification d'autorisation de groupe en obtenant les informations de groupe de l'utilisateur à partir d'un serveur RADIUS, LDAP ou TACACS +. Si des informations de groupe sont disponibles pour l'utilisateur, Citrix Gateway vérifie les ressources réseau autorisées pour le groupe.

Pour contrôler les ressources auxquelles les utilisateurs peuvent accéder, vous devez créer des stratégies d'autorisation. Si vous n'avez pas besoin de créer des stratégies d'autorisation, vous pouvez configurer l'autorisation globale par défaut.

Si vous créez une expression dans la stratégie d'autorisation qui refuse l'accès à un chemin d'accès au fichier, vous ne pouvez utiliser que le chemin du sous-répertoire et non le répertoire racine. Par exemple, use fs.path contains "\\dir1\\dir2" au lieu de fs.path contains "\\rootdir\\dir1\\dir2". Si vous utilisez la deuxième version dans cet exemple, la stratégie échoue.

Après avoir configuré la stratégie d'autorisation, vous la liez ensuite à un utilisateur ou à un groupe.

Par défaut, les stratégies d'autorisation sont validées d'abord par rapport aux stratégies que vous liez au serveur virtuel, puis aux stratégies liées globalement. Si vous liez une stratégie globalement et que vous souhaitez que la stratégie globale ait priorité sur une stratégie que vous liez à un utilisateur, un groupe ou un serveur virtuel, vous pouvez modifier le numéro de priorité de la stratégie. Les numéros de priorité commencent à zéro. Un numéro de priorité inférieur donne une priorité plus élevée à la politique.

Par exemple, si la stratégie globale a un numéro de priorité de un et que l'utilisateur a une priorité de deux, la stratégie d'authentification globale est appliquée en premier.

> **Important :**
>
> - Les stratégies d'autorisation classiques sont appliquées uniquement sur le trafic TCP.
> - La stratégie d'autorisation avancée peut être appliquée à tous les types de trafic (TCP/UDP/ICMP/DNS).
>   - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
>   - While binding, if "type" is not explicitly mentioned or "type" is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
>   - The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

Pour plus d'informations sur les stratégies d'autorisation avancées, consultez l'article https://support.citrix.com/article/CTX232237.

Configurer et lier une stratégie d'autorisation

Configurer une stratégie d'autorisation à l'aide de l'interface graphique

1. Accédez à **Citrix Gateway > Stratégies > Autorisation.**
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez un nom pour la stratégie.
4. Dans **Action**, sélectionnez **Autoriser** ou **Refuser**.
5. Dans **Expression**, cliquez sur **Éditeur d'expression**.

6. Pour commencer à configurer l'expression, cliquez sur **Sélectionner** et choisissez les éléments nécessaires.
7. Cliquez sur **Terminé** lorsque votre expression est terminée.
8. Cliquez sur **Créer**.

Lier une stratégie d'autorisation à un utilisateur à l'aide de l'interface graphique

1. Accédez à **Citrix Gateway > Administration des utilisateurs.**
2. Cliquez sur **Utilisateurs AAA**.
3. Dans le volet d'informations, sélectionnez un utilisateur, puis cliquez sur **Modifier**.
4. Dans **Paramètres avancés**, cliquez sur **Stratégies d'autorisation**.
5. Dans la page **Liaison de stratégie**, sélectionnez une stratégie ou créez une stratégie.
6. Dans **Priorité**, définissez le numéro de priorité.
7. Dans **Type**, sélectionnez le type de demande, puis cliquez sur **OK**.

Lier une stratégie d'autorisation à un groupe à l'aide de l'interface graphique

1. Accédez à **Citrix Gateway > Administration des utilisateurs**.
2. Cliquez sur **Groupes AAA**.
3. Dans le volet d'informations, sélectionnez un groupe, puis cliquez sur **Modifier**.
4. Dans **Paramètres avancés**, cliquez sur **Stratégies d'autorisation**.
5. Dans la page **Liaison de stratégie**, sélectionnez une stratégie ou créez une stratégie.
6. Dans **Priorité**, définissez le numéro de priorité.
7. Dans **Type**, sélectionnez le type de demande, puis cliquez sur **OK**.

Autorisation spécifie les ressources réseau auxquelles les utilisateurs ont accès lorsqu'ils se connectent à Citrix Gateway. Le paramètre par défaut pour l'autorisation est de refuser l'accès à toutes les ressources réseau. Citrix recommande d'utiliser le paramètre global par défaut, puis de créer des stratégies d'autorisation pour définir les ressources réseau auxquelles les utilisateurs peuvent accéder.

Vous configurez l'autorisation sur Citrix Gateway à l'aide d'une stratégie et d'expressions d'autorisation. Après avoir créé une stratégie d'autorisation, vous pouvez la lier aux utilisateurs ou aux groupes que vous avez configurés sur l'appliance.

Autorisation globale par défaut

Pour définir les ressources auxquelles les utilisateurs ont accès sur le réseau interne, vous pouvez configurer l'autorisation globale par défaut. Vous configurez l'autorisation globale en autorisant ou en refusant l'accès aux ressources réseau globalement sur le réseau interne.

Toute action d'autorisation globale que vous créez est appliquée à tous les utilisateurs qui n'ont pas encore de stratégie d'autorisation associée à eux, directement ou via un groupe. Une stratégie d'autorisation d'utilisateur ou de groupe remplace toujours l'action d'autorisation globale. Si l'action d'autorisation par défaut est définie sur Refuser, vous devez appliquer des stratégies d'autorisation à tous les utilisateurs ou groupes afin de rendre les ressources réseau accessibles à ces utilisateurs ou groupes. Cette exigence contribue à améliorer la sécurité.

Pour définir l'autorisation globale par défaut :

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Citrix Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres globaux.
3. Sous l'onglet Sécurité, en regard de Action d'autorisation par défaut, sélectionnez Autoriser ou Refuser, puis cliquez sur OK.

Profils d'authentification

August 20, 2021

Lorsque vous souhaitez que les mêmes paramètres d'authentification soient utilisés par plusieurs serveurs virtuels de gestion du trafic, vous pouvez créer un profil d'authentification qui spécifie le serveur virtuel d'authentification, l'hôte d'authentification, le domaine d'authentification et le niveau d'authentification.

Ce profil d'authentification peut être associé aux serveurs virtuels de gestion du trafic concernés.

Configurer un profil d'authentification

Configurer un profil d'authentification à l'aide de l'interface de ligne de commande

- Créez le profil d'authentification et définissez les paramètres requis.

  Par exemple, pour créer un profil avec un serveur virtuel d'authentification nommé « AuthVs ».

```
1  add authentication authnProfile authProfile1 -authnVsName authVS
      -authenticationHost authnVS.example.com -authenticationDomain
      example.com -authenticationLevel
2  <!--NeedCopy-->
```

> **Remarque :**
>
> Le poids ou le niveau d'authentification dépend du serveur virtuel auquel le trafic est lié. Une session créée en s'authentifiant par rapport au serveur virtuel de gestion du trafic à un niveau

> donné ne peut pas être utilisée pour accéder au serveur virtuel de gestion du trafic à un niveau supérieur.

- Liez le profil d'authentification aux serveurs virtuels de gestion du trafic concernés.

  Par exemple, pour lier AuthProfile1 à un serveur virtuel d'équilibrage de charge nommé « vserver1".

```
1 set lb vserver vserver1 -authnProfile authProfile1
2 <!--NeedCopy-->
```

Configurer un profil d'authentification à l'aide de l'interface graphique

Dans l'onglet **Configuration**, accédez à **Sécurité > AAA - Trafic d'application > Profil d'authentification**, puis configurez le profil d'authentification selon vos besoins.

> **Remarque :**
>
> - Vous pouvez créer un profil d'authentification à l'aide de l'assistant Citrix Gateway. Le profil contient tous les paramètres de la stratégie d'authentification. Vous configurez le profil lorsque vous créez la stratégie d'authentification.
> - Avec l'assistant Citrix Gateway, vous pouvez utiliser le type d'authentification choisi pour configurer l'authentification. Si vous souhaitez configurer d'autres stratégies d'authentification après l'exécution de l'Assistant, vous pouvez utiliser l'utilitaire de configuration. Pour plus d'informations sur l'assistant Citrix Gateway, voir Configuration des paramètres à l'aide de l'assistant Citrix Gateway].

Stratégies d'authentification

August 20, 2021

Lorsque les utilisateurs ouvrent une session sur l'appliance Citrix ADC ou Citrix Gateway, ils sont authentifiés selon une stratégie que vous créez. Une stratégie d'authentification comprend une expression et une action. Les stratégies d'authentification utilisent des expressions Citrix ADC.

Après avoir créé une action d'authentification et une stratégie d'authentification, liez-la à un serveur virtuel d'authentification et attribuez-lui une priorité. Lorsque vous la liez, désignez-la également comme une stratégie primaire ou secondaire. Les stratégies primaires sont évaluées avant les stratégies secondaires. Dans les configurations qui utilisent les deux types de stratégie, les stratégies primaires sont généralement des stratégies plus spécifiques, tandis que les stratégies secondaires sont généralement des stratégies plus générales. Il est destiné à gérer l'authentification pour tous les comptes d'utilisateur qui ne répondent pas aux critères les plus spécifiques. La stratégie définit le

type d'authentification. Une stratégie d'authentification unique peut être utilisée pour des besoins d'authentification simples et est généralement liée au niveau global. Vous pouvez également utiliser le type d'authentification par défaut, qui est local. Si vous configurez l'authentification locale, vous devez également configurer les utilisateurs et les groupes sur l'appliance.

Vous pouvez configurer plusieurs stratégies d'authentification et les lier pour créer une procédure d'authentification détaillée et des serveurs virtuels. Par exemple, vous pouvez configurer l'authentification en cascade et à deux facteurs en configurant plusieurs stratégies. Vous pouvez également définir la priorité des stratégies d'authentification pour déterminer les serveurs et l'ordre dans lequel l'appliance vérifie les informations d'identification de l'utilisateur. Une stratégie d'authentification inclut une expression et une action. Par exemple, si vous définissez l'expression sur Valeur True, lorsque les utilisateurs ouvrent une session, l'action évalue l'ouverture de session utilisateur sur true, puis les utilisateurs ont accès aux ressources réseau.

Après avoir créé une stratégie d'authentification, vous liez la stratégie au niveau global ou aux serveurs virtuels. Lorsque vous liez au moins une stratégie d'authentification à un serveur virtuel, toutes les stratégies d'authentification liées au niveau global ne sont pas utilisées lorsque les utilisateurs ouvrent une session sur le serveur virtuel, sauf si le type d'authentification global a une priorité supérieure à la stratégie liée au serveur virtuel.

Lorsqu'un utilisateur ouvre une session sur l'appliance, l'authentification est évaluée dans l'ordre suivant :

- Le serveur virtuel est vérifié pour toutes les stratégies d'authentification liées.
- Si les stratégies d'authentification ne sont pas liées au serveur virtuel, l'appliance vérifie les stratégies d'authentification globales.
- Si une stratégie d'authentification n'est pas liée à un serveur virtuel ou globalement, l'utilisateur est authentifié via le type d'authentification par défaut.

Si vous configurez des stratégies d'authentification LDAP et RADIUS et que vous souhaitez lier les stratégies globalement pour l'authentification à deux facteurs, vous pouvez sélectionner la stratégie dans l'utilitaire de configuration, puis choisir si la stratégie est le type d'authentification principal ou secondaire. Vous pouvez également configurer une stratégie d'extraction de groupe.

> **Remarque :**
>
> Citrix ADC ou Citrix Gateway code uniquement les caractères UTF-8 pour l'authentification, et il n'est pas compatible avec les serveurs qui utilisent des caractères ISO-8859-1.

Créer une stratégie d'authentification

Créer une stratégie d'authentification à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification**, puis sélectionnez le type de stratégie que vous souhaitez créer.

Pour Citrix Gateway, accédez à **Citrix Gateway > Stratégies > Authentification**.

2. Dans le volet d'informations, sous l'onglet **Stratégies**, effectuez l'une des opérations suivantes :
   - Pour créer une stratégie, cliquez sur **Ajouter**.
   - Pour modifier une stratégie existante, sélectionnez l'action, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue Créer une stratégie d'authentification ou Configurer une stratégie d'authentification, tapez ou sélectionnez les valeurs des paramètres.
   - **Nom** — nom de la stratégie (ne peut pas être modifié pour une action précédemment configurée)
   - **Type d'authentification** — `authtype`
   - **Serveur** — `authVsName`
   - **Expression** — règle (vous entrez des expressions en choisissant d'abord le type d'expression dans la liste déroulante la plus à gauche sous la fenêtre Expression, puis en tapant votre expression directement dans la zone de texte de l'expression, ou en cliquant sur Ajouter pour ouvrir la boîte de dialogue Ajouter une expression et en utilisant le menu déroulant pour construire votre expression.)
4. Cliquez sur **Créer** ou **sur OK**. La stratégie que vous avez créée apparaît dans la page Stratégies.
5. Cliquez sur l'onglet **Serveurs** et, dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour utiliser un serveur existant, sélectionnez-le, puis cliquez sur.
   - Pour créer un serveur, cliquez sur Ajouter, puis suivez les instructions.
6. Si vous souhaitez désigner cette stratégie comme stratégie d'authentification secondaire, sous l'onglet Authentification, cliquez sur Secondaire. Si vous souhaitez désigner cette stratégie comme stratégie d'authentification principale, ignorez cette étape.
7. Cliquez sur **Insérer une stratégie**.
8. Choisissez la stratégie que vous souhaitez lier au serveur virtuel d'authentification dans la liste déroulante.
9. Dans la colonne **Priorité** à gauche, modifiez la priorité par défaut pour vous assurer que la stratégie est évaluée dans l'ordre approprié.
10. Cliquez sur **OK**. Un message apparaît dans la barre d'état indiquant que la stratégie a été correctement configurée.

Modifier une stratégie d'authentification à l'aide de l'interface graphique

Vous pouvez modifier les stratégies et les profils d'authentification configurés, tels que l'adresse IP du serveur d'authentification ou l'expression.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **Citrix Gateway > Stratégies > Authentification**.
   Remarque : Vous pouvez également configurer la stratégie dans **Sécurité > AAA - Trafic des applications > Stratégies > Authentification**, puis sélectionner le type de stratégie que vous souhaitez modifier.
2. Dans le volet de navigation, sous Authentification, sélectionnez un type d'authentification.
3. Dans le volet d'informations, sous l'onglet Serveurs, sélectionnez un serveur, puis cliquez sur Ouvrir.

Supprimer une stratégie d'authentification à l'aide de l'interface graphique

Si vous avez modifié ou supprimé un serveur d'authentification de votre réseau, supprimez la stratégie d'authentification correspondante de Citrix Gateway.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **Citrix Gateway > Stratégies \ > Authentification**.
   Remarque : Pour configurer à partir d'ADC, naviguez **Sécurité > AAA - Trafic des applications > Stratégies > Authentification**, puis sélectionnez le type de stratégie à supprimer.
2. Dans le volet de navigation, sous Authentification, sélectionnez un type d'authentification.
3. Dans le volet d'informations, sous l'onglet Stratégies, sélectionnez une stratégie, puis cliquez sur Supprimer.

Créer une stratégie d'authentification à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
add authentication negotiatePolicy <name> <rule> <reqAction>

show authentication localPolicy <name>

bind authentication vserver <name> -policy <policyname> [-priority <
    priority>][-secondary]]

show authentication vserver <name>
<!--NeedCopy-->
```

Exemple :

```
    > add authentication localPolicy Authn-Pol-1 ns_true
      Done
    > show authentication localPolicy
    1)      Name: Authn-Pol-1       Rule: ns_true          Request
       action: LOCAL   Done
```



```
    > bind authentication vserver Auth-Vserver-2 -policy Authn-Pol-1
    Done
    > show authentication vserver Auth-Vserver-2
        Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT State: UP
            Client Idle
        Timeout: 180 sec Down state flush: DISABLED
        Disable Primary Vserver On Down : DISABLED
        Authentication : ON
        Current AAA Users: 0
        Authentication Domain: myCompany.employee.com
    1)  Primary authentication policy name:  Authn-Pol-1 Priority: 0
        Done
<!--NeedCopy-->
```

Modifier une stratégie d'authentification existante à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour modifier une stratégie d'authentification existante :

```
set authentication localPolicy <name> <rule> [-reqaction <action>]<!--
   NeedCopy-->
```

```
Exemple

<!--NeedCopy-->
```

set authentication localPolicy Authn-Pol-1 'ns_true'

```
### Supprimer une stratégie d'authentification à l'aide de l'interface
   de ligne de commande

À l'invite de commandes, tapez la commande suivante pour supprimer une
   stratégie d'authentification :

<!--NeedCopy-->
```

rm authentication localPolicy

```
Exemple

<!--NeedCopy-->
```

rm authentication localPolicy Authn-Pol-1


```
### Lier une stratégie d'authentification

Aprés avoir configuré les stratégies d'authentification, vous liez la stratégie soit globalement, soit à un serveur virtuel. Vous pouvez utiliser l'utilitaire de configuration pour lier une stratégie d'authentification.

Pour lier une stratégie d'authentification globalement à l'aide de l'utilitaire de configuration :

1.  Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **Citrix Gateway > Stratégies \ > Authentification**.
    Remarque : Pour configurer à partir d'ADC, naviguez **Sécurité > AAA - Trafic des applications > Stratégies > Authentification**
1.  Cliquez sur un type d'authentification.
1.  Dans le volet d'informations, sous l'onglet Stratégies, cliquez sur un serveur, puis dans Action, cliquez sur Liaisons globales.
1.  Sous l'onglet Principal ou Secondaire, sous Détails, cliquez sur Insérer une stratégie.
1.  Sous Nom de la stratégie, sélectionnez la stratégie, puis cliquez sur OK.

    **Remarque :** lorsque vous sélectionnez la stratégie, Citrix Gateway définit automatiquement l'expression sur la valeur True.

Pour délier une stratégie d'authentification globale à l'aide de l'utilitaire de configuration :

1.  Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **Citrix Gateway > Stratégies \ > Authentification**.
    Remarque : Pour configurer à partir d'ADC, naviguez **Sécurité > AAA - Trafic des applications > Stratégies > Authentification**
1.  Sous l'onglet Stratégies, dans Action, cliquez sur Liaisons globales.
1.  Dans la boîte de dialogue Lier/Annuler la liaison des stratégies d'authentification à l'ensemble, sous l'onglet Primaire ou Secondaire, dans Nom de la stratégie, sélectionnez la stratégie, cliquez sur Annuler la stratégie, puis cliquez sur OK.

## Ajouter une action d'authentification

### Ajouter une action d'authentification à l'aide de l'interface de ligne de commande

```



```
Si vous n'utilisez pas l'authentification LOCAL, vous devez ajouter une action d'authentification explicite. À l'invite de commandes, tapez la commande suivante :

<!--NeedCopy-->
```

add authentication tacacsAction -serverip [-serverPort][-authTimeout][...]

```
Exemple

<!--NeedCopy-->
```

add authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -serverport 1812 -authtimeout 15 -tacacsSecret “minotaur” -authorization OFF -accounting ON -auditFailedCmds OFF -defaultAuthenticationGroup “users”

```
### Configurer une action d'authentification à l'aide de l'interface de ligne de commande

Pour configurer une action d'authentification existante, à l'invite de commandes, tapez la commande suivante :

<!--NeedCopy-->
```

set authentication tacacsAction -serverip [-serverPort][-authTimeout][...]

```
Exemple

<!--NeedCopy-->
```

set authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -serverport 1812 -authtimeout 15 -tacacsSecret “minotaur” -authorization OFF -accounting ON -auditFailedCmds OFF -defaultAuthenticationGroup “users”

```
### Supprimer une action d'authentification à l'aide de l'interface de ligne de commande

Pour supprimer une action RADIUS existante, à l'invite de commandes, tapez la commande suivante :

<!--NeedCopy-->
```

rm authentication radiusAction

```
Exemple
```



```
2
3 <!--NeedCopy-->
```

rm authentication tacacsaction Authn-Act-1

```
1 ## L'authentification NoAuth
2
3 L'appliance Citrix ADC prend en charge la fonctionnalité d'
    authentification NoAuth qui permet au client de configurer un paramé
    tre DefaultAuthenticationGroup dans la `noAuthAction` commande,
    lorsqu'un utilisateur exécute cette stratégie. L'administrateur peut
     vérifier la présence de ce groupe dans le groupe d'utilisateurs
    pour déterminer la navigation de l'utilisateur via la stratégie
    NoAuth.
4
5 ### Pour configurer une authentification NoAuth à l'aide de l'interface
     de ligne de commande
6
7 À l'invite de commandes, tapez ;
8
9 <!--NeedCopy-->
```

add authentication noAuthAction [-defaultAuthenticationGroup]

```
1 **Exemple :**
2
3 <!--NeedCopy-->
```

add authentication noAuthAction noauthact –defaultAuthenticationGroup mynoauthgroup

```
1 ## Types d'authentification globale par défaut
2
3 Lorsque vous avez installé Citrix Gateway et exécuté l'Assistant Citrix
     Gateway, vous avez configuré l'authentification dans l'Assistant.
    Cette stratégie d'authentification est automatiquement liée au
    niveau global Citrix Gateway. Le type d'authentification que vous
    configurez dans l'assistant Citrix Gateway est le type d'
    authentification par défaut. Vous pouvez modifier le type d'
    autorisation par défaut en exécutant à nouveau l'assistant Citrix
    Gateway ou modifier les paramétres d'authentification globaux dans l
    'utilitaire de configuration.
4
5 Si vous devez ajouter d'autres types d'authentification, vous pouvez
    configurer des stratégies d'authentification sur Citrix Gateway et
    lier les stratégies à Citrix Gateway à l'aide de l'utilitaire de
```



```
    configuration. Lorsque vous configurez l'authentification
    globalement, vous définissez le type d'authentification, configurez
    les paramétres et définissez le nombre maximal d'utilisateurs
    pouvant être authentifiés.
6
7   Aprés avoir configuré et lié la stratégie, vous pouvez définir la
    priorité pour définir quel type d'authentification a priorité. Par
    exemple, vous configurez les stratégies d'authentification LDAP et
    RADIUS. Si la stratégie LDAP a un numéro de priorité de 10 et que la
     stratégie RADIUS a un numéro de priorité de 15, la stratégie LDAP a
     priorité, quel que soit l'endroit où vous liez chaque stratégie. C'
    est ce qu'on appelle l'authentification en cascade.
8
9   Vous pouvez choisir de remettre des pages d'ouverture de session à
    partir du cache en mémoire Citrix Gateway ou du serveur HTTP s'exé
    cutant sur Citrix Gateway. Si vous choisissez de remettre la page d'
    ouverture de session à partir du cache en mémoire, la remise de la
    page d'ouverture de session à partir de Citrix Gateway est plus
    rapide qu'à partir du serveur HTTP. Le choix de remettre la page d'
    ouverture de session à partir du cache en mémoire réduit le temps d'
    attente lorsque de nombreux utilisateurs ouvrent une session en même
     temps. Vous ne pouvez configurer la remise des pages d'ouverture de
     session à partir du cache que dans le cadre d'une stratégie d'
    authentification globale.
10
11  Vous pouvez également configurer l'adresse IP NAT (Network Address
    Translation) qui est une adresse IP spécifique pour l'
    authentification. Cette adresse IP est unique pour l'
    authentification et n'est pas le sous-réseau Citrix Gateway, mappé
    ou adresses IP virtuelles. Ce paramétre est facultatif.
12
13  **Remarque :**
14  >
15  >Vous ne pouvez pas utiliser l'assistant Citrix Gateway pour configurer
     l'authentification SAML.
16
17  Vous pouvez utiliser l'Assistant Configuration rapide pour configurer l
    'authentification par certificat LDAP, RADIUS et client. Lorsque
    vous exécutez l'Assistant, vous pouvez sélectionner un serveur LDAP
    ou RADIUS existant configuré sur Citrix Gateway. Vous pouvez é
    galement configurer les paramétres pour LDAP ou RADIUS. Si vous
    utilisez l'authentification à deux facteurs, Citrix recommande d'
    utiliser LDAP comme type d'authentification principal.
18
19  ### Configuration des types d'authentification globaux par défaut
```



```
20
21 1.  Dans l'utilitaire de configuration, sous l'onglet Configuration,
       dans le volet de navigation, développez Citrix Gateway, puis cliquez
        sur Paramétres globaux.
22 1.  Dans le volet d'informations, sous Paramétres, cliquez sur Modifier
        les paramétres d'authentification.
23 1.  Dans Nombre maximal d'utilisateurs, tapez le nombre d'utilisateurs
       pouvant être authentifiés à l'aide de ce type d'authentification.
24 1.  Dans Adresse IP NAT, tapez l'adresse IP unique pour l'
       authentification.
25 1.  Sélectionnez Activer la mise en cache statique pour livrer les
       pages d'ouverture de session plus rapidement.
26 1.  Sélectionnez Activer la rétroaction d'authentification améliorée
       pour envoyer un message aux utilisateurs en cas d'échec de l'
       authentification. Le message que les utilisateurs reçoivent incluent
        les erreurs de mot de passe, compte désactivé ou verrouillé, ou l'
       utilisateur est introuvable, pour n'en nommer que quelques-uns.
27 1.  Dans Type d'authentification par défaut, sélectionnez le type d'
       authentification.
28 1.  Configurez les paramétres de votre type d'authentification, puis
       cliquez sur OK.
29 <!--NeedCopy-->
```

Utilisateurs et groupes

August 20, 2021

Après avoir configuré l'authentification, l'autorisation et l'audit de la configuration de base, vous créez des utilisateurs et des groupes. Vous créez d'abord un compte d'utilisateur pour chaque personne qui s'authentifie via l'appliance Citrix ADC. Si vous utilisez l'authentification locale contrôlée par l'appliance Citrix ADC elle-même, vous créez des comptes d'utilisateur locaux et attribuez des mots de passe à chacun de ces comptes.

Vous créez également des comptes d'utilisateur sur l'appliance Citrix ADC si vous utilisez un serveur d'authentification externe. Dans ce cas, cependant, chaque compte d'utilisateur doit correspondre exactement à un compte pour cet utilisateur sur le serveur d'authentification externe, et vous n'affectez pas de mots de passe aux comptes d'utilisateur que vous créez sur Citrix ADC. Le serveur d'authentification externe gère les mots de passe des utilisateurs qui s'authentifient auprès du serveur d'authentification externe.

Si vous utilisez un serveur d'authentification externe, vous pouvez toujours créer des comptes d'utilisateur locaux sur l'appliance Citrix ADC si, par exemple, vous souhaitez autoriser des util-

isateurs temporaires (tels que les visiteurs) à se connecter mais ne souhaitez pas créer d'entrées pour ces utilisateurs sur le serveur d'authentification. Vous attribuez un mot de passe à chaque compte d'utilisateur local, comme vous le feriez si vous utilisiez l'authentification locale pour tous les comptes d'utilisateur.

Chaque compte d'utilisateur doit être lié à des stratégies d'authentification et d'autorisation. Pour simplifier cette tâche, vous pouvez créer un ou plusieurs groupes et leur attribuer des comptes d'utilisateur. Vous pouvez ensuite lier des stratégies à des groupes au lieu de comptes d'utilisateur individuels.

Configurer des stratégies avec des groupes

Après avoir configuré des groupes, vous pouvez utiliser la boîte de dialogue **Groupe** pour appliquer des stratégies et des paramètres qui spécifient l'accès utilisateur. Si vous utilisez l'authentification locale, vous créez des utilisateurs et les ajoutez à des groupes configurés sur Citrix Gateway. Les utilisateurs héritent ensuite des paramètres de ce groupe.

Vous pouvez configurer les stratégies ou paramètres suivants pour un groupe d'utilisateurs dans la boîte de dialogue **Groupe** :

- Utilisateurs
- Stratégies d'autorisation
- Règles d'audit
- Stratégies de session
- Stratégies de trafic
- Signets
- Applications Intranet
- Adresses IP de l'intranet

Dans votre configuration, vous pouvez avoir des utilisateurs appartenant à plusieurs groupes. En outre, chaque groupe peut avoir une ou plusieurs stratégies de session liées, avec différents paramètres configurés. Les utilisateurs appartenant à plusieurs groupes héritent des stratégies de session affectées à tous les groupes auxquels l'utilisateur appartient. Pour vérifier quelle évaluation de stratégie de session a priorité sur l'autre, vous devez définir la priorité de la stratégie de session.

Par exemple, vous avez group1 qui est lié par une stratégie de session configurée avec la page d'accueil www.homepage1.com. Group2 est lié par une stratégie de session configurée avec la page d'accueil www.homepage2.com. Lorsque ces stratégies sont liées à des groupes respectifs sans numéro de priorité ou avec un même numéro de priorité, la page d'accueil qui apparaît aux utilisateurs qui appartiennent aux deux groupes dépend de la stratégie traitée en premier. En définissant un numéro de priorité inférieur, ce qui donne une priorité plus élevée, pour la stratégie de session avec la page d'accueil www.homepage1.com, vous pouvez vous assurer que les utilisateurs qui appartiennent aux deux groupes reçoivent la page d'accueil www.homepage1.com.

Si aucun numéro de priorité n'est attribué aux stratégies de session ou n'ont pas le même numéro de priorité, la priorité est évaluée dans l'ordre suivant :

- Utilisateur
- Groupe
- Serveur virtuel
- Global

Si les stratégies sont liées au même niveau, sans numéro de priorité ou si les stratégies ont le même numéro de priorité, l'ordre d'évaluation correspond à l'ordre de liaison de la stratégie. Les stratégies qui sont liées d'abord à un niveau reçoivent la priorité sur les stratégies liées ultérieurement.

Si nous avons un utilisateur lié à plusieurs groupes avec chaque groupe ayant IIP lié, l'utilisateur peut obtenir une adresse IP gratuite de n'importe lequel des groupes liés.

Créer des utilisateurs et des groupes

Configurer l'authentification, l'autorisation et l'audit des utilisateurs locaux à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic des applications > Utilisateurs**
   de Citrix Gateway, développez **Citrix Gateway > Administration des utilisateurs**, puis cliquez sur **Utilisateurs AAA**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau compte d'utilisateur, cliquez sur **Ajouter**.
   - Pour modifier un compte d'utilisateur existant, sélectionnez-le, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Créer un utilisateur AAA**, dans la zone de texte **Nom d'utilisateur**, tapez un nom pour l'utilisateur.
4. Si vous créez un compte d'utilisateur authentifié localement, désactivez la case à cocher **Authentification externe** et fournissez un mot de passe local que l'utilisateur utilise pour ouvrir une session.
5. Cliquez sur **Créer** ou **OK**, puis cliquez sur **Fermer**. Un message apparaît dans la barre d'état indiquant que l'utilisateur a bien été configuré.

Configurez l'authentification, l'autorisation et l'audit des groupes locaux et ajoutez des utilisateurs à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Groupes**
   à partir de Citrix Gateway, développez **Citrix Gateway > Administration des utilisateurs**, puis cliquez sur **Groupes AAA**.

2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer un groupe, cliquez sur **Ajouter**.
   - Pour modifier un groupe existant, sélectionnez-le, puis cliquez sur **Modifier**.
3. Si vous créez un groupe, dans la boîte de dialogue **Créer un groupe AAA**, dans la zone de texte **Nom du groupe**, tapez un nom pour le groupe.
4. Dans la zone **Avancé** à droite, cliquez sur **Utilisateurs AAA** .
   - Pour ajouter un utilisateur au groupe, sélectionnez-le, puis cliquez sur **Ajouter**.
   - Pour supprimer un utilisateur du groupe, sélectionnez-le, puis cliquez sur **Supprimer**.
   - Pour créer un nouveau compte d'utilisateur et l'ajouter au groupe, cliquez sur l'icône **Plus**, puis suivez les instructions de « Pour configurer l'authentification, l'autorisation et l'audit des utilisateurs locaux à l'aide de l'utilitaire de configuration. »
5. Cliquez sur **Créer** ou **sur OK**. Le groupe que vous avez créé apparaît dans la page **Groupes AAA** .

Supprimer un groupe à l'aide de l'interface graphique

Vous pouvez également supprimer des groupes d'utilisateurs de Citrix Gateway.

1. Accédez à **Sécurité > AAA - Trafic des applications > Groupes**
   à partir de Citrix Gateway, ExpandCitrix **Gateway > Administration des utilisateurs,** puis cliquez sur **Groupes AAA**.
   Dans le volet d'informations, sélectionnez le groupe, puis cliquez sur Supprimer.

Configurer l'authentification, l'autorisation et l'audit des utilisateurs locaux à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
add aaa group <groupname>

bind aaa group <groupname> -username <username>
<!--NeedCopy-->
```

Exemple :

```
add aaa group group-2

bind aaa group group-2 -username user-2
<!--NeedCopy-->
```


Supprimer des utilisateurs d'un groupe d'authentification, d'autorisation et d'audit à l'aide de l'interface de ligne de commande

À l'invite de commandes, dissociez les utilisateurs du groupe en tapant la commande suivante une fois pour chaque compte d'utilisateur lié au groupe :

```
unbind aaa group <groupname> -username <username><!--NeedCopy-->
```

```
**Exemple :**

<!--NeedCopy-->
```

unbind aaa group group-hr -username user-hr-1

```
### Supprimer un groupe d'authentification, d'autorisation et d'audit à
    l'aide de l'interface de ligne de commande

Supprimez d'abord tous les utilisateurs du groupe. Ensuite, à l'invite
   de commandes, tapez la commande suivante pour supprimer un groupe
   Citrix ADC AAA et vérifier la configuration :

<!--NeedCopy-->
```

rm aaa group

```
**Exemple :**

<!--NeedCopy-->
```

rm aaa group group-hr

```
> **Remarque**
>
>Vous ne pouvez pas ajouter de nom d'utilisateur avec un domaine si le
   nom d'utilisateur est déjà ajouté sans domaine. Si le nom d'
   utilisateur avec domaine est ajouté d'abord suivi du même nom d'
   utilisateur sans domaine, l'appliance Citrix ADC ajoute le nom d'
   utilisateur à la liste des utilisateurs.

L'exemple suivant montre comment ajouter un nom d'utilisateur avec un
   domaine n'est pas autorisé si le même nom d'utilisateur est ajouté
   sans domaine.

<!--NeedCopy-->
```



```
add aaa user u47985
Done
show aaa users
1) UserName: u47985
Done
add aaa user u47985@domain.com
ERROR: User already exists
```

L'exemple suivant montre si le nom d'utilisateur avec domaine est ajouté en premier, suivi du même nom d'utilisateur sans domaine, puis l'appliance Citrix ADC ajoute le nom d'utilisateur à la liste des utilisateurs.

```
> add aaa user u47985@domain.com
Done
> add aaa user u47985
Done
> sh aaa user
1)   UserName: u47985@domain.com
2)   UserName: u47985
```

Méthodes d'authentification

January 21, 2021

L'appliance Citrix ADC peut authentifier les utilisateurs à l'aide de comptes d'utilisateurs locaux ou à l'aide d'un serveur d'authentification externe. L'appliance prend en charge les types d'authentification suivants :

- **LOCAL :** s'authentifie auprès de l'appliance Citrix ADC à l'aide d'un mot de passe, sans référence à un serveur d'authentification externe. Les données utilisateur sont stockées localement sur l'appliance Citrix ADC.
- **RADIUS :** authentifier auprès d'un serveur RADIUS externe.
- **LDAP :** s'authentifie auprès d'un serveur d'authentification LDAP externe.
- **TACACS :** Authentification auprès d'un serveur d'authentification TACACS (Terminal Access Controller Access Control System) externe.
- **CERT :** s'authentifie auprès de l'appliance Citrix ADC à l'aide d'un certificat client, sans référence à un serveur d'authentification externe.

- **NEGOTIATE :** s'authentifie auprès d'un serveur d'authentification Kerberos. S'il y a une erreur dans l'authentification Kerberos, Citrix ADC utilise l'authentification NTLM.
- **SAML :** s'authentifie auprès d'un serveur prenant en charge le langage SAML (Security Assertion Markup Language).
- **IDP SAML :** configure Citrix ADC pour servir de fournisseur d'identité (IdP) (Security Assertion Markup Language) (SAML).
- **WEB :** s'authentifie auprès d'un serveur Web, en fournissant les informations d'identification requises par le serveur Web dans une requête HTTP et en analysant la réponse du serveur Web pour déterminer si l'authentification de l'utilisateur a réussi.
- **OTP natif :** l'appliance Citrix ADC prend en charge les mots de passe à usage unique (OTP) sans avoir à utiliser un serveur tiers.
- **Notification Push :** Citrix Gateway prend en charge les notifications push pour OTP. Les utilisateurs n'ont pas besoin d'entrer manuellement l'OTP reçu sur leurs périphériques enregistrés pour se connecter à Citrix Gateway. Les administrateurs peuvent configurer Citrix Gateway de sorte que les notifications de connexion soient envoyées aux périphériques enregistrés des utilisateurs à l'aide des services de notification push.
- **Email OTP :** La méthode Email OTP vous permet de vous authentifier à l'aide du mot de passe à usage unique (OTP) envoyé à l'adresse e-mail enregistrée. Lorsque vous essayez de vous authentifier sur un service, le serveur envoie un OTP à l'adresse e-mail enregistrée de l'utilisateur.
- **Authentification reCAPTCHA** - Citrix Gateway prend en charge une nouvelle action de première classe 'CaptchaAction' qui simplifie la configuration de reCAPTCHA. Comme reCAPTCHA est un premier recours collectif, il peut être un facteur qui lui est propre. Vous pouvez injecter reCAPTCHA n'importe où dans le flux nFactor.
- **Authentification nFactor :** l'authentification multifacteur améliore la sécurité d'une application en exigeant des utilisateurs qu'ils fournissent plusieurs preuves d'identification pour obtenir l'accès. L'appliance Citrix ADC offre une approche extensible et flexible de la configuration de l'authentification multifacteur. Cette approche est appelée authentification NFactor.
- **Authentification OAuth :** l'authentification OAuth autorise et authentifie les utilisateurs à des services hébergés sur des applications telles que Google, Facebook et Twitter.

Authentification NFactor

September 8, 2021

> **Important**
>
> - L'authentification nFactor est prise en charge à partir de NetScaler 11.0 Build 62.x.
> - Pour que l'authentification nFactor fonctionne avec Citrix ADC, une licence Advanced ou Premium est requise.
> - À partir de la version 13.0 build 67.x, l'authentification NFactor est prise en charge avec la licence Standard uniquement pour le serveur virtuel Gateway/VPN. Pour plus d'informations sur l'authentification NFactor avec Citrix Gateway, consultez nFactor for Gateway Authentication.
> - L'authentification NFactor n'est pas prise en charge pour le client Linux.

L'authentification multifacteur améliore la sécurité d'une application en exigeant des utilisateurs qu'ils fournissent plusieurs preuves d'identification pour y accéder. L'appliance Citrix ADC offre une approche extensible et flexible pour configurer l'authentification multifacteur. Cette approche est appelée *authentification NFactor*.

Fonctionnement de l'authentification NFactor

Chaque facteur d'authentification effectue les tâches suivantes :

- Collecte les informations d'identification de l'utilisateur. Les mécanismes d'authentification pris en charge par Citrix ADC incluent LDAP, RADIUS, assertion SAML, certificat client, OAuth OpenID Connect, Kerberos, etc.
- Évalue les informations d'identification fournies pour décider si l'authentification a réussi, échoué ou si les actions telles que l'extraction de groupe, l'extraction d'attributs doit être effectuée.
- Sur la base des résultats de l'évaluation, l'accès est soit accordé, soit refusé, soit un facteur suivant est sélectionné.
- Répétez ces étapes jusqu'à ce qu'il n'y ait plus de facteurs à évaluer.

Avec l'authentification NFactor, vous pouvez :

- Configurez un certain nombre de facteurs d'authentification.
- Fonder la sélection du facteur suivant sur le résultat de l'exécution du facteur précédent.
- Personnalisez l'interface de connexion. Par exemple, vous pouvez personnaliser les noms des étiquettes, les messages d'erreur et le texte d'aide.
- Extrayez les informations du groupe d'utilisateurs sans effectuer d'authentification.
- Configurez le passage pass-through pour un facteur d'authentification. Cela signifie qu'aucune interaction de connexion explicite n'est requise pour ce facteur.
- Configurez l'ordre dans lequel les différents types d'authentification sont appliqués. Tous les mécanismes d'authentification pris en charge par l'appliance Citrix ADC peuvent être configurés

comme n'importe quel facteur de la configuration de l'authentification nFactor. Ces facteurs sont exécutés dans l'ordre dans lequel ils sont configurés.

- Configurez Citrix ADC pour passer à un facteur d'authentification qui doit être exécuté en cas d'échec de l'authentification. Pour ce faire, vous configurez une autre stratégie d'authentification avec exactement la même condition, mais avec la priorité la plus élevée suivante et avec l'action définie sur « NO_AUTH ». Vous devez configurer le facteur suivant, qui doit spécifier le mécanisme d'authentification alternatif à appliquer.

Chiffrement des informations de connexion Citrix Gateway pour l'authentification NFactor

Citrix Gateway avec authentification nFactor peut chiffrer les champs de demande de connexion envoyés par un client (navigateur ou applications SSO) pendant le processus d'authentification. Les champs de demande de connexion chiffrés fournissent une couche de sécurité supplémentaire pour protéger les données sensibles de l'utilisateur contre la divulgation.

Navigateurs compatibles

Le tableau suivant répertorie les navigateurs ainsi que les détails de version qui prennent en charge le chiffrement de connexion.

Navigateurs	Version
Chrome	78 et plus
Firefox	69 ans et plus
Internet Explorer	11
Bord	42 ans et plus
Safari	11.0 et plus
Opéra	66

Clients compatibles

La section suivante répertorie les clients ainsi que les détails de version qui prennent en charge le chiffrement des informations de connexion Citrix Gateway.

- L'application Citrix Workspace sur Mac prend en charge le chiffrement uniquement lorsque la version du système d'exploitation est 10.14.x et supérieure.
- L'application Citrix SSO sur Mac prend en charge le chiffrement uniquement lorsque la version du système d'exploitation est 10.14.x et supérieure.

- L'application Windows SSO n'a pas de restrictions quant à la compatibilité.
- Le chiffrement des mots de passe dans l'application Citrix Workspace pour les clients Windows est pris en charge uniquement dans la version Internet Explorer 11.

Pour activer le chiffrement de connexion à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set aaa parameter [-loginEncryption (ENABLED | DISABLED)]
```

> **Remarque**
>
> Le paramètre LoginEncryption est DÉSACTIVÉ par défaut. Vous devez l'ACTIVER.

Pour activer le chiffrement de connexion à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA — Trafic des applications**, cliquez sur **Modifier les paramètres AAA d'authentification dans la section Paramètres d'authentification** .
2. Sur la page **Configurer les paramètres AAA**, faites défiler vers le bas jusqu'à l'option de **chiffrement de connexion** et activez-la.

Concepts, entités et terminologie de nFactor

August 20, 2021

Cette rubrique décrit certaines des principales entités impliquées dans l'authentification nFactor et leur importance.

Schéma de connexion

nFactor découple la 'vue', l'interface utilisateur, avec le 'modèle' qui est la gestion de l'exécution. La vue de nFactor est définie par le schéma de connexion'. Le schéma de connexion est une entité qui définit ce que l'utilisateur voit et spécifie comment extraire les données de l'utilisateur.

Pour définir la vue, le schéma de connexion pointe vers un fichier sur le disque qui définit le formulaire d'ouverture de session. Ce fichier doit être conforme à la spécification de « Citrix Common Forms Protocol ». Ce fichier est essentiellement une définition XML du formulaire d'ouverture de session.

Outre le fichier XML, le schéma de connexion contient des expressions de stratégie avancées pour glaner le nom d'utilisateur et le mot de passe à partir de la demande de connexion de l'utilisateur.

Ces expressions sont facultatives et peuvent être omises si le nom d'utilisateur et le mot de passe de l'utilisateur arrivent avec les noms de variables de forme attendus.

Le schéma de connexion définit également, si l'ensemble actuel d'informations d'identification doit être utilisé comme informations d'identification SingleSignon par défaut.

Étiquette de stratégie

Une étiquette de stratégie est un ensemble de stratégies. Il s'agit d'une construction qui n'est pas étrangère à l'infrastructure de stratégie de Citrix ADC. L'étiquette de stratégie définit un facteur d'authentification. Autrement dit, il contient toutes les stratégies nécessaires pour déterminer si les informations d'identification de l'utilisateur sont satisfaites. Toutes les stratégies d'une étiquette de stratégie peuvent être considérées comme homogènes. L'étiquette de stratégie pour l'authentification ne peut pas prendre de stratégies de type différent, par exemple réécriture. Pour mettre d'une manière différente, toutes les stratégies d'une étiquette de stratégie valident le même mot de passe/informations d'identification de l'utilisateur, principalement. Le résultat des stratégies dans un PolicyLabel suit une condition logique OU. Par conséquent, si l'authentification spécifiée par la première stratégie réussit, les autres stratégies suivantes sont ignorées.

L'étiquette de stratégie peut être créée en exécutant la commande CLI suivante :

```
1 add authentication policy label mylabel -loginSchema <>
2 <!--NeedCopy-->
```

Une étiquette de stratégie prend le schéma de connexion comme propriété. Le schéma de connexion définit l'affichage de cette étiquette de stratégie. Si le schéma de connexion n'est pas spécifié, un schéma de connexion implicite, LSCHEMA_INT, est associé à cette étiquette de stratégie. Le schéma de connexion détermine si une étiquette de stratégie devient un passthrough ou non.

Étiquette de serveur virtuel

Dans l'infrastructure de stratégie avancée de Citrix ADC, un serveur virtuel est également une étiquette de stratégie implicite. En effet, le serveur virtuel peut également être lié à plusieurs stratégies. Cependant, un serveur virtuel est spécial car il est le point d'entrée du trafic client et peut prendre des stratégies d'un type différent. Chacune des stratégies qu'il a placées sous sa propre étiquette au sein du serveur virtuel. Par conséquent, le serveur virtuel est une conglomération d'étiquettes.

Facteur suivant

Chaque fois qu'une stratégie est liée à un serveur virtuel ou à une étiquette de stratégie, elle peut être spécifiée avec le facteur suivant. Le facteur suivant détermine ce qui doit être fait si une authentifica-

tion donnée réussit. S'il n'y a pas de facteur suivant, cela conclut le processus d'authentification pour cet utilisateur.

Chaque stratégie liée à un serveur virtuel ou à un libellé de stratégie peut avoir un facteur suivant différent. Cela permet une flexibilité ultime où le succès de chaque stratégie peut définir un nouveau chemin pour l'authentification de l'utilisateur. L'administrateur peut tirer parti de ce fait et créer des facteurs de secours intelligents pour les utilisateurs qui ne respectent pas certaines stratégies.

Stratégie de non-Auth

nFactor introduit un type spécial de stratégie intégrée appelé NO_AUTHN. La stratégie NO_AUTHN renvoie toujours le succès en tant que résultat d'authentification. La stratégie sans authentification peut être créée en exécutant la commande CLI suivante :

```
1 add authentication policy noauthpolicy  - rule <> -action NO_AUTHN
2 <!--NeedCopy-->
```

Conformément à la commande, la stratégie de no-authentification prend une règle qui peut être n'importe quelle expression de stratégie avancée. Le résultat de l'authentification est toujours un succès de NO_AUTHN.

Une stratégie sans authentification en soi ne semble pas ajouter de valeur. Cependant, lorsqu'il est utilisé avec des étiquettes de stratégie passthrough, il offre une grande flexibilité pour prendre des décisions logiques pour piloter le flux d'authentification des utilisateurs. NO_AUTHN et les facteurs de transmission offrent une nouvelle dimension à la flexibilité de nFactor.

Remarque : Consultez les exemples qui illustrent l'utilisation de la non-autorisation et du passage dans les sections suivantes.

Facteur/étiquette de passage

Une fois que l'utilisateur a passé l'authentification sur le serveur virtuel (pour le premier facteur), les authentifications suivantes se produisent aux étiquettes de stratégie ou aux facteurs (secondaires) définis par l'utilisateur.
Chaque étiquette/facteur de stratégie est associé à une entité de schéma de connexion pour afficher la vue de ce facteur. Cela permet de personnaliser les vues en fonction du chemin que l'utilisateur aurait emprunté pour arriver à un facteur donné.

Il existe des types spécialisés d'étiquettes de stratégie qui ne pointent pas explicitement vers un schéma de connexion. Les étiquettes de stratégie spécialisées pointent vers un schéma de connexion qui ne pointe pas réellement vers le fichier XML de la vue. Ces étiquettes/facteurs de stratégie sont appelés facteurs « passthrough ».

Les facteurs de passage peuvent être créés en exécutant les commandes CLI suivantes :

Exemple 1 :

```
1 add authentication policylabel example1
2 <!--NeedCopy-->
```

Exemple 2 :

```
1 add loginschema passthrough_schema  - authenticationSchema noschema
2
3 add authentication policylabel example2  - loginschema
     passthrough_schema
4 <!--NeedCopy-->
```

Le facteur de transmission implique que le sous-système d'authentification, d'autorisation et d'audit ne doit pas revenir à l'utilisateur pour obtenir les informations d'identification définies pour ce facteur. Au lieu de cela, c'est un indice pour l'authentification, l'autorisation et l'audit de continuer avec les informations d'identification déjà obtenues. Ceci est utile dans les cas où l'intervention de l'utilisateur n'est pas souhaitée. Par exemple,

- Lorsque l'utilisateur est présenté deux champs de mot de passe. Après le premier facteur, le deuxième facteur n'a pas besoin d'intervention de l'utilisateur
- Lorsque l'authentification d'un type (par exemple certificat) est terminée, et l'administrateur doit extraire des groupes pour cet utilisateur.

Le facteur de passage peut être utilisé avec la stratégie NO_AUTH pour effectuer des sauts conditionnels.

Flux d'authentification nFactor

L'authentification commence toujours sur le serveur virtuel dans nFactor. Le serveur virtuel définit le premier facteur pour l'utilisateur. Le premier formulaire que l'utilisateur voit est servi par le serveur virtuel. Le formulaire d'ouverture de session que l'utilisateur voit peut être personnalisé sur le serveur virtuel à l'aide de stratégies de schéma de connexion. S'il n'y a pas de stratégie de schéma de connexion, un seul champ nom d'utilisateur et mot de passe s'affiche pour l'utilisateur.

Si plusieurs champs de mot de passe doivent être affichés à l'utilisateur sur un formulaire personnalisé, les stratégies de schéma de connexion doivent être utilisées. Ils permettent d'afficher différents formulaires en fonction des règles configurées (comme l'utilisateur intranet par rapport à l'utilisateur externe, le fournisseur de services A par rapport au fournisseur de services B).

Une fois les informations d'identification de l'utilisateur publiées, l'authentification commence à l'authentification serveur virtuel, le premier facteur. Étant donné que le serveur virtuel d'authentification peut être configuré avec plusieurs stratégies, chacune d'entre elles est évaluée dans une séquence. À un moment donné, si une stratégie d'authentification réussit, le facteur suivant

spécifié par rapport à elle est pris. S'il n'y a pas de facteur suivant, le processus d'authentification se termine. Si le facteur suivant existe, il est vérifié si ce facteur est un facteur de passage ou un facteur régulier. S'il s'agit d'un transfert, les stratégies d'authentification sur ce facteur sont évaluées sans intervention de l'utilisateur. Sinon, le schéma de connexion associé à ce facteur est affiché à l'utilisateur.

Exemple d'utilisation de stratégies de facteur de transmission et de non-authentification pour prendre des décisions logiques

L'administrateur souhaite décider NextFactor en fonction des groupes.

- Add authentication policylabel group check
- Add authentication policy admin group –rule http.req.user.is_member_of("Administrators") –action NO_AUTHN
- Add authentication policy nonadmins –rule true –action NO_AUTHN
- Bind authentication policy label group check –policy admingroup –pri 1 –nextFactor factor-for-admin
- Bind authentication policy label groupcheck –policy nonadmins –pri 10 –nextfactor factor-for-others
- Add authentication policy first_factor_policy –rule <> -action <>
- Bind authentication vserver <> -policy first_factor_policy –priority 10 –nextFactor groupcheck

Configuration de l'authentification NFactor

October 5, 2021

Vous pouvez configurer plusieurs facteurs d'authentification à l'aide de la configuration nFactor plutôt que de deux facteurs seulement. La configuration nFactor n'est prise en charge que dans les éditions Citrix ADC Advanced et Premium.

Méthodes de configuration de NFactor

Vous pouvez configurer l'authentification NFactor en utilisant l'une des méthodes suivantes :

- **nFactor Visualizer :** nFactor Visualizer vous permet de lier facilement des facteurs ou des étiquettes de stratégie dans un seul volet et de modifier la liaison des facteurs dans le même volet. Vous pouvez créer un flux nFactor à l'aide du visualiseur et lier ce flux à un serveur virtuel Citrix ADC AAA. Pour plus d'informations sur nFactor Visualizer et un exemple de configuration de nFactor à l'aide de visualizer, consultez nFactor Visualizer pour une configuration simplifiée.

- **interface graphique Citrix ADC :** pour plus de détails, reportez-vous à la section **Éléments de configuration impliqués dans la configuration de NFactor**.
- **Citrix ADC CLI :** Pour obtenir un extrait de code de configuration nFactor à l'aide de l'interface de ligne de commande Citrix ADC, reportez-vous à Exemple d'extrait de code sur la configuration de nFactor à l'aide de l'interface de ligne de commande Citrix ADC.

> **Important :** Cette rubrique contient des détails sur la configuration de NFactor à l'aide de l'interface graphique Citrix ADC.

Éléments de configuration impliqués dans la configuration NFactor

Les éléments suivants sont impliqués dans la configuration de NFactor. Pour connaître les étapes détaillées, reportez-vous aux sections appropriées de cette rubrique.

Élément de configuration	Tâches à effectuer
Serveur virtuel AAA	Créer un serveur virtuel AAA
	Liez le thème du portail au serveur virtuel AAA
	Activer l'authentification par certificat client
Schéma de connexion	Configurer un profil de schéma de connexion
	Créer et lier une stratégie de schéma de connexion
Stratégies d'authentification avancées	Créer des stratégies d'authentification avancées
	Lier la stratégie d'authentification avancée de premier facteur au serveur virtuel Citrix ADC AAA
	Utiliser les groupes LDAP extraits pour sélectionner le facteur d'authentification suivant
Étiquette de stratégie d'authentification	Créer une étiquette de stratégie d'authentification
	Libellé de stratégie d'authentification de liaison
nFactor pour Citrix Gateway	Créer un profil d'authentification pour lier un serveur virtuel Citrix ADC AAA au serveur virtuel Citrix Gateway

Élément de configuration	Tâches à effectuer
	Configuration des paramètres SSL et du certificat d'autorité de certification pour Citrix Gateway
	Configurer la stratégie de trafic Citrix Gateway pour l'authentification unique nFactor vers StoreFront

Comment fonctionne NFactor

Lorsqu'un utilisateur se connecte au serveur virtuel Citrix ADC AAA ou Citrix Gateway, la séquence d'événements qui se produisent est la suivante :

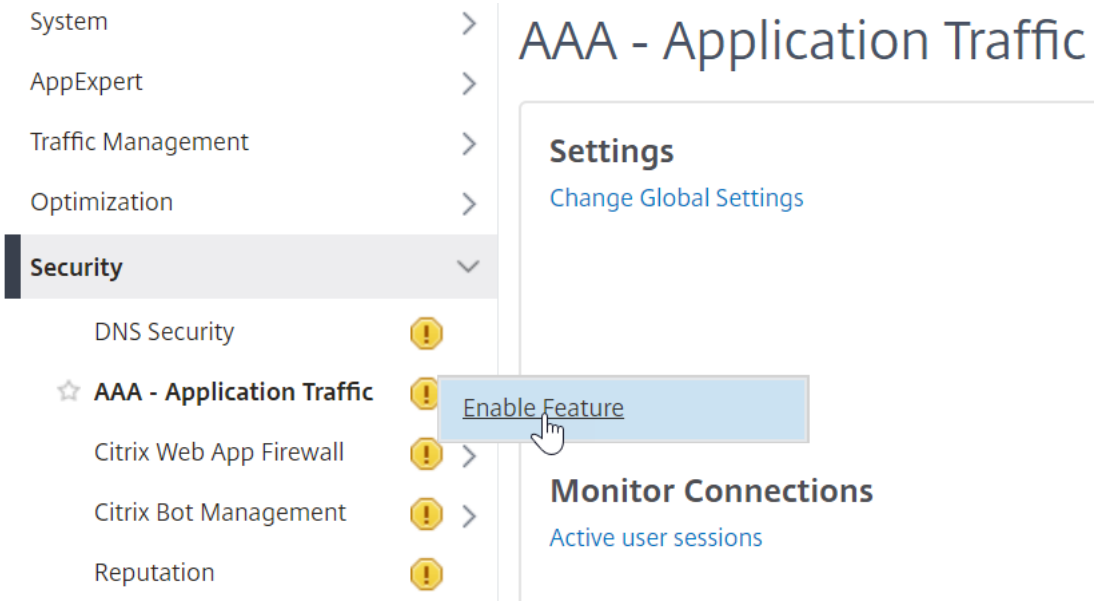
1. Si l'authentification basée sur les formulaires est utilisée, le schéma de connexion lié au serveur virtuel Citrix ADC AAA s'affiche.
2. Les stratégies d'authentification avancées liées au serveur virtuel Citrix ADC AAA sont évaluées.
    - Si la stratégie d'authentification avancée réussit et si le facteur suivant (étiquette de stratégie d'authentification) est configuré, le facteur suivant est évalué. Si Next Factor n'est pas configuré, l'authentification est terminée et réussie.
    - Si la stratégie d'authentification avancée échoue et si Goto Expression est définie sur Suivant, la stratégie d'authentification avancée liée suivante est évaluée. Si aucune des stratégies d'authentification avancée ne réussit, l'authentification échoue.
3. Si l'étiquette de stratégie d'authentification des facteurs suivante est liée à un schéma de connexion, il est affiché pour l'utilisateur.
4. Les stratégies d'authentification avancées liées au libellé de stratégie d'authentification par facteur suivant sont évaluées.
    - Si la stratégie d'authentification avancée réussit et si le facteur suivant (étiquette de stratégie d'authentification) est configuré, le facteur suivant est évalué.
    - Si Next Factor n'est pas configuré, l'authentification est terminée et réussie.
5. Si la stratégie d'authentification avancée échoue et si Goto Expression est Next (Suivant), la stratégie d'authentification avancée liée suivante est évaluée.
6. Si aucune des stratégies d'authentification avancée ne réussit, l'authentification échoue.

Serveur virtuel AAA

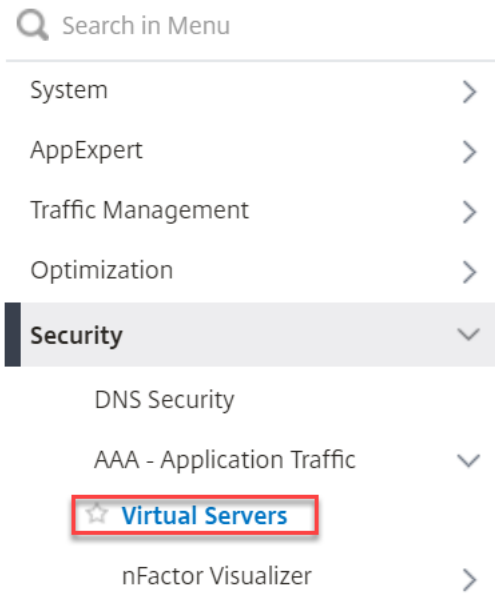
Pour utiliser nFactor avec Citrix Gateway, vous devez d'abord le configurer sur un serveur virtuel AAA. Ensuite, vous lierez le serveur virtuel AAA au serveur virtuel Citrix Gateway.

Créer un serveur virtuel AAA

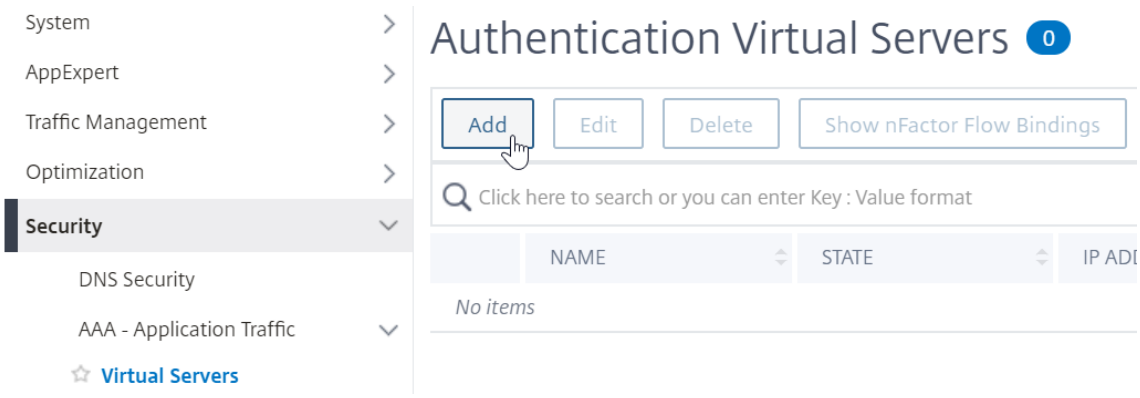
1. Si la fonctionnalité AAA n'est pas déjà activée, accédez à **Sécurité > AAA — Trafic des applications**, puis cliquez avec le bouton droit de la souris pour activer la fonctionnalité.



2. Accédez à **Configuration > Sécurité > AAA - Trafic des applications > Serveurs virtuels**.

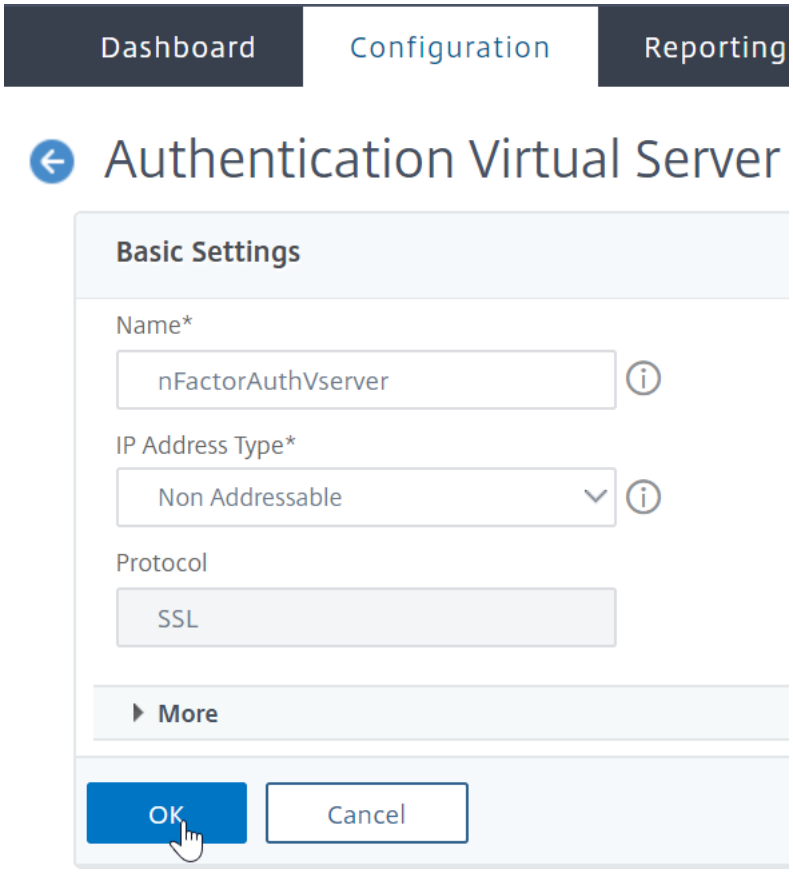


3. Cliquez sur **Ajouter** pour créer un serveur virtuel d'authentification.

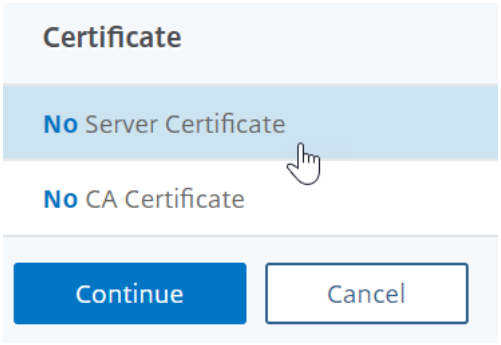


4. Entrez les informations suivantes, puis cliquez sur **OK**.

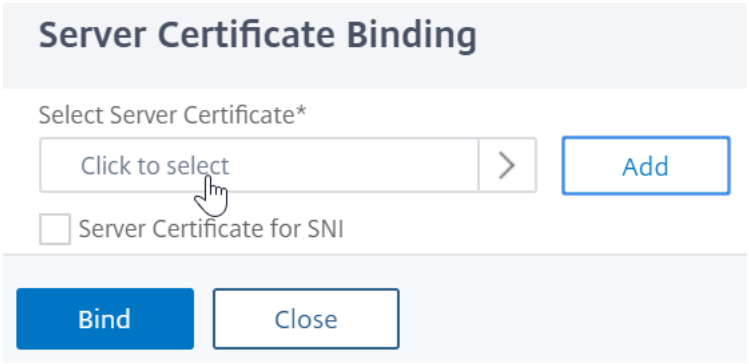
Nom du paramètre	Description des paramètres
Nom	Nom du serveur virtuel AAA.
Type d'adresse IP	Modifiez le type d'adresse IP sur **Non adressable** si ce serveur virtuel est utilisé uniquement pour Citrix Gateway.



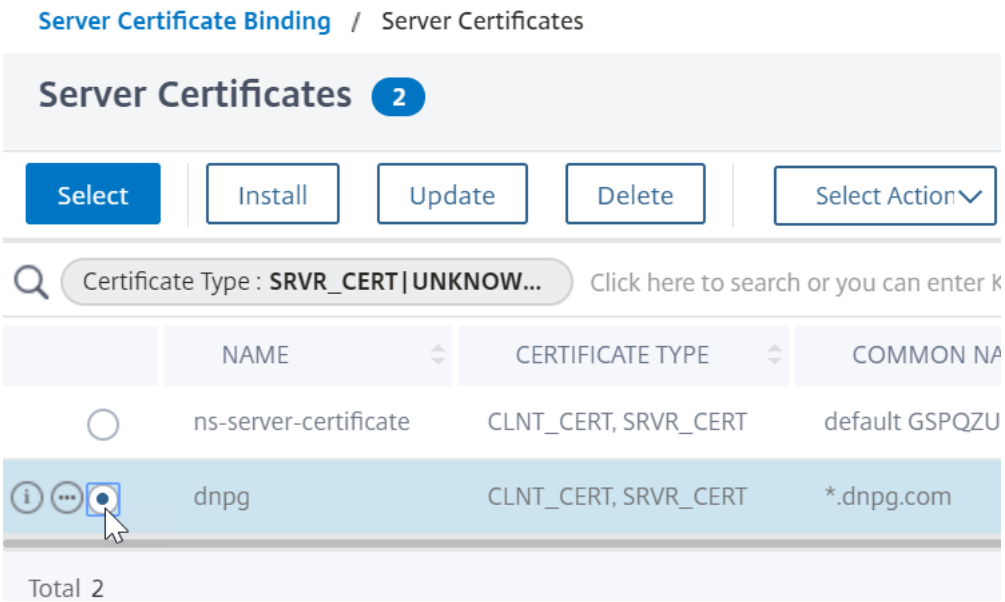
5. Sous Certificat, sélectionnez **Aucun certificat de serveur**.



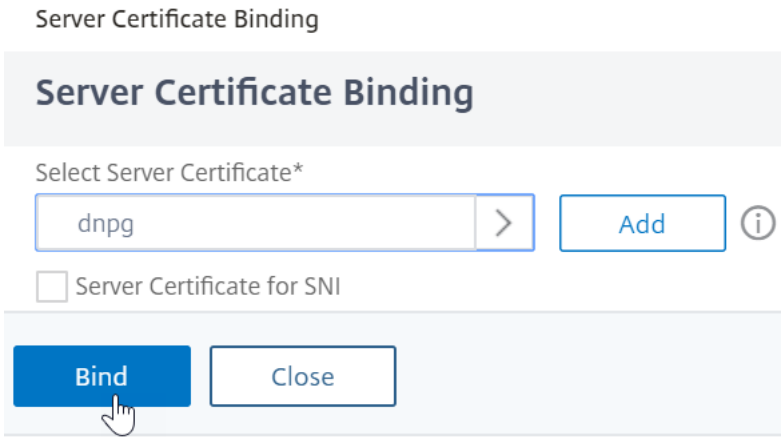
6. Cliquez sur le texte, **cliquez sur pour sélectionner** le certificat de serveur.



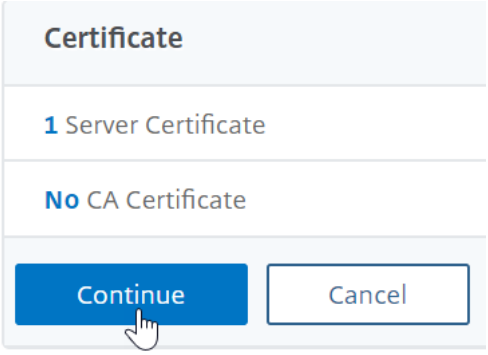
7. Cliquez sur le bouton radio en regard d'un certificat pour le serveur virtuel AAA, puis cliquez sur **Sélectionner**. Le certificat choisi n'a pas d'importance car ce serveur n'est pas directement accessible.



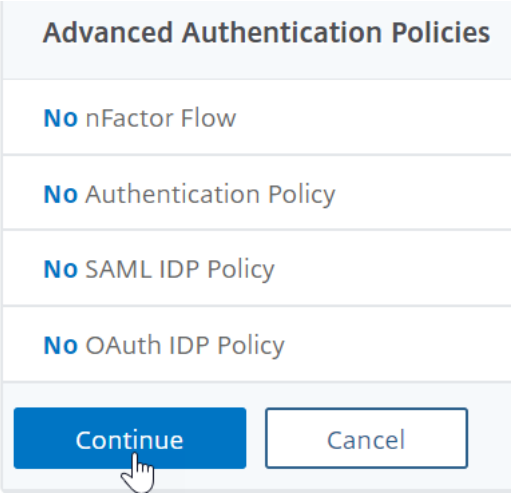
8. Cliquez sur **Bind**.



9. Cliquez sur **Continuer** pour fermer la section **Certificat** .

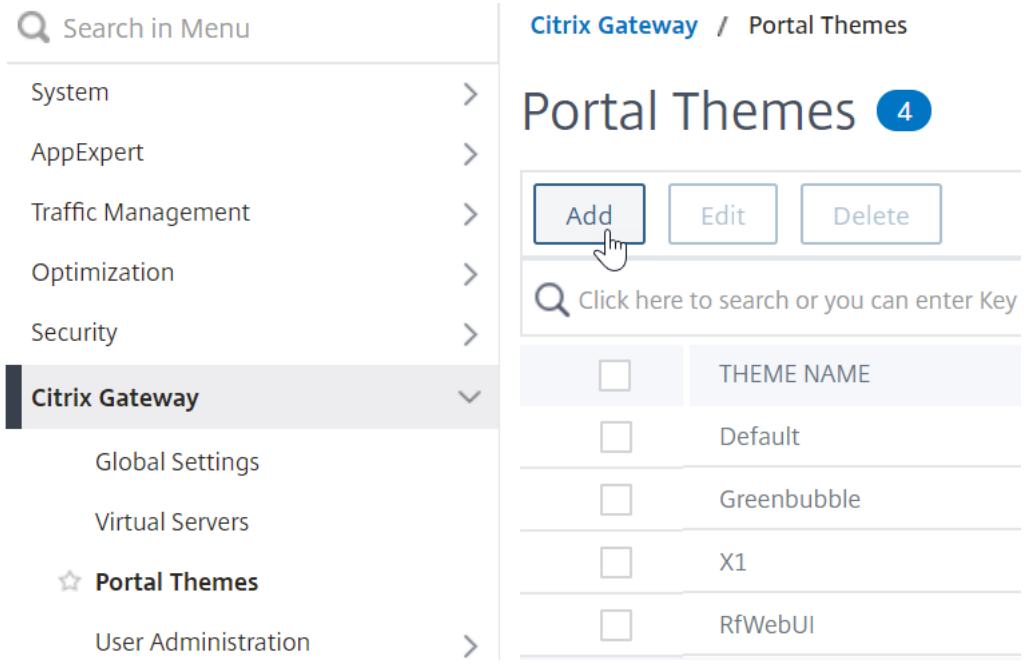


10. Cliquez sur **Continuer**.

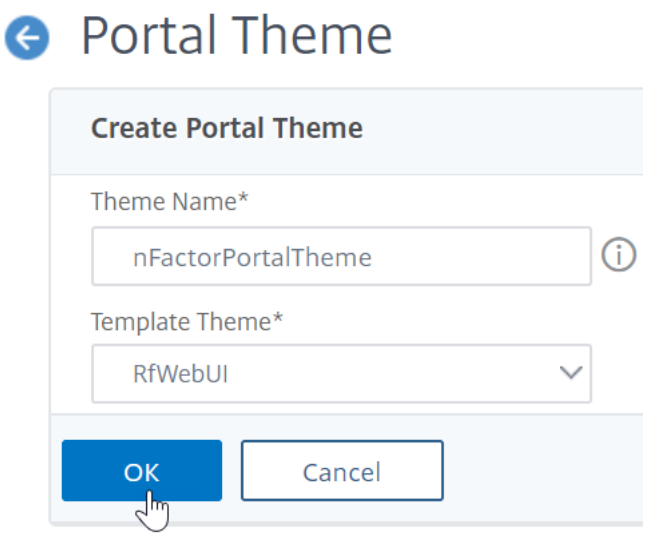


Liez le thème du portail au serveur virtuel AAA

1. Accédez à **Citrix Gateway > Thèmes du portail**, puis ajoutez un thème. Vous créez le thème sous Citrix Gateway, puis vous le liez ultérieurement au serveur virtuel AAA.

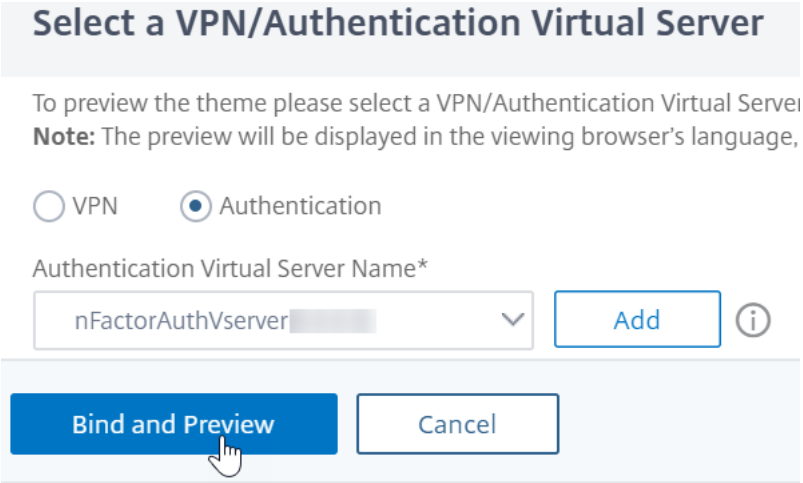


2. Créez un thème basé sur le thème du modèle RFWebUI.



3. Après avoir ajusté le thème comme vous le souhaitez, en haut de la page d'édition du thème du portail, **cliquez sur Cliquez pour lier et afficher le thème configuré**.

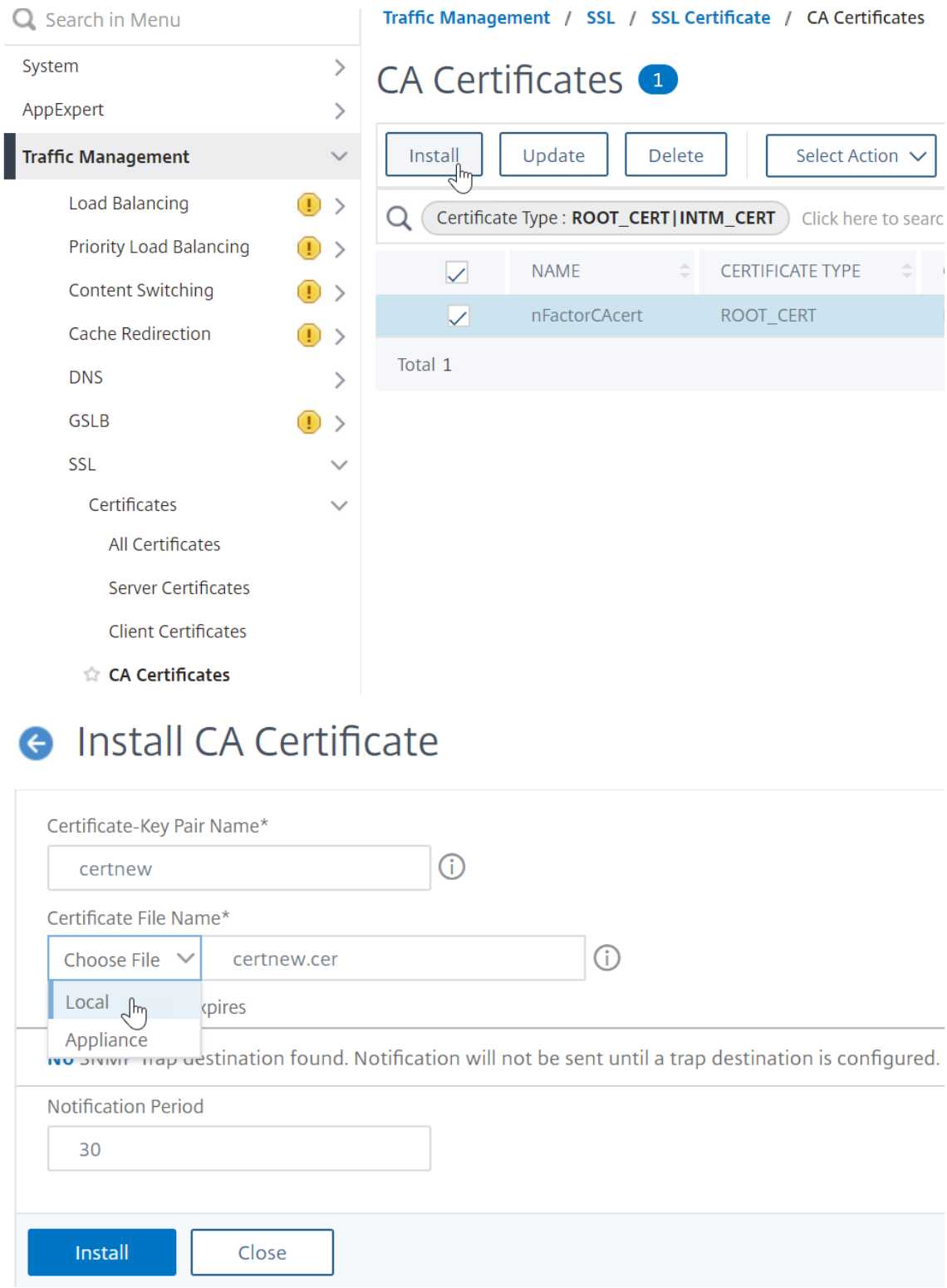
4. Changez la sélection sur Authentification. Dans le menu déroulant **Nom du serveur virtuel d'authentification**, sélectionnez le serveur virtuel AAA, puis cliquez sur **Liaison et aperçu et** fermez la fenêtre d'aperçu.



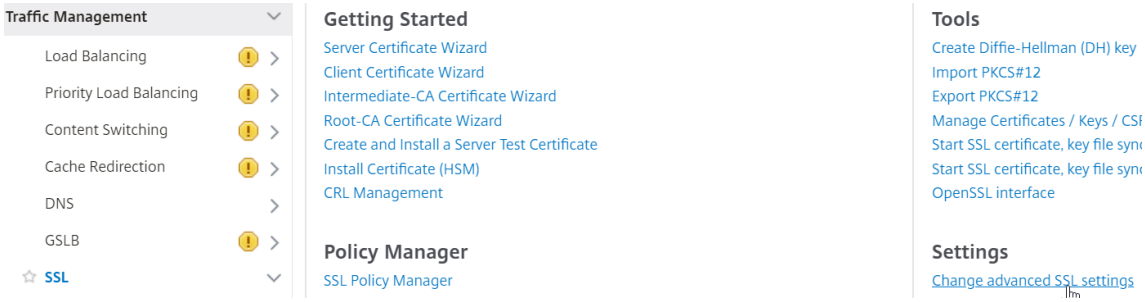
Activer l'authentification par certificat client

Si l'un de vos facteurs d'authentification est le certificat client, vous devez effectuer une configuration SSL sur le serveur virtuel AAA :

1. Accédez à **Gestion du trafic > SSL > Certificats > Certificats d'autorité**de certification, puis installez le certificat racine de l'émetteur des certificats clients. Les certificats racine n'ont pas de fichier clé.



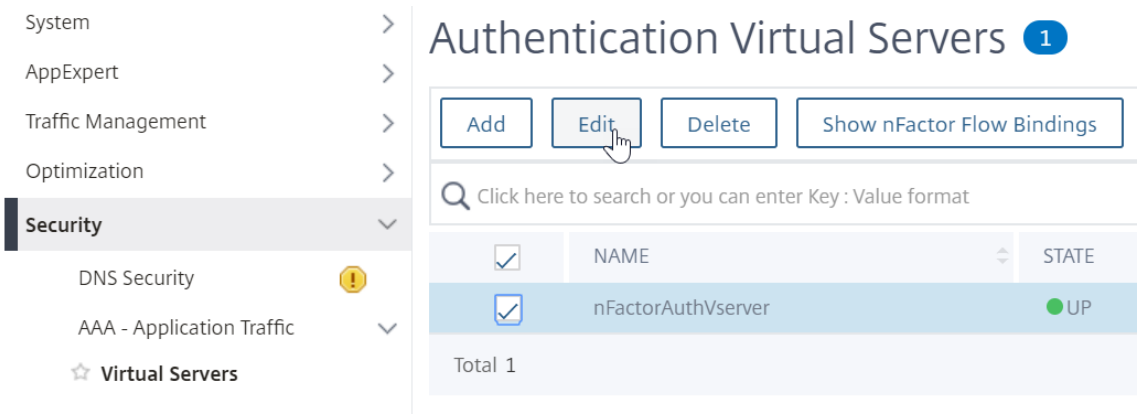
2. Accédez à **Gestion du trafic > SSL > Modifier les paramètres SSL avancés**.



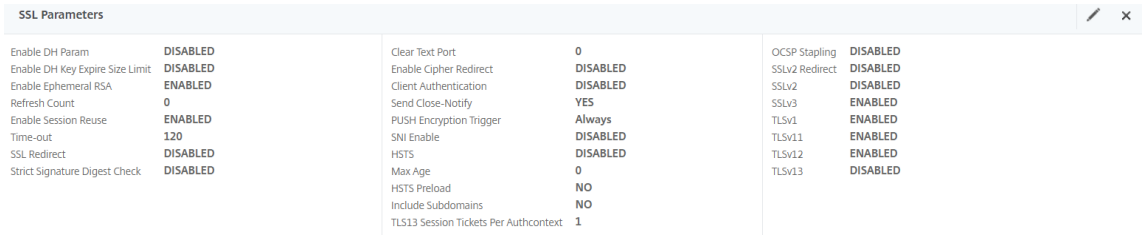
a. Faites défiler l'écran vers le bas pour vérifier si le **profil par défaut** est **ACTIVÉ**. Si oui, vous devez utiliser un profil SSL pour activer l'authentification par certificat client. Sinon, vous pouvez activer l'authentification du certificat client directement sur le serveur virtuel AAA dans la section Paramètres SSL.

3. Si les profils SSL par défaut ne sont pas activés :

a. Accédez à **Sécurité > AAA - Application > Serveurs virtuels**, puis modifiez un serveur virtuel AAA existant.

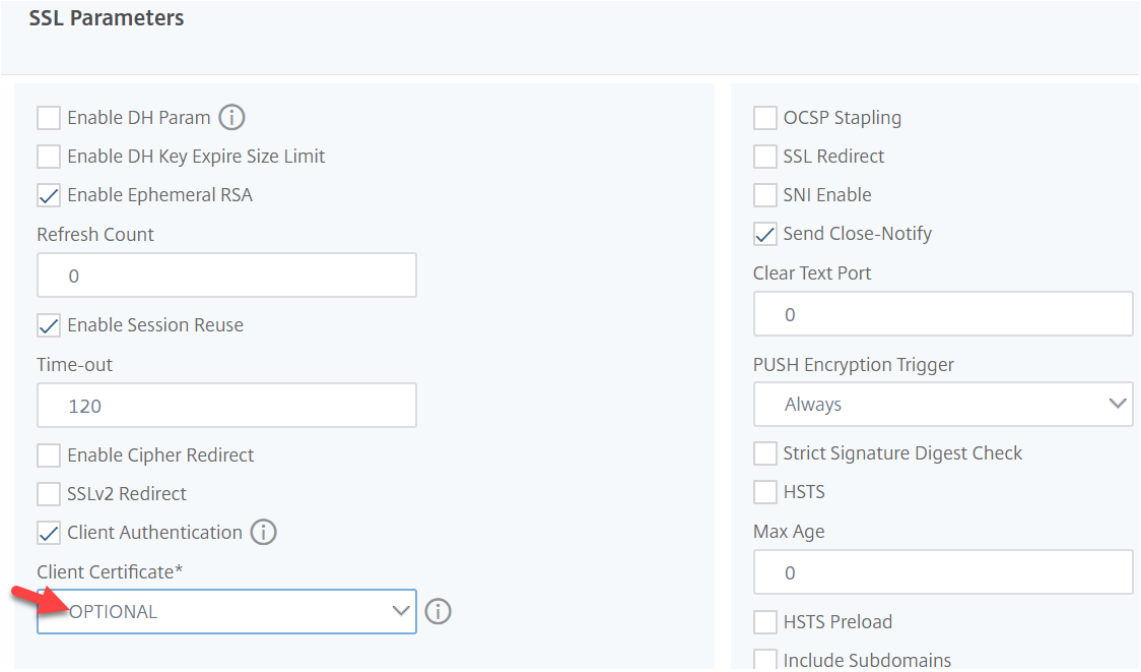


b. Sur la gauche, dans la section **Paramètres SSL**, cliquez sur l'icône en forme de crayon.



c. Cochez la case en regard de l' **authentification du client**.

d. Assurez-vous que l' **option Facultatif** est sélectionnée dans le menu déroulant **Certificat client**, puis cliquez sur **OK**.



4. Si les profils SSL par défaut sont activés, créez un nouveau profil SSL avec l'authentification du client activée :

   a. Dans le menu de gauche, développez Système, puis cliquez sur Profils.

   b. En haut à droite, accédez à l'onglet Profil SSL.

   c. Cliquez avec le bouton droit de la souris sur le profil ns_default_ssl_profile_frontend, puis cliquez sur Ajouter. Cette option permet de copier les paramètres du profil par défaut.

   d. Donnez un nom au profil. Le but de ce profil est d'activer les certificats clients.

   e. Faites défiler vers le bas et trouvez la case à cocher Authentification du client Cochez la case.

   f. Changez la liste déroulante Certificat client sur FACULTATIF.

   g. La copie du profil SSL par défaut ne copie pas les chiffrements SSL, vous devrez donc les refaire.

   h. Cliquez sur Terminé lorsque vous avez terminé de créer le profil SSL.

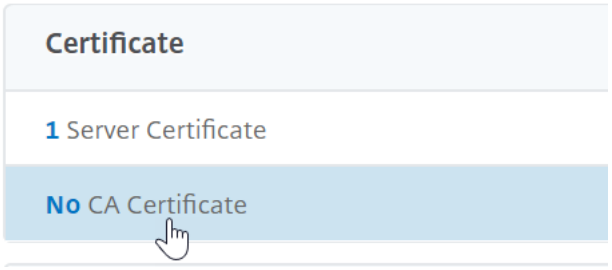
   i. Accédez à Sécurité > AAA — Trafic des applications > Serveurs virtuels, puis modifiez un vServer AAA.

   j. Faites défiler l'écran jusqu'à la section Profil SSL et cliquez sur le crayon.

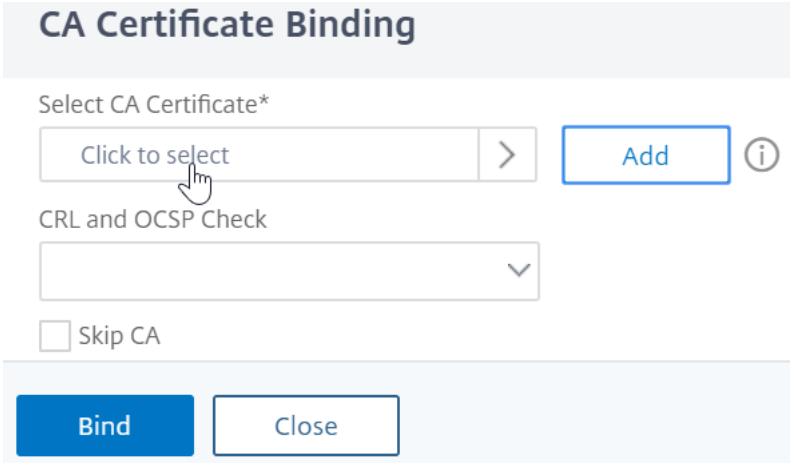
   k. Changez la liste déroulante Profil SSL par le profil sur lequel les certificats client sont activés. Cliquez sur OK.

   l. Faites défiler cet article jusqu'à ce que vous obteniez les instructions pour lier le certificat de l'autorité de certification.

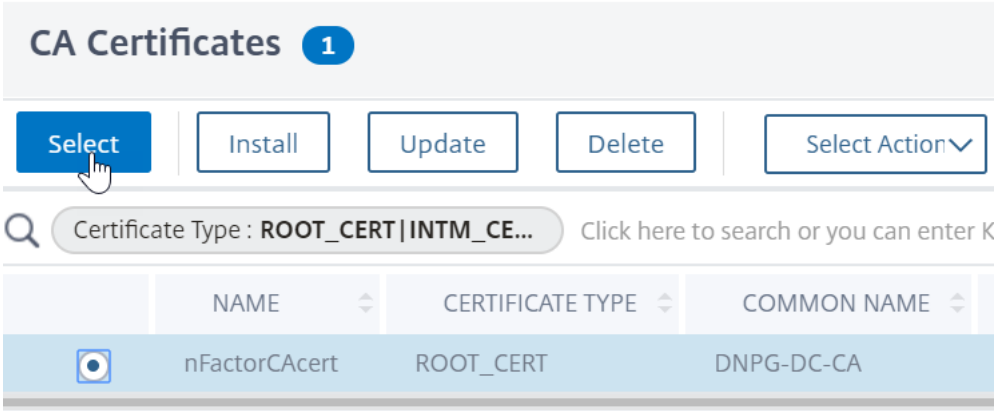
5. Sur la gauche, dans la section **Certificats**, cliquez à l'endroit où il est indiqué **Aucun certificat d'autorité de certification**.



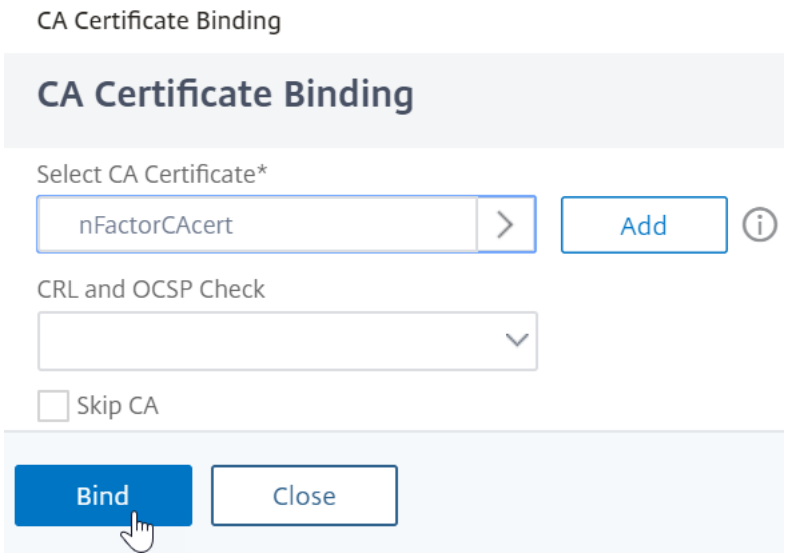
6. Cliquez sur le texte, **cliquez sur pour le sélectionner**.



7. Cliquez sur le bouton radio en regard du certificat racine de l'émetteur des certificats clients, puis cliquez sur **Sélectionner**.



8. Cliquez sur **Bind**.



Fichier XML du schéma de connexion

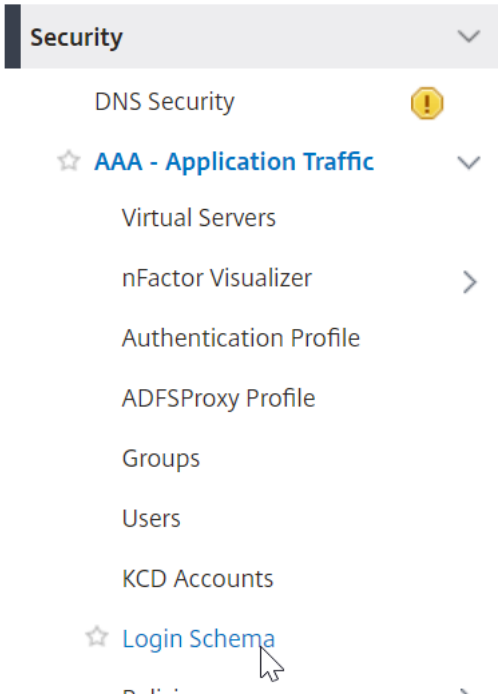
Le schéma de connexion est un fichier XML fournissant la structure des pages d'ouverture de session d'authentification basées sur des formulaires.

NFactor implique plusieurs facteurs d'authentification qui sont enchaînés ensemble. Chaque facteur peut avoir des pages/fichiers de schéma de connexion différents. Dans certains scénarios d'authentification, plusieurs écrans d'ouverture de session peuvent être présentés aux utilisateurs.

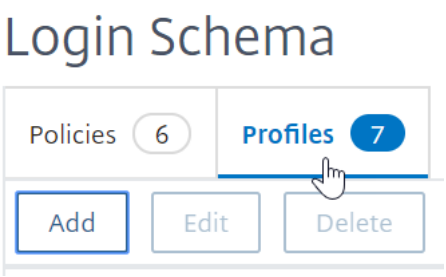
Configurer un profil de schéma de connexion

Pour configurer un profil de schéma de connexion, procédez comme suit :

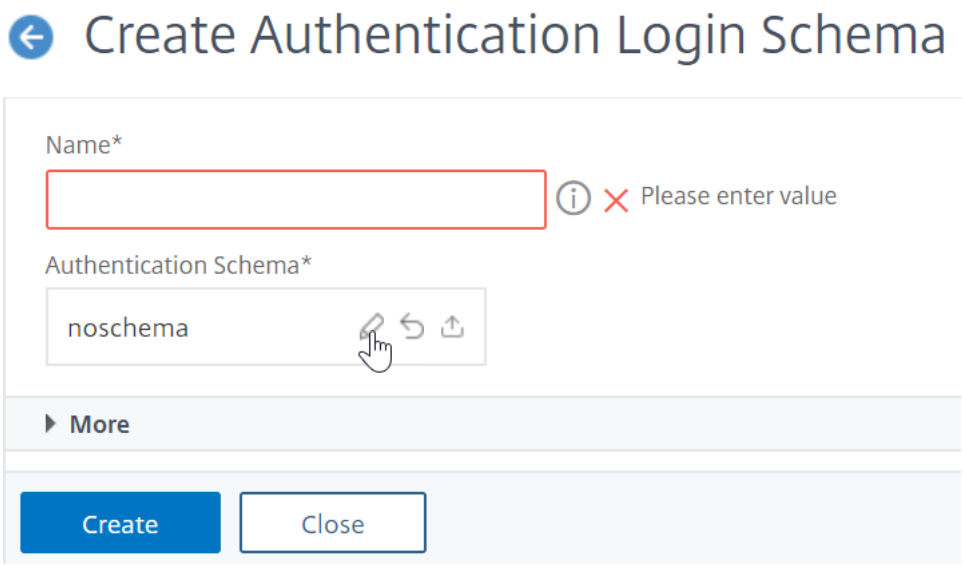
1. Créez ou modifiez un fichier .XML de schéma de connexion basé sur votre conception nFactor.
2. Accédez à **Sécurité > AAA - Trafic des applications > Schéma de connexion**.



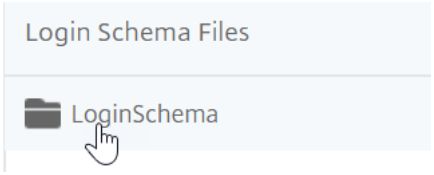
3. Sur la droite, accédez à l'onglet **Profils**, puis cliquez sur **Ajouter**.



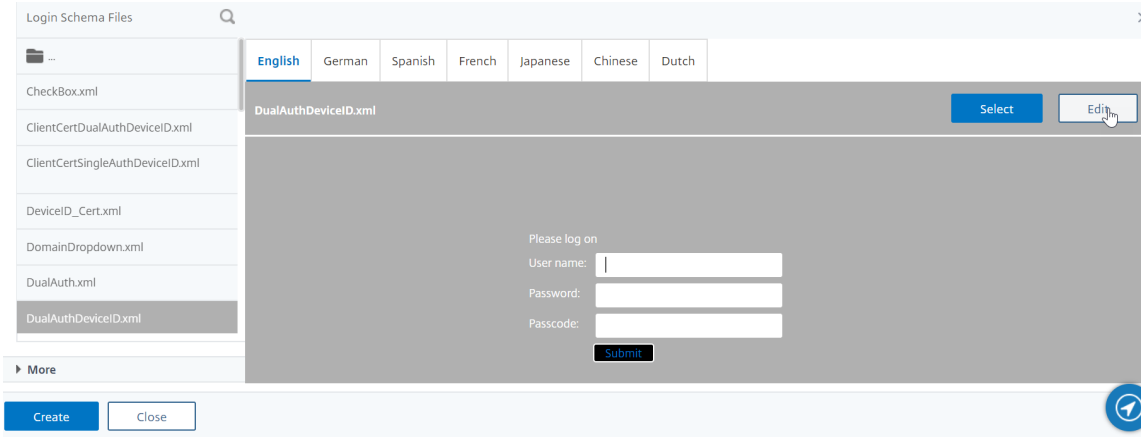
4. Dans le champ **Schéma d'authentification**, cliquez sur l'icône en forme de crayon.



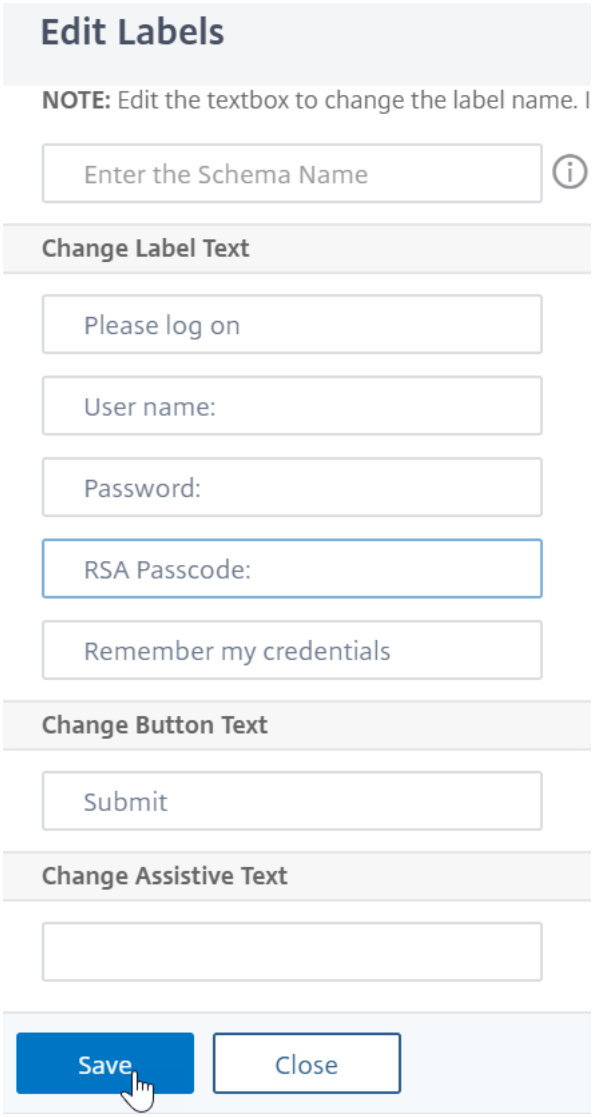
5. Cliquez sur le dossier LoginSchema pour afficher les fichiers qu'il contient.



6. Sélectionnez l'un des fichiers. Vous pouvez voir un aperçu sur la droite. Les étiquettes peuvent être modifiées en cliquant sur le bouton **Modifier** en haut à droite.

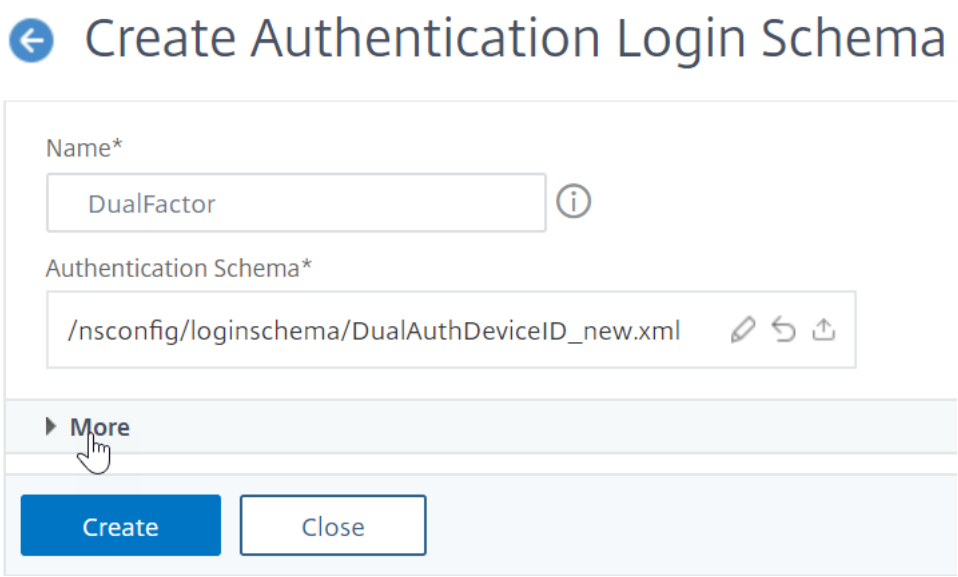


7. Lorsque vous enregistrez les modifications, un nouveau fichier est créé sous /NSconfig/loginSchema.



8. En haut à droite, cliquez sur **Sélectionner**.

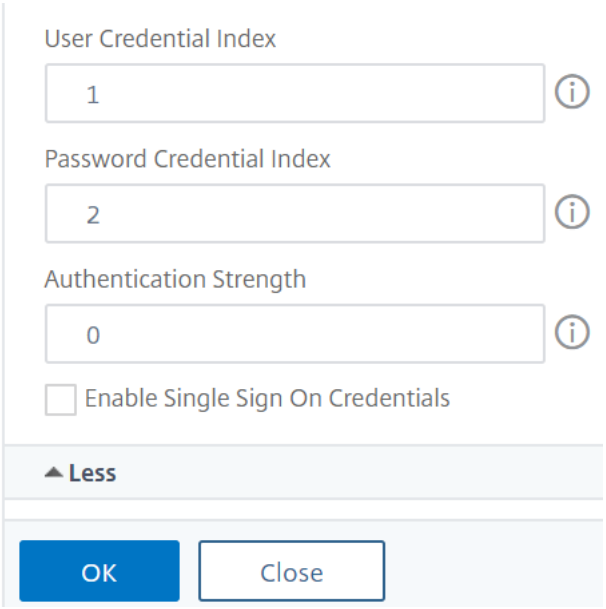
9. Donnez un nom au schéma de connexion, puis cliquez sur **Plus**.



10. Vous devrez peut-être utiliser le nom d'utilisateur et le mot de passe entrés dans le schéma de connexion pour Single Sign-On (SSO) vers un service principal, par exemple StoreFront.

    Vous pouvez utiliser les informations d'identification saisies dans le schéma de connexion comme informations d'identification Single Sign-On en utilisant l'une des méthodes suivantes.

    - Cliquez sur **Plus** en bas de la page **Créer un schéma de connexion d'authentification** et sélectionnez **Activer les informations d'identification de connexion unique**.
    - Cliquez sur **Plus** en bas de la page **Créer un schéma de connexion d'authentification** et entrez des valeurs uniques pour l'index des informations d'identification de l'utilisateur et l'index des informations d'identification de mot de passe. Ces valeurs peuvent être comprises entre 1 et 16. Plus tard, vous référencerez ces valeurs d'index dans une stratégie/un profil de trafic en utilisant l'expression AAA.USER.ATTRIBUTE (#).



11. Cliquez sur **OK** pour créer le profil de schéma de connexion.

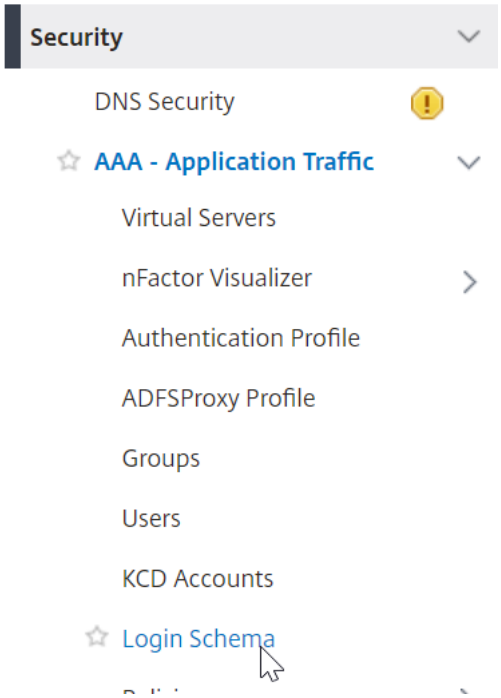
> **Remarque :** Si vous modifiez le fichier de schéma de connexion (.xml) ultérieurement, pour que les modifications soient reflétées, vous devez modifier le profil du schéma de connexion et sélectionner à nouveau le fichier de schéma de connexion (.xml).

Créer et lier une stratégie de schéma de connexion

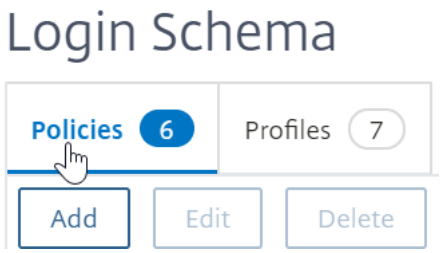
Pour lier un profil de schéma de connexion à un vServer AAA, vous devez d'abord créer une stratégie de schéma de connexion. Les stratégies de schéma de connexion ne sont pas obligatoires lorsque vous liez le profil de schéma de connexion à une étiquette de stratégie d'authentification, comme indiqué plus loin.

Pour créer et lier une stratégie de schéma de connexion, procédez comme suit :

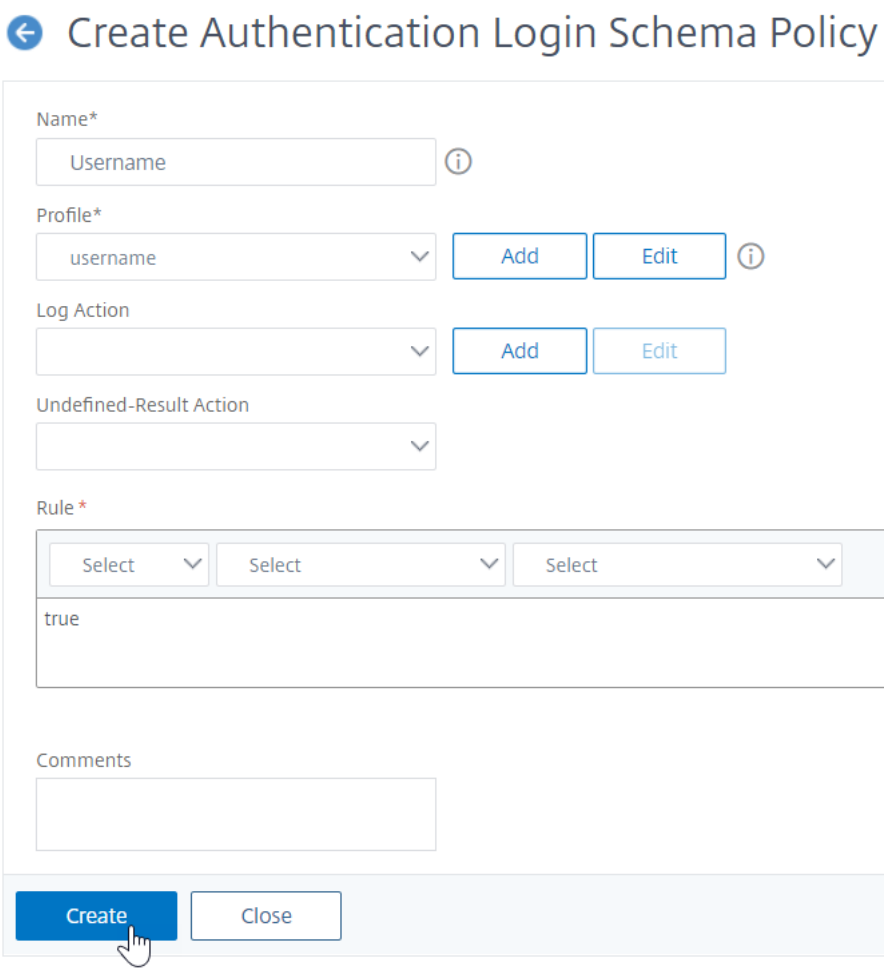
1. Accédez à **Sécurité > AAA - Trafic des applications > Schéma de connexion**.



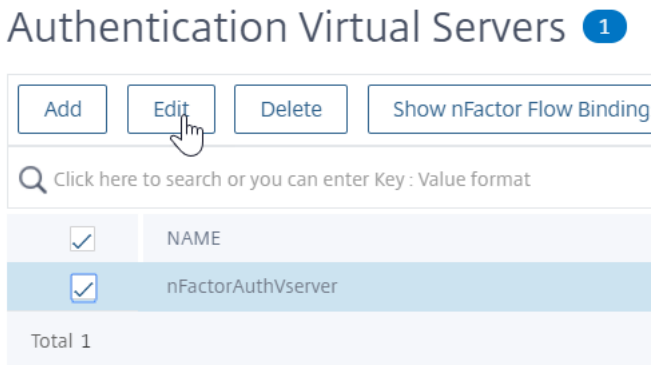
2. Dans l'onglet **Policies**, cliquez sur **Add**.



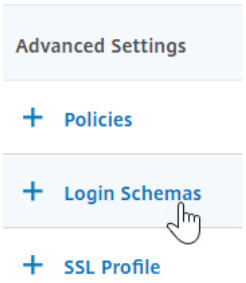
3. Utilisez le menu déroulant **Profil** pour sélectionner le profil de schéma de connexion que vous avez déjà créé.
4. Entrez une expression de stratégie avancée (par exemple, true) dans la zone **Règle**, puis cliquez sur **Créer**.



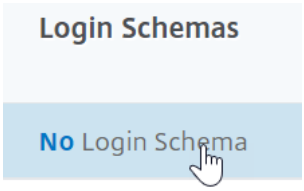
5. Sur la gauche, accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**, puis modifiez un serveur virtuel AAA existant.



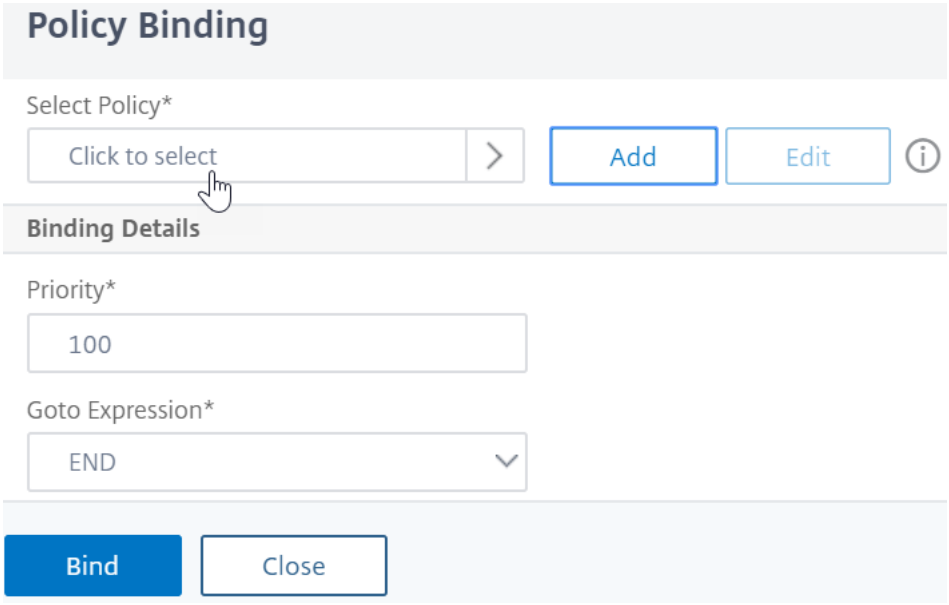
6. Dans la colonne Paramètres avancés, cliquez sur **Schémas de connexion**.



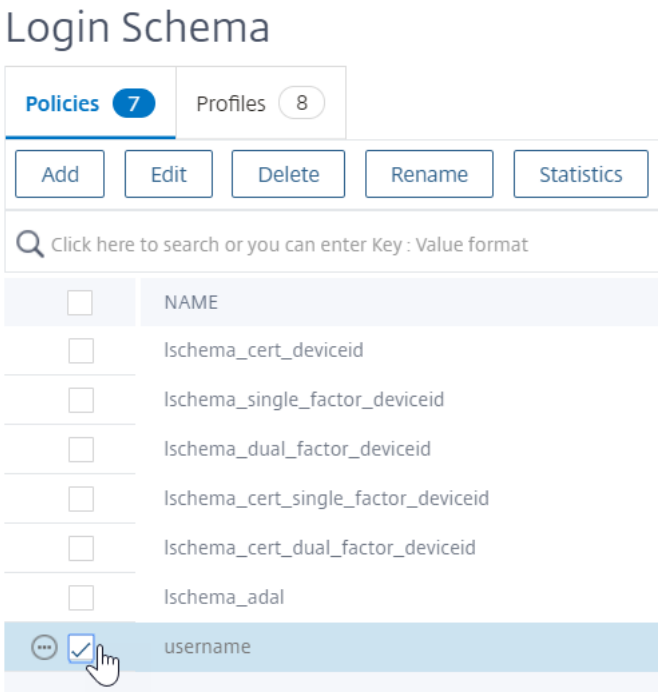
7. Dans la section Schémas de connexion, cliquez sur le texte **Aucun schéma de connexion**.



8. Cliquez sur le texte, **cliquez sur pour le sélectionner**.



9. Cliquez sur le bouton radio en regard de la stratégie de schéma de connexion, puis cliquez sur **Sélectionner**. Seules les stratégies de schéma de connexion apparaissent dans cette liste. Les profils de schéma de connexion (sans stratégie) n'apparaissent pas.



10. Cliquez sur **Bind**.

Stratégies d'authentification avancées

Les stratégies d'authentification sont une combinaison d'expression de stratégie et d'action de stratégie. Si l'expression est vraie, évaluez l'action d'authentification.

Créer des stratégies d'authentification avancées

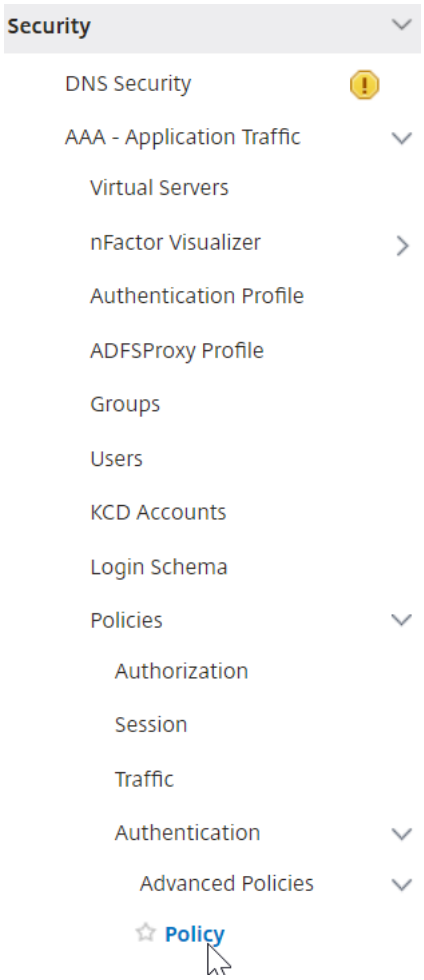
Les stratégies d'authentification sont une combinaison d'expression de stratégie et d'action de stratégie. Si l'expression est vraie, évaluez l'action d'authentification.

Vous aurez besoin d'actions/serveurs d'authentification (par exemple, LDAP, RADIUS, CERT, SAML, etc.)
Lors de la création d'une stratégie d'authentification avancée, une icône plus (Ajouter) vous permet de créer des actions/serveurs d'authentification.

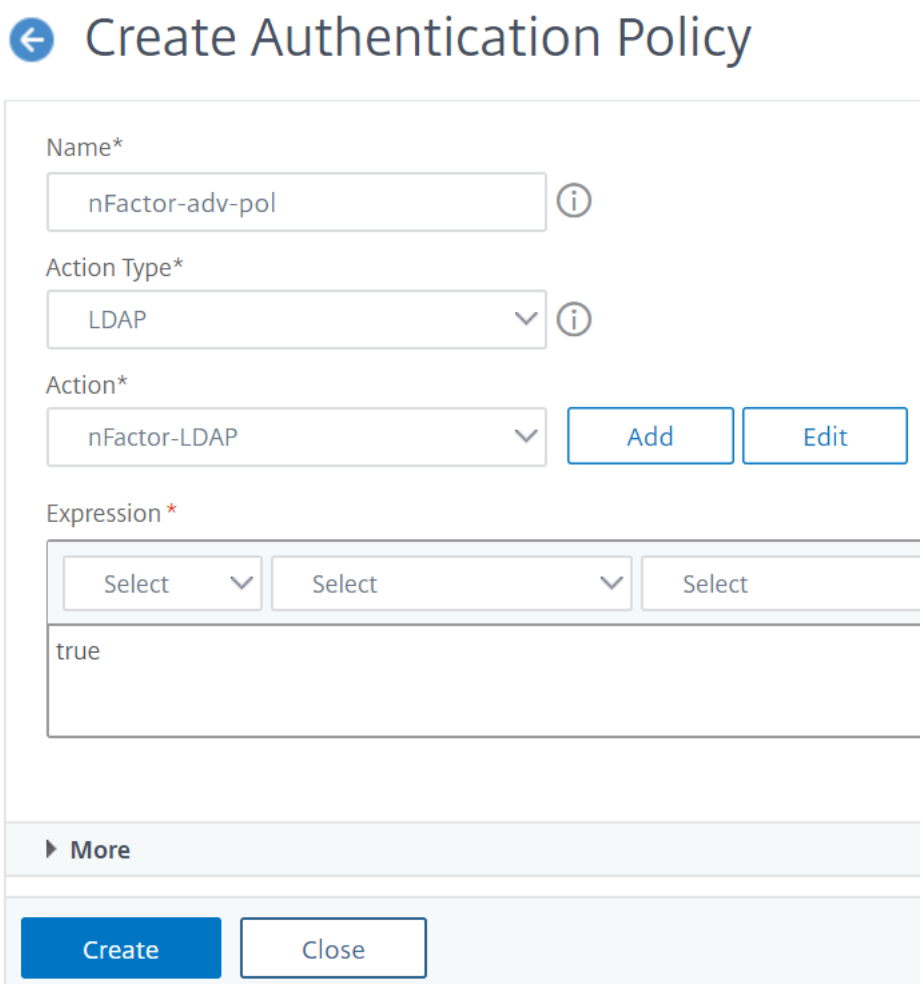
Vous pouvez également créer des actions d'authentification (serveurs) avant de créer la stratégie d'authentification avancée. Les serveurs d'authentification se trouvent sous **Authentification > Tableau de bord**. Sur la droite, cliquez sur Ajouter et sélectionnez un type de serveur. Les instructions de création de ces serveurs d'authentification ne sont pas détaillées ici. Consultez les procédures Authentification — NetScaler 12/Citrix ADC 12.1.

Pour créer une stratégie d'authentification avancée, procédez comme suit :

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Stratégie**



2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une stratégie, cliquez sur **Ajouter**.
   - Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Créer une stratégied'authentification ou Configurer la stratégie** d'authentification, tapez ou sélectionnez des valeurs pour les paramètres.



- **Nom : nom** de la stratégie. Impossible de modifier une stratégie précédemment configurée.
- **Type d'action** : type de stratégie : Cert, Negotiate, LDAP, RADIUS, SAML, SAMLIDP, TACACS ou WEBAUTH.
- **Action : action** d'authentification (profil) à associer à la stratégie. Vous pouvez choisir une action d'authentification existante ou cliquer sur le signe plus et créer une action du type approprié.
- **Action de consignation** : action d'audit à associer à la stratégie. Vous pouvez choisir une action d'audit existante ou cliquer sur le signe plus et créer une action.
  Aucune action n'est configurée. Pour créer une action, cliquez sur **Ajouter** et terminez les étapes.
- **Expression** : règle qui sélectionne les connexions auxquelles vous souhaitez appliquer l'action que vous avez spécifiée. La règle peut être simple (« true » sélectionne tout le trafic) ou complexe. Pour entrer des expressions, commencez par choisir le type d'expression dans la liste déroulante située le plus à gauche sous la fenêtre Expression, puis en tapant votre expression directement dans la zone de texte de l'expression, ou en

cliquant sur Ajouter pour ouvrir la boîte de dialogue Ajouter une expression et en utilisant les listes déroulantes qu'elle contient pour créer votre expression.)

- **Commentaire** : vous pouvez saisir un commentaire décrivant le type de trafic auquel cette stratégie d'authentification s'applique. Facultatif.

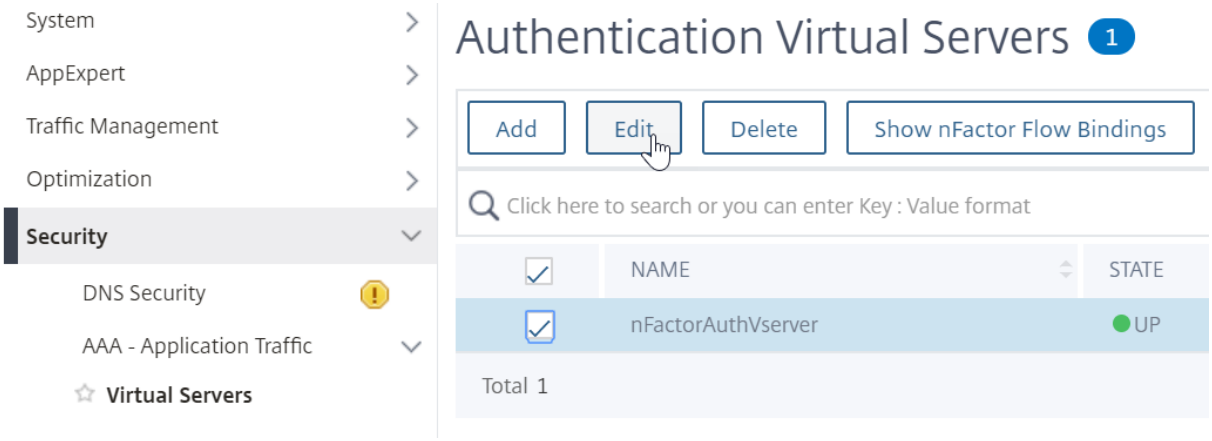
4. Cliquez sur **Create**, puis cliquez sur **Close**. Si vous avez créé une stratégie, cette stratégie apparaît dans la page Stratégies et serveurs d'authentification.

Vous devez créer des stratégies d'authentification avancées supplémentaires selon vos besoins en fonction de votre conception nFactor.

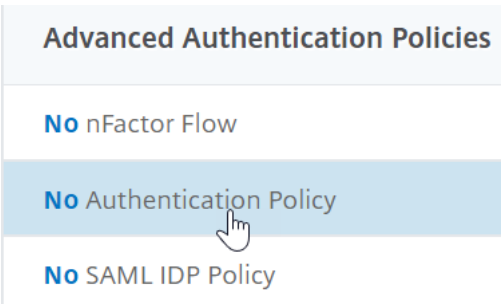
Lier la stratégie d'authentification avancée de premier facteur à Citrix ADC AAA

Vous pouvez lier directement des stratégies d'authentification avancées pour le premier serveur virtuel Factor the Citrix ADC AAA. Pour les facteurs suivants, vous devez lier les stratégies d'authentification avancées aux étiquettes de stratégie d'authentification.

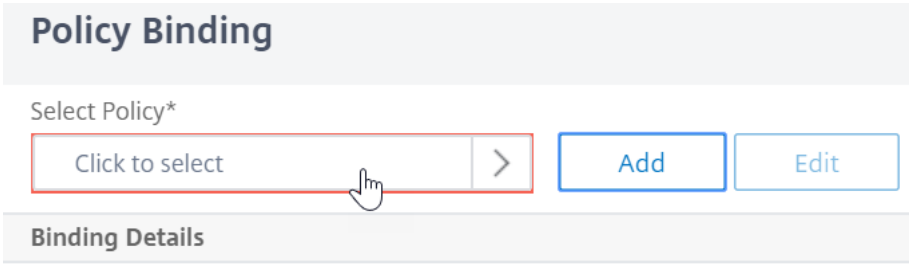
1. Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**. Modifiez un serveur virtuel existant.



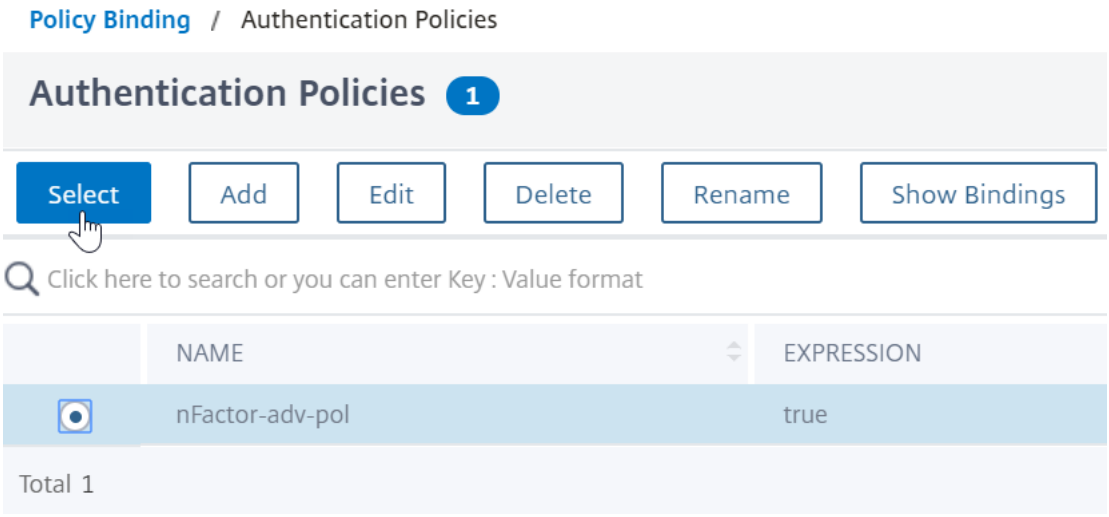
1. Sur la gauche, dans la section Stratégies d'authentification avancées, cliquez sur **Aucune stratégie d'authentification**.



2. Dans **Sélectionner une stratégie**, cliquez sur le texte, **cliquez sur pour sélectionner**.

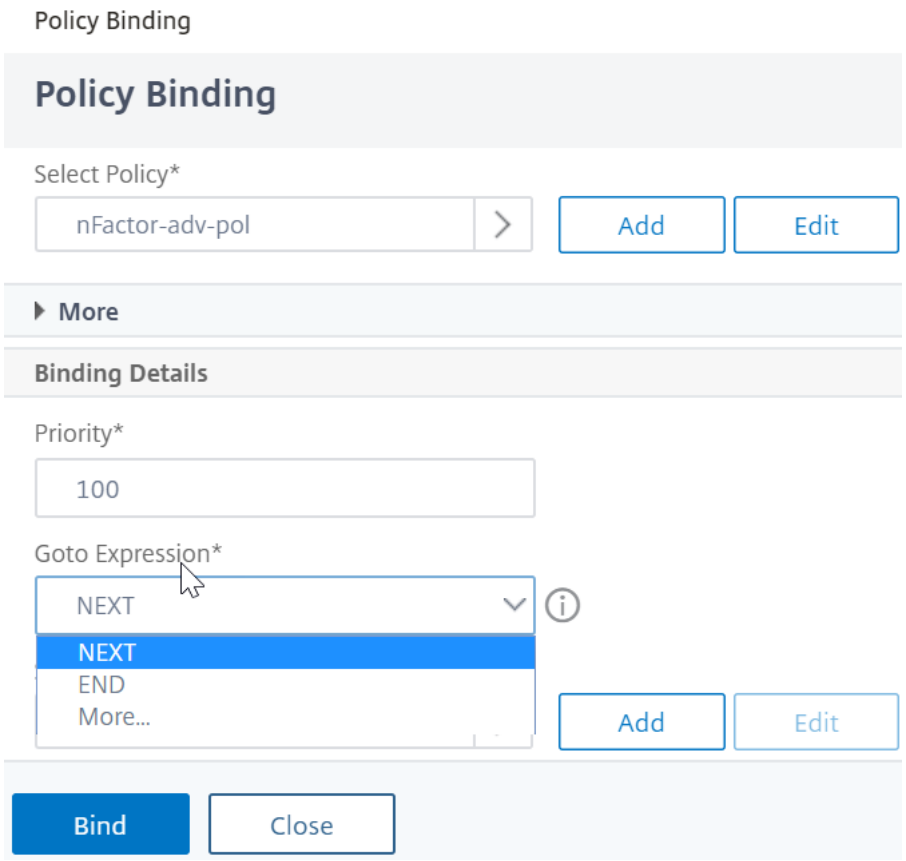


3. Cliquez sur le bouton radio en regard de la **stratégie d'authentification avancée**, puis cliquez sur **Sélectionner**.

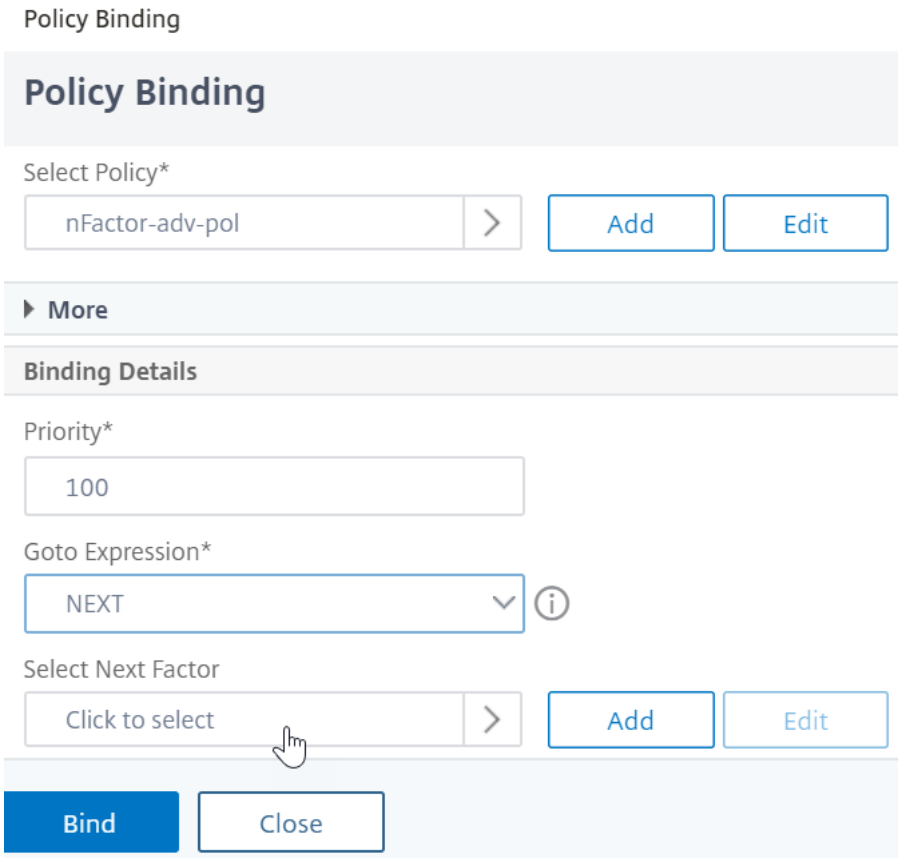


4. Dans la section Détails de la liaison, l' **expression Goto** détermine ce qui se passe ensuite si cette stratégie d'authentification avancée échoue.

   - Si **Goto Expression** est défini sur **NEXT**, la stratégie d'authentification avancée suivante liée à ce serveur virtuel Citrix ADC AAA est évaluée.
   - Si **Goto Expression** est défini sur **END**, ou si aucune stratégie d'authentification avancée n'est liée à ce serveur virtuel AAA Citrix ADC, l'authentification est terminée et marquée comme ayant échoué.



5. Dans **Sélectionner le facteur suivant**, vous pouvez sélectionner peut pointer vers une étiquette de stratégie d'authentification. Le facteur suivant est évalué uniquement si la stratégie d'authentification avancée réussit. Enfin, cliquez sur **Bind**.



Utiliser les groupes LDAP extraits pour sélectionner le facteur d'authentification suivant

Vous pouvez utiliser les groupes LDAP extraits pour sélectionner le prochain facteur d'authentification sans authentifier réellement avec LDAP.

1. Lorsque vous créez ou modifiez un serveur LDAP ou une action LDAP, désactivez la case à cocher **Authentification** .
2. Dans **Autres paramètres**, sélectionnez les valeurs appropriées dans **Attribut de groupe** et **Nom de sous-attribut**.

Authentification de l'étiquette de stratégie

Lorsque vous liez une stratégie d'authentification avancée au serveur virtuel AAA Citrix ADC et que vous avez sélectionné un facteur suivant, le facteur suivant est évalué uniquement si la stratégie d'authentification avancée est sélectionnée. Le prochain facteur qui est évalué est une étiquette de stratégie d'authentification.

L'étiquette de stratégie d'authentification spécifie un ensemble de stratégies d'authentification pour un facteur particulier. Chaque étiquette de stratégie correspond à un seul facteur. Il spécifie également le formulaire de connexion qui doit être présenté à l'utilisateur. L'étiquette de stratégie

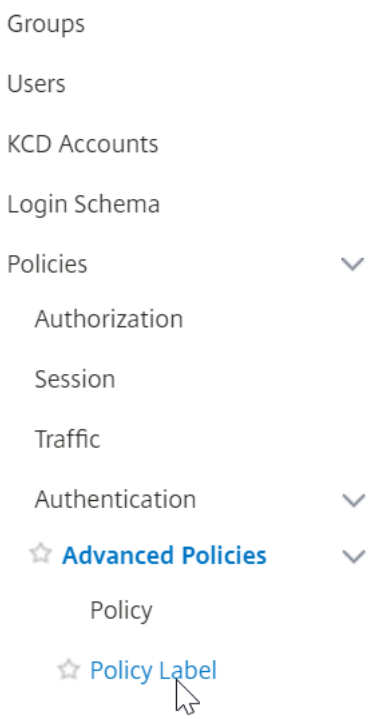
d'authentification doit être liée en tant que facteur suivant d'une stratégie d'authentification ou d'une autre étiquette de stratégie d'authentification.

Remarque : Chaque facteur n'a pas besoin d'un schéma de connexion. Le profil de schéma de connexion n'est requis que si vous liez un schéma de connexion à une étiquette de stratégie d'authentification.

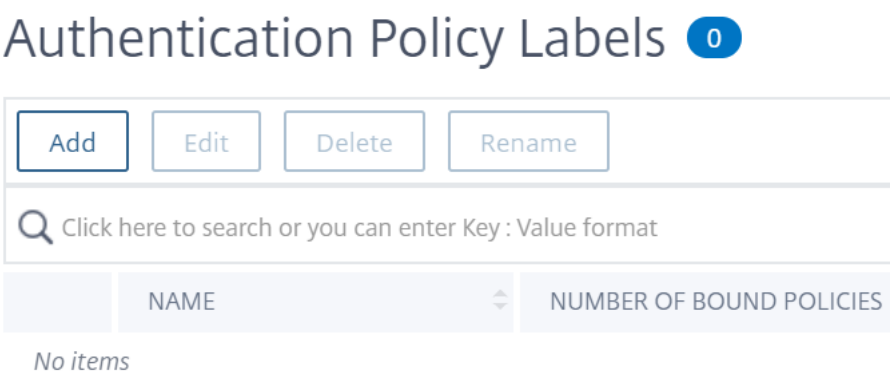
Créer une étiquette de stratégie d'authentification

Une étiquette de stratégie spécifie les stratégies d'authentification pour un facteur particulier. Chaque étiquette de stratégie correspond à un seul facteur. L'étiquette de stratégie spécifie le formulaire de connexion qui doit être présenté à l'utilisateur. L'étiquette de stratégie doit être liée en tant que facteur suivant d'une stratégie d'authentification ou d'une autre étiquette de stratégie d'authentification. En règle générale, une étiquette de stratégie inclut des stratégies d'authentification pour un mécanisme d'authentification spécifique. Toutefois, vous pouvez également avoir une étiquette de stratégie qui comporte des stratégies d'authentification pour différents mécanismes d'authentification.

1. Accédez à **Sécurité > AAA — Trafic des applications > Stratégies > Authentification > Stratégies avancées > Libellé de stratégie**.



2. Cliquez sur le bouton **Add**.

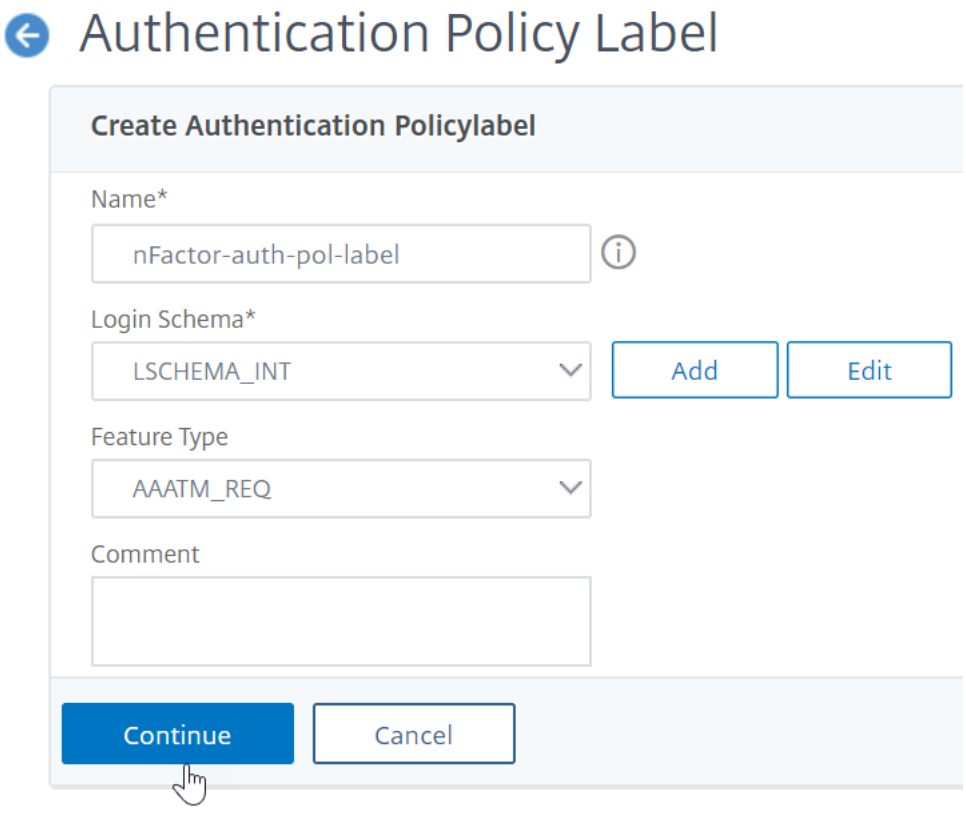


3. Remplissez les champs suivants pour créer une étiquette de stratégie d'authentification :

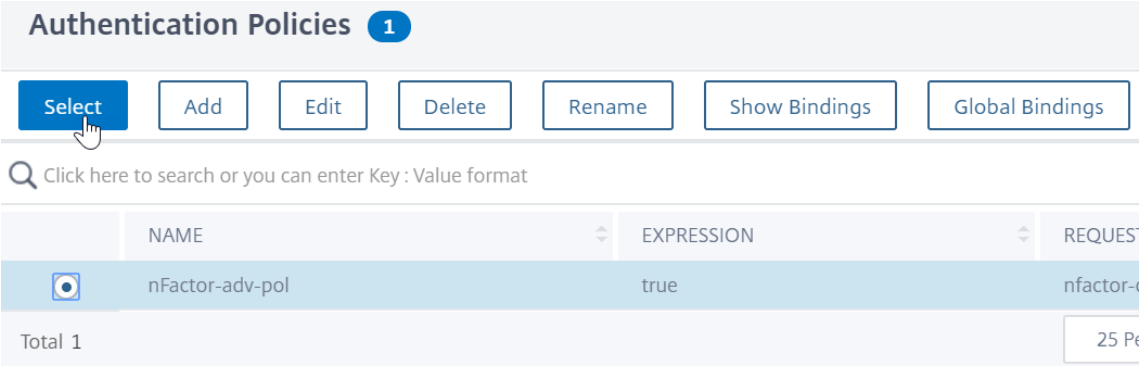
   a) Entrez le **nom de** la nouvelle étiquette de stratégie d'authentification.

   b) Sélectionnez le **schéma de connexion** associé à l'étiquette de stratégie d'authentification. SI vous ne souhaitez rien afficher à l'utilisateur, vous pouvez sélectionner un profil de schéma de connexion défini sur noschema (LSCHEMA_INT).

   c) Cliquez sur **Continuer**.



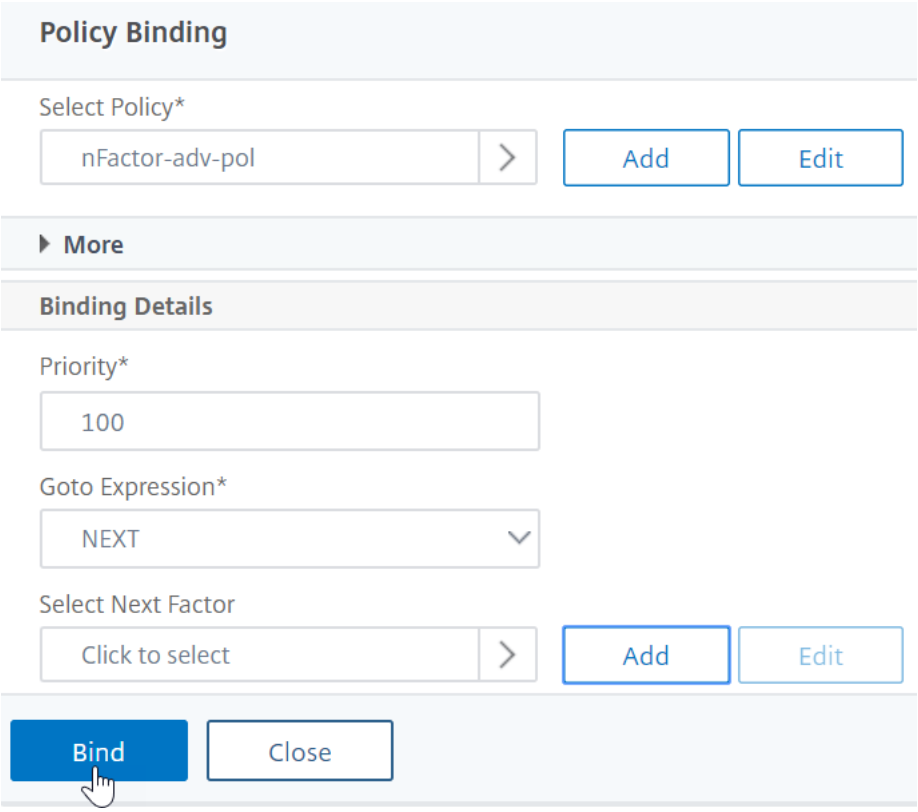
4. Dans **la section Liaison de stratégie**, cliquez à l'endroit où il est indiqué **Cliquez pour sélectionner**.
5. Sélectionnez la stratégie d'authentification qui évalue ce facteur.



6. Renseignez les champs suivants :

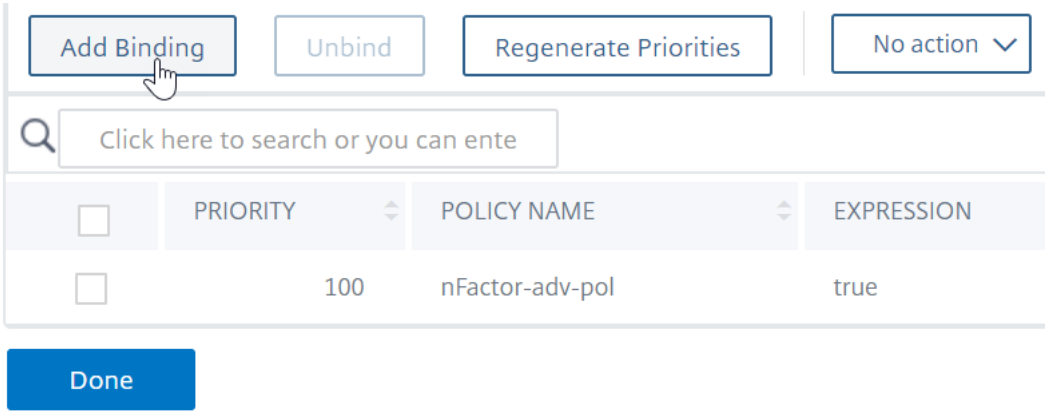
   a) Entrez la **priorité** de la liaison de stratégie.

   b) Dans **Goto Expression**, sélectionnez **SUIVANT** si vous souhaitez lier des stratégies d'authentification plus avancées à ce facteur ou sélectionnez **FIN**.



7. Dans **Sélectionner le facteur suivant**, si vous souhaitez ajouter un autre facteur, cliquez sur pour sélectionner et lier l'étiquette de stratégie d'authentification suivante (facteur suivant). Si vous ne sélectionnez pas le facteur suivant, et si cette stratégie d'authentification avancée réussit, l'authentification est réussie et terminée.
8. Cliquez sur **Bind**.
9. Vous pouvez cliquer sur **Ajouter une liaison** pour ajouter des stratégies d'authentification plus

avancées à cette étiquette de stratégie (facteur). Cliquez sur **Terminé lorsque vous avez** terminé.



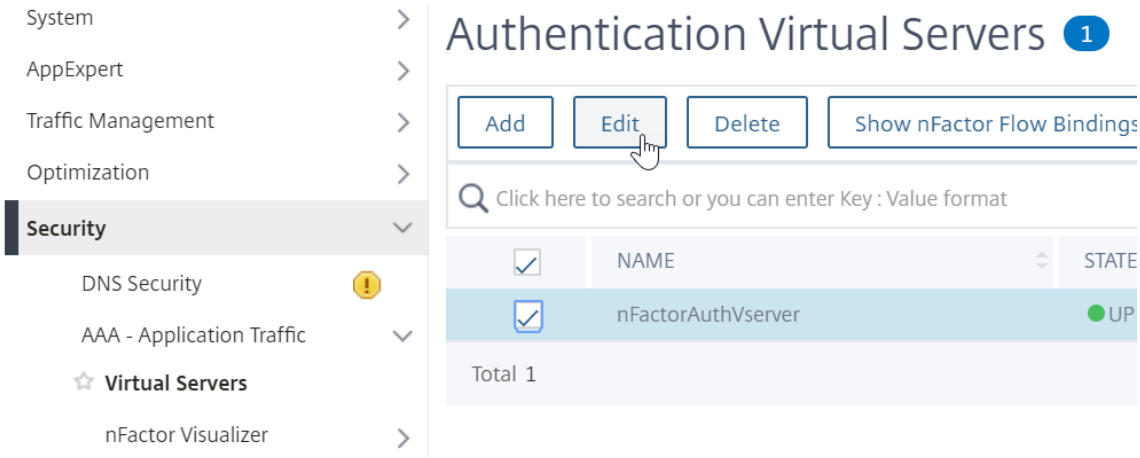
Libellé de stratégie d'authentification de liaison

Une fois que vous avez créé l'étiquette de stratégie, vous la liez à une stratégie d'authentification avancée existante qui lie les facteurs de chaîne ensemble.

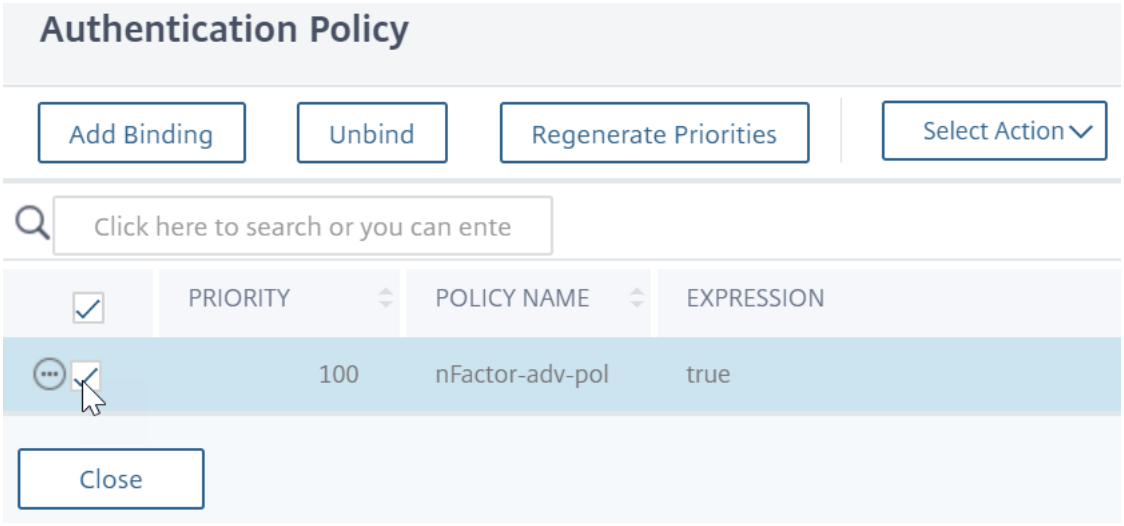
Vous pouvez sélectionner le facteur suivant lorsque vous modifiez un serveur virtuel Citrix ADC AAA existant auquel une stratégie d'authentification avancée est liée ou lorsque vous modifiez une étiquette de stratégie différente pour inclure le facteur suivant.

Pour modifier un serveur virtuel Citrix ADC AAA existant auquel une stratégie d'authentification avancée est déjà liée

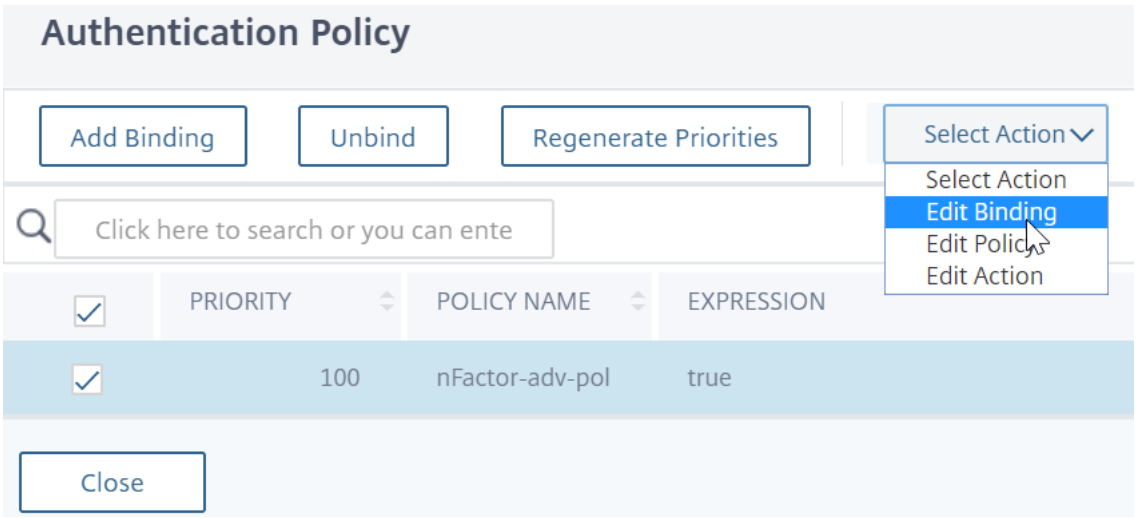
1. Accédez à **Sécurité > AAA — Trafic des applications > Serveurs virtuels.** Sélectionnez le serveur virtuel et cliquez sur **Modifier**.



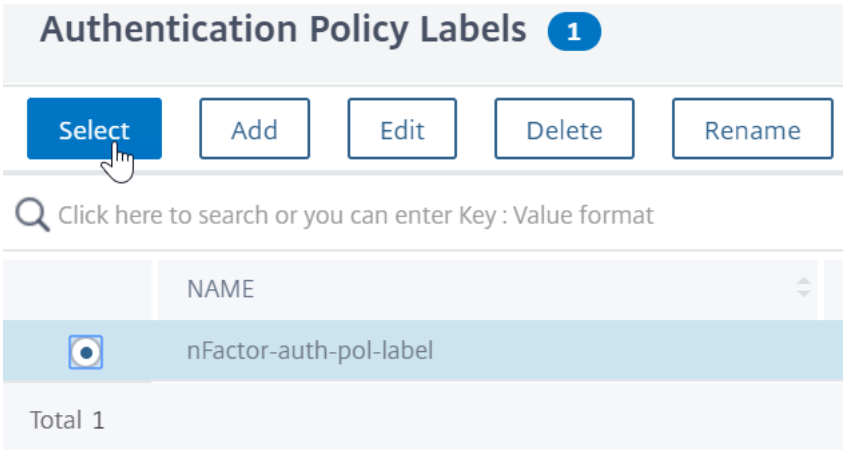
2. Sur la gauche, dans la section **Stratégies d'authentification avancées**, cliquez sur une liaison de stratégie d'authentification existante.



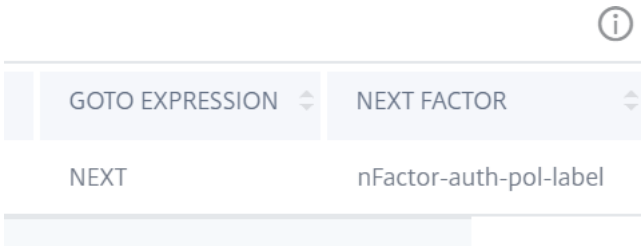
3. Dans **Sélectionner une action**, cliquez sur **Modifier la liaison**.



4. Dans **Sélectionner le facteur suivant**, cliquez sur, puis sélectionnez une étiquette de stratégie d'authentification existante (facteur suivant).

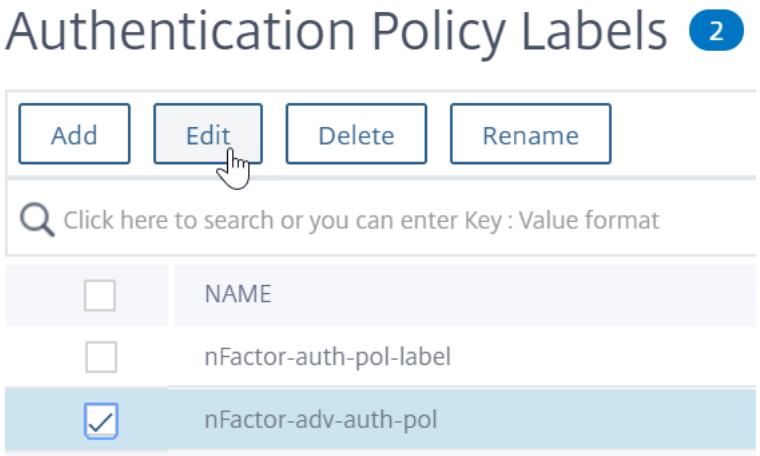


5. Cliquez sur **Bind**. Vous pouvez voir le facteur suivant à l'extrême droite.

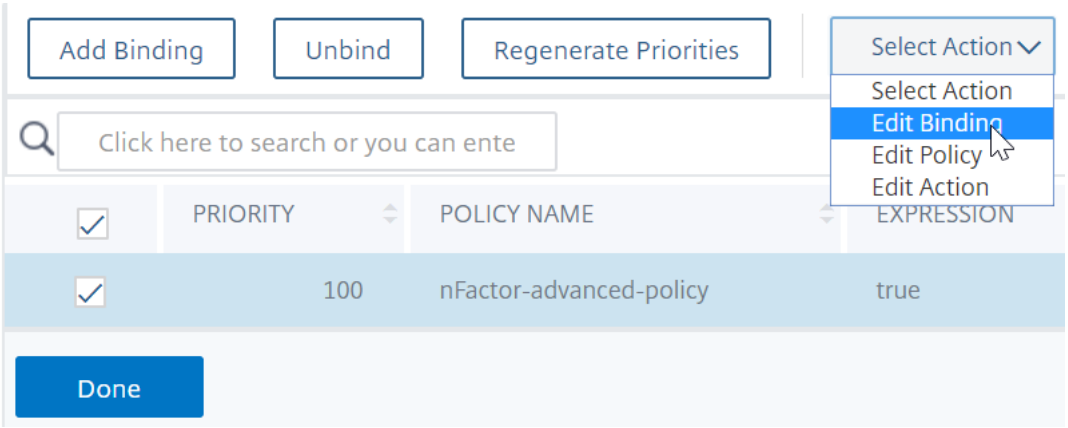


Pour ajouter un facteur suivant d'étiquette de stratégie à un autre libellé de stratégie

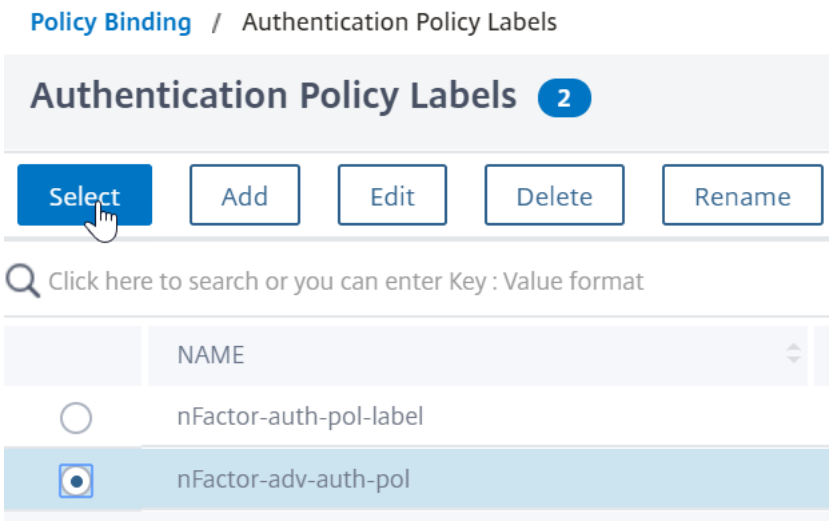
1. Accédez à **Sécurité > AAA — Trafic des applications > Stratégies > Authentification > Stratégies avancées > Libellé de stratégie**. Sélectionnez un autre libellé de stratégie, puis cliquez sur **Modifier.**



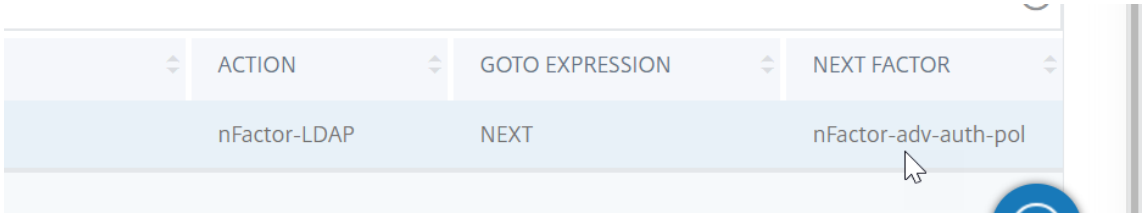
2. Dans **Sélectionner une action**, cliquez sur **Modifier la liaison**.



3. Dans **Détails de la liaison > Sélectionner le facteur suivant**, cliquez sur pour sélectionner le facteur suivant.
4. Choisissez le libellé de stratégie pour le facteur suivant, puis cliquez sur le bouton **Sélectionner** .



5. Cliquez sur **Bind.** Vous pouvez voir le facteur suivant sur la droite.

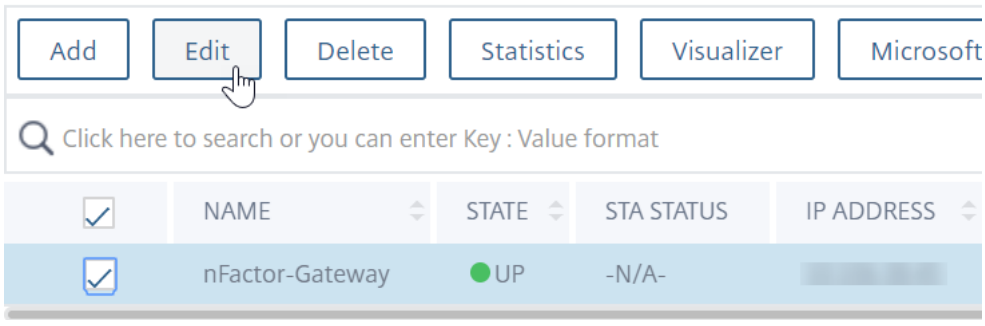


nFactor pour Citrix Gateway

Pour activer nFactor sur Citrix Gateway, un profil d'authentification doit être lié à un serveur virtuel Citrix ADC AAA.

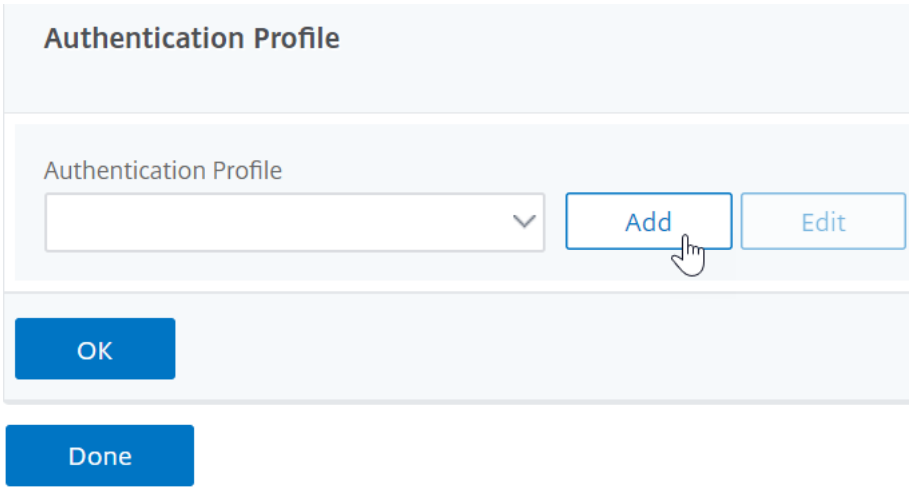
Créer un profil d'authentification pour lier un serveur virtuel Citrix ADC AAA au serveur virtuel Citrix Gateway

1. Accédez à **Citrix Gateway > Serveurs virtuels** et sélectionnez un serveur virtuel de passerelle existant à modifier.

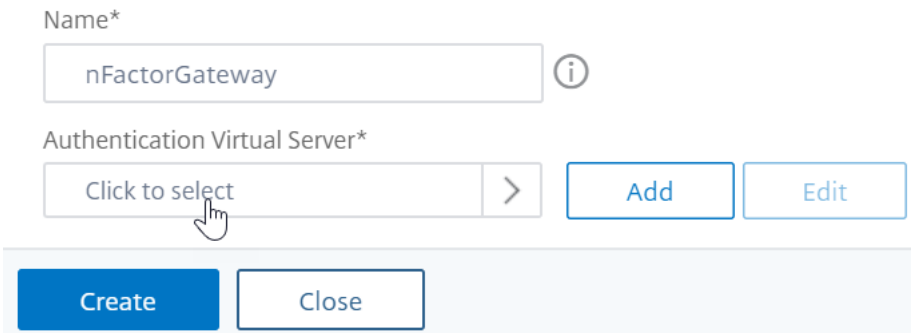


2. Dans **les paramètres avancés**, cliquez sur **Profil d'authentification**.

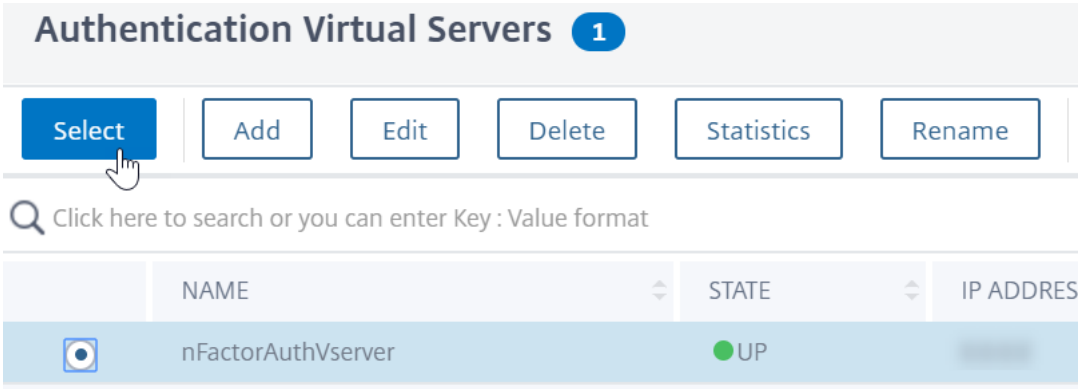
3. Cliquez sur **Ajouter** sous **Profil d'authentification**



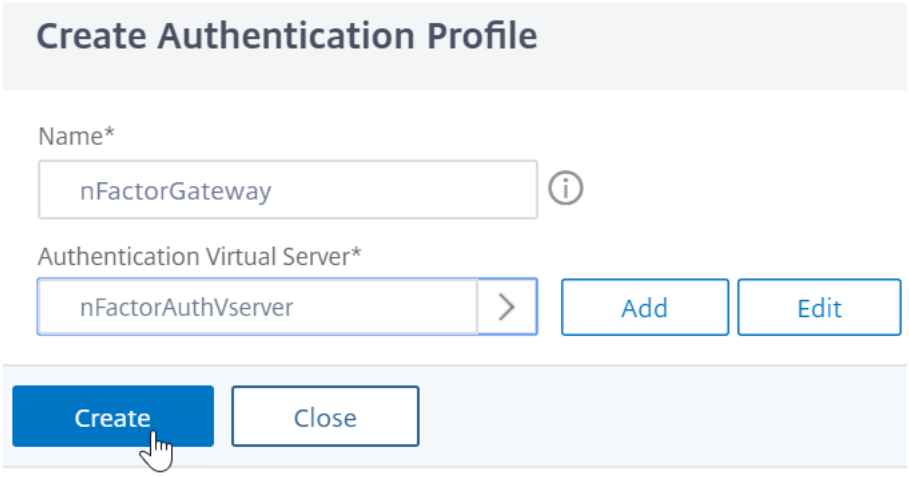
4. Entrez le nom du profil d'authentification et cliquez à l'endroit où il est indiqué **Cliquez pour sélectionner**.



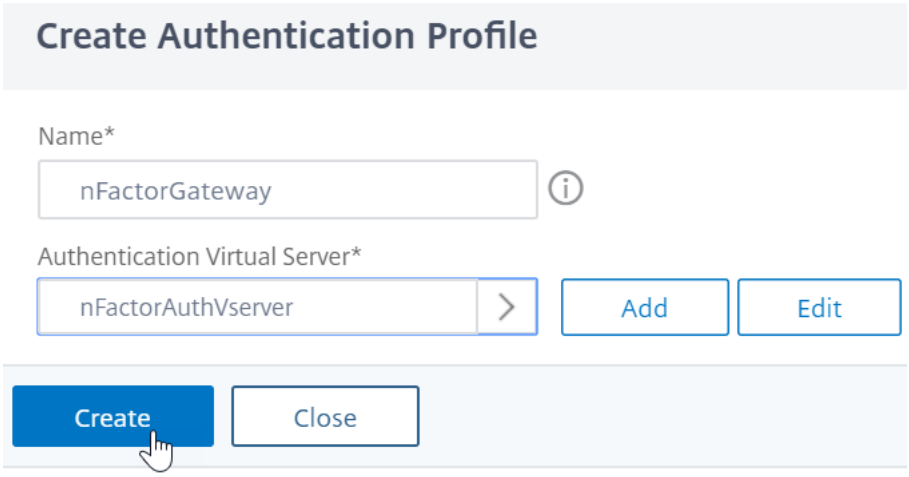
5. Dans **Authentication Virtual Server**, sélectionnez un serveur existant dont le schéma de connexion, la stratégie d'authentification avancée et les étiquettes de stratégie d'authentification sont configurés. Vous pouvez également créer un serveur virtuel d'authentification. Le serveur virtuel Citrix ADC AAA n'a pas besoin d'adresse IP. Cliquez sur **Sélectionner**.



6. Cliquez sur **Create**.



7. Cliquez sur **OK** pour fermer la section Profil d'authentification.



Remarque : Si vous avez configuré l'un des facteurs en tant que certificats client, vous devez configurer les paramètres SSL et le certificat d'autorité de certification.

Une fois que vous avez terminé de lier le profil d'authentification à un serveur virtuel AAA et que vous accédez à votre Citrix Gateway, vous pouvez afficher les écrans d'authentification nFactor.

Configuration des paramètres SSL et du certificat d'autorité de certification

Si l'un des facteurs d'authentification est un certificat, vous devez effectuer une configuration SSL sur le serveur virtuel Citrix Gateway.

1. Accédez à **Gestion du trafic > SSL > Certificats > Certificats d'autorité**de certification, puis installez le certificat racine de l'émetteur des certificats clients. Les certificats d'autorité de certification n'ont pas besoin de fichiers clés.

   Si les profils SSL par défaut sont activés, vous devez avoir déjà créé un profil SSL pour lequel l'authentification client est activée.

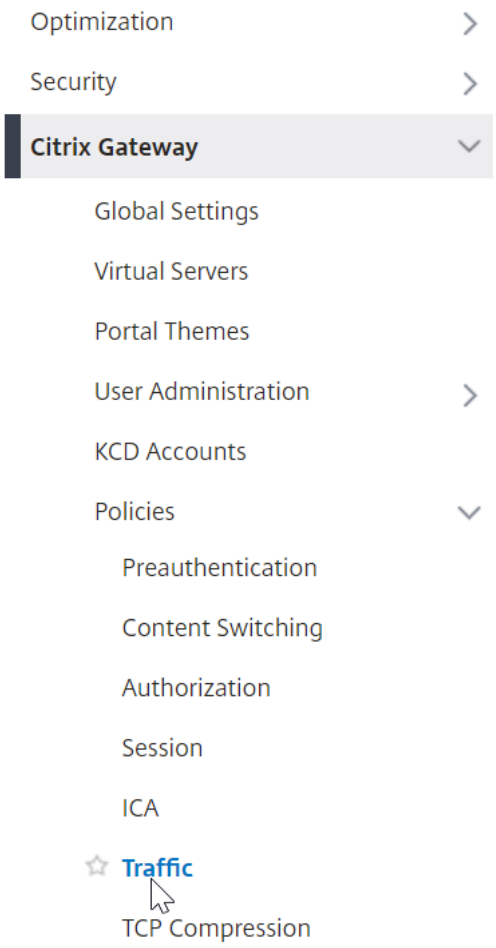
2. Accédez à **Citrix Gateway > Serveurs virtuels**et modifiez un serveur virtuel Citrix Gateway existant qui est activé pour nFactor.
    - Si les profils SSL par défaut sont activés, cliquez sur l'icône de modification.
    - Dans la liste Profil SSL, sélectionnez le profil SSL pour lequel l'authentification du client est activée et définie sur FACULTATIF.
    - Si les profils SSL par défaut ne sont pas activés, cliquez sur l'icône de modification.
    - Cochez la case Authentification du client.
    - Assurez-vous que le certificat client est défini sur Facultatif
3. Cliquez sur OK.
4. Dans la section Certificats, cliquez sur **Aucun certificat d'autorité de certification.**
5. Dans Sélectionner un certificat d'autorité de certification, cliquez sur pour sélectionner et sélectionner le certificat racine de l'émetteur des certificats clients.
6. Cliquez sur Bind.

Remarque : Il se peut que vous deviez également lier tous les certificats d'autorité de certification intermédiaires qui ont émis les certificats clients.

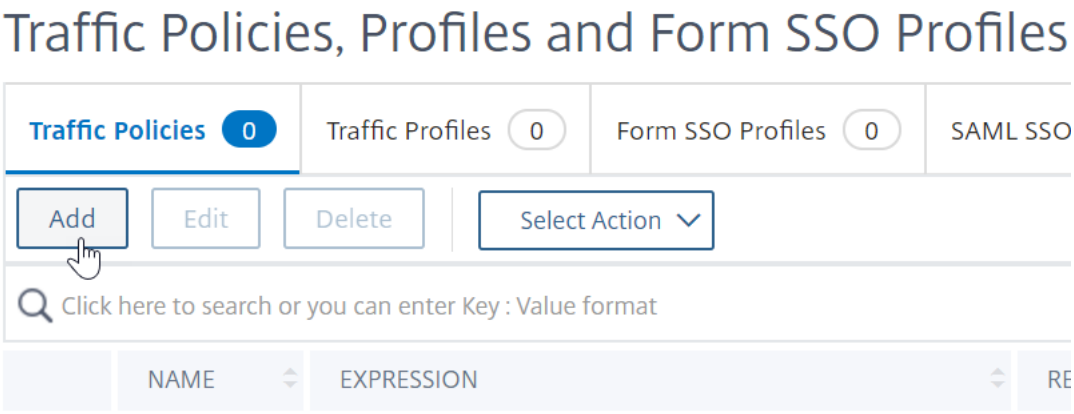
Configurer la stratégie de trafic Citrix Gateway pour l'authentification unique nFactor vers StoreFront

Pour l'authentification unique à StoreFront, nFactor utilise par défaut le dernier mot de passe saisi. Si LDAP n'est pas le dernier mot de passe saisi, vous devez créer une stratégie/un profil de trafic pour remplacer le comportement par défaut de NFactor.

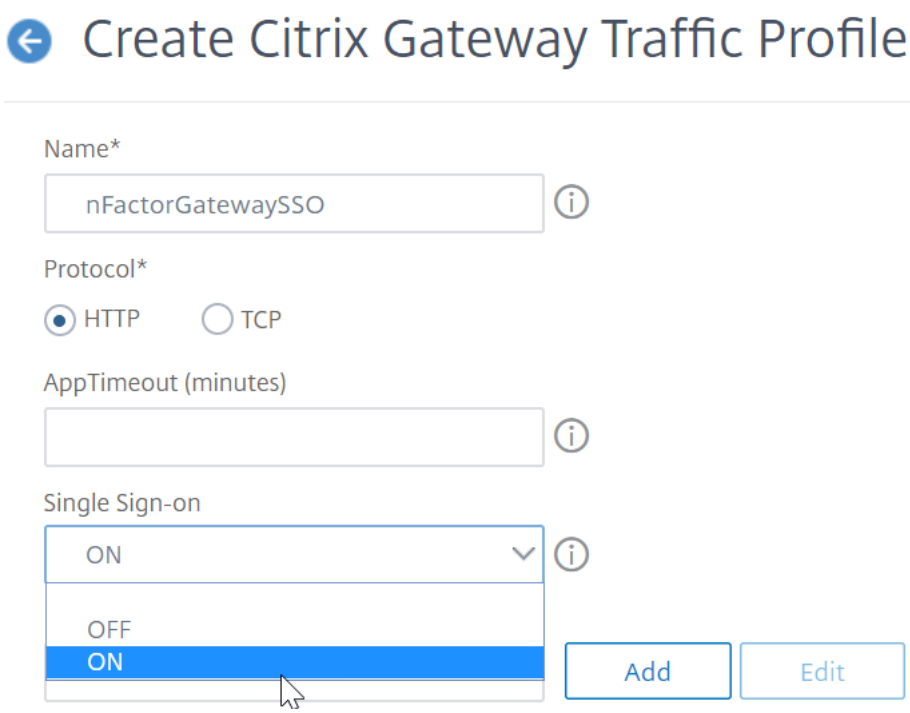
1. Accédez à **Citrix Gateway > Stratégies > Trafic**.



2. Dans l'onglet **Profils de trafic**, cliquez sur **Ajouter**.

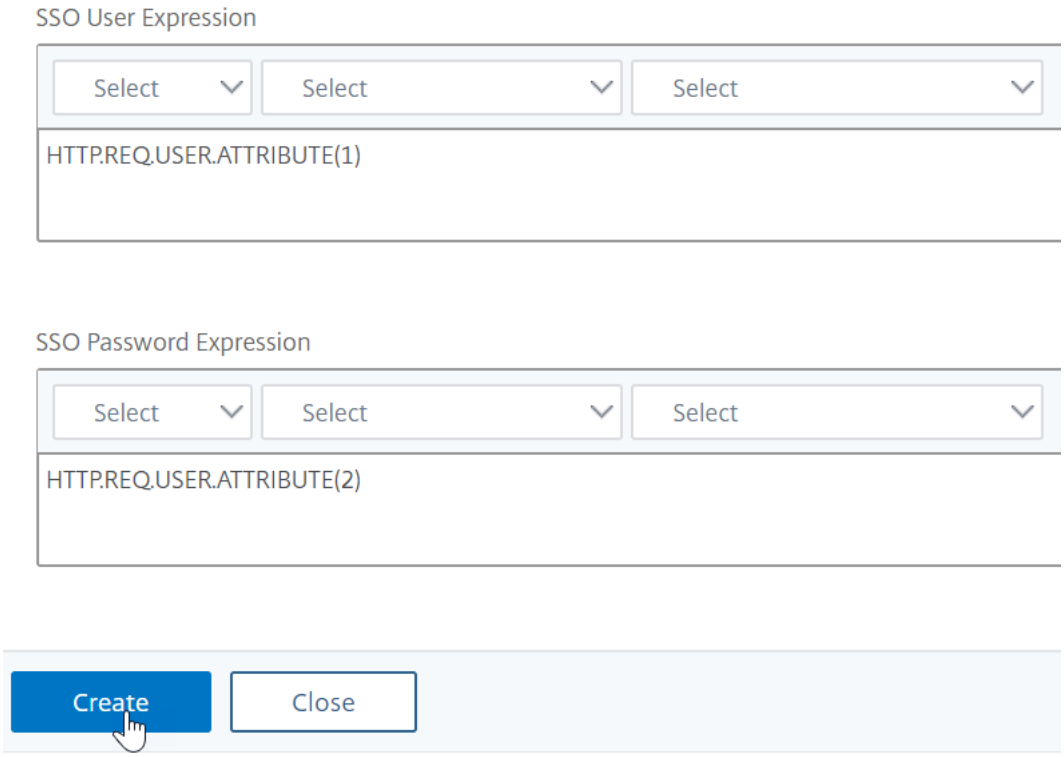


3. Entrez le nom du profil de trafic. Sélectionnez le protocole **HTTP** .
   Dans **Single Sign-on**, sélectionnez **ON**.



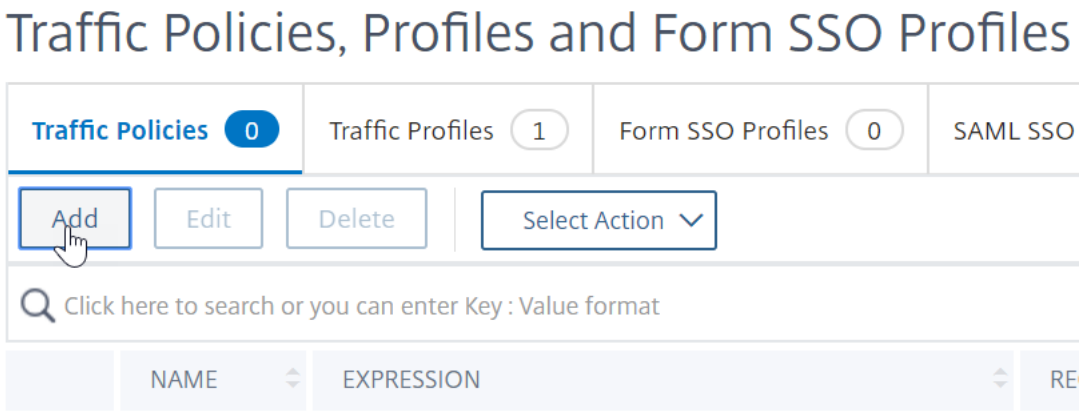
4. Dans l' **expression SSO**, entrez une expression AAA.USER.ATTRIBUTE (#) qui correspond aux index spécifiés dans le schéma de connexion, puis cliquez sur **Créer**.

> **Remarque :**
> L'expression AAA.USER est maintenant implémentée pour remplacer les expressions HTTP.REQ.USER obsolètes.



5. Cliquez sur **l'onglet Stratégies de trafic**, puis sur **Ajouter**.

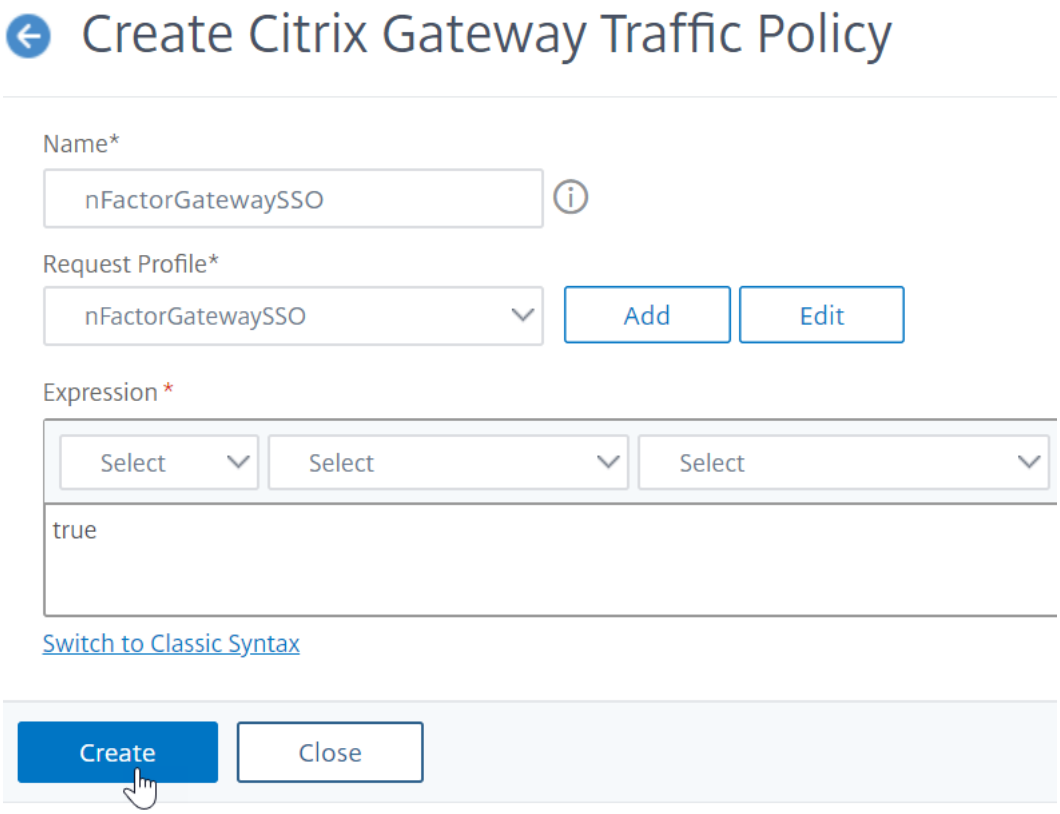
   Entrez un nom pour la stratégie.
   Sélectionnez le profil de trafic créé à l'étape précédente.
   Dans **Expression**, saisissez une expression avancée, par exemple true.
   Cliquez sur **Créer**.



6. Accédez à **Citrix Gateway > Citrix Gateway Virtual Server**.

   - Sélectionnez un serveur virtuel existant et cliquez sur **Modifier**.
   - Dans la section **Politiques**, cliquez sur le signe **+** .
   - Dans **Choisir une stratégie**, sélectionnez **Trafic**.
   - Dans **Choisir le type**, sélectionnez **Demande**.

- Sélectionnez la stratégie de trafic que vous avez créée, puis cliquez sur **Liaison**.



Exemple d'extrait de code sur la configuration nFactor à l'aide de l'interface de ligne de commande Citrix ADC

Pour comprendre les configurations pas à pas de l'authentification nFactor, considérons un déploiement d'authentification à deux facteurs dans lequel le premier facteur est l'authentification LDAP et le second est l'authentification RADIUS.

Cet exemple de déploiement nécessite que l'utilisateur se connecte aux deux facteurs à l'aide d'un seul formulaire de connexion. Par conséquent, nous définissons un formulaire de connexion unique qui accepte deux mots de passe. Le premier mot de passe est utilisé pour l'authentification LDAP et l'autre pour l'authentification RADIUS.
Voici les configurations qui sont effectuées :

1. Configurer le serveur virtuel d'équilibrage de charge pour l'authentification

   ajouter lb vserver lbvs89 HTTP 1.136.19.55 80 -AuthenticationHost auth56.aaatm.com -Authentication ON

2. Configurez le serveur virtuel d'authentification.

   ajouter authentification vserver auth56 SSL 10.106.30.223 443 - AuthenticationDomain aaatm.com

3. Configurez le schéma de connexion pour le formulaire de connexion et liez-le à une stratégie de schéma de connexion.

   add authentication loginSchema login1 -authenticationSchema login-2passwd.xml -userCredentialIndex 1 -passwordCredentialIndex 2

   > **Remarque**
   >
   > Vous devrez peut-être utiliser le nom d'utilisateur et l'un des mots de passe entrés dans le schéma de connexion pour Single Sign-On (SSO) vers un service principal, par exemple StoreFront. Vous pouvez référencer ces valeurs d'index dans l'action de trafic en utilisant l'expression AAA.USER.ATTRIBUTE (#). Les valeurs peuvent être comprises entre 1 et 16.
   >
   > Vous pouvez également utiliser les informations d'identification saisies dans le schéma de connexion comme informations d'identification Single Sign-On à l'aide de la commande suivante.
   >
   > **add authentication loginSchema** login1 -authenticationSchema login-2passwd.xml -SSOCredentials YES

   add authentication loginSchemaPolicy login1 -rule true -action login1

4. Configurez un schéma de connexion pour le relais et liez-le à une étiquette de stratégie

   add authentication loginSchema login2 -authenticationSchema noschema

   add authentication policylabel label1 -loginSchema login2

5. Configurez les stratégies LDAP et RADIUS.

   add authentication ldapAction ldapAct1 -serverIP 10.17.103.28 -ldapBase "dc=aaatm, dc=com" -ldapBindDn administrator@aaatm.com -ldapBindDnPassword 81qw1b99ui971mn1289op1abc125 -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName samAccountName -groupAttrName memberOf -subAttributeName CN

   add authentication Policy ldap -rule true -action ldapAct1

   add authentication radiusAction radius -serverIP 10.101.14.3 -radKey n231d9a8cao8671or4a9ace940d8623 -encrypted -encryptmethod ENCMTHD_3 -radNASip ENABLED -radNASid NS28.50 -radAttributeType 11 -ipAttributeType 8

   add authentication Policy radius -rule true -action radius

6. Liez la stratégie de schéma de connexion au serveur virtuel d'authentification

   bind authentication vserver auth56 -policy login1 -priority 1 -gotoPriorityExpression END

7. Liez la stratégie LDAP (premier facteur) au serveur virtuel d'authentification.

   bind authentication vserver auth56 -policy ldap -priority 1 -nextFactor label1 -gotoPriorityExpression next

8. Liez la stratégie RADIUS (deuxième facteur) à l'étiquette de stratégie d'authentification.

   bind authentication policylabel label1 -policyName radius -priority 2 -gotoPriorityExpression end

nFactor Visualizer pour une configuration simplifiée

August 20, 2021

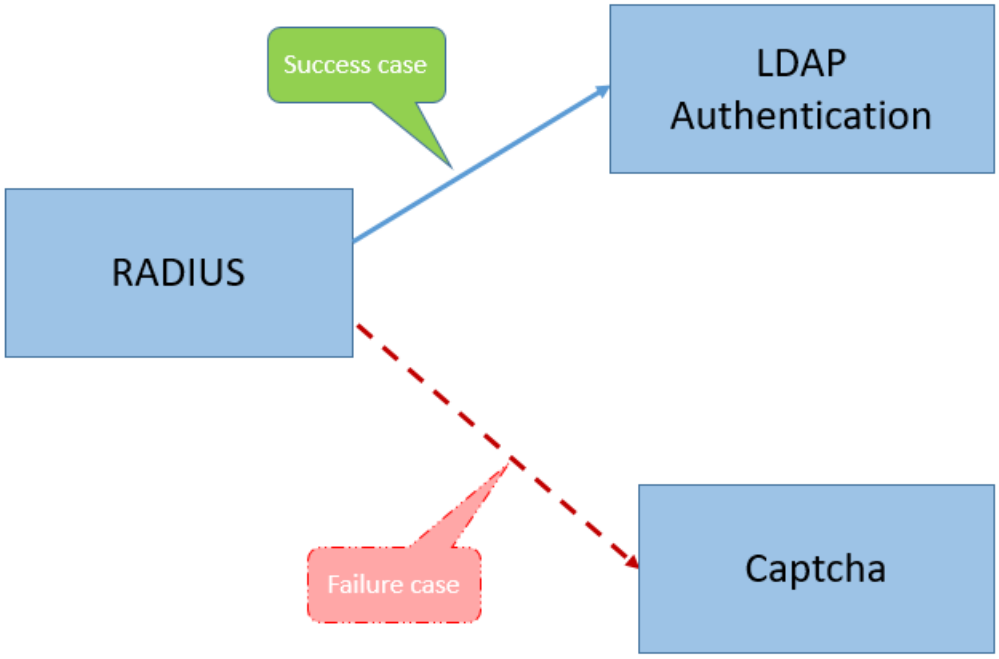
À partir de Citrix ADC version 13.0 build 36.27, la configuration de NFactor via l'interface graphique est simplifiée à l'aide de NFactor Visualizer. Le visualiseur nFactor aide les administrateurs à ajouter plusieurs facteurs sans perdre la trace de chaque facteur. Le groupe de facteurs qui sont construits dans le flux est affiché en un seul endroit. Les administrateurs peuvent ajouter séparément les chemins de réussite et d'échec de l'authentification. Après avoir créé le flux, les administrateurs doivent lier le flux nFactor à un serveur virtuel d'authentification.

> **Remarque**
>
> - Tous les facteurs créés par un administrateur dans le flux nFactor sont conservés pour toute utilisation future.
> - À partir de la fonctionnalité Citrix ADC version 13.0 build 64.35 et supérieure, à l'aide du visualiseur NFactor, vous pouvez démarrer le flux NFactor avec un bloc de décision.

Auparavant, la configuration de nFactor était lourde dans laquelle les administrateurs devaient visiter de nombreuses pages pour la configurer. Si une modification était nécessaire, les administrateurs devaient revoir les sections configurées à chaque fois. De plus, il n'y avait aucune option pour afficher la configuration complète en un seul endroit.

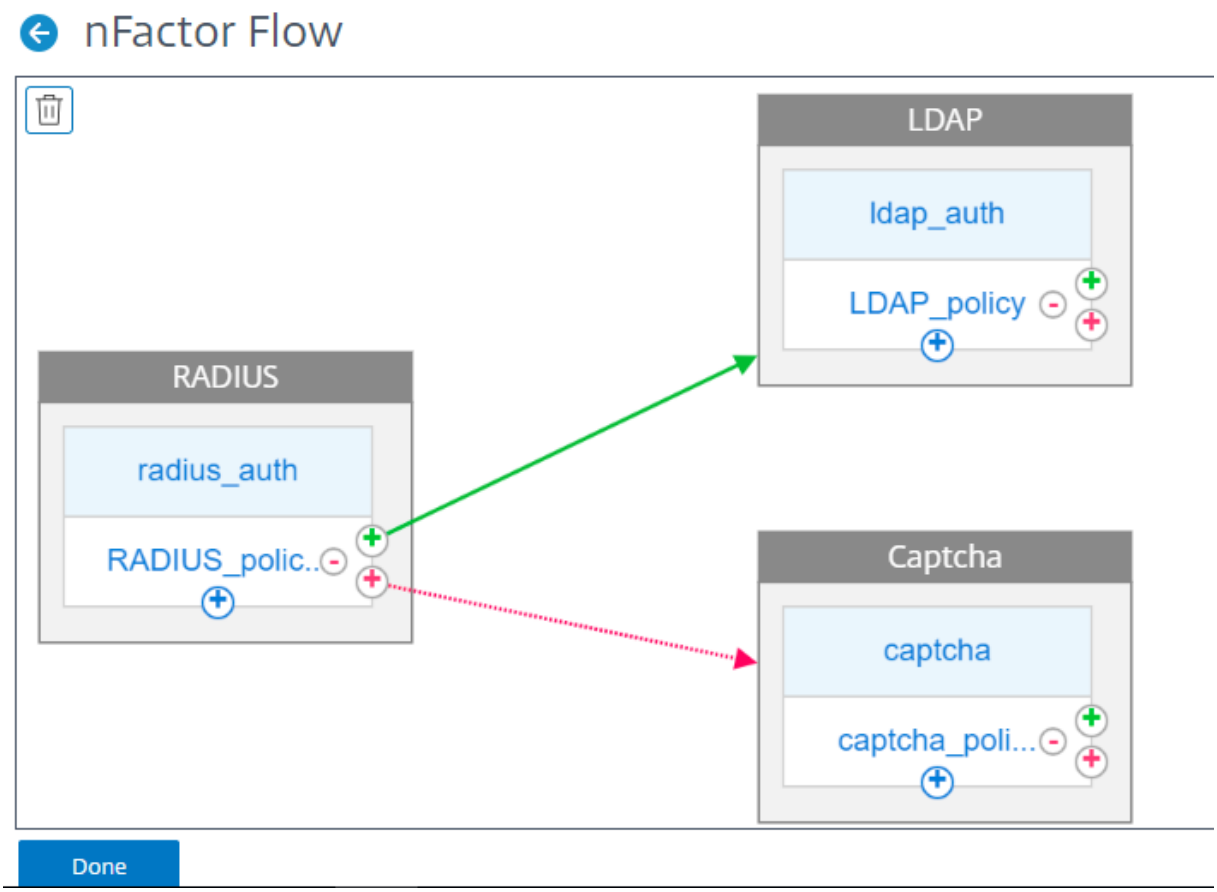
Cas d'utilisation 1 : RADIUS suivi de l'authentification LDAP, sinon repli à Captcha via nFactor Visualizer

Atteignez l'authentification RADIUS comme authentification de premier niveau suivie de l'authentification LDAP. En cas d'échec de RADIUS, l'authentification doit revenir à Captcha.



Pour atteindre ce cas d'utilisation, vous pouvez utiliser nFactor Visualizer. Le Visualizer fournit divers contrôles qui peuvent être utilisés pour ajouter ce flux et les éléments associés.

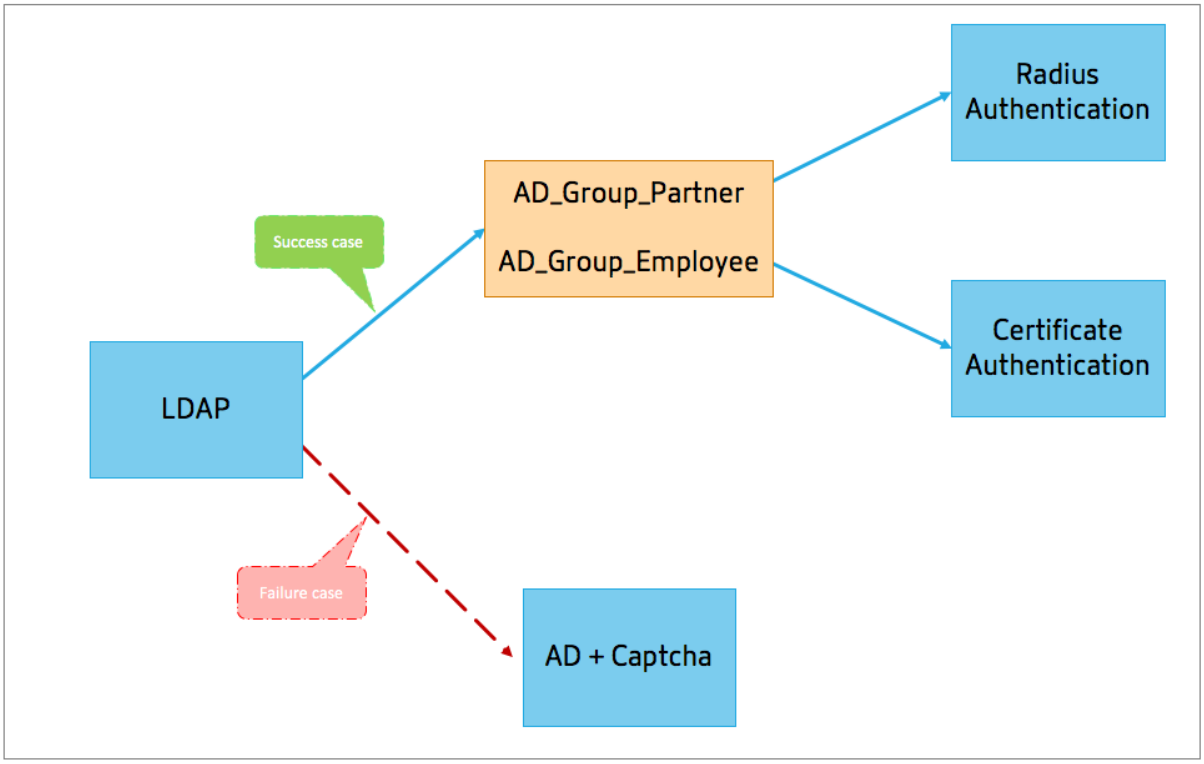
La figure suivante affiche le flux nFactor créé pour le cas d'utilisation mentionné précédemment à l'aide du visualiseur.



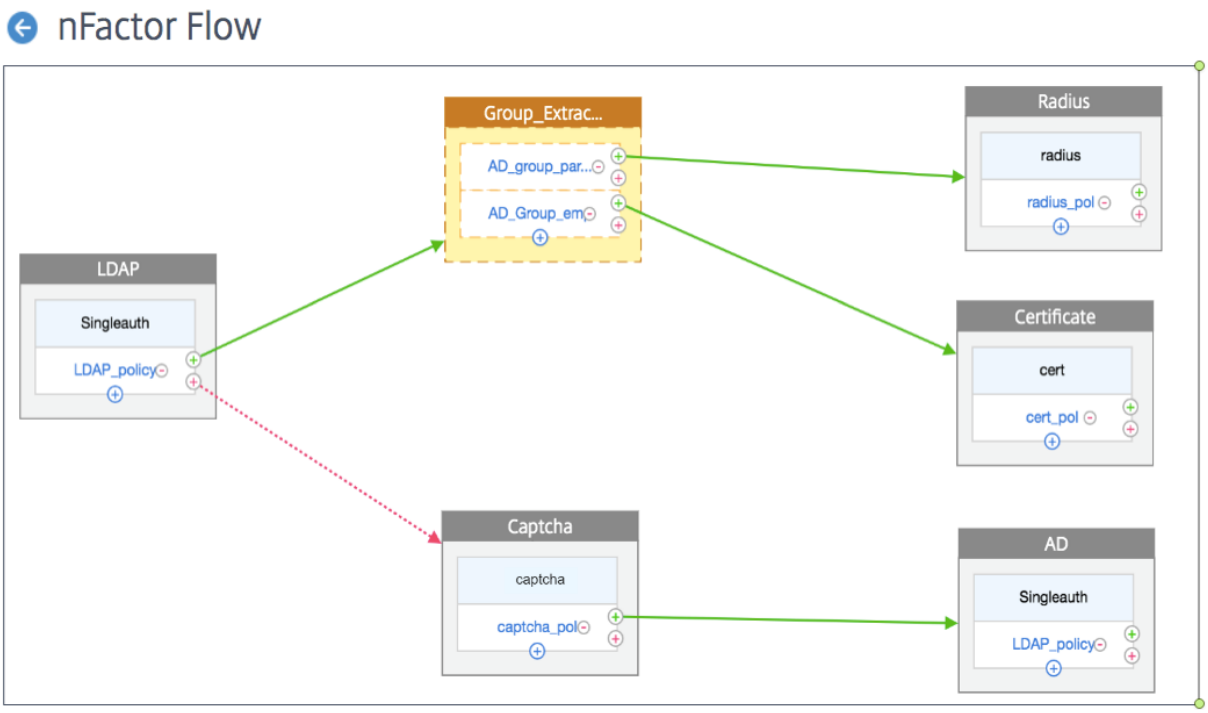
- **RADIUS.** Vous configurez RADIUS comme premier facteur. Vous ajoutez un schéma de connexion et une stratégie. Dans cet exemple, radius_auth et Radius_Policy sont le schéma et la stratégie de connexion ajoutés. Pour Radius_Policy, vous pouvez ajouter un autre facteur pour le cas de réussite. Dans cet exemple, un bloc de facteur LDAP est ajouté pour le cas de réussite. Pour le cas d'échec, vous pouvez ajouter un facteur Captcha.
- **LDAP.** Vous configurez l'authentification LDAP comme deuxième facteur. Vous ajoutez un schéma de connexion et une stratégie. Dans cet exemple, ldap_auth et ldap_Policy sont le schéma de connexion et la stratégie ajoutés.
- **Captcha.** Pour le cas d'échec de stratégie RADIUS, vous créez un facteur Captcha. Dans cet exemple, captcha et captcha_policy sont le schéma de connexion et la stratégie ajoutés.

Cas d'utilisation 2 : LDAP suivi de l'authentification Radius/certificat avec Captcha basée sur l'appartenance au groupe LDAP via nFactor Visualizer

Atteignez l'authentification RADIUS comme authentification de premier niveau suivie de l'authentification LDAP. En cas d'échec de RADIUS, l'authentification doit revenir à Captcha.



La figure suivante affiche le flux nFactor créé pour le cas d'utilisation mentionné précédemment à l'aide du visualiseur.



- **LDAP.** Vous configurez LDAP comme premier facteur. Vous ajoutez un schéma de connexion et une stratégie. Dans cet exemple, SingleAuth et LDAP_Policy sont le schéma et la stratégie de

connexion qui sont ajoutés. Pour LDAP_Policy, vous pouvez ajouter un autre facteur pour le cas de réussite. Dans cet exemple, un bloc de décision est ajouté pour le cas de réussite. Pour le cas d'échec, vous pouvez ajouter Captcha suivi du facteur AD.

- **LDAP d'extraction de groupe.** Est le bloc de décision ajouté pour le cas de réussite LDAP. Le bloc de décision est utilisé comme facteur de sortie de branche pour débrancher les utilisateurs en fonction des règles de stratégie. Visualizer permet de configurer uniquement une stratégie NO_AUTHN pour le bloc de décision.

  Dans cet exemple, Group_Extraction_LDAP est le bloc de décision. Vous ajoutez deux stratégies (`AD_Group_Partner and AD_Group_Employee`) à ce bloc de décision. Comme expliqué dans les cas d'utilisation, toutes les demandes acheminées via la stratégie AD_Group_Partner utilisent l'authentification RADIUS. Par conséquent, vous connectez le cas de réussite de cette stratégie au facteur suivant qui est le facteur RADIUS. De même, toutes les demandes acheminées via la stratégie AD_Group_Employee utilisent l'authentification de certification. Par conséquent, vous connectez le cas de réussite de cette stratégie au facteur suivant qui est le facteur d'authentification de certification.

  - **RADIUS.** Pour le cas de réussite de la stratégie AD_Group_Partner, vous créez le facteur d'authentification RADIUS.
  - **Certificat.** Pour le cas de réussite de la stratégie AD_Group_Employee, vous créez le facteur d'authentification de certificat.

- **Captcha.** Pour le cas d'échec de stratégie LDAP, vous créez deux facteurs suivants, Captcha et le facteur AD.

> **Remarque**
>
> - Si vous avez un cas d'utilisation pour déconnecter en premier lieu, vous pouvez soit créer deux flux et lier séparément, soit créer un flux avec le premier comme branche out, et le lier au serveur virtuel.
> - Si vous disposez de plusieurs blocs et pour afficher l'intégralité du flux dans l'écran NFactor Flow, cliquez sur le visualiseur et faites glisser le flux vers l'extrême gauche.
> - Citrix recommande de modifier les flux NFactor à l'aide de la page Flux NFactor uniquement.

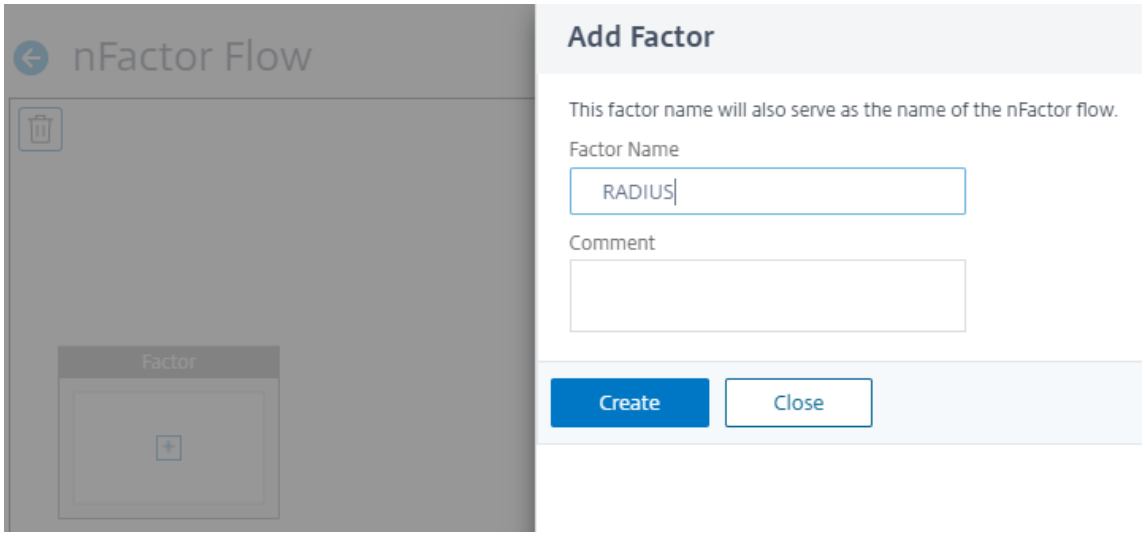
Pour configurer nFactor à l'aide de nFactor Visualizer

> **Remarque**
>
> La configuration nFactor suivante est un exemple simple qui vous aide à réaliser les configurations de scénario de cas d'utilisation 1.

1. Accédez à **Sécurité > AAA — Trafic d'application > nFactor Visualizer > nFactor Flows**.
2. Cliquez sur **Ajouter**.

3. Sur la page **nFlux de facteurs**, cliquez sur **+** pour ajouter un premier facteur pour le flux. Le premier facteur sert également d'identificateur pour ce flux nFactor.

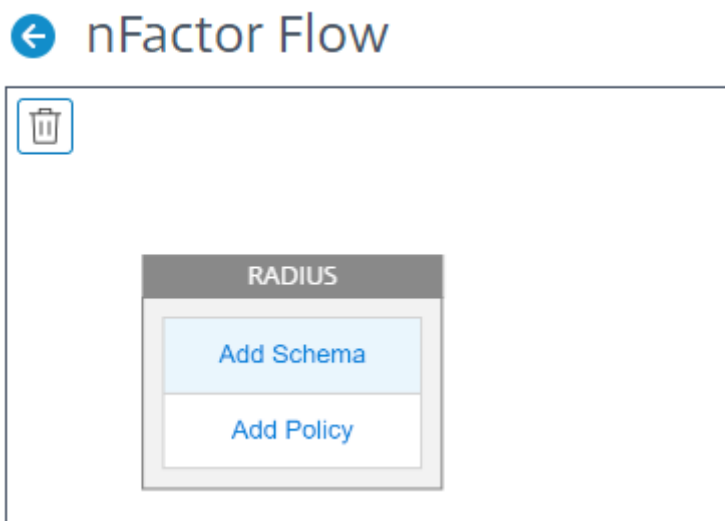
4. Entrez le nom du facteur et cliquez sur **Créer**.



Le nom du facteur apparaît sur le bloc de facteur dans la page nFactor Flow.

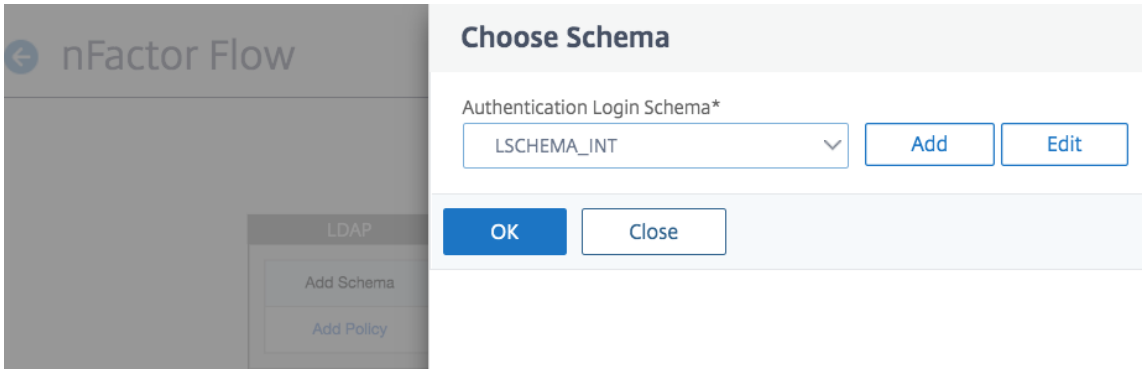
> **Remarque**
>
> Citrix vous recommande de ne pas utiliser les noms d'étiquettes de stratégie tels que,`__root` et `__<flow_name>` comme suffixe et `_db_` comme préfixe. Il est utilisé comme noms de facteurs créés dans le flux nFactor.

5. Une fois le facteur RADIUS créé, les Ajouter un schéma et Ajouter une stratégie doivent être créés.

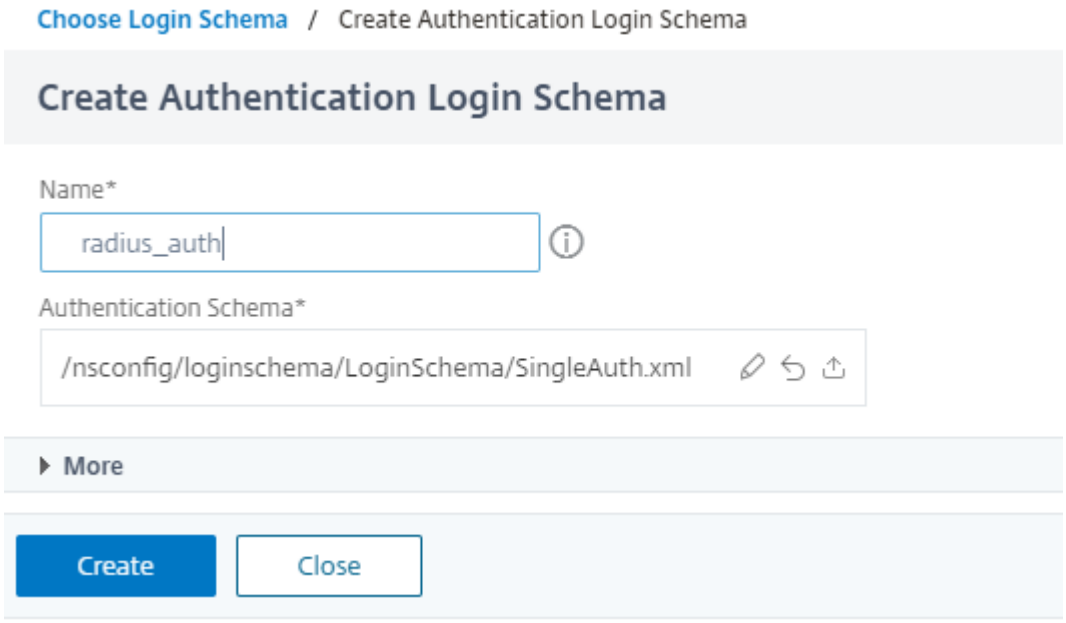


> **Remarque**
>
> Pour plus d'informations, voir Concepts, entités et terminologie de NFactor.

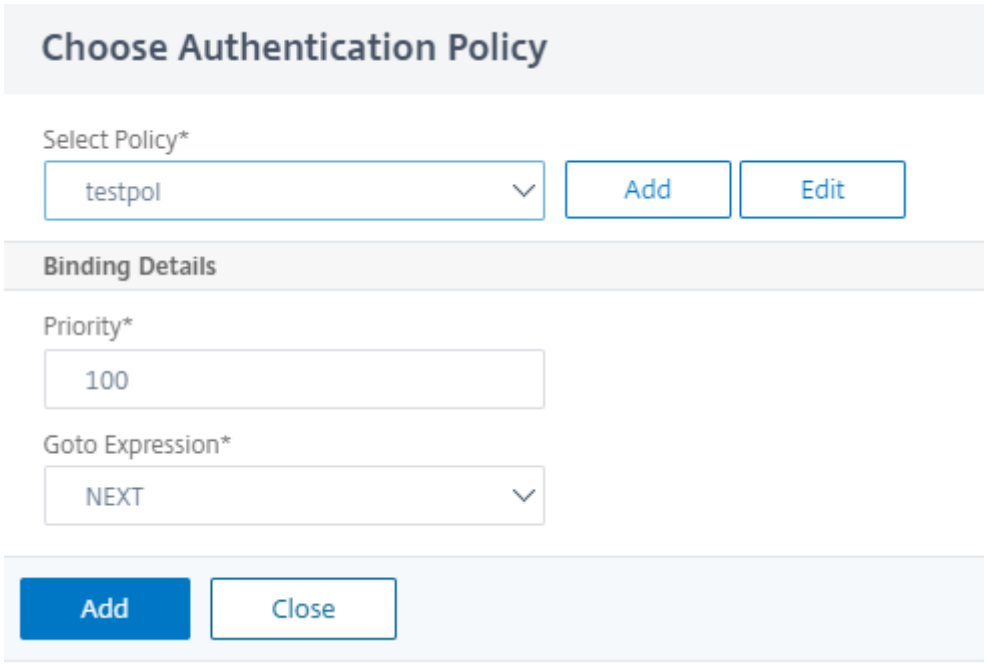
6. Cliquez sur **Ajouter un schéma**. Vous pouvez ajouter un nouveau schéma de connexion ou sélectionner un schéma de connexion existant dans la liste **Schéma de connexion d'authentification** .



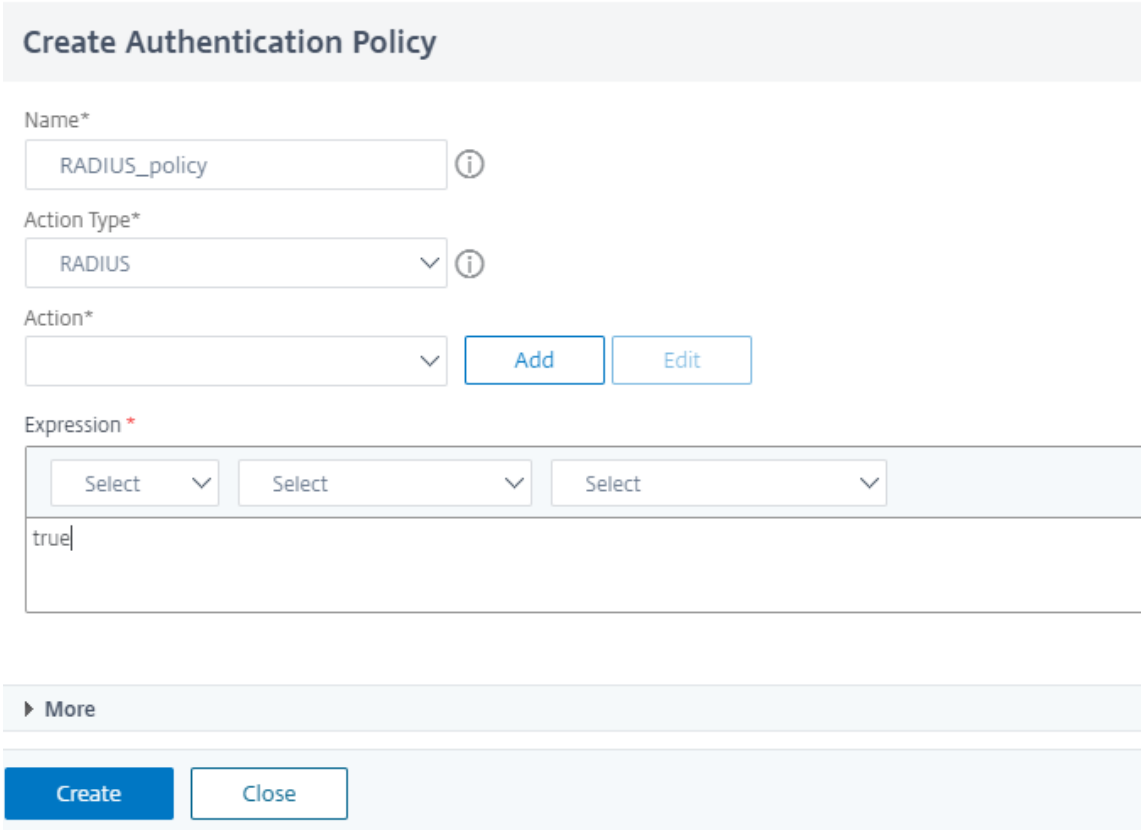
7. Pour créer un schéma de connexion, cliquez sur **Ajouter** et, dans la page **Créer un schéma de connexion d'authentification**, entrez le nom du schéma. Cliquez sur **Modifier** (icône en forme de crayon) pour sélectionner les **fichiers de schéma de connexion** dans la liste.



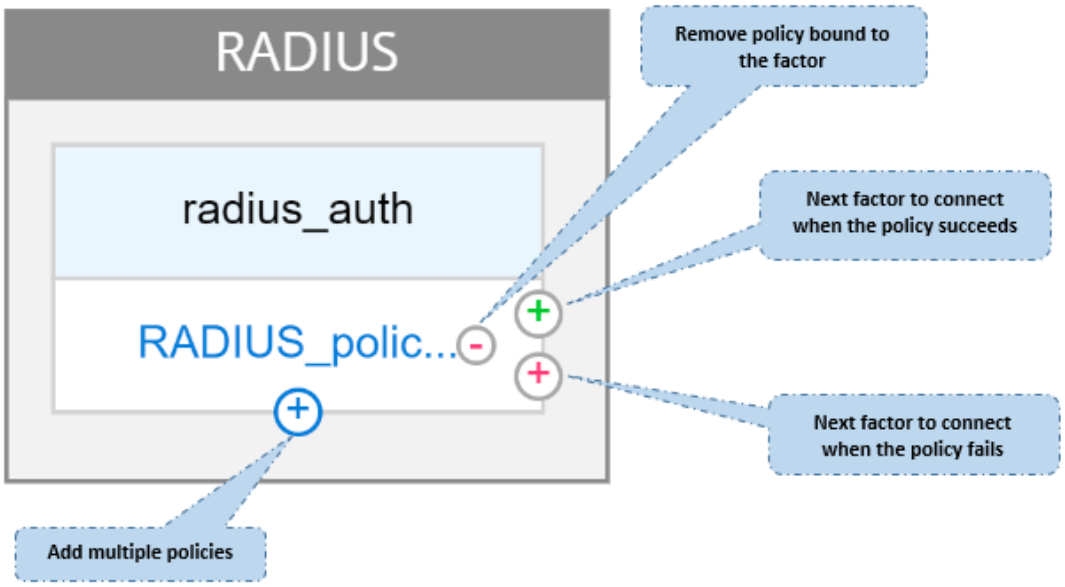
8. Cliquez sur **Ajouter une stratégie**. Vous pouvez créer une stratégie d'authentification ou sélectionner une stratégie d'authentification existante.



9. Pour créer une stratégie, cliquez sur **Ajouter** et, dans la page **Créer une stratégie d'authentification**, entrez le nom de la stratégie, puis cliquez sur **Créer** .



10. Après avoir ajouté un schéma de connexion et une stratégie au facteur, le schéma de connexion et la stratégie apparaissent sur le facteur dans le Visualizer, comme indiqué dans la figure suivante. Pour un facteur donné, vous pouvez ajouter plusieurs stratégies et définir le facteur suivant pour le succès et l'échec de chaque stratégie. Vous pouvez également supprimer les stratégies qui font partie du facteur.



11. Après avoir créé le flux, vous pouvez ensuite lier le flux nFactor à un serveur virtuel d'authentification.

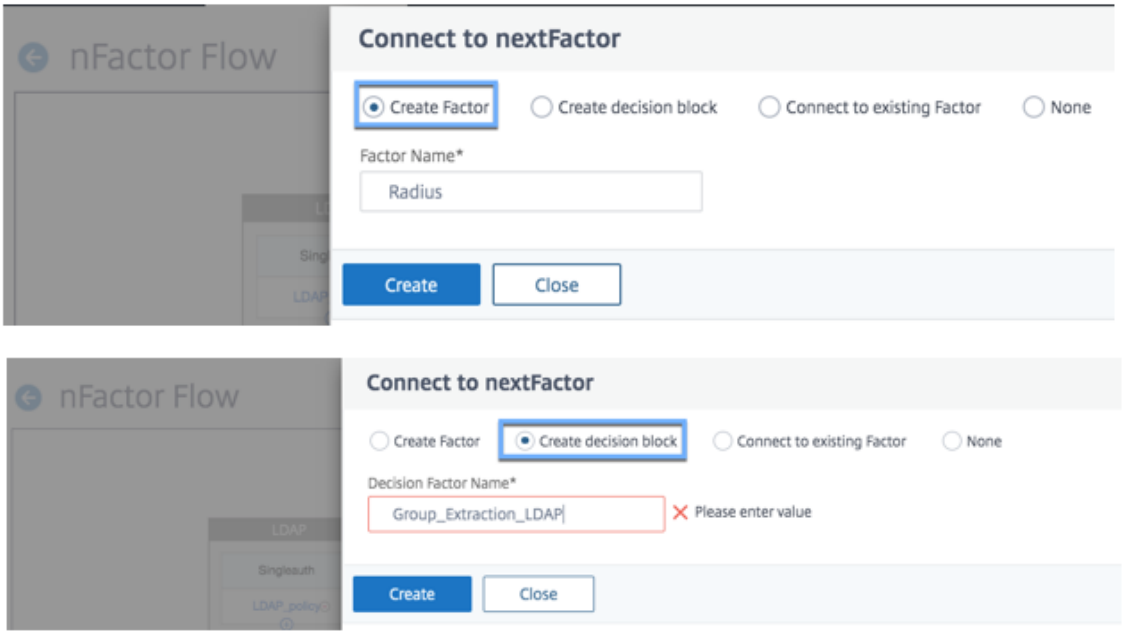
Ajout du facteur suivant

Pour ajouter le facteur suivant, vous pouvez sélectionner l'une des options suivantes selon votre besoin :

- **Créer un facteur**. Créez un facteur. Chaque facteur créé dans un flux est exclusif à ce flux.
- **Créez un bloc de décision.** Créer un bloc de décision pour servir de facteur de sortie de succursale. Vous ne pouvez pas ajouter de schéma de connexion au bloc de décision. Visualizer permet de configurer uniquement une stratégie NO_AUTHN pour le bloc de décision.

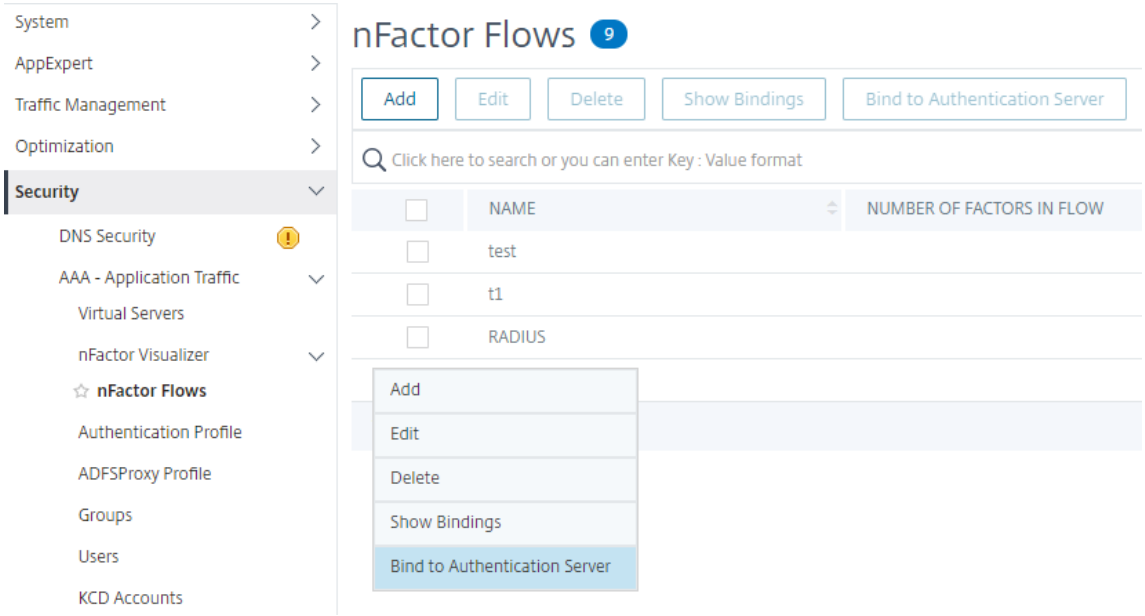
  > **Remarque**
  >
  > Vous pouvez uniquement ajouter ou modifier le bloc de décision via l'interface graphique Citrix ADC. Il n'y a pas d'option pour configurer le bloc de décision à partir de la commande CLI.

- **Connectez-vous à un facteur existant**. Sélectionnez un facteur existant comme facteur suivant. Tous les facteurs qui apparaissent dans la liste existante sont créés exclusivement pour ce flux.
- **Aucun.** Supprimez une connexion existante.



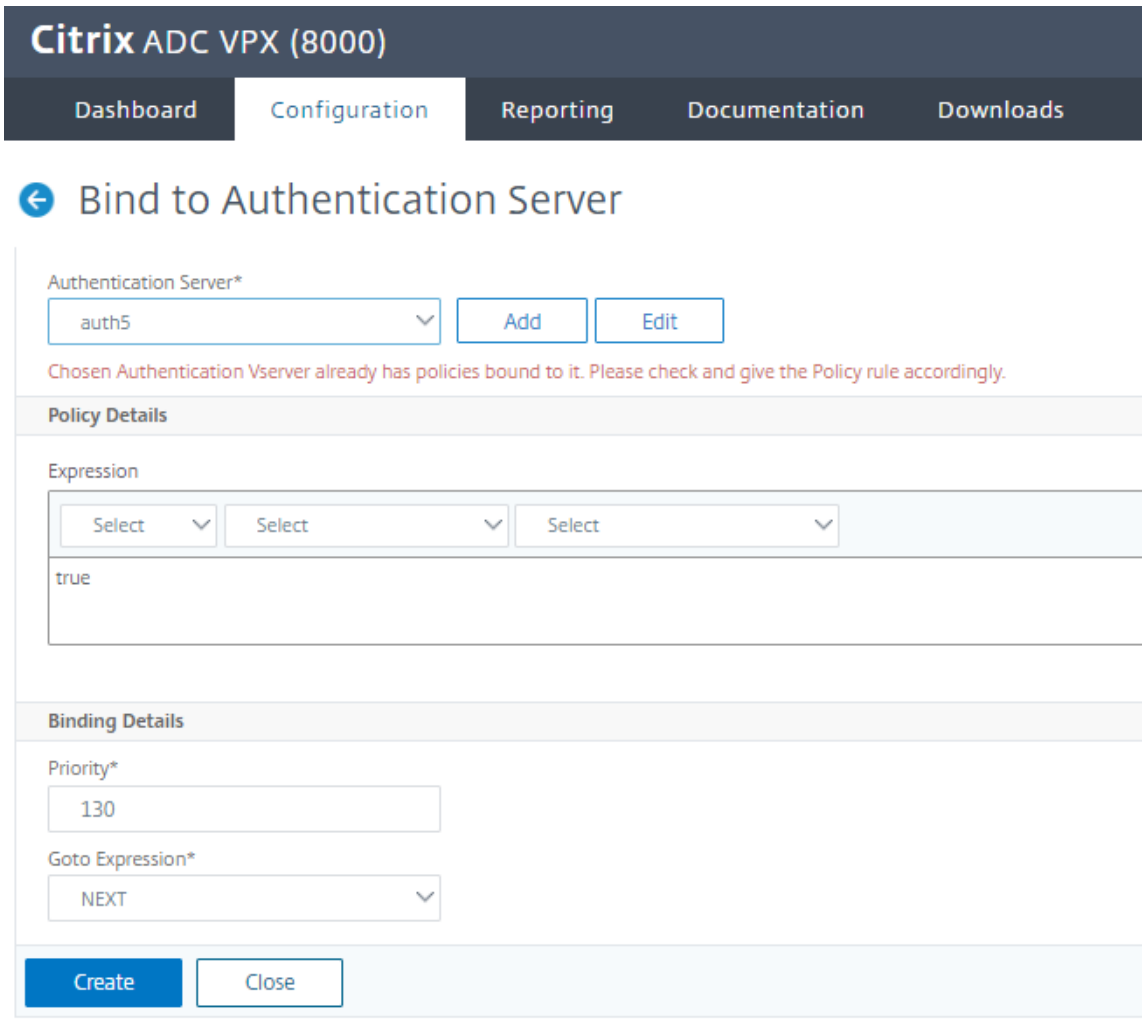
Pour lier le flux nFactor au serveur d'authentification

1. Sur la page **nFlux Factor**, sélectionnez un flux nFactor que vous préférez lier à un serveur virtuel d'authentification.
2. Cliquez sur l'icône hamburger pour sélectionner l'option **Lier au serveur d'authentification** ou, dans le volet d'informations, cliquez sur **Lier au serveur d'authentification** .

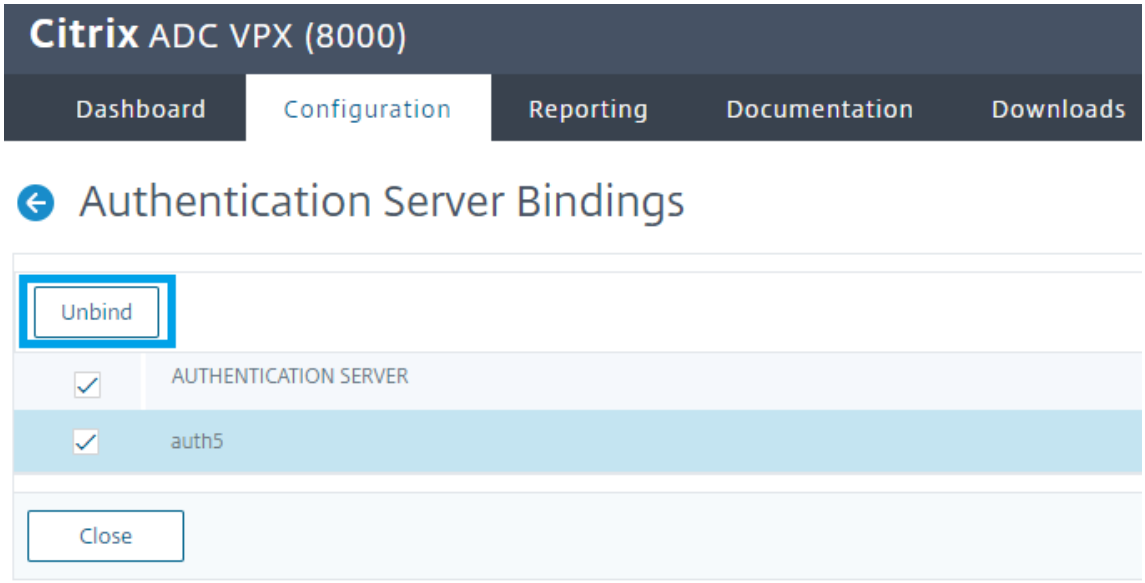


3. Sur la page **Lier au serveur d'authentification**, vous pouvez effectuer les actions suivantes :
   - Pour ajouter un **serveur virtuel d'authentification**, cliquez sur **Ajouter**.

- Pour sélectionner un serveur d'authentification existant dans la liste, cliquez sur le champ **Serveur d'authentification** .



4. Cliquez sur **Afficher les liaisons** à partir de l'icône hamburger pour afficher les liaisons.
5. Pour dissocier le serveur d'authentification du flux nFactor spécifique, effectuez les opérations suivantes :
   - Sur la page **NFactor Flows**, cliquez sur **Afficher les liaisons** à partir de l'icône Hamburger.
   - Dans la page **Liaisons du serveur d'authentification**, sélectionnez le serveur d'authentification à dissocier et cliquez sur **Dissocier**. Cliquez sur **Fermer**.



Pour plus d'informations sur l'authentification nFactor, consultez les rubriques suivantes :

- Concept : Authentification multi-facteurs (nFactor).
- Workflow : Fonctionnement de l'authentification NFactor.
- Configuration : configuration de l'authentification NFactor.

Améliorations apportées au visualiseur nFactor

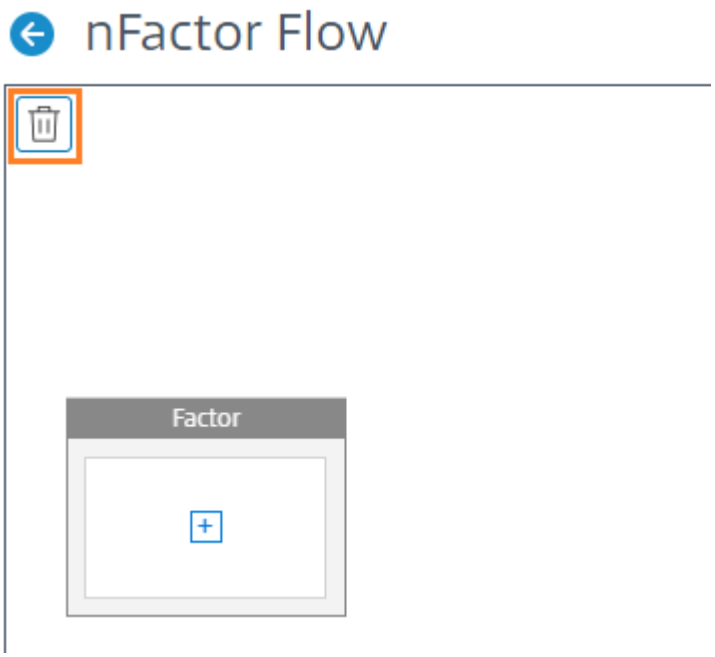
À partir de Citrix ADC version 13.0 build 41.20, les améliorations suivantes sont apportées dans nFactor Visualizer.

- Les administrateurs peuvent déplacer les facteurs créés vers l'icône de la corbeille.
- Affichez les flux nFactor dans la page Authentification serveur virtuel.

Icône Corbeille. Les administrateurs peuvent uniquement supprimer les nœuds qui n'ont pas de connexion. Toutefois, les stratégies sous-jacentes ou les schémas créés pour le facteur ne sont pas supprimés si le facteur est déplacé dans la corbeille.

Pour afficher l'icône de corbeille :

1. Accédez à **Sécurité > AAA — Trafic d'application > nFactor Visualizer > nFactor Flows**.

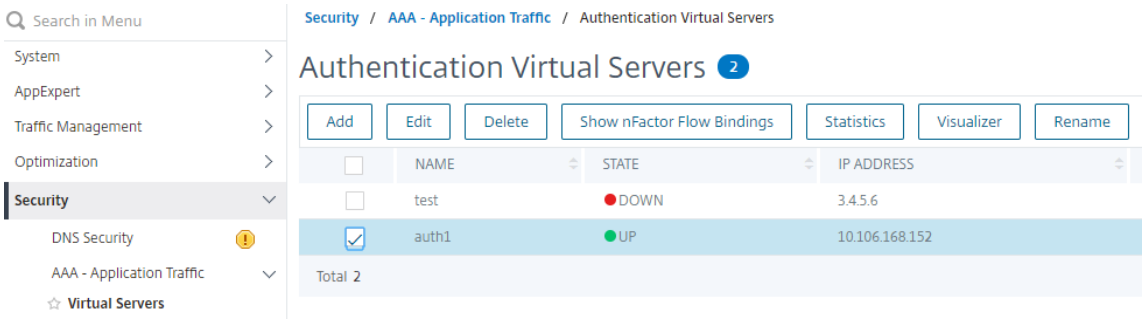


2. Pour supprimer le facteur, cliquez sur le bloc de facteur et faites-le glisser vers la corbeille.

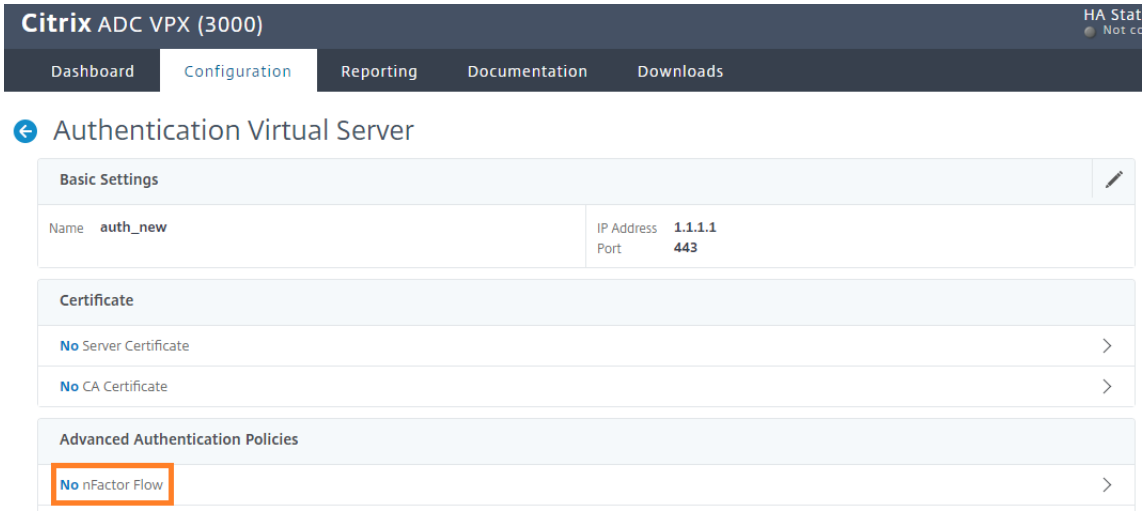
Afficher le flux nFactor à partir du serveur virtuel d'authentification. Les administrateurs peuvent également afficher les flux NFactor créés à partir de la page Authentification Virtual Server.

Pour afficher le flux nFactor à partir de la page Authentication Virtual Server :

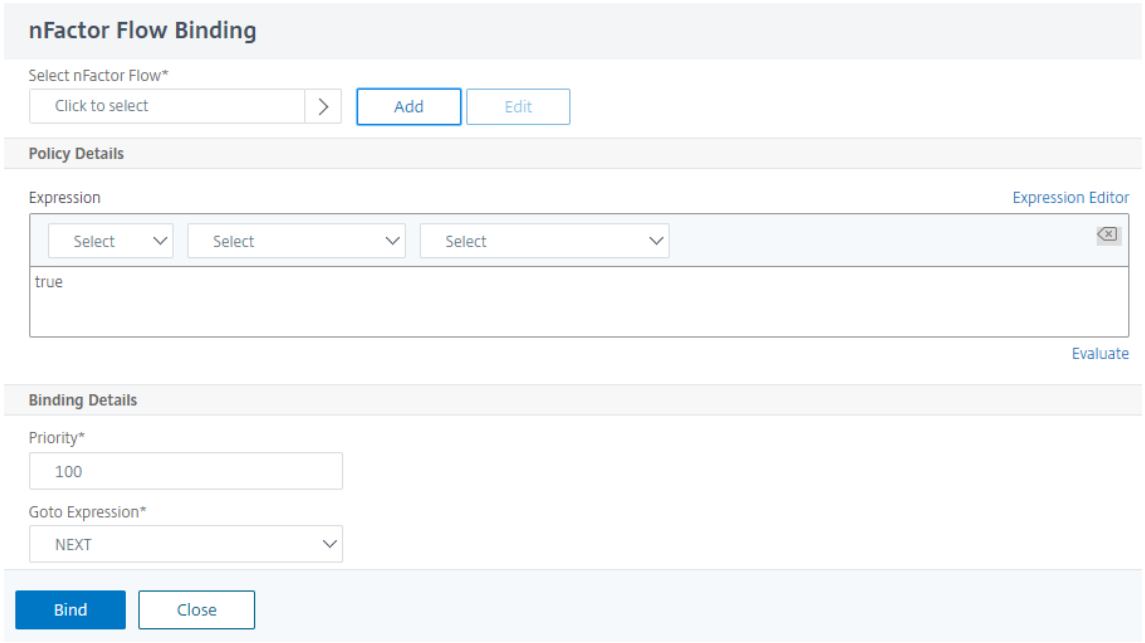
1. Accédez à **Sécurité > AAA — Trafic des applications > Serveurs virtuels**. Sur la page **Authentification des serveurs virtuels**, vous pouvez effectuer les opérations suivantes :
   - Pour ajouter un serveur virtuel d'authentification, cliquez sur **Ajouter**.
   - Pour modifier un serveur virtuel d'authentification existant, cliquez sur l'option **Modifier** dans le volet d'informations.



2. Sur la page **Authentification serveur virtuel**, vous pouvez afficher l'option **nFactor Flow** sous **Stratégies d'authentification avancées** .



3. Si aucun flux nFactor n'est lié au serveur virtuel, vous pouvez cliquer sur l'option **No nFactor Flow** sous la section **Stratégies d'authentification avancées** pour ajouter un nouveau flux nFactor ou sélectionner le flux nFactor existant dans la liste.



nFactor Extensibilité

August 20, 2021

Le cadre d'authentification nFactor offre la flexibilité d'ajouter des personnalisations pour rendre l'interface d'ouverture de session plus intuitive pour une expérience utilisateur riche. Vous pouvez ajouter des étiquettes de connexion personnalisées, des informations d'identification de connexion

personnalisées, la personnalisation des affichages de l'interface utilisateur, etc.

Avec nFactor, chaque facteur peut avoir son propre écran d'ouverture de session. Dans chaque écran d'ouverture de session, vous pouvez présenter toutes les informations provenant de l'un des facteurs précédents ou plus d'informations qui sont invisibles dans d'autres facteurs. Par exemple, votre dernier facteur peut être une page informative où l'utilisateur lit les instructions et clique sur continuer.

Avant nFactor, les pages de connexion personnalisées étaient limitées et les personnalisations et nécessitaient un support. Il était possible de remplacer le tmindex.html ou d'appliquer des règles de réécriture pour modifier une partie de son comportement. Cependant, il n'a pas été possible d'atteindre la fonctionnalité sous-jacente.

Les personnalisations associées à nFactor suivantes sont capturées en détail dans cette rubrique.

- Personnaliser les étiquettes de connexion
- Personnaliser l'interface utilisateur pour afficher les images
- Personnaliser le formulaire d'ouverture de session Citrix ADC nFactor

Hypothèses

Vous êtes familier avec nFactor, les commandes Shell, XML et les éditeurs de texte.

Conditions préalables

- La personnalisation décrite dans cette rubrique n'est possible que lorsque le thème de l'interface utilisateur RFWeb (ou basé sur un thème) est configuré sur Citrix ADC.
- La stratégie d'authentification doit être liée au serveur virtuel d'authentification, d'autorisation et d'audit, sinon le flux ne fonctionne pas comme prévu. Pour plus de détails, voir CTX224241.
- Vous avez les éléments suivants liés à nFactor
  - Schéma XML
  - JavaScript
  - Actions d'authentification
  - Authentification serveur virtuel
  - Citrix ADC version 11.1 et ultérieure

Personnaliser les étiquettes d'ouverture de session

Pour personnaliser les étiquettes d'ouverture de session, vous avez besoin des éléments suivants :

- Schéma XML qui décrit l'apparence de la page d'ouverture de session.
- Le fichier script.js qui contient le JavaScript utilisé pour modifier le processus de rendu.

Fonctionnement

Le JavaScript analyse le fichier XML, rendant chaque élément à l'intérieur de la<Requirements> balise. Chaque élément correspond à une ligne du formulaire HTML. Par exemple, un champ de connexion est une ligne, le champ de mot de passe est une autre ligne, de même que le bouton d'ouverture de session. Pour introduire de nouvelles lignes, vous devez les spécifier dans le fichier de schéma XML à l'aide du SDK StoreFront. Le SDK StoreFront permet à la page d'ouverture de session avec un schéma XML d'utiliser la<Requirement> balise et de définir des éléments dessus. Ces éléments permettent d'utiliser JavaScript pour introduire dans cet espace les éléments HTML requis. Dans ce cas, une ligne est créée avec du texte sous la forme de HTML.

Le XML qui peut être utilisé est le suivant :

```
<Requirement>
<Credential>
<Type>nsg-custom-cred</Type>
<ID>passwd</ID>
</Credential>
<Label>
<Type>nsg-custom-label</Type>
</Label>
</Requirement>
<!--NeedCopy-->
```

<Requirement>: espace fourni dans la page d'ouverture de session. Les informations d'identification remplissent l'espace et les autres pièces acheminent le moteur vers les informations correctes. Dans ce cas, tapez nsg-custom-cred. Ceci est défini comme du texte brut et l'étiquette est définie pour son corps.
L'exigence XML est associée au code JavaScript pour obtenir les résultats requis.

```
// Custom Label Handler for Self Service Links
CTXS.ExtensionAPI.addCustomAuthLabelHandler({

getLabelTypeName: function () {
  return "nsg-custom-label";  }
 ,
getLabelTypeMarkup: function (requirements) {

return $("< Your HTML Code Here>");
 }
 ,
// Instruction to parse the label as if it was a standard type
parseAsType: function () {

return "plain";
```



```
 }

 }
 );
//Custom Credential Handler for Self Service Links
CTXS.ExtensionAPI.addCustomCredentialHandler({

getCredentialTypeName: function () {
  return "nsg-custom-cred";  }
 ,
getCredentialTypeMarkup: function (requirements) {

return $("<div/>");
 }
 ,
 }
 );
<!--NeedCopy-->
```

La partie XML indique la page d'ouverture de session à afficher, et le code JavaScript fournit le texte réel. Le gestionnaire d'informations d'identification ouvre l'espace et l'étiquette remplit l'espace. Comme tout le trafic d'authentification est désormais invisible pour réécrire et répondre, vous pouvez modifier l'apparence de la page.

Configuration pour personnaliser les étiquettes de connexion

1. Créez et liez un thème basé sur RFWeb.

   ```
   add vpn portaltheme RfWebUI_MOD -basetheme RfWebUI

   bind vpn vserver TESTAAA  - portaltheme RfWebUI_MOD
   <!--NeedCopy-->
   ```

   Le chemin d'accès des fichiers basés sur le thème est disponible dans le répertoire ; /var/netscaler/logon/themes/rfwebui_mod

2. Ajoutez l'extrait suivant à la fin du fichier script.js :

   Remarque : Ne pas inclure les lignes précédentes dans le fichier correct ou manquant pour inclure des fonctions JavaScript empêche le chargement du XML. L'erreur ne peut être visible que dans la Console du développeur du navigateur avec le texte suivant : « Type non défini nsg-custom-cred. »

   ```
   // Custom Label Handler for Self Service Links
   CTXS.ExtensionAPI.addCustomAuthLabelHandler({

   ```



```
getLabelTypeName: function () {
  return "nsg-custom-label";  }
 ,
getLabelTypeMarkup: function (requirements) {

return $("<a href="https://identity.test.com/identity/faces/
   register" style="font-size: 16px;" style="text-align: center;">
   Self Registration</a><br><a href="https://identity.test.com/
   identity/faces/forgotpassword" style="font-size: 16px;" style="
   text-align: center;">Forgot Password</a><br><a href="https://
   identity.test.com/identity/faces/forgotuserlogin" style="font-
   size: 16px;" style="text-align: center;">Forgot User Login</a
   >");
 }
 ,
// Instruction to parse the label as if it was a standard type
parseAsType: function () {

return "plain";
 }

 }
 );
//Custom Credential Handler for Self Service Links
CTXS.ExtensionAPI.addCustomCredentialHandler({

getCredentialTypeName: function () {
  return "nsg-custom-cred";  }
 ,
getCredentialTypeMarkup: function (requirements) {

return $("<div/>");
 }
 ,
 }
 );
<!--NeedCopy-->
```

Schéma de connexion utilisé dans cet exemple

```
<?xml version="1.0" encoding="utf-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
   /1">
<Status>success</Status>
```



```
<Result>more-info</Result>
<StateContext/>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/Citrix/Authentication/ExplicitForms/CancelAuthenticate
   </CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement>
<Credential>
<ID>login</ID>
<SaveID>Username</SaveID>
<Type>username</Type>
</Credential>
<Label>
<Text>User name</Text>
<Type>plain</Type>
</Label>
<Input>
<AssistiveText>Please supply either domain\username or user@fully.
   qualified.domain</AssistiveText>
<Text>
<Secret>false</Secret>
<ReadOnly>false</ReadOnly>
<InitialValue></InitialValue>
<Constraint>.+</Constraint>
</Text>
</Input>
</Requirement>
<Requirement>
<Credential>
<ID>passwd</ID>
<SaveID>Password</SaveID>
<Type>password</Type>
</Credential>
<Label>
<Text>Password:</Text>
<Type>plain</Type>
</Label>
<Input>
<Text>
<Secret>true</Secret>
<ReadOnly>false</ReadOnly>
<InitialValue/>
<Constraint>.+</Constraint>
```



```
</Text>
</Input>
</Requirement>
<Requirement>
<Credential>
<Type>nsg-custom-cred</Type>
<ID>passwd</ID>
</Credential>
<Label>
<Type>nsg-custom-label</Type>
</Label>
</Requirement>
<Requirement>
<Credential>
<ID>loginBtn</ID>
<Type>none</Type>
</Credential>
<Label>
<Type>none</Type>
</Label>
<Input>
<Button>Please Log On</Button>
</Input>
</Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

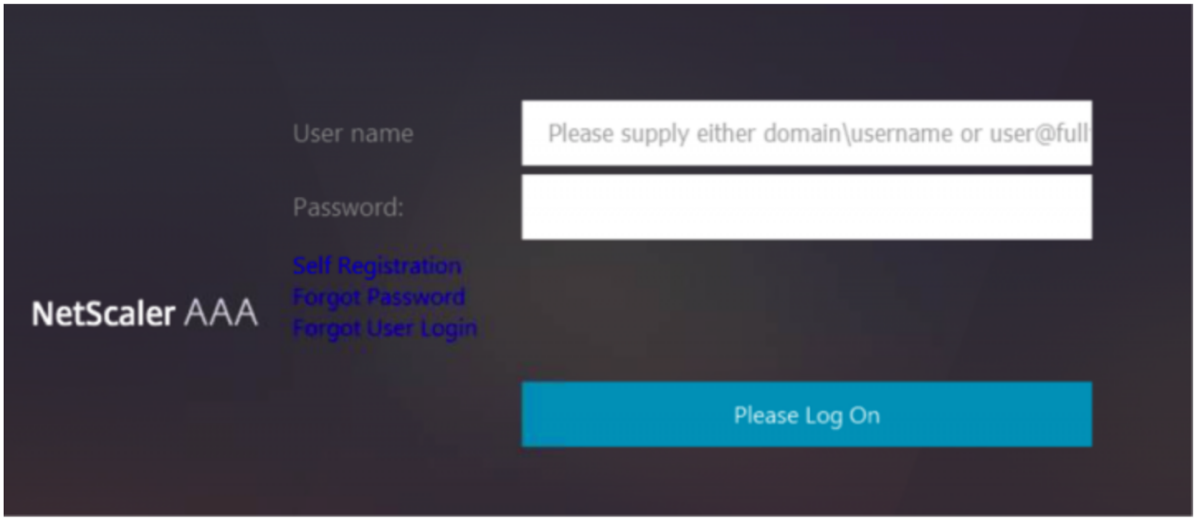
Exécutez les commandes suivantes pour charger le schéma personnalisé dans la configuration.

```
add authentication loginSchema custom -authenticationSchema custom.xml

add authentication loginSchemaPolicy custom -rule true -action custom

bind authentication vserver AAATEST -policy custom -priority 100 -
    gotoPriorityExpression END
<!--NeedCopy-->
```

La figure suivante affiche la page de connexion qui est rendue avec cette configuration.



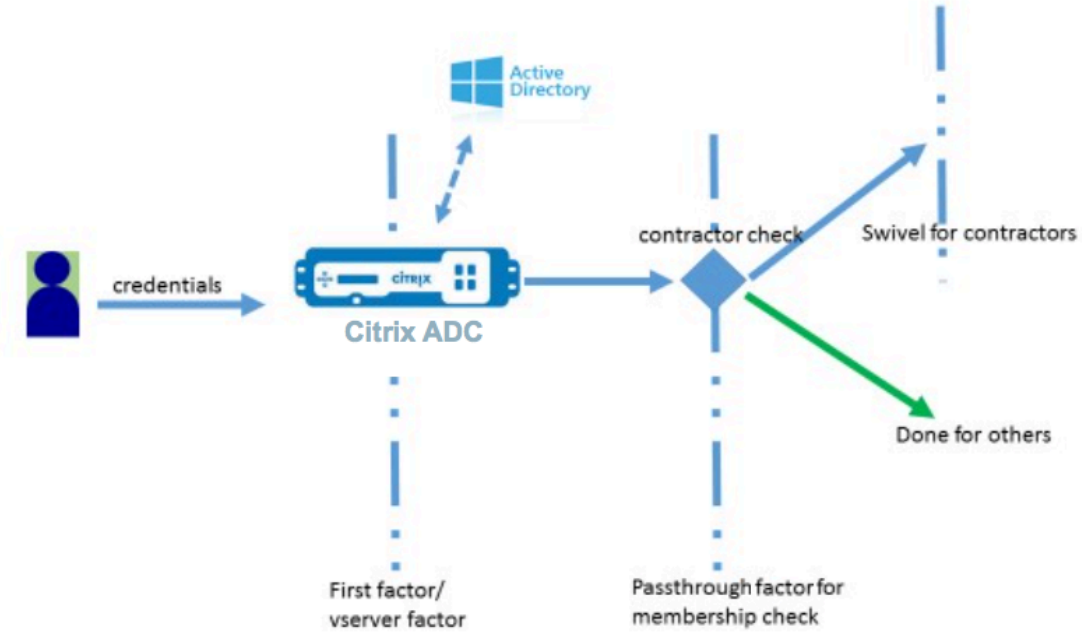
Personnaliser l'interface utilisateur pour afficher les images

nFactor permet un affichage personnalisé avec l'utilisation de fichiers loginschema. Il peut être nécessaire d'autres personnalisations autres que celles offertes par les fichiers loginschema intégrés. Par exemple, afficher un lien hypertexte ou écrire une logique personnalisée dans l'interface utilisateur. Ceux-ci peuvent être obtenus en utilisant des « informations d'identification personnalisées » qui comprennent l'extension loginschema et le fichier javascript correspondant.

Pour la personnalisation de l'interface utilisateur pour afficher des images, un flux de déploiement dans l'intégration « Citrix ADC-Swivel » est utilisé à titre d'exemple.

Il y a deux facteurs dans ce flux.

- Premier facteur : Vérifie les informations d'identification AD de l'utilisateur.
- Deuxième facteur : invite l'utilisateur à ouvrir une session en fonction de l'appartenance au groupe.



Dans ce flux, tous les utilisateurs passent par le premier facteur. Avant le deuxième facteur, il y a un pseudo-facteur pour vérifier si certains utilisateurs peuvent être omis du facteur « pivotement ». Si l'utilisateur a besoin d'un facteur « pivotant », une image et une zone de texte s'affichent pour entrer le code.

Solution

La solution de personnalisation de l'interface utilisateur pour afficher les images contient deux parties ;

- Extension Loginschema.
- Script personnalisé pour traiter l'extension loginschema.

Extension Loginschema

Pour contrôler le rendu du formulaire, un identifiant personnalisé est injecté dans le loginschema. Cela peut être fait en réutilisant le schéma existant et en modifiant selon l'exigence.

Dans l'exemple, un loginschema qui n'a qu'un seul champ de texte (tel que /nsconfig/loginschema/loginschema/OnlyPassword.xml) est pris en compte.
L'extrait suivant est ajouté à la loginschema.

```
1 <Requirement><Credential><ID>swivel_cred</ID><Type>swivel_cred</Type><
     Input><Text><Hidden>true</Hidden><InitialValue>${
2  http.req.user.name }
3  </InitialValue></Text></Input></Credential></Requirement>
```



```
<!--NeedCopy-->
```

Dans l'extrait, « swivel_cred » est spécifié comme « Type » des informations d'identification. Comme cela n'est pas reconnu comme une « identification » intégrée, l'interface utilisateur recherche un gestionnaire pour ce type et l'appelle s'il existe.
Une valeur initiale est envoyée pour ces informations d'identification, qui est une expression que Citrix ADC remplit dynamiquement. Dans l'exemple, il s'agit du nom de l'utilisateur utilisé pour notifier le serveur pivotant du nom d'utilisateur. Il peut ne pas être nécessaire tout le temps ou il peut être augmenté avec d'autres données. Ces détails doivent être ajoutés au besoin.

Javascript pour gérer les informations d'identification personnalisées

Lorsque l'interface utilisateur trouve des informations d'identification personnalisées, elle recherche un gestionnaire. Tous les gestionnaires personnalisés sont écrits dans /var/netscaler/logon/logonpoint/custom/script.js pour le thème de portail par défaut.
Pour les thèmes de portail personnalisés, script.js peut être trouvé dans le répertoire/var/netscaler/logon/themes/<custom_theme>/.

Le script suivant est ajouté pour rendre le marquage des informations d'identification personnalisées.

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the server
    getCredentialTypeName: function () {
  return "swivel_cred";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $("<div></div>");
        var image = $("<img/>");
        var username = requirements.input.text.initialValue; //Get the secret from the response
        image.attr({

            "style" : "width:200px;height:200px;",
            "id" : "qrcodeimg",
            "src" : "https://myswivelserver.citrix.com:8443/pinsafe/SCImage?username=" + username
         }
 );
        div.append(image);
        return div;
```



```
22       }
23
24   }
25   );
26 <!--NeedCopy-->
```

Cet extrait sert à gérer le balisage pour 'swivel_cred'. Le nom des informations d'identification en surbrillance doit correspondre au « type » spécifié précédemment dans l'extension loginschema. Pour générer un balisage, une image dont la source pointe vers le serveur pivotant doit être ajoutée. Une fois cela fait, l'interface utilisateur charge l'image à partir de l'emplacement spécifié. Étant donné que ce loginschema a également une zone de texte, l'interface utilisateur rend cette zone de texte.

Remarque : L'administrateur peut modifier le « style » de l'élément d'image pour redimensionner l'image. Actuellement, il est configuré pour 200x200 pixels.

Configuration pour la personnalisation de l'interface utilisateur pour afficher les images

La configuration nFactor est mieux construite de bas en haut, c'est le dernier facteur en premier car lorsque vous essayez de spécifier 'NextFactor' pour les facteurs précédents, vous avez besoin du nom du facteur suivant.

Configuration du facteur de pivotement :

```
1 add loginschema swivel_image -authenticationSchema /nsconfig/
     loginschema/SwivelImage.xml
2
3 add authentication policylabel SwivelFactor -loginSchema swivel_image
4
5 bind authentication policylabel SwivelFactor -policy <policy-to-check-
     swivel-image> -priority 10
6 <!--NeedCopy-->
```

Remarque : Téléchargez SwiveLimage.xml à partir du loginschema utilisé dans l'exemple.

Pseudo facteur pour la configuration du contrôle de groupe :

```
1 add authentication policylabel GroupCheckFactor
2
3 add authentication policy contractors_auth_policy -rule 'http.req.
     user.is_member_of( "contractors" )' -action NO_AUTHN
4
5 add authentication policy not_contractors _auth_policy -rule true -
     action NO_AUTHN
6
```



```
bind authentication policylabel GroupCheckFactor -policy
    contractors_auth_policy -pri 10 -nextFactor SwivelFactor

bind authentication policylabel GroupCheckFactor -policy
    not_contractors_auth_policy -pri 20
<!--NeedCopy-->
```

Premier facteur pour la connexion à Active Directory :

```
add ldapAction <>

add authentication policy user_login_auth_policy -rule true -action
    <>

bind authentication vserver <> -policy user_login_auth_policy -pri 10
    -nextFactor GroupCheckFactor
<!--NeedCopy-->
```

Dans la configuration, trois facteurs sont spécifiés dont un est implicite/pseudo.

Schéma de connexion utilisé dans cet exemple

Voici un exemple de schéma avec des informations d'identification pivotantes et une zone de texte.

Remarque : lors de la copie de données pour le navigateur Web, les guillemets peuvent s'afficher différemment. Copiez des données dans des éditeurs comme le bloc-notes avant de les enregistrer dans des fichiers.

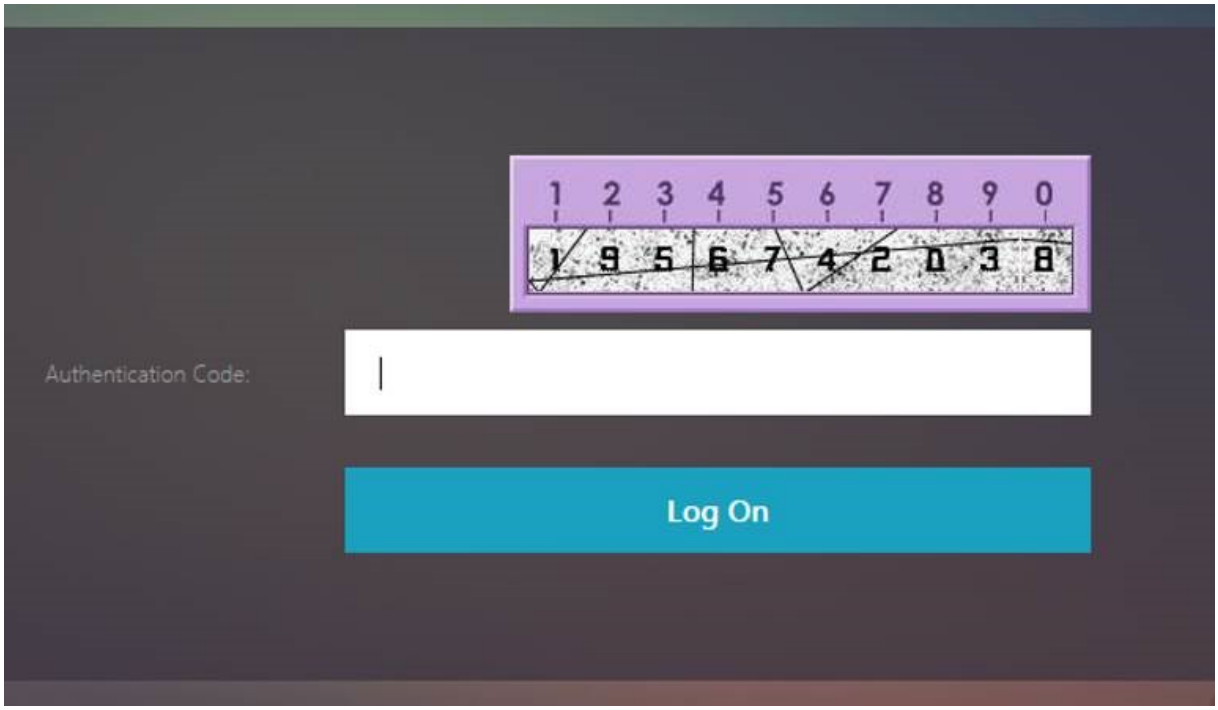
```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
    /1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>swivel_cred</ID><Type>swivel_cred</Type><
    Input><Text><Hidden>true</Hidden><InitialValue>${
 http.req.user.name }
 </InitialValue></Text></Input></Credential></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password
    </SaveID><Type>password</Type></Credential><Label><Text>Password:</
```



```
      Text><Type>plain</Type></Label><Input><Text><Secret>true</Secret><
      ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint
      >.+</Constraint></Text></Input></Requirement>
15 <Requirement><Credential><Type>none</Type></Credential><Label><Text>
      Hello ${
16  http.req.user.name }
17  , Please enter passcode from above image.</Text><Type>confirmation</
       Type></Label><Input /></Requirement>
18 <Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials
      </Type></Credential><Label><Text>Remember my password</Text><Type>
      plain</Type></Label><Input><CheckBox><InitialValue>false</
      InitialValue></CheckBox></Input></Requirement>
19 <Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential
      ><Label><Type>none</Type></Label><Input><Button>Log On</Button></
      Input></Requirement>
20 </Requirements>
21 </AuthenticationRequirements>
22 </AuthenticateResponse>
23 <!--NeedCopy-->
```

Résultat

Une fois la configuration effectuée, l'image suivante s'affiche.



Remarque : La hauteur et le placement de l'image peuvent être modifiés dans le JavaScript.

Personnaliser le formulaire d'ouverture de session Citrix ADC nFactor pour afficher ou masquer les champs

L'interface utilisateur RFWeb de Citrix Gateway permet une grande variété de personnalisations. Cette fonctionnalité, associée à la structure d'authentification nFactor, permet aux clients de configurer des flux complexes sans compromettre les flux de travail existants.

Dans cet exemple, deux options d'authentification, OAuth et LDAP sont disponibles à partir de la liste Type d'ouverture de session. Lorsque le formulaire est chargé pour la première fois, les champs nom d'utilisateur et mot de passe (LDAP est affiché en premier) sont affichés. Si OAuth est sélectionné, tous les champs sont masqués car OAuth implique un déchargement de l'authentification vers un serveur tiers. De cette façon, l'administrateur peut configurer des workflows intuitifs selon la commodité de l'utilisateur.

Remarque :

- Les valeurs de la liste Type d'ouverture de session peuvent être modifiées avec des modifications simples au fichier de script.
- Cette section décrit uniquement la partie de l'interface utilisateur du flux. La gestion du temps d'exécution de l'authentification est hors du champ d'application de cet article. Il est recommandé aux utilisateurs de se référer à la documentation nFactor pour la configuration de l'authentification.

Comment personnaliser le formulaire d'ouverture de session nFactor

Personnaliser le formulaire d'ouverture de session nFactor peut être classé en deux parties

- Envoi de loginschema droit à l'interface utilisateur
- Ecrire un gestionnaire pour interpréter les sélections loginschema et utilisateur

Envoyer loginschema droit à l'interface utilisateur

Dans cet exemple, une revendication/exigence simple est envoyée dans le loginschema.

Pour cela, le fichier SingleAuth.xml est modifié. SingleAuth.xml est livré avec le firmware Citrix ADC et se trouve dans le répertoire /nsconfig/loginschema/loginschema.

Étapes pour envoyer loginschema :

1. Connectez-vous via SSH et passez à shell (tapez 'shell').
2. Copiez SingleAuth.xml dans un autre fichier pour modification.

   Remarque : le dossier de destination est différent du dossier loginschemas Citrix ADC par défaut.

cp /nsconfig/loginschema/LoginSchema/SingleAuth.xml /nsconfig/loginschema/SingleAuth-Dynamic.xml

3. Ajoutez la revendication suivante à SingleAuthDynamic.xml.

```
<Requirement><Credential><ID>nsg_dropdown</ID><Type>nsg_dropdown</Type></Credential><Label><Text>Logon Type:</Text><Type>plain</Type></Label></Requirement>
<!--NeedCopy-->
```

4. Configurez Citrix ADC pour envoyer ce loginschema pour charger le premier formulaire.

```
add loginschema single_auth_dynamic -authenticationSchema SingleAuthDynamic.xml

add loginschemaPolicy single_auth_dynamic -rule true -action single_auth_dynamic

bind authentication vserver aaa_nfactor -policy single_auth_dynamic -pri 10
<!--NeedCopy-->
```

Modifications de script pour charger le formulaire et gérer les événements utilisateur

Vous pouvez modifier le JavaScript qui permet à l'administrateur de personnaliser l'affichage du formulaire d'ouverture de session. Dans cet exemple, le champ Nom d'utilisateur et mot de passe s'affiche si LDAP est choisi et sont masqués si OAuth est choisi. L'administrateur peut également masquer uniquement le mot de passe.Les
administrateurs doivent ajouter l'extrait suivant à « script.js » qui se trouve dans le répertoire « /var/netscaler/logon/logonpoint/custom ».

Remarque : Comme ce répertoire est un répertoire global, créez un thème de portail et modifiez le fichier « script.js » dans ce dossier, à"/var/netscaler/logon/themes/<THEME_NAME>".

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the server
    getCredentialTypeName: function () {
  return "nsg_dropdown";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

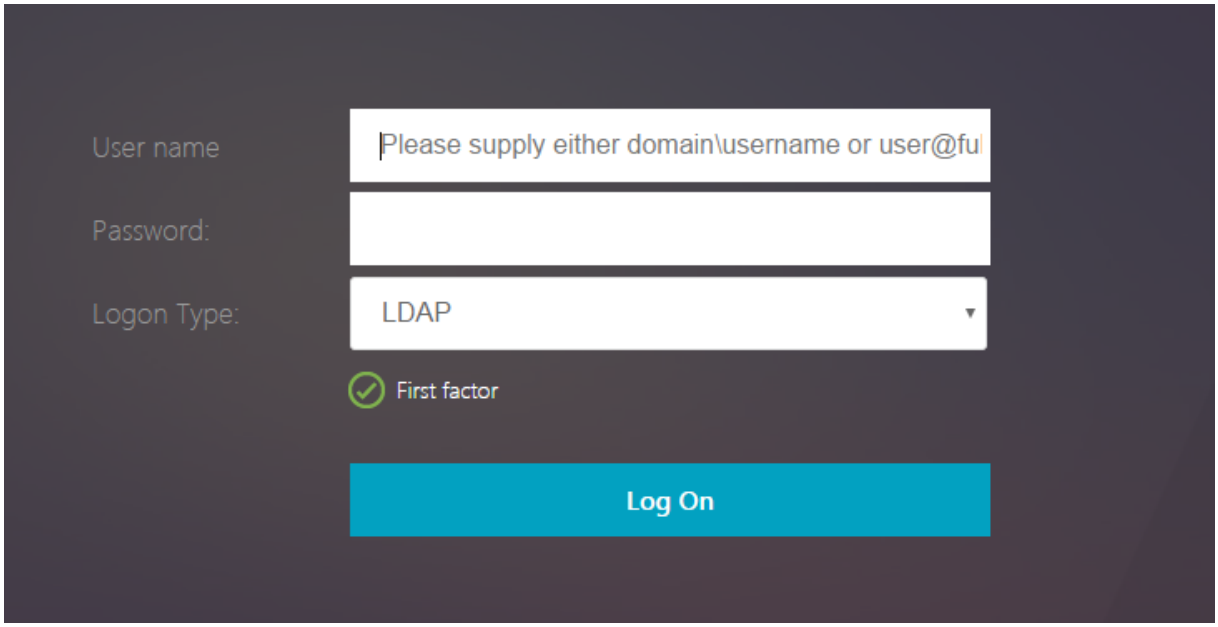
        var div = $("<div></div>");
```



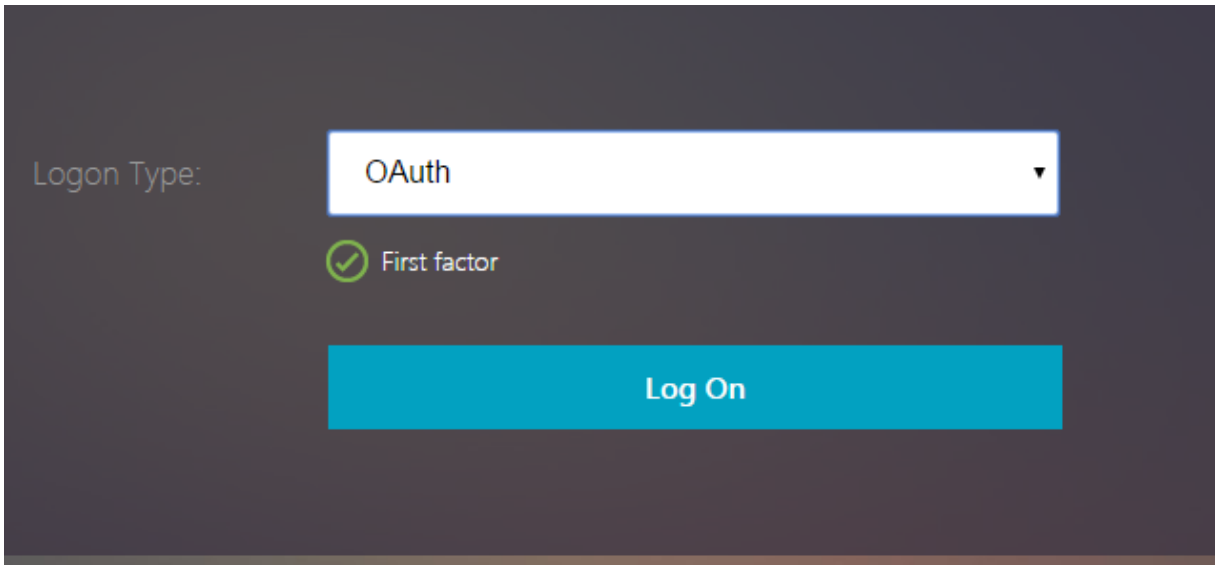
```
11          var select = $("<select name='nsg_dropdown'></select>").attr("
               id", "nsg_dropdown");
12
13          var rsa = $("<option></option>").attr("selected", "selected").
               text("LDAP").val("LDAP");
14          var OAuthID = $("<option></option>").text("OAuth").val("OAuth")
               ;
15          select.append(rsa, OAuthID);
16
17          select.change(function(e) {
18
19              var value = $(this).val();
20              var ldapPwd = $($(".credentialform").find(".
                   CredentialTypepassword")[0]);
21              var ldapUname = $($(".credentialform").find(".
                   CredentialTypeusername"));
22              if(value == "OAuth") {
23
24                  if (ldapPwd.length)
25                          ldapPwd.hide();
26                  if (ldapUname.length)
27                          ldapUname.hide();
28               }
29    else if(value == "LDAP") {
30
31                  if (ldapPwd.length)
32                          ldapPwd.show();
33                  if (ldapUname.length)
34                          ldapUname.show();
35               }
36
37           }
38  );
39        div.append(select);
40         return div;
41      }
42
43  }
44  );
45 <!--NeedCopy-->
```


Expérience utilisateur final

Lorsqu'un utilisateur final charge la page d'ouverture de session pour la première fois, l'écran suivant apparaît.



Si **OAuth** est sélectionné dans **Type d'ouverture de session, les** champs nom d'utilisateur et mot de passe sont masqués.



Si **LDAP** est sélectionné, le nom d'utilisateur et le mot de passe s'affichent. De cette façon, la page d'ouverture de session peut être chargée dynamiquement en fonction de la sélection de l'utilisateur.

Schéma de connexion utilisé dans cet exemple


```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response/1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>login</ID><SaveID>ExplicitForms-Username</SaveID><Type>username</Type></Credential><Label><Text>User name</Text><Type>plain</Type></Label><Input><AssistiveText>Please supply either domain\username or user@fully.qualified.domain</AssistiveText><Text><Secret>false</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password</SaveID><Type>password</Type></Credential><Label><Text>Password:</Text><Type>plain</Type></Label><Input><Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>nsg_dropdown</ID><Type>nsg_dropdown</Type></Credential><Label><Text>Logon Type:</Text><Type>plain</Type></Label></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>First factor</Text><Type>confirmation</Type></Label><Input /></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials</Type></Credential><Label><Text>Remember my password</Text><Type>plain</Type></Label><Input><CheckBox><InitialValue>false</InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential><Label><Type>none</Type></Label><Input><Button>Log On</Button></Input></Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

> **Important :** Pour plus de détails sur divers sujets liés à NFactor, voir nFactor.

Définir un cookie à l'aide de nFactor

January 21, 2021

Vous pouvez appliquer les étiquettes personnalisées NFactor et définir un cookie comme facteur du flux d'authentification. Grâce à des étiquettes personnalisées, vous pouvez utiliser JavaScript pour manipuler le schéma de connexion.

Pour définir un cookie comme facteur, vous n'avez pas besoin d'afficher d'informations à l'utilisateur, ce qui est effectué avec une connexion sans schéma. Au lieu de cela, vous devez interagir avec le navigateur de l'utilisateur pour demander au schéma de connexion de stocker les données souhaitées. Un schéma de connexion est nécessaire pour définir le cookie lorsque la page est chargée. Le cookie est défini avec une étiquette personnalisée et un code JavaScript.

Pour implémenter un facteur qui définit un cookie, créez un fichier XML appelé cookie.xml pour stocker le schéma dans le répertoire /nsconfig/loginschema/ avec le contenu suivant :

```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
   /1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>

<Requirement>
<Credential><ID>nsg_cookie</ID><Type>nsg_cookie</Type></Credential>
<Label><Text>Logon Type:</Text><Type>Plain</Type></Label>
</Requirement>

<Requirement>
<Credential><ID>loginBtn</ID><Type>none</Type></Credential>
<Label><Type>none</Type></Label><Input><Button>Log On</Button></Input>
</Requirement>

</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```


Dans ce XML ;

- L'étiquette personnalisée nsg_cookie est utilisée pour créer le cookie et envoyer le formulaire, et le bouton formulaire.
- RFWEbui_Custom est le nouveau thème Portal basé sur le thème RFWEbui.

Étapes pour définir un cookie à l'aide de NFactor

1. Créez un thème de portail basé sur le thème RFWEbui.

```
add vpn portaltheme RfWebUI_custom -basetheme RfWebUI
<!--NeedCopy-->
```

   Cette commande crée un dossier pour ce thème dans /var/netscaler/logon/themes/RFWEbui_Custom

2. Modifiez le fichier /var/netscaler/logon/themes/RfWebUI_custom/script.js et ajoutez le script suivant :

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the server
    getCredentialTypeName: function () {
  return "nsg_cookie";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $("<div></div>");
        $(document).ready(function() {

        //Set cookie valid for 1000 days
        var exdays = 1000;
        var d = new Date();
        d.setTime(d.getTime() + (exdays\*24\*60\*60\*1000));
        var expires = "expires="+ d.toUTCString();
        document.cookie = "NSC_COOKIE_NAME=CookieValeu;" + expires + ";path=/";

        //Submit form
        document.getElementById('loginBtn').click();
         }
 );
        return div;
```



```
25         }
26
27    }
28    );
29  <!--NeedCopy-->
```

Ce code effectue les opérations suivantes :

- Attend que le navigateur termine le chargement de la page
- Définit un cookie appelé NSC_COOKIE_NAME avec la valeur CookieValue, valide pendant 1000 jours
- Soumet automatiquement le formulaire.

Le cookie est créé et l'utilisateur n'a pas besoin d'interagir avec la page.

3. Créez un schéma de connexion à lier à l'étiquette de stratégie qui représente le facteur de cookie défini.

```
1  add authentication loginSchema Cookie_LS -authenticationSchema "/
      nsconfig/loginschema/cookie.xml"
2  <!--NeedCopy-->
```

4. Créez une stratégie d'authentification NO_AUTHN à lier à l'étiquette de stratégie qui représente le facteur de cookie défini.

```
1  add authentication Policy NO_AUTHN_POL -rule TRUE -action NO_AUTHN
2  <!--NeedCopy-->
```

Cette stratégie est toujours évaluée comme true, en déplaçant l'utilisateur vers le facteur suivant ou en terminant le flux d'authentification.

5. Liez le thème de portail RFWEbui_Custom au serveur virtuel Citrix Gateway ou au serveur virtuel Citrix ADC AAA.

Exemples de déploiements utilisant l'authentification nFactor

January 21, 2021

Voici les exemples de déploiements utilisant l'authentification NFactor :

- Obtenir deux mots de passe avant, passer dans le facteur suivant. Read
- Extraction de groupe suivie d'une authentification par certificat ou LDAP, basée sur l'appartenance à un groupe. Read

- SAML suivi d'une authentification LDAP ou de certificat, basée sur les attributs extraits pendant SAML. Read
- SAML dans le premier facteur, suivi de l'extraction de groupe, puis LDAP ou authentification de certificat, basé sur les groupes extraits. Read
- Préremplissage du nom d'utilisateur à partir du certificat. Read
- Authentification de certificat suivie d'une extraction de groupe pour 401 serveurs virtuels de gestion du trafic activés. Read
- Nom d'utilisateur et deux mots de passe avec extraction de groupe en troisième facteur. Read
- Repli de certificat vers LDAP dans la même cascade ; un serveur virtuel pour l'authentification de certificat et LDAP. Read
- LDAP dans le premier facteur et WebAuth dans le second facteur. Read
- Domaine liste déroulante dans le premier facteur, puis différentes évaluations de stratégie basées sur le groupe. Read

Liste des articles pratiques

October 5, 2021

Les articles « Comment faire » sur l'authentification, l'autorisation et l'audit sont simples, pertinents et faciles à mettre en œuvre. Ces articles contiennent des informations sur certaines des fonctionnalités populaires d'authentification, d'autorisation et d'audit telles que l'authentification LDAP et l'authentification multifacteur. Pour obtenir certains des articles les plus populaires sur la configuration et le dépannage de l'authentification via Citrix ADC, consultez Authentification Citrix ADC : Comment faire ?

Analyse des points de terminaison

Configurer l'analyse Endpoint Analysis de pré-authentification en tant que facteur d'authentification nFactor

Configurer l'analyse Endpoint Analysis post-authentification en tant que facteur dans l'authentification Citrix ADC nFactor

Configurer l'analyse EPA de pré-authentification et de post-authentification en tant que facteur d'authentification nFactor

Configurer l'analyse périodique d'Endpoint Analysis en tant que facteur d'authentification nFactor

Configurer l'analyse EPA de pré-authentification Citrix Gateway pour la vérification du domaine

Combinaisons de configuration du premier facteur et du deuxième facteur

Configurez nFactor pour Citrix Gateway avec WebAuth dans le premier facteur et LDAP avec changement de mot de passe dans le second facteur

Configurez SAML suivi de l'authentification LDAP ou de certificat basée sur l'extraction d'attributs SAML dans l'authentification nFactor

Configurez l'authentification de certificat comme premier facteur et LDAP comme deuxième facteur dans l'authentification Citrix ADC nFactor

Configurez l'authentification à deux facteurs avec un schéma de connexion et un schéma de relais dans l'authentification Citrix ADC nFactor

Configurer le nom d'utilisateur et deux mots de passe avec l'extraction de groupe en troisième facteur par l'authentification nFactor

Configurer la liste déroulante du domaine, le nom d'utilisateur et le champ mot de passe dans le premier facteur et l'évaluation de stratégie en fonction des groupes du facteur suivant

Configurer l'extraction de groupe basée sur l'ID de messagerie (ou nom d'utilisateur) au premier facteur pour décider du flux d'authentification du facteur suivant

Configurer une liste déroulante de domaine pour la saisie de l'utilisateur dans le premier facteur afin de décider du prochain flux d'authentification du facteur

CLUF en tant que facteur d'authentification

Configurer le CLUF en tant que facteur d'authentification dans le système Citrix ADC nFactor

Préremplissage du nom d'utilisateur à partir du certificat

Configurer le nom d'utilisateur de préremplissage à partir du certificat dans l'authentification Citrix ADC nFactor

Authentification par étapes

Configurer NFactor pour les applications ayant des exigences de site de connexion différentes, y compris l'authentification par étapes

Authentification SAML

January 21, 2021

SAML (Security Assertion Markup Language) est un mécanisme d'authentification XML qui fournit une fonctionnalité d'authentification unique et est défini par le comité technique des services de sécurité OASIS.

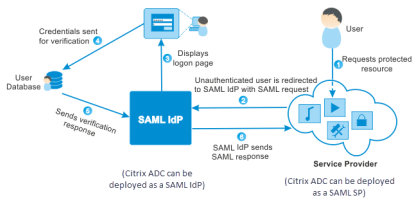
> Remarque
>
> À partir de NetScaler 12.0 Build 51.x, l'appliance Citrix ADC utilisée comme fournisseur de services SAML avec authentification Multi-Factor (nFactor) préremplit désormais le champ nom d'utilisateur sur la page de connexion. L'appliance envoie un attribut NameID dans le cadre d'une demande d'autorisation SAML, extrait la valeur de l'attribut NameID du fournisseur d'identité Citrix ADC SAML (IdP) et préremplit le champ nom d'utilisateur.

Pourquoi utiliser l'authentification SAML

Considérez un scénario dans lequel un fournisseur de services (LargeProvider) héberge un certain nombre d'applications pour un client (BigCompany). BigCompany a des utilisateurs qui doivent accéder de façon transparente à ces applications. Dans une configuration traditionnelle, LargeProvider devrait gérer une base de données des utilisateurs de BigCompany. Cela soulève certaines préoccupations pour chacun des intervenants suivants :

- LargeProvider doit assurer la sécurité des données utilisateur.
- BigCompany doit valider les utilisateurs et tenir les données utilisateur à jour, non seulement dans sa propre base de données, mais aussi dans la base de données utilisateur gérée par LargeProvider. Par exemple, un utilisateur supprimé de la base de données BigCompany doit également être supprimé de la base de données LargeProvider.
- Un utilisateur doit se connecter individuellement à chacune des applications hébergées.

Le mécanisme d'authentification SAML offre une approche alternative. Le diagramme de déploiement suivant illustre le fonctionnement de SAML (flux initié par le SP).



Les préoccupations soulevées par les mécanismes traditionnels d'authentification sont résolues comme suit :

- LargeProvider n'a pas besoin de gérer une base de données pour les utilisateurs de BigCompany. Libéré de la gestion des identités, LargeProvider peut se concentrer sur la fourniture de meilleurs services.
- BigCompany ne supporte pas le fardeau de s'assurer que la base de données utilisateur LargeProvider est synchronisée avec sa propre base de données utilisateur.

- Un utilisateur peut ouvrir une session une fois sur une application hébergée sur LargeProvider et être automatiquement connecté aux autres applications qui y sont hébergées.

L'appliance Citrix ADC peut être déployée en tant que fournisseur de services SAML (SP) et fournisseur d'identité SAML (IdP). Lisez les rubriques pertinentes pour comprendre les configurations qui doivent être effectuées sur le dispositif Citrix ADC.

Une appliance Citrix ADC configurée en tant que fournisseur de services SAML peut désormais appliquer une vérification des restrictions d'audience. La condition de restriction d'audience est évaluée à « Valide » uniquement si la partie de réponse SAML est membre d'au moins une des audiences spécifiées.

Vous pouvez configurer une appliance Citrix ADC pour analyser les attributs dans les assertions SAML en tant qu'attributs de groupe. Leur analyse en tant qu'attributs de groupe permet à l'appliance de lier des stratégies aux groupes.

Citrix ADC en tant que SP SAML

August 20, 2021

Le fournisseur de services (SP) SAML est une entité SAML déployée par le fournisseur de services. Lorsqu'un utilisateur tente d'accéder à une application protégée, le SP évalue la demande du client. Si le client n'est pas authentifié (ne dispose pas d'un cookie NSC_TMAA ou NSC_TMAS valide), le SP redirige la demande vers le fournisseur d'identité SAML (IdP).

Le SP valide également les assertions SAML reçues de l'IdP.

Lorsque l'appliance Citrix ADC est configurée en tant que SP, toutes les demandes utilisateur sont reçues par un serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu) associé à l'action SAML correspondante.

L'appliance Citrix ADC prend également en charge les liaisons POST et Redirection lors de la déconnexion.

> **Remarque**
>
> Une appliance Citrix ADC peut être utilisée en tant que SP SAML dans un déploiement où l'IdP SAML est configuré sur l'appliance ou sur n'importe quel IdP SAML externe.

Lorsqu'il est utilisé en tant que SP SAML, une appliance Citrix ADC :

- Peut extraire les informations utilisateur (attributs) du jeton SAML. Ces informations peuvent ensuite être utilisées dans les stratégies configurées sur l'appliance Citrix ADC. Par exemple, si vous souhaitez extraire les attributs GroupMember et Emailaddress, dans le champ SAMLAction,

spécifiez le paramètre **Attribute2** en tant que GroupMember et le paramètre **Attribute3** en tant qu'adresse e-mail.

> **Remarque**
>
> Les attributs par défaut tels que le nom d'utilisateur, le mot de passe et l'URL de déconnexion ne doivent pas être extraits dans les attributs 1 à 16, car ils sont implicitement analysés et stockés dans la session.

- Peut extraire des noms d'attributs allant jusqu'à 127 octets à partir d'une assertion SAML entrante. La limite précédente était de 63 octets.
- Prend en charge les liaisons de poste, de redirection et d'artefact.

  > **Remarque**
  >
  > La liaison de redirection ne doit pas être utilisée pour une grande quantité de données, lorsque l'assertion après gonflage ou décodage est supérieure à 10K.

- Peut décrypter les assertions.
- Peut extraire des attributs à valeurs multiples à partir d'une assertion SAML. Ces attributs sont envoyés est des balises XML imbriquées telles que :

  <AttributeValue> <AttributeValue>Value1</AttributeValue>
  <AttributeValue>Value2</AttributeValue>
  </AttributeValue>

  > **Remarque**
  >
  > À partir de Citrix ADC 13.0 Build 63.x et supérieur, la longueur maximale individuelle des attributs SAML a été augmentée pour permettre un maximum de 40 000 octets. La taille de tous les attributs ne doit pas dépasser 40 000 octets.

  Lorsqu'il est présenté avec XML précédent, l'appliance Citrix ADC peut extraire Value1 et Value2 en tant que valeurs d'un attribut donné, par opposition à l'ancien firmware qui extrait uniquement Value1.

- Peut spécifier la validité d'une assertion SAML.

  Si l'heure système sur Citrix ADC SAML IdP et le SP SAML homologue n'est pas synchronisée, les messages peuvent être invalidés par l'une ou l'autre partie. Pour éviter de tels cas, vous pouvez maintenant configurer la durée pendant laquelle les assertions sont valides.

  Cette durée, appelée « temps d'inclinaison », spécifie le nombre de minutes pendant lesquelles le message doit être accepté. Le temps d'inclinaison peut être configuré sur le SP SAML et l'IdP SAML.

- Peut envoyer un attribut supplémentaire appelé 'ForceAuth' dans la demande d'authentification à un IdP externe (Identity Provider). Par défaut, la valeur ForceAuthn est définie sur « False ». Il

peut être défini sur « True » pour suggérer au IdP de forcer l'authentification malgré le contexte d'authentification existant. En outre, Citrix ADC SP effectue une demande d'authentification dans le paramètre de requête lorsqu'il est configuré avec la liaison d'artefact.

Pour configurer l'appliance Citrix ADC en tant que SP SAML à l'aide de l'interface de ligne de commande

1. Configurez une action SP SAML.

   Exemple

   La commande suivante ajoute une action SAML qui redirige les demandes utilisateur non authentifiées.

   ```
   add authentication samlAction SamlSPAct1 -samlIdPCertName nssp -samlSigningCertNa
    nssp -samlRedirectUrl https://auth1.example.com -relaystateRule "AAA.
   LOGIN.RELAYSTATE.EQ(\"https://lb.example1.com/\")"
   ```

   Points à noter

   - Le certificat prévu `-samlIdPCertName` dans la commande SamlAction doit correspondre au certificat correspondant de l'IdP pour que la vérification de la signature réussisse.
   - SAML prend uniquement en charge le certificat RSA. Les autres certificats tels que HSM, FIPS, etc. ne sont pas pris en charge.
   - Citrix recommande d'avoir un nom de domaine complet avec «/» dans l'expression.
   - Les administrateurs doivent configurer une expression pour **RelaysStateRule** dans la commande SamlAction. L'expression doit contenir la liste des domaines publiés auxquels l'utilisateur se connecte avant d'être redirigé vers le serveur virtuel d'authentification. Par exemple, l'expression doit contenir les domaines du serveur virtuel frontal (VPN, LB ou CS) qui utilise cette action SAML pour l'authentification.

   Pour plus de détails sur la commande, reportez-vous https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction aux sections et https://support.citrix.com/article/CTX316577.

2. Configurez la stratégie SAML.

   Exemple

   La commande suivante définit une stratégie SAML qui applique l'action SAML précédemment définie à tout le trafic.

   ```
   add authentication policy SamlSPPol1 -rule true -action SamlSPAct1
   ```

3. Liez la stratégie SAML au serveur virtuel d'authentification.

   Exemple

La commande suivante lie la stratégie SAML à un serveur virtuel d'authentification nommé « av_saml ».

```
bind authentication vserver av_saml -policy SamlSPPol1
```

4. Liez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic approprié.

   Exemple

   La commande suivante ajoute un serveur virtuel d'équilibrage de charge nommé « lb1_ssl » et associe le serveur virtuel d'authentification nommé « av_saml » au serveur virtuel d'équilibrage de charge.

   ```
   add lb vserver lb1_ssl SSL 10.217.28.224 443 -persistenceType NONE -
   cltTimeout 180 -AuthenticationHost auth1.example.com -Authentication ON
    -authnVsName av_saml
   ```

   Pour plus de détails sur la commande, consultez https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction

Pour configurer une appliance Citrix ADC en tant que SP SAML à l'aide de l'interface graphique

1. Accédez à **Sécurité>Stratégies AAA->Authentification>Stratégies de base>SAML**.
2. Sélectionnez l'onglet **Serveurs**, cliquez sur **Ajouter**, entrez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   Description du paramètre :

   Nom : nom du serveur

   URL de redirection - URL contre laquelle les utilisateurs s'authentifieront. Certains IdP ont des URL spéciales qui ne sont pas accessibles sauf dans la configuration SAML.

   URL de déconnexion unique : URL spécifiée pour que Citrix ADC puisse reconnaître quand renvoyer le client à l'IdP pour terminer le processus de déconnexion. Nous ne l'utiliserons pas dans ce simple déploiement.

   Liaison SAML - Méthode utilisée pour déplacer le client du SP vers l'IdP. Cela doit être le même sur l'IdP afin qu'il comprenne comment le client va s'y connecter.
   Lorsque Citrix ADC agit en tant que SP, il prend en charge les liaisons POST, REDIRECT et ARTIFACT.

   Reliure de déconnexion - REDIRECT

   Nom du certificat IDP - Certificat IDPCert (Base64) présent sous le certificat de signature SAML.

   Champ utilisateur : section du formulaire d'authentification SAML de l'IdP qui contient le nom d'utilisateur que le SP doit extraire si nécessaire.

Nom du certificat de signature : sélectionnez le certificat SP SAML (avec clé privée) utilisé par Citrix ADC pour signer des demandes d'authentification à l'IdP. Le même certificat (sans clé privée) doit être importé sur l'IdP, de sorte que l'IdP puisse vérifier la signature de la demande d'authentification. Ce champ n'est pas nécessaire à la plupart des déplacés internes.

Nom de l'émetteur - Identifiant. ID unique spécifié sur le SP et l'IdP pour aider à identifier le fournisseur de services entre eux.

Rejeter l'assertion non signée - Option que vous pouvez spécifier si vous souhaitez que les assertions de l'IdP soient signées. Vous pouvez vous assurer que seule l'assertion doit être signée (ON) ou que l'assertion et la réponse de l'IdP doivent être signées (STRICT).

Audience - Audience pour laquelle une assertion envoyée par IdP est applicable. Il s'agit généralement d'un nom d'entité ou d'une URL qui représente ServiceProvider.

Algorithme de signature - RSA-SHA256

Méthode de digest - SHA256

Groupe d'authentification par défaut : groupe par défaut choisi lorsque l'authentification réussit en plus des groupes extraits.

Champ Nom du groupe : nom de la balise dans l'assertion contenant des groupes d'utilisateurs.

Temps d'inclinaison (minutes) : cette option spécifie l'inclinaison d'horloge autorisée en nombre de minutes que Citrix ADC ServiceProvider autorise sur une assertion entrante.

3. De même, créez une stratégie SAML correspondante et liez-la au serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**et associez la stratégie SAML au serveur virtuel d'authentification.

4. Associez le serveur d'authentification au serveur virtuel de gestion du trafic approprié.

   Accédez à **Gestion du trafic > Équilibrage de charge** (ou **Commutation de contenu**) > **Serveurs virtuels**, sélectionnez le serveur virtuel et associez le serveur virtuel d'authentification à celui-ci.

Citrix ADC en tant qu'IdP SAML

August 20, 2021

L'IdP SAML (Identity Provider) est une entité SAML déployée sur le réseau client. L'IdP reçoit des demandes du SP SAML et redirige les utilisateurs vers une page d'ouverture de session, où ils doivent entrer leurs informations d'identification. L'IdP authentifie ces informations d'identification avec Active Directory (serveur d'authentification externe, tel que LDAP), puis génère une assertion SAML envoyée au SP.

Le SP valide le jeton, et l'utilisateur est ensuite autorisé à accéder à l'application protégée demandée.

Lorsque l'appliance Citrix ADC est configurée en tant qu'IdP, toutes les demandes sont reçues par un serveur virtuel d'authentification associé au profil IdP SAML approprié.

> **Remarque**
>
> Une appliance Citrix ADC peut être utilisée comme IdP dans un déploiement où le SP SAML est configuré sur l'appliance ou sur n'importe quel SP SAML externe.

Lorsqu'il est utilisé en tant qu'IdP SAML, une appliance Citrix ADC :

- Prend en charge toutes les méthodes d'authentification qu'il prend en charge pour les ouvertures de session traditionnelles.
- Signature numérique des assertions.
- Prend en charge l'authentification à un facteur et à deux facteurs. SAML ne doit pas être configuré comme mécanisme d'authentification secondaire.
- Peut chiffrer les assertions à l'aide de la clé publique du SP SAML. Ceci est recommandé lorsque l'assertion inclut des informations sensibles.
- Peut être configuré pour accepter uniquement les demandes signées numériquement à partir du SP SAML.
- Vous pouvez vous connecter à l'IdP SAML à l'aide des mécanismes d'authentification basés sur 401 suivants : Negotiate, NTLM et Certificate.
- Peut être configuré pour envoyer 16 attributs en plus de l'attribut NameID. Les attributs doivent être extraits du serveur d'authentification approprié. Pour chacun d'eux, vous pouvez spécifier le nom, l'expression, le format et un nom convivial dans le profil IdP SAML.
- Si l'appliance Citrix ADC est configurée en tant qu'IdP SAML pour plusieurs SP SAML, un utilisateur peut accéder aux applications sur les différents SP sans s'authentifier explicitement à chaque fois. L'appliance Citrix ADC crée un cookie de session pour la première authentification, et chaque requête ultérieure utilise ce cookie pour l'authentification.
- Peut envoyer des attributs à plusieurs valeurs dans une assertion SAML.
- Prend en charge les liaisons de poste et de redirection. La prise en charge de la liaison d'artefact est introduite dans Citrix ADC version 13.0 Build 36.27.
- Peut spécifier la validité d'une assertion SAML.

  Si l'heure système sur Citrix ADC SAML IdP et le SP SAML homologue n'est pas synchronisée, les messages peuvent être invalidés par l'une ou l'autre partie. Pour éviter de tels cas, vous pouvez maintenant configurer la durée pendant laquelle les assertions sont valides.

Cette durée, appelée « temps d'inclinaison », spécifie le nombre de minutes pour lesquelles le message doit être accepté. Le temps d'inclinaison peut être configuré sur le SP SAML et l'IdP SAML.

- Peut être configuré pour servir des assertions uniquement aux SP SAML préconfigurés sur ou approuvés par l'IdP. Pour cette configuration, l'IdP SAML doit avoir l'ID du fournisseur de services (ou le nom de l'émetteur) des SP SAML concernés.

> **Remarque**
>
> Avant de continuer, assurez-vous que vous disposez d'un serveur virtuel d'authentification lié à un serveur d'authentification LDAP.

Pour configurer une appliance Citrix ADC en tant qu'IdP SAML à l'aide de l'interface de ligne de commande

1. Configurez un profil IdP SAML.

   Exemple

   Ajout d'une appliance Citrix ADC en tant qu'IdP avec SiteMinder en tant que SP.

```
add authentication samlIdPProfile samlIDPProf1 -samlSPCertName siteminder
-cert -encryptAssertion ON -samlIdPCertName ns-cert -assertionConsumerServiceURL
 http://sm-proxy.nsi-test.com:8080/affwebservices/public/saml2assertionconsumer
 -rejectUnsignedRequests ON -signatureAlg RSA-SHA256 -digestMethod
SHA256 -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.REGEX_MATCH(re##^https://
example2\.com/cgi/samlauth$##)
```

   Points à noter

   - Dans le profil IdP SAML, configurez **AcSurlRule** qui prend une expression de la liste des URL de fournisseurs de services applicables à cet IdP. Cette expression dépend du SP utilisé. Si Citrix ADC est configuré en tant que SP, l'URL ACS le sera `https://<SP-domain_name>/cgi/samlauth`. Citrix recommande d'avoir une URL complète dans l'expression pour correspondre.
   - SAML prend uniquement en charge le certificat RSA. Les autres certificats tels que HSM, FIPS, etc. ne sont pas pris en charge.
   - Vous devez spécifier le début du domaine avec le signe « ^ » (exemple : ^https) ainsi que le signe dollar « $ » à la fin de la chaîne (exemple : samlauth$).

   Pour plus de détails sur la commande, reportez-vous https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction aux sections et https://support.citrix.com/article/CTX316577.

2. Configurez la stratégie d'authentification SAML et associez le profil IdP SAML comme action de la stratégie.

   ```
   add authentication samlIdPPolicy samlIDPPol1 -rule true -action samlIDPProf1
   ```

3. Liez la stratégie au serveur virtuel d'authentification.

   ```
   bind authentication vserver saml-auth-vserver -policy samlIDPPol1 -
   priority 100
   ```

   Pour plus de détails sur la commande, reportez-vous à la section https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlIdPProfile.

Pour configurer une appliance Citrix ADC en tant qu'IdP SAML à l'aide de l'interface graphique

1. Accédez à **Sécurité>Stratégies AAA->Authentification>Stratégies avancées>IdP SAML**.
2. Sélectionnez l'onglet **Serveurs**, cliquez sur **Ajouter**, entrez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   Description du paramètre :

   URL Assertion Consumer Service - URL vers laquelle l'utilisateur authentifié sera redirigé.

   Nom du certificat IdP : paire de clés de certificat utilisée pour la page d'authentification.

   Nom du certificat SP - Certificat du fournisseur de services dans ce scénario, la clé n'est pas requise pour cela.

   Signer l'assertion : option permettant de signer l'assertion et la réponse lors de la redirection du client vers le fournisseur de services.

   Nom de l'émetteur - Identifiant. ID unique spécifié sur le SP et l'IdP pour aider à identifier le fournisseur de services entre eux.

   ID du fournisseur de services - ID unique qui sera spécifié à la fois sur le SP et l'IdP pour aider à identifier le fournisseur de services entre eux. Il peut s'agir de n'importe quoi et ne doit pas nécessairement correspondre à l'URL spécifiée ci-dessous, mais doit être la même sur les profils SP et IdP.

   Rejeter les demandes non signées - Option que vous pouvez spécifier pour garantir que seules les assertions signées avec le certificat SP sont acceptées.

   Algorithme de signature - Algorithme utilisé pour signer et vérifier les assertions entre l'IdP et le SP, ce qui doit être le même pour les profils IdP et SP.

Méthode Digest - Algorithme utilisé pour vérifier l'intégrité des assertions entre l'IdP et le SP, ce qui doit être le même pour les profils IdP et SP.

Liaison SAML : identique à celle décrite dans le profil SP, elle doit être la même sur le SP et sur l'IdP.

3. Associez la stratégie IdP SAML à un serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**et associez la stratégie IdP SAML au serveur virtuel d'authentification.

Configuration de l'authentification unique SAML

October 5, 2021

Pour fournir des fonctionnalités d'authentification unique aux applications hébergées sur le fournisseur de services, vous pouvez configurer l'authentification unique SAML sur le SP SAML.

Configuration de l'authentification unique SAML à l'aide de l'interface de ligne de commande

1. Configurez le profil SSO SAML.

   Exemple

   Dans la commande suivante, Exemple est le serveur virtuel d'équilibrage de charge doté d'un lien Web depuis le portail SharePoint. NSSP.Example.com est le serveur virtuel de gestion du trafic qui équilibrent la charge du serveur SharePoint.

   ```
   add tm samlSSOProfile tm-saml-sso -samlSigningCertName nssp -assertionConsumerSer
    "https://nssp2.example.com/cgi/samlauth"-relaystateRule "\\"https://
   nssp2.example.com/samlsso.html\\"" -sendPassword ON -samlIssuerName
   nssp.example.com<!--NeedCopy-->
   ```

2. Associez le profil SSO SAML à l'action de trafic.

   Exemple

   La commande suivante active l'accès SSO et lie le profil SSO SAML créé ci-dessus à une action de trafic.

   ```
   add tm trafficAction html\\_act -SSO ON -samlSSOProfile tm-saml-sso<!--
   NeedCopy-->
   ```

3. Configurez la stratégie de trafic qui spécifie quand l'action doit être exécutée.

   Exemple

La commande suivante associe l'action de trafic à une stratégie de trafic.

```
add tm trafficPolicy html_pol "HTTP.REQ.URL.CONTAINS(\\"abc.html\\")"
html_act<!--NeedCopy-->
```

4. Liez la stratégie de trafic créée précédemment à un serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu). Alternativement, la stratégie de trafic peut être associée globalement.

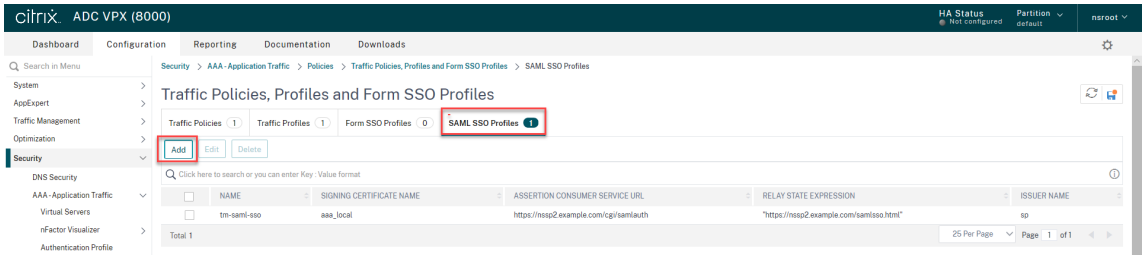
> **Remarque**
>
> Ce serveur virtuel de gestion du trafic doit être associé au serveur virtuel d'authentification approprié associé à l'action SAML.

```
bind lb vserver lb1_ssl -policyName html_pol -priority 100 -gotoPriorityExpressio
 END -type REQUEST<!--NeedCopy-->
```

Configuration de l'authentification unique SAML à l'aide de l'interface graphique

Pour configurer l'authentification unique SAML, vous devez définir le profil SSO SAML, le profil de trafic et la stratégie de trafic et lier la stratégie de trafic à un serveur virtuel de gestion du trafic ou globalement à l'appliance Citrix ADC.

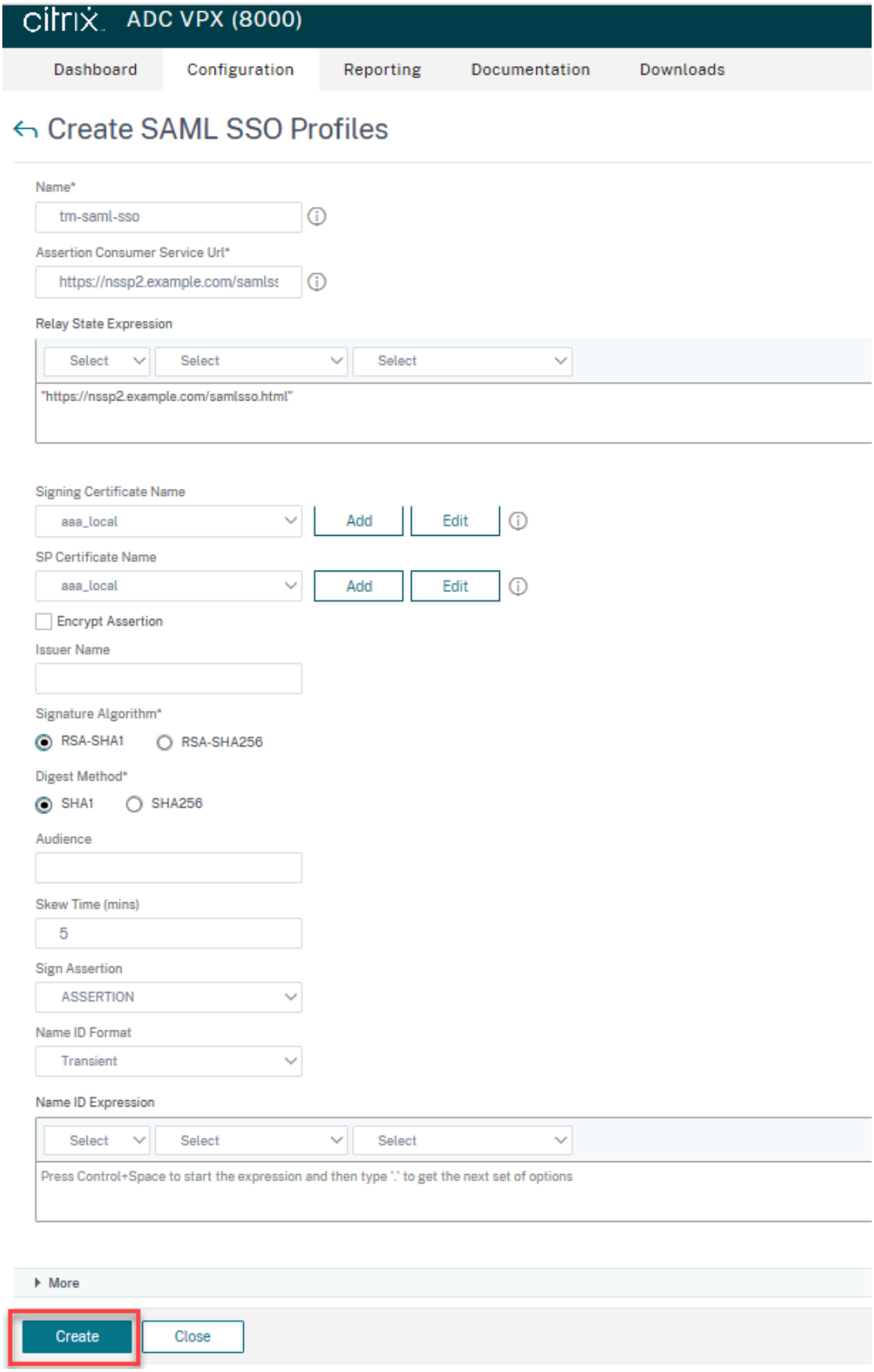
1. Accédez à **Sécurité > Trafic des applications AAA > Stratégies > Trafic > Profils SSO SAML**, puis cliquez sur **Ajouter**.



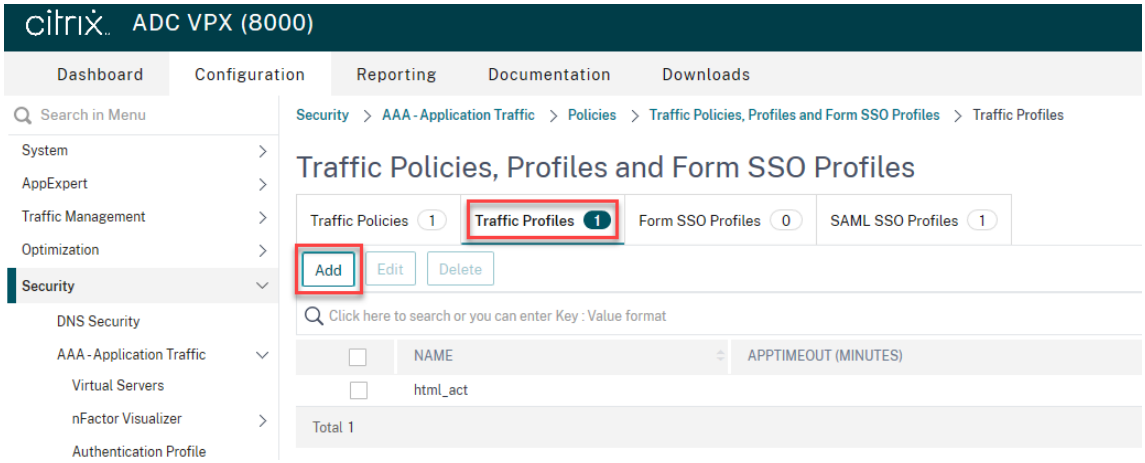
2. Sur la page **Créer des profils SSO SAML**, entrez les valeurs des champs suivants, puis cliquez sur **Créer**.

   - Nom : nom du profil SSO SAML
   - Assertion Consumer Service Url - URL à laquelle l'assertion doit être envoyée
   - Nom du certificat de signature : nom du certificat SSL utilisé pour signer une assertion
   - Nom du certificat SP : nom du certificat SSL d'un homologue/destinataire utilisant lequel l'assertion est chiffrée
   - Nom de l'émetteur : nom à utiliser dans les demandes envoyées de Citrix ADC à l'IdP pour identifier Citrix ADC de manière unique.
   - Algorithme de signature - Algorithme à utiliser pour signe/vérifier les transactions SAML

- Méthode Digest - Audience pour laquelle une assertion envoyée par IdP est applicable. Il s'agit généralement d'un nom d'entité ou d'une URL qui représente un fournisseur de services.
- Audience - Audience pour laquelle une assertion envoyée par IdP est applicable. Il s'agit généralement d'un nom d'entité ou d'une URL qui représente un fournisseur de services.
- Temps d'inclinaison (minutes) : nombre de minutes de chaque côté de l'heure actuelle pendant lesquelles l'assertion serait valide
- Sign Assertion : option permettant de signer des parties d'assertion lorsque Citrix ADC IDP en envoie une. En fonction de la sélection de l'utilisateur, l'assertion ou la réponse ou les deux ou aucun ne peut être signé.
- Format d'ID de nom : format de l'identificateur de nom envoyé dans l'assertion
- Expression d'ID de nom - Expression qui sera évaluée pour obtenir NameIdentifier à envoyer dans une assertion

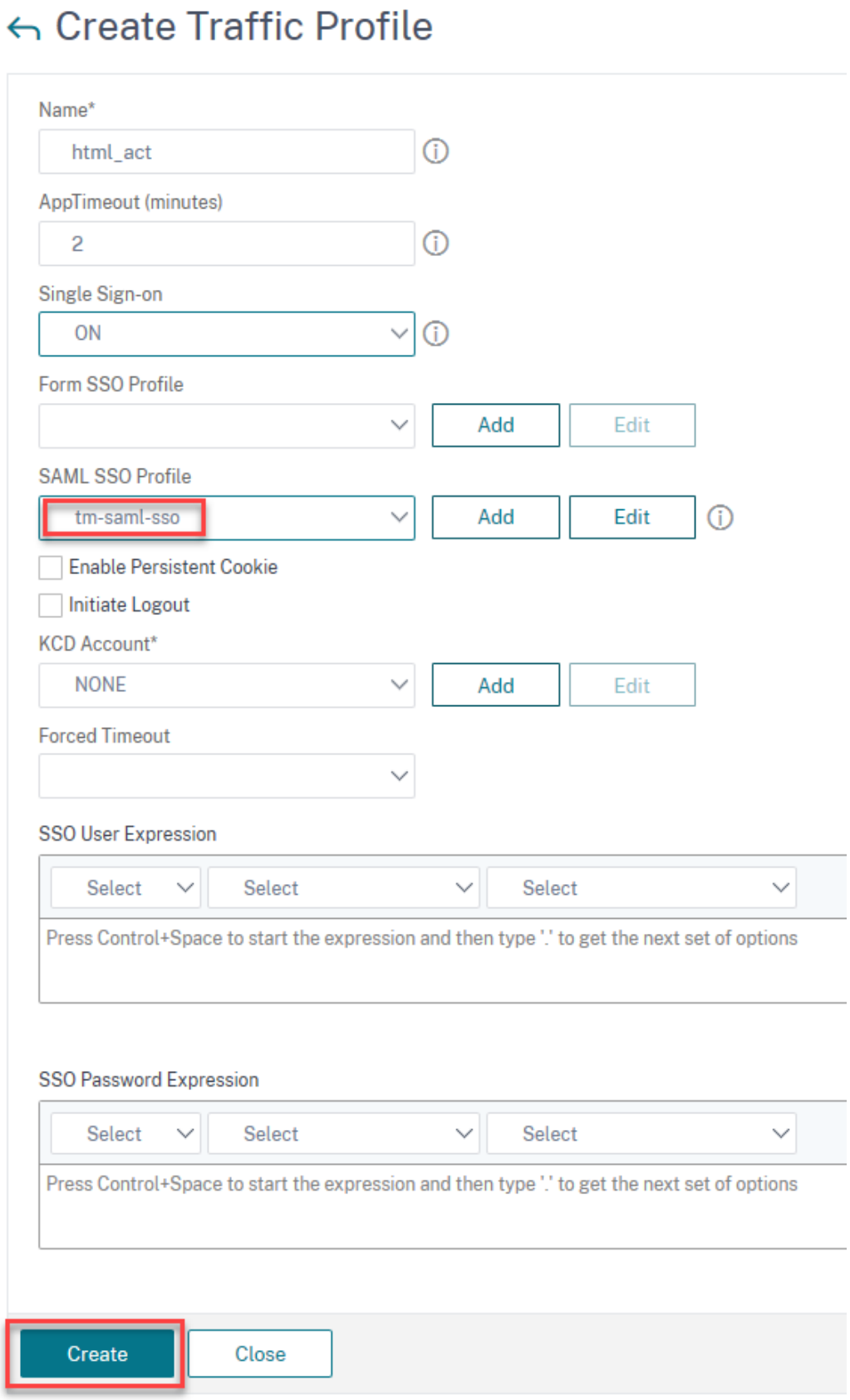


3. Accédez à **Sécurité > Trafic des applications AAA > Stratégies> Trafic > Profils de trafic**, puis cliquez sur **Ajouter**.

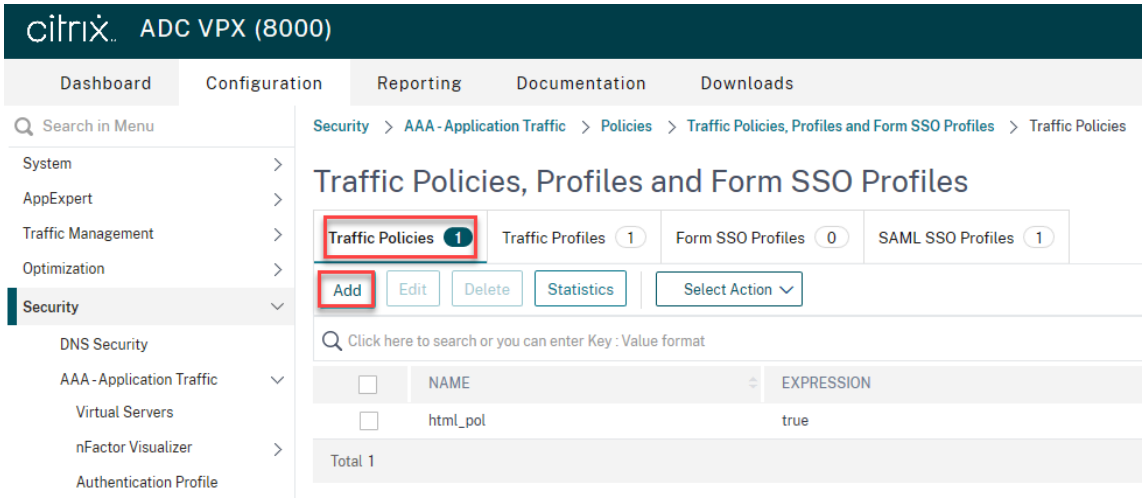


4. Sur la page **Créer un profil de trafic**, entrez des valeurs pour les champs suivants, puis cliquez sur **Créer**.

   - Nom : nom de l'action de trafic.
   - AppTimeout (minutes) - Intervalle de temps, en minutes, d'inactivité de l'utilisateur après lequel la connexion est fermée.
   - Single Sign-On - Sélectionnez ON
   - Profil SSO SAML - Sélectionnez le profil SSSO SAML créé
   - Compte KCD - Nom de compte de délégation contrainte Kerberos
   - Expression utilisateur SSO - Expression qui sera évaluée pour obtenir le nom d'utilisateur pour SingleSignon
   - Expression de mot de passe SSO - Expression qui sera évaluée pour obtenir le mot de passe pour SingleSignon

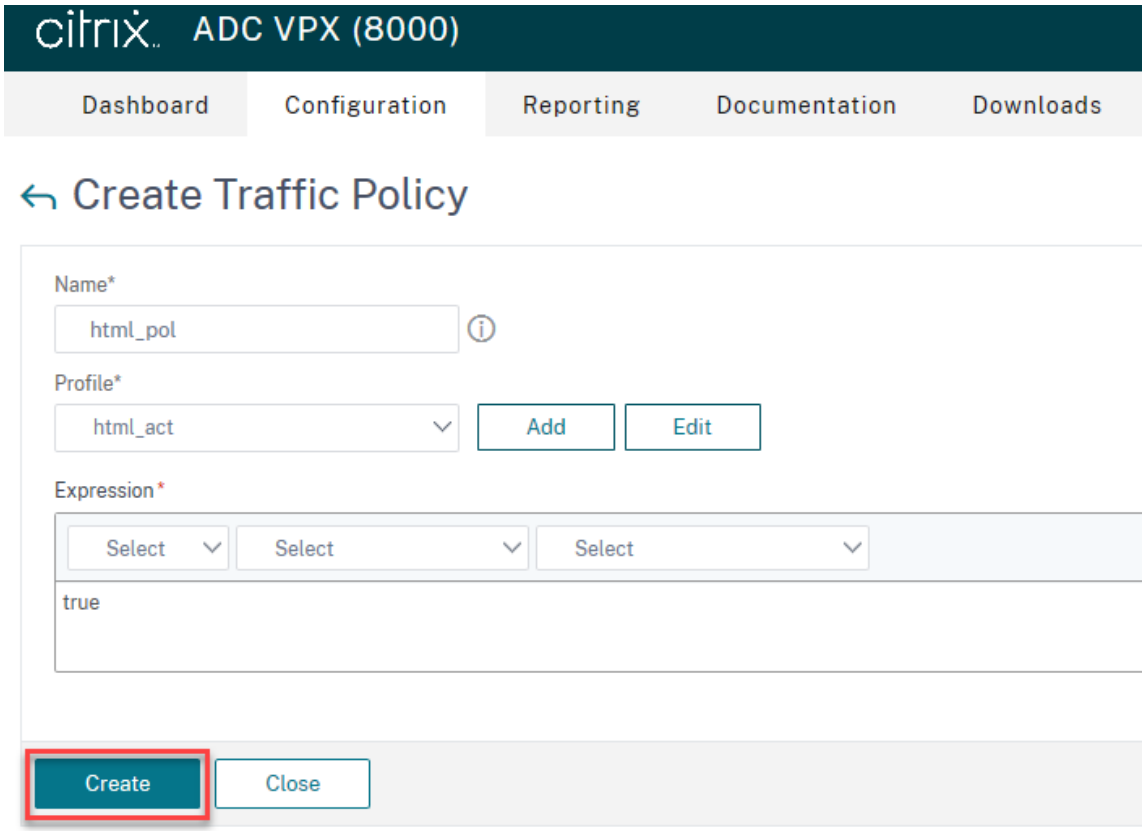


5. Accédez à **Sécurité > Trafic des applications AAA > Stratégies > Trafic > Stratégies de trafic**, puis cliquez sur **Ajouter**.

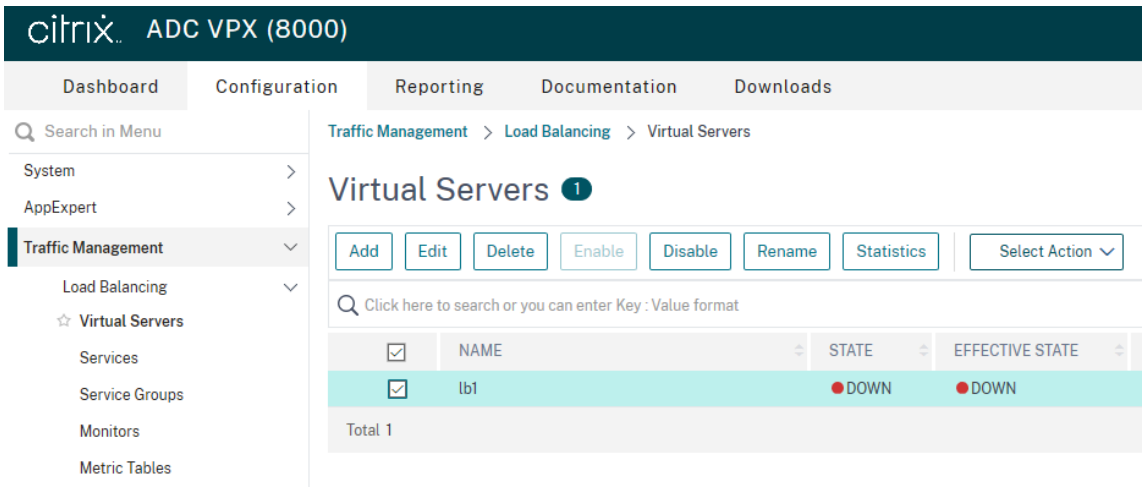


6. Sur la page **Créer une stratégie de trafic**, entrez les valeurs suivantes, puis cliquez sur **Créer**.

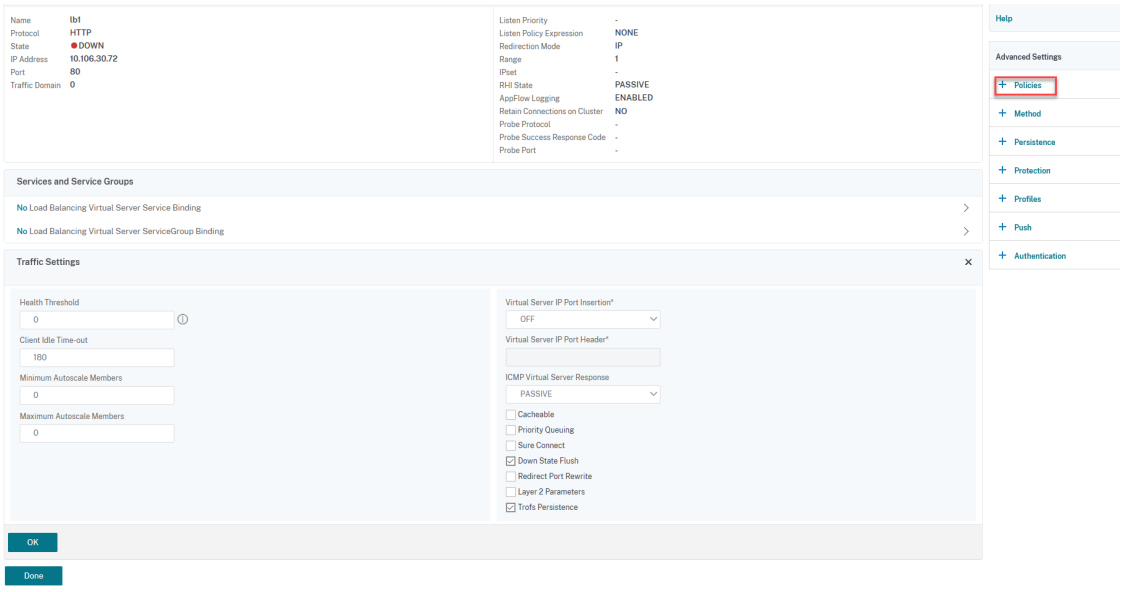
   - Nom : nom de la stratégie de trafic à créer.
   - Profil : sélectionnez le profil de trafic créé
   - Expression : expression de stratégie avancée utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, vrai.



7. Pour lier la stratégie de trafic à un serveur virtuel de gestion du trafic, sélectionnez un serveur virtuel.



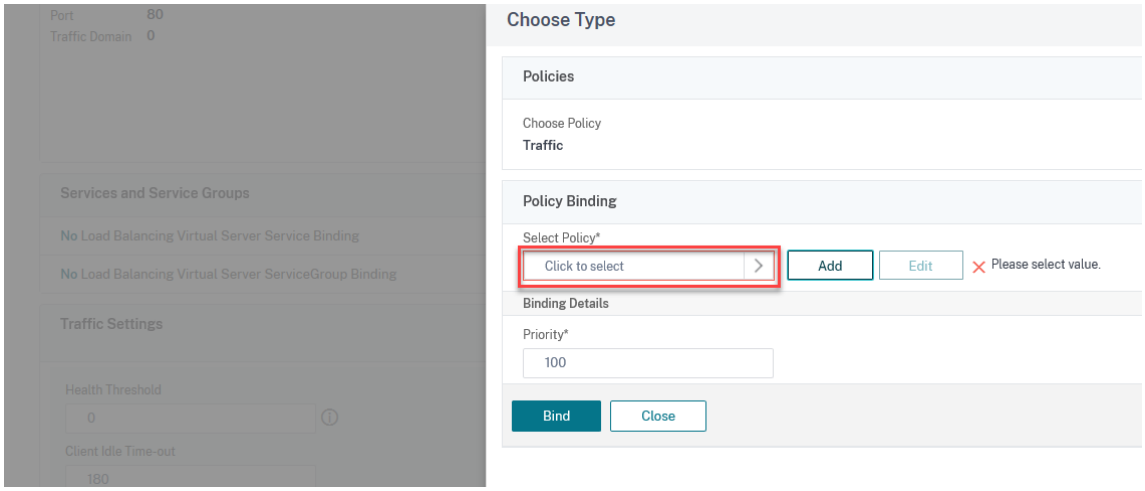
8. Cliquez sur **Stratégies**.



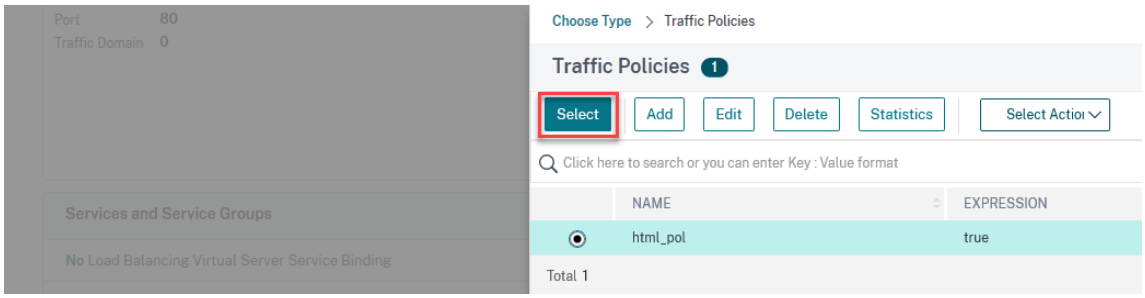
9. Sélectionnez **Trafic** dans le champ **Choisir une stratégie** et sélectionnez **Demander** dans le champ **Choisir un type**, puis cliquez sur **Continuer**.

   ! [Cliquez ici pour ajouter une stratégie (/en-us/citrix-adc/media/saml-9.png)

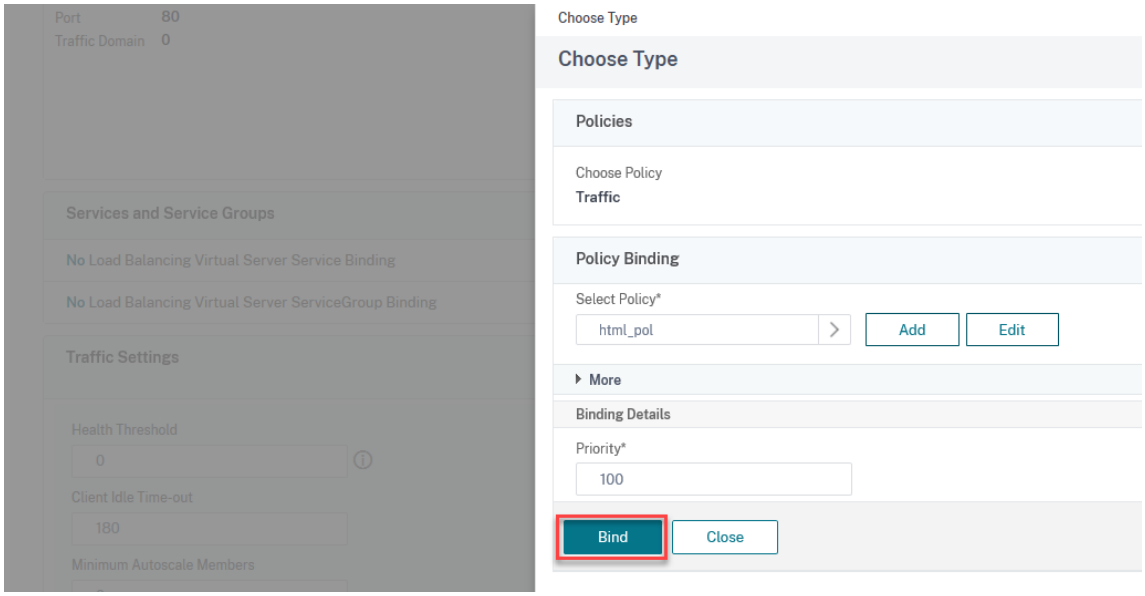
10. Sous le champ **Sélectionner une stratégie**, cliquez sur pour sélectionner le trafic créé.



11. Cliquez sur **Sélectionner**.



12. Cliquez sur **Lier pour lier** la stratégie de trafic au serveur virtuel.



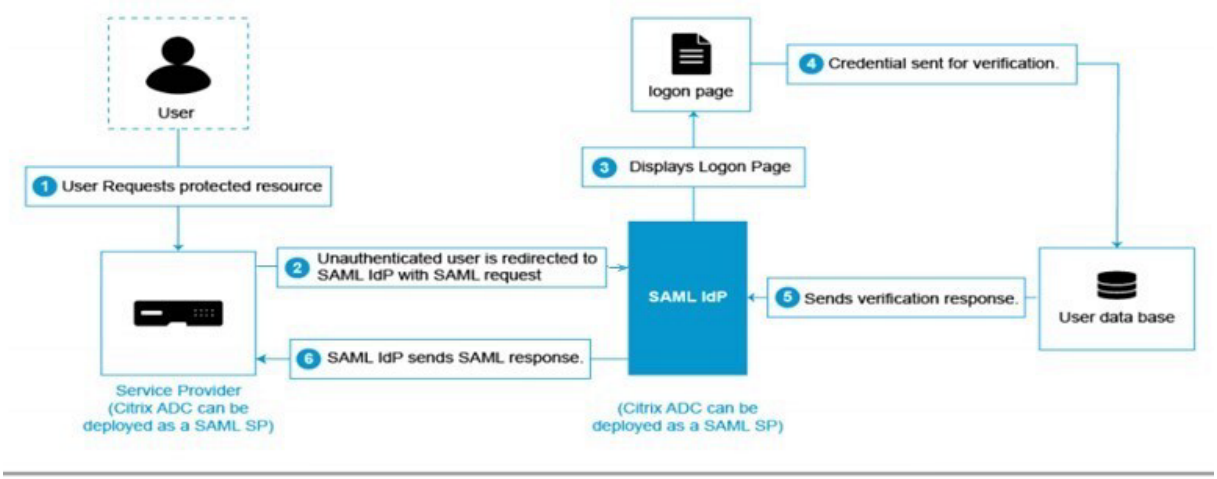
Configurer Azure AD en tant que fournisseur d'identité SAML et Citrix ADC en tant que SP SAML

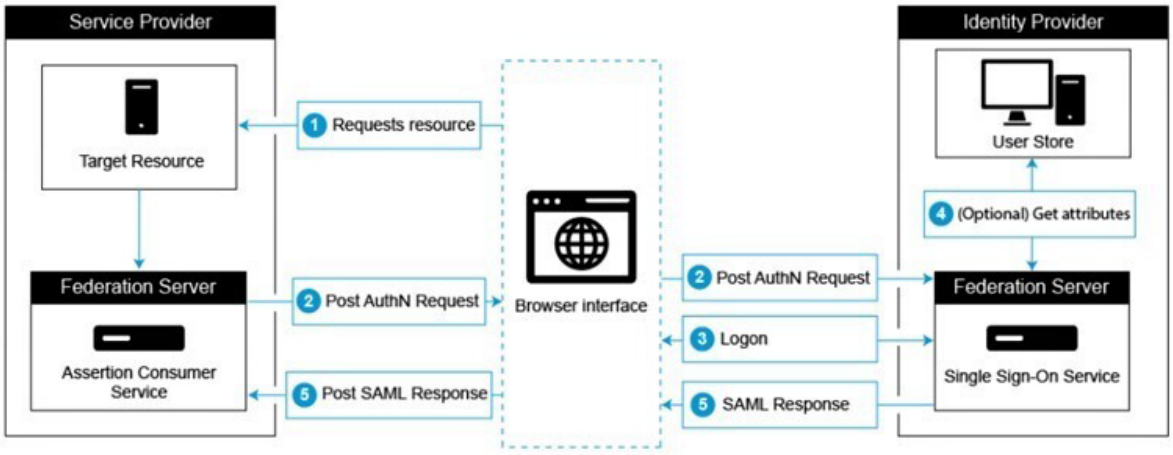
August 20, 2021

Le fournisseur de services SAML (SP) est une entité SAML déployée par le fournisseur de services. Lorsqu'un utilisateur tente d'accéder à une application protégée, le SP évalue la demande du client. Si le client n'est pas authentifié (ne dispose pas d'un cookie NSC_TMAA ou NSC_TMAS valide), le SP redirige la demande vers le fournisseur d'identité SAML (IdP). Le SP valide également les assertions SAML reçues de l'IdP.

L'IdP SAML (Identity Provider) est une entité SAML déployée sur le réseau client. L'IdP reçoit des demandes du SP SAML et redirige les utilisateurs vers une page d'ouverture de session, où ils doivent entrer leurs informations d'identification. L'IdP authentifie ces informations d'identification avec le répertoire utilisateur (serveur d'authentification externe, tel que LDAP), puis génère une assertion SAML envoyée au SP. Le SP valide le jeton, et l'utilisateur est ensuite autorisé à accéder à l'application protégée demandée.

Le diagramme suivant illustre le mécanisme d'authentification SAML.

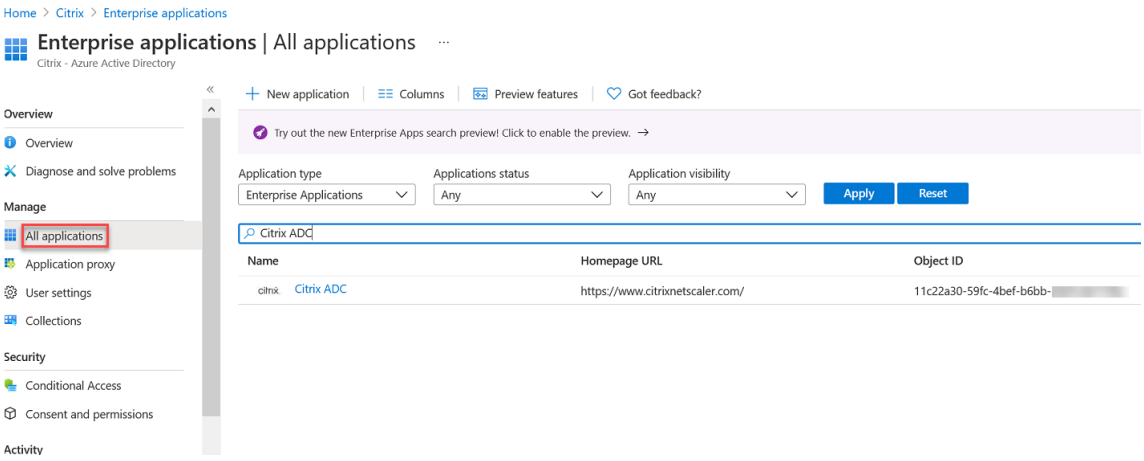




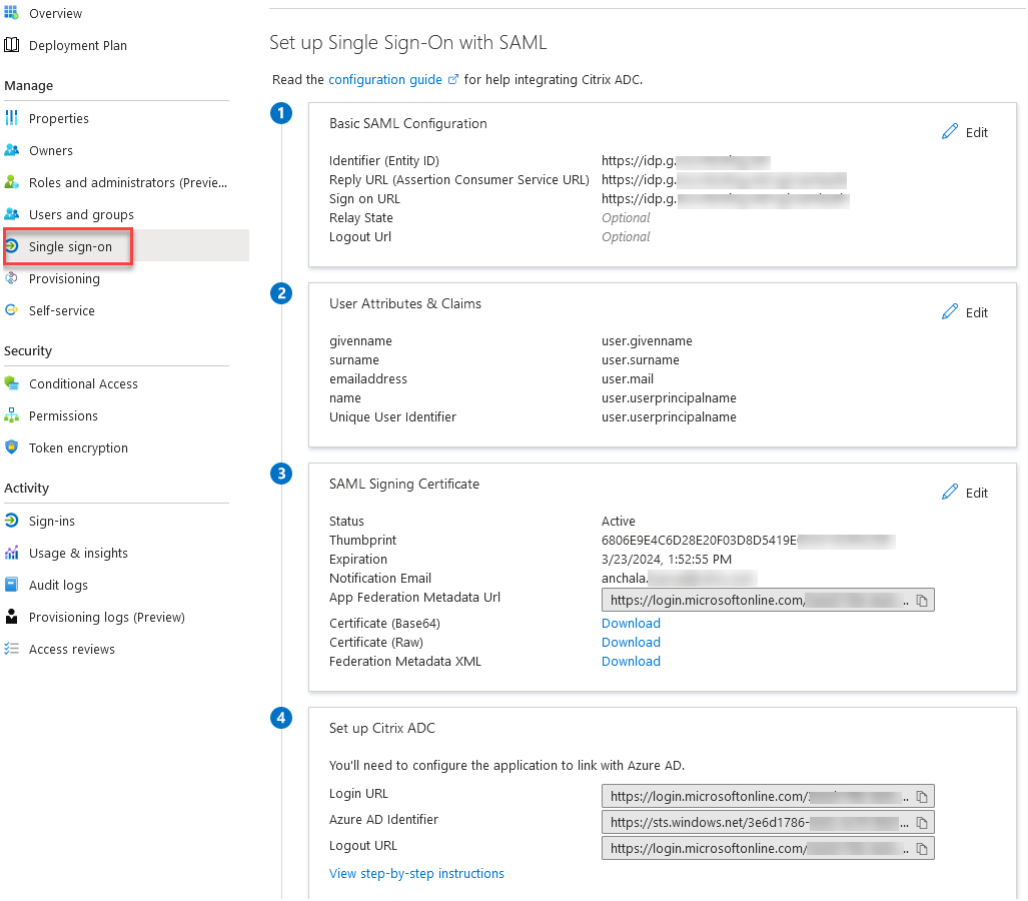
Configurations côté Azure AD

Configurez les paramètres d'authentification unique :

1. Sur le portail Azure, cliquez sur **Azure Active Directory**.
2. Sous la section **Gérer** dans le volet de navigation, cliquez sur **Applications d'entreprise**. Un échantillon aléatoire des applications de votre locataire Azure AD apparaît.
3. Dans la barre de recherche, saisissez Citrix ADC.



4. Dans la section **Gérer**, sélectionnez **Single Sign-On**.
5. Sélectionnez **SAML** pour configurer l'authentification unique. La page **Configurer l'authentification unique avec SAML - Aperçu** apparaît. Ici, Azure agit en tant qu'IdP SAML.
6. Téléchargez le certificat (Base64) présent sous le **certificat de signature SAML** à utiliser comme SamlidPcertName lors de la configuration de Citrix ADC en tant que SP SAML.



7. **Configurez les options SAML de base :**

Identifiant (ID d'entité) : requis pour certaines applications. Identifie de manière unique l'application pour laquelle l'authentification unique est en cours de configuration. Azure AD envoie l'identificateur à l'application en tant que paramètre d'audience du jeton SAML. L'application est censée le valider. Cette valeur apparaît également sous la forme d'ID d'entité dans toutes les métadonnées SAML fournies par l'application.

URL de réponse - Obligatoire. Spécifie l'endroit où l'application s'attend à recevoir le jeton SAML. L'URL de réponse est également appelée URL ASSERTION Consumer Service (ACS).

URL de connexion - Lorsqu'un utilisateur ouvre cette URL, le fournisseur de services redirige vers Azure AD pour s'authentifier et se connecter à l'utilisateur.

État du relais : indique à l'application où rediriger l'utilisateur une fois l'authentification terminée.

Configurations côté Citrix ADC

1. Accédez à **Sécurité>Stratégies AAA->Authentification>Stratégies de base>SAML**.
2. Sélectionnez l'onglet **Serveurs**, cliquez sur **Ajouter**, entrez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   Description du paramètre :

   La valeur des paramètres en gras doit être extraites des configurations côté Azure.

   Nom : nom du serveur

   URL de redirection - Entrez l'URL de connexion utilisée précédemment dans la section « Configuration de Citrix ADC » d'Azure AD. `https://login.microsoftonline.com/3e6d1786-4e0c-4c70-86d2-ae7811f97f79/saml2`

   URL de déconnexion unique - `https://login.microsoftonline.com/3e6d1786-4e0c-4c70-86d2-ae7811f97f79/saml2`

   Reliure SAML - POST

   Reliure de déconnexion - REDIRECT

   Nom du certificat IDP - Certificat IDPCert (Base64) présent sous le certificat de signature SAML.

   Champ utilisateur - UserPrincipalName. Pris de la section « Attributs et revendications de l'utilisateur » d'Azure IdP.

   Nom du certificat de signature - Non nécessaire pour Azure AD. Sélectionnez le certificat SP SAML (avec clé privée) utilisé par Citrix ADC pour signer des demandes d'authentification à l'IdP. Le même certificat (sans clé privée) doit être importé sur l'IdP, de sorte que l'IdP puisse vérifier la signature de la demande d'authentification. Ce champ n'est pas nécessaire à la plupart des déplacés internes.

IssuerName - Identifiant. `https://idp.g.nssvctesting.net`

Rejeter une assertion non signée - ON

Audience - Audience pour laquelle une assertion envoyée par IdP est applicable. Il s'agit généralement d'un nom d'entité ou d'une URL qui représente ServiceProvider.

Algorithme de signature - RSA-SHA256

Méthode de digest - SHA256

Groupe d'authentification par défaut : groupe par défaut choisi lorsque l'authentification réussit en plus des groupes extraits.

Champ Nom du groupe : nom de la balise dans l'assertion contenant des groupes d'utilisateurs.

Temps d'inclinaison (minutes) : cette option spécifie l'inclinaison d'horloge autorisée en nombre de minutes que Citrix ADC ServiceProvider autorise sur une assertion entrante.

Deux facteurs - OFF

Contexte d'authentification demandé - exact

Type de classe d'authentification - Aucune

Envoyer une empreinte de pouce - OFF

Appliquer le nom d'utilisateur - ON

Forcer l'authentification - OFF

Réponse SAML de stockage - OFF

De même, créez une stratégie SAML correspondante et liez-la au serveur virtuel d'authentification.

Remarque : Azure AD ne s'attend pas au champ Objet ID dans la demande SAML. Pour que Citrix ADC n'envoie pas le champ ID du sujet, tapez la commande suivante à l'invite de commandes Citrix ADC.

```
nsapimgr_wr.sh -ys call="ns_saml_dont_send_subject"
```

Fonctionnalités supplémentaires prises en charge pour SAML

August 20, 2021

Les fonctionnalités suivantes sont pris en charge pour SAML.

Prise en charge de la lecture et de la génération des métadonnées pour la configuration du SP et de l'IdP SAML

L'appliance Citrix ADC prend désormais en charge les fichiers de métadonnées en tant que moyens d'entités de configuration pour le fournisseur de services SAML (SP) et le fournisseur d'identité (IdP).

Le fichier de métadonnées est un fichier XML structuré qui décrit la configuration d'une entité. Les fichiers de métadonnées pour le SP et IdP sont séparés. En fonction du déploiement, et parfois, une entité SP ou IdP peut disposer de plusieurs fichiers de métadonnées.
En tant qu'administrateur, vous pouvez exporter et importer des fichiers de métadonnées (SAML SP et IdP) sur Citrix ADC.
Les fonctionnalités d'exportation et d'importation de métadonnées pour le SP et IdP SAML sont expliquées dans les sections suivantes.

Exportation de métadonnées pour le SP SAML

Prenons un exemple où Citrix ADC est configuré en tant que SP SAML et qu'un IdP SAML souhaite importer des métadonnées contenant la configuration SP Citrix ADC. Supposons que l'appliance Citrix ADC est déjà configurée avec un attribut « SAMLAction » qui spécifie la configuration du SP SAML.

Pour exporter des métadonnées à partir d'utilisateurs ou d'administrateurs, interroger Citrix Gateway ou serveur virtuel d'authentification comme indiqué ci-dessous :

```
1 https://vserver.company.com/metadata/samlsp/<action-name>
```

Importation de métadonnées pour SAML SP

Actuellement, la configuration SAML Action sur l'appliance Citrix ADC prend différents paramètres. L'administrateur les spécifie manuellement. Cependant, les administrateurs ne sont souvent pas au courant de la nomenclature s'il s'agit d'interopérabilité avec différents systèmes SAML. Si les métadonnées de IdP sont disponibles, la majeure partie de la configuration dans l'entité 'SAMLAction' peut être évitée. En fait, toute la configuration spécifique à l'IdP peut être omise si le fichier de métadonnées IdP est fourni. L'entité 'SAMLAction' prend désormais un paramètre supplémentaire pour lire la configuration à partir du fichier de métadonnées.

Lorsque vous importez des métadonnées dans un dispositif Citrix ADC, les métadonnées ne contiennent aucun algorithme de signature à utiliser, elles contiennent les détails du point de terminaison. Une métadonnées peut être signée avec certains algorithmes qui peuvent être utilisés pour vérifier les métadonnées elles-mêmes. Les algorithmes ne sont pas stockés dans l'entité 'SAMLAction'.

Par conséquent, ce que vous spécifiez dans l'entité 'SamlAction' sont ceux utilisés lors de l'envoi des données. Une donnée entrante peut contenir un algorithme différent pour une appliance Citrix ADC à traiter.

Pour récupérer les fichiers de métadonnées à l'aide de l'interface de ligne de commande.

```
1 set samlAction <name> [-metadataUrl <url> [-metadataRefreshInterval <
      int>] https://idp.citrix.com/samlidp/metadata.xml
```


> **Remarque**
>
> Le paramètre MetadatareFreshInterval est l'intervalle en minutes pour récupérer les informations de métadonnées à partir de l'URL de métadonnées spécifiée. Valeur par défaut 36000.

Importation de métadonnées pour IdP SAML

Le paramètre "samlIdPProfile" prend un nouvel argument pour lire toute la configuration spécifique au SP. La configuration SAML IdP peut être simplifiée en remplaçant les propriétés spécifiques du SP par un fichier de métadonnées SP. Ce fichier est interrogé via HTTP.

Pour lire à partir du fichier de métadonnées à l'aide de l'interface de ligne de commande :

```
set samlIdPProfile <name> [-metadataUrl <url>] [-
    metadataRefreshInterval <int>]
```

Prise en charge des attributs nom-valeur pour l'authentification SAML

Vous pouvez désormais configurer les attributs d'authentification SAML avec un nom unique ainsi que des valeurs. Les noms sont configurés dans le paramètre d'action SAML et les valeurs sont obtenues en interrogeant les noms. En spécifiant la valeur de l'attribut name, les administrateurs peuvent facilement rechercher la valeur d'attribut associée au nom de l'attribut. De plus, les administrateurs n'ont plus à se souvenir de l'attribut par sa seule valeur.

> **Important**
>
> - Dans la commande SamlAction, vous pouvez configurer un maximum de 64 attributs séparés par une virgule avec une taille totale inférieure à 2048 octets.
> - Citrix vous recommande d'utiliser la liste des attributs. L'utilisation de « l'attribut 1 à l'attribut 16 » entraînera l'échec de la session si la taille de l'attribut extrait est grande.

Pour configurer les attributs nom-valeur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add authentication samlAction <name> [-Attributes <string>]
```

Exemple :

```
add authentication samlAction samlAct1 -attributes  "mail,sn,
    userprincipalName"
```


Prise en charge de l'URL du service de consommation d'assertion pour IdP SAML

Une appliance Citrix ADC configurée en tant que fournisseur d'identité SAML (IdP) prend désormais en charge l'indexation ACS (Assertion Consumer Service) pour traiter la demande de fournisseur de services (SP) SAML. L'IdP SAML importe la configuration d'indexation ACS à partir des métadonnées SP ou permet de saisir manuellement les informations d'index ACS.
Le tableau suivant répertorie certains articles spécifiques aux déploiements où l'appliance Citrix ADC est utilisée en tant que SP SAML ou IdP SAML.

Le tableau suivant répertorie certains articles spécifiques aux déploiements où l'appliance Citrix ADC est utilisée en tant que SP SAML ou IdP SAML.

SAML SP	Fournisseur d'identité SAML	Lien d'information
Citrix ADC	Microsoft Azure AD	support Citrix
Okta	Citrix ADC	support Citrix
AWS	Citrix ADC	support Citrix

Quelques informations sur d'autres déploiements spécifiques :

- NetScaler en tant que SP SAML sur un périphérique FIPS
- Configuration d'Office365 pour Single Sign-On avec NetScaler en tant qu'IdP SAML

Prise en charge des types d'informations d'identification WebView pour les mécanismes d'authentification

L'authentification d'une appliance Citrix ADC peut désormais prendre en charge le protocole AuthV3. Le type d'informations d'identification WebView dans le protocole Authv3 prend en charge tous les types de mécanismes d'authentification (y compris SAML et OAuth). Le type d'informations d'identification WebView fait partie de Authv3, qui est implémenté par Citrix Receiver et le navigateur dans les applications Web.

L'exemple suivant explique le flux des événements WebView via Citrix Gateway et Citrix Receiver :

1. Citrix Receiver négocie avec Citrix Gateway pour la prise en charge du protocole AuthV3.
2. L'appliance Citrix ADC répond positivement et suggère une URL de démarrage spécifique.
3. Citrix Receiver se connecte ensuite au point de terminaison (URL) spécifique.
4. Citrix Gateway envoie une réponse au client pour démarrer WebView.
5. Citrix Receiver démarre WebView et envoie la demande initiale à l'appliance Citrix ADC.
6. L'appliance Citrix ADC redirige l'URI vers le point de terminaison de connexion du navigateur.
7. Une fois l'authentification terminée, l'appliance Citrix ADC envoie une réponse d'achèvement à WebView.

8. Le WebView se ferme maintenant et donne le contrôle à Citrix Receiver pour continuer le protocole Authv3 pour l'établissement de session.

Augmentation de la taille de SessionIndex dans le SP SAML

La taille SessionIndex du fournisseur de services (SP) SAML est augmentée à 96 octets. Auparavant, la taille maximale par défaut de SessionIndex était de 63 octets.

> **Remarque**
>
> Prise en charge introduite dans NetScaler 13.0 Build 36.x

Prise en charge des références de classe d'authentification personnalisée pour le SP SAML

Vous pouvez configurer l'attribut de référence de classe d'authentification personnalisée dans la commande action SAML. À l'aide de l'attribut de référence de classe d'authentification personnalisé, vous pouvez personnaliser les noms de classe dans les balises SAML appropriées. L'attribut de référence de classe d'authentification personnalisée ainsi que l'espace de noms sont envoyés à l'IdP SAML dans le cadre de la demande d'authentification SAML SP.

Auparavant, à l'aide de la commande d'action SAML, vous pouviez configurer uniquement un ensemble de classes prédéfinies définies dans l'attribut authNCTXClassRef.

> **Important**
>
> Lors de la configuration de l'attribut CustomAuthNCTXClassRef, assurez-vous de ce qui suit :

- Les noms des classes doivent inclure des caractères alphanumériques ou une URL valide avec des balises XML appropriées.
- Si vous devez configurer plusieurs classes personnalisées, chaque classe doit être séparée par des virgules

Pour configurer les attributs CustomAuthNCTXClassRef à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- add authentication samlAction <name> [-customAuthnCtxClassRef <string>]
- set authentication samlAction <name> [-customAuthnCtxClassRef <string>]

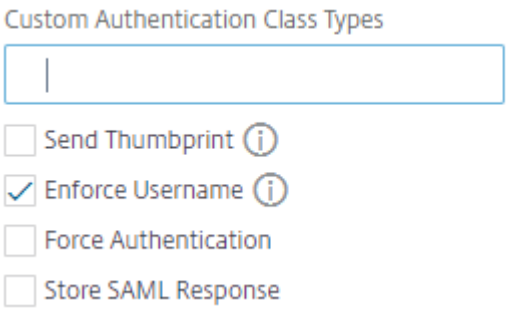
Exemple :

- `add authentication samlAction samlact1 -customAuthnCtxClassRef http://www.class1.com/LoA1,http://www.class2.com/LoA2`

- `set authentication samlAction samlact2 -customAuthnCtxClassRef http://www.class3.com/LoA1,http://www.class4.com/LoA2`

Pour configurer les attributs CustomAuthNCTXClassRef à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Actions > SAML**.
2. Sur la page SAML, sélectionnez l'onglet **Serveurs** et cliquez sur **Ajouter** .
3. Sur la page **Créer une authentification Serveur SAML**, entrez le nom de l'action SAML.
4. Faites défiler la page vers le bas pour configurer les types de classe dans la section **Types de classe d'authentification personnalisée**.



Prise en charge de la liaison d'artefact dans l'IdP SAML

L'appliance Citrix ADC configurée en tant que fournisseur d'identité SAML (IdP) prend en charge la liaison d'artefacts. La liaison d'artefact améliore la sécurité de l'IdP SAML et empêche les utilisateurs malveillants d'inspecter l'assertion.

Prise en charge de l'URL du service de consommation d'assertion pour IdP SAML

Une appliance Citrix ADC configurée en tant que fournisseur d'identité SAML (IdP) prend désormais en charge l'indexation ACS (Assertion Consumer Service) pour traiter la demande de fournisseur de services (SP) SAML. L'IdP SAML importe la configuration d'indexation ACS à partir des métadonnées SP ou permet de saisir manuellement les informations d'index ACS.

Prise en charge du déchargement FIPS

Une appliance FIPS Citrix ADC MPX utilisée en tant que fournisseur de services SAML prend désormais en charge les assertions chiffrées. En outre, un dispositif Citrix ADC MPX FIPS fonctionnant en tant que fournisseur de services SAML ou fournisseur d'identité SAML peut désormais être configuré pour utiliser les algorithmes SHA2 sur le matériel FIPS.

> **Remarque**
>
> En mode FIPS, seul l'algorithme RSA-V1_5 est pris en charge en tant qu'algorithme de transport clé.

Configuration de la prise en charge du déchargement FIPS à l'aide de l'interface de ligne de commande :

1. Ajouter SSL FIPS

   add ssl fipsKey fips-key

2. Créez un CSR et utilisez-le sur le serveur CA pour générer un certificat. Vous pouvez ensuite copier le certificat dans **/nsconfig/ssl**. Supposons que le fichier est *fips3cert.cer*.

   ```
   add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key<!--
   NeedCopy-->
   ```

3. Spécifiez ce certificat dans l'action SAML pour le module SP SAML

   ```
   set samlAction <name> -samlSigningCertName fips-cert<!--NeedCopy-->
   ```

4. Utiliser le certificat dans le module SAMLIDPProfile pour SAML IDP

   ```
   set samlidpprofile fipstest -samlIdpCertName fips-cert<!--NeedCopy-->
   ```

Terminologies SAML courantes

Voici quelques terminologies SAML courantes :

- **Assertion :** Une assertion SAML est un document XML renvoyé par le fournisseur d'identité au fournisseur de services après l'authentification de l'utilisateur. L'assertion a une structure très spécifique, telle que définie par la norme SAML.
- **Types d'assertions :** Voici les types d'assertion.
  - Authentification - l'utilisateur est authentifié par un moyen particulier à un moment donné
  - Autorisation - l'utilisateur s'est vu accorder ou refuser l'accès à une ressource spécifiée
  - Attributs - l'utilisateur est associé aux attributs fournis
- **Assertion Consumer Service (ACS) :** point de terminaison (URL) du fournisseur de services responsable de la réception et de l'analyse d'une assertion SAML
- **Restriction d'audience :** Valeur de l'assertion SAML qui spécifie à qui (et seulement qui) l'assertion est destinée. Le « public » sera le fournisseur de services et est généralement une URL, mais peut techniquement être formaté comme n'importe quelle chaîne de données.
- **Fournisseur d'identité (IdP) :** En termes de SAML, le fournisseur d'identité est l'entité qui vérifie l'identité de l'utilisateur, en réponse à une demande du fournisseur de services.

Le fournisseur d'identité est responsable de la maintenance et de l'authentification de l'identité de l'utilisateur

- **Fournisseur de services (SP) :** En termes de SAML, le fournisseur de services (SP) offre un service à l'utilisateur et permet à l'utilisateur de se connecter en utilisant SAML. Lorsque l'utilisateur tente de se connecter, le SP envoie une demande d'authentification SAML au fournisseur d'identité (IdP)
- **Binding SAML :** Les demandeurs et les répondeurs SAML communiquent en échangeant des messages. Le mécanisme de transport de ces messages est appelé liaison SAML.
- **Artefact HTTP :** une des options de liaison prises en charge par le protocole SAML. HTTP Artefact est utile dans les scénarios où le demandeur et le répondeur SAML utilisent un agent utilisateur HTTP et ne veulent pas transmettre le message entier, que ce soit pour des raisons techniques ou de sécurité. Au lieu de cela, un artefact SAML est envoyé, qui est un ID unique pour l'ensemble des informations. L'IdP peut ensuite utiliser l'artefact pour récupérer l'information complète. L'émetteur d'artefact doit maintenir l'état pendant que l'artefact est en attente. Un service de résolution d'artefact (ARS) doit être configuré.

  HTTP Artefact envoie l'artefact en tant que paramètre de requête.
- **HTTP POST :** Une des options de liaison prises en charge par le protocole SAML.

  HTTP POST envoie le contenu du message en tant que paramètre POST, dans la charge utile.
- **Redirection HTTP :** une des options de liaison prises en charge par le protocole SAML.

  Lorsque la redirection HTTP est utilisée, le fournisseur de services redirige l'utilisateur vers le fournisseur d'identité où se produit la connexion, et le fournisseur d'identité redirige l'utilisateur vers le fournisseur de services. La redirection HTTP nécessite une intervention de l'User-Agent (le navigateur).

  HTTP Redirection envoie le contenu du message dans l'URL. Pour cette raison, il ne peut pas être utilisé pour la réponse SAML, car la taille de la réponse dépassera généralement la longueur d'URL autorisée par la plupart des navigateurs.

  Remarque : L'appliance Citrix ADC prend en charge les liaisons POST et redirection lors de la déconnexion.
- Métadonnées : Les métadonnées sont les données de configuration dans SP et IDP pour savoir comment communiquer entre eux, ce qui sera dans les normes XML

Autres articles Citrix utiles liés à l'authentification SAML

Les articles suivants relatifs à l'authentification SAML peuvent être utiles.

- https://support.citrix.com/article/CTX277558

- https://support.citrix.com/article/CTX259127
- https://support.citrix.com/article/CTX228135
- https://support.citrix.com/article/CTX221631
- https://support.citrix.com/article/CTX138988

Authentification OAuth

October 5, 2021

La fonctionnalité de gestion du trafic d'authentification, d'autorisation et d'audit prend en charge l'authentification OAuth et OpenID Connect (OIDC). Il autorise et authentifie les utilisateurs sur des services hébergés sur des applications telles que Google, Facebook et Twitter.

Points à noter

- Citrix ADC Advanced Edition et versions ultérieures sont nécessaires au fonctionnement de la solution.
- Une appliance Citrix ADC doit être sur la version 12.1 ou ultérieure pour qu'elle fonctionne en tant que fournisseur d'identité OAuth à l'aide d'OIDC.
- OAuth sur une appliance Citrix ADC est qualifié pour tous les IdP SAML conformes à « OpenID connect 2.0 ».

Une appliance Citrix ADC peut être configurée pour se comporter en tant que fournisseur de services (SP) ou fournisseur d'identité (IdP), à l'aide de SAML et OIDC. Auparavant, une appliance Citrix ADC configurée en tant que fournisseur d'identité ne prend en charge que le protocole SAML. À partir de la version 12.1 de Citrix ADC, Citrix ADC prend également en charge l'OIDC.

OIDC est une extension de l'autorisation/délégation OAuth. Une appliance Citrix ADC prend en charge les protocoles OAuth et OIDC dans la même classe d'autres mécanismes d'authentification. OIDC est un module complémentaire à OAuth car il fournit un moyen d'obtenir des informations utilisateur à partir du serveur d'autorisation, contrairement à OAuth qui n'obtient qu'un jeton qui ne peut pas être glané pour les informations utilisateur.

Le mécanisme d'authentification facilite la vérification en ligne des jetons OpenID. Une appliance Citrix ADC peut être configurée pour obtenir des certificats et vérifier les signatures sur le jeton.

L'un des principaux avantages de l'utilisation des mécanismes OAuth et OIDC est que les informations utilisateur ne sont pas envoyées aux applications hébergées. Par conséquent, le risque de vol d'identité est considérablement réduit.

L'appliance Citrix ADC configurée pour l'authentification, l'autorisation et l'audit accepte désormais les jetons entrants signés à l'aide de l'algorithme HMAC HS256. En outre, les clés publiques du four-

nisseur d'identité SAML (IdP) sont lues à partir d'un fichier, au lieu d'apprendre à partir d'un point de terminaison d'URL.

Dans l'implémentation Citrix ADC, l'application est accessible par le serveur virtuel de gestion du trafic d'authentification, d'autorisation et d'audit. Par conséquent, pour configurer OAuth, vous devez configurer une stratégie OAuth qui doit ensuite être associée à un serveur virtuel de gestion du trafic d'authentification, d'autorisation et d'audit.

Configurer le protocole OpenID Connect

Une appliance Citrix ADC peut désormais être configurée en tant que fournisseur d'identité à l'aide du protocole OIDC. Le protocole OIDC renforce les capacités de fourniture d'identité de l'appliance Citrix ADC. Vous pouvez désormais accéder à l'application hébergée à l'échelle de l'entreprise avec une authentification unique. L'OIDC offre plus de sécurité en ne transférant pas le mot de passe utilisateur, mais fonctionne avec des jetons ayant une durée de vie spécifique. OIDC est également conçu pour s'intégrer à des clients autres que des navigateurs, tels que des applications et des services. Par conséquent, de nombreuses implémentations adoptent largement l'OIDC.

Avantages de la prise en charge d'OpenID Connect

- OIDC élimine les frais généraux liés à la gestion de plusieurs mots de passe d'authentification, car l'utilisateur possède une identité unique au sein de l'organisation.
- OIDC fournit une sécurité solide pour votre mot de passe, car le mot de passe est partagé uniquement avec votre fournisseur d'identité et non avec aucune application à laquelle vous accédez.
- L'OIDC dispose d'une grande interopérabilité avec divers systèmes, ce qui facilite l'acceptation d'OpenID par les applications hébergées.
- OIDC est un protocole simple qui permet aux clients natifs de s'intégrer facilement aux serveurs.

Pour configurer une appliance Citrix ADC en tant que fournisseur d'identité à l'aide du protocole OpenID Connect à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > IdP OAuth**.
2. Cliquez sur **Profil**, puis sur **Ajouter.**

   Dans l'écran **Créer un profil de fournisseur d'identité OAuth d'authentification**, définissez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   - **Nom** : nom du profil d'authentification.
   - **ID client** : chaîne unique qui identifie le SP.
   - **Client Secret** : secret unique qui identifie le SP.

- **URL de redirection** : point de terminaison sur le SP auquel le code/jeton doit être publié.
- **Nom de l'émetteur** : chaîne qui identifie le fournisseur d'identité.
- **Audience** : destinataire cible du jeton envoyé par l'IdP. Cela peut être vérifié par le destinataire.
- **Skew Time (Temps** d'inclinaison) : durée pendant laquelle le jeton reste valide.
- **Groupe d'authentification par défaut** : groupe ajouté à la session pour ce profil afin de simplifier l'évaluation des stratégies et d'aider à personnaliser les stratégies.

3. Cliquez sur **Stratégies** et cliquez sur **Ajouter.**
4. Dans l'écran **Créer une stratégie de fournisseur d'identité OAuth d'authentification**, définissez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   - **Nom :** nom de la stratégie d'authentification.
   - **Action** : nom du profil créé précédemment.
   - **Action de consignation : nom de l'action du journal** des messages à utiliser lorsqu'une demande correspond à cette stratégie. Ce n'est pas un dépôt obligatoire.
   - Action**à résultat non défini — Action** à exécuter si le résultat de l'évaluation de la politique n'est pas défini (UNDEF). Ce champ n'est pas obligatoire.
   - **Expression** : expression de stratégie avancée utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, vrai.
   - **Commentaires** : tout commentaire concernant la stratégie.

Liaison de la stratégie OAuthIDP et de la stratégie LDAP au serveur virtuel d'authentification

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Actions > LDAP**.
2. Dans l'écran **Actions LDAP**, cliquez sur **Ajouter**.
3. Dans l'écran **Créer un serveur LDAP d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer**.

   - **Nom :** nom de l'action LDAP
   - **ServerName/ServerIP :** fournit le nom de domaine complet ou l'adresse IP du serveur LDAP
   - Choisissez les valeurs appropriées **pour le type de sécurité, le port, le type de serveur et le délai d'expiration**
   - Assurez-vous que **l'authentification** est cochée
   - **DN de base :** base à partir de laquelle lancer la recherche LDAP. Par exemple, dc=aaa, dc=local.
   - **Administrator Bind DN :** nom d'utilisateur de la liaison au serveur LDAP. Par exemple, admin@aaa.local.
   - **Mot de passe administrateur/Confirmer le mot de passe : mot de passe pour lier LDAP**

- Cliquez sur **Tester la connexion** pour tester vos paramètres.
- **Attribut de nom d'ouverture de session du serveur :** choisissez « **SAMAccountName** »
- Les autres champs ne sont pas obligatoires et peuvent donc être configurés comme requis.

4. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Stratégie.**
5. Dans **l'écran Stratégies d'authentification**, cliquez sur **Ajouter**.
6. Sur la page **Créer une stratégie d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer.**

   - **Nom :** nom de la stratégie d'authentification LDAP.
   - **Type d'action :** choisissez **LDAP.**
   - **Action :** choisissez l'action LDAP.
   - **Expression :** expression de stratégie avancée utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, c'est vrai**.

Pour configurer l'appliance Citrix ADC en tant que fournisseur d'identité à l'aide du protocole OpenID Connect à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add authentication OAuthIDPProfile <name> [-clientID <string>][-clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]<!--NeedCopy-->`
- `add authentication OAuthIdPPolicy <name> -rule <expression> [-action <string> [-undefAction <string>] [-comment <string>][-logAction <string >]<!--NeedCopy-->`
- `add authentication ldapAction aaa-ldap-act -serverIP 10.0.0.10 -ldapBase "dc=aaa,dc=local"<!--NeedCopy-->`
- `ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -ldapLoginName sAMAccountName<!--NeedCopy-->`
- `add authentication policy aaa-ldap-adv-pol -rule true -action aaa-ldap-act<!--NeedCopy-->`
- `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority 100 -gotoPriorityExpression NEXT<!--NeedCopy-->`
- `bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -priority 5 -gotoPriorityExpression END<!--NeedCopy-->`
- `bind vpn global -certkey <><!--NeedCopy-->`

> **Remarque**
>
> Vous pouvez lier plusieurs clés. Les parties publiques des certificats liés sont envoyées en réponse à `jwks\\_uri query (https://gw/oauth/idp/certs).`

Citrix ADC en tant que SP OAuth

August 20, 2021

La fonctionnalité de gestion du trafic d'authentification, d'autorisation et d'audit prend en charge l'authentification OAuth pour authentifier les utilisateurs auprès d'applications hébergées sur des applications telles que Google, Facebook et Twitter.

Points à noter

- Citrix ADC Advanced Edition et version ultérieure est nécessaire pour que la solution fonctionne.
- OAuth sur l'appliance Citrix ADC est qualifié pour tous les IDP SAML conformes à « OpenID connect 2.0 ».

Pour configurer OAuth à l'aide de l'utilitaire de configuration

1. Configurez l'action et la stratégie OAuth.

   Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées**> Stratégie, créez une stratégie avec OAuth comme type d'action et associez l'action OAuth requise à la stratégie.

2. Associez la stratégie OAuth à un serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**et associez la stratégie OAuth au serveur virtuel d'authentification.

> **Remarque**
>
> Les attributs (1 à 16) peuvent être extraits dans la réponse OAuth. Actuellement, ces attributs ne sont pas évalués. Ils sont ajoutés pour la référence future.

Pour configurer OAuth à l'aide de l'interface de ligne de commande :**

1. Définissez une action OAuth.


```
add authentication OAuthAction <name> -authorizationEndpoint <URL>
     -tokenEndpoint <URL> [-idtokenDecryptEndpoint <URL>] -clientID
     <string> -clientSecret <string> [-defaultAuthenticationGroup <
    string>][-tenantID <string>][-GraphEndpoint <string>][-
    refreshInterval <positive_integer>] [-CertEndpoint <string>][-
    audience <string>][-userNameField <string>][-skewTime <mins>][-
    issuer <string>][-Attribute1 <string>][-Attribute2 <string>][-
    Attribute3 <string>]...
<!--NeedCopy-->
```

2. Associez l'action à une stratégie d'authentification avancée.

```
add authentication Policy** <name> -rule <expression> -action <
    string>
<!--NeedCopy-->
```

Exemple :

```
add authentication oauthAction a -authorizationEndpoint https://example
.com/ -tokenEndpoint https://example.com/ -clientiD sadf -clientsecret
df
```

Pour plus d'informations sur les paramètres OAuthAction d' authentification, voir AuthAction AuthAction d'authentification.

> **Remarque**
>
> Lorsqu'un CertendPoint est spécifié, l'appliance Citrix ADC interroge ce point de terminaison à la fréquence configurée pour connaître les clés.

Pour configurer un Citrix ADC pour lire le fichier local et analyser les clés de ce fichier, une nouvelle option de configuration est introduite comme suit :

```
set authentication OAuthAction <> -\*\*CertFilePath\*\* <path to local
    file with jwks>
<!--NeedCopy-->
```

La fonctionnalité OAuth prend désormais en charge les fonctionnalités suivantes dans l'API de jeton du côté de la partie de confiance (RP) et du côté IdP de Citrix Gateway et Citrix ADC.

- Prise en charge de PKCE (Preuve Key for Code Exchange)
- Prise en charge de client_assertion

Prise en charge des attributs nom-valeur pour l'authentification OAuth

Vous pouvez désormais configurer les attributs d'authentification OAuth avec un nom unique avec les valeurs. Les noms sont configurés dans le paramètre d'action OAuth en tant que « Attributs » et les valeurs sont obtenues en interrogeant les noms. Les attributs extraits sont stockés dans la session d'authentification, d'autorisation et d'audit. Les administrateurs peuvent interroger ces attributs en utilisant`http.req.user.attribute("attribute name")` ou`http.req.user.attribute(1)` en fonction de la méthode choisie pour spécifier les noms d'attributs.

En spécifiant le nom de l'attribut, les administrateurs peuvent facilement rechercher la valeur d'attribut associée à ce nom d'attribut. De plus, les administrateurs n'ont plus à se souvenir de l'attribut « attribute1 à attribute16 » par son seul numéro.

> **Important**
>
> Dans une commande OAuth, vous pouvez configurer un maximum de 64 attributs séparés par des virgules avec une taille totale inférieure à 1024 octets.
>
> **Remarque**
>
> L'échec de session peut être évité si la taille totale de la valeur de « attribut 1 à l'attribut 16 » et les valeurs des attributs spécifiées dans « Attributs » ne dépassent pas 10 Ko.

Pour configurer les attributs nom-valeur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add authentication OAuthAction <name> [-Attributes <string>]`
- `set authentication OAuthAction <name> [-Attributes <string>]`

Exemples :

- `add authentication OAuthAction a1 -attributes "email,company"-attribute1 email`
- `set authentication OAuthAction oAuthAct1 -attributes "mail,sn,userprincipalName"`

Citrix ADC en tant que fournisseur d'identité OAuth

October 5, 2021

Une appliance Citrix ADC peut désormais être configurée en tant que fournisseur d'identité à l'aide du protocole OpenID-Connect (OIDC). Le protocole OIDC renforce les capacités de fourniture d'identité de l'appliance Citrix ADC. Vous pouvez désormais accéder à l'application hébergée à l'échelle de

l'entreprise avec une authentification unique, car OIDC offre plus de sécurité en ne transférant pas le mot de passe utilisateur, mais en utilisant des jetons avec une durée de vie spécifique. OpenID est également conçu pour s'intégrer à des clients autres que des navigateurs, tels que des applications et des services. Par conséquent, le protocole OIDC est largement adopté par de nombreuses implémentations.

> **Remarque**
>
> Citrix ADC doit être sur la version 12.1 ou ultérieure pour que l'appliance fonctionne en tant que fournisseur d'identité OAuth à l'aide du protocole OIDC.

Avantages de Citrix ADC en tant que fournisseur d'identité OAuth

- Élimine les frais liés à la gestion de plusieurs mots de passe d'authentification, car l'utilisateur possède une identité unique au sein de l'organisation.
- Fournit une sécurité solide pour votre mot de passe, car le mot de passe est partagé uniquement avec votre fournisseur d'identité et non avec les applications auxquelles vous accédez.
- Fournit une interopérabilité étendue avec divers systèmes, ce qui facilite l'acceptation d'OpenID par les applications hébergées.

> **Remarque**
>
> Citrix ADC Advanced Edition et versions ultérieures sont nécessaires au fonctionnement de la solution.

Pour configurer l'appliance Citrix ADC en tant que fournisseur d'identité OAuth à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > IdP OAuth**.
2. Cliquez sur **Profil**, puis sur **Ajouter.**

   Dans l'écran **Créer un profil de fournisseur d'identité OAuth d'authentification**, définissez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   - **Nom** : nom du profil d'authentification. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), la livre (#), l'espace (), à (@), égal à (=), deux-points (:) et les caractères de soulignement. Impossible de modifier une fois le profil créé.
   - **ID client** : chaîne unique qui identifie le SP. Le serveur d'autorisation déduit la configuration du client à l'aide de cet ID. Longueur maximale : 127.
   - **Client Secret** : chaîne secrète établie par l'utilisateur et le serveur d'autorisation. Longueur maximale : 239.

- **URL de redirection** : point de terminaison sur le SP auquel le code/jeton doit être publié.
- **Nom de l'émetteur** : identité du serveur dont les jetons doivent être acceptés. Longueur maximale : 127.
- **Audience** : destinataire cible du jeton envoyé par l'IdP. Cela peut être vérifié par le destinataire.
- **Skew Time** (Temps d'inclinaison) : cette option spécifie le décalage d'horloge autorisé en minutes que Citrix ADC autorise sur un jeton entrant. Par exemple, si SkewTime est 10, le jeton sera valide de (heure actuelle - 10) min à (heure actuelle + 10) min, soit 20 min en tout. Valeur par défaut : 5.
- **Groupe d'authentification par défaut** : groupe ajouté à la liste de groupes interne de la session lorsque ce profil est choisi par l'IdP qui peut être utilisé dans le flux nFactor. Il peut être utilisé dans l'expression (AAA.USER.IS_MEMBER_OF (« xxx »)) pour les stratégies d'authentification
  identifier le flux de facteurs lié à la partie de confiance. Longueur maximale : 63

A group added to the session for this profile to simplify policy evaluation and help in customizing policies. This is the default group that is chosen when the authenticatiob succeeds in addition to the extracted groups. Maximum Length: 63.

3. Cliquez sur **Stratégies** et cliquez sur **Ajouter.**
4. Dans l'écran **Créer une stratégie de fournisseur d'identité OAuth d'authentification**, définissez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.
   - **Nom** : nom de la stratégie d'authentification.
   - **Action** : nom du profil créé ci-dessus.
   - **Action de consignation : nom de l'action du journal** des messages à utiliser lorsqu'une demande correspond à cette stratégie. Ce n'est pas un dépôt obligatoire.
   - Action**à résultat non défini — Action** à exécuter si le résultat de l'évaluation de la politique n'est pas défini (UNDEF). Ce champ n'est pas obligatoire.
   - **Expression** : expression de stratégie avancée utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, vrai.
   - **Commentaires** : tout commentaire concernant la stratégie.

Liaison de la stratégie OAuthIDP et de la stratégie LDAP au serveur virtuel d'authentification

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Actions > LDAP**.
2. Dans l'écran **Actions LDAP**, cliquez sur **Ajouter**.
3. Dans l'écran **Créer un serveur LDAP d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer**.

- **Nom :** nom de l'action LDAP
- **ServerName/ServerIP :** fournit le nom de domaine complet ou l'adresse IP du serveur LDAP
- Choisissez les valeurs appropriées **pour le type de sécurité, le port, le type de serveur et le délai d'expiration**
- Assurez-vous que **l'authentification** est cochée
- **DN de base :** base à partir de laquelle lancer la recherche LDAP. Par exemple, dc=aaa, dc=local.
- **Administrator Bind DN :** nom d'utilisateur de la liaison au serveur LDAP. Par exemple, admin@aaa.local.
- **Mot de passe administrateur/Confirmer le mot de passe : mot de passe pour lier LDAP**
- Cliquez sur **Tester la connexion** pour tester vos paramètres.
- **Attribut de nom d'ouverture de session du serveur :** choisissez **« SAMAccountName »**
- Les autres champs ne sont pas obligatoires et peuvent donc être configurés comme requis.

4. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Stratégie.**
5. Dans l'écran **Stratégies d'authentification**, cliquez sur **Ajouter**.
6. Sur la page **Créer une stratégie d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer.**

   - **Nom :** nom de la stratégie d'authentification LDAP.
   - **Type d'action :** choisissez **LDAP.**
   - **Action :** choisissez l'action LDAP.
   - **Expression :** expression de stratégie avancée utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, c'est vrai**.

La fonctionnalité OAuth prend désormais en charge les fonctionnalités suivantes dans l'API de jeton du côté de la partie de confiance (RP) et du côté IdP de Citrix Gateway et Citrix ADC.

- Prise en charge de PKCE (Proof Key for Code Exchange)
- Prise en charge de client_assertion

Pour configurer l'appliance Citrix ADC en tant que fournisseur d'identité à l'aide du protocole OIDC avec la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
1 add authentication OAuthIDPProfile <name> [-clientID <string>][-
      clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <
      string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]
2
```



```
add authentication OAuthIdPPolicy <name> -rule <expression> [-action <string> [-undefAction <string>] [-comment <string>][-logAction <string>]

add authentication ldapAction aaa-ldap-act -serverIP 10.0.0.10 -ldapBase "dc=aaa,dc=local"

ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -ldapLoginName sAMAccountName

add authentication policy aaa-ldap-adv-pol -rule true -action aaa-ldap-act

bind authentication vserver auth_vs -policy <ldap_policy_name> -priority 100 -gotoPriorityExpression NEXT

bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -priority 5 -gotoPriorityExpression END

bind vpn global  - certkey <>
<!--NeedCopy-->
```

> **Remarque**
>
> Vous pouvez lier plusieurs clés. Les parties publiques des certificats liés sont envoyées en réponse à `jwks\\_uri query (https://gw/oauth/idp/certs)`.

Prise en charge des jetons cryptés sur le protocole OIDC

L'appliance Citrix ADC avec le mécanisme OIDC prend désormais en charge l'envoi de jetons chiffrés avec des jetons signés. L'appliance Citrix ADC utilise les spécifications de cryptage Web JSON pour calculer les jetons chiffrés et ne prend en charge que la sérialisation compacte des jetons chiffrés. Pour chiffrer un jeton OpenID, une appliance Citrix ADC a besoin de la clé publique de la partie de confiance (RP). La clé publique est obtenue dynamiquement en interrogeant le point de terminaison de configuration bien connu de la partie de confiance.

Une nouvelle option « RelyingPartyMetadataUrl » est introduite dans le profil d'authentification OAuthIDPProfile. « profil.

Pour configurer le point de terminaison de la partie de confiance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

“‘set authentication OAuthIDPProfile [-relyingPartyMetadataURL] [-refreshInterval] [-status < >]

```
- **RelyingPartyMetadataURL**  : point de terminaison sur lequel le fournisseur d'identité Citrix ADC peut obtenir des détails sur la partie de confiance en cours de configuration. La réponse aux mé tadonnées doit inclure des points de terminaison pour jwks_uri pour les clés publiques RP.

- **RefreshInterval**  : définit la fréquence à laquelle ce point de terminaison doit être interrogé pour mettre à jour les certificats en quelques minutes.

- **status** - Indique le statut de l'opération d'interrogation. L'é tat est terminé une fois que l'appliance Citrix ADC a obtenu les clé s publiques.

 **Exemple**

 ```
 set authentication OAuthIDPProfile sample_profile -
    relyingPartyMetadataURL https://rp.customer.com/metadata -
    refreshInterval 50 -status < >
 <!--NeedCopy-->
```

Une fois le point de terminaison configuré, une appliance Citrix ADC interroge d’abord le point de terminaison bien connu de la partie de confiance pour lire la configuration. Actuellement, l’appliance Citrix ADC traite uniquement le point de terminaison « jwks_uri ».

- Si le ‘jwks_uri’ est absent de la réponse, l’état du profil n’est pas complet.
- Si le ‘jwks_uri’ est présent dans la réponse, Citrix ADC interrogeait également ce point de terminaison pour lire les clés publiques de la partie de confiance.

> **Remarque :** seuls les algorithmes de chiffrement RSAES-OAEP et AES GCM sont pris en charge pour le chiffrement des jetons.

Prise en charge des attributs personnalisés sur OpenID Connect

Les parties de confiance OpenID peuvent nécessiter plus qu’un nom d’utilisateur ou un nom d’utilisateur principal (UPN) dans le jeton pour créer le profil utilisateur ou prendre des décisions d’autorisation. Le plus souvent, les groupes d’utilisateurs sont tenus d’appliquer des stratégies d’autorisation pour l’utilisateur. Parfois, des détails supplémentaires, tels que le prénom ou le nom de famille, sont nécessaires pour provisionner un compte d’utilisateur.

L’appliance Citrix ADC configurée en tant que fournisseur d’identité peut être utilisée pour envoyer des attributs supplémentaires dans OIDCID_Token à l’aide d’expressions. Les expressions de stratégie


```

avancées sont utilisées pour envoyer les attributs personnalisés conformément aux exigences. L'IdP Citrix évalue les expressions correspondant aux attributs, puis calcule le jeton final.

Appliance Citrix ADC JSONifie automatiquement les données de sortie. Par exemple, les nombres (tels que SSN) ou les valeurs booléennes (true ou false) ne sont pas entourés de guillemets. Les attributs à valeurs multiples, tels que les groupes, sont placés dans un marqueur de tableau ([» » et «] »). Les attributs de type complexe ne sont pas calculés automatiquement et vous pouvez configurer l'expression PI de ces valeurs complexes selon votre besoin.

**Pour configurer le point de terminaison de la partie de confiance à l'aide de l'interface de ligne de commande**

À l'invite de commandes, tapez :

```
set oauthidpprofile <name> -attributes <AAA-custom-attribute-pattern>
<!--NeedCopy-->
```

Le <AAA-custom-attribute-pattern> peut être décrit comme :

Attribute1=PI-Expression@@@attribute2=PI-Expression@@@

'attribute1', 'attribute2' sont des chaînes littérales qui représentent le nom de l'attribut à insérer dans le id_token.

> **Remarque :** Vous pouvez configurer jusqu'à 2 000 octets d'attributs.

Exemple : `set oauthidpprofile sample_1 -attributes q{ myname=http.req.user.name@@@ssn="123456789"@@@jit="false"@@@groups=http.req.user.groups }`

- L'expression PI précédente est une expression de stratégie avancée qui représente la valeur à utiliser pour l'attribut. L'expression PI peut être utilisée pour envoyer un littéral de chaîne, tel que « 'chaîne codée en dur » '. Le littéral de chaîne est entouré de guillemets doubles autour de guillemets simples ou de guillemets doubles autour d'un début et d'un motif (comme indiqué précédemment, le motif de début est « q {«). Si la valeur de l'attribut n'est pas un littéral de chaîne, l'expression est évaluée au moment de l'exécution et sa valeur est envoyée en jeton. Si la valeur au moment de l'exécution est vide, l'attribut correspondant n'est pas ajouté au jeton d'identification.
- Comme défini dans l'exemple, « false » est une chaîne littérale pour l'attribut « jit ». De plus, « ssn » a une valeur codée en dur pour référence. Les groupes et « monnom » sont des expressions PI qui génèrent des chaînes.

Prise en charge des déploiements GSLB actifs-actifs sur Citrix Gateway

Citrix Gateway configuré en tant que fournisseur d'identité (IdP) à l'aide du protocole OIDC peut prendre en charge les déploiements GSLB actifs-actifs. Le déploiement GSLB actif-actif sur le fournisseur

d'identité Citrix Gateway permet d'équilibrer la charge d'une demande de connexion utilisateur entrante sur plusieurs emplacements géographiques.

> **Important**
>
> Citrix vous recommande de lier des certificats d'autorité de certification au service SSL et d'activer la validation des certificats sur le service SSL pour une sécurité accrue.

Pour plus d'informations sur la configuration de la configuration de GSLB, voir Exemple de configuration et de configuration GSLB.

Authentification API avec l'appliance Citrix ADC

January 21, 2021

Il y a un changement de paradigme dans la façon dont les applications modernes interagissent avec leurs clients. Traditionnellement, les clients du navigateur étaient utilisés pour accéder aux services. Les applications définissent généralement des cookies de session pour suivre le contexte de l'utilisateur. Les applications modernes et distribuées rendent difficile la maintenance des sessions utilisateur sur les microservices. Pour cette raison, la plupart des accès à l'application sont devenus basés sur l'API.

Les clients qui communiquent avec ces services distribués ont également évolué. La plupart des clients obtiennent des jetons d'une entité approuvée appelée Serveur d'autorisation pour prouver l'identité et l'accès de l'utilisateur. Ces clients présentent ensuite le jeton à l'application avec chaque demande d'accès. Par conséquent, les périphériques proxy traditionnels comme Citrix ADC doivent évoluer pour prendre en charge ces clients. Une appliance Citrix ADC permet aux administrateurs de gérer ce trafic. Citrix ADC peut être déployé en tant que passerelle API pour front-end tout le trafic destiné aux services publiés. Une passerelle API peut être déployée pour les environnements natifs traditionnels (hybride Multi Cloud ou HMC) ou Cloud. L'API Gateway met fin à tout le trafic entrant pour offrir plusieurs services tels que l'authentification, l'autorisation, la limitation de débit, le routage, la mise en cache, le déchargement SSL, le pare-feu d'application, etc. Par conséquent, il devient un élément essentiel de l'infrastructure.

Types de jetons

Les jetons échangés pendant l'accès à l'API sont généralement conformes au protocole OAuth/OpenID Connect (OIDC). Les jetons d'accès utilisés uniquement pour « accès délégué » sont conformes au protocole OAuth, tandis que les jetons d'ID qui sont conformes à OIDC contiennent également des informations utilisateur.

Les jetons d'accès sont normalement un blob de données opaque ou aléatoire. Cependant, ils peu-

vent parfois être chantés jetons conformes aux normes JWT (Json Web Token). Les jetons d'ID sont toujours signés JWT.

Accès à l'API avec OAuth

Le type d'authentification OAuth sur une appliance Citrix ADC peut être utilisé pour gérer les protocoles OAuth et OIDC. OIDC est une extension du protocole OAuth.

OAuthAction sur une appliance Citrix ADC peut être utilisée pour gérer des clients interactifs tels que les navigateurs et les clients natifs tels que les applications clientes. Les clients interactifs sont redirigés vers Identity Provider pour se connecter à l'aide du protocole OIDC. Les clients natifs peuvent obtenir des jetons hors bande et peuvent présenter ces jetons sur une appliance Citrix ADC pour l'accès.

> **Remarque :**
>
> Le jeton d'accès obtenu à partir des points de terminaison peut être mis en cache pour les demandes suivantes, améliorant ainsi les performances de l'API.

Pour configurer la prise en charge de la mise en cache des jetons à l'aide de l'interface de ligne de commande, tapez la commande suivante à l'invite de commandes :

```
set aaaparameter  - apITokenCache <ENABLED>

<!--NeedCopy-->
```

Les sections suivantes décrivent la méthode d'accès à l'API effectuée par les clients natifs.

Serveur virtuel pour l'accès aux API

Pour déployer une appliance Citrix ADC pour un accès API, un serveur virtuel de gestion du trafic (TM) est déployé avec l'authentification 401. Il est associé à un serveur virtuel d'authentification (authentification, autorisation et audit) pour contenir les stratégies d'authentification et de session. L'extrait de configuration suivant crée un tel serveur virtuel.

```
Add lb vserver lb-api-access SSL <IP> 443 -authn401 On -AuthnVsName
    auth-api-access

Bind ssl vserver lb-api-access -certkeyName <ssl-cert-entity>

Add authentication vserver auth-api-access SSL
<!--NeedCopy-->
```


> **Remarque :**
>
> Vous devez lier un service au serveur TM vserver et une stratégie d'authentification (avec OAuthAction décrite comme suit) au serveur virtuel d'authentification pour terminer la configuration.

Après avoir créé le serveur virtuel, il faut ajouter une OAuthAction avec la stratégie correspondante. Il existe plusieurs autres options dans une action OAuth en fonction du type de jeton, et d'autres mécanismes de sécurité.

Configuration OAuth pour les jetons d'ID

Les jetons d'ID sont toujours signés JWT. C'est-à-dire qu'ils portent l'en-tête, la charge utile et la signature. Comme il s'agit de jetons autonomes, une appliance Citrix ADC peut valider ces jetons localement. Pour valider ces jetons, l'appliance doit connaître la clé publique de la clé privée correspondante utilisée pour signer ces jetons.

Voici un exemple de OAuthAction avec certains arguments obligatoires avec "certEndpoint".

```
1 Add authentication OAuthAction oauth-api-access -clientid <your-client-
     id> -clientsecret <your-client-secret> -authorizationEndpoint <URL
     to which users would be redirected for login> -tokenEndpoint <
     endpoint at which tokens could be obtained> -certEndpoint <uri at
     which public keys of IdP are published>
2 <!--NeedCopy-->
```

Où,

- **ID client** — Chaîne unique qui identifie le SP. Le serveur d'autorisation infère la configuration du client à l'aide de cet ID. Longueur maximale : 127.
- **Client Secret** — Chaîne secrète établie par l'utilisateur et le serveur d'autorisation. Longueur maximale : 239.
- **AuthorizationEndPoint** - URL à laquelle les utilisateurs se connecteraient normalement (lors de l'utilisation de clients interactifs).
- **TokenEndPoint** - URL sur le serveur d'autorisation à partir duquel les jetons/code sont obtenus/échangés
- **CertEndPoint** - URL à laquelle le serveur d'autorisation publie les clés publiques utilisées pour signer les jetons. Le serveur d'autorisation peut publier plusieurs clés et choisir l'une d'entre elles pour signer des jetons.

> **Remarque :** L'ID client/Client Secret/AuthorizationEndPoint/TokenEndpoint sont des paramètres facultatifs pour l'accès à l'API. Toutefois, il est recommandé de fournir des valeurs pour ces paramètres, car l'entité d'action peut être réutilisée à des fins différentes.

Dans la configuration précédente, 'CertendPointPoint' est essentiel pour la validation du jeton d'ID. Ce point de terminaison contient les clés publiques du certificat utilisé pour signer les jetons. Ces clés publiques doivent correspondre à la spécification JWK (Json Web Keys).

Une fois que CertendPoint est configuré au niveau de l'appliance Citrix ADC, il interroge périodiquement le point de terminaison (avec l'intervalle par défaut d'un jour pouvant être personnalisable dans la configuration) pour maintenir les clés publiques à jour. Une fois les clés publiques disponibles, ADC peut effectuer la validation locale des jetons d'ID entrants.

Configuration OAuth pour les jetons d'accès opaques

Les jetons opaques ne peuvent pas être vérifiés localement sur l'appliance Citrix ADC. Ceux-ci doivent être validés sur le serveur d'autorisation. Une appliance Citrix ADC utilise le « protocole d'introspection » mentionné dans les spécifications OAuth afin de vérifier ces jetons. Une nouvelle option, IntroSpectURL, est fournie dans la configuration OAuth pour vérifier les jetons opaques.

```
set oauthAction oauth-api-acccess -introspectURL <uri of the
    Authorization Server for introspection>

<!--NeedCopy-->
```

Le format de l'API introspection est conforme à la spécification `https://tools.ietf.org/html/rfc7662##section-2.1` comme suit :

```
POST /introspect HTTP/1.1
Host: server.example.com
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
token=mF_9.B5f-4.1JqM&token_type_hint=access_token

<!--NeedCopy-->
```

Stratégie de liaison à Authentication vserver

Une fois OAuthAction créé, la stratégie correspondante doit être créée pour l'appeler.

```
add authentication policy oauth-api-access -rule <> -action <oauth-api-
    access><!--NeedCopy-->
```


bind authentication vserver auth-api-access -policy oauth-api-access -pri 100

```
## Paramétres de sécurité supplémentaires sur une appliance Citrix ADC

La validation des jetons inclut des vérifications de durée de vie des jetons. Les jetons en dehors de la durée acceptable sont rejetés. Voici les paramétres supplémentaires pour une sécurité supplémentaire. Certains d'entre eux sont recommandés pour être configurés toujours.

**Audience** : OAuth Action peut être configurée avec un destinataire prévu du jeton. Tous les jetons sont mis en correspondance avec cette URL configurée. Une appliance Citrix ADC dispose d'une fonctionnalité supplémentaire dans laquelle le champ d'audience pointe réellement vers un modéle défini sur l'appliance. À l'aide de ce jeu de modéles, un administrateur peut configurer plusieurs URL pour l'audience.

<!--NeedCopy-->
```

add policy patset oauth_audiences

bind patset oauth_audiences https://app1.company.com

bind patset oauth_audiences https://app2.company.com

bind patset oauth_audiences httpsL//app1.company.com/path1

set oAuthAccess oauth-api-access -audience oauth_audiences

```
Dans l'exemple précédent, plusieurs audiences sont spécifiées dans un jeu de motifs. Par conséquent, un jeton entrant n'est autorisé que s'il contient l'une des URL configurées dans le jeu de motifs.

**Émetteur** : Identité du serveur dont les jetons doivent être acceptés.  Longueur maximale : 127. Il est recommandé de configurer l'émetteur des jetons dans l'action OAuth. Cela garantit que les jetons émis par un serveur d'autorisation incorrect ne sont pas autorisés.

**SkewTime** : spécifie l'inclinaison d'horloge autorisée en nombre de minutes qu'une appliance Citrix ADC autorise sur un jeton entrant. Par exemple, si SkewTime est 10, alors le jeton sera valide de (heure actuelle - 10) min à (heure actuelle + 10) min, c'est-à-dire 20 min en tout. Valeur par défaut : 5

**AllowedAlgorithms** : Cette option permet à l'administrateur de restreindre certains algorithmes dans les jetons entrants. Par dé
```



```
    faut, toutes les méthodes prises en charge sont autorisées.
    Cependant, ces derniers peuvent être contrôlés en utilisant cette
    option.
8
9 La configuration suivante garantit que seuls les jetons utilisant RS256
     et RS512 sont autorisés :
10
11 <!--NeedCopy-->
```

set oAuthAction oauth-api-access -allowedAlgorithms RS256 RS512

```
1 Aprés la configuration ci-dessus, seuls les jetons qui utilisent RS256
    et RS512 sont autorisés.
2
3 ## Contournement de certains trafic de l'authentification
4
5 Dans de nombreux cas, certaines API de découverte sont accessibles
    publiquement aux clients. Ces API révélent généralement la
    configuration et les capacités du service lui-même. Un
    administrateur peut configurer l'appliance Citrix ADC pour
    contourner l'authentification à partir de ces URL de métadonnées à l
    'aide de la stratégie « Aucune authentification » décrite comme
    suit :
6
7 <!--NeedCopy-->
```

add authentication policy auth-bypass-policy -rule <> -action NO_AUTHN

bind authentication vserver auth-api-access -policy auth-bypass-policy -pri 110

```
1 NO_AUTHN est une action implicite qui entraîne la fin de l'
    authentification lorsque la régle correspond. Il existe d'autres
    utilisations de l'action NO_AUTHN au-delà de la portée de l'accés à
    l'API.
2 <!--NeedCopy-->
```

Authentification LDAP

August 20, 2021

Comme pour les autres types de stratégies d'authentification, une stratégie d'authentification LDAP (Lightweight Directory Access Protocol) comprend une expression et une action. Après avoir créé une

stratégie d'authentification, vous la liez à un serveur virtuel d'authentification et lui attribuez une priorité. Lorsque vous la liez, vous la définissez également comme stratégie principale ou secondaire. En plus des fonctions d'authentification standard, LDAP peut rechercher d'autres serveurs Active Directory (AD) des comptes d'utilisateurs qui n'existent pas localement. Cette fonction est appelée support de référence ou recherche de référence.

Normalement, vous configurez Citrix ADC pour qu'il utilise l'adresse IP du serveur d'authentification lors de l'authentification. Avec les serveurs d'authentification LDAP, vous pouvez également configurer ADC pour qu'il utilise le nom de domaine complet du serveur LDAP au lieu de son adresse IP pour authentifier les utilisateurs. L'utilisation d'un nom de domaine complet peut simplifier une configuration d'authentification, d'autorisation et d'audit beaucoup plus complexe dans les environnements où le serveur d'authentification peut se trouver à l'une des adresses IP multiples, mais utilise toujours un seul nom de domaine complet. Pour configurer l'authentification à l'aide du nom de domaine complet d'un serveur au lieu de son adresse IP, vous suivez le processus de configuration normal, sauf lors de la création de l'action d'authentification. Lors de la création de l'action, vous utilisez le paramètre **ServerName** au lieu du paramètre **ServerIP** et remplacez le nom de domaine complet du serveur par son adresse IP.

Avant de décider si ADC doit utiliser l'adresse IP ou le nom de domaine complet de votre serveur LDAP pour authentifier les utilisateurs, considérez que la configuration de l'authentification, de l'autorisation et de l'audit pour s'authentifier auprès d'un nom de domaine complet au lieu d'une adresse IP ajoute une étape supplémentaire au processus d'authentification. Chaque fois que ADC authentifie un utilisateur, il doit résoudre le nom de domaine complet. Si un grand nombre d'utilisateurs tentent de s'authentifier simultanément, les recherches DNS résultantes peuvent ralentir le processus d'authentification.

La prise en charge des références LDAP est désactivée par défaut et ne peut pas être activée globalement. Il doit être explicitement activé pour chaque action LDAP. Assurez-vous que le serveur AD accepte les mêmes `binddn credentials` que ceux utilisés avec le serveur de référence (GC). Pour activer la prise en charge des références, vous configurez une action LDAP pour suivre les références et spécifiez le nombre maximal de références à suivre.

Si la prise en charge des références est activée et que Citrix ADC reçoit une réponse LDAP_REFERRAL à une demande, à l'authentification, à l'autorisation et à l'audit suit la référence vers le serveur Active Directory (AD) contenu dans la référence et effectue la mise à jour sur ce serveur. Tout d'abord, l'authentification, l'autorisation et l'audit recherche le serveur de référence dans DNS et se connecte à ce serveur. Si la stratégie de parrainage nécessite SSL/TLS, elle se connecte via SSL/TLS. Il se lie ensuite au nouveau serveur avec `binddn credentials` celui utilisé avec le serveur précédent, et effectue l'opération qui a généré le référencement. Cette fonctionnalité est transparente pour l'utilisateur.

Les numéros de port pour les connexions LDAP sont les suivants :

- 389 pour les connexions LDAP non sécurisées (pour LDAP en texte brut)

- 636 pour les connexions LDAP sécurisées (pour SSL LDAP)
- 3268 pour les connexions LDAP non sécurisées Microsoft (pour le serveur de catalogue global en texte brut)
- 3269 pour les connexions LDAP sécurisées Microsoft (pour SSL Global Catalog Server)

Le tableau suivant contient des exemples de champs d'attributs utilisateur pour les serveurs LDAP :

Serveur LDAP	Attribut utilisateur	Sensible à la casse
Serveur Microsoft Active Directory	sAMAccountName	Non
Novell eDirectory	ou	Oui
IBM Directory Server	Uid	Oui
Lotus Domino	CN	Oui
Sun ONE Directory (anciennement iPlanet)	uid ou cn	Oui

Ce tableau contient des exemples de DN de base :

Serveur LDAP	DN de base
Serveur Microsoft Active Directory	DC =citrix, DC = local
Novell eDirectory	ou=users,ou=dev
IBM Directory Server	cn=users
Lotus Domino	OU=ville, O=Citrix, C=US
Sun ONE Directory (anciennement iPlanet)	OU=personnes, dc=citrix, dc=com

Le tableau suivant contient des exemples de liaison DN :

Serveur LDAP	Relier le nom distinctif
Serveur Microsoft Active Directory	CN=Administrateur, CN=Utilisateurs, DC =citrix, DC = local
Novell eDirectory	cn=admin, o=citrix
IBM Directory Server	LDAP_dn
Lotus Domino	CN=Administrateur des notes, O=Citrix, C=US

Serveur LDAP	Relier le nom distinctif
Sun ONE Directory (anciennement iPlanet)	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

Pour plus d'informations sur la configuration des stratégies d'authentification en général, voir Stratégies d'authentification. Pour plus d'informations sur les expressions Citrix ADC, utilisées dans la règle de stratégie, voir Stratégies et expressions.

Pour créer un serveur d'authentification LDAP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

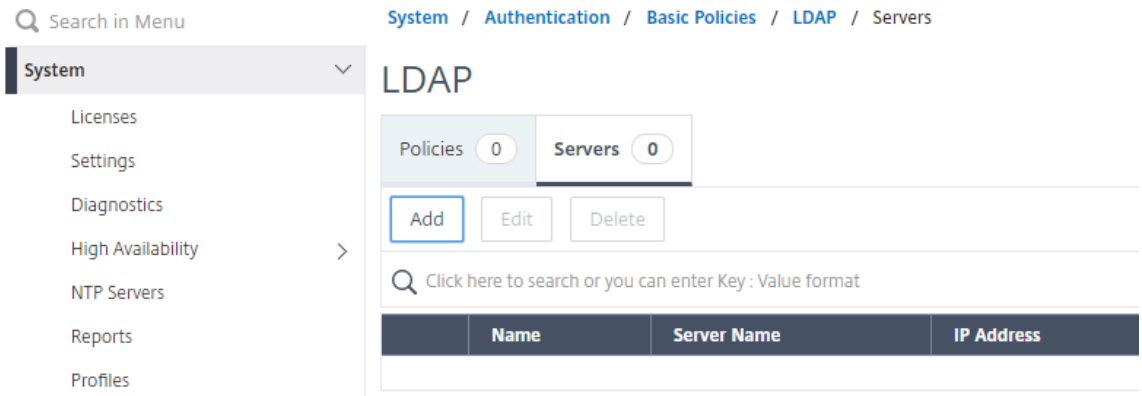
```
add authentication ldapAction <name> {
 -serverIP }
  <ip_addr|ipv6_addr|> | {
 -serverName <string> }
  }
```

Exemple

```
add authentication ldapAction ldap_server -serverip 1.1.1.1 -serverName
    ldap_test
```

Pour créer un serveur d'authentification LDAP à l'aide de l'utilitaire de configuration

1. Accédez à **Système > Authentification > Stratégies de base > LDAP > Serveurs > Ajouter**.



2. Dans la page **Créer un serveur LDAP d'authentification**, configurez les paramètres du serveur LDAP.

3. Cliquez sur **Créer**.

Pour activer une stratégie d'authentification à l'aide de l'interface de ligne de commande

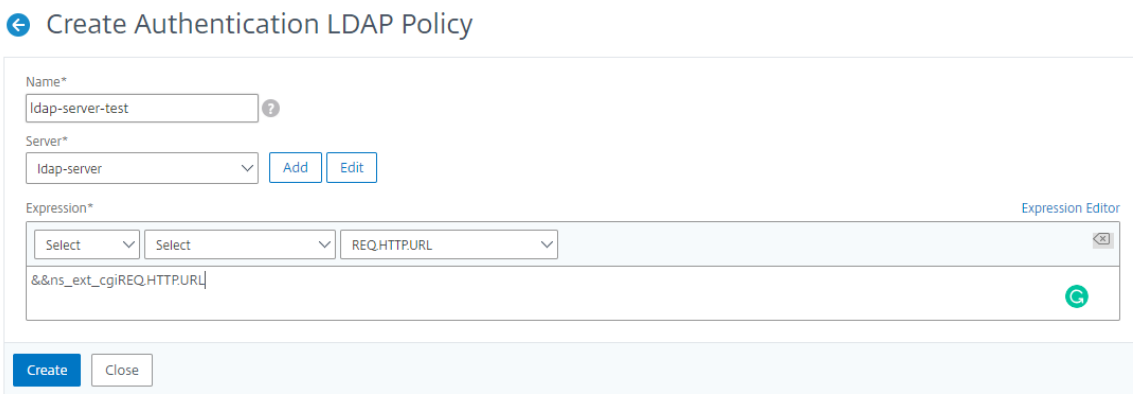
```
add authentication ldappolicy <name> <rule> [<reqAction>]
```

Exemple :

```
add authentication ldappolicy ldap-service-policy ns_true ldap_Server
```

Pour créer une stratégie d'authentification LDAP à l'aide de l'utilitaire de configuration

1. Accédez à **Système > Authentification > Stratégies de base > LDAP > Stratégies > Ajouter**
2. Dans la page **Créer une stratégie LDAP d'authentification**, configurez les paramètres de la stratégie LDAP.



3. Cliquez sur **Créer**.

> **Remarque**
>
> Vous pouvez configurer les serveurs/stratégies LDAP via l'onglet **Sécurité**. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies de base > LDAP > Serveurs/Stratégies**.

Pour activer la prise en charge des références LDAP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set authentication ldapAction <name> -followReferrals ON<!--NeedCopy-->`

- `set authentication ldapAction <name> -maxLDAPReferrals <integer><!--NeedCopy-->`

Exemple

```
1 > set authentication ldapAction ldapAction-1 -followReferrals ON
2 > set authentication ldapAction ldapAction-1 -maxLDAPReferrals 2
```

Prise en charge de l'authentification par clé pour les utilisateurs LDAP

Avec l'authentification par clé, vous pouvez désormais récupérer la liste des clés publiques stockées sur l'objet utilisateur dans le serveur LDAP via SSH. L'appliance Citrix ADC pendant le processus d'authentification basée sur les rôles (RBA) doit extraire les clés SSH publiques du serveur LDAP. La clé publique récupérée, qui est compatible avec SSH, doit vous permettre de vous connecter via la méthode RBA.

Un nouvel attribut « sshPublicKey » est introduit dans les commandes « add authentication ldapAction » et « set authentication ldapAction ». En utilisant cet attribut, vous pouvez obtenir les avantages suivants :

- Peut stocker la clé publique récupérée, et l'action LDAP utilise cet attribut pour récupérer les informations de clé SSH à partir du serveur LDAP.
- Peut extraire des noms d'attributs allant jusqu'à 24 Ko.

> Remarque
>
> Le serveur d'authentification externe, tel que LDAP, est utilisé uniquement pour récupérer les informations de clé SSH. Il n'est pas utilisé à des fins d'authentification.

Voici un exemple du flux d'événements à travers SSH :

- Le démon SSH envoie une requête AAA_AUTHENTICATE avec un champ de mot de passe vide au port du démon d'authentification, d'autorisation et d'audit.
- Si LDAP est configuré pour stocker la clé publique SSH, l'authentification, l'autorisation et l'audit répond avec l'attribut « sshPublicKey » ainsi que d'autres attributs.
- Le démon SSH vérifie ces clés avec les clés client.
- Le démon SSH transmet le nom d'utilisateur dans la charge utile de la requête, et l'authentification, l'autorisation et l'audit renvoie les clés spécifiques à cet utilisateur ainsi que les clés génériques.

Pour configurer l'attribut sshPublicKey, à l'invite de commandes, tapez les commandes suivantes :

- Avec l'opération add, vous pouvez ajouter l'attribut « sshPublicKey » lors de la configuration de la commande ldapAction.


```
add authentication ldapAction <name> { -serverIP <ip_addr|ipv6_addr
|*> | { -serverName <string> } } [-serverPort <port>] … [-Attribute1 <
string>] … [-Attribute16 <string>][-sshPublicKey <string>][-authentication
 off]<!--NeedCopy-->
```

- Avec l'opération set, vous pouvez configurer l'attribut « sshPublicKey » à une commande ldapAction déjà ajoutée.

```
set authentication ldapAction <name> [-sshPublicKey <string>][-authentication
 off]<!--NeedCopy-->
```

Prise en charge des attributs nom-valeur pour l'authentification LDAP

Vous pouvez maintenant configurer les attributs de l'authentification LDAP avec un nom unique ainsi que des valeurs. Les noms sont configurés dans le paramètre d'action LDAP et les valeurs sont obtenues en interrogeant le nom. En utilisant cette fonctionnalité, un administrateur d'appliance Citrix ADC peut désormais bénéficier des avantages suivants :

- Minimise l'effort pour les administrateurs en mémorisant l'attribut par nom (pas seulement par valeur)
- Améliore la recherche pour interroger la valeur d'attribut associée à un nom
- Fournit une option pour extraire plusieurs attributs

Pour configurer cette fonctionnalité à l'invite de commandes du dispositif Citrix ADC, tapez :

"'add authentication ldapAction [-Attribute1]

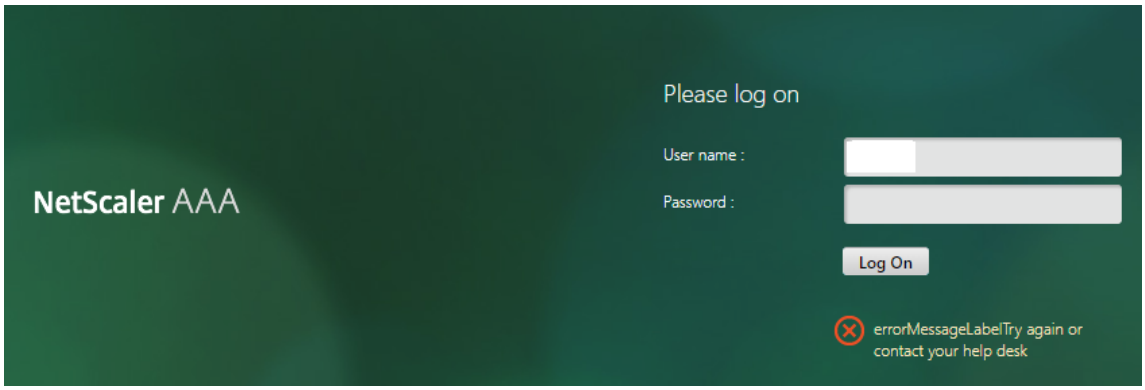
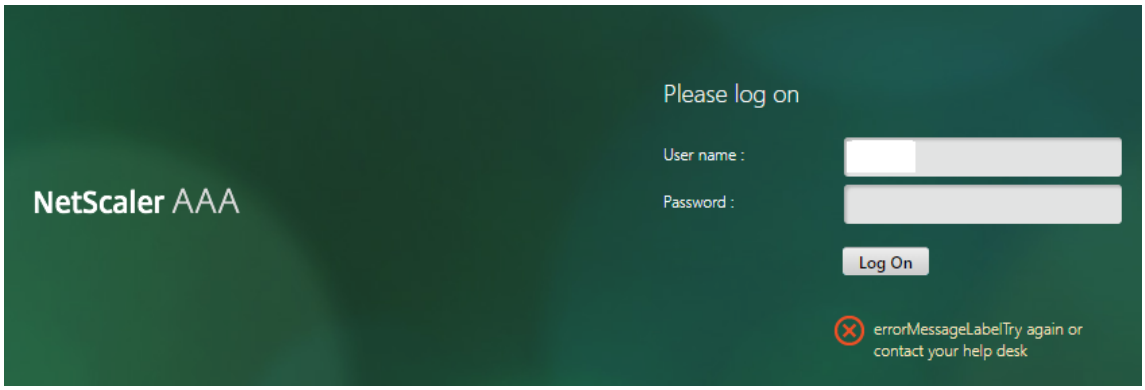
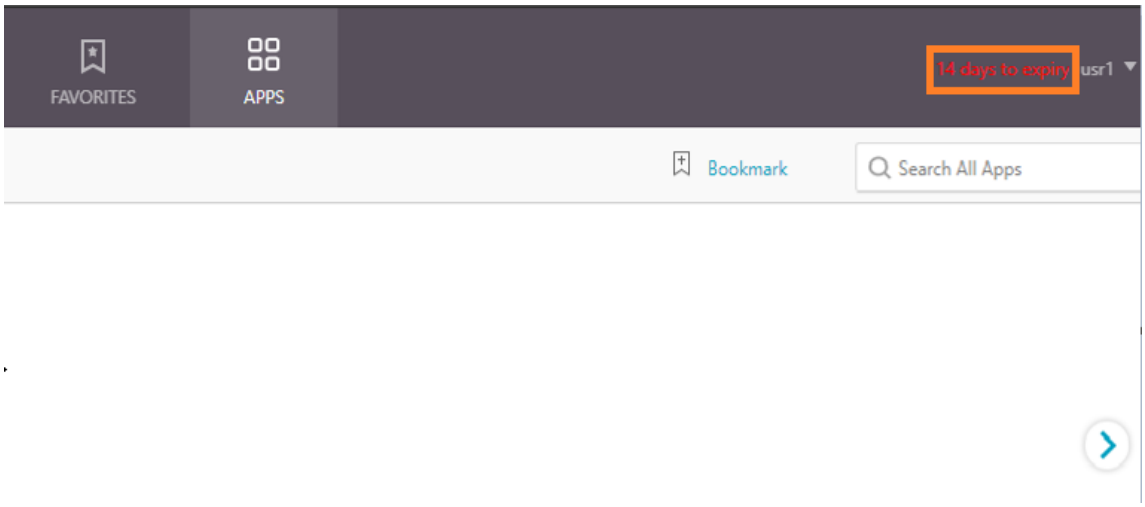
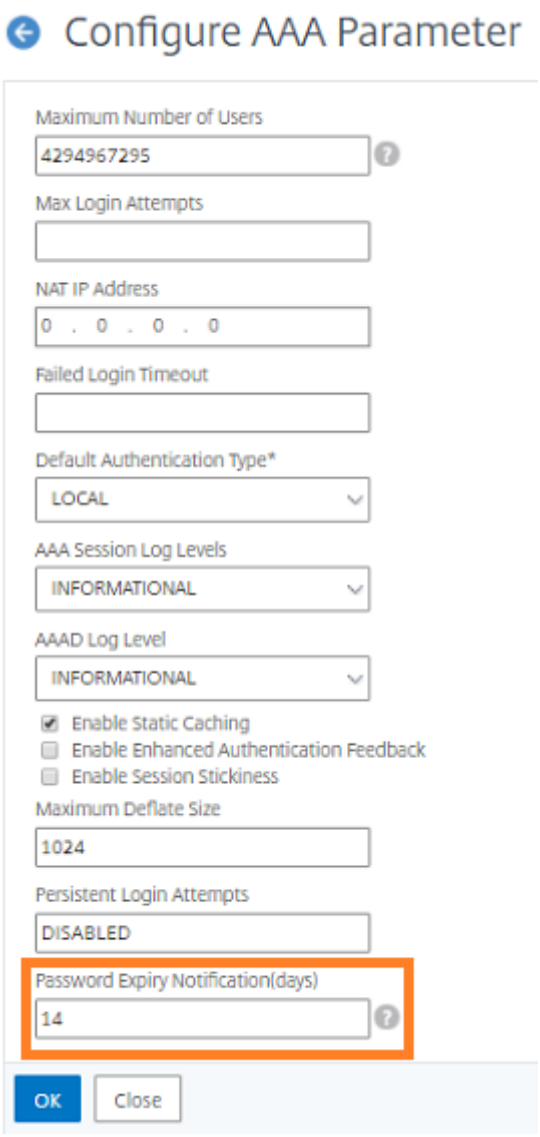
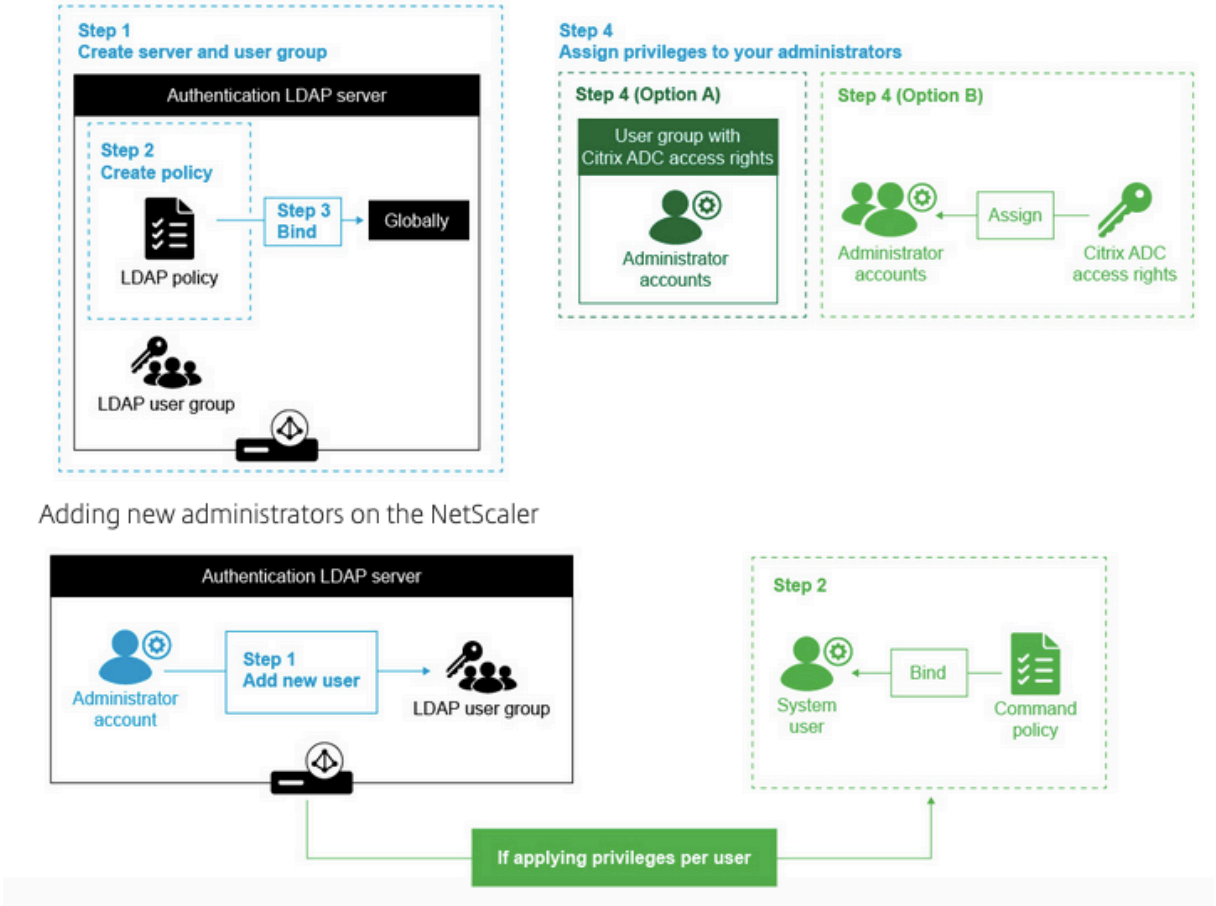
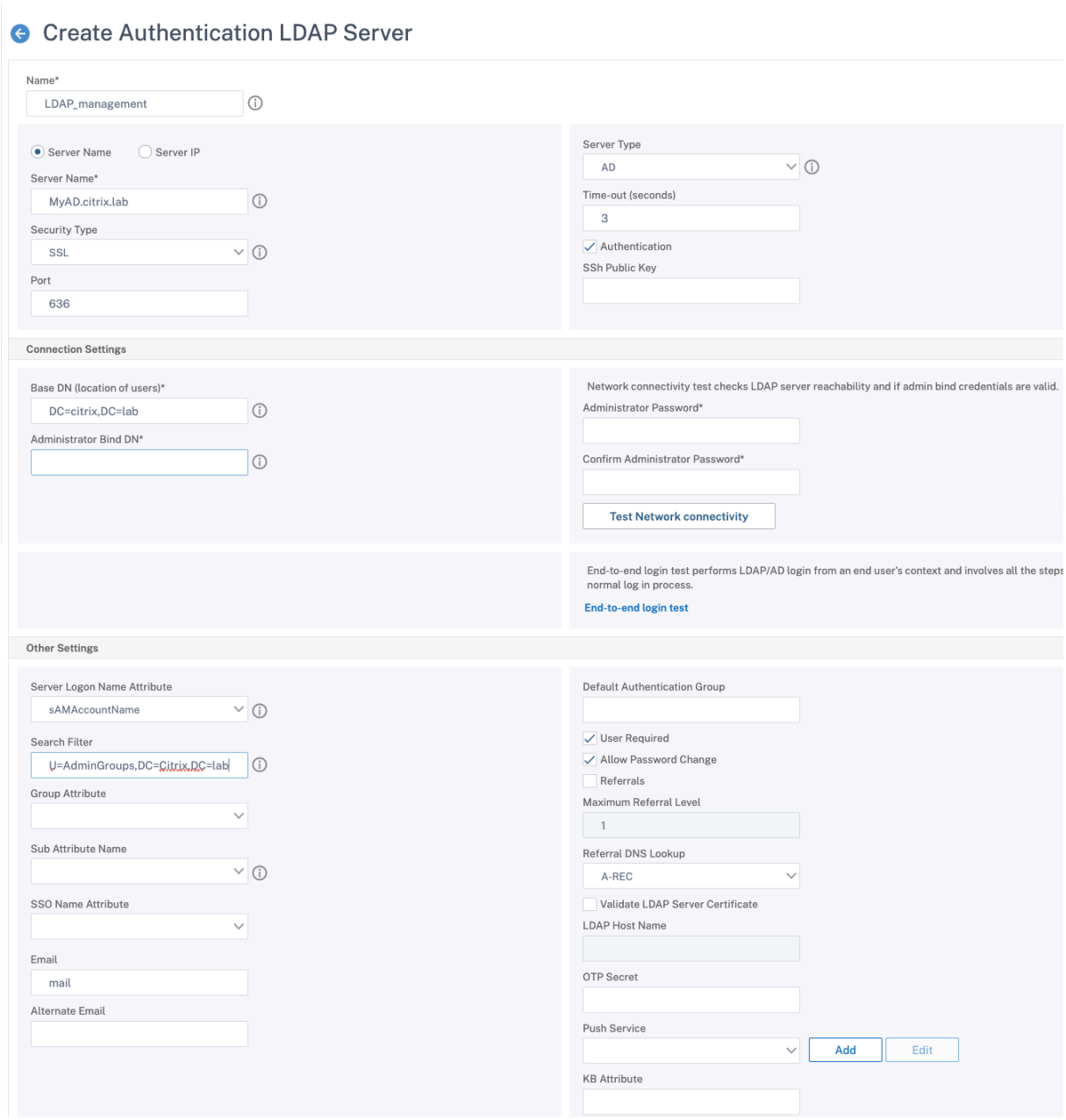
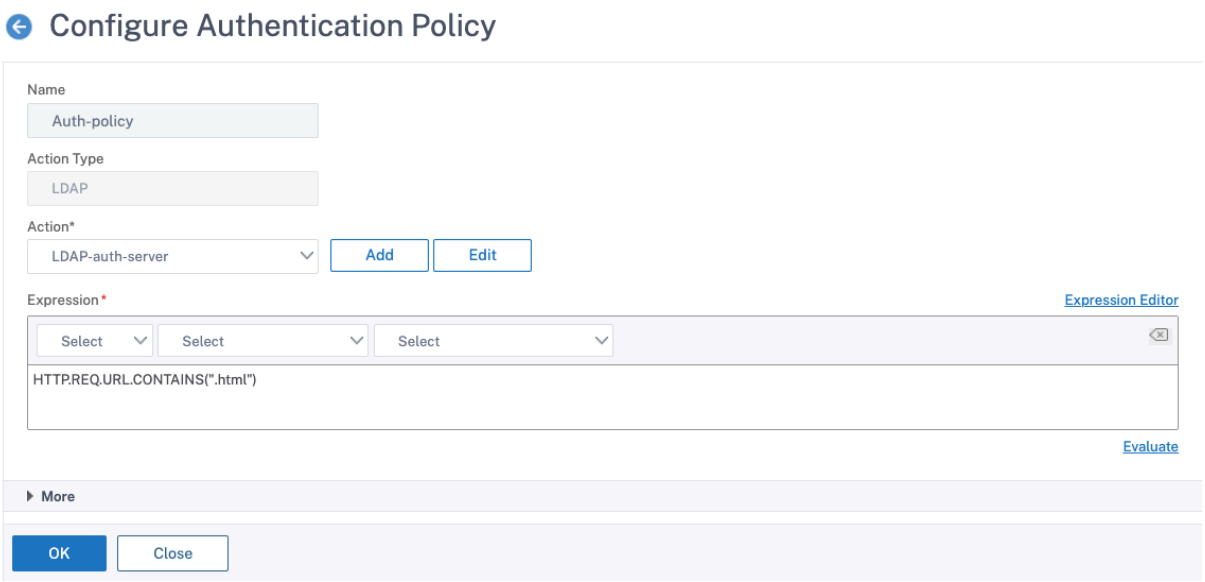
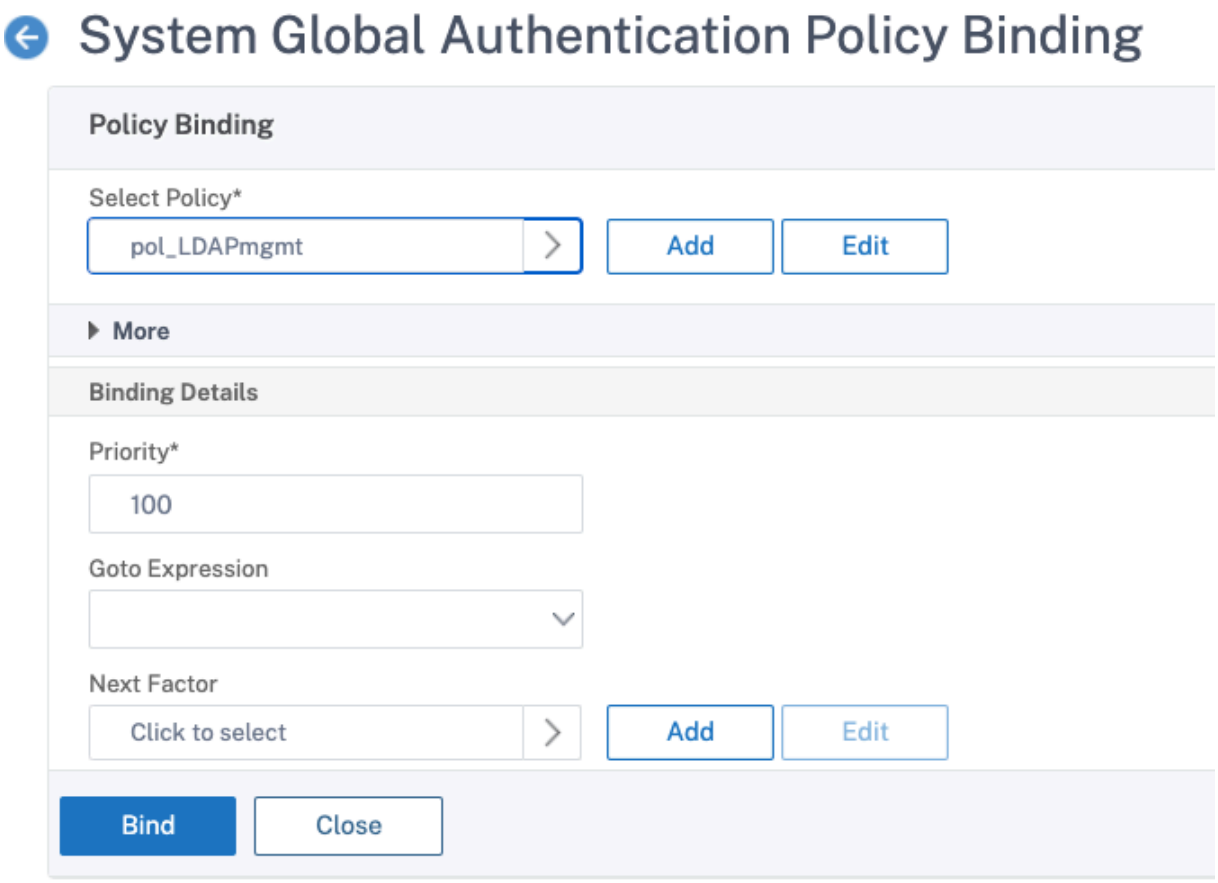
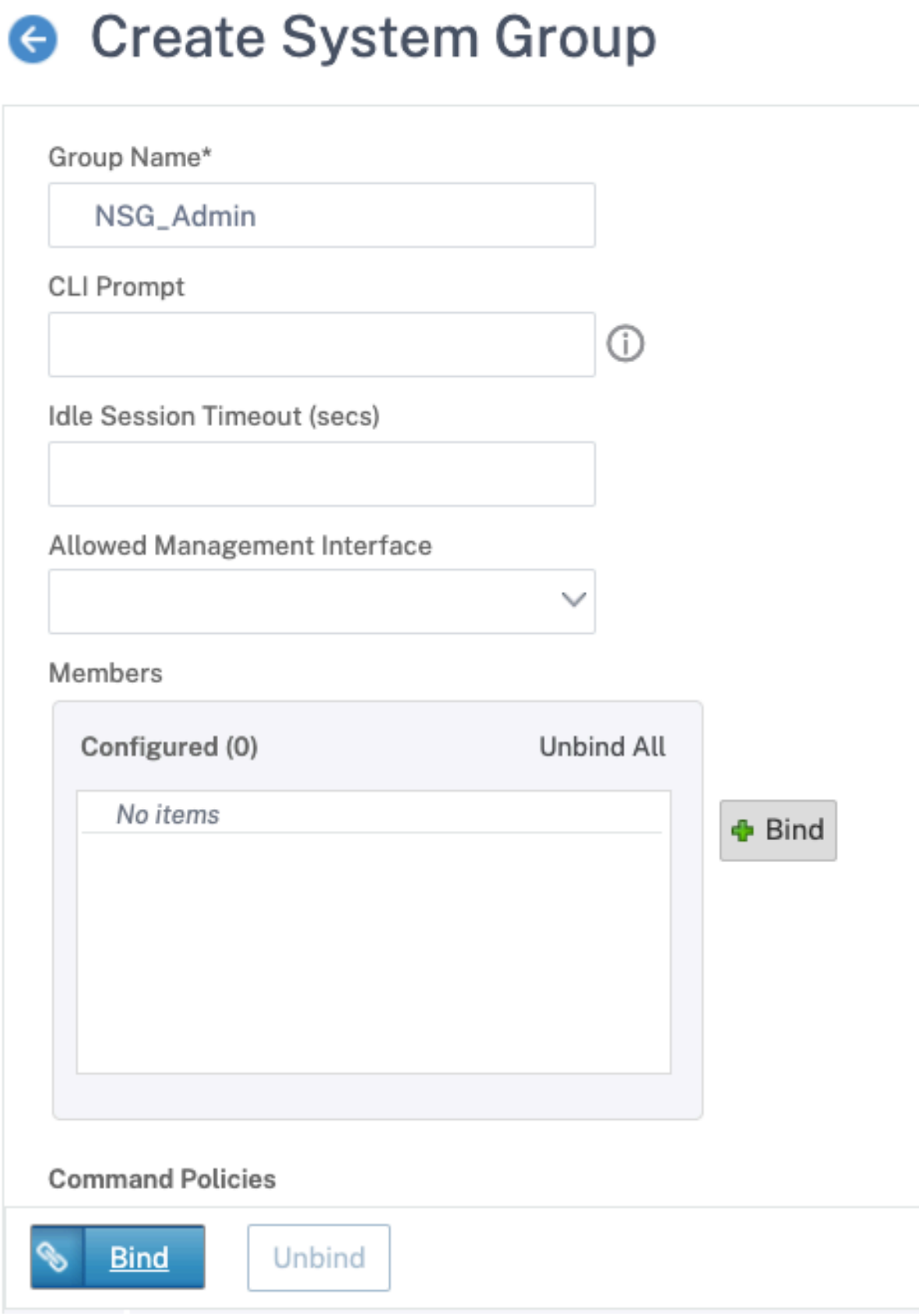
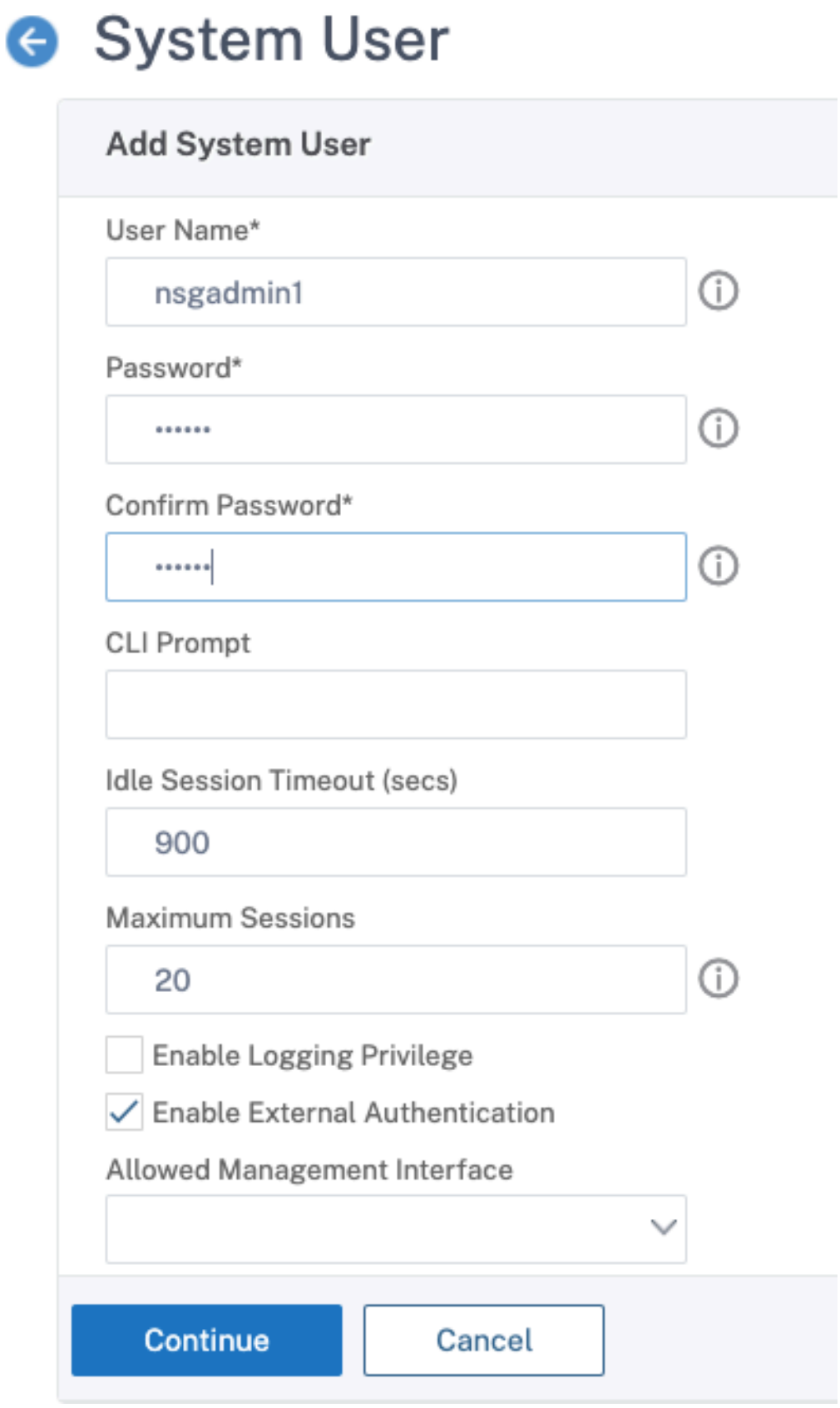
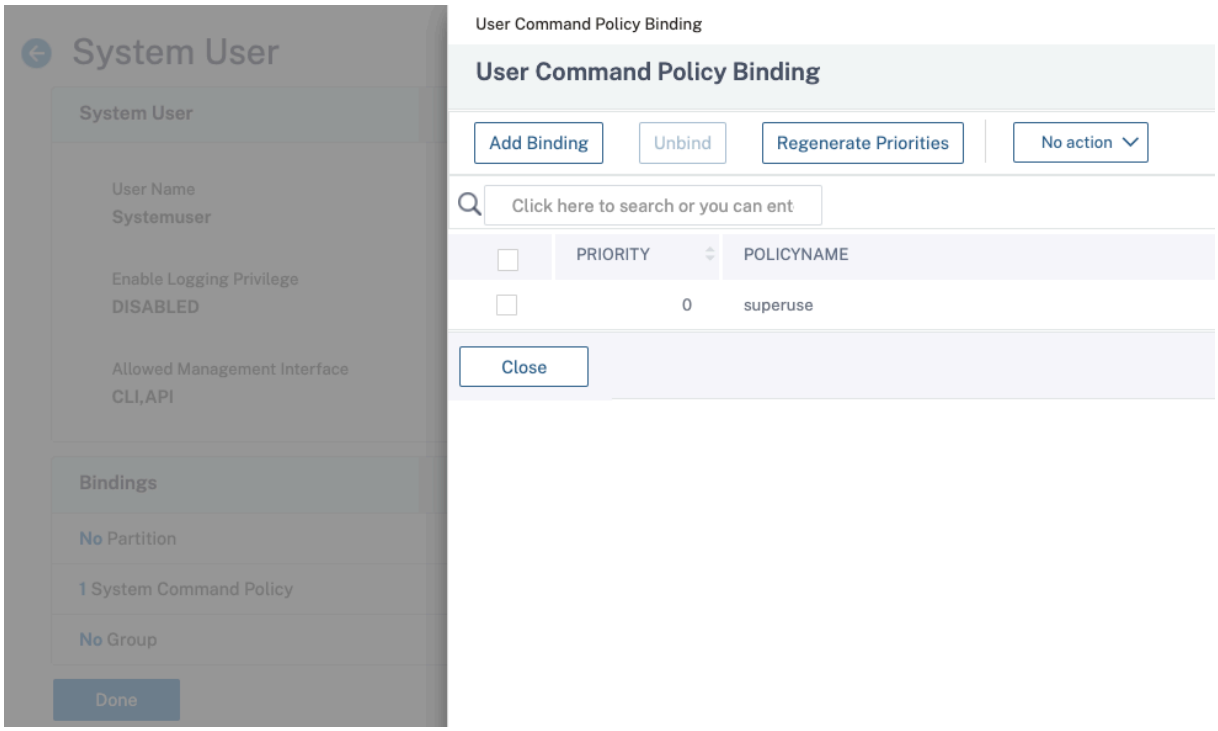
```
Exemple

```add authentication ldapAction ldapAct1 attribute1 mail<!--NeedCopy
   -->
```

Prise en charge de la validation de l'authentification LDAP de bout en bout

L'appliance Citrix ADC peut désormais valider l'authentification LDAP de bout en bout via l'interface graphique. Pour valider cette fonctionnalité, un nouveau bouton « test » est introduit dans l'interface graphique. Un administrateur d'appliance Citrix ADC peut utiliser cette fonctionnalité pour obtenir les avantages suivants :

- Consolide le flux complet (moteur de paquets — démon AAA Citrix ADC — serveur externe) pour une meilleure analyse
- Réduction du temps de validation et de dépannage des problèmes liés à des scénarios individuels


```

Vous disposez de deux options pour configurer et afficher les résultats de test de l'authentification de bout en bout LDAP à l'aide de l'interface graphique.

**Option du système**

1. Accédez à **Système > Authentification > Stratégies de base > LDAP,** cliquez sur onglet **Serveurs**.
2. Sélectionnez l**action LDAP** disponible dans la liste.
3. Sur la page **Configurer l'authentification serveur LDAP**, vous disposez de deux options sous la section **Paramètres de connexions**.
4. Pour vérifier la connexion au serveur LDAP, cliquez sur l'onglet **Tester l'accessibilité LDAP**. Vous pouvez afficher un message contextuel de connexion réussie au serveur LDAP avec les détails du port TCP et l'authenticité des informations d'identification valides.
5. Pour afficher l'authentification LDAP de bout en bout, cliquez sur le lien **Tester la connexion de l'utilisateur final** .
6. Dans la page **Tester la connexion de l'utilisateur final**, cliquez sur **Tester**.
   - Sur la page d'authentification, entrez les informations d'identification valides pour vous connecter. L'écran de réussite s'affiche.


   - Si l'authentification échoue, l'écran d'erreur s'affiche.




 

**À partir de l'option Authentification**

1. Accédez à **Authentification > Tableau de bord**, sélectionnez l'action LDAP disponible dans la liste.
2. Sur la page **Configurer l'authentification serveur LDAP**, vous disposez de deux options sous la section **Paramètres de connexions**.
3. Pour vérifier la connexion au serveur LDAP, cliquez sur l'onglet **Tester l'accessibilité LDAP**. Vous pouvez afficher un message contextuel de connexion réussie au serveur LDAP avec les détails du port TCP et l'authenticité des informations d'identification valides.
4. Pour afficher l'état de l'authentification LDAP de bout en bout, cliquez sur le lien **Tester la connexion de l'utilisateur final** .
5. Dans la page **Tester la connexion de l'utilisateur final**, cliquez sur **Tester**.
   - Sur la page d'authentification, entrez les informations d'identification valides pour vous connecter. L'écran de réussite s'affiche.


   - Si l'authentification échoue, l'écran d'erreur s'affiche.




## Notification d'expiration de mot de passe de 14 jours pour l'authentification LDAP

L'appliance Citrix ADC prend désormais en charge la notification d'expiration de mot de passe de 14 jours pour l'authentification basée sur LDAP. En utilisant cette fonctionnalité, les administrateurs peuvent informer les utilisateurs finaux du délai d'expiration du mot de passe, en jours. La notification d'expiration du mot de passe de 14 jours est un précurseur de la réinitialisation du mot de passe en libre-service (SSPR).

 

> **Remarque**
>
> La durée maximale ou seuil en jours pour la notification d'expiration du mot de passe est de 255 jours.

### Avantages de la notification d'expiration du mot de passe

- Permettre aux utilisateurs de réinitialiser eux-mêmes leurs mots de passe et fournir aux administrateurs un moyen flexible d'informer l'utilisateur final de l'expiration de leur mot de passe en quelques jours.
- Élimine la dépendance des utilisateurs finaux pour suivre leurs jours d'expiration de mot de passe.
- Envoie des notifications à la page du portail VPN aux utilisateurs (en fonction du nombre de jours) pour modifier leur mot de passe avant l'expiration.

> **Remarque**
>
> Cette fonctionnalité n'est applicable que pour les schémas d'authentification basés sur LDAP, et non pour RADIUS ou TACACS.

### Comprendre la notification de mot de passe de 14 jours

L'appliance Citrix ADC récupère deux attributs (`Max-Pwd-Age and Pwd-Last-Set`) du serveur d'authentification LDAP.

- **Max-Pwd-Age.** Cet attribut indique la durée maximale, par intervalles de 100 nanosecondes, jusqu'à ce que le mot de passe soit valide. La valeur est stockée sous la forme d'un grand nombre entier qui représente le nombre d'intervalles de 100 nanosecondes à partir du moment où le mot de passe a été défini avant l'expiration du mot de passe.
- **Pwd-Dernier Set.** Cet attribut détermine la date et l'heure auxquelles le mot de passe d'un compte a été modifié pour la dernière fois.

En récupérant les deux attributs à partir du serveur d'authentification LDAP, l'appliance Citrix ADC détermine le temps restant à expiration du mot de passe pour un utilisateur particulier. Ces informations sont collectées lorsque les informations d'identification de l'utilisateur sont validées sur le serveur d'authentification et qu'une notification est renvoyée à l'utilisateur.

Un nouveau paramètre « pwdExpiryNotification » est introduit dans la `set aaa parameter` commande. En utilisant ce paramètre, un administrateur peut suivre le nombre de jours restant pour l'expiration du mot de passe. L'appliance Citrix ADC peut maintenant commencer à avertir l'utilisateur final de l'expiration de son mot de passe.

 

> **Remarque**
>
> Actuellement, cette fonctionnalité fonctionne uniquement pour les serveurs d'authentification ayant des serveurs Microsoft AD avec implémentation LDAP. La prise en charge des serveurs basés sur OpenLDAP est ciblée ultérieurement.

Voici un exemple de flux d'événements pour définir une notification d'expiration de mot de passe de 14 jours :

1. Un administrateur, à l'aide de l'appliance Citrix ADC, définit un délai (14 jours) pour l'expiration du mot de passe.
2. L'utilisateur envoie une requête HTTP ou HTTPS pour accéder à une ressource sur le serveur principal.
3. Avant de fournir l'accès, l'appliance Citrix ADC valide les informations d'identification de l'utilisateur avec ce qui est configuré sur le serveur d'authentification LDAP.
4. Avec cette requête au serveur d'authentification, l'appliance Citrix ADC transporte la demande pour récupérer les détails de deux attributs (`Max-Pwd-Age and Pwd-Last-Set`).
5. Une notification d'expiration s'affiche en fonction du temps restant à courir pour que le mot de passe expire.
6. L'utilisateur prend ensuite les mesures appropriées pour mettre à jour le mot de passe.

**Pour configurer une notification d'expiration de 14 jours à l'aide de l'interface de ligne de commande**

> **Remarque**
>
> La notification d'expiration de 14 jours peut être configurée pour les cas d'utilisation VPN sans client et VPN complet et non pour ICA Proxy.

À l'invite de commandes, tapez les commandes suivantes :

- `set aaa parameter -pwdExpiryNotificationDays <positive_integer><!--NeedCopy-->`
- `show aaa parameter<!--NeedCopy-->`

Exemple

```
1 > set aaa parameter -pwdExpiryNotificationDays 14
2 Done
3 > show aaa parameter   Configured AAA parameters
      EnableStaticPageCaching: YES EnableEnhancedAuthFeedback: NO
    DefaultAuthType: LOCAL MaxAAAUsers: Unlimited
                                             AAAD nat ip: None
    EnableSessionStickiness : NO aaaSessionLoglevel : INFORMATIONAL
                 AAAD Log Level : INFORMATIONAL   Dynamic
     address: OFF
```


```
4     GUI mode: ON
5     Max Saml Deflate Size: 1024              Password Expiry
         Notification Days: 14
```

Pour configurer une notification d'expiration de 14 jours à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic des applications > Paramètres d'authentification**.
2. Cliquez sur **Modifier les paramètres AAA de l'authentification**.
3. Dans la page **Configurer le paramètre AAA**, spécifiez les jours dans le champ **Notification d'expiration du mot de passe (jours)**.



4. Cliquez sur **OK.**

   La notification apparaît dans le coin supérieur droit de la page du portail VPN.



Configurer l'authentification LDAP sur l'appliance Citrix ADC à des fins de gestion

August 20, 2021

Vous pouvez configurer l'ouverture de session de l'utilisateur sur l'appliance Citrix ADC à l'aide des informations d'identification Active Directory (nom d'utilisateur et mot de passe) à des fins de gestion (superutilisateur, lecture seule, privilèges réseau, etc.).

Conditions préalables

- Serveurs de contrôleur de domaine Windows Active Directory
- Un groupe de domaines dédié aux administrateurs NetScaler
- Citrix Gateway 10.1 et versions ultérieures

Les figures suivantes illustrent l'authentification LDAP sur l'appliance Citrix ADC.



Étapes de configuration de haut niveau

1. Créer un serveur LDAP
2. Créer une stratégie LDAP
3. Lier la stratégie LDAP
4. Attribuez des privilèges à vos administrateurs de l'une des manières suivantes
    - Appliquer des privilèges sur le groupe
    - Appliquer des privilèges individuellement pour chaque utilisateur

Créer un serveur LDAP d'authentification

1. Accédez à **Système > Authentification > LDAP**.
2. Cliquez sur l'onglet **Serveur**, puis cliquez sur **Ajouter**.
3. Terminez la configuration, puis cliquez sur **Créer**.



> **Remarque :**
>
> dans cet exemple, l'accès est limité à l'appliance Citrix ADC en filtrant l'authentification sur l'appartenance au groupe d'utilisateurs en définissant le filtre de recherche. La valeur utilisée pour cet exemple est - & (memberOf=CN=NSG_admin, OU=AdminGroups, DC=Citrix, DC=lab)

Créer une stratégie LDAP

1. Accédez à **Système > Authentification > Stratégies avancées > Stratégie**.
2. Cliquez sur **Ajouter**.
3. Entrez un nom pour la stratégie, sélectionnez le serveur que vous avez créé au cours des étapes précédentes.
4. Dans le champ de texte Expression, entrez l'expression appropriée, puis cliquez sur **Créer**.



Lier la politique LDAP à l'échelle mondiale

1. Accédez à **Système > Authentification > Stratégies avancées > Stratégie**.
2. Dans la page Stratégies d'authentification, cliquez sur **Liaisons globales**.
3. Sélectionnez la stratégie que vous avez créée (dans cet exemple, Pol_LDAPMgmt).
4. Choisissez une priorité en conséquence (plus le nombre est bas, plus la priorité est élevée)
5. Cliquez sur **Liaison,** puis **Terminé**. Une coche verte apparaît dans la colonne **Bound Bound**.



Attribuer des privilèges à vos administrateurs

Vous pouvez choisir l'une des deux options suivantes.

- **Appliquer des privilèges sur un groupe :** ajoutez un groupe dans l'appliance Citrix ADC et attribuez les mêmes droits d'accès à chaque utilisateur qui est membre de ce groupe.
- **Appliquer des privilèges individuellement pour chaque utilisateur :** créez chaque compte d'administrateur utilisateur et attribuez des droits à chacun d'eux.

Appliquer des privilèges sur un groupe

Lorsque vous appliquez des privilèges sur un groupe, les utilisateurs membres du groupe Active Directory configuré dans le filtre de recherche (dans cet exemple, NSG_Admin) peuvent se connecter à l'interface de gestion Citrix ADC et disposer d'une stratégie de commande de superutilisateur.

1. Accédez à **Système > Administration des utilisateurs > Groupes**.
2. Entrez les détails selon l'exigence, puis cliquez sur **Créer**.



Vous avez défini le groupe Active Directory auquel appartiennent les utilisateurs ainsi que le niveau de stratégie de commande qui doit être associé au compte lors de la connexion. Vous pouvez ajouter de nouveaux utilisateurs administrateur au groupe LDAP que vous avez configuré dans le filtre de recherche.

> **Remarque :**
>
> le nom du groupe doit correspondre à l'enregistrement Active Directory.

Appliquer des privilèges individuellement pour chaque utilisateur

Dans ce scénario, les utilisateurs qui sont membres de votre groupe Active Directory configuré dans le filtre de recherche (dans cet exemple, NSG_Admin) peuvent se connecter à l'interface de gestion Citrix ADC mais ne disposent pas de privilèges tant que vous n'avez pas créé l'utilisateur spécifique sur l'appliance Citrix ADC et y lier la stratégie de commande.

1. Accédez à **Système > Administration des utilisateurs > Utilisateurs**.
2. Cliquez sur **Ajouter**.
3. Entrez les détails selon le besoin.

   Remarque : veillez à sélectionner **Activer l'authentification externe**.



1. Cliquez sur **Continuer**.

Vous avez défini l'utilisateur Active Directory et le niveau de stratégie de commande qui doivent être associés au compte lors de la connexion.

> **Remarque :**
>
> - Le nom d'utilisateur doit correspondre à l'enregistrement Active Directory de l'utilisateur existant.
> - Lorsque vous ajoutez un utilisateur à Citrix ADC pour l'authentification externe, vous devez fournir un mot de passe, si l'authentification externe n'est pas disponible. Pour que l'authentification externe fonctionne correctement, le mot de passe interne ne doit pas être le même que le mot de passe LDAP du compte d'utilisateur.

Ajouter une stratégie de commande à l'utilisateur

1. Accédez à **Système > Administration des utilisateurs > Utilisateurs**.
2. Sélectionnez l'utilisateur que vous avez créé, puis cliquez sur **Modifier.**
3. Dans Liaisons, cliquez sur **Stratégie de commande système**.
4. Sélectionnez la stratégie de commande appropriée à appliquer à votre utilisateur.
5. Cliquez sur **Lier,** puis sur **Fermer**.



Pour ajouter d'autres administrateurs ;

- Ajoutez les utilisateurs administrateur au groupe LDAP que vous avez configuré dans le filtre de recherche.

- Créez l'utilisateur système dans Citrix ADC et attribuez la stratégie de commande correcte.

Pour configurer l'authentification LDAP sur l'appliance Citrix ADC à des fins de gestion à l'aide de l'interface de ligne de commande

Utilisez les commandes suivantes comme référence pour configurer la connexion d'un groupe disposant de privilèges de superutilisateur sur l'interface de ligne de commande Citrix ADC Appliance CLI.

1. Créer un serveur LDAP

```
add authentication ldapAction LDAP_mgmt -serverIP myAD.citrix.lab
    -serverPort 636 -ldapBase "DC=citrix,DC=lab" -ldapBindDn
    readonly@citrix.lab -ldapBindDnPassword -ldapLoginName
    sAMAccountName -searchFilter "&(memberof=CN=NSG_Admin,OU=
    AdminGroups,DC=citrix,DC=lab)" -groupAttrName memberOf
<!--NeedCopy-->
```

2. Créer et stratégie LDAP

```
add authentication ldapPolicy pol_LDAPmgmt ns_true LDAP_mgmt
<!--NeedCopy-->
```

3. Liaison de la stratégie LDAP

```
bind system global pol_LDAPmgmt -priority 110
<!--NeedCopy-->
```

4. Attribuer des privilèges à vos administrateurs

   - Pour appliquer des privilèges sur le groupe

```
add system group NSG_Admin
bind system group NSG_Admin -policyName superuser 100
<!--NeedCopy-->
```

   - Pour appliquer des privilèges individuellement à chaque utilisateur

```
add system user admyoa
bind system user admyoa superuser 100
<!--NeedCopy-->
```


Authentification RADIUS

August 20, 2021

Comme pour les autres types de stratégies d'authentification, une stratégie d'authentification RADIUS (Remote Authentication Dial In User Service) comprend une expression et une action. Après avoir créé une stratégie d'authentification, vous la liez à un serveur virtuel d'authentification et lui attribuez une priorité. Lorsque vous la liez, vous la définissez également comme stratégie principale ou secondaire. Toutefois, la configuration d'une stratégie d'authentification RADIUS comporte certaines exigences particulières décrites ci-dessous.

Normalement, vous configurez Citrix ADC pour qu'il utilise l'adresse IP du serveur d'authentification lors de l'authentification. Avec les serveurs d'authentification RADIUS, vous pouvez maintenant configurer ADC pour qu'il utilise le nom de domaine complet du serveur RADIUS au lieu de son adresse IP pour authentifier les utilisateurs. L'utilisation d'un nom de domaine complet peut simplifier une configuration d'authentification, d'autorisation et d'audit beaucoup plus complexe dans les environnements où le serveur d'authentification peut se trouver à l'une des adresses IP multiples, mais utilise toujours un seul nom de domaine complet. Pour configurer l'authentification à l'aide du nom de domaine complet d'un serveur au lieu de son adresse IP, vous suivez le processus de configuration normal, sauf lors de la création de l'action d'authentification. Lors de la création de l'action, vous remplacez le paramètre **ServerName** par le paramètre **ServerIP** .

Avant de décider s'il convient de configurer Citrix ADC pour qu'il utilise l'adresse IP ou le nom de domaine complet de votre serveur RADIUS pour authentifier les utilisateurs, considérez que la configuration de l'authentification, de l'autorisation et de l'audit pour s'authentifier auprès d'un nom de domaine complet au lieu d'une adresse IP ajoute une étape supplémentaire au processus d'authentification. Chaque fois que ADC authentifie un utilisateur, il doit résoudre le nom de domaine complet. Si un grand nombre d'utilisateurs tentent de s'authentifier simultanément, les recherches DNS résultantes peuvent ralentir le processus d'authentification.

> **Remarque**
>
> Ces instructions supposent que vous connaissez déjà le protocole RADIUS et que vous avez déjà configuré le serveur d'authentification RADIUS choisi.

Pour ajouter une action d'authentification pour un serveur RADIUS à l'aide de l'interface de ligne de commande

Si vous vous authentifiez sur un serveur RADIUS, vous devez ajouter une action d'authentification explicite. Pour ce faire, à l'invite de commandes, tapez la commande suivante :

```
1 add authentication radiusAction <name> [-serverip <IP> | -serverName] <
      FQDN>][-serverPort <port>] [-authTimeout <positive_integer>] {
```



```
 -radKey  }
  [-radNASip ( ENABLED | DISABLED )][-radNASid <string>] [-radVendorID
     <positive_integer>][-radAttributeType <positive_integer>][-
     radGroupsPrefix <string>] [-radGroupSeparator <string>][-
     passEncoding <passEncoding>][-ipVendorID <positive_integer>] [-
     ipAttributeType <positive_integer>][-accounting ( ON | OFF )][-
     pwdVendorID <positive_integer> [-pwdAttributeType <
     positive_integer>]] [-defaultAuthenticationGroup <string>] [-
     callingstationid ( ENABLED | DISABLED )]

<!--NeedCopy-->
```

L'exemple suivant ajoute une action d'authentification RADIUS nommée **Authn-Act-1**, avec l'IP du serveur **10.218.24.65**, le port du serveur **1812**, le délai d'authentification de **15**minutes, la clé rayon **WarethElorax**, l'IP du NAS désactivée et l'ID du NAS **NAS1**.

```
add authentication radiusaction Authn-Act-1 -serverip 10.218.24.65 -
   serverport 1812 -authtimeout 15 -radkey WareTheLorax -radNASip
   DISABLED -radNASid NAS1
Done

<!--NeedCopy-->
```

L'exemple suivant ajoute la même action d'authentification RADIUS, mais en utilisant le nom de domaine complet du serveur **rad01.example.com** au lieu de l'adresse IP.

```
add authentication radiusaction Authn-Act-1 -serverName rad01.example.
   com -serverport 1812 -authtimeout 15 -radkey WareTheLorax -radNASip
   DISABLED -radNASid NAS1
Done

<!--NeedCopy-->
```

Pour configurer une action d'authentification pour un serveur RADIUS externe à l'aide de la ligne de commande

Pour configurer une action RADIUS existante, à l'invite de commandes, tapez la commande suivante :

```
set authentication radiusAction <name> [-serverip <IP> | -serverName] <
   FQDN>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -radKey  }
  [-radNASip ( ENABLED | DISABLED )][-radNASid <string>] [-radVendorID
     <positive_integer>][-radAttributeType <positive_integer>][-
     radGroupsPrefix <string>] [-radGroupSeparator <string>][-
```



```
        passEncoding <passEncoding>][-ipVendorID <positive_integer>] [-
        ipAttributeType <positive_integer>][-accounting ( ON | OFF )][-
        pwdVendorID <positive_integer> [-pwdAttributeType <
        positive_integer>]] [-defaultAuthenticationGroup <string>] [-
        callingstationid ( ENABLED | DISABLED )]
4
5 <!--NeedCopy-->
```

Pour supprimer une action d'authentification pour un serveur RADIUS externe à l'aide de l'interface de ligne de commande

Pour supprimer une action RADIUS existante, à l'invite de commandes, tapez la commande suivante :

```
1 rm authentication radiusAction <name>
2
3 <!--NeedCopy-->
```

Exemple

```
1 rm authentication radiusaction Authn-Act-1
2 Done
3
4 <!--NeedCopy-->
```

Pour configurer un serveur RADIUS à l'aide de l'utilitaire de configuration

> **Remarque**
>
> Dans l'utilitaire de configuration, le terme serveur est utilisé à la place de l'action, mais fait référence à la même tâche.

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Rayon**
2. Dans le volet d'informations, sous l'onglet **Serveurs**, effectuez l'une des opérations suivantes :
   - Pour créer un serveur RADIUS, cliquez sur **Ajouter**.
   - Pour modifier un serveur RADIUS existant, sélectionnez le serveur, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Créer un serveur RADIUSd'authentification ou Configurer un serveur RADIUS**d'authentification, tapez ou sélectionnez des valeurs pour les paramètres. Pour remplir les paramètres qui apparaissent sous**Send Calling Station ID**, développez**Détails**.
   - name*—radiusActionName (Impossible de changer pour une action configurée précédemment)

- Type d'authentification*: authtype (défini sur RADIUS, ne peut pas être modifié)
- Nom du serveur/Adresse IP* : choisissez le nom du serveur ou l'adresse IP du serveur
  - <FQDN>Nom du serveur* : nom du serveur
  - Adresse IP*—ServerIP <IP> Si une adresse IP IPv6 est attribuée au serveur, activez la case à cocher IPv6.
- Port*—serverPort
- Délai d'expiration (secondes)*—AuthTimeout
- Clé secrète*—Clé radkey (secret partagé RADIUS).
- Confirmer la clé secrète *(Confirm Secret Key) : saisissez le secret partagé RADIUS une seconde fois. (Pas d'équivalent en ligne de commande.)
- Envoyer l'ID de la station d'appel : CallingStationID
- Identificateur du fournisseur de groupe—RadvendorID
- Type d'attribut de groupe—RadAttributeType
- Identificateur du fournisseur d'adresse IP : IPVendorID
- PWDVendorID—PWDVendorID
- Encodage de mot de passe : encodage de mot de passe
- Groupe d'authentification par défaut—DefaultAuthenticationGroup
- NAS ID—radNASid
- Activer l'extraction de l'adresse IP du NAS — radNASip
- Préfixe de groupe—radGroupsPrefix
- Séparateur de groupe—radGroupSeparator
- Type d'attribut d'adresse IP—ipAttributeType
- Type d'attribut de mot de passe—pwdAttributeType
- Comptabilité — accounting

4. Cliquez sur **Créer** ou **sur OK**. La stratégie que vous avez créée apparaît dans la page Serveurs.

Prise en charge de passer par l'attribut RADIUS 66 (Tunnel-Client-Endpoint)

L'appliance Citrix ADC autorise désormais la transmission de l'attribut RADIUS 66 (Tunnel-Client-Endpoint) pendant l'authentification RADIUS. En appliquant cette fonctionnalité, l'adresse IP des clients est reçue par l'authentification de second facteur de confier à prendre des décisions d'authentification basées sur le risque.

Un nouvel attribut « TunnelEndPointClientIP » est introduit à la fois dans la commande « add authentication RadiusAction » et « set RadiusParams ».

Pour utiliser cette fonctionnalité, à l'invite de commandes du dispositif Citrix ADC, tapez :

```
add authentication radiusAction <name> {
 -serverIP <ip_addr|ipv6_addr|*> | {
 -serverName <string> }
  }
  [-serverPort <port>] … [-tunnelEndpointClientIP (ENABLED|DISABLED)]

set radiusParams {
 -serverIP <ip_addr|ipv6_addr|*> |{
 -serverName <string> }
  }
  [-serverPort<port>] … [-tunnelEndpointClientIP(ENABLED|DISABLED)]

<!--NeedCopy-->
```

Exemple

```
add authentication radiusAction radius -severIP 1.217.22.20 -serverName
     FQDN -serverPort 1812 -tunnelEndpointClientIp ENABLED

set radiusParams -serverIp 1.217.22.20 -serverName FQDN1 -serverPort
    1812 -tunnelEndpointClientIP ENABLED

<!--NeedCopy-->
```

Prise en charge de la validation de l'authentification RADIUS de bout en bout

L'appliance Citrix ADC peut désormais valider l'authentification RADIUS de bout en bout via une interface graphique. Pour valider cette fonctionnalité, un nouveau bouton « test » est introduit dans l'interface graphique. Un administrateur d'appliance Citrix ADC peut tirer parti de cette fonctionnalité pour obtenir les avantages suivants :

- Consolide le flux complet (moteur de paquets — démon aaa — serveur externe) pour fournir une meilleure analyse
- Réduction du temps de validation et de dépannage des problèmes liés à des scénarios individuels

Vous disposez de deux options pour configurer et afficher les résultats de test de l'authentification de bout en bout RADIUS à l'aide de l'interface graphique.

Option du système

1. Accédez à **Système > Authentification > Stratégies de base > RADIUS,** cliquez sur l'onglet **Serveurs**.
2. Sélectionnez l'**action RADIUS** disponible dans la liste.
3. Sur la page **Configurer le serveur RADIUS d'authentification**, vous disposez de deux options sous la section **Paramètres de connexion**.
4. Pour vérifier la connexion au serveur RADIUS, cliquez sur l'onglet **Tester l'accessibilité RADIUS**.
5. Pour afficher l'authentification RADIUS de bout en bout, cliquez sur le lien **Tester la connexion de l'utilisateur final** .

À partir de l'option Authentification

1. Accédez à **Authentification > Tableau de bord**, sélectionnez l'action RADIUS disponible dans la liste.
2. Sur la page **Configurer le serveur RADIUS d'authentification**, vous disposez de deux options sous la section **Paramètres de connexion**.
3. Pour vérifier la connexion au serveur RADIUS, cliquez sur l'onglet **Tester l'accessibilité RADIUS**.
4. Pour afficher l'état de l'authentification RADIUS de bout en bout, cliquez sur le lien **Tester la connexion de l'utilisateur final** .

authentification TACACS

August 20, 2021

La stratégie d'authentification TACACS s'authentifie auprès d'un serveur d'authentification TACACS (Terminal Access Controller Access Control System) externe.
Une fois qu'un utilisateur s'est authentifié auprès d'un serveur TACACS, Citrix ADC se connecte au même serveur TACACS pour toutes les autorisations suivantes. Lorsqu'un serveur TACACS principal n'est pas disponible, cette fonctionnalité empêche tout retard pendant que ADC attend l'échéance du premier serveur TACACS. Cela se produit avant de renvoyer la demande d'autorisation au deuxième serveur TACACS.

> **Remarque :**
>
> le serveur d'autorisation TACACS ne prend pas en charge les commandes dont la longueur de chaîne dépasse 255 caractères.
>
> **Solution :** utilisez l'autorisation locale au lieu d'un serveur d'autorisation TACACS.

Lors de l'authentification via un serveur TACACS, l'authentification, l'autorisation et l'audit des journaux de gestion du trafic exécutent uniquement les commandes TACACS. Il empêche les journaux

d'afficher les commandes TACACS saisies par les utilisateurs qui n'étaient pas autorisés à les exécuter.

À partir de NetScaler 12.0 Build 57.x, le Terminal Access Controller Access-Control System (TACACS) ne bloque pas le processus d'authentification, d'autorisation et d'audit lors de l'envoi de la demande TACACS. Autoriser l'authentification LDAP et RADIUS à poursuivre la demande. La demande d'authentification TACACS reprend une fois que le serveur TACACS a accusé réception de la demande TACACS.

> **Important :**
>
> - Citrix vous recommande de ne pas modifier les configurations associées TACACS lorsque vous exécutez une commande « clear ns config ».
> - La configuration associée à TACACS liée aux stratégies avancées est effacée et réappliquée lorsque le paramètre « RBAConfig » est défini sur NO dans la commande « clear ns config » pour la stratégie avancée.

Prise en charge des attributs nom-valeur pour l'authentification TACACS

Vous pouvez désormais configurer les attributs d'authentification TACACS avec un nom unique ainsi que des valeurs. Les noms sont configurés dans le paramètre d'action TACACS et les valeurs sont obtenues en interrogeant les noms. En spécifiant la valeur de l'attribut name, les administrateurs peuvent facilement rechercher la valeur d'attribut associée au nom de l'attribut. De plus, les administrateurs n'ont plus à se souvenir de l'attribut par sa seule valeur.

> **Important**
>
> - Dans la commande TacacsAction, vous pouvez configurer un maximum de 64 attributs séparés par une virgule avec une taille totale inférieure à 2048 octets.

Pour configurer les attributs nom-valeur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add authentication tacacsAction <name> [-Attributes <string>]
2 <!--NeedCopy-->
```

Exemple :

```
1 add authentication tacacsAction tacacsAct1 -attributes  "mail,sn,
     userprincipalName"
2 <!--NeedCopy-->
```


Pour ajouter une action d'authentification à l'aide de l'interface de ligne de commande

Si vous n'utilisez pas l'authentification LOCAL, vous devez ajouter une action d'authentification explicite. À l'invite de commandes, tapez la commande suivante :

```
1 add authentication tacacsAction <name> -serverip <IP> [-serverPort <
     port>][-authTimeout <positive_integer>][ ... ]
2 <!--NeedCopy-->
```

Exemple

```
1 add authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
     serverport 1812                    -authtimeout 15 -tacacsSecret "
     minotaur" -authorization OFF -accounting ON -auditFailedCmds OFF -
     defaultAuthenticationGroup "users"
2 <!--NeedCopy-->
```

Pour configurer une action d'authentification à l'aide de l'interface de ligne de commande

Pour configurer une action d'authentification existante, à l'invite de commandes, tapez la commande suivante :

```
1 set authentication tacacsAction <name> -serverip <IP> [-serverPort <
     port>][-authTimeout <positive_integer>][ ... ]
2 <!--NeedCopy-->
```

Exemple

```
1      > set authentication tacacsaction Authn-Act-1 -serverip
          10.218.24.65 -serverport 1812                    -authtimeout 15
          -tacacsSecret "minotaur" -authorization OFF -accounting ON -
          auditFailedCmds OFF -defaultAuthenticationGroup "users"    Done
2 <!--NeedCopy-->
```

Pour supprimer une action d'authentification à l'aide de l'interface de ligne de commande

Pour supprimer une action RADIUS existante, à l'invite de commandes, tapez la commande suivante :

```
1 rm authentication radiusAction <name>
2 <!--NeedCopy-->
```

Exemple


```
rm authentication tacacsaction Authn-Act-1
<!--NeedCopy-->
```

Authentification du certificat client

August 20, 2021

Les sites Web qui contiennent du contenu sensible, tels que les sites Web bancaires en ligne ou les sites Web contenant des renseignements personnels sur les employés, nécessitent parfois des certificats client pour l'authentification. Pour configurer l'authentification, l'autorisation et l'audit pour authentifier les utilisateurs sur la base des attributs de certificat côté client, vous activez d'abord l'authentification client sur le serveur virtuel de gestion du trafic et liez le certificat racine au serveur virtuel d'authentification. Ensuite, vous implémentez l'une des deux options. Vous pouvez configurer le type d'authentification par défaut sur le serveur virtuel d'authentification en tant que CERT, ou créer une action de certificat qui définit ce que Citrix ADC doit faire pour authentifier les utilisateurs sur la base d'un certificat client. Dans les deux cas, votre serveur d'authentification doit prendre en charge les listes de révocation de certificats. Vous configurez ADC pour extraire le nom d'utilisateur du champ SubjectCN ou d'un autre champ spécifié dans le certificat client.

Lorsque l'utilisateur tente de se connecter à un serveur virtuel d'authentification pour lequel une stratégie d'authentification n'est pas configurée et qu'une cascade globale n'est pas configurée, les informations de nom d'utilisateur sont extraites du champ spécifié du certificat. Si le champ requis est extrait, l'authentification réussit. Si l'utilisateur ne fournit pas de certificat valide pendant la poignée de main SSL, ou si l'extraction du nom d'utilisateur échoue, l'authentification échoue. Après avoir validé le certificat client, ADC présente une page d'ouverture de session à l'utilisateur.

Les procédures suivantes supposent que vous avez déjà créé une configuration d'authentification, d'autorisation et d'audit fonctionnelle et, par conséquent, elles expliquent uniquement comment activer l'authentification à l'aide de certificats clients. Ces procédures supposent également que vous avez obtenu votre certificat racine et vos certificats client et que vous les avez placés sur ADC dans le répertoire /nsconfig/ssl.

Configurer l'authentification du certificat client

Pour configurer les paramètres de certificat client d'authentification, d'autorisation et d'audit à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué, pour configurer le certificat et vérifier la configuration :


```
add ssl certKey <certkeyName> -cert <certFile> -key <keyFile> -password
    -inform <inform> -expiryMonitor <expiryMonitor> -notificationPeriod
    <notificationPeriod>

bind ssl certKey <certkeyName> -vServer <certkeyName> -CA -crlCheck
   Mandatory

show ssl certKey [<certkeyName>]

set aaa parameter -defaultAuthType CERT

show aaa parameter

set aaa certParams -userNameField "Subject:CN"

show aaa certParams
<!--NeedCopy-->
```

Pour configurer les paramètres de certificat client d'authentification, d'autorisation et d'audit à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels.**
2. Dans le volet d'informations, sélectionnez le serveur virtuel que vous souhaitez configurer pour gérer l'authentification de certificat client, puis cliquez sur **Modifier.**
3. Dans la page **Configuration**, sous **Certificats**, cliquez sur la flèche droite (>) pour ouvrir la boîte de dialogue d'installation de la clé de certification CA.
4. Dans la boîte de dialogue **Clé Cert CA**, cliquez sur **Insérer.**
5. Dans la boîte de dialogue **CA Cert Key - Certificats SSL**, cliquez sur **Installer.**
6. Dans la boîte de dialogue **Installer le certificat**, définissez les paramètres suivants, dont les noms correspondent aux noms des paramètres CLI comme indiqué :
   - Nom de la paire de clés de certificat*—CertkeyName
   - Nom du fichier de certificat — certFile
   - Nom du fichier de clé — keyFile
   - Format du certificat — inform
   - Mot de passe — password
   - Bundle de certificats — bundle
   - Notifier à expiration — expiryMonitor
   - Période de notification — notificationPeriod
7. Cliquez sur **Installer**, puis cliquez sur **Fermer**.
8. Dans la boîte de dialogue **Clé de certification**, dans la liste **Certificat**, sélectionnez le certificat

racine.

9. Cliquez sur **Enregistrer**.
10. Cliquez sur **Précédent** pour revenir à l'écran de configuration principal.
11. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > CERT**.
12. Dans le volet d'informations, sélectionnez la stratégie que vous souhaitez configurer pour gérer l'authentification de certificat client, puis cliquez sur **Modifier**.
13. Dans la boîte de dialogue **Configurer la stratégie CERT d'authentification**, liste déroulante Serveur, sélectionnez le serveur virtuel que vous venez de configurer pour gérer l'authentification par certificat client.
14. Cliquez sur **OK**. Un message apparaît dans la barre d'état indiquant que la configuration s'est terminée correctement.

Authentification du certificat client à l'aide de

Voici les étapes pour configurer l'authentification de certificat client sur Citrix ADC à l'aide de stratégies avancées.

1. Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel que vous souhaitez configurer pour gérer l'authentification de certificat client, puis cliquez sur **Modifier**.

   > **Remarque :**
   >
   > Si vous avez importé un certificat d'autorité de certification valide et un certificat de serveur pour le serveur virtuel, vous pouvez passer les **étapes 3 à 10**.

3. Dans la page **Configuration**, sous **Certificats**, cliquez sur **>** pour ouvrir la boîte de dialogue d'installation de la **clé de certification CA**.
4. Dans la boîte de dialogue **Clé de certification CA**, cliquez sur **Insérer**.
5. Dans la boîte de dialogue **Clé de certification CA - Certificats SSL**, cliquez sur **Installer**.
6. Dans la boîte de dialogue **Installer le certificat**, définissez les paramètres suivants, dont les noms correspondent aux noms des paramètres CLI comme indiqué :

   - Nom de la paire de clé-certificat — certkeyName
   - Nom du fichier de certificat — certFile
   - Nom du fichier de clé — keyFile
   - Format du certificat — inform
   - Mot de passe — password
   - Bundle de certificats — bundle
   - Notifier à expiration — expiryMonitor
   - Période de notification — notificationPeriod

7. Cliquez sur **Installer**, puis sur Fermer.
8. Dans la boîte de dialogue **Clé de certification**, sélectionnez le certificat racine dans la liste Certificat.
9. Cliquez sur **Enregistrer**.
10. Cliquez sur **Précédent** pour revenir à l'écran de configuration principal.
11. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées**, puis sélectionnez **Stratégie**.
12. Dans le volet d'informations, effectuez l'une des opérations suivantes :
    - Pour créer une stratégie, cliquez sur **Ajouter**.
    - Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Modifier**.
13. Dans la boîte de dialogue **Créer une stratégie d'authentification** ou **Configurer une stratégie d'authentification**, tapez ou sélectionnez des valeurs pour les paramètres.
    - Nom : nom de la stratégie. Impossible de modifier une stratégie précédemment configurée.
    - Type d'action - Sélectionner un certificat
    - Action : action d'authentification (profil) à associer à la stratégie. Vous pouvez choisir une action d'authentification existante ou cliquer sur le bouton plus et créer une action du type approprié.
    - Action de journalisation : action d'audit à associer à la stratégie. Vous pouvez choisir une action d'audit existante ou cliquer sur le bouton « Plus » et créer une nouvelle action.
    - Expression : règle qui sélectionne les connexions auxquelles vous souhaitez appliquer l'action que vous avez spécifiée. La règle peut être simple (« true » sélectionne tout le trafic) ou complexe. Vous entrez des expressions en choisissant d'abord le type d'expression dans la liste déroulante la plus à gauche sous la fenêtre Expression, puis en tapant votre expression directement dans la zone de texte de l'expression, ou en cliquant sur Ajouter pour ouvrir la boîte de dialogue Ajouter une expression et en utilisant les listes déroulantes qu'elle contient pour construire votre expression.)
    - Commentaire - Vous pouvez taper un commentaire décrivant le type de trafic auquel cette stratégie d'authentification s'appliquera. Facultatif.
14. Cliquez sur **Créer** ou **OK**, puis cliquez sur **Fermer**. Si vous avez créé une stratégie, cette stratégie apparaît dans la page Stratégies d'authentification et serveurs.

Pass-through du certificat client

Citrix ADC peut désormais être configuré pour transmettre des certificats client à des applications protégées qui nécessitent des certificats client pour l'authentification utilisateur. ADC authentifie d'abord

l'utilisateur, puis insère le certificat client dans la demande et l'envoie à l'application. Cette fonctionnalité est configurée en ajoutant des stratégies SSL appropriées.

Le comportement exact de cette fonctionnalité lorsqu'un utilisateur présente un certificat client dépend de la configuration du serveur virtuel VPN.

- Si le serveur virtuel VPN est configuré pour accepter les certificats clients mais ne les requiert pas, ADC insère le certificat dans la demande, puis transmet la demande à l'application protégée.
- Si l'authentification de certificat client est désactivée sur le serveur virtuel VPN, ADC renégocie le protocole d'authentification et réauthentifie l'utilisateur avant d'insérer le certificat client dans l'en-tête et de transfère la demande à l'application protégée.
- Si le serveur virtuel VPN est configuré pour exiger l'authentification du certificat client, ADC utilise le certificat client pour authentifier l'utilisateur, puis insère le certificat dans l'en-tête et transmet la demande à l'application protégée.

Dans tous ces cas, vous configurez la transmission de certificat client comme suit.

Créer et configurer le transfert de certificat client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
1 add vpn vserver <name> SSL <IP> 443
2 <!--NeedCopy-->
```

Pour *name*, remplacez un nom pour le serveur virtuel. Le nom doit contenir entre un et 127 caractères ASCII, commençant par une lettre ou un trait de soulignement (_), et ne contenant que des lettres, des chiffres et le trait de soulignement, hachage (#), point (.), espace, deux-points (:), à (@), égal à (=) et tiret (-). Pour <IP>, remplacez l'adresse IP attribuée au serveur virtuel.

```
1 set ssl vserver <name> -clientAuth ENABLED -clientCert <clientcert>
2 <!--NeedCopy-->
```

Pour <name>, remplacez le nom du serveur virtuel que vous venez de créer. Pour <clientCert>, remplacez l'une des valeurs suivantes :

- désactivé : désactive l'authentification de certificat client sur le serveur virtuel VPN.
- mandatory : configure le serveur virtuel VPN pour exiger l'authentification des certificats client.
- option : configure le serveur virtuel VPN pour autoriser l'authentification de certificat client, mais ne l'exige pas.

```
1 bind vpn vserver <name> -policy local
2 <!--NeedCopy-->
```

Pour <name>, remplacez le nom du serveur virtuel VPN que vous avez créé.


```
bind vpn vserver <name> -policy cert
<!--NeedCopy-->
```

Pour <name>, remplacez le nom du serveur virtuel VPN que vous avez créé.

```
bind ssl vserver <name> -certkeyName <certkeyname>
<!--NeedCopy-->
```

Pour <name>, remplacez le nom du serveur virtuel que vous avez créé. Pour <certkeyName>, remplacez la clé de certificat client.

```
bind ssl vserver <name> -certkeyName <cacertkeyname> -CA -ocspCheck
   Optional
<!--NeedCopy-->
```

Pour <name>, remplacez le nom du serveur virtuel que vous avez créé. Pour <cacertkeyName>, remplacez la clé de certificat de l'autorité de certification.

```
add ssl action <actname> -clientCert ENABLED -certHeader CLIENT-CERT
<!--NeedCopy-->
```

Pour <actname>, remplacez un nom à l'action SSL.

```
add ssl policy <polname> -rule true -action <actname>
<!--NeedCopy-->
```

Pour <polname>, remplacez un nom à votre nouvelle stratégie SSL. Pour <actname>, remplacez le nom de l'action SSL que vous venez de créer.

```
bind ssl vserver <name> -policyName <polname> -priority 10
<!--NeedCopy-->
```

Pour <name>, remplacez le nom du serveur virtuel VPN.

Exemple

```
add vpn vserver vs-certpassthru SSL 10.121.250.75 443
set ssl vserver vs-certpassthru -clientAuth ENABLED -clientCert
   optional
bind vpn vserver vs-certpassthru -policy local
bind vpn vserver vs-certpassthru -policy cert
bind ssl vserver vs-certpassthru -certkeyName mycertKey
bind ssl vserver vs-certpassthru -certkeyName mycertKey -CA -ocspCheck
   Optional
```



```
add ssl action act-certpassthru -clientCert ENABLED -certHeader CLIENT-
    CERT
add ssl policy pol-certpassthru -rule true -action act-certpassthru
bind ssl vserver vs-certpassthru -policyName pol-certpassthru -priority
     10
<!--NeedCopy-->
```

Négociation d'authentification

February 12, 2021

Comme pour les autres types de stratégies d'authentification, une stratégie d'authentification Négocier est composée d'une expression et d'une action. Après avoir créé une stratégie d'authentification, vous la liez à un serveur virtuel d'authentification et lui attribuez une priorité. Lorsque vous la liez, vous la définissez également comme stratégie principale ou secondaire.

Outre les fonctions d'authentification standard, la commande Négocier l'action peut désormais extraire les informations utilisateur d'un fichier keytab au lieu de vous obliger à entrer ces informations manuellement. Si un keytab comporte plusieurs SPN, l'authentification, l'autorisation et l'audit sélectionne le SPN correct. Vous pouvez configurer cette fonctionnalité à partir de la ligne de commande ou à l'aide de l'utilitaire de configuration.

> **Remarque**
>
> Ces instructions supposent que vous connaissez déjà le protocole LDAP et que vous avez déjà configuré le serveur d'authentification LDAP choisi.

Pour configurer l'authentification, l'autorisation et l'audit afin d'extraire les informations utilisateur d'un fichier keytab à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande appropriée :

```
add authentication negotiateAction <name> {
 -domain <string> }
  {
 -domainUser <string> }
  {
 -domainUserPasswd  }
  [-defaultAuthenticationGroup <string>] [-keytab <string>] [-NTLMPath
     <string>]

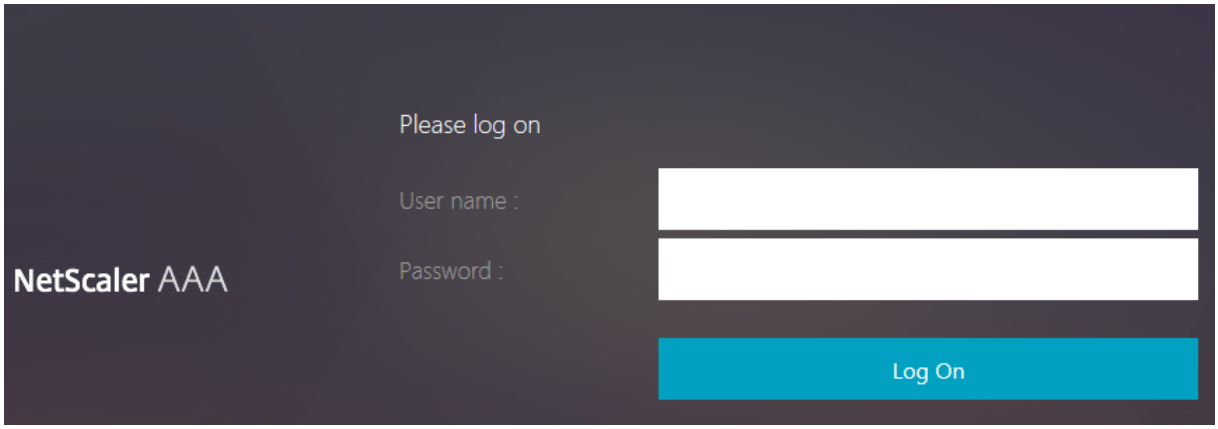
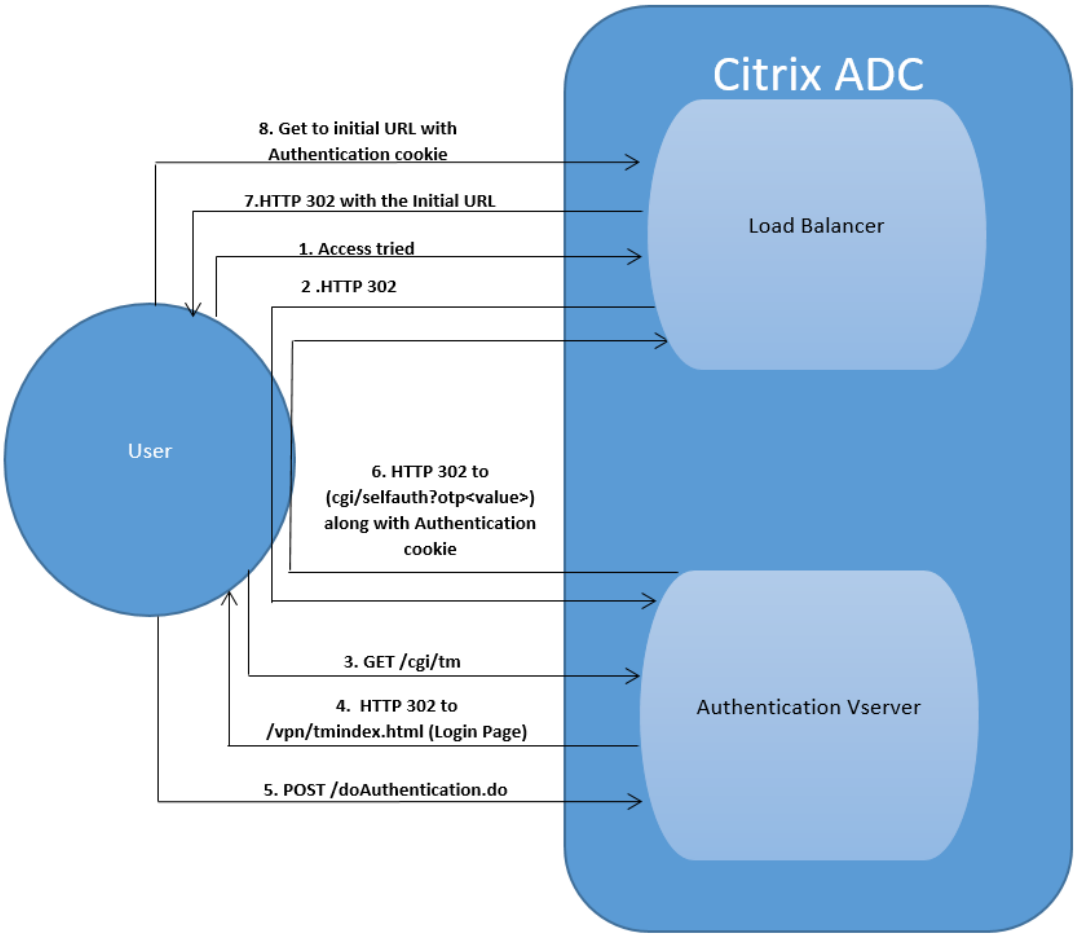
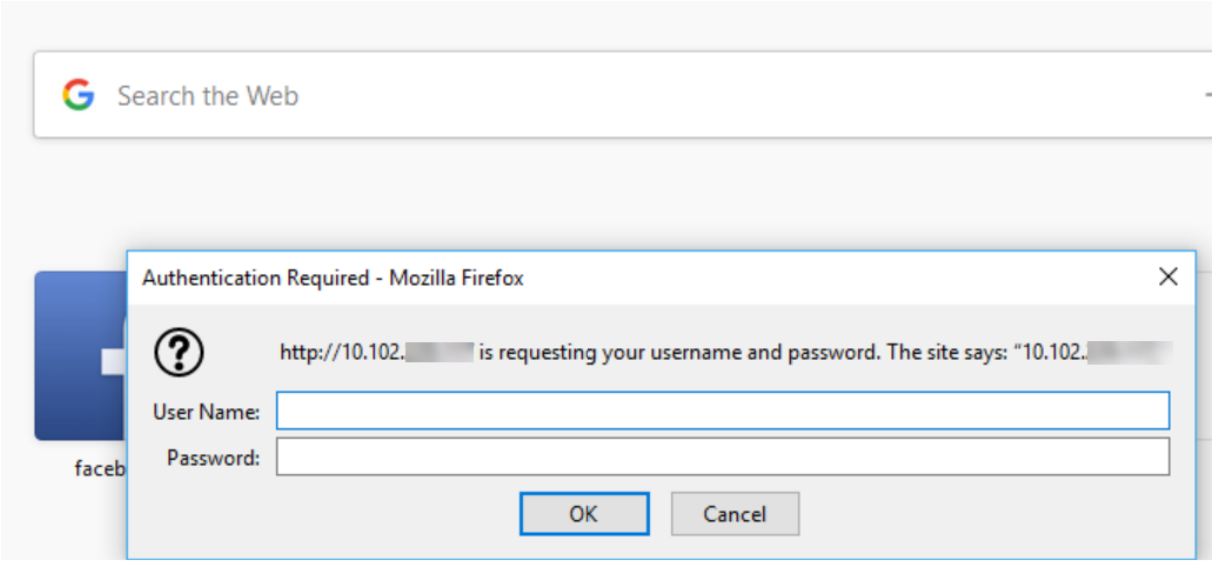
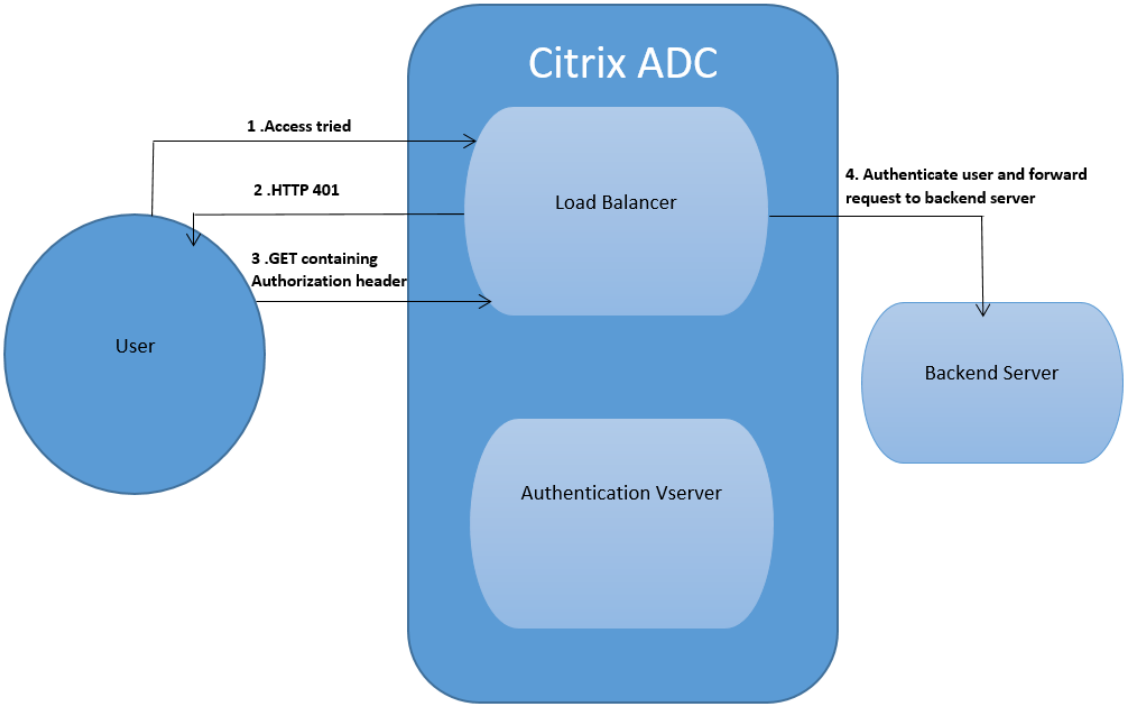
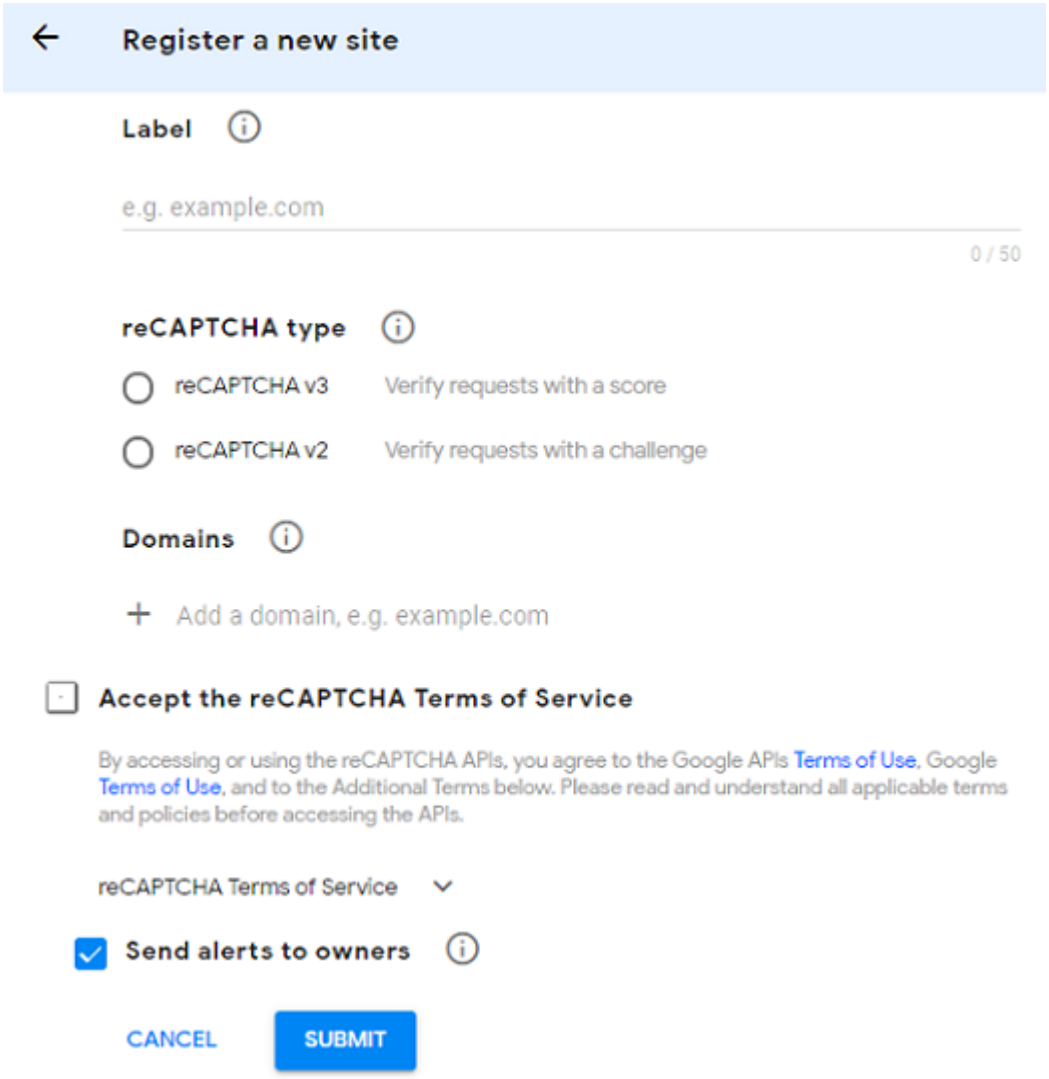
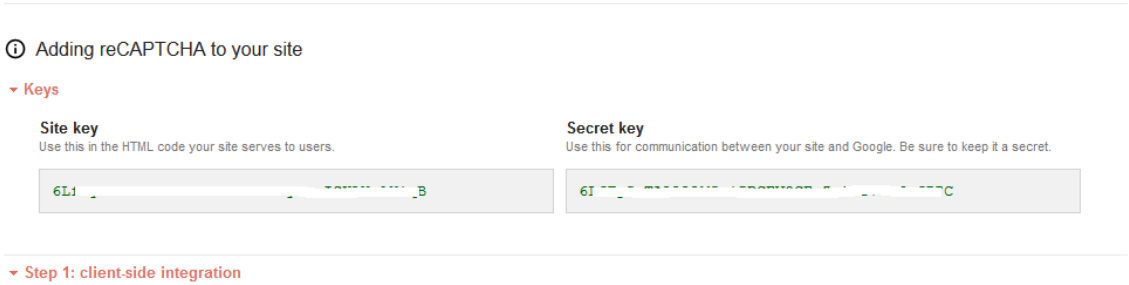
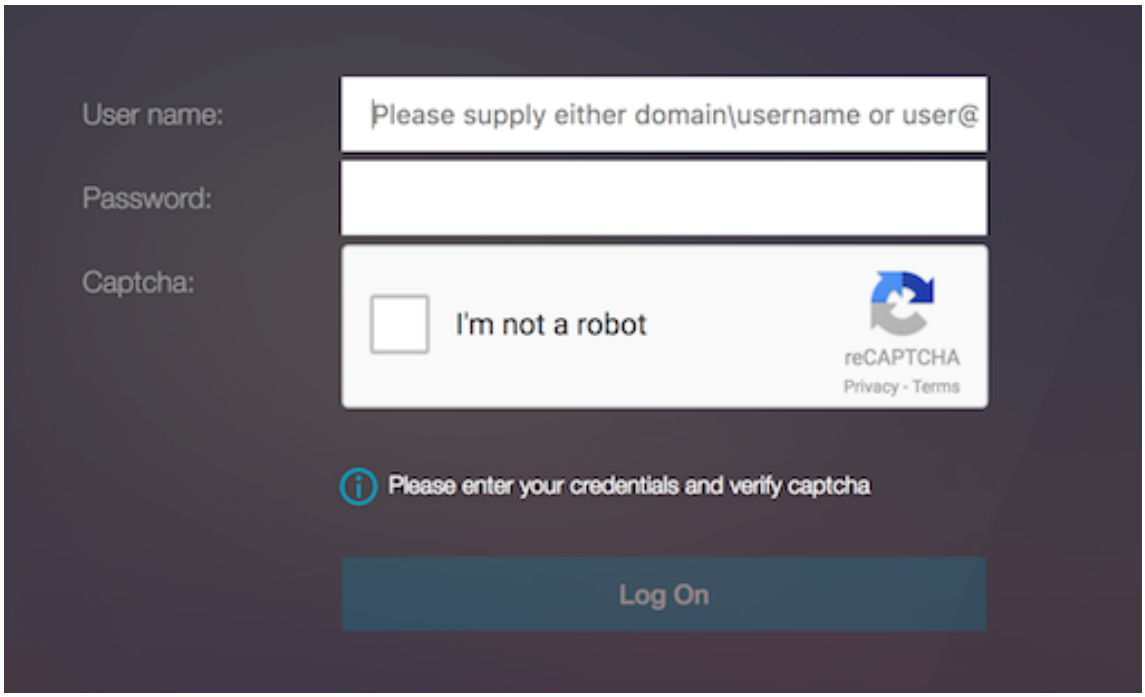
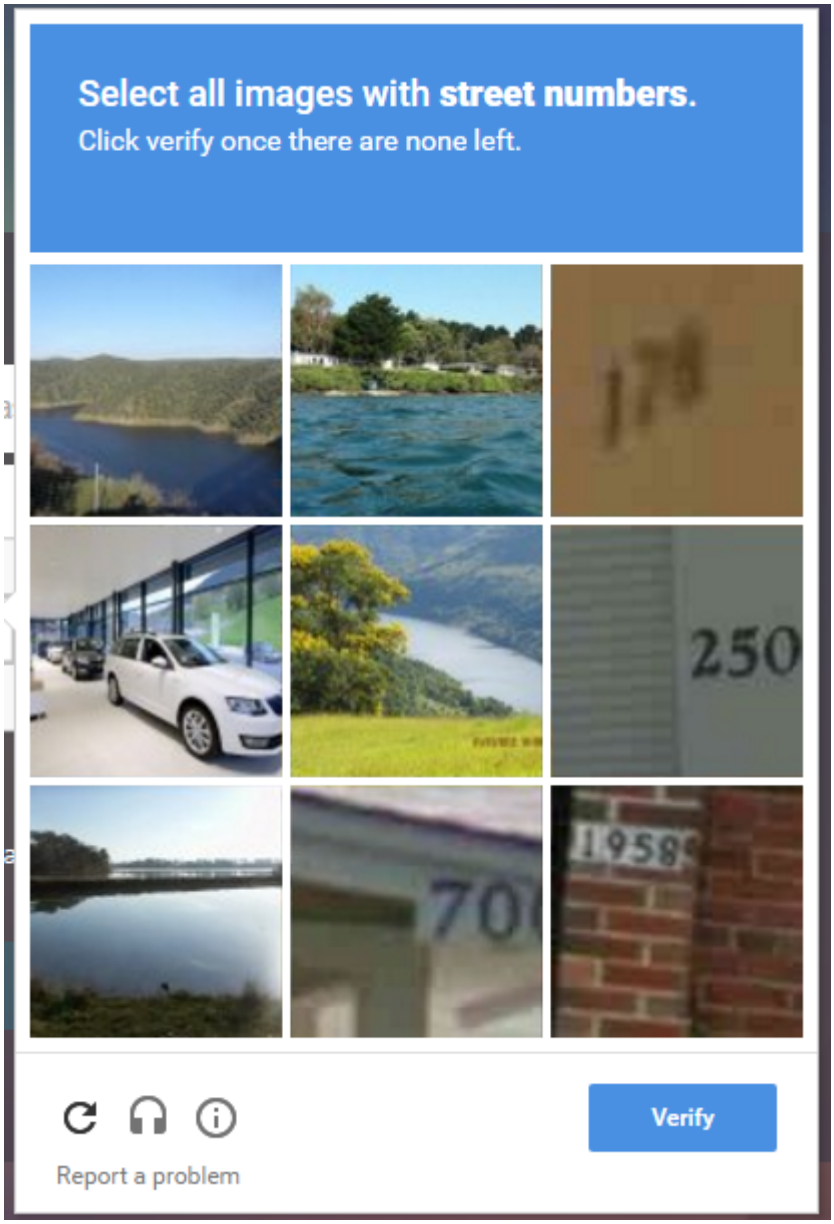
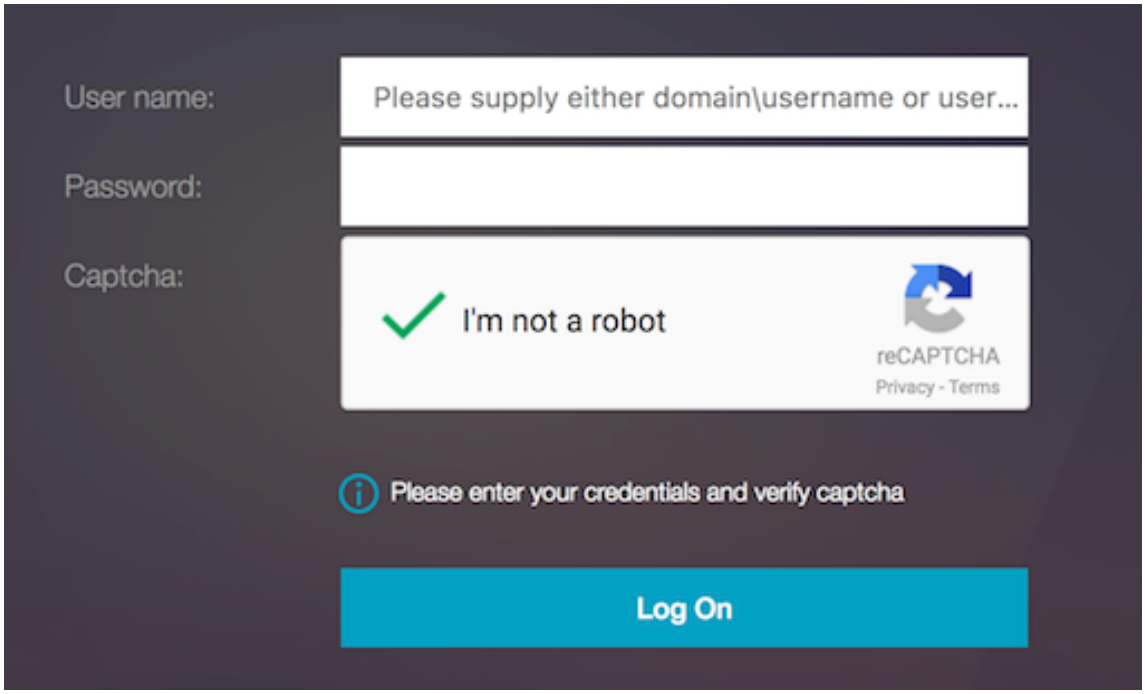
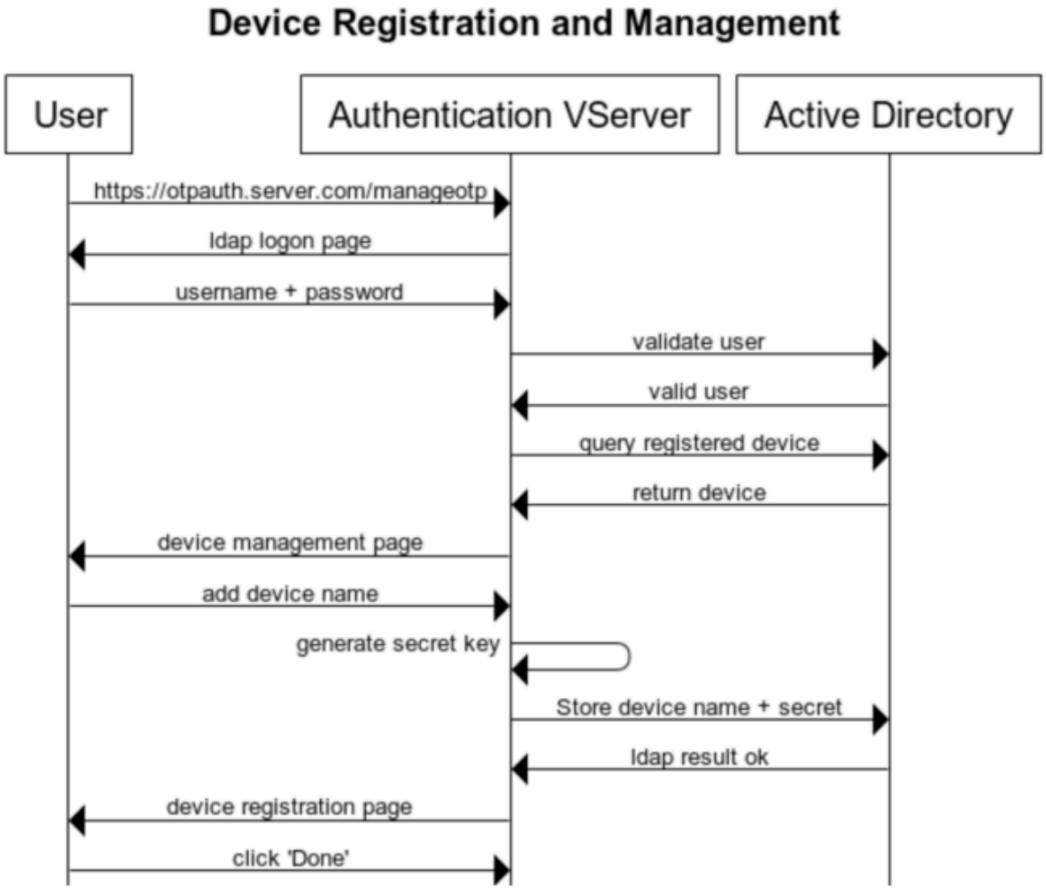
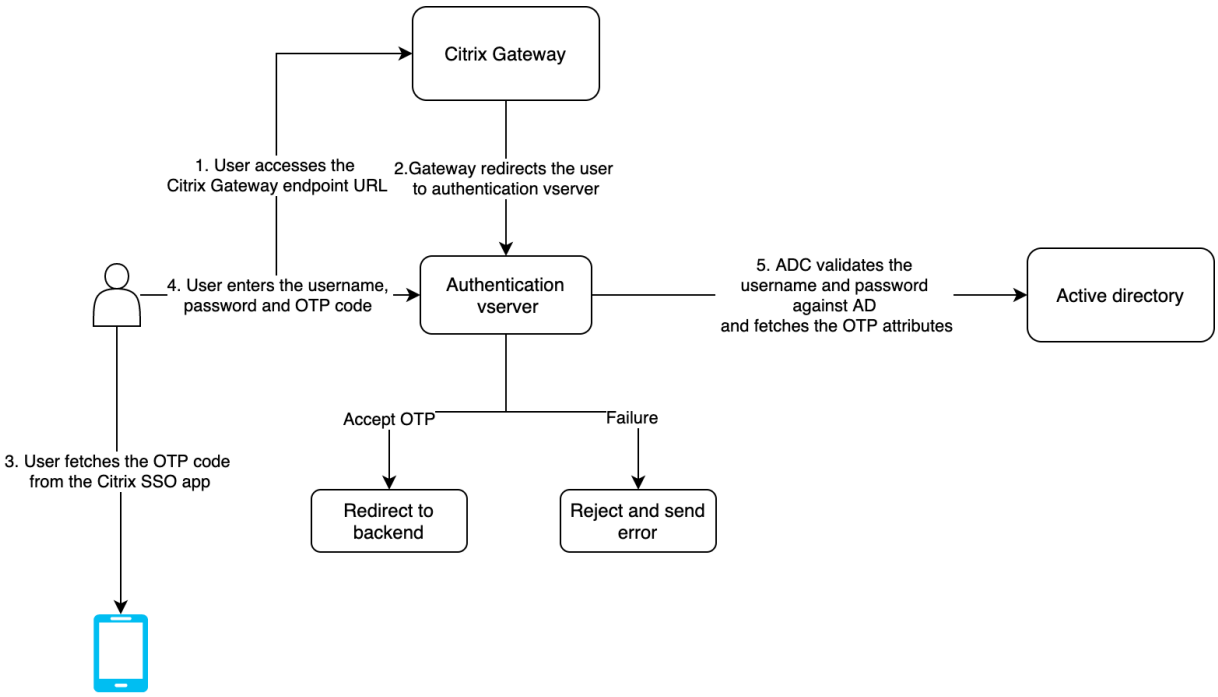
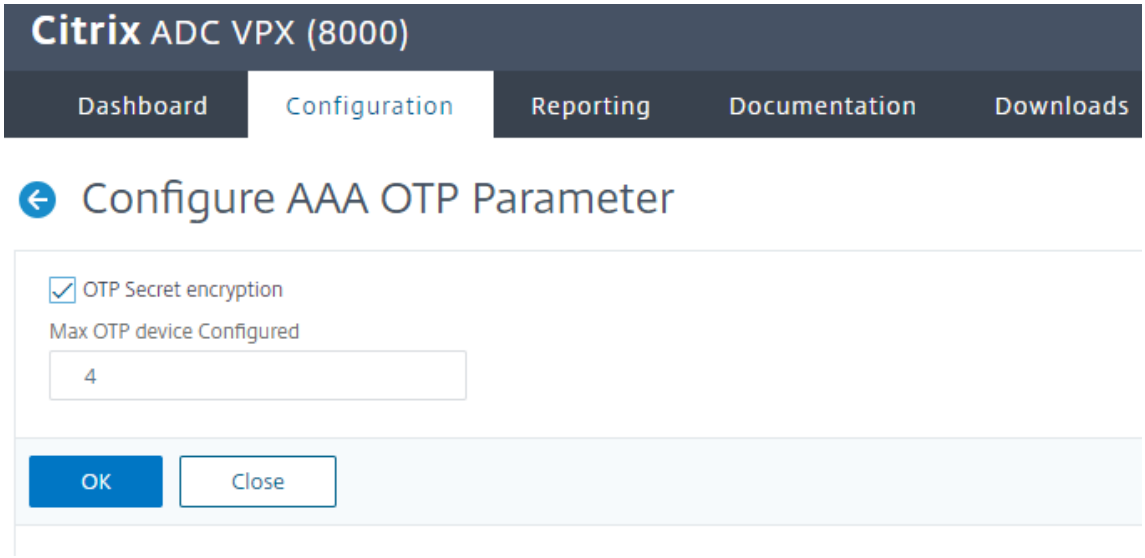
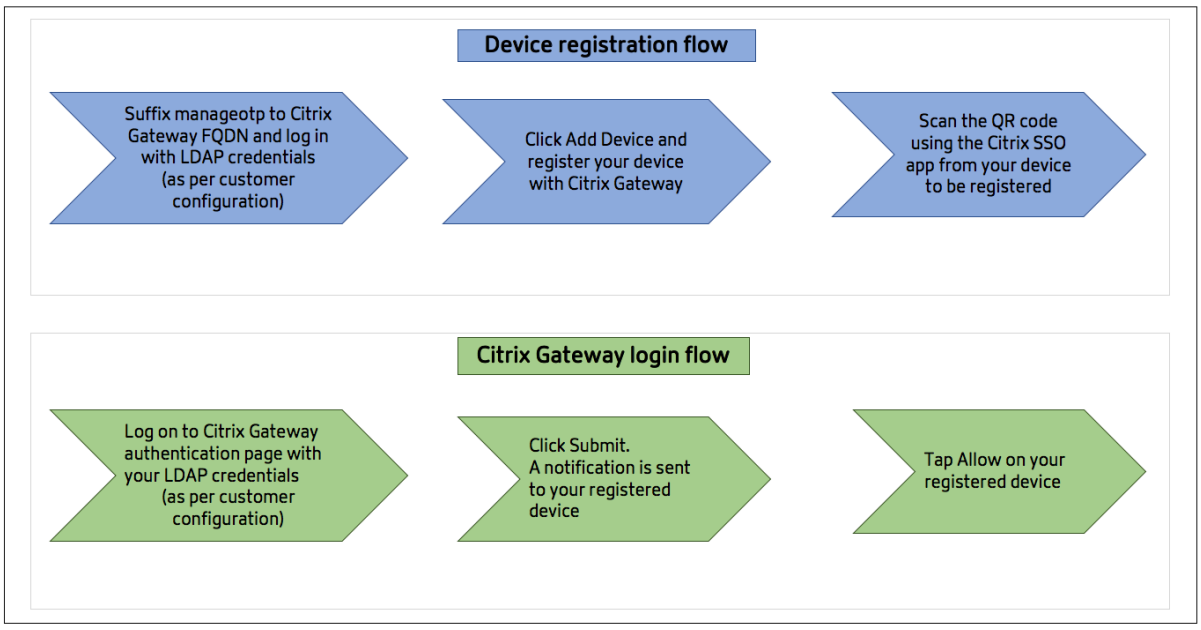
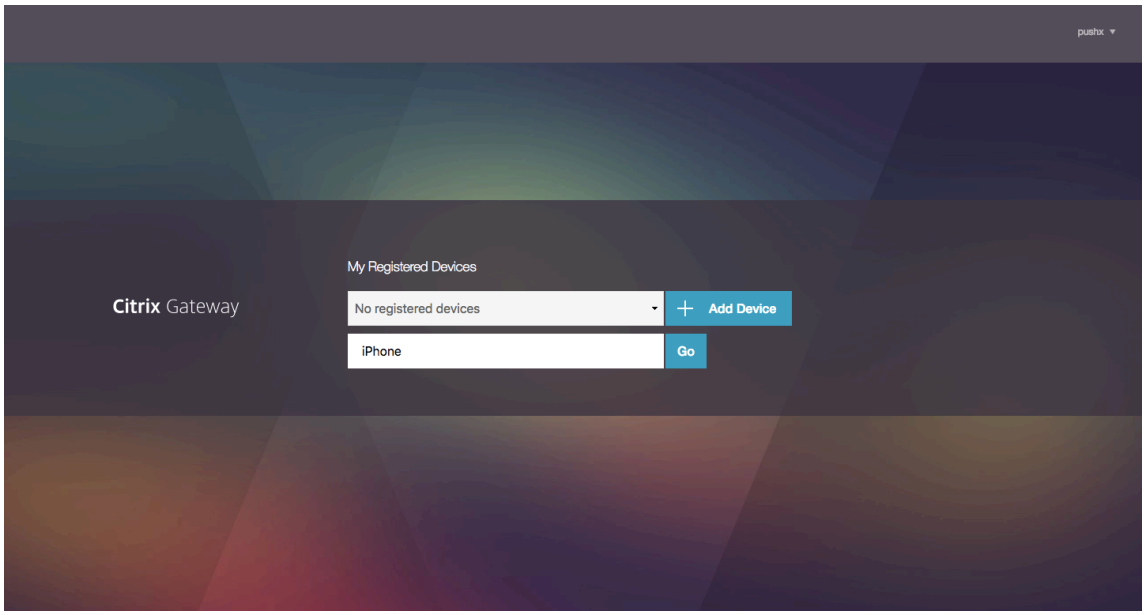
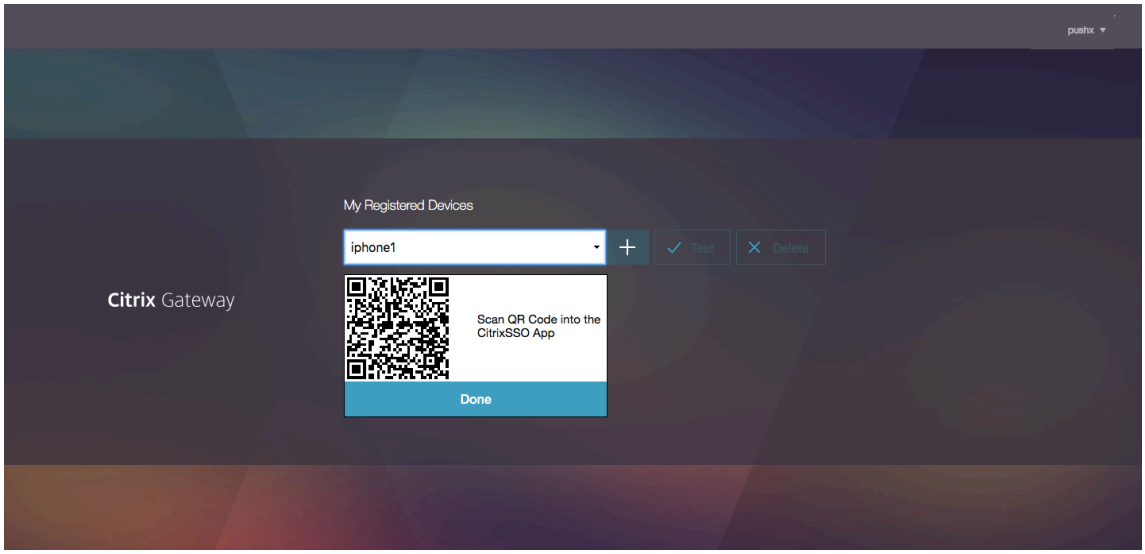
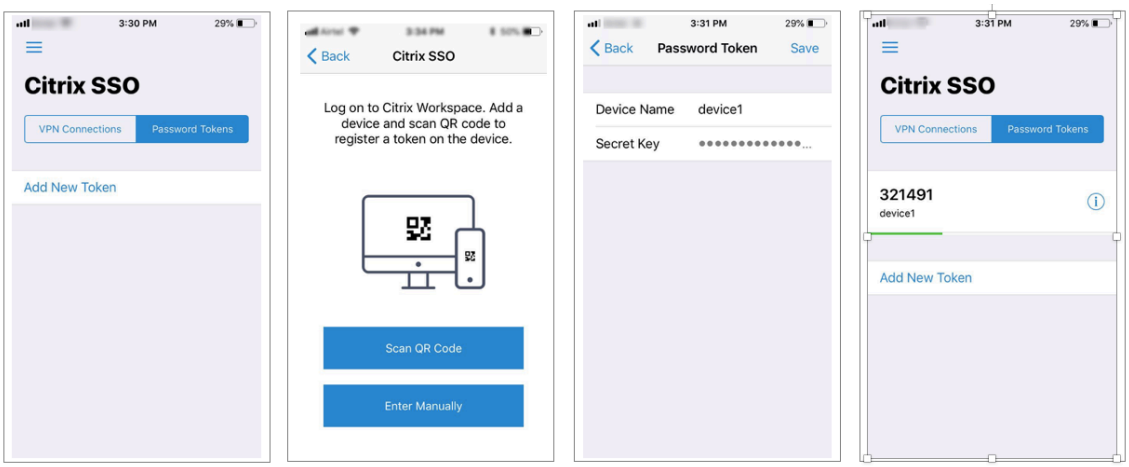
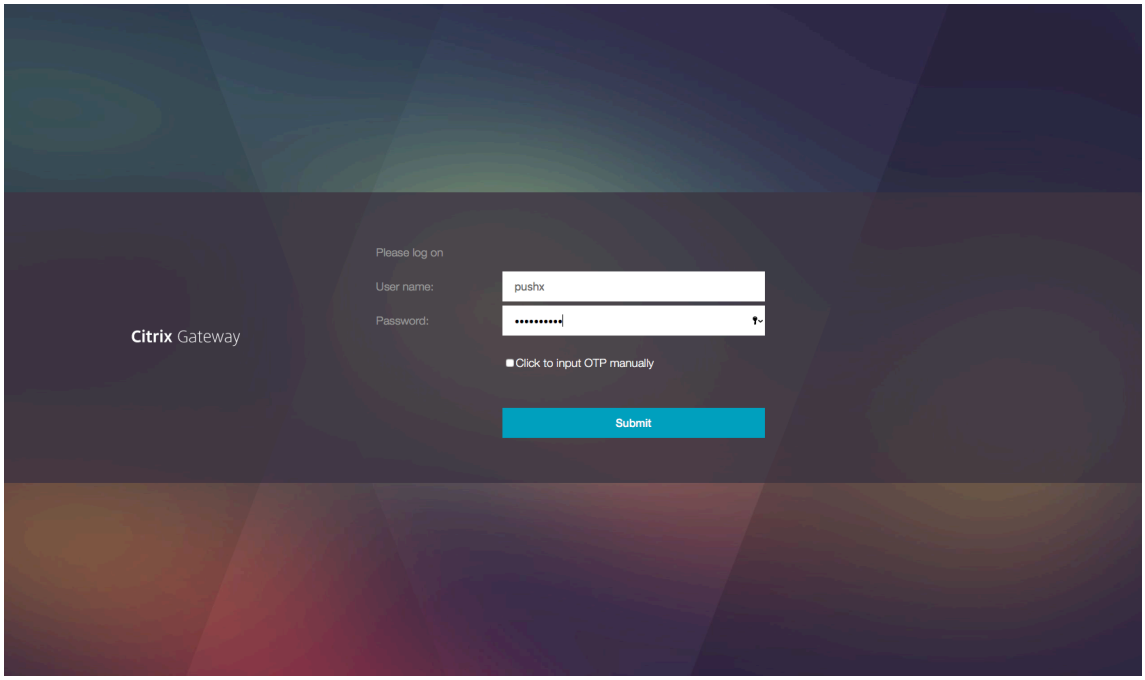
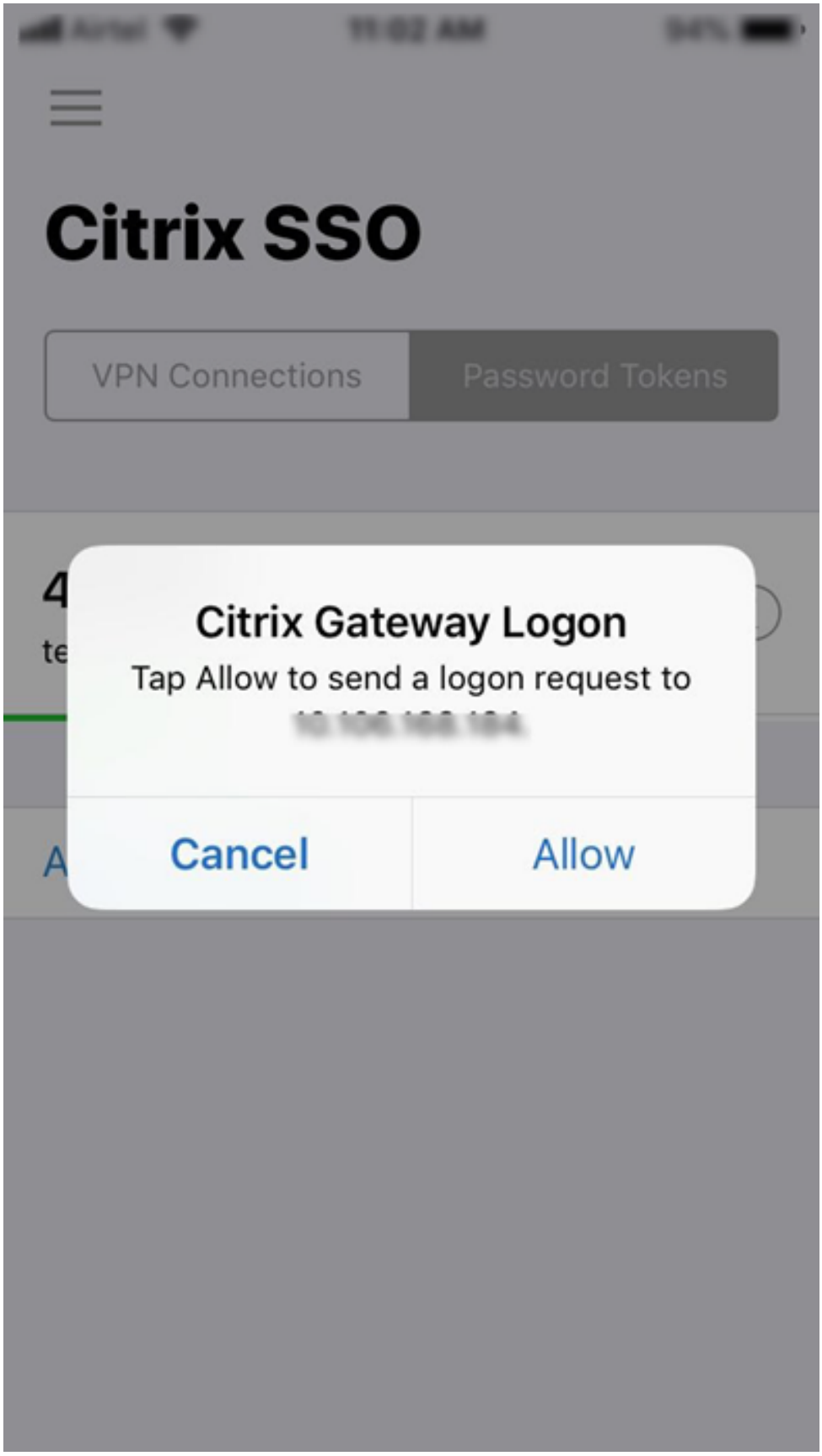
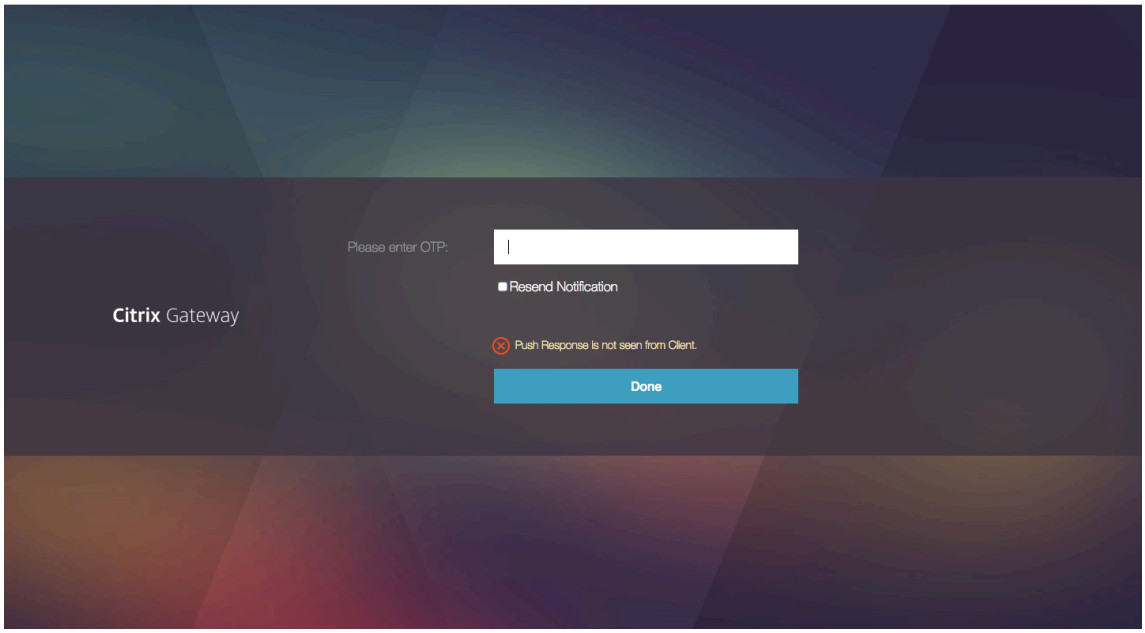
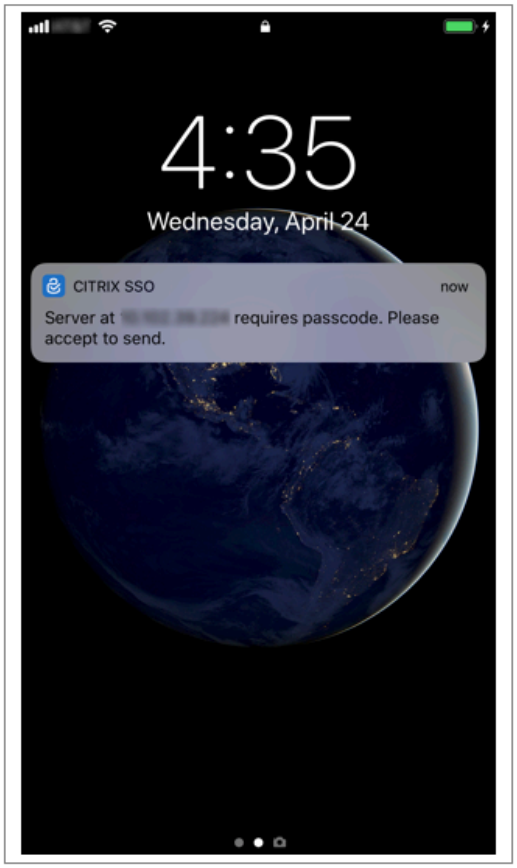
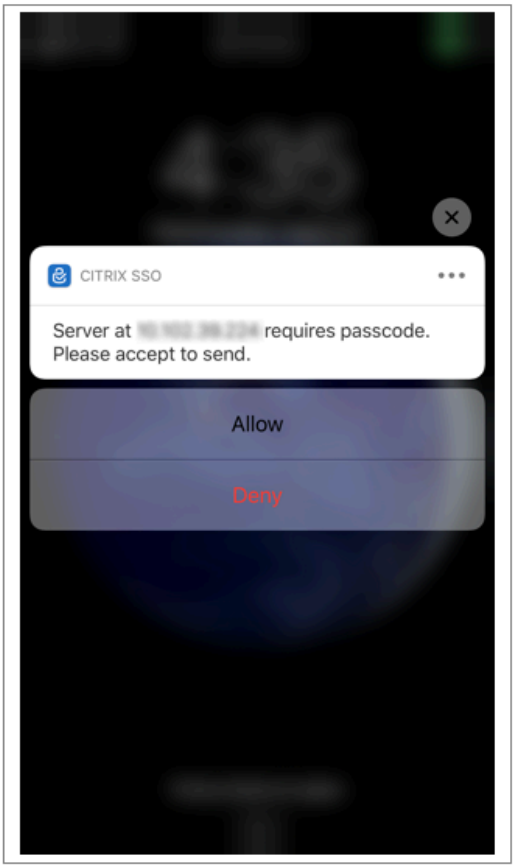
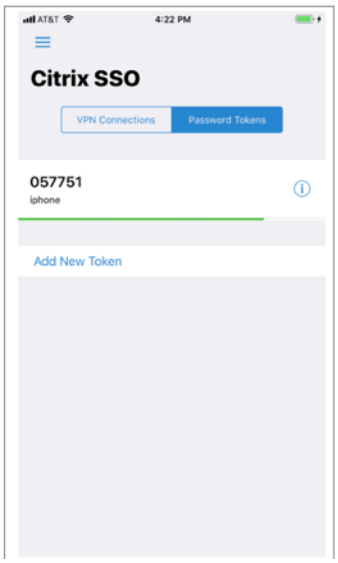
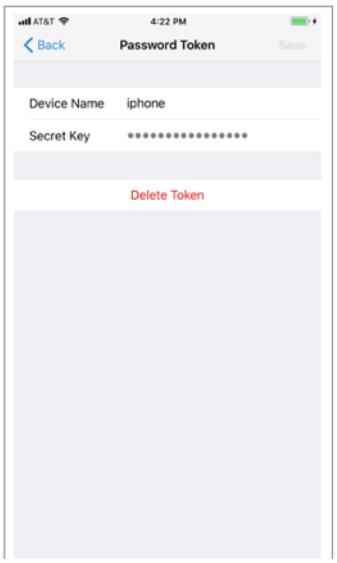
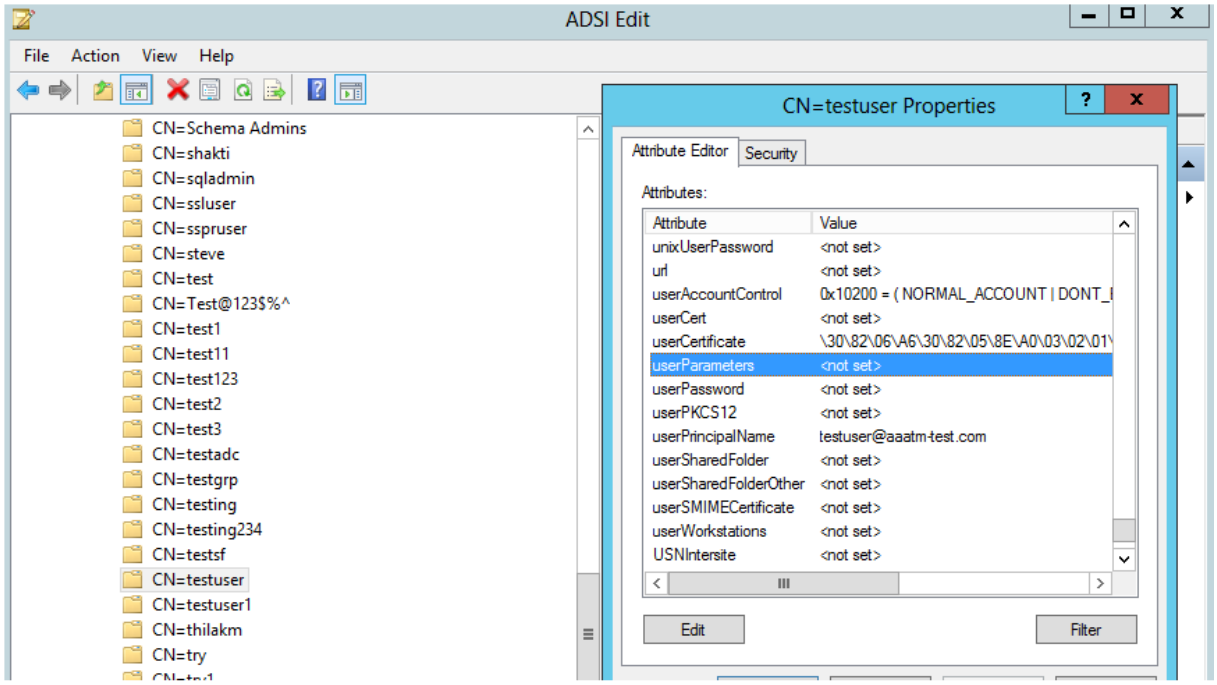
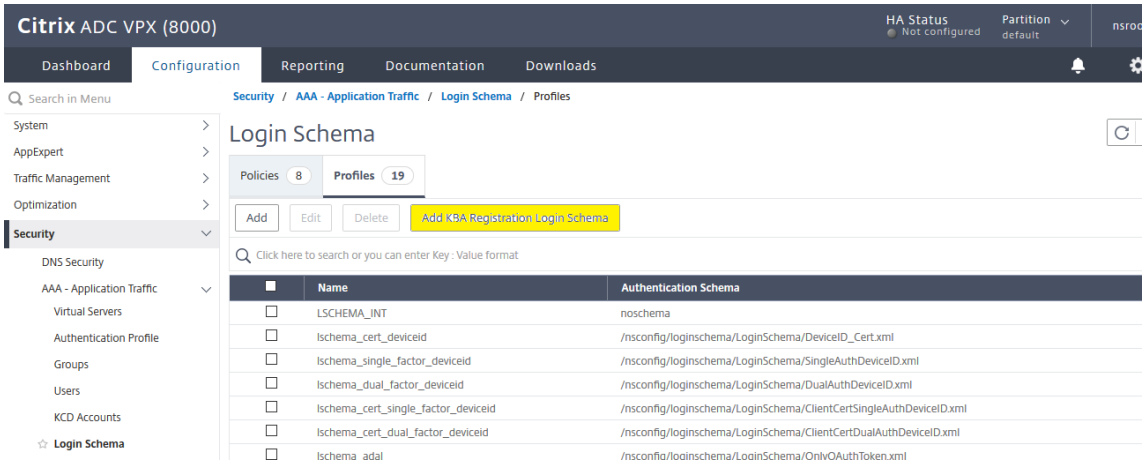
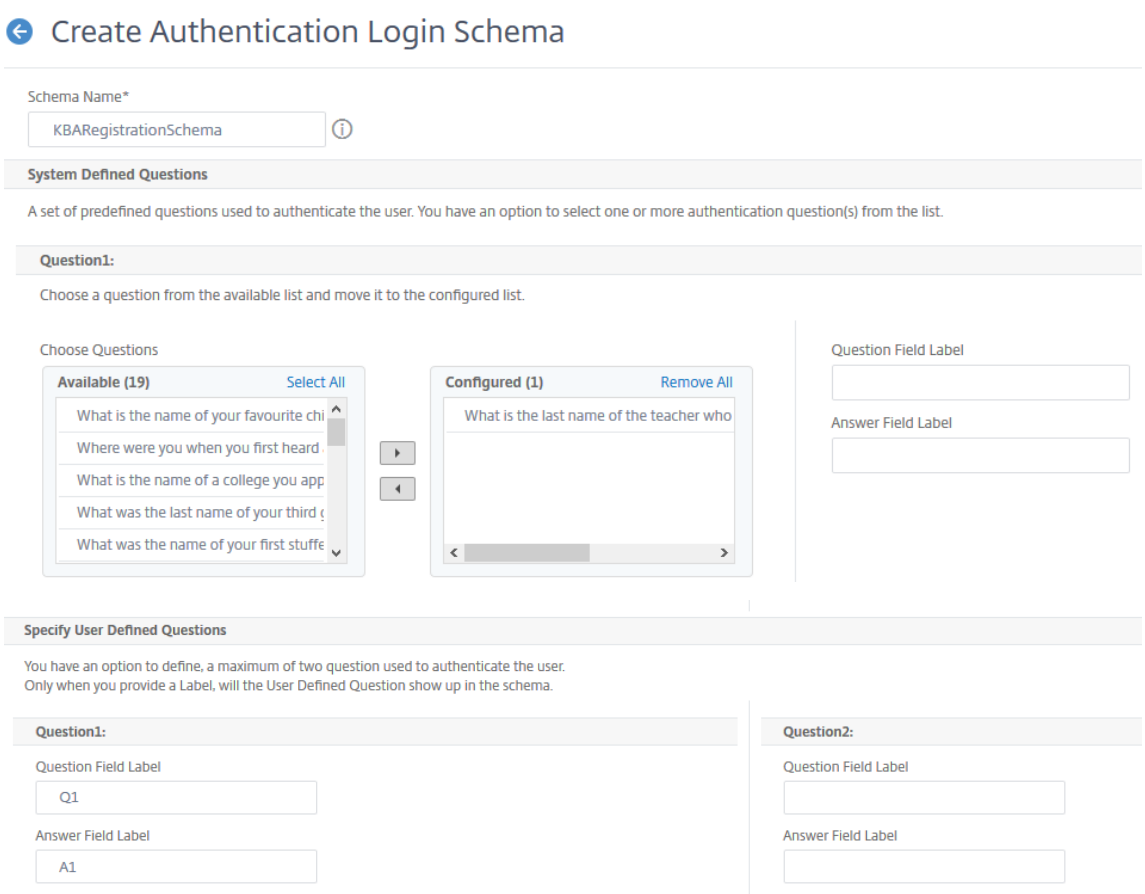
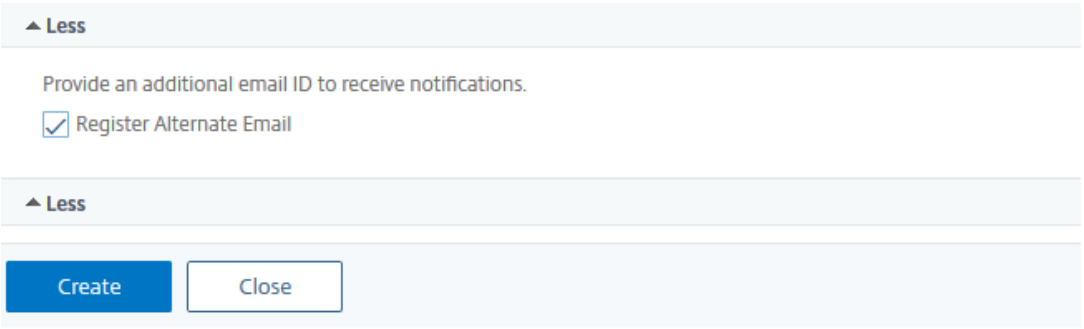
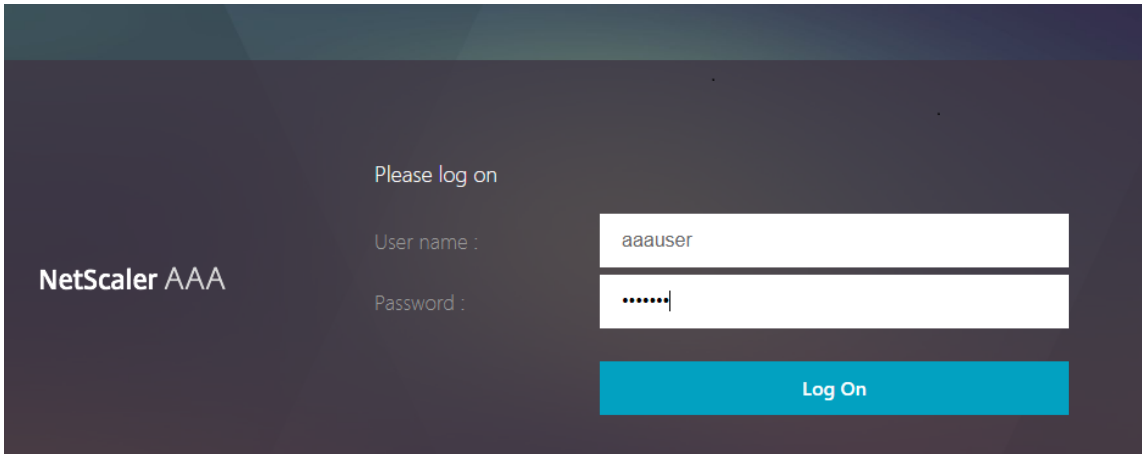
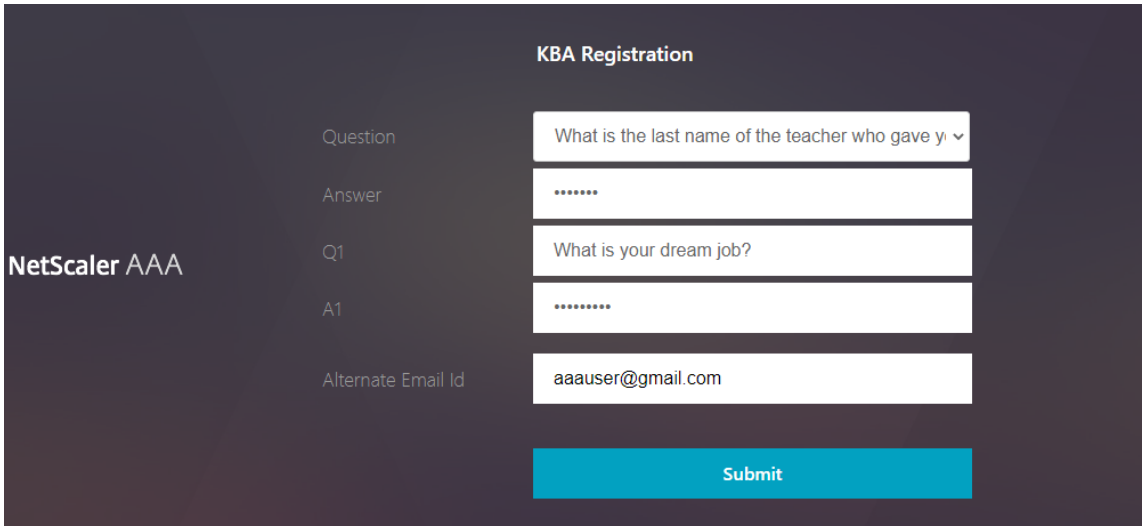
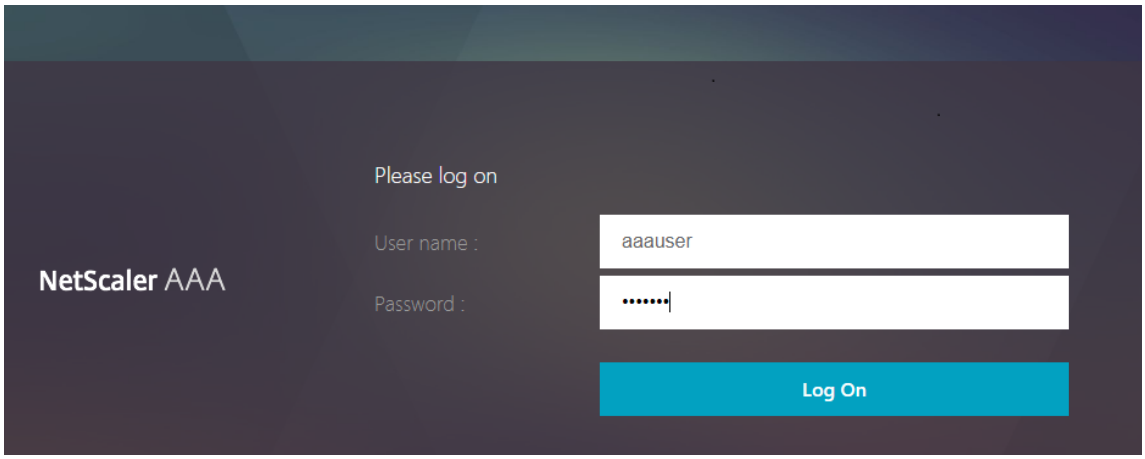
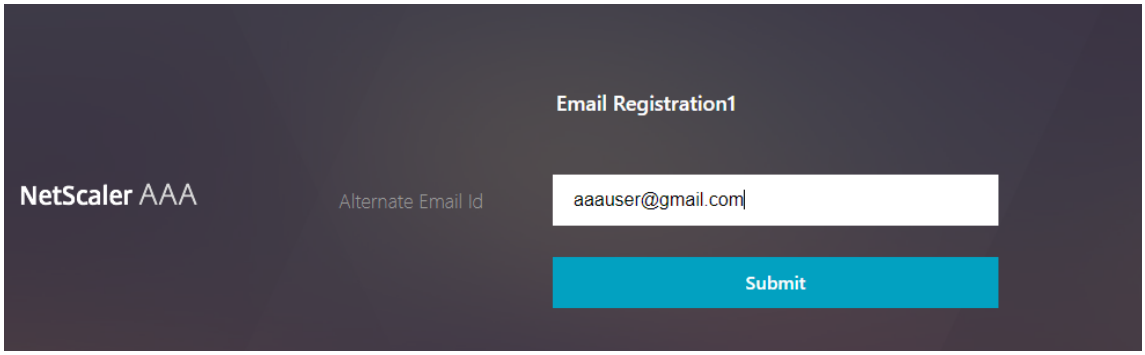
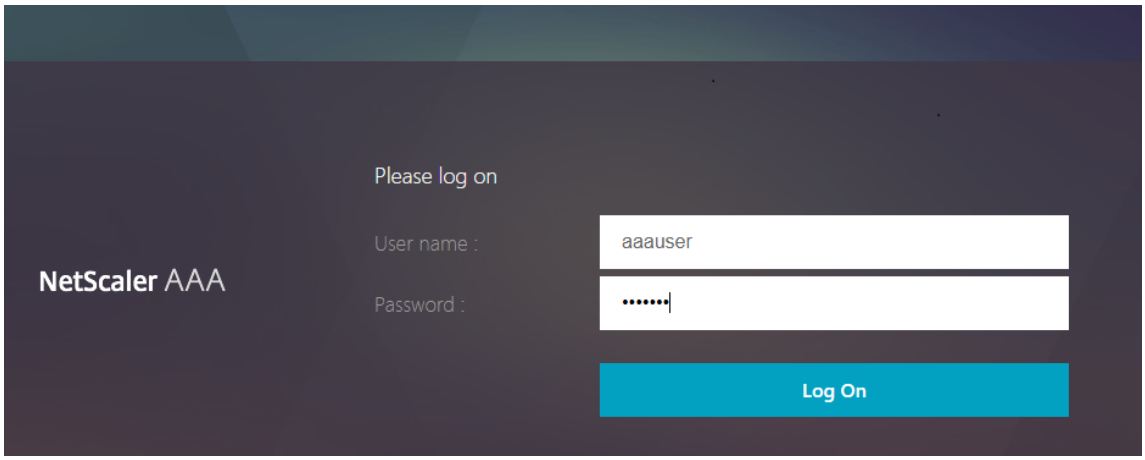
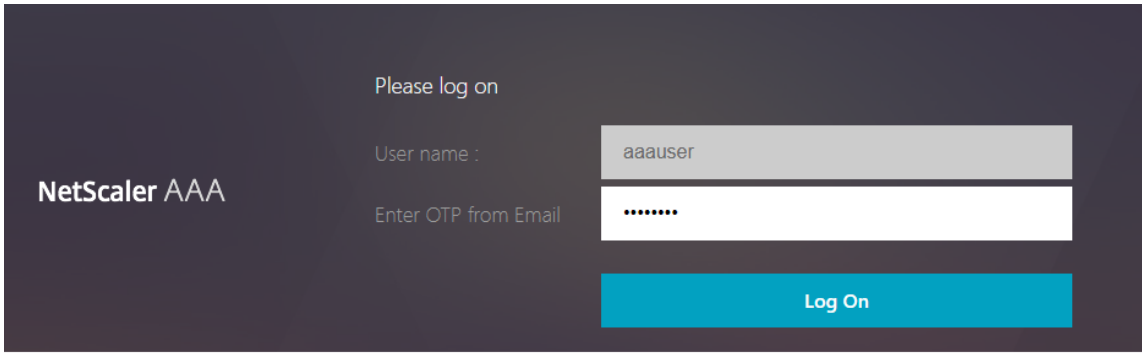
```



```
set authentication negotiateAction <name> {
 -domain <string> }
  {
 -domainUser <string> }
  {
 -domainUserPasswd }
  [-defaultAuthenticationGroup <string>] [-keytab <string>] [-NTLMPath
     <string>]
<!--NeedCopy-->
```

Parameter description

- **name** - Nom de l'action de négociation à utiliser.
- **domain** - Nom de domaine du principal de service qui représente Citrix ADC.
- **DomainUser** - Nom d'utilisateur du compte qui est mappé avec Citrix ADC principal. Cela peut être donné avec le domaine et le mot de passe lorsque le fichier keytab n'est pas disponible. Si le nom d'utilisateur est donné avec le fichier keytab, alors ce fichier keytab sera recherché pour les informations d'identification de cet utilisateur. Longueur maximale : 127
- **DomainUserPasswd** - Mot de passe du compte qui est mappé au principal Citrix ADC.
- **DefaultAuthenticationGroup** - Il s'agit du groupe par défaut qui est choisi lorsque l'authentification réussit en plus des groupes extraits. Longueur maximale : 63
- **keytab** - Chemin d'accès au fichier keytab utilisé pour déchiffrer les tickets kerberos présentés à Citrix ADC. Si keytab n'est pas disponible, le domaine/nom d'utilisateur/mot de passe peut être spécifié dans la configuration de l'action de négociation. Longueur maximale : 127
- **NTLMPath** - Chemin d'accès au site activé pour l'authentification NTLM, y compris le nom de domaine complet du serveur. Ceci est utilisé lorsque les clients reviennent à NTLM. Longueur maximale : 127

Pour configurer l'authentification, l'autorisation et l'audit afin d'extraire les informations utilisateur d'un fichier keytab à l'aide de l'utilitaire de configuration

> Remarque
>
> Dans l'utilitaire de configuration, le terme serveur est utilisé à la place de l'action, mais fait référence à la même tâche.

1. Accédez à **Sécurité > AAA - Trafic des applications > Authentification > Stratégies avancées > Actions > NEGOCIATE Actions**.
2. Dans le volet d'informations, sous l'onglet **Serveurs**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez créer une action **Négocier**, cliquez sur **Ajouter**.

- Si vous souhaitez modifier une action **Négocier** existante, sélectionnez l'action dans le volet de données, puis cliquez sur **Modifier** .

3. Si vous créez une action **Négocier**, dans la zone de texte **Nom**, tapez un nom pour votre nouvelle action. Le nom peut comporter entre un et 127 caractères et peut être composé de majuscules et minuscules, de chiffres et de tiret (-) et de trait de soulignement (_). Si vous modifiez une action Négocier existante, ignorez cette étape. Le nom est en lecture seule ; vous ne pouvez pas le modifier.
4. Sous **Négocier**, si la case Utiliser le fichier Keytab n'est pas déjà cochée, cochez-la.
5. Dans la zone de texte Chemin d'accès au fichier Keytab, tapez le chemin d'accès complet et le nom de fichier du keytab que vous souhaitez utiliser.
6. Dans la zone de texte Groupe d'authentification par défaut, tapez le groupe d'authentification que vous souhaitez définir par défaut pour cet utilisateur.
7. Cliquez sur **Créer** ou sur **OK** pour enregistrer vos modifications.

Points à noter lorsque les chiffrements avancés sont utilisés pour l'authentification Kerberos

> - **Exemple de configuration lorsque keytab est utilisé :** add authentication negotiateAction neg_act_aes256 -keytab "/nsconfig/krb/lbvs_aes256.keytab"
> - **Utilisez la commande suivante lorsque keytab a plusieurs types de chiffrement.** La commande capture en outre les paramètres utilisateur du domaine : add authentication negotiateAction neg_act_keytab_all -keytab "/nsconfig/krb/lbvs_all.keytab" -domainUser "HTTP/lbvs.aaa.local"
> - **Utilisez les commandes suivantes lorsque les informations d'identification de l'utilisateur sont utilisées :** add authentication negotiateAction neg_act_user -domain AAA.LOCAL -domainUser "HTTP/lbvs.aaa.local" -domainUserPasswd <password>
> - Assurez-vous que les informations **DomainUser** correctes sont fournies. Vous pouvez rechercher le nom d'ouverture de session de l'utilisateur dans AD.

L'authentification Web

October 5, 2021

L'authentification, l'autorisation et l'audit permettent désormais d'authentifier un utilisateur auprès d'un serveur Web, en fournissant les informations d'identification requises par le serveur Web dans une requête HTTP et en analysant la réponse du serveur Web pour déterminer si l'authentification de l'utilisateur a réussi. Comme pour les autres types de stratégies d'authentification, une stratégie

d'authentification Web est composée d'une expression et d'une action. Après avoir créé une stratégie d'authentification, vous la liez à un serveur virtuel d'authentification et vous lui attribuez une priorité. Lorsque vous la liez, vous la désignez également en tant que stratégie principale ou secondaire.

Pour configurer l'authentification Web avec un serveur Web spécifique, vous devez d'abord créer une action d'authentification Web. Étant donné que l'authentification sur les serveurs Web n'utilise pas de format rigide, vous devez spécifier exactement quelles informations le serveur Web a besoin et dans quel format lors de la création de l'action. Pour ce faire, vous créez une expression dans la stratégie avancée de l'appliance Citrix ADC qui contient les éléments suivants :

- **IP du serveur** : adresse IP du serveur Web d'authentification.
- **Port du serveur** : port du serveur Web d'authentification.
- **Règle d'authentification** : expression dans la stratégie avancée de l'appliance Citrix ADC qui contient les informations d'identification de l'utilisateur dans le format attendu par le serveur Web.
- **Scheme**—HTTP (pour l'authentification Web non chiffrée) ou HTTPS (pour l'authentification Web cryptée).
- **Règle de réussite** : expression dans la stratégie avancée de l'appliance Citrix ADC qui correspond à la chaîne de réponse du serveur Web qui indique que l'utilisateur s'est authentifié avec succès.

Pour tous les autres paramètres, suivez les règles normales de la commande d'ajout d'une action d'authentification.

Vous créez ensuite une stratégie associée à cette action. La stratégie est similaire à une stratégie LDAP, et comme les stratégies LDAP, elle utilise la syntaxe de l'appliance Citrix ADC.

> **Remarque**
>
> Ces instructions supposent que vous connaissez déjà les exigences d'authentification du ou des serveurs Web sur lesquels vous souhaitez vous authentifier et que vous avez déjà configuré le serveur d'authentification Web.

Pour configurer une action d'authentification Web à l'aide de l'interface de ligne de commande

Pour créer une action d'authentification Web sur la ligne de commande, tapez la commande suivante sur la ligne de commande :

```
add authentication webAuthAction <name> -serverIP <ip_addr|ipv6_addr
    |\*> -serverPort <port|\*> [-fullReqExpr <string>] -scheme ( http |
    https ) -successRule <expression> [-defaultAuthenticationGroup <
    string>][-Attribute1 <string>][-Attribute2 <string>] [-Attribute3 <
    string>][-Attribute4 <string>] [-Attribute5 <string>][-Attribute6 <
    string>] [-Attribute7 <string>][-Attribute8 <string>] [-Attribute9 <
```



```
    string>][-Attribute10 <string>] [-Attribute11 <string>][-Attribute12
     <string>] [-Attribute13 <string>][-Attribute14 <string>] [-
    Attribute15 <string>][-Attribute16 <string>]
<!--NeedCopy-->
```

Exemple

```
add policy expression post_data ""username=" + http.REQ.BODY(1000).
    SET_TEXT_MODE(IGNORECASE).AFTER_STR("login=").BEFORE_STR("&") + "&
    passwort=" + http.REQ.BODY(1000).SET_TEXT_MODE(IGNORECASE).AFTER_STR
    ("passwd=")"

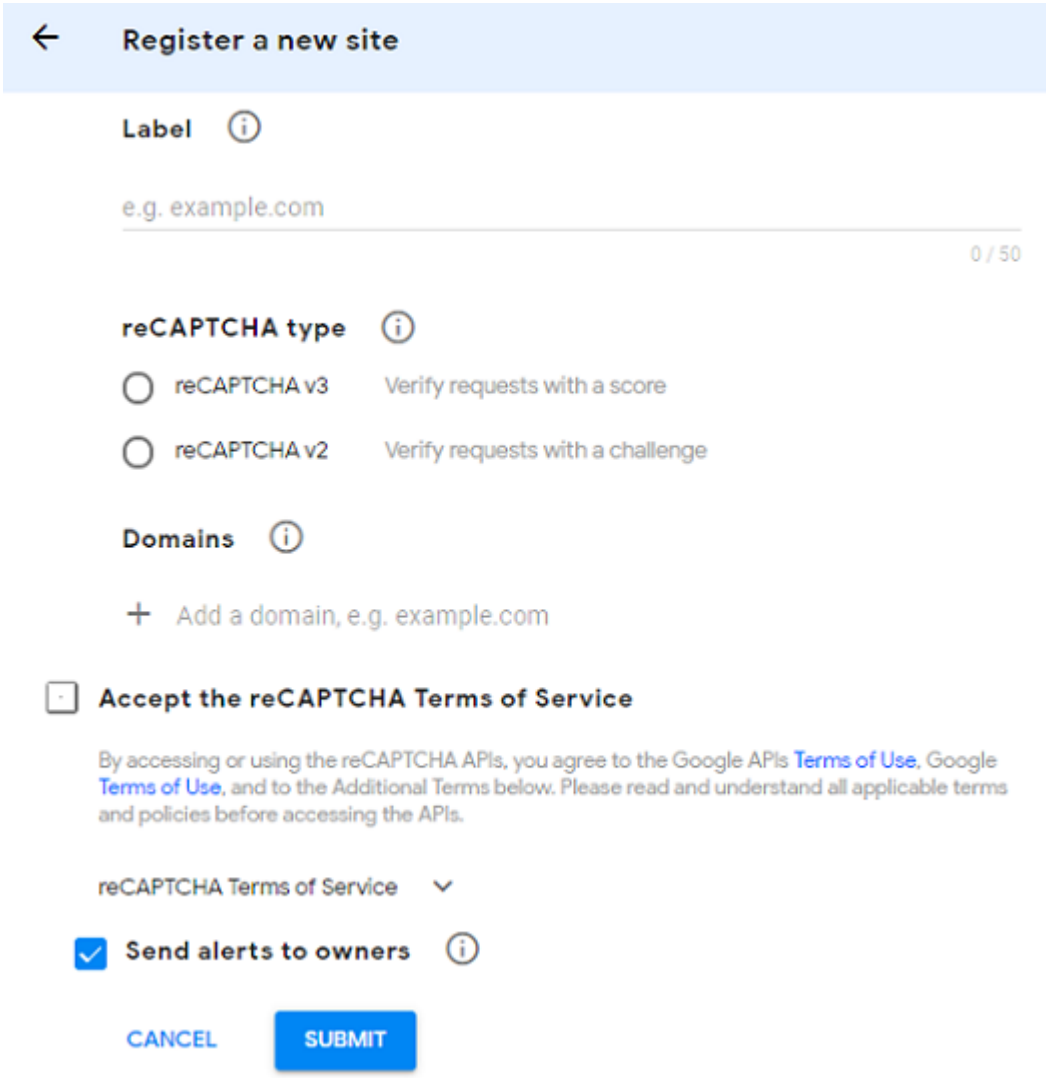
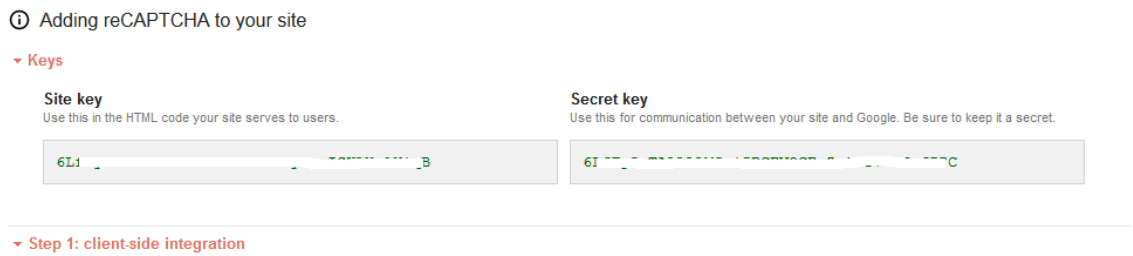
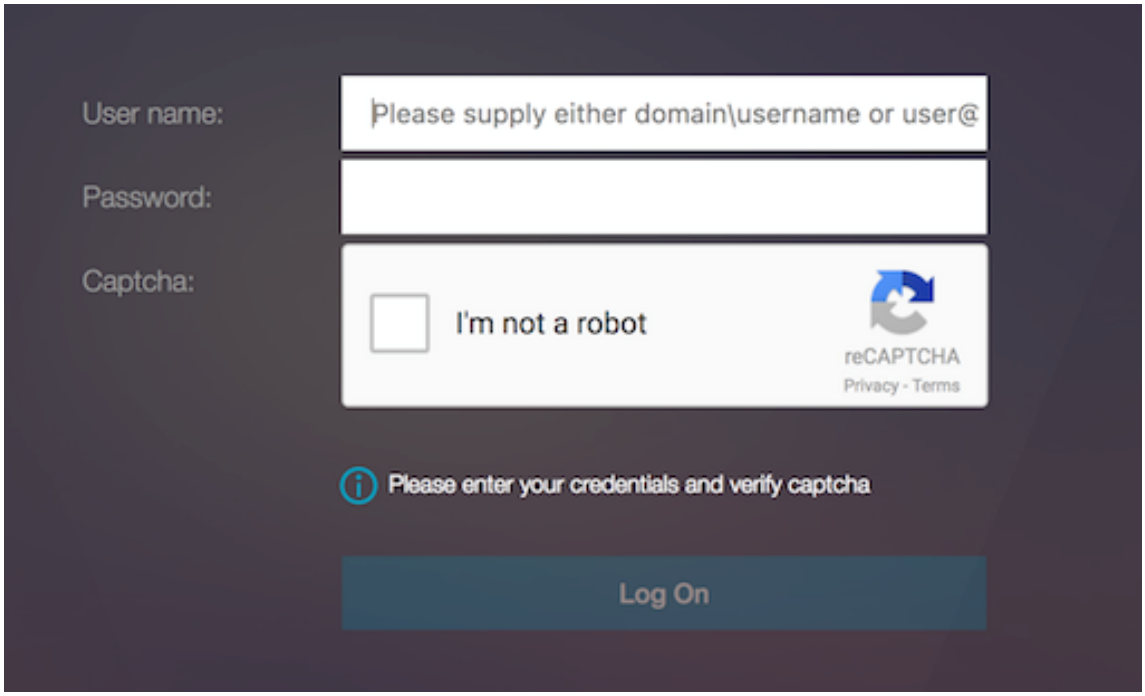
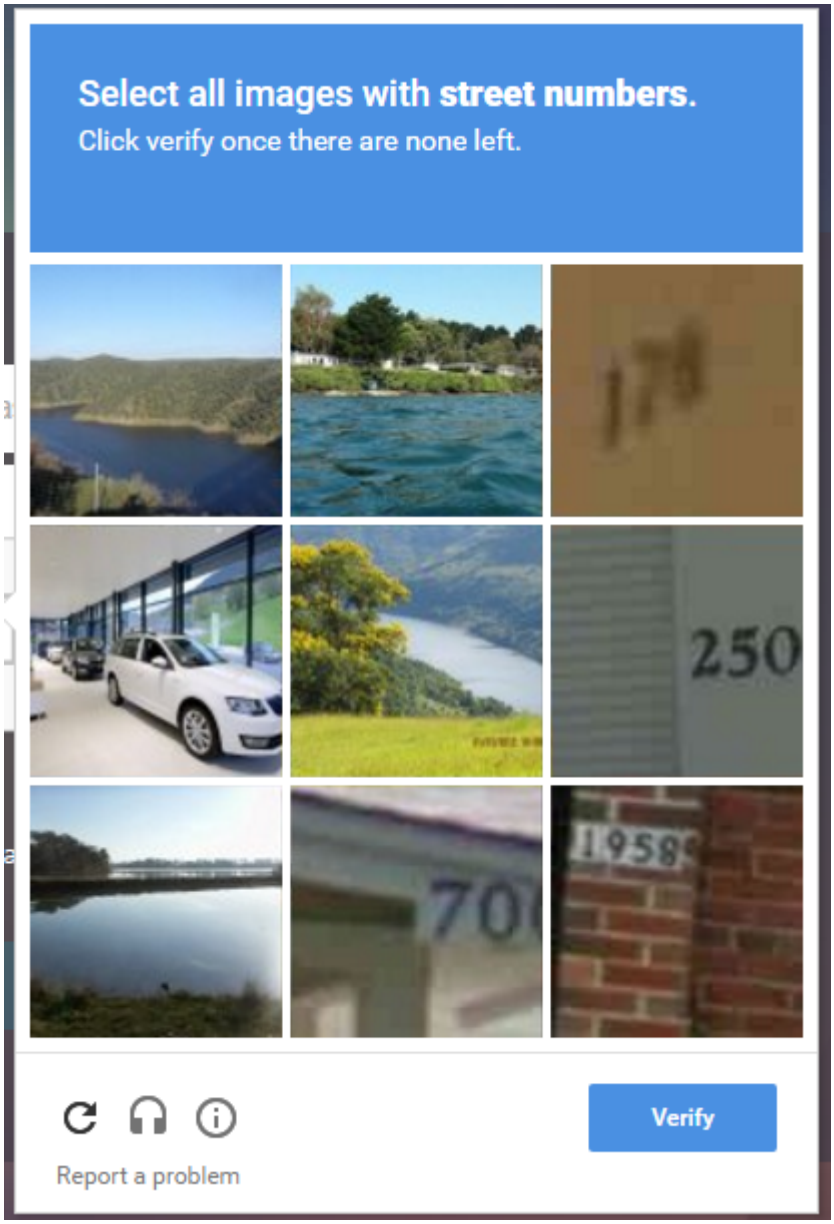
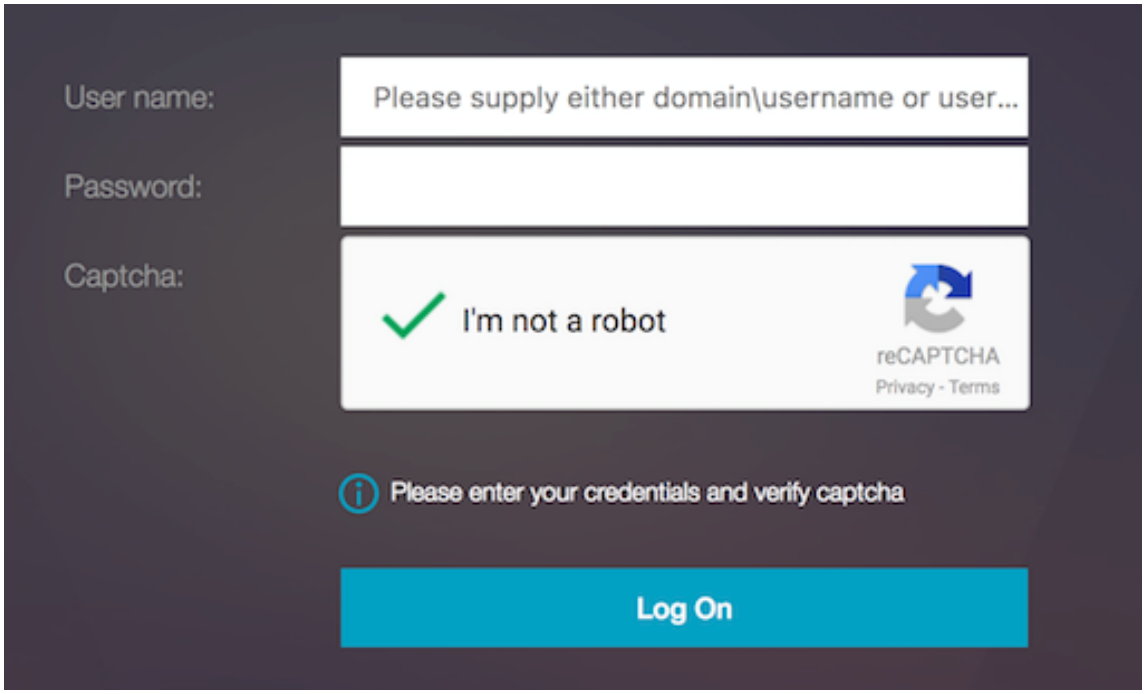
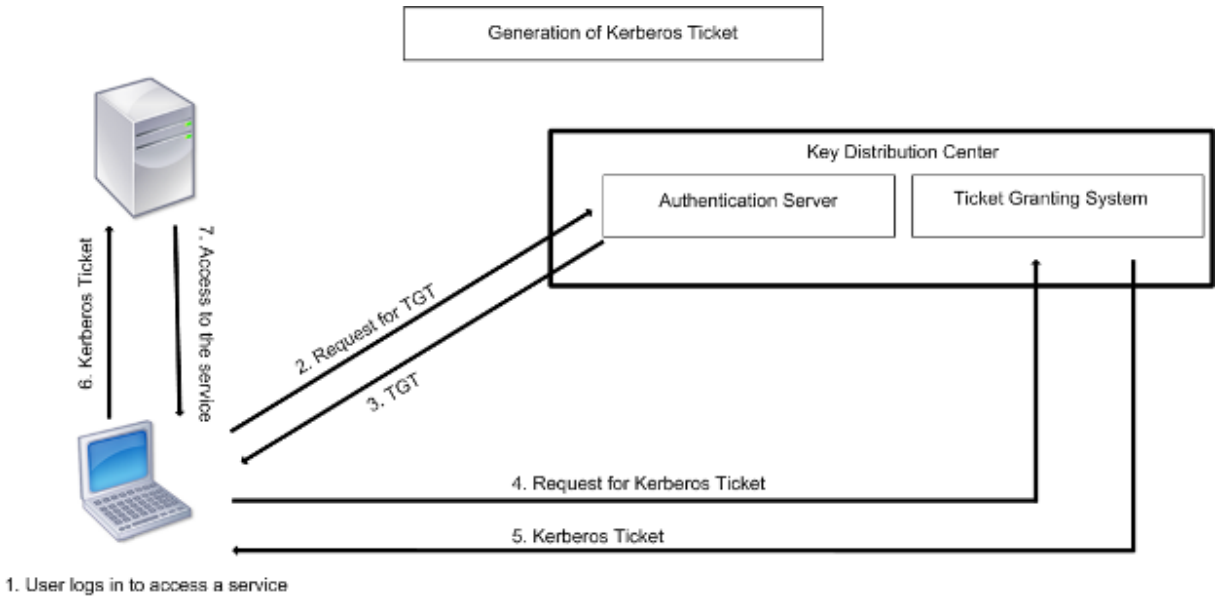
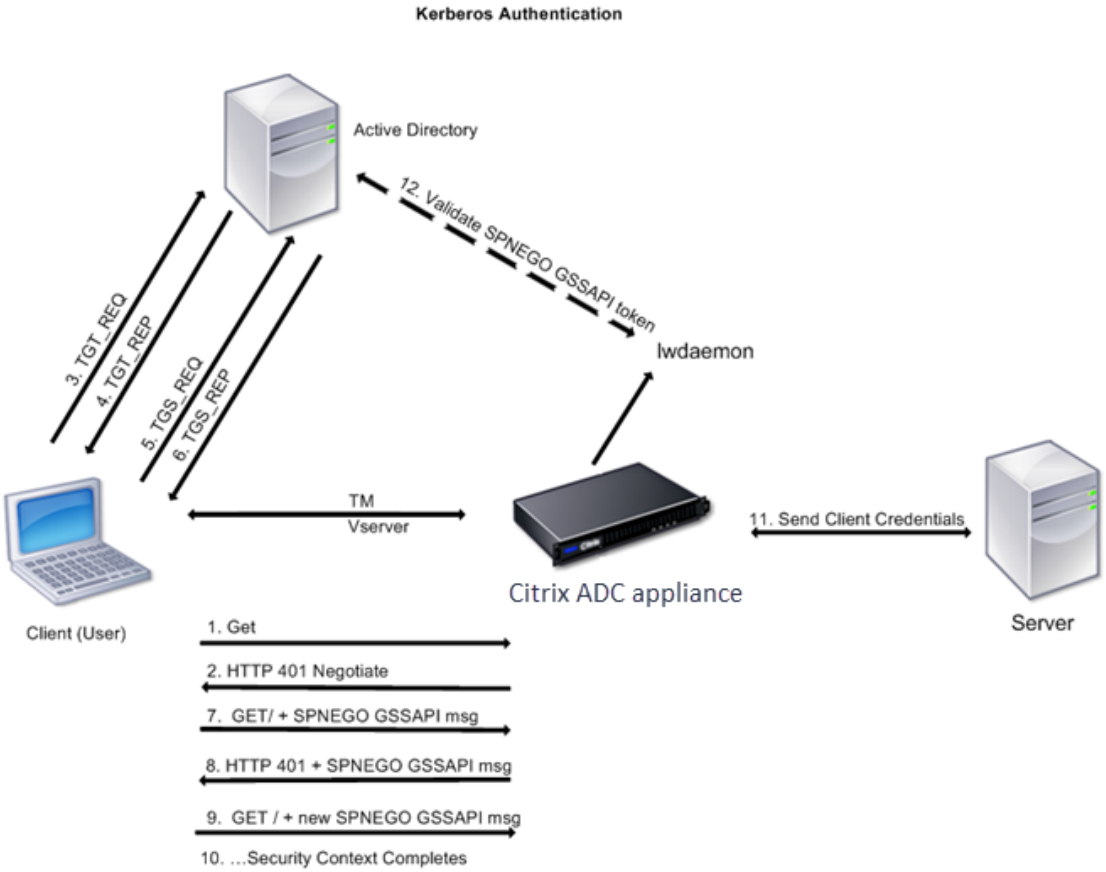
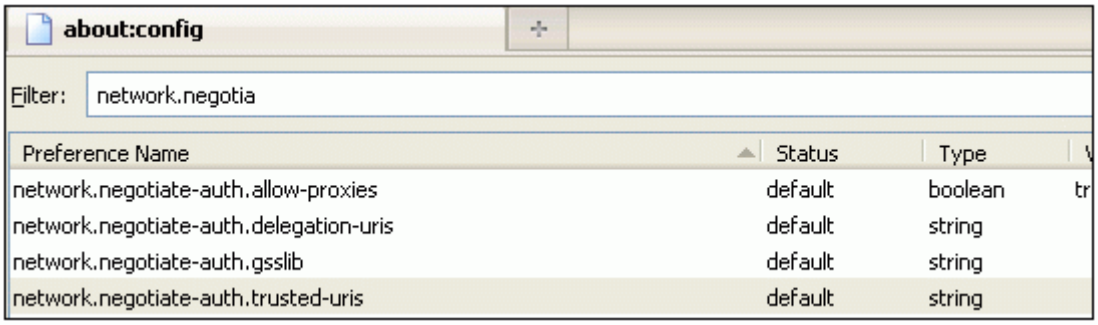
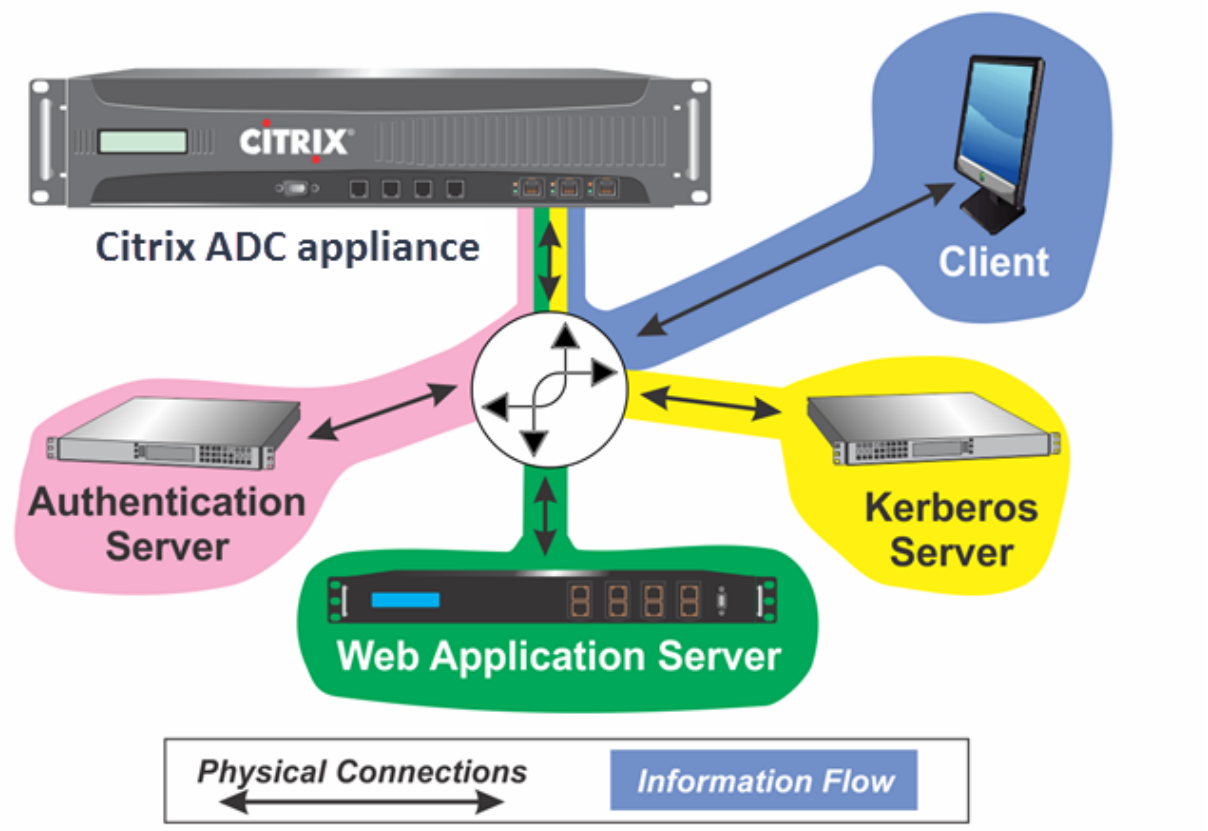
add policy expression length_post_data "("username= " + http.REQ.BODY
    (1000).SET_TEXT_MODE(IGNORECASE).AFTER_STR("login=").BEFORE_STR("&")
     + "passwort=" + http.REQ.BODY(1000).SET_TEXT_MODE(IGNORECASE).
    AFTER_STR("passwd=")).length"

add authentication webAuthAction webAuth_POST -serverIP 10.106.187.54 -
    serverPort 80 -fullReqExpr q{
 "POST /MyPHP/auth.php HTTP/" + http.req.version.major + "." + http.req
     .version.major + "\r\nAccept:\*/\*\r\nHost: 10.106.187.54\r\
     nReferer: http://10.106.187.54/MyPHP/auth.php\r\nAccept-Language:
     en-US\r\nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT
     6.1; Trident/5.0)\r\nContent-Type: application/x-www-form-
     urlencoded\r\n" + "Content-Length: " + length_post_data + "\r\
     nConnection: Keep-Alive\r\n\r\n" + post_data }
  -scheme http -successRule "http.res.status.eq(200)"
<!--NeedCopy-->
```

Pour configurer une action d'authentification Web à l'aide de l'utilitaire de configuration

> **Remarque**
>
> Dans l'utilitaire de configuration, le terme serveur est utilisé au lieu d'action, mais fait référence à la même tâche.

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > LDAP**.
2. Dans le volet d'informations, sous l'onglet **Serveurs**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez créer une nouvelle action d'authentification Web, cliquez sur **Ajouter**.
   - Si vous souhaitez modifier une action d'authentification Web existante, sélectionnez l'action dans le volet de données, puis cliquez sur **Modifier**.

3. Si vous créez une nouvelle action d'authentification Web, dans la boîte de dialogue **Créer un serveur Web d'authentification**, zone de texte **Nom**, tapez un nom pour la nouvelle action d'authentification Web. Le nom peut comporter de un à 127 caractères et peut être composé de lettres majuscules et minuscules, de chiffres et de traits d'union (-) et de traits de soulignement (_). Si vous modifiez une action d'authentification Web existante, ignorez cette étape. Le nom est en lecture seule ; vous ne pouvez pas le modifier.
4. Dans la zone de texte **Adresse IP du serveur Web**, tapez l'adresse IP IPv4 ou IPv6 du serveur Web d'authentification. Si l'adresse est une adresse IP IPv6, cochez d'abord la case IPv6.
5. Dans la zone de texte Port, tapez le numéro de port sur lequel le serveur Web accepte les connexions.
6. Sélectionnez **HTTP** ou **HTTPS** dans la liste déroulante **Protocole** .
7. Dans la zone de texte Expression de demande HTTP, tapez une expression régulière au format PCRE qui crée la demande de serveur Web qui contient les informations d'identification de l'utilisateur dans le format exact attendu par le serveur Web d'authentification.
8. Dans la zone de texte Expression pour valider l'authentification, tapez une expression de stratégie avancée de l'appliance Citrix ADC qui décrit les informations contenues dans la réponse du serveur Web indiquant que l'authentification de l'utilisateur a réussi.
9. Remplissez les champs restants comme décrit dans la documentation générale des actions d'authentification.
10. Cliquez sur **OK**.

Authentification à deux facteurs par SMS à l'aide de

August 20, 2021

Citrix ADC peut désormais être intégré à un fournisseur SMS tiers pour fournir une couche supplémentaire d'authentification.

L'appliance Citrix ADC peut être configurée pour envoyer un OTP sur le mobile de l'utilisateur en tant que deuxième facteur d'authentification. L'appliance présente à l'utilisateur un formulaire d'ouverture de session pour entrer dans l'OTP après une connexion AD réussie. Ce n'est qu'après l'authentification réussie du deuxième facteur que l'utilisateur se voit présenter la ressource demandée.

Configurer l'authentification à deux facteurs SMS avec Citrix ADC

Avant de configurer la fonctionnalité d'authentification à deux facteurs SMS, une authentification LDAP doit être configurée sur une appliance Citrix ADC comme premier facteur avec l'authentification activée. Pour obtenir des instructions sur la configuration de l'authentification LDAP, reportez-vous à la section Pour configurer l'authentification LDAP à l'aide de l'utilitaire de configuration.

> **Remarque**
>
> Le numéro de téléphone portable peut être extrait à l'aide de AAA.USER.ATTRIBUTE (1) et peut être inclus lors de l'envoi vers un serveur principal.

Attribuer une variable NS

À l'invite de commandes, tapez les commandes suivantes :

```
1 add ns variable <variable name> -type "map(text(65),text(6),100000)" -
     ifValueTooBig undef -ifNoValue undef -expires 5
2
3 add ns assignment<variable name> -variable "$test[AAA.USER.SESSIONID]"
     -set ("000000" + SYS.RANDOM.MUL(1000000).TYPECAST_UNSIGNED_LONG_AT.
     TYPECAST_TEXT_T).SUFFIX(6)
4 <!--NeedCopy-->
```

Exemple d'affectation de variables NS

```
1 add ns variable test -type "map(text(65),text(6),100000)" -
     ifValueTooBig undef -ifNoValue undef -expires 5
2
3 add ns assignment test -variable "$test[AAA.USER.SESSIONID]" -set ("
     000000" + SYS.RANDOM.MUL(1000000).TYPECAST_UNSIGNED_LONG_AT.
     TYPECAST_TEXT_T).SUFFIX(6)
4 <!--NeedCopy-->
```

Configurer l'action Webauth

À l'invite de commandes, tapez les commandes suivantes :

```
1 add policy expression <expression name> ""method=sendMessage&send_to=&
     msg=OTP i " + $test[AAA.USER.SESSIONID] + "for login into secure
     access  gateway. Valid till EXPIRE_TIME. Do not share the OTP with
     anyone for security reasons.&userid=#####&password=###=1.0""
2
3 add authentication webAuthAction webAuth_Get -serverIP <SERVER_IP> -
     serverPort <SERVER_PORT> -fullReqExpr q{
```



```
 "GET /GatewayAPI/rest?" + <expression name> + "HTTP/" + http.req.
    version.major + "." + http.req.version.minor.sub(1) + "\r\nAccept
    :\*/\*\r\nHost: <FQDN>\r\n" }
  -successRule "http.res.status.eq(200)" -scheme -successRule true

set authentication webAuthAction <web auth action name> <server IP
    address> -serverPort 8080 -fullReqExpr q{
 "POST /MyPHP/auth.php HTTP/" + http.req.version.major + "." + http.req
    .version.major + "\r\nAccept:\*/\*\r\nHost: <server IP address> \r\
    nContent-Length: 10\r\n\r\n" + <name in the format expected by SMS
    server> }
  -scheme http -successRule true
<!--NeedCopy-->
```

Exemple de configuration d'action Webauth

```
add policy expression otp_exp ""method=sendMessage&send_to=&msg=OTP i "
    + $test[AAA.USER.SESSIONID] + "for login into secure access
    gateway. Valid till EXPIRE_TIME. Do not share the OTP with anyone
    for security reasons.&userid=######&password=###=1.0""

add authentication webAuthAction webAuth_Get -serverIP -serverIP
    10.106.168.210 -serverPort 8080 -fullReqExpr q{
 "GET /GatewayAPI/rest?" + otp_exp + "HTTP/" + http.req.version.major +
    "." + http.req.version.minor.sub(1) + "\r\nAccept:\*/\*\r\nHost: <
    FQDN>\r\n" }
  -successRule "http.res.status.eq(200)" -scheme -successRule true

set authentication webAuthAction webAuth_POST -serverIP 10.106.168.210
    -serverPort 8080 -fullReqExpr q{
 "POST /MyPHP/auth.php HTTP/" + http.req.version.major + "." + http.req
    .version.major + "\r\nAccept:\*/\*\r\nHost: 10.106.168.210 \r\
    nContent-Length: 10\r\n\r\n" + otp_set }
  -scheme http -successRule true
<!--NeedCopy-->
```

Exemple de configuration du premier facteur

```
add authentication ldapAction ldap_action -serverIP 1.1.1.1 -serverPort
    3268 -authTimeout 30 -ldapBase "dc=nsi-test,dc=com" -ldapBindDn
    Administrator@nsi-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samaccountname -groupAttrName memberOf -
    ssoNameAttribute samaccountname  -Attribute1 mobile -email mail -
    CloudAttributes DISABLED
```



```
2
3 add authentication Policy ldap_policy -rule true -action ldap_action
4 <!--NeedCopy-->
```

Exemple de configuration du deuxième facteur

```
1  add authentication policylabel set_otp -loginSchema LSCHEMA_INT
2  add authentication Policy set_otp -rule true -action test
3
4  bind authentication policylabel set_otp -policyName set_otp -priority 1
       -gotoPriorityExpression NEXT
5  bind authentication policylabel set_otp -policyName cascade_noauth -
       priority 2 -gotoPriorityExpression NEXT -nextFactor check_otp
6
7  add authentication Policy check_otp -rule "$test.valueExists(AAA.USER.
       SESSIONID)" -action NO_AUTHN
8  add authentication policylabel check_otp -loginSchema LSCHEMA_INT
9  bind authentication policylabel check_otp -policyName wpp -priority 1 -
       gotoPriorityExpression NEXT
10 bind authentication policylabel check_otp -policyName
       wpp_cascade_noauth -priority 2 -gotoPriorityExpression NEXT -
       nextFactor otp_verify
11
12 add authentication Policy wpp -rule true -action webAuth_POST
13 add authentication Policy wpp_cascade_noauth -rule true -action
       NO_AUTHN
14
15 add authentication Policy otp_verify -rule "AAA.LOGIN.PASSWORD.EQ($test
       [AAA.USER.SESSIONID])" -action NO_AUTHN
16 add authentication policylabel otp_verify -loginSchema onlyPassword
17 bind authentication policylabel otp_verify -policyName otp_verify -
       priority 1 -gotoPriorityExpression NEXT
18
19 add authentication vserver avs SSL 10.106.40.121 443
20 bind authentication vserver avs -policy ldap_policy  -priority 1 -
       nextFactor set_otp -gotoPriorityExpression NEXT
21 <!--NeedCopy-->
```

Authentification par formulaire

January 21, 2021

Avec l'authentification basée sur les formulaires, un formulaire d'ouverture de session est présenté à l'utilisateur final. Ce type de formulaire d'authentification prend en charge à la fois l'authentification multifacteur (nFactor) et l'authentification classique.



Assurez-vous de ce qui suit pour que l'authentification basée sur les formulaires fonctionne :

- L'authentification du serveur virtuel d'équilibrage de charge doit être **activée**.
- Le paramètre 'AuthenticationHost' doit être spécifié vers lequel l'utilisateur doit être redirigé pour l'authentification. La commande pour configurer la même chose est la suivante :

```
1  set lb vs lb1 -authentication on  - authenticationhost aaavs-ip/
       fqdn
```

- L'authentification basée sur les formulaires est compatible avec le navigateur qui prend en charge HTML

Les étapes suivantes expliquant le fonctionnement de l'authentification basée sur les formulaires :

1. Le client (navigateur) envoie une requête GET pour une URL sur le serveur virtuel TM (équilibrage de charge/CS).
2. Le serveur virtuel TM détermine que le client n'a pas été authentifié et envoie une réponse HTTP 302 au client. La réponse contient un script masqué qui provoque le client à émettre une requête GET pour /cgi/tm au serveur virtuel d'authentification.
3. Le client envoie GET /cgi/tm contenant l'URL cible au serveur virtuel d'authentification.
4. Le serveur virtuel d'authentification envoie une redirection vers la page de connexion.
5. L'utilisateur envoie ses informations d'identification au serveur virtuel d'authentification avec un POST /doAuthentication.do. L'authentification est effectuée par le serveur virtuel d'authentification.
6. Si les informations d'identification sont correctes, le serveur virtuel d'authentification envoie une réponse HTTP 302 à l'URL cgi/selfauth sur le serveur d'équilibrage de charge avec un jeton unique (OTP).

7. Le serveur d'équilibrage de charge envoie HTTP 302 au client.
8. Le client envoie une requête GET pour son URL cible initiale avec un cookie de 32 octets.



Authentification basée sur 401

August 20, 2021

Avec l'authentification 401, l'appliance Citrix ADC présente une boîte de dialogue contextuelle à l'utilisateur final.



AAA-TM basé sur les formulaires fonctionne sur les messages de redirection. Cependant, certaines applications ne prennent pas en charge les redirections. Dans de telles applications, l'authentification 401 activée AAA-TM est utilisée.

Assurez-vous que 401 Authentication Activé AAA-TM fonctionne :

- La valeur du paramètre 'AuthNVSName' pour le serveur virtuel d'équilibrage de charge doit être le nom du serveur virtuel d'authentification à utiliser pour authentifier les utilisateurs.
- Le paramètre 'authn401' doit être activé. La commande pour configurer la même chose est la suivante :

```
1  set lb vs lb1 -authn401 on -authnvsName <aaavs-name>
```

Les étapes suivantes expliquant le fonctionnement de l'authentification 401 :

1. L'utilisateur tente d'accéder à une URL particulière à l'aide du serveur virtuel d'équilibrage de charge.
2. Le serveur virtuel d'équilibrage de charge renvoie une réponse HTTP 401 à l'utilisateur indiquant que l'authentification est requise pour l'accès.
3. L'utilisateur envoie ses informations d'identification au serveur virtuel d'équilibrage de charge dans l'en-tête d'autorisation.
4. Le serveur virtuel d'équilibrage de charge authentifie l'utilisateur, puis le connecte aux serveurs back-end.



Configuration de reCAPTCHA pour l'authentification nFactor

January 21, 2021

Citrix Gateway prend en charge une nouvelle action de première classe 'CaptChaAction' qui simplifie la configuration reCAPTCHA. Comme reCAPTCHA est un premier recours collectif, il peut être un facteur qui lui est propre. Vous pouvez injecter reCAPTCHA n'importe où dans le flux nFactor.

Auparavant, vous deviez écrire des stratégies WebAuth personnalisées avec des modifications à l'interface utilisateur RFWeb. Avec l'introduction de CaptChaAction, vous n'avez pas à modifier le JavaScript.

> **Important**
>
> Si reCAPTCHA est utilisé avec les champs nom d'utilisateur ou mot de passe dans le schéma, le bouton d'envoi est désactivé jusqu'à ce que reCAPTCHA soit rempli.

Configuration reCAPTCHA

La configuration reCAPTCHA comporte deux parties.

1. Configuration sur Google pour l'enregistrement de reCAPTCHA.

2. Configuration sur l'appliance Citrix ADC pour utiliser reCAPTCHA dans le cadre du flux de connexion.

Configuration reCAPTCHA sur Google

Enregistrez un domaine pour reCAPTCHA àhttps://www.google.com/recaptcha/admin.

1. Lorsque vous accédez à cette page, l'écran suivant apparaît.



> **Remarque**
>
> Utilisez reCAPTCHA v2 uniquement. Invisible reCAPTCHA est toujours en version bêta.

2. Après l'enregistrement d'un domaine, les « SiteKey » et « SecretKey » s'affichent.



> **Remarque**
>
> Les « SiteKey » et « SecretKey » sont grisés pour des raisons de sécurité. « SecretKey » doit être gardé en sécurité.

Configuration reCAPTCHA sur l'appliance Citrix ADC

La configuration reCAPTCHA sur l'appliance Citrix ADC peut être divisée en trois parties :

- Afficher l'écran reCaptcha
- Publier la réponse reCaptcha sur le serveur Google
- La configuration LDAP est le deuxième facteur pour l'ouverture de session utilisateur (facultatif)

Afficher l'écran reCaptcha

La personnalisation du formulaire de connexion se fait via le loginschema SingleAuthCaptcha.xml. Cette personnalisation est spécifiée au serveur virtuel d'authentification et est envoyée à l'interface utilisateur pour le rendu du formulaire de connexion. Le loginschema intégré, SingleAuthCaptcha.xml, se trouve dans le répertoire /NSConfig/LoginsChema/LoginsChema sur l'appliance Citrix ADC.

> **Important**
>
> - En fonction de votre cas d'utilisation et de différents schémas, vous pouvez modifier le schéma existant. Par exemple, si vous n'avez besoin que d'un facteur reCAPTCHA (sans nom d'utilisateur ni mot de passe) ou d'une double authentification avec reCAPTCHA.
> - Si des modifications personnalisées sont effectuées ou si le fichier est renommé, Citrix recommande de copier tous les LoginsChemas du répertoire /nsconfig/loginschema/loginschema vers le répertoire parent, /nsconfig/loginschema.

Pour configurer l'affichage de reCAPTCHA à l'aide de l'interface de ligne de commande

- `add authentication loginSchema singleauthcaptcha -authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml`
- `add authentication loginSchemaPolicy singleauthcaptcha -rule true -action singleauthcaptcha`

- add authentication vserver auth SSL <IP> <Port>
- add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-key-file>
- bind ssl vserver auth -certkey vserver-cert
- bind authentication vserver auth -policy singleauthcaptcha -priority 5 -gotoPriorityExpression END

Publier la réponse reCaptcha sur le serveur Google

Après avoir configuré le reCAPTCHA qui doit être affiché aux utilisateurs, les administrateurs publient la configuration au serveur Google pour vérifier la réponse reCAPTCHA du navigateur.

Pour vérifier la réponse reCAPTCHA à partir du navigateur

- add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-from-google> -secretkey <secretkey-from-google>
- add authentication policy myrecaptcha -rule **true** -action myrecaptcha
- bind authentication vserver auth -policy myrecaptcha -priority 1

Les commandes suivantes sont nécessaires pour configurer si l'authentification AD est souhaitée. Sinon, vous pouvez ignorer cette étape.

- add authentication ldapAction ldap-**new** -serverIP x.x.x.x -serverPort 636 -ldapBase "cn=users,dc=aaatm,dc=com"-ldapBindDn adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup
- add authenticationpolicy ldap-**new** -rule **true** -action ldap-**new**

La configuration LDAP est le deuxième facteur pour l'ouverture de session utilisateur (facultatif)

L'authentification LDAP se produit après reCAPTCHA, vous l'ajoutez au deuxième facteur.

- add authentication policylabel second-factor
- bind authentication policylabel second-factor -policy ldap-**new** -priority 10
- bind authentication vserver auth -policy myrecaptcha -priority 1 -nextFactor second-factor

L'administrateur doit ajouter des serveurs virtuels appropriés selon que le serveur virtuel d'équilibrage de charge ou l'appliance Citrix Gateway est utilisé pour l'accès. L'administrateur doit configurer la commande suivante si le serveur virtuel d'équilibrage de charge est requis :

- `add lb vserver lbtest HTTP <IP> <Port> -authentication ON -authenticationHost nssp.aaatm.com`

  nssp.aaatm.com — Résout à l'authentification du serveur virtuel.

Validation par l'utilisateur de reCAPTCHA

Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, vous devez voir les captures d'écran de l'interface utilisateur ci-dessous.

1. Une fois que le serveur virtuel d'authentification charge la page de connexion, l'écran d'ouverture de session s'affiche. L'**ouverture de session** est désactivée jusqu'à ce que reCAPTCHA soit terminé.



2. Sélectionnez Je ne suis pas une option de robot. Le widget reCAPTCHA s'affiche.



3. Vous naviguez à travers les séries d'images reCAPTCHA, avant l'affichage de la page de fin.
4. Entrez les informations d'identification AD, activez la case à cocher **Je ne suis pas un robot** et cliquez **sur Connexion** . Si l'authentification réussit, vous êtes redirigé vers la ressource souhaitée.



Remarques

- Si reCAPTCHA est utilisé avec l'authentification AD, le bouton Envoyer pour les informations d'identification est désactivé jusqu'à ce que reCAPTCHA soit terminé.
- Le reCAPTCHA se produit dans un facteur qui lui est propre. Par conséquent, toute validation ultérieure comme AD doit se produire dans le « nextfactor » de reCaptcha.

Prise en charge OTP native pour l'authentification

October 5, 2021

Citrix ADC prend en charge les mots de passe à usage unique (OTP) sans avoir à utiliser de serveur tiers. Le mot de passe à usage unique est une option hautement sécurisée pour l'authentification auprès de serveurs sécurisés, car le numéro ou le code d'accès généré est aléatoire. Auparavant, des entreprises spécialisées, telles que RSA avec des appareils spécifiques générant des nombres aléatoires, proposaient les OTP. Ce système doit être en communication constante avec le client pour générer un nombre attendu par le serveur.

En plus de réduire les dépenses d'investissement et d'exploitation, cette fonctionnalité améliore le contrôle de l'administrateur en conservant l'intégralité de la configuration sur l'appliance Citrix ADC.

Remarque

Étant donné que les serveurs tiers ne sont plus nécessaires, l'administrateur Citrix ADC doit con-

> figurer une interface pour gérer et valider les machines utilisateur.

L'utilisateur doit être inscrit auprès d'un serveur virtuel Citrix ADC pour utiliser la solution OTP. L'enregistrement n'est requis qu'une seule fois par appareil unique et peut être limité à certains environnements. La configuration et la validation d'un utilisateur enregistré sont similaires à la configuration d'une stratégie d'authentification supplémentaire.

Avantages de la prise en charge du protocole OTP natif

- Réduit les coûts d'exploitation en éliminant la nécessité de disposer d'une infrastructure supplémentaire sur un serveur d'authentification en plus d'Active Directory.
- Consolide la configuration uniquement sur l'appliance Citrix ADC, offrant ainsi un excellent contrôle aux administrateurs.
- Élimine la dépendance du client à un serveur d'authentification supplémentaire pour générer un nombre attendu par les clients.

Workflow OTP natif

La solution OTP native est un processus à deux volets et le flux de travail est classé comme suit :

- Enregistrement de l'appareil
- Connexion de l'utilisateur final

Important : Vous pouvez ignorer le processus d'enregistrement si vous utilisez des solutions tierces ou si vous gérez d'autres appareils en dehors de l'appliance Citrix ADC. La chaîne finale que vous ajoutez doit être au format spécifié par Citrix ADC.

La figure suivante illustre le flux d'enregistrement des appareils pour enregistrer un nouveau périphérique à recevoir OTP.

Remarque : L'enregistrement de l'appareil peut être effectué à l'aide d'un certain nombre de facteurs. Le facteur unique (tel que spécifié dans la figure précédente) est utilisé à titre d'exemple pour expliquer le processus d'enregistrement des appareils.

La figure suivante illustre la vérification de l'OTP via l'appareil enregistré.

La figure suivante illustre le flux d'enregistrement et de gestion des appareils.



La figure suivante illustre le flux de l'utilisateur final pour la fonctionnalité OTP native.



Conditions préalables

Pour utiliser la fonctionnalité OTP native, assurez-vous que les conditions préalables suivantes sont remplies.

- La version de la fonctionnalité Citrix ADC est 12.0 build 51.24 et ultérieur.
- La licence Advanced ou Premium Edition est installée sur Citrix Gateway.
- Citrix ADC est configuré avec une adresse IP de gestion et la console de gestion est accessible à la fois à l'aide d'un navigateur et d'une ligne de commande.
- Citrix ADC est configuré avec l'authentification, l'autorisation et l'audit du serveur virtuel pour authentifier les utilisateurs. Pour plus d'informations, voir AAA
- L'appliance Citrix ADC est configurée avec Unified Gateway et le profil d'authentification, d'autorisation et d'audit est attribué au serveur virtuel Gateway.
- La solution OTP native est limitée au flux d'authentification nFactor. Des stratégies avancées sont nécessaires pour configurer la solution. Pour plus de détails, voir OTP natif

Vérifiez également ce qui suit pour Active Directory :

- La longueur minimale des attributs est de 256 caractères.
- Le type d'attribut doit être « DirectoryString », par exemple UserParameters. Ces attributs peuvent contenir des valeurs de chaîne.
- Le type de chaîne d'attribut doit être Unicode, si le nom de l'appareil est en caractères non anglais.
- L'administrateur LDAP Citrix ADC doit disposer d'un accès en écriture à l'attribut AD sélectionné.

- L'appliance Citrix ADC et la machine cliente doivent être synchronisées avec un serveur de temps réseau commun.

Configuration du protocole OTP natif à l'aide de l'interface graphique

L'enregistrement OTP natif n'est pas seulement une authentification à facteur unique. Les sections suivantes vous aident à configurer l'authentification à un facteur et à un deuxième facteur.

Créer un schéma de connexion pour le premier facteur

1. Accédez à **Sécurité AAA > Trafic des applications > Schéma de connexion**.
2. Accédez à **Profils** et cliquez sur **Ajouter**.
3. Sur la page **Créer un schéma de connexion d'authentification**, saisissez *lschema_single_auth_manage_otp* dans le champ **Nom** et cliquez sur **Modifier** en regard de **noschema**.
4. Cliquez sur le dossier **LoginSchema** .
5. Faites défiler l'écran vers le bas pour sélectionner **SingleAuth.xml**, puis cliquez sur **Sélectionner**.
6. Cliquez sur **Create**.
7. Cliquez sur **Stratégies**, puis sur **Ajouter**.
8. Dans l'écran **Créer une stratégie de schéma de connexion d'authentification**, entrez les valeurs suivantes.

   Nom : lpol_single_auth_manage_otp_by_url

   Profil : Sélectionnez lschema_single_auth_manage_otp dans la liste.

   Règle : HTTP.REQ.COOKIE.VALUE (« NSC_TASS ») .EQ (»`manageotp`«)

Configuration du serveur virtuel d'authentification, d'autorisation et d'audit

1. Accédez à **Sécurité > AAA — Trafic des applications > Serveurs virtuels d'authentification**. Cliquez pour modifier le serveur virtuel existant. Pour plus d'informations, voir AAA
2. Cliquez sur l'icône **+** en regard de **Schemas de connexion** sous **Paramètres avancés** dans le volet droit.
3. Sélectionnez **Aucun schéma de connexion**.
4. Cliquez sur la flèche et sélectionnez la stratégie **lpol_single_auth_manage_otp_by_url**, cliquez sur **Sélectionner**, puis sur **Lier**.

5. Faites défiler la page vers le haut et sélectionnez **1 Stratégie d'authentification** sous **Stratégie d'authentification avancée** .
6. Cliquez avec le bouton droit sur la **stratégie nFactor** et sélectionnez **Modifier la liaison** . Cliquez avec le bouton droit sur la stratégie nFactor déjà configurée ou reportez-vous à NFactor pour en créer une et sélectionner Modifier la liaison.
7. Cliquez sur la flèche située sous **Sélectionner le facteur suivant,** pour sélectionner une configuration existante ou cliquez sur **Ajouter** pour créer un nouveau facteur.
8. Dans l'écran **Créer une stratégie d'authentification**, entrez ce qui suit et cliquez sur **Continuer** :

   Nom : manage_otp_flow_label

   Schéma de connexion : Lschema_Int
9. Sur l'écran **Étiquette de stratégie d'authentification**, cliquez sur **Ajouter** pour créer une stratégie.

   ```
   Create a policy for a normal LDAP server.
   ```
10. Dans l'écran **Créer une stratégie d'authentification**, entrez les éléments suivants :

    Nom : auth_pol_ldap_native_otp
11. Sélectionnez le type d'action comme **LDAP** à l'aide de la liste **Type d'action** .
12. Dans le champ **Action**, cliquez sur **Ajouter** pour créer une action.

    ```
    Create the first LDAP action with authentication enabled to be used for
     single factor.
    ```
13. Dans la page **Créer une authentification serveur LDAP**, sélectionnez le bouton radio **IP du serveur**, désactivez la case à cocher en regard de **Authentification**, entrez les valeurs suivantes et sélectionnez **Tester la connexion** . Voici un exemple de configuration.

    Nom : ldap_native_otp

    Adresse IP : 192.168.xx.xx

    DN de base : DC=Formation, DC=Lab

    Administrateur : Administrator@training.lab

    mot de passe : `xxxxx`

    ```
    Create a policy for OTP .
    ```
14. Dans l'écran **Créer une stratégie d'authentification**, entrez les éléments suivants :

    Nom : auth_pol_ldap_otp_action
15. Sélectionnez le type d'action comme **LDAP** à l'aide de la liste **Type d'action** .

16. Dans le champ **Action**, cliquez sur **Ajouter** pour créer une action.

    `Create the second LDAP action to set OTP authenticator with OTP secret configuration and authentication unchecked.`

17. Dans la page **Créer une authentification serveur LDAP**, sélectionnez le bouton radio **IP du serveur**, désactivez la case à cocher en regard de **Authentification**, entrez les valeurs suivantes et sélectionnez **Tester la connexion** . Voici un exemple de configuration.

    Nom : ldap_otp_action

    Adresse IP : 192.168.xx.xx

    DN de base : DC=Formation, DC=Lab

    Administrateur : Administrator@training.lab

    mot de passe : `xxxxx`

18. Faites défiler l'écran jusqu'à la section **Autres paramètres** . Utilisez le menu déroulant pour sélectionner les options suivantes.
    Attribut de nom d'ouverture de session du serveur comme **nouveau** et saisissez **userprincipalname**.

19. Utilisez le menu déroulant pour sélectionner **Attribut de nom SSO** comme **Nouveau** et saisissez **userprincipalname**.

20. Saisissez « UserParameters » dans le champ **secret OTP** et cliquez sur **Plus**.

21. Saisissez les attributs suivants.

    Attribut 1 = mail
    Attribut 2 = ObjectGuid
    Attribut 3 = ImmutableID

22. Cliquez sur **OK**.

23. Sur la page **Créer une stratégie d'authentification**, définissez l'expression sur **true** et cliquez sur **Créer**.

24. Sur la page **Créer une étiquette de stratégie d'authentification**, cliquez sur **Liaison**, puis sur **Terminé.**

25. Sur la page **Liaison de stratégie**, cliquez sur **Liaison**.

26. Dans la page **Stratégie d'authentification**, cliquez sur **Fermer** et cliquez sur **Terminé** .

    `Create OTP for OTP verification.`

27. Dans l'écran **Créer une stratégie d'authentification**, entrez les éléments suivants :

    Nom : auth_pol_ldap_otp_verify

28. Sélectionnez le type d'action comme **LDAP** à l'aide de la liste **Type d'action** .
29. Dans le champ **Action**, cliquez sur **Ajouter** pour créer une action.

    `Create the third LDAP action to verify OTP.`
30. Dans la page **Créer une authentification serveur LDAP**, sélectionnez le bouton radio **IP du serveur**, désactivez la case à cocher en regard de **Authentification**, entrez les valeurs suivantes et sélectionnez **Tester la connexion** . Voici un exemple de configuration.

    Nom : ldap_verify_otp

    Adresse IP : 192.168.xx.xx

    DN de base : DC=Formation, DC=Lab

    Administrateur : Administrator@training.lab

    mot de passe : `xxxxx`
31. Faites défiler l'écran jusqu'à la section **Autres paramètres** . Utilisez le menu déroulant pour sélectionner les options suivantes.
    Attribut de nom d'ouverture de session du serveur comme **nouveau** et saisissez **userprincipalname**.
32. Utilisez le menu déroulant pour sélectionner **Attribut de nom SSO** comme **Nouveau** et saisissez **userprincipalname**.
33. Saisissez « UserParameters » dans le champ **secret OTP** et cliquez sur **Plus**.
34. Saisissez les attributs suivants.

    Attribut 1 = mail
    Attribut 2 = ObjectGuid
    Attribut 3 = ImmutableID
35. Cliquez sur **OK**.
36. Sur la page **Créer une stratégie d'authentification**, définissez l'expression sur **true** et cliquez sur **Créer**.
37. Sur la page **Créer une étiquette de stratégie d'authentification**, cliquez sur **Liaison**, puis sur **Terminé.**
38. Sur la page **Liaison de stratégie**, cliquez sur **Liaison**.
39. Dans la page **Stratégie d'authentification**, cliquez sur **Fermer** et cliquez sur **Terminé** .

Vous ne disposez probablement pas déjà d'une stratégie d'authentification avancée pour votre serveur LDAP normal.
Changez le type d'action sur LDAP.
Sélectionnez votre serveur LDAP normal, qui est celui sur lequel l'authentification est activée.

Saisissez true comme expression. Cette option utilise la stratégie avancée au lieu de la syntaxe classique.
Cliquez sur Créer.

> **Remarque**
>
> Le serveur virtuel d'authentification doit être lié au thème du portail RFWebUI. Liez un certificat de serveur au serveur. L'adresse IP du serveur « 1.2.3.5 » doit avoir un nom de domaine complet correspondant, à savoir otpauth.server.com, pour une utilisation ultérieure.

Créer un schéma de connexion pour le deuxième facteur OTP

1. Accédez à **Sécurité > Trafic des applications AAA > Serveurs virtuels**. Sélectionnez le serveur virtuel à modifier.
2. Faites défiler l'écran vers le bas et sélectionnez **1 schéma de connexion**.
3. Cliquez sur **Ajouter une liaison**.
4. Dans la section **Liaison de stratégie**, cliquez sur **Ajouter** pour ajouter une stratégie.
5. Sur la page **Créer une stratégie de schéma de connexion d'authentification**, entrez Nom comme OTP, puis cliquez sur **Ajouter** pour créer un profil.
6. Sur la page **Créer un schéma de connexion d'authentification**, entrez Nom en tant qu'OTP, puis cliquez sur l'icône en forme de crayon en regard de **noschema**.
7. Cliquez sur le dossier **Loginschema**, sélectionnez **DualAuthManageOTP.xml**, puis cliquez sur **Sélectionner**.
8. Cliquez sur **Plus** et faites défiler vers le bas.
9. Dans le champ **Index des informations d'identification du mot** de passe, entrez 1. Ainsi, nFactor enregistre le mot de passe de l'utilisateur dans l'attribut AAA #1, qui peut être utilisé ultérieurement dans une stratégie de trafic vers Single Sign-On to StoreFront. Si ce n'est pas le cas, Citrix Gateway essaie d'utiliser le code secret pour s'authentifier auprès de StoreFront, ce qui ne fonctionne pas.
10. Cliquez sur **Create**.
11. Dans la section **Règle**, saisissez **Vrai**. Cliquez sur **Create**.
12. Cliquez sur **Bind**.
13. Notez les deux facteurs d'authentification. Cliquez sur **Fermer**, puis sur **Terminé** .

Stratégie de trafic pour Single Sign-On

1. Accédez à **Citrix Gateway > Stratégies > Trafic**.
2. Dans l'onglet **Profils de trafic**, cliquez sur **Ajouter**.
3. Entrez un nom pour le profil de trafic pour OTP.

4. Faites défiler vers le bas, dans la zone Expression de mot de passe SSO, entrez ce qui suit, puis cliquez sur **Créer**. C'est ici que nous utilisons l'attribut mot de passe du schéma de connexion spécifié pour le deuxième facteur OTP.

   ```
   http.REQ.USER.ATTRIBUTE(1)
   ```

5. Dans **l'onglet Stratégies de trafic**, cliquez sur **Ajouter**.
6. Dans le champ **Nom**, entrez un nom pour la stratégie de trafic.
7. Dans le champ **Demander un profil**, sélectionnez le profil de trafic que vous avez créé.
8. Dans la zone Expression, saisissez **True**. Si votre serveur virtuel Citrix Gateway autorise un VPN complet, modifiez l'expression comme suit.

   ```
   http.req.method.eq(post)||http.req.method.eq(get)&& false
   ```

9. Cliquez sur **Create**.

Configurer la stratégie de commutation de contenu pour gérer OTP

Les configurations suivantes sont requises si vous utilisez Unified Gateway.

1. Accédez à **Gestion du trafic > Changement de contenu > Stratégies**. Sélectionnez la stratégie de changement de contenu, cliquez avec le bouton droit de la souris et sélectionnez **Modifier**.
2. Modifiez l'expression pour évaluer l'instruction OR suivante, puis cliquez sur **OK** :

is_vpn_url||HTTP.REQ.URL.CONTAINS("manageotp")

Configuration du protocole OTP natif à l'aide de la CLI

Vous devez disposer des informations suivantes pour configurer la page de gestion des appareils OTP :

- IP attribuée au serveur virtuel d'authentification
- FQDN correspondant à l'adresse IP attribuée
- Certificat de serveur pour serveur virtuel d'authentification

> **Remarque :** L'OTP natif est une solution Web uniquement.

Pour configurer la page d'enregistrement et de gestion des appareils OTP

Créer un serveur virtuel d'authentification

```
add authentication vserver authvs SSL 1.2.3.5 443
bind authentication vserver authvs -portaltheme RFWebUI
bind ssl vserver authvs -certkeyname otpauthcert
```


> **Remarque :** Le serveur virtuel d'authentification doit être lié au thème du portail RFWEbui. Liez un certificat de serveur au serveur. L'adresse IP du serveur « 1.2.3.5 » doit avoir un nom de domaine complet correspondant, à savoir otpauth.server.com, pour une utilisation ultérieure.

Pour créer une action d'ouverture de session LDAP

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
    -  serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
    ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
```

Exemple :

```
add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName userprincipalname
```

Pour ajouter une stratégie d'authentification pour l'ouverture de session LDAP

```
add authentication Policy auth_pol_ldap_logon -rule true -action
    ldap_logon_action
```

Pour présenter l'interface utilisateur via LoginsChema

Afficher le champ nom d'utilisateur et le champ de mot de passe aux utilisateurs lors de l'ouverture de session

```
add authentication loginSchema lschema_single_auth_manage_otp -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/
    SingleAuthManageOTP.xml"
```

Afficher la page d'enregistrement et de gestion des périphériques

Citrix recommande deux façons d'afficher l'écran d'enregistrement et de gestion des appareils : URL ou nom d'hôte.

- **Utilisation de l'URL**

  Lorsque l'URL contient « /manageotp »


```
- add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url
  -rule "http.req.cookie.value("NSC_TASS").contains("manageotp")"-
  action lschema_single_auth_manage_otp
- bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url
  -priority 10 -gotoPriorityExpression END
```

- **Utiliser le nom d'hôte**

  Lorsque le nom d'hôte est « alt.server.com »

```
- add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host
  -rule "http.req.header("host").eq("alt.server.com")"-action
  lschema_single_auth_manage_otp
- bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_hos
  -priority 20 -gotoPriorityExpression END
```

Pour configurer la page de connexion utilisateur à l'aide de l'interface de ligne de commande

Vous devez disposer des informations suivantes pour configurer la page Ouverture de session utilisateur :

- IP pour un serveur virtuel d'équilibrage de charge
- Nom de domaine complet correspondant pour le serveur virtuel d'équilibrage de charge
- Certificat de serveur pour le serveur virtuel d'équilibrage de charge

  bind ssl vserver lbvs_https -certkeyname lbvs_server_cert

Le service back-end dans l'équilibrage de charge est représenté comme suit :

```
1 add service iis_backendsso_server_com 1.2.3.210 HTTP 80
2 bind lb vserver lbvs_https iis_backendsso_server_com
```

Pour créer une action de validation du code secret OTP

```
1 add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
    -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
    ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
    authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>`
```

Exemple :

```
1 add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
```



```
    ldapLoginName userprincipalname -authentication DISABLED -OTPSecret
    userParameters
```

> **Important :** La différence entre l'ouverture de session LDAP et l'action OTP est la nécessité de désactiver l'authentification et d'introduire un nouveau paramètre `OTPSecret`. N'utilisez pas la valeur de l'attribut AD.

Pour ajouter une stratégie d'authentification pour la validation du code d'accès OTP

```
1 add authentication Policy auth_pol_otp_validation -rule true -action
    ldap_otp_action
```

Pour présenter l'authentification à deux facteurs via LoginSchema

Ajoutez l'interface utilisateur pour l'authentification à deux facteurs.

```
1 add authentication loginSchema lscheme_dual_factor -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/DualAuth.xml
    "
2 add authentication loginSchemaPolicy lpol_dual_factor -rule true -
    action lscheme_dual_factor
```

Pour créer un facteur de validation de code secret via l'étiquette de stratégie

Créer une étiquette de stratégie de flux OTP de gestion pour le facteur suivant (le premier facteur est l'ouverture de session LDAP)

```
1 add authentication loginSchema lschema_noschema -authenticationSchema
    noschema
2 add authentication policylabel manage_otp_flow_label -loginSchema
    lschema_noschema
```

Pour lier la stratégie OTP à l'étiquette de stratégie

```
1 bind authentication policylabel manage_otp_flow_label -policyName
    auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

Pour lier le flux de l'interface utilisateur

Liez l'ouverture de session LDAP suivie de la validation OTP avec le serveur virtuel d'authentification.


```
1 bind authentication vserver authvs -policy auth_pol_ldap_logon -
    priority 10 -nextFactor  manage_otp_flow_label -
    gotoPriorityExpression NEXT
2 bind authentication vserver authvs -policy lpol_dual_factor -priority
    30 -gotoPriorityExpression END
```

Enregistrez votre appareil avec Citrix ADC

1. Accédez au nom de domaine complet Citrix ADC (première adresse IP publique), avec un suffixe /manageotp. Par exemple, https://otpauth.server.com/manageotp connectez-vous avec les informations d'identification de l'utilisateur.
2. Cliquez sur l'icône **+** pour ajouter un appareil.
3. Entrez le nom d'un appareil et appuyez sur **Go**. Un code-barres apparaît à l'écran.
4. Cliquez sur **Commencer la configuration**, puis sur **Scanner le code-barres**.
5. Survolez le code QR avec la caméra de l'appareil. Vous pouvez éventuellement entrer le code à 16 chiffres.

   > **Remarque** : Le code QR affiché est valide pendant 3 minutes.

6. Une fois la numérisation réussie, un code temporel à 6 chiffres vous est présenté, qui peut être utilisé pour vous connecter.
7. Pour tester, cliquez sur **Terminé** sur l'écran QR, puis cliquez sur la coche verte à droite.
8. Sélectionnez votre appareil dans le menu déroulant et saisissez le code de Google Authenticator (il doit être bleu et non rouge), puis cliquez sur **OK**.
9. Assurez-vous de vous déconnecter à l'aide du menu déroulant situé dans le coin supérieur droit de la page.

Connectez-vous à Citrix ADC à l'aide de l'OTP

1. Accédez à votre première URL publique et saisissez votre OTP à partir de Google Authenticator pour ouvrir une session.
2. Authentifiez-vous sur la page de démarrage de Citrix ADC.

Stockage des données secrètes OTP dans un format crypté

August 20, 2021

À partir de Citrix ADC version 13.0 build 41.20, les données secrètes OTP peuvent être stockées dans un format crypté au lieu de texte brut.

Auparavant, l'appliance Citrix ADC stockait le secret OTP sous forme de texte brut dans AD. Le stockage du secret OTP en texte brut constitue une menace pour la sécurité car un attaquant malveillant ou un administrateur peut exploiter les données en visualisant le secret partagé d'autres utilisateurs.

Le paramètre de chiffrement active le chiffrement du secret OTP dans AD. Lorsque vous enregistrez un nouveau périphérique avec Citrix ADC version 13.0 build 41.20 et que vous activez le paramètre de chiffrement, le secret OTP est stocké dans un format chiffré, par défaut. Toutefois, si le paramètre de chiffrement est désactivé, le secret OTP est stocké au format texte brut.

Pour les périphériques enregistrés avant la version 13.0 41.20, vous devez effectuer les opérations suivantes comme pratique recommandée :

1. Mettez à niveau l'appliance Citrix ADC 13.0 vers la version 13.0 41.20.
2. Activez le paramètre de chiffrement sur l'appliance.
3. Utilisez l'outil de migration secrète OTP pour migrer les données secrètes OTP du format texte brut au format chiffré.

Pour plus d'informations sur l'outil de migration secrète OTP, voir Outil de chiffrement OTP.

> **Important**
>
> Citrix vous recommande en tant qu'administrateur pour vous assurer que les critères suivants sont remplis :
>
> - Un nouveau certificat doit être configuré pour chiffrer les secrets OTP si vous n'utilisez pas KBA dans le cadre de la fonctionnalité de réinitialisation de mot de passe en libre-service.
>   - To bind the certificate to VPN global, you can use the following command:
>
>     ```
>     bind vpn global -userDataEncryptionKey <certificate name>
>     ```
> - Si vous utilisez déjà un certificat pour chiffrer KBA, vous pouvez utiliser le même certificat pour chiffrer les secrets OTP.

Pour activer les données de chiffrement OTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set aaa otpparameter [-encryption ( ON | OFF )]
```

Exemple

```
set aaa otpparameter -encryption ON
```


Pour configurer le chiffrement OTP à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA — Trafic d'application** et cliquez sur **Modifier l'authentification AAA OTP Parameter** sous la section **Paramètres d'authentification**.
2. Sur la page **Configurer le paramètre OTP AAA**, sélectionnez **Chiffrement secret OTP** .
3. Cliquez sur OK.

Configuration du nombre de périphériques utilisateur final pour recevoir des notifications OTP

Les administrateurs peuvent désormais configurer le nombre de périphériques qu'un utilisateur final peut enregistrer pour recevoir une notification ou une authentification OTP.

Pour configurer le nombre de périphériques dans OTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set aaa otpparameter [-maxOTPDevices <positive_integer>]
```

Exemple

```
set aaa otpparameter -maxOTPDevices 4
```

Pour configurer le nombre de périphériques à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA — Trafic d'application**, cliquez sur **Modifier l'authentification AAA OTP Parameter**sous la section **Paramètres d'authentification**.
2. Sur la page **Configurer le paramètre OTP AAA**, entrez la valeur du **périphérique OTP Max configuré** .
3. Cliquez sur **OK**.



Outil de chiffrement OTP

August 20, 2021

À partir de Citrix ADC version 13.0 build 41.20, les données secrètes OTP sont stockées dans un format crypté au lieu d'un texte brut pour une sécurité renforcée. Le stockage du secret OTP dans un format crypté est automatique et ne nécessite pas d'intervention manuelle.

Auparavant, l'appliance Citrix ADC stockait le secret OTP sous forme de texte brut dans le répertoire actif. Le stockage du secret OTP dans un format texte brut constituait une menace pour la sécurité car un attaquant malveillant ou un administrateur pourrait exploiter les données en visualisant le secret partagé d'autres utilisateurs.

L'outil de chiffrement OTP offre les avantages suivants :

- N'entraîne pas de perte de données, même si vous avez d'anciens appareils utilisant l'ancien format (texte brut).
- La prise en charge de la rétrocompatibilité avec les anciennes versions de Citrix Gateway permet d'intégrer et de travailler avec les périphériques existants, ainsi qu'avec le nouveau périphérique.
- L'outil de chiffrement OTP aide les administrateurs à migrer toutes les données secrètes OTP de tous les utilisateurs à la fois.

> **Remarque :**
>
> l'outil de chiffrement OTP ne crypte ni ne déchiffre les données d'enregistrement KBA ou d'enregistrement des e-mails.

Utilisation de l'outil de chiffrement OTP

L'outil de chiffrement OTP peut être utilisé pour les éléments suivants :

- **Chiffrement**. Stockez le secret OTP au format crypté. L'outil extrait les données OTP des périphériques enregistrés avec Citrix ADC, puis convertit les données OTP au format texte brut au format chiffré.
- **Décryptage**. Rétablir le secret OTP au format texte brut.
- **Mettre à jour les certificats**. Les administrateurs peuvent mettre à jour le certificat vers un nouveau certificat à tout moment. Les administrateurs peuvent utiliser l'outil pour entrer le nouveau certificat et mettre à jour toutes les entrées avec les nouvelles données de certificat. Le chemin d'accès au certificat doit être soit un chemin absolu, soit un chemin relatif.

> **Important**
>
> - Vous devez activer le paramètre de chiffrement dans l'appliance Citrix ADC pour utiliser l'outil de chiffrement OTP.
> - Pour les périphériques enregistrés auprès de Citrix ADC avant la version 41.20, vous devez effectuer les opérations suivantes :
>   - Upgrade the 13.0 Citrix ADC appliance to 13.0 build 41.20.
>   - Enable the encryption parameter on the appliance.
>   - Use the OTP Secret migration tool to migrate OTP secret data from plain text format to encrypted format.

Données secrètes OTP au format texte brut

Exemple :

```
##@devicename=<16 or more bytes>&tag=<64bytes>&,
```

Comme vous pouvez le voir, le motif de départ pour l'ancien format est toujours « #@ » et le motif de fin est toujours « & ». Toutes les données entre « devicename= » et le motif de fin, constituent des données OTP de l'utilisateur.

Données secrètes OTP au format crypté

Le nouveau format crypté des données OTP est du format suivant :

Exemple :

```
1     {
2
3          "otpdata" : {
4
5           "devices" : {
```



```
6
7                           “device1” :  “value1” ,
8                           “device2” :  “value2” , ···
9                       }
10
11              }
12
13      }
14
15 <!--NeedCopy-->
```

Où, value1 est la valeur encodée base64 de données kid + IV +chiffrement

Les données de chiffrement sont structurées comme suit :

```
1     {
2
3       secret:<16-byte secret>,
4       tag : <64-byte tag value>
5       alg: <algorithm used> (not mandatory, default is sha1, specify
           the algorithm only if it is not default)
6      }
7
8 <!--NeedCopy-->
```

- Dans « devices », vous avez une valeur par rapport à chaque nom. La valeur est base64encode (kid) .base64encode (IV) .base64encode (cipherdata).
- Dans les algorithmes AES standard, IV est toujours envoyé en tant que 16 ou 32 premiers octets de données chiffrées. Vous pouvez suivre le même modèle.
- IV diffère pour chaque appareil bien que la clé reste la même.

Configuration de l’outil de chiffrement OTP

L’outil de chiffrement OTP se trouve dans le répertoire\var\netscaler\otptool. Vous devez télécharger le code à partir de la source Citrix ADC et exécuter l’outil avec les informations d’identification AD requises.

- Conditions préalables à l’utilisation de l’outil de chiffrement OTP :
  - Installez python 3.5 ou version supérieure dans l’environnement où cet outil est exécuté.
  - Installez pip3 ou versions ultérieures.
- Exécutez les commandes suivantes :
  - **pip install requirements.txt**. Installe automatiquement les exigences
  - **Python main.py**. Invoque l’outil de chiffrement OTP. Vous devez fournir les arguments requis en fonction de votre besoin pour la migration des données secrètes OTP.

- L'outil peut être localisé à`\var\netscaler\otptool` partir de l'invite de shell.
- Exécutez l'outil avec les informations d'identification AD requises.

Interface de l'outil de chiffrement OTP

La figure suivante affiche un exemple d'interface d'outil de chiffrement OTP. L'interface contient tous les arguments qui doivent être définis pour le chiffrement, le décryptage et la mise à niveau de certificat. De plus, une brève description de chaque argument est saisie.

Argument OPERATION

Vous devez définir l'argument OPERATION pour utiliser l'outil de chiffrement OTP pour le chiffrement, le déchiffrement ou la mise à niveau de certificat.

Le tableau suivant résume certains des scénarios dans lesquels vous pouvez utiliser l'outil de chiffrement OTP et les valeurs d'argument OPERATION correspondantes.

Scénario	Valeur de l'argument d'opération et autres arguments
Convertir le secret OTP en texte brut au format chiffré dans le même attribut	Entrez la valeur de l'argument OPÉRATION sur 0 et fournissez la même valeur pour l'attribut source et cible. **Exemple :** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute unixhomedirectory -operation 0 -cert_path aaatm_wild_all.cert`
Convertir un secret OTP en texte brut au format chiffré dans un attribut différent	Entrez la valeur de l'argument OPÉRATION sous la forme 0 et indiquez les valeurs correspondantes pour l'attribut source et cible. **Exemple :** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute userparameters -operation 0 -cert_path aaatm_wild_all.cert`

Scénario	Valeur de l'argument d'opération et autres arguments
Convertir les entrées chiffrées en texte clair	Entrez la valeur de l'argument OPÉRATION comme 1 et indiquez les valeurs correspondantes pour l'attribut source et cible. **Exemple :** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute userparameters -operation 1 -cert_path aaatm_wild_all.cert`
Mettre à jour le certificat vers un nouveau certificat	Entrez la valeur 2 de l'argument OPÉRATION et indiquez tous les détails du certificat précédent et du nouveau certificat dans les arguments correspondants. **Exemple :** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute userparameters -operation 2 -cert_path aaatm_wild_all.cert -new_cert_path aaatm_wild_all_new.cert`

Argument CERT_PATH

L'argument CERT_PATH spécifie le certificat utilisé dans Citrix ADC pour chiffrer les données. L'utilisateur doit fournir cet argument pour les trois opérations, à savoir les **certificats de **chiffrement**, de **déchiffrement**et de mise à jour**.

> **Points à noter sur le certificat**
>
> - L'utilisateur doit fournir le même certificat lié globalement dans Citrix ADC pour le chiffrement des données utilisateur.
> - Le certificat doit contenir le certificat public codé Base64 et sa clé privée RSA correspondante dans le même fichier.

> - Le format du certificat doit être PEM ou CERT. Le certificat doit respecter le format X509.
> - Le format de certificat protégé par mot de passe et le fichier *.pfx* ne sont pas acceptés par cet outil. L'utilisateur doit convertir les certificats PFX en *.cert* avant de fournir les certificats à l'outil.

Argument SEARCH_FILTER

L'argument SEARCH_FILTER est utilisé pour filtrer les domaines AD ou les utilisateurs. Le format de ce filtre de recherche est identique au format de filtre de recherche LDAP utilisé dans la commande d'action LDAP dans Citrix ADC.

Activation de l'option de chiffrement dans l'appliance Citrix ADC

Pour chiffrer le format de texte brut, vous devez activer l'option de chiffrement dans l'appliance Citrix ADC.

Pour activer les données de chiffrement OTP à l'aide de l'interface de ligne de commande, tapez :

```
set aaa otpparameter [-encryption ( ON | OFF )]
```

Exemple :

```
set aaa otpparameter -encryption ON
```

Cas d'utilisation de l'outil de chiffrement OTP

L'outil de chiffrement OTP peut être utilisé dans les cas d'utilisation suivants.

Enregistrer de nouveaux périphériques avec l'appliance Citrix ADC version 13.0 build 41.20

Lorsque vous enregistrez votre nouveau périphérique auprès de l'appliance Citrix ADC version 13.0 build 41.x, et si l'option de chiffrement est activée, les données OTP sont enregistrées dans un format chiffré. Vous pouvez éviter une intervention manuelle.

Si l'option de chiffrement n'est pas activée, les données OTP sont stockées au format texte brut.

Migrer les données OTP pour les périphériques enregistrés avant la version 13.0 41.20

Vous devez effectuer les opérations suivantes pour chiffrer les données secrètes OTP pour les périphériques qui sont enregistrés auprès de l'appliance Citrix ADC avant la version 13.0 41.20.

- Utilisez l'outil de conversion pour migrer les données OTP du format texte brut au format chiffré.
- Activez le paramètre « Encryption » sur l'appliance Citrix ADC.
  - Pour activer l'option de chiffrement à l'aide de l'interface de ligne de commande :

    * `set aaa otpparameter -encryption ON`
  - Pour activer les options de chiffrement à l'aide de l'interface graphique :
    * Accédez à **Sécurité > AAA — Trafic d'application** et cliquez sur **Modifier l'authentification AAA OTP Parameter** sous la section **Paramètres d'authentification**.
    * Sur la page **Configurer le paramètre OTP AAA**, sélectionnez **Chiffrement secret OTP**, puis cliquez sur **OK** .
  - Connectez-vous avec les informations d'identification AD valides.
  - Si cela est nécessaire, enregistrez des périphériques supplémentaires (facultatif).

Migrer des données chiffrées de l'ancien certificat vers le nouveau certificat

Si les administrateurs souhaitent mettre à jour le certificat vers un nouveau certificat, l'outil fournit une option pour mettre à jour les nouvelles entrées de données de certificat.

Pour mettre à jour le certificat vers un nouveau certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

Exemple :

```
python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local
-search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -
target_attribute userparameters -operation 2 -cert_path aaatm_wild_all.cert
 -new_cert_path aaatm_wild_all_new.cert
```

> **Remarque**
>
> - Les certificats doivent contenir à la fois des clés privées et publiques.
> - Actuellement, la fonctionnalité est fournie uniquement pour OTP.

Rechiffrer ou migrer vers un nouveau certificat pour les périphériques enregistrés après la mise à niveau de l'appliance vers la version 13.0 41.20 avec chiffrement

Admin peut utiliser l'outil sur les périphériques déjà chiffrés avec un certificat et peut mettre à jour ce certificat avec un nouveau certificat.

Convertir les données chiffrées au format texte brut

Admin peut décrypter le secret OTP et les rétablir au format de texte brut original. L'outil de chiffrement OTP scanne tous les utilisateurs pour le secret OTP au format crypté et les convertit au format déchiffré.

Pour mettre à jour le certificat vers un nouveau certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

Exemple :

```
python3 main.py -Host 192.0.2.1 - Port 636 -username ldapbind_user@aaa
    .local -search_base cn=users,dc=aaa,dc=local -source_attribute
    unixhomedirectory -target_attribute userparameters -operation 1
<!--NeedCopy-->
```

Résolution des problèmes

L'outil génère les fichiers journaux suivants.

- **app.log**. Consigne toutes les étapes principales de l'exécution et les informations sur les erreurs, les avertissements et les échecs.
- **unmodified_users.txt**. Contient une liste des noms de domaine utilisateur qui n'ont pas été mis à niveau du texte brut au format chiffré. Ces journaux sont générés à une erreur de format ou peuvent être dus à une autre raison.

Notification Push pour OTP

October 5, 2021

Citrix Gateway prend en charge les notifications push pour OTP. Les utilisateurs n'ont pas besoin d'entrer manuellement l'OTP reçu sur leurs appareils enregistrés pour se connecter à Citrix Gateway. Les administrateurs peuvent configurer Citrix Gateway de sorte que les notifications de connexion soient envoyées aux appareils enregistrés des utilisateurs à l'aide des services de notification push. Lorsque les utilisateurs reçoivent la notification, ils doivent simplement appuyer sur Autoriser sur la notification pour se connecter à Citrix Gateway. Lorsque la passerelle reçoit un accusé de réception de la part de l'utilisateur, elle identifie la source de la demande et envoie une réponse à cette connexion au navigateur.

Si la réponse de notification n'est pas reçue dans le délai d'expiration (30 secondes), les utilisateurs sont redirigés vers la page de connexion de Citrix Gateway. Les utilisateurs peuvent ensuite entrer l'OTP manuellement ou cliquer sur **Renvoyer la notification** pour recevoir à nouveau la notification sur l'appareil enregistré.

Les administrateurs peuvent faire de l'authentification par notification push l'authentification par défaut en utilisant les schémas de connexion créés pour les notifications push.

> **Important :**
>
> La fonctionnalité de notification push est disponible avec une licence Citrix ADC Premium Edition.

Avantages des notifications push

- Les notifications push fournissent un mécanisme d'authentification multifacteur plus sécurisé. L'authentification auprès de Citrix Gateway échoue tant que l'utilisateur n'a pas approuvé la tentative de connexion.
- La notification Push est facile à administrer et à utiliser. Les utilisateurs doivent télécharger et installer l'application mobile Citrix SSO qui ne nécessite aucune assistance d'administrateur.
- Les utilisateurs n'ont pas besoin de copier ou de mémoriser le code. Ils doivent simplement appuyer sur l'appareil pour s'authentifier.
- Les utilisateurs peuvent enregistrer plusieurs appareils.

Fonctionnement des notifications push

Le flux de travail de notification push peut être classé en deux catégories :

- Enregistrement de l'appareil
- Connexion de l'utilisateur final



Conditions préalables à l'utilisation de la notification push

- Terminez le processus d'intégration de Citrix Cloud.
  1. Créez un compte d'entreprise Citrix Cloud ou rejoignez un compte existant. Pour obtenir des processus détaillés et des instructions sur la marche à suivre, consultez la section Inscription à Citrix Cloud.
  2. Connectez-vous https://citrix.cloud.comà et sélectionnez le client.

3. Dans le menu, sélectionnez **Gestion des identités et des accès**, puis accédez à l'onglet **Accès API** pour créer un client pour le compte.
4. Copiez l'ID, le secret et l'ID client. L'ID et le secret sont nécessaires pour configurer le service push dans Citrix ADC en tant que « ClientID » et « ClientSecret » respectivement.

> **Important :**
>
> - Les mêmes informations d'identification d'API peuvent être utilisées sur plusieurs centres de données.
> - Les appliances Citrix ADC locales doivent être en mesure de résoudre les adresses de serveur mfa.cloud.com et trust.citrixworkspacesapi.net et sont accessibles depuis l'appliance. Cela permet de s'assurer qu'il n'y a pas de pare-feu ou de blocage d'adresse IP pour ces serveurs sur le port 443.

- Téléchargez l'application mobile Citrix SSO depuis l'App Store et le Play Store pour les appareils iOS et Android respectivement. La notification push est prise en charge sur iOS à partir de la version 1.1.13 sur Android à partir de la version 2.3.5.
- Vérifiez les points suivants pour Active Directory.
  - La longueur minimale des attributs doit être d'au moins 256 caractères.
  - Le type d'attribut doit être « DirectoryString », par exemple UserParameters. Ces attributs peuvent contenir des valeurs de chaîne.
  - Le type de chaîne d'attribut doit être Unicode, si le nom de l'appareil est en caractères non anglais.
  - L'administrateur LDAP Citrix ADC doit disposer d'un accès en écriture à l'attribut AD sélectionné.
  - Citrix ADC et la machine cliente doivent être synchronisés avec un serveur de temps réseau commun.

Configuration des notifications Push

Voici les étapes de haut niveau qui doivent être effectuées pour utiliser la fonctionnalité de notification push.

- L'administrateur Citrix Gateway doit configurer l'interface pour gérer et valider les utilisateurs.
  1. Configurez un service Push.
  2. Configurez Citrix Gateway pour la gestion OTP et la connexion de l'utilisateur final.

     Les utilisateurs doivent enregistrer leurs appareils auprès de Gateway pour se connecter à Citrix Gateway.
  3. Enregistrez votre appareil auprès de Citrix Gateway.
  4. Connectez-vous à Citrix Gateway.

Créer un service Push

1. Accédez à **Sécurité** > **Trafic des applications AAA** > **Stratégies** > **Authentification** > **Stratégies avancées** > **Actions** > **Service push**, puis cliquez sur **Ajouter**.
2. Dans la zone **Nom**, saisissez le nom du service Push.
3. Dans **ID client**, saisissez l'identité unique de la partie de confiance pour communiquer avec le serveur Citrix Push dans le cloud.
4. Dans **Client Secret**, saisissez le secret unique de la partie de confiance pour communiquer avec le serveur Citrix Push dans le cloud.
5. Dans **Customer ID**, saisissez l'ID client ou le nom du compte dans le cloud utilisé pour créer la paire ID client et secret client.

> **Important**
>
> La version TLS 1.2 est requise pour le service push. Pour plus d'informations, reportez-vous à la section Détails de configuration TLS 1.2.

Configurer Citrix Gateway pour la gestion OTP et la connexion de l'utilisateur final

Suivez les étapes suivantes pour la gestion OTP et la connexion de l'utilisateur final.

- Créer un schéma de connexion pour la gestion OTP
- Configuration du serveur virtuel d'authentification, d'autorisation et d'audit
- Configuration de serveurs virtuels VPN ou d'équilibrage de charge
- Configuration de l'étiquette de stratégie
- Créer un schéma de connexion pour la connexion de l'utilisateur final

Pour plus de détails sur la configuration, voir Prise en charge OTP native.

Important : Pour les notifications push, les administrateurs doivent configurer explicitement les éléments suivants :

- Créez un service Push.
- Lors de la création d'un schéma de connexion pour la gestion OTP, sélectionnez le schéma de connexion SingleAuthManageOTP.xml ou équivalent selon les besoins.
- Lors de la création d'un schéma de connexion pour la connexion de l'utilisateur final, sélectionnez le schéma de connexion DualAuthOrPush.xml ou équivalent selon les besoins.

Enregistrez votre appareil auprès de Citrix Gateway

Les utilisateurs doivent enregistrer leurs appareils auprès de Citrix Gateway pour utiliser la fonctionnalité de notification push.

1. Dans votre navigateur Web, accédez au nom de domaine complet Citrix Gateway et ajoutez le suffixe **/manageotp** au nom de domaine complet.

   La page d'authentification est chargée.
   Exemple : https://gateway.company.com/manageotp

2. Connectez-vous à l'aide de vos informations d'identification LDAP ou des mécanismes d'authentification à deux facteurs appropriés, le cas échéant.



3. Cliquez sur **Ajouter appareil**.
4. Entrez un nom pour votre appareil, puis cliquez sur **OK**.

   Un code QR s'affiche sur la page du navigateur Citrix Gateway.



5. Scannez ce code QR à l'aide de l'application Citrix SSO depuis l'appareil à enregistrer.

Citrix SSO valide le code QR, puis s'enregistre auprès de Gateway pour les notifications push. S'il n'y a pas d'erreur dans le processus d'inscription, le jeton est correctement ajouté à la page des jetons de mot de passe.



6. S'il n'y a pas d'autres appareils à ajouter/gérer, déconnectez-vous à l'aide de la liste située dans le coin supérieur droit de la page.

Test de l'authentification par mot de passe unique

1. Pour tester l'OTP, cliquez sur votre appareil dans la liste, puis cliquez sur **Test**.
2. Saisissez le code OTP que vous avez reçu sur votre appareil, puis cliquez sur **OK**.

   Le message de vérification OTP réussi s'affiche.
3. Déconnectez-vous en utilisant la liste en haut à droite de la page.

Remarque : Vous pouvez utiliser le portail de gestion OTP à tout moment pour tester l'authentification, supprimer des appareils enregistrés ou enregistrer d'autres appareils.

Connectez-vous à Citrix Gateway

Après avoir enregistré leurs appareils auprès de Citrix Gateway, les utilisateurs peuvent utiliser la fonctionnalité de notification push pour l'authentification.

1. Accédez à la page d'authentification Citrix Gateway (par exemple : https://gateway.company.com)

   Vous êtes invité à entrer uniquement vos informations d'identification LDAP en fonction de la configuration du schéma de connexion.



2. Saisissez votre nom d'utilisateur et votre mot de passe LDAP, puis sélectionnez **Soumettre**.

   Une notification est envoyée sur votre appareil enregistré.

   Remarque : Si vous souhaitez entrer manuellement l'OTP, vous devez sélectionner **Cliquer** pour saisir manuellement le code OTP et entrer l'OTP dans le champ **TOTP** .

3. Ouvrez l'application Citrix SSO sur votre appareil enregistré et appuyez sur **Autoriser**.



Remarque :

- Dans le cas d'un appareil iOS, vous êtes invité à entrer l'identifiant tactile/face-ID ou code d'accès comme facteur d'authentification supplémentaire.
- Le serveur d'authentification attend la réponse de notification du serveur push jusqu'à ce que le délai d'expiration configuré expire. Après l'expiration du délai, Citrix Gateway affiche la page de connexion. Les utilisateurs peuvent ensuite entrer l'OTP manuellement ou cliquer sur **Renvoyer la notification** pour recevoir à nouveau la notification sur l'appareil enregistré. En fonction de l'option sélectionnée, Gateway valide l'OTP que vous avez entré ou renvoie la notification sur votre appareil enregistré.



- Aucune notification n'est envoyée à votre appareil enregistré concernant un échec de connexion.

Conditions de panne

- L'enregistrement de l'appareil peut échouer dans les cas suivants.
  - Le certificat de serveur n'est peut-être pas approuvé par la machine de l'utilisateur final.
  - Citrix Gateway utilisé pour s'inscrire à OTP n'est pas accessible par le client.
- Les notifications peuvent échouer dans les cas suivants.
  - La machine utilisateur n'est pas connectée à Internet
  - Les notifications sur la machine utilisateur sont bloquées
  - L'utilisateur n'approuve pas la notification sur l'appareil

Dans ces cas, le serveur d'authentification attend l'expiration du délai d'expiration configuré. Après l'expiration du délai, Citrix Gateway affiche une page de connexion avec les options permettant de

saisir manuellement l'OTP ou de renvoyer la notification sur votre appareil enregistré. En fonction de l'option sélectionnée, une validation supplémentaire se produit.

Journaux d'échec

Les journaux suivants sont attendus lorsque le service Push OTP n'est pas accessible.

- Échec de la notification Push lorsque la machine utilisateur n'est pas connectée à Internet - Push : échec de la préparation de la demande Push à`client name`"pour le service Push.
- Journal d'échec de l'enregistrement des appareils - Push : Aucun appareil n'est enregistré pour envoyer une demande Push au cloud pour "`client name`».
- Dans le cas où l'utilisateur n'accepte pas le push - Push : La réponse n'est pas vue du client, pour`user name`"», vérifiant les options de nouvelle tentative.

Comportement de l'application Citrix SSO sur iOS — points à noter

Raccourcis de notification

L'application Citrix SSO iOS inclut la prise en charge des notifications exploitables afin d'améliorer l'expérience utilisateur. Une fois qu'une notification est reçue sur un appareil iOS, et si l'appareil est verrouillé ou que l'application Citrix SSO n'est pas au premier plan, les utilisateurs peuvent utiliser les raccourcis intégrés à la notification pour approuver ou refuser la demande de connexion.

Pour accéder aux raccourcis de notification, les utilisateurs doivent soit forcer le toucher (3D touch), soit appuyer longuement sur la notification en fonction du matériel de l'appareil. La sélection de l'action Autoriser le raccourci envoie une demande de connexion à Citrix ADC. Selon la façon dont la stratégie d'authentification est configurée sur le serveur virtuel d'authentification, d'autorisation et d'audit ;

- La demande de connexion peut être envoyée en arrière-plan sans qu'il soit nécessaire de lancer l'application au premier plan ou de déverrouiller l'appareil.
- L'application peut demander à entrer Touch-ID/Face-ID/Passcode comme facteur supplémentaire, auquel cas l'application est lancée au premier plan.





Suppression des jetons de mot de passe de Citrix SSO

1. Pour supprimer un jeton de mot de passe enregistré pour le push dans l'application Citrix SSO, les utilisateurs doivent effectuer les opérations suivantes :
2. Désinscrivez (supprimez) l'appareil iOS/Android sur la passerelle. Le code QR permettant de supprimer l'enregistrement de l'appareil s'affiche.
3. Ouvrez l'application Citrix SSO et appuyez sur le bouton d'informations du jeton de mot de passe à supprimer.
4. Appuyez sur **Supprimer le jeton** et scannez le code QR.

Remarque :

- Si le code QR est valide, le jeton est correctement supprimé de l'application Citrix SSO.
- Les utilisateurs peuvent appuyer sur Forcer la suppression pour supprimer un jeton de mot de passe sans avoir à scanner le code QR si l'appareil est déjà retiré de la passerelle. La suppression forcée peut faire en sorte que l'appareil continue de recevoir des notifications si l'appareil n'a pas été supprimé de Citrix Gateway.





Authentification OTP par e-mail

January 21, 2021

Email OTP est introduit avec Citrix ADC 12.1 build 51.x. La méthode Email OTP vous permet de vous authentifier à l'aide du mot de passe à usage unique (OTP) envoyé à l'adresse e-mail enregistrée. Lorsque vous essayez de vous authentifier sur un service, le serveur envoie un OTP à l'adresse e-mail enregistrée de l'utilisateur.

Pour utiliser la fonction Email OTP, vous devez d'abord enregistrer votre identifiant de messagerie secondaire. Une autre inscription d'ID e-mail est nécessaire pour que l'OTP puisse être envoyé à cet ID de messagerie, car vous ne pourrez pas accéder à l'ID de messagerie principal en cas de verrouillage du compte ou en cas d'oubli du mot de passe AD.

Vous pouvez utiliser la validation Email OTP sans enregistrement d'ID e-mail si vous avez déjà fourni l'ID de messagerie alternatif dans le cadre d'un attribut AD. Vous pouvez vous référer au même attribut dans l'action e-mail au lieu de spécifier l'ID de messagerie alternatif dans la section Adresse de messagerie.

Conditions préalables

Avant de configurer la fonctionnalité Email OTP, consultez les conditions préalables suivantes :

- Fonctionnalité Citrix ADC version 12.1 build 51.28 et versions ultérieures
- La fonction Email OTP est disponible uniquement dans le flux d'authentification NFactor

- Pour plus de détails, reportez-vous à https://support.citrix.com/pages/citrix-adc-authentication-how#nfactor
- Prise en charge pour AAA-TM, Citrix Gateway (navigateur, plug-in natif et Receiver).

Paramètre Active Directory

- La version prise en charge est le niveau de fonction de domaine Active Directory 2016/2012 et 2008
- Le nom d'utilisateur Citrix ADC LDAPbind doit disposer d'un accès en écriture au chemin AD de l'utilisateur

Serveur de messagerie

- Pour que la solution Email OTP fonctionne, assurez-vous que l'authentification basée sur la connexion est activée sur le serveur SMTP. Citrix ADC prend en charge uniquement l'authentification basée sur la connexion Auth pour que l'OTP Email fonctionne.
- Pour vous assurer que l'authentification basée sur la connexion Auth est activée, tapez la commande suivante sur le serveur SMTP. Si l'authentification basée sur la connexion est activée, vous remarquez que le texte AUTH LOGIN apparaît en **gras** dans la sortie.

```
root@ns# telnet <IP address of the SMTP server><Port number of the server>
ehlo
root@ns# telnet 10.106.3.
Trying 10.106.
Connected to 10.106.
Escape character is '^]'.
220 E2K13.NSGSanity.com Microsoft ESMTP MAIL Service ready at Fri, 22 Nov
2019 16:24:17 +0530
ehlo
250-E2K13.NSGSanity.com Hello [10.221.
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
For information on how to enable login based authentication, see
https://support.microfocus.com/kb/doc.php?id=7020367
```

Limitations

- Cette fonctionnalité n'est prise en charge que si le back-end d'authentification est LDAP.
- Vous ne pouvez pas voir d'autre ID e-mail déjà enregistré.

- Seul l'ID de messagerie secondaire de la page Enregistrement KBA ne peut pas être mis à jour.
- L'authentification et l'enregistrement KBA et Email OTP ne peuvent pas être les premiers facteurs du flux d'authentification. C'est par la conception pour obtenir une authentification robuste.
- Le même attribut AD doit être configuré pour KBA et ID de messagerie secondaire si vous utilisez la même action LDAP d'authentification.
- Pour le plug-in natif et Receiver, l'enregistrement est pris en charge uniquement via un navigateur.

Configuration d'Active Directory

- Email OTP utilise l'attribut Active Directory comme stockage de données utilisateur.
- Une fois que vous avez enregistré l'ID de messagerie secondaire, ils sont envoyés à l'appliance Citrix ADC et l'appliance le stocke dans l'attribut Base de connaissances configurée dans l'objet utilisateur AD.
- L'ID de messagerie secondaire est chiffré et stocké dans l'attribut AD configuré.

Lors de la configuration d'un attribut AD, tenez compte des éléments suivants :

- La longueur du nom d'attribut prise en charge doit comporter au moins 128 caractères.
- Le type d'attribut doit être 'DirectoryString'.
- Le même attribut AD peut être utilisé pour les données d'enregistrement OTP et KBA natives.
- L'administrateur LDAP doit disposer d'un accès en écriture à l'attribut AD sélectionné.

Utilisation des attributs existants

L'attribut utilisé dans cet exemple est « UserParameters ». Étant donné qu'il s'agit d'un attribut existant au sein de l'utilisateur AD, vous n'avez pas besoin d'apporter des modifications à l'AD lui-même. Cependant, vous devez vous assurer que l'attribut n'est pas utilisé.

Pour vous assurer que l'attribut n'est pas utilisé, accédez à **ADSI** et sélectionnez utilisateur, cliquez avec le bouton droit de la souris sur l'utilisateur et faites défiler jusqu'à la liste d'attributs. Vous devez voir la valeur d'attribut pour **UserParameters** comme **non définie**. Cela indique que l'attribut n'est pas utilisé pour le moment.



Configuration de la messagerie OTP

La solution Email OTP se compose des deux parties suivantes :

- Enregistrement e-mail
- Validation d'e-mail

Enregistrement e-mail

Il existe deux façons d'enregistrer l'ID de messagerie secondaire d'un utilisateur :

1. Avec l'inscription KBA
2. Uniquement l'enregistrement de l'ID de messagerie - Cette méthode est prise en charge à partir de 13.0 build 61.x et plus ; et 12.1 build 58.x et supérieur.

Avec l'enregistrement KBA

Schéma de connexion d'enregistrement KBA

1. Accédez à **Sécurité > AAA — Trafic des applications > Schéma de connexion > Profils** et cliquez sur **Ajouter des journaux d'enregistrement KBASchema**.



2. Configurer le schéma d'authentification d'enregistrement KBA. Ce loginschema une fois généré affiche toutes les questions configurées pour l'utilisateur final pendant le processus d'enregistrement. Dans la section **Enregistrement par courrier électronique**, cochez l'option Enregistrer un autre e-mail pour enregistrer l'ID de messagerie secondaire de l'utilisateur.



3. Dans la section Enregistrement par courrier électronique, cochez **Enregistrer un autre e-mail** pour enregistrer un autre ID de messagerie.



Procédez à la configuration suivante à l'aide de l'invite de commande CLI une fois que le schéma d'enregistrement KBA susmentionné a été créé avec succès.

1. Lier le thème du portail et le certificat à VPN global.

```
bind authentication vserver authvs -portaltheme RfWebUI
bind vpn global -userDataEncryptionKey c1
<!--NeedCopy-->
```

> **Remarque :**
>
> La liaison de certificat précédente est requise pour chiffrer les données utilisateur (Q&R Ko et ID de messagerie secondaire enregistré) stockées dans l'attribut AD

2. Créez une stratégie d'authentification LDAP.

```
add authentication ldapAction ldap -serverIP 10.102.2.2 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samAccountName -secType SSL
add authentication Policy ldap -rule true -action ldap
<!--NeedCopy-->
```

3. Créez un Loginschema d'enregistrement KBA et un Label PolicyLabel.

```
add authentication loginSchema Registrationschema -
    authenticationSchema /nsconfig/loginschema/LoginSchema/
    KBARegistrationSchema.xml [This is the authentication schema
    created in the previous section.]
add authentication policylabel Registrationfactor -loginSchema
    Registrationschema
add authentication ldapAction ldap_registration -serverIP
    10.102.2.2 -serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -
    ldapBindDn administrator@aaatm-test.com -ldapBindDnPassword
```



```
    freebsd -ldapLoginName samAccountName -secType SSL  -
    KBAttribute userParameters -alternateEmailAttr userParameters
4 add authentication Policy ldap_registration -rule true -action
    ldap_registration
5 bind authentication policylabel Registrationfactor -policyName
    ldap_registration -priority 1 -gotoPriorityExpression NEXT
6 <!--NeedCopy-->
```

4. Lier la stratégie d'authentification au serveur virtuel d'authentification.

```
1 bind authentication vserver authvs - policy ldap -priority 1 -
    nextFactor Registrationfactor -gotoPriorityExpression NEXT
2 <!--NeedCopy-->
```

5. Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, vous devez voir l'écran de l'interface graphique suivante. Lors de l'accès via une URL par exemple, https://lb1.server.com/ vous êtes présenté avec une page de connexion initiale qui nécessite uniquement les informations d'identification de connexion LDAP.



6. Après vous être connecté avec des informations d'identification valides, la page d'enregistrement de l'utilisateur s'affiche comme suit.



7. Cliquez sur **Soumettre** pour que l'inscription des utilisateurs soit réussie et que la session soit créée.

Enregistrement de l'ID de courriel uniquement

Faites la configuration suivante à l'aide de l'invite de commande CLI après la création du schéma d'enregistrement KBA susmentionné :

1. Lier le thème du portail et le certificat à VPN global.

```
bind authentication vserver authvs -portaltheme RfWebUI
bind vpn global -userDataEncryptionKey c1
<!--NeedCopy-->
```

> **Remarque :**
>
> La liaison Cert précédente est requise pour chiffrer les données utilisateur (Q&A Ko et ID de courrier alternatif enregistré) stockées dans l'attribut AD.

2. Créez une stratégie d'authentification LDAP.

```
add authentication ldapAction ldap -serverIP 10.102.2.2 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samAccountName -secType SSL
add authentication Policy ldap -rule true -action ldap
<!--NeedCopy-->
```

3. Créez une stratégie d'authentification LDAP pour l'enregistrement par courrier électronique.


```
add authentication ldapAction ldap_email_registration -serverIP
    10.102.2.2 -serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -
    ldapBindDn administrator@aaatm-test.com -ldapBindDnPassword
    freebsd -ldapLoginName samAccountName -secType SSL -KBAttribute
     userParameters -alternateEmailAttr userParameters
add authentication Policy ldap_email_registration -rule true -
    action ldap_email_registration
<!--NeedCopy-->
```

4. Créez un Loginschema d'enregistrement par e-mail et un Label PolicyLabel.

```
add authentication loginSchema onlyEmailRegistration -
    authenticationSchema /nsconfig/loginschema/LoginSchema/
    AltEmailRegister.xml
add authentication policylabel email_Registration_factor -
    loginSchema onlyEmailRegistration
bind authentication policylabel email_Registration_factor -
    policyName ldap_email_registration -priority 1 -
    gotoPriorityExpression NEXT
<!--NeedCopy-->
```

5. Lier la stratégie d'authentification au serveur virtuel d'authentification.

```
bind authentication vserver authvs  - policy ldap -priority 1 -
    nextFactor email_Registration_factor -gotoPriorityExpression
    NEXT
<!--NeedCopy-->
```

6. Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, vous devez voir l'écran de l'interface graphique suivante. Lors de l'accès via URL par exemple, https://lb1.server.com/ une page de connexion initiale nécessite uniquement des informations d'identification LDAP suivies d'une autre page d'inscription par e-mail.





Validation d'e-mail

Procédez comme suit pour la validation des e-mails.

1. Lier le thème du portail et le certificat à VPN global

```
bind authentication vserver authvs -portaltheme RfWebUI
bind vpn global -userDataEncryptionKey c1
<!--NeedCopy-->
```

> **Remarque :**
>
> La liaison de certificat précédente est requise pour déchiffrer les données utilisateur (Q&R Ko et ID de messagerie secondaire enregistré) stockées dans l'attribut AD.

2. Créez une stratégie d'authentification LDAP. LDAP doit être un facteur antérieur au facteur de validation des e-mails car vous avez besoin de l'ID de messagerie électronique de l'utilisateur ou de l'ID de messagerie alternatif pour la validation de l'Email OTP

```
add authentication ldapAction ldap1 -serverIP 10.102.2.2 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -   ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samAccountName -secType SSL -KBAttribute
    userParameters -alternateEmailAttr userParameters
add authentication Policy ldap1 -rule true -action ldap1
<!--NeedCopy-->
```

3. Créer une stratégie d'authentification par courrier électronique

```
add authentication emailAction email -userName sqladmin@aaa.com -
    password freebsd-encrypted -encryptmethod ENCMTHD_3 -serverURL
    "smtps://10.2.3.3:25" -content "OTP is $code" -
    defaultAuthenticationGroup emailgrp -emailAddress "aaa.user.
    attribute("alternate_mail")"
add authentication Policy email -rule true  - action email
```



```
3 <!--NeedCopy-->
```

> Dans la commande mentionnée précédemment, l'**adresse e-mail** est l'autre utilisateur d'ID e-mail fourni lors de l'enregistrement KBA.

4. Créez une stratégie de validation Email OTP Label.

```
1 add authentication policylabel email_Validation_factor
2 bind authentication policylabel email_Validation_factor -
     policyName email -priority 1 -gotoPriorityExpression NEXT
3 <!--NeedCopy-->
```

5. Lier la stratégie d'authentification au serveur virtuel d'authentification

```
1 bind authentication vserver authvs - policy ldap1 -priority 1 -
     nextFactor email_Validation_factor -gotoPriorityExpression NEXT
2 <!--NeedCopy-->
```

6. Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, vous devez voir l'écran de l'interface graphique suivante pour la validation EMAIL OTP. Lors de l'accès via URL par exemple, https://lb1.server.com/ vous recevez une page de connexion initiale qui nécessite uniquement les informations d'identification de connexion LDAP suivies de la page E-MAIL OTP Validation.

> **Remarque :**
>
> Dans la stratégie LDAP, il est important de configurer AlternateEmailAttr pour pouvoir interroger l'identifiant de messagerie de l'utilisateur à partir de l'attribut AD.





Résolution des problèmes

Avant d'analyser le journal, il est préférable de définir le niveau du journal à déboguer comme suit.

```
set syslogparams -loglevel DEBUG
<!--NeedCopy-->
```

Enregistrement — Scénario réussi

Les entrées suivantes indiquent une inscription d'utilisateur réussie.

```
"ns_aaa_insert_hash_keyValue_entry key:kba_registered value:1"
Nov 14 23:35:51 <local0.debug> 10.102.229.76 11/14/2018:18:05:51 GMT
    0-PPE-1 : default SSLVPN Message 1588 0 :  "
    ns_aaa_insert_hash_keyValue_entry key:alternate_mail value:
    eyJ2ZXJzaW9uIjoiMSIsICJraWQiOiIxbk1oWjN0T2NjLVVvZUx6NDRwZFhxdS01dTA9IiwgImtleS
    ==.oKmvOalaOJ3a9z7BcGCSegNPMw=="

<!--NeedCopy-->
```

Enregistrement — Scénario échoué

Sur la page de connexion de l'utilisateur, le message d'erreur suivant s'affiche, « Impossible de compléter votre demande ». Cela indique que certkey à délimitée à VPN global pour chiffrer les données utilisateur est manquant.

```
Jul 31 08:51:46 <local0.info> 10.102.229.79 07/31/2020:03:21:4 6 GMT
    0-PPE-1 : default SSLVPN Message 696 0 :  "Encrypt UserData: No
    Encryption cert is bound to vpn global"
```



```
Jul 31 08:51:46 <local0.info> 10.102.229.79 07/31/2020:03:21:46 GMT  0-PPE-1 : default SSLVPN Message 697 0 :  "KBA Register: Alternate email id Encrypted blob length is ZERO aaauser"
<!--NeedCopy-->
```

Validation des e-mails — Scénario de réussite

Les entrées suivantes indiquent une validation Email OTP réussie.

```
"NFactor: Successfully completed email auth, nextfactor is pwd_reset"
<!--NeedCopy-->
```

Validation des e-mails — Scénario d'échec

Sur la page de connexion de l'utilisateur, le message d'erreur « Impossible de compléter votre demande » s'affiche. Cela indique que l'authentification basée sur la connexion n'est pas activée sur le serveur de messagerie et que la même chose doit être activée.

```
" /home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp [100]: void ThreadWorker_SendMailJob(SMTPJob*) 0-215: [POCO][JobID: 8]SMTP Configuration is Secure..
/home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp[108]: void ThreadWorker_SendMailJob(SMTPJob*) 0-215: [POCO][JobID: 8] First login succeeded
Wed Mar  4 17:16:28 2020
/home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/naaad.c[697]: main 0-0: timer 2 firing...
/home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp[127]: void ThreadWorker_SendMailJob(SMTPJob*) 0-0: [POCO-ERROR][JobID: 8] Poco SMTP Mail Dispatch  Failed. SMTP TYPE:1, SMTPException: Exception occurs. SMTP Exception: The mail service does not support LOGIN authentication: 250-smtprelay.citrix.com Hello [10.9.154.239]
250-SIZE 62914560
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-BINARYMIME
250 CHUNKING
<!--NeedCopy-->
```


Configuration de reCAPTCHA pour l'authentification nFactor

January 21, 2021

Citrix Gateway prend en charge une nouvelle action de première classe 'CaptChaAction' qui simplifie la configuration reCAPTCHA. Comme reCAPTCHA est un premier recours collectif, il peut être un facteur qui lui est propre. Vous pouvez injecter reCAPTCHA n'importe où dans le flux nFactor.

Auparavant, vous deviez écrire des stratégies WebAuth personnalisées avec des modifications à l'interface utilisateur RFWeb. Avec l'introduction de CaptChaAction, vous n'avez pas à modifier le JavaScript.

> **Important**
>
> Si reCAPTCHA est utilisé avec les champs nom d'utilisateur ou mot de passe dans le schéma, le bouton d'envoi est désactivé jusqu'à ce que reCAPTCHA soit rempli.

Configuration reCAPTCHA

La configuration reCAPTCHA comporte deux parties.

1. Configuration sur Google pour l'enregistrement de reCAPTCHA.
2. Configuration sur l'appliance Citrix ADC pour utiliser reCAPTCHA dans le cadre du flux de connexion.

Configuration reCAPTCHA sur Google

Enregistrez un domaine pour reCAPTCHA àhttps://www.google.com/recaptcha/admin.

1. Lorsque vous accédez à cette page, l'écran suivant apparaît.



> **Remarque**
>
> Utilisez reCAPTCHA v2 uniquement. Invisible reCAPTCHA est toujours en version bêta.

2. Après l'enregistrement d'un domaine, les « SiteKey » et « SecretKey » s'affichent.



> **Remarque**
>
> Les « SiteKey » et « SecretKey » sont grisés pour des raisons de sécurité. « SecretKey » doit

> être gardé en sécurité.

Configuration reCAPTCHA sur l'appliance Citrix ADC

La configuration reCAPTCHA sur l'appliance Citrix ADC peut être divisée en trois parties :

- Afficher l'écran reCaptcha
- Publier la réponse reCaptcha sur le serveur Google
- La configuration LDAP est le deuxième facteur pour l'ouverture de session utilisateur (facultatif)

Afficher l'écran reCaptcha

La personnalisation du formulaire de connexion se fait via le loginschema SingleAuthCaptcha.xml. Cette personnalisation est spécifiée au serveur virtuel d'authentification et est envoyée à l'interface utilisateur pour le rendu du formulaire de connexion. Le loginschema intégré, SingleAuthCaptcha.xml, se trouve dans le répertoire /NSConfig/LoginsChema/LoginsChema sur l'appliance Citrix ADC.

> **Important**
>
> - En fonction de votre cas d'utilisation et de différents schémas, vous pouvez modifier le schéma existant. Par exemple, si vous n'avez besoin que d'un facteur reCAPTCHA (sans nom d'utilisateur ni mot de passe) ou d'une double authentification avec reCAPTCHA.
> - Si des modifications personnalisées sont effectuées ou si le fichier est renommé, Citrix recommande de copier tous les LoginsChemas du répertoire /nsconfig/loginschema/loginschema vers le répertoire parent, /nsconfig/loginschema.

Pour configurer l'affichage de reCAPTCHA à l'aide de l'interface de ligne de commande

- `add authentication loginSchema singleauthcaptcha -authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml`
- `add authentication loginSchemaPolicy singleauthcaptcha -rule true -action singleauthcaptcha`
- `add authentication vserver auth SSL <IP> <Port>`
- `add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-key-file>`
- `bind ssl vserver auth -certkey vserver-cert`
- `bind authentication vserver auth -policy singleauthcaptcha -priority 5 -gotoPriorityExpression END`

Publier la réponse reCaptcha sur le serveur Google

Après avoir configuré le reCAPTCHA qui doit être affiché aux utilisateurs, les administrateurs publient la configuration au serveur Google pour vérifier la réponse reCAPTCHA du navigateur.

Pour vérifier la réponse reCAPTCHA à partir du navigateur

- `add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-from-google> -secretkey <secretkey-from-google>`
- `add authentication policy myrecaptcha -rule true -action myrecaptcha`
- `bind authentication vserver auth -policy myrecaptcha -priority 1`

Les commandes suivantes sont nécessaires pour configurer si l'authentification AD est souhaitée. Sinon, vous pouvez ignorer cette étape.

- `add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort 636 -ldapBase "cn=users,dc=aaatm,dc=com"-ldapBindDn adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup`
- `add authenticationpolicy ldap-new -rule true -action ldap-new`

La configuration LDAP est le deuxième facteur pour l'ouverture de session utilisateur (facultatif)

L'authentification LDAP se produit après reCAPTCHA, vous l'ajoutez au deuxième facteur.

- `add authentication policylabel second-factor`
- `bind authentication policylabel second-factor -policy ldap-new -priority 10`
- `bind authentication vserver auth -policy myrecaptcha -priority 1 -nextFactor second-factor`

L'administrateur doit ajouter des serveurs virtuels appropriés selon que le serveur virtuel d'équilibrage de charge ou l'appliance Citrix Gateway est utilisé pour l'accès. L'administrateur doit configurer la commande suivante si le serveur virtuel d'équilibrage de charge est requis :

- `add lb vserver lbtest HTTP <IP> <Port> -authentication ON -authenticationHost nssp.aaatm.com`

  nssp.aaatm.com — Résout à l'authentification du serveur virtuel.

Validation par l'utilisateur de reCAPTCHA

Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, vous devez voir les captures d'écran de l'interface utilisateur ci-dessous.

1. Une fois que le serveur virtuel d'authentification charge la page de connexion, l'écran d'ouverture de session s'affiche. L'**ouverture de session** est désactivée jusqu'à ce que reCAPTCHA soit terminé.



2. Sélectionnez Je ne suis pas une option de robot. Le widget reCAPTCHA s'affiche.



3. Vous naviguez à travers les séries d'images reCAPTCHA, avant l'affichage de la page de fin.
4. Entrez les informations d'identification AD, activez la case à cocher **Je ne suis pas un robot** et cliquez **sur Connexion** . Si l'authentification réussit, vous êtes redirigé vers la ressource souhaitée.



Remarques

- Si reCAPTCHA est utilisé avec l'authentification AD, le bouton Envoyer pour les informations d'identification est désactivé jusqu'à ce que reCAPTCHA soit terminé.
- Le reCAPTCHA se produit dans un facteur qui lui est propre. Par conséquent, toute validation ultérieure comme AD doit se produire dans le « nextfactor » de reCaptcha.

Configuration d'authentification, d'autorisation et d'audit pour les protocoles couramment utilisés

January 21, 2021

La configuration de l'appliance Citrix ADC pour l'authentification, l'autorisation et l'audit nécessite une configuration spécifique sur l'appliance Citrix ADC et les navigateurs des clients. La configuration varie selon le protocole utilisé pour l'authentification, l'autorisation et l'audit.

Pour plus d'informations sur la configuration de l'appliance Citrix ADC pour l'authentification Kerberos, reportez-vous à la section Gestion de l'authentification, de l'autorisation et de l'audit avec Kerberos/NTLM.

Gestion de l'authentification, de l'autorisation et de l'audit avec Kerberos/NTLM

January 21, 2021

Kerberos, un protocole d'authentification de réseau informatique, fournit une communication sécurisée sur Internet. Conçu principalement pour les applications client-serveur, il fournit une authentification mutuelle par laquelle le client et le serveur peuvent chacun garantir l'authenticité de l'autre. Kerberos utilise un tiers de confiance, appelé Key Distribution Center (KDC). Un KDC se compose d'un serveur d'authentification (AS), qui authentifie un utilisateur, et d'un serveur d'octroi de tickets (TGS).

Chaque entité du réseau (client ou serveur) possède une clé secrète qui n'est connue que de elle-même et du KDC. La connaissance de cette clé implique l'authenticité de l'entité. Pour la communication entre deux entités du réseau, le KDC génère une clé de session, appelée ticket Kerberos ou ticket de service. Le client demande au AS des informations d'identification pour un serveur spécifique. Le client reçoit alors un ticket, appelé Ticket d'octroi de tickets (TGT). Le client communique ensuite avec le TGS, en utilisant le TGT qu'il a reçu de l'AS pour prouver son identité, et demande un service. Si le client est admissible au service, le TGS émet un ticket Kerberos au client. Le client contacte ensuite le serveur hébergeant le service (appelé le serveur de service), en utilisant le ticket Kerberos pour prouver qu'il est autorisé à recevoir le service. Le ticket Kerberos a une durée de vie configurable. Le client s'authentifie avec l'AS une seule fois. S'il contacte le serveur physique plusieurs fois, il réutilise le ticket AS.

La figure suivante montre le fonctionnement de base du protocole Kerberos.

Figure 1. **Fonctionnement de Kerberos**



L'authentification Kerberos présente les avantages suivants :

- Authentification plus rapide. Lorsqu'un serveur physique obtient un ticket Kerberos d'un client, le serveur dispose de suffisamment d'informations pour authentifier le client directement. Il n'a pas besoin de contacter un Controller de domaine pour l'authentification du client, et donc le processus d'authentification est plus rapide.
- Authentification mutuelle. Lorsque le KDC émet un ticket Kerberos à un client et que le client utilise le ticket pour accéder à un service, seuls les serveurs authentifiés peuvent déchiffrer le ticket Kerberos. Si le serveur virtuel de l'appliance Citrix ADC est en mesure de déchiffrer le ticket Kerberos, vous pouvez conclure que le serveur virtuel et le client sont tous deux authentifiés. Ainsi, l'authentification du serveur se produit avec l'authentification du client.
- Connexion unique entre Windows et d'autres systèmes d'exploitation prenant en charge Kerberos.

L'authentification Kerberos peut présenter les inconvénients suivants :

- Kerberos a des délais stricts ; les horloges des hôtes concernés doivent être synchronisées avec l'horloge du serveur Kerberos pour s'assurer que l'authentification n'échoue pas. Vous pouvez atténuer cet inconvénient en utilisant les démons Network Time Protocol pour garder les horloges de l'hôte synchronisées. Les tickets Kerberos ont une période de disponibilité, que vous pouvez configurer.
- Kerberos a besoin que le serveur central soit disponible en continu. Lorsque le serveur Kerberos est en panne, personne ne peut ouvrir une session. Vous pouvez atténuer ce risque en utilisant plusieurs serveurs Kerberos et des mécanismes d'authentification de secours.
- Comme toute l'authentification est contrôlée par un KDC centralisé, tout compromis dans cette infrastructure, tel que le mot de passe de l'utilisateur pour un poste de travail local volé, peut permettre à un attaquant de se faire passer pour n'importe quel utilisateur. Vous pouvez atténuer ce risque dans une certaine mesure en utilisant uniquement un ordinateur de bureau ou un ordinateur portable en qui vous avez confiance, ou en appliquant la préauthentification au moyen d'un jeton matériel.

Pour utiliser l'authentification Kerberos, vous devez la configurer sur l'appliance Citrix ADC et sur chaque client.

Optimisation de l'authentification Kerberos lors de l'authentification, de l'autorisation et de l'audit

L'appliance Citrix ADC optimise et améliore désormais les performances du système lors de l'authentification Kerberos. Le démon d'authentification, d'autorisation et d'audit se souvient de la demande Kerberos en attente pour le même utilisateur afin d'éviter le chargement sur Key Distribution Center (KDC), ce qui évitera les demandes en double.

Comment Citrix ADC implémente Kerberos pour l'authentification client

January 21, 2021

> **Important**
>
> L'authentification Kerberos/NTLM est prise en charge uniquement dans la version NetScaler 9.3 nCore ou ultérieure, et elle peut être utilisée uniquement pour l'authentification, l'autorisation et l'audit des serveurs virtuels de gestion du trafic.

Citrix ADC gère les composants impliqués dans l'authentification Kerberos de la manière suivante :

Centre de distribution de clés (KDC)

Dans Windows 2000 Server ou versions ultérieures, le contrôleur de domaine et le contrôleur de domaine KDC font partie du serveur Windows. Si Windows Server est opérationnel et en cours d'exécution, il indique que le contrôleur de domaine et le contrôleur de domaine KDC sont configurés. Le KDC est également le serveur Active Directory.

> **Remarque**
>
> Toutes les interactions Kerberos sont validées avec le contrôleur de domaine Kerberos Windows.

Service d'authentification et négociation de protocole

Une appliance Citrix ADC prend en charge l'authentification Kerberos sur les serveurs virtuels d'authentification, d'autorisation et d'audit de gestion du trafic. Si l'authentification Kerberos échoue, Citrix ADC utilise l'authentification NTLM.

Par défaut, Windows 2000 Server et les versions ultérieures de Windows Server utilisent Kerberos pour l'authentification, l'autorisation et l'audit. Si vous créez une stratégie d'authentification avec NEGOTIATE comme type d'authentification, Citrix ADC tente d'utiliser le protocole Kerberos pour l'authentification, l'autorisation et l'audit et si le navigateur du client ne parvient pas à recevoir un ticket Kerberos, l'ADC Citrix utilise l'authentification NTLM. Ce processus est appelé négociation.

Le client peut ne pas recevoir de ticket Kerberos dans l'un des cas suivants :

- Kerberos n'est pas pris en charge sur le client.
- Kerberos n'est pas activé sur le client.
- Le client se trouve dans un domaine autre que celui du KDC.
- Le répertoire d'accès sur le KDC n'est pas accessible au client.

Pour l'authentification Kerberos/NTLM, Citrix ADC n'utilise pas les données présentes localement sur l'appliance Citrix ADC.

Autorisation

Le serveur virtuel de gestion du trafic peut être un serveur virtuel d'équilibrage de charge ou un serveur virtuel de commutation de contenu.

Audit

L'appliance Citrix ADC prend en charge l'audit de l'authentification Kerberos avec l'enregistrement d'audit suivant :

- Trail d'audit complet de l'activité de l'utilisateur final de gestion du trafic
- SYSLOG et enregistrement TCP hautes performances
- Trail d'audit complet des administrateurs système
- Tous les événements système
- Format de journal scriptable

Environnement pris en charge

L'authentification Kerberos n'a besoin d'aucun environnement spécifique sur Citrix ADC. Le client (navigateur) doit fournir la prise en charge de l'authentification Kerberos.

Haute disponibilité

Dans une configuration haute disponibilité, seul Citrix ADC actif rejoint le domaine. En cas de basculement sur incident, le démon Citrix ADC lwagent joint l'appliance Citrix ADC secondaire au domaine. Aucune configuration spécifique n'est requise pour cette fonctionnalité.

Processus d'authentification Kerberos

La figure suivante illustre un processus typique d'authentification Kerberos dans l'environnement Citrix ADC.

Figure 1. Processus d'authentification Kerberos sur Citrix ADC



L'authentification Kerberos se produit dans les étapes suivantes :

Le client s'authentifie auprès du KDC

1. L'appliance Citrix ADC reçoit une demande d'un client.
2. Le serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu) sur l'appliance Citrix ADC envoie un défi au client.
3. Pour répondre au défi, le client obtient un ticket Kerberos.
   - Le client envoie au serveur d'authentification du KDC une demande de ticket d'octroi de tickets (TGT) et reçoit le TGT. (Voir 3, 4 dans la figure, Processus d'authentification Kerberos.)
   - Le client envoie le TGT au serveur d'octroi de tickets du KDC et reçoit un ticket Kerberos. (Voir 5, 6 dans la figure, Processus d'authentification Kerberos.)

> **Remarque**
>
> Le processus d'authentification ci-dessus n'est pas nécessaire si le client dispose déjà d'un ticket Kerberos dont la durée de vie n'a pas expiré. En outre, les clients tels que les services Web, .NET ou J2EE, qui prennent en charge SPNEGO, obtiennent un ticket Kerberos pour le serveur cible,

> créent un jeton SPNEGO et insèrent le jeton dans l'en-tête HTTP lorsqu'ils envoient une requête HTTP. Ils ne passent pas par le processus d'authentification du client.

Le client demande un service.

1. Le client envoie le ticket Kerberos contenant le jeton SPNEGO et la requête HTTP au serveur virtuel de gestion du trafic sur le Citrix ADC. Le jeton SPNEGO a les données GSSAPI nécessaires.
2. L'appliance Citrix ADC établit un contexte de sécurité entre le client et le Citrix ADC. Si Citrix ADC ne peut pas accepter les données fournies dans le ticket Kerberos, le client est invité à obtenir un ticket différent. Ce cycle se répète jusqu'à ce que les données GSSAPI soient acceptables et que le contexte de sécurité soit établi. Le serveur virtuel de gestion du trafic sur Citrix ADC agit comme un proxy HTTP entre le client et le serveur physique.

L'**appliance Citrix ADC termine l'authentification.**

1. Une fois le contexte de sécurité terminé, le serveur virtuel de gestion du trafic valide le jeton SPNEGO.
2. À partir du jeton SPNEGO valide, le serveur virtuel extrait l'ID utilisateur et les informations d'identification GSS et les transmet au démon d'authentification.
3. Une authentification réussie termine l'authentification Kerberos.

Configuration de l'authentification kerberos sur l'appliance Citrix ADC

August 20, 2021

Cette rubrique fournit les étapes détaillées pour configurer l'authentification Kerberos sur l'appliance Citrix ADC à l'aide de l'interface de ligne de commande et de l'interface graphique.

Configuration de l'authentification Kerberos sur l'interface de ligne de commande

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit pour garantir l'authentification du trafic sur l'appliance.

   ns-cli-prompt> **activer la fonctionnalité ns** AAA

2. Ajoutez le fichier keytab à l'appliance Citrix ADC. Un fichier keytab est nécessaire pour déchiffrer le secret reçu du client lors de l'authentification Kerberos. Un seul fichier keytab contient des détails d'authentification pour tous les services liés au serveur virtuel de gestion du trafic sur l'appliance Citrix ADC.

   Générez d'abord le fichier keytab sur le serveur Active Directory, puis transférez-le à l'appliance Citrix ADC.

- Ouvrez une session sur le serveur Active Directory et ajoutez un utilisateur pour l'authentification Kerberos. Par exemple, pour ajouter un utilisateur nommé "Kerb-SVC-Account":

  net user Kerb-SVC-Account freebsd!@#456 /add

  > **Remarque**
  >
  > Dans la section **Propriétés de l'utilisateur**, assurez-vous que l'option « Modifier le mot de passe lors de la prochaine ouverture de session » n'est pas sélectionnée et que l'option « Mot de passe n'expire pas » est sélectionnée.

- Mappez le service HTTP à l'utilisateur ci-dessus et exportez le fichier keytab. Par exemple, exécutez la commande suivante sur le serveur Active Directory :

  ktpass /out keytabfile /princ HTTP/owa.newacp.com@NEWACP.COM /pass freebsd!@#456 /mapuser newacp\dummy /ptype KRB5_NT_PRINCIPAL

  > **Remarque**
  >
  > Vous pouvez mapper plusieurs services si l'authentification est requise pour plusieurs services. Si vous souhaitez mapper d'autres services, répétez la commande ci-dessus pour chaque service. Vous pouvez donner le même nom ou des noms différents pour le fichier de sortie.

- Transférez le fichier keytab vers l'appliance Citrix ADC à l'aide de la commande unix **ftp** ou de tout autre utilitaire de transfert de fichiers de votre choix.

3. L'appliance Citrix ADC doit obtenir l'adresse IP du Controller de domaine à partir du nom de domaine complet (FQDN). Par conséquent, Citrix recommande de configurer Citrix ADC avec un serveur DNS.

   ns-cli-prompt> **add dns nameserver** <ip-address>

   > **Remarque**
   >
   > Vous pouvez également ajouter des entrées d'hôte statiques ou utiliser tout autre moyen pour que l'appliance Citrix ADC puisse résoudre le nom de domaine complet du Controller de domaine en une adresse IP.

4. Configurez l'action d'authentification, puis associez-la à une stratégie d'authentification.

   - Configurez l'action de négociation.

     ns-cli-prompt **ajouter l'authentification Négocier l'action** <name><domain name>- domaine - Utilisateur du domaine <domain user name>- DomainUserPassWD <domain user password>- Groupe d'authentification par défaut <default authentication group>- keytab <string>- chemin NTLM <string>

Remarque : Pour la configuration de l'utilisateur du domaine et du nom de domaine, accédez au client et utilisez la commande klist comme illustré dans l'exemple suivant :

Client : nom d'utilisateur @ AAA.LOCAL

Serveur : http/OnPrem_IDP.AAA.Local @ AAA.LOCAL

ajout d'authentification Negotiate Action <name>- domaine <AAA.LOCAL>- DomainUser <HTTP/onprem_idp.aaa.local>

- Configurez la stratégie de négociation et associez l'action de négociation à cette stratégie.

  ns-cli-prompt> **add authentication negotiatePolicy** <name> <rule> <reqAction>

5. Créez un serveur virtuel d'authentification et associez la stratégie de négociation à celui-ci.
   - Créez un serveur virtuel d'authentification.

     ns-cli-prompt> **add authentication vserver** <name> SSL <ipAuthVserver> 443 -authenticationDomain <domainName>
   - Liez la stratégie de négociation au serveur virtuel d'authentification.

     ns-cli-prompt> **bind authentication vserver** <name> -policy <negotiatePolicyName>
6. Associez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu).

   ns-cli-prompt> **set lb vserver** <name> -authn401 ON -authnVsName <string>

   > **Remarque**
   >
   > Des configurations similaires peuvent également être effectuées sur le serveur virtuel de commutation de contenu.
7. Vérifiez les configurations en procédant comme suit :
   - Accédez au serveur virtuel de gestion du trafic à l'aide du nom de domaine complet. Par exemple, Sample
   - Affichez les détails de la session sur l'interface de ligne de commande.

     ns-cli-prompt> **show aaa session**

Configuration de l'authentification Kerberos sur l'interface graphique

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit.

   Accédez à **Système** > **Paramètres**, cliquez sur **Configurer les fonctionnalités de base** et activez la fonctionnalité d'authentification, d'autorisation et d'audit.
2. Ajoutez le fichier keytab comme détaillé à l'étape 2 de la procédure CLI mentionnée ci-dessus.

3. Ajoutez un serveur DNS.

   Accédez à **Gestion du trafic > DNS > Serveurs de noms**et spécifiez l'adresse IP du serveur DNS.

4. Configurez l'action et la stratégie **Négocier** .

   Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Stratégie**, puis créez une stratégie avec **Négocier**comme type d'action. Cliquez sur **ADD** pour créer un nouveau serveur de négociation d'authentification ou sur **Modifier** pour configurer les détails existants.

5. Liez la stratégie de négociation au serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**et associez la stratégie **Négocier**au serveur virtuel d'authentification.

6. Associez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu).

   Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et spécifiez les paramètres d'authentification appropriés.

   > **Remarque**
   >
   > Des configurations similaires peuvent également être effectuées sur le serveur virtuel de commutation de contenu.

7. Vérifiez les configurations décrites à l'étape 7 de la procédure CLI mentionnée ci-dessus.

Configurer l'authentification kerberos sur un client

January 21, 2021

La prise en charge de Kerberos doit être configurée sur le navigateur pour utiliser Kerberos pour l'authentification. Vous pouvez utiliser n'importe quel navigateur compatible Kerberos. Suivez les instructions pour configurer la prise en charge de Kerberos sur Internet Explorer et Mozilla Firefox. Pour les autres navigateurs, consultez la documentation du navigateur.

Pour configurer Internet Explorer pour l'authentification Kerberos

1. Dans le menu **Outils**, sélectionnez **Options Internet** .
2. Sous l'onglet **Sécurité**, cliquez sur **Intranet local**, puis sur **Sites** .
3. Dans la boîte de dialogue **Intranet local**, assurez-vous que l'option Détecter automatiquement le réseau intranet est sélectionnée, puis cliquez sur **Avancé** .

4. Dans la boîte de dialogue **Intranet local**, ajoutez les sites Web des domaines du serveur virtuel de gestion du trafic sur l'appliance Citrix ADC. Les sites spécifiés deviennent des sites intranet locaux.
5. Cliquez sur **Fermer** ou sur **OK** pour fermer les boîtes de dialogue.

Pour configurer Mozilla Firefox pour l'authentification Kerberos

1. Assurez-vous que Kerberos est correctement configuré sur votre ordinateur.
2. Tapez about:config dans la barre d'URL.
3. Dans la zone de texte du filtre, tapez network.negotiate.
4. Remplacez network.negotiate-auth.delegation-uris par le domaine que vous souhaitez ajouter.
5. Changez network.negotiate-auth.trusted-uris par le domaine que vous souhaitez ajouter.

> **Remarque :** Si vous exécutez Windows, vous devez également entrer sspi dans la zone de texte du filtre et changer l'option network.auth.use-sspi sur False.

Décharger l'authentification Kerberos des serveurs physiques

October 5, 2021

L'appliance Citrix ADC peut décharger les tâches d'authentification des serveurs. Au lieu que les serveurs physiques authentifient les demandes des clients, Citrix ADC authentifie toutes les demandes des clients avant de les transmettre à l'un des serveurs physiques qui lui sont liés. L'authentification de l'utilisateur est basée sur des jetons Active Directory.

Il n'y a pas d'authentification entre Citrix ADC et le serveur physique, et le déchargement de l'authentification est transparent pour les utilisateurs finaux. Après l'ouverture de session initiale sur un ordinateur Windows, l'utilisateur final n'a pas besoin de saisir d'informations d'authentification supplémentaires dans une fenêtre contextuelle ou sur une page d'ouverture de session.

Dans la version actuelle de l'appliance Citrix ADC, l'authentification Kerberos n'est disponible que pour les serveurs virtuels d'authentification, d'autorisation et d'audit de gestion du trafic. L'authentification Kerberos n'est pas prise en charge pour le VPN SSL dans l'appliance Citrix Gateway Advanced Edition ou pour la gestion de l'appliance Citrix ADC.

L'authentification Kerberos nécessite une configuration sur l'appliance Citrix ADC et sur les navigateurs clients.

Pour configurer l'authentification Kerberos sur l'appliance Citrix ADC

> **Remarque**
>
> Les mots de passe utilisés dans l'exemple de configuration suivant ne sont que des exemples et non les mots de passe de configuration réels.

1. Créez un compte utilisateur sur Active Directory. Lors de la création d'un compte utilisateur, vérifiez les options suivantes dans la section Propriétés de l'utilisateur :
   - Assurez-vous de ne pas sélectionner l'option Modifier le mot de passe lors de la prochaine connexion.
   - Assurez-vous de sélectionner l'option Le mot de passe n'expire pas.
2. Sur le serveur AD, à l'invite de commandes de l'interface de ligne de commande, tapez :
   - ktpass -princ HTTP/ kerberos.crete.lab.net@crete.lab.net -ptype KRB5_NT_PRINCIPAL -mapuser kerbuser@crete.lab.net -mapop set -pass <password> -out C:\kerbtabfile.txt

   > **Remarque**
   >
   > N'oubliez pas de taper la commande ci-dessus sur une seule ligne. La sortie de la commande ci-dessus est écrite dans le fichier C:\kerbtabfile.txt.
3. Téléchargez le fichier kerbtabfile.txt dans le répertoire /etc de l'appliance Citrix ADC à l'aide d'un client SCP (Secure Copy).
4. Exécutez la commande suivante pour ajouter un serveur DNS à l'appliance Citrix ADC.
   - add dns nameserver 1.2.3.4

   L'appliance Citrix ADC ne peut pas traiter les demandes Kerberos sans le serveur DNS. Assurez-vous d'utiliser le même serveur DNS que celui utilisé dans le domaine Microsoft Windows.
5. Basculez vers l'interface de ligne de commande de Citrix ADC.
6. Exécutez la commande suivante pour créer un serveur d'authentification Kerberos :
   - add authentication negotiateAction KerberosServer -domain "crete.lab.net" -domainUser kerbuser -domainUserPasswd <password> -keytab /var/mykcd.keytab

   > **Remarque**
   >
   > Si keytab n'est pas disponible, vous pouvez spécifier les paramètres suivants : domain, DomainUser et -DomainUserPasswd.
7. Exécutez la commande suivante pour créer une stratégie de négociation :
   - `add authentication negotiatePolicy Kerberos-Policy "REQ.IP.DESTIP == 192.168.17.200"KerberosServer<!--NeedCopy-->`
8. Exécutez la commande suivante pour créer un serveur virtuel d'authentification.
   - `add authentication vserver Kerb-Auth SSL 192.168.17.201 443 -AuthenticationDomain crete.lab.net<!--NeedCopy-->`

9. Exécutez la commande suivante pour lier la stratégie Kerberos au serveur virtuel d'authentification :

   - `bind authentication vserver Kerb-Auth -policy Kerberos-Policy -priority 100<!--NeedCopy-->`

10. Exécutez la commande suivante pour lier un certificat SSL au serveur virtuel d'authentification. Vous pouvez utiliser l'un des certificats de test, que vous pouvez installer à partir de l'appliance Citrix ADC GUI. Exécutez la commande suivante pour utiliser l'exemple de certificat ServerTestCert.

    - `bind ssl vserver Kerb-Auth -certkeyName ServerTestCert<!--NeedCopy-->`

11. Créez un serveur virtuel d'équilibrage de charge HTTP avec l'adresse IP 192.168.17.200.

    Assurez-vous de créer un serveur virtuel à partir de l'interface de ligne de commande pour les versions NetScaler 9.3 si elles sont antérieures à 9.3.47.8.

12. Exécutez la commande suivante pour configurer un serveur virtuel d'authentification :

    - `set lb vserver <name>-authn401 ON -authnVsName Kerb-Auth<!--NeedCopy-->`

13. Entrez l' exemple de nom d'hôte dans la barre d'adresse du navigateur Web.

    Le navigateur Web affiche une boîte de dialogue d'authentification car l'authentification Kerberos n'est pas configurée dans le navigateur.

    > **Remarque**
    >
    > L'authentification Kerberos nécessite une configuration spécifique sur le client. Assurez-vous que le client peut résoudre le nom d'hôte, ce qui entraîne la connexion du navigateur Web à un serveur virtuel HTTP.

14. Configurez Kerberos sur le navigateur Web de l'ordinateur client.

    - Pour la configuration sur Internet Explorer, reportez-vous à la section Configuration de l'authentification Internet Explorer pour Kerberos.
    - Pour la configuration sur Mozilla Firefox, reportez-vous à la section Configuration de l'authentification Internet Explorer pour Kerberos.

15. Vérifiez si vous pouvez accéder au serveur physique principal sans authentification.

Pour configurer l'authentification Internet Explorer pour Kerberos

1. Sélectionnez **Options Internet** dans le menu **Outils** .
2. Activez l'onglet **Sécurité** .
3. Sélectionnez **Intranet local dans** la section Sélectionner une zone pour afficher les paramètres de sécurité des modifications.

4. Cliquez sur **Sites**.
5. Cliquez sur **Avancé**.
6. Spécifiez l'URL, Exemple, puis cliquez sur **Ajouter**.
7. Redémarrez **Internet Explorer**.

Pour configurer l'authentification Mozilla Firefox pour Kerberos

1. Entrez about:config dans la barre d'adresse du navigateur.
2. Cliquez sur l'avertissement de non-responsabilité.
3. Tapez **Network.Negotiate-Auth.Trusted-URIS** dans la zone **Filtre** .
4. Double-cliquez sur **Network.Negotiate-Auth.Trusted-URIS.** Un exemple d'écran est présenté ci-dessous.



5. Dans la boîte de dialogue Saisir une valeur de chaîne, spécifiez www.crete.lab.net.
6. Redémarrez Firefox.

Types d'authentification unique

August 20, 2021

Les fonctionnalités d'authentification, d'autorisation et d'audit Citrix ADC prennent en charge les types d'authentification unique suivants.

- **authentification unique Citrix ADC kerberos : les appliances** Citrix ADC prennent désormais en charge l'authentification unique (SSO) à l'aide du protocole Kerberos 5. Les utilisateurs ouvrent une session sur un proxy, l'Application Delivery Controller (ADC), qui donne ensuite accès aux ressources protégées. Pour plus de détails, consultez Citrix ADC Kerberos Single Sign-on.
- **SSO pour l'authentification Basic, Digest et NTLM :** la configuration SSO (Single Sign-On) dans Citrix ADC et Citrix Gateway peut être activée au niveau global et également par niveau de trafic. Par défaut, la configuration SSO est OFF et un administrateur peut activer l'interface SSO

par trafic ou globalement. Du point de vue de la sécurité, Citrix recommande aux administrateurs de désactiver l'option SSO globalement et d'activer l'option par trafic. Cette amélioration vise à rendre la configuration SSO plus sécurisée en désactivant certains types de méthodes SSO globalement. Pour plus de détails, voir SSO pour l'authentification Basic, Digest et NTLM.

Citrix ADC kerberos authentification unique

January 21, 2021

Les appliances Citrix ADC prennent désormais en charge l'authentification unique (SSO) à l'aide du protocole Kerberos 5. Les utilisateurs ouvrent une session sur un proxy, l'Application Delivery Controller (ADC), qui donne ensuite accès aux ressources protégées.

L'implémentation de l'authentification unique Citrix ADC Kerberos nécessite le mot de passe de l'utilisateur pour les méthodes SSO qui reposent sur l'authentification de base, NTLM ou basée sur des formulaires. Le mot de passe de l'utilisateur n'est pas requis pour l'authentification unique Kerberos, bien que si l'authentification unique Kerberos échoue et que l'appliance Citrix ADC possède le mot de passe de l'utilisateur, elle utilise ce mot de passe pour tenter l'authentification unique NTLM.

Si le mot de passe de l'utilisateur est disponible, le compte KCD est configuré avec un domaine de compétence et qu'aucune information utilisateur déléguée n'est présente, le moteur d'authentification unique Citrix AD Kerberos emprunte l'identité de l'utilisateur pour obtenir l'accès aux ressources autorisées. L'emprunt d'identité est également appelé délégation sans contrainte.

Le moteur Citrix ADC Kerberos SSO peut également être configuré pour utiliser un compte délégué pour obtenir l'accès aux ressources protégées pour le compte de l'utilisateur. Cette configuration nécessite des informations d'identification utilisateur déléguées, un keytab ou un certificat utilisateur délégué et un certificat d'autorité de certification correspondant. La configuration qui utilise un compte délégué est appelée délégation contrainte.

Vue d'ensemble de Citrix ADC kerberos SSO

January 21, 2021

Pour utiliser la fonctionnalité d'authentification unique Citrix ADC Kerberos, les utilisateurs s'authentifient d'abord auprès de Kerberos ou d'un serveur d'authentification tiers pris en charge. Une fois authentifié, l'utilisateur demande l'accès à une application Web protégée. Le serveur Web répond par une demande de preuve que l'utilisateur est autorisé à accéder à cette application Web. Le navigateur de l'utilisateur contacte le serveur Kerberos, qui vérifie que l'utilisateur est autorisé à

accéder à cette ressource, puis fournit au navigateur de l'utilisateur un ticket de service qui fournit une preuve. Le navigateur envoie la demande de l'utilisateur au serveur d'applications Web avec le ticket de service joint. Le serveur d'applications Web vérifie le ticket de service, puis permet à l'utilisateur d'accéder à l'application.

La gestion du trafic d'authentification, d'autorisation et d'audit implémente ce processus comme illustré dans le diagramme suivant. Le diagramme illustre le flux d'informations via l'appliance Citrix ADC et la gestion de l'authentification, de l'autorisation et de l'audit du trafic, sur un réseau sécurisé avec authentification LDAP et autorisation Kerberos. Les environnements de gestion du trafic d'authentification, d'autorisation et d'audit qui utilisent d'autres types d'authentification ont essentiellement le même flux d'informations, bien qu'ils puissent différer dans certains détails.

Figure 1. Un réseau sécurisé avec LDAP et Kerberos



L'authentification, l'autorisation et l'audit de la gestion du trafic avec l'authentification et l'autorisation dans un environnement Kerberos nécessitent que les actions suivantes soient effectuées.

1. Le client envoie une demande de ressource au serveur virtuel de gestion du trafic sur l'appliance Citrix ADC.
2. Le serveur virtuel de gestion du trafic transmet la demande au serveur virtuel d'authentification, qui authentifie le client, puis transmet la demande au serveur virtuel de gestion du trafic.

3. Le serveur virtuel de gestion du trafic envoie la demande du client au serveur d'applications Web.
4. Le serveur d'applications Web répond au serveur virtuel de gestion du trafic avec un message 401 non autorisé qui demande l'authentification Kerberos, avec secours à l'authentification NTLM si le client ne prend pas en charge Kerberos.
5. Le serveur virtuel de gestion du trafic contacte le démon SSO Kerberos.
6. Le démon SSO Kerberos contacte le serveur Kerberos et obtient un ticket d'octroi de tickets (TGT) lui permettant de demander des tickets de service autorisant l'accès aux applications protégées.
7. Le démon Kerberos SSO obtient un ticket de service pour l'utilisateur et envoie ce ticket au serveur virtuel de gestion du trafic.
8. Le serveur virtuel de gestion du trafic attache le ticket à la demande initiale de l'utilisateur et renvoie la demande modifiée au serveur d'applications Web.
9. Le serveur d'applications Web répond avec un message 200 OK.

Ces étapes sont transparentes pour le client, qui envoie simplement une demande et reçoit la ressource demandée.

Intégration de Citrix ADC Kerberos SSO avec des méthodes d'authentification

Tous les mécanismes d'authentification, d'autorisation et d'audit de gestion du trafic prennent en charge Citrix ADC Kerberos SSO. La gestion du trafic d'authentification, d'autorisation et d'audit prend en charge le mécanisme d'authentification unique Kerberos avec les mécanismes d'authentification Kerberos, CAC (Smart Card) et SAML avec n'importe quelle forme d'authentification client vers l'appliance Citrix ADC. Il prend également en charge les mécanismes SSO HTTP-Basic, HTTP-Digest, Forms et NTLM (versions 1 et 2) si le client utilise l'authentification HTTP-Basic ou Forms pour se connecter à l'appliance Citrix ADC.

Le tableau suivant présente chaque méthode d'authentification côté client prise en charge et la méthode d'authentification côté serveur prise en charge pour cette méthode côté client.

Tableau 1. Méthodes d'authentification prises en charge

	Basique/Digest/NTLM	Délégation Kerberos contrainte	Emprunt d'identité d'un utilisateur
CAC (Smart Card) : à la couche LS SSL/T		X	X
À base de formulaires (LDAP/RADIUS/TACACS)	X	X	X

	Basique/Digest/NTLM	Délégation Kerberos contrainte	Emprunt d'identité d'un utilisateur
HTTP Basic (LDAP/RADIUS/TACACS)	X	X	X
Kerberos		X	
NT LM v1/v2		X	X
SAML		X	
SAML à deux facteurs	X	X	X
Certificat à deux facteurs	X	X	X

Configuration de l'authentification SSO Citrix ADC

October 5, 2021

Vous pouvez configurer Citrix ADC SSO pour qu'il fonctionne de deux manières : par emprunt d'identité ou par délégation. La connexion SSO par emprunt d'identité est une configuration plus simple que l'SSO par délégation, et est donc généralement préférable lorsque votre configuration le permet. Pour configurer l'authentification unique Citrix ADC par emprunt d'identité, vous devez disposer du nom d'utilisateur et du mot de passe de l'utilisateur.

Pour configurer l'authentification unique Citrix ADC par délégation, vous devez disposer des informations d'identification de l'utilisateur délégué dans l'un des formats suivants : le nom d'utilisateur et le mot de passe de l'utilisateur, la configuration de l'onglet clé qui inclut le nom d'utilisateur et un mot de passe chiffré, ou le certificat d'utilisateur délégué et le certificat d'autorité de certification correspondant.

Conditions préalables à la configuration de Citrix ADC SSO

Avant de configurer l'authentification unique Citrix ADC, votre appliance Citrix ADC doit être entièrement configurée pour gérer le trafic vers vos serveurs d'applications Web et l'authentification de ces serveurs. Par conséquent, vous devez configurer l'équilibrage de charge ou la commutation de contenu, puis l'authentification, l'autorisation et l'audit pour ces serveurs d'applications Web. Vous devez également vérifier le routage entre l'appliance, votre serveur LDAP et votre serveur Kerberos.

Si votre réseau n'est pas déjà configuré de cette manière, effectuez les tâches de configuration suivantes :

- Configurez un serveur et un service pour chaque serveur d'applications Web.
- Configurez un serveur virtuel de gestion du trafic pour gérer le trafic vers et depuis votre serveur d'applications Web.

Voici de brèves instructions et exemples pour effectuer chacune de ces tâches à partir de la ligne de commande Citrix ADC. Pour obtenir de l'aide supplémentaire, voir Configuration d'un serveur virtuel d'authentification.

> **Remarque**
>
> À partir de la version 13.1 de Citrix ADC, la traversée entre le domaine racine et le domaine d'arborescence est prise en charge pendant l'authentification SSO Kerberos pour le serveur principal à partir de l'appliance Citrix ADC.

Pour créer un serveur et un service à l'aide de l'interface de ligne de commande

Pour que Citrix ADC SSO obtienne un TGS (ticket de service) pour un service, soit le nom de domaine complet attribué à l'entité de serveur sur l'appliance Citrix ADC doit correspondre au nom de domaine complet du serveur d'applications Web, soit le nom de l'entité de serveur doit correspondre au nom NetBIOS du serveur d'applications Web. Vous pouvez adopter l'une des approches suivantes :

- Configurez l'entité de serveur Citrix ADC en spécifiant le nom de domaine complet du serveur d'applications Web.
- Configurez l'entité de serveur Citrix ADC en spécifiant l'adresse IP du serveur d'applications Web et attribuez à l'entité de serveur le même nom que le nom NetBIOS du serveur d'applications Web.

À l'invite de commandes, tapez les commandes suivantes :

```
1 - add server name <serverFQDN>
2
3 - add service name serverName serviceType port
4 <!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **ServerName**. Nom de l'appliance Citrix ADC à utiliser pour faire référence à ce serveur.
- Nom**de domaine complet du serveur**. Le nom de domaine complet du serveur. Si aucun domaine n'est attribué au serveur, utilisez l'adresse IP du serveur et assurez-vous que le nom de l'entité du serveur correspond au nom NetBIOS du serveur d'applications Web.
- **ServiceName**. Nom de l'appliance Citrix ADC à utiliser pour faire référence à ce service.
- **type**. Protocole utilisé par le service, HTTP ou MSSQLSVC.
- **port**. Port sur lequel le service écoute. Les services HTTP écoutent normalement sur le port 80. Les services HTTPS sécurisés écoutent normalement sur le port 443.

Exemple :

Les exemples suivants ajoutent des entrées de serveur et de service sur l'appliance Citrix ADC pour le serveur d'applications Web was1.example.com. Le premier exemple utilise le nom de domaine complet du serveur d'applications Web ; le second utilise l'adresse IP.

Pour ajouter le serveur et le service à l'aide du nom de domaine complet du serveur d'applications Web, was1.example.com, vous devez taper les commandes suivantes :

```
1 add server was1 was1.example.com
2 add service was1service was1 HTTP 80
3 <!--NeedCopy-->
```

Pour ajouter le serveur et le service à l'aide de l'adresse IP du serveur d'applications Web et du nom NetBIOS, où l'adresse IP du serveur d'applications Web est 10.237.64.87 et son nom NetBIOS est WAS1, vous devez taper les commandes suivantes :

```
1 add server WAS1 10.237.64.87
2 add service was1service WAS1 HTTP 8
3 <!--NeedCopy-->
```

Pour créer un serveur virtuel de gestion du trafic à l'aide de l'interface de ligne de commande

Le serveur virtuel de gestion du trafic gère le trafic entre le client et le serveur d'applications Web. Vous pouvez utiliser un serveur virtuel d'équilibrage de charge ou de commutation de contenu comme serveur de gestion du trafic. La configuration SSO est la même pour les deux types.

Pour créer un serveur virtuel d'équilibrage de charge, à l'invite de commandes, tapez la commande suivante :

```
1 add lb vserver <vserverName> <type> <IP> <port>
2 <!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **VServerName** : nom de l'appliance Citrix ADC à utiliser pour faire référence à ce serveur virtuel.
- **type** : protocole utilisé par le service, HTTP ou MSSQLSVC.
- **IP** : adresse IP attribuée au serveur virtuel. Il s'agit normalement d'une adresse IP non publique réservée par l'IANA sur votre réseau local.
- **port**—Port sur lequel le service écoute. Les services HTTP écoutent normalement sur le port 80. Les services HTTPS sécurisés écoutent normalement sur le port 443.

Exemple :

Pour ajouter un serveur virtuel d'équilibrage de charge appelé tmvserver1 à une configuration qui gère le trafic HTTP sur le port 80, en lui attribuant une adresse IP LAN 10.217.28.20, puis en liant le serveur virtuel d'équilibrage de charge au service wasservice1, vous devez taper les commandes suivantes :

```
add lb vserver tmvserver1 HTTP 10.217.28.20 80
bind lb vserver tmvserv1 wasservice1
<!--NeedCopy-->
```

Pour créer un serveur virtuel d'authentification à l'aide de l'interface de ligne de commande

Le serveur virtuel d'authentification gère le trafic d'authentification entre le client et le serveur d'authentification (LDAP). Pour créer un serveur virtuel d'authentification, à l'invite de commandes, tapez les commandes suivantes :

```
add authentication vserver <authvserverName> SSL <IP> 443
<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **AuthvServerName** : nom de l'appliance Citrix ADC à utiliser pour faire référence à ce serveur virtuel d'authentification. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), la livre (#), l'espace (), à (@), égal à (=), deux-points (:) et les caractères de soulignement. Peut être modifié après l'ajout du serveur virtuel d'authentification à l'aide de la commande rename authentication vserver.
- **IP** : adresse IP attribuée au serveur virtuel d'authentification. Comme pour le serveur virtuel de gestion du trafic, cette adresse est normalement une adresse IP non publique réservée par l'IANA sur votre réseau local.
- **domain** : domaine attribué au serveur virtuel. Il s'agit généralement du domaine de votre réseau. Il est habituel, bien que non obligatoire, d'entrer le domaine dans toutes les capitales lors de la configuration du serveur virtuel d'authentification.

Exemple :

Pour ajouter un serveur virtuel d'authentification appelé authverver1 à votre configuration et lui attribuer l'adresse IP LAN 10.217.28.21 et le domaine EXAMPLE.COM, vous devez taper les commandes suivantes :

```
add authentication vserver authvserver1 SSL 10.217.28.21 443
<!--NeedCopy-->
```


Pour configurer un serveur virtuel de gestion du trafic afin qu'il utilise un profil d'authentification

Le serveur virtuel d'authentification peut être configuré pour gérer l'authentification pour un seul domaine ou pour plusieurs domaines. S'il est configuré pour prendre en charge l'authentification pour plusieurs domaines, vous devez également spécifier le domaine pour Citrix ADC SSO en créant un profil d'authentification, puis en configurant le serveur virtuel de gestion du trafic pour utiliser ce profil d'authentification.

> **Remarque**
>
> Le serveur virtuel de gestion du trafic peut être un serveur virtuel d'équilibrage de charge (lb) ou de commutation de contenu (cs). Les instructions suivantes supposent que vous utilisez un serveur virtuel d'équilibrage de charge. Pour configurer un serveur virtuel de commutation de contenu, il suffit de remplacer
> set cs vserver par set lb vserver. Sinon, la procédure est la même.

Pour créer le profil d'authentification, puis le configurer sur un serveur virtuel de gestion du trafic, tapez les commandes suivantes :

```
-  add authentication authnProfile <authnProfileName> {
 -authvserverName <string> }
  {
 -authenticationHost <string> }
  {
 -authenticationDomain <string> }

-  set lb vserver <vserverName> -authnProfile <authnprofileName>
<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **AuthnProfileName** : nom du profil d'authentification. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et doit comprendre de un à trente et un caractères alphanumériques ou un trait d'union (-), un point (.) livre (#), espace (), à (@), égal à (=), deux-points (:) et caractères de soulignement.
- **AuthvServerName** : nom du serveur virtuel d'authentification utilisé par ce profil pour l'authentification.
- **AuthenticationHost** : nom d'hôte du serveur virtuel d'authentification.
- **AuthenticationDomain** : domaine pour lequel Citrix ADC SSO gère l'authentification. Requis si le serveur virtuel d'authentification effectue l'authentification pour plusieurs domaines, de sorte que le domaine approprié soit inclus lorsque l'appliance Citrix ADC définit le cookie de serveur virtuel de gestion du trafic.

Exemple :

Pour créer un profil d'authentification nommé AuthnProfile1 pour l'authentification du domaine example.com et pour configurer le serveur virtuel d'équilibrage de charge vserver1 pour utiliser le profil d'authentification AuthnProfile1, tapez les commandes suivantes :

```
1 add authentication authnProfile authnProfile1 -authnvsName
     authvsesrver1
2       -authenticationHost authvsesrver1 -authenticationDomain example.
           com
3 set lb vserver vserver1 -authnProfile authnProfile1
4 <!--NeedCopy-->
```

Configuration de SSO

August 20, 2021

La configuration de l'authentification SSO Citrix ADC pour s'authentifier par emprunt d'identité est plus simple que la configuration de l'authentification SSO pour s'authentifier par délégation, et est donc préférable lorsque votre configuration le permet. Vous créez un compte KCD. Vous pouvez utiliser le mot de passe de l'utilisateur.

Si vous ne disposez pas du mot de passe de l'utilisateur, vous pouvez configurer l'authentification unique Citrix ADC pour qu'elle s'authentifie par délégation. Bien que plus complexe que la configuration de l'authentification SSO pour s'authentifier par emprunt d'identité, la méthode de délégation offre une flexibilité dans la mesure où les informations d'identification d'un utilisateur peuvent ne pas être disponibles pour l'appliance Citrix ADC en toutes circonstances.

Pour l'emprunt d'identité ou la délégation, vous devez également activer l'authentification intégrée sur le serveur d'applications Web.

Activer l'authentification intégrée sur le serveur d'applications Web

Pour configurer l'authentification unique Citrix ADC Kerberos sur chaque serveur d'applications Web géré par Kerberos SSO, utilisez l'interface de configuration sur ce serveur pour configurer le serveur pour qu'il requiert une authentification. Sélectionnez l'authentification Kerberos (négocier) par préférence, avec une solution de secours NTLM pour les clients qui ne prennent pas en charge Kerberos.

Voici les instructions pour configurer Microsoft Internet Information Server (IIS) pour exiger l'authentification. Si votre serveur d'applications Web utilise un logiciel autre que IIS, consultez la documentation de ce logiciel de serveur Web pour obtenir des instructions.

Pour configurer Microsoft IIS pour utiliser l'authentification intégrée

1. Connectez-vous au serveur IIS et ouvrez **Internet Information Services Manager.**
2. Sélectionnez le site Web pour lequel vous souhaitez activer l'authentification intégrée. Pour activer l'authentification intégrée pour tous les serveurs Web IIS gérés par IISM, configurez les paramètres d'authentification pour le site Web par défaut. Pour activer l'authentification intégrée pour des services individuels (tels que Exchange, Exadmin, ExchWeb et Public), configurez ces paramètres d'authentification pour chaque service individuellement.
3. Ouvrez la boîte de dialogue **Propriétés** du site Web par défaut ou du service individuel, puis cliquez sur l'onglet **Sécurité d'annuaire**.
4. En regard de **l'authentification** et du **contrôle d'accès**, sélectionnez **Modifier.**
5. Désactivez l'accès anonyme.
6. Activer l'authentification Windows intégrée (uniquement). L'activation de l'authentification Windows intégrée doit automatiquement définir la négociation de protocole pour le serveur Web sur Négocier, NTLM, qui spécifie l'authentification Kerberos avec repli vers NTLM pour les périphériques non compatibles Kerberos. Si cette option n'est pas automatiquement sélectionnée, définissez manuellement la négociation de protocole sur Négocier, NTLM.

Configurer l'identité SSO par emprunt d'identité

Vous pouvez configurer le compte KCD pour Citrix ADC SSO par emprunt d'identité. Dans cette configuration, l'appliance Citrix ADC obtient le nom d'utilisateur et le mot de passe de l'utilisateur lorsque l'utilisateur s'authentifie auprès du serveur d'authentification et utilise ces informations d'identification pour emprunter l'identité de l'utilisateur afin d'obtenir un ticket d'octroi de tickets (TGT). Si le nom de l'utilisateur est au format UPN, l'appliance obtient le domaine de l'utilisateur auprès de l'UPN. Sinon, il obtient le nom et le domaine de l'utilisateur en l'extrayant à partir du domaine SSO utilisé lors de l'authentification initiale, ou du profil de session.

> **Remarque**
>
> Vous ne pouvez pas ajouter un nom d'utilisateur avec domaine si le nom d'utilisateur est déjà ajouté sans domaine. Si le nom d'utilisateur avec domaine est ajouté d'abord suivi du même nom d'utilisateur sans domaine, l'appliance Citrix ADC ajoute le nom d'utilisateur à la liste des utilisateurs.

Lors de la configuration du compte KCD, vous devez définir le paramètre realm sur le domaine du service auquel l'utilisateur accède. Le même domaine est également utilisé comme domaine de domaine de l'utilisateur si celui-ci ne peut pas être obtenu à partir de l'authentification avec l'appliance Citrix ADC ou du profil de session.

Pour créer le compte KCD pour SSO par emprunt d'identité avec un mot de passe

À l'invite de commandes, tapez la commande suivante :

```
add aaa kcdaccount <accountname> -realmStr <realm>

<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **accountname**. Nom du compte KCD.
- **realm**. Domaine attribué à SSO Citrix ADC.

Exemple

Pour ajouter un compte KCD nommé kcdccount1 et utiliser le keytab nommé kcdvserver.keytab, tapez la commande suivante :

```
add aaa kcdAccount kcdaccount1 -keytab kcdvserver.keytab

<!--NeedCopy-->
```

Pour plus d'informations sur la configuration de l'usurpation d'identité Kerberos via l'interface graphique Citrix ADC, consultez le support Citrix.

Configurer l'authentification SSO par délégation

Pour configurer SSO par délégation, vous devez effectuer les tâches suivantes :

- Si vous configurez la délégation par certificat utilisateur délégué, installez les certificats d'autorité de certification correspondants sur l'appliance Citrix ADC et ajoutez-les à la configuration de Citrix ADC.
- Créez le compte KCD sur l'appliance. L'appliance utilise ce compte pour obtenir des tickets de service pour vos applications protégées.
- Configurez le serveur Active Directory.

> **Remarque**
>
> Pour plus d'informations sur la création d'un compte KCD et la configuration sur l'appliance NetScaler, reportez-vous aux rubriques suivantes :
>
> - Gestion de l'authentification, de l'autorisation et de l'audit avec Kerberos/NTLM

- Comment Citrix ADC implémente Kerberos pour l'authentification client
- Configuration de l'authentification kerberos sur l'appliance Citrix ADC

Installation du certificat d'autorité de certification client sur l'appliance Citrix ADC

Si vous configurez l'authentification SSO Citrix ADC avec un certificat client, vous devez copier le certificat d'autorité de certification correspondant pour le domaine de certificat client (le certificat d'autorité de certification client) vers l'appliance Citrix ADC, puis installer le certificat d'autorité de certification. Pour copier le certificat de l'autorité de certification client, utilisez le programme de transfert de fichiers de votre choix pour transférer le certificat et le fichier de clé privée vers l'appliance Citrix ADC et stocker les fichiers dans /nsconfig/ssl.

Pour installer le certificat d'autorité de certification client sur l'appliance Citrix ADC

À l'invite de commandes, tapez la commande suivante :

```
add ssl certKey <certkeyName> -cert <cert> [(-key <key> [-password]) |
   -fipsKey <fipsKey>][-inform ( DER | PEM )][-expiryMonitor ( ENABLED
   | DISABLED | UNSET ) [-notificationPeriod <positive_integer>]] [-
   bundle ( YES | NO )]

<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **certkeyName**. Nom du certificat d'autorité de certification client. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et doit être composé de un à trente et un caractères. Les caractères autorisés comprennent les caractères alphanumériques ASCII, soulignement, hachage (#), point (.), espace, deux-points (:), at (@), égal (=) et tiret (-). Ne peut pas être modifié après la création de la paire de clés de certificat. Si le nom comporte un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « mon cert » ou « mon cert »).
- **Cert**. Nom du chemin d'accès complet et nom du fichier de certificat X509 utilisé pour former la paire de clés de certificat. Le fichier de certificat doit être stocké sur l'appliance Citrix ADC, dans le répertoire /nsconfig/ssl/.
- **key**. Nom du chemin d'accès complet et nom du fichier contenant la clé privée du fichier de certificat X509. Le fichier de clé doit être stocké sur l'appliance Citrix ADC dans le répertoire /nsconfig/ssl/.
- **mot de passe**. Si une clé privée est spécifiée, la phrase secrète utilisée pour chiffrer la clé privée. Utilisez cette option pour charger des clés privées chiffrées au format PEM.

- **fipsKey**. Nom de la clé FIPS créée dans le Hardware Security Module (HSM) d'une appliance FIPS ou d'une clé importée dans le HSM.

  > **Remarque**
  >
  > Vous pouvez spécifier une clé ou une clé FIPSKey, mais pas les deux.

- **inform**. Format du certificat et des fichiers de clé privée, PEM ou DER.
- **passplain**. Expression de passage utilisée pour chiffrer la clé privée. Obligatoire lors de l'ajout d'une clé privée chiffrée au format PEM.
- **expiryMonitor**. Configurez l'appliance Citrix ADC pour émettre une alerte lorsque le certificat est sur le point d'expirer. Valeurs possibles : ENABLED, DISABLED, UNSET.
- **notificationPeriod**. Si ExpiryMonitor est activé, nombre de jours avant l'expiration du certificat pour émettre une alerte.
- **bundle**. Analysez la chaîne de certificats en tant que fichier unique après avoir lié le certificat du serveur au certificat de son émetteur dans le fichier. Valeurs possibles : OUI, NON.

Exemple

L'exemple suivant montre comment ajouter le certificat utilisateur délégué spécifié customer-cert.pem à la configuration de Citrix ADC avec la clé customer-key.pem, puis définir le mot de passe, le format du certificat, le moniteur d'expiration et la période de notification.

Pour ajouter le certificat utilisateur délégué, tapez les commandes suivantes :

```
1 add ssl certKey customer -cert "/nsconfig/ssl/customer-cert.pem"
2 -key "/nsconfig/ssl/customer-key.pem" -password "dontUseDefaultPWs!"
3 -inform PEM -expiryMonitor ENABLED [-notificationPeriod 14]
4
5 <!--NeedCopy-->
```

Création du compte KCD

Si vous configurez l'authentification unique Citrix ADC par délégation, vous pouvez configurer le compte KCD pour qu'il utilise le nom d'ouverture de session et le mot de passe de l'utilisateur, pour utiliser le nom d'ouverture de session et l'onglet keytab de l'utilisateur, ou pour utiliser le certificat client de l'utilisateur. Si vous configurez l'authentification unique avec un nom d'utilisateur et un mot de passe, l'appliance Citrix ADC utilise le compte d'utilisateur délégué pour obtenir un ticket d'octroi de tickets (TGT), puis utilise le TGT pour obtenir des tickets de service pour les services spécifiques demandés par chaque utilisateur. Si vous configurez l'authentification SSO avec le fichier keytab, l'appliance Citrix ADC utilise les informations relatives au compte d'utilisateur délégué et à l'onglet keytab. Si vous configurez l'authentification SSO avec un certificat utilisateur délégué, l'appliance Citrix ADC utilise le certificat utilisateur délégué.

Pour créer le compte KCD pour SSO par délégation avec un mot de passe

À l'invite de commandes, tapez les commandes suivantes :

```
add aaa kcdAccount <kcdAccount> {
 -keytab <string> }
  {
 -realmStr <string> }
  {
 -delegatedUser <string> }
  {
 -kcdPassword  }
  {
 -usercert <string> }
  {
 -cacert <string> }
  [-userRealm <string>]
[-enterpriseRealm <string>] [-serviceSPN <string>]
<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **kcdAccount** - Un nom pour le compte KCD.Ceci est un argument obligatoire. Longueur maximale : 31
- **keytab** - Chemin d'accès au fichier keytab. Si spécifié d'autres paramètres dans cette commande n'ont pas besoin d'être donnés. Longueur maximale : 127
- **realmStr** - Le royaume de Kerberos. Longueur maximale : 255
- **delegatedUser** - Nom d'utilisateur qui peut effectuer la délégation contrainte kerberos. Longueur maximale : 255
- **kcdPassword - Mot** de passe pour l'utilisateur délégué. Longueur maximale : 31
- **usercert** - SSL Cert (y compris la clé privée) pour l'utilisateur délégué. Longueur maximale : 255
- **cacert** - CA Cert pour UserCert ou lorsque vous faites PKINIT backchannel. Longueur maximale : 255
- **userRealm** - Royaume de l'utilisateur. Longueur maximale : 255
- **enterpriseRealm** - Enterprise Realm de l'utilisateur. Cela ne doit être donné que dans certains déploiements KDC où KDC attend un nom d'utilisateur Enterprise au lieu de Nom principal. Longueur maximale : 255
- **serviceSPN** - Service SPN. Lorsqu'il est spécifié, cela sera utilisé pour récupérer les tickets kerberos. Si ce n'est pas spécifié, Citrix ADC construira le SPN à l'aide du service fqdn. Longueur maximale : 255

Exemple (format UPN)

Pour ajouter un compte KCD nommé kcdaccount1 à la configuration de l'appliance Citrix ADC avec un mot de passe de password1 et un domaine d'EXAMPLE.COM, en spécifiant le compte utilisateur délégué au format UPN (en tant que root), tapez les commandes suivantes :

```
add aaa kcdaccount kcdaccount1  - delegatedUser root
-kcdPassword password1 -realmStr EXAMPLE.COM

<!--NeedCopy-->
```

Exemple (format SPN)

Pour ajouter un compte KCD nommé kcdaccount1 à la configuration de l'appliance Citrix ADC avec un mot de passe de password1 et un domaine d'EXAMPLE.COM, en spécifiant le compte d'utilisateur délégué au format SPN, tapez les commandes suivantes :

```
add aaa kcdAccount kcdaccount1 -realmStr EXAMPLE.COM
-delegatedUser "host/kcdvserver.example.com" -kcdPassword password1

<!--NeedCopy-->
```

Création du compte KCD pour SSO par délégation avec un keytab

Si vous prévoyez d'utiliser un fichier keytab pour l'authentification, commencez par créer l'onglet keytab. Vous pouvez créer manuellement le fichier keytab en vous connectant au serveur AD et en utilisant l'utilitaire ktpass, ou vous pouvez utiliser l'utilitaire de configuration Citrix ADC pour créer un script batch, puis exécuter ce script sur le serveur AD pour générer le fichier keytab. Ensuite, utilisez FTP ou un autre programme de transfert de fichiers pour transférer le fichier keytab vers l'appliance Citrix ADC et le placer dans le répertoire /nsconfig/krb. Enfin, configurez le compte KCD pour Citrix ADC SSO par délégation et indiquez le chemin d'accès et le nom de fichier du fichier keytab à l'appliance Citrix ADC.

Pour créer manuellement le fichier keytab

Ouvrez une session sur la ligne de commande du serveur AD et, à l'invite de commandes, tapez la commande suivante :

"'ktpass princ ptype KRB5_NT_PRINCIPAL mapuser pass -out

```
Pour les variables, remplacez les valeurs suivantes :

-  **SPN**. Nom principal de service du compte de service KCD.
-  **DOMAIN**. Domaine du serveur Active Directory.
```



```
- **username**. Nom d'utilisateur du compte KSA.
- **mot de passe**. Mot de passe du compte KSA.
- **path**. Nom du chemin d'accés complet du répertoire dans lequel stocker le fichier keytab une fois qu'il est généré.

##### Pour utiliser l'utilitaire de configuration Citrix ADC pour créer un script pour générer le fichier keytab

1. Accédez à **Sécurité > AAA - Trafic des applications.**
1. Dans le volet de données, sous **Délégation contrainte Kerberos**, cliquez sur Fichier **batch**pour générer l'onglet Keytab.
1. Dans la boîte de dialogue **Générer KCD (Kerberos Constrained Délégation) Keytab Script**, définissez les paramétres suivants :
   - **Domain User Name**. Nom d'utilisateur du compte KSA.
   - **Domain Password**. Mot de passe du compte KSA.
   - **Service Principal**. Nom principal de service pour le KSA.
   - **Output File Name**. Chemin d'accés complet et nom de fichier vers lesquels enregistrer le fichier keytab sur le serveur AD.
1. Désactivez la case à cocher **Créer un compte d'utilisateur de domaine** .
1. Cliquez sur **Générer un script**.
1. Ouvrez une session sur le serveur Active Directory et ouvrez une fenêtre de ligne de commande.
1. Copiez le script à partir de la fenêtre **Script généré** et collez-le directement dans la fenêtre de ligne de commande du serveur Active Directory. L'onglet keytab est généré et stocké dans le répertoire sous le nom de fichier que vous avez spécifié comme **Nom de fichier de sortie**.
1. Utilisez l'utilitaire de transfert de fichiers de votre choix pour copier le fichier keytab du serveur Active Directory vers l'appliance Citrix ADC et le placer dans le répertoire /nsconfig/krb.

##### Pour créer le compte KCD

À l'invite de commandes, tapez la commande suivante :
```

add aaa kcdaccount –keytab

```
Exemple

Pour ajouter un compte KCD nommé kcdccount1 et utiliser le keytab nommé kcdvserver.keytab, tapez les commandes suivantes :
```

add aaa kcdaccount kcdaccount1 –keytab kcdvserver.keytab


```
#### Pour créer le compte KCD pour SSO par délégation avec un
    certificat d'utilisateur délégué

À l'invite de commandes, tapez la commande suivante :
```

add aaa kcdaccount -realmStr -delegatedUser -usercert -cacert

```
Pour les variables, remplacez les valeurs suivantes :

- **accountname**. Un nom pour le compte KCD.
- **realmStr**. Domaine du compte KCD, généralement le domaine pour
    lequel l'authentification SSO est configurée.
- **delegatedUser**. Nom d'utilisateur délégué, au format SPN.
- **usercert**. Chemin d'accés complet et nom du fichier de certificat
     utilisateur délégué sur l'appliance Citrix ADC. Le certificat
    utilisateur délégué doit contenir à la fois le certificat client et
    la clé privée, et doit être au format PEM. Si vous utilisez l'
    authentification par carte à puce, vous devrez peut-être créer un
    modéle de certificat de carte à puce pour autoriser l'importation de
     certificats avec la clé privée.
- **cacert**. Chemin d'accés complet et nom du fichier de certificat d
    'autorité de certification sur l'appliance Citrix ADC.

Exemple

Pour ajouter un compte KCD nommé kcdccount1 et utiliser le keytab nommé
     kcdvserver.keytab, tapez la commande suivante :
```

add aaa kcdaccount kcdaccount1 -realmStr EXAMPLE.COM
-delegatedUser “host/kcdvserver.example.com” -usercert /certs/usercert
-cacert /cacerts/cacert

“‘

Configuration d’Active Directory pour Citrix ADC SSO

Lorsque vous configurez SSO par délégation, en plus de créer le KCDAccount sur l’appliance Citrix ADC, vous devez également créer un compte Kerberos Service (KSA) correspondant sur votre serveur Active Directory LDAP et configurer le serveur pour SSO. Pour créer le KSA, utilisez le processus de création de compte sur le serveur Active Directory. Pour configurer l’authentification unique sur le serveur Active Directory, ouvrez la fenêtre des propriétés de l’authentification de base de données. Dans l’onglet **Délégation**, activez les options suivantes : Faites confiance à cet utilisateur pour la délégation aux services spécifiés uniquement et Utiliser n’importe quel protocole d’authentification. (L’option Ker-

beros uniquement ne fonctionne pas, car elle n'active pas la transition de protocole ou la délégation contrainte.) Enfin, ajoutez les services que Citrix ADC SSO gère.

> **Remarque**
>
> Si l'onglet Délégation n'est pas visible dans la boîte de dialogue Propriétés du compte KSA, avant de pouvoir configurer le KSA comme décrit, vous devez utiliser l'outil de ligne de commande Microsoft
> setspn pour configurer le serveur Active Directory afin que l'onglet soit visible.

Pour configurer la délégation pour le compte de service Kerberos

1. Dans la boîte de dialogue de configuration du compte LDAP pour le compte de service Kerberos que vous avez créé, cliquez sur l'onglet **Délégation** .
2. Choisissez « Faire confiance à cet utilisateur pour la délégation aux services spécifiés uniquement ».
3. Sous « Faire confiance à cet utilisateur pour la délégation aux services spécifiés uniquement », choisissez « Utiliser n'importe quel protocole d'authentification ».
4. Sous « Services auxquels ce compte peut présenter des informations d'identification déléguées », cliquez sur **Ajouter.**
5. Dans la boîte de dialogue **Ajouter des services**, cliquez sur **Utilisateurs**ou **Ordinateurs**, choisissez le serveur qui héberge les ressources à affecter au compte de service, puis cliquez sur **OK**.

   > **Remarque**
   >
   > ```
   > 1 - La délégation contrainte ne prend pas en charge les
   >     services hébergés dans des domaines autres que le domaine
   >     attribué au compte, même si Kerberos peut avoir une
   >     relation d'approbation avec d'autres domaines.
   > ```
   >
   > - Utilisez la commande suivante pour créer le setspn si un nouvel utilisateur est créé dans Active Directory : setspn -A host/kcdvserver.example.com examplekcdtest

6. Dans la boîte de dialogue **Ajouter des services**, dans la liste Services disponibles, choisit les services affectés au compte de service. L'authentification SSO Citrix ADC prend en charge les services HTTP et MSSQLSVC.
7. Cliquez sur **OK.**

Points à noter lorsque les chiffrements avancés sont utilisés pour configurer le compte KCD

- **Exemple de configuration lorsque keytab est utilisé :** add kcdaccount lbvs_keytab_aes256 -keytab “/nsconfig/krb/kcd2_aes256.keytab”
- **Utilisez la commande suivante lorsque keytab a plusieurs types de chiffrement.** La commande capture en outre les paramètres utilisateur du domaine : add kcdaccount lbvs_keytab_aes256 -keytab “/nsconfig/krb/kcd2_aes256.keytab” –domainUser “HTTP/lbvs.aaa.local”
- **Utilisez les commandes suivantes lorsque des informations d’identification utilisateur sont utilisées :** add kcdaccount kslb2_user -realmStr AAA.LOCAL -delegatedUser lbvs -kcdPassword <password>
- Assurez-vous que les informations **DomainUser** correctes sont fournies. Vous pouvez rechercher le nom d’ouverture de session de l’utilisateur dans AD.

Générer le script keytab KCD

January 21, 2021

La boîte de dialogue KCD Keytab Script génère le script keytab, qui à son tour génère le fichier keytab nécessaire pour configurer KCD sur Citrix ADC.

Pour générer le script keytab KCD à l’aide de l’utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications.**
2. Dans le volet d’informations, sous **Délégation contrainte Kerberos**, cliquez sur Fichier batch pour générer l’onglet keytab.
3. Dans la boîte de dialogue Générer KCD (Kerberos Constrained Délégation) **Keytab Script**, remplissez les champs comme décrit ci-dessous.
   - **Nom d’utilisateur du domaine :** nom de l’utilisateur du domaine.
   - **Mot de passe du domaine :** mot de passe de l’utilisateur du domaine.
   - **Principal de service :** Le principal de service.
   - **Nom du fichier de sortie : nom** de fichier pour le fichier de script KCD.
   - **Créer un compte d’utilisateur de domaine :** cochez cette case pour créer le compte d’utilisateur de domaine spécifié.
4. Cliquez sur **Générer un script** pour générer le script. Le script est généré et apparaît dans la zone de texte **Script généré** sous le bouton **Générer un script** .
5. Copiez le script et enregistrez-le en tant que fichier sur votre Controller de domaine AD. Vous devez maintenant exécuter ce script sur le Controller de domaine pour générer le fichier keytab, puis copier le fichier keytab dans le répertoire /nsconfig/krb/ sur l’appliance Citrix ADC.
6. Cliquez sur **OK.**

Activer l'authentification SSO pour l'authentification Basic, Digest et NTLM

August 20, 2021

À partir de la fonctionnalité Citrix ADC version 13.0 build 64.35 et supérieure, les types SSO suivants sont désactivés globalement.

- L'authentification de base
- Authentification Digest Access
- NTLM sans Négocier la clé NTLM2 ou le signe de négociation

La configuration SSO (Single Sign-On) dans Citrix ADC et Citrix Gateway peut être activée au niveau global et également par niveau de trafic. Par défaut, la configuration SSO est **OFF** et un administrateur peut activer l'interface SSO par trafic ou globalement. **Du point de vue de la sécurité, Citrix recommande aux administrateurs de désactiver l'option SSO globalement et d'activer l'option par trafic.** Cette amélioration vise à rendre la configuration SSO plus sécurisée en désactivant certains types de méthodes SSO globalement.

> La configuration SSO StoreFront est affectée (désactivée) uniquement pour la version 13.0 64.35. La configuration ne sera pas affectée dans les futures versions 13.0.

Types SSO non affectés

Les types SSO suivants ne sont pas affectés par cette amélioration.

- Authentification Kerberos
- Authentification SAML
- Authentification basée sur un formulaire
- Authentification au porteur OAuth
- NTLM avec une clé de négociation NTLM2 ou un signe de négociation

Configurations SSO affectées

Voici les configurations SSO impactées (désactivées).

Configurations globales

```
set tmsessionparam -SSO ON
set vpnparameter -SSO ON
add tmsessionaction tm_act -SSO ON
add vpn sessionaction tm_act -SSO ON
```


> Vous pouvez activer/désactiver l'option SSO dans son ensemble et ne pouvez pas modifier les types d'SSO individuels.

Mesures de sécurité à appliquer

Dans le cadre des mesures de sécurité, les types SSO sensibles à la sécurité sont désactivés dans la configuration globale, mais sont autorisés uniquement via une configuration d'action de trafic.
Par conséquent, si un serveur back-end attend Basic, Digest ou NTLM sans la clé Negotiate NTLM2 ou Negotiate Sign, l'administrateur peut autoriser SSO uniquement via la configuration suivante.

Action sur le trafic

```
add vpn trafficaction tf_act  http -SSO ON
add tm trafficaction tf_act -SSO ON
```

Politique de trafic

```
add tm trafficpolicy <name> <rule> tf_act
add vpn trafficpolicy <name> <rule> tf-act
```

> L'administrateur doit disposer d'une règle appropriée configurée pour la stratégie de trafic pour s'assurer que l'authentification unique est activée uniquement pour le serveur principal approuvé.

AAA-TM

Scénarios basés sur la configuration globale :

```
set tmsessionparam -SSO ON
```

Solution :

```
add tm trafficaction tf_act -SSO ON
add tm trafficpolicy tf_pol true tf_act
```

Liez la stratégie de trafic suivante à tous les serveurs virtuels LB où SSO est attendu :

```
bind lb vserver <LB VS Name> -policy tf_pol -priority 65345
```

Scénarios basés sur la configuration de stratégie de session :


```
add tmsessionaction tm_act -SSO ON
add tmsession policy <name> <rule> tm_act
add tm trafficaction tf_act -SSO ON
add tm trafficpolicy tf_pol <same rule as session Policy> tf_act
```

Points à noter :

- L'utilisateur/groupe Citrix ADC AAA pour la stratégie de session précédente doit être remplacé par la stratégie de trafic.
- Liez la stratégie suivante aux serveurs virtuels d'équilibrage de charge pour la stratégie de session précédente,
  `bind lb vserver [LB VS Name] -policy tf_pol -priority 65345`
- Si une stratégie de trafic avec une autre priorité est configurée, la commande précédente ne sert pas correctement.

La section suivante traite des scénarios basés sur des conflits avec plusieurs stratégies de trafic associées à un trafic :

Pour un trafic TM particulier, une seule stratégie de trafic TM est appliquée. En raison du paramètre global des modifications de fonctionnalité SSO, l'application d'une stratégie de trafic TM supplémentaire avec une faible priorité peut ne pas être applicable dans le cas où une stratégie de trafic TM avec une priorité élevée (qui n'a pas de configuration SSO requise) est déjà appliquée. La section suivante décrit la méthode permettant de s'assurer que de tels cas sont traités.

Considérez que les trois stratégies de trafic suivantes avec une priorité plus élevée sont appliquées au serveur virtuel d'équilibrage de charge (LB) :

```
add tm trafficaction tf_act1 <Addition config>
add tm trafficaction tf_act2 <Addition config>
add tm trafficaction tf_act3 <Addition config>

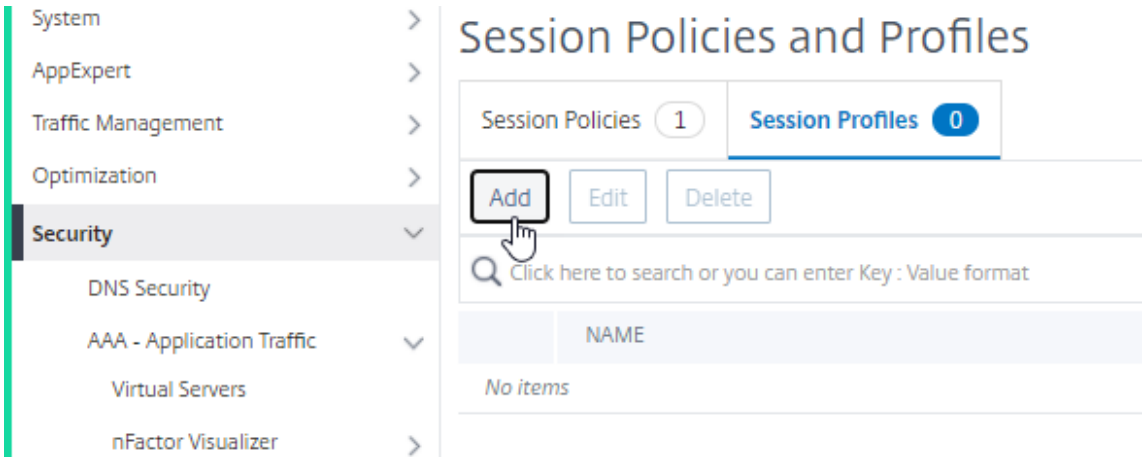
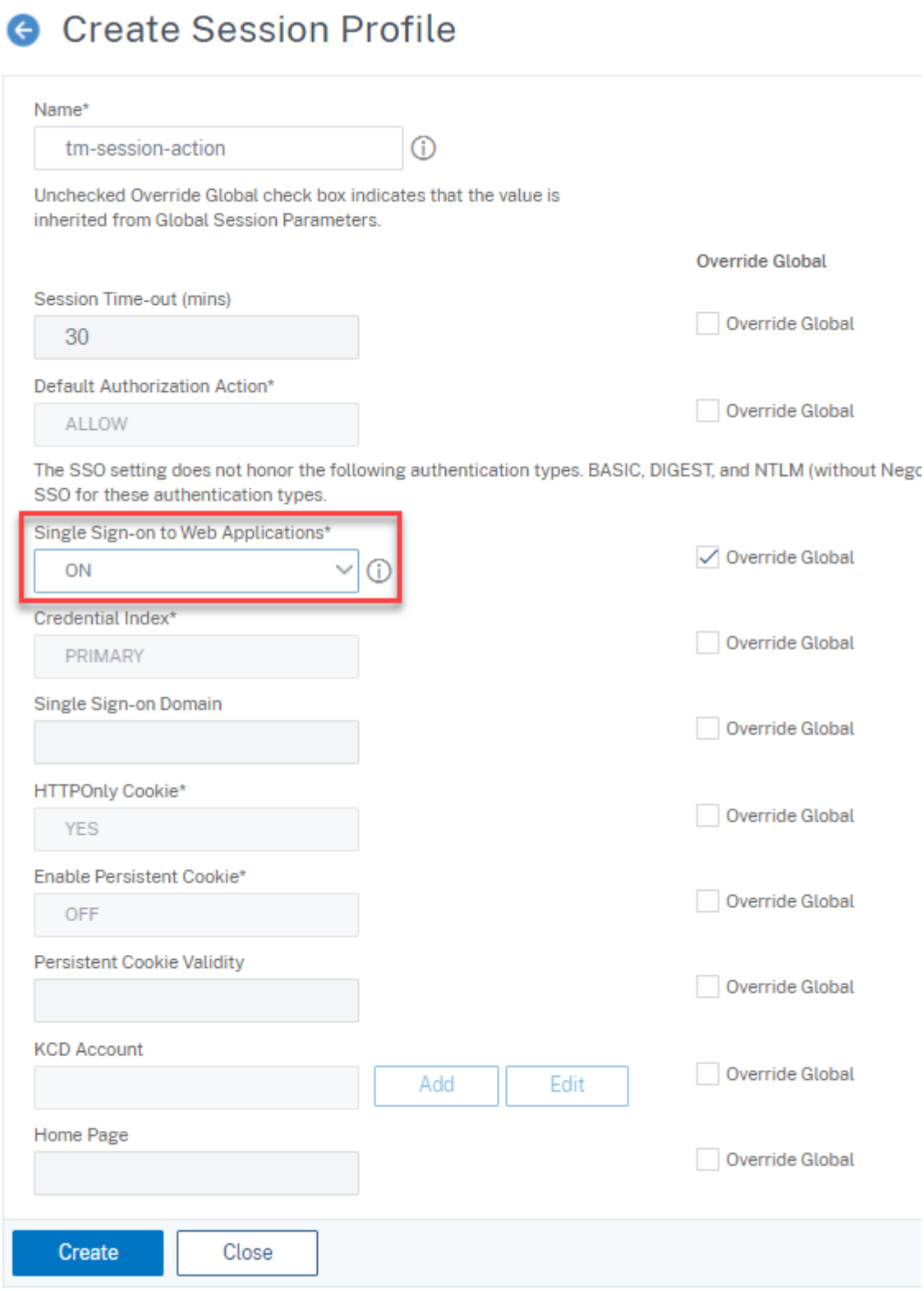
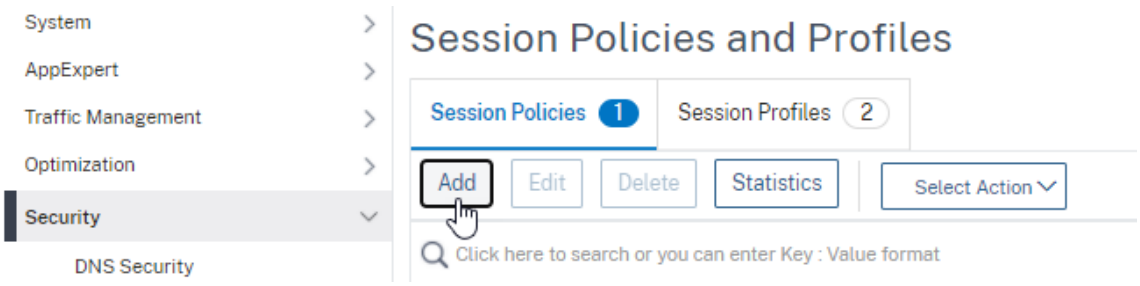
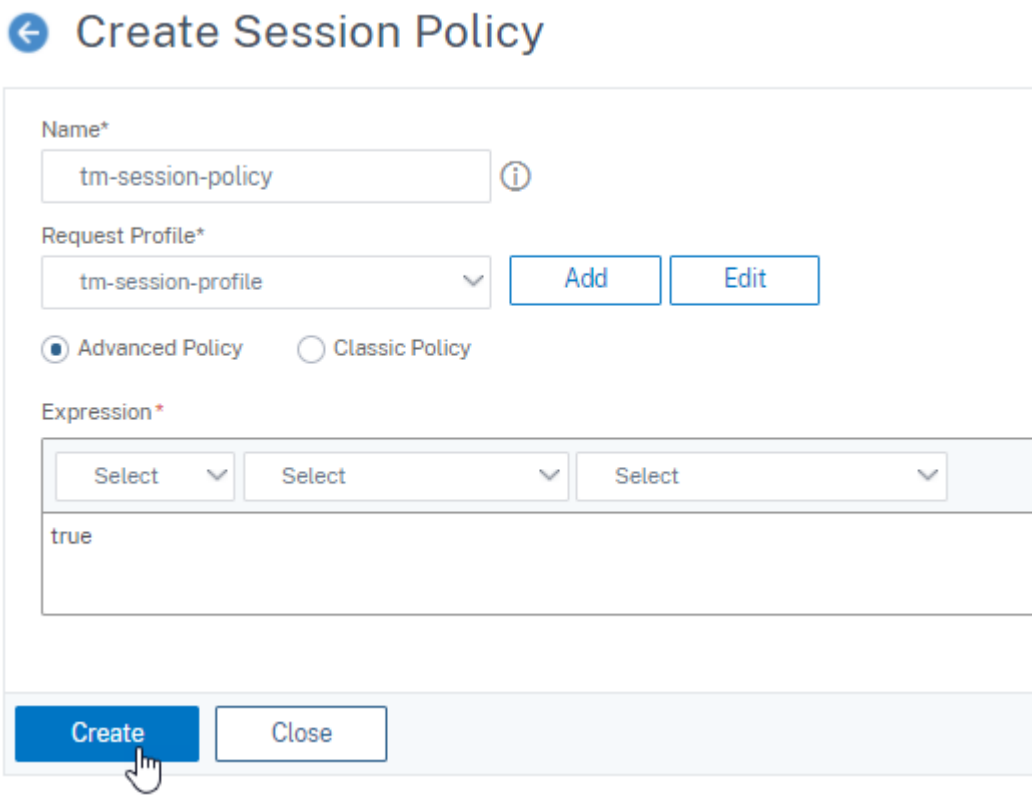
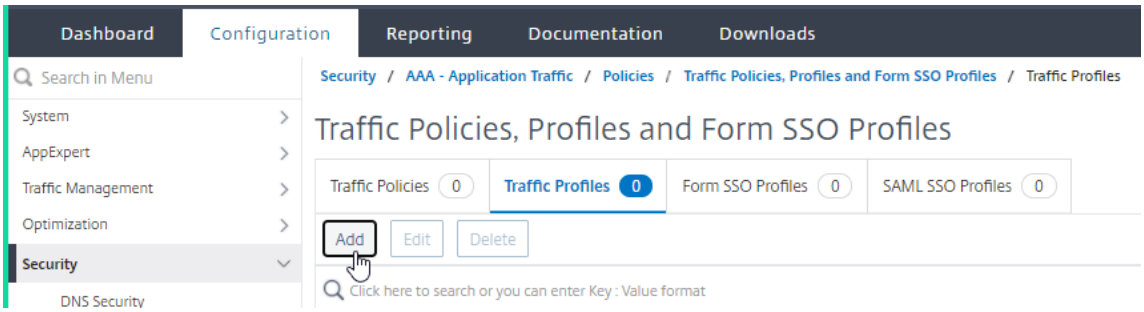
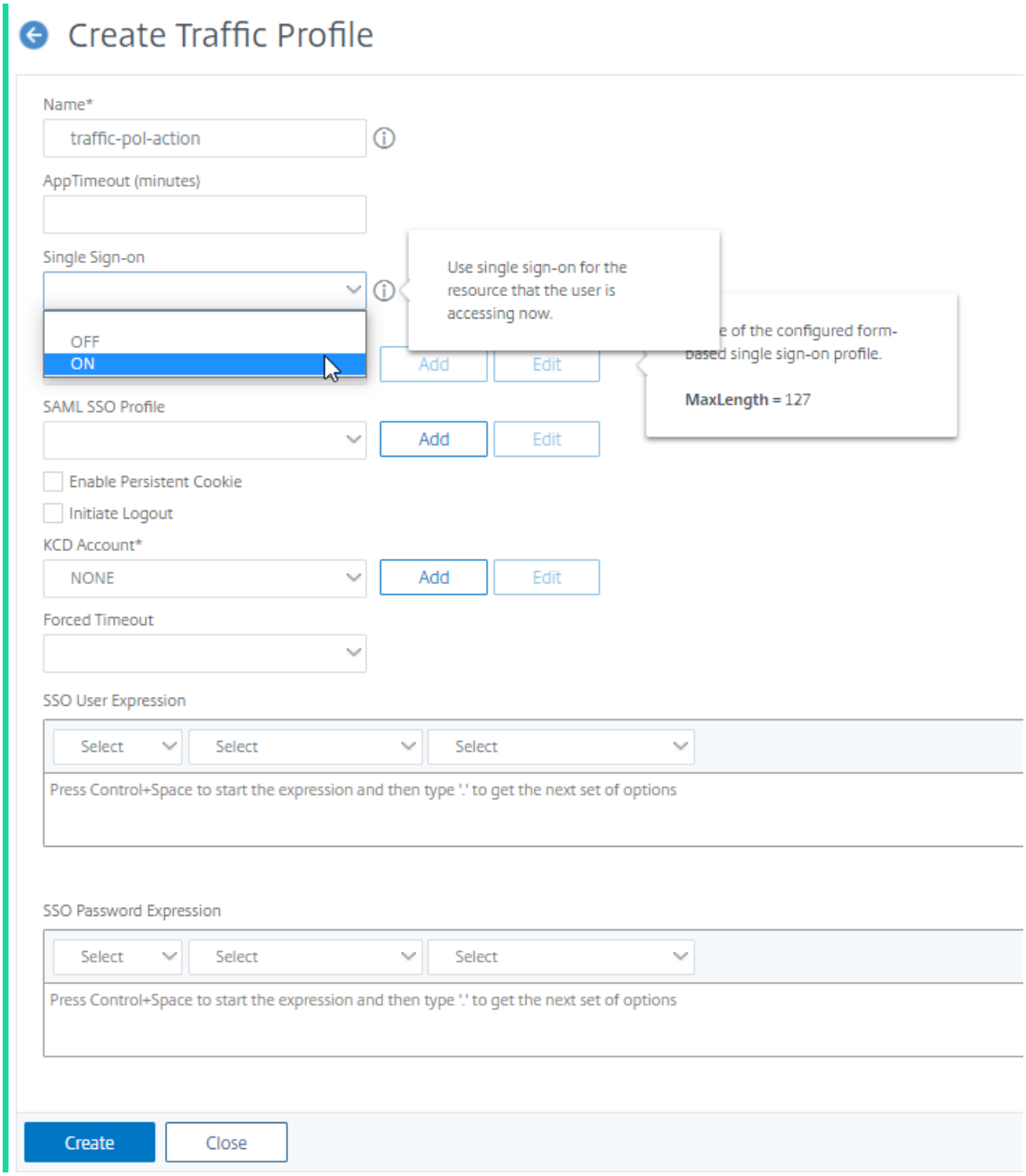
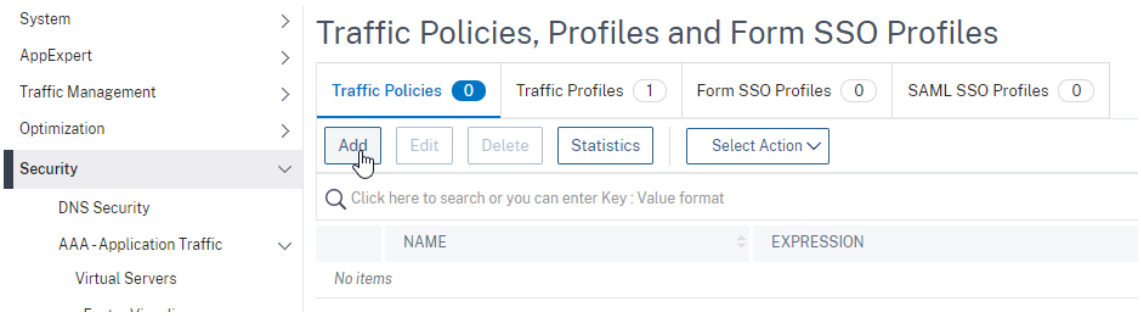
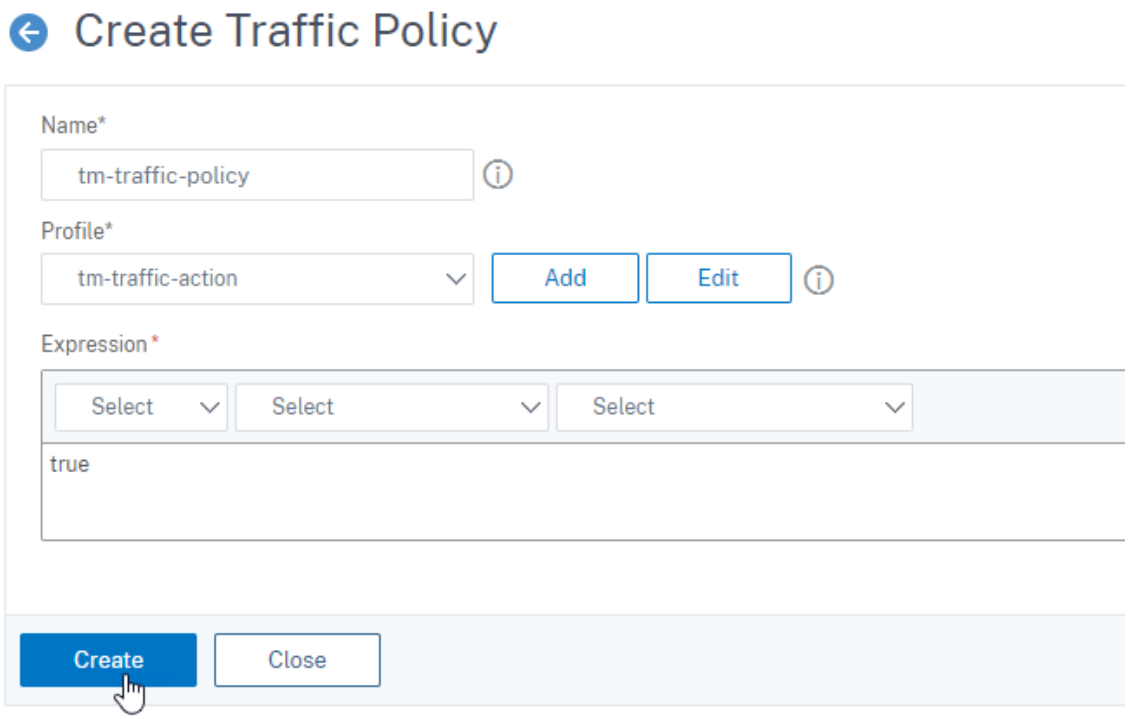
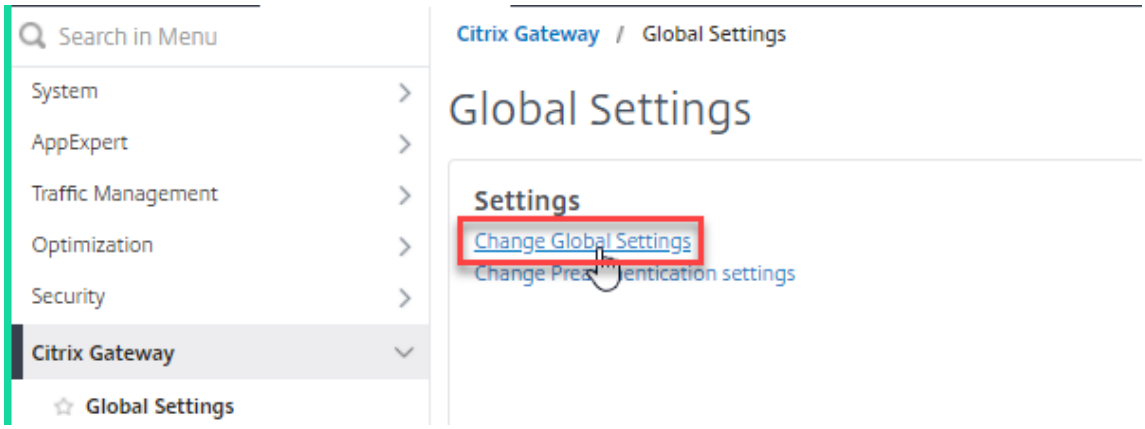
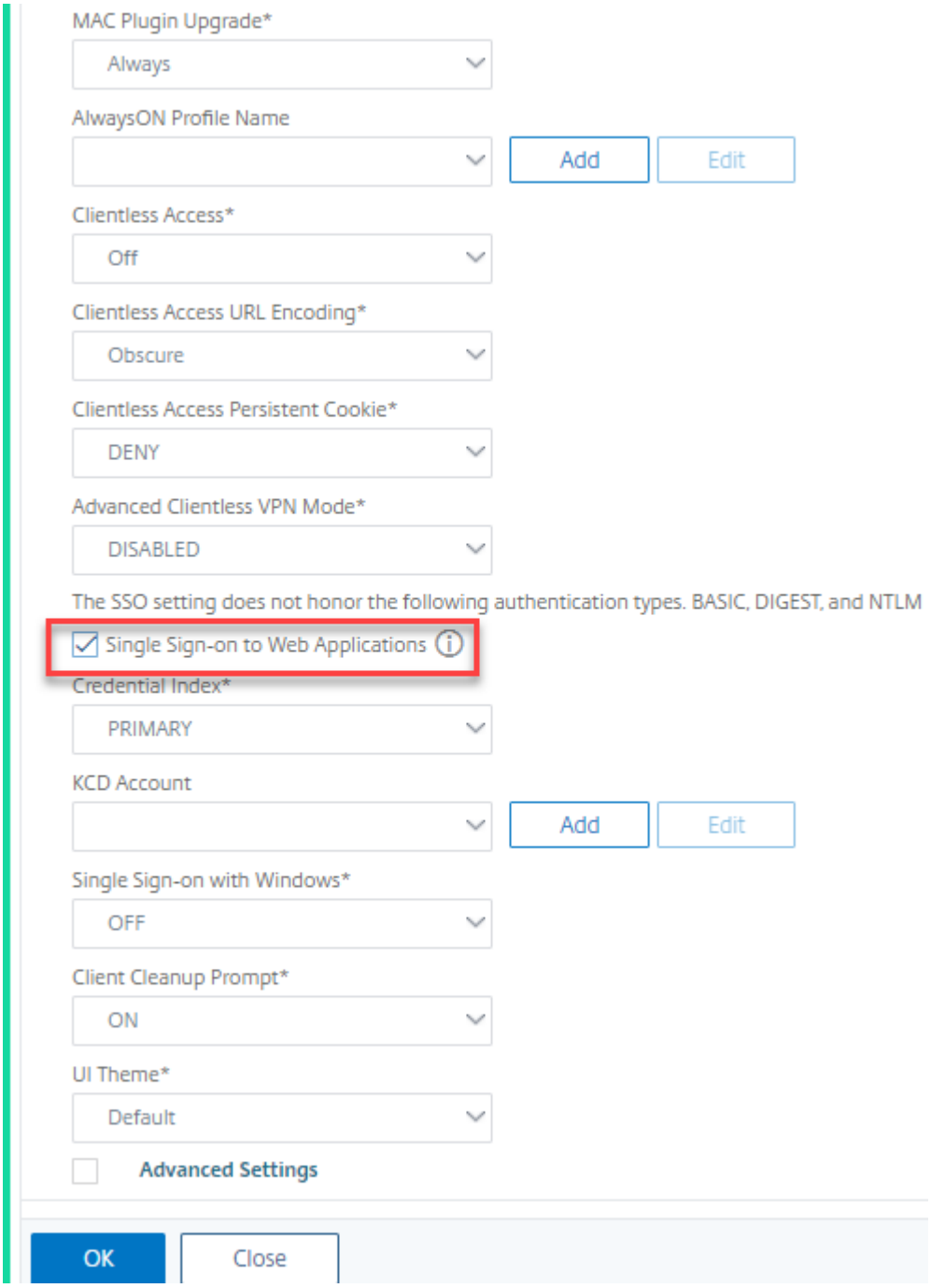
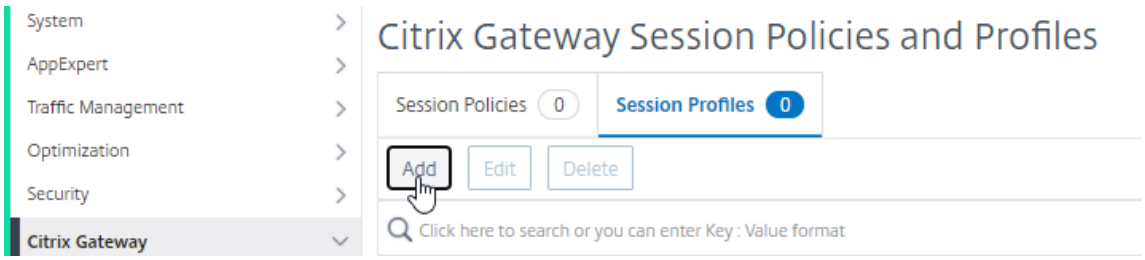
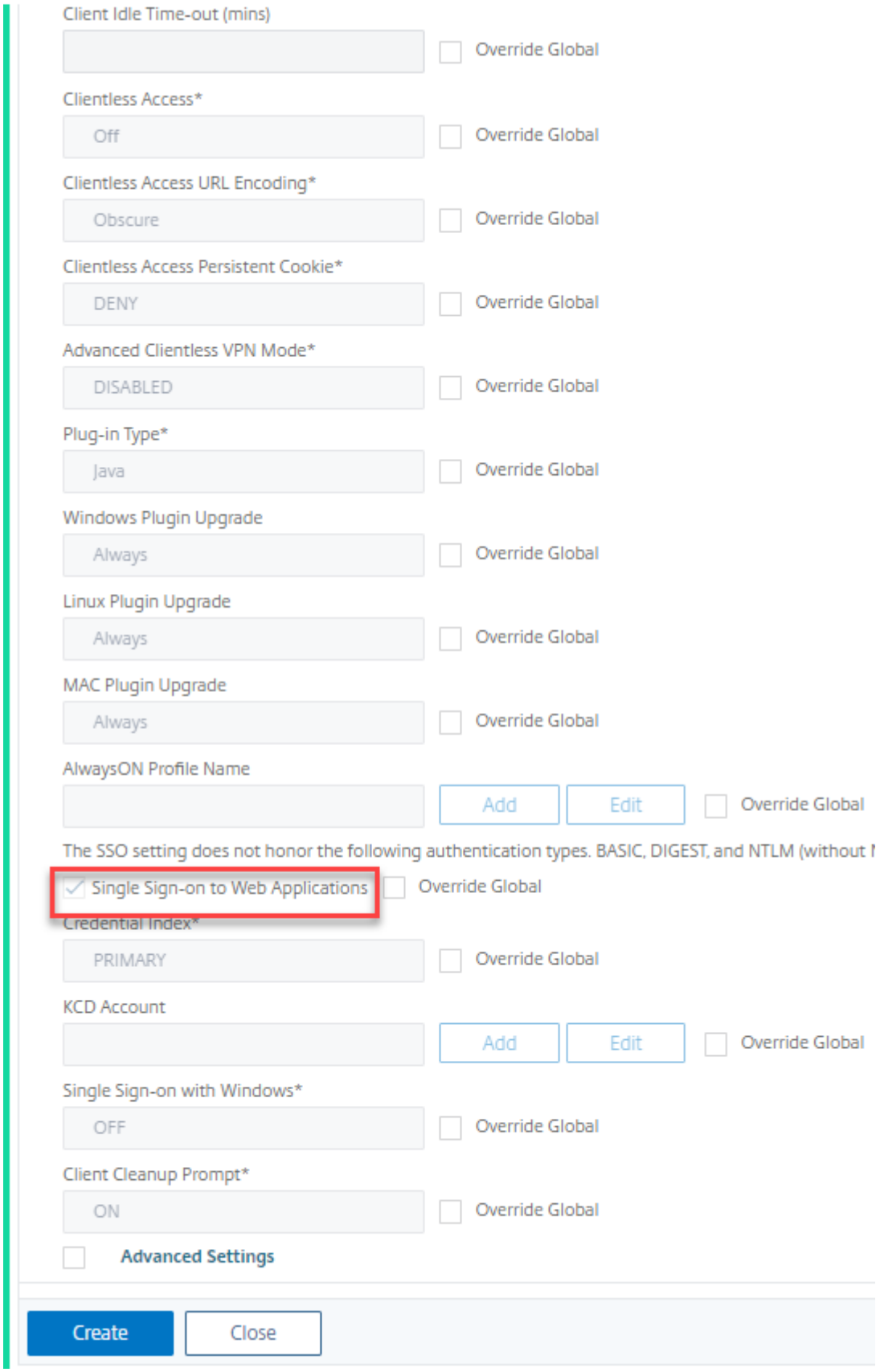
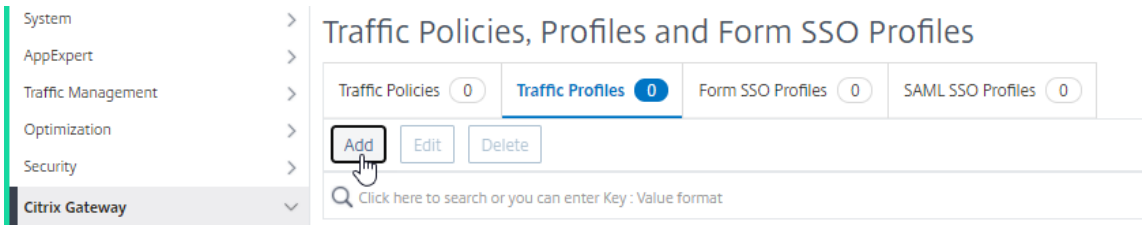
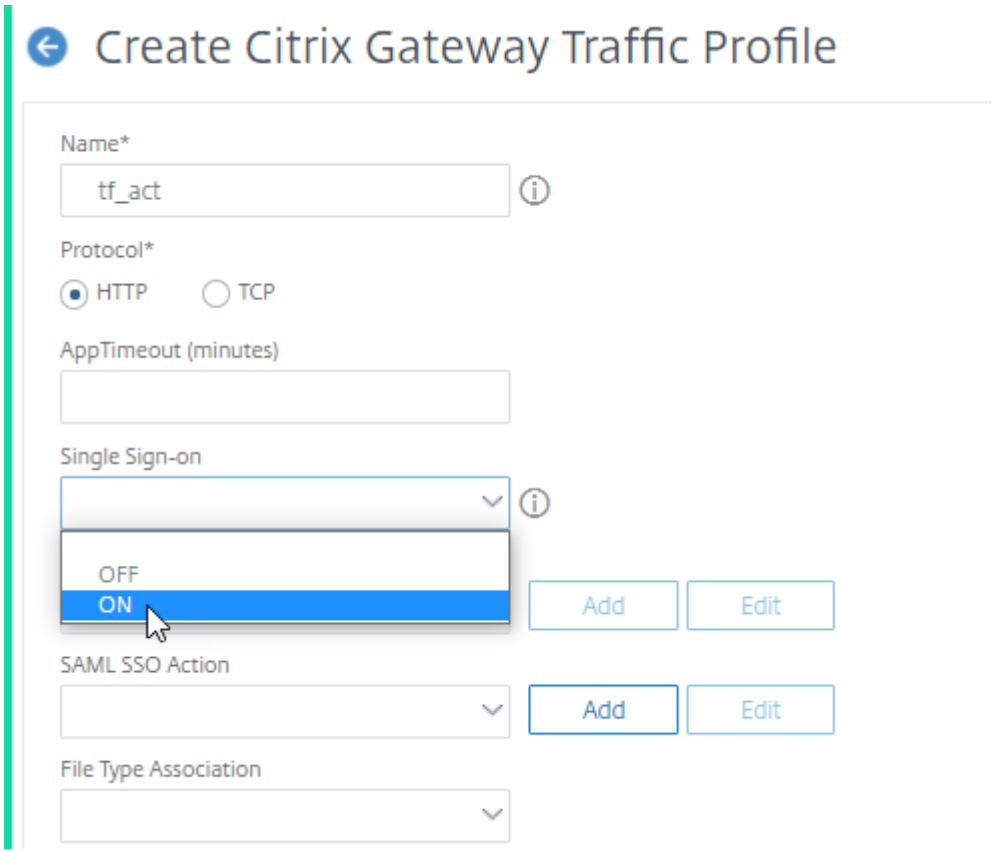
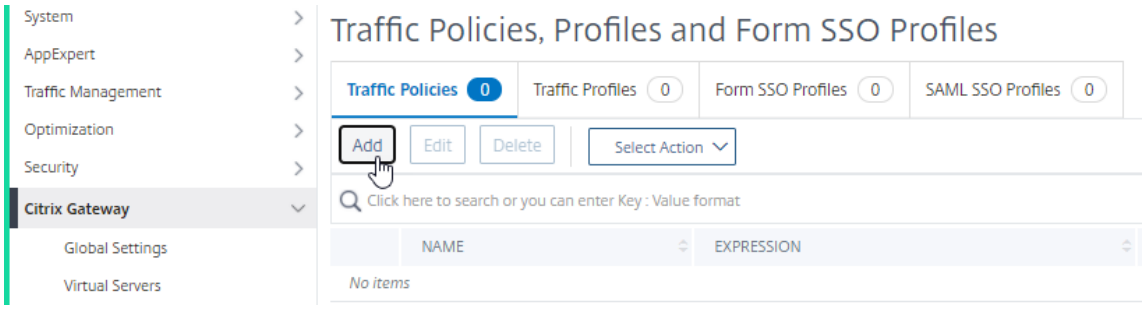
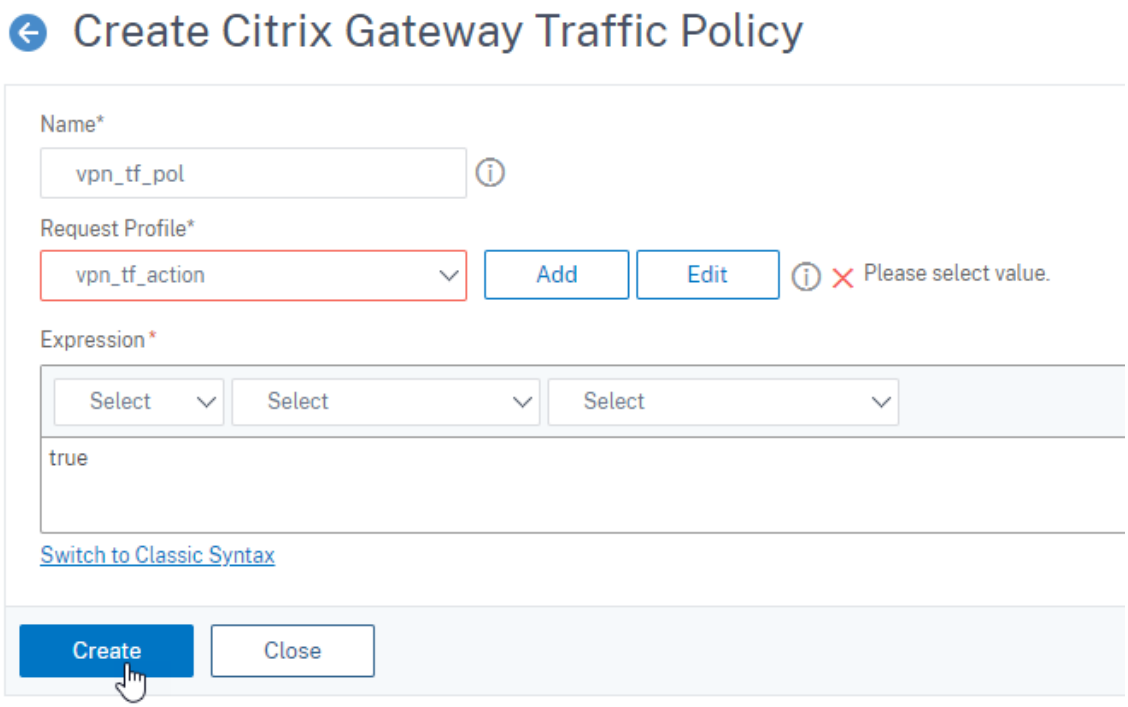
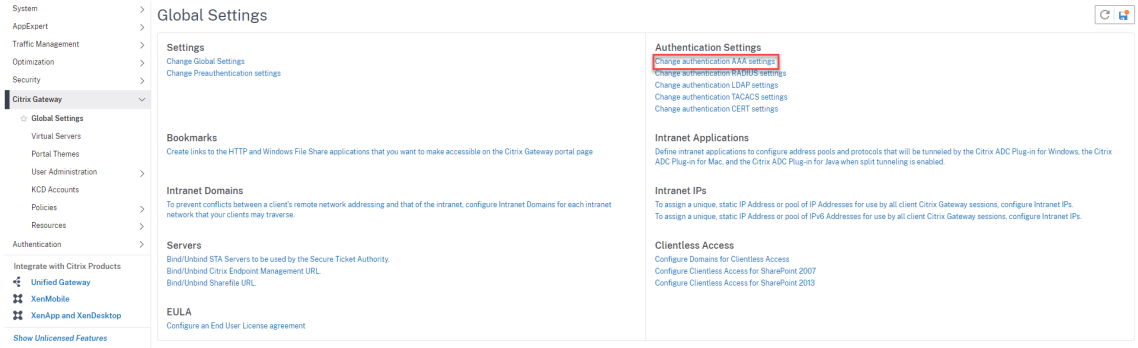
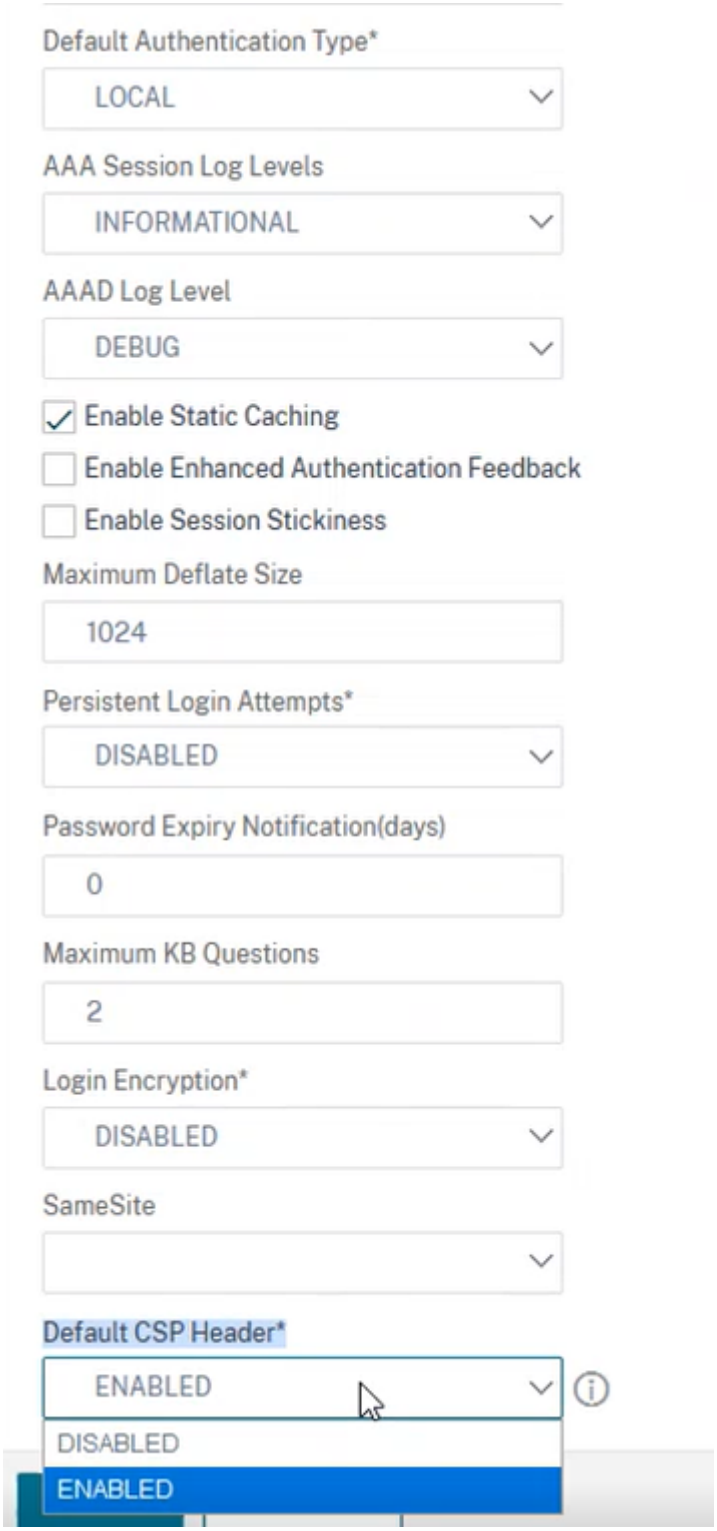
add tm trafficpolicy tf_pol1 <rule1> tf_act1
add tm trafficpolicy tf_pol2 <rule2> tf_act2
add tm trafficpolicy tf_pol3 <rule3> tf_act3

bind lb vserver <LB VS Name> -policy tf_pol1 -priority 100
bind lb vserver <LB VS Name> -policy tf_pol2 -priority 200
bind lb vserver <LB VS Name> -policy tf_pol3 -priority 300
```

Méthode sujette aux erreurs - Pour résoudre la configuration SSO globale, vous ajoutez la configuration suivante :

```
add tm trafficaction tf_act_default -SSO ON
add tm trafficpolicy tf_pol_default true tf_act_default
```



```
3
4 bind lb vserver <LB VS Name> -policy tf_pol_default -priority 65345
```

Remarque : La modification précédente peut rompre l'authentification unique pour le trafic qui touche <tf_pol1/tf_pol2/tf_pol3> comme pour ce trafic, stratégie de trafic <tf_pol_default> n'est pas appliqué.

Méthode correcte - Pour atténuer ce problème, la propriété SSO doit être appliquée individuellement pour chacune des actions de trafic correspondantes :

Par exemple, dans le scénario précédent, pour que l'authentification unique se produise pour le trafic touchant tf_pol1/tf_pol3, la configuration suivante doit être appliquée avec <tf_pol_default>.

```
1 add tm trafficaction tf_act1 <Addition config> -SSO ON
2 add tm trafficaction tf_act3 <Addition config> -SSO ON
```

Cas Citrix Gateway

Scénarios basés sur la configuration globale :

```
1 set vpnparameter -SSO ON
```

Solution :

```
1 add vpn trafficaction vpn_tf_act http  -SSO ON
2 add vpn trafficpolicy vpn_tf_pol  true vpn_tf_act
```

Liez la stratégie de trafic suivante à tous les serveurs virtuels VPN où SSO est attendu :

```
1 bind vpn vserver vpn_vs -policy vpn_tf_pol -priority 65345
```

Scénarios basés sur la configuration de stratégie de session :

```
1 add vpn sessionaction vpn_sess_act -SSO ON
2 add vpnsession policy <name> <rule> vpn_sess_act
```

Points à noter :

- L'utilisateur/groupe Citrix ADC AAA pour la stratégie de session précédente doit être remplacé par la stratégie de trafic.
- Liez la stratégie suivante aux serveurs virtuels LB pour la stratégie de session précédente, `bind lb virtual server [LB VS Name] -policy tf_pol -priority 65345`.

- Si une stratégie de trafic avec une autre priorité est configurée, la commande précédente ne sert pas correctement. La section suivante traite des scénarios basés sur des conflits avec plusieurs stratégies de trafic associées au trafic.

Scénarios fonctionnels basés sur des conflits avec plusieurs stratégies de trafic associées à un trafic :

Pour un trafic Citrix Gateway particulier, une seule stratégie de trafic VPN est appliquée. En raison de la définition globale des modifications de fonctionnalité SSO, l'application d'une stratégie de trafic VPN supplémentaire avec une faible priorité peut ne pas être applicable s'il existe d'autres stratégies de trafic VPN avec une priorité élevée qui n'ont pas de configuration SSO requise.

La section suivante décrit la méthode pour s'assurer que de tels cas sont traités :

Considérez qu'il existe trois stratégies de trafic avec une priorité plus élevée appliquées à un serveur virtuel VPN :

```
add vpn trafficaction tf_act1 <Addition config>
add vpn trafficaction tf_act2 <Addition config>
add vpn trafficaction tf_act3 <Addition config>

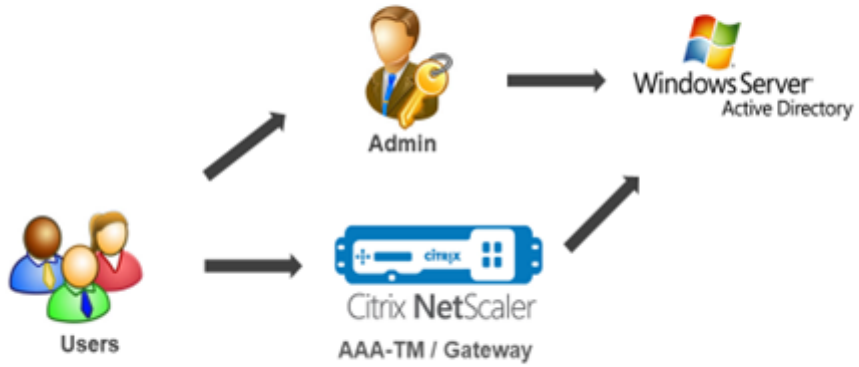
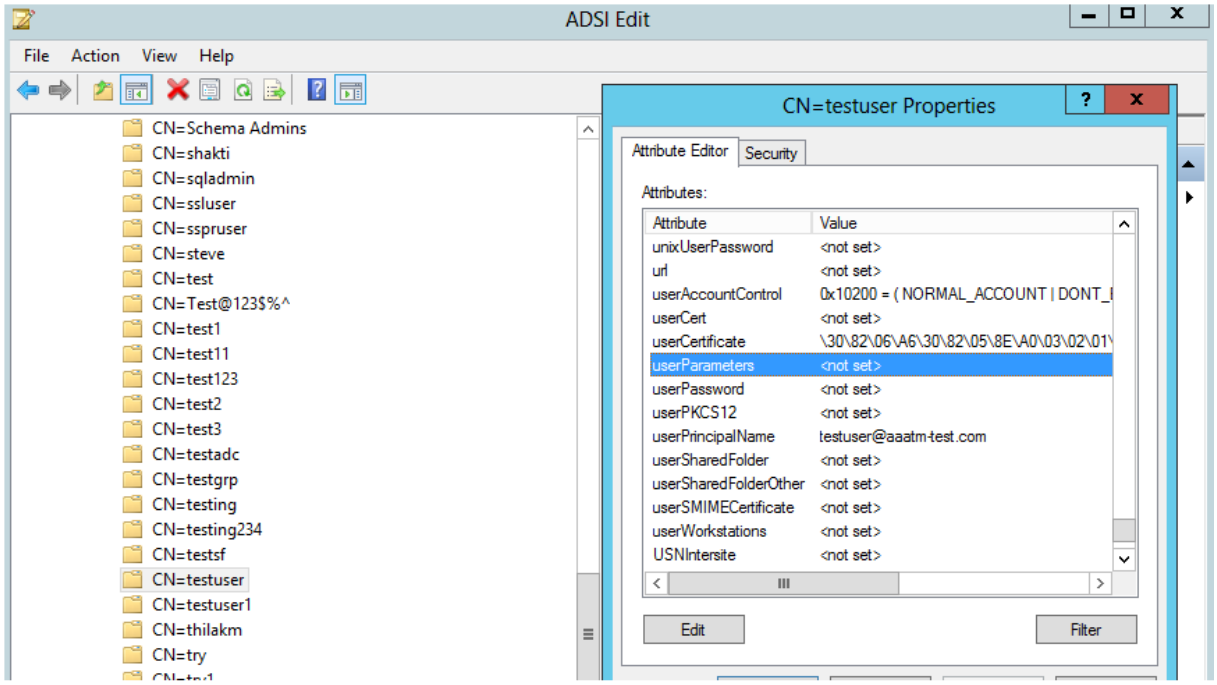
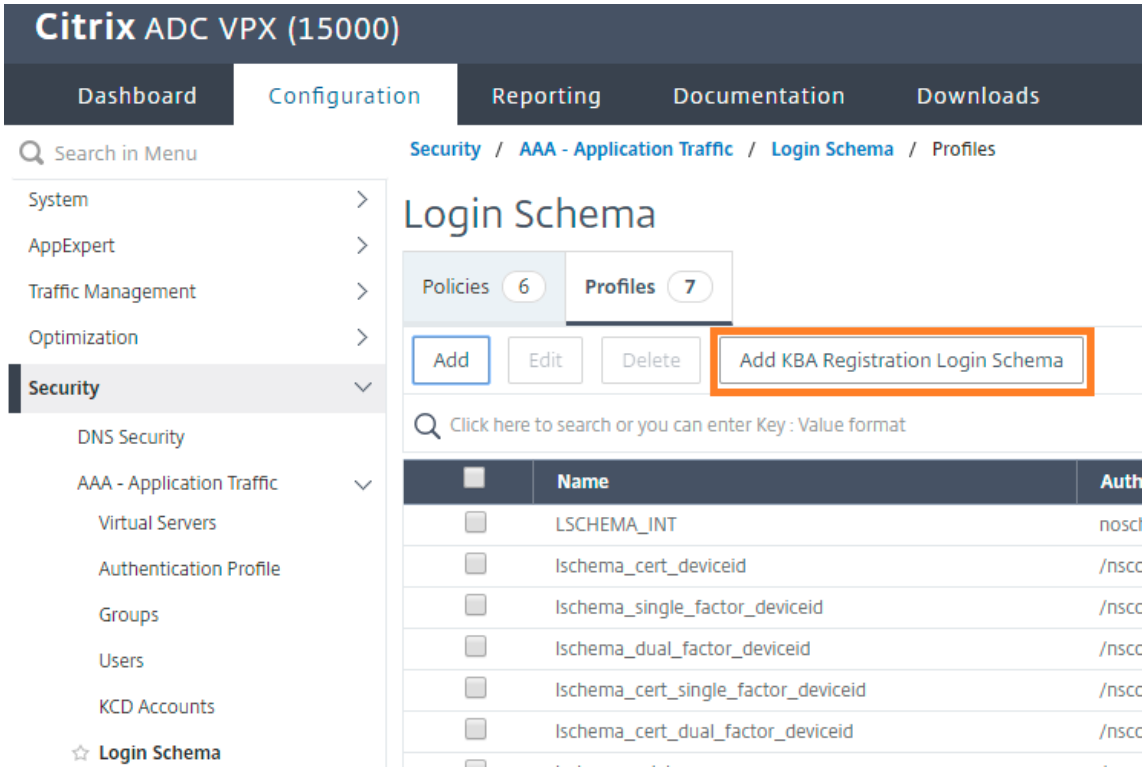
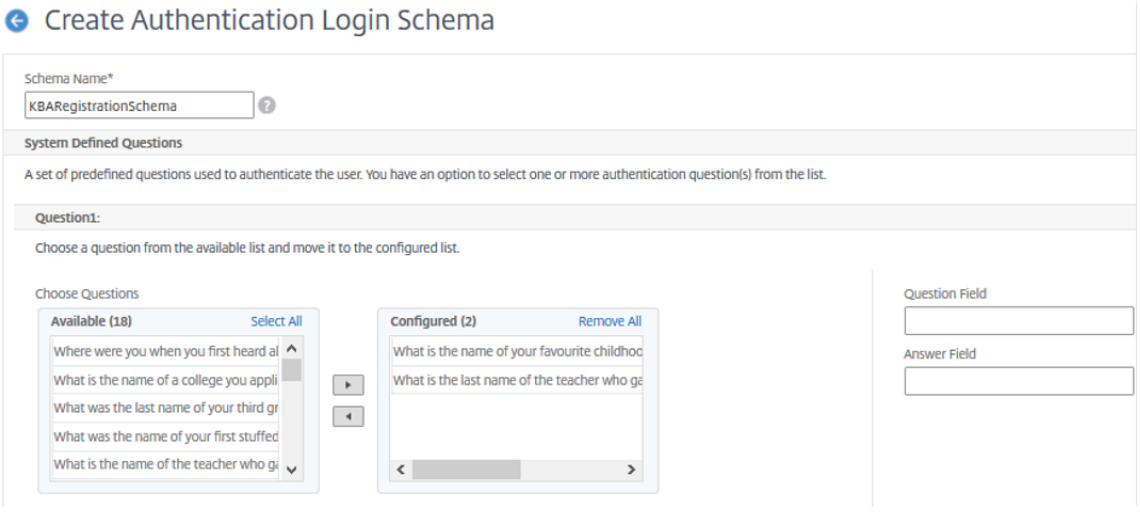
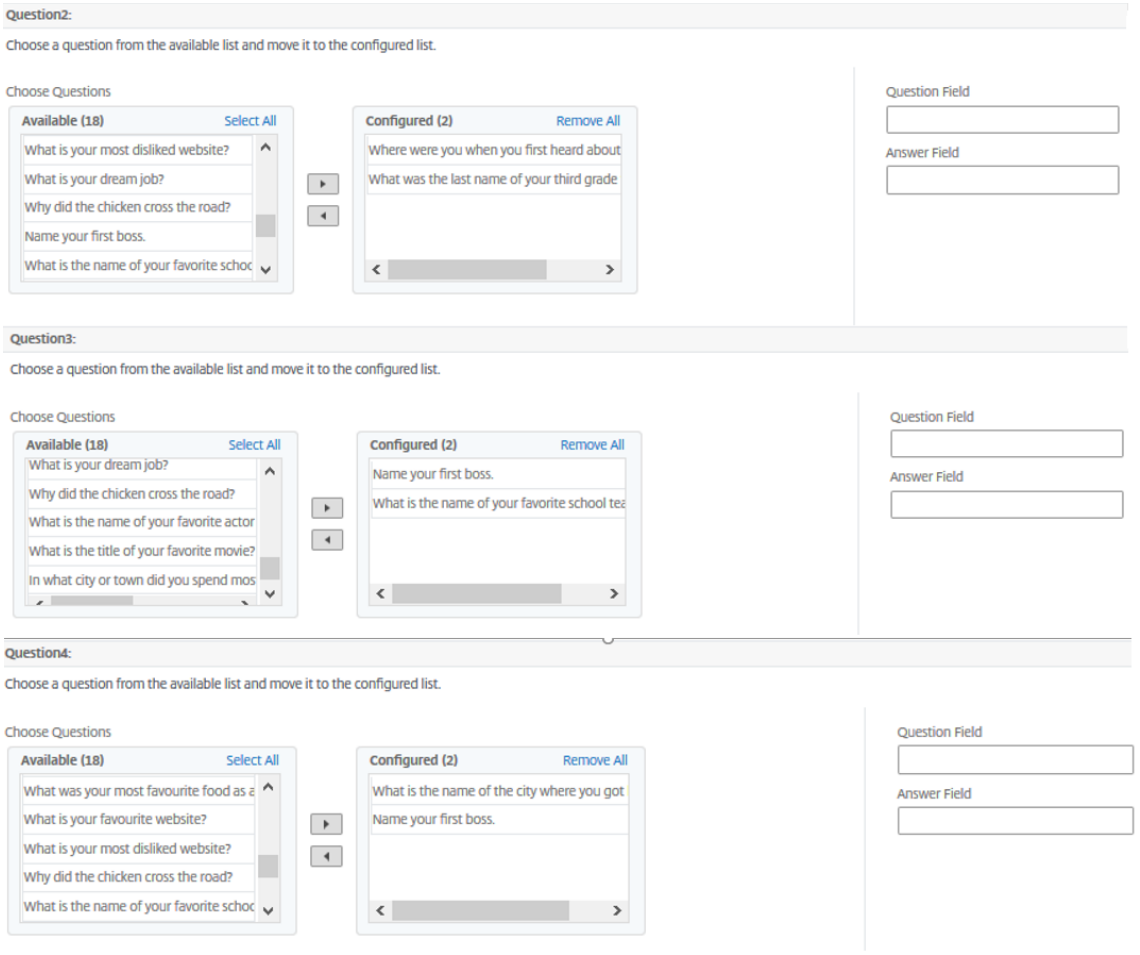
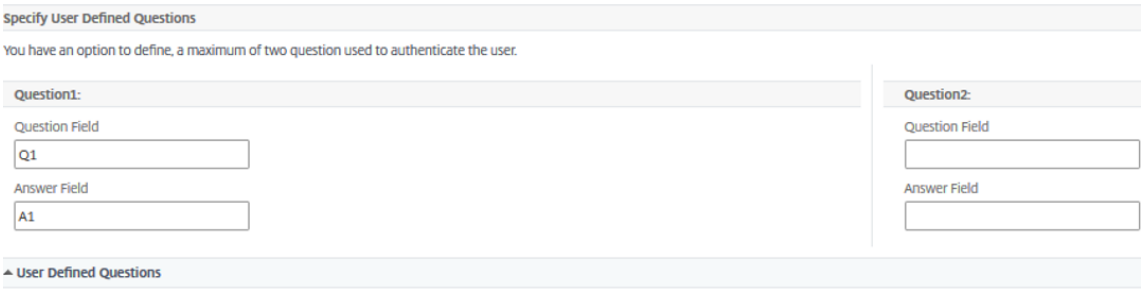
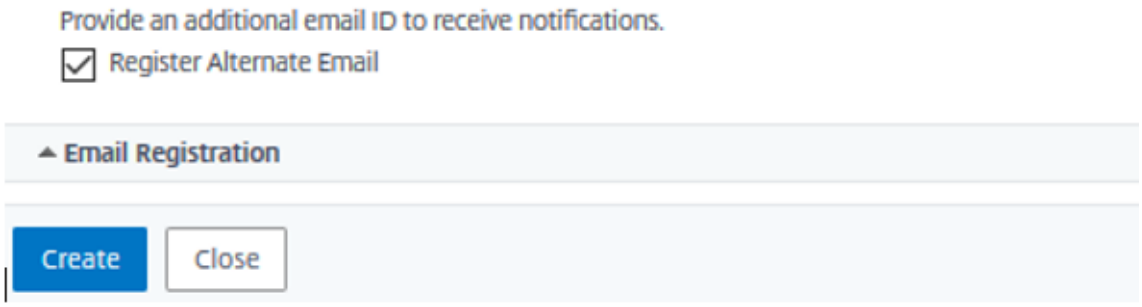
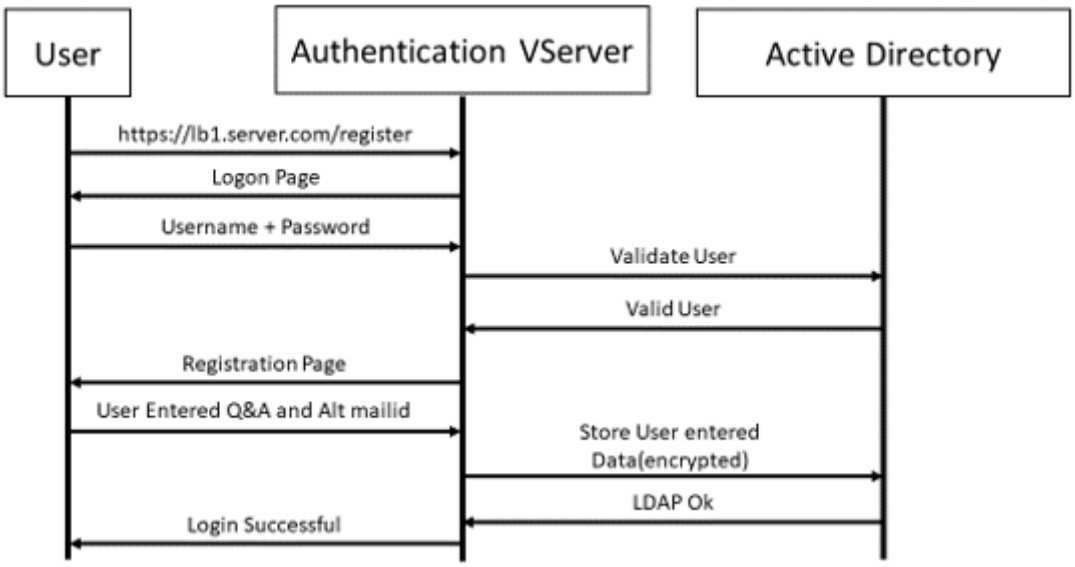
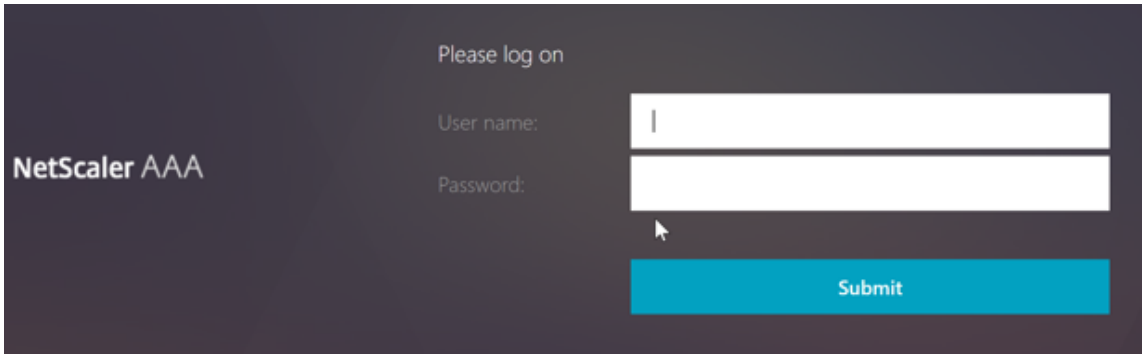
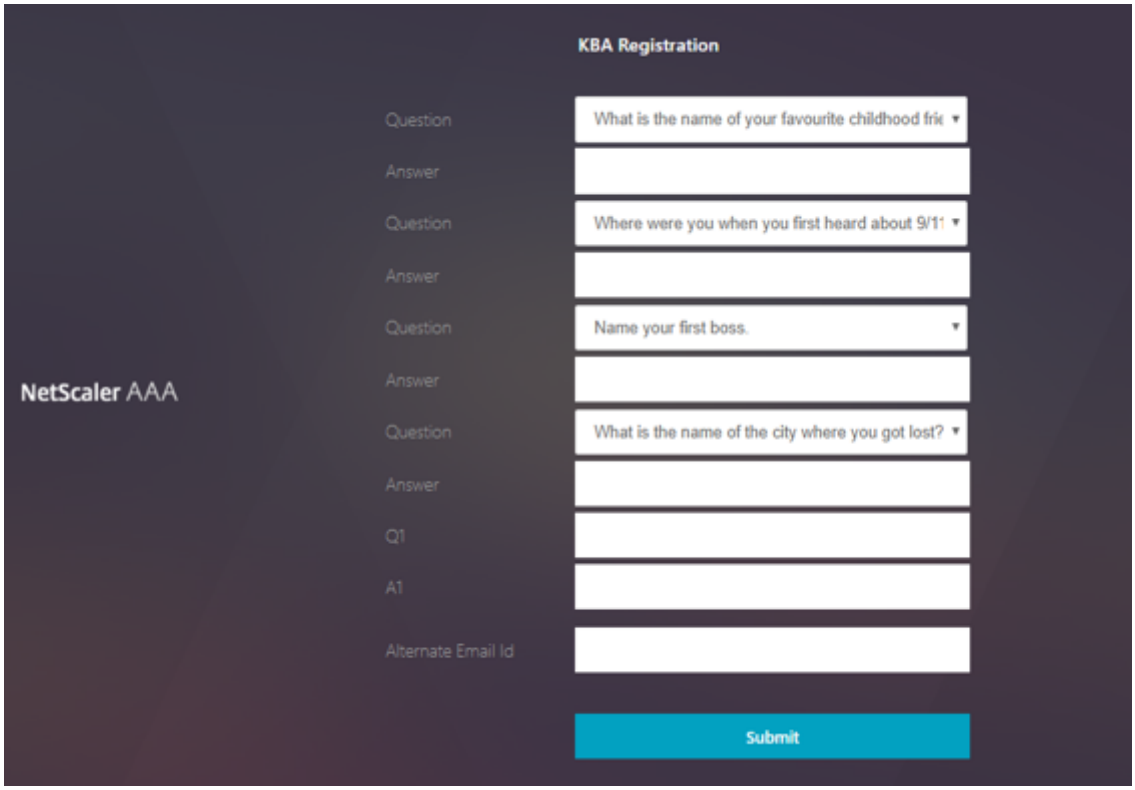
add vpn trafficpolicy tf_pol1 <rule1> tf_act1
add vpn trafficpolicy tf_pol2 <rule2> tf_act2
add vpn trafficpolicy tf_pol3 <rule3> tf_act3

bind vpn vserver <VPN VS Name> -policy tf_pol1 -priority 100
bind vpn vserver <VPN VS Name> -policy tf_pol2 -priority 200
bind vpn vserver <VPN VS Name> -policy tf_pol3 -priority 300
```

Méthode sujette aux erreurs : Pour résoudre la configuration SSO globale, vous ajoutez la configuration suivante :

```
add vpn trafficaction tf_act_default -SSO ON
add vpn trafficpolicy tf_pol_default true tf_act_default

bind vpn vserver <VPN VS Name> -policy tf_pol_default -priority 65345
```

Remarque : La modification précédente peut rompre l'authentification unique pour le trafic qui atteint, <tf_pol1/tf_pol2/tf_pol3> comme pour ce trafic, stratégie de trafic <tf_pol_default> n'est pas appliqué.

Méthode correcte : pour atténuer ce problème, la propriété SSO doit être appliquée individuellement pour chacune des actions de trafic correspondantes.

Par exemple, dans le scénario précédent, pour que l'authentification unique se produise pour le trafic touchant tf_pol1/tf_pol3, la configuration suivante doit être appliquée avec <tf_pol_default>.


```
add vpn trafficaction tf_act1 [Additional config] -SSO ON

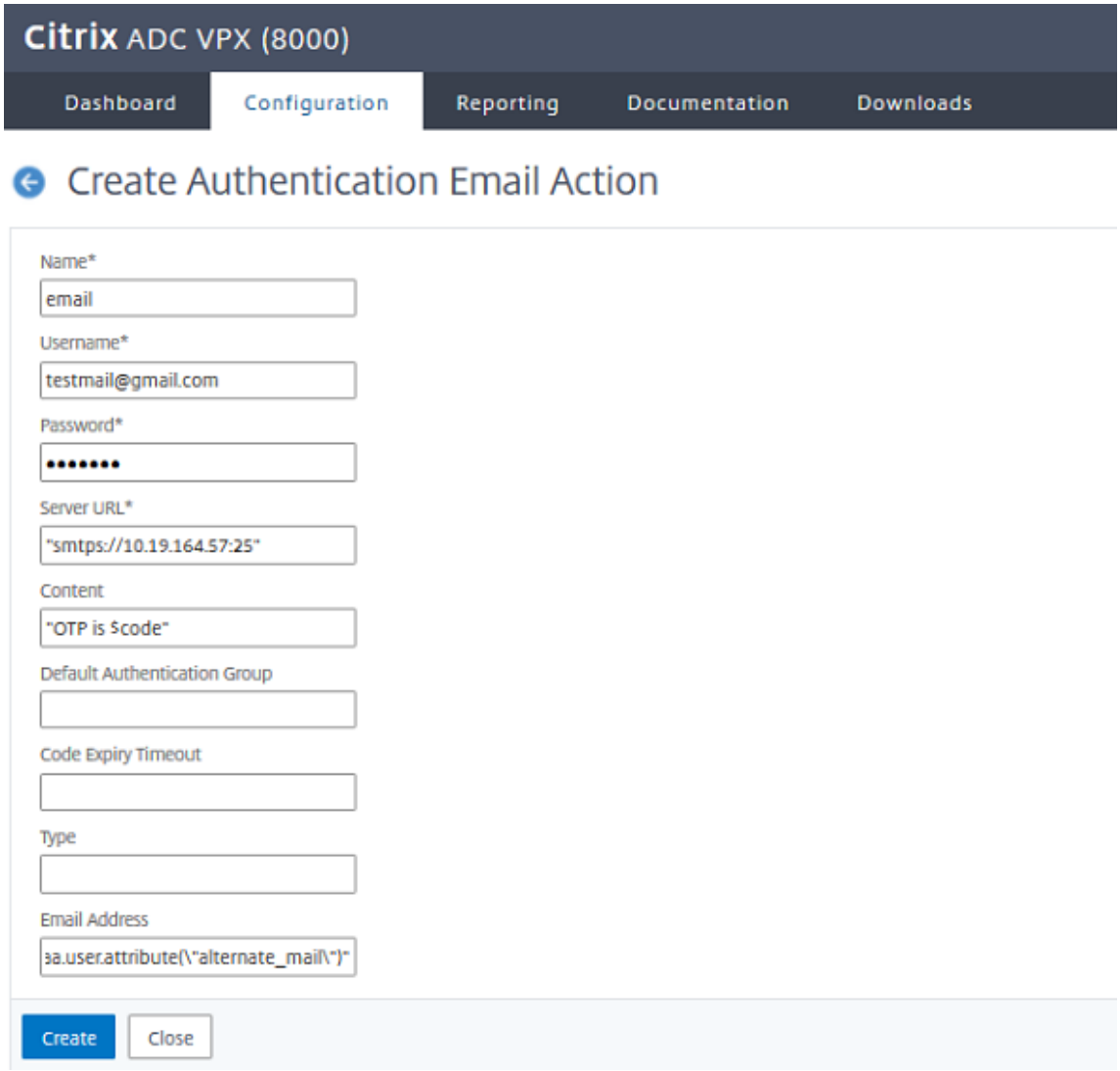
add vpn trafficaction tf_act3 [Additional config] -SSO ON
```

Configurer SSO à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA — Trafic des applications > Stratégies > Session**, sélectionnez l'onglet **Profils de session**, puis cliquez sur **Ajouter**.



2. Entrez un nom pour le profil de session, cliquez sur la case à cocher **Remplacer globalement** en regard du champ **Connexion unique aux applications Web**, puis cliquez sur **Créer**.



3. Accédez à **Sécurité > AAA — Trafic des applications > Stratégies > Session**, sélectionnez **l'onglet Stratégies de session**, puis cliquez sur **Ajouter**.



4. Entrez un nom pour la stratégie de session, entrez « True » dans le champ **Expression** et cliquez sur **Créer**.



5. Accédez à **Sécurité > AAA — Trafic des applications > Stratégies > Trafic**, sélectionnez l'onglet **Profils de trafic**, puis cliquez sur **Ajouter**.



6. Entrez un nom pour le profil de trafic, sélectionnez **ON** dans le menu déroulant **Single Sign-On**,

puis cliquez sur **Créer**.



7. Accédez à **Sécurité > AAA — Trafic des applications > Stratégies> Trafic**, sélectionnez **l'onglet Stratégies de trafic**, puis cliquez sur **Ajouter**.



8. Entrez un nom pour la stratégie de trafic, entrez « True » dans le champ **Expression** et cliquez sur **Créer**.



9. Accédez à **Citrix Gateway > Paramètres globaux**, puis cliquez sur **Modifier les paramètres globaux**.



10. dans la page **Paramètres globaux Citrix Gateway**, sélectionnez l'onglet **Expérience client** et cochez **le champ Connexion unique aux applications Web**.



11. Accédez à **Citrix Gateway > Stratégies> Session**, sélectionnez l'onglet **Profils de session**, puis cliquez sur **Ajouter**.



12. Sur la page **Créer un profil de session Citrix Gateway**, sélectionnez l'onglet **Expérience client** et cochez **le champ Connexion unique aux applications Web**.



13. Accédez à **Citrix Gateway > Stratégies > Trafic**, sélectionnez l'onglet **Profils de trafic**, puis cliquez sur **Ajouter**.



14. Entrez un nom pour le profil de trafic, sélectionnez **ON** dans le menu déroulant **Single Sign-On**, puis cliquez sur **Créer**.



15. Accédez à **Citrix Gateway > Stratégies> Trafic**, sélectionnez **l'onglet Stratégies de trafic**, puis cliquez sur **Ajouter**.



16. Sur la page **Créer une stratégie de trafic Citrix Gateway**, entrez le nom de la stratégie de trafic, entrez « True » dans le champ **Expression** et cliquez sur **Créer**.



Réécriture pour Citrix Gateway et les réponses générées par le serveur d'authentification

August 20, 2021

Réécriture fait référence à la réécriture de certaines informations dans les demandes ou réponses traitées par l'appliance Citrix ADC. La réécriture peut aider à fournir un accès au contenu demandé sans exposer de détails inutiles sur la configuration réelle du site Web. Pour obtenir des informations détaillées sur le concept de réécriture, voir Réécriture.

À partir de la version 13.0-76.29 de Citrix ADC, la prise en charge des stratégies de réécriture a été étendue aux réponses générées par le serveur virtuel Citrix Gateway et le serveur virtuel d'authentification.

> **Remarque**
>
> Un type de liaison **AAA_Response** est introduit pour prendre en charge les stratégies de réécriture des réponses générées par le serveur virtuel Citrix Gateway et les réponses générées par le serveur virtuel d'authentification.

Exemple d'utilisation de Rewrite

Vous pouvez utiliser Rewrite pour partager les ressources disponibles sur Citrix ADC sur site avec Citrix Cloud. Cela peut être atteint en toute sécurité en implémentant le partage des ressources d'origine CORS. La réécriture peut être utilisée comme suit pour implémenter l'en-tête CORS.

Exemple de configuration

```
1 add rewrite action cors_header_action insert_http_header access-control
     -allow-credentials \"true\"
2
3 add rewrite policy cors_header_pol true cors_header_action
4
5 add rewrite action non_cors_header_action insert_http_header X-Frame-
     Options \'\"DENY\"\'
6
7 add rewrite policy non_cors_header_pol true non_cors_header_action
8
9 bind authentication vserver av_cors -policy cors_header_pol -priority
     100 -type AAA_RESPONSE
10
11 bind vpn vserver av_cors -policy cors_header_pol -priority 100 -type
     AAA_RESPONSE
```

Prise en charge des en-têtes de réponse Content Security Policy pour Citrix Gateway et réponses générées par le serveur virtuel

September 8, 2021

À partir de la version 13.0-76.29 de Citrix ADC, l'en-tête de réponse CSP (Content-Security-Policy) est pris en charge pour Citrix Gateway et les réponses générées par le serveur virtuel d'authentification.

L'en-tête de réponse CSP (Content-Security-Policy) est une combinaison de stratégies utilisées par le navigateur pour éviter les attaques CSS (Cross Site Scripting).
L'en-tête de réponse HTTP CSP permet aux administrateurs de sites Web de contrôler les ressources que l'agent utilisateur est autorisé à charger pour une page donnée. À quelques exceptions près, les stratégies impliquent principalement la spécification des origines du serveur et des points de terminaison de script. Cela permet de se prémunir contre les attaques de scripts intersites.
L'en-tête CSP est conçu pour modifier la façon dont les navigateurs affichent les pages, et donc pour protéger contre diverses injections intersites, y compris le CSS. Il est important de définir correctement la valeur de l'en-tête, de manière à ne pas empêcher le bon fonctionnement du site Web. Par

exemple, si l'en-tête est défini pour empêcher l'exécution de JavaScript en ligne, le site Web ne doit pas utiliser de JavaScript en ligne dans ses pages.

Voici les avantages de l'en-tête de réponse CSP.

- La fonction principale d'un en-tête de réponse CSP est de prévenir les attaques CSS.
- En plus de restreindre les domaines à partir desquels le contenu peut être chargé, le serveur peut spécifier quels protocoles peuvent être utilisés. Par exemple (et idéalement, du point de vue de la sécurité), un serveur peut spécifier que tous les contenus doivent être chargés à l'aide de HTTPS.
- CSP aide à sécuriser Citrix ADC contre les attaques par script intersite en sécurisant des fichiers tels que "tmindex.html" et « homepage.html ». Le fichier "tmindex.html" est lié à l'authentification et le fichier "homepage.html" est lié aux applications/liens publiés.

Configuration de l'en-tête Content-Security-Policy pour Citrix Gateway et les réponses générées par le serveur virtuel d'authentification

Pour activer l'en-tête CSP, vous devez configurer votre serveur Web pour renvoyer l'en-tête HTTP CSP.

> **Points à noter**
>
> 1. Par défaut, l'en-tête CSP est désactivé.
> 2. Lors de l'activation/de la désactivation de la stratégie CSP par défaut, il est recommandé d'exécuter la commande suivante. `Flush cache contentgroup loginstaticobjects`
>
> 3. Pour modifier la stratégie CSP pour tmindex.html, homepage.html, etc., il est recommandé de la modifier `httpd.conf`. Pour modifier `httpd.conf`, ouvrez `httpd.conf` dans n'importe quel éditeur XML, faites défiler jusqu'à la balise **DirectoryMatch** et recherchez les répertoires suivants, « /netscaler/ns_gui/vpns », « /netscaler/ns_gui/epa », puis modifiez « Header set Content-Security-Policy ».

Pour configurer CSP pour le serveur virtuel d'authentification et les réponses générées par Citrix Gateway à l'aide de l'interface de ligne de commande, tapez la commande suivante à l'invite de commandes :

```
1 set aaa parameter -defaultCSPHeader <ENABLE/DISABLE>
```

Pour configurer CSP pour Citrix Gateway et les réponses générées par le serveur virtuel d'authentification à l'aide de l'interface graphique.

1. Accédez à **Citrix Gateway > Paramètres globaux**, cliquez sur **Modifier les paramètres AAA** d'authentification sous Paramètres d'authentification.



2. Sur la page **Configurer les paramètres AAA**, sélectionnez le **champ En-tête CSP par défaut** .



Exemple de personnalisation des en-têtes Content-Security-Policy

Voici un exemple de personnalisation des en-têtes CSP pour inclure des images et des scripts uniquement provenant des deux sources spécifiées suivantes, respectivement, `https://company.fqdn.com, https://example.com.`

Exemple de configuration

```
add rewrite action modify_csp insert_http_header Content-Security-Policy "\"default-src 'self'; script-src 'self' https://company.fqdn.com 'unsafe-inline' 'unsafe-eval'; connect-src 'self'; img-src http://localhost:* https://example.com 'self' data: http: https:; style-src 'self' 'unsafe-inline'; font-src 'self'; frame-src 'self'; child-src 'self' com.citrix.agmacepa://* citrixng://* com.citrix.nsgclient://*; form-action 'self'; object-src 'self'; report-uri /nscsp_violation/report_uri\""

add rewrite policy add_csp true modify_csp

bind authentication vserver auth1 -policy add_csp -priority 1 -gotoPriorityExpression NEXT -type AAA_RESPONSE
```

Réinitialisation du mot de passe

August 20, 2021

La réinitialisation des mots de passe en libre-service est une solution de gestion des mots de passe basée sur le Web. Il est disponible dans les fonctions d'authentification, d'autorisation et d'audit de Citrix ADC et Citrix Gateway. Il élimine la dépendance de l'utilisateur à l'égard de l'assistance de l'administrateur pour changer le mot de passe.

La réinitialisation du mot de passe en libre-service permet à l'utilisateur final de réinitialiser ou de créer un mot de passe en toute sécurité dans les scénarios suivants :

- L'utilisateur a oublié le mot de passe.
- L'utilisateur ne peut pas ouvrir de session.

Jusqu'à présent, si un utilisateur final oublie un mot de passe AD, l'utilisateur final devait contacter l'administrateur AD pour réinitialiser le mot de passe. Grâce à la fonctionnalité de réinitialisation de mot de passe en libre-service, un utilisateur final peut réinitialiser le mot de passe sans intervention d'un administrateur.

Voici quelques-uns des avantages de l'utilisation de la réinitialisation de mot de passe en libre-service :

- Augmentation de la productivité grâce au mécanisme de changement automatique de mot de passe, ce qui élimine le délai pour les utilisateurs d'attendre la réinitialisation du mot de passe.
- Grâce au mécanisme automatique de changement de mot de passe, les administrateurs peuvent se concentrer sur d'autres tâches critiques.

La figure suivante illustre le flux de réinitialisation du mot de passe en libre-service pour réinitialiser le mot de passe.



Pour utiliser la réinitialisation du mot de passe en libre-service, un utilisateur doit être enregistré avec l'authentification, l'autorisation et l'audit Citrix ou avec le serveur virtuel Citrix Gateway.

La réinitialisation du mot de passe en libre-service offre les fonctionnalités suivantes :

- **Auto-inscription des nouveaux utilisateurs.** Vous pouvez vous inscrire automatiquement en tant que nouvel utilisateur.
- **Configurer les questions basées sur les connaissances.** En tant qu'administrateur, vous pouvez configurer un ensemble de questions pour les utilisateurs.
- **Enregistrement de l'ID de courriel alternatif.** Vous devez fournir un autre ID de courriel lors de l'inscription. L'OTP est envoyé à l'ID de messagerie secondaire car l'utilisateur a oublié le mot de passe principal de l'ID de messagerie.

> **Remarque :**
>
> À partir de la version 12.1 build 51.xx, l'enregistrement alternatif de l'ID d'e-mail peut être effectué en tant que autonome. Un nouveau Loginschema, **AlteMailRegister.xml** est in-

> troduit pour effectuer uniquement l'enregistrement d'ID de courriel alternatif. Auparavant, l'enregistrement d'un identifiant de messagerie alternatif ne pouvait être effectué que lors de l'enregistrement KBA.

- **Réinitialiser le mot de passe oublié.** L'utilisateur peut réinitialiser le mot de passe en répondant aux questions basées sur les connaissances. En tant qu'administrateur, vous pouvez configurer et stocker les questions.

La réinitialisation du mot de passe en libre-service fournit les deux nouveaux mécanismes d'authentification suivants :

- **Question et réponse fondée sur les connaissances.** Vous devez vous inscrire à l'authentification Citrix, à l'autorisation et à l'audit ou à un Citrix Gateway avant de sélectionner le schéma de questions et réponses basé sur les connaissances.
- **Authentification OTP par e-mail.** Un OTP est envoyé à l'ID de messagerie secondaire, que l'utilisateur a enregistré lors de l'enregistrement en libre-service de réinitialisation du mot de passe.

> **Remarque**
>
> Ces mécanismes d'authentification peuvent être utilisés pour les cas d'utilisation de réinitialisation de mot de passe en libre-service, et à des fins d'authentification similaires à n'importe quel mécanisme d'authentification existant.

Conditions préalables

Avant de configurer la réinitialisation du mot de passe en libre-service, vérifiez les conditions préalables suivantes :

- Fonctionnalité Citrix ADC version 12.1, build 50.28.
- La version prise en charge est le niveau de fonction de domaine AD 2016, 2012 et 2008.
- Le nom d'utilisateur LdAPBind lié au Citrix ADC doit disposer d'un accès en écriture au chemin AD des utilisateurs.

> **Remarque**
> La réinitialisation du mot de passe en
> libre-service est prise en charge dans le flux d'authentification nFactor uniquement. Pour plus d'informations, voir Authentification nFactor via Citrix ADC.

Limitations

Voici quelques-unes des limitations de la réinitialisation du mot de passe en libre-service :

- La réinitialisation du mot de passe en libre-service n'est disponible que si le principal d'authentification est LDAP.
- L'utilisateur ne peut pas voir l'ID de messagerie secondaire déjà enregistré.
- Les questions et réponses basées sur les connaissances, et l'authentification et l'enregistrement OTP par courriel ne peuvent pas être le premier facteur dans le flux d'authentification.
- Pour Native Plug-in et Receiver, l'enregistrement est pris en charge uniquement via le navigateur.
- La taille minimale du certificat utilisée pour la réinitialisation du mot de passe en libre-service est de 1024 octets et doit respecter la norme x.509.

Paramètre Active Directory

La question et réponse basée sur les connaissances Citrix ADC et e-mail OTP utilise l'attribut AD pour stocker les données des utilisateurs. Vous devez configurer un attribut AD pour stocker les questions et réponses ainsi que l'ID de messagerie alternatif. L'appliance Citrix ADC le stocke dans l'attribut KB configuré dans l'objet utilisateur AD. Lors de la configuration d'un attribut AD, tenez compte des éléments suivants :

- La longueur de l'attribut doit comporter au moins 128 caractères.
- L'attribut AD doit prendre en charge la valeur 32k de longueur maximale.
- Le type d'attribut doit être un 'DirectoryString'.
- Un seul attribut AD peut être utilisé pour les questions et réponses basées sur les connaissances et les identifiants de messagerie alternatifs.
- Un seul attribut AD ne peut pas être utilisé pour l'enregistrement de questions et réponses basées sur les connaissances ou d'autres identifiants de messagerie.
- L'administrateur LDAP Citrix ADC doit disposer d'un accès en écriture à l'attribut AD sélectionné.

Vous pouvez également utiliser un attribut AD existant. Cependant, assurez-vous que l'attribut que vous envisagez d'utiliser n'est pas utilisé dans d'autres cas. Par exemple, UserParameters est un attribut existant au sein de l'utilisateur AD que vous pouvez utiliser. Pour vérifier cet attribut, effectuez les opérations suivantes :

1. Accédez à **ADSI > sélectionner l'utilisateur**.
2. Cliquez avec le bouton droit et faites défiler jusqu'à la liste des attributs.
3. Dans le volet de fenêtre **CN=TestUser Properties**, vous pouvez voir que l'attribut **UserParameters** n'est pas défini.



Enregistrement de réinitialisation du mot de passe en libre-service

Pour implémenter une solution de réinitialisation de mot de passe en libre-service sur une appliance Citrix ADC, vous devez effectuer les opérations suivantes :

- Réinitialisation du mot de passe en libre-service (question basée sur les connaissances et identificateur de réponse/e-mail).
- Page d'ouverture de session de l'utilisateur (pour la réinitialisation du mot de passe, qui inclut les questions et réponses basées sur les connaissances, la validation OTP et le facteur de réinitialisation final du mot de passe).

Un ensemble de catalogue de questions prédéfinies est fourni sous forme de fichier JSON. En tant qu'administrateur, vous pouvez sélectionner les questions et créer un schéma de connexion d'enregistrement de réinitialisation de mot de passe en libre-service via l'interface graphique Citrix ADC. Vous pouvez choisir l'une des options suivantes :

- Sélectionnez un maximum de quatre questions définies par le système.
- Offrez aux utilisateurs la possibilité de personnaliser deux questions et réponses.

Pour afficher le fichier JSON de questions basées sur les connaissances par défaut à partir de l'interface de ligne de commande

```
root@ns# cd /nsconfig/loginschema/LoginSchema/
root@ns# cat KBQuestions.json
[
    {"question":"What is the last name of the teacher who gave you your first failing
grade?"},
    {"question":"What is the name of your favourite childhood friend?"},
    {"question":"Where were you when you first heard about 9/11?"},
    {"question":"What is the name of a college you applied to but didn't attend?"},
    {"question":"What was the last name of your third grade teacher?"},
    {"question":"What was the name of your first stuffed animal?"},
    {"question":"What is the name of the teacher who gave you your first A?"},
    {"question":"What is the name of the city where you got lost?"},
    {"question":"In what city or town did your mother and father meet?"},
    {"question":"What was your most hated food as a child?"},
    {"question":"What was your most favourite food as a child?"},
    {"question":"What is your favourite website?"},
    {"question":"What is your most disliked website?"},
    {"question":"What is your dream job?"},
    {"question":"Why did the chicken cross the road?"},
    {"question":"Name your first boss."},
    {"question":"What is the name of your favorite school teacher?"},
    {"question":"What is the name of your favorite actor or actress?"},
    {"question":"What is the title of your favorite movie?"},
    {"question":"In what city or town did you spend most of your youth?"}
]
```

Remarque

- Citrix Gateway inclut l'ensemble de questions définies par le système par défaut. L'administrateur peut modifier le fichier « KBQuestions.json » pour inclure son choix de questions.
- Les questions définies par le système sont affichées uniquement en anglais et la prise en charge de la localisation de la langue n'est pas disponible pour ces questions.

Pour terminer l'enregistrement des questions et réponses basée sur les connaissances Login Schema à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA — Trafic des applications > Schéma de connexion**.



2. Dans la page **Schéma de connexion**, cliquez sur **Profils** .
3. Cliquez sur **Ajouter un schéma de connexion d'enregistrement KBA**.
4. Dans la page **Créer un schéma de connexion d'authentification**, spécifiez un nom dans le champ **Nom du schéma** .





5. Sélectionnez les questions de votre choix et déplacez-les dans la liste **Configuré** .
6. Dans la section **Questions définies par l'utilisateur**, vous pouvez fournir des questions et des réponses dans les champs Q1 et A1.



7. Dans la section **Enregistrement par e-mail**, cochez l'option **Enregistrer un autre courriel** . Vous pouvez enregistrer l'**ID de courriel alternatif** à partir de la page d'ouverture de session d'enregistrement de l'utilisateur pour recevoir l'OTP.



8. Cliquez sur **Créer**. Le schéma de connexion une fois généré affiche toutes les questions configurées à l'utilisateur final pendant le processus d'inscription.

Créer un flux de travail d'enregistrement et de gestion des utilisateurs à l'aide de l'interface

Les éléments suivants sont requis avant de commencer la configuration :

- Adresse IP attribuée au serveur virtuel d'authentification
- FQDN correspondant à l'adresse IP attribuée
- Certificat de serveur pour l'authentification serveur virtuel

Pour configurer la page d'enregistrement et de gestion des périphériques, vous avez besoin d'un serveur virtuel d'authentification. La figure suivante illustre l'enregistrement de l'utilisateur.



Pour créer un serveur virtuel d'authentification

1. Configurez un serveur virtuel d'authentification. Il doit être de type SSL et assurez-vous de lier l'authentification serveur virtuel avec le thème du portail.


```
> add authentication vserver <vServerName> SSL <ipaddress> <port>
> bind authentication vserver <vServerName> [-portaltheme<string>]
```

2. Liez la paire de clés de certificat du serveur virtuel SSL.

```
> bind ssl vserver <vServerName> certkeyName <string>
```

Exemple :

```
> add authentication vserver authvs SSL 1.2.3.4 443
> bind authentication vserver authvs -portaltheme RFWebUI
> bind ssl vserver authvs -certkeyname c1
```

Pour créer une action d'ouverture de session LDAP

```
    > add authentication ldapAction <name> {
-serverIP <ipaddr|ipv6_addr|> [-serverPort <port>] [-ldapBase <BASE> ]
     [-ldapBindDn <AD USER>] [-ldapBindDnPassword <PASSWORD>] [-
    ldapLoginName <USER FORMAT>]
```

> **Remarque**
>
> Vous pouvez configurer n'importe quelle stratégie d'authentification comme premier facteur.

Exemple :

```
    > add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4
      -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -
     ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword
     PASSWORD -ldapLoginName samAccountName -serverport 636 -sectype
     SSL -KBAttribute userParameters
```

Pour créer une stratégie d'authentification pour l'ouverture de session LDAP

```
    > add authentication policy <name> <rule> [<reqAction]
```

Exemple :

```
    > add authentication policy ldap_logon -rule true -action
      ldap_logon_action
```


Pour créer une action d'enregistrement de questions et réponses basée sur les connaissances

Deux nouveaux paramètres sont introduits dans ldapaction. « KBatTribute » pour l'authentification KBA (enregistrement et validation) et « AlternateEmailAttr » pour l'enregistrement de l'ID e-mail alternatif de l'utilisateur.

```
1     > add authentication ldapAction <name> {
2  -serverIP  <ipaddr|ipv6_addr|> [-serverPort <port>] [-ldapBase <BASE>
      ] [-ldapBindDn <AD USER>] [-ldapBindDnPassword <PASSWORD>] [-
      ldapLoginName <USER FORMAT>] [-KBAttribute <LDAP ATTRIBUTE>] [-
      alternateEmailAttr <LDAP ATTRIBUTE>]
```

Exemple :

```
1     > add authentication ldapAction ldap1 -serverIP 1.2.3.4 -sectype
         ssl -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -
         ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword
         PASSWORD -ldapLoginName samAccountName -KBAttribute
         userParameters -alternateEmailAttr userParameters
```

Afficher l'écran d'enregistrement et de gestion des utilisateurs

Le schéma de connexion « KbaRegistrationSchema.xml » est utilisé pour afficher la page d'enregistrement de l'utilisateur à l'utilisateur final. Utilisez l'interface de ligne de commande suivante pour afficher le schéma de connexion.

```
1 > add authentication loginSchema <name> -authenticationSchema <string>
```

Exemple :

```
1 > add authentication loginSchema kba_register -authenticationSchema /
     nsconfig/loginschema/LoginSchema/KBARegistrationSchema.xml
```

Citrix recommande deux façons d'afficher l'écran d'enregistrement et de gestion des utilisateurs : URL ou attribut LDAP.

Utilisation de l'URL

Si le chemin d'accès à l'URL contient '/register' (par exemple,https://lb1.server.com/register), la page d'enregistrement de l'utilisateur s'affiche à l'aide de l'URL.

Pour créer et lier une stratégie d'inscription


```
> add authentication policylabel user_registration -loginSchema
    kba_register
> add authentication policy ldap1 -rule true -action ldap1
> bind authentication policylabel user_registration -policy ldap1 -
    priority 1
```

Pour lier la stratégie d'authentification à l'authentification, l'autorisation et l'audit du serveur virtuel lorsque l'URL contient '/register'

```
> add authentication policy ldap_logon -rule "http.req.cookie.value(\"
    NSC_TASS\").contains(\"register\")" -action ldap_logon
> bind authentication vserver authvs -policy ldap_logon -nextfactor
    user_registration -priority 1
```

Pour lier un certificat au VPN global

```
bind vpn global -userDataEncryptionKey c1
```

> **Remarque**
>
> Vous devez lier le certificat pour chiffrer les données utilisateur (Q&R et ID de messagerie alternatif enregistré) stockées dans l'attribut AD.

Utilisation de l'attribut

Vous pouvez lier la stratégie d'authentification au serveur virtuel d'authentification, d'autorisation et d'audit pour vérifier si l'utilisateur est déjà inscrit ou non. Dans ce flux, toutes les stratégies précédentes avant le facteur d'enregistrement des questions et réponses basées sur les connaissances doivent être LDAP avec attribut KBA configuré. Ceci permet de vérifier si l'utilisateur AD est enregistré ou n'utilise pas un attribut AD.

> **Important**
>
> La règle « AAA.USER.ATTRIBUTE (« kba_registered ») .EQ (« 0") » oblige les nouveaux utilisateurs à s'inscrire aux questions et réponses basées sur les connaissances et aux e-mails alternatifs.

Pour créer une stratégie d'authentification pour vérifier si l'utilisateur n'est pas déjà enregistré

```
> add authentication policy switch_to_kba_register -rule "AAA.USER.
    ATTRIBUTE(\"kba_registered\").EQ(\"0\")" -action NO_AUTHN
```



```
2 > add authentication policy first_time_login_forced_kba_registration -
    rule true -action ldap1
```

Pour créer une étiquette de stratégie d'enregistrement et lier à la stratégie d'enregistrement LDAP

```
1 > add authentication policylabel auth_or_switch_register -loginSchema
    LSCHEMA_INT
2 > add authentication policylabel kba_registration -loginSchema
    kba_register
3
4 > bind authentication policylabel auth_or_switch_register -policy
    switch_to_kba_register -priority 1 -nextFactor kba_registration
5 > bind authentication policylabel kba_registration -policy
    first_time_login_forced_kba_registration -priority 1
```

Pour lier la stratégie d'authentification à l'authentification, à l'autorisation et à l'audit du serveur virtuel

```
1 bind authentication vserver authvs -policy ldap_logon -nextfactor
    auth_or_switch_register -priority 2
```

Enregistrement des utilisateurs et validation de la gestion

Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, vous devriez voir les captures d'écran de l'interface utilisateur ci-dessous.

1. Entrez l'URL lb vserver ; par exemple https://lb1.server.com. L'écran d'ouverture de session s'affiche.



2. Entrez le nom d'utilisateur et le mot de passe. Cliquez sur **Soumettre**. L'écran **Enregistrement des utilisateurs** s'affiche.



3. Sélectionnez la question préférée dans la liste déroulante et entrez la **réponse**.
4. Cliquez sur **Soumettre**. L'écran d'enregistrement de l'utilisateur s'affiche.

Page Configurer l'ouverture de session utilisateur

Dans cet exemple, l'administrateur suppose que le premier facteur est l'ouverture de session LDAP (pour laquelle l'utilisateur final a oublié le mot de passe). L'utilisateur suit ensuite l'enregistrement des questions et réponses basée sur les connaissances et la validation OTP de l'ID d'e-mail, et réinitialise finalement le mot de passe en utilisant la réinitialisation du mot de passe en libre-service.

Vous pouvez utiliser n'importe quel mécanisme d'authentification pour réinitialiser le mot de passe en libre-service. Citrix recommande d'avoir une question et une réponse basées sur les connaissances, et d'envoyer un e-mail à OTP ou les deux pour obtenir une confidentialité solide et éviter toute réinitialisation de mot de passe utilisateur illégitime.

Les éléments suivants sont requis avant de commencer à configurer la page d'ouverture de session de l'utilisateur :

- IP du serveur virtuel d'équilibrage de charge
- FQDN correspondant pour le serveur virtuel d'équilibrage de charge
- Certificat de serveur pour l'équilibreur de charge

Créer un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

Pour accéder au site Web interne, vous devez créer un serveur virtuel LB pour accéder au service principal et déléguer la logique d'authentification au serveur virtuel d'authentification.

```
> add lb vserver lb1 SSL 1.2.3.162 443 -persistenceType NONE -
   cltTimeout 180 -AuthenticationHost otpauth.server.com -
   Authentication ON -authnVsName authvs

> bind ssl vserver lb1 -certkeyname c1
```

Pour représenter le service principal dans l'équilibrage de charge :

```
> add service iis_backendsso_server_com 1.2.3.4 HTTP 80

> bind lb vserver lb1 iis_backendsso_server_com
```

Créer une action LDAP avec l'authentification désactivée en tant que première stratégie

```
> add authentication ldapAction ldap3 -serverIP 1.2.3.4 -serverPort 636
    -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
   administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
   ldapLoginName samAccountName -authentication disabled

> add authentication policy ldap3 -rule aaa.LOGIN.VALUE("passwdreset").
   EQ("1") -action ldap3
```

Créer une action de validation des questions et réponses basée sur les connaissances

Pour la validation des questions et réponses basée sur les connaissances dans le flux de réinitialisation des mots de passe en libre-service, vous devez configurer le serveur LDAP avec l'authentification désactivée.

```
> add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP
   > -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
   ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
   KBAttribute  <LDAP ATTRIBUTE> - alternateEmailAttr <LDAP ATTRIBUTE>
   -authentication DISABLED
```

Exemple :

```
> add authentication ldapAction ldap2 -serverIP 1.2.3.4 -serverPort 636
    -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
```



```
administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
ldapLoginName samAccountName -KBAttribute userParameters -
alternateEmailAttr userParameters -authentication disabled
```

Pour créer une stratégie d'authentification pour la validation des questions et réponses basée sur les connaissances à l'aide de l'interface de ligne de commande

```
add authentication policy kba_validation -rule true -action ldap2
```

Créer une action de validation par e-mail

LDAP doit être un facteur antérieur au facteur de validation des e-mails car vous avez besoin de l'ID e-mail de l'utilisateur ou de l'ID de messagerie secondaire dans le cadre de l'enregistrement de réinitialisation du mot de passe en libre-service.

> **Remarque :**
>
> Pour que la solution Email OTP fonctionne, assurez-vous que l'authentification basée sur la connexion est activée sur le serveur SMTP.

Pour vous assurer que l'authentification basée sur la connexion est activée, tapez la commande suivante sur le serveur SMTP. Si l'authentification basée sur la connexion est activée, vous remarquerez que le texte **AUTH LOGIN** apparaît en gras dans la sortie.

```
root@ns# telnet <IP address of the SMTP server><Port number of the
   server>
ehlo
```

Exemple :

```
root@ns# telnet 10.106.3.66 25
Trying 10.106.3.66...
Connected to 10.106.3.66.
Escape character is '^]'.
220 E2K13.NSGSanity.com Microsoft ESMTP MAIL Service ready at Fri, 22
   Nov 2019 16:24:17 +0530
ehlo
250-E2K13.NSGSanity.com Hello [10.221.41.151]
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
```



```
250-X-ANONYMOUSTLS
250-AUTH LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
```

Pour plus d'informations sur l'activation de l'authentification basée sur la connexion, reportez-vous à la section https://support.microfocus.com/kb/doc.php?id=7020367.

Pour configurer une action de messagerie à l'aide de l'interface de ligne de commande

```
add authentication emailAction emailact -userName sender@example.com -
    password <Password> -serverURL "smtps://smtp.example.com:25" -
    content "OTP is $code"
```

Exemple :

```
add authentication emailAction email -userName testmail@gmail.com -
    password 298
    a34b1a1b7626cd5902bbb416d04076e5ac4f357532e949db94c0534832670 -
    encrypted -encryptmethod ENCMTHD_3 -serverURL "smtps
    ://10.19.164.57:25" -content "OTP is $code" -emailAddress "aaa.user.
    attribute(\"alternate_mail\")"
```

> **Remarque**
>
> Le paramètre « EmailAddress » dans la configuration est une expression PI. Par conséquent, cela est configuré pour prendre soit l'ID de messagerie utilisateur par défaut de la session, soit l'ID de messagerie alternatif déjà enregistré.

Pour configurer l'ID de messagerie à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA — Trafic des applications > Stratégies > Authentification > Stratégies avancées > Actions > Action par e-mail d'authentification**. Cliquez sur **Ajouter**.
2. Dans la page **Créer une action par e-mail d'authentification**, saisissez les détails et cliquez sur **Créer** .



Pour créer une stratégie d'authentification pour la validation des e-mails à l'aide de l'interface de ligne de commande

```
1 add authentication policy email_validation -rule true -action email
```

Pour créer une stratégie d'authentification pour le facteur de réinitialisation du mot de passe

```
1 add authentication policy ldap_pwd -rule true -action ldap_logon_action
```


Présentation de l'interface utilisateur via le schéma de connexion

Il y a trois LoginsSchema pour la réinitialisation du mot de passe en libre-service pour réinitialiser le mot de passe. Utilisez les commandes CLI suivantes pour afficher les trois schémas de connexion :

```
root@ns# cd  /nsconfig/loginschema/LoginSchema/
root@ns# ls -ltr | grep -i password
-r--r--r--  1 nobody  wheel  2088 Nov 13 08:38
   SingleAuthPasswordResetRem.xml
-r--r--r--  1 nobody  wheel  1541 Nov 13 08:38
   OnlyUsernamePasswordReset.xml
-r--r--r--  1 nobody  wheel  1391 Nov 13 08:38 OnlyPassword.xml
```

Pour créer une réinitialisation de mot de passe d'authentification unique à l'aide de l'interface de ligne de commande

```
> add authentication loginSchema lschema_password_reset -
   authenticationSchema "/nsconfig/loginschema/LoginSchema/
   SingleAuthPasswordResetRem.xml"

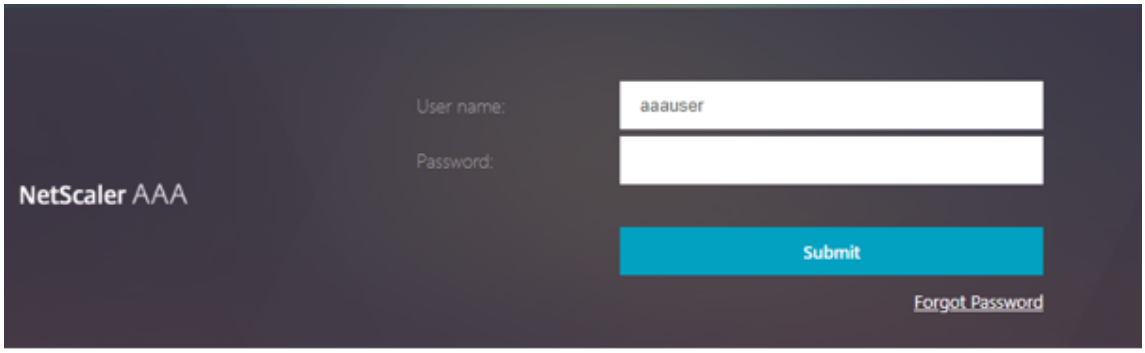
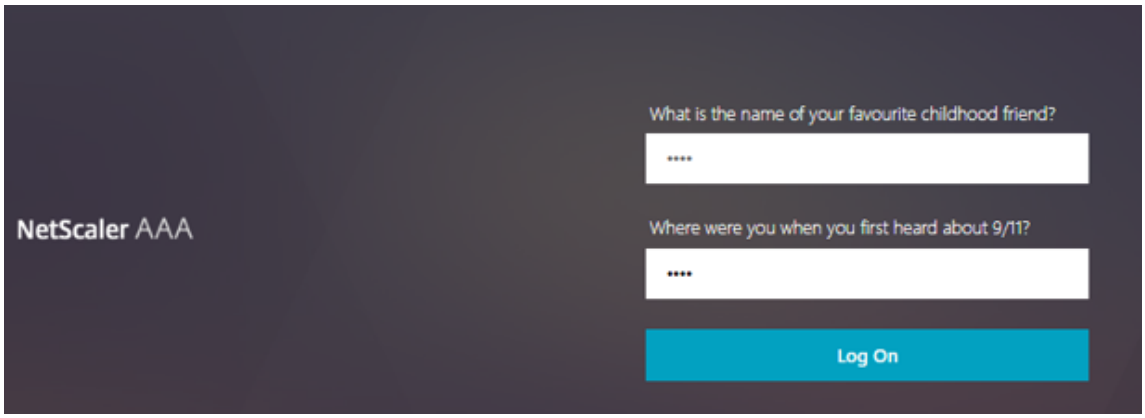
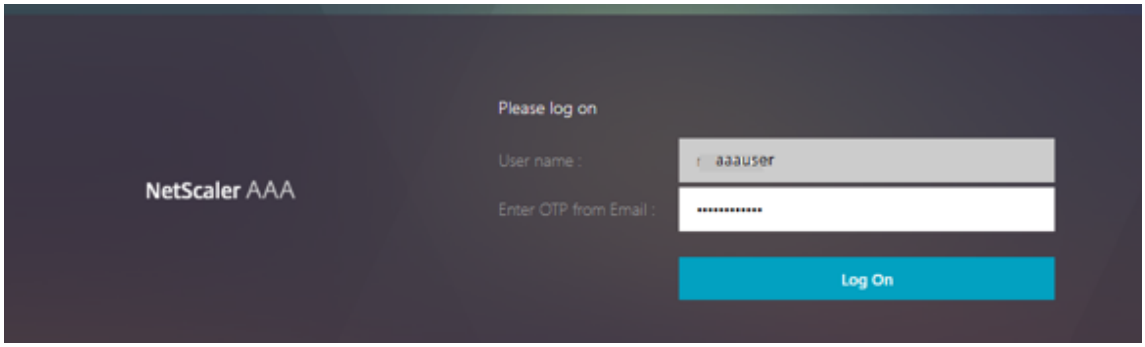
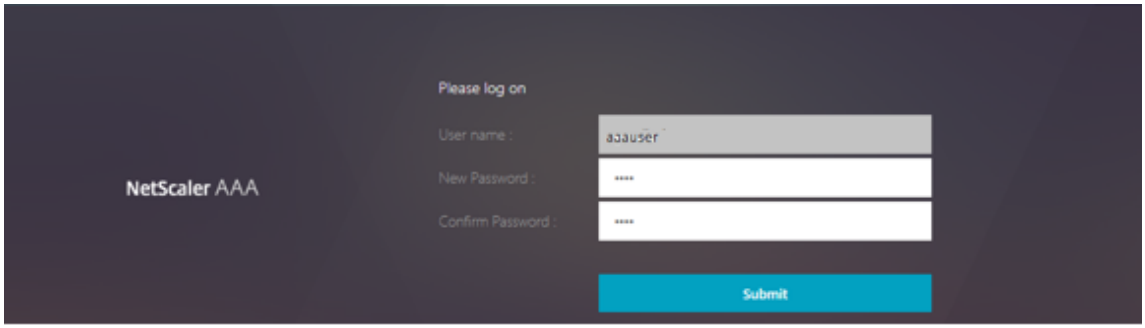
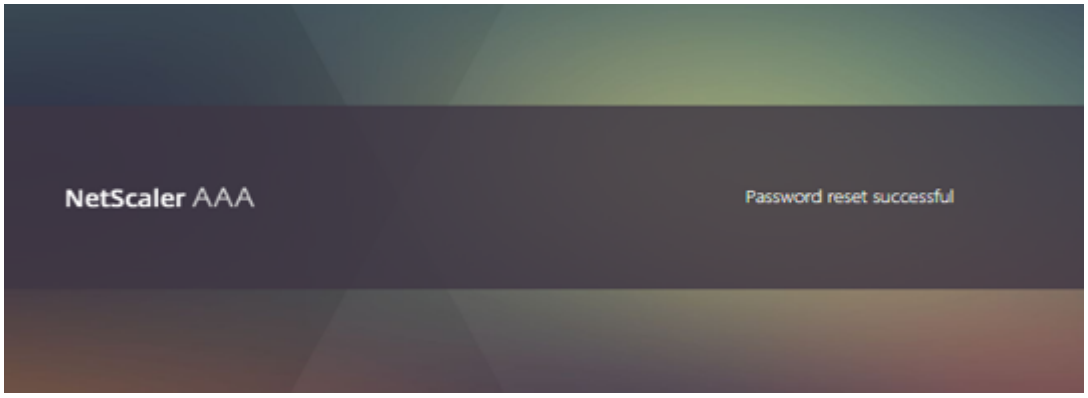
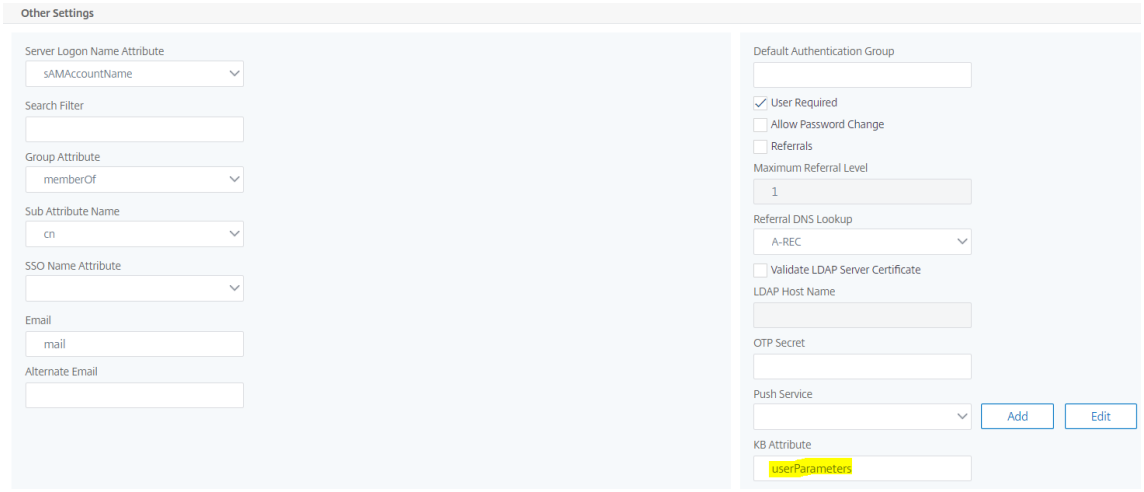
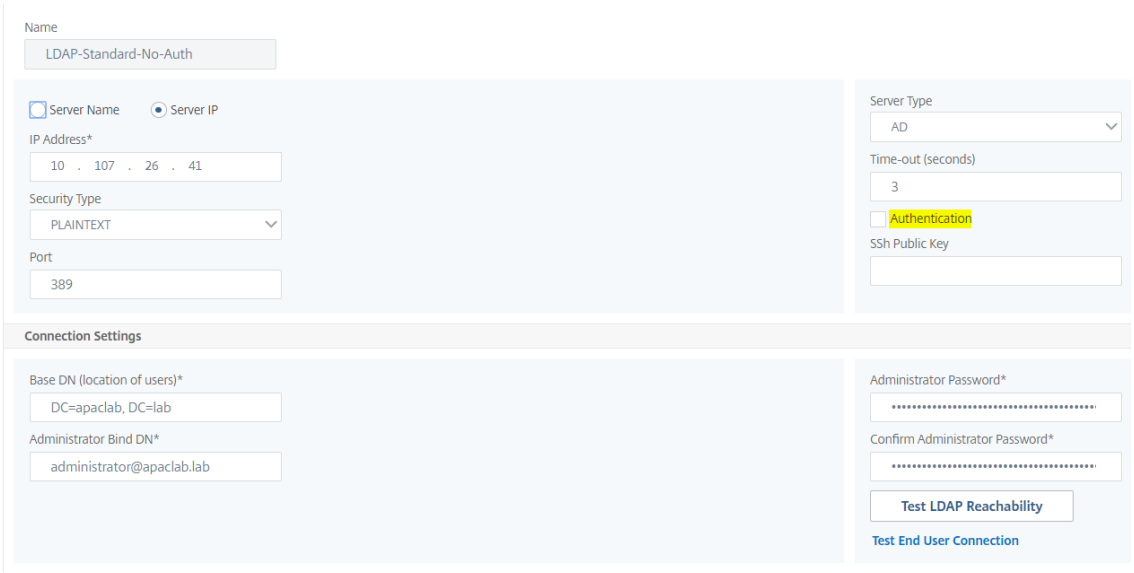
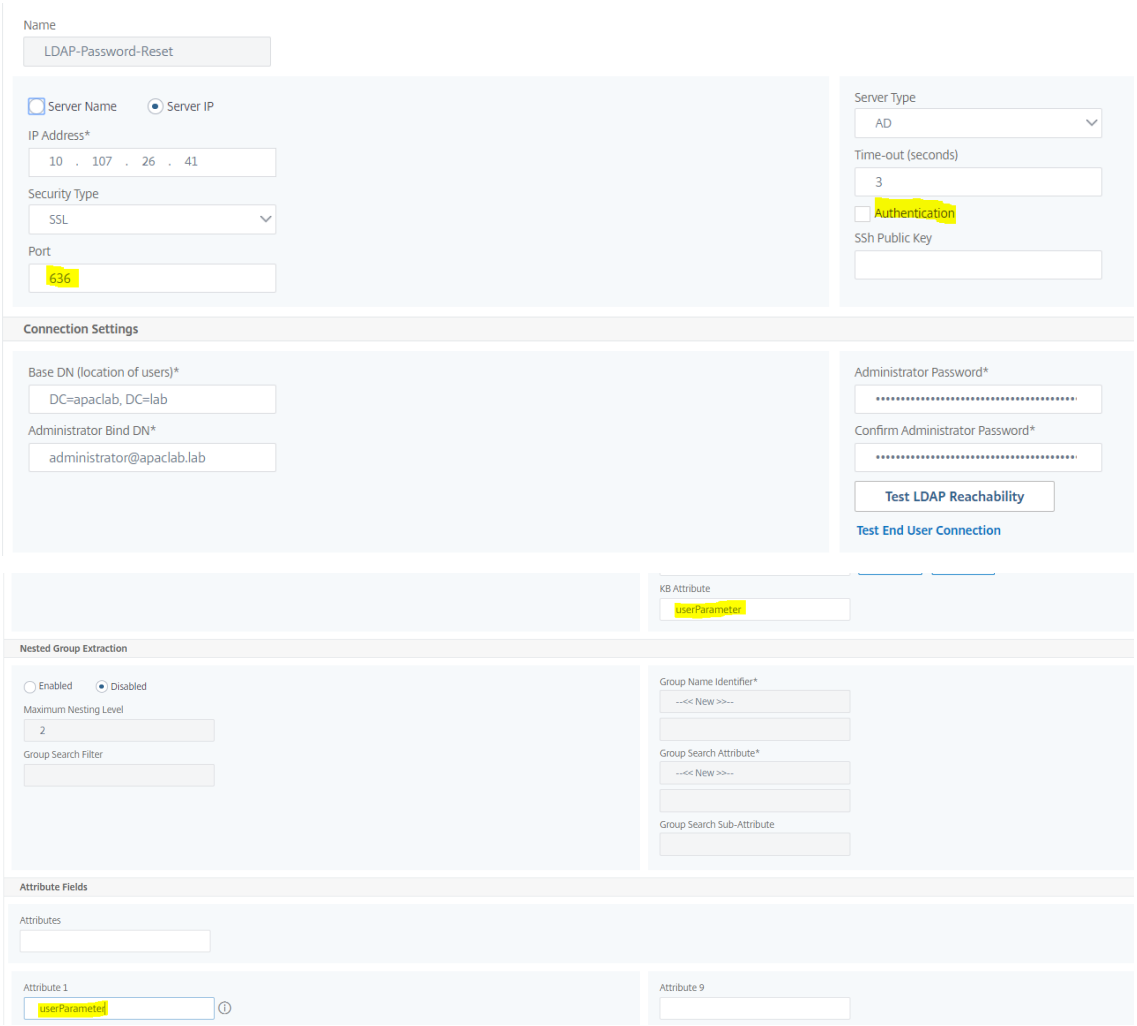
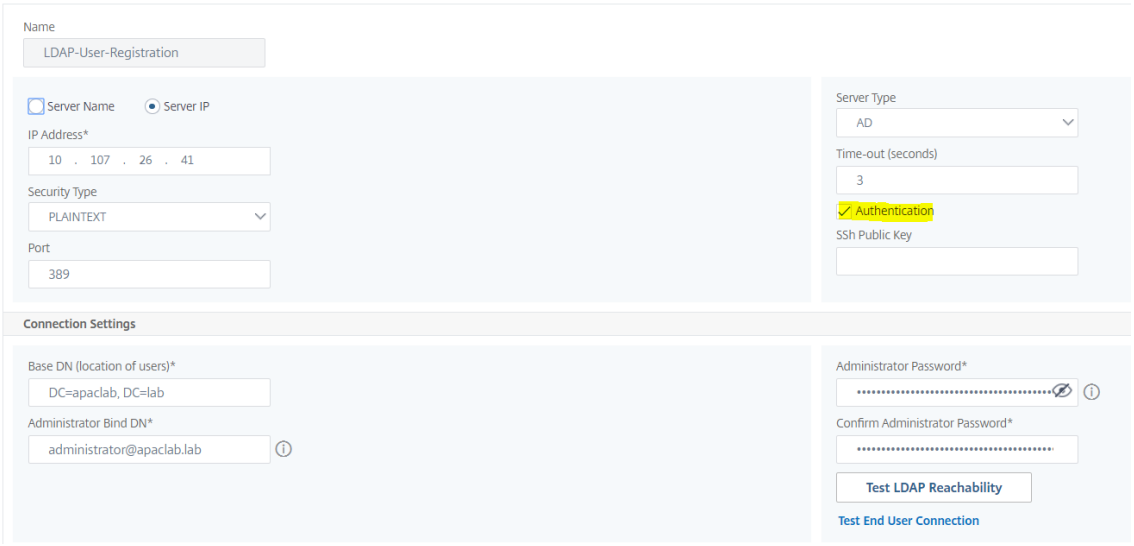
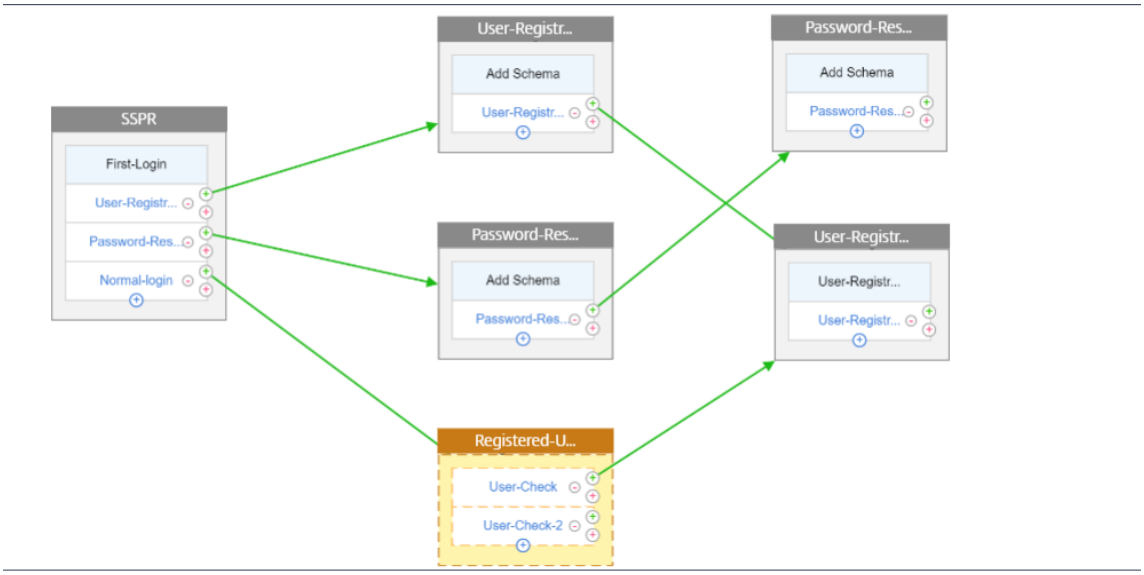
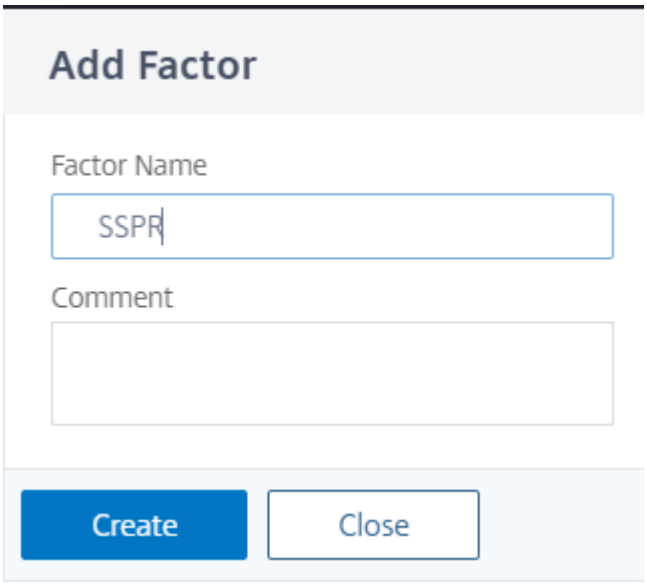
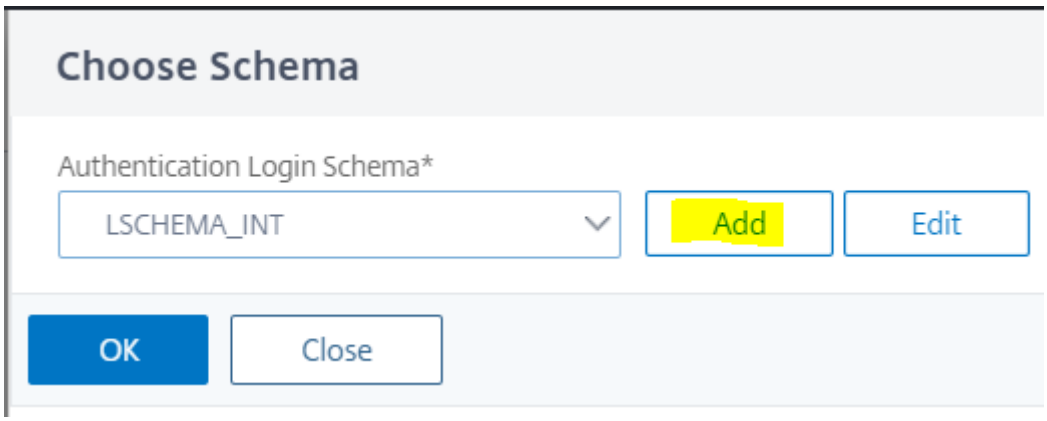
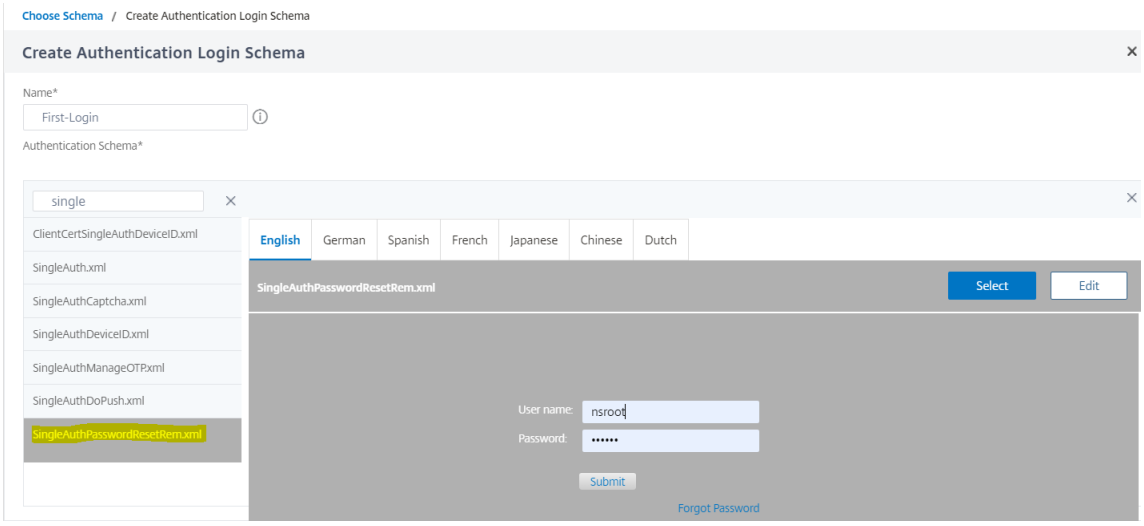
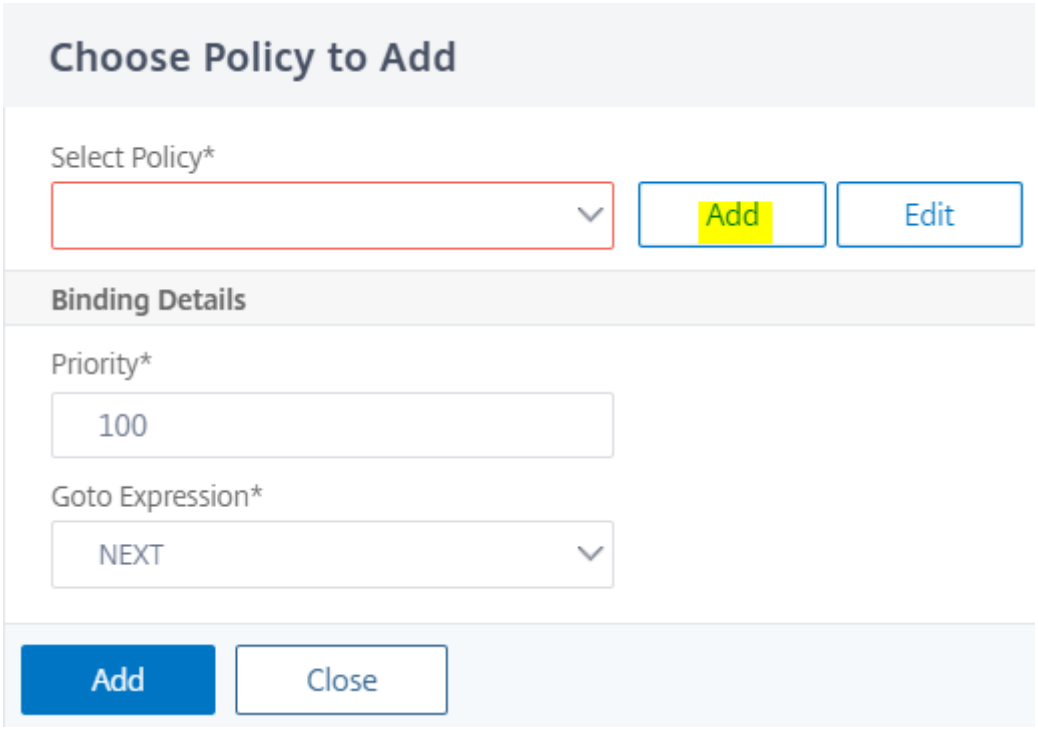
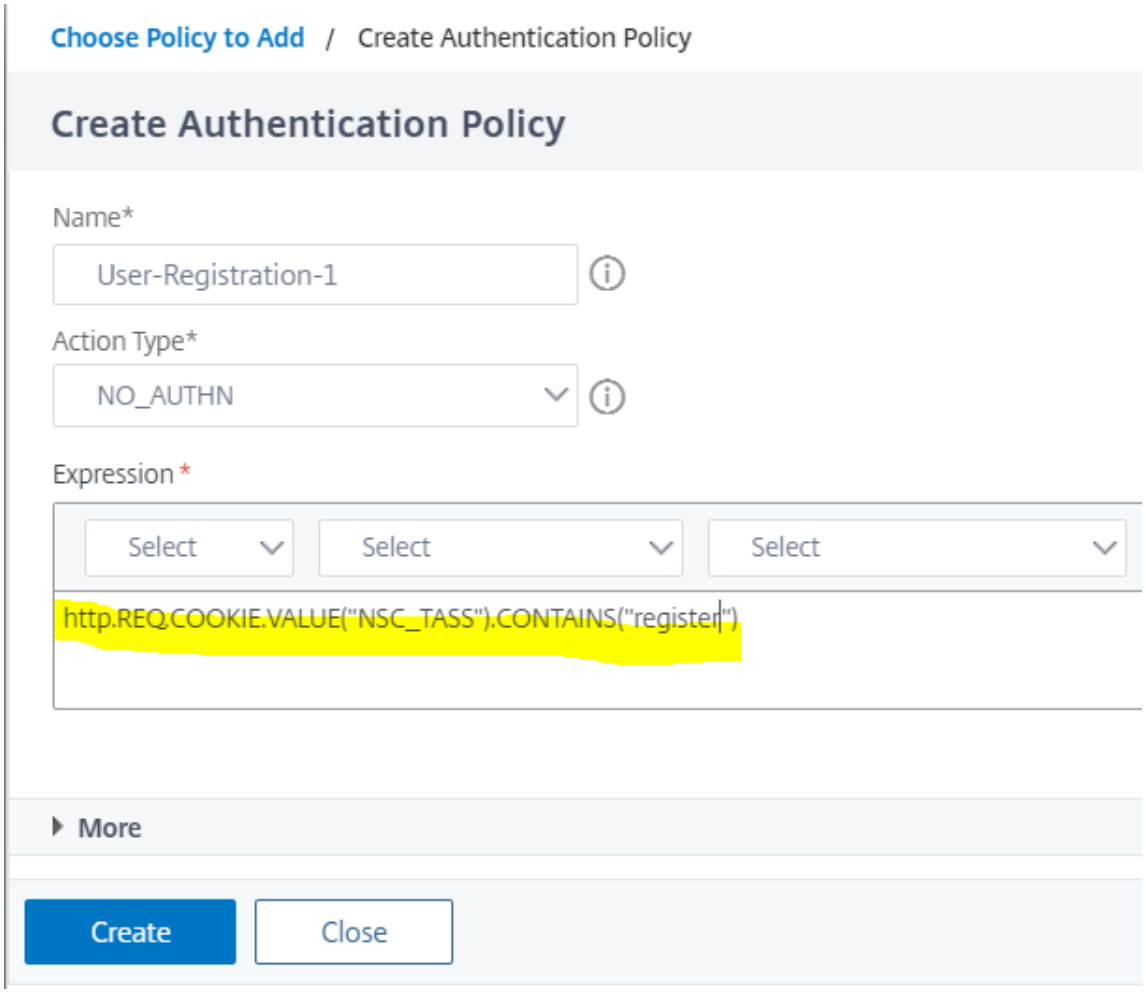
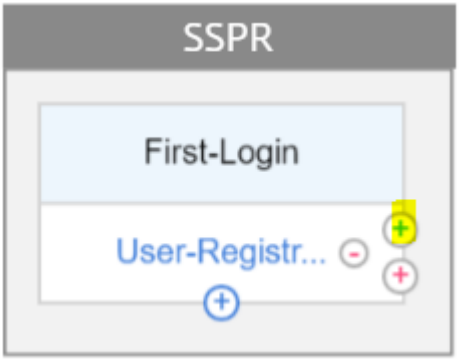
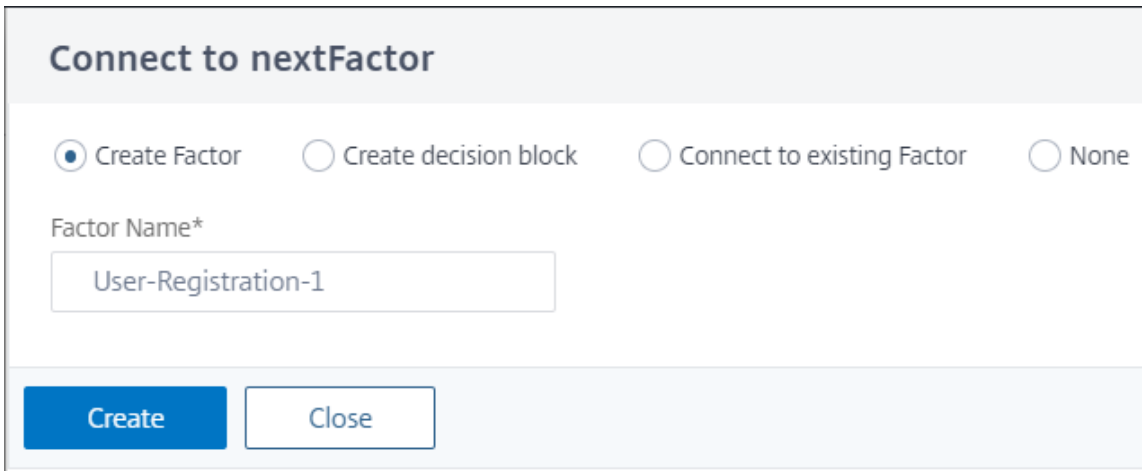
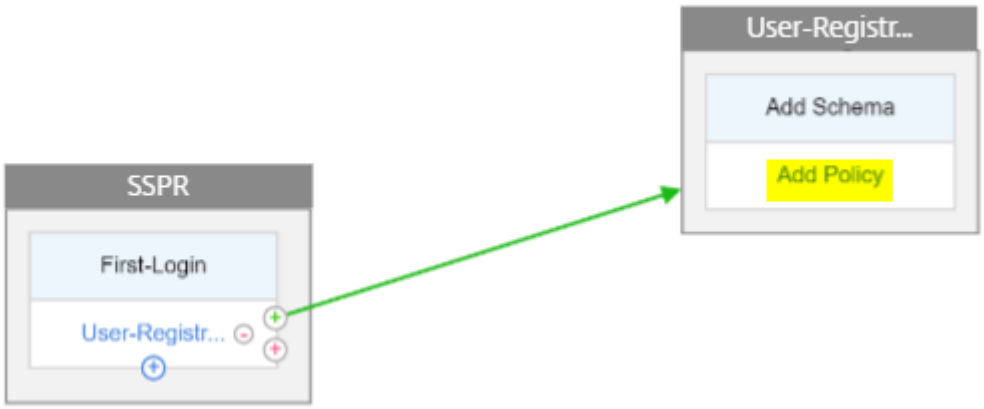
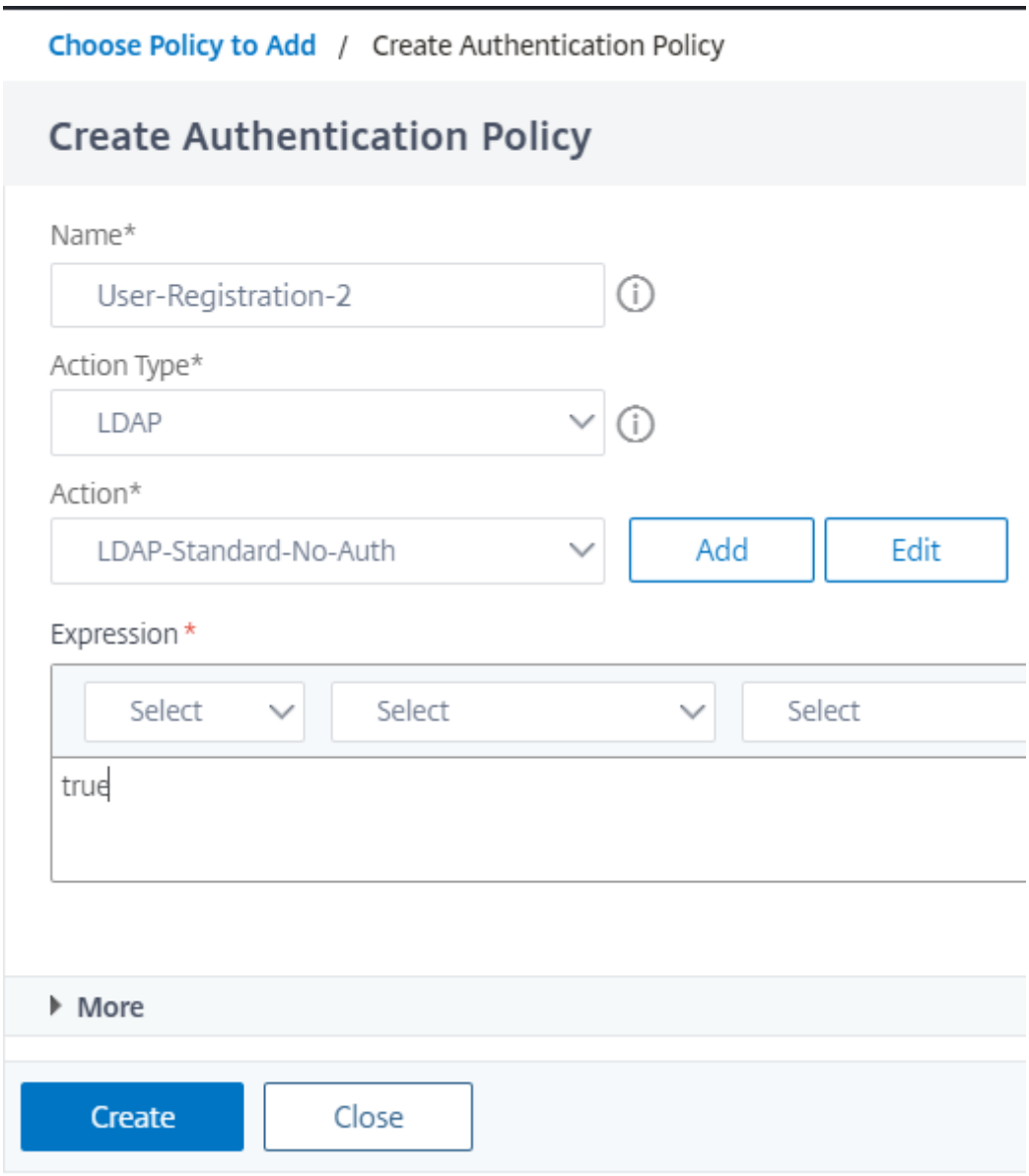
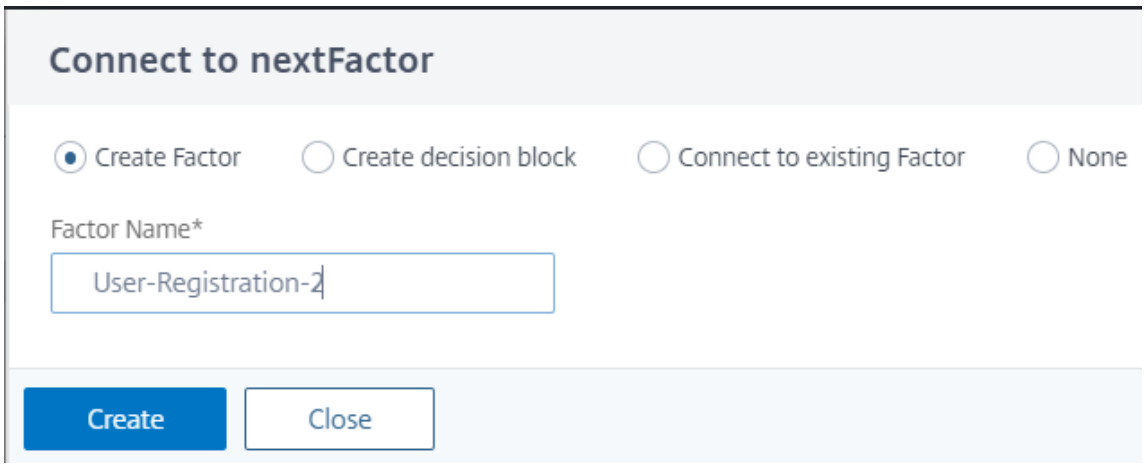
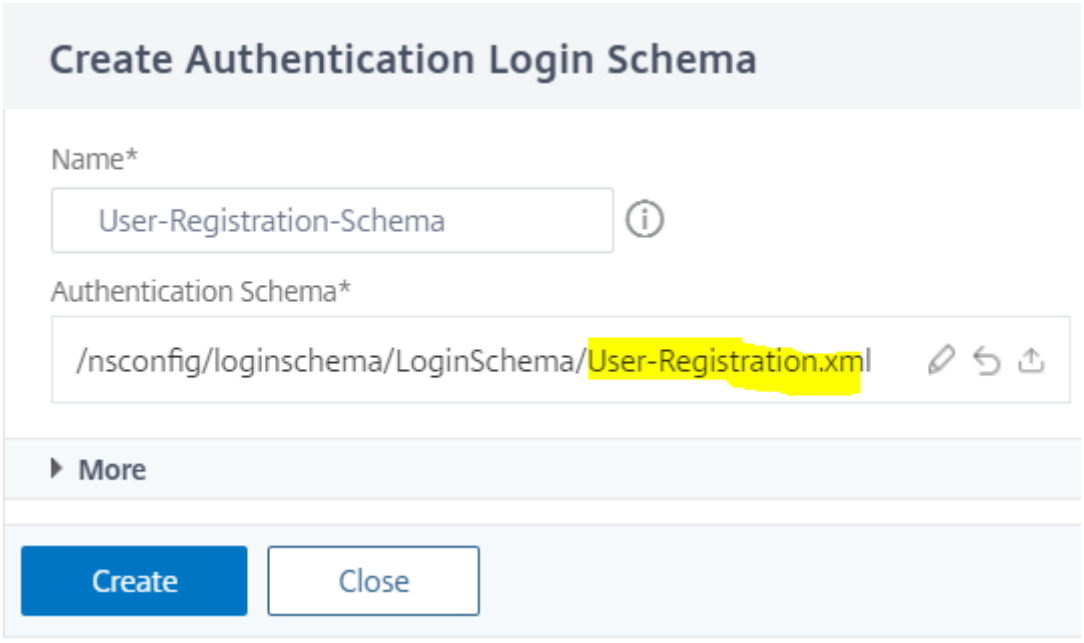
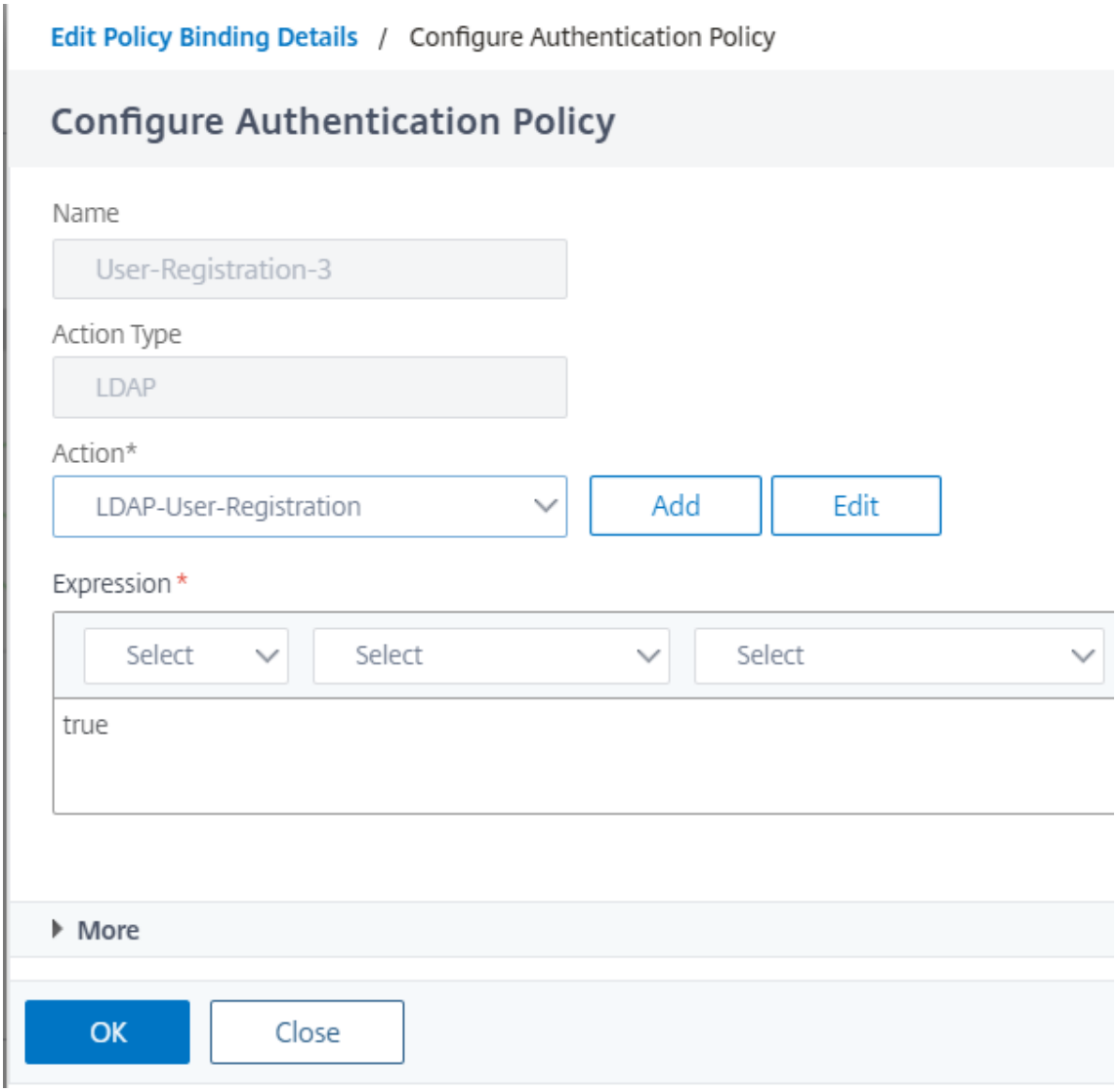
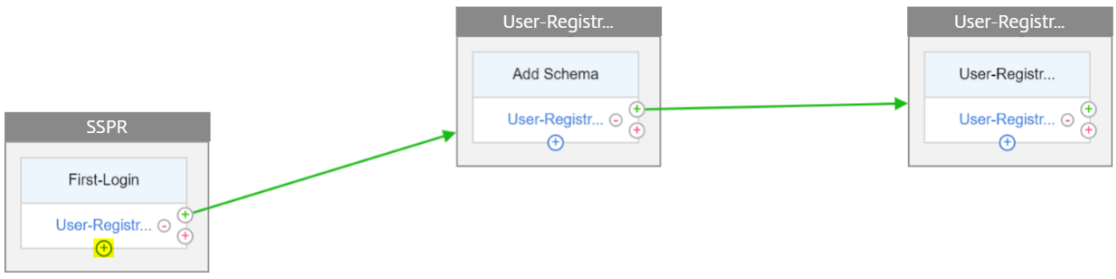
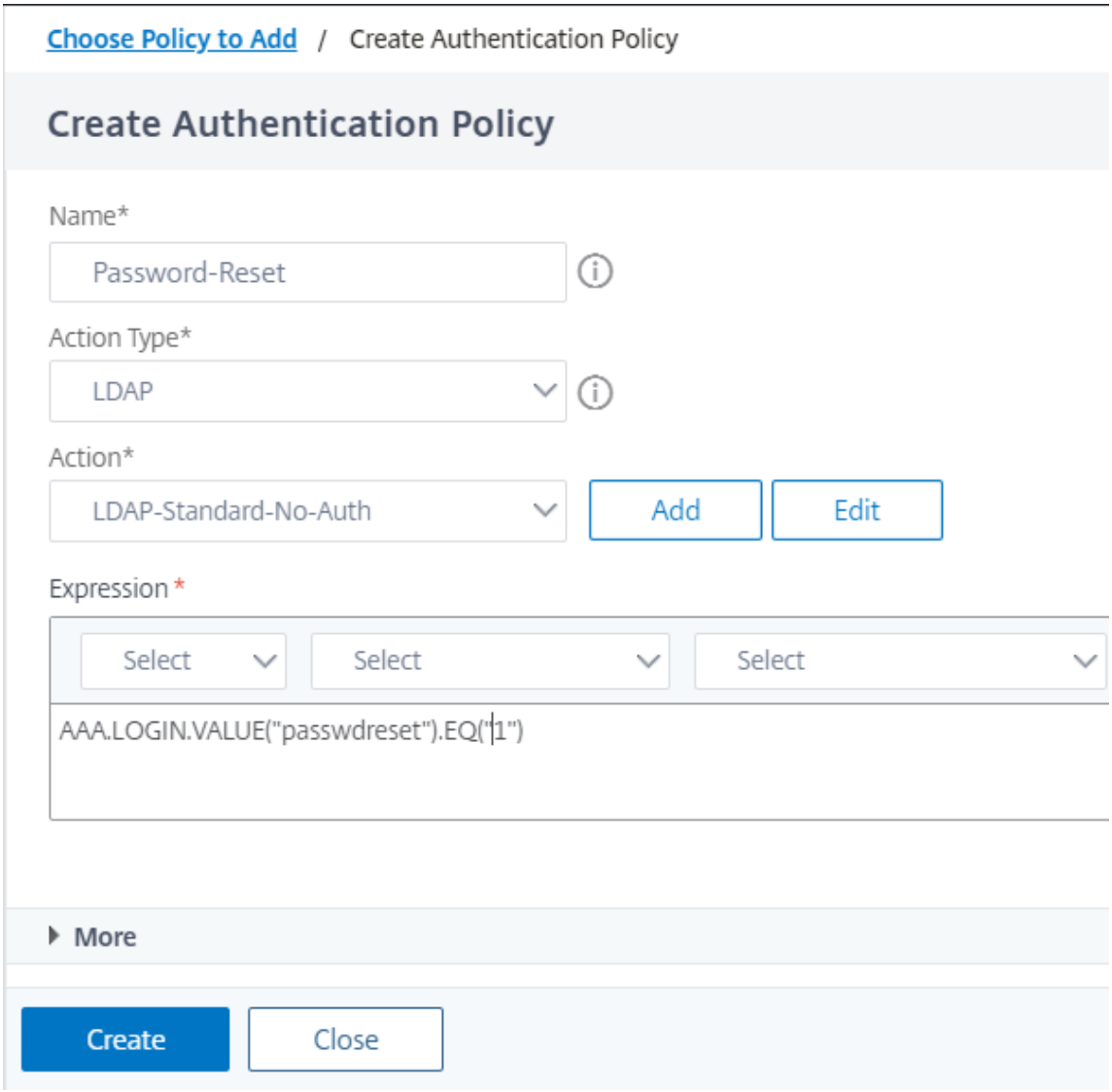
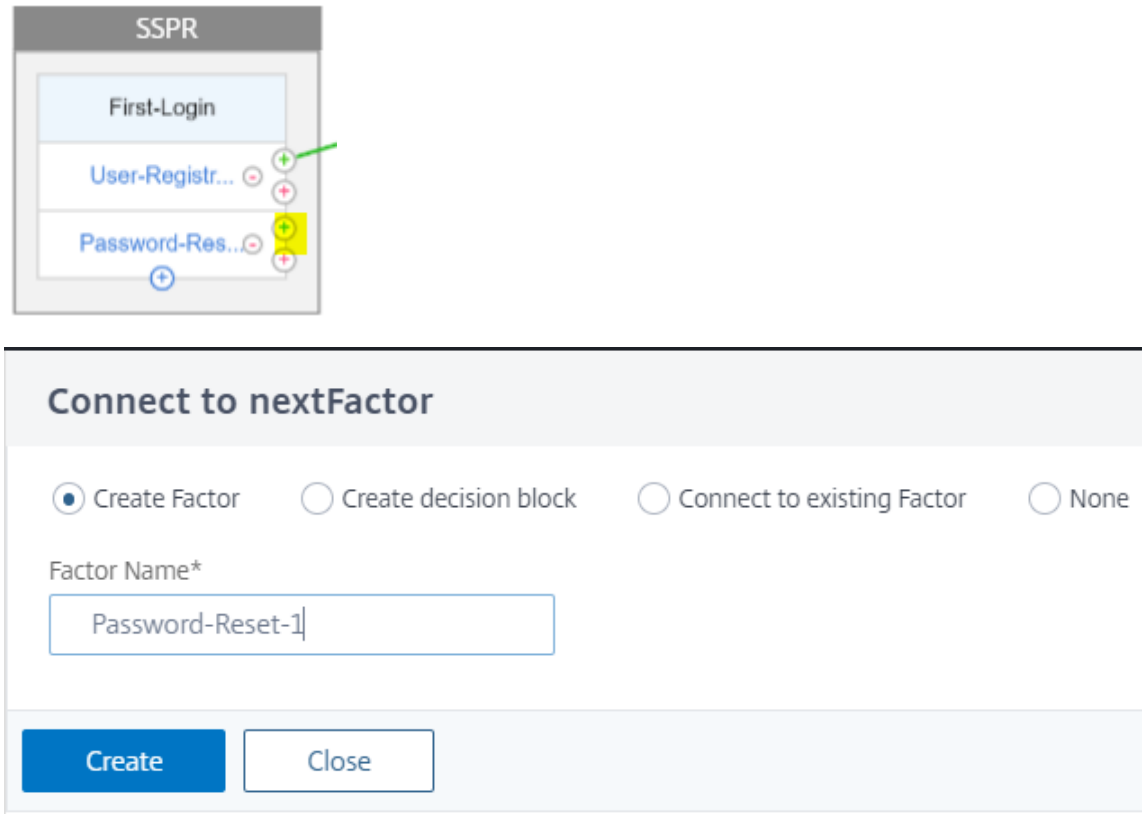
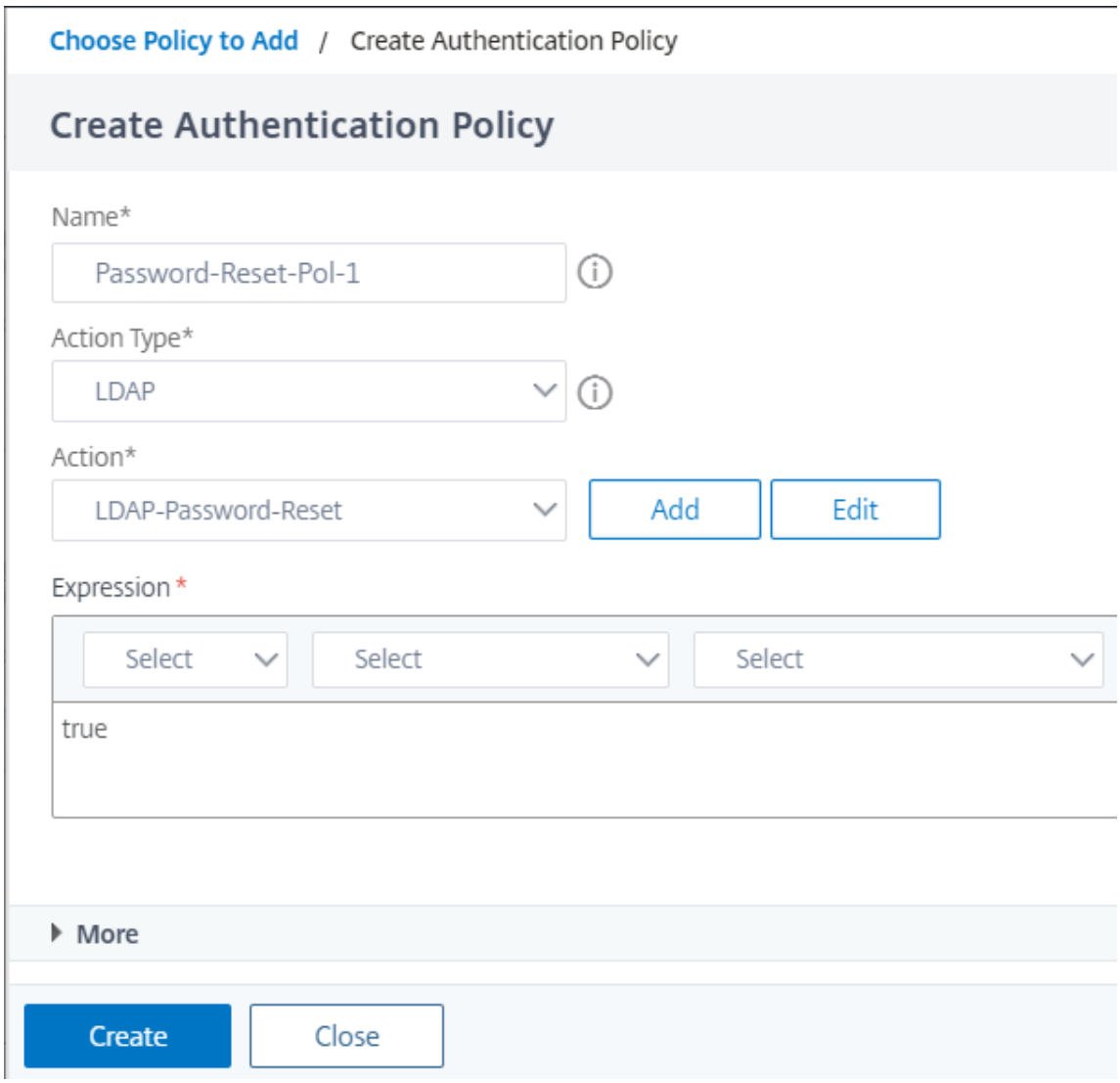
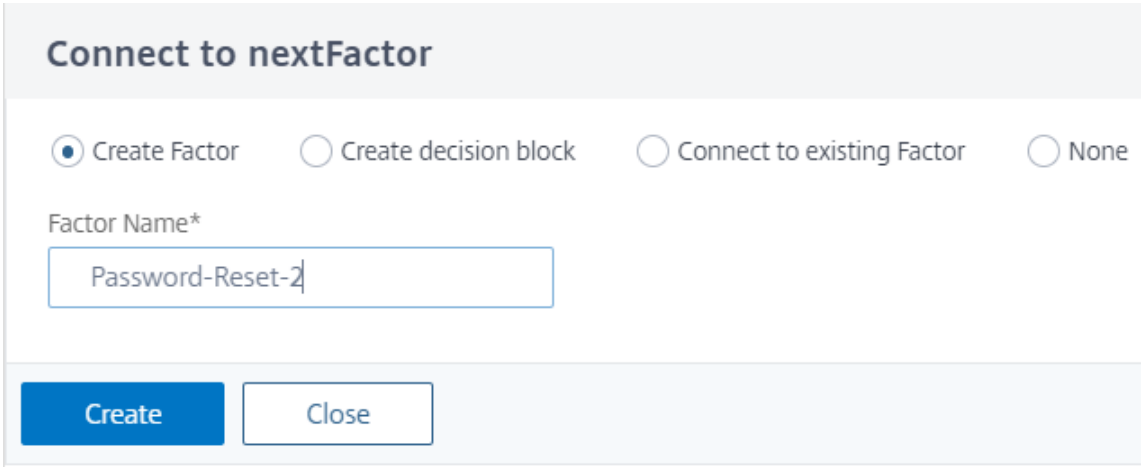
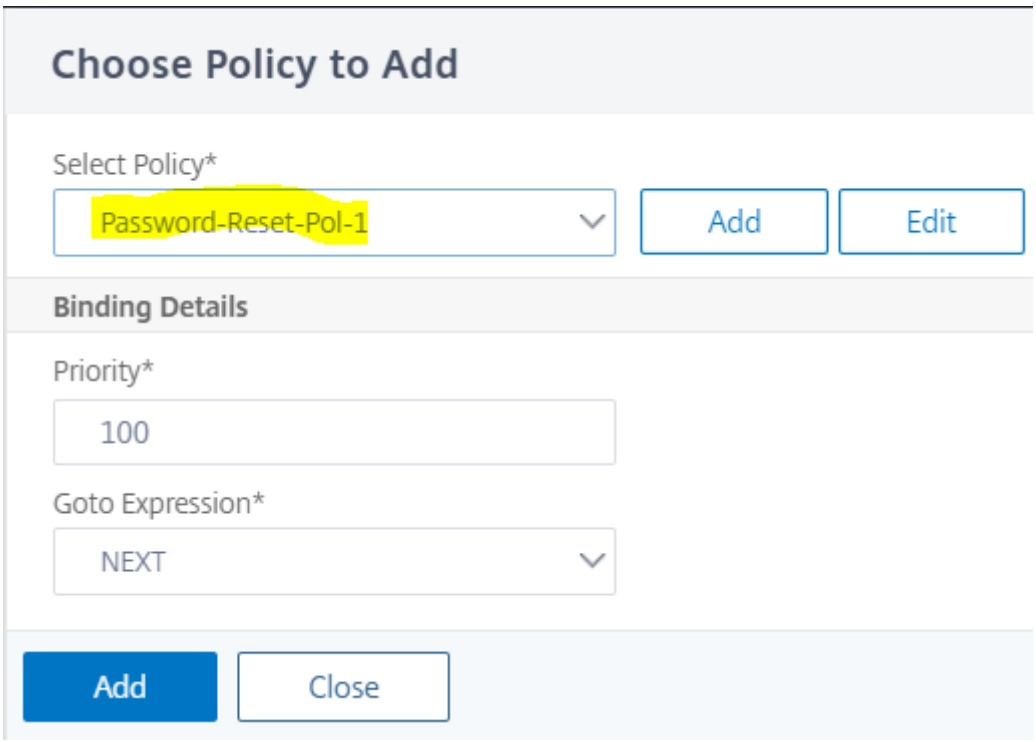
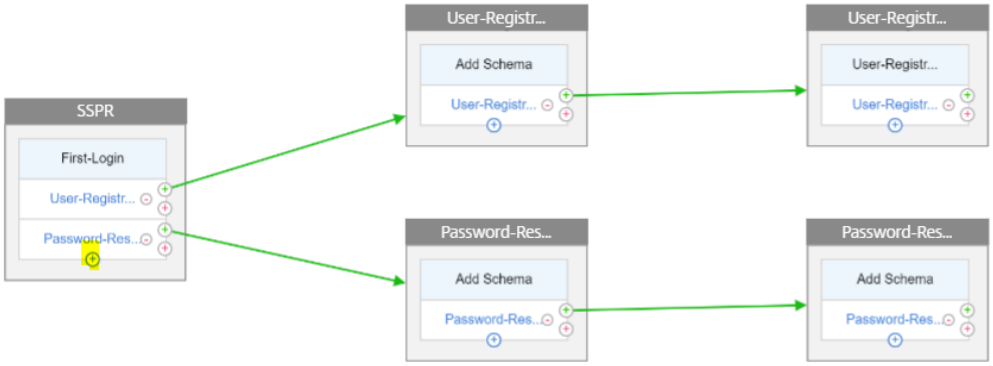
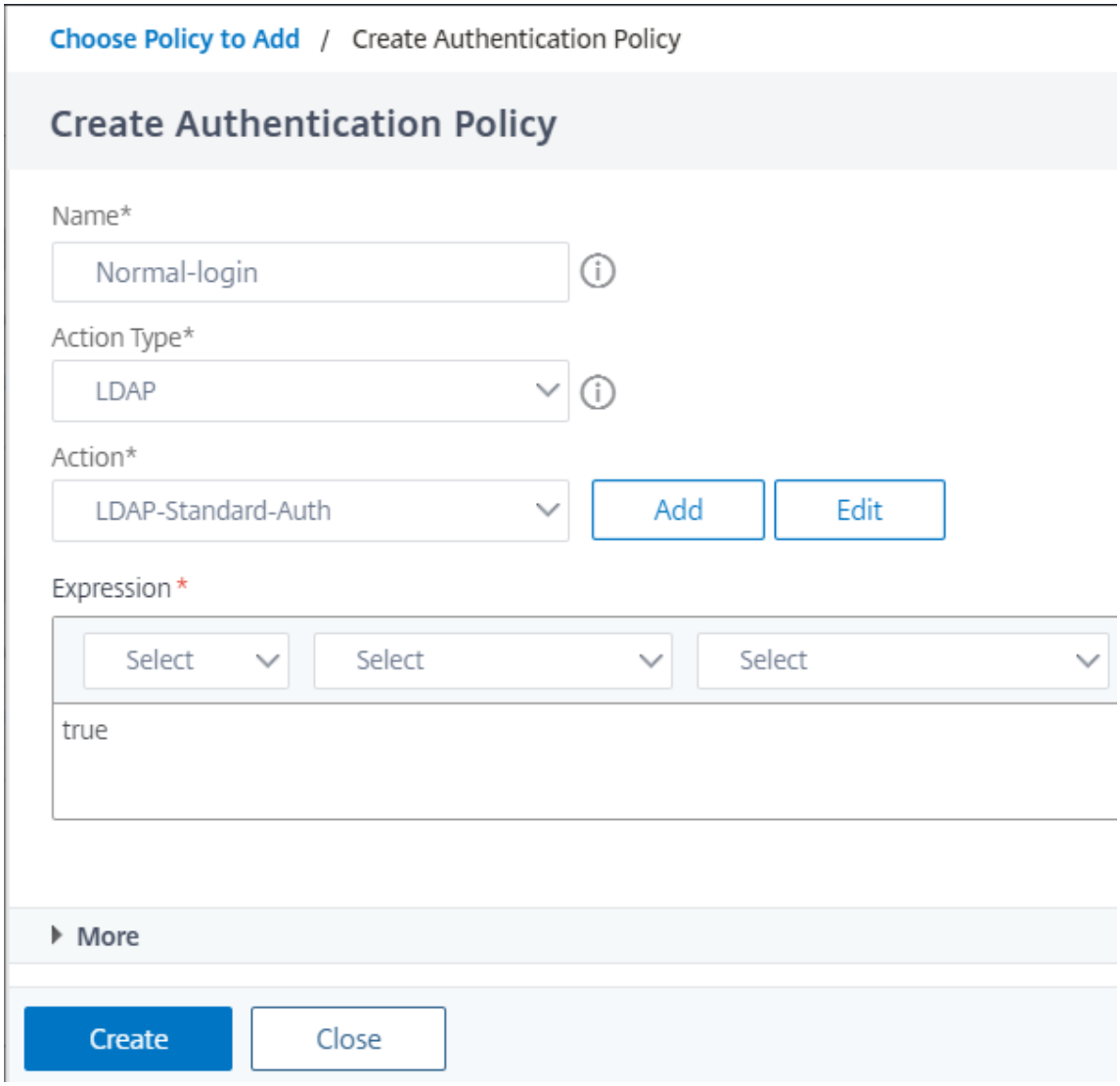
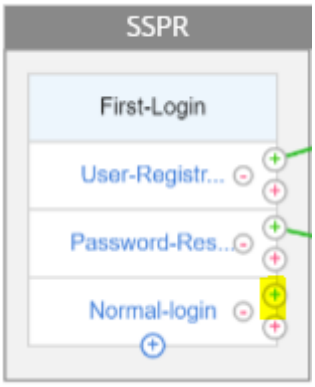
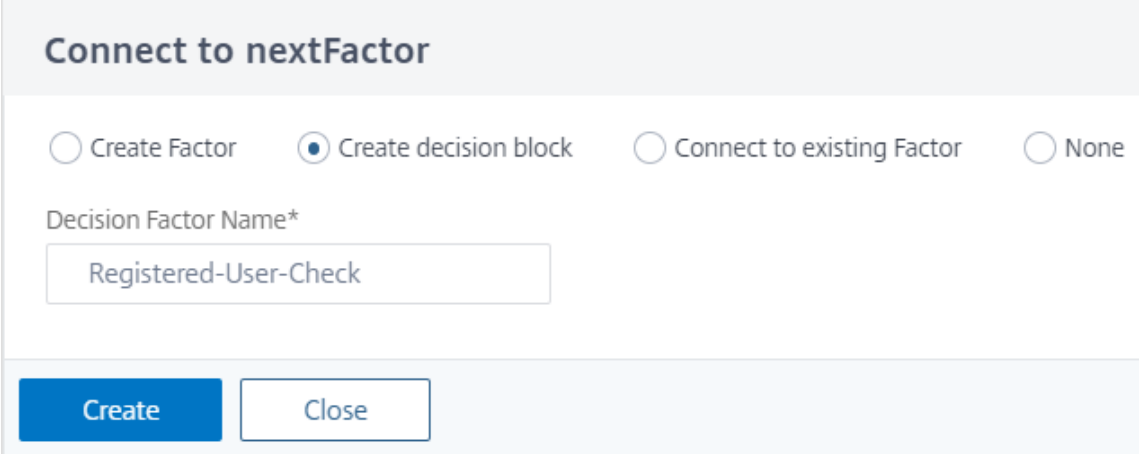
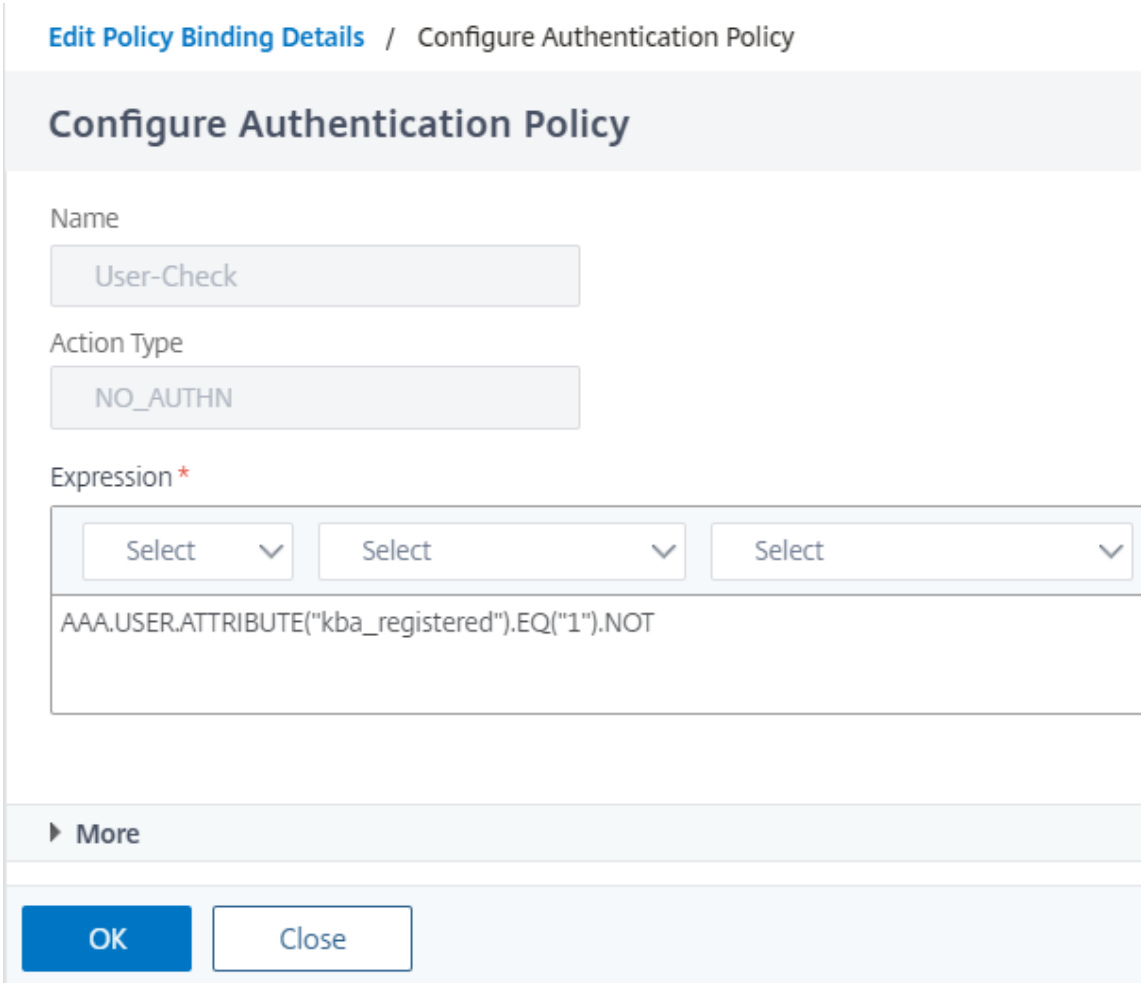
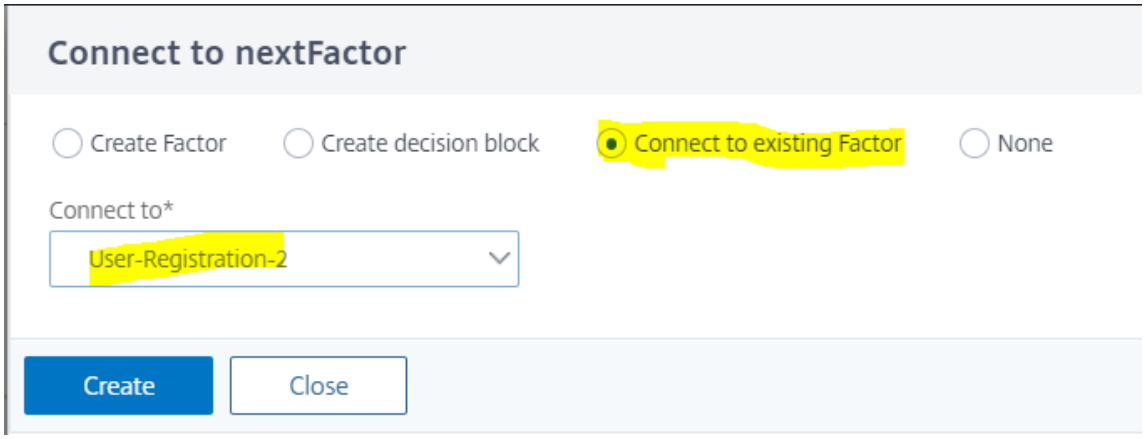
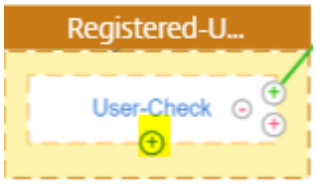
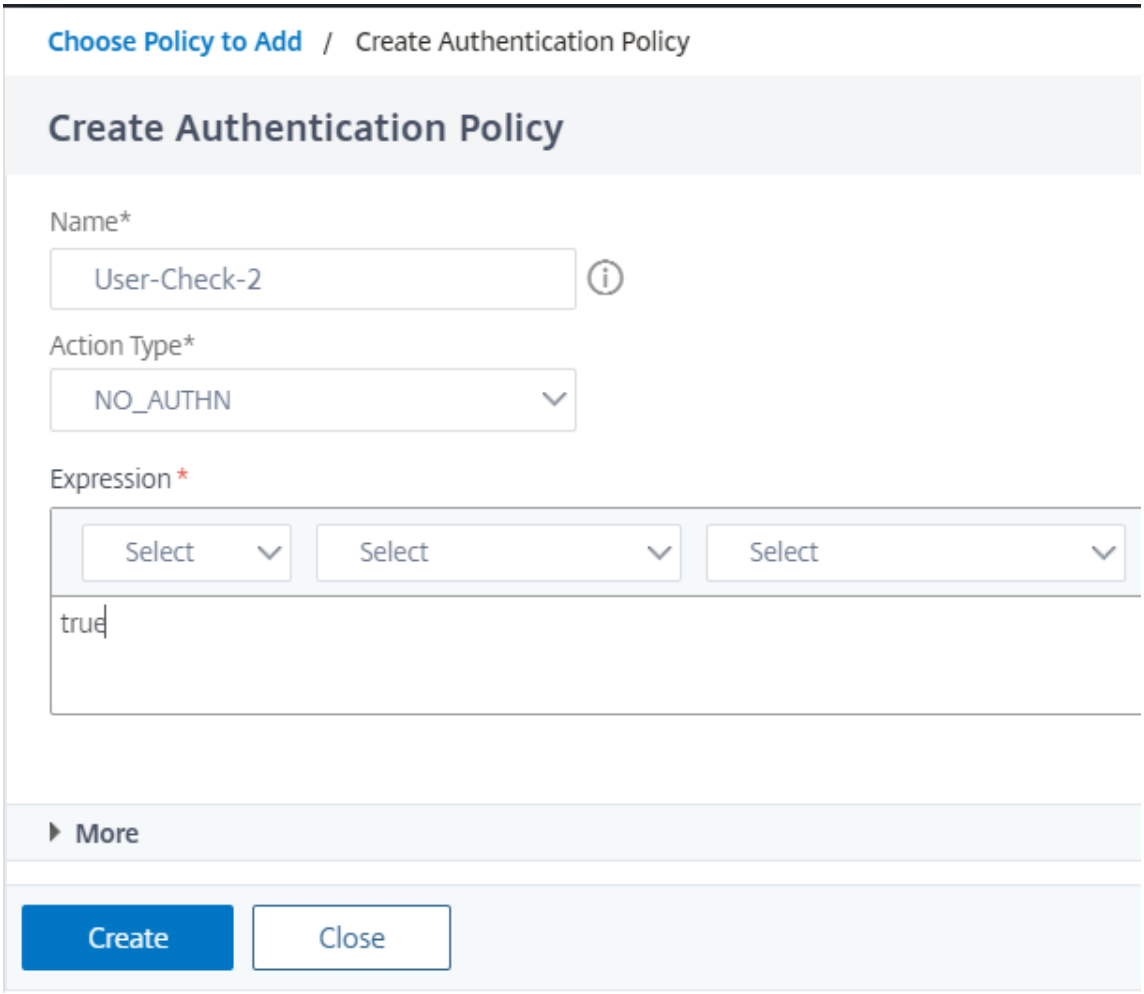
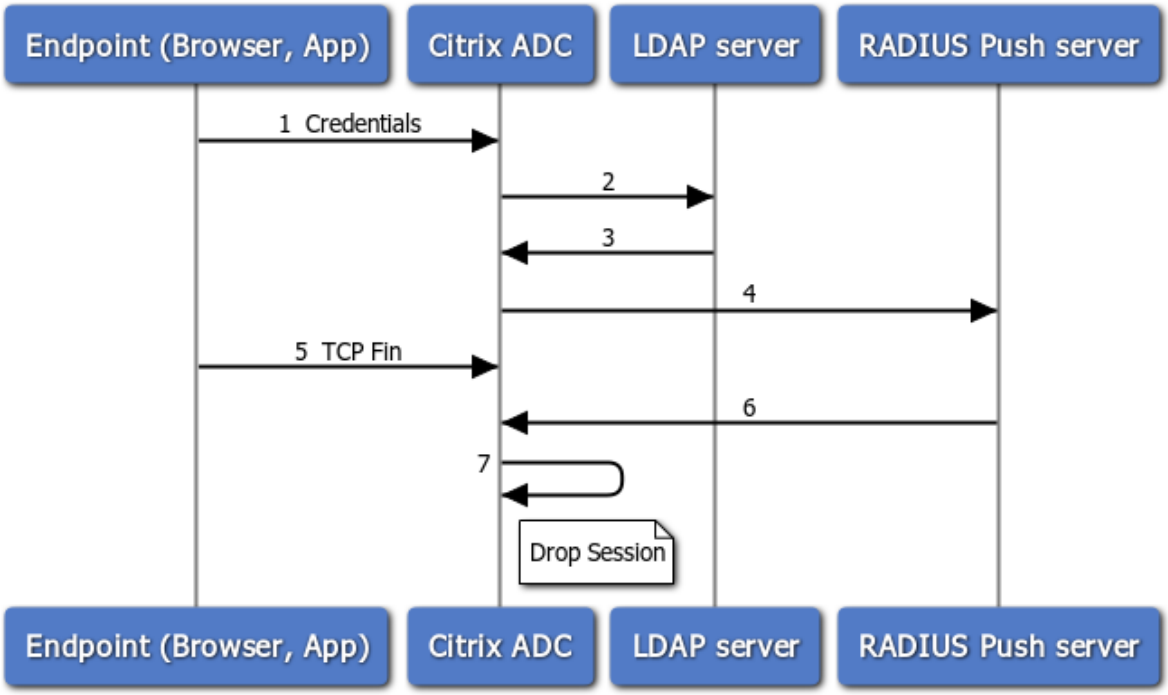
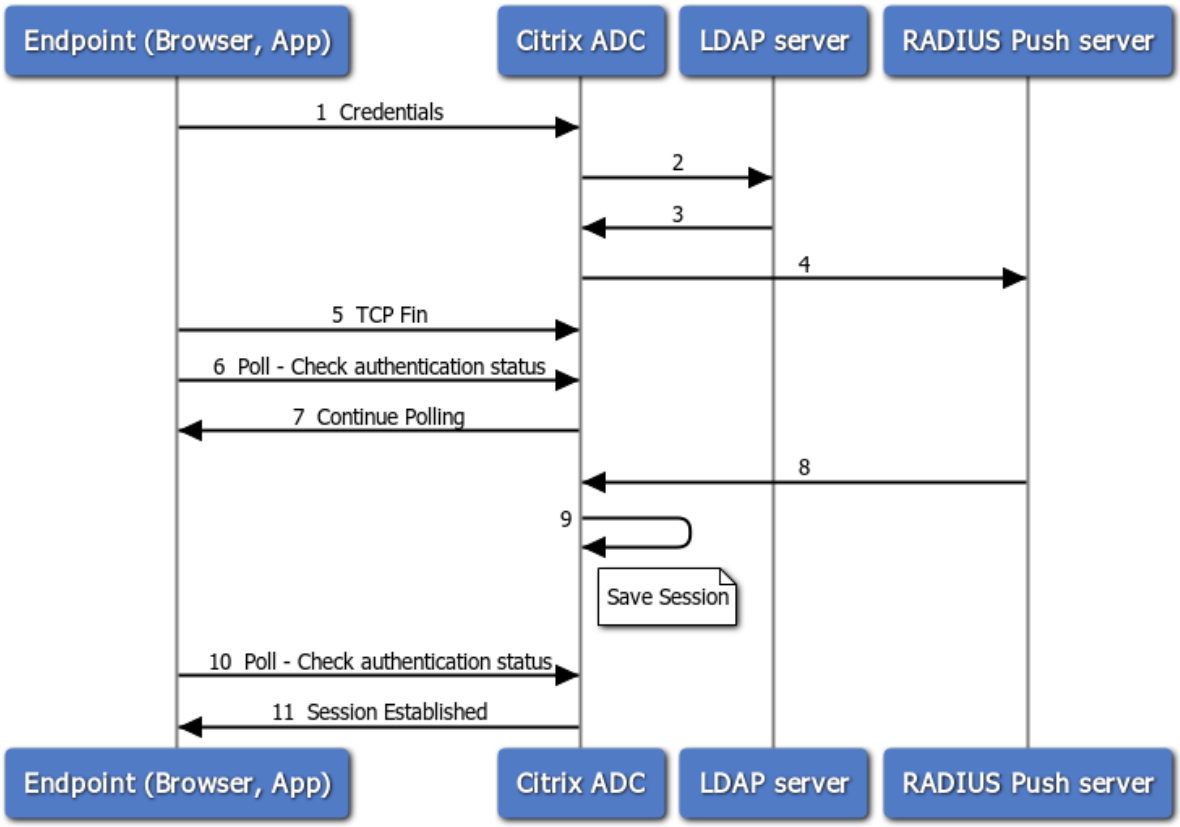
> add authentication loginSchemaPolicy lpol_password_reset -rule true -
   action lschema_password_reset
```

Créer des questions et réponses basées sur les connaissances et envoyer un facteur de validation OTP par e-mail via une étiquette de stratégie

Si le premier facteur est l'ouverture de session LDAP, vous pouvez créer une question et une réponse basées sur les connaissances et envoyer des étiquettes de stratégie OTP pour le facteur suivant à l'aide des commandes suivantes.

```
> add authentication loginSchema lschema_noschema -authenticationSchema
    noschema

> add authentication policylabel kba_validation -loginSchema
   lschema_noschema

> add authentication policylabel email_validation -loginSchema
   lschema_noschema
```


Créer un facteur de réinitialisation du mot de passe via l'étiquette de stratégie

Vous pouvez créer un facteur de réinitialisation de mot de passe via l'étiquette de stratégie à l'aide des commandes suivantes.

```
> add authentication loginSchema lschema_noschema -authenticationSchema
    noschema

> add authentication policylabel password_reset -loginSchema
    lschema_noschema

> bind authentication policylabel password_reset -policyName ldap_pwd -
    priority 10 -gotoPriorityExpression NEXT
```

Liez la question et la réponse basées sur les connaissances et la stratégie d'e-mail aux stratégies créées précédemment à l'aide des commandes suivantes.

```
> bind authentication policylabel email_validation -policyName
    email_validation -nextfactor password_reset -priority 10 -
    gotoPriorityExpression NEXT

> bind authentication policylabel kba_validation -policyName
    kba_validation -nextfactor email_validation -priority 10 -
    gotoPriorityExpression NEXT
```

Lier le flux

Le flux d'ouverture de session LDAP doit être créé en vertu de la stratégie d'authentification pour l'ouverture de session LDAP. Dans ce flux, l'utilisateur clique sur le lien de mot de passe oublié présenté sur la première page d'ouverture de session LDAP, puis la validation KBA suivie par la validation OTP et enfin la page de réinitialisation du mot de passe.

```
bind authentication vserver authvs -policy ldap3 -nextfactor
    kba_validation -priority 10 -gotoPriorityExpression NEXT
```

Pour lier tout le flux de l'interface utilisateur

```
bind authentication vserver authvs -policy lpol_password_reset -
    priority 20 -gotoPriorityExpression END
```


Workflow d'ouverture de session utilisateur pour réinitialiser le mot de passe

Voici un flux de travail d'ouverture de session utilisateur si l'utilisateur a besoin de réinitialiser le mot de passe :

1. Entrez l'URL lb vserver ; par exemple https://lb1.server.com. L'écran d'ouverture de session s'affiche.



2. Cliquez sur **Mot de passe oublié**. Un écran de validation affiche deux questions sur un maximum de six questions et réponses enregistrées auprès d'un utilisateur AD.



3. Répondez aux questions et cliquez **sur Se connecter**. Un écran de validation OTP par e-mail dans lequel vous devez entrer le OTP reçu sur l'ID de courriel secondaire enregistré s'affiche.



4. Entrez l'e-mail OTP. Une fois que la validation OTP de l'e-mail est réussie, la page de réinitialisation du mot de passe s'affiche.



5. Entrez un nouveau mot de passe et confirmez le nouveau mot de passe. Cliquez sur **Soumettre**. Une fois la réinitialisation du mot de passe réussie, l'écran de réinitialisation du mot de passe réussie s'affiche.



Vous pouvez maintenant vous connecter à l'aide du mot de passe de réinitialisation.

Résolution des problèmes

Citrix fournit une option pour résoudre certains des problèmes de base que vous pourriez rencontrer lors de l'utilisation de la réinitialisation du mot de passe en libre-service. La section suivante vous aide à résoudre certains des problèmes qui peuvent se produire dans des domaines spécifiques.

Journal NS

Avant d'analyser le journal, il est recommandé de définir le niveau du journal pour le déboguer à l'aide de la commande suivante :

```
1 > set syslogparams -loglevel DEBUG
```

Enregistrement

Le message suivant indique que l'enregistrement de l'utilisateur a réussi.


```
"ns_aaa_insert_hash_keyValue_entry key:kba_registered value:1"
Nov 14 23:35:51 <local0.debug> 10.102.229.76 11/14/2018:18:05:51 GMT
    0-PPE-1 : default SSLVPN Message 1588 0 :  "
    ns_aaa_insert_hash_keyValue_entry key:alternate_mail value:
    eyJ2ZXJzaW9uIjoiMSIsICJraWQiOiIxbk1oWjN0T2NjLVVvZUx6NDRwZFhxdS01dTA9IiwgImtleS
    ==.oKmvOalaOJ3a9z7BcGCSegNPMw=="
```

Validation des questions et réponses basée sur les connaissances

Le message suivant indique une validation réussie des questions et réponses basée sur les connaissances.

```
"NFactor: Successfully completed KBA Validation, nextfactor is email"
```

Validation de l'ID de courriel

Le message suivant indique une réinitialisation réussie du mot de passe.

```
"NFactor: Successfully completed email auth, nextfactor is pwd_reset"
```

Configurer SSPR à l'aide du visualiseur NFactor

Avant de commencer la configuration SSPR, nous devons ajouter les serveurs LDAP suivants :

1. Serveur LDAP standard avec authentification activée pour l'authentification utilisateur et attribut AD spécifié.



2. Serveur LDAP pour l'extraction des paramètres utilisateur sans authentification.



3. Serveur LDAP pour la réinitialisation du mot de passe sur SSL sans authentification. En outre, l'attribut AD à utiliser pour stocker les détails de l'utilisateur doit être défini dans ce serveur.



4. Serveur LDAP pour l'enregistrement des utilisateurs, avec authentification activée et attribut AD spécifié



5. Le flux complet est illustré ci-dessous :



6. Liez le certificat globalement à l'aide de la commande CLI suivante :

```
1 bind vpn global -userDataEncryptionKey Wildcard
```

Maintenant que les serveurs LDAP sont ajoutés, procédez à la configuration NFactor à l'aide de visualiseur

1. Accédez à, **Sécurité > AAA > Trafic des applications > nFactor Visualizer > nFactor Flux**, cliquez sur **Ajouter** et cliquez sur l'icône plus à l'intérieur de la boîte.

2. Donnez un nom au flux.



3. Cliquez sur **Ajouter un schéma**, qui servira de schéma par défaut. Cliquez sur **Ajouter** sur la page du schéma de connexion.



4. Après avoir donné un nom au schéma, sélectionnez le schéma comme indiqué ci-dessous. Cliquez sur **Sélectionner** dans le coin supérieur droit pour le schéma à sélectionner.



5. Cliquez sur **Créer**, puis sur **OK**.

Une fois le schéma par défaut ajouté, nous devons configurer les trois flux suivants :

- **Inscription utilisateur** : Pour l'enregistrement explicite de l'utilisateur
- **Réinitialisation du mot**de passe : pour la ré
- **Connexion normale + Vérification de l'utilisateur enregistré** : Dans le cas où l'utilisateur est inscrit et saisit le mot de passe correct, l'utilisateur sera connecté. Dans le cas où l'utilisateur n'est pas enregistré, il l'emmènera à la page d'enregistrement.

Enregistrement de l'utilisateur

Continuons d'où nous sommes partis après l'ajout du schéma.

1. Cliquez sur **Ajouter une stratégie**, cela vérifiera si l'utilisateur tente de s'inscrire explicitement.





2. Cliquez sur **Créer**, puis sur **Ajouter**.
3. Cliquez sur l'icône '+' en surbrillance verte pour ajouter le facteur d'authentification suivant au flux d'enregistrement des utilisateurs.





4. Cliquez sur **Créer**.
5. Cliquez sur **Ajouter une stratégie** pour le facteur Inscription des utilisateurs 1.



6. Créez la stratégie d'authentification. Cette stratégie extrait les informations utilisateur et les valide avant de les rediriger vers la page d'enregistrement.



7. Cliquez sur **Créer**, puis sur **Ajouter**.
8. Cliquez maintenant sur l'icône verte '+' pour créer un autre facteur pour l'enregistrement de l'utilisateur et cliquez sur **Créer**. Cliquez sur **Ajouter un schéma**.



9. Créez le schéma suivant.



10. Cliquez sur **Ajouter une stratégie** et créez la stratégie d'authentification suivante.



11. Cliquez sur **Créer**, puis sur **Ajouter**.

Réinitialisation du

1. Cliquez sur l'icône « + » bleue pour ajouter une autre stratégie (flux de réinitialisation du mot de passe) pour le facteur SSPR parent.



2. Cliquez sur **Ajouter** et créez la stratégie d'authentification ci-dessous. Cette stratégie sera déclenchée si l'utilisateur clique sur « Mot de passe oublié » sur la page de connexion.



3. Cliquez sur **Créer**, puis sur **Ajouter**.
4. Cliquez sur l'icône verte « + » pour la stratégie d'authentification de réinitialisation du mot de passe pour ajouter un autre facteur.



5. Cliquez sur **Créer**.
6. Cliquez sur **Ajouter une stratégie** pour créer une stratégie d'authentification pour le facteur créé ci-dessus. Ce facteur servira à valider l'utilisateur.



7. Cliquez sur **Créer**, puis sur **Ajouter**.
8. Cliquez sur l'icône verte '+' pour ajouter un autre facteur pour le flux de facteurs de mot de passe, cela validera les réponses fournies pour la réinitialisation du mot de passe. Cliquez sur **Créer**.



9. Cliquez sur **Ajouter une stratégie** pour ajouter une stratégie d'authentification pour le facteur.
10. Sélectionnez la même stratégie d'authentification dans le menu déroulant que nous avons créé précédemment et cliquez sur **Ajouter**.



Connexion normale + Vérification de l'utilisateur enregistré

1. Cliquez sur l'icône « + » bleue pour ajouter une autre stratégie d'authentification (flux de connexion normal) au facteur SSPR parent.



2. Cliquez sur **Ajouter**pour créer la stratégie d'authentification ci-dessous pour la connexion utilisateur normale.



3. Cliquez sur **Créer** et cliquez sur **Ajouter**.

4. Cliquez sur l'icône verte « + » pour la stratégie créée ci-dessus pour ajouter un autre facteur, par exemple un bloc de décision. Cliquez sur **Créer**.



5. Cliquez sur **Créer**.



6. Cliquez sur **Ajouter une stratégie** pour créer une stratégie d'authentification pour ce facteur de décision.



7. Cliquez sur **Créer**, puis sur **Ajouter**. Cela vérifiera si l'utilisateur est enregistré ou non.
8. Cliquez sur l'icône verte '+' pour pointer l'utilisateur vers la politique d'enregistrement.

9. Sélectionnez le facteur d'inscription dans le menu déroulant et cliquez sur **Créer**.



10. Cliquez maintenant sur l'icône « + » bleue pour ajouter une autre stratégie au bloc de décision, cette stratégie sera pour l'utilisateur enregistré de mettre fin à l'authentification.



11. Cliquez sur **Ajouter une stratégie** pour créer la stratégie d'authentification ci-dessous.



12. Cliquez sur **Créer**, puis sur **Ajouter**.

Interrogation pendant l'authentification

August 20, 2021

À partir de la version 13.0.79.64 de Citrix ADC, une appliance Citrix ADC peut être configurée pour le mécanisme d'interrogation pendant l'authentification multifacteur.

Si l'interrogation est configurée sur une appliance Citrix ADC, les points de terminaison (comme un navigateur Web ou une application) peuvent interroger (sonder) l'appliance pendant l'authentification aux intervalles configurés pour obtenir l'état de la demande d'authentification envoyée.

L'interrogation peut être configurée pour gérer les authentifications lorsqu'un point de terminaison abandonne une connexion TCP lors de l'authentification auprès d'une appliance Citrix ADC.

Points à noter

- La configuration de sondage est prise en charge pour les méthodes d'authentification LDAP, RADIUS et TACACS.
- Le client peut sonner les demandes d'authentification à partir du second facteur.

Pourquoi configurer l'interrogation ?

Parfois, lors de l'authentification, le basculement entre les applications (par exemple une application de connexion et une application d'authentification) entraîne la perte de connexion des points de terminaison avec l'appliance Citrix ADC, ce qui entraîne une interruption du flux d'authentification. Une fois l'interrogation configurée, cette interruption de l'authentification peut être évitée.

Comprendre le mécanisme de sondage

Voici un exemple de flux d'événements pendant l'authentification sans interrogation configurée.

Le mécanisme d'interrogation permet à une appliance Citrix ADC de reprendre une authentification continue avec le point de terminaison sans devoir redémarrer le processus d'authentification dans un cas rare de réinitialisation de la connexion TCP au point de terminaison.



1. Un point de terminaison (application ou navigateur Web) s'authentifie avec des informations d'identification.

2. Le nom d'utilisateur et le mot de passe sont vérifiés par rapport à un répertoire de premier facteur existant (LDAP/Active Directory).
3. Si les informations d'identification correctes sont fournies, l'authentification passe au facteur suivant.
4. À ce stade, l'appliance Citrix ADC envoie une demande au serveur RADIUS Push.
5. Pendant que l'appliance Citrix ADC attend une réponse du serveur RADIUS, le point de terminaison supprime la connexion TCP.
6. Le Citrix ADC reçoit une réponse du serveur RADIUS Push.
7. Comme aucune connexion TCP client n'est trouvée, l'appliance Citrix ADC abandonne la session et la connexion échoue.

L'exemple suivant illustre le flux d'événements pendant l'authentification avec Polling configuré.



1. Un point de terminaison (application ou navigateur Web) s'authentifie avec des informations d'identification.
2. Le nom d'utilisateur et le mot de passe sont vérifiés par rapport à un répertoire de premier facteur existant (LDAP/Active Directory).
3. Si les informations d'identification correctes sont fournies, l'authentification passe au facteur suivant.
4. À ce stade, l'appliance Citrix ADC envoie une demande au serveur RADIUS Push.
5. Pendant que l'appliance Citrix ADC attend une réponse du serveur RADIUS, le point de terminai-

son supprime la connexion TCP.

6. Endpoint envoie un sondage (sonde) à l'appliance Citrix ADC pour vérifier l'état de l'authentification.
7. Comme l'appliance Citrix ADC n'a pas de nouvelles du serveur RADIUS, elle demande au point de terminaison de poursuivre l'interrogation.
8. L'appliance Citrix ADC reçoit une réponse du serveur RADIUS Push.
9. Aucune connexion TCP client n'étant trouvée, ADC enregistre l'état de la session.
10. Endpoint interroge à nouveau pour vérifier l'état de l'authentification.
11. L'appliance Citrix ADC établit la session et la connexion réussit.

Configuration du sondage à l'aide de l'interface de ligne

Voici un exemple de configuration CLI.

Configurer le premier facteur

```
add authentication ldapAction ldap-new -serverIP 10.106.40.65 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword 2
    f63d3659103464a4fad0ade65e2ccfd4e8440e36ddff941d29796af03e01139 -
    encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -
    groupAttrName memberof -subAttributeName CN -secType SSL -
    alternateEmailAttr userParameters

add authentication Policy ldap-new -rule true -action ldap-new

bind authentication vserver avs -policy ldap-new -priority 1 -
    nextFactor rad_factor
<!--NeedCopy-->
```

Configurer le deuxième facteur

```
add authentication radiusAction rad1 -serverIP 10.102.229.120 -radKey 1
    b1613760143ce2371961e9a9eb5392c86a4954a62397f29a01b5d12b42ce232 -
    encrypted -encryptmethod ENCMTHD_3

add authentication Policy rad -rule true -action rad1
<!--NeedCopy-->
```

Configurer le schéma de connexion Poll.xml


```
add authentication loginSchema polling_schema -authenticationSchema
    LoginSchema/Poll.xml

add authentication policylabel rad_factor -loginSchema polling_schema

bind authentication policylabel rad_factor -policyName rad -priority 1
    -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Configuration du sondage à l'aide de l'interface

Pour obtenir des étapes détaillées sur la configuration de l'authentification multifacteur à l'aide de l'interface graphique, voir Configuration de l'authentification nFactor.

Voici les exemples d'étapes de haut niveau requises pour configurer Citrix ADC for Polling à partir du second facteur.

1. Créez un premier facteur d'authentification, par exemple LDAP.
2. Créez un deuxième facteur d'authentification, par exemple RADIUS.
3. Ajoutez **Poll.xml** présent dans Citrix ADC (/NSconfig/LoginSchema/LoginSchema/) comme schéma de connexion pour le deuxième facteur.

Gestion des sessions et du trafic

October 5, 2021

Paramètres de session

Après avoir configuré vos profils d'authentification, d'autorisation et d'audit, vous configurez les paramètres de session pour personnaliser vos sessions utilisateur. Les paramètres de session sont les suivants :

- **Le délai d'expiration de la session.**

  Contrôle la période après laquelle l'utilisateur est automatiquement déconnecté et doit s'authentifier à nouveau pour accéder à votre intranet.

- **Le paramètre d'autorisation par défaut.**

  Détermine si l'appliance Citrix ADC autorise ou refuse par défaut l'accès au contenu pour lequel il n'existe aucune stratégie d'autorisation spécifique.

- **Le paramètre d'authentification unique.**

  Détermine si l'appliance Citrix ADC connectera automatiquement les utilisateurs à toutes les applications Web après leur authentification, ou transmettra les utilisateurs à la page d'ouverture de session de l'application Web pour s'authentifier pour chaque application.

- **Le paramètre d'index des informations d'identification.**

  Détermine si l'appliance Citrix ADC utilise les informations d'identification d'authentification principale ou secondaire pour l'authentification unique.

Pour configurer les paramètres de session, vous pouvez adopter l'une des deux approches. Si vous souhaitez des paramètres différents pour différents comptes ou groupes d'utilisateurs, vous devez créer un profil pour chaque compte d'utilisateur ou groupe pour lequel vous souhaitez configurer des paramètres de session personnalisés. Vous créez également des stratégies pour sélectionner les connexions auxquelles appliquer des profils particuliers, et vous liez les stratégies aux utilisateurs ou aux groupes. Vous pouvez également lier une stratégie au serveur virtuel d'authentification qui gère le trafic auquel vous souhaitez appliquer le profil.

Si vous souhaitez obtenir les mêmes paramètres pour toutes les sessions, ou si vous souhaitez personnaliser les paramètres par défaut des sessions qui n'ont pas de profils et de stratégies spécifiques configurés, vous pouvez simplement configurer les paramètres de session globaux.

Profils de session

Pour personnaliser vos sessions utilisateur, vous devez d'abord créer un profil de session. Le profil de session vous permet de remplacer les paramètres globaux de tous les paramètres de session.

> **Remarque**
>
> Les termes « profil de session » et « action de session » signifient la même chose.

Pour créer un profil de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un profil de session et vérifier la configuration :

```
1 add tm sessionAction <name> [-sessTimeout <mins>] [-
     defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
     ssoCredential ( PRIMARY | SECONDARY )] [-ssoDomain <string>][-
     httpOnlyCookie ( YES | NO )] [-persistentCookie ( ENABLED | DISABLED
      )] [-persistentCookieValidity <minutes>]
2
3 show tm sessionAction <name>
4 <!--NeedCopy-->
```


Exemple

```
> add tm sessionAction session-profile -sessTimeout 30 -
   defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
        Authorization action : ALLOW
        Session timeout: 30 minutes
 Done
<!--NeedCopy-->
```

Pour modifier un profil de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour modifier un profil de session et vérifier la configuration :

```
set tm sessionAction <name> [-sessTimeout <mins>] [-
   defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
   ssoCredential ( PRIMARY | SECONDARY )] [-ssoDomain <string>][-
   httpOnlyCookie ( YES | NO )] [-persistentCookie ( ENABLED | DISABLED
    )] [-persistentCookieValidity <minutes>]

show tm sessionAction
<!--NeedCopy-->
```

Exemple

```
> set tm sessionAction session-profile -sessTimeout 30 -
   defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
        Authorization action : ALLOW
        Session timeout: 30 minutes
 Done
<!--NeedCopy-->
```

Pour supprimer un profil de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour supprimer un profil de session :

```
rm tm sessionAction <name>
<!--NeedCopy-->
```


Pour configurer les profils de session à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Session.**
2. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Session.**
3. Dans le volet d'informations, cliquez sur l'onglet **Profils** .
4. Dans l'onglet **Profils**, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau profil de session, cliquez sur **Ajouter.**
   - Pour modifier un profil de session existant, sélectionnez-le, puis cliquez sur **Modifier.**
5. Dans la boîte de dialogue Créer un profil de session TM ou Configurer un profil de session TM, tapez ou sélectionnez des valeurs pour les paramètres.
   - Name* : actionName (ne peut pas être modifié pour une action de session précédemment configurée.)
   - Délai d'expiration de la session : SessTimeout
   - Connexion unique aux applications Web : authentification unique
   - Action d'autorisation par défaut : DefaultAuthorizationAction
   - Index des informations d'identification — SSOCredential
   - Domaine d'authentification unique : SSODomain
   - HTTPOnly Cookie—httpOnlyCookie
   - Enable Persistent Cookie—persistentCookie
   - Persistent Cookie Validity—persistentCookieValidity
6. Cliquez sur **Créer** ou **sur OK**. Le profil de session que vous avez créé apparaît dans le volet Stratégies et profils de session.

Stratégies de session

Après avoir créé un ou plusieurs profils de session, vous créez des stratégies de session, puis vous liez les stratégies globalement ou à un serveur virtuel d'authentification pour les mettre en œuvre.

Pour créer une stratégie de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une stratégie de session et vérifier la configuration :

```
1 -  add tm sessionPolicy <name> <rule> <action>
2 -  show tm sessionPolicy <name>
3 <!--NeedCopy-->
```

Exemple

```
1 > add tm sessionPolicy session-pol "URL == /\*.png" session-profile
2 Done
3 > show tm sessionPolicy session-pol
```



```
1)      Name: session-pol       Rule: URL == '/\*.png'
        Action: session-profile
 Done
<!--NeedCopy-->
```

Pour modifier une stratégie de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour modifier une stratégie de session et vérifier la configuration :

```
-  set tm sessionPolicy <name> [-rule <expression>] [-action <action>]
-  show tm sessionPolicy <name>
<!--NeedCopy-->
```

Exemple

```
> set tm sessionPolicy session-pol "URL == /\*.png" session-profile
 Done
> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/\*.png'
        Action: session-profile
 Done
<!--NeedCopy-->
```

Pour lier globalement une stratégie de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier globalement une stratégie de session et vérifier la configuration :

```
bind tm global -policyName <policyname> [-priority <priority>]
<!--NeedCopy-->
```

Exemple

```
> bind tm global -policyName session-pol
 Done

> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/*.png'
        Action: session-profile
        Policy is bound to following entities
        1) TM GLOBAL    PRIORITY : 0
 Done
```



```
10
11 <!--NeedCopy-->
```

Pour lier une stratégie de session à un serveur virtuel d'authentification à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour lier une stratégie de session à un virtuel d'authentification et vérifier la configuration :

```
1 bind authentication vserver <name> -policy <policyname> [-priority <
     priority>]
2 <!--NeedCopy-->
```

Exemple

```
1 bind authentication vserver auth-vserver-1 -policyName Session-Pol-1 -
     priority 1000
2 Done
3 <!--NeedCopy-->
```

Pour délier une stratégie de session d'un serveur virtuel d'authentification à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour délier une stratégie de session d'un serveur virtuel d'authentification et vérifier la configuration :

```
1 unbind authentication vserver <name> -policy <policyname>
2 <!--NeedCopy-->
```

Exemple

```
1 unbind authentication vserver auth-vserver-1 -policyName Session-Pol-1
2 Done
3 <!--NeedCopy-->
```

Pour annuler la liaison d'une stratégie de session globalement liée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier une stratégie de session liée globalement :


```
unbind tm global -policyName <policyname>
<!--NeedCopy-->
```

Exemple

```
unbind tm global -policyName Session-Pol-1
Done
<!--NeedCopy-->
```

Pour supprimer une stratégie de session à l'aide de l'interface de ligne de commande

Commencez par délier la stratégie de session de la stratégie globale, puis, à l'invite de commandes, tapez les commandes suivantes pour supprimer une stratégie de session et vérifier la configuration :

```
rm tm sessionPolicy <name>
<!--NeedCopy-->
```

Exemple

```
rm tm sessionPolicy Session-Pol-1
Done

<!--NeedCopy-->
```

Pour configurer et lier des stratégies de session à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Session**.
2. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Session**.
3. Dans le volet d'informations, sous **l'onglet Stratégies**, effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle stratégie de session, cliquez sur **Ajouter**.
   - Pour modifier une stratégie de session existante, sélectionnez-la, puis cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Créer une stratégie** de **session ou Configurer la stratégie** de session, tapez ou sélectionnez les valeurs des paramètres.
   - NAME* : PolicyName (ne peut pas être modifié pour une stratégie de session précédemment configurée.)
   - Profil de demande* — ActionName
   - Expression* : règle (Vous saisissez des expressions en choisissant d'abord le type d'expression dans la liste déroulante située à gauche sous la zone de texte Expression,

puis en tapant votre expression directement dans la zone de texte de l'expression, ou en cliquant sur **Ajouter** pour ouvrir la boîte de dialogue Ajouter une expression et en utilisant la liste déroulante contient des listes pour construire votre expression.)

5. Cliquez sur **Créer** ou **sur OK**. La stratégie que vous avez créée apparaît dans le volet d'informations de la page **Stratégies** et **profils** de session.
6. Pour lier globalement une stratégie de session, dans le volet d'informations, sélectionnez **Liaisons globales** dans la liste déroulante **Action**, puis remplissez la boîte de dialogue.
   - Sélectionnez le nom de la stratégie de session que vous souhaitez lier globalement.
   - Cliquez sur **OK**.
7. Pour lier une stratégie de session à un serveur virtuel d'authentification, dans le volet de navigation, cliquez sur **Serveurs virtuels**, puis ajoutez cette stratégie à la liste des stratégies.
   - Dans le volet d'informations, sélectionnez le serveur virtuel, puis cliquez sur **Modifier**.
   - Dans les **sélections avancées** à droite de la zone de détails, cliquez sur **Stratégies**.
   - Sélectionnez une stratégie ou cliquez sur l'icône **Plus** pour ajouter une stratégie.
   - Dans la colonne **Priorité** de gauche, modifiez la priorité par défaut pour vous assurer que la stratégie est évaluée dans le bon ordre.
   - Cliquez sur **OK**.
     Un message apparaît dans la barre d'état, indiquant que la stratégie a été correctement configurée.

Paramètres de session globaux

En plus ou au lieu de créer des profils et des stratégies de session, vous pouvez configurer les paramètres de session globaux. Ces paramètres contrôlent la configuration de la session lorsqu'aucune stratégie explicite ne les remplace.

Pour configurer les paramètres de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer les paramètres de session globaux et vérifier la configuration :

```
set tm sessionParameter [-sessTimeout <mins>][-
    defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
    ssoCredential ( PRIMARY | SECONDARY )][-ssoDomain <string>][-
    httpOnlyCookie ( YES | NO )][-persistentCookie ( ENABLED | DISABLED
    )] [-persistentCookieValidity <minutes>]
<!--NeedCopy-->
```

Exemple

```
> set tm sessionParameter -sessTimeout 30
  Done
```



```
> set tm sessionParameter -defaultAuthorizationAction DENY
  Done
> set tm sessionParameter -SSO ON
  Done
> set tm sessionParameter -ssoCredential PRIMARY
  Done
<!--NeedCopy-->
```

Pour configurer les paramètres de session à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur Modifier les paramètres globaux.
3. Dans la boîte de dialogue **Paramètres globaux de la session**, saisissez ou sélectionnez des valeurs pour les paramètres.
   - Délai d'expiration de la session : SessTimeout
   - Action d'autorisation par défaut : DefaultAuthorizationAction
   - Connexion unique aux applications Web : authentification unique
   - Index des informations d'identification — SSOCredential
   - Domaine d'authentification unique : SSODomain
   - HTTPOnly Cookie—httpOnlyCookie
   - Enable Persistent Cookie—persistentCookie
   - Validité des cookies persistants (minutes) — PersistentCookieValidity
   - Page d'accueil : page d'accueil
4. Cliquez sur **OK**.

Paramètres de trafic

Si vous utilisez l'authentification unique (SSO) basée sur des formulaires ou SAML pour vos applications protégées, vous configurez cette fonctionnalité dans les paramètres de trafic. La connexion unique permet à vos utilisateurs de se connecter une seule fois pour accéder à toutes les applications protégées, plutôt que de leur demander de se connecter séparément pour accéder à chacune d'elles.

L'authentification unique basée sur les formulaires vous permet d'utiliser un formulaire Web de votre propre conception comme méthode de connexion au lieu d'une fenêtre contextuelle générique. Vous pouvez donc mettre le logo de votre entreprise et d'autres informations que vous souhaiteriez voir voir apparaître sur le formulaire d'ouverture de session. L'authentification unique SAML vous permet de configurer un dispositif Citrix ADC ou une instance d'appliance virtuelle pour s'authentifier auprès d'un autre dispositif Citrix ADC au nom des utilisateurs qui se sont authentifiés avec le premier dispositif.

Pour configurer l'un ou l'autre type d'authentification SSO, vous devez d'abord créer un formulaire ou

un profil SSO SAML. Ensuite, vous créez un profil de trafic et vous le liez au profil SSO que vous avez créé. Ensuite, vous créez une stratégie et vous la liez au profil de trafic. Enfin, vous liez la stratégie globalement ou à un serveur virtuel d'authentification pour mettre en œuvre votre configuration.

Profils de trafic

Après avoir créé au moins un formulaire ou un profil SSO SAML, vous devez ensuite créer un profil de trafic.

> **Remarque :**
>
> Dans cette fonctionnalité, les termes « profil » et « action » signifient la même chose.

Pour créer un profil de trafic à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add tm trafficAction <name> [-appTimeout <mins>][-SSO ( ON | OFF ) [-
    formSSOAction <string>]][-persistentCookie ( ENABLED | DISABLED )][-
    InitiateLogout ( ON | OFF )]
<!--NeedCopy-->
```

Exemple

```
add tm trafficAction Traffic-Prof-1  - appTimeout 10 -SSO ON -
    formSSOAction SSO-Prof-1
<!--NeedCopy-->
```

Pour modifier un profil de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set tm trafficAction <name> [-appTimeout <mins>] [-SSO ( ON | OFF ) [-
    formSSOAction <string>]] [-persistentCookie ( ENABLED | DISABLED )]
    [-InitiateLogout ( ON | OFF )]
<!--NeedCopy-->
```

Exemple

```
set tm trafficAction Traffic-Prof-1  - appTimeout 10 -SSO ON -
    formSSOAction SSO-Prof-1
<!--NeedCopy-->
```


Pour supprimer un profil de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm tm trafficAction <name>
<!--NeedCopy-->
```

Exemple

```
rm tm trafficAction Traffic-Prof-1
<!--NeedCopy-->
```

Pour configurer les profils de trafic à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Trafic.**
2. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Trafic.**
3. Dans le volet d'informations, cliquez sur l'onglet Profils.
4. Dans l'onglet Profils, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau profil de trafic, cliquez sur **Ajouter.**
   - Pour modifier un profil de trafic existant, sélectionnez-le, puis cliquez sur **Modifier.**
5. Dans la boîte de dialogue **Créer un profil de traficou Configurer le profil** de trafic, spécifiez les valeurs des paramètres.
   - NOM* : nom (ne peut pas être modifié pour une action de session précédemment configurée.)
   - AppTimeout — AppTimeout
   - Connexion unique : authentification unique
   - Action SSO de formulaire — FormssoAction
   - Action SSO SAML—SAMLSSOAction
   - Enable Persistent Cookie—persistentCookie
   - Initier la déconnexion : initiateLogout
6. Cliquez sur **Créer** ou **sur OK**. Le profil de trafic que vous avez créé apparaît dans les stratégies de trafic, les profils et le volet Form SSO Profiles ou SAML SSO Profiles, selon le cas.

Prise en charge des expressions AAA.USER et AAA.LOGIN

L'expression AAA.USER est maintenant implémentée pour remplacer les expressions HTTP.REQ.USER existantes. L'expression AAA.USER est applicable pour gérer le trafic non HTTP, tel que le mécanisme de Secure Web Gateway (SWG) et d'accès basé sur les rôles (RBA). Les expressions AAA.USER sont équivalentes aux expressions HTTP.REQ.USER.

Vous pouvez utiliser l'expression lors de différentes actions ou configurations de profils.

À l'invite de commandes, tapez :


```
add tm trafficAction <name> [SSO (ON|OFF)] [-userExpression <string>]

add tm trafficAction <name> [SSO (ON|OFF)] [-passwdExpression <string>]

<!--NeedCopy-->
```

Exemple

```
add tm trafficAction tm_act -SSO ON -userExpression "AAA.USER.NAME"

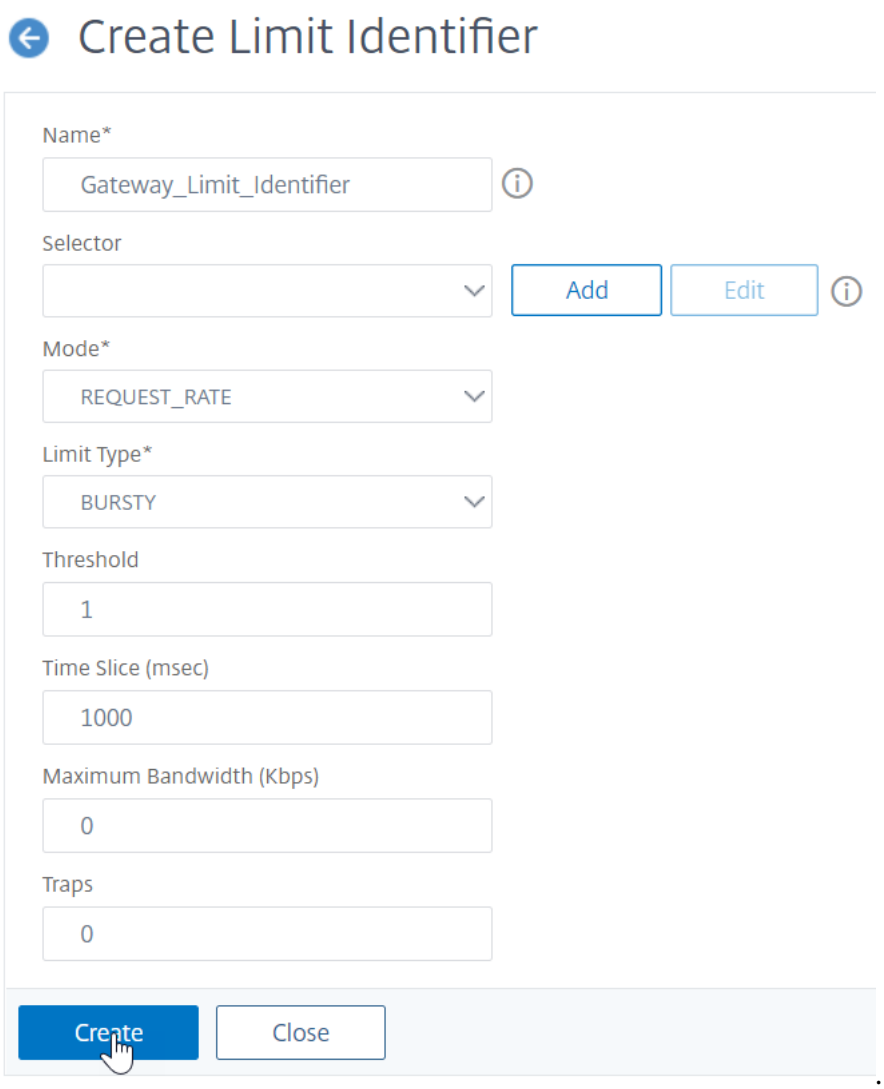
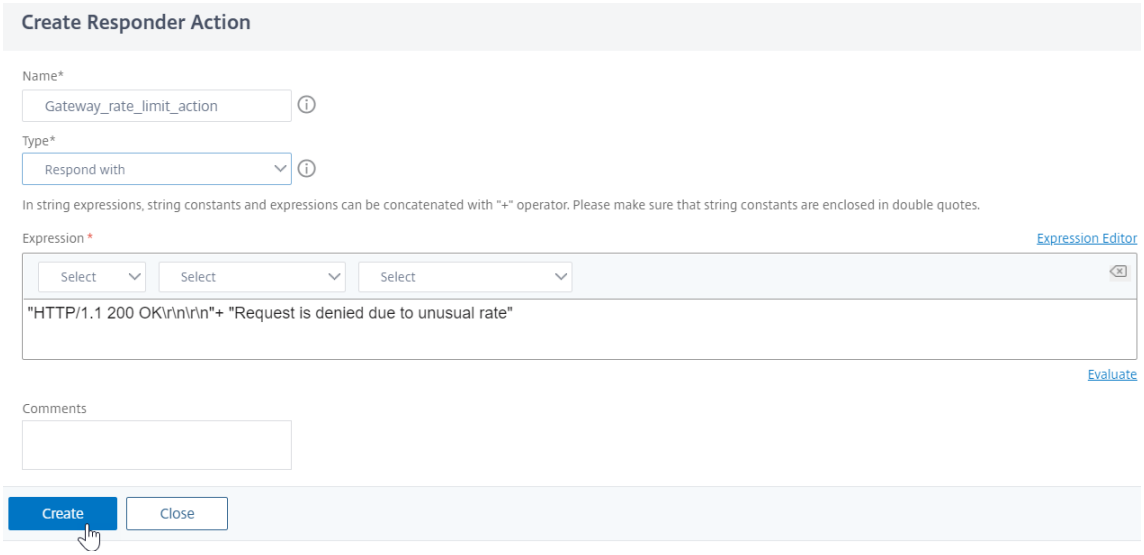
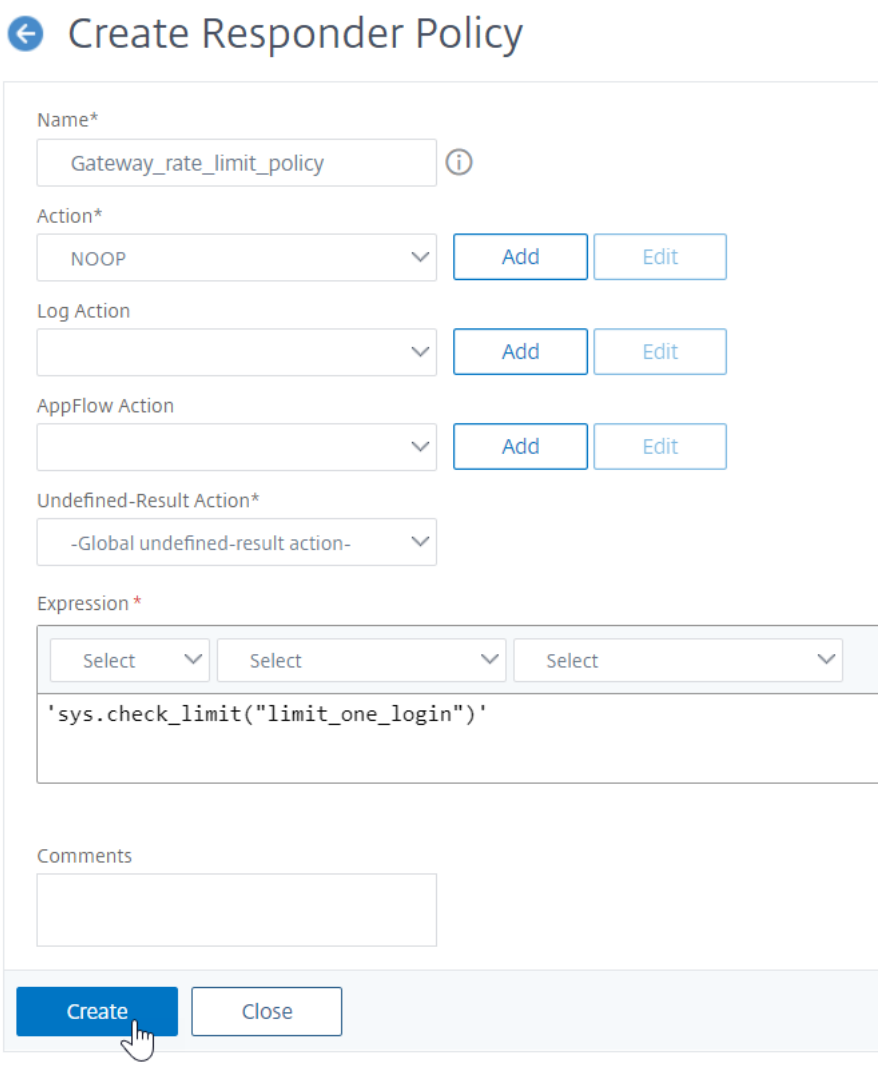
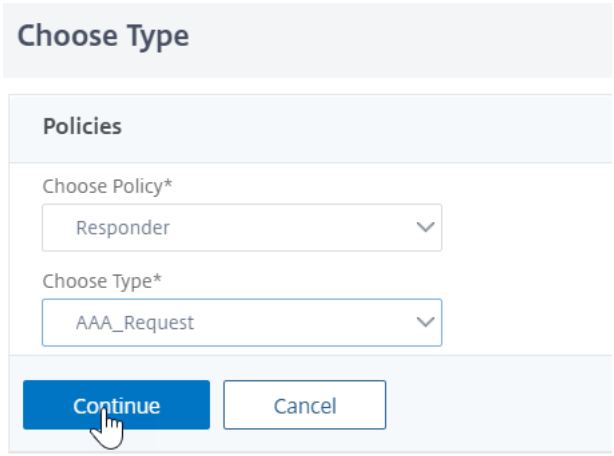
add tm trafficAction tm_act -SSO ON -userExpression "AAA.USER.PASSWD"

add tm trafficPolicy tm_pol true tm_act

bind lb vserver lb1 -policyName tm_pol -priority 2
<!--NeedCopy-->
```

> **Remarque :**
>
> Si vous utilisez l'expression HTTP.REQ.USER, un message d'avertissement « HTTP.REQ.USER est obsolète. Utiliser AAA.USER à la place » apparaît à l'invite de commande.

- **Expression AAA.LOGIN.** L'expression LOGIN représente la pré-connexion, également appelée demande de connexion. La demande de connexion peut émaner de Citrix Gateway, du fournisseur d'identité SAML ou de l'authentification OAuth. Citrix ADC extrait les attributs requis de la configuration de la stratégie. L'expression AAA.LOGIN contient les attributs, qui peuvent être récupérés en fonction des éléments suivants :
  - **AAA.LOGIN.USERNAME.** Le nom d'utilisateur (s'il est trouvé) est extrait de la demande de connexion en cours. La même expression appliquée à une demande de non-connexion (déterminée par une authentification, une autorisation et un audit) génère une chaîne vide.
  - **AAA.LOGIN.PASSWORD.** Le mot de passe utilisateur (s'il est trouvé) est récupéré à partir de la demande de connexion en cours. L'expression génère une chaîne vide si le mot de passe n'est pas trouvé.
  - **AAA.LOGIN.PASSWORD2.** Le deuxième mot de passe (s'il est trouvé) est récupéré à partir de la demande de connexion.
  - **AAA.LOGIN.DOMAINE.** Les informations de domaine sont récupérées à partir de la demande de connexion.
- **AAA.USER.ATTRIBUTE (« # »).** L'expression est utilisée pour stocker l'attribut utilisateur. Ici, # peut être soit une valeur entière (entre 1 et 16), soit une valeur de chaîne. Vous pouvez utiliser ces valeurs d'index en utilisant l'expression AAA.USER.ATTRIBUTE (« # »). Le module d'authentification, d'autorisation et d'audit recherche l'attribut sessions utilisateur et

`AAA.USER.ATTRIBUTE("##")` interroge la table de hachage pour cet attribut particulier. Par exemple, s'il `Attributes("samaccountname")` est défini, `AAA.USER.ATTRIBUTE("samaccountname")` interroge la table de hachage et récupère la valeur correspondant à `samaccountname`.

Politiques de trafic

Après avoir créé un ou plusieurs profils d'identification unique et de trafic de formulaire, vous créez des stratégies de trafic, puis vous liez les stratégies, globalement ou à un serveur virtuel de gestion du trafic, pour les mettre en œuvre.

Pour créer une stratégie de trafic à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add tm trafficPolicy <name> <rule> <action>
2 <!--NeedCopy-->
```

Exemple

```
1 add tm trafficPolicy Traffic-Pol-1 "HTTP.REQ.HEADER("Cookie").CONTAINS(
     "login=true")" Traffic-Prof-1
2 <!--NeedCopy-->
```

Pour modifier une stratégie de trafic à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 set tm trafficPolicy <name> <rule> <action>
2 <!--NeedCopy-->
```

Exemple

```
1 set tm trafficPolicy Traffic-Pol-1 "HTTP.REQ.HEADER("Cookie").CONTAINS(
     "login=true")" Traffic-Prof-1
2 <!--NeedCopy-->
```

Pour lier globalement une stratégie de trafic à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
bind tm global -policyName <string> [-priority <priority>]
<!--NeedCopy-->
```

Exemple

```
bind tm global -policyName Traffic-Pol-1
<!--NeedCopy-->
```

Pour lier une stratégie de trafic à un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
bind lb vserver <name> -policy <policyName> [-priority <priority>]

bind cs vserver <name> -policy <policyName> [-priority <priority>]
<!--NeedCopy-->
```

Exemple

```
bind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1 -
    priority 1000
<!--NeedCopy-->
```

Pour annuler la liaison d'une stratégie de trafic globalement liée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind tm global -policyName <policyname>
<!--NeedCopy-->
```

Exemple

```
unbind tm global -policyName Traffic-Pol-1
<!--NeedCopy-->
```

Pour délier une stratégie de trafic d'un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :


```
unbind lb vserver <name> -policy <policyname>

unbind cs vserver <name> -policy <policyname>
<!--NeedCopy-->
```

Exemple

```
unbind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1
<!--NeedCopy-->
```

Pour supprimer une stratégie de trafic à l'aide de l'interface de ligne de commande

Commencez par délier la stratégie de session de global, puis, à l'invite de commandes, tapez :

```
rm tm trafficPolicy <name>
<!--NeedCopy-->
```

Exemple

```
rm tm trafficPolicy Traffic-Pol-1
<!--NeedCopy-->
```

Pour configurer et lier des stratégies de trafic à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Trafic.**
2. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Trafic.**
3. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle stratégie de session, cliquez sur **Ajouter.**
   - Pour modifier une stratégie de session existante, sélectionnez-la, puis cliquez sur **Modifier.**
4. Dans la boîte de dialogue **Créer une stratégie** de **trafic ou Configurer la stratégie** de trafic, spécifiez les valeurs des paramètres.
   - NAME* : PolicyName (ne peut pas être modifié pour une stratégie de session précédemment configurée.)
   - Profile* — ActionName
   - Expression : règle (Vous saisissez des expressions en choisissant d'abord le type d'expression dans la liste déroulante située à l'extrême gauche sous la zone de texte Expression, puis en tapant votre expression directement dans la zone de texte de l'expression, ou en cliquant sur Ajouter pour ouvrir la boîte de dialogue Ajouter une expression et en utilisant les listes déroulantes qui s'y trouvent pour construisez votre expression.)

5. Cliquez sur **Créer** ou **sur OK**. La stratégie que vous avez créée apparaît dans le volet d'informations de la page **Stratégies** et **profils** de session.

Formulaire de profils SSO

Pour activer et configurer l'authentification SSO basée sur les formulaires, vous devez d'abord créer un profil SSO.

> **Remarque**
>
> - L'authentification unique basée sur les formulaires ne fonctionne pas si le formulaire est personnalisé pour inclure Javascript.
> - Dans cette fonctionnalité, les termes « profil » et « action » signifient la même chose.

Pour créer un profil SSO de formulaire à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add tm formSSOAction <name> -actionURL <URL> -userField <string> -
    passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <
    string>] [-responsesize <positive_integer>][-nvtype ( STATIC |
    DYNAMIC )][-submitMethod ( GET | POST )]

show tm formSSOAction [<name>]
<!--NeedCopy-->
```

Exemple

```
add tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-nameValuePair "loginID passwd" -responsesize "9096"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nvtype STATIC -submitMethod GET
 - sessTimeout 10 -defaultAuthorizationAction ALLOW
<!--NeedCopy-->
```

Pour modifier une connexion unique de formulaire à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set tm formSSOAction <name> -actionURL <URL> -userField <string> -
    passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <
    string>] [-responsesize <positive_integer>][-nvtype ( STATIC |
    DYNAMIC )][-submitMethod ( GET | POST )]
```



```
<!--NeedCopy-->
```

Exemple

```
set tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nameValuePair "loginID passwd" -responsesize "9096"
-nvtype STATIC -submitMethod GET
 - sessTimeout 10 -defaultAuthorizationAction ALLOW
<!--NeedCopy-->
```

Pour supprimer un profil SSO de formulaire à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm tm formSSOAction <name>
<!--NeedCopy-->
```

Exemple

```
rm tm sessionAction SSO-Prof-1
<!--NeedCopy-->
```

Pour configurer les profils SSO de formulaire à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Trafic**.
2. Dans le volet d'informations, cliquez sur l'onglet **Form SSO Profiles** .
3. Dans l'onglet Form SSO Profiles, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau profil SSO de formulaire, cliquez sur **Ajouter**.
   - Pour modifier un profil SSO de formulaire existant, sélectionnez-le, puis cliquez sur Modifier.
4. Dans la boîte de dialogue **Créer un profil SSO deformulaire ou Configurer un profil SSO de** formulaire, spécifiez les valeurs des paramètres :
   - NOM* : nom (ne peut pas être modifié pour une action de session précédemment configurée.)
   - URL de l'action*—ActionUrl
   - Champ Nom d'utilisateur*—Champ utilisateur
   - Champ de mot de passe*—PassField
   - Expression* : règle de réussite SSO
   - Paire de valeurs de nom—NameValuePair

- Taille de la réponse : taille de la réponse
- Extraction : type NV
- Méthode d'envoi : méthode d'envoi

5. Cliquez sur **Créer** ou sur **OK**, puis cliquez sur **Fermer**. Le profil SSO de formulaire que vous avez créé apparaît dans le volet **Stratégies de trafic**, **Profils**et **Profils SSO de formulaire** .

Profils SSO SAML

Pour activer et configurer l'authentification SSO SAML, vous devez d'abord créer un profil SSO SAML.

Pour créer un profil SSO SAML à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add tm samlSSOProfile <name> -samlSigningCertName <string> -
    assertionConsumerServiceURL <URL> -relaystateRule <expression> -
    sendPassword (ON | OFF) [-samlIssuerName <string>]
<!--NeedCopy-->
```

Exemple

```
add tm samlSSOProfile saml-SSO-Prof-1 -samlSigningCertName "Example,
    Inc."  -assertionConsumerServiceURL "https://service.example.com" -
    relaystateRule "true"  -sendPassword "ON" -samlIssuerName "Example,
    Inc."
<!--NeedCopy-->
```

Pour modifier un SSO SAML à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set tm samlSSOProfile <name> -samlSigningCertName <string> -
    assertionConsumerServiceURL <URL> -relaystateRule <expression> -
    sendPassword (ON | OFF) [-samlIssuerName <string>]
<!--NeedCopy-->
```

Exemple

```
set tm samlSSOProfile saml-SSO-Prof-1 -samlSigningCertName "Example,
    Inc."  -assertionConsumerServiceURL "https://service.example.com" -
    relaystateRule "true"  -sendPassword "ON" -samlIssuerName "Example,
    Inc."
<!--NeedCopy-->
```


Pour supprimer un profil SSO SAML à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm tm samlSSOProfile <name>
<!--NeedCopy-->
```

Exemple

```
rm tm sessionAction saml-SSO-Prof-1
<!--NeedCopy-->
```

Pour configurer un profil SSO SAML à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Trafic.**
2. Dans le volet d'informations, cliquez sur l'onglet **Profils SSO SAML** .
3. Dans l'onglet **Profils SSO SAML**, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau profil SSO SAML, cliquez sur **Ajouter.**
   - Pour modifier un profil SSO SAML existant, sélectionnez-le, puis cliquez sur **OuvrirModifier**.
4. Dans la boîte de dialogue **Créer des profils SSOSAML ou Configurer les profils SSO** SAML, définissez les paramètres suivants :
   - Nom*
   - Nom du certificat de signation*
   - URL ACS *
   - Règle de l'état du relais *
   - Envoyer mot de passe
   - Nom de l'émetteur
5. Cliquez sur **Créer** ou sur **OK**, puis cliquez sur **Fermer.** Le profil SSO SAML que vous avez créé apparaît dans le volet Stratégies de trafic, profils et profils SSO SAML.

Délai d'expiration de session pour OWA 2010

Vous pouvez désormais forcer le délai d'expiration des connexions OWA 2010 après une période d'inactivité spécifiée. OWA envoie des requêtes Keepalive répétées au serveur pour éviter les délais d'expiration. Le fait de garder les connexions ouvertes peut interférer avec l'authentification unique.

Pour forcer l'expiration d'OWA 2010 après une période spécifiée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :


```
add tm trafficAction <actname> [-forcedTimeout <forcedTimeout> -
    forcedTimeoutVal <mins>]
<!--NeedCopy-->
```

Par<actname>, remplacez un nom pour votre stratégie de trafic. Pour<mins>, remplacez le nombre de minutes après lesquelles un délai d'expiration forcé doit être initié. Pour <forcedTimeout>, remplacez l'une des valeurs suivantes :

-**START** — Démarre le minuteur pour un délai d'expiration forcé si aucun minuteur n'a déjà été démarré. S'il existe un minuteur en cours d'exécution, n'a aucun effet.
-**STOP — Arrête** une minuterie en cours d'exécution. Si aucune minuterie n'est trouvée, n'a aucun effet.
-**RESET** — Redémarre une minuterie en cours d'exécution. Si aucune minuterie en cours d'exécution n'est trouvée, démarre une minuterie comme si l'option START avait été utilisée.

```
add tm trafficPolicy <polname> <rule> <actname>
<!--NeedCopy-->
```

Par<polname>, remplacez un nom pour votre stratégie de trafic. Pour<rule>, remplacez une règle dans la stratégie Citrix ADC Advanced.

```
bind lb vserver <vservername>  - policyName <name> -priority <number>
<!--NeedCopy-->
```

Par<vservername>, remplacez le nom du serveur virtuel de gestion du trafic d'authentification, d'autorisation et d'audit. Par<priority>, remplacez un entier qui désigne la priorité de la stratégie.

Exemple

```
add tm trafficAction act-owa2010timeout -forcedTimeout RESET -
    forcedTimeoutVal 10
add tm trafficPolicy pol-owa2010timeout true act-owa2010timeout
bind lb vserver vs-owa2010 -policyName pol-owa2010timeout -priority 10
<!--NeedCopy-->
```

Limitation du débit pour Citrix Gateway

October 5, 2021

La fonctionnalité de limitation de débit de Citrix Gateway vous permet de définir la charge maximale pour une entité réseau ou une entité virtuelle donnée sur l'appliance Citrix Gateway. Étant donné que

l'appliance Citrix Gateway consomme tout le trafic non authentifié, elle est souvent exposée à des demandes de traitement à un taux élevé. La fonction de limitation de débit vous permet de configurer l'appliance Citrix Gateway pour surveiller le débit de trafic associé à une entité et prendre des mesures préventives, en temps réel, en fonction du trafic. Pour plus d'informations sur le fonctionnement de la limitation de débit dans une appliance Citrix ADC, voir Limitation de débit.

Citrix ADC dispose de la fonction de limitation de débit qui fournit une protection aux serveurs back-end pour un taux imprévu. Étant donné que la fonctionnalité de Citrix ADC ne servait pas le trafic non authentifié que Citrix Gateway gère, Citrix Gateway avait besoin de sa propre fonctionnalité de limitation de débit. Cela est nécessaire pour vérifier un taux imprévu de demandes provenant de diverses sources auxquelles l'appliance Citrix Gateway est exposée. Par exemple, les demandes de connexion/de contrôle non authentifiées et certaines API exposées pour les validations des utilisateurs finaux ou des appareils.

Cas d'utilisation courants pour la limitation de débit

- Limitez le nombre de demandes par seconde à partir d'une URL.
- Supprimer une connexion basée sur les cookies reçus dans la demande d'un hôte particulier si la demande dépasse la limite de débit.
- Limitez le nombre de requêtes HTTP qui arrivent du même hôte (avec un masque de sous-réseau particulier) et qui ont la même adresse IP de destination.

Configurer la limitation de débit pour Citrix Gateway

Conditions préalables

Un serveur virtuel d'authentification configuré.

Points à noter

- Au cours des étapes de configuration, un exemple d'identificateur de limite est configuré. La même chose peut être configurée avec tous les paramètres pris en charge comme le sélecteur de flux, mode. Pour obtenir une description exhaustive des capacités de limitation de débit, voir Limitation de débit.
- La stratégie peut également être liée à un serveur virtuel VPN comme suit. Vous avez besoin d'un serveur virtuel VPN configuré pour lier les stratégies à l'aide de la commande suivante.

```
1 bind vpn vserver -policy denylogin -pri 1 -type aaa_request
2 <!--NeedCopy-->
```


- AAA_REQUEST est un nouveau point de liaison introduit pour les stratégies de répondeur. Les stratégies configurées à ce point de liaison sont appliquées à toutes les demandes entrantes sur le serveur virtuel spécifié. Les stratégies sont traitées pour le trafic non authentifié/de contrôle avant tout autre traitement.
- La liaison de la stratégie au serveur virtuel Citrix Gateway permet de limiter le débit au niveau du point de liaison AAA_REQUEST pour tout le trafic consommé par Citrix Gateway, y compris les demandes non authentifiées.
- La liaison de la stratégie à un débit de serveur virtuel d'authentification limite les demandes non authentifiées/de contrôle qui touchent le serveur virtuel d'authentification.

Pour configurer la limitation de débit à l'aide de l'interface de ligne de commande, à l'invite de commandes, tapez les commandes suivantes :

```
1 add limitIdentifier <limitIdentifier name> -threshold <positive_integer
     > -timeslice <positive_integer> -mode <mode type>
2 <!--NeedCopy-->
```

```
1 Example: add limitIdentifier limit_one_login -threshold 10 -timeslice
     4294967290 -mode REQUEST_RATE
2 <!--NeedCopy-->
```

```
1 add responderaction denylogin respondwith  ' "HTTP/1.1 200 OK\r\n\r\n"
      +  "Request is denied due to unusual rate" '
2 <!--NeedCopy-->
```

```
1 add responder policy denylogin 'sys.check_limit("limit_one_login")'
     denylogin
2 <!--NeedCopy-->
```

```
1 bind authentication vserver <vserver name> -policy denylogin  -pri 1  -
     type aaa_request
2 <!--NeedCopy-->
```

```
1 Example: bind authentication vserver authvserver -policy denylogin  -
     pri 1  -type aaa_request
2 <!--NeedCopy-->
```

Description des paramètres

- **LimitIdentifier :** nom d'un identificateur de limite de taux. Doit commencer par une lettre ASCII ou un caractère de soulignement (_) et ne doit être composé que de caractères

alphanumériques ou de soulignement ASCII. Les mots réservés ne doivent pas être utilisés. Il s'agit d'un argument obligatoire. Longueur maximale : 31

- **threshold :** nombre maximal de demandes autorisées dans la tranche de temps donnée lorsque les demandes (le mode est défini sur REQUEST_RATE) sont suivies par tranche de temps. Lorsque les connexions (le mode est défini sur CONNECTION) sont suivies, il s'agit du nombre total de connexions qui seraient laissées passer. Valeur par défaut : 1 Valeur minimale : 1 Valeur maximale : 4294967295
- **TimeSlice -** Intervalle de temps, en millisecondes, spécifié en multiples de 10, pendant lequel les demandes sont suivies pour vérifier si elles dépassent le seuil. L'argument n'est nécessaire que lorsque le mode est défini sur REQUEST_RATE. Valeur par défaut : 1000 Valeur minimale : 10 Valeur maximale : 4294967295
- **mode -** Définit le type de trafic à suivre.
  - REQUEST_RATE - Effectue le suivi des requêtes/tranche de temps.
  - CONNEXION - Effectue le suivi des transactions actives.

Pour configurer la limitation de débit à l'aide de l'interface graphique Citrix ADC :

1. Accédez à **AppExpert > Limitation de débit > Identificateurs de limite**, cliquez sur **Ajouter** et spécifiez les détails pertinents comme indiqué dans la section CLI.



2. Accédez à **AppExpert>Responder>Stratégies**. Sur la page **Stratégies de répondeur**, cliquez sur **Ajouter**.
3. Sur la page **Créer une stratégie de répondeur**, créez une stratégie de répondeur avec une action de répondeur qui possède l'identificateur de limite.
4. Pour créer une action de répondeur, cliquez sur **Ajouter** en regard de **Action** et saisissez un nom pour l'action du répondeur.
5. Sélectionnez le type **Répondre avec** dans le menu déroulant, spécifiez l'expression suivante, « HTTP/1.1 200 OK \ r \ n \ r \ n"+ « La demande est refusée en raison d'un taux inhabituel », puis cliquez sur **Créer**.



6. Pour créer une stratégie de répondeur, sur la page **Créer une stratégie de répondeur**, entrez un nom pour la stratégie de répondeur, spécifiez l'expression suivante, 'sys.check_limit (« limit_one_login ») ', puis cliquez sur **Créer**.



7. Liez la stratégie de répondeur au serveur virtuel d'authentification.
   - a. Accédez à **Security>AAA-Application Traffic>Virtual Server**.
   - b. Sélectionnez le serveur virtuel.
   - c. Ajoutez une stratégie.
   - d. Choisissez la stratégie de répondeur que vous souhaitez lier au serveur, définissez la priorité.
   - e. Choisissez le type **AAA-REQUEST** et cliquez sur **Continuer**.



> **Remarque :** Vous pouvez également activer la limitation de débit au point de liaison AAA_REQUEST pour le serveur virtuel VPN.

Configuration pour les cas d'utilisation courants de l'application de la limitation de débit à Citrix Gateway

Voici des exemples de commandes permettant de configurer des cas d'utilisation courants.

- Limitez le nombre de demandes par seconde à partir d'une URL.

```
1  add stream selector ipStreamSelector http.req.url  "client.ip.src
       "
2
3  add ns limitIdentifier ipLimitIdentifier  -threshold 4  -
       timeslice 1000  -mode request_rate  -limitType smooth  -
       selectorName ip StreamSelector
4
5  add responder policy ipLimitResponderPolicy  "http.req.url.
       contains(\" myasp.asp\" ) && sys.check_limit(\"
       ipLimitIdentifier\" )"  myWebSiteRedirectAction
6
7  bind authentication virtual server authvserver -policy denylogin
       -pri 1  -type aaa_request
8  <!--NeedCopy-->
```

- Supprimer une connexion basée sur les cookies reçus à la demande de www.yourcompany.com si la demande dépasse la limite de débit.

```
1  add stream selector cacheStreamSelector  "http.req.cookie.value(\
       " mycookie\" )"   "client.ip.src.subnet(24)"
2
```



```
add ns limitIdentifier myLimitIdentifier -Threshold 2 -
    timeSlice 3000 -selectorName reqCookieStreamSelector

add responder action sendRedirectURL redirect `"http://www.
    mycompany.com"` + http.req.url'

add responder policy rateLimitCookiePolicy

 “http.req.url.contains(\www.yourcompany.com) && sys.check_limit
    (\” myLimitIdentifier\” )” sendRedirectUrl

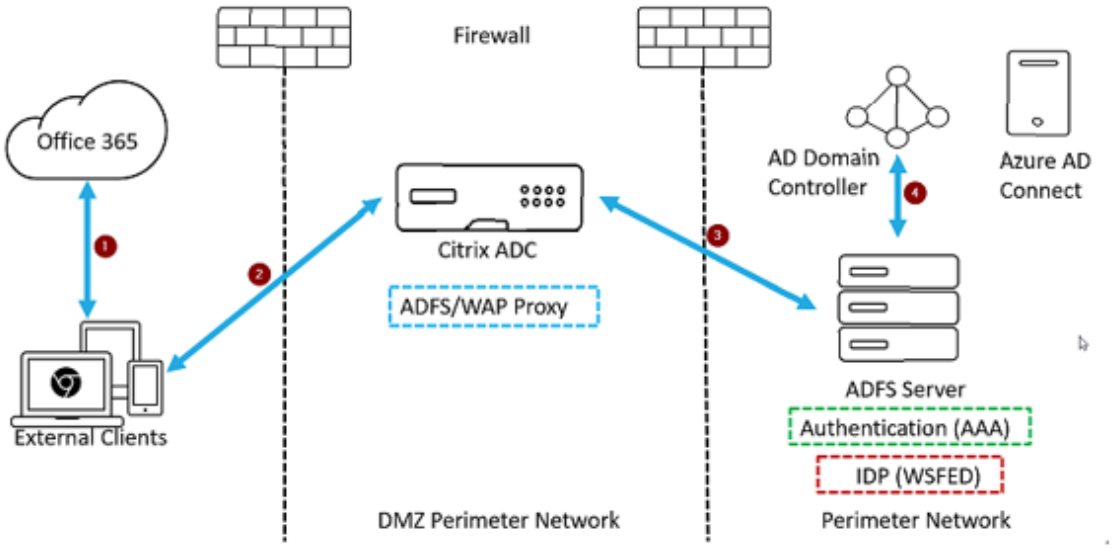
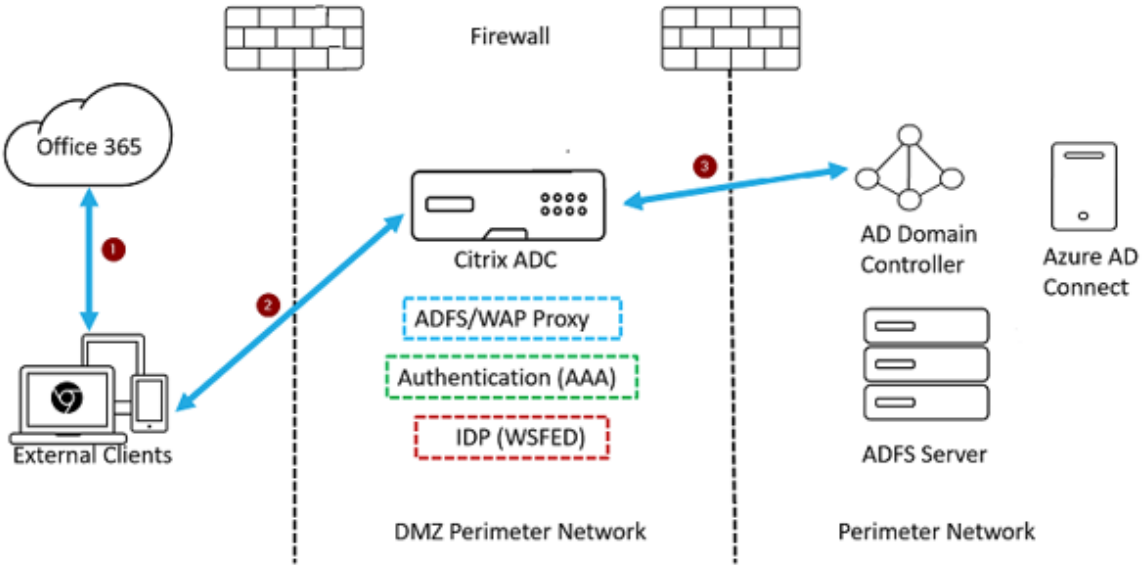
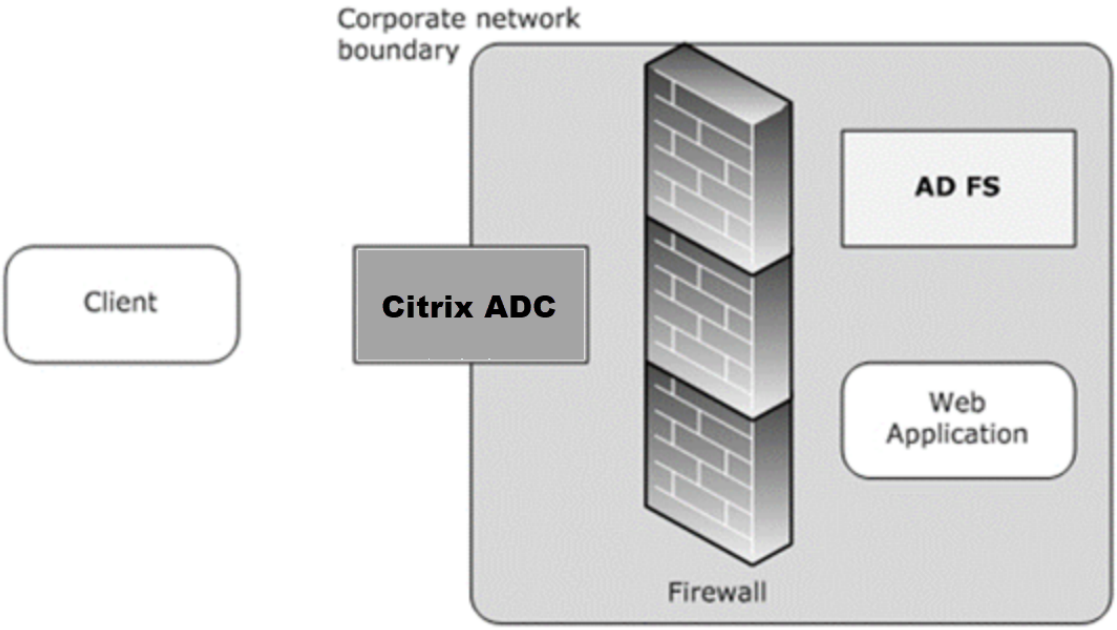
<!--NeedCopy-->
```

- Limitez le nombre de requêtes HTTP qui arrivent du même hôte (avec un masque de sous-réseau de 32) et qui ont la même adresse IP de destination.

```
add stream selector ipv6_sel “CLIENT.IPv6.src.subnet(32)” CLIENT
    .IPv6.dst Q.URL

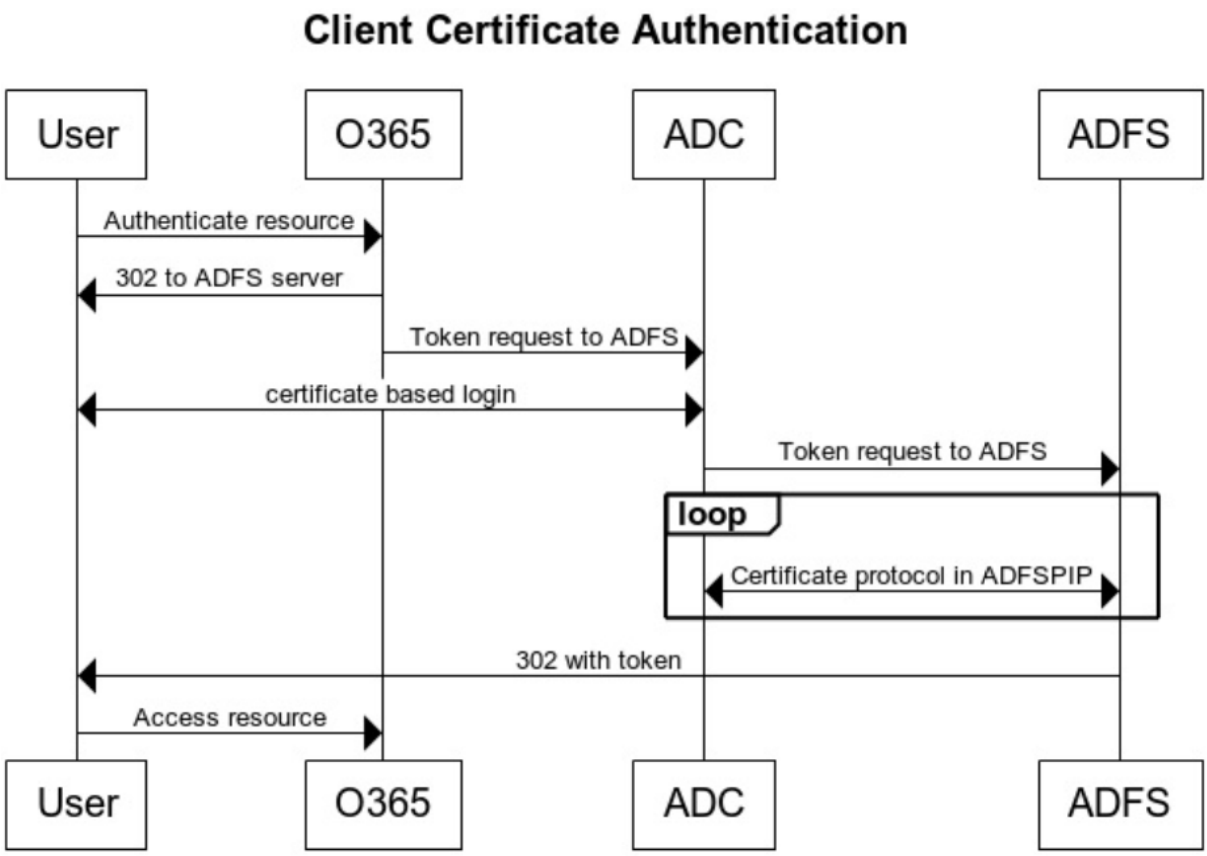
add ns limitIdentifier ipv6_id -imeSlice 20000 -selectorName
    ipv6_sel

add lb vserver ipv6_vip HTTP 3ffe:: 209 80 -persistenceType NONE
     -cltTime

add responder action redirect_page redirect “\” `http://
    redirectpage.com/\” "`

add responder policy ipv6_resp_pol “SYS.CHECK_LIMIT(\” ipv6_id\
    ” )” redirect_page

bind responder global ipv6_resp_pol 5 END -type DEFAULT
<!--NeedCopy-->
```

Autorisation de l’accès des utilisateurs aux ressources applicatives

January 21, 2021

Vous pouvez contrôler les ressources auxquelles un utilisateur authentifié peut accéder dans une application.

Pour ce faire, associez une stratégie d’autorisation à chacun des utilisateurs, individuellement ou en associant la stratégie à un groupe d’utilisateurs. La stratégie d’autorisation doit spécifier les éléments

suivants :

- **Règle.** Ressource à laquelle l'accès doit être autorisé. Cela peut être spécifié à l'aide d'expressions de base ou avancées.
- **Action.** Indique si l'accès à la ressource doit être autorisé ou refusé.

Par défaut, l'accès à toutes les ressources d'une application est **REFUSÉ** à tous les utilisateurs. Toutefois, vous pouvez modifier cette action d'autorisation par défaut pour **autoriser** l'accès à tous les utilisateurs (en définissant les paramètres de session dans le profil de session ou en définissant les paramètres de session globaux).

> **Avertissement**
>
> Pour une sécurité optimale, Citrix vous recommande de ne pas modifier l'action d'autorisation par défaut de DENY à ALLOW. Au lieu de cela, il est conseillé de créer des stratégies d'autorisation spécifiques pour les utilisateurs qui ont besoin d'accéder à des ressources spécifiques.

Pour configurer l'autorisation à l'aide de l'interface de ligne de commande

1. Configurez la stratégie d'autorisation.

   ns-cli-prompt> **add authorization policy <name> <rule> <action>**

2. Associez la stratégie à l'utilisateur ou au groupe approprié.

   - Liez la stratégie à un utilisateur spécifique.

     ns-cli-prompt> **bind aaa user <username> -policy** <policyname>

   - Liez la stratégie à un groupe spécifique.

     ns-cli-prompt> **bind aaa group <groupName> -policy** <policyname>

Pour configurer l'autorisation à l'aide de l'interface graphique (onglet Configuration)

1. Créez la stratégie d'autorisation.

   Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Autorisation**, cliquez sur **Ajouter**, puis définissez la stratégie selon vos besoins.

2. Associez la stratégie à l'utilisateur ou au groupe approprié.

   Accédez à **Sécurité > AAA - Trafic des applications > Utilisateurs** ou **groupes**, puis modifiez l'utilisateur ou le groupe concerné pour l'associer à la stratégie d'autorisation.

Exemples de configurations d'autorisation

Voici quelques exemples de configurations pour autoriser l'accès utilisateur à certaines ressources d'application. Notez qu'il s'agit de commandes CLI. Vous pouvez faire des configurations similaires à l'aide de l'interface graphique, bien que vous ne devez pas placer l'expression entre guillemets («).

- `add authorization policy authzpol1 "HTTP.REQ.URL.SUFFIX.EQ(\"gif\")" ALLOW<!--NeedCopy-->`
- `bind aaa user user1 -policy authzpol1<!--NeedCopy-->`
- `add authorization policy authzpol2 "HTTP.REQ.URL.SUFFIX.EQ(\"png\")" DENY<!--NeedCopy-->`
- `bind aaa group group1 -policy authzpol2<!--NeedCopy-->`

Audit des sessions authentifiées

January 21, 2021

Vous pouvez configurer l'appliance Citrix ADC pour conserver un journal de tous les événements déclenchés dans une session authentifiée. À l'aide de ces informations, vous pouvez auditer les informations d'état et d'état, pour afficher l'historique des utilisateurs dans l'ordre chronologique.

Pour ce faire, définissez une stratégie d'audit qui spécifie les éléments suivants :

- **Type de journal.** Les journaux peuvent être stockés à distance (syslog) ou localement sur l'appliance Citrix ADC (nslog).
- **Règle.** Conditions dans lesquelles les journaux sont stockés.
- **Action.** Détails du serveur de journaux et autres détails pour créer les entrées de journal.

Cette stratégie d'audit peut être configurée à différents niveaux : niveau utilisateur, niveau groupe, authentification, autorisation et audit serveur virtuel, et niveau système global. Les stratégies configurées au niveau de l'utilisateur ont la priorité la plus élevée.

> **Remarque**
>
> Cette rubrique détaille les étapes d'utilisation de syslog. Apportez les modifications nécessaires pour utiliser nslog.

Pour configurer l'audit syslog à l'aide de l'interface de ligne de commande

1. Configurez le serveur d'audit avec les paramètres de journal pertinents.

   ns-cli-prompt> **add audit syslogAction <name> <serverIP> ...**

2. Configurez la stratégie d'audit en associant le serveur d'audit.

   ns-cli-prompt> **add audit syslogPolicy <name> <rule> <action>**

3. Associez la stratégie d'audit à l'une des entités suivantes :

   - Liez la stratégie à un utilisateur spécifique.

     ns-cli-prompt> **bind aaa user <userName>-policy** <policyname> …

   - Liez la stratégie à un groupe spécifique.

     ns-cli-prompt> **bind aaa group <groupName>-policy** <policyname> …

   - Liez la stratégie à un serveur virtuel d'authentification, d'autorisation et d'audit.

     ns-cli-prompt> **bind authentication vserver <name> -policy** <policyname> …

   - Liez la stratégie globalement à l'appliance Citrix ADC.

     ns-cli-prompt> **bind tm global -policyName** <policyname> …

Pour configurer l'audit syslog à l'aide de l'interface graphique (onglet Configuration)

1. Configurez le serveur d'audit et la stratégie.

   Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Audit > Syslog**, puis configurez le serveur et la stratégie dans les onglets correspondants.

2. Associez la stratégie à l'une des options suivantes :

   - Liez la stratégie à un utilisateur spécifique.

     Accédez à **Sécurité > AAA - Trafic des applications > Utilisateurs** et associez la stratégie d'autorisation à l'utilisateur concerné.

   - Liez la stratégie à un groupe spécifique.

     Accédez à **Sécurité > AAA - Trafic des applications > Groupes** et associez la stratégie d'autorisation au groupe concerné.

   - Liez la stratégie à un serveur virtuel d'authentification, d'autorisation et d'audit.

     Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels** et associez la stratégie d'autorisation au serveur virtuel concerné.

   - Liez la stratégie globalement à l'appliance Citrix ADC.

     Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Audit > Syslog** ou **Nslog**, sélectionnez la stratégie d'autorisation et cliquez sur **Action > Liaisons globales** pour lier la stratégie globalement.

Citrix ADC en tant que proxy Active Directory Federation Services

August 20, 2021

ADFS (Active Directory Federation Services) est un service Microsoft qui permet une expérience d'authentification unique (SSO) pour les clients authentifiés Active Directory vers des ressources en dehors du centre de données d'entreprise. Une batterie de serveurs ADFS permet aux utilisateurs internes d'accéder à des services hébergés dans le cloud externe. Mais au moment où les utilisateurs externes sont intégrés dans le mélange, les utilisateurs externes doivent avoir un moyen de se connecter à distance et d'accéder aux services basés sur le cloud via une identité fédérée. La plupart des entreprises ne préfèrent pas que le serveur ADFS soit exposé dans la zone DMZ. Par conséquent, le proxy ADFS joue un rôle critique dans la connectivité des utilisateurs distants et l'accès aux applications.

Depuis plus d'une décennie, l'appliance Citrix ADC joue des rôles similaires en matière de connectivité utilisateur distante et d'accès aux applications. L'appliance Citrix ADC devient la solution préférée à utiliser comme proxy ADFS pour prendre en charge une nouvelle implémentation ADFS pour activer les services suivants :

- Connectivité sécurisée.
- Authentification et gestion de l'identité fédérée.

Pour plus d'informations sur Citrix ADC en tant qu'IdP SAML, consultez Citrix ADC as a SAML IdP.

Avantages du proxy ADFS

- Réduit l'empreinte dans la zone DMZ pour répondre aux besoins de la plupart des entreprises.
- Offre une expérience SSO pour les utilisateurs finaux.
- Prend en charge des méthodes riches pour la pré-authentification et permet l'authentification multifactorielle.
- Prend en charge les clients actifs et passifs.

Conditions préalables à l'utilisation de Citrix ADC en tant que proxy ADFS

Avant de configurer l'appliance Citrix ADC en tant que proxy ADFS, assurez-vous que les conditions préalables suivantes sont remplies.

- Une appliance Citrix ADC avec version 12.1 ou version ultérieure.
- Serveur ADFS de domaine.
- Certificat SSL de domaine.
- IP virtuelle pour le serveur virtuel de commutation de contenu.

- Activez les fonctionnalités d'équilibrage de charge, de déchargement SSL, de commutation de contenu, de réécriture et d'authentification, d'autorisation et d'audit de gestion du trafic sur l'appliance Citrix ADC.

Configurer l'appliance Citrix ADC en tant que proxy ADFS

Pour atteindre ce cas d'utilisation, vous configurez Citrix ADC en tant que proxy ADFS dans la zone DMZ. Le serveur ADFS est configuré avec le contrôleur de domaine AD dans le back-end.



1. Une demande client pour accéder à Microsoft Office365 est redirigée vers Citrix ADC déployé en tant que proxy ADFS.
2. Les informations d'identification de l'utilisateur sont transmises au serveur ADFS.
3. Le serveur ADFS authentifie les informations d'identification avec AD local du domaine.
4. Le serveur ADFS lors de la validation réussie des informations d'identification avec AD, génère un jeton qui est transmis à Microsoft Office365 pour l'établissement de session.

Voici les étapes de haut niveau impliquées dans la configuration de l'appliance Citrix ADC avant de configurer en tant que proxy ADFS.

À l'invite de commandes Citrix ADC, tapez les commandes suivantes :

1. Créez un profil SSL pour back-end et activez SNI dans le profil SSL. Désactivez SSLV3/TLS1.

   ```
   add ssl profile <new SSL profile> -sniEnable ENABLED -ssl3 DISABLED -
   tls1 DISABLED -commonName <FQDN of ADFS>
   ```

2. Désactivez SSLV3/TLS1 pour le service.

   ```
   set ssl service <adfs service name> -sslProfile <SSL profile created in
    the above step>
   ```


3. Activez l'extension SNI pour les poignées de main du serveur principal.

   - `set vpn parameter -backendServerSni ENABLED`
   - `set ssl parameter -denySSLReneg NONSECURE`

Configurer l'appliance Citrix ADC en tant que proxy ADFS à l'aide de l'interface de ligne de commande

Les sections suivantes sont catégorisées en fonction de la nécessité d'effectuer les étapes de configuration.

Pour configurer le service ADFS

1. Configurez le service ADFS sur Citrix ADC pour le serveur ADFS.

   ```
   add service <Domain_ADFS_Service> <ADFS Server IP> SSL 443 -gslb NONE -
   maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF
   -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
   ```

   Exemple

   add service CTXTEST_ADFS_Service 1.1.1.1 SSL 443 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

2. Configurez le nom de domaine complet pour le serveur virtuel de commutation de contenu et activez SNI.

   ```
   set ssl service <Domain_ADFS_Service> -SNIEnable ENABLED -commonName <
   sts.domain.com>
   ```

   Exemple

   set ssl service CTXTEST_ADFS_Service -SNIEnable ENABLED -commonName sts.ctxtest.com

Pour configurer le serveur virtuel d'équilibrage de charge ADFS

> **Important**
>
> Le certificat SSL de domaine (SSL_CERT) est requis pour le trafic sécurisé.

1. Configurez le serveur virtuel d'équilibrage de charge ADFS.

   ```
   add lb vserver <Domain_ADFS_LBVS> SSL <IP_address> -persistenceType
   NONE -cltTimeout 180
   ```

   Exemple


```
add lb vserver CTXTEST_ADFS_LBVS SSL 192.168.1.0 -persistenceType NONE
-cltTimeout 180
```

2. Liez le serveur virtuel d'équilibrage de charge ADFS au service ADFS.

   ```
   bind lb vserver <Domain_ADFS_LBVS> <Domain_ADFS_Service>
   ```

   Exemple

   ```
   bind lb vserver CTXTEST_ADFS_LBVS CTXTEST_ADFS_Service
   ```

3. Liez une paire de clés de certificat de serveur virtuel SSL.

   ```
   bind ssl vserver <Domain_ADFS_LBVS> -certkeyName <SSL_CERT>
   ```

   Exemple

   ```
   bind ssl vserver CTXTEST_ADFS_LBVS -certkeyName ctxtest_newcert_2019
   ```

Pour configurer le serveur virtuel de commutation de contenu pour le domaine

> **Remarque**
>
> Une IP virtuelle gratuite (par exemple, 2.2.2.2), qui est Natted à IP publique est nécessaire pour le serveur virtuel de commutation de contenu. Il doit être accessible à la fois pour le trafic externe et interne.

1. Créez un serveur virtuel de commutation de contenu avec VIP gratuit.

   ```
   add cs vserver <Domain_CSVS> SSL <FREE VIP> 443 -cltTimeout 180 -
   persistenceType NONE
   ```

   Exemple

   ```
   add cs vserver CTXTEST_CSVS SSL 2.2.2.2 443 -cltTimeout 180 -persistenceType
    NONE
   ```

2. Liez le serveur virtuel de commutation de contenu au serveur virtuel d'équilibrage de charge.

   ```
   bind cs vserver <Domain_CSVS> -lbvserver <Domain_ADFS_LBVS>
   ```

   Exemple

   - `bind cs vserver CTXTEST_CSVS -lbvserver CTXTEST_ADFS_LBVS`
   - `set ssl vserver CTXTEST_CSVS -sessReuse DISABLED`

3. Liez une paire de clés de certificat de serveur virtuel SSL.

   ```
   bind ssl vserver <Domain_CSVS> -certkeyName <SSL_CERT>
   ```

   Exemple

   ```
   bind ssl vserver CTXTEST_CSVS -certkeyName ctxtest_newcert_2019
   ```


Protocoles pris en charge

Les protocoles fournis par Microsoft jouent un rôle essentiel dans l'intégration avec l'appliance Citrix ADC. Citrix ADC en tant que proxy ADFS prend en charge les protocoles suivants :

- **WS-Federation**. Pour plus de détails, voir Protocole Web Services Federation.
- **ADFSPIP**. Pour plus de détails, voir Conformité au protocole d'intégration du proxy Active Directory Federation Service

> **Remarque**
>
> L'appliance Citrix ADC ne prend pas en charge l'authentification par certificat de périphérique lorsqu'elle est déployée en tant que proxy ADFS.

Protocole Web Services Federation

January 21, 2021

Web Services Federation (WS-Federation) est un protocole d'identité qui permet à un service de jeton de sécurité (STS) dans un domaine d'approbation de fournir des informations d'authentification à un STS dans un autre domaine d'approbation lorsqu'il existe une relation d'approbation entre les deux domaines.

Avantages de WS-Federation

WS-Federation prend en charge les clients actifs et passifs tandis que SAML IdP ne prend en charge que les clients passifs.

- Les clients actifs sont des clients natifs Microsoft tels que Outlook et Office (Word, PowerPoint, Excel et OneNote).
- Les clients passifs sont des clients basés sur un navigateur tels que Google Chrome, Mozilla Firefox et Internet Explorer.

Conditions préalables à l'utilisation de Citrix ADC en tant que WS-Federation

Avant de configurer l'appliance Citrix ADC en tant que proxy ADFS, vérifiez les points suivants :

- Active Directory.
- Certificat SSL de domaine.
- Le certificat SSL Citrix ADC et le certificat de signature de jeton ADFS sur le serveur ADFS doivent être identiques.

> **Important**
>
> IdP SAML est désormais capable de gérer le protocole WS-Federation. Par conséquent, pour configurer l'IdP WS-Federation, vous devez réellement configurer l'IdP SAML. Vous ne voyez aucune interface utilisateur mentionnant explicitement WS-Federation.

Fonctionnalités prises en charge par Citrix ADC lorsqu'il est configuré en tant que proxy ADFS et IdP WS-Federation

Le tableau suivant répertorie les fonctionnalités prises en charge par l'appliance Citrix ADC lorsqu'elles sont configurées en tant que proxy ADFS et IdP de fédération WS-.

Fonctionnalités	Configurer l'appliance Citrix ADC en tant que proxy ADFS	Citrix ADC en tant que fournisseur d'identité WS-Federation	Citrix ADC en tant qu'ADFSPIP
Équilibrage de charge	Oui	Oui	Oui
Terminaison SSL	Oui	Oui	Oui
Limitation de taux	Oui	Oui	Oui
Consolidation (réduction de l'encombrement des serveurs DMZ et sauvegarde des adresses IP publiques)	Oui	Oui	Oui
Pare-feu d'application Web (WAF)	Oui	Oui	Oui
Déchargement de l'authentification vers l'appliance Citrix ADC	Non	Oui (Clients actifs et passifs)	Oui
Connexion unique (SSO)	Non	Oui (Clients actifs et passifs)	Oui
Authentification multifacteur (nFactor)	Non	Oui (Clients actifs et passifs)	Oui
Authentification multifacteur Azure	Non	Oui (Clients actifs et passifs)	Oui

Fonctionnalités	Configurer l'appliance Citrix ADC en tant que proxy ADFS	Citrix ADC en tant que fournisseur d'identité WS-Federation	Citrix ADC en tant qu'ADFSPIP
La batterie de serveurs ADFS peut être évitée	Non	Oui	Oui

Configurer l'appliance Citrix ADC en tant que fournisseur d'identité WS-Federation

Configurez Citrix ADC en tant qu'IdP WS-Federation (IdP SAML) dans une zone DMZ. Le serveur ADFS est configuré avec le contrôleur de domaine AD dans le back-end.



1. La demande client vers Microsoft Office365 est redirigée vers l'appliance Citrix ADC.
2. L'utilisateur saisit les informations d'identification pour l'authentification multifacteur.
3. Citrix ADC valide les informations d'identification avec AD et génère un jeton nativement sur l'appliance Citrix ADC. Les informations d'identification sont transmises à Office365 pour y accéder.

> **Remarque**
>
> La prise en charge des IdP WS-Federation est effectuée en mode natif via l'appliance Citrix ADC par rapport à l'équilibreur de charge F5 Networks.

Configurer l'appliance Citrix ADC en tant qu'IdP de fédération WS-(IdP SAML) à l'aide de l'interface de ligne de commande

Les sections suivantes sont catégorisées en fonction de la nécessité d'effectuer les étapes de configuration.

Pour configurer l'authentification LDAP et ajouter une stratégie

> **Important**
>
> Pour les utilisateurs de domaine, pour ouvrir une session à l'appliance Citrix ADC à l'aide de leurs adresses de messagerie d'entreprise, vous devez configurer les éléments suivants :

- Configurez le serveur d'authentification LDAP et la stratégie sur l'appliance Citrix ADC.
- Liez-la à votre authentification, autorisation et adresse IP virtuelle d'audit (l'utilisation d'une configuration LDAP existante est également prise en charge).
- `add authentication ldapAction <Domain_LDAP_Action> -serverIP <Active Directory IP> -serverPort 636 -ldapBase "cn=Users,dc=domain,dc=com"-ldapBindDn "cn=administrator,cn=Users,dc=domain,dc=com"-ldapBindDnPassword <administrator password> -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberOf -subAttributeName cn -secType SSL -ssoNameAttribute UserPrincipalName -followReferrals ON -Attribute1 mail -Attribute2 objectGUID`
- `add authentication Policy <Domain_LDAP_Policy> -rule true -action <Domain_LDAP_Action>`

Exemple

- `add authentication ldapAction CTXTEST_LDAP_Action -serverIP 3.3.3.3 -serverPort 636 -ldapBase "cn=Users,dc=ctxtest,dc=com"-ldapBindDn "cn=administrator,cn=Users,dc=ctxtest,dc=com"-ldapBindDnPassword xxxxxxxxxx -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberOf -subAttributeName cn -secType SSL -ssoNameAttribute UserPrincipalName -followReferrals ON -Attribute1 mail -Attribute2 objectGUID`
- `add authentication Policy CTXTEST_LDAP_Policy -rule true -action CTXTEST_LDAP_Action`

Pour configurer Citrix ADC en tant qu'IdP de fédération WS-ou IdP SAML

Créez une action et une stratégie WS-Federation IdP (IdP SAML) pour la génération de jetons. Associez-le au serveur virtuel d'authentification, d'autorisation et d'audit au stade ultérieur.

- add authentication samlIdPProfile <Domain_SAMLIDP_Profile> -samlIdPCertName <SSL_CERT> -assertionConsumerServiceURL "https://login.microsoftonline.com/login.srf"-samlIssuerName <Issuer Name for Office 365 in ADFS Server> -rejectUnsignedRequests OFF -audience urn:federation:MicrosoftOnline -NameIDFormat persistent -NameIDExpr "HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"-Attribute1 IDPEmail -Attribute1Expr "HTTP.REQ.USER.ATTRIBUTE(1)"
- add authentication samlIdPPolicy <Domain_SAMLIDP_Policy> -rule "HTTP.REQ.HEADER(\"referer\").CONTAINS(\"microsoft\")|| true"-action <Domain_SAMLIDP_Profile>

Exemple

- add authentication samlIdPProfile CTXTEST_SAMLIDP_Profile -samlIdPCertName ctxtest_newcert_2019 -assertionConsumerServiceURL "https://login.microsoftonline.com/login.srf"-samlIssuerName "http://ctxtest.com/adfs/services/trust/"-rejectUnsignedRequests OFF -audience urn:federation:MicrosoftOnline -NameIDFormat persistent -NameIDExpr "HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"-Attribute1 IDPEmail -Attribute1Expr "HTTP.REQ.USER.ATTRIBUTE(1)"
- add authentication samlIdPPolicy CTXTEST_SAMLIDP_Policy -rule "HTTP.REQ.HEADER(\"referer\").CONTAINS(\"microsoft\")|| true"-action CTXTEST_SAMLIDP_Profi

Pour configurer l'authentification, l'autorisation et l'audit du serveur virtuel afin d'authentifier les employés qui se connectent à Office365 à l'aide des informations d'identification d'entreprise

```
add authentication vserver <Domain_AAA_VS> SSL <IP_address>
```

Exemple

- add authentication vserver CTXTEST_AAA_VS SSL 192.168.1.0
- bind authentication vserver CTXTEST_AAA_VS -portaltheme RfWebUI

Pour lier un serveur virtuel d'authentification et une stratégie

- bind authentication vserver <Domain_AAA_VS> -policy <Domain_SAMLIDP_Policy> -priority 100 -gotoPriorityExpression NEXT
- bind authentication vserver <Domain_AAA_VS> -policy <Domain_LDAP_Policy> -priority 100 -gotoPriorityExpression NEXT

Exemple

- bind authentication vserver CTXTEST_AAA_VS -policy CTXTEST_SAMLIDP_Policy -priority 100 -gotoPriorityExpression NEXT
- bind authentication vserver CTXTEST_AAA_VS -policy CTXTEST_LDAP_Policy -priority 100 -gotoPriorityExpression NEXT
- bind ssl vserver CTXTEST_AAA_VS -certkeyName ctxtest_newcert_2019

Pour configurer la commutation de contenu

- add cs action <Domain_CS_Action> -targetVserver <Domain_AAA_VS>
- add cs policy <Domain_CS_Policy> -rule "is_vpn_url || http.req.url.contains(\"/adfs/ls\")|| http.req.url.contains(\"/adfs/services/trust\")|| -action <Domain_CS_Action>

Exemple

- add cs action CTXTEST_CS_Action -targetVserver CTXTEST_AAA_VS
- add cs policy CTXTEST_CS_Policy -rule "is_vpn_url || http.req.url.contains(\"/adfs/ls\")|| http.req.url.contains(\"/adfs/services/trust\")|| -action CTXTEST_CS_Action

Pour lier le contenu commutant de serveur virtuel à une stratégie

```
bind cs vserver CTXTEST_CSVS -policyName CTXTEST_CS_Policy -priority 100
```

Conformité au protocole d'intégration du proxy de service Active Directory Federation

August 20, 2021

Si des proxy tiers doivent être utilisés à la place du proxy d'application Web, ils doivent prendre en charge le protocole MS-ADFSPIP qui spécifie les règles d'intégration ADFS et WAP. ADFSPIP intègre les services de fédération Active Directory avec un proxy d'authentification et d'application pour permettre l'accès aux services situés à l'intérieur des limites du réseau d'entreprise pour les clients situés à l'extérieur de cette limite.



Conditions préalables

Pour établir la confiance entre le serveur proxy et la batterie ADFS, consultez la configuration suivante dans l'appliance Citrix ADC :

- Créez un profil SSL pour back-end et activez SNI dans le profil SSL. Désactivez SSLV3/TLS1. À l'invite de commandes, tapez la commande suivante :

```
add ssl profile <new SSL profile> -sniEnable ENABLED -ssl3
   DISABLED -tls1 DISABLED -commonName <FQDN of ADFS>
<!--NeedCopy-->
```

- Désactivez SSLV3/TLS1 pour le service. À l'invite de commandes, tapez la commande suivante :

```
set ssl service <adfs service name> -sslProfile
   ns_default_ssl_profile_backend
<!--NeedCopy-->
```

- Activez l'extension SNI pour les poignées de main du serveur principal. À l'invite de commandes, tapez la commande suivante :

```
set vpn parameter  - backendServerSni ENABLED

set ssl parameter -denySSLReneg NONSECURE
<!--NeedCopy-->
```


> **Important**
>
> Pour les scénarios de découverte Domicile (HRD) où l'authentification doit être déchargée sur le serveur ADFS, Citrix vous recommande de désactiver l'authentification et l'authentification unique sur l'appliance Citrix ADC.

Mécanisme d'authentification

Voici le flux d'événements de haut niveau pour l'authentification.

1. **Établir la confiance avec le serveur ADFS** — Le serveur Citrix ADC établit la confiance avec le serveur ADFS en enregistrant un certificat client. Une fois l'approbation établie, l'appliance Citrix ADC rétablit l'approbation après le redémarrage sans intervention de l'utilisateur.

   À l'expiration du certificat, vous devez rétablir l'approbation en supprimant et en ajoutant à nouveau le profil proxy ADFS.

2. **Points de terminaison publiés** : l'appliance Citrix ADC récupère automatiquement la liste des points de terminaison publiés sur l'établissement de post-approbation du serveur ADFS. Ces points de terminaison publiés filtrent les demandes transmises au serveur ADFS.

3. **Insérer des en-têtes dans les requêtes client** : lorsque l'appliance Citrix ADC tunnel les requêtes client, les en-têtes HTTP associés à ADFSPIP sont ajoutés dans le paquet lors de leur envoi au serveur ADFS. Vous pouvez implémenter le contrôle d'accès sur le serveur ADFS en fonction de ces valeurs d'en-tête. Les en-têtes suivants sont pris en charge.

   - X-MS-Proxy
   - X-MS-Endpoint-Absolute-Path
   - X-MS-Forwarded-Client-IP
   - X-MS-Proxy
   - X-MS-Target-Role
   - X-MS-ADFS-Proxy-client-IP

4. **Gérer le trafic des utilisateurs finaux** — Le trafic des utilisateurs finaux est acheminé en toute sécurité vers les ressources souhaitées.

   > **Remarque**
   >
   > L'appliance Citrix ADC utilise l'authentification basée sur les formulaires.

Configurer Citrix ADC pour qu'il fonctionne avec le serveur ADFS

Conditions préalables

- Configurez le serveur CS (Context Switching) en tant que serveur frontal avec authentification, autorisation et serveur d'audit derrière CS. À l'invite de commandes, tapez :


```
add cs vserver <cs vserver name> SSL 10.220.xxx.xx 443
-cltTimeout 180 -AuthenticationHost <adfs server hostname> -
   Authentication OFF -persistenceType NONE
<!--NeedCopy-->
```

```
add cs action <action name1> -targetLBVserver <lb vserver name>
<!--NeedCopy-->
```

```
add cs action <action name2> -targetLBVserver <lb vserver name>
<!--NeedCopy-->
```

```
add cs policy <policy name1> -rule " http.req.url.contains("/adfs
   /services/trust") || http.req.url.contains("federationmetadata
   /2007-06/federationmetadata.xml")" -action <action name1>
<!--NeedCopy-->
```

```
add cs policy <policy name2> -rule "HTTP.REQ.URL.CONTAINS("/adfs/
   ls")" -action <action name2>
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -policyName <policy name1> -
   priority 100
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -policyName <policy name2> -
   priority 110
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -lbvserver <lb vserver name>
<!--NeedCopy-->
```

- Ajouter un service ADFS. À l'invite de commandes, tapez :

```
add service <adfs service name> <adfs server ip> SSL 443
<!--NeedCopy-->
```

```
set ssl service <adfs service name> -sslProfile
   ns_default_ssl_profile_backend
<!--NeedCopy-->
```

- Ajoutez un serveur virtuel équilibré de charge. À l'invite de commandes, tapez :


```
add lb vserver <lb vserver name> SSL 0.0.0.0 0
<!--NeedCopy-->
```

```
set ssl vserver <lb vserver name> -sslProfile
   ns_default_ssl_profile_frontend
<!--NeedCopy-->
```

- Liez le service au serveur à charge équilibrée. À l'invite de commandes, tapez :

```
bind lb vserver <lb vserver name> <adfs service name>
<!--NeedCopy-->
```

Pour configurer Citrix ADC pour qu'il fonctionne avec le serveur ADFS, procédez comme suit :

1. Créer une clé de profil SSL CertKey à utiliser avec le profil proxy ADFS
2. Créer un profil proxy ADFS
3. Associer le profil proxy ADFS au serveur virtuel LB

Créer un certificat SSL avec clé privée à utiliser avec le profil proxy ADFS

À l'invite de commandes, tapez :

```
    add ssl certkey <certkeyname>  - cert <certificate path> -key <
       keypath>
<!--NeedCopy-->
```

Remarque : le fichier de certificat et le fichier de clé doivent être présents dans l'appliance Citrix ADC. Créer un profil proxy ADFS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add authentication adfsProxyProfile  <profile name> -serverUrl <https:
   //<server FQDN or IP address>/> -username <adfs admin user name> -
   password <password for admin user> -certKeyName <name of the CertKey
    profile created above>
<!--NeedCopy-->
```

Où ;

Profile name : nom du profil proxy AFDS à créer

ServerURL — Nom de domaine complet du service ADFS, y compris le protocole et le port. Par exemple, `https://adfs.citrix.com`

Nom d'utilisateur — Nom d'utilisateur d'un compte administrateur existant sur le serveur ADFS

Mot de passe — Mot de passe du compte admin utilisé comme nom d'utilisateur

CertKeyName — Nom du profil CertKey SSL créé précédemment

Associer le profil proxy ADFS au serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

Dans le déploiement ADFS, il existe deux serveurs virtuels d'équilibrage de charge, l'un pour le trafic client et l'autre pour l'échange de métadonnées. Le profil proxy ADFS doit être associé au serveur virtuel d'équilibrage de charge qui est en tête du serveur ADFS.

À l'invite de commandes, tapez :

```
set lb vserver <adfs-proxy-lb> -adfsProxyProfile <name of the ADFS
   proxy profile>
<!--NeedCopy-->
```

Soutien au renouvellement de la confiance pour ADFSPIP

Vous pouvez renouveler l'approbation des certificats existants qui sont sur le point d'expirer ou si le certificat existant n'est pas valide. Le renouvellement d'approbation des certificats n'est effectué que lorsque l'approbation est établie entre l'appliance Citrix ADC et le serveur ADFS. Pour renouveler la confiance du certificat, vous devez fournir le nouveau certificat.

> **Important**
>
> Une intervention manuelle est requise pour le renouvellement de confiance de nouveaux certificats.

L'exemple suivant répertorie les étapes impliquées dans le renouvellement de l'approbation de certificat :

1. L'appliance Citrix ADC envoie à la fois les anciens certificats (SerializedTrustCertificate) et les nouveaux certificats (SerializedReplacementCertificate) dans la demande POST au serveur ADFS pour renouvellement d'approbation.
2. Le serveur ADFS répond avec 200 OK si l'approbation est renouvelée avec succès.
3. L'appliance Citrix ADC met à jour l'état "ESTABLISHED_RENEW_SUCCESS" si le renouvellement de l'approbation est réussi. Si le renouvellement de l'approbation échoue, l'état est mis à jour en tant que "ESTABLISHED_RENEW_FAILED" et l'appliance Citrix ADC continue d'utiliser l'ancien certificat.

> **Remarque**
>
> Vous ne pouvez pas mettre à jour la clé de certificat si elle est déjà liée à un profil proxy ADFS.

Pour configurer le renouvellement d'approbation des certificats à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set authentication adfsProxyProfile <name> [-CertKeyName <string>]
<!--NeedCopy-->
```

Exemple :

```
set authentication adfsProxyProfile adfs_2 -CertKeyName ca_cert1
<!--NeedCopy-->
```

Authentification basée sur le certificat client sur le serveur ADFS

À partir de Windows Server 2016, Microsoft a introduit une nouvelle façon d'authentifier les utilisateurs lorsque ADFS est accessible via des serveurs proxy. Maintenant, les utilisateurs finaux peuvent se connecter avec leurs certificats, évitant ainsi l'utilisation de mot de passe.

Les utilisateurs finaux accèdent souvent à ADFS via un proxy, surtout lorsqu'ils ne sont pas dans les locaux. Par conséquent, les serveurs proxy ADFS sont requis pour prendre en charge l'authentification de certificat client via le protocole ADFSPIP.

Lorsque ADFS est équilibré en charge à l'aide d'une appliance Citrix ADC, pour prendre en charge l'authentification basée sur le certificat sur le serveur ADFS, les utilisateurs doivent également se connecter à l'appliance Citrix ADC à l'aide du certificat. Cela permet à Citrix ADC de transmettre un certificat utilisateur à ADFS pour fournir l'authentification SSO au serveur ADFS.

Le diagramme suivant illustre le flux d'authentification du certificat client.



Configurer l'authentification SSO pour le serveur ADFS à l'aide d'un certificat client

Pour configurer l'authentification unique pour le serveur ADFS à l'aide du certificat client, vous devez d'abord configurer l'authentification de certificat client sur l'appliance Citrix ADC. Vous devez ensuite lier la stratégie d'authentification de certificat à l'authentification, à l'autorisation et à l'audit du serveur virtuel.

À l'invite de commandes, tapez ;

```
add authentication certAction <action name>

add authentication Policy <policy name> -rule <expression> -action <
    action name>

add authentication policylable <label Name>

bind authentication policylabel <label Name> -policyName <name of the
    policy> -priority<integer>

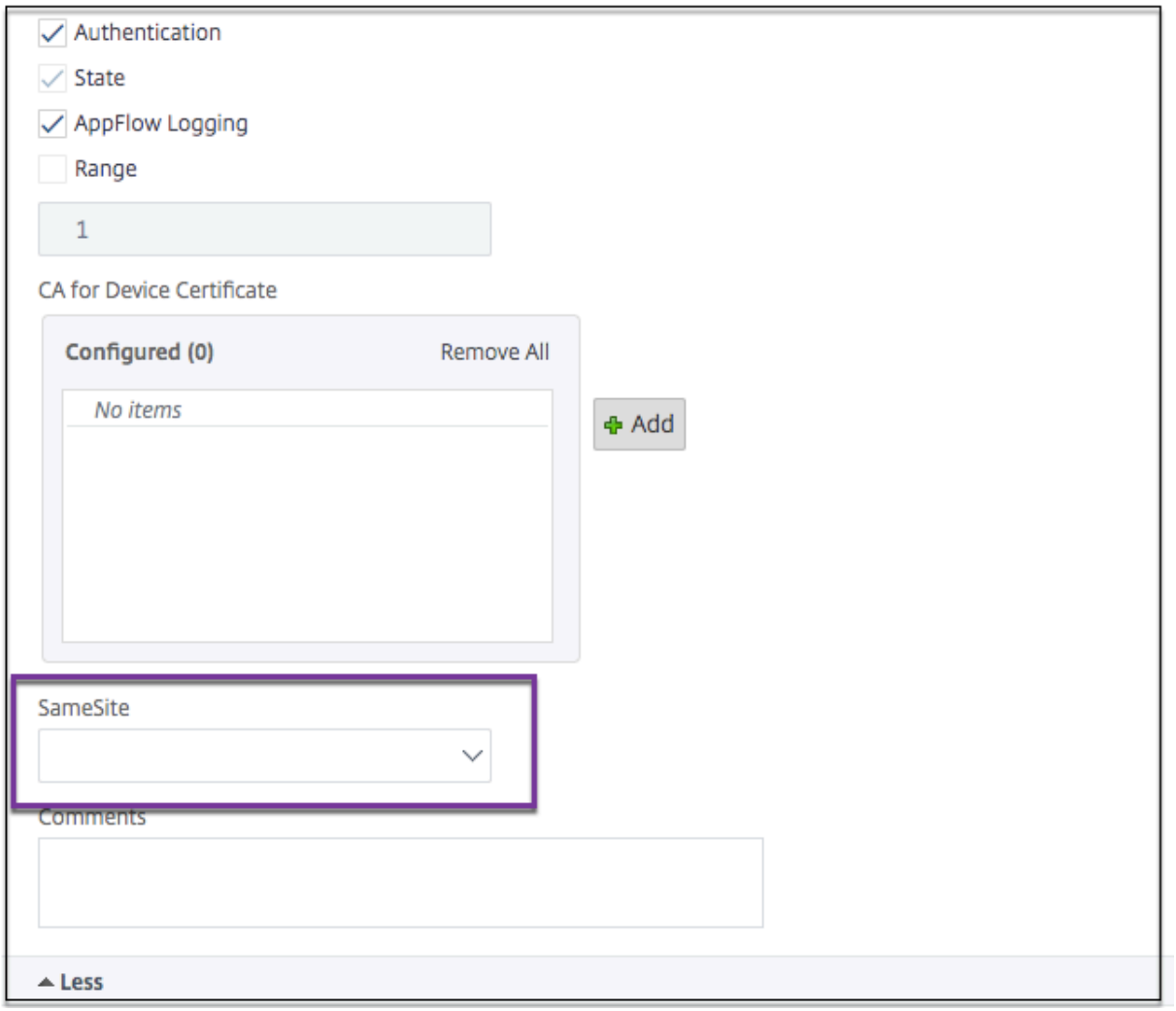
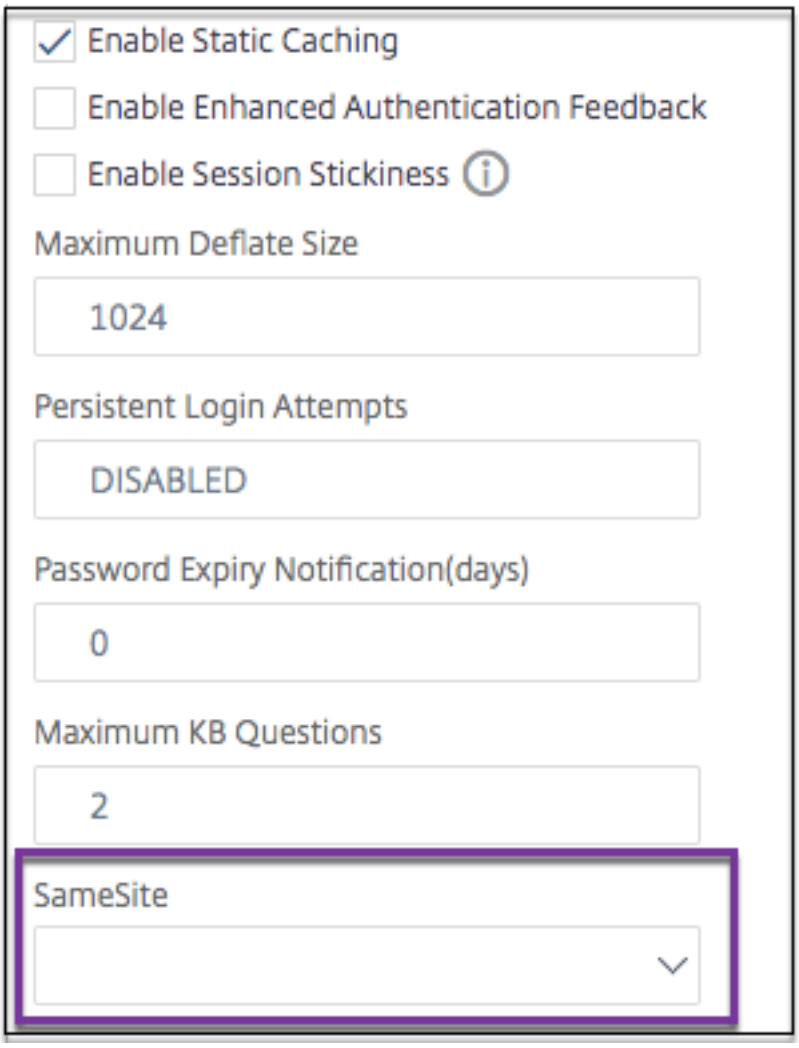
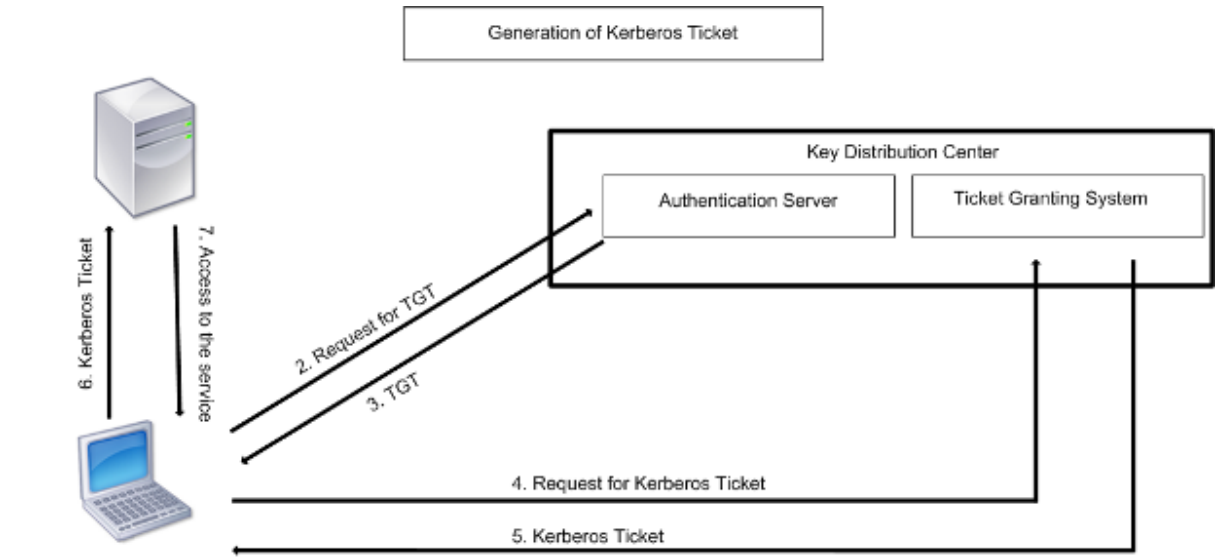
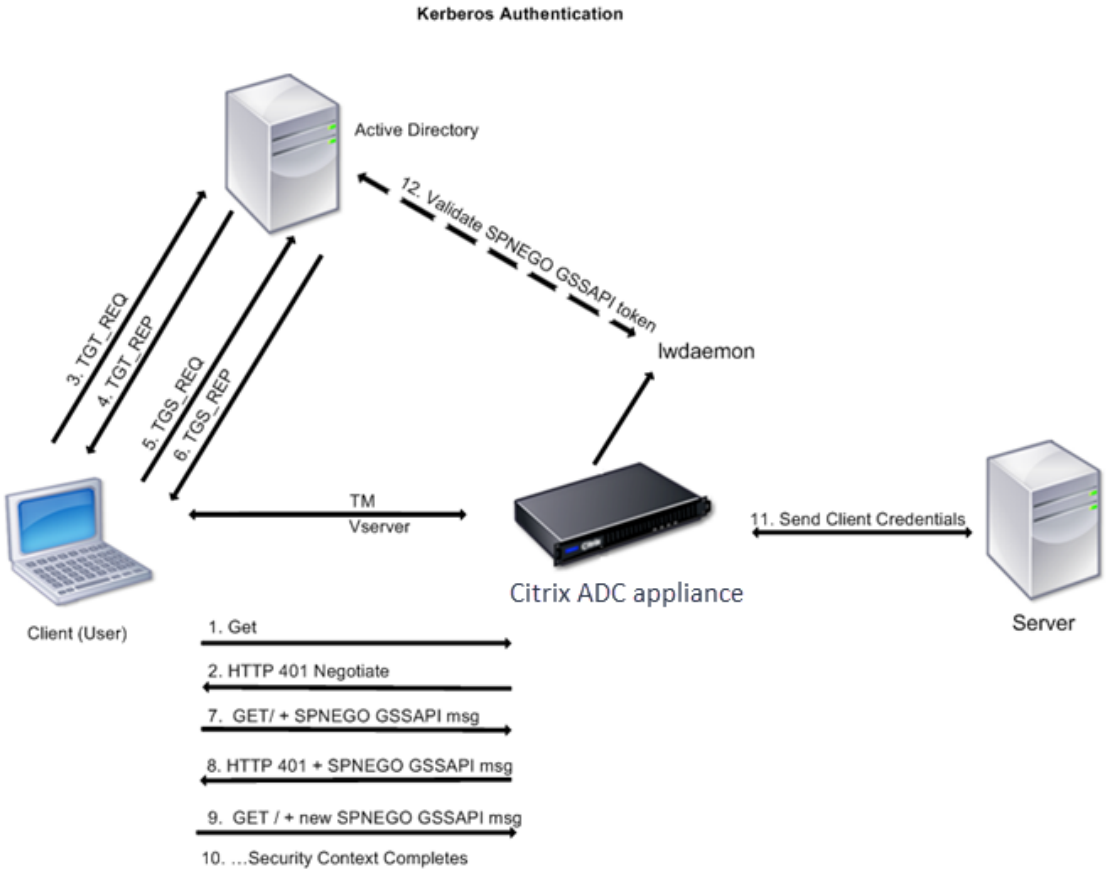
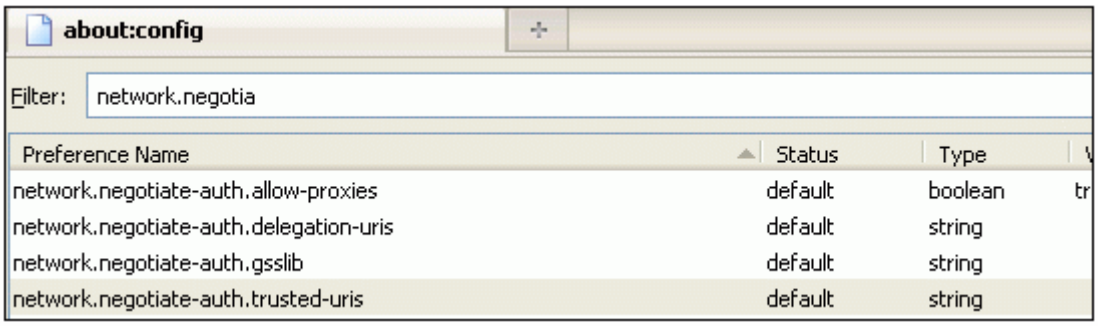
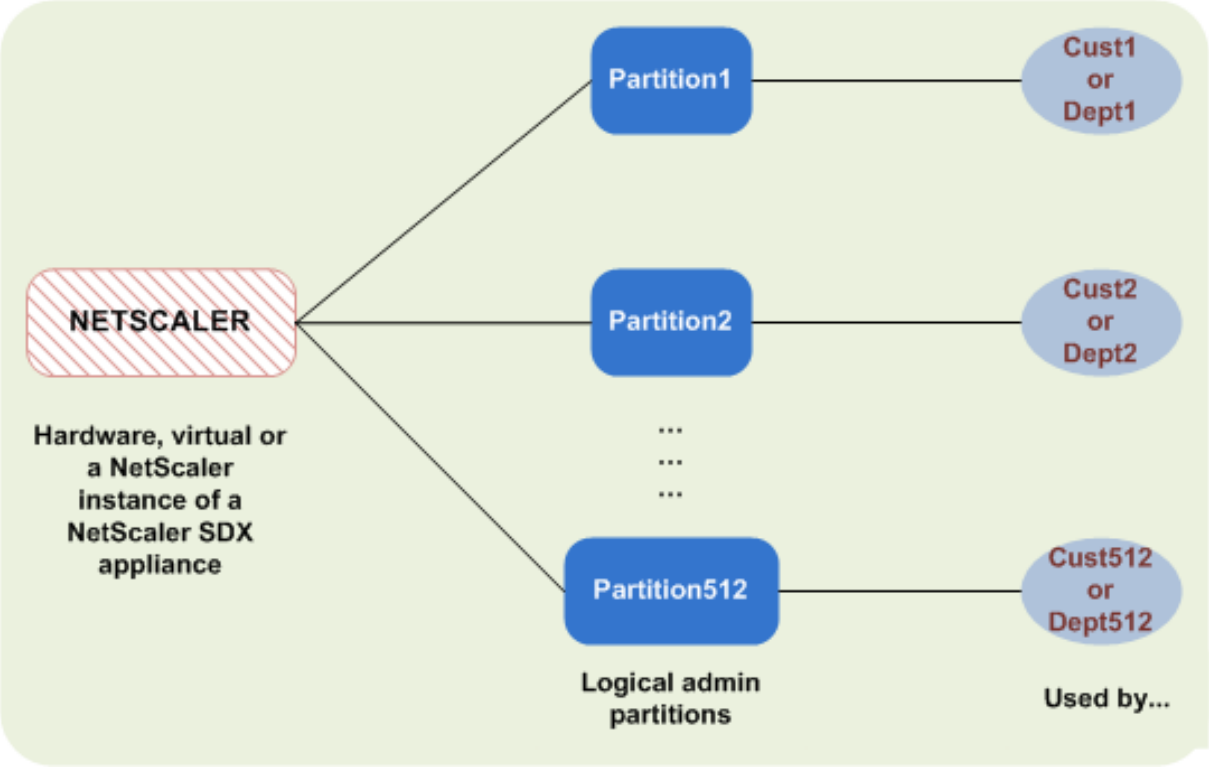
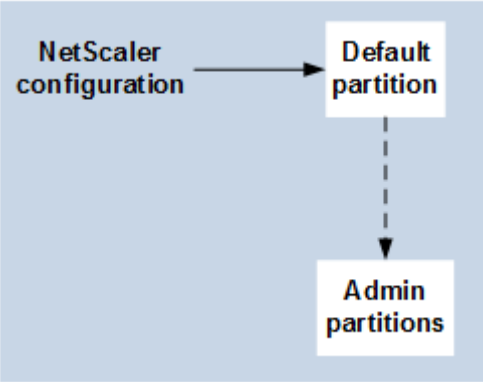
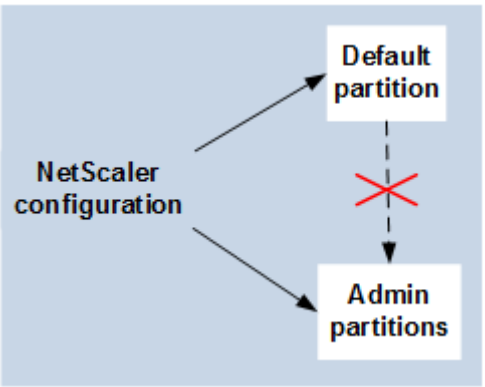
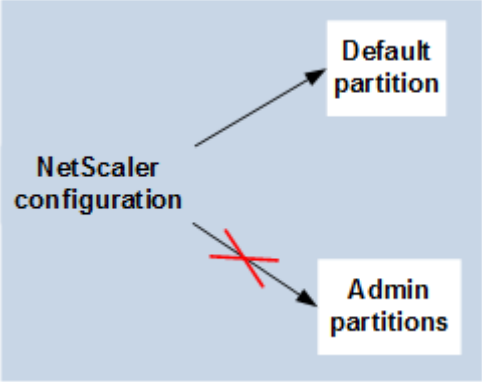
<!--NeedCopy-->
```


Exemple :

```
add authentication certAction adfsproxy-cert

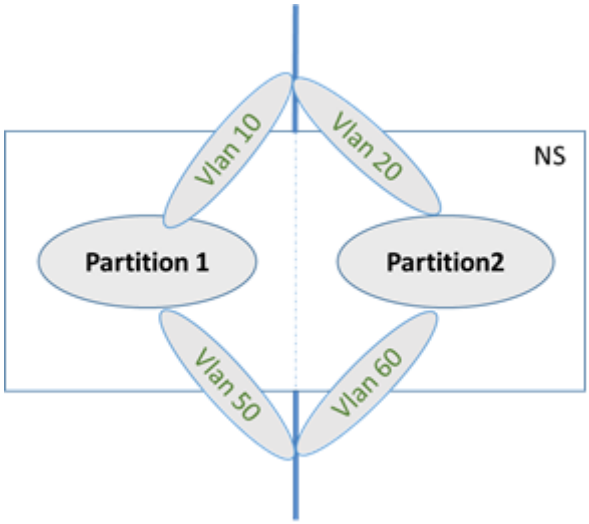
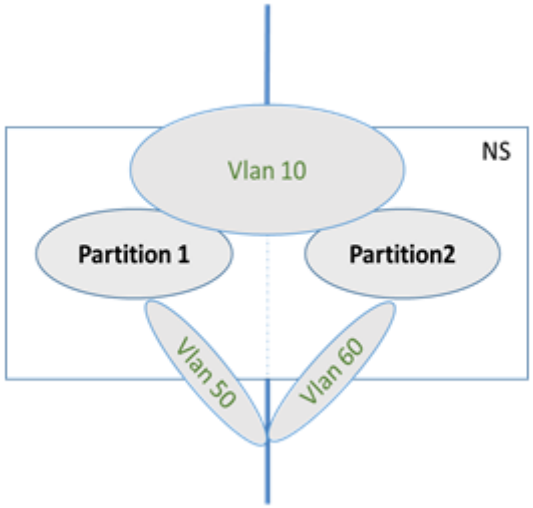
add authentication Policy cert1 -rule TRUE -action adfsproxy-cert

add authentication policylable certfactor

bind authentication policylabel certfactor  - policyName cert1  -
    priority 100

<!--NeedCopy-->
```

Pour plus d'informations sur la configuration du certificat client sur l'appliance Citrix ADC, voir Configurer l'authentification des certificats clients à l'aide de stratégies avancées.

Utiliser une passerelle Citrix Gateway locale en tant que fournisseur d'identité pour Citrix Cloud

September 8, 2021

Citrix Cloud prend en charge l'utilisation de Citrix Gateway local en tant que fournisseur d'identité pour authentifier les abonnés qui se connectent à leurs espaces de travail.

En utilisant l'authentification Citrix Gateway, vous pouvez :

- Continuer à authentifier les utilisateurs via votre Citrix Gateway existant afin qu'ils puissent accéder aux ressources de votre déploiement local d'applications et de bureaux virtuels via Citrix Workspace.
- Utilisez les fonctions d'authentification, d'autorisation et d'audit Citrix Gateway avec Citrix Workspace.
- Utilisez des fonctions telles que l'authentification unique, les cartes à puce, les jetons sécurisés, les stratégies d'accès conditionnel, la fédération et bien d'autres, tout en fournissant à vos utilisateurs l'accès aux ressources dont ils ont besoin via Citrix Workspace.

L'authentification Citrix Gateway est prise en charge pour une utilisation avec les versions de produit suivantes :

- Citrix Gateway 13.0 41.20 Édition Advanced ou ultérieure
- Citrix Gateway 12.1 54.13 Édition Advanced ou ultérieure

Conditions préalables

- Cloud Connectors - Vous avez besoin d'au moins deux serveurs sur lesquels installer le logiciel Citrix Cloud Connector.
- Active Directory - Effectuez les vérifications nécessaires.
- Configuration requise pour Citrix Gateway
  - Utilisez des stratégies avancées sur la passerelle locale en raison de la dépréciation des stratégies classiques.
  - Lors de la configuration de la passerelle pour authentifier les abonnés à Citrix Workspace, la passerelle agit en tant que fournisseur OpenID Connect. Les messages entre Citrix Cloud et Gateway sont conformes au protocole OIDC, qui inclut la signature numérique de jetons. Par conséquent, vous devez configurer un certificat pour signer ces jetons.
  - Synchronisation de l'horloge - La passerelle doit être synchronisée à l'heure NTP.

Pour plus de détails, consultez la section Conditions préalables.

Créer une stratégie d'IdP OAuth sur le site Citrix Gateway

> **Important :**
>
> Vous devez avoir généré l'ID client, le secret et l'URL de redirection dans **Citrix Cloud > Gestion des identités et des accès > Authentification** . Pour plus d'informations, voir Connecter une Citrix Gateway locale à Citrix Cloud.

La création d'une stratégie d'authentification OAuth IdP implique les tâches suivantes :

1. Créez un profil IdP OAuth.
2. Ajoutez une stratégie OAuth IdP.
3. Liez la stratégie IdP OAuth à un serveur virtuel d'authentification.
4. Liez le certificat globalement.

Création d'un profil IdP OAuth à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
add authentication OAuthIDPProfile <name> [-clientID <string>][-
    clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <
    string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]

add authentication OAuthIdPPolicy <name> -rule <expression> [-action <
    string> [-undefAction <string>] [-comment <string>][-logAction <
    string>]
```



```
4
5 add authentication ldapAction <name> -serverIP <IP> -ldapBase "dc=aaa,
     dc=local"
6
7 ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -
     ldapLoginName sAMAccountName
8
9 add authentication policy <name> -rule <expression> -action <string>
10
11 bind authentication vserver auth_vs -policy <ldap_policy_name> -
     priority <integer> -gotoPriorityExpression NEXT
12
13 bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -
     priority <integer> -gotoPriorityExpression END
14
15 bind vpn global  - certkey <>
16 <!--NeedCopy-->
```

Création d'un profil IdP OAuth à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA — Trafic des applications > Stratégies > Authentification > Stratégies avancées > OAuth IDP**.

   ! [Oauth-IDP-navigation] (/en-us/citrix-adc/media/oauth-navigation-to-idp.png)

2. Dans la page **IdP OAuth**, sélectionnez l'onglet **Profils** et cliquez sur **Ajouter**.
3. Configurez le profil IdP OAuth.

   > **Remarque :**
   >
   > - Copiez et collez les valeurs d'ID client, de secret et d'URL de redirection depuis **Citrix Cloud > Gestion des identités et des accès > Authentification** pour établir la connexion à Citrix Cloud.
   > - Saisissez correctement l'URL de la passerelle dans l'exemple de **nom de l'émetteur** : https://GatewayFQDN.com
   > - Copiez et collez également l'ID client dans le champ **Audience** .
   > - **Envoyer le mot de passe** : activez cette option pour la prise en charge de l'authentification unique. Par défaut, cette option est désactivée.

4. Sur l'écran **Create Authentication OAuth IDP Profile**, définissez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   - **Nom** : nom du profil d'authentification. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait

d'union (-), point (.) livre (#), espace (), à (@), égal à (=), deux-points (:) et caractères de soulignement. Impossible de modifier une fois le profil créé.

- **ID client** : chaîne unique qui identifie le SP. Le serveur d'autorisation déduire la configuration du client à l'aide de cet ID. Longueur maximale : 127.
- **Client Secret** — Chaîne secrète établie par l'utilisateur et le serveur d'autorisation. Longueur maximale : 239.
- **URL de redirection** : point de terminaison sur SP sur lequel le code/jeton doit être publié.
- **Nom de l'émetteur** : identité du serveur dont les jetons doivent être acceptés. Longueur maximale : 127. Exemple : https://GatewayFQDN.com
- **Audience** : destinataire cible du jeton envoyé par IdP. Cela peut être vérifié par le destinataire.
- **Temps d'inclinaison** : cette option spécifie l'inclinaison d'horloge autorisée en minutes que Citrix ADC autorise sur un jeton entrant. Par exemple, si SkewTime est de 10, le jeton sera valide de (temps actuel - 10) min à (temps actuel + 10) min, soit 20 minutes en tout. Valeur par défaut : 5.
- **Groupe d'authentification par défaut** : groupe ajouté à la liste des groupes internes de session lorsque ce profil est choisi par IdP qui peut être utilisé dans nFactor Flow. Il peut être utilisé dans l'expression (AAA.USER.IS_MEMBER_OF (« xxx ») pour les stratégies d'authentification afin d'identifier le flux NFactor lié à la partie de confiance. Longueur maximale : 63

Un groupe est ajouté à la session pour ce profil afin de simplifier l'évaluation des stratégies et d'aider à personnaliser les stratégies. Il s'agit du groupe par défaut choisi lorsque l'authentification réussit en plus des groupes extraits. Longueur maximale : 63.

! [Oauth-IDP-profile-parameters] (/en-us/citrix-adc/media/oauth-idp-profile.png)

5. Cliquez sur **Stratégies** et cliquez sur **Ajouter.**
6. Sur l'écran **Create Authentication OAuth IDP Policy**, définissez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.
   - **Nom** : nom de la stratégie d'authentification.
   - **Action** : nom du profil créé précédemment.
   - **Action de journal** : nom de l'action de journal des messages à utiliser lorsqu'une demande correspond à cette stratégie. Ce n'est pas obligatoire.
   - Action à**résultat non défini — Action** à réaliser si le résultat de l'évaluation des politiques n'est pas défini (UNDEF). Ce champ n'est pas obligatoire.
   - **Expression : expression** syntaxique par défaut utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, vrai.

- **Commentaires** — Tout commentaire concernant la politique.

! [Oauth-IDP-policy] (/en-us/citrix-adc/media/oauth-idp-policy.png)

> **Remarque :**
>
> Lorsque **SendPassword** est défini sur ON (OFF par défaut), les informations d'identification de l'utilisateur sont chiffrées et transmises à Citrix Cloud via un canal sécurisé. La transmission des informations d'identification des utilisateurs via un canal sécurisé vous permet d'activer l'authentification unique sur Citrix Virtual Apps and Desktops lors du lancement.

Liaison de la stratégie OAuthIDP et de la stratégie LDAP au serveur virtuel d'authentification

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Actions > LDAP**.
2. Sur l'écran **Actions LDAP**, cliquez sur **Ajouter**.
3. Sur l'écran **Créer un serveur LDAP d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer**.
   - **Nom :** nom de l'action LDAP
   - **ServerName/ServerIP —** Indiquez le nom de domaine complet ou l'adresse IP du serveur LDAP
   - Choisissez les valeurs appropriées **pour le type de sécurité, le port, le type de serveur, le délai d'expiration**
   - Assurez-vous que **l'authentification** est cochée
   - **DN de base —** Base à partir de laquelle lancer la recherche LDAP. Par exemple, `dc=aaa`, `dc=local`.
   - **DN de liaison administrateur :** nom d'utilisateur de la liaison au serveur LDAP. Par exemple, admin@aaa.local.
   - **Mot de passe administrateur/Confirmer le mot de passe : mot de passe pour lier LDAP**
   - Cliquez sur **Tester la connexion** pour tester vos paramètres.
   - **Attribut de nom d'ouverture de session du serveur :** choisissez **« SamAccountName »**
   - Les autres champs ne sont pas obligatoires et peuvent donc être configurés au besoin.
4. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Stratégie.**
5. Sur l'écran **Stratégies d'authentification**, cliquez sur **Ajouter**.
6. Sur la page **Créer une stratégie d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer.**
   - **Nom :** nom de la stratégie d'authentification LDAP.
   - **Type d'action :** choisissez **LDAP.**

- **Action :** choisissez l'action LDAP.
- **Expression : expression** syntaxique par défaut utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, c'est vrai**.

Prise en charge des déploiements GSLB actif-actif sur Citrix Gateway

Citrix Gateway configuré en tant que fournisseur d'identité (IdP) à l'aide du protocole OIDC peut prendre en charge les déploiements GSLB actif-actif. Le déploiement GSLB actif-actif sur Citrix Gateway IdP permet d'équilibrer la charge d'une demande de connexion utilisateur entrante sur plusieurs emplacements géographiques.

> **Important**
>
> Citrix vous recommande de lier des certificats d'autorité de certification au service SSL et d'activer la validation des certificats sur le service SSL pour une sécurité accrue.

Pour plus d'informations sur la configuration de la configuration de GSLB, voir Exemple de configuration et de configuration GSLB.

Prise en charge de la configuration de l'attribut de cookie SameSite

August 20, 2021

L'attribut SameSite indique au navigateur si le cookie peut être utilisé pour le contexte inter-site ou uniquement pour le contexte de même site. En outre, si une application a l'intention d'être accédée dans un contexte intersite, elle ne peut le faire que via une connexion HTTPS. Pour plus de détails, voir RFC6265.

Jusqu'en février 2020, l'attribut SameSite n'était pas explicitement défini dans Citrix ADC. Le navigateur a pris la valeur par défaut (None). La non-définition de l'attribut SameSite n'a pas eu d'impact sur les déploiements Citrix Gateway et Citrix ADC AAA.

Avec la mise à niveau de certains navigateurs, tels que Google Chrome 80, il y a un changement dans le comportement inter-domaine par défaut des cookies. L'attribut SameSite peut être défini sur l'une des valeurs suivantes. La valeur par défaut de Google Chrome est définie sur Lax. Pour certaines versions d'autres navigateurs, la valeur par défaut de l'attribut SameSite peut toujours être définie sur Aucun.

- **Aucun** : indique que le navigateur doit utiliser cookie dans un contexte intersite uniquement sur des connexions sécurisées.
- **Lax** : Indique le navigateur à utiliser des cookies pour les requêtes sur le contexte du même site. Dans un contexte intersite, seules les méthodes HTTP sûres comme la requête GET peuvent utiliser le cookie.

- **Strict** : Utilisez le cookie uniquement dans le même contexte de site.

S'il n'y a pas d'attribut SameSite dans le cookie, Google Chrome assume la fonctionnalité de SameSite = Lax.
Par conséquent, pour les déploiements dans un iframe avec contexte intersite nécessitant l'insertion de cookies par le navigateur, Google Chrome ne partage pas les cookies intersites. Par conséquent, l'iframe dans le site Web peut ne pas se charger.

Configurer l'attribut cookie SameSite

Un nouvel attribut de cookie nommé SameSite est ajouté aux serveurs virtuels VPN et Citrix ADC AAA. Cet attribut peut être défini au niveau global et au niveau du serveur virtuel.

Pour configurer l'attribut SameSite, vous devez effectuer les opérations suivantes :

1. Définir l'attribut SameSite pour le serveur virtuel
2. Lier les cookies au jeu de patchs (si le navigateur supprime les cookies intersites)

Définition de l'attribut SameSite à l'aide de l'interface de ligne de commande

Pour définir l'attribut Samesite au niveau du serveur virtuel, utilisez les commandes suivantes.

```
set vpn vserver VP1 -SameSite [STRICT | LAX | None]
set authentication vserver AV1 -SameSite [STRICT | LAX | None]
<!--NeedCopy-->
```

Pour définir l'attribut Samesite au niveau global, utilisez les commandes suivantes.

```
set aaa parameter -SameSite [STRICT | LAX | None]
set vpn parameter -SameSite [STRICT | LAX | None]
<!--NeedCopy-->
```

Remarque : le paramètre de niveau serveur virtuel prend la préférence sur le paramètre de niveau global. Citrix recommande de définir l'attribut de cookie Samesite au niveau du serveur virtuel.

Liaison des cookies au patset à l'aide de l'interface de ligne de commande

Si le navigateur supprime les cookies intersites, vous pouvez lier cette chaîne de cookies au patset NS_Cookies_Samesite existant afin que l'attribut SameSite soit ajouté au cookie.

Exemple :

```
bind patset ns_cookies_SameSite "NSC_TASS"
bind patset ns_cookies_SameSite "NSC_TMAS"
<!--NeedCopy-->
```


Définition de l'attribut SameSite à l'aide de l'interface graphique

Pour définir l'attribut SameSite au niveau du serveur virtuel :

1. Accédez à **Sécurité > AAA — Trafic des applications > Serveurs virtuels.**
2. Sélectionnez un serveur virtuel et cliquez sur **Modifier**.
3. Cliquez sur l'icône Modifier dans la section **Paramètres de base**et cliquez sur **Plus**.
4. Dans **SameSite**, sélectionnez l'option selon les besoins.



Pour définir l'attribut SameSite au niveau global :

1. Accédez à **Sécurité > AAA — Trafic des applications > Modifier les paramètres d'authentification.**

2. Dans la page **Configurer le paramètre AAA**, cliquez sur la liste **Samesite** et sélectionnez l'option selon vos besoins.



Configuration d'authentification, d'autorisation et d'audit pour les protocoles couramment utilisés

January 21, 2021

La configuration de l'appliance Citrix ADC pour l'authentification, l'autorisation et l'audit nécessite une configuration spécifique sur l'appliance Citrix ADC et les navigateurs des clients. La configuration varie selon le protocole utilisé pour l'authentification, l'autorisation et l'audit.

Pour plus d'informations sur la configuration de l'appliance Citrix ADC pour l'authentification Kerberos, reportez-vous à la section Gestion de l'authentification, de l'autorisation et de l'audit avec Kerberos/NTLM.

Gestion de l'authentification, de l'autorisation et de l'audit avec Kerberos/NTLM

January 21, 2021

Kerberos, un protocole d'authentification de réseau informatique, fournit une communication sécurisée sur Internet. Conçu principalement pour les applications client-serveur, il fournit une authentification mutuelle par laquelle le client et le serveur peuvent chacun garantir l'authenticité de l'autre. Kerberos utilise un tiers de confiance, appelé Key Distribution Center (KDC). Un KDC se compose d'un serveur d'authentification (AS), qui authentifie un utilisateur, et d'un serveur d'octroi de tickets (TGS).

Chaque entité du réseau (client ou serveur) possède une clé secrète qui n'est connue que de elle-même et du KDC. La connaissance de cette clé implique l'authenticité de l'entité. Pour la communication entre deux entités du réseau, le KDC génère une clé de session, appelée ticket Kerberos ou ticket de service. Le client demande au AS des informations d'identification pour un serveur spécifique. Le client reçoit alors un ticket, appelé Ticket d'octroi de tickets (TGT). Le client communique ensuite avec le TGS, en utilisant le TGT qu'il a reçu de l'AS pour prouver son identité, et demande un service. Si le client est admissible au service, le TGS émet un ticket Kerberos au client. Le client contacte ensuite le serveur hébergeant le service (appelé le serveur de service), en utilisant le ticket Kerberos pour prouver qu'il est autorisé à recevoir le service. Le ticket Kerberos a une durée de vie configurable. Le client s'authentifie avec l'AS une seule fois. S'il contacte le serveur physique plusieurs fois, il réutilise le ticket AS.

La figure suivante montre le fonctionnement de base du protocole Kerberos.

Figure 1. **Fonctionnement de Kerberos**



L'authentification Kerberos présente les avantages suivants :

- Authentification plus rapide. Lorsqu'un serveur physique obtient un ticket Kerberos d'un client, le serveur dispose de suffisamment d'informations pour authentifier le client directement. Il n'a pas besoin de contacter un Controller de domaine pour l'authentification du client, et donc le processus d'authentification est plus rapide.
- Authentification mutuelle. Lorsque le KDC émet un ticket Kerberos à un client et que le client utilise le ticket pour accéder à un service, seuls les serveurs authentifiés peuvent déchiffrer le ticket Kerberos. Si le serveur virtuel de l'appliance Citrix ADC est en mesure de déchiffrer le ticket Kerberos, vous pouvez conclure que le serveur virtuel et le client sont tous deux authentifiés. Ainsi, l'authentification du serveur se produit avec l'authentification du client.
- Connexion unique entre Windows et d'autres systèmes d'exploitation prenant en charge Kerberos.

L'authentification Kerberos peut présenter les inconvénients suivants :

- Kerberos a des délais stricts ; les horloges des hôtes concernés doivent être synchronisées avec l'horloge du serveur Kerberos pour s'assurer que l'authentification n'échoue pas. Vous pouvez atténuer cet inconvénient en utilisant les démons Network Time Protocol pour garder les horloges de l'hôte synchronisées. Les tickets Kerberos ont une période de disponibilité, que vous pouvez configurer.
- Kerberos a besoin que le serveur central soit disponible en continu. Lorsque le serveur Kerberos est en panne, personne ne peut ouvrir une session. Vous pouvez atténuer ce risque en utilisant plusieurs serveurs Kerberos et des mécanismes d'authentification de secours.
- Comme toute l'authentification est contrôlée par un KDC centralisé, tout compromis dans cette infrastructure, tel que le mot de passe de l'utilisateur pour un poste de travail local volé, peut permettre à un attaquant de se faire passer pour n'importe quel utilisateur. Vous pouvez at-

ténuer ce risque dans une certaine mesure en utilisant uniquement un ordinateur de bureau ou un ordinateur portable en qui vous avez confiance, ou en appliquant la préauthentification au moyen d'un jeton matériel.

Pour utiliser l'authentification Kerberos, vous devez la configurer sur l'appliance Citrix ADC et sur chaque client.

Optimisation de l'authentification Kerberos lors de l'authentification, de l'autorisation et de l'audit

L'appliance Citrix ADC optimise et améliore désormais les performances du système lors de l'authentification Kerberos. Le démon d'authentification, d'autorisation et d'audit se souvient de la demande Kerberos en attente pour le même utilisateur afin d'éviter le chargement sur Key Distribution Center (KDC), ce qui évitera les demandes en double.

Comment Citrix ADC implémente Kerberos pour l'authentification client

January 21, 2021

> **Important**
>
> L'authentification Kerberos/NTLM est prise en charge uniquement dans la version NetScaler 9.3 nCore ou ultérieure, et elle peut être utilisée uniquement pour l'authentification, l'autorisation et l'audit des serveurs virtuels de gestion du trafic.

Citrix ADC gère les composants impliqués dans l'authentification Kerberos de la manière suivante :

Centre de distribution de clés (KDC)

Dans Windows 2000 Server ou versions ultérieures, le contrôleur de domaine et le contrôleur de domaine KDC font partie du serveur Windows. Si Windows Server est opérationnel et en cours d'exécution, il indique que le contrôleur de domaine et le contrôleur de domaine KDC sont configurés. Le KDC est également le serveur Active Directory.

> **Remarque**
>
> Toutes les interactions Kerberos sont validées avec le contrôleur de domaine Kerberos Windows.

Service d'authentification et négociation de protocole

Une appliance Citrix ADC prend en charge l'authentification Kerberos sur les serveurs virtuels d'authentification, d'autorisation et d'audit de gestion du trafic. Si l'authentification Kerberos échoue, Citrix ADC utilise l'authentification NTLM.

Par défaut, Windows 2000 Server et les versions ultérieures de Windows Server utilisent Kerberos pour l'authentification, l'autorisation et l'audit. Si vous créez une stratégie d'authentification avec NEGOTIATE comme type d'authentification, Citrix ADC tente d'utiliser le protocole Kerberos pour l'authentification, l'autorisation et l'audit et si le navigateur du client ne parvient pas à recevoir un ticket Kerberos, l'ADC Citrix utilise l'authentification NTLM. Ce processus est appelé négociation.

Le client peut ne pas recevoir de ticket Kerberos dans l'un des cas suivants :

- Kerberos n'est pas pris en charge sur le client.
- Kerberos n'est pas activé sur le client.
- Le client se trouve dans un domaine autre que celui du KDC.
- Le répertoire d'accès sur le KDC n'est pas accessible au client.

Pour l'authentification Kerberos/NTLM, Citrix ADC n'utilise pas les données présentes localement sur l'appliance Citrix ADC.

Autorisation

Le serveur virtuel de gestion du trafic peut être un serveur virtuel d'équilibrage de charge ou un serveur virtuel de commutation de contenu.

Audit

L'appliance Citrix ADC prend en charge l'audit de l'authentification Kerberos avec l'enregistrement d'audit suivant :

- Trail d'audit complet de l'activité de l'utilisateur final de gestion du trafic
- SYSLOG et enregistrement TCP hautes performances
- Trail d'audit complet des administrateurs système
- Tous les événements système
- Format de journal scriptable

Environnement pris en charge

L'authentification Kerberos n'a besoin d'aucun environnement spécifique sur Citrix ADC. Le client (navigateur) doit fournir la prise en charge de l'authentification Kerberos.

Haute disponibilité

Dans une configuration haute disponibilité, seul Citrix ADC actif rejoint le domaine. En cas de basculement sur incident, le démon Citrix ADC lwagent joint l'appliance Citrix ADC secondaire au domaine. Aucune configuration spécifique n'est requise pour cette fonctionnalité.

Processus d'authentification Kerberos

La figure suivante illustre un processus typique d'authentification Kerberos dans l'environnement Citrix ADC.

Figure 1. Processus d'authentification Kerberos sur Citrix ADC



L'authentification Kerberos se produit dans les étapes suivantes :

Le client s'authentifie auprès du KDC

1. L'appliance Citrix ADC reçoit une demande d'un client.
2. Le serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu) sur l'appliance Citrix ADC envoie un défi au client.
3. Pour répondre au défi, le client obtient un ticket Kerberos.

- Le client envoie au serveur d'authentification du KDC une demande de ticket d'octroi de tickets (TGT) et reçoit le TGT. (Voir 3, 4 dans la figure, Processus d'authentification Kerberos.)
- Le client envoie le TGT au serveur d'octroi de tickets du KDC et reçoit un ticket Kerberos. (Voir 5, 6 dans la figure, Processus d'authentification Kerberos.)

> **Remarque**
>
> Le processus d'authentification ci-dessus n'est pas nécessaire si le client dispose déjà d'un ticket Kerberos dont la durée de vie n'a pas expiré. En outre, les clients tels que les services Web, .NET ou J2EE, qui prennent en charge SPNEGO, obtiennent un ticket Kerberos pour le serveur cible, créent un jeton SPNEGO et insèrent le jeton dans l'en-tête HTTP lorsqu'ils envoient une requête HTTP. Ils ne passent pas par le processus d'authentification du client.

Le client demande un service.

1. Le client envoie le ticket Kerberos contenant le jeton SPNEGO et la requête HTTP au serveur virtuel de gestion du trafic sur le Citrix ADC. Le jeton SPNEGO a les données GSSAPI nécessaires.
2. L'appliance Citrix ADC établit un contexte de sécurité entre le client et le Citrix ADC. Si Citrix ADC ne peut pas accepter les données fournies dans le ticket Kerberos, le client est invité à obtenir un ticket différent. Ce cycle se répète jusqu'à ce que les données GSSAPI soient acceptables et que le contexte de sécurité soit établi. Le serveur virtuel de gestion du trafic sur Citrix ADC agit comme un proxy HTTP entre le client et le serveur physique.

L'**appliance Citrix ADC termine l'authentification.**

1. Une fois le contexte de sécurité terminé, le serveur virtuel de gestion du trafic valide le jeton SPNEGO.
2. À partir du jeton SPNEGO valide, le serveur virtuel extrait l'ID utilisateur et les informations d'identification GSS et les transmet au démon d'authentification.
3. Une authentification réussie termine l'authentification Kerberos.

Configuration de l'authentification kerberos sur l'appliance Citrix ADC

August 20, 2021

Cette rubrique fournit les étapes détaillées pour configurer l'authentification Kerberos sur l'appliance Citrix ADC à l'aide de l'interface de ligne de commande et de l'interface graphique.

Configuration de l'authentification Kerberos sur l'interface de ligne de commande

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit pour garantir l'authentification du trafic sur l'appliance.

ns-cli-prompt> **activer la fonctionnalité ns** AAA

2. Ajoutez le fichier keytab à l'appliance Citrix ADC. Un fichier keytab est nécessaire pour déchiffrer le secret reçu du client lors de l'authentification Kerberos. Un seul fichier keytab contient des détails d'authentification pour tous les services liés au serveur virtuel de gestion du trafic sur l'appliance Citrix ADC.

   Générez d'abord le fichier keytab sur le serveur Active Directory, puis transférez-le à l'appliance Citrix ADC.

   - Ouvrez une session sur le serveur Active Directory et ajoutez un utilisateur pour l'authentification Kerberos. Par exemple, pour ajouter un utilisateur nommé "Kerb-SVC-Account":

     net user Kerb-SVC-Account freebsd!@#456 /add

     > **Remarque**
     >
     > Dans la section **Propriétés de l'utilisateur**, assurez-vous que l'option « Modifier le mot de passe lors de la prochaine ouverture de session » n'est pas sélectionnée et que l'option « Mot de passe n'expire pas » est sélectionnée.

   - Mappez le service HTTP à l'utilisateur ci-dessus et exportez le fichier keytab. Par exemple, exécutez la commande suivante sur le serveur Active Directory :

     ktpass /out keytabfile /princ HTTP/owa.newacp.com@NEWACP.COM /pass freebsd!@#456 /mapuser newacp\dummy /ptype KRB5_NT_PRINCIPAL

     > **Remarque**
     >
     > Vous pouvez mapper plusieurs services si l'authentification est requise pour plusieurs services. Si vous souhaitez mapper d'autres services, répétez la commande ci-dessus pour chaque service. Vous pouvez donner le même nom ou des noms différents pour le fichier de sortie.

   - Transférez le fichier keytab vers l'appliance Citrix ADC à l'aide de la commande unix **ftp** ou de tout autre utilitaire de transfert de fichiers de votre choix.

3. L'appliance Citrix ADC doit obtenir l'adresse IP du Controller de domaine à partir du nom de domaine complet (FQDN). Par conséquent, Citrix recommande de configurer Citrix ADC avec un serveur DNS.

   ns-cli-prompt> **add dns nameserver** <ip-address>

   > **Remarque**
   >
   > Vous pouvez également ajouter des entrées d'hôte statiques ou utiliser tout autre moyen

> pour que l'appliance Citrix ADC puisse résoudre le nom de domaine complet du Controller de domaine en une adresse IP.

4. Configurez l'action d'authentification, puis associez-la à une stratégie d'authentification.
   - Configurez l'action de négociation.

     ns-cli-prompt **ajouter l'authentification Négocier l'action** <name><domain name>- domaine - Utilisateur du domaine <domain user name>- DomainUserPassWD <domain user password>- Groupe d'authentification par défaut <default authentication group>- keytab <string>- chemin NTLM <string>

     Remarque : Pour la configuration de l'utilisateur du domaine et du nom de domaine, accédez au client et utilisez la commande klist comme illustré dans l'exemple suivant :

     Client : nom d'utilisateur @ AAA.LOCAL

     Serveur : http/OnPrem_IDP.AAA.Local @ AAA.LOCAL

     ajout d'authentification Negotiate Action <name>- domaine <AAA.LOCAL>- DomainUser <HTTP/onprem_idp.aaa.local>
   - Configurez la stratégie de négociation et associez l'action de négociation à cette stratégie.

     ns-cli-prompt> **add authentication negotiatePolicy** <name> <rule> <reqAction>
5. Créez un serveur virtuel d'authentification et associez la stratégie de négociation à celui-ci.
   - Créez un serveur virtuel d'authentification.

     ns-cli-prompt> **add authentication vserver** <name> SSL <ipAuthVserver> 443 -authenticationDomain <domainName>
   - Liez la stratégie de négociation au serveur virtuel d'authentification.

     ns-cli-prompt> **bind authentication vserver** <name> -policy <negotiatePolicyName>
6. Associez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu).

   ns-cli-prompt> **set lb vserver** <name> -authn401 ON -authnVsName <string>

   > **Remarque**
   >
   > Des configurations similaires peuvent également être effectuées sur le serveur virtuel de commutation de contenu.
7. Vérifiez les configurations en procédant comme suit :
   - Accédez au serveur virtuel de gestion du trafic à l'aide du nom de domaine complet. Par exemple, Sample
   - Affichez les détails de la session sur l'interface de ligne de commande.

     ns-cli-prompt> **show aaa session**

Configuration de l'authentification Kerberos sur l'interface graphique

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit.

   Accédez à **Système** > **Paramètres**, cliquez sur **Configurer les fonctionnalités de base** et activez la fonctionnalité d'authentification, d'autorisation et d'audit.

2. Ajoutez le fichier keytab comme détaillé à l'étape 2 de la procédure CLI mentionnée ci-dessus.

3. Ajoutez un serveur DNS.

   Accédez à **Gestion du trafic > DNS > Serveurs de noms**et spécifiez l'adresse IP du serveur DNS.

4. Configurez l'action et la stratégie **Négocier** .

   Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Stratégie**, puis créez une stratégie avec **Négocier**comme type d'action. Cliquez sur **ADD** pour créer un nouveau serveur de négociation d'authentification ou sur **Modifier** pour configurer les détails existants.

5. Liez la stratégie de négociation au serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**et associez la stratégie **Négocier**au serveur virtuel d'authentification.

6. Associez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu).

   Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et spécifiez les paramètres d'authentification appropriés.

   > **Remarque**
   >
   > Des configurations similaires peuvent également être effectuées sur le serveur virtuel de commutation de contenu.

7. Vérifiez les configurations décrites à l'étape 7 de la procédure CLI mentionnée ci-dessus.

Configurer l'authentification kerberos sur un client

January 21, 2021

La prise en charge de Kerberos doit être configurée sur le navigateur pour utiliser Kerberos pour l'authentification. Vous pouvez utiliser n'importe quel navigateur compatible Kerberos. Suivez les instructions pour configurer la prise en charge de Kerberos sur Internet Explorer et Mozilla Firefox. Pour les autres navigateurs, consultez la documentation du navigateur.

Pour configurer Internet Explorer pour l'authentification Kerberos

1. Dans le menu **Outils**, sélectionnez **Options Internet** .
2. Sous l'onglet **Sécurité**, cliquez sur **Intranet local**, puis sur **Sites** .
3. Dans la boîte de dialogue **Intranet local**, assurez-vous que l'option Détecter automatiquement le réseau intranet est sélectionnée, puis cliquez sur **Avancé** .
4. Dans la boîte de dialogue **Intranet local**, ajoutez les sites Web des domaines du serveur virtuel de gestion du trafic sur l'appliance Citrix ADC. Les sites spécifiés deviennent des sites intranet locaux.
5. Cliquez sur **Fermer** ou sur **OK** pour fermer les boîtes de dialogue.

Pour configurer Mozilla Firefox pour l'authentification Kerberos

1. Assurez-vous que Kerberos est correctement configuré sur votre ordinateur.
2. Tapez about:config dans la barre d'URL.
3. Dans la zone de texte du filtre, tapez network.negotiate.
4. Remplacez network.negotiate-auth.delegation-uris par le domaine que vous souhaitez ajouter.
5. Changez network.negotiate-auth.trusted-uris par le domaine que vous souhaitez ajouter.

> **Remarque :** Si vous exécutez Windows, vous devez également entrer sspi dans la zone de texte du filtre et changer l'option network.auth.use-sspi sur False.

Décharger l'authentification Kerberos des serveurs physiques

October 5, 2021

L'appliance Citrix ADC peut décharger les tâches d'authentification des serveurs. Au lieu que les serveurs physiques authentifient les demandes des clients, Citrix ADC authentifie toutes les demandes des clients avant de les transmettre à l'un des serveurs physiques qui lui sont liés. L'authentification de l'utilisateur est basée sur des jetons Active Directory.

Il n'y a pas d'authentification entre Citrix ADC et le serveur physique, et le déchargement de l'authentification est transparent pour les utilisateurs finaux. Après l'ouverture de session initiale sur un ordinateur Windows, l'utilisateur final n'a pas besoin de saisir d'informations d'authentification supplémentaires dans une fenêtre contextuelle ou sur une page d'ouverture de session.

Dans la version actuelle de l'appliance Citrix ADC, l'authentification Kerberos n'est disponible que pour les serveurs virtuels d'authentification, d'autorisation et d'audit de gestion du trafic. L'authentification Kerberos n'est pas prise en charge pour le VPN SSL dans l'appliance Citrix Gateway Advanced Edition ou pour la gestion de l'appliance Citrix ADC.

L'authentification Kerberos nécessite une configuration sur l'appliance Citrix ADC et sur les navigateurs clients.

Pour configurer l'authentification Kerberos sur l'appliance Citrix ADC

> **Remarque**
>
> Les mots de passe utilisés dans l'exemple de configuration suivant ne sont que des exemples et non les mots de passe de configuration réels.

1. Créez un compte utilisateur sur Active Directory. Lors de la création d'un compte utilisateur, vérifiez les options suivantes dans la section Propriétés de l'utilisateur :
   - Assurez-vous de ne pas sélectionner l'option Modifier le mot de passe lors de la prochaine connexion.
   - Assurez-vous de sélectionner l'option Le mot de passe n'expire pas.
2. Sur le serveur AD, à l'invite de commandes de l'interface de ligne de commande, tapez :
   - ktpass -princ HTTP/ kerberos.crete.lab.net@crete.lab.net -ptype KRB5_NT_PRINCIPAL -mapuser kerbuser@crete.lab.net -mapop set -pass <password> -out C:\kerbtabfile.txt

   > **Remarque**
   >
   > N'oubliez pas de taper la commande ci-dessus sur une seule ligne. La sortie de la commande ci-dessus est écrite dans le fichier C:\kerbtabfile.txt.
3. Téléchargez le fichier kerbtabfile.txt dans le répertoire /etc de l'appliance Citrix ADC à l'aide d'un client SCP (Secure Copy).
4. Exécutez la commande suivante pour ajouter un serveur DNS à l'appliance Citrix ADC.
   - add dns nameserver 1.2.3.4

   L'appliance Citrix ADC ne peut pas traiter les demandes Kerberos sans le serveur DNS. Assurez-vous d'utiliser le même serveur DNS que celui utilisé dans le domaine Microsoft Windows.
5. Basculez vers l'interface de ligne de commande de Citrix ADC.
6. Exécutez la commande suivante pour créer un serveur d'authentification Kerberos :
   - add authentication negotiateAction KerberosServer -domain "crete.lab.net" -domainUser kerbuser -domainUserPasswd <password> -keytab /var/mykcd.keytab

   > **Remarque**
   >
   > Si keytab n'est pas disponible, vous pouvez spécifier les paramètres suivants : domain, DomainUser et -DomainUserPasswd.
7. Exécutez la commande suivante pour créer une stratégie de négociation :

- `add authentication negotiatePolicy Kerberos-Policy "REQ.IP.DESTIP == 192.168.17.200"KerberosServer<!--NeedCopy-->`

8. Exécutez la commande suivante pour créer un serveur virtuel d'authentification.
   - `add authentication vserver Kerb-Auth SSL 192.168.17.201 443 -AuthenticationDomain crete.lab.net<!--NeedCopy-->`
9. Exécutez la commande suivante pour lier la stratégie Kerberos au serveur virtuel d'authentification :
   - `bind authentication vserver Kerb-Auth -policy Kerberos-Policy -priority 100<!--NeedCopy-->`
10. Exécutez la commande suivante pour lier un certificat SSL au serveur virtuel d'authentification. Vous pouvez utiliser l'un des certificats de test, que vous pouvez installer à partir de l'appliance Citrix ADC GUI. Exécutez la commande suivante pour utiliser l'exemple de certificat ServerTestCert.
    - `bind ssl vserver Kerb-Auth -certkeyName ServerTestCert<!--NeedCopy-->`
11. Créez un serveur virtuel d'équilibrage de charge HTTP avec l'adresse IP 192.168.17.200.

    Assurez-vous de créer un serveur virtuel à partir de l'interface de ligne de commande pour les versions NetScaler 9.3 si elles sont antérieures à 9.3.47.8.
12. Exécutez la commande suivante pour configurer un serveur virtuel d'authentification :
    - `set lb vserver <name>-authn401 ON -authnVsName Kerb-Auth<!--NeedCopy-->`
13. Entrez l' exemple de nom d'hôte dans la barre d'adresse du navigateur Web.

    Le navigateur Web affiche une boîte de dialogue d'authentification car l'authentification Kerberos n'est pas configurée dans le navigateur.

    > **Remarque**
    >
    > L'authentification Kerberos nécessite une configuration spécifique sur le client. Assurez-vous que le client peut résoudre le nom d'hôte, ce qui entraîne la connexion du navigateur Web à un serveur virtuel HTTP.
14. Configurez Kerberos sur le navigateur Web de l'ordinateur client.
    - Pour la configuration sur Internet Explorer, reportez-vous à la section Configuration de l'authentification Internet Explorer pour Kerberos.
    - Pour la configuration sur Mozilla Firefox, reportez-vous à la section Configuration de l'authentification Internet Explorer pour Kerberos.
15. Vérifiez si vous pouvez accéder au serveur physique principal sans authentification.

Pour configurer l'authentification Internet Explorer pour Kerberos

1. Sélectionnez **Options Internet** dans le menu **Outils** .
2. Activez l'onglet **Sécurité** .
3. Sélectionnez **Intranet local dans** la section Sélectionner une zone pour afficher les paramètres de sécurité des modifications.
4. Cliquez sur **Sites**.
5. Cliquez sur **Avancé**.
6. Spécifiez l'URL, Exemple, puis cliquez sur **Ajouter**.
7. Redémarrez **Internet Explorer**.

Pour configurer l'authentification Mozilla Firefox pour Kerberos

1. Entrez about:config dans la barre d'adresse du navigateur.
2. Cliquez sur l'avertissement de non-responsabilité.
3. Tapez **Network.Negotiate-Auth.Trusted-URIS** dans la zone **Filtre** .
4. Double-cliquez sur **Network.Negotiate-Auth.Trusted-URIS.** Un exemple d'écran est présenté ci-dessous.



5. Dans la boîte de dialogue Saisir une valeur de chaîne, spécifiez www.crete.lab.net.
6. Redémarrez Firefox.

Résoudre les problèmes liés à l'authentification et à l'autorisation

October 5, 2021

Localiser les messages d'erreur

Localiser les messages d'erreur générés par le système Citrix ADC nFactor

Résoudre les problèmes d'authentification avec le module aaad.debug

Résoudre les problèmes d'authentification dans Citrix ADC et Citrix Gateway avec le module aaad.debug

Partition Admin

September 8, 2021

Une appliance Citrix ADC peut être partitionnée en entités logiques appelées partitions d'administration. Chaque partition peut être configurée et utilisée comme appliance Citrix ADC distincte. La figure suivante montre les partitions d'un Citrix ADC utilisées par différents clients et services :



Une appliance Citrix ADC partitionnée possède une partition par défaut unique et une ou plusieurs partitions d'administration. Le tableau suivant fournit des informations supplémentaires sur les deux types de partitions :

> **Remarque**
>
> Dans une appliance partitionnée, le mode BridgeBPDU peut être activé uniquement dans la partition par défaut et non dans les partitions administratives.

Disponibilité :

L'appliance Citrix ADC est livrée avec une seule partition, appelée partition par défaut. La partition par défaut est conservée même après le partitionnement de l'appliance Citrix ADC.

Doit être créé explicitement comme décrit dans Configurer les partitions d'administration.

Nombre de partitions :

Un

Une appliance Citrix ADC peut comporter une ou plusieurs partitions d'administration (au maximum 512).

Accès utilisateur et rôles :

Tous les utilisateurs Citrix ADC, qui ne sont pas associés à une stratégie de commande *spécifique à une partition*, peuvent accéder à la partition par défaut et la configurer. Comme toujours, la stratégie de commande associée limite les opérations qu'un utilisateur peut effectuer.

L'accès utilisateur et les rôles sont créés par les superutilisateurs Citrix ADC qui spécifient également les utilisateurs de cette partition. Seuls les superutilisateurs et les utilisateurs associés de la partition peuvent accéder à la partition d'administration et la configurer.

> **Remarque**
>
> Les utilisateurs de partitions ne disposent pas d'un accès shell.

Structure du fichier :

Tous les fichiers d'une partition par défaut sont stockés dans la structure de fichiers Citrix ADC par défaut.

Par exemple, le répertoire */nsconfig* stocke le fichier de configuration Citrix ADC et le répertoire */var/log/* stocke les journaux Citrix ADC.

Tous les fichiers d'une partition d'administration sont stockés dans des chemins d'accès au répertoire portant le nom de la partition d'administration.

Par exemple, le fichier de configuration Citrix ADC (ns.conf) est stocké dans le `/nsconfig/partitions/<partitionName>` répertoire. Les autres fichiers spécifiques à une partition sont stockés dans les `/var/partitions/<partitionName>` répertoires.

Voici d'autres chemins d'accès dans une partition d'administration :

- Fichiers téléchargés : `/var/partitions/<partitionName>/download/`
- Fichiers journaux : `/var/partitions/<partitionName>/log/`

> **Remarque**
>
> Actuellement, la journalisation n'est pas prise en charge au niveau de la partition. Par conséquent, ce répertoire est vide et tous les journaux sont stockés dans le `/var/log/` répertoire.

- Fichiers liés au certificat SSL CRL : `/var/partitions/<partitionName>/netscaler/ssl`

Ressources disponibles :

Toutes les ressources Citrix ADC.

Ressources Citrix ADC explicitement affectées à la partition d'administration.

Accès utilisateur et rôles

Lors de l'authentification et de l'autorisation d'une appliance Citrix ADC partitionnée, un administrateur racine peut affecter un administrateur de partition à une ou plusieurs partitions. L'administrateur de partition peut autoriser les utilisateurs à accéder à cette partition sans affecter d'autres partitions. Les utilisateurs de la partition sont autorisés à accéder uniquement à cette partition à l'aide de l'adresse SNIP. L'administrateur racine et l'administrateur de partition peuvent tous deux configurer l'accès basé sur les rôles (RBA) en autorisant les utilisateurs à accéder à différentes applications.

Les rôles des administrateurs et des utilisateurs peuvent être décrits comme suit :

Administrateur racine. Accède à l'appliance partitionnée via son adresse NSIP et peut accorder aux utilisateurs l'accès à une ou plusieurs partitions. L'administrateur peut également affecter des administrateurs de partition à une ou plusieurs partitions. L'administrateur peut créer un administrateur de partition à partir de la partition par défaut à l'aide d'une adresse NSIP ou passer à une partition, puis créer un utilisateur et attribuer un accès administrateur de partition à l'aide d'une adresse SNIP.

Administrateur de partition. Permet d'accéder à la partition spécifiée via une adresse NSIP attribuée par l'administrateur racine. L'administrateur peut attribuer un accès basé sur les rôles à l'accès utilisateur de partition à cette partition et également configurer l'authentification du serveur externe à l'aide d'une configuration spécifique à la partition.

Utilisateur système. Permet d'accéder aux partitions via l'adresse NSIP. Permet d'accéder aux partitions et aux ressources spécifiées par l'administrateur racine.

Utilisateur de partition. Permet d'accéder à une partition via une adresse SNIP. Le compte utilisateur est créé par l'administrateur de partition et l'utilisateur a accès aux ressources, uniquement au sein de la partition.

Points à retenir

Voici quelques points à retenir lorsque vous fournissez un accès basé sur les rôles dans une partition.

1. Les utilisateurs Citrix ADC qui accèdent à l'interface graphique via l'adresse NSIP utilisent la configuration d'authentification de partition par défaut pour se connecter à l'appliance.
2. Les utilisateurs du système de partition qui accèdent à l'interface graphique via une adresse SNIP de partition utilisent une configuration d'authentification spécifique à la partition pour se connecter à l'appliance.

3. L'utilisateur de partition créé dans une partition ne peut pas se connecter à l'aide de l'adresse NSIP.
4. L'utilisateur Citrix ADC lié à une partition ne peut pas se connecter à l'aide de l'adresse SNIP de la partition.
5. Les utilisateurs système qui s'authentifient via un serveur d'authentification externe (par exemple, LDAP, RADIUS, TACACS) doivent accéder à une partition via une adresse SNIP.

Cas d'utilisation pour gérer l'accès basé sur les rôles dans une configuration partitionnée

Pensez à un scénario dans lequel une organisation d'entreprise, www.exemple.com, dispose de plusieurs unités commerciales et d'un administrateur centralisé qui gère toutes les instances de son réseau. Toutefois, ils souhaitent fournir des privilèges utilisateur et un environnement exclusifs à chaque unité commerciale.

Voici les administrateurs et les utilisateurs gérés par la configuration d'authentification de partition par défaut et la configuration spécifique à la partition dans une appliance partitionnée.

John : Administrateur racine

George : Administrateur de partition

Adam : Utilisateur système

Jane : Utilisateur de partition

John, est l'administrateur racine d'une appliance Citrix ADC partitionnée. John gère tous les comptes utilisateur et les comptes d'utilisateurs administratifs sur les partitions (par exemple, P1, P2, P3, P4 et P5) au sein de l'appliance. John fournit un accès granulaire basé sur les rôles aux entités à partir de la partition par défaut de la solution matérielle-logicielle. John crée des comptes d'utilisateurs et attribue un accès à une partition à chaque compte. George étant ingénieur réseau au sein de l'organisation, il préfère disposer d'un accès basé sur les rôles à quelques applications exécutées sur la partition P2. Basé sur la gestion des utilisateurs, John crée un rôle d'administrateur de partition pour George et associe son compte utilisateur à une stratégie de commande partition-admin dans la partition P2. Adam étant un autre ingénieur réseau, il préfère accéder à une application exécutée sur P2. John crée un compte d'utilisateur système pour Adam et associe son compte d'utilisateur à une partition P2. Une fois le compte créé, Adam peut se connecter à l'appliance pour accéder à l'interface de gestion Citrix ADC via l'adresse NSIP et peut passer à la partition P2 en fonction de la liaison utilisateur/groupe.

Supposons que Jane, qui est une autre ingénieure réseau, veuille accéder directement à une application exécutée uniquement sur la partition P2, George (administrateur de partition) peut créer un compte d'utilisateur de partition pour elle et associer son compte à des stratégies de commande pour

les privilèges d'autorisation. Le compte utilisateur de Jane créé dans la partition est désormais directement associé à P2. Jane peut désormais accéder à l'interface de gestion Citrix ADC via l'adresse SNIP et ne peut passer à aucune autre partition.

> **Remarque**
>
> Si le compte utilisateur de Jane est créé par un administrateur de partition dans la partition P2, l'administrateur peut accéder à l'interface de gestion Citrix ADC uniquement via l'adresse SNIP (créée dans la partition). L'administrateur n'est pas autorisé à accéder à l'interface via l'adresse NSIP. De même, si le compte utilisateur d'Adam est créé par un administrateur racine dans la partition par défaut et est lié à une partition P2. L'administrateur peut accéder à l'interface de gestion Citrix ADC uniquement via l'adresse NSIP ou l'adresse SNIP créée dans la partition par défaut (avec accès de gestion activé). Il n'est pas autorisé à accéder à l'interface de partition via l'adresse SNIP créée dans la partition administrative.

Configurer les rôles et les responsabilités des administrateurs de partitions

Voici les configurations exécutées par un administrateur racine dans une partition par défaut.

Création de partitions administratives et d'utilisateurs système : un administrateur racine crée des partitions administratives et des utilisateurs système dans la partition par défaut de l'appliance. L'administrateur associe ensuite les utilisateurs à différentes partitions. Si vous êtes lié à une ou plusieurs partitions, vous pouvez passer d'une partition à une autre en fonction des liaisons utilisateur. En outre, votre accès à une ou plusieurs partitions liées est autorisé uniquement par l'administrateur racine.

Autorisation de l'utilisateur système en tant qu'administrateur de partition pour une partition spécifique : une fois qu'un compte d'utilisateur est créé, l'administrateur racine passe à une partition spécifique et autorise l'utilisateur en tant qu'administrateur de partition. Cela se fait en attribuant une stratégie de commande partition-admin au compte utilisateur. L'utilisateur peut désormais accéder à la partition en tant qu'administrateur de partition et gérer les entités au sein de la partition.

Voici les configurations exécutées par un administrateur de partition dans une partition administrative.

Configuration de l'adresse SNIP dans une partition administrative : l'administrateur de la partition se connecte à la partition, crée une adresse SNIP et fournit un accès de gestion à l'adresse.

Création et liaison d'un utilisateur de système de partition avec une stratégie de commande de partition - L'administrateur de partition crée des utilisateurs de partition et définit la portée de l'accès des utilisateurs. Cela se fait en liant le compte utilisateur aux stratégies de commande de partition.

Création et liaison d'un groupe d'utilisateurs de système de partition avec une stratégie de commande de partition -L'administrateur de partition crée des groupes d'utilisateurs de partitions et définit la

portée de l'accès aux groupes d'utilisateurs. Cela se fait en liant le compte du groupe d'utilisateurs aux stratégies de commande de partition.

Configuration de l'authentification du serveur externe pour les utilisateurs externes (facultatif) -Cette configuration permet d'authentifier les utilisateurs TACACS externes accédant à la partition à l'aide de l'adresse SNIP.

Voici les tâches exécutées lors de la configuration de l'accès basé sur les rôles pour les utilisateurs de partitions dans une partition administrative.

1. Création d'une partition administrative : avant de créer des utilisateurs de partition dans une partition administrative, vous devez d'abord créer la partition. En tant qu'administrateur racine, vous pouvez créer une partition à partir de la partition par défaut à l'aide de l'utilitaire de configuration ou d'une interface de ligne de commande.
2. Passage de l'accès utilisateur de la partition par défaut à la partition P2 — Si vous êtes administrateur de partition qui accède à l'appliance à partir de la partition par défaut, vous pouvez passer de la partition par défaut à une partition spécifique. Par exemple, partition P2 basée sur la liaison utilisateur.
3. Ajout d'une adresse SNIP au compte utilisateur de partition avec accès de gestion activé une fois que vous avez basculé votre accès à une partition d'administration. Vous créez une adresse SNIP et fournissez un accès de gestion à cette adresse.
4. Stratégie de création et de liaison d'un utilisateur système de partition avec Partition Command Policy - Si vous êtes administrateur de partition, vous pouvez créer des utilisateurs de partition et définir la portée de l'accès utilisateur. Cela se fait en liant le compte utilisateur aux stratégies de commande de partition.
5. Création et liaison d'un groupe d'utilisateurs de partitions à l'aide d'une stratégie de commande de partition - Si vous êtes administrateur de partitions, vous pouvez créer des groupes d'utilisateurs de partitions et définir la portée du contrôle d'accès utilisateur. Cela se fait en liant le compte du groupe d'utilisateurs aux stratégies de commande de partition.

Configuration de l'authentification du serveur externe pour les utilisateurs externes (facultatif) -Cette configuration permet d'authentifier les utilisateurs TACACS externes accédant à la partition à l'aide d'une adresse SNIP.

Avantages de l'utilisation de partitions d'administration

Vous pouvez profiter des avantages suivants en utilisant des partitions d'administration pour votre déploiement :

- Permet de déléguer la propriété administrative d'une application au client.
- Réduit le coût de possession d'ADC sans compromettre les performances et la facilité d'utilisation.

- Protège contre les modifications injustifiées de configuration. Dans une appliance Citrix ADC non partitionnée, les utilisateurs autorisés de l'autre application peuvent modifier intentionnellement ou involontairement les configurations requises pour votre application. Cela peut entraîner un comportement indésirable. Cette possibilité est réduite dans une appliance Citrix ADC partitionnée.
- Isole le trafic entre différentes applications en utilisant des VLAN dédiés pour chaque partition.
- Accélère et permet aux déploiements d'applications d'évoluer.
- Permet une gestion et des rapports au niveau de l'application ou localisés.

Laissez-nous analyser quelques cas pour comprendre les scénarios dans lesquels vous pouvez utiliser des partitions d'administration.

Cas d'utilisateur 1 : comment la partition d'administration est utilisée dans un réseau d'entreprise

Considérons un scénario auquel est confrontée une entreprise nommée **Foo.com**.

- **Foo.com** possède un seul Citrix ADC.
- Il existe cinq départements et chaque département possède une application qui doit être déployée avec Citrix ADC.
- Chaque application doit être gérée indépendamment par un ensemble différent d'utilisateurs ou d'administrateurs.
- Les autres utilisateurs doivent être limités à accéder aux configurations.
- L'application ou le back-end doit pouvoir partager des ressources telles que des adresses IP.
- Le service informatique mondial doit être en mesure de contrôler les paramètres de niveau Citrix ADC qui doivent être communs à toutes les partitions.
- Les demandes doivent être indépendantes les unes des autres. Une erreur dans la configuration d'une application ne doit pas affecter l'autre.

Un Citrix ADC non partitionné ne serait pas en mesure de satisfaire ces exigences. Toutefois, vous pouvez répondre à toutes ces exigences en partitionnant un Citrix ADC.

Il suffit de créer une partition pour chacune des applications, d'attribuer les utilisateurs requis aux partitions, de spécifier un VLAN pour chaque partition et de définir des paramètres globaux sur la partition par défaut.

Cas d'utilisation 2 : comment une partition d'administration est utilisée par un fournisseur de services

Considérons un scénario auquel est confronté un fournisseur de services nommé **BigProvider** :

- BigProvider compte 5 clients : 3 petites entreprises et 2 grandes entreprises.

- **SmallBiz**, **SmallBiz**et **StartupBiz** n'ont besoin que des fonctionnalités Citrix ADC les plus basiques.
- **BigBiz** et **LargeBiz** sont de grandes entreprises et ont des applications qui attirent un trafic important. Ils aimeraient utiliser certaines des fonctionnalités Citrix ADC les plus complexes.

Dans une approche non partitionnée, l'administrateur Citrix ADC utilise généralement une appliance Citrix ADC SDX et provisionne une instance Citrix ADC pour chaque client.

La solution convient à **BigBiz** et **LargeBiz** car leurs applications ont besoin de la puissance non diminuée de l'ensemble de l'appliance Citrix ADC non partitionnée. Toutefois, cette solution peut ne pas être aussi rentable pour l'entretien de **SmallBiz, SmallBiz**et**StartupBiz**.

Par conséquent, **BigProvider** décide de la solution suivante :

- Utilisation d'une appliance Citrix ADC SDX pour créer des instances Citrix ADC dédiées pour **BigBiz** et **LargeBiz**.
- Utiliser une seule Citrix ADC partitionnée en trois partitions, une pour **SmallBiz**, **SmallBiz**et **StartupBiz**.

L'administrateur Citrix ADC (superutilisateur) crée une partition d'administration pour chacun de ces clients et spécifie les utilisateurs des partitions. Et spécifie également les ressources Citrix ADC pour les partitions, et spécifie le VLAN à utiliser par le trafic destiné à chacune des partitions.

Prise en charge des configurations Citrix ADC dans la partition d'administration

October 5, 2021

Les configurations Citrix ADC peuvent être classées dans les trois types de configurations suivants. Cela dépend de la configuration Citrix et de la partition dans laquelle la configuration est effectuée.

> **Remarque**
>
> - Les partitions d'administration ne peuvent pas être configurées sur un cluster Citrix ADC. Cela signifie qu'un cluster Citrix ADC ne peut pas être partitionné.
> - Les partitions d'administration ne peuvent pas être configurées sur une appliance FIPS Citrix ADC 14000.
> - Lecas 3 répertorie les fonctionnalités Citrix ADC qui ne sont pas prises en charge dans les partitions d'administration.
> - Les modèles d'équilibrage de charge ne sont pas pris en charge dans les partitions d'administration.

Cas 1 (configurations globales)

Configurations qui peuvent être exécutées UNIQUEMENT dans la partition par défaut et qui sont disponibles ou qui ont un impact sur toutes les partitions d'administration.



- Mises à jour des entités intégrées pour les moniteurs, les profils TCP, les profils HTTP, etc.
- Mises à jour des paramètres globaux pour syslog, NSLOG, weblog, commutation de contenu, IPSEC, SIP, DHCP, protection contre les surtensions, mise en mémoire tampon TCP et collecte de systèmes.
- Configurations haute disponibilité (HA)
- Modifications de l'interface et du VLAN
- Configurations utilisateur

Cas 2 (configurations spécifiques aux partitions)

Configurations pouvant être exécutées indépendamment dans les partitions par défaut et d'administration. Ces configurations s'appliquent uniquement à la partition dans laquelle elles sont exécutées.



- Obtention des statistiques de niveau de trafic pour une partition.
- L'administrateur de partition peut mettre à jour les liaisons IP pour le VLAN qui est lié à cette partition. Mais il n'est pas possible de mettre à jour les liaisons d'interface.
- Effacer les configurations Citrix ADC.

- Paramètres spécifiques aux fonctionnalités pour les fonctionnalités suivantes : AppFlow, AppQoE, compression HTTP, DNS, TCP, HTTP, chiffrement, répondeur, réécriture et SSL.
- Configurations spécifiques aux fonctionnalités telles que les serveurs virtuels, les services et les moniteurs.

Cas 3

Configurations qui ne peuvent pas être exécutées sur les partitions d'administration. Ces fonctionnalités peuvent être configurées dans la partition par défaut, mais elles n'ont aucun impact sur les partitions d'administration.



> **Remarque :**
>
> Les configurations prises en charge sur les partitions d'administration pour une version particulière sont marquées comme **Oui**.

Composant caractéristique	Fonctionnalité Citrix ADC	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0	Citrix ADC 13.1
Mise en réseau	Domaine de trafic	Non (non pris en charge à partir de la version 60.13)	Non	Non	Non	Non
Stratégie	Extensibilité	Oui	Oui	Oui	Oui	Oui
Équilibrage de charge	Mise à l'Autoscale DBS	Oui	Oui	Oui	Oui	Oui
Équilibrage de charge	DNSSEC	Non	Non	Oui	Oui	Oui

Composant caractéristique	Fonctionnalité Citrix ADC	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0	Citrix ADC 13.1
Équilibrage de charge	Diameter	Oui	Oui	Oui	Oui	Oui
Équilibrage de charge	RTSP	Non	Non	Non	Non	Non
Équilibrage de charge	Sure Connect	Oui	Oui	Obsolète	Obsolète	Supprimé
Équilibrage de charge	Groupe de services Autoscale	Oui	Oui	Oui	Oui	Oui
Facilité de gestion	Authentificati externe RBA	Oui	Oui	Oui	Oui	Oui
Facilité de gestion	Cisco RISE	Non	Non	Non	Oui	Oui
Facilité de gestion	ACI-Cisco	Oui	Oui	Oui	Oui	Oui
Facilité de gestion	AppExpert	Oui	Oui	Oui	Oui	Oui
Facilité de gestion	HDX Insight	Non	Non	Non	Non	Non
Facilité de gestion	Insight	Non	Non	Non	Non	Non
VPN	Connecteur Citrix Cloud-Bridge	Non	Non	Non	Non	Non
VPN	VPN Citrix Gateway ou SSL	Non	Non	Non	Non	Non
VPN	Proxy ICA VPN SSL	Non	Non	Non	Non	Non

Composant caractéristique	Fonctionnalité Citrix ADC	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0	Citrix ADC 13.1
VPN	Interface Web sur Citrix ADC	Non	Non	Non	Non	Non
SSL	Profil SSL	Oui	Oui	Oui	Oui	Oui
SSL	SSL-FIPS	Non	Non	Non	Non	Non
SSL	HSM externe	Non	Non	Non	Non	Non
Infra	Redirection de cache	Non	Non	Non	Non	Non
Infra	Mise en cache intégrée	Oui	Oui	Oui	Oui	Oui
Réseau	VXLAN	Oui	Oui	Oui	Oui	Oui
Réseau	Arrêt gracieux	Oui	Oui	Oui	Oui	Oui
Réseau	LSN	Non	Non	Non	Non	Non
Réseau	Logo IPv6 Ready	Oui	Oui	Oui	Oui	Oui
Réseau	vPath	Oui	Oui	Oui	Oui	Oui
Équilibrage de charge	flux de données	Oui	Oui	Oui	Oui	Oui
Journalisation	Journalisation Web	Oui	Oui	Oui	Oui	Oui
Réseau	Paramètre L2/L3	Oui	Oui	Oui	Oui	Oui
Réseau	Tunnel GRE	Oui	Oui	Oui	Oui	Oui
équilibrage de charge-ment	Surveillance scriptable	Oui	Oui	Oui	Oui	Oui
Équilibrage de charge	GSLB	Oui	Oui	Oui	Oui	Oui

Composant caractéristique	Fonctionnalité Citrix ADC	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0	Citrix ADC 13.1
Infra	Mise en miroir des connexions	Oui	Oui	Oui	Oui	Oui
Infra	FEO	Oui	Oui	Oui	Oui	Oui
Infra	Trace Ns	Oui	Oui	Oui	Oui	Oui
Équilibrage de charge	File d'attente prioritaire	Oui	Oui	Obsolète	Obsolète	Supprimé
Réseau	HDOSP	Oui	Oui	Obsolète	Obsolète	Supprimé
Réseau	Profil net	Oui	Oui	Oui	Oui	Oui
Réseau	Mise en réseau (fonctionnalité restreinte)	Oui	Oui	Oui	Oui	Oui
Réseau	VRRP (fonctionnalité restreinte)	Oui	Oui	Oui	Oui	Oui
Journalisatio	Journalisatio d'audit (SYSLOG-TCP, LB de serveurs Syslog, prise en charge de SNIP et prise en charge du nom de domaine complet pour Syslog)	Oui	Oui	Oui	Oui	Oui

Composant caractéristique	Fonctionnalité Citrix ADC	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0	Citrix ADC 13.1
VPN	Citrix Gateway	Non	Non	Non	Non	Non
VPN	AAA-TM	Oui	Oui	Oui	Oui	Oui
AppFlow	AppFlow	Non	Oui (IPFIX uniquement)	Oui (IPFIX uniquement)	Oui	Oui
AppFW	Pare-feu d'application	Non	Non	Non	Non	Non
Transformation d'URL	Transformation d'URL	Non	Non	Non	Non	Non
Équilibrage de charge	Mise en mémoire tampon TCP	Non	Non	Non	Non	Non
Stratégies	Répondeur OCSP	Oui	Oui	Oui	Oui	Oui
Journal d'audit	SYSLOG-TCP	Non	Oui	Oui	Oui	Oui
Optimisation	Optimisation front-end	Non	Oui	Oui	Oui	Oui
AppQoE	AppQoE	Oui	Oui	Oui	Oui	Oui

Le tableau précédent répertorie certaines des fonctionnalités sous forme de **fonctionnalités restreintes** dans la configuration de la partition d'administration. La section suivante explique pourquoi certaines des fonctionnalités sont mentionnées comme des **fonctionnalités restreintes**.

- **VRRP**. Le VRRP est une fonctionnalité restreinte dans la partition d'administration en raison de ce qui suit :
  - L'ajout ou la suppression de VRID ne peuvent être effectués qu'à partir du contexte de partition par défaut. Toutefois, une fois qu'un VRID est créé, il peut être utilisé dans des partitions autres que par défaut.
  - La fonctionnalité VRRP est prise en charge uniquement sur les VLAN dédiés.
  - La fonctionnalité VRRP n'est pas prise en charge sur les VLAN partagés, utilisés par la par-

tition d'administration. Il est bloqué en interne. Aucun message d'erreur n'est affiché pendant la configuration. Le protocole est bloqué sur un VLAN partagé (balisé ou non balisé) lié à une partition par défaut ou à n'importe quelle partition administrative.

> **Important**
>
> Pour prendre en charge le déploiement actif-actif à l'aide de VRRP, les VIP principal et de sauvegarde doivent utiliser le même VRID. Les différents VRID ne peuvent pas être utilisés.

- **Mise en réseau**. Certaines configurations réseau (L2 Param et L3 Param) ne sont pas prises en charge ou valides dans le contexte de la partition. Si vous rencontrez de telles configurations, le message d'erreur suivant s'affiche. « ERREUR : Cette option de configuration n'est pas prise en charge sur la partition autre que par défaut. «

Configurer les partitions d'administration

September 8, 2021

> **Important**
>
> - Seuls les superutilisateurs sont autorisés à créer et à configurer des partitions d'administration.
> - Sauf indication contraire, les configurations pour configurer une partition d'administration doivent être effectuées à partir de la partition par défaut.

En partitionnant une appliance Citrix ADC, vous créez en effet plusieurs instances d'une seule appliance Citrix ADC. Chaque instance possède ses propres configurations et le trafic de chacune de ces partitions est isolé de l'autre. Cela se fait en attribuant à chaque partition un VLAN dédié ou un VLAN partagé.

Une partition Citrix ADC partitionnée possède une partition par défaut et les partitions d'administration créées. Pour configurer une partition d'administration, vous devez d'abord créer une partition avec les ressources pertinentes (mémoire, bande passante maximale et connexions). Spécifiez ensuite les utilisateurs qui peuvent accéder à la partition et le niveau d'autorisation de chacun des utilisateurs de la partition.

L'accès à un Citrix ADC partitionné est identique à l'accès à un Citrix ADC non partitionné : via l'adresse NSIP ou toute autre adresse IP de gestion. En tant qu'utilisateur, après avoir fourni vos informations d'identification de connexion valides, vous êtes redirigé vers la partition à laquelle vous êtes lié. Toutes les configurations que vous créez sont enregistrées sur cette partition. Si vous êtes associé à plusieurs partitions, vous êtes dirigé vers la première partition à laquelle vous avez été associé. Si vous souhaitez configurer des entités sur l'une de vos autres partitions, vous devez explicitement passer à cette partition.

Après avoir accédé à la partition appropriée, les configurations que vous effectuez sont enregistrées sur cette partition et sont spécifiques à cette partition.

> **Remarque**
>
> - Les superutilisateurs Citrix ADC et autres utilisateurs non partitionnés sont reconduits vers la partition par défaut.
> - Les utilisateurs de toutes les partitions 512 peuvent se connecter simultanément.

Conseil

Pour accéder à une appliance Citrix ADC partitionnée via HTTPS à l'aide du SNIP (avec accès de gestion activé), assurez-vous que chaque partition possède le certificat de son administrateur de partition. Dans la partition, l'administrateur de la partition doit effectuer les opérations suivantes :

1. Ajoutez le certificat à Citrix ADC.

   ```
   add ssl certKey ns-server-certificate -cert ns-server.cert-key ns-server.key
   ```

2. Liez-le à un service nommé `nshttps-<SNIP>-3009`, où `<SNIP>` doit être remplacé par l'adresse SNIP, dans ce cas 100.10.10.1.

   ```
   bind ssl service nshttps-100.10.10.1-3009 -certkeyName ns-server-certificate
   ```

Limitation des ressources de partition

Dans une appliance Citrix ADC partitionnée, un administrateur réseau peut créer une partition avec des ressources de partition telles que la mémoire, la bande passante et la limite de connexion configurées comme illimitées. Pour ce faire, spécifiez Zero comme valeur de ressource de partition. Lorsque Zero indique que la ressource est illimitée sur la partition et qu'elle peut être consommée jusqu'aux limites système. La configuration des ressources de partition est utile lorsque vous migrez un déploiement de domaine de trafic vers une partition administrative ou si vous ne connaissez pas la limite d'allocation de ressources pour une partition dans un déploiement donné.

La limite de ressources pour une partition administrative est la suivante :

1. **Mémoire de partition**. Il s'agit de la mémoire maximale allouée à une partition. Assurez-vous de spécifier les valeurs lors de la création d'une partition.

   > **Remarque**
   >
   > À partir de NetScaler 12.0, lorsque vous créez une partition, vous pouvez définir la limite de

> mémoire sur Zero. Si une partition est déjà créée avec une limite de mémoire spécifique, vous pouvez réduire la limite à n'importe quelle valeur ou définir la limite sur Zero.

Paramètre : MaxMemLimit

La mémoire maximale est allouée en Mo dans une partition. Une valeur zéro indique que la mémoire est illimitée sur la partition et qu'elle peut consommer jusqu'aux limites du système.

Valeur par défaut : 10

2. **Bande passante de partition**. Bande passante maximale allouée pour une partition. Si vous spécifiez une limite, assurez-vous qu'elle se situe dans le débit sous licence de la solution matérielle-logicielle. Sinon, vous ne limitez pas la bande passante utilisée par la partition. La limite spécifiée est responsable de la bande passante requise par l'application. Si la bande passante de l'application dépasse la limite spécifiée, les paquets sont supprimés.

   > **Remarque**
   >
   > À partir de NetScaler 12.0, lorsque vous pouvez créer une partition, vous pouvez définir la limite de bande passante de partition sur Zero. Si une partition est déjà créée avec une bande passante spécifique, vous pouvez réduire la bande passante ou définir la limite sur Zero.

   Paramètre : MaxBandwidth

   La bande passante maximale est allouée en Kbits/s dans une partition. Une valeur zéro indique que la bande passante n'est pas restreinte. C'est-à-dire que la partition peut consommer jusqu'aux limites du système.

   Valeur par défaut : 10240

   Valeur maximale : 4294967295

3. **Connexion à la partition**. Nombre maximal de connexions simultanées pouvant être ouvertes dans une partition. La valeur doit prendre en compte le flux simultané maximal attendu dans la partition. Les connexions de partition sont comptabilisées à partir de la mémoire de quota de partition. Auparavant, les connexions étaient comptabilisées à partir de la mémoire de quota de partition par défaut. Il est configuré uniquement côté client, et non sur les connexions TCP principales côté serveur. Les nouvelles connexions ne peuvent pas être établies au-delà de cette valeur configurée.

   > **Remarque**
   >
   > À partir de NetScaler 12.0, vous pouvez créer une partition dont le nombre de connexions ouvertes est défini sur Zero. Si vous avez déjà créé une partition avec un nombre spécifique de connexions ouvertes, vous pouvez réduire la limite de connexion ou définir la limite sur Zero.

   Paramètre : MaxConnections

Nombre maximal de connexions simultanées pouvant être ouvertes dans la partition. Une valeur zéro indique qu'il n'y a pas de limite au nombre de connexions ouvertes.

Valeur par défaut : 1024

Valeur minimale : 0

Valeur maximale : 4294967295

Configurer une partition d'administration

Pour configurer une partition d'administration, effectuez les tâches suivantes.

Pour accéder à une partition d'administration à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'appliance Citrix ADC.
2. Vérifiez si vous êtes dans la bonne partition. L'invite de commandes affiche le nom de la partition actuellement sélectionnée.
3. Si oui, passez à l'étape suivante.
4. Si non, obtenez une liste des partitions auxquelles vous êtes associé et passez à la partition appropriée.
   - `show system user <username>`
   - `switch ns partition <partitionName>`
5. Vous pouvez désormais effectuer les configurations requises comme Citrix ADC non partitionnée.

Pour accéder à une partition d'administration à l'aide de l'interface graphique

1. Connectez-vous à l'appliance Citrix ADC.
2. Vérifiez si vous êtes dans la bonne partition. La barre supérieure de l'interface graphique affiche le nom de la partition actuellement sélectionnée.
   - Si oui, passez à l'étape suivante.
   - Si non, accédez à **Configuration > Système > Administration des partitions > Partitions**, cliquez avec le bouton droit sur la partition vers laquelle vous souhaitez basculer, puis sélectionnez **Commutateur**.
3. Vous pouvez désormais effectuer les configurations requises comme Citrix ADC non partitionnée.

Ajouter une partition d'administration

L'administrateur racine ajoute une partition administrative à partir de la partition par défaut et lie la partition avec VLAN 2.

Pour créer une partition administrative à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add partition <partitionname>
```

Basculer l'accès utilisateur de la partition par défaut vers une partition d'administration

Vous pouvez désormais basculer l'accès utilisateur de la partition par défaut à la partition Par1.

Pour passer d'un compte d'utilisateur d'une partition par défaut à une partition d'administration à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
Switch ns partition <pname>
```

Ajout d'une adresse SNIP à un compte d'utilisateur de partition avec l'accès à la gestion activé

Dans la partition, créez une adresse SNIP avec l'accès à la gestion activé.

Pour ajouter une adresse SNIP au compte utilisateur de partition dont l'accès de gestion est activé à l'aide de l'interface de ligne de commande, procédez comme suit :

À l'invite de commandes, tapez :

```
> add ns ip <ip address> <subnet mask> -mgmtAccess enabled
```

Créer et lier un utilisateur de partition à l'aide d'une stratégie de commande de partition

Dans la partition, créez un utilisateur de système de partition et liez l'utilisateur à des stratégies de commande partition-admin.

Pour créer et lier un utilisateur de système de partition avec une stratégie de commande de partition à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :


```
> add system user <username> <password>

Done
```

Création et liaison d'un groupe d'utilisateurs de partition avec une stratégie de commande de partition

Dans Partition Par1, créez un groupe d'utilisateurs de système de partition et liez le groupe avec une stratégie de commande de partition telle que l'administrateur de partition, la lecture seule de partitions, l'opérateur de partition ou le réseau de partition.

Pour créer et lier un groupe d'utilisateurs de partition avec la stratégie de commande de partition à l'aide de l'interface de ligne de commande :

```
1 > add system group <groupName>
2 > bind system group <groupname> (-userName | -policyName <cmdpolicy> <
     priority> | -partitionName)
```

Configuration de l'authentification du serveur externe pour les utilisateurs externes

Dans la partition Par1, vous pouvez configurer une authentification de serveur externe pour authentifier les utilisateurs TACACS externes accédant à la partition via une adresse SNIP.

Pour configurer l'authentification du serveur externe pour des utilisateurs externes à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 > add authentication tacacsaction <name> -serverip <IP> -tacacsSecret <
     secret key> -authorization ON -accounting ON
2 > add authentication policy <policname> -rule true -action <name>
3 > bind system global <policyname> -priority <value>1
```

Configurer un compte utilisateur du système de partition dans une partition à l'aide de l'interface graphique

Pour configurer un compte d'utilisateur de partition dans une partition administrative, vous devez créer un utilisateur de partition ou un groupe d'utilisateurs de partition et le lier aux stratégies de commande de partition. Vous pouvez également configurer l'authentification du serveur externe pour un utilisateur externe.

Pour créer un compte utilisateur de partition dans une partition à l'aide de l'interface graphique

Accédez à **Système > Administration**des **utilisateurs, cliquez sur Utilisateurs** pour ajouter un utilisateur de système de partition et liez l'utilisateur aux stratégies de commande (partitionadmin/partitionlecture seule/partition-operator/partition-network).

Pour créer un compte de groupe d'utilisateurs de partitions dans une partition à l'aide de l'interface graphique

Accédez à **Système > Administration des utilisateurs**, cliquez sur **Groupes** pour ajouter un groupe d'utilisateurs de système de partition et lier le groupe d'utilisateurs aux stratégies de commande (partitionadmin/partitionlecture seule/partition-operator/partition-network).

Pour configurer l'authentification de serveur externe pour des utilisateurs externes à l'aide de l'interface graphique

Accédez à **Système > Authentification > Actions de base** et cliquez sur **TACACS** pour configurer un serveur TACACS pour authentifier les utilisateurs externes accédant à la partition.

Exemple de configuration

La configuration suivante montre comment créer un utilisateur de partition ou un groupe d'utilisateurs de partitions et de les lier aux stratégies de commande de partition. De plus, comment configurer l'authentification du serveur externe pour l'authentification d'un utilisateur externe.

```
1  > add partition Par1
2  > switch ns partition Par1
3  > add ns ip 10.102.29.203 255.255.255.0 -mgmtAccessenabled
4  > add system user John Password
5  > bind system user Jane partition-read-only -priority 1
6  > add system group Retail
7  > bind system group Retail -policyname partition-network 1 (where 1 is
       the priority number)
8  > bind system group Retail  - username Jane
9  > add authentication tacacssaction tacuser  - serverip 10.102.29.200  -
       tacacsSecret Password  - authorization ON  - accounting ON
10 > add authentication policy polname  - rule true  - action tacacsAction
11 > bind system global polname  - priority 1
```


Stratégies de commande pour les utilisateurs de partition et les groupes d'utilisateurs de partition dans la partition d'administration

Commandes permettant d'autoriser un compte utilisateur dans une partition administrative	Stratégies de commande disponibles dans une partition administrative (stratégies intégrées)	Type d'accès au compte utilisateur
ajouter un utilisateur système	Administrateur de partitions	SNIP (avec accès à la gestion activé)
ajouter un groupe de systèmes	Réseau de partitions	SNIP (avec accès à la gestion activé)
ajout d'authentification `<action, policy>`, système de liaison global `<policy name>`	Partition en lecture seule	SNIP (avec accès à la gestion activé)
supprimer l'utilisateur système	Administrateur de partitions	SNIP (avec accès à la gestion activé)
supprimer un groupe de systèmes	Administrateur de partitions	SNIP (avec accès à la gestion activé)
`bind system cmdpolicy` à l'utilisateur système ; `bind system cmdpolicy` au groupe système	Administrateur de partitions	SNIP (avec accès à la gestion activé)

Configurer un canal Ethernet LACP sur la partition d'administration par défaut

Avec le protocole LACP (Link Aggregation Control Protocol), vous pouvez combiner plusieurs ports en une seule liaison haute vitesse (également appelée canal). Une appliance compatible LACP échange des unités de données LACP (LACPDU) sur le canal.

Il existe trois modes de configuration LACP que vous pouvez activer dans la partition par défaut d'une appliance Citrix ADC :

1. Actif. Un port en mode actif envoie des LACPDU. L'agrégation de liens est formée si l'autre extrémité de la liaison Ethernet est en mode actif ou passif LACP.
2. passif. Un port en mode passif envoie des LACPDU uniquement lorsqu'il reçoit des LACPDU. L'agrégation de liens est formée si l'autre extrémité de la liaison Ethernet est en mode actif LACP.
3. Désactiver. L'agrégation de liens n'est pas formée.

> **Remarque**
>
> Par défaut, l'agrégation de liens est désactivée dans la partition par défaut de l'appliance.

LACP échange LACPDU entre appareils connectés par une liaison Ethernet. Ces appareils sont généralement appelés acteurs ou partenaires.

Une unité de données LACPDU contient les paramètres suivants :

- Mode LACP. Actif, passif ou désactivé.
- Délai d'attente LACP. La période d'attente avant le chronométrage du partenaire ou de l'acteur. Valeurs possibles : Long et Courte. Par défaut : Long.
- Clé de port. Pour distinguer les différents canaux. Lorsque la clé est 1, LA/1 est créé. Lorsque la clé est 2, LA/2 est créé. Valeurs possibles : entier compris entre 1 et 8. 4 à 8 est destiné au cluster CLAG.
- Priorité portuaire. Valeur minimale : 1. Valeur maximale : 65535. Par défaut : 32768.
- Priorité système. Utilise cette priorité avec le MAC système pour former l'ID système afin d'identifier le système de manière unique lors des négociations LACP avec le partenaire. Définit la priorité système de 1 et 65535. La valeur par défaut est définie sur 32768.
- Interface. Prend en charge 8 interfaces par canal sur l'appliance NetScaler 10.1 et prend en charge 16 interfaces par canal sur les appliances NetScaler 10.5 et 11.0.

Après avoir échangé des LACPDU, l'acteur et le partenaire négocient les paramètres et décident d'ajouter les ports à l'agrégation.

Configurer et vérifier LACP

La section suivante explique comment configurer et vérifier LACP dans la partition d'administration.

Pour configurer et vérifier LACP sur une appliance Citrix ADC à l'aide de l'interface de ligne de commande

1. Activez LACP sur chaque interface.

   ```
   set interface <Interface_ID> -lacpMode PASSIVE -lacpKey 1<!--NeedCopy
   -->
   ```

   Lorsque vous activez LACP sur une interface, les canaux sont créés dynamiquement. De plus, lorsque vous activez LACP sur une interface et que vous définissez LacpKey sur 1, l'interface est automatiquement liée au canal LA/1.

   > **Remarque**
   >
   > Lorsque vous liez une interface à un canal, les paramètres de canal ont priorité sur les paramètres de l'interface, de sorte que les paramètres de l'interface sont ignorés. Si un

> canal est créé dynamiquement par LACP, vous ne pouvez pas effectuer les opérations d'ajout, de liaison, de déliaison ou de suppression sur le canal. Un canal créé dynamiquement par LACP est automatiquement supprimé lorsque vous désactivez LACP sur toutes les interfaces du canal.

2. Définissez la priorité système.

   ```
   set lacp -sysPriority <Positive_Integer><!--NeedCopy-->
   ```

3. Vérifiez que LACP fonctionne comme prévu.

   "'show interface

   ```
   1 ```show channel<!--NeedCopy-->
   ```

   ```
   show LACP<!--NeedCopy-->
   ```

   > **Remarque**
   >
   > Dans certaines versions de Cisco Internetwork Operating System (iOS), l'exécution de la <VLAN_ID>commande VLAN natif switchport trunk entraîne l'étiquetage du commutateur Cisco sur les PDU LACP. Cela provoque l'échec du canal LACP entre le commutateur Cisco et l'appliance Citrix ADC. Toutefois, ce problème n'affecte pas les canaux d'agrégation de liens statiques configurés dans la procédure précédente.

Enregistrer la configuration de toutes les partitions d'administration à partir de la partition par défaut

Les administrateurs peuvent enregistrer la configuration de toutes les partitions d'administration en même temps à partir de la partition par défaut.

Enregistrer toutes les partitions d'administration de la partition par défaut à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
save ns config -all
```

Prise en charge des rapports personnalisés basés sur partitions et grappes

L'interface graphique Citrix ADC affiche uniquement les rapports personnalisés créés dans la partition d'affichage actuelle ou dans le cluster.

Auparavant, l'interface graphique Citrix ADC stockait les noms des rapports personnalisés directement dans le fichier backend sans mentionner le nom de partition ou de cluster à différencier.

Pour afficher les rapports personnalisés de la partition ou du cluster actuel dans l'interface graphique

- Accédez à l'onglet **Reporting** .
- Cliquez sur **Rapports personnalisés** pour afficher les rapports créés dans la partition actuelle ou dans le cluster.

Prise en charge de la liaison de certificats globaux VPN dans une configuration partitionnée pour l'IdP OAuth

Dans une configuration partitionnée, vous pouvez désormais lier les certificats à un VPN global pour les déploiements d'IdP OAuth.

Pour lier les certificats dans la configuration partitionnée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind vpn global [-certkeyName <string>] [-userDataEncryptionKey <string
    >]
```

Configuration VLAN pour les partitions d'administration

October 5, 2021

Les VLAN peuvent être liés à une partition en tant que VLAN « dédié » ou VLAN « partagé ». En fonction de votre déploiement, vous pouvez lier un VLAN à une partition pour isoler son trafic réseau des autres partitions.

VLAN dédié — Un VLAN lié à une seule partition avec l'option « Partage » désactivée et doit être un VLAN balisé. Par exemple, dans un déploiement client-serveur, pour des raisons de sécurité, un administrateur système crée un VLAN dédié pour chaque partition côté serveur.

VLAN partagé : VLAN lié (partagé entre) à plusieurs partitions avec l'option « Partage » activée. Par exemple, dans un déploiement client-serveur, si l'administrateur système n'a pas le contrôle sur le réseau côté client, un VLAN est créé et partagé sur plusieurs partitions.

Le VLAN partagé peut être utilisé sur plusieurs partitions. Il est créé dans la partition par défaut et vous pouvez lier un VLAN partagé à plusieurs partitions. Par défaut, un VLAN partagé est implicitement lié à la partition par défaut et ne peut donc pas être lié explicitement.

Remarque

- Une appliance Citrix ADC déployée sur n'importe quelle plate-forme hyperviseur (ESX, KVM, Xen et Hyper-V) doit respecter les conditions suivantes dans un domaine de configuration de partition et de trafic :
  - Enable the promiscuous mode, MAC changes, MAC spoofing, or forged transmit for shared VLANs with partition.
  - Enable the VLAN with port group properties of the virtual switch, if the traffic is through a dedicated VLAN.
- Dans un dispositif Citrix ADC partitionné (multilocataire), un administrateur système peut isoler le trafic circulant vers une ou plusieurs partitions particulières. Cela se fait en liant un ou plusieurs VLAN à chaque partition. Un VLAN peut être dédié à une partition ou partagé sur plusieurs partitions.

VLAN dédiés

Pour isoler le trafic entrant dans une partition, créez un VLAN et associez-le à la partition. Le VLAN n'est alors visible que par la partition associée, et le trafic passant par le VLAN est classé et traité uniquement dans la partition associée.



Pour implémenter un VLAN dédié pour une partition particulière, procédez comme suit.

1. Ajoutez un VLAN (V1).
2. Liez une interface réseau au VLAN en tant qu'interface réseau balisée.
3. Créez une partition (P1).
4. Liez la partition (P1) au VLAN dédié (V1).

Configurez les éléments suivants à l'aide de la CLI

- Créer un VLAN

  ```
  add vlan <id>
  ```

Exemple

```
1     add vlan 100
```

- Lier un VLAN

  ```
  bind vlan <id> -ifnum <interface> -tagged
  ```

Exemple

```
1     bind vlan 100  - ifnum 1/8 -tagged
```

- Créer une partition

  ```
  Add ns partition <partition name> [-maxBandwidth <positive_integer>][-
  maxConn <positive_integer>] [-maxMemLimit <positive_integer>]
  ```

Exemple

```
1     Add ns partition P1  - maxBandwidth 200  - maxconn 50  - maxmemlimit
         90
2
3     Done
```

- Lier une partition à un VLAN

  ```
  bind partition <partition-id> -vlan <id>
  ```

Exemple

```
1     bind partition P1  - vlan 100
```

Configurer un VLAN dédié à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Configuration > Système > Réseau VLAN** et cliquez sur **Ajouter** pour créer un VLAN.
2. Sur la page **Créer un VLAN**, définissez les paramètres suivants :
   - ID DE VLAN
   - Nom de l'alias
   - Unité de transmission maximale
   - Routage dynamique

- Routage dynamique IPv6
- Partage de partitions

3. Dans la section **Liaisons d'interface**, sélectionnez une ou plusieurs interfaces et liez-les au VLAN.
4. Dans la section **Liaisons IP**, sélectionnez une ou plusieurs adresses IP et liez le VLAN.
5. Cliquez sur **OK** et **Terminé**.

VLAN partagé

Dans une configuration de VLAN partagé, chaque partition possède une adresse MAC, et le trafic reçu sur le VLAN partagé est classé par adresse MAC. Seul un VLAN de couche 3 est recommandé car il peut restreindre le trafic de sous-réseau. Une adresse MAC de partition est applicable et importante uniquement pour un déploiement de VLAN partagé.

> **Remarque**
>
> À partir de Citrix ADC version 12.1 build 51.16, le VLAN partagé dans un dispositif partitionné prend en charge le protocole de routage dynamique.

Le diagramme suivant montre comment un VLAN (VLAN 10) est partagé entre deux partitions.



Pour déployer une configuration de VLAN partagé, procédez comme suit :

1. Créez un VLAN avec l'option de partage « activée » ou activez l'option de partage sur un VLAN existant. Par défaut, l'option est « désactivée ».
2. Liez l'interface de partition au VLAN partagé.
3. Créez les partitions, chacune avec sa propre adresse PartitionMac.
4. Liez les partitions au VLAN partagé.

Configurer un VLAN partagé à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour ajouter un VLAN ou définir le paramètre de partage d'un VLAN existant :

```
add vlan <id> [-sharing (ENABLED | DISABLED)]

set vlan <id> [-sharing (ENABLED | DISABLED)]

add vlan 100  - sharing ENABLED

set vlan 100  - sharing ENABLED
```

Liez une partition à un VLAN partagé à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind partition <partition-id> -vlan <id>

bind partition P1  - vlan 100

add ns partition P1  - maxBandwidth 200  - maxconn 50    - maxmemlimit 90
   -partitionMAC<mac_addr

Done
```

Configurer une adresse MAC de partition à l'aide de l'interface de ligne de commande

```
set ns partition <partition name> [-partitionMAC<mac_addr>]

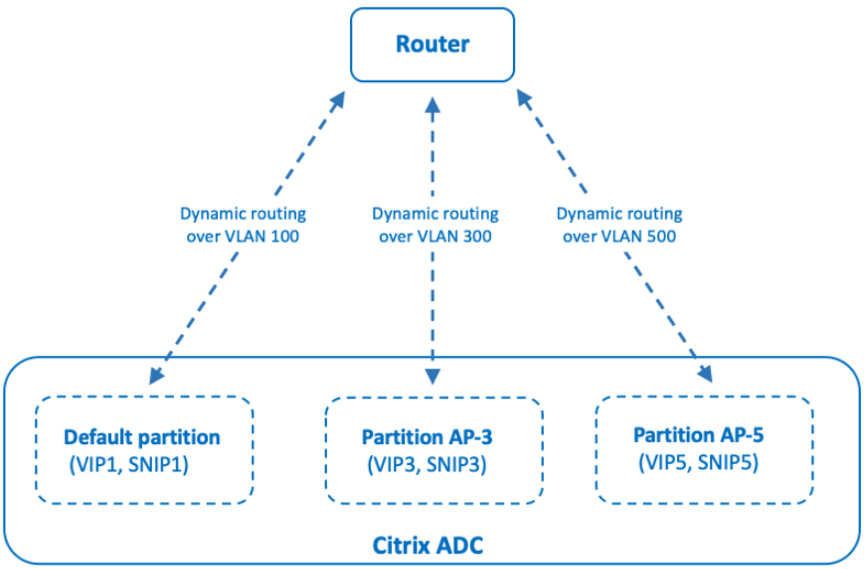
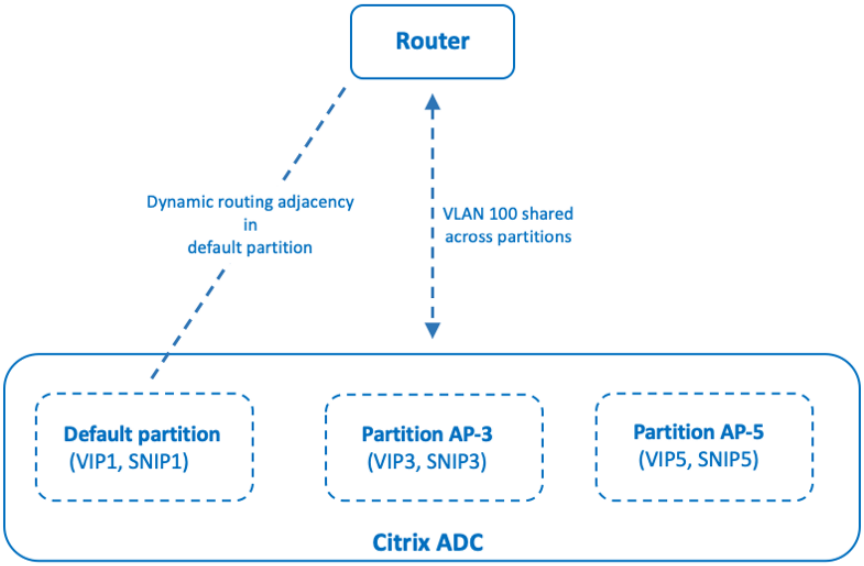
set ns partition P1  - partitionMAC 22:33:44:55:66:77
```

Lier des partitions à un VLAN partagé à l'aide de l'interface de ligne de commande

```
bind partition <partition-id> -vlan <id>

bind partition <partition-id> -vlan <id>

bind partition P1  - vlan 100

bind partition P2  - vlan 100

```



```
bind partition P3 -vlan 100

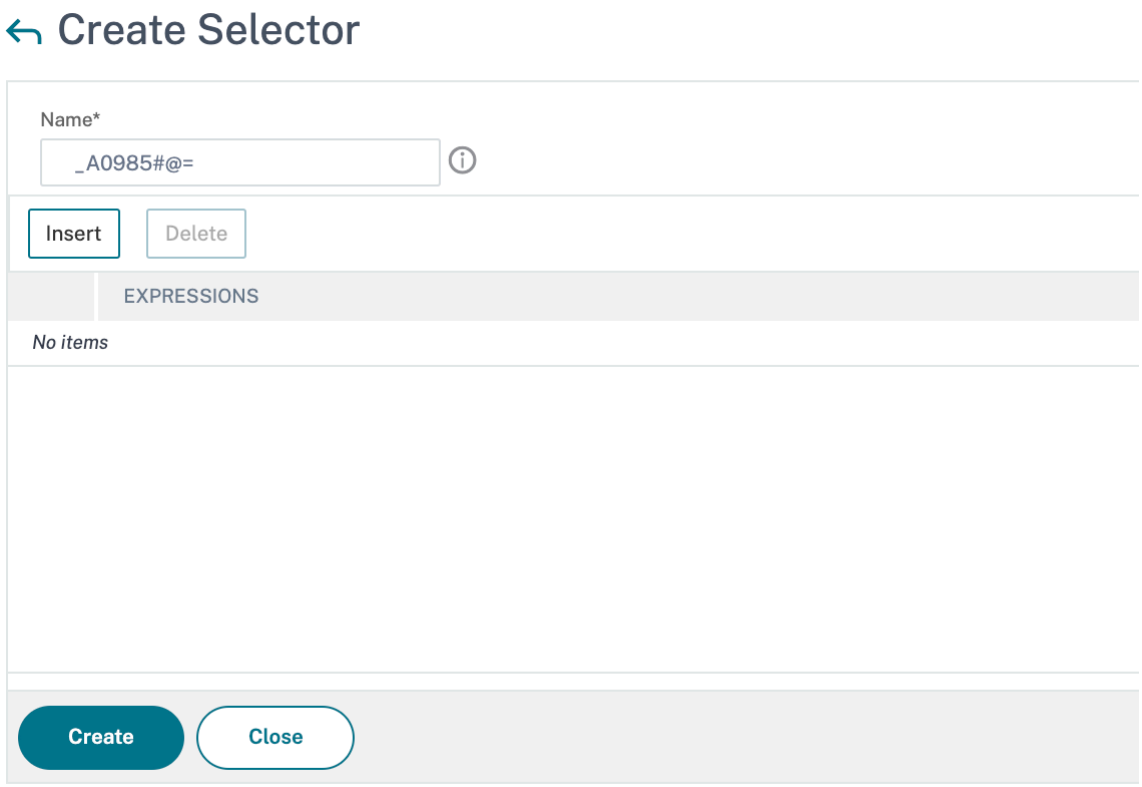
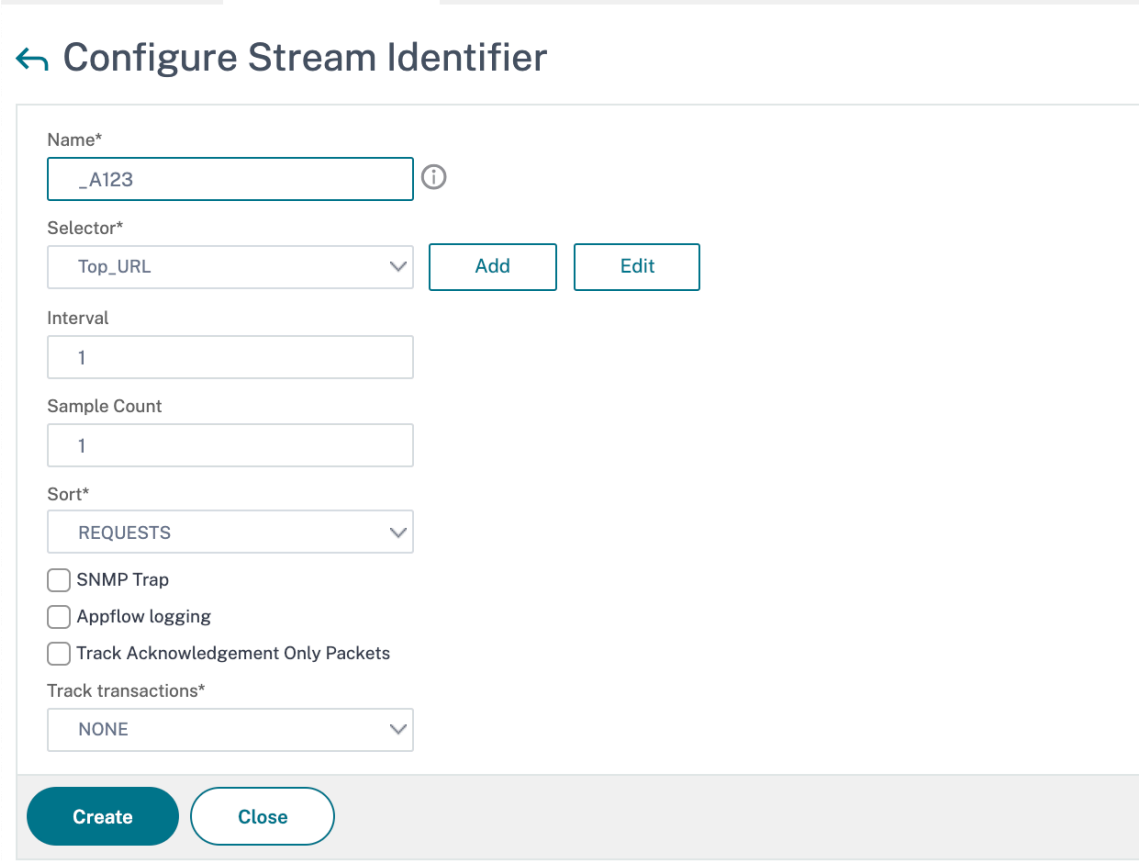
bind partition P4 -vlan 100
```

Configurer le VLAN partagé à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Configuration > Système > Réseau > VLAN**, puis sélectionnez un profil **VLAN** et cliquez sur **Modifier** pour définir le paramètre de partage de partition.
2. Sur la page **Créer un VLAN**, cochez la case **Partage des partitions** .
3. Cliquez sur **OK**, puis sur **Terminé**.

Routage dynamique sur un VLAN partagé entre les partitions d'administration

Les partitions d'administration d'une appliance Citrix ADC permettent d'héberger plusieurs locataires.

À partir de Citrix ADC version 12.1 build 51.16, un VLAN partagé dans un dispositif partitionné prend en charge le protocole de routage dynamique. Le routage peut être configuré dans des VLAN dédiés ou partagés associés aux partitions d'administration.

VLAN dédié d'une partition d'administration. Dans un VLAN dédié, le chemin de données du locataire est identifié à l'aide d'un ou de plusieurs VLAN. Il en résulte une configuration stricte et une isolation des chemins de données pour le locataire. Pour annoncer la santé d'une adresse VIP, le routage dynamique est activé dans chaque partition et la contiguïté de routage est établie par partition.



Dynamic routing over a dedicated VLAN per partition

Un VLAN partagé entre les partitions d'administration. Dans un VLAN partagé, les adresses VIP configurées dans une partition autre que celle par défaut peuvent être publiées via une seule adjacence ou un appairage formé dans la partition par défaut. Une adresse SNIP dans la partition autre que celle par défaut est utilisée comme saut suivant pour toutes les adresses VIP (configurées avec l'option **AdvertiseOnDefaultPartition) de cette partition** autre que celle par défaut. L'adresse SNIP configurée est marquée comme adresse IP de saut suivant dans les annonces de routage.

Prenons un exemple de configuration de partitions d'administration dans une appliance Citrix ADC, le VLAN 100 est partagé sur la partition par défaut et les partitions autres que celles par défaut : AP-3 et AP-5. Adresses SNIP SNIP1 est ajouté dans la partition par défaut, SNIP3 est ajouté dans AP-3 et SNIP5 est ajouté dans AP-5. SNIP1, SNIP3 et SNIP5 sont accessibles via le vlan-100. Les adresses VIP VIP1 sont ajoutées dans la partition par défaut, VIP3 dans AP-3 et VIP5 dans AP-5. VIP3 et VIP5 sont annoncés via l'adjacence ou l'appairage unique formé dans la partition par défaut.



Dynamic routing over a shared VLAN across partitions

Avant de commencer

Avant de configurer le routage dynamique sur un VLAN partagé dans une partition d'administration autre que celle par défaut, assurez-vous que :

- Le**routage dynamique est configuré sur le VLAN partagé dans la partition par défaut**. La configuration du routage dynamique sur le VLAN partagé dans la partition par défaut comprend les étapes suivantes :
  1. Activez le routage dynamique sur le VLAN partagé.
  2. Ajoutez une adresse IP SNIP avec le routage dynamique activé. Cette adresse IP SNIP est utilisée pour le routage dynamique avec l'amont.

3. Liez le sous-réseau IP SNIP au VLAN partagé.

- **Un ou plusieurs protocoles de routage dynamique sont configurés sur la partition par défaut**. Pour plus d'informations, voir Configurer les protocoles de routage dynamique.

Étapes de configuration

La configuration du routage dynamique sur un VLAN partagé dans une partition d'administration autre que celle par défaut comprend les étapes suivantes :

1. **Ajoutez une adresse IP SNIP dans la partition autre que celle par défaut**. Cette adresse IP SNIP doit se trouver dans le même sous-réseau de l'adresse IP SNIP utilisée pour le routage dynamique dans la partition par défaut.
2. **Définissez ou activez les paramètres suivants pour la publication d'une adresse VIP, dans une partition autre que celle par défaut, à l'aide du routage dynamique**.
   - Passerelle de route hôte (HostrTGW). Définissez ce paramètre sur l'adresse SNIP ajoutée à l'étape précédente.
   - Publicité sur la partition par défaut (AdvertiseOnDefaultPartition). Activez ce paramètre.

Exemple de configuration

Prenons un exemple de configuration de partition d'administration dans une appliance Citrix ADC. Une partition d'administration AP-3 autre que celle par défaut est configurée sur cette appliance. Un VLAN VLAN100 partagé est lié à AP-3. L'exemple de configuration suivant configure le routage dynamique, via VLAN100, dans AP-3.

Étapes	Exemple de configuration
Sur la partition d'administration par défaut	-
Activer le routage dynamique sur VLAN 100 partagé.	`set vlan 100 -dynamicRouting enabled`
Ajoutez l'adresse IP SNIP 192.0.2.10 avec le routage dynamique activé.Cette adresse IP SNIP est utilisée pour le routage dynamique avec l'amont.	`add ns ip 192.0.2.10 255.255.255.0 -type SNIP -dynamicRouting enabled`
Liez le sous-réseau 192.0.2.10 au VLAN 100 partagé.	`bind vlan 100 -IPAddress 192.0.2.10 255.255.255.0`
Sur la partition d'administration non par défaut AP-3	-

Étapes	Exemple de configuration
Ajouter l'adresse IP SNIP 192.0.2.30. Cette adresse IP SNIP se trouve dans le même sous-réseau que l'adresse IP SNIP 192.0.2.10 sur la partition par défaut.	`add ns ip 192.0.2.30 255.255.255.0 -type SNIP`
Pour la publicité de l'adresse VIP 203.0.113.300 utilisant le routage dynamique, activez le `advertiseOnDefaultPartition` paramètre et définissez le `hostRtGw`paramètre sur 192.0.2.30.	`set ns ip 203.0.113.300 255.255.255.255 -hostRoute enabled -advertiseOnDefaultPartition enabled -hostRtGw 192.0.2.30`

Routage dynamique d'IPv6 sur un VLAN partagé sur une partition d'administration

Les `set L3Param -ipv6DynamicRouting ENABLED` commandes `enable ns feature IPv6PT` et doivent être activées pour qu'une adresse IPv6 puisse router dynamiquement sur un VLAN partagé dans une partition d'administration. Les exemples de configurations suivants vous aident à configurer le routage dynamique d'IPv6 sur VLAN partagé.

Exemple de configuration

L'exemple de configuration suivant configure le routage dynamique, via le VLAN 100, dans AP-3.

Étapes	Exemple de configuration
Sur la partition d'administration par défaut	-
Activer le routage dynamique sur VLAN 100 partagé.	`set vlan 100 -dynamicRouting enabled`
Ajoutez l'adresse IP SNIP 2001:b:c:d 1/64 avec le routage dynamique activé. L'adresse IP SNIP est utilisée pour le routage dynamique avec l'amont.	`add ns ip6 2001:b:c:d::1/64 -type SNIP -dynamicRouting enabled`
Liez le sous-réseau 2001 : b:c:d 1/64 au VLAN 100 partagé.	`bind vlan 100 -IPAddress 2001:b:c:d::1/64`
Sur la partition d'administration non par défaut AP-3	-

Étapes	Exemple de configuration
Ajoutez l'adresse IP SNIP 2001:b:c:d 2/64. Cette adresse IP SNIP se trouve dans le même sous-réseau que l'adresse IP SNIP 2001:b:c:d 2/64 sur la partition par défaut.	`add ns ip6 2001:b:c:d::2/64 -type SNIP`
Pour la publicité de l'adresse VIP 2002 1/128 en utilisant le routage dynamique, activez le `advertiseOnDefaultPartition` paramètre et définissez le `ip6hostRtGw`paramètre sur 2001:b:c:d 2.	`set ns ip6 2002::1/128 -hostRoute enabled -advertiseOnDefaultPartition enabled -ip6hostRtGw 2001:b:c:d::2`

Le VIP présent dans la partition d'administration doit être vu sur VTYSH de la partition par défaut comme une route du noyau.

```
> switch partition default
Done

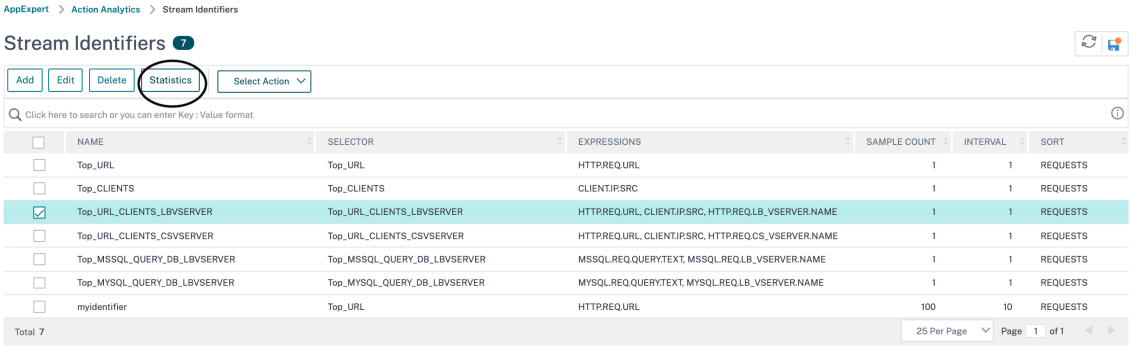
>vtysh
ns#

ns# sh ipv6 route kernel

IPv6 routing table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
   IA - OSPF inter area, E1 - OSPF external type 1,
   E2 - OSPF external type 2, I - IS-IS, B - BGP
Timers: Uptime

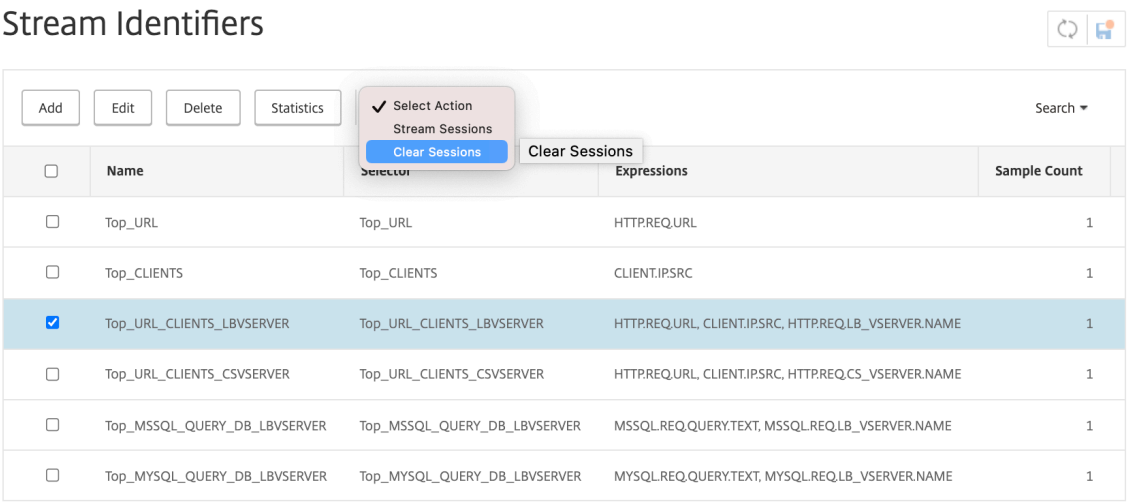
K      2002::1/128 via 2001:b:c:d::2, vlan0, 01:24:15
                                >> on Default Partition, VIP : 2002::1
    present in AP known via SNIP6 : 2001:b:c:d::2 is present in AP as a
    Kernel Route
```

Il peut être annoncé en amont en utilisant l'option « redistribuer le noyau » sous OSPFV3/BGP+ dans la partition par défaut.

```
ns# sh run router ipv6 ospf
!
router ipv6 ospf 1
redistribute kernel
!
```


VLAN partagé avec partition d'administration sur l'appliance Citrix ADC SDX

Sur l'appliance SDX, vous devez générer et configurer l'adresse PMAC à l'aide de l'interface utilisateur du service de gestion, avant d'utiliser les partitions d'administration avec des VLAN partagés. Le service de gestion vous permet de générer des adresses MAC de partition en :

- Utilisation d'une adresse MAC de base
- Spécification d'adresses MAC personnalisées
- Adresses MAC générées aléatoirement

> **Remarque**
>
> - Les adresses MAC générées aléatoirement sont utilisées pour d'autres déploiements autres que la haute disponibilité.
> - Après avoir généré les adresses MAC de partition, vous devez redémarrer l'instance Citrix ADC avant de configurer les partitions d'administration. Pour plus d'informations sur la génération d'adresses MAC de partition à partir de l'appliance SDX, consultez Génération d'adresses MAC de partition pour configurer une partition d'administration sur une instance Citrix ADC dans l'appliance SDX.

Prise en charge de VXLAN pour les partitions d'administration

August 20, 2021

Dans une appliance Citrix ADC partitionnée, similaire à la configuration d'un VLAN, vous pouvez configurer un VXLAN dans la partition par défaut. Après avoir configuré un VXLAN, vous pouvez le lier à une partition administrative ou, si un VXLAN étend un VLAN lié à une partition, l'appliance lie le VXLAN à la partition sous le même domaine de diffusion. Il est applicable pour dissocier un VLAN qui dissocie un VXLAN de la partition.

Pour plus d'informations sur le fonctionnement de VXLAN dans une appliance Citrix ADC, consultez VXLAN.

De plus, pour plus d'informations sur le fonctionnement du VLAN dans une appliance Citrix ADC partitionnée, reportez-vous à Partitionnement administrateur.

Points à retenir avant de configurer un VXLAN

Rappelez-vous les points suivants avant de configurer un VXLAN dans une appliance Citrix ADC partitionnée :

- Lorsque vous étendez un VLAN sur VXLAN, assurez-vous que VLAN est lié à la partition.

- Seul un administrateur de partition doit configurer l'IP et le routage dynamique du VXAN dans la partition administrative.

Un VXLAN partagé n'est pas pris en charge dans une appliance partitionnée. Par conséquent, un VXLAN ne peut pas être balisé sur un VLAN partagé ou vous ne pouvez pas faire d'un VLAN partagé lorsqu'il est balisé sur un VXLAN.

Configurations VXLAN supportables

Voici les configurations VXLAN supportables.

Extension de VLAN sur un VXLAN dans le même domaine de diffusion

Les étapes CLI suivantes vous aident à étendre un VLAN sur un VXLAN et de la manière opposée dans le même domaine de diffusion.

1. Ajouter un VLAN dans la partition par défaut

```
1  add vlan <id>
```

2. Étendre le VLAN sur un VXLAN dans le même domaine de diffusion.

```
1 add vxlan <vxlan id>  - vlan <id>
```

3. Configurez un homologue `vtep` pour transporter tout le trafic BUM (diffusion inconnue de multidiffusion).

> **Remarque**
>
> L' adresse `vtep` peut être une adresse de multidiffusion.

```
1 add bridgetable -mac <mac_addr> -vxlan <positive_integer> -vtep <
     ip_addr> [-vni <positive_integer>][-deviceVlan <
     positive_integer>]
```

4. Liez les adresses IP au VXLAN.

```
1 bind vxlan <id> [-srcIP <ip_addr>][-IPAddress <ip_addr|ipv6_addr
     |*> [<netmask>]]
```

5. Liez un VLAN à une partition administrative.

```
1 bind partition <partition-id> -vxlan <id>
2
3 add vlan 3000
4
```



```
5  add vxlan 3000  -vlan 10
6
7  add bridgetable  -mac 00:00:00:00:00:00  -vxlan 3000 -vtep
       10.102.58.8  -vni 11
8
9  bind vxlan 3000  -  srcIP 10.102.101.15
10
11 bind partition p1  -vlan 10
```

Prise en charge de SNMP pour les partitions d'administration

January 21, 2021

Une appliance Citrix ADC partitionnée utilise l'infrastructure SNMP pour limiter le débit de partition et surveiller les détails de l'utilisation des ressources de partition.

Interruptions SNMP pour limitation du taux de partition d'administration

Sur une appliance Citrix ADC partitionnée, une alarme PARTITION-RATE-LIMIT peut générer neuf interruptions SNMP pour notifier qu'une ressource de partition (telle que la bande passante, la connexion ou la mémoire) a atteint sa limite ou est revenue à la normale.

Les neuf interruptions SNMP suivantes sont générées lorsque :

- **partitionCONNThresholdReached**. Le nombre de connexions actives pour une partition dépasse son pourcentage de seuil élevé.
- **partitionCONNThresholdNormal**. Le nombre de connexions actives est inférieur ou égal au pourcentage de seuil normal.
- **partitionBWThresholdReached**. L'utilisation de la bande passante de la partition atteint son pourcentage de seuil élevé.
- **partitionMEMThresholdReached**. L'utilisation actuelle de la mémoire de la partition dépasse son pourcentage de seuil élevé.
- **partitionMEMThresholdNormal**. L'utilisation actuelle de la mémoire de la partition devient inférieure ou égale au pourcentage de seuil normal.
- **partitionMEMLimitExceeded.** L'utilisation actuelle de la mémoire de la partition dépasse son pourcentage limite de mémoire.
- **partitionCONNLimitExceeded**. Le nombre de connexions actives pour une partition dépasse sa limite configurée et les nouvelles connexions sont supprimées.
- **partitionCONNLimitNormal**. Le nombre de connexions actives pour une partition est inférieur à sa limite configurée et la partition peut désormais accepter une nouvelle connexion.

- **partitionBWLimitExceeded**. L'utilisation actuelle de la bande passante pour une partition a dépassé sa limite configurée.

Les valeurs de seuil des interruptions SNMP ne sont pas configurables et sont les suivantes :

- Seuil élevé = 80 % (applicable à tous les pièges à taux de partage)
- Seuil bas = 60 % (applicable à tous les pièges de limite de débit de partage)
- Limite de mémoire = 95 % (applicable uniquement pour les interruptions de mémoire de partition)

Configuration de l'alarme PARTITION-RATE-LIMIT

Pour configurer l'alarme PARTITION-RATE-LIMIT dans une partition spécifique et activer la génération des messages d'interruption SNMP.

1. Activer l'alarme PARTITION-RATE-LIMIT
2. Configurer l'alarme PARTITION-RATE-LIMIT
3. Configurer la destination d'interruption SNMP

Pour activer l'alarme PARTITION-RATE-LIMIT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
enable snmp alarm PARTITION-RATE-LIMIT

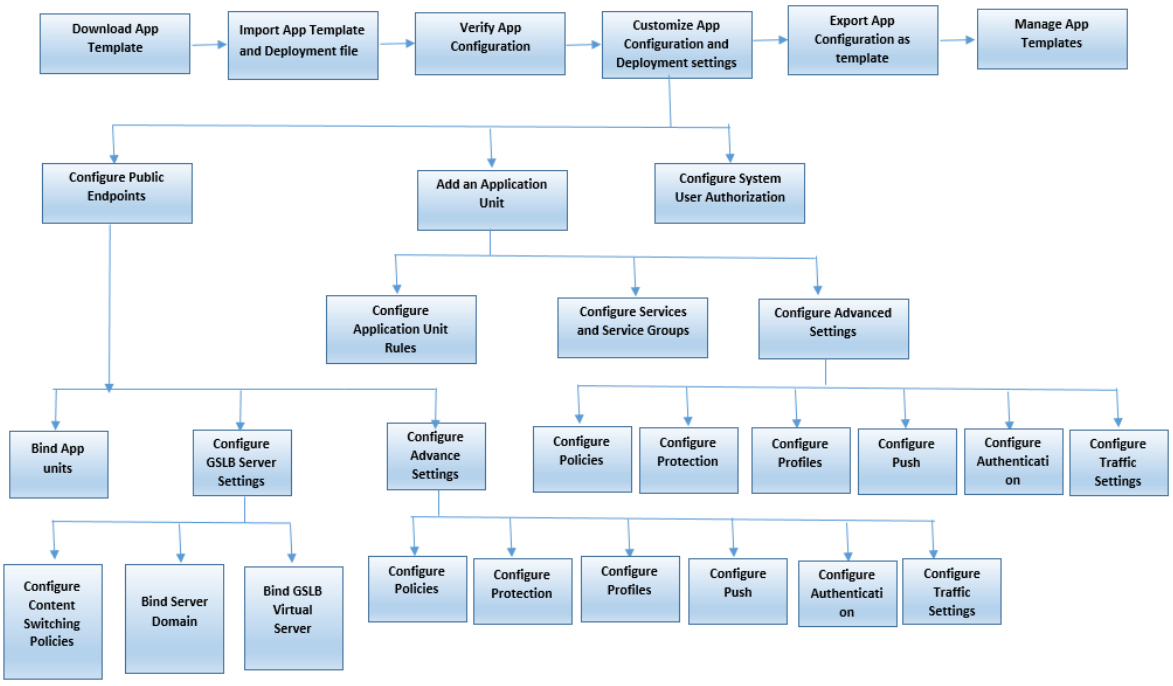
show snmp alarm PARTITION-RATE-LIMIT
```

Pour configurer l'alarme PARTITION-RATE-LIMIT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set snmp alarm PARTITION-RATE-LIMIT [-state ( ENABLED | DISABLED )] [-
    severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Pour configurer la destination des interruptions SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
add snmp trap <trapClass> <trapDestination> [-version <version>] [-td <
    positive_integer>] [-destPort <port>] [-communityName <string>] [-
    srcIP <ip_addr|ipv6_addr>] [-severity <severity>] [-allPartitions (
    ENABLED | DISABLED )]
```


Pour configurer l'alarme de limite de taux de partitionnement à l'aide de l'interface graphique

Accédez à **Système > SNMP > Alarmes**, sélectionnez Alarme **PARTITION-RATE-LIMIT** et configurez les paramètres d'alarme.

Pour configurer la destination des interruptions SNMP à l'aide de l'interface graphique

Accédez à **Système > SNMP > Interruption**, spécifiez l'adresse IP du périphérique de destination.

Surveillance SNMP pour l'utilisation des ressources de partition

Grâce à SNMP, vous pouvez surveiller les détails d'utilisation des ressources d'une partition (telles que la bande passante, la connexion et la mémoire) en temps réel sur une appliance Citrix ADC. Cela se fait en envoyant une requête SNMP (telle que SNMP GET, SNMP GET BULK, SNMP GETNEXT ou SNMP WALK) à partir du gestionnaire SNMP.

> **Remarque**
>
> Pour surveiller les ressources de partition, vous devez configurer la communauté SNMP dans la partition par défaut. Dans lequel le *PartitionTable* est conservé dans la partition par défaut et la communication SNMP est effectuée via l'adresse NSIP de l'appliance.

Considérons un scénario dans lequel un administrateur Citrix ADC souhaite connaître l'utilisation de la bande passante de la partition P1 sur l'appliance. Le gestionnaire SNMP récupère ces informations en envoyant une requête GET SNMP sur l'OID correspondant (PartitionCurrentBandWidth) à l'adresse NSIP de l'appliance. L'agent SNMP sur la partition par défaut récupère et envoie l'utilisation actuelle de la bande passante de P1 au gestionnaire SNMP via l'adresse NSIP.

Le tableau suivant répertorie les compteurs SNMP qui font partie de *PartitionTable* et sa description :

Paramètre SNMP	SNMP OID	Description
partitionName	1.3.6.1.4.1.5951.4.1.1.88.1.1	Nom de la partition
partitionCurrentBandwidth	1.3.6.1.4.1.5951.4.1.1.88.1.2	Utilisation actuelle de la bande passante de la partition.
partitionCurrentConnections	1.3.6.1.4.1.5951.4.1.1.88.1.3	Nombre actuel de connexions actives de la partition.
partitionMemoryUsagePcnt	1.3.6.1.4.1.5951.4.1.1.88.1.4	Utilisation actuelle de la mémoire (en pourcentage) de la partition.

Prise en charge des journaux d'audit pour les partitions d'administration

August 20, 2021

Sur une appliance Citrix ADC partitionnée, pour améliorer la sécurité des données, vous pouvez configurer la journalisation d'audit dans une partition administrative à l'aide de stratégies avancées. Par exemple, vous pouvez afficher les journaux (états et informations d'état) d'une partition spécifique. Il a plusieurs utilisateurs accédant à différents ensembles de fonctionnalités en fonction de leurs niveaux d'autorisation dans la partition.

Points à retenir

1. Les journaux d'audit générés à partir de la partition sont stockés sous la forme d'un fichier journal unique (/var/log/ns.log).
2. Configurez l'adresse de sous-réseau du serveur de journaux d'audit (syslog ou ns log) comme adresse IP source dans la partition pour l'envoi des messages du journal d'audit.
3. La partition par défaut utilise le NSIP comme adresse IP source pour les messages du journal d'audit par défaut.
4. Vous pouvez afficher le message du journal d'audit à l'aide de la commande « Afficher les messages d'audit ».

Pour plus d'informations sur la configuration du journal d'audit, reportez-vous à la section Configuration du dispositif NetScaler Appliance for Audit Logging.

Configuration de la journalisation d'audit dans l'appliance Citrix ADC partitionnée

Effectuez les tâches suivantes pour configurer la journalisation d'audit dans une partition administrative.

1. Configurez l'adresse IP du sous-réseau de partition. Adresse SNIP IPv4 d'une partition administrative.
2. Configurer l'action Audit-log (syslog et ns log). Une action d'audit est un ensemble d'informations qui spécifie les messages à consigner et comment enregistrer les messages sur le serveur de journaux externe.
3. Configurez les stratégies audit-log (syslog et ns log). Les stratégies de journal d'audit définissent les messages de journal pour la partition source vers le serveur de journaux syslog ou ns.
4. Liez la stratégie de journal d'audit à l'entité SysGlobal et NSGlobal. Liez une stratégie de journal d'audit à une entité globale système.
5. Consultez les statistiques du journal d'audit. Affichez les statistiques du journal d'audit et évaluez la configuration.

Configurez les éléments suivants à l'aide de la CLI

1. Créer l'adresse IP du sous-réseau d'une partition

```
add ns ip <ip address> <subnet mask>
```

2. Créer une action syslog

```
add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel
 <logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY )] [-transport ( TCP |
UDP )]
```

3. Créer une action de journal ns

```
add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel
<logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY )]
```

4. Créer des stratégies de journal d'audit syslog

```
add audit syslogpolicy syslog-pol1 true audit-action1
```

5. Créer un journal des stratégies d'audit-journal ns

```
add audit nslogpolicy nslog-pol1 true audit-action1
```

6. Lier une stratégie de journal d'audit à l'entité SyslogGlobal

```
bind audit sysloggloba l -policyName <name> -priority <priority_integer>
 -globalBindType SYSTEM_GLOBAL
```

7. Lier une stratégie de journal d'audit à l'entité NSlogGlobal

```
bind audit nsloggloba l -policyName <name> -priority <priority_integer>
-globalBindType SYSTEM_GLOBAL
```

8. Afficher les statistiques d'un journal d'audit

```
stat audit -detail
```

Exemple

```
1 add ns ip 10.102.1.1 255.255.255.0
2 add audit syslogAction syslog_action1 10.102.1.2 - logLevel
     INFORMATIONAL - dateFormat MMDDYYYY - transport UDP
3 add audit syslogpolicy syslog-pol1 true syslog_action1
4 bind audit sysloggloba l - policyName syslog-pol1 - priority 1 -
     globalBindType SYSTEM_GLOBAL
```


Stockage des journaux

Lorsque le serveur SYSLOG ou NSLOG collecte des informations de journal à partir de toutes les partitions, il est stocké en tant que messages de journal dans le fichier ns.log. Les messages du journal contiennent les informations suivantes :

- Nom de la partition.
- L'adresse IP.
- Un horodatage.
- Le type de message
- Les niveaux de journalisation prédéfinis (Critique, Erreur, Avis, Avertissement, Informations, Débogage, Alerte et Urgence)
- Les informations du message.

Afficher les adresses PMAC configurées pour la configuration de VLAN partagé

October 5, 2021

Pour utiliser une configuration de partition avec une configuration VLAN partagée, vous avez besoin d'une adresse MAC virtuelle appelée adresse MAC de partition (PMAC). La partition utilise l'adresse PMAC pour sa communication sur le VLAN partagé. Une adresse PMAC unique est configurée pour chaque partition et elle est utilisée sur tous les VLAN partagés liés à cette partition. Dans le cas d'une plate-forme non SDX (VPX ou MPX), l'adresse PMAC peut être spécifiée par l'utilisateur ou générée en interne par un dispositif Citrix ADC. Si l'adresse PMAC n'est pas spécifiée pour une partition, elle est générée en interne lorsque la partition est liée au premier VLAN partagé. Dans le cas d'une plate-forme SDX, les adresses PMAC doivent toujours être configurées à partir de l'outil SVM, puis attribuées à une partition.

Pour afficher la liste des PMAC configurés, vous pouvez utiliser la commande **Show ns PartitionMac** . La commande vous permet de vérifier les PMAC configurés via l'interface de ligne de commande Citrix ADC ou l'interface graphique. La commande affiche toutes les adresses PMAC et les partitions correspondantes (si elles sont affectées). Dans le cas d'une plate-forme non SDX, la commande affiche toutes les adresses PMAC et leurs partitions correspondantes car l'adresse PMAC est attribuée à une partition uniquement en fonction des besoins (lorsqu'une partition est liée à un VLAN partagé). Toutefois, dans le cas d'une plate-forme SDX, vous pouvez avoir des PMAC non attribués dans la liste.

Pour plus d'informations sur la façon de générer un PMAC pour la plate-forme SDX, consultez la rubrique Génération d'adresses MAC de partition .

Afficher les PMAC à l'aide de l'interface de ligne de commande Citrix ADC

À l'invite de commandes, tapez la commande suivante :

```
show ns partitionMAC
```

```
1 Partition MAC Partition Name
2
3 1) f2:0c:64:da:f6:d7
4
5 2) b4:0c:43:da:f6:d2
6
7 3) a6:e7:b2:6c:48:e0
8
9 Done
```

Afficher les adresses PMAC à l'aide de l'interface graphique Citrix ADC

1. Connectez-vous à l'appliance Citrix ADC et accédez à **Configuration > Système > Partition MAC**.
2. La page Partition MAC affiche la liste des PMACs et de ses partitions.

AppExpert

October 5, 2021

Les rubriques suivantes fournissent une référence conceptuelle et des instructions de configuration pour AppExpert et d'autres fonctionnalités de l'appliance Citrix ADC.

> **Remarque**
>
> Pour plus d'informations sur les extensions de stratégie, voir Extensions de stratégie.

- Action Analytics : collecte des statistiques d'exécution sur la base de critères prédéfinis. Lorsqu'elle est utilisée avec des stratégies, la fonctionnalité vous fournit également l'infrastructure permettant d'optimiser automatiquement le trafic en temps réel.
- Applications et modèles AppExpert : simplifiez les étapes de configuration de l'appliance Citrix® NetScaler® en utilisant des applications, des modèles d'application, des applications Citrix Gateway et des modèles d'entités.
- AppQoE : AppQoE (Application level Quality of Experience) intègre plusieurs fonctionnalités de sécurité basées sur des règles existantes de l'appliance Citrix ADC dans une seule fonctionnal-

ité intégrée qui tire parti d'un nouveau mécanisme de mise en file d'attente, une file d'attente équitable.

- Modèle d'entité : décrit comment utiliser des modèles d'entités pour configurer et configurer des entités Citrix ADC individuelles, telles qu'une stratégie ou un serveur virtuel. Un modèle d'entité fournit une spécification et un ensemble de valeurs par défaut pour l'objet.
- Appels HTTP : requête HTTP que l'appliance Citrix ADC génère et envoie à une application externe lorsque certains critères sont satisfaits lors de l'évaluation de la stratégie.
- Jeux de motifs : autorise la correspondance de chaînes pendant l'évaluation d'une stratégie avancée.
- Stratégies et expressions : règles qui déterminent les opérations que l'appliance Citrix ADC doit effectuer.
- Limitation de débit : définit la charge maximale pour une entité réseau ou une entité virtuelle donnée sur l'appliance Citrix ADC.
- Répondeur : base les réponses sur qui envoie la demande, d'où elle est envoyée et sur d'autres critères ayant des implications en matière de sécurité et de gestion du système.
- Réécriture : réécrit les informations des requêtes ou des réponses gérées par l'appliance Citrix ADC.
- String Maps : effectuez une correspondance de motifs dans toutes les fonctionnalités Citrix ADC qui utilisent la syntaxe de stratégie par défaut.

Analyse des actions

October 5, 2021

Les performances de votre site Web ou de votre application dépendent de la façon dont vous optimisez la diffusion du contenu le plus fréquemment demandé. Des techniques telles que la mise en cache et la compression permettent d'accélérer la fourniture de services aux clients, mais vous devez être en mesure d'identifier les ressources les plus demandées, puis de mettre en cache ou de compresser ces ressources. Vous pouvez identifier les ressources les plus fréquemment utilisées en agrégeant des statistiques en temps réel sur le trafic du site Web ou des applications. Des statistiques telles que la fréquence d'accès à une ressource par rapport aux autres ressources et la quantité de bande passante consommée par ces ressources vous aident à déterminer si ces ressources doivent être mises en cache ou compressées pour améliorer les performances du serveur et l'utilisation du réseau. Des statistiques telles que les temps de réponse et le nombre de connexions simultanées à l'application vous aident à déterminer si vous devez améliorer les ressources côté serveur.

Si le site Web ou l'application ne change pas fréquemment, vous pouvez utiliser des produits qui collectent des données statistiques, puis analysent manuellement les statistiques et optimisent la diffusion du contenu. Toutefois, si vous ne souhaitez pas effectuer d'optimisations manuelles ou si votre site Web ou application est de nature dynamique, vous avez besoin d'une infrastructure capable non seulement de collecter des données statistiques, mais également d'optimiser automatiquement la fourniture de ressources sur la base des statistiques. Sur l'appliance Citrix ADC, cette fonctionnalité est fournie par la fonctionnalité d'analyse des actions. La fonctionnalité fonctionne sur une seule appliance Citrix ADC et collecte des statistiques d'exécution sur la base des critères que vous définissez. Lorsqu'elle est utilisée avec les stratégies Citrix ADC, la fonctionnalité vous fournit également l'infrastructure dont vous avez besoin pour une optimisation automatique du trafic en temps réel.

Lors de la configuration de la fonctionnalité d'analyse des actions, vous spécifiez les attributs de demande pour lesquels vous souhaitez collecter des données statistiques, par exemple des URL et des méthodes HTTP, en configurant des expressions de stratégie avancées dans une entité appelée sélecteur. Ensuite, vous configurez un identificateur pour configurer des paramètres tels que l'intervalle d'échantillonnage et le nombre d'échantillons. Vous configurez également une stratégie qui permet à la solution matérielle-logicielle d'évaluer le trafic tel que spécifié par la paire sélecteur-identificateur. Enfin, vous liez la stratégie à un point de liaison pour commencer à collecter des statistiques.

La solution matérielle-logicielle vous fournit également un ensemble de sélecteurs, d'identificateurs et de stratégies de répondeur intégrés que vous pouvez utiliser pour commencer à utiliser cette fonctionnalité.

La solution matérielle-logicielle regroupe les statistiques suivantes :

- Le nombre de demandes.
- La bande passante consommée par les demandes.
- Le temps de réponse.
- Nombre de connexions simultanées.

Vous pouvez configurer la fonctionnalité pour effectuer le tri des enregistrements au moment de l'exécution sur un attribut de votre choix. Vous pouvez afficher les données statistiques à l'aide de l'interface de ligne de commande ou de l'outil Sessions en continu dans l'utilitaire de configuration.

Configurer un sélecteur

October 5, 2021

Un sélecteur est un filtre permettant d'identifier les demandes. Il comprend jusqu'à cinq expressions de stratégie avancée individuelles qui identifient les attributs de la demande tels que l'adresse IP du client et l'URL de la demande. Chaque expression est une expression de stratégie avancée non

composée et est considérée comme étant dans une relation AND avec les autres expressions. Voici quelques exemples d'expressions de sélecteur :

- `HTTP.REQ.URL`
- `CLIENT.IP.SRC`
- `HTTP.RES.BODY(1000).AFTER_STR("<string>").BEFORE_STR("<string>")"`
- `CLIENT.IP.SRC.SUBNET(24)`

Les sélecteurs sont utilisés dans les configurations de limitation de débit et d'analyse des actions. Un sélecteur est facultatif dans une configuration de limitation de débit, mais il est requis dans une configuration d'analyse des actions.

L'ordre dans lequel vous spécifiez les paramètres est significatif. Par exemple, si vous configurez une adresse IP et un domaine (dans cet ordre) dans un sélecteur, puis que vous spécifiez le domaine et l'adresse IP (dans l'ordre inverse) dans un autre sélecteur, Citrix ADC considère ces valeurs comme uniques. Cela peut entraîner le comptage deux fois de la même transaction. De plus, si plusieurs stratégies invoquent le même sélecteur, Citrix ADC peut, là encore, compter la même transaction plusieurs fois.

Si vous modifiez une expression dans un sélecteur, une erreur peut s'afficher si une stratégie qui l'appelle est liée à une nouvelle étiquette de stratégie ou à un nouveau point de liaison. Par exemple, supposons que vous créiez un sélecteur nommé MyLimitSelector1, que vous l'appeliez à partir de MyLimitID1 et que vous invoquez l'identificateur à partir d'une stratégie DNS nommée DNSRateLimit1. Si vous modifiez l'expression dans MyLimitSelector1, vous risquez de recevoir une erreur lors de la liaison de DNSRateLimit1 à un nouveau point de liaison. La solution de contournement consiste à modifier ces expressions avant de créer les stratégies qui les invoquent.

L'appliance Citrix ADC fournit des sélecteurs intégrés au format pdf pour certains des cas d'utilisation les plus courants. Reportez-vous au pdf.

Vous pouvez également configurer un sélecteur avec des expressions qui identifient les attributs de demande de votre choix. Par exemple, vous pouvez créer un enregistrement pour une demande qui arrive avec un en-tête spécifique. Pour évaluer l'en-tête, vous pouvez l' `HTTP.REQ.HEADER("<header_name>")` ajouter au sélecteur que vous souhaitez utiliser.

Pour configurer un sélecteur à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour configurer un sélecteur et vérifier la configuration :

- `add stream selector <name> <rule> ...`
- `show stream selector`

Exemple


```
> add stream selector myselector HTTP.REQ.URL CLIENT.IP.SRC
 Done
> show stream selector myselector
    Name: myselector
    Expressions:
        1) HTTP.REQ.URL
        2) CLIENT.IP.SRC
 Done
>
<!--NeedCopy-->
```

Pour modifier ou supprimer un sélecteur à l'aide de l'interface de ligne de commande :

- Pour modifier un sélecteur, tapez la commande set stream selector, le nom du sélecteur et le paramètre de règle avec les expressions. Saisissez les expressions existantes que vous souhaitez conserver, ainsi que les nouvelles expressions que vous souhaitez ajouter.
- Pour supprimer un sélecteur, tapez la commande rm stream selector et le nom du sélecteur.

Pour configurer un sélecteur à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Action Analytics** > **Selectors**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer un sélecteur, cliquez sur **Ajouter**.
   - Pour modifier un sélecteur, sélectionnez-le, puis cliquez sur **Modifier**.
3. Dans la page **Créer un sélecteur** ou **Configurer le sélecteur**, définissez les paramètres suivants :
   - Name. Pour ajouter un nom au sélecteur, entrez le nom dans le champ **Nom** . Le nom doit commencer par un caractère ASCII, alphanumérique ou de soulignement. Le nom doit contenir uniquement des caractères alphanumériques ASCII, soulignement, hachage, point, espace, deux-points, at, égal et trait d'union.
   - Expressions. Pour ajouter l'expression à la configuration du sélecteur, cliquez sur **Insérer**. Pour supprimer une expression de la configuration du sélecteur, dans la zone Expression, sélectionnez l'expression, puis cliquez sur **Supprimer**. Remarque : Dans la zone Expressions, saisissez un paramètre valide. Par exemple, saisissez HTTP. Ensuite, saisissez une période après ce paramètre. Un menu déroulant apparaît. Le contenu de ce menu fournit les mots-clés qui peuvent suivre le mot-clé initial que vous avez saisi. Pour sélectionner le mot-clé suivant dans ce préfixe d'expression, double-cliquez sur la sélection dans le menu déroulant. La zone de texte **Expressions** affiche les premier et deuxième mots-clés du préfixe d'expression, par exemple HTTP.REQ. Continuez à ajouter des composants d'expression jusqu'à ce que l'expression complète soit formée.
4. Cliquez sur **Insérer**.
5. Continuez à ajouter jusqu'à cinq expressions non composées.

6. Cliquez sur **Créer**, puis sur **Fermer**.



Configurer un identifiant de flux

August 20, 2021

Vous configurez un identificateur de flux pour spécifier les paramètres de collecte de données statistiques à partir de demandes identifiées par un sélecteur donné. Un identificateur spécifie le sélecteur à utiliser, l'intervalle de collecte des statistiques, le nombre d'échantillons et le champ sur lequel les enregistrements doivent être triés.

L'appliance Citrix ADC inclut les identificateurs de flux intégrés suivants pour les cas d'utilisation courants. Tous les identificateurs intégrés spécifient un nombre d'échantillons de 1 et un intervalle de 1 minute. En outre, ils trient les données sur l'attribut
REQUESTS. Ils ne diffèrent que par leur association avec différents sélecteurs intégrés. Chaque identifiant intégré est associé à un sélecteur intégré du même nom (par exemple, l'identifiant intégré Top_URL est associé au sélecteur intégré
Top_URL). Voici les identificateurs intégrés :

- Top_URL

- Top_CLIENTS
- Top_URL_CLIENTS_LBVSERVER
- Top_URL_CLIENTS_CSVSERVER
- Top_MSSQL_QUERY_DB_LBVSERVER
- Top_MYSQL_QUERY_DB_LBVSERVER

Pour plus d'informations sur les sélecteurs intégrés, voir Configuration d'un sélecteur.

Remarque : La longueur maximale pour stocker les résultats de chaîne des sélecteurs (par exemple, HTTP.REQ.URL) est de 60 caractères. Si la chaîne (par exemple, URL) a une longueur de 1000 caractères, dont 50 caractères suffisent pour identifier une chaîne de caractères de manière unique, utilisez une expression pour extraire uniquement les 50 caractères requis.

Vous ne pouvez pas modifier la configuration d'un identificateur intégré. Cependant, vous pouvez créer un identifiant avec la configuration de votre choix.

Pour configurer un identifiant de flux à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un identificateur de flux et vérifier la configuration :

- `add stream identifier <name> <selectorName> [-interval <positive_integer>] [-SampleCount <positive_integer>] [-sort <sort>]`
- `show stream identifier <name>`

Exemple

```
1 > add stream identifier myidentifier Top_URL -interval 10 -sampleCount
     100
2  Done
3 <!--NeedCopy-->
```

Pour configurer un identificateur de flux à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Analytics** > **Identificateurs de flux**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer un identifiant de flux, cliquez sur **Ajouter**.
   - Pour modifier un identificateur de flux, sélectionnez-le, puis cliquez sur **Modifier**.
3. Dans la page Configurer l'identificateur de flux, définissez les paramètres suivants :
   - Nom
   - Sélecteur
   - Intervalle
   - Nombre d'échantillons
   - Trier

4. Cliquez sur **Créer**, puis sur **Fermer**.



Afficher les statistiques

August 20, 2021

Vous pouvez afficher les statistiques collectées au format tabulaire dans l'interface de ligne de commande et au format graphique dans l'utilitaire de configuration.

Le tableau suivant décrit les statistiques collectées :

Statistiques	Nom de colonne dans la sortie de la commande <identifier name> stat stream identifier	Description
Nombre de demandes	**Req**	Nombre de demandes pour lesquelles des enregistrements ont été créés au cours des<interval> dernières minutes.
Bande passante consommée	**BandW**	Bande passante totale consommée par les demandes reçues au cours des<interval> dernières minutes. La bande passante totale d'une demande est la bande passante consommée par la demande et sa réponse. La valeur est arrondie à la valeur entière supérieure ou inférieure suivante. Il peut donc être légèrement différent de la valeur attendue. Par exemple, si la consommation totale de bande passante d'une demande est de 2,2 Ko. Une instance de la demande peut être affichée comme ayant consommé 2 Ko. Deux instances peuvent être affichées comme ayant consommé 4 Ko, mais trois instances peuvent être affichées comme ayant consommé 7 Ko.

Statistiques	Nom de colonne dans la sortie de la commande <identifier name> stat stream identifier	Description
Temps de réponse	**RspTime**	Temps de réponse moyen pour toutes les demandes reçues au cours des<interval> dernières minutes.
Connexions simultanées	**Conn**	Nombre total de connexions simultanées actuellement ouvertes.

Pour afficher les données statistiques collectées pour un identifiant de flux à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
stat stream identifier <name> [<pattern> ...] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-sortBy <sortBy> [<sortOrder>]
```

Exemples

Exemple 1 trie la sortie de la colonne BandW, dans l'ordre décroissant. Exemple 2 trie la sortie dans l'exemple 1, dans la colonne **Req** et dans l'ordre croissant

Exemple 1

```
1  > stat stream identifier myidentifier -sortBy BandW Descending -
       fullValues
2  Stream Session statistics
3                       Req                 BandW
4  User1                508                125924
5  User2               5020                 12692
6  User3               2025                  4316
7
8                   RspTime                  Conn
9  User1               5694                     0
10 User2                109                     0
11 User3                  3                     0
12  Done
```



```
<!--NeedCopy-->
```

Exemple 2

```
> stat stream identifier myidentifier -sortBy Req Ascending -
    fullValues
Stream Session statistics
                    Req                 BandW
User1               508                125924
User3              2025                  4316
User2              5020                 12692

                RspTime                  Conn
User1              5694                     0
User3                 3                     0
User2               109                     0
 Done
<!--NeedCopy-->
```

Pour afficher les données statistiques collectées pour un identifiant de flux à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Analytics** > **Identificateurs de flux**.
2. Sélectionnez l'identificateur de flux dont vous souhaitez afficher les sessions, puis cliquez sur Statistiques Pour plus d'informations sur la façon de regrouper la sortie sur la base des valeurs collectées pour diverses expressions de sélecteur.



Regroupement des enregistrements sur les valeurs d'attribut

August 20, 2021

Des informations statistiques telles que le nombre de fois qu'une URL particulière a été accédé globalement et par client, et le nombre total de demandes GET et POST par client peuvent fournir des

informations précieuses pour savoir si l'une de vos ressources doit être développée pour répondre à la demande ou être optimisée pour la livraison. Pour obtenir de telles statistiques, vous devez utiliser un ensemble approprié d'expressions de sélection, puis utiliser le paramètre pattern dans la commande stat stream identifier. Le regroupement est basé sur le modèle spécifié dans la commande. Le regroupement peut être effectué simultanément sur les valeurs de plusieurs expressions.

Dans l'interface de ligne de commande, vous pouvez regrouper la sortie en utilisant les modèles de votre choix. Dans l'utilitaire de configuration, le motif dépend des choix que vous effectuez lors de l'exploration vers le bas des valeurs de diverses expressions de sélecteur. Par exemple, considérez un sélecteur qui a les expressions `HTTP.REQ.URL`, `CLIENT.IP.SRC`, et `HTTP.REQ.LB_VSERVER.NAME`, dans cet ordre. La page d'accueil des statistiques affiche des icônes pour chacune de ces expressions. Si vous cliquez sur l'icône pour `CLIENT.IP.SRC`, la sortie est basée sur les motifs *?*. La sortie affiche des statistiques pour chaque adresse IP du client. Si vous cliquez sur une adresse IP, la sortie est basée sur les modèles * `<IP address>` ? et ? `<IP address>` * où `<IP address>` est l'adresse IP que vous avez sélectionnée. Dans la sortie résultante, si vous cliquez sur une URL, le modèle utilisé est `<URL> <IP address> ?`.

Pour regrouper les enregistrements sur les valeurs des expressions de sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, entrez la commande suivante pour regrouper les enregistrements sur la base d'une expression de sélecteur :

```
stat stream identifier <name> [<pattern> ...]
```

Les exemples suivants utilisent un modèle différent pour démontrer l'effet du motif sur la sortie de la commande stat stream identifier. Les expressions sélectrices sont HTTP.REQ.URL et HTTP.REQ.HEADER (« UserHeader »), dans cet ordre. Les requêtes contiennent un en-tête personnalisé dont le nom est UserHeader. Notez que dans les exemples, une valeur statistique donnée change selon le regroupement, mais la somme totale des valeurs pour un champ donné reste la même.

Exemple 1

Dans la commande suivante, le modèle utilisé est ? ?. L'appliance regroupe la sortie sur les valeurs collectées pour les deux expressions de sélecteur. Les en-têtes de ligne sont constitués des valeurs d'expression séparées par un point d'interrogation (?). La ligne avec l'en-tête /mysite/mypage1.html? Ed affiche les statistiques des requêtes faites par l'utilisateur Ed pour l'URL /mysite/mypage1.html.

> **Remarque :**
>
> Vous devez vous assurer de taper la commande suivante avec "?" au lieu de "?". Par exemple, Si sélecteur utilise une expression - client.ip.src et client.tcp.srcport. La commande Stat pour

> regrouper la sortie sur les valeurs collectées pour le sélecteur est 'stat stream identifier myidentifier ? ? -fullValues' comme indiqué ci-dessous.

```
> stat stream identifier myidentifier ? ? -fullValues
Stream Session statistics
                                          Req                  BandW
/mysite/mypage2.html?Grace                  1                   2553
/mysite/mypage1.html?Grace                  2                      4
/mysite/mypage1.html?Ed                     8                     16
/mysite/mypage2.html?Joe                    1                   2554
/mysite/mypage1.html?Joe                    5                     10
/mysite/?Joe                                1                      4

                                       RspTime                  Conn
/mysite/mypage2.html?Grace                  0                      0
/mysite/mypage1.html?Grace                  0                      0
/mysite/mypage1.html?Ed                     0                      0
/mysite/mypage2.html?Joe                    0                      0
/mysite/mypage1.html?Joe                    0                      0
/mysite/?Joe                                6                      0
 Done
<!--NeedCopy-->
```

Exemple 2

Dans la commande suivante, le motif utilisé est * ?. L'appliance regroupe la sortie sur les valeurs accumulées pour la deuxième expression HTTP.REQ.HEADER (« userHeader »). Les lignes affichent des statistiques pour toutes les demandes faites par les utilisateurs Grace, Ed et Joe.

> **Remarque :**
>
> Assurez-vous de taper la commande suivante avec "?" au lieu de "?".

```
> stat stream identifier myidentifier * ?
Stream Session statistics
                  Req    BandW  RspTime     Conn
Grace               3     2557        0        0
Ed                  8       16        0        0
Joe                 7     2568        6        0
 Done
<!--NeedCopy-->
```

Exemple 3

Dans la commande suivante, le modèle utilisé est ? *, qui est le modèle par défaut. La sortie est groupée sur les valeurs collectées pour la première expression de sélecteur. Chaque ligne affiche des statistiques pour une URL.

> **Remarque :**
>
> Assurez-vous de taper la commande suivante avec “?” au lieu de “?”.

```
> stat stream identifier myidentifier ? * -fullValues
Stream Session statistics

                                        Req                 BandW
/mysite/mypage2.html                      2                  5107
/mysite/mypage1.html                     15                    30
/mysite/                                  1                     4

                                    RspTime                  Conn
/mysite/mypage2.html                      0                     0
/mysite/mypage1.html                      0                     0
/mysite/                                  6                     0
 Done
<!--NeedCopy-->
```

Exemple 4

Dans la commande suivante, le modèle utilisé est `* *`. L’appliance affiche un ensemble de statistiques collectives pour toutes les demandes reçues, sans titre de ligne.

```
> stat stream identifier myidentifier * *
Stream Session statistics
                  Req    BandW  RspTime     Conn
                   18     5141        6        0
 Done
<!--NeedCopy-->
```

Exemple 5

Dans la commande suivante, le modèle est /mysite/mypage1.html *. L’appliance affiche un ensemble de statistiques collectives pour toutes les demandes reçues pour l’URL /mysite/mypage1.html, sans titre de ligne.

```
> stat stream identifier myidentifier /mysite/mypage1.html *
Stream Session statistics
                  Req    BandW  RspTime     Conn
                   15       30        0        0
 Done
<!--NeedCopy-->
```


Effacement d'une session de flux

August 20, 2021

Vous pouvez vider tous les enregistrements qui ont été accumulés pour un identifiant de flux.

Pour effacer une session de flux à l'aide de l'interface de ligne de commande

À l'invite de commandes, entrez les commandes suivantes pour effacer une session de flux et vérifier les résultats :

- session de flux effacer
- identificateur de flux stat

Exemple

Cet exemple utilise d'abord la commande stat stream identifier, de sorte qu'une comparaison peut être effectuée avec la commande stat stream identifier utilisée pour vérifier le résultat de la commande clear stream session.

```
1  >stat stream identifier myidentifier
2  Stream Session statistics
3                   Req    BandW  RspTime     Conn
4  /aed....html       2        0        0        0
5  /                636      303       12        0
6   Done
7  >clear stream session myidentifier
8   Done
9  >stat stream identifier myidentifier
10  Done
11 <!--NeedCopy-->
```

Pour effacer une session de flux à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Analytics** > **Identificateurs de flux**.
2. Sélectionnez l'identificateur de flux dont vous souhaitez effacer les sessions, puis cliquez sur **Effacer les sessions**.



Configurer la stratégie d'optimisation du trafic

October 5, 2021

Pour que la paire sélecteur-identificateur de votre configuration d'analyse des actions entre en vigueur, vous devez associer la paire au point du flux de trafic auquel vous souhaitez collecter des statistiques. Vous pouvez le faire en configurant une stratégie avancée et en référençant l'identificateur de flux à partir de la règle de stratégie. Vous pouvez utiliser des stratégies de compression, des stratégies de mise en cache, des stratégies de réécriture, des stratégies de pare-feu d'application, des stratégies de répondeur et toute autre stratégie dont l'action est basée sur une expression booléenne.

La fonctionnalité d'analyse des actions introduit un ensemble d'expressions de stratégie avancées et de fonctions de collecte et d'évaluation des données. L'expression `ANALYTICS.STREAM(<identifier_name>)` est utilisée pour référencer l'identificateur que vous souhaitez utiliser. L'expression COLLECT_STATS est utilisée pour collecter des données statistiques. Des fonctions telles que `IS_TOP(<uint>)` et `IS_TOP_FREQUENTS(<uint>)` sont utilisées pour prendre des décisions automatiques et en temps réel en matière d'optimisation du trafic.

- **IS_TOP (<number>).** Trouve si un objet donné se trouve en haut <number>des éléments. Par exemple, l'élément figure parmi les 10 premiers éléments. Lorsque plusieurs éléments sont comptés, ils sont considérés comme étant de nature similaire. La fonction de tri doit être activée pour éviter une condition undef.
- **IS_TOP_FREQUENTS(<frequency>).** Recherche si un objet donné se trouve au top de <frequency> des éléments qui se trouvent dans les éléments supérieurs. Par exemple, l'élément se situe parmi les 50 % les plus importants de tous les éléments les plus importants

maintenus. Les éléments ayant les mêmes valeurs sont considérés comme similaires par nature. La fonction de tri doit être activée pour éviter une condition undef.

C'est la configuration de votre stratégie qui détermine si l'appliance Citrix ADC doit uniquement collecter des données à partir du trafic ou effectuer une action. Si la solution matérielle-logicielle doit uniquement collecter des données statistiques, vous pouvez configurer une stratégie avec la règle `ANALYTICS.STREAM(<identifier_name>).COLLECT_STATS` et l'action NOOP. La stratégie NOOP doit être la stratégie ayant la priorité la plus élevée au point de liaison. Cette stratégie est suffisante si vous ne collectez que des statistiques. Les décisions d'optimisation du trafic, telles que les éléments à compresser ou à mettre en cache, doivent être basées sur une évaluation manuelle et périodique des données statistiques.

Si, en plus de collecter des statistiques, l'appliance doit également effectuer une action sur le trafic, vous devez configurer le paramètre GoToPriorityExpression de la stratégie NOOP de sorte qu'une autre stratégie comportant la règle et l'action souhaitées soit évaluée ultérieurement. Cette deuxième stratégie doit comporter une règle commençant par le `ANALYTICS.STREAM(<identifier_name>)` préfixe et une fonction qui évalue les données.

Voici un exemple de deux stratégies de répondeur configurées et liées globalement. La stratégie responder_stat_collection permet à la solution matérielle-logicielle de collecter des statistiques basées sur l'identificateur myidentifier. La stratégie responder_notify évalue les données collectées.

Exemple

```
> add responder action send_notification respondwith '"You are in the
   Top 10 list for bandwidth consumption"'
 Done
> add responder policy responder_stat_collection' ANALYTICS.STREAM("
   myidentifier").COLLECT_STATS' NOOP
Done
> add responder policy responder_notify 'ANALYTICS.STREAM("myidentifier
   ").BANDWIDTH.IS_TOP(10)' send_notification
 Done
> bind responder global responder_stat_collection 10 NEXT
 Done
> bind responder global responder_notify 20 END
 Done
<!--NeedCopy-->
```


Comment limiter la consommation de bande passante par utilisateur ou périphérique client

August 20, 2021

Votre site Web, application ou service d'hébergement de fichiers dispose de ressources réseau et serveur limitées pour servir tous ses utilisateurs. L'une des ressources les plus importantes est la bande passante. Une consommation importante de bande passante par seulement un sous-ensemble de la base d'utilisateurs peut entraîner une congestion du réseau et une réduction de la disponibilité des ressources pour les autres utilisateurs. Pour éviter la congestion réseau, vous devrez peut-être limiter la consommation de bande passante d'un client en utilisant des techniques de déni de service temporaires telles que la réponse à une demande client avec une page HTML si elle a dépassé une valeur de bande passante préconfigurée sur une période de temps fixe précédant la demande.

En général, vous pouvez réguler la consommation de bande passante par appareil client ou par utilisateur. Ce cas d'utilisation montre comment vous pouvez limiter la consommation de bande passante par client à 100 Mo sur une période d'une heure. Le cas d'utilisation montre également comment vous pouvez réguler la consommation de bande passante par utilisateur à 100 Mo sur une période d'une heure, à l'aide d'un en-tête personnalisé qui fournit le nom d'utilisateur. Dans les deux cas, le suivi de la consommation de bande passante sur une période de déplacement d'une heure est réalisé en définissant le paramètre d'intervalle dans l'identificateur de flux sur 60 minutes. Les cas d'utilisation montrent également comment importer une page HTML à envoyer à un client qui a dépassé la limite. L'importation d'une page HTML simplifie non seulement la configuration de l'action du répondeur dans ces cas d'utilisation, mais simplifie également la configuration de toutes les actions du répondeur qui nécessitent la même réponse.

Pour limiter la consommation de bande passante par utilisateur ou par périphérique client à l'aide de l'interface de ligne de commande

Dans l'interface de ligne de commande, effectuez les tâches suivantes pour configurer l'analyse des actions afin de limiter la consommation de bande passante d'un client ou d'un utilisateur. Chaque étape comprend des exemples de commandes et leur sortie.

1. **Configurez votre configuration d'équilibrage de charge.** Configurez le serveur virtuel d'équilibrage de charge mysitevip, puis configurez tous les services dont vous avez besoin. Liez les services au serveur virtuel. L'exemple suivant crée dix services et lie les services à mysitevip.

```
> add lb vserver mysitevip HTTP 192.0.2.17 80
 Done
> add service service[1-10] 192.0.2.[240-249] HTTP 80
service "service1" added
service "service2" added
```



```
service "service3" added
.
.
.
service "service10" added
 Done
> bind lb vserver vserver1 service[1-10]
service "service1" bound
service "service2" bound
service "service3" bound
.
.
.
service "service10" bound
 Done
<!--NeedCopy-->
```

2. **Configurez le sélecteur de flux.** Configurez l'un des sélecteurs de flux suivants :

   - Pour limiter la consommation de bande passante par client, configurez un sélecteur de flux qui identifie l'adresse IP du client.

     ```
     > add stream selector myselector CLIENT.IP.SRC
      Done
     <!--NeedCopy-->
     ```

   - Pour limiter la consommation de bande passante par utilisateur sur la base de la valeur d'un en-tête de demande qui fournit le nom d'utilisateur, configurez un sélecteur de flux qui identifie l'en-tête. Dans l'exemple suivant, le nom de l'en-tête est UserHeader.

     ```
     > add stream selector myselector HTTP.REQ.HEADER( "UserHeader
         " )
      Done
     <!--NeedCopy-->
     ```

3. **Configurez un identifiant de flux.** Configurez un identificateur de flux qui utilise le sélecteur de flux. Définissez le paramètre d'intervalle sur 60 minutes.

   ```
   > add stream identifier myidentifier myselector -interval 60 -
       sampleCount 1 -sort BANDWIDTH
    Done
   <!--NeedCopy-->
   ```

4. **Configurez l'action du répondeur.** Importez la page HTML que vous souhaitez envoyer aux utilisateurs ou aux clients qui ont dépassé la limite de consommation de bande passante, puis

utilisez la page dans l'action répondeur crossed_limits.

```
> import responder htmlpage http://.1.1.1/stdpages/wait.html
   crossed-limits.html
This operation may take some time, Please wait...

 Done
> add responder action crossed_limits respondwithhtmlpage crossed-
   limits.html
 Done
<!--NeedCopy-->
```

5. **Configurez les stratégies de répondeur.** Configurez la stratégie de répondeur myrespol1 avec la règle ANALYTICS.STREAM (« myidentifier ») .COLLECT_STATS et l'action NOOP. Ensuite, configurez la stratégie myrespol2 pour déterminer si un client ou un utilisateur a dépassé la limite de 100 Mo. La stratégie myrespol2 est configurée avec l'action du répondeur crossed_limits.

```
> add responder policy myrespol1 'ANALYTICS.STREAM("myidentifier")
   .COLLECT_STATS' NOOP
 Done
> add responder policy myrespol2 'ANALYTICS.STREAM("myidentifier")
   .BANDWIDTH.GT(104857600)' crossed_limits
 Done
<!--NeedCopy-->
```

6. **Liez les stratégies du répondeur au serveur virtuel d'équilibrage de charge.** La stratégie myrespol1, qui ne recueille que des données statistiques, doit avoir la priorité la plus élevée et une expression GOTO de NEXT.

```
> bind lb vserver mysitevip -policyName myrespol1 -priority 1 -
   gotoPriorityExpression NEXT
 Done
> bind lb vserver mysitevip -policyName myrespol2 -priority 2 -
   gotoPriorityExpression END
 Done
<!--NeedCopy-->
```

7. **Testez la configuration.** Testez la configuration en envoyant des requêtes HTTP de test, provenant de plusieurs clients ou utilisateurs, au serveur virtuel d'équilibrage de charge et en utilisant la commande stat stream identifier pour afficher les statistiques collectées pour l'identificateur spécifié. La sortie suivante affiche des statistiques pour les clients.

```
> stat stream identifier myidentifier -sortBy BandW  - fullValues
Stream Session statistics
```



```
3                                   Req             BandW
4  192.0.2.30                       5000            3761
5  192.0.2.31                       29              2602
6  192.0.2.32                       25              51
7
8                                   RspTime         Conn
9  192.0.2.30                       2               0
10 192.0.2.31                       0               0
11 192.0.2.32                       0               0
12  Done
13 >
14 <!--NeedCopy-->
```

Applications et modèles AppExpert

October 5, 2021

> **Avertissement**
>
> La fonctionnalité du modèle d'application est obsolète à partir de Citrix ADC 13.0 build 82.x et Citrix vous recommande d'utiliser les livres de style. Pour plus d'informations, consultez la rubrique Livres de style .

Une application AppExpert est un ensemble de configurations que vous avez configurées sur l'appliance Citrix ADC. La gestion des applications AppExpert est simplifiée par une interface graphique (GUI) qui vous permet de spécifier des sous-ensembles de trafic d'applications et un ensemble distinct de stratégies de sécurité et d'optimisation pour le traitement de chaque sous-ensemble de trafic. En outre, il consolide les étapes de déploiement dans une seule vue, ce qui vous permet de configurer rapidement les adresses IP cibles pour les clients et de spécifier des serveurs hôtes.

Pour commencer à utiliser une application AppExpert, vous devez d'abord obtenir le modèle d'application approprié et importer le modèle dans l'appliance Citrix ADC. Une fois l'application AppExpert configurée, vous devez vérifier que l'application fonctionne correctement. Si nécessaire, vous pouvez personnaliser la configuration en fonction de vos besoins.

Périodiquement, vous pouvez vérifier et surveiller la configuration en affichant les compteurs de divers composants d'application, statistiques et Application Visualizer. Vous pouvez également configurer des stratégies d'authentification, d'autorisation et d'audit (authentification, autorisation et audit) pour l'application.

Terminologie de l'application AppExpert

Voici les termes utilisés dans la fonctionnalité AppExpert AppExpert et les descriptions des entités pour lesquelles ils sont utilisés :

Point de terminaison public. Combinaison d'adresse IP et de port au niveau de laquelle l'appliance Citrix ADC reçoit les demandes des clients pour l'application Web associée. Un point de terminaison public peut être configuré pour recevoir du trafic HTTP ou HTTP sécurisé (HTTPS). Toutes les demandes du client pour l'application Web doivent être envoyées à un point de terminaison public. Il est possible d'attribuer plusieurs points de terminaison à une application AppExpert. Vous configurez les points de terminaison publics après avoir importé un modèle.

Unité d'application. Entité d'application AppExpert qui traite un sous-ensemble du trafic des applications Web et équilibre la charge d'un ensemble de services qui hébergent le contenu associé. Le sous-ensemble du trafic qu'une unité d'application doit gérer est défini par une règle. Chaque unité d'application définit également son propre ensemble de stratégies d'optimisation du trafic et de sécurité pour les demandes et les réponses qu'elle gère. Les services Citrix ADC associés à ces stratégies sont la compression, la mise en cache, la réécriture, le répondeur et le pare-feu d'application.

Par défaut, chaque application AppExpert comportant au moins une unité d'application inclut une unité d'application par défaut, qui ne peut pas être supprimée. L'unité d'application par défaut n'est pas associée à une règle d'identification des demandes et est toujours placée en dernier dans l'ordre des unités d'application. Il définit un ensemble de stratégies pour le traitement de toute demande qui ne correspond pas aux règles configurées pour les autres unités d'application. Ainsi, toutes les demandes des clients sont traitées.

Les unités d'application et leurs règles, stratégies et actions associées sont incluses dans les modèles d'application AppExpert.

Service. Combinaison de l'adresse IP du serveur qui héberge l'instance d'application Web et du port auquel l'application est mappée sur le serveur, au format `\<IP address\>:\<Port\>`. Une application Web qui répond à de nombreuses demandes est hébergée sur plusieurs serveurs. Chaque serveur héberge une instance de l'application Web et chaque instance de l'application Web est représentée par un service sur l'appliance Citrix ADC. Les services sont spécifiques au déploiement et ne sont donc pas inclus dans les modèles. Vous devez configurer les services après avoir importé un modèle.

Règle de l'unité d'application. Expression de stratégie avancée qui définit les caractéristiques d'un sous-ensemble de trafic pour une unité d'application. L'exemple de règle suivant est une expression de stratégie avancée qui identifie un sous-ensemble de trafic composé de quatre types d'images :

```
HTTP.REQ.URL.SUFFIX.EQ("bmp")|| HTTP.REQ.URL.SUFFIX.EQ("gif")|| HTTP.REQ.
URL.SUFFIX.EQ("png")|| HTTP.REQ.URL.SUFFIX.EQ("jpg")
```

Pour plus d'informations sur les expressions de stratégie avancées, consultez la section Stratégies et expressions.

Sous-ensemble de trafic. Ensemble de demandes client qui nécessitent un ensemble commun de stratégies d'optimisation du trafic et de sécurité. Un sous-ensemble de trafic est géré par une unité d'application et est défini par une règle.

Fonctionnement de l'application AppExpert

January 21, 2021

Lorsque le point de terminaison reçoit une demande client, l'appliance Citrix ADC évalue la demande par rapport à la règle configurée pour l'unité d'application la plus haute. Si la demande satisfait à cette règle, la demande est traitée par les stratégies configurées pour l'unité d'application, puis transférée à un service. Le choix du service dépend des services configurés pour l'application et des paramètres tels que l'algorithme d'équilibrage de charge et la méthode de persistance configurés pour l'unité d'application.

Si la demande ne satisfait pas à la règle, la demande est évaluée par rapport à la règle de l'unité d'application la plus haute suivante. Dans cet ordre, la demande est évaluée par rapport à chaque règle d'unité d'application jusqu'à ce que la demande satisfasse à une règle. Si la demande ne satisfait à aucune des règles configurées, elle est traitée par l'unité d'application par défaut, qui est toujours la dernière unité d'application.

Vous pouvez configurer plusieurs points de terminaison publics pour une application AppExpert. Dans une telle configuration, par défaut, chaque unité d'application traite les demandes reçues par tous les points de terminaison publics et équilibre la charge tous les services configurés pour l'application. Toutefois, vous pouvez spécifier qu'une unité d'application traite uniquement le trafic à partir d'un sous-ensemble des points de terminaison publics et n'équilibre la charge qu'un sous-ensemble des services configurés pour l'application AppExpert.

Le diagramme de flux suivant illustre la séquence de flux AppExpert Application pour l'utilisation d'un modèle d'application intégré.



Si vous préférez créer une application personnalisée sans utiliser de modèle, procédez comme suit :

1. Créez une application personnalisée.
2. Configurez les paramètres d'application et de déploiement.
3. Exportez la configuration vers de nouveaux fichiers de modèle (facultatif).
4. Importer les fichiers de modèle vers d'autres appliances Citrix ADC nécessitant une configuration d'application AppExpert similaire

Premiers pas avec AppExpert

August 20, 2021

Pour commencer à utiliser une application AppExpert, vous devez d'abord obtenir un modèle d'application et l'importer dans une appliance Citrix ADC. Une fois l'application AppExpert configurée, vous devez vérifier que l'application fonctionne correctement. Si nécessaire, vous pouvez personnaliser la configuration en fonction de vos besoins.

Périodiquement, vous pouvez vérifier et surveiller la configuration en affichant les compteurs d'accès des différents composants de l'application. Vous pouvez également configurer des stratégies d'authentification, d'autorisation et d'audit (AAA) pour l'application.

Le processus de mise en place d'une application peut se faire de deux façons :

- Utilisation d'un modèle d'application prédéfini

- Création d'une application personnalisée sans utiliser de modèle.

Si vous préférez configurer l'application à l'aide d'un modèle d'application prédéfini, procédez comme suit :

1. Télécharger un modèle d'application.
2. Importez des fichiers de modèle dans l'appliance Citrix ADC.
3. Vérifiez la configuration de l'application.
4. Configurez les paramètres d'application et de déploiement.
5. Exportez la configuration vers de nouveaux fichiers de modèle (facultatif).
6. Importez les fichiers de modèle vers d'autres appliances Citrix ADC qui nécessitent une configuration d'application AppExpert similaire.

Les didacticiels vidéo de Citrix ADC vous permettent de comprendre facilement et facilement les fonctionnalités de Citrix ADC. Regardez lahttps://www.youtube.com/watch?v=aqayflvCR_0 vidéo pour savoir comment configurer une application à l'aide du modèle AppExpert Application.

Téléchargement d'un modèle d'application

August 20, 2021

Remarque : Citrix ne prend plus en charge les modèles d'applications AppExpert et ne permet pas de télécharger une copie. Si vous utilisez Citrix ADC version 13.0 ou antérieure, vous pouvez contacter le support Citrix pour obtenir une copie d'un modèle d'application.

Pour configurer l'application AppExpert, vous devez d'abord télécharger un modèle d'application depuis le site Web de la communauté Citrix sur http://community.citrix.com votre ordinateur local ou sur l'appliance Citrix ADC. Les modèles d'application sont importés et exportés, ce qui vous permet de partager facilement des configurations spécifiques à une application au sein d'une organisation ou d'une organisation à l'autre. Un modèle d'application comprend l'ensemble d'entités suivant :

1. Composants d'applications (par exemple, pages Web, fichiers, archives et services Web)
2. Entités de gestion du trafic (par exemple, adresses IP du serveur virtuel et algorithmes d'équilibrage de charge associés, et paramètres de déchargement SSL) pour les composants de l'application.
3. Stratégies Citrix ADC utilisées pour optimiser le trafic de l'application.

Remarque : Les modèles d'application sont disponibles dans différentes versions pour configurer différents types d'appliances Citrix ADC.

Importation d'un modèle d'application

August 20, 2021

Pour Citrix ADC version 9.3 ou ultérieure, chaque modèle AppExpert comporte deux fichiers XML : un fichier modèle et un fichier de déploiement. Vous devez importer les deux fichiers de votre ordinateur local vers une appliance Citrix ADC. Vous pouvez soit importer les fichiers de modèle de votre ordinateur dans le répertoire des modèles d'application AppExpert dans l'appliance Citrix ADC, soit télécharger des fichiers dans une appliance Citrix ADC, puis les importer à partir de l'appliance.

Remarque : lorsque vous importez un modèle à partir d'une appliance, vous devez indiquer la valeur variable disponible dans le modèle. Par défaut, la valeur préconfigurée est affichée/`fr-fr/citrix-adc/current-release/appexpert/appexpert-application-templates/creating-managing-templates/citrix-adc-application-template-deployment-files.html`

Après avoir importé les fichiers de modèle, les informations de configuration et de déploiement de l'application remplissent automatiquement l'application cible. L'appliance importe toute la configuration à partir des fichiers de modèle via l'API NITRO. Si vous n'importez pas le fichier de déploiement, le système génère une application remplie avec la configuration du serveur virtuel de commutation de contenu. Pour plus d'informations sur le format des modèles d'application et des fichiers de déploiement, voir Présentation des modèles d'application Citrix ADC et des fichiers de déploiement.

Lorsque vous importez un modèle, si vous n'incluez pas de fichier de déploiement, vous devez configurer les points de terminaison publics dans l'application que le système génère automatiquement à partir du modèle. Un point de terminaison pour HTTP et un autre point de terminaison pour HTTPS. Lors de la configuration d'un point de terminaison public de type HTTPS, assurez-vous d'activer la fonctionnalité SSL, de lier le certificat serveur et d'inclure les fichiers de certificat serveur et de clé de certificat.

Pour plus d'informations sur la configuration des points de terminaison après avoir importé un modèle, voir Configuration des points de terminaison publics.

Pour importer des fichiers de modèle d'application AppExpert vers une appliance Citrix ADC à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez sur **Importer le modèle**.
3. Dans la page **Importer**, définissez les paramètres suivants :
   a) Nom de la demande (obligatoire)
   b) Fichier modèle (obligatoire)
   c) Utiliser le fichier de déploiement
4. Cliquez sur **Continuer** pour remplir automatiquement les informations de configuration et de déploiement de l'application dans une application.

Les didacticiels vidéo de Citrix ADC vous permettent de comprendre facilement et simplement les fonctionnalités de Citrix ADC. Regardez lahttps://www.youtube.com/watch?v=AR9TwSD9uJM vidéo pour savoir comment importer un modèle d'application.

Vérification et test de la configuration de l'application

January 21, 2021

L'interface graphique inclut des icônes qui indiquent les états des entités dans l'application AppExpert. Ces icônes sont affichées pour les applications et les unités d'application et sont basées sur les vérifications d'intégrité effectuées périodiquement par l'appliance Citrix ADC sur les services et les entités. Le tableau suivant répertorie les icônes et décrit leur signification.

Icône	Entité	Indique que
	Application	Au moins un point de terminaison public est en place. L'application acceptera les demandes client des points de terminaison publics qui sont en service.
	Unité d'application	L'unité d'application est en place. L'unité d'application est en service lorsqu'au moins un service ou un groupe de services est en service.
	Application	Le point de terminaison public est hors service (désactivé). Cet indicateur s'affiche lorsqu'un seul point de terminaison public est configuré pour l'application AppExpert.

Icône	Entité	Indique que
	Application	Tous les points de terminaison configurés pour l'application sont hors service. Cet indicateur s'affiche uniquement lorsque plusieurs points de terminaison sont configurés pour l'application.
	Unité d'application	Tous les services configurés pour l'unité d'application sont en panne.

Vous devez vous assurer que les icônes de chaque application et de ses unités d'application sont vertes en tout temps. Si l'icône affichée pour une application n'est pas verte, vérifiez que vous avez correctement configuré les points de terminaison publics. Si l'icône affichée pour une unité d'application n'est pas verte, vérifiez que les services sont correctement configurés. Toutefois, notez qu'un indicateur vert ne signifie pas que l'état de toutes les entités associées est UP. Cela signifie seulement que l'application dispose de ressources suffisantes (points de terminaison et services) pour répondre aux demandes des clients. Pour vérifier que l'état de toutes les entités associées est UP, vérifiez l'intégrité de toutes les entités sur la page de statistiques de l'application.

Personnalisation de la configuration

January 21, 2021

Après avoir vérifié que l'application AppExpert fonctionne correctement, vous pouvez personnaliser la configuration en fonction de vos besoins.

Après avoir vérifié que la configuration de l'application AppExpert fonctionne correctement, vous pouvez configurer l'application et les paramètres de déploiement en fonction de vos besoins. Lorsque vous importez un modèle d'application et un fichier de déploiement, le système remplit automatiquement l'application cible avec les paramètres de configuration disponibles (tels que les unités d'application, les règles d'unité d'application, les stratégies, les paramètres de persistance, les méthodes d'équilibrage de charge, les profils et les paramètres de trafic). Dans cette application, vous pouvez configurer des paramètres de déploiement tels que les points de terminaison publics, les services et les groupes de services pour chaque sous-ensemble de trafic. Si vous souhaitez que l'application

AppExpert gère un sous-ensemble de trafic qui n'est pas inclus dans le modèle, vous pouvez ajouter une unité d'application pour un sous-ensemble de trafic ou modifier l'unité d'application existante. Après avoir personnalisé la configuration, vous pouvez également spécifier l'ordre d'évaluation pour chaque sous-ensemble de trafic géré par l'application.

La configuration d'une application AppExpert comporte les étapes suivantes :

1. Configuration des points de terminaison publics
2. Configuration des unités d'application
3. Préciser l'ordre d'évaluation
4. Affichage de la configuration de l'application à l'aide de Visualizer

Vous pouvez également configurer les stratégies fournies par le modèle. Si le modèle d'application AppExpert n'inclut pas de stratégies pour une fonctionnalité particulière de Citrix ADC, telle que Réécriture ou pare-feu d'application, vous pouvez configurer vos propres stratégies.

Configurer les points de terminaison publics

August 20, 2021

Si vous n'avez pas spécifié de point de terminaison public lors de l'importation d'une application AppExpert, vous pouvez spécifier des points de terminaison publics après avoir créé l'application. Vous pouvez configurer un point de terminaison public de type HTTP et un point de terminaison public de type HTTPS pour votre application AppExpert.

Si les points de terminaison sont déjà configurés pour l'application, vous pouvez dissocier les points de terminaison de l'application AppExpert et supprimer les points de terminaison dont vous n'avez plus besoin. Notez que lorsque vous dissociez un point de terminaison public de l'application AppExpert, le point de terminaison est automatiquement dissocié de l'unité d'application associée, mais il n'est pas supprimé du système.

Pour configurer les points de terminaison publics pour une application AppExpert :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur l'application pour laquelle vous souhaitez configurer les points de terminaison publics, puis cliquez sur Modifier.
3. Dans la page **Applications**, accédez à la section **Public Endpoint** et cliquez sur l'icône en forme de crayon.
4. Dans le curseur **Public Endpoint**, définissez les paramètres suivants.
    a) Type de point de terminaison public. Sélectionnez le bouton radio pour définir le type de point de terminaison.
    b) Nom. Nom du point de terminaison public.
    c) Adresse IP. Adresse IP du point de terminaison public.

d) Port. Numéro de port du point de terminaison public.
e) Protocole. Sélectionnez un type de protocole HTTP ou HTTPS.

5. Cliquez sur **Continuer.**
6. Dans la section **Unités d'application**, sélectionnez une unité d'application dans la liste.
7. Cliquez sur **Continuer** pour définir la stratégie et les détails du serveur.
8. Cliquez sur **OK**, puis sur Terminé.
9. Cliquez sur Fermer.

Pour plus d'informations sur les paramètres de la boîte de dialogue **Configurer le point de terminaison public**, voir Commutation de contenu.

Configurer les services et les groupes de services pour une unité d'application

August 20, 2021

Lorsque vous configurez un service ou un groupe de services, vous modifiez un service ou un groupe de services existant ou ajoutez de nouveaux services à l'application AppExpert. Vous ajoutez des services ou des groupes de services si vous ne les avez pas spécifiés lors de l'importation du modèle d'application. Vous ajoutez également des services et des groupes de services lorsque vous augmentez le nombre de serveurs qui hébergent des instances de l'application. Vous ne pouvez configurer un service et un groupe de services pour une unité d'application qu'après avoir configuré le service ou le groupe de services pour l'application AppExpert.

Pour configurer un service ou un groupe de services pour l'application AppExpert :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur l'application, puis cliquez sur **Modifier.**
3. Dans la page **Applications**, sélectionnez une unité d'application, puis cliquez sur **Continuer** .
4. Dans la section **Services et groupes de services**, procédez comme suit :
   a) Dans le curseur Liaison de service, définissez les paramètres suivants.
      i. Service. Sélectionnez un service d'équilibrage de charge dans la liste ou créez un nouveau service.
      ii. Poids. Indiquez une valeur de poids pour le service.
   b) Cliquez sur **Liaison**, puis **Terminé.**
   c) Dans le curseur Liaison ServiceGroup, définissez les paramètres suivants :
      i. Nom du groupe de services. Sélectionnez un groupe de services d'équilibrage de charge ou créez un nouveau groupe de services.
      ii. Cliquez sur **Lier**, puis sur **Terminé**.

d) Cliquez sur **Terminé**.

5. Cliquez sur **Continuer** pour définir d'autres configurations.

Créer des unités d'application

October 5, 2021

Il se peut que vous deviez ajouter des unités d'application pour les sous-ensembles de trafic qui sont spécifiques à votre implémentation d'application Web ou qui ne sont pas définis dans le modèle. Lorsque vous créez une unité d'application, vous devez configurer une règle pour cette unité d'application.

Pour créer une unité d'application pour l'application AppExpert, procédez comme suit :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit de la souris sur l'application pour laquelle vous souhaitez ajouter une unité d'application, puis cliquez sur **Ajouter**.
3. Dans la page **Applications**, accédez à la section **Unités d'application** et cliquez sur l'icône en forme de **crayon** .

Pour configurer les expressions de stratégie pour une unité d'application :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit de la souris sur l'application pour laquelle vous souhaitez ajouter une unité d'application, puis cliquez sur **Ajouter**.
3. Dans la page **Applications**, accédez à la section **Unités d'application** et cliquez sur l'icône **+** pour créer une unité et ajouter des expressions de stratégie.
4. Pour spécifier le format de la nouvelle expression, effectuez l'une des opérations suivantes :
   a) Pour spécifier que vous souhaitez configurer une expression de stratégie dans la zone Règle, cliquez sur Syntaxe classique.
   b) Pour spécifier que vous souhaitez configurer une expression avancée dans la zone Règle, cliquez sur Stratégie avancée.
   c) Dans la zone Règle, configurez l'expression.
5. Cliquez sur **OK**.

Configuration des règles d'unité d'application

October 5, 2021

Vous souhaiterez peut-être configurer une règle d'unité d'application pour inclure ou exclure certains

types de trafic. Lorsque vous configurez la règle, vous pouvez également définir la syntaxe de l'expression.

Pour configurer une règle d'unité d'application :

1. Dans le volet de navigation de l'interface graphique, développez AppExpert, puis cliquez sur **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit de la souris sur l'unité d'application pour laquelle vous souhaitez modifier la règle, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue Configurer l'unité d'application, procédez comme suit :
   a) Pour spécifier le format de la nouvelle expression, effectuez l'une des opérations suivantes :
      - Pour spécifier que vous souhaitez configurer une expression de stratégie avancée dans la zone Règle, cliquez sur **Syntaxe classique**.
      - Pour spécifier que vous souhaitez configurer une expression avancée dans la zone Règle, cliquez sur **Stratégie avancée**.
   b) Dans la zone Règle, configurez l'expression.
4. Cliquez sur **OK**.

Configuration des stratégies pour les unités d'application

October 5, 2021

Pour une application AppExpert, vous pouvez configurer des stratégies de compression, de mise en cache, de réécriture, de répondeur et de pare-feu d'application. Les modèles que vous téléchargez à partir du site Web de la Citrix Community vous fournissent un ensemble de stratégies qui répondent aux exigences de gestion des applications les plus courantes. Vous souhaiterez peut-être peaufiner ou personnaliser ces stratégies. Si l'ensemble de stratégies fourni pour une unité d'application donnée n'inclut pas de stratégies pour une fonctionnalité particulière, vous pouvez créer et lier vos propres stratégies pour cette fonctionnalité.

Si vous créez une application AppExpert sans utiliser de modèle, vous devez configurer toutes les stratégies dont l'application Web a besoin.

L'interface graphique utilise diverses icônes pour indiquer si des stratégies sont configurées pour une fonctionnalité. Pour une unité d'application, si une stratégie est configurée pour une fonctionnalité donnée, une icône représentant la fonctionnalité s'affiche. Par exemple, si une stratégie de compression est configurée pour une unité d'application, une icône de compression s'affiche dans la colonne Compression de l'unité d'application. Pour les fonctionnalités pour lesquelles aucune stratégie n'est configurée, une icône représentant un signe plus (+) s'affiche.

Remarque : Lorsque vous configurez des stratégies pour les unités d'application, vous devrez

peut-être configurer des stratégies et des expressions qui se trouvent dans la stratégie classique ou avancée. En outre, lorsque vous configurez des stratégies de stratégie avancées, vous devrez peut-être spécifier des paramètres tels que les expressions Goto et invoquer des banques de stratégies.

Pour plus d'informations sur la configuration des stratégies et des expressions dans les deux formats, voir Stratégies et expressions.

Configuration des stratégies de compression

Vous pouvez utiliser des stratégies classiques ou avancées pour configurer la compression, mais vous ne pouvez pas lier des stratégies de compression des deux types à la même unité d'application.

Pour configurer une stratégie de compression pour une unité d'application, procédez comme suit :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, dans la ligne de l'unité d'application que vous souhaitez configurer, cliquez sur l'icône fournie dans la colonne Compression.
3. Dans la boîte de dialogue Configurer les stratégies de compression, effectuez une ou plusieurs des opérations suivantes, en fonction des tâches de configuration que vous souhaitez effectuer :
   - Cliquez sur Basculer vers la stratégie avancée si vous souhaitez configurer une stratégie de compression de stratégie avancée. Si vous souhaitez lier ou configurer des stratégies de compression classiques, et si vous êtes dans la vue des stratégies avancées, vous pouvez cliquer sur Basculer vers la syntaxe classique pour revenir à la vue de stratégie classique et commencer à modifier les stratégies classiques liées ou créer et lier de nouvelles stratégies de compression classiques.
     Important : Ce paramètre détermine également les stratégies affichées lorsque vous souhaitez insérer une stratégie. Par exemple, si vous êtes dans la vue des stratégies avancées, lorsque vous cliquez sur Insérer une stratégie, la liste qui apparaît dans la colonne Nom de la stratégie inclut uniquement les stratégies de stratégie avancées. Vous ne pouvez pas lier des stratégies des deux types à une unité d'application.
   - Si vous souhaitez configurer des stratégies classiques, cliquez sur Demande ou Réponse, selon que vous souhaitez que la stratégie soit évaluée au moment de la demande ou au moment de la réponse.
     Vous pouvez configurer des stratégies de compression classiques de temps de demande et de temps de réponse pour une unité d'application. Après avoir évalué toutes les stratégies de temps de demande, si aucune correspondance n'est trouvée, la solution matérielle-logicielle évalue les stratégies de temps de réponse.
   - Pour modifier une stratégie de compression déjà liée à l'unité d'application, cliquez sur le nom de la stratégie, puis sur Modifier la stratégie. Ensuite, dans la boîte de dialogue Configurer la stratégie de compression, modifiez la stratégie, puis cliquez sur OK.

Pour plus d'informations sur la modification d'une stratégie de compression, voir Compression.

- Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur Délier la stratégie.
- Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
- Pour régénérer les priorités affectées, cliquez sur Régénérer les priorités.
- Pour insérer une nouvelle stratégie, cliquez sur **Insérer une stratégie** et, dans la liste qui s'affiche dans la colonne Nom de la stratégie, cliquez sur **Nouvelle stratégie**. Ensuite, dans la boîte de dialogue Créer une stratégie de compression, configurez la stratégie, puis cliquez sur **Créer**.
  Pour plus d'informations sur la modification d'une stratégie de compression, voir Compression.
- Si vous configurez une expression de stratégie avancée, procédez comme suit :
  - Dans la colonne Expression Goto, sélectionnez une expression Goto.
  - Dans la colonne Invoke (Invoke), spécifiez la banque de stratégies que vous souhaitez appeler si la stratégie actuelle est évaluée à TRUE.

4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des stratégies de mise en cache

Vous ne pouvez utiliser que des stratégies et expressions avancées pour configurer les stratégies de mise en cache.

Pour configurer les stratégies de mise en cache pour une unité d'application :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, dans la ligne de l'unité d'application que vous souhaitez configurer, cliquez sur l'icône fournie dans la colonne Mise en cache.
3. Dans la boîte de dialogue Configurer les stratégies de cache, effectuez une ou plusieurs des opérations suivantes, en fonction des tâches de configuration que vous souhaitez effectuer :
   - Cliquez sur Demande ou Réponse, selon que vous souhaitez que la stratégie soit évaluée au moment de la demande ou au moment de la réponse.
     Vous pouvez configurer des stratégies de mise en cache de temps de demande et de temps de réponse pour une unité d'application. Après avoir évalué toutes les stratégies de temps de demande, si aucune correspondance n'est trouvée, la solution matérielle-logicielle évalue les stratégies de temps de réponse.
   - Pour modifier une stratégie de mise en cache déjà liée à l'unité d'application, cliquez sur le nom de la stratégie, puis sur Modifier la stratégie. Ensuite, dans la boîte de dialogue **Configurer la stratégie de cache**, modifiez la stratégie, puis cliquez sur **OK** .
     Pour plus d'informations sur la modification d'une stratégie de mise en cache, reportez-

vous à la section Mise en cache intégrée.

- Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur **Délier la stratégie**.
- Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
- Pour régénérer les priorités affectées, cliquez sur **Régénérer les priorités**.
- Pour insérer une nouvelle stratégie, cliquez sur **Insérer une stratégie** et, dans la liste qui s'affiche dans la colonne Nom de la stratégie, cliquez sur **Nouvelle stratégie**. Ensuite, dans la boîte de dialogue **Créer une stratégie de cache**, configurez la stratégie, puis cliquez sur **Créer** .
  Pour plus d'informations sur la modification d'une stratégie de mise en cache, reportez-vous à la section Mise en cache intégrée.
- Dans la colonne Expression Goto, sélectionnez une expression Goto.
- Dans la colonne Invoke (Invoke), spécifiez la banque de stratégies que vous souhaitez appeler si la stratégie actuelle est évaluée à TRUE.

4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des stratégies de réécriture

Vous ne pouvez utiliser que des stratégies et expressions avancées pour configurer des stratégies de réécriture.

Pour configurer des stratégies de réécriture pour une unité d'application, procédez comme suit :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, dans la ligne de l'unité d'application que vous souhaitez configurer, cliquez sur l'icône fournie dans la colonne Réécriture.
3. Dans la boîte de dialogue **Configurer les stratégies de réécriture**, effectuez une ou plusieurs des opérations suivantes, en fonction des tâches de configuration que vous souhaitez effectuer :
   - Cliquez sur Demande ou Réponse, selon que vous souhaitez que la stratégie soit évaluée au moment de la demande ou au moment de la réponse.
     Vous pouvez configurer des stratégies de réécriture en temps de demande et en temps de réponse pour une unité d'application. Après avoir évalué toutes les stratégies de temps de demande, si aucune correspondance n'est trouvée, la solution matérielle-logicielle évalue les stratégies de temps de réponse.
   - Pour modifier une stratégie de réécriture déjà liée à l'unité d'application, cliquez sur le nom de la stratégie, puis sur **Modifier la stratégie**. Ensuite, dans la boîte de dialogue Configurer la stratégie de réécriture, modifiez la stratégie, puis cliquez sur **OK**.
     Pour plus d'informations sur la modification d'une stratégie de réécriture, voir Réécriture.
   - Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur **Délier la stratégie**.

- Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
- Pour régénérer les priorités affectées, cliquez sur **Régénérer les priorités**.
- Pour insérer une nouvelle stratégie, cliquez sur **Insérer une stratégie** et, dans la liste qui s'affiche dans la colonne **Nom de la stratégie**, cliquez sur **Nouvelle stratégie.** Ensuite, dans la boîte de dialogue **Créer une stratégie de réécriture**, configurez la stratégie, puis cliquez sur **Créer** .
  Pour plus d'informations sur la modification d'une stratégie de réécriture, voir Réécriture.
- Dans la colonne Expression Goto, sélectionnez une expression Goto.
- Dans la colonne Invoke (Invoke), spécifiez la banque de stratégies que vous souhaitez appeler si la stratégie actuelle est évaluée à TRUE.

4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des stratégies de répondeur

Vous ne pouvez utiliser que des stratégies et expressions avancées pour configurer les stratégies de répondeur.

Pour configurer les stratégies de répondeur pour une unité d'application, procédez comme suit :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, dans la ligne de l'unité d'application que vous souhaitez configurer, cliquez sur l'icône fournie dans la colonne Répondeur.
3. Dans la boîte de dialogue **Configurer les stratégies de répondeur**, effectuez une ou plusieurs des opérations suivantes, en fonction des tâches de configuration que vous souhaitez effectuer :
   - Pour modifier une stratégie de filtre déjà liée à l'unité d'application, cliquez sur le nom de la stratégie, puis sur **Modifier la stratégie**. Ensuite, dans la boîte de dialogue Configurer la stratégie de répondeur, modifiez la stratégie, puis cliquez sur **OK**.
     Pour plus d'informations sur la modification d'une stratégie de répondeur, voir Répondeur.
   - Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur **Délier la stratégie**.
   - Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
   - Pour régénérer les priorités affectées, cliquez sur **Régénérer les priorités**.
   - Pour insérer une nouvelle stratégie, cliquez sur Insérer une stratégie et, dans la liste affichée dans la colonne Nom de la stratégie, cliquez sur Nouvelle stratégie. Ensuite, dans la boîte de dialogue Créer une stratégie de répondeur, configurez la stratégie, puis cliquez sur Créer.
     Pour plus d'informations sur la modification d'une stratégie de répondeur, voir Répondeur.

- Dans la colonne Expression Goto, sélectionnez une expression Goto.
- Dans la colonne Invoke (Invoke), spécifiez la banque de stratégies que vous souhaitez appeler si la stratégie actuelle est évaluée à TRUE.

4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des stratégies de pare-feu d'application

Vous pouvez configurer des stratégies et expressions classiques et avancées pour le pare-feu d'application. Toutefois, si une stratégie d'un type est déjà liée globalement ou à un serveur virtuel configuré sur l'appliance, vous ne pouvez pas lier une stratégie de l'autre type à une unité d'application. Par exemple, si une stratégie avancée est déjà liée globalement ou à un serveur virtuel, vous ne pouvez pas lier une stratégie classique à une unité d'application.

Pour configurer des stratégies de pare-feu d'application pour une unité d'application :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, dans la ligne de l'unité d'application que vous souhaitez configurer, cliquez sur l'icône fournie dans la colonne **Pare-feu d'application** .
3. Dans la boîte de dialogue **Configurer les stratégies de pare-feu d'application**, effectuez une ou plusieurs des opérations suivantes, en fonction des tâches de configuration que vous souhaitez effectuer :
   - Cliquez sur Expression classique ou Expression avancée en fonction du type d'expression que vous souhaitez configurer pour la stratégie de pare-feu d'application.
     Important : Ce paramètre détermine également les stratégies affichées lorsque vous souhaitez insérer une stratégie. Par exemple, si vous sélectionnez Expression avancée, lorsque vous cliquez sur **Insérer une stratégie**, la liste qui apparaît dans la colonne **Nom de la stratégie** inclut uniquement les stratégies de stratégie avancées. Vous ne pouvez pas lier des stratégies des deux types à une unité d'application. Cette option n'est pas disponible si une stratégie de l'un ou l'autre type est déjà liée globalement ou à un serveur virtuel.
   - Pour modifier une stratégie de pare-feu d'application déjà liée à l'unité d'application, cliquez sur le nom de la stratégie, puis sur Modifier la stratégie. Ensuite, dans la boîte de dialogue Configurer la stratégie de pare-feu d'application, modifiez la stratégie, puis cliquez sur OK.
     Pour plus d'informations sur la modification d'une stratégie de pare-feu d'application, voir Stratégies.
   - Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur Délier la stratégie.
   - Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
   - Pour régénérer les priorités affectées, cliquez sur Régénérer les priorités.

- Pour insérer une nouvelle stratégie, cliquez sur **Insérer une stratégie** et, dans la liste affichée dans la colonne **Nom de la stratégie**, cliquez sur Nouvelle stratégie. Ensuite, dans la boîte de dialogue **Créer une stratégie de pare-feu d'application**, configurez la stratégie, puis cliquez sur **Créer** .
  Pour plus d'informations sur la modification d'une stratégie de pare-feu d'application, voir Stratégies.

4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des unités d'application

January 21, 2021

Pour configurer une unité d'application à l'aide de l'interface graphique :

1. Accédez à la section **AppExpert** > **Applications** > **Application Unit**, puis cliquez sur l'icône plus pour ajouter une nouvelle unité d'application pour un sous-ensemble de trafic.
2. Dans le curseur **Unité d'application**, définissez les paramètres suivants :
   - Nom
   - Expression

   Vous pouvez insérer une expression soit en ajoutant les composants d'expression manuellement, soit en utilisant le lien Éditeur d'expression. Pour ajouter manuellement une expression, entrez un composant sélecteur, puis tapez un point (.) pour afficher une liste à partir de laquelle vous pouvez sélectionner le composant suivant. Par exemple, tapez HTTP, puis tapez un point. Un menu déroulant s'affiche. Le contenu de ce menu fournit les mots-clés qui peuvent suivre le mot-clé initial que vous avez entré. Sélectionnez un composant dans le menu déroulant. La zone de texte Expression* affiche désormais les composants que vous avez ajoutés à l'expression (par exemple, HTTP.REQ). Continuez à ajouter des composants jusqu'à ce que l'expression complète soit formée.

   Si vous préférez l'assistance pour former l'expression, vous pouvez utiliser le lien Expression Editor. Sur la page Éditeur d'expression, vous pouvez former une expression en sélectionnant des composants dans les zones déroulantes. Sélectionnez les composants et cliquez sur Terminé pour insérer l'expression dans la page Unité d'application.
3. Cliquez sur **Continuer** pour lier les services et les groupes de services.
4. Cliquez sur la section **Service** pour sélectionner ou ajouter un service virtuel et le lier à l'unité d'application.
5. Cliquez sur **Continuer**, puis cliquez sur la section **Groupe de services** pour sélectionner ou ajouter un groupe de services virtuel et le lier à l'unité d'application.

6. Cliquez sur **Liaison** et **Continuer** pour configurer les paramètres avancés (tels que Stratégies, Méthode, Persistance, Protection, Profils, Push, Authentification et Paramètres de trafic) pour l'unité d'application.
7. Cliquez sur l'icône **plus** dans chaque section pour définir les paramètres de configuration.
8. Cliquez sur **OK**, puis sur **Terminé**.

Pour modifier une unité d'application pour une application à l'aide de l'interface graphique :

Accédez à **AppExpert** > **Applications**, sélectionnez une application et cliquez sur **Modifier**. Dans la section **Unité de l'application**, sélectionnez une entité, cliquez sur l'icône Modifier et modifiez les paramètres de l'unité de l'application.

Remarque : Vous ne pouvez pas modifier le nom et l'expression de règle d'une unité d'application existante.

Les didacticiels vidéo de Citrix ADC vous permettent de comprendre les fonctionnalités Citrix ADC de manière simple et simple. Regardez la https://www.youtube.com/watch?v=bJ5_i8fV2hc vidéo pour découvrir comment configurer une unité d'application.

Configuration des points de terminaison publics pour une application

August 20, 2021

Pour configurer des points de terminaison publics pour une application à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Applications**, sélectionnez une entité d'application, puis cliquez sur **Modifier**.
2. Dans la section **Public Endpoint**, cliquez sur **+** pour configurer un nouveau point de terminaison public.
3. Dans le curseur **Public Endpoint**, effectuez l'une des opérations suivantes :
   a) Cliquez sur **Nouveau** pour créer un point de terminaison.
   b) Cliquez sur **Point de terminaison public existant** pour sélectionner un point de terminaison dans la liste déroulante.
4. Définissez les paramètres de point de terminaison suivants :
   a) Nom
   b) Adresse IP
   c) Protocole
   d) Port
5. Cliquez sur **Continuer** pour configurer des paramètres supplémentaires tels que les unités d'application, les liaisons de serveur GSLB, les stratégies, les profils, la transmission, les paramètres de trafic et l'authentification.

6. Cliquez sur **OK**, puis sur **Terminé**.
7. Cliquez sur **Continuer**, puis **Terminé**.

Pour modifier un point de terminaison public pour une application à l'aide de l'interface graphique :

Accédez à **AppExpert** > **Applications**, sélectionnez une application et cliquez sur **Modifier** . Dans la section **Public Endpoint**, sélectionnez un point de terminaison, cliquez sur l'icône du stylet et modifiez les paramètres du point de terminaison.

Pour supprimer un point de terminaison public pour une application à l'aide de l'interface graphique :

Accédez à **AppExpert** > **Applications** > **Point de terminaison public,** cliquez sur l'icône du stylet pour afficher l'icône de suppression en regard de l'entité.

Les didacticiels vidéo de Citrix ADC vous permettent de comprendre facilement et simplement les fonctionnalités de Citrix ADC. Regardez la https://www.youtube.com/watch?v=z4v-edQiVpw vidéo pour savoir comment configurer un point de terminaison public.

Préciser l'ordre d'évaluation des unités de demande

January 21, 2021

Les règles d'unité d'application sont évaluées dans l'ordre dans lequel elles sont placées dans l'interface graphique. La règle configurée pour l'unité d'application la plus haute est toujours configurée en premier, suivie de la règle configurée pour la deuxième unité d'application la plus haute, etc. L'unité d'application par défaut est toujours évaluée en dernier.

Lorsqu'une demande correspond à la règle configurée pour une unité d'application, la demande est traitée par l'unité d'application et aucune autre correspondance n'est effectuée. Par conséquent, l'ordre d'évaluation des unités d'application devient un facteur important si les sous-ensembles de trafic pour deux ou plusieurs unités d'application se chevauchent. Si les sous-ensembles de trafic de deux unités d'application ou plus se chevauchent, vous devez spécifier l'ordre dans lequel une demande entrante est mise en correspondance avec les règles d'unité d'application.

Pour spécifier l'ordre d'évaluation des unités d'application :

1. Accédez à **AppExpert** > **Applications**, sélectionnez une application et cliquez sur **Modifier**. Dans la section **Unité d'application**, cliquez sur l'icône **Crayon**, puis placez le curseur sur la case à cocher située à gauche du nom de l'unité d'application. Cliquez sur l'icône qui apparaît en regard de la case à cocher et maintenez la souris enfoncée pour faire glisser l'application vers le haut ou vers le bas vers un nouvel emplacement dans la liste des priorités.

Configuration des groupes de persistance pour les unités d'application

January 21, 2021

Vous pouvez configurer un groupe de persistance pour les unités d'application dans une application AppExpert. Dans le contexte d'une application AppExpert, un groupe de persistance est un groupe d'unités d'application que vous pouvez traiter comme une seule entité aux fins de l'application de paramètres de persistance communs. Lorsque l'application est exportée vers un fichier de modèle d'application, les paramètres de groupe de persistance sont inclus et ils sont automatiquement appliqués aux unités d'application lorsque vous importez l'application AppExpert.

Pour configurer un groupe de persistance pour une application à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans la boîte de dialogue **Affichage des applications**, cliquez sur le nom de l'application dont vous souhaitez configurer un groupe de persistance, puis cliquez sur Configurer les **groupes de persistance** .
3. Dans la boîte de dialogue **Configurer les groupes de persistance**, effectuez l'une des opérations suivantes :
    - Pour ajouter un groupe de persistance, cliquez sur **Ajouter**.
    - Pour modifier un groupe de persistance, cliquez sur **Ouvrir**.
4. Dans la boîte de dialogue **Créer un groupe** de **persistance ou Configurer un groupe de persistance**, définissez les paramètres suivants :
    - Nom du groupe (Group Name) : nom du groupe de persistance. Pour que l'appliance Citrix ADC reconnaisse le groupe de persistance dans la configuration de l'application, le nom de l'application AppExpert doit être inclus dans le nom du groupe de persistance, en tant que préfixe. Par conséquent, par défaut, l'appliance affiche le préfixe dans la zone Nom du groupe, et vous ne pouvez pas supprimer ce préfixe. Entrez le nom de votre choix après le préfixe.
    - Persistance : type de persistance pour le serveur virtuel. Si vous sélectionnez SOURCEIP, dans la zone Masque de réseau IPv4, entrez un masque réseau qui spécifie le nombre de bits que l'appliance doit prendre en compte lors de la création de sessions de persistance. Si vous sélectionnez COOKIEINSERT, dans les zones Domaine des cookies et Nom du cookie, spécifiez un attribut de domaine à envoyer dans la directive Set-Cookie et un nom pour le cookie, respectivement.
    - Délai d'attente : période pendant laquelle une session de persistance est en vigueur.
    - Sauvegarde persistance (Backup persistance) : type de persistance de sauvegarde pour le groupe.
    - Délai d'attente de sauvegarde : période, en minutes, pendant laquelle la persistance de la sauvegarde est en vigueur.
    - Unités d'application : pour ajouter une unité d'application au groupe de persistance, dans

la zone Unités d'application disponibles, cliquez sur l'unité d'application, puis cliquez sur Ajouter. Pour supprimer une unité d'application du groupe de persistance, dans la zone Unités d'application configurées, cliquez sur l'unité d'application, puis cliquez sur **Supprimer**.

5. Cliquez sur **OK**.

Affichage des applications AppExpert et configuration des entités à l'aide du visualiseur d'applications

January 21, 2021

La fonction Visualizer affiche une représentation graphique de la configuration d'une application. Il inclut le nom du point de terminaison public, les unités d'application affectées au point de terminaison public et le nombre de stratégies et de services liés à l'application. Vous pouvez utiliser Visualizer pour obtenir une vue d'ensemble visuelle de la configuration d'une application AppExpert et configurer certaines des entités affichées. Par défaut, le Visualizer affiche les unités d'application, les services et les moniteurs pour l'application sélectionnée.

Pour afficher une application AppExpert à l'aide du Visualizer d'application :

1. Accédez à **AppExpert** > **Applications**, sélectionnez une entité d'application et cliquez sur **Visualizer** .

Configuration de l'authentification utilisateur, de l'autorisation et de l'audit

January 21, 2021

Vous pouvez configurer l'autorisation pour les utilisateurs et les groupes afin qu'ils puissent ensuite accéder à une application AppExpert. Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez configurer les autorisations n'a pas encore été créé, vous pouvez le créer à partir d'AppExpert, puis configurer les autorisations pour l'accès à l'application.

Pour configurer des utilisateurs AAA et des groupes d'utilisateurs AAA pour une application à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Applications**, sélectionnez une entité d'application, puis cliquez sur **Modifier**.
2. Dans la section **Paramètres avancés**, cliquez sur **Autorisation** et configurez les utilisateurs autorisés et les groupes d'utilisateurs.

3. Cliquez sur la section utilisateur **AAA** pour lier les utilisateurs autorisés à l'application.
4. Dans le curseur **Utilisateur AAA**, définissez les paramètres.
5. Cliquez sur **Continuer**, puis sur **Stratégies d'autorisation**dans la section **Paramètres avancés**.
6. Dans le curseur **Stratégie d'autorisation**, liez une stratégie d'autorisation à l'application.
7. Cliquez sur **Continuer**, puis sur la section **Groupe d'autorisations**dans la section **Paramètres avancés**.
8. Dans le curseur de **liaison de groupe AAA**, liez un groupe d'utilisateurs d'autorisation à l'application.
9. Cliquez sur **Continuer**, puis sur **Stratégies**dans la section **Paramètres avancés**.
10. Dans le curseur **Stratégies**, liez une stratégie **Audit Syslog** ou **Audit NsLog** à l'application.
11. Cliquez sur **Continuer**, puis **Terminé**.

Pour modifier les utilisateurs AAA et les groupes d'utilisateurs AAA d'une application à l'aide de l'interface graphique :

Accédez à **AppExpert** > **Applications** > **Paramètres avancés** et cliquez sur **Autorisation** . Cliquez ensuite sur l'icône Modifier et spécifiez des valeurs pour les paramètres d'autorisation utilisateur ou de groupe d'utilisateurs.

Pour supprimer des utilisateurs AAA et des groupes d'utilisateurs AAA à l'aide de l'interface graphique :

Accédez à **AppExpert** > **Applications**, sélectionnez une application et cliquez sur **Modifier**. Dans la page **Applications**, cliquez sur **Paramètres avancés**, puis sur **Autorisation** . Cliquez sur l'icône Supprimer en regard de l'entité.

Surveillance d'une application Citrix ADC

January 21, 2021

Après avoir personnalisé l'application AppExpert, vous pouvez afficher les statistiques de l'application pour vous assurer que l'application et toutes ses entités fonctionnent correctement. Vous pouvez également utiliser Application Visualizer pour surveiller les statistiques associées à certaines entités telles que les stratégies et les serveurs virtuels.

Vous pouvez également afficher les compteurs d'accès de diverses entités à intervalles réguliers pour vous assurer que les compteurs sont en cours de mise à jour.

Afficher les statistiques d'application

Dans le nœud **Applications**, vous pouvez sélectionner une application et afficher la page Statistiques de l'application. Sur la page Statistiques, vous pouvez surveiller l'état et l'état des points de terminaison publics et des unités d'application, et afficher les informations statistiques suivantes :

- Demandes et réponses par seconde pour chacun des points de terminaison publics et des unités d'application.
- Octets par seconde, à chaque point de terminaison, pour le trafic entrant et sortant.
- Compteurs d'accès de l'unité d'application et nombre de connexions client et serveur pour chaque unité d'application.
- Statistiques pour les services liés aux unités d'application.

Sur la page Statistiques, vous pouvez également afficher l'utilisation de l'UC, l'utilisation de la mémoire et les journaux système.

Pour afficher les statistiques d'une application :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez sur l'application pour laquelle vous souhaitez afficher les statistiques, puis cliquez sur **Statistiques**.

Surveillance d'une application à l'aide du Visualizer d'application

Vous pouvez utiliser Application Visualizer pour surveiller le nombre de requêtes reçues par seconde à un moment donné par les serveurs vservers et le nombre d'accès par seconde à un moment donné pour les stratégies de réécriture, de répondeur et de cache.

Pour afficher des informations statistiques sur les serveurs vservers, les stratégies de réécriture, les stratégies de répondeur et les stratégies de cache dans Visualizer :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, sélectionnez l'application pour laquelle vous souhaitez afficher des informations statistiques, puis cliquez sur **Visualizer**.
3. Dans la fenêtre **Application Visualizer**, procédez comme suit :
    - Pour afficher les statistiques, cliquez sur **Afficher les statistiques**.
      Les informations statistiques sont affichées sur les nœuds respectifs dans le Visualizer. Ces informations ne sont pas mises à jour en temps réel et doivent être actualisées manuellement.
    - Pour actualiser les informations statistiques, cliquez sur **Actualiser les statistiques**.

Affichage des résultats

Les compteurs d'accès fournis pour diverses entités d'application AppExpert vous permettent de surveiller le fonctionnement des points de terminaison publics et des unités d'application. Pour une application, la boîte de dialogue Résultats affiche le nombre total de demandes reçues par chaque point de terminaison public configuré. Pour une unité d'application, la boîte de dialogue Résultats affiche le nombre de demandes traitées par l'unité d'application à partir de chacun des points de

terminaison publics et le nombre total d'appels. Pour obtenir des instructions sur l'affichage des compteurs d'accès, reportez-vous à la section Vérification et test de la configuration.

Suppression d'une application

January 21, 2021

Si vous n'avez plus besoin d'une application et de ses unités d'application, vous pouvez la supprimer. Lorsque vous supprimez une application AppExpert, les services backend ne sont pas supprimés et les points de terminaison publics utilisés par l'application deviennent disponibles pour une utilisation par d'autres applications.

Lorsque vous supprimez une application, vous êtes également invité à spécifier si vous souhaitez supprimer des stratégies et actions liées qui ne sont pas utilisées ailleurs.

Pour supprimer une unité d'application pour une application à l'aide de l'interface graphique :

Accédez à **AppExpert** > **Applications**, sélectionnez une application et cliquez sur **Modifier**. Dans la section **Application Unit**, cliquez sur l'icône Supprimer en regard de l'entité

Configurer l'authentification, l'autorisation et l'audit d'applications

August 20, 2021

Vous pouvez configurer l'authentification, l'autorisation et l'audit (AAA) pour les applications que vous configurez sur l'appliance. Une stratégie d'authentification configurée pour une application définit le type d'authentification à appliquer lorsqu'un utilisateur ou un groupe tente d'accéder à l'application. Si l'authentification externe est utilisée, la stratégie spécifie également le serveur d'authentification externe. Les stratégies d'autorisation configurées pour une application spécifient si un utilisateur ou un groupe particulier peut accéder à l'application. Les stratégies d'audit définissent le type de journal d'audit, le niveau auquel la journalisation est effectuée et d'autres paramètres du serveur d'audit. Les stratégies d'authentification et d'audit utilisent le format de stratégie classique.

Les stratégies d'authentification, les stratégies d'autorisation et les stratégies d'audit peuvent être configurées dans n'importe quel ordre. Toutefois, avant de configurer AAA pour une application, vous devez configurer un point de terminaison public pour l'application.

La configuration de l'authentification pour une application implique la spécification d'un nom de domaine complet d'authentification, d'un serveur virtuel d'authentification, d'un certificat de serveur et de stratégies d'authentification et de session. Les stratégies d'authentification sont automatiquement liées au serveur virtuel d'authentification spécifié pour l'application.

Pour configurer l'authentification pour une application AppExpert :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   a) Cliquez sur Ajouter pour ajouter une authentification pour une nouvelle application.
   b) Cliquez sur Modifier pour modifier une application existante.
3. Dans la page **Applications**, sélectionnez une unité d'application.
4. Dans la page du curseur **Unité d'application**, cliquez sur Authentification dans la section **Paramètres avancés** .
5. Dans la section **Authentification**, sélectionnez le type d'authentification comme suit :
   a) Authentification basée sur un formulaire
   b) Authentification basée sur 401
   c) Aucune
6. Cliquez sur **OK**, puis sur **Terminé**.

Configurer l'autorisation d'application

Vous pouvez configurer l'autorisation pour les utilisateurs et les groupes afin qu'ils puissent ensuite accéder à une application AppExpert. Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez configurer les autorisations n'a pas encore été créé, vous pouvez le créer à partir d'AppExpert, puis configurer les autorisations pour l'accès à l'application.

Pour configurer les autorisations permettant à un utilisateur ou un groupe AAA d'accéder à une application AppExpert :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez sur l'application AppExpert pour laquelle vous souhaitez configurer un accès utilisateur ou groupe.
3. Dans la page **Applications**, puis cliquez sur Autorisation dans la section **Paramètres avancés**.
4. Procédez comme suit :
   - Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez configurer des autorisations se trouve déjà dans l'arborescence Groups/Utilisateurs, faites glisser l'utilisateur ou le groupe de l'arborescence Groups/Utilisateurs vers le nœud Utilisateurs ou Groupes dans l'arborescence des applications. Ensuite, cliquez avec le bouton droit sur l'utilisateur ou le groupe et cliquez sur Autoriser.
   - Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez configurer des autorisations n'est pas configuré sur l'appliance, dans l'arborescence des applications, cliquez avec le bouton droit sur Utilisateurs ou groupes, puis cliquez sur Ajouter. Dans la boîte de dialogue Créer un groupeAAA ou Créer un utilisateur AAA, renseignez les valeurs, cliquez sur Créer, puis cliquez sur Fermer.
     L'utilisateur ou le groupe est créé avec l'autorisation définie sur Autoriser. Pour modifier le paramètre d'autorisation, cliquez avec le bouton droit sur le groupe ou l'utilisateur, puis

cliquez sur le paramètre d'autorisation.

5. Cliquez sur **Terminé**, puis sur **Fermer** .

Configurer l'audit des applications

Lorsque vous configurez des stratégies d'audit pour une application, vous devez spécifier le serveur vers lequel les messages de journal doivent être dirigés, le format des messages consignés et le niveau de journal. Vous pouvez également configurer d'autres paramètres, tels que la fonction de journalisation et le format de date. Les stratégies d'audit sont automatiquement liées à tous les points de terminaison publics de l'application AppExpert.

Pour configurer des stratégies d'audit pour une application :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez sur l'application pour laquelle vous souhaitez configurer les stratégies d'audit.
3. Dans la page du curseur Unité d'application, cliquez sur l'icône + dans la section **Stratégies** pour configurer les stratégies d'audit.
4. Dans la page du curseur **Stratégies**, sélectionnez le type de stratégie comme Audit Syslog ou Audit Nslog, puis cliquez sur **Continuer** .
5. Dans la section Liaison de stratégie, définissez les paramètres suivants.
   a) Sélectionnez une stratégie à lier. Si vous n'avez pas de stratégie de liaison, cliquez sur + pour créer une nouvelle stratégie.
   b) Pour créer une stratégie d'audit, sous Nom de la stratégie, cliquez sur **Nouvelle stratégie,** puis, dans la page **Stratégie**, procédez comme suit :
      i. Dans la zone Nom, tapez un nom pour la stratégie.
      ii. La zone Nom contient déjà la chaîne requise au début du nom du serveur. Vous ne pouvez pas modifier la chaîne.
      iii. Dans la liste Type d'audit, sélectionnez le type d'audit (SYSLOG ou NSLOG).
      iv. Si le serveur d'audit que vous souhaitez spécifier est déjà répertorié dans la liste Serveur, sélectionnez le serveur dans la liste, puis, si vous souhaitez modifier les paramètres du serveur, cliquez sur Modifier. Dans la boîte de dialogue Configurer le serveur d'audit, modifiez les paramètres le cas échéant, puis cliquez sur OK. Pour plus d'informations sur les paramètres de la boîte de dialogue Configurer le serveur d'Auditing, consultez Audit des sessions authentifiées.
      v. Si vous souhaitez configurer un nouveau serveur d'audit, cliquez sur Nouveau, puis, dans la boîte de dialogue Créer un serveur d'audit, tapez un nom pour le serveur, spécifiez l'adresse IP du serveur, le numéro de port et les autres paramètres appropriés. Lorsque vous avez terminé, cliquez sur **OK**.
      vi. Cliquez sur **Créer**.
   c) Pour modifier les priorités des nouvelles stratégies d'audit que vous avez créées, sous

Priorité, pour chaque stratégie pour laquelle vous souhaitez modifier la priorité, double-cliquez sur la valeur de priorité et tapez une nouvelle valeur de priorité.

d) Pour régénérer les priorités, cliquez sur **Régénérer les priorités**.
e) Pour dissocier une stratégie, cliquez sur la stratégie, puis cliquez sur **Dissocier stratégie**.
f) Pour modifier une stratégie, cliquez sur la stratégie, puis cliquez sur **Modifier la stratégie.**

6. Cliquez sur **Appliquer les modifications,** puis cliquez sur **Fermer**.

Désactivation de l'AAA pour une application

Après avoir configuré AAA pour une application, vous pouvez désactiver la configuration AAA pour cette application. Lorsque vous désactivez AAA pour une application, la configuration n'est pas perdue. Vous pouvez activer AAA pour l'application lorsque vous souhaitez réappliquer la configuration.

Pour activer ou désactiver AAA pour une application :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez sur l'application pour laquelle vous souhaitez activer ou désactiver AAA, puis effectuez l'une des opérations suivantes :
3. Pour désactiver AAA pour l'application, cliquez sur **Désactiver AAA.**
4. Pour activer AAA pour l'application, cliquez **sur Activer AAA**.

Configuration d'une application Citrix ADC personnalisée

August 20, 2021

Si un modèle d'application AppExpert n'est pas disponible pour l'application Web que vous souhaitez gérer via l'appliance Citrix ADC, ou si les modèles d'application AppExpert disponibles ne répondent pas à vos besoins, vous pouvez créer une application AppExpert sans modèle.

Pour créer une application AppExpert sans modèle, vous devez d'abord créer une application et des unités d'application. Ensuite, vous configurez les points de terminaison publics, les services et les groupes de services. Enfin, vous configurez les stratégies qui déterminent la façon dont le trafic d'application est évalué et traité.

Après avoir créé les unités d'application et d'application et configuré les stratégies, vous devez vérifier la configuration et la tester pour vous assurer qu'elle fonctionne correctement, comme vous le feriez lorsque vous configurez une application à l'aide d'un modèle d'application AppExpert prédéfini. Ensuite, vous devez surveiller l'application pour vous assurer que l'application et ses entités fonctionnent correctement.

Création d'une application

Lorsque vous créez une application AppExpert, l'appliance crée un conteneur auquel vous pouvez ajouter des unités d'application. L'unité d'application par défaut n'est créée qu'après avoir créé la première unité d'application.

Pour créer une application AppExpert à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur **Applications**, puis cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une application**, dans Nom, entrez un nom pour l'application, puis cliquez sur **OK** .

Création d'unités d'application

Pour chaque sous-ensemble de trafic associé à votre application Web, vous devez créer une unité d'application.

Pour créer une unité d'application pour l'application AppExpert à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur l'application pour laquelle vous souhaitez ajouter une unité d'application, puis cliquez sur **Ajouter**.
3. Cliquez sur **Créer**.

Configuration des points de terminaison publics pour une application AppExpert

Après avoir créé toutes les unités d'application dont vous avez besoin, vous devez configurer un ou plusieurs points de terminaison publics pour permettre aux clients d'accéder à l'application Web via l'appliance Citrix ADC.

Pour configurer les points de terminaison publics pour une application AppExpert à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur l'application pour laquelle vous souhaitez configurer les points de terminaison publics, puis cliquez sur **Configurer les points de terminaison publics**.
3. Dans la boîte de dialogue Choisir des points de terminaison publics pour l'application, effectuez l'une des opérations suivantes :
    - Si les points de terminaison de votre choix sont répertoriés dans la boîte de dialogue, activez les cases à cocher correspondantes.
    - Si vous souhaitez spécifier tous les points de terminaison publics, cliquez sur **Activer tout**.

- Si vous souhaitez dissocier les points de terminaison de l'application AppExpert, désactivez les cases à cocher correspondantes.
- Si vous souhaitez créer un point de terminaison public, cliquez sur **Ajouter**. Ensuite, dans la boîte de dialogue Créer un point de terminaison public, configurez les paramètres du point de terminaison, puis cliquez sur **OK**.
  Dans la boîte de dialogue **Créer un point de terminaison public**, vous pouvez spécifier uniquement le nom, l'adresse IP, le port et le protocole du point de terminaison. Vous pouvez spécifier des paramètres supplémentaires de point de terminaison après avoir créé le point de terminaison public. Pour spécifier des paramètres de point de terminaison supplémentaires, après avoir créé le point de terminaison, dans la boîte de dialogue Choisir des points de terminaison publics, cliquez sur le point de terminaison, puis cliquez sur **Ouvrir**. Ensuite, dans la boîte de dialogue **Configurer le point de terminaison public**, fournissez des paramètres supplémentaires, puis cliquez sur **OK** .
  Pour plus d'informations sur les paramètres des boîtes de dialogue **Créer un point de terminaison public** et **Configurer un point de terminaison public**, voir Commutation de contenu.
- Si vous souhaitez modifier un point de terminaison public, cliquez sur le point de terminaison, puis cliquez sur **Ouvrir**. Ensuite, dans la boîte de dialogue **Configurer le point de terminaison public**, modifiez les paramètres du point de terminaison, puis cliquez sur **OK**.
  Pour plus d'informations sur les paramètres de la boîte de dialogue Configurer le point de terminaison public, voir Commutation de contenu.

4. Cliquez sur **Fermer**.

Configuration des points de terminaison publics pour une unité d'application

Pour une unité d'application, vous spécifiez les points de terminaison publics de la même manière que les points de terminaison publics pour une application créée à partir d'un modèle d'application AppExpert. Pour plus d'informations sur la spécification d'un sous-ensemble de points de terminaison pour une unité d'application, voir Configuration des points de terminaison pour une unité d'application.

Pour configurer les points de terminaison d'une unité d'application à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur l'unité d'application pour laquelle vous souhaitez spécifier des points de terminaison publics, puis cliquez sur **Configurer les points de terminaison publics**.
3. Dans la boîte de dialogue **Choisir des points de terminaison publics** pour l'unité d'application, effectuez l'une des opérations suivantes :
   - Si vous spécifiez pour la première fois des points de terminaison pour l'unité d'application, désactivez les cases à cocher correspondant aux points de terminaison que vous ne

souhaitez pas être liés à l'unité d'application.
- Si vous souhaitez spécifier des points de terminaison répertoriés dans la boîte de dialogue mais qui ne sont pas actuellement liés à l'unité d'application, activez les cases à cocher correspondantes.

4. Cliquez sur **OK**.

Configuration des services et des groupes de services pour une application AppExpert

Les services et les groupes de services ne sont disponibles pour les unités d'application qu'après avoir configuré les services et les groupes de services pour l'application AppExpert. Par conséquent, vous devez configurer les services et les groupes de services pour l'application AppExpert avant de configurer les services pour les unités d'application. Tous les services et groupes de services que vous configurez pour une application AppExpert doivent utiliser le même protocole (HTTP ou HTTPS). La procédure de configuration des services et des groupes de services pour une application AppExpert qui n'est pas créée à partir d'un modèle est identique à celle d'une application créée à partir d'un modèle.

Pour configurer un service ou un groupe de services pour l'application AppExpert à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur l'application pour laquelle vous souhaitez configurer des services ou des groupes de services, puis cliquez sur **Configurer les services d'arrière-plan**.
3. Dans la boîte de dialogue Configurer les services principaux, effectuez l'une des opérations suivantes :
   - Pour configurer les services, cliquez sur l'onglet **Services**.
   - Pour configurer des groupes de services, cliquez sur l'onglet **Groupesde services**.
4. Sous l'onglet **Serviceou Groupes de services**, effectuez l'une des opérations suivantes :
   - Si les services ou groupes de services que vous souhaitez sont répertoriés dans l'onglet, activez les cases à cocher correspondantes.
   - Si vous souhaitez spécifier tous les services ou groupes de services, cliquez sur **Activer tout**.
   - Si vous souhaitez créer un service ou un groupe de services, cliquez sur **Ajouter**. Ensuite, dans la boîte de dialogue **Créer un service** ou **Créer un groupe de services** boîte de dialogue, configurez les paramètres du service ou du groupe de services, respectivement, puis cliquez sur **Créer** .
   - Si vous souhaitez modifier un service, cliquez sur le service, puis cliquez sur Ouvrir. Ensuite, dans la boîte de dialogue **Configurer** le **service ou Créer un groupe** de services boîte de dialogue, configurez les paramètres du service ou du groupe de services, respectivement, puis cliquez sur **OK** .

Pour plus d'informations sur les paramètres des boîtes de dialogue Créer un service, Configurer **un service et Créer un groupe** de services, voir Équilibrage de charge.

Configuration des services et des groupes de services pour une unité d'application

Après avoir configuré les services et les groupes de services, vous devez configurer les services et les groupes de services pour chaque unité d'application. Toutefois, cette étape n'est pas nécessaire si chaque service principal héberge tout le contenu associé à l'application Web. Vous configurez les services et les groupes de services pour une unité d'application si le contenu associé à l'unité d'application est hébergé uniquement sur un sous-ensemble des serveurs principaux.

Pour configurer des services ou des groupes de services pour une unité d'application à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur l'unité d'application pour laquelle vous souhaitez configurer un service ou un groupe de services, puis cliquez sur **Configurer les services d'arrière-plan**.
3. Dans la boîte de **dialogue Configurer les services** principaux, effectuez l'une des opérations suivantes :
   - Pour configurer les services, cliquez sur l'onglet **Services**.
   - Pour configurer des groupes de services, cliquez sur l'onglet **Groupes de services** .
4. Dans l'onglet **Services** ou **groupes de services**, effectuez l'une des opérations suivantes :
   - Désactivez les cases à cocher correspondant aux services ou groupes de services que vous ne souhaitez pas configurer pour l'unité d'application. Assurez-vous que les cases à cocher correspondant aux services ou groupes de services que vous souhaitez configurer pour l'unité d'application sont cochées. Ensuite, dans la colonne Poids, spécifiez la pondération que vous souhaitez affecter à chaque service configuré.
   - Pour spécifier tous les services ou groupes de services, cliquez sur **Activer tout**.
5. Dans les onglets **Méthode** et **Persistance** et **Avancé**, spécifiez les paramètres souhaités.
6. Cliquez sur **OK**.

Configuration des stratégies

Les procédures de configuration des stratégies pour une application AppExpert créée sans utiliser de modèle sont les mêmes que celles pour une application AppExpert créée à partir d'un modèle. Pour plus d'informations, voir Configuration des stratégies pour les unités d'application.

Création et gestion de fichiers modèles

August 20, 2021

Après avoir configuré une application AppExpert et l'avoir personnalisée en fonction de vos besoins, vous pouvez créer un modèle à partir de la configuration, puis le partager avec d'autres administrateurs. Vous pouvez également créer un modèle, puis importer le modèle vers d'autres appliances Citrix ADC qui nécessitent une configuration d'application AppExpert similaire. Cela simplifie et accélère le processus de configuration d'applications similaires sur d'autres appareils.

Les fichiers de modèle d'application AppExpert peuvent être exportés soit vers le répertoire de modèles de l'appliance Citrix ADC, soit vers un dossier de votre ordinateur local. Vous pouvez ensuite charger et télécharger les modèles vers et depuis l'appliance Citrix ADC et renommer les modèles stockés dans le répertoire des modèles d'application AppExpert de votre appliance.

Les fichiers de modèle d'application AppExpert peuvent être exportés soit vers le répertoire de modèles de l'appliance Citrix ADC, soit vers un dossier de votre ordinateur local. Vous pouvez ensuite charger et télécharger les modèles vers et depuis l'appliance Citrix ADC et renommer les modèles stockés dans le répertoire des modèles d'application AppExpert de votre appliance.

Exportation d'une application AppExpert vers un fichier modèle

January 21, 2021

Lorsque vous exportez une application AppExpert, toutes les informations de configuration d'application sont exportées vers un fichier de modèle et toutes les informations spécifiques au déploiement sont exportées vers un fichier de déploiement. La chaîne _deployment est automatiquement ajoutée au nom du fichier modèle pour créer le nom du fichier de déploiement. Les deux fichiers sont au format XML. Si vous choisissez d'exporter le fichier de modèle d'application vers l'appliance Citrix ADC, le fichier de modèle est stocké dans le répertoire /nsconfig/nstemplates/applications et le fichier de déploiement est stocké dans le répertoire /nsconfig/nstemplates/applications/deployment_files/. Si vous avez configuré une application Citrix Gateway, vous pouvez choisir d'inclure les stratégies Citrix Gateway dans le modèle.

Pour exporter une application AppExpert vers un fichier modèle à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Application**, sélectionnez une entité d'application, puis cliquez sur **Modifier** .
2. Dans la page **Applications**, cliquez sur le lien **Exporter** en tant que modèle pour exporter les paramètres de configuration et de déploiement de l'application en tant que modèle.
3. Dans le curseur **Exporter l'application**, définissez les paramètres suivants :

a) Nom du fichier du modèle
b) Nom du fichier de déploiement

4. Cliquez sur **Continuer** et **Terminé** .
5. Accédez à **AppExpert** > **Application** et cliquez sur **Gérer les modèles** pour afficher la configuration exportée sous forme de fichiers dans les onglets **Fichier de modèle** et **Fichier de déploiement** .

Exportation d'une configuration de serveur virtuel de commutation de contenu vers un fichier modèle

August 20, 2021

Vous pouvez également exporter une configuration de commutation de contenu en tant que modèle d'application. Vous pouvez exporter une configuration de serveur virtuel de commutation de contenu vers un modèle d'application à partir du volet Content Switching Virtual Servers ou du Visualizer de commutation de contenu. Les informations de configuration, qui comprennent le serveur virtuel de commutation de contenu, tous les serveurs virtuels d'équilibrage de charge associés, les services, les groupes de services et les stratégies, sont exportées vers un fichier de modèle et toutes les informations spécifiques au déploiement sont exportées vers un fichier de déploiement. La chaîne « _deployment » est automatiquement ajoutée au nom du fichier modèle pour créer le nom du fichier de déploiement. Les deux fichiers sont au format XML. Si vous choisissez d'exporter le fichier de modèle d'application vers l'appliance Citrix ADC, le fichier de modèle est stocké dans le répertoire /nsconfig/nstemplates/applications de l'appliance Citrix ADC et le fichier de déploiement est stocké dans le répertoire /nsconfig/nstemplates/applications/deployment_files/.

Pour plus d'informations sur le format des modèles d'application et des fichiers de déploiement, voir Présentation des modèles d'application Citrix ADC et des fichiers de déploiement. Les informations de configuration exportées incluent le serveur virtuel de commutation de contenu, tous les serveurs virtuels d'équilibrage de charge associés, les services, les groupes de services et les stratégies.

Toutefois, si le serveur virtuel de commutation de contenu est déjà configuré comme point de terminaison public pour une application AppExpert, vous ne pouvez pas exporter la configuration vers un fichier modèle. Dans ce scénario, vous devez exporter l'application AppExpert associée vers un modèle.

Pour plus d'informations sur l'exportation d'une application AppExpert vers un fichier de modèle, consultez Exportation d'une application AppExpert vers un fichier de modèle.

Pour exporter une configuration de commutation de contenu vers un fichier de modèle d'application à partir du Visualiseur de commutation de contenu à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Changement de contenu > Serveurs virtuels.

2. Dans le volet d'informations, cliquez sur le nom du serveur virtuel de commutation de contenu dont vous souhaitez exporter la configuration en tant que fichier de modèle, puis cliquez sur Visualizer.
3. Dans le Visualizer de commutation de contenu, cliquez sur l'icône du vserver de commutation de contenu, cliquez sur Tâches associées, puis cliquez sur Créer un modèle.
4. Dans la boîte de dialogue Exporter… en tant que modèle, entrez un nom pour le fichier de modèle, puis effectuez l'une des opérations suivantes :
    - Pour exporter le fichier de modèle vers l'appliance, assurez-vous que l'option Parcourir (Appliance) s'affiche.
    - Pour exporter le fichier modèle sur votre ordinateur, cliquez sur le menu déroulant Parcourir (Appliance), cliquez sur Local, accédez à l'emplacement où vous souhaitez enregistrer le fichier, puis cliquez sur Enregistrer.
5. Fournir les renseignements suivants :
    - **Description de l'introduction**—Tout texte introduisant le modèle d'application AppExpert lors de l'importation. Ce texte s'affiche dans la page Spécifier le nom de l'application de l'Assistant Modèle AppExpert lors de l'importation du modèle.
    - **Description récapitulative**—Tout résumé que vous souhaitez afficher sur la page Récapitulatif de l'Assistant Modèle AppExpert lors de l'importation du modèle.
    - **Auteur**—Nom de l'auteur du modèle.
    - **Major**—Numéro de version principale du modèle.
    - **Minor**—Numéro de version mineure du modèle. Ce numéro est ajouté au numéro de version principale et affiché sur la page Résumé de l'Assistant Modèle AppExpert, lors de l'importation, au format Major.Minor.
6. Cliquez sur OK.

Pour exporter une configuration de commutation de contenu vers un fichier de modèle d'application à partir du volet Serveurs virtuels de commutation de contenu à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Changement de contenu > Serveurs virtuels.
2. Dans le volet d'informations, cliquez sur le nom du serveur virtuel de commutation de contenu dont vous souhaitez exporter la configuration en tant que fichier modèle, puis cliquez sur Créer un modèle AppExpert.
3. Effectuez les étapes 4 à 6 décrites dans **Pour exporter une configuration de commutation de contenu vers un fichier de modèle d'application à partir de la procédure Visualiseur de commutation de contenu**.

Création de variables dans les modèles d'application

August 20, 2021

Les modèles d'application prennent en charge la déclaration de variables dans les expressions de stratégie et les actions configurées pour une application. La possibilité de déclarer des variables dans les expressions de stratégie et les actions vous permet de remplacer les valeurs préconfigurées dans les expressions (par exemple, les paramètres configurables tels que le nom d'hôte d'un serveur ou la cible d'une action Réécriture) par des valeurs correspondant à l'environnement dans lequel vous importez le modèle. Si des variables ont été configurées pour un modèle d'application AppExpert, l'Assistant Modèle AppExpert, qui apparaît lorsque vous importez un modèle d'application AppExpert, inclut une page Spécifier les valeurs de variable sur laquelle vous pouvez spécifier les valeurs appropriées pour les variables configurées pour le modèle.

À titre d'exemple, considérez l'expression de stratégie suivante qui est configurée pour évaluer la valeur de l'en-tête Host dans une requête HTTP :

```
1 HTTP.REQ.HEADER("Host").CONTAINS("server1")
2 <!--NeedCopy-->
```

Si vous voulez que le nom du serveur soit configurable au moment de l'importation, vous pouvez spécifier la chaîne « server1" en tant que variable. Lors de l'importation du modèle, vous pouvez spécifier une nouvelle valeur pour la variable dans l'onglet Variables.

Après avoir créé une variable, vous pouvez effectuer les opérations suivantes :

- Attribuez des chaînes supplémentaires à une variable existante. Après avoir créé une variable pour une chaîne, vous pouvez sélectionner et affecter d'autres parties de la même expression ou d'une expression différente à la variable. Les chaînes que vous attribuez à une variable ne doivent pas nécessairement être les mêmes. Au moment de l'importation, toutes les chaînes affectées à la variable sont remplacées par la valeur que vous fournissez.
- Affichez la ou les chaînes qui sont affectées à la variable.
- Affichez une liste de toutes les entités et paramètres qui utilisent la variable.

Dans l'assistant d'exportation de modèle d'application, vous pouvez définir des variables dans certains champs pour les entités suivantes :

- Stratégies de cache
- Réécrire les stratégies
- Actions de réécriture
- Stratégies de répondeur
- Actions du répondeur

Pour configurer une variable dans une expression de stratégie ou une action à l'aide de l'interface graphique :

1. Accédez à **AppExpert > Variables**.
2. Dans la page **Variables**, cliquez sur **Ajouter**.

3. Dans la page **Créer des variables**, définissez les paramètres suivants.
   Nom. Nom de la variable.

   Portée. Sélectionnez l'étendue comme Global ou Transaction.

   Type. Sélectionnez le type de variable comme texte, ulong, map.

   Expire dans. Entrez la date d'expiration.

   Si Complète*. Action à effectuer si une affectation à une carte dépasse ses entrées max-entrées configurées :
   lru - (par défaut) réutilise l'entrée la moins récemment utilisée dans la carte.
   undef - forcer l'affectation à renvoyer un résultat non défini (Undef) à la stratégie exécutant l'affectation.
   Valeurs possibles : undef, lru Valeur
   par défaut : lru.

   si aucune valeur. Expiration de la valeur en secondes. Si la valeur n'est pas référencée pendant la période d'expiration, elle sera supprimée. 0 (valeur par défaut) signifie pas d'expiration. Valeur minimale : 0, Valeur maximale : 31622400

   Valeur d'init. Valeur d'initialisation pour cette variable, à laquelle une variable singleton ou une entrée de mappage sera définie si elle est référencée avant qu'une action d'affectation ne lui ait assigné une valeur. Si une valeur a déjà été affectée à la variable singleton ou à l'entrée de carte, la définition de ce paramètre n'aura aucun effet sur cette valeur de variable. Par défaut : 0 pour ulong, NULL pour le texte Longueur maximale : 127

   Commentaires. Une brève description de la variable.

4. Cliquez sur **Fermer**.

Chargement et téléchargement de fichiers de modèle

August 20, 2021

Les fichiers de modèle peuvent être téléchargés depuis votre ordinateur local vers l'appliance Citrix ADC ou téléchargés depuis l'appliance vers votre ordinateur local. Sur l'appliance, les modèles d'application AppExpert sont toujours stockés dans le répertoire des modèles d'application AppExpert, c'est-à-dire `/nsconfig/nstemplates/applications/`.

Pour télécharger un modèle d'application AppExpert à partir de votre ordinateur local vers l'appliance Citrix ADC :

1. Accédez à **AppExpert > Applications**.
2. Dans le volet d'informations, cliquez sur **Gérer les modèles**.

3. Dans la boîte de dialogue Modèles d'application, cliquez sur **Charger**.
4. Accédez au répertoire dans lequel le fichier de modèle est stocké, cliquez sur le fichier de modèle, puis cliquez sur **Sélectionner**.

   Le fichier modèle est téléchargé dans le répertoire des modèles d'application AppExpert de l'appliance.

Pour télécharger un modèle d'application AppExpert à partir de l'appliance Citrix ADC sur votre ordinateur local :

1. Accédez à **AppExpert > Applications**.
2. Dans le volet d'informations, cliquez sur **Gérer les modèles**.
3. Dans la boîte de dialogue Modèles d'application, cliquez sur le modèle d'application AppExpert que vous souhaitez télécharger, puis cliquez sur **Télécharger**.
4. Accédez au répertoire dans lequel vous souhaitez enregistrer le fichier, puis cliquez sur **Enregistrer**.

Présentation des modèles d'application Citrix ADC et des fichiers de déploiement

January 21, 2021

Lorsque vous exportez une application Citrix ADC, les deux fichiers suivants sont automatiquement créés :

- **Fichier modèle d'application Citrix ADC**. Contient des informations de configuration d'application telles que les unités d'application, les règles et les stratégies configurées.
- **Fichier de déploiement**. Contient des informations spécifiques au déploiement telles que les points de terminaison publics, les services, les adresses IP associées et les variables configurées.

Dans un fichier modèle ou un fichier de déploiement, chaque unité d'informations de configuration d'application est encapsulée dans un élément XML spécifique destiné à ce type d'unité. Par exemple, chaque point de terminaison public et les détails de terminaison associés sont encapsulés dans les balises <appendpoint> et </appendpoint>, et tous les éléments de terminaison sont encapsulés dans les balises <appendpoint_list> et </appendpoint_list>.

Remarque : Après avoir exporté une application Citrix ADC, vous pouvez ajouter des éléments, supprimer des éléments et modifier des éléments existants avant d'importer l'application dans une appliance Citrix ADC.

Exemple de modèle d'application Citrix ADC

Voici un exemple de fichier modèle créé à partir d'une application Citrix ADC appelée **SharePoint_TEAM_Site** :

```
<?xml version="1.0" encoding="UTF-8" ?>
<template>
<template_info>
   <application_name>SharePoint_Team_Site</application_name>
   <templateversion_major>1</templateversion_major>
   <templateversion_minor>1</templateversion_minor>
   <author>Ed</author>
   <introduction>An application for managing a SharePoint team site
      with images, reports, and, XML content.</introduction>
   <summary>This template includes variables</summary>
   <version_major>9</version_major>
   <version_minor>3</version_minor>
   <build_number>38</build_number>
</template_info>
<apptemplate>
   <rewrite>
      <rewriteaction_list>
         <rewriteaction>
            <name>Rw_name</name>
            <type>replace</type>
            <target>HTTP.REQ.BODY(10000).AFTER_REGEX(re/number/).
               BEFORE_REGEX(re/address/)</target>
            <stringbuilderexpr>"NA"</stringbuilderexpr>
            <allow_unsafe_pi1>NO</allow_unsafe_pi1>
         </rewriteaction>
         <rewriteaction>
            .
            .
            .
         </rewriteaction>
         .
         .
         .
      </rewriteaction_list>
      <rewritepolicy_list>
         <rewritepolicy>
            <name>Rw_number_NA</name>
            <rule>HTTP.REQ.BODY(100000).CONTAINS("admin")</rule>
            <action>Rw_name</action>
         </rewritepolicy>
```



```
39          <rewritepolicy>
40             .
41             .
42             .
43          </rewritepolicy>
44          .
45          .
46          .
47       </rewritepolicy_list>
48    </rewrite>
49    <appunit_list>
50       <appunit>
51          <name>SharePoint_Team_Sitedefault</name>
52          <rule />
53          <expressiontype>PE</expressiontype>
54          <servicetype>HTTP</servicetype>
55          <ipv46>0.0.0.0</ipv46>
56          <ipmask>*</ipmask>
57          <port>0</port>
58          <range>1</range>
59          <persistencetype>NONE</persistencetype>
60          <timeout>2</timeout>
61          <persistencebackup>NONE</persistencebackup>
62          <backuppersistencetimeout>2</backuppersistencetimeout>
63          <lbmethod>LEASTCONNECTION</lbmethod>
64          <persistmask>255.255.255.255</persistmask>
65          <v6persistmasklen>128</v6persistmasklen>
66          <pq>OFF</pq>
67          <sc>OFF</sc>
68          <m>IP</m>
69          <datalength>0</datalength>
70          <dataoffset>0</dataoffset>
71          <sessionless>DISABLED</sessionless>
72          <state>ENABLED</state>
73          <connfailover>DISABLED</connfailover>
74          <clttimeout>180</clttimeout>
75          <somethod>NONE</somethod>
76          <sopersistence>DISABLED</sopersistence>
77          <redirectportrewrite>DISABLED</redirectportrewrite>
78          <downstateflush>DISABLED</downstateflush>
79          <gt2gb>DISABLED</gt2gb>
80          <ipmapping>0.0.0.0</ipmapping>
81          <disableprimaryondown>DISABLED</disableprimaryondown>
82          <insertvserveripport>OFF</insertvserveripport>
83          <authentication>OFF</authentication>
```



```
            <authn401>OFF</authn401>
            <push>DISABLED</push>
            <pushlabel>none</pushlabel>
            <l2conn>OFF</l2conn>
         </appunit>
         <appunit>
            .
            .
            .
         </appunit>
         .
         .
         .
      </appunit_list>
      </apptemplate>
      <parameters>
         <property_list>
            <property>
               <variable_definition_list>
                  <variable_definition>
                     <name>body_size</name>
                     <defaultvalue>10000</defaultvalue>
                     <description>Evaluation Scope</description>
                     <startindex>14</startindex>
                     <length>5</length>
                  </variable_definition>
                  .
                  .
                  .
               </variable_definition_list>
               <object_type>rewriteaction</object_type>
               <object_name>Rw_name</object_name>
               <name>target</name>
            </property>
            .
            .
            .
         </property_list>
      </parameters>
</template>
<!--NeedCopy-->
```


Exemple de fichier de déploiement

Voici le fichier de déploiement associé à l'application **SharePoint_Team_Site** dans l'exemple précédent :

```
<?xml version="1.0" encoding="UTF8" ?>
<template_deployment>
   <template_info>
      <application_name>SharePoint_Team_Site</application_name>
      <templateversion_major>1</templateversion_major>
      <templateversion_minor>1</templateversion_minor>
      <author>Ed</author>
      <introduction>An application for managing a SharePoint team site
         with images, reports, and, XML content.</introduction>
      <summary>This template includes variables</summary>
      <version_major>9</version_major>
      <version_minor>3</version_minor>
      <build_number>38</build_number>
   </template_info>
   <appendpoint_list>
      <appendpoint>
         <ipv46>10.111.111.1</ipv46>
         <port>80</port>
         <servicetype>HTTP</servicetype>
      </appendpoint>
   </appendpoint_list>
   <service_list>
      <service>
         <ip>10.102.29.5</ip>
         <port>80</port>
         <servicetype>HTTP</servicetype>
      </service>
      <service>
         .
         .
         .
      </service>
      .
      .
      .
   </service_list>
   <variable_list>
      <variable>
         <name>body_size</name>
         <description>Evaluation Scope</description>
```



```
            <value>10000</value>
        </variable>
        <variable>
            .
            .
            .
        </variable>
        .
        .
        .
    </variable_list>
</template_deployment>
<!--NeedCopy-->
```

Suppression d'un fichier modèle

January 21, 2021

Si vous n'avez plus besoin d'un modèle d'application et de sa configuration, vous pouvez le supprimer. Lorsque vous supprimez un modèle, le fichier XML du modèle qui est stocké dans le répertoire du modèle d'application est supprimé. Lorsque vous supprimez un fichier modèle, vous êtes invité à confirmer la suppression. Cliquez sur **Oui** pour confirmer et supprimer le fichier sélectionné du répertoire.

Pour supprimer un fichier de modèle du répertoire de modèle d'application à l'aide de l'interface graphique :

1. Accédez à **AppExpert > Applications**, puis cliquez sur **Gérer le modèle** . Sélectionnez un fichier dans la page de l'onglet **Fichiers de modèle** ou de l'onglet **Fichiers de déploiement**, puis cliquez sur **Supprimer** .

Applications de Gateway Citrix

January 21, 2021

Lorsque vous configurez une application AppExpert pour gérer une application Web via l'appliance Citrix® Citrix ADC®, vous créez également un ensemble d'unités d'application et configurez un ensemble de stratégies d'optimisation du trafic et de sécurité pour chaque unité. Les stratégies que vous configurez pour chaque unité d'application (stratégies pour des fonctionnalités telles que Compression, Mise en cache et Réécriture) évaluent le trafic destiné uniquement à cette unité. En plus de

ces stratégies, vous pouvez configurer les stratégies Access Gateway pour l'application dans son ensemble afin d'optimiser le trafic de l'application lors de l'accès via Access Gateway. La fonctionnalité Applications de passerelle d'accès vous permet de configurer les stratégies de passerelle d'accès (autorisation, trafic, accès sans client et compression TCP) pour une application AppExpert. Après avoir configuré les stratégies Citrix Gateway pour les applications AppExpert, vous pouvez inclure la configuration de stratégie dans les modèles d'application AppExpert que vous créez.

Vous pouvez également configurer des stratégies Citrix Gateway pour les sous-réseaux intranet, les partages de fichiers et d'autres ressources réseau. Enfin, vous pouvez créer des signets pour les applications AppExpert et certaines ressources si vous souhaitez que les utilisateurs puissent y accéder à partir de la page d'accueil de Citrix Gateway.

Vous pouvez configurer les entités dans la fonctionnalité Applications Citrix Gateway uniquement à l'aide de l'interface graphique.

Fonctionnement d'une application Citrix Gateway

Lorsque vous créez une application AppExpert dans le nœud Applications de l'interface graphique, une application Access Gateway correspondante est automatiquement créée dans le nœud Applications Access Gateway. En outre, une règle qui utilise le point de terminaison public configuré de l'application AppExpert est automatiquement créée pour l'entrée de l'application Access Gateway. Si plusieurs points de terminaison sont configurés pour l'application AppExpert, la règle inclut tous les points de terminaison publics configurés. L'appliance Citrix ADC utilise cette règle pour appliquer toutes les stratégies Access Gateway configurées au trafic reçu au point de terminaison public de l'application AppExpert. Le trafic reçu au point de terminaison public de l'application AppExpert est d'abord évalué par rapport aux stratégies Citrix Gateway, puis évalué par rapport aux stratégies configurées pour les unités d'application AppExpert.

La règle créée pour les stratégies d'accès sans client pour une application Access Gateway est une expression avancée qui utilise également le point de terminaison public configuré pour l'application AppExpert. Par conséquent, avant de configurer les stratégies Citrix Gateway pour une application AppExpert, vous devez configurer les points de terminaison publics pour l'application AppExpert.

Lorsque vous incluez la configuration Citrix Gateway dans un modèle d'application, les informations spécifiques au déploiement, telles que les informations d'adresse IP et de port, et la règle créée à partir de ces informations ne sont pas incluses dans le modèle.

Fonctionnement d'une configuration Citrix ADC pour un partage de fichiers

Sur l'appliance Citrix ADC, vous pouvez configurer des stratégies d'autorisation pour un partage de fichiers hébergé sur le réseau de votre organisation.

Lorsque vous créez un partage de fichiers, vous spécifiez un nom pour le partage de fichiers et le chemin d'accès réseau au partage de fichiers. Dans le chemin d'accès réseau, vous pouvez spécifier le nom du serveur ou l'adresse IP du serveur. Une règle qui utilise les composants du chemin de partage de fichiers est automatiquement créée pour le partage de fichiers. Cette règle permet à l'appliance d'identifier les demandes de fichiers hébergés sur le serveur de partage de fichiers. Toutes les stratégies d'autorisation configurées pour le partage de fichiers sont appliquées aux demandes entrantes.

La configuration de Citrix ADC pour un partage de fichiers ne peut pas être enregistrée dans les modèles d'application AppExpert.

Fonctionnement d'une configuration Citrix ADC pour un sous-réseau intranet

Pour les sous-réseaux intranet qui font partie de votre réseau, vous pouvez configurer des stratégies d'autorisation, de trafic et de compression TCP sur l'appliance Citrix ADC. Lorsque vous ajoutez un sous-réseau intranet, vous spécifiez l'adresse IP et le masque de réseau du sous-réseau intranet. Une règle qui utilise ces deux paramètres est automatiquement créée pour le sous-réseau intranet. L'appliance applique les stratégies configurées à toute demande dont l'adresse IP de destination et le masque de réseau sont respectivement définis sur l'adresse IP et le masque de réseau du sous-réseau.

La configuration de Citrix ADC pour un sous-réseau intranet ne peut pas être enregistrée dans les modèles d'application AppExpert.

Fonctionnement de la catégorie des autres ressources

La catégorie Autres ressources vous permet de configurer des stratégies Access Gateway pour n'importe quelle ressource réseau à l'aide d'une règle de votre choix. Lorsque vous configurez l'appliance Citrix ADC pour traiter les demandes de la ressource réseau, vous configurez une expression classique pour identifier les demandes associées à la ressource réseau. Vous pouvez configurer les stratégies Autorisation, Trafic, Accès sans client et Compression TCP pour une ressource réseau dans Autres ressources. L'appliance Citrix ADC applique les stratégies Citrix Gateway configurées à toutes les demandes correspondant à la règle configurée.

La configuration de Citrix ADC pour une ressource réseau dans Autres ressources ne peut pas être enregistrée dans les modèles d'application AppExpert.

Conventions de dénomination des entités

La fonctionnalité Applications Citrix Gateway applique une convention d'affectation de noms pour certaines entités que vous créez dans cette fonctionnalité. Par exemple, les noms des profils que vous créez pour les stratégies de trafic pour un sous-réseau intranet commencent toujours par une chaîne composée du nom du sous-réseau intranet suivi d'un trait de soulignement (_). Le nom que vous fournissez pour l'entité est ajouté à cette chaîne. Si le nom d'un sous-réseau est « subnet1 », le nom du

profil commence par “subnet1_.” Lorsqu’une telle convention de dénomination est requise (dans la zone de texte dans laquelle vous tapez le nom d’une entité, par exemple), l’interface utilisateur insère automatiquement la chaîne avec laquelle le nom de l’entité doit commencer et ne vous permet pas de le modifier.

Ajout de sous-réseaux intranet

August 20, 2021

Vous pouvez spécifier des stratégies d’autorisation et de trafic pour le trafic lié aux sous-réseaux intranet configurés dans votre réseau. Les règles de ces stratégies sont créées automatiquement à l’aide des paramètres que vous spécifiez pour le sous-réseau.

Pour configurer un sous-réseau intranet à l’aide de l’interface graphique :

1. Dans le volet de navigation de l’interface graphique, développez **AppExpert**, puis cliquez sur Access Gateway Applications.
2. Dans le volet d’informations, effectuez l’une des opérations suivantes :
   - Pour ajouter un sous-réseau intranet, cliquez sur **Sous-réseaux intranet**, puis cliquez sur **Ajouter**.
   - Pour modifier un sous-réseau intranet, cliquez sur un sous-réseau intranet, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Créer un sous-réseauintranet ou Configurer un sous-réseau** intranet, procédez comme suit :
   a) Dans la zone Nom, tapez un nom pour le sous-réseau intranet que vous ajoutez. Ce paramètre ne peut pas être modifié pour un sous-réseau intranet existant.
   b) Dans la zone Adresse IP, tapez l’adresse IP du sous-réseau intranet.
   c) Dans la zone Masque réseau, tapez le masque de réseau qui sera utilisé pour le sous-réseau intranet.
   d) Cliquez sur **Créer** ou **OK**, puis cliquez sur **Fermer**.

Ajout d’autres ressources

October 5, 2021

Pour une ressource réseau que vous ajoutez aux autres ressources, vous devez configurer l’expression de stratégie avancée qui identifie le sous-ensemble du trafic associé à la ressource.

Pour configurer une ressource dans d’autres ressources à l’aide de l’interface graphique :

1. Dans le volet de navigation de l'interface graphique, développez AppExpert, puis cliquez sur **Access Gateway Applications**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour ajouter une ressource, cliquez sur **Autres ressources**, puis sur **Ajouter**.
   - Pour modifier une ressource, cliquez sur une ressource, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Créer une ressourceou Configurer** une ressource, procédez comme suit :
   a) Dans la zone Nom, tapez le nom de la ressource que vous ajoutez. Ce paramètre ne peut pas être modifié pour une ressource existante.
   b) Dans la zone Règle, tapez la règle qui identifiera le sous-ensemble du trafic associé à la ressource que vous ajoutez.
   Vous pouvez également cliquer sur **Configurer**, puis créer la règle dans la boîte de dialogue **Créer une expression** .
   c) Cliquez sur **Créer** ou sur **OK**, puis cliquez sur **Fermer**.

Configuration des stratégies d'autorisation

August 20, 2021

Vous pouvez configurer des stratégies d'autorisation Citrix Gateway pour les utilisateurs et groupes AAA pour qu'ils puissent accéder à une ressource.

Pour configurer les autorisations permettant à un utilisateur ou un groupe AAA d'accéder à une ressource à l'aide de l'interface graphique :

1. Dans le volet de navigation de l'interface graphique, développez AppExpert, puis cliquez sur **Access Gateway Applications**.
2. Dans le volet d'informations, dans la colonne Autorisation, cliquez sur l'icône correspondant à l'application, au partage de fichiers, au sous-réseau intranet ou à la ressource pour laquelle vous souhaitez configurer des stratégies d'autorisation pour les utilisateurs et groupes AAA.
3. Procédez comme suit :
   - Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez configurer des autorisations se trouve déjà dans l'arborescence Groups/Utilisateurs, faites glisser l'utilisateur ou le groupe de l'arborescence Groups/Utilisateurs vers le nœud Utilisateurs ou Groupes de l'<application name>arborescence. Ensuite, cliquez avec le bouton droit sur l'utilisateur ou le groupe et cliquez sur **Autoriser**.
   - Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez configurer des autorisations n'est pas configuré sur l'appliance, dans l'<application name>arborescence, cliquez avec le bouton droit sur Utilisateurs ou groupes, puis cliquez sur **Ajouter** . Dans la boîte de dialogue Créer un **groupeAAA ou Créer un utilisateur**AAA, renseignez les valeurs, cliquez

sur**Créer**, puis cliquez sur**Fermer**.
L'utilisateur ou le groupe est créé avec l'autorisation définie sur Autoriser. Pour modifier le paramètre d'autorisation, cliquez avec le bouton droit sur le groupe ou l'utilisateur, puis cliquez sur le paramètre d'autorisation.

4. Cliquez sur **Fermer**.

Configuration des stratégies de trafic

October 5, 2021

Les stratégies de trafic que vous configurez pour les ressources du nœud Applications Citrix Gateway contrôlent les connexions des clients à l'application. Il n'est pas nécessaire de configurer une règle pour la ressource. La règle est créée automatiquement lorsque vous créez la ressource. Il suffit d'associer un profil de demande à la stratégie de trafic. Dans le profil de trafic, vous spécifiez des paramètres tels que le protocole, le délai d'expiration de l'application et l'association des types de fichiers.

Pour configurer les stratégies de trafic pour une ressource

1. Dans le volet de navigation de l'interface graphique, développez AppExpert, puis cliquez sur Access Gateway Applications.
2. Dans le volet d'informations, dans la colonne Trafic, cliquez sur l'icône fournie pour l'application, le partage de fichiers, le sous-réseau intranet ou la ressource pour laquelle vous souhaitez configurer des stratégies de trafic.
3. Dans la boîte de dialogue **Configurer les stratégies de trafic**, procédez comme suit :
   - Pour spécifier une stratégie de trafic existante, cliquez sur **Insérer une stratégie**, puis, dans la colonne Nom de la stratégie, cliquez sur le nom de la stratégie.
   - Pour configurer une nouvelle stratégie, cliquez sur Insérer une stratégie, puis, dans la colonne Nom de la stratégie, cliquez sur Nouvelle stratégie. Dans la boîte de dialogue Créer une stratégie de trafic, dans la zone Nom, après le trait de soulignement (_), tapez un nom pour la stratégie. Ensuite, dans Profil de demande, sélectionnez un profil de demande existant ou cliquez sur Nouveau pour configurer un nouveau profil de demande. Vous pouvez également sélectionner un profil existant, puis cliquer sur Modifier pour modifier le profil.
     Pour plus d'informations sur la configuration d'une stratégie ou d'un profil de trafic, consultez Citrix Gateway.
   - Pour modifier une stratégie que vous avez insérée, dans la colonne Nom de la stratégie, cliquez sur le nom de la stratégie, puis cliquez sur Modifier la stratégie. Pour modifier uniquement le profil associé, dans la colonne Profil, cliquez sur le nom du profil, puis sur **Modifier le profil**.

- Pour régénérer les priorités attribuées aux stratégies, cliquez sur **Régénérer les priorités**.
- Pour spécifier une nouvelle valeur de priorité pour une stratégie, dans la colonne Priorité, double-cliquez sur la priorité attribuée, puis entrez la valeur souhaitée.
- Pour délier une stratégie, cliquez sur la stratégie, puis cliquez sur **Délier la stratégie**.

4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des stratégies d'accès sans client

October 5, 2021

L'accès sans client, lorsqu'il est configuré pour une ressource sur l'appliance Citrix ADC, permet aux utilisateurs finaux d'accéder à la ressource sans utiliser le logiciel client Citrix Gateway. Les utilisateurs peuvent utiliser des navigateurs Web pour accéder à des ressources telles qu'Outlook Web Access. Vous configurez l'accès sans client pour une ressource en configurant une stratégie d'accès sans client associée à un profil d'accès sans client.

Pour configurer une stratégie d'accès sans client pour une ressource dans le nœud Applications Citrix Gateway, procédez comme suit :

1. Dans le volet de navigation de l'interface graphique, développez **AppExpert**, puis cliquez sur **Applications Access Gateway**.
2. Dans le volet d'informations, dans la colonne **Accès sans client**, cliquez sur l'icône de l'application, du partage de fichiers, du sous-réseau intranet ou de la ressource pour laquelle vous souhaitez configurer une stratégie d'accès sans client.
3. Dans la boîte de dialogue **Configurer les stratégies d'accès sans client**, procédez comme suit :
   - Pour spécifier une stratégie d'accès sans client existante, cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur le nom de la stratégie.
   - Pour configurer une nouvelle stratégie d'accès sans client, cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur **Nouvelle stratégie**. Dans la boîte de dialogue **Créer une stratégie d'accès sans client**, dans la zone Nom, après le trait de soulignement (_), tapez un nom pour la stratégie. Ensuite, dans Profil, sélectionnez un profil existant ou cliquez sur Nouveau pour configurer un nouveau profil. Vous pouvez également sélectionner un profil existant, puis cliquer sur **Modifier** pour modifier le profil.
     Pour plus d'informations sur la configuration d'une stratégie ou d'un profil d'accès sans client, consultez Citrix Gateway.
   - Pour modifier une stratégie que vous avez insérée, dans la colonne Nom de la stratégie, cliquez sur le nom de la stratégie, puis sur **Modifier la stratégie**. Pour modifier uniquement le profil associé, dans la colonne Profil, cliquez sur le nom du profil, puis sur Modifier le profil.

- Pour spécifier une nouvelle valeur de priorité pour une stratégie, dans la colonne Priorité, double-cliquez sur la priorité attribuée, puis entrez la valeur souhaitée.
- Pour délier une stratégie, cliquez sur la stratégie, puis cliquez sur **Délier la stratégie**.

4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des stratégies de compression TCP

October 5, 2021

Vous pouvez configurer des stratégies de compression TCP pour une application afin d'augmenter ses performances. La compression TCP réduit la latence du réseau, réduit les besoins en bande passante et augmente la vitesse de transmission. Lorsque vous configurez une stratégie de compression TCP, vous associez une action de compression à la stratégie. L'action de compression spécifie Compress, GZIP, Deflate, ou NoCompress comme type de compression. Pour plus d'informations sur les stratégies de compression et les actions de compression, consultez Citrix Gateway.

Pour configurer une stratégie de compression TCP pour une ressource dans le nœud Applications Citrix Gateway

1. Dans le volet de navigation de l'interface graphique, développez **AppExpert**, puis cliquez sur **Applications Access Gateway**.
2. Dans le volet d'informations, dans la colonne Compression TCP, cliquez sur l'icône de l'application, du partage de fichiers, du sous-réseau intranet ou de la ressource pour laquelle vous souhaitez configurer une stratégie de compression TCP.
3. Dans la boîte de dialogue **Configurer les stratégies de compression TCP**, procédez comme suit :
   - Pour spécifier une stratégie de compression TCP existante, cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur le nom de la stratégie.
   - Pour créer une nouvelle stratégie de compression TCP, cliquez sur Insérer une stratégie, puis, dans la colonne Nom de la stratégie, cliquez sur Nouvelle stratégie. Dans la boîte de dialogue Créer une stratégie de compression TCP, dans la zone Nom de la stratégie, après le trait de soulignement (« _ »), tapez un nom pour la stratégie. Ensuite, dans Action, sélectionnez une action existante ou cliquez sur Nouveau et configurez une nouvelle action. Vous pouvez également cliquer sur Affichage pour afficher le type de compression configuré.
     Pour plus d'informations sur la configuration d'une stratégie ou d'une action de compression TCP, consultez Citrix Gateway, Advanced Edition at Citrix Gateway.
   - Pour modifier une stratégie que vous avez insérée, dans la colonne Nom de la stratégie, cliquez sur le nom de la stratégie, puis sur **Modifier la stratégie**.
   - Pour régénérer les priorités attribuées aux stratégies, cliquez sur **Régénérer les priorités**.

- Pour spécifier une nouvelle valeur de priorité pour une stratégie, dans la colonne Priorité, double-cliquez sur la priorité attribuée, puis entrez la valeur souhaitée.
- Pour délier une stratégie, cliquez sur la stratégie, puis cliquez sur **Délier la stratégie**.

4. Cliquez sur **Appliquer les modifications,** puis cliquez sur **Fermer**.

Configurer les signets

August 20, 2021

Vous pouvez configurer des signets pour les applications internes ou les ressources disponibles pour un utilisateur autorisé. Vous pouvez ensuite lier le signet à un utilisateur, un groupe d'utilisateurs ou un serveur virtuel globalement et l'activer pour l'utilisateur dans l'interface d'accès. Les liens de signet que vous créez apparaissent dans les volets des sites Web sous les sites Web d'entreprise.

Pour plus d'informations, consultez la rubrique Création et application de liens Web .

AppQoE

October 5, 2021

AppQoE (Application level Quality of Experience) intègre plusieurs fonctionnalités de sécurité basées sur des stratégies existantes de l'appliance Citrix ADC dans une seule fonctionnalité intégrée qui tire parti d'un nouveau mécanisme de mise en file d'attente, une mise en file d'attente équitable. La mise en file d'attente pondérée gère les demandes vers des serveurs Web et des applications à charge équilibrée au niveau du serveur virtuel plutôt qu'au niveau du service, ce qui lui permet de gérer la file d'attente de toutes les demandes vers un site Web ou une application en tant que groupe avant l'équilibrage de charge, plutôt que comme des flux distincts après l'équilibrage de charge.

- **Surcharge simple.** Tout serveur, quelle que soit sa robustesse, ne peut accepter qu'un nombre limité de connexions en même temps. Lorsqu'un site Web ou une application protégé reçoit trop de demandes en même temps, la fonction Protection contre les surtensions détecte la surcharge et met en file d'attente les connexions excédentaires jusqu'à ce que le serveur puisse les accepter. La fonctionnalité AppQoE affiche une autre page Web qui avertit les utilisateurs que la ressource demandée n'est pas disponible.
- **Attaques par déni de service (DOS).** Toute ressource destinée au public est vulnérable aux attaques dont le but est de faire tomber ce service et d'en interdire l'accès aux utilisateurs légitimes. La fonction de protection contre les surtensions permet de gérer les attaques DOS en plus des autres types de charge élevée. En outre, la fonctionnalité de protection par déni de

service HTTP cible les attaques DOS contre vos sites Web, en envoyant des défis aux attaquants suspects et en abandonnant les connexions si les clients n'envoient pas de réponse appropriée.

Jusqu'à la version actuelle du système d'exploitation Citrix ADC, ces fonctionnalités ont été implémentées au niveau du service, ce qui signifie que chaque service a reçu ses propres files d'attente. Bien que les files d'attente de niveau service fonctionnent, elles présentent également certains inconvénients, dont la plupart sont dus au fait que l'appliance Citrix ADC doit effectuer des demandes d'équilibrage de charge avant d'implémenter l'une des fonctionnalités de protection qui dépendent de la mise en file d'attente. L'implémentation de fonctions de protection avant la mise en file d'attente présente divers avantages, dont certains sont énumérés ci-dessous :

- Les connexions ne sont pas vidé si un service transitions état, comme elles le sont dans une file d'attente de niveau service.
- Pendant les périodes de charge élevée, telles qu'une attaque par déni de service, et les déni de service HTTP entrent en jeu avant l'équilibrage de charge, ce qui permet à ces fonctionnalités de détecter et de détourner le trafic indésirable ou de priorité inférieure de l'équilibreur de charge avant que l'équilibreur de charge ne puisse y faire face.

En plus de mettre en œuvre une file d'attente équitable, AppQoE intègre un ensemble de fonctionnalités qui fournissent chacun un ensemble d'outils différents pour atteindre un objectif commun : protéger vos ressources réseau contre une demande excessive ou inappropriée. L'intégration de ces fonctionnalités dans un cadre commun vous permet de les configurer et de les implémenter plus facilement.

Activation d'AppQoE

August 20, 2021

Pour configurer AppQoE, vous devez d'abord activer la fonctionnalité.

Pour activer AppQoE à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- activer la fonction ns appqoe
- show ns feature

Exemple :

```
1 > enable ns feature appqoe
2  Done
3 > show ns feature
4
```



```
5          Feature                        Acronym              Status
6          -------                        -------              ------
7   1)     Web Logging                    WL                   ON
8   2)     Surge Protection               SP                   ON
9   3)     Load Balancing                 LB                   ON
10  ...
11  1)     AppQoE                         AppQoE               ON
12  Done
13 <!--NeedCopy-->
```

Pour activer AppQoE à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans le volet d'informations, cliquez sur **Configurer les fonctionnalités avancées**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, activez la case à cocher **AppQoE** .
4. Cliquez sur **OK**.

Actions AppQoE

August 20, 2021

Après avoir activé la fonctionnalité AppQoE, vous devez configurer une ou plusieurs actions pour la gestion des demandes.

> **Important :**
>
> Aucun paramètre spécifique n'est requis pour créer une action, mais vous devez inclure au moins un paramètre sinon vous ne pouvez pas créer l'action.

Pour configurer une action AppQoE à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appqoe action <name> [-priority <priority>] [-respondWith (ACS|NS)[<customfile>] [-altContentSvcName <string>] [-altContentPath <string>] [-maxConn <positive_integer>] [-delay <usecs>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-dosTrigExpression <expression>] [-dosAction (**SimpleResponse** | **HICResponse**)]`
- `show appqoe action`

Exemple

Pour configurer la file d'attente de priorité avec des profondeurs de file d'attente de stratégie de 10 et 1000 pour les files d'attente de priorité moyenne et inférieure, respectivement :

```
> add appqoe action appqoe-act-basic-prhigh -priority HIGH
 Done

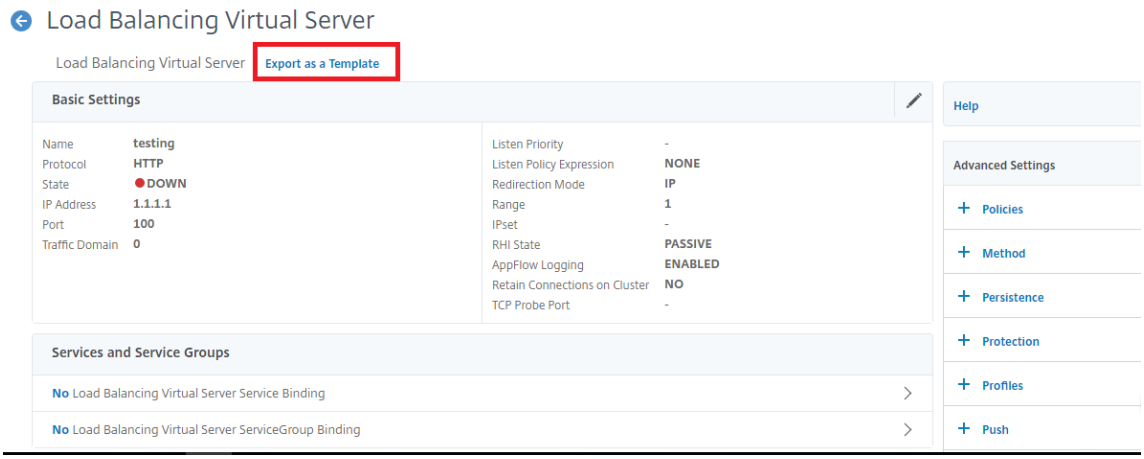
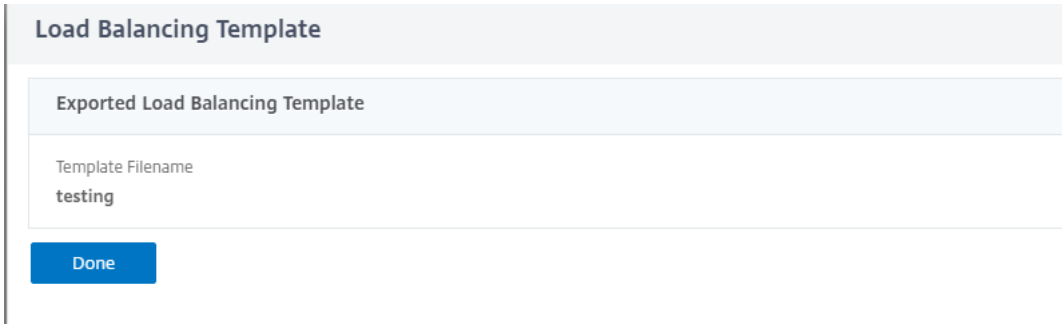
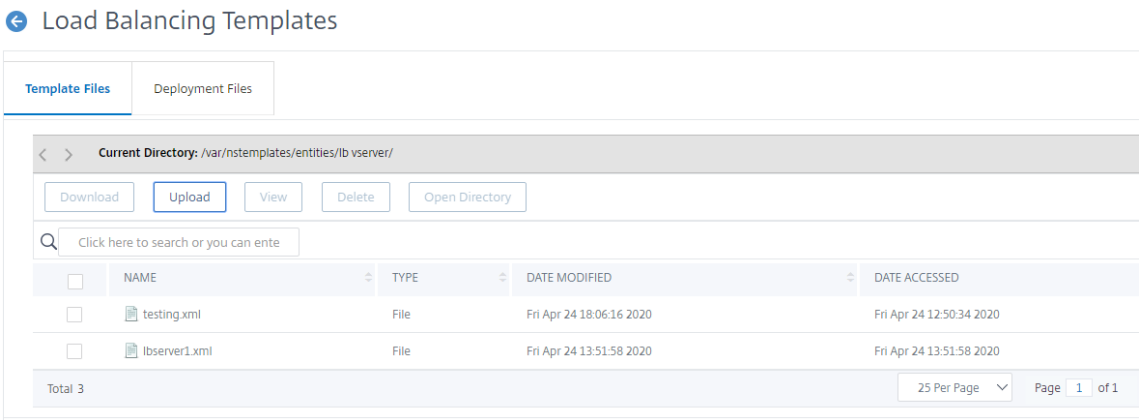
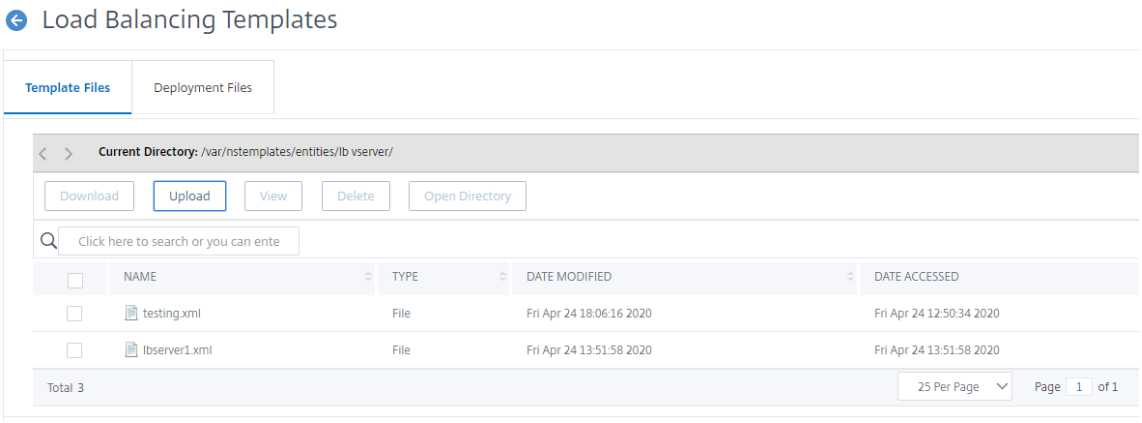
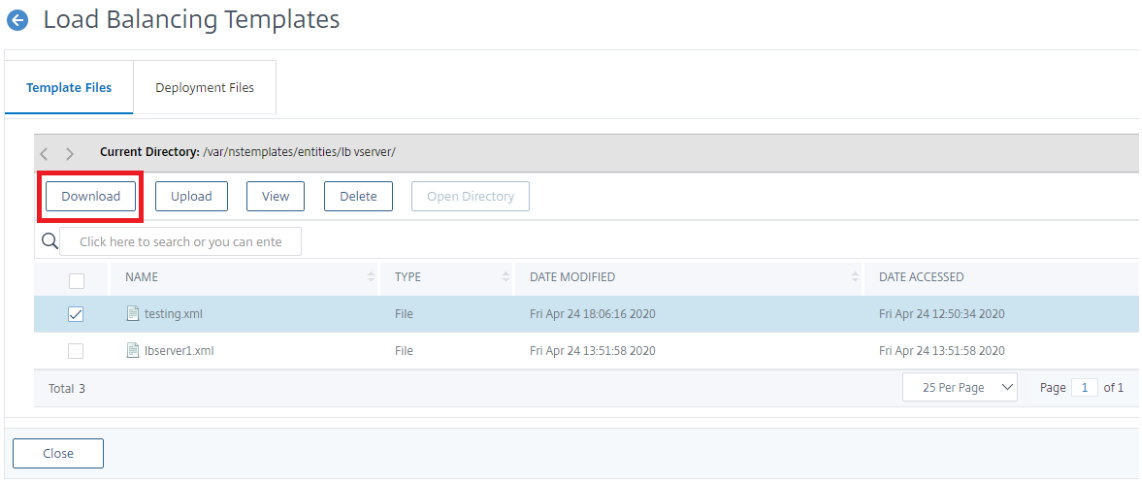
> add appqoe action appqoe-act-basic-prmedium -priority MEDIUM -
   polqDepth 10
 Done

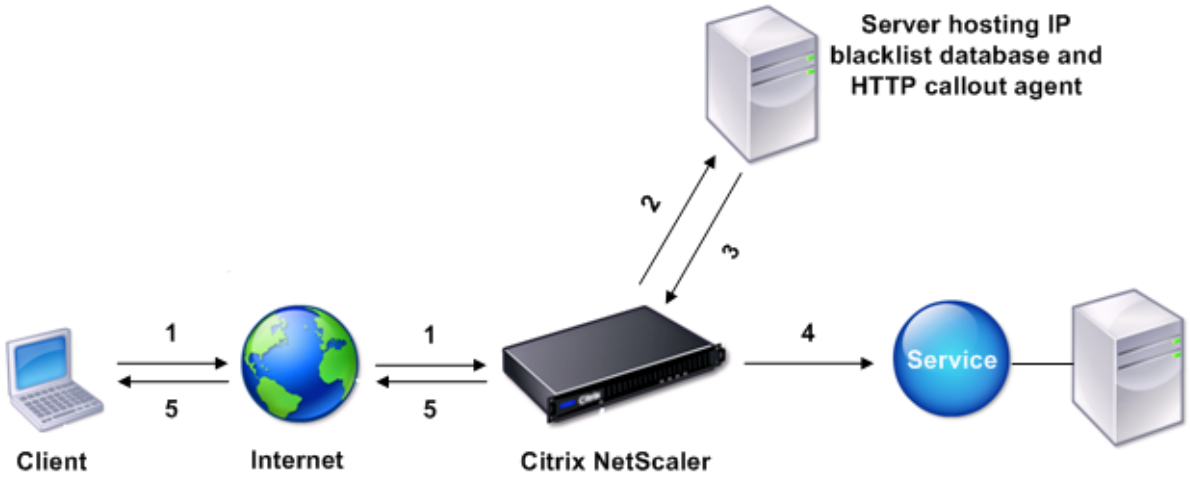
> add appqoe action appqoe-act-basic-prlow -priority LOW -polqDepth
   1000
 Done

> show appqoe action

1.       Name: appqoe-act-basic-prhigh
        ActionType: PRIORITY_QUEUING
        Priority: HIGH
        PolicyQdepth: 0
        Qdepth: 0

1.      Name: appqoe-act-basic-prmedium
        ActionType: PRIORITY_QUEUING
        Priority: MEDIUM
        PolicyQdepth: 10
        Qdepth: 0

1.      Name: appqoe-act-basic-prlow
        ActionType: PRIORITY_QUEUING
        Priority: LOW
        PolicyQdepth: 1000
        Qdepth: 0
Done
<!--NeedCopy-->
```

Pour modifier une action AppQoE existante à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appqoe action <name> [-priority <priority>] [-altContentSvcName <string>] [-altContentPath <string>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-maxConn <positive_integer>] [-delay <`


```
usecs>] [-dosTrigExpression <expression>] [-dosAction ( SimpleResponse
| HICResponse )]
```

- `show appqoe action`

Pour supprimer une action AppQoE à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `rm appqoe action <name>`
- `show appqoe action`

Paramètres de configuration d'une action AppQoE

- de l'utilisateur. Nom de la nouvelle action ou nom de l'action existante que vous souhaitez modifier. Le nom peut commencer par une lettre, un nombre ou le symbole de trait de soulignement, et peut être composé de un à des lettres, des chiffres et le tiret (-), point (.) livre (#), espace (), signe (@), égal (=), deux-points (:) et soulignement (_).
- priorité. File d'attente de priorité à laquelle la demande est affectée. Lorsqu'un serveur Web protégé ou une application est chargé et ne peut pas accepter de demandes supplémentaires, spécifie l'ordre dans lequel les demandes en attente doivent être traitées lorsque les ressources sont disponibles. Les choix sont les suivants :

1. **HIGH.** Réponde à la demande dès que les ressources sont disponibles.
2. **MEDIUM.** Remplit la demande après avoir rempli toutes les demandes de la file d'attente de priorité HAUTE.
3. **LOW.** Remplit la demande après avoir rempli toutes les demandes dans les files d'attente de priorité HAUT et MOYENNE.
4. **LOWEST.** Remplit la demande uniquement après avoir rempli toutes les demandes dans les files d'attente de priorité supérieure.

Si la priorité n'est pas configurée, l'appliance Citrix ADC affecte la demande à la file d'attente de priorité LOWEST par défaut.

- respondWith. Configure Citrix ADC pour qu'il prenne l'action Répondeur spécifiée lorsque le seuil spécifié est atteint. Doit être utilisé avec l'un des paramètres suivants :
  - **ACS :** Sert du contenu provenant d'un service de contenu alternatif. Seuil : maxConn (connexions maximales) ou délai.
  - **NS :** Sert une réponse intégrée à partir de Citrix ADC. Seuil : maxConn (connexions maximales) ou délai.
  - **NO ACTION :** Ne sert pas de contenu alternatif. Affecte des connexions à la file d'attente de priorité LOWEST si le seuil maxConn (connexions maximales) ou de délai est atteint.

- altContentSvcName. Si -ResponseWith ACS est spécifié, le nom du service de contenu alternatif, généralement une URL absolue vers le serveur Web qui héberge le contenu alternatif.
- altContentPath. Si -responseWith (ACS | NS) est spécifié, le chemin d'accès au contenu alternatif.
- olqDepth. Valeur de seuil de profondeur de file d'attente de stratégie pour la file d'attente de stratégie associée à cette action. Lorsque le nombre de connexions dans la file d'attente de stratégies associée à cette action augmente au nombre spécifié, les demandes suivantes sont affectées à la file d'attente de stratégies LOWEST. Valeur minimale : 1 Valeur maximale : 4,294,967,294
- priqDepth. Valeur de seuil de profondeur de file d'attente de stratégie pour la file d'attente prioritaire spécifiée. Si le nombre de demandes dans la file d'attente spécifiée sur le serveur virtuel auquel la stratégie associée à l'action en cours est liée augmente jusqu'au nombre spécifié, les demandes suivantes sont affectées à la file d'attente de priorité BAS. Valeur minimale : 1 Valeur maximale : 4,294,967,294
- maxConn. Nombre maximal de connexions pouvant être ouvertes pour les demandes qui correspondent à la règle de stratégie. Valeur minimale : 1 Valeur maximale : 4,294,967,294
- delay. Seuil de délai, en microsecondes, pour les demandes qui correspondent à la règle de stratégie. Si une demande correspondante a été retardée plus longtemps que le seuil, l'appliance
  Citrix ADC exécute l'action spécifiée. Si NO ACTION est spécifié, l'appliance affecte les demandes à la file d'attente de priorité la plus basse. Valeur minimale : 1 Valeur maximale : 599999,999
- dosTrigExpression. Ajoute une vérification facultative de deuxième niveau pour déclencher des actions DoS.
- dosAction. Action à prendre lorsque l'appliance détermine qu'elle ou un serveur protégé fait l'objet d'une attaque DoS. Valeurs possibles : SimpleReponse, HiCResponse.

Ces valeurs spécifient des méthodes de réponse de défi HTTP pour valider l'authenticité des requêtes entrantes afin d'atténuer une attaque HTTP-DDoS.

Dans le processus de génération et de validation de la réponse HTTP, AppQoE utilise des cookies pour valider la réponse du client et vérifier que le client semble authentique. Lors de l'envoi d'un défi, une appliance Citrix ADC génère deux cookies :

Header cookie (_DOSQ). Contient des informations spécifiques au client, afin que l'appliance Citrix ADC puisse vérifier la réponse.

Body cookie (_DOSH). Informations utilisées pour valider l'ordinateur client. Le navigateur du client (ou l'utilisateur, dans le cas de HIC) calcule une valeur pour ce cookie. L'appliance Citrix ADC compare cette valeur à la valeur attendue pour vérifier le client.

Les informations que l'appliance envoie au client pour calculer la valeur _DOSH sont basées sur la configuration de l'action DoS.

1. SimpleReponse : dans ce cas, un appliance Citrix ADC fractionne la valeur et génère un code JavaScript pour combiner la valeur finale. Une machine client capable de calculer la valeur d'origine est considérée comme authentique.
2. HICResponse : dans ce cas, une appliance Citrix ADC génère deux numéros à un chiffre et génère des images pour ces numéros. Ensuite, à l'aide d'une structure de backpatch, l'appliance insère ces images sous forme de chaînes base64.

Limitations

1. Ce n'est pas une implémentation triviale CAPTCHA, c'est pourquoi ce terme n'est pas utilisé.
2. Le numéro de validation est basé sur un numéro généré par Citrix ADC qui ne change pas pendant 120 secondes. Ce numéro doit être dynamique ou spécifique au client.

Pour configurer une action AppQoE à l'aide de l'utilitaire de configuration

1. Accédez à **App-Expert** > **AppQoE** > **Actions** .
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une action, cliquez sur **Ajouter**.
   - Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Modifier**.
3. Dans l'écran **Créer une action AppQoE** ou **Configurer une action AppQoE**, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres pour configurer l'action AppQoE » comme suit (un astérisque indique un paramètre requis) :
   - Name—name
   - Type d'action—respondWith
   - Priorité—priority
   - Profondeur de la file d'attente des stratégies—polqDepth
   - Profondeur de file d'attente—priqDepth
   - Action DOS—dosAction
4. Cliquez sur **Créer** ou **sur OK**.

Paramètres AppQoE

January 21, 2021

Dans les paramètres AppQoE, vous configurez la durée de vie de session d'une session AppQoE, le nom du fichier contenant la réponse personnalisée et le nombre de connexions clientes pouvant être placées dans une file d'attente.

Pour configurer les paramètres AppQoE à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appqoe parameter [-sessionLife <secs>] [-avgwaitingclient <positive_integer>] [-MaxAltRespBandWidth <positive_integer>] [-dosAttackThresh <positive_integer>]`
- `show appqoe parameter`

Paramètres de configuration des paramètres AppQoE

- sessionLife

  Nombre de secondes à attendre après l'affichage du contenu alternatif avant que l'appliance affiche à nouveau le même contenu. Valeur par défaut : 300 Valeur minimale maximale : 1 Valeur maximale : 4,294,967,294

- avgwaitingclient

  Nombre moyen de demandes client pouvant se trouver dans la file d'attente de service. Valeur par défaut : 1000000 Valeur maximale : 4,294,967,294

- MaxAltrespBandwidth

  Bande passante maximale à consommer lors de l'envoi de réponses alternatives. Si le maximum est atteint, l'appliance quitte l'envoi du contenu alternatif jusqu'à ce que la consommation de bande passante diminue. Valeur par défaut : 100 Valeur minimale : 1 Valeur maximale : 4,294,967,294

- dosAtckThrsh

  Seuil d'attaque par déni de service. Nombre de connexions qui doivent être en attente dans les files d'attente avant que l'appliance ne réponde par des mesures de protection DoS. Valeur par défaut : 2000 Valeur minimale : 0 Valeur maximale : 4,294,967,294

Pour configurer les paramètres AppQoE à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **AppQoE** .
2. Dans le volet d'informations, cliquez sur **Configurer les paramètres AppQoE**.
3. Dans l'écran **Configurer les paramètres AppQoE**, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans

« Paramètres pour la configuration des paramètres AppQoE » comme suit (un astérisque indique un paramètre requis) :

- Vie de session (secondes)
- sessionLife
- Client en attente moyenne—avgwaitingclient
- Limite de bande passante de réponse alternative (Mbps) —MaxAltrespBandwidth
- Seuil d'attaque DOS —DosAttackThresh

4. Cliquez sur **OK**.

Stratégies AppQoE

August 20, 2021

Pour implémenter AppQoE, vous devez configurer au moins une stratégie pour indiquer à votre Citrix ADC comment distinguer les connexions à mettre en file d'attente dans une file d'attente spécifique.

Pour configurer une stratégie AppQoE à l'aide de la ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
add appqoe policy <name> -rule <expression> -action <string>
```

Exemple :

L'exemple suivant sélectionne les demandes avec un en-tête User-Agent contenant « Android » et les affecte à la file d'attente de priorité moyenne. Ces demandes proviennent de smartphones et de tablettes qui exécutent le système d'exploitation Google Android.

```
1  > add appqoe action appqoe-act-primd -priority MEDIUM
2  Done
3  > add appqoe policy appqoe-pol-primd -rule "HTTP.REQ.HEADER("User-Agent
       ").CONTAINS("Android")" -action appqoe-act-primd
4  Done
5  > sh appqoe policy appqoe-pol-primd
6          Name: appqoe-pol-primd
7          Rule: HTTP.REQ.HEADER("User-Agent").CONTAINS("Android")
8          Action: appqoe-act-primd
9          Hits: 0
10
11 Done
12 <!--NeedCopy-->
```


Paramètres de configuration d'une stratégie AppQoE

- de l'utilisateur. Nom de la stratégie AppQoE. Le nom peut commencer par une lettre, un nombre ou le symbole de trait de soulignement, et peut être composé de un à 127 lettres, chiffres et tiret (-), point (.) dièse (#), espace ( ), arobase (@), égal (=), deux-points (:) et soulignement (_). Vous devez choisir un nom qui aide à identifier le type d'action.
- règle. Expression Citrix ADC qui indique à l'appliance quelles connexions il doit gérer.
- action. Action AppQoE à effectuer lorsqu'une connexion correspond à la stratégie.

Pour configurer une stratégie AppQoE à l'aide de l'utilitaire de configuration

1. Accédez à **App-Expert** > **AppQoE** > **Stratégies** .
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une stratégie, cliquez sur **Ajouter**.
   - Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Modifier**.
3. Si vous créez une stratégie, dans la boîte de dialogue **Créer une stratégie AppQoE**, dans la zone de texte Nom, tapez un nom pour votre nouvelle stratégie.

   Le nom peut commencer par une lettre, un nombre ou le symbole de trait de soulignement, et peut être composé de un à 127 lettres, chiffres et tiret (-), point (.) dièse (#), espace ( ), arobase (@), égal (=), deux-points (:) et soulignement (_). Vous devez choisir un nom qui aide à identifier l'objet et l'effet de cette stratégie.

   Si vous modifiez une stratégie existante, ignorez cette étape. Vous ne pouvez pas modifier le nom d'une stratégie existante.
4. Dans la liste déroulante **Action**, choisissez l'action AppQoE à effectuer lorsque la stratégie correspond à une connexion. Cliquez sur le bouton plus (+) pour ouvrir la boîte de dialogue **Ajouter une action AppQoE** et ajouter une nouvelle action.
5. Dans la zone de texte **Règle**, entrez directement l'expression de stratégie ou cliquez sur Nouveau pour créer une expression de stratégie. Si vous cliquez sur Nouveau, effectuez les opérations suivantes :

   a) Dans la boîte de dialogue **Créer une expression**, cliquez sur **Ajouter**.
   1 Dans la boîte de dialogue **Ajouter une expression**, sélectionnez une expression commune dans la liste déroulante **Expressions fréquemment utilisées** ou utilisez les listes déroulantes **Construire une expression** pour créer l'expression qui définit le trafic à filtrer.
   Si vous choisissez de créer votre propre expression, vous commencez par sélectionner le premier terme dans la première liste déroulante située à gauche de la zone Construire une expression. Les choix de cette liste sont les suivants :

- HTTP
- SYS
- CLIENT
- SERVER
- ANALYTIQUE
- TEXTE

Le choix par défaut est HTTP. Après avoir fait un choix dans la première liste déroulante (ou accepté le terme par défaut), vous pouvez choisir le terme suivant dans votre expression dans la liste déroulante située à droite de celle-ci. Les termes de cette liste et d'autres listes qui suivent changent en fonction de vos choix précédents. Les listes proposent uniquement des termes qui sont des choix valides. Continuez à sélectionner des termes jusqu'à ce que vous ayez terminé l'expression.

a) Lorsque vous avez créé l'expression souhaitée, cliquez sur **OK**. L'expression est ajoutée dans la zone de texte **Expression**.

6. Cliquez sur **Créer**. L'expression apparaît dans la zone de texte **Règle**.

Modèle d'entité pour l'équilibrage de charge du serveur virtuel

August 20, 2021

> **Avertissement**
>
> La fonctionnalité du modèle d'entité est obsolète à partir de Citrix ADC 13.0 build 82.x et Citrix vous recommande d'utiliser les livres de style. Pour plus d'informations, consultez la rubrique Livres de style .

Un modèle d'entité est un ensemble d'informations permettant de créer un modèle de serveur virtuel d'équilibrage de charge sur une appliance Citrix ADC. Il fournit une spécification et un ensemble de valeurs par défaut à configurer pour un serveur virtuel d'équilibrage de charge. En utilisant un modèle qui définit un ensemble de valeurs par défaut, vous pouvez rapidement configurer plusieurs serveurs virtuels nécessitant une configuration similaire tout en éliminant plusieurs étapes de configuration.

Vous pouvez créer un modèle d'entité en exportant les détails du serveur virtuel d'équilibrage de charge dans un fichier modèle. Cela ne peut être fait que via l'interface graphique Citrix ADC. Vous utilisez l'interface graphique Citrix ADC pour exporter, importer et gérer des modèles d'entité. Vous pouvez partager des modèles d'entité avec d'autres administrateurs et gérer les modèles enregistrés localement sur votre appliance ou votre machine. Vous pouvez également importer des modèles d'entité à partir de l'appliance ou de votre ordinateur local.

Avant de créer un modèle, vous devez être familier avec la configuration du serveur virtuel d'équilibrage de charge.

Modèle de serveur virtuel d'équilibrage de charge

Les modèles d'entité d'équilibrage de charge sont créés de la même manière que les modèles d'application Citrix ADC. Lorsque vous exportez un serveur virtuel d'équilibrage de charge vers un fichier modèle, les deux fichiers suivants sont automatiquement créés :

- Fichier modèle de serveur virtuel d'équilibrage de charge. Contient des éléments XML qui stockent les valeurs des paramètres configurés pour le serveur virtuel d'équilibrage de charge. Le fichier contient également des éléments XML permettant de stocker des informations sur les stratégies liées.
- Fichier de déploiement. Contient des éléments XML qui stockent des informations spécifiques au déploiement, telles que des services, des groupes de services et des variables configurées. Dans les fichiers de modèle et de déploiement, chaque unité d'informations de configuration est encapsulée dans un élément XML spécifique destiné à ce type d'unité. Par exemple, le paramètre de méthode d'équilibrage de charge, LBMethod, est encapsulé dans les `</lbmethod>` balises `<lbmethod>` et.

> **Remarque :**
>
> Après avoir exporté un serveur virtuel d'équilibrage de charge, vous pouvez ajouter des éléments, supprimer des éléments et modifier des éléments existants avant d'importer les informations de configuration dans une appliance Citrix ADC.

Fonctionnement d'un modèle de serveur virtuel d'équilibrage de charge

Lorsque vous créez un modèle pour un serveur virtuel d'équilibrage de charge, vous spécifiez des valeurs par défaut pour le serveur. Vous spécifiez les valeurs qui doivent être en lecture seule, les valeurs qui ne doivent pas être affichées et les valeurs que les utilisateurs peuvent configurer. Vous configurez également les pages qui composent l'assistant d'importation de modèles. Toutes les informations et les paramètres que vous fournissez sont stockés dans le fichier de modèle.
Lorsqu'un utilisateur importe le modèle vers une appliance Citrix ADC, l'interface graphique guide l'utilisateur à travers les différentes pages que vous avez configurées pour le modèle. L'interface graphique affiche les valeurs des paramètres en lecture seule et invite l'utilisateur à spécifier des valeurs pour les paramètres configurables. Une fois que l'utilisateur a suivi les instructions, l'appliance crée l'entité avec les valeurs configurées.
Vous pouvez créer ou modifier un modèle d'entité pour un serveur virtuel d'équilibrage de charge à partir du nœud Gestion du trafic.
Pour exporter les détails du serveur virtuel vers un modèle, vous devez spécifier les options et paramètres suivants pour le modèle :

- Valeur par défaut d'un paramètre.
- Indique si les valeurs par défaut sont visibles pour les utilisateurs.
- Indique si les valeurs par défaut peuvent être modifiées par les utilisateurs.
- Nombre de pages dans l'assistant d'importation d'entités, y compris les noms de pages, le texte et les paramètres disponibles.
- Entités qui doivent être liées à l'entité pour laquelle le modèle est créé.

Par exemple, lorsque vous créez un modèle de serveur virtuel d'équilibrage de charge, vous pouvez spécifier les stratégies que vous souhaitez lier au serveur virtuel que vous créez à partir du modèle. Toutefois, seules les informations de liaison sont incluses dans le modèle. Les entités liées ne sont pas incluses. Si le modèle d'entité est importé dans un autre dispositif Citrix ADC, les entités liées doivent exister sur l'appliance au moment de l'importation pour que la liaison réussisse. Si aucune des entités liées n'existe sur l'appliance cible, l'entité (pour laquelle le modèle a été configuré) est créée sans aucune liaison. Si seul un sous-ensemble des entités liées existe sur l'appliance cible, elles sont liées à l'entité créée à partir du modèle.
Lorsque vous exportez un modèle pour le serveur virtuel d'équilibrage de charge, les paramètres de configuration de l'entité apparaissent dans le modèle. Toutes les entités liées sont sélectionnées par défaut, mais vous pouvez modifier les liaisons si nécessaire. Comme dans le cas d'un modèle qui n'est pas basé sur une entité existante, seules les informations contraignantes sont incluses et non les entités. Vous pouvez enregistrer le modèle avec les paramètres de configuration existants ou les utiliser comme base pour créer une nouvelle configuration pour un modèle.

Configurer les variables dans le modèle de serveur virtuel d'équilibrage de charge

Les modèles de serveur virtuel d'équilibrage de charge prennent en charge la déclaration de variables dans les paramètres d'équilibrage de charge configurés ainsi que dans les stratégies et actions liées. La possibilité de déclarer des variables vous permet de remplacer des valeurs préconfigurées par des valeurs adaptées à l'environnement dans lequel vous importez le modèle.

À titre d'exemple, considérez l'expression suivante configurée pour une stratégie liée à un serveur virtuel d'équilibrage de charge pour lequel vous créez un modèle. L'expression évalue la valeur de l'en-tête accept-language dans une requête HTTP.

```
HTTP.REQ.HEADER("Accept-Language").CONTAINS("en-us")
```

Si vous voulez que la valeur de l'en-tête soit configurable au moment de l'importation, vous pouvez spécifier la chaîne en-us en tant que variable.

Après avoir créé une variable, vous pouvez effectuer les opérations suivantes :

- Attribuez d'autres chaînes à une variable existante. Après avoir créé une variable pour une chaîne, vous pouvez sélectionner et affecter d'autres parties de la même expression ou d'une expression différente à la variable. Les chaînes que vous attribuez à une variable ne doivent pas

nécessairement être les mêmes. Au moment de l'importation, toutes les chaînes affectées à la variable sont remplacées par la valeur que vous fournissez.

- Affichez la ou les chaînes qui sont affectées à la variable.
- Afficher la liste de toutes les entités et paramètres qui utilisent la variable

Pour configurer des variables dans un modèle de serveur virtuel d'équilibrage de charge

Suivez la procédure suivante pour configurer les variables d'un modèle de serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**
2. Dans le volet d'informations, cliquez avec le bouton droit sur le serveur virtuel que vous souhaitez exporter vers un fichier de modèle, puis cliquez sur **Ajouter**.
3. Dans la page **Créer un serveur virtuel d'équilibrage de charge**, définissez les paramètres du serveur virtuel. Pour plus d'informations sur la configuration d'un serveur virtuel d'équilibrage de charge, voir Fonctionnement de l'équilibrage de charge.
4. Une fois que vous avez défini les paramètres du serveur virtuel d'équilibrage de charge, cliquez sur **Terminé**.



5. Cliquez sur le lien **Exporter en tant que modèle** en haut pour exporter les détails du serveur sous forme de fichier modèle.
6. Dans la page **Créer un modèle d'équilibrage de charge**, entrez les paramètres du modèle.
7. Cliquez sur **Terminé**.



Modifier un modèle de serveur virtuel d'équilibrage de charge

Vous ne pouvez modifier que les paramètres, les liaisons et les pages configurées pour un modèle. Le nom et l'emplacement du modèle spécifiés lors de la création du modèle ne peuvent pas être modifiés. L'appliance Citrix ADC ne vous offre pas la possibilité de modifier un modèle de serveur virtuel d'équilibrage de charge.

Pour modifier un serveur virtuel d'équilibrage de charge à l'aide de Citrix ADC GUI

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans la page **Serveur virtuel d'équilibrage de charge**, modifiez les paramètres d'entité.
3. Cliquez sur Terminé.
4. Cliquez sur le lien **Exporter en tant que modèle**.
5. Les modifications modifiées sont désormais disponibles dans le fichier de modèle de serveur virtuel d'équilibrage de charge.
6. Dans la page **Modèle d'équilibrage de charge exporté**, cliquez sur **Terminé**.

Gérer les modèles de serveur virtuel d'équilibrage de charge

Vous pouvez organiser les fichiers de modèle de serveur virtuel d'équilibrage de charge et les fichiers de déploiement à l'aide de l'interface graphique Citrix ADC.

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans la page **Serveurs virtuels**, sélectionnez l'**action Gérer le modèle**.
3. Dans la page **Modèles d'équilibrage de charge**, cliquez sur l'onglet **Fichier de modèle**.
4. Dans l'onglet **Fichiers de modèles**, vous pouvez télécharger ou télécharger un modèle depuis et vers le dossier de modèles d'appliance.



5. Cliquez sur **Fermer**.

Pour télécharger un modèle d'entité de serveur virtuel d'équilibrage de charge à l'aide de Citrix ADC GUI

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans la page **Serveurs virtuels**, cliquez sur **Sélectionner une action**, puis sélectionnez **Gérer le modèle**.
3. Dans la page Modèles d'équilibrage de charge, cliquez sur l'onglet **Fichiers de modèles** .
4. Dans l'onglet **Fichiers de modèle**, cliquez sur **Télécharger** pour charger un modèle.
5. Cliquez sur **Fermer**.



Pour télécharger un modèle d'entité de serveur virtuel d'équilibrage de charge à l'aide de Citrix ADC GUI

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans la page **Serveurs virtuels**, cliquez sur **Sélectionner une action**, puis sélectionnez **Gérer le modèle**.

3. Dans la page **Modèles d'équilibrage de charge**, cliquez sur l'onglet **Fichiers de modèles**.
4. Dans l'onglet Fichiers modèles, sélectionnez un fichier modèle et cliquez sur Télécharger.
5. Cliquez sur Fermer.



Exemple de modèle de serveur virtuel d'équilibrage de charge et modèle de déploiement

Voici un exemple de fichier modèle qui a été créé à partir d'un serveur virtuel d'équilibrage de charge appelé « Lbvip » :

```
COPY

<?xml version="1.0" encoding="UTF-8" ?>
  <template>
    <template_info>
      <entity_name>Lbvip</entity_name>
      <version_major>10</version_major>
      <version_minor>0</version_minor>
      <build_number>40.406</build_number>
    </template_info>
    <entitytemplate>
      <lbvserver_list>
        <lbvserver>
          <name>Lbvip</name>
          <servicetype>HTTP</servicetype>
          <ipv46>0.0.0.0</ipv46>
          <ipmask>*</ipmask>
          <port>0</port>
          <range>1</range>
          <persistencetype>NONE</persistencetype>
          <timeout>2</timeout>
```



```
            <persistencebackup>NONE</persistencebackup>
            <backuppersistencetimeout>2</backuppersistencetimeout>
            <lbmethod>LEASTCONNECTION</lbmethod>
            <persistmask>255.255.255.255</persistmask>
            <v6persistmasklen>128</v6persistmasklen>
            <pq>OFF</pq>
            <sc>OFF</sc>
            <m>IP</m>
            <datalength>0</datalength>
            <dataoffset>0</dataoffset>
            <sessionless>DISABLED</sessionless>
            <state>ENABLED</state>
            <connfailover>DISABLED</connfailover>
            <clttimeout>180</clttimeout>
            <somethod>NONE</somethod>
            <sopersistence>DISABLED</sopersistence>
            <sopersistencetimeout>2</sopersistencetimeout>
            <redirectportrewrite>DISABLED</redirectportrewrite>
            <downstateflush>DISABLED</downstateflush>
            <gt2gb>DISABLED</gt2gb>
            <ipmapping>0.0.0.0</ipmapping>
            <disableprimaryondown>DISABLED</disableprimaryondown>
            <insertvserveripport>OFF</insertvserveripport>
            <authentication>OFF</authentication>
            <authn401>OFF</authn401>
            <push>DISABLED</push>
            <pushlabel>none</pushlabel>
            <l2conn>OFF</l2conn>
            <appflowlog>DISABLED</appflowlog>
            <icmpvsrresponse>PASSIVE</icmpvsrresponse>
            <lbvserver_cmppolicy_binding_list>
              <lbvserver_cmppolicy_binding>
                <name>Lbvip</name>
                <policyname>NOPOLICY-COMPRESSION</policyname>
                <priority>100</priority>
                <gotopriorityexpression>END</gotopriorityexpression>
                <bindpoint>REQUEST</bindpoint>
              </lbvserver_cmppolicy_binding>
            </lbvserver_cmppolicy_binding_list>
          </lbvserver>
        </lbvserver_list>
      </entitytemplate>
    </template>
<!--NeedCopy-->
```


Exemple de fichier de déploiement

Voici le fichier de déploiement associé au serveur virtuel dans l'exemple précédent :

COPY

```
<?xml version="1.0" encoding="UTF-8" ?>
  <template_deployment>
    <template_info>
      <entity_name>Lbvip</entity_name>
      <version_major>10</version_major>
      <version_minor>0</version_minor>
      <build_number>40.406</build_number>
    </template_info>
    <service_list>
      <service>
      <ip>1.2.3.4</ip>
      <port>80</port>
      <servicetype>HTTP</servicetype>
      </service>
    </service_list>
    <servicegroup_list>
      <servicegroup>
        <name>svcgrp</name>
        <servicetype>HTTP</servicetype>
        <servicegroup_servicegroupmember_binding_list>
          <servicegroup_servicegroupmember_binding>
            <ip>1.2.3.90</ip>
            <port>80</port>
          </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.8.0</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.8.1</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.9.0</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
      </servicegroup_servicegroupmember_binding_list>
    </servicegroup>
  </servicegroup_list>
</template_deployment>
```



```
41
42 <!--NeedCopy-->
```

légendes HTTP

October 5, 2021

Pour certains types de demandes, ou lorsque certains critères sont remplis au cours de l'évaluation des stratégies, vous pouvez interrompre brièvement l'évaluation des stratégies, extraire des informations d'un serveur, puis effectuer une action spécifique qui dépend des informations récupérées. D'autres fois, lorsque vous recevez certains types de demandes, vous pouvez souhaiter mettre à jour une base de données ou le contenu hébergé sur un serveur Web. Les légendes HTTP vous permettent d'effectuer toutes ces tâches.

Une légende HTTP est une demande HTTP ou HTTPS que l'appliance Citrix ADC génère et envoie à une application externe lorsque certains critères sont remplis lors de l'évaluation de la stratégie. Les informations extraites du serveur peuvent être analysées par des expressions de stratégie avancées, et une action appropriée peut être effectuée. Vous pouvez configurer des légendes HTTP pour la commutation de contenu HTTP, la commutation de contenu TCP, la réécriture, le répondeur et pour la méthode d'équilibrage de charge basée sur des jetons.

Avant de configurer une légende HTTP, vous devez configurer une application sur le serveur auquel la légende sera envoyée. L'application, appelée *agent de légende HTTP*, doit être configurée pour répondre à la demande de légende HTTP avec les informations requises. L'agent de légende HTTP peut également être un serveur Web qui sert les données pour lesquelles l'appliance Citrix ADC envoie la légende. Vous devez vous assurer que le format de la réponse à une légende HTTP ne change pas d'un appel à l'autre.

Après avoir configuré l'agent de légende HTTP, vous configurez la légende HTTP sur l'appliance Citrix ADC. Enfin, pour appeler la légende, vous l'incluez dans une stratégie avancée dans la fonctionnalité Citrix ADC appropriée, puis liez la stratégie au point de liaison auquel vous souhaitez que la stratégie soit évaluée.

Après avoir configuré la légende HTTP, vous devez vérifier la configuration pour vous assurer que la légende fonctionne correctement.

Fonctionnement d'une légende HTTP

January 21, 2021

Lorsque l'appliance Citrix ADC reçoit une demande client, l'appliance évalue la demande en fonction des stratégies liées à différents points de liaison. Au cours de cette évaluation, si l'appliance rencontre l'expression de légende HTTP`SYS.HTTP_CALLOUT(<name>)`, elle bloque brièvement l'évaluation de la stratégie et envoie une demande à l'agent de légende HTTP à l'aide des paramètres configurés pour la légende HTTP spécifiée. À la réception de la réponse, l'appliance inspecte la partie spécifiée de la réponse, puis exécute une action ou évalue la stratégie suivante, selon que l'évaluation de la réponse de l'agent de légende HTTP vaut TRUE ou FALSE, respectivement. Par exemple, si la légende HTTP est incluse dans une stratégie de répondeur, si l'évaluation de la réponse prend la valeur TRUE, l'appliance exécute l'action associée à la stratégie de répondeur.

Si la configuration de la légende HTTP est incorrecte ou incomplète, ou si la légende s'invoque elle-même de manière récursive, l'appliance déclenche une condition UNDEF et met à jour le compteur d'accès non défini.

La figure suivante illustre le fonctionnement d'une légende HTTP appelée à partir d'une stratégie de répondeur globalement liée. La légende HTTP est configurée pour inclure l'adresse IP du client associée à une requête entrante. Lorsque l'appliance Citrix ADC reçoit une demande d'un client, l'appliance génère la demande de légende et l'envoie au serveur de légende, qui héberge une base de données d'adresses IP figurant sur la liste noire et un agent de légende HTTP qui vérifie si l'adresse IP du client est répertoriée dans la base de données. L'agent de légende HTTP reçoit la demande de légende, vérifie si l'adresse IP du client est répertoriée et envoie une réponse évaluée par l'appliance Citrix ADC. Si la réponse indique que l'adresse IP du client ne figure pas sur la liste noire, l'appliance transmet la réponse au service configuré. Si l'adresse IP du client figure sur la liste noire, l'appliance réinitialise la connexion client

Figure 1. Modèle d'entité de légende HTTP



1: Client request
2: HTTP callout request to check whether the client is blacklisted
3: Response from HTTP callout agent
4: Request forwarded to service if 3 indicates a safe IP address
5: Connection RESET if 3 indicates a bad IP address

Remarques sur le format des requêtes et réponses HTTP

January 21, 2021

L'appliance Citrix ADC ne vérifie pas la validité de la demande de légende HTTP. Par conséquent, avant de configurer les légendes HTTP, vous devez connaître le format d'une requête HTTP. Vous devez également connaître le format d'une réponse HTTP, car la configuration d'une légende HTTP implique la configuration d'expressions qui évaluent la réponse de l'agent de légende HTTP.

Cette section comprend les sections suivantes :

- Format d'une requête HTTP
- Format d'une réponse HTTP

Format d'une requête HTTP

Une requête HTTP contient une série de lignes qui se terminent chaque fois par un retour chariot et un saut de ligne, représentée par l'une ou l'autre`<CR><LF> or \r\n`.

La première ligne d'une requête (la *ligne de message*) contient la méthode HTTP et la cible. Par exemple, une ligne de message pour une requête GET contient le mot-clé GET et une chaîne qui représente l'objet à récupérer, comme indiqué dans l'exemple suivant :


```
GET /mysite/mydirectory/index.html HTTP/1.1\r\n
<!--NeedCopy-->
```

Le reste de la demande contient des en-têtes HTTP, y compris un en-tête hôte obligatoire et, le cas échéant, un corps de message.

La demande se termine par une ligne bancaire (un supplément<CR><LF> or \r\n).

Voici un exemple de demande :

```
Get /mysite/index.html HTTP/1.1\r\n
Host: 10.101.101.10\r\n
Accept: \*/\*\r\n
\r\n
<!--NeedCopy-->
```

Format d'une réponse HTTP

Une réponse HTTP contient un message d'état, des en-têtes HTTP de réponse et l'objet demandé ou, si l'objet demandé ne peut pas être servi, un message d'erreur.

Voici un exemple de réponse :

```
HTTP/1.1 200 OK\r\n
Content-Length: 55\r\n
Content-Type: text/html\r\n
Last-Modified: Wed, 12 Aug 1998 15:03:50 GMT\r\n
Accept-Ranges: bytes\r\n
ETag:  "04f97692cbd1:377" \r\n
Date: Thu, 19 Jun 2008 19:29:07 GMT\r\n
\r\n
<55-character response>
<!--NeedCopy-->
```

Configuration d'une légende HTTP

October 5, 2021

Lorsque vous configurez une légende HTTP, vous spécifiez le type de demande (HTTP ou HTTPS), la destination et le format de la demande. Le format attendu de la réponse et, enfin, la partie de la réponse que vous souhaitez analyser.

Pour la destination, vous spécifiez soit l'adresse IP et le port de l'agent de légende HTTP. Vous pouvez également engager un serveur virtuel d'équilibrage de charge, de commutation de contenu ou de redirection de cache pour gérer les demandes de légende HTTP.

Dans le premier cas, les demandes de légende HTTP sont envoyées directement à l'agent de légende HTTP. Dans le second cas, les demandes de légende HTTP sont envoyées à l'adresse IP virtuelle (VIP) du serveur virtuel spécifié. Le serveur virtuel traite la demande de la même manière qu'il traite une demande client. Par exemple, si vous attendez à ce que de nombreuses légendes soient générées, vous pouvez configurer des instances de l'agent de légende HTTP sur plusieurs serveurs, lier ces instances (en tant que services) à un serveur virtuel d'équilibrage de charge, puis spécifier le serveur virtuel d'équilibrage de charge dans la configuration de légende HTTP. Le serveur virtuel d'équilibrage de charge équilibre ensuite la charge sur ces instances configurées comme déterminé par l'algorithme d'équilibrage de charge.

Pour le format de la demande de légende HTTP, vous pouvez spécifier les attributs individuels de la demande de légende HTTP (légende HTTP basée sur des attributs), ou vous pouvez spécifier l'intégralité de la demande de légende HTTP en tant qu'expression de stratégie avancée (légende HTTP basée sur une expression).

Pour le format de la demande de légende HTTP, vous pouvez spécifier les attributs individuels de la demande de légende HTTP (une légende HTTP basée sur des attributs) ou vous pouvez spécifier l'intégralité de la demande de légende HTTP en tant qu'expression de stratégie avancée (une légende HTTP basée sur une expression).

Pour plus d'informations, voir Policy-HttpCallout

Paramètre	Description
Nom	Nom de la légende, 127 caractères maximum
Adresse IP et port (adresse *IP/port*) ou nom du serveur virtuel (vserver)	Adresse IPv4 ou IPv6 du serveur vers lequel la légende est envoyée, ou un caractère générique, et le port du serveur vers lequel la légende est envoyée, ou un caractère générique. Ou bien, le nom d'un serveur virtuel d'équilibrage de charge, de commutation de contenu ou de redirection de cache avec un type de service HTTP.
Méthode HTTP (HttpMethod)	Méthode HTTP (HttpMethod). Méthode utilisée dans la requête HTTP envoyée par cette légende. Valeurs valides : GET ou POST. Par défaut : GET.

Paramètre	Description
Expression de l'hôte (HostexPR)	Expression de l'hôte (HosteXPR). Expression de texte avancée pour configurer l'en-tête Host. Longueur maximale : 255. L'expression peut être une valeur littérale ou une expression avancée qui dérive la valeur. Exemples : « 10.101.10.11 », « http.req.header (« hôte ») »
Expression de tige d'URL (URLStemExpr)	Expression de tige URL (URLSemExpr) Expression de chaîne avancée permettant de générer la souche d'URL. Longueur maximale : 8191. L'expression peut être une chaîne littérale ou une expression qui dérive la valeur. Exemples : « » /mysite/index.html « » « http.req.url »
En-têtes HTTP (en-têtes)	En-têtes HTTP (en-têtes). Expression de texte avancée pour insérer des en-têtes HTTP et leurs valeurs dans la demande de légende HTTP. Spécifiez une valeur pour chaque en-tête. Vous spécifiez le nom de l'en-tête sous forme de chaîne et la valeur d'en-tête en tant qu'expression avancée. Spécifiez les en-têtes séparés par l'espace. Tels que -headers cip(client.ip.src) hdr(http.req.header("HDR")). Le nombre d'en-têtes peut être de 8
Demande d'envoi au serveur basée sur des expressions (FullReqExpr)	Demande HTTP exacte que Citrix ADC doit envoyer en tant qu'expression avancée à 8191 caractères. Si vous spécifiez ce paramètre, vous devez omettre les arguments HttpMethod, HostexPR, URLStemExpr, en-têtes et paramètres. L'expression de requête est limitée par la fonction dans laquelle la légende est utilisée. Par exemple, une expression HTTP.RES ne peut pas être utilisée dans une banque de stratégies au moment de la demande ou dans une banque de stratégies de changement de contenu TCP.

Paramètre	Description
Demande d'envoi au serveur basée sur des expressions (BodyExpr)	Expression de chaîne avancée permettant de générer le corps de la requête. L'expression peut contenir une chaîne littérale ou une expression qui dérive la valeur (par exemple, client.ip.src). S'exclut mutuellement avec -FullReqExpr.
Paramètres	Expression avancée permettant d'insérer des paramètres de requête dans la requête HTTP envoyée par la légende. Spécifiez une valeur pour chaque paramètre que vous configurez. Si la demande de légende utilise la méthode GET, ces paramètres sont insérés dans l'URL. Si la demande de légende utilise la méthode POST, ces paramètres sont insérés dans le corps POST. Vous configurez le nom du paramètre de requête sous forme de chaîne et la valeur en tant qu'expression avancée. Les valeurs des paramètres sont codées par URL. Spécifiez les paramètres séparés par l'espace comme ⊠paramètres name1 (« name1") name2 (http.req.header (« hdr »)). Le maximum de 8 paramètres peut être configuré.
Type de retour (ReturnType)	Type de données renvoyées par l'application cible dans la réponse à la légende. Valeurs valides : TEXT : Traitez la valeur renvoyée comme une chaîne de texte. NUM : Traitez la valeur renvoyée comme un nombre. BOOL : Traitez la valeur renvoyée comme une valeur booléenne. Remarque : Vous ne pouvez pas modifier le type de retour une fois qu'il a été défini.

Paramètre	Description
Expression pour extraire des données de la réponse (ResultExpr)	Expression avancée qui extrait les objets HTTP.RES de la réponse à la légende HTTP. La longueur maximale est de 8191. Les opérations de cette expression doivent correspondre au type de retour. Par exemple, si vous configurez un type de texte renvoyé, l'expression de résultat doit être une expression textuelle. Si le type de retour est num, l'expression de résultat (ResultExpr) doit renvoyer une valeur numérique similaire à la suivante : « http.res.body (10000) .length » Remarque : Parfois, si vous définissez un type de retour TEXT et que le résultat envoyé par le serveur dépasse 16 Ko, l'expression de résultat peut renvoyer NULL. Par exemple, lorsque le résultat est une chaîne concaténée qui dépasse 16 Ko.
Modèle	Type de schéma pour le serveur de légende. Exemple : HTTP, https
Cache pour Secs	Durée, en secondes, pour laquelle la réponse de légende est mise en cache. Les réponses mises en cache sont stockées dans un groupe de contenu de mise en cache intégré appelé « CalloutContentGroup ». Si aucune durée n'est configurée, les réponses de légende ne sont pas mises en cache à moins qu'une configuration normale de mise en cache soit utilisée pour les mettre en cache. Ce paramètre prévaut sur toute configuration normale de mise en cache qui s'appliquerait autrement à ces réponses.

Remarque : L'appliance ne vérifie pas la validité de la demande. Vous devez vous assurer que la demande est valide et qu'elle ne contient aucune information confidentielle. Une configuration de légende HTTP incorrecte ou incomplète entraîne une condition UNDEF d'exécution qui n'est pas associée à une action. La condition UNDEF met simplement à jour le compteur d'accès non définis, ce qui vous permet de dépanner une légende HTTP mal configurée. Toutefois, l'appliance analyse

la demande de légende HTTP pour vous permettre de configurer certaines fonctionnalités de Citrix ADC pour la légende. Cela peut conduire à une légende HTTP qui s'appelle elle-même. Pour plus d'informations sur la récursion de légende et sur la façon de l'éviter, reportez-vous à la section Éviter la récursion des légendes HTTP.

Enfin, que vous utilisiez des attributs de requête HTTP ou une expression pour définir le format de la demande de légende HTTP, vous devez spécifier le format de la réponse à partir de l'agent de légende HTTP et la partie de la réponse que vous souhaitez évaluer. Le type de réponse peut être une valeur booléenne, un nombre ou un texte. En fonction de ce type de retour uniquement, vous pouvez utiliser les autres méthodes d'expression sur la réponse de légende. Si le type de retour est un nombre, vous pouvez utiliser l'expression basée sur le nombre sur la réponse de légende. La partie de la réponse que vous souhaitez évaluer est spécifiée par une expression. Par exemple, si vous spécifiez que la réponse contient du texte, vous pouvez utiliser `HTTP.RES.BODY(<unit>)` pour spécifier que l'appliance doit évaluer uniquement les premiers <unit>octets de la réponse de l'agent de légende.

Sur la ligne de commande, vous créez d'abord une légende HTTP à l'aide de la commande add. Lorsque vous ajoutez une légende, tous les paramètres sont définis sur la valeur par défaut NONE, à l'exception de la méthode HTTP, qui est définie sur la valeur par défaut GET. Vous configurez ensuite les paramètres de la légende à l'aide de la commande set. La commande set permet de configurer les deux types de légendes (basées sur l'attribut et sur l'expression). La différence réside dans les paramètres utilisés pour configurer les deux types de légendes. Ainsi, les instructions de ligne de commande suivantes incluent une commande set pour configurer une légende basée sur des attributs et une commande set pour configurer une légende basée sur une expression. Dans l'utilitaire de configuration, toutes ces tâches de configuration sont exécutées dans une seule boîte de dialogue.

Remarque : Avant de placer une légende HTTP dans une stratégie, vous pouvez modifier tous les paramètres configurés à l'exception du type de retour. Une fois qu'une légende HTTP est dans une stratégie, vous ne pouvez pas modifier complètement une expression configurée dans la légende. Par exemple, vous ne pouvez pas remplacer HTTP.REQ.HEADER (« myval ») par CLIENT.IP.SRC. Vous pouvez modifier les opérateurs et les arguments transmis à l'expression. Par exemple, vous pouvez changer `HTTP.REQ.HEADER("myVal1")` sur `HTTP.REQ.HEADER("myVal2")`, ou `HTTP.REQ.HEADER("myVal")` sur `HTTP.REQ.HEADER("myVal").AFTER_STR(<string>)`. Si la commande set échoue, créez une légende HTTP.

La configuration des légendes HTTP implique la configuration des expressions de stratégie avancées. Pour plus d'informations sur la configuration des expressions de stratégie avancées, consultez Configuration des expressions de stratégie avancées : mise en route.

Pour configurer une légende HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

Créez une légende HTTP.


```
add policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port<
    port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod (
    GET | POST )] [-hostExpr <expression>]  [-urlStemExpr <expression>]
    [-headers <name(value)> ...] [-parameters <name(value)> ...] [-
    bodyExpr <expression>] [-fullReqExpr <expression>] [-scheme ( http |
     https )] [-resultExpr <expression>] [-cacheForSecs <secs>] [-
    comment <string>]

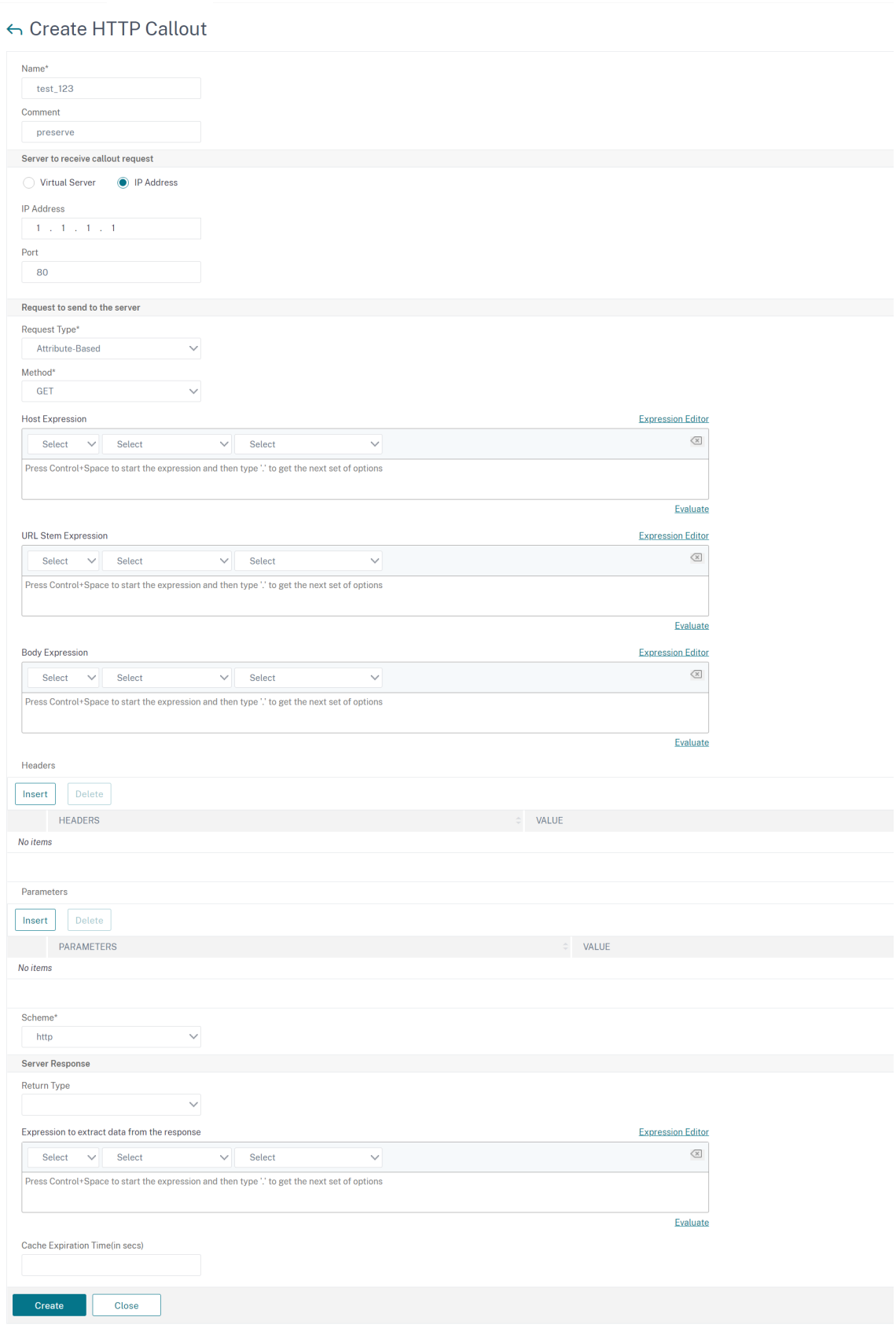
<!--NeedCopy-->
```

Exemple :

```
add policy httpCallout mycallout -vserver lbv1 -returnType num -
    httpMethod GET -hostExpr 'http.req.header("Host")'-urlStemExpr "http
    .req.url" -parameters Name("My Name") -headers Name("MyHeader")-
    resultExpr "http.res.body(10000).length"

<!--NeedCopy-->
```

Modifiez la configuration de la légende HTTP.

```
set policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr|\*>] [-
    port <port|\*>] [-vServer <string>] [-returnType <returnType>] [-
    httpMethod ( GET | POST )] [-hostExpr <string>] [-urlStemExpr <
    string>] [-headers <name(value)> ...] [-parameters <name(value)>
    ...] [-resultExpr <string>]

<!--NeedCopy-->
```

Exemple :

```
> set policy httpCallout mycallout -vserver lbv1 -returnType num -
    httpMethod GET -hostExpr 'http.req.header("Host")'-urlStemExpr "http
    .req.url" -parameters Name("My Name") -headers Name("MyHeader") -
    resultExpr "http.res.body(10000).length"
<!--NeedCopy-->
```

Configurez la légende HTTP à l'aide du paramètre FullReqExpr.

```
set policy httpCallout <name> [-vServer <string>] [-returnType <
    returnType>] [-fullReqExpr <string>] [-resultExpr <string>]
<!--NeedCopy-->
```

Exemple :


```
> set policy httpCallout mycallout1 -vserver lbv1 -returnType num
    fullReqExpr q{
 "GET " + http.req.url + "HTTP/" + http.req.version.major + "." + http.
    req.version.minor.sub(1) + "r\nHost:10.101.10.10\r\nAccept: \*/\*\r
    \n\r\n" }


<!--NeedCopy-->
```

Vérifiez les configurations de la légende HTTP.

```
show policy httpCallout `<name>`

sh policy httpCallout mycallout1
> Name: mycallout1
>Vserver: lbv1 (UP)
Effective Vserver state: UP
Return type: TEXT
Scheme: HTTP
Full REQ expr: "GET " + http.req.url + "HTTP/" + http.req.version.major
    + "." + http.req.version.minor.sub(1)+ "r\nHost:10.101.10.10\r\
   nAccept: \*/\*\r\n\r\n"
Result expr: http.res.body(100)
Hits: 0
Undef Hits: 0
Done
>

<!--NeedCopy-->
```

Pour configurer une légende HTTP à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert > AppExpert** > **AppAllets HTTP**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une légende HTTP**, configurez les paramètres de la légende HTTP. Pour obtenir une description du paramètre, placez le curseur de la souris sur la case à cocher.
4. Cliquez sur **Create**, puis cliquez sur **Close**.



Vérification de la configuration

August 20, 2021

Pour qu'une légende HTTP fonctionne correctement, tous les paramètres de légende HTTP et les entités associées à la légende doivent être configurés correctement. Bien que l'appliance Citrix ADC ne vérifie pas la validité des paramètres de légende HTTP, elle indique l'état des entités liées, à savoir le serveur ou le serveur virtuel auquel la légende HTTP est envoyée. Le tableau suivant répertorie les icônes et décrit les conditions dans lesquelles les icônes sont affichées.

Icône	Indique que
	L'état du serveur qui héberge l'agent de légende HTTP ou du serveur virtuel d'équilibrage de charge, de commutation de contenu ou de redirection de cache auquel la légende HTTP est envoyée est UP.
	L'état du serveur qui héberge l'agent de légende HTTP ou du serveur virtuel d'équilibrage de charge, de commutation de contenu ou de redirection de cache vers lequel la légende HTTP est envoyée est OUT DE SERVICE.
	L'état du serveur qui héberge l'agent de légende HTTP ou du serveur virtuel d'équilibrage de charge, de commutation de contenu ou de redirection de cache vers lequel la légende HTTP est envoyée est DOWN.

Tableau 1. Icônes indiquant les états des entités liées à une légende HTTP

Pour qu'une légende HTTP fonctionne correctement, l'icône doit être verte à tout moment. Si l'icône n'est pas verte, vérifiez l'état du serveur de légende ou du serveur virtuel auquel la légende HTTP est envoyée. Si la légende HTTP ne fonctionne pas comme prévu même si l'icône est verte, vérifiez les paramètres configurés pour la légende.

Vous pouvez également vérifier la configuration en envoyant des demandes de test correspondant à la stratégie à partir de laquelle la légende HTTP est appelée, en vérifiant le compteur d'accès pour la stratégie et la légende HTTP, et en vérifiant les réponses que l'appliance Citrix ADC envoie au client.

Remarque : Une légende HTTP peut parfois s'appeler récursivement une seconde fois. Dans ce cas, le

compteur de résultats est incrémenté de deux comptes pour chaque légende générée par l'appliance. Pour que le compteur de hits affiche la valeur correcte, vous devez configurer la légende HTTP de telle sorte qu'elle ne s'invoque pas une seconde fois. Pour plus d'informations sur la façon d'éviter la récursion de légende HTTP, consultez la section Éviter la récursion des légendes HTTP.

Pour afficher le compteur d'accès d'une légende HTTP

1. Accédez à **AppExpert > AppExpert** > **AppAllets HTTP**.
2. Dans le volet d'informations, cliquez sur la légende HTTP pour laquelle vous souhaitez afficher le compteur de résultats, puis affichez les résultats dans la zone **Détails** .

Appel d'une légende HTTP

October 5, 2021

Après avoir configuré une légende HTTP, vous l'appelez en incluant l' `SYS.HTTP_CALLOUT(<name>)` expression dans une règle de stratégie avancée. Dans cette expression, `<name>` il s'agit du nom de la légende HTTP que vous souhaitez appeler.

Vous pouvez utiliser des opérateurs d'expression de stratégie avancée avec l'expression de légende pour traiter la réponse, puis effectuer une action appropriée. Le type de retour de la réponse de l'agent de légende HTTP détermine le jeu d'opérateurs que vous pouvez utiliser sur la réponse. Si la partie de la réponse que vous souhaitez analyser est du texte, vous pouvez utiliser un opérateur de texte pour analyser la réponse. Par exemple, vous pouvez utiliser l'<string>opérateur CONtains () pour vérifier si la partie spécifiée de la réponse contient une chaîne particulière, comme dans l'exemple suivant :

```
SYS.HTTP_CALLOUT(mycallout).contains("Good IP address")
<!--NeedCopy-->
```

Si vous utilisez l'expression précédente dans une stratégie de répondeur, vous pouvez configurer une action de répondeur appropriée.

De même, si la partie de la réponse que vous souhaitez évaluer est un nombre, vous pouvez utiliser un opérateur numérique tel que GT (int). Si la réponse contient une valeur booléenne, vous pouvez utiliser un opérateur booléen.

Remarque : Une légende HTTP peut s'appeler elle-même de manière récursive. La récursion des légendes HTTP peut être évitée en combinant l'expression de légende HTTP avec une expression de stratégie avancée qui empêche la récursion. Pour plus d'informations sur la façon d'éviter la récursion de légende HTTP, reportez-vous à la section Éviter la récursion des légendes HTTP.

Vous pouvez également mettre en cascade les légendes HTTP en configurant des stratégies qui appellent chacune une légende après avoir évalué les légendes générées précédemment. Dans ce scénario, après qu'une stratégie appelle une légende, lorsque l'appliance Citrix ADC analyse la légende avant d'envoyer la légende au serveur de légendes, un deuxième ensemble de stratégies peut évaluer la légende et appeler des appels supplémentaires, qui peuvent à leur tour être évalués par un troisième ensemble de stratégies, etc. Une telle implémentation est décrite dans l'exemple suivant.

Tout d'abord, vous pouvez configurer une légende HTTP appelée MyCallout1, puis configurer une stratégie de répondeur, Pol1, pour appeler MyCallout1. Vous pouvez ensuite configurer une deuxième légende HTTP, MyCallout2, et une stratégie de répondeur, Pol2. Vous configurez Pol2 pour évaluer MyCallout1 et invoquer MyCallout2. Vous liez les deux stratégies de répondeur globalement.

Pour éviter la récursion des légendes HTTP, MyCallout1 est configuré avec un en-tête HTTP personnalisé unique appelé « Request1 ». « Pol1 est configuré pour éviter la récursion des légendes HTTP à l'aide de l'expression de stratégie avancée,

```
1 HTTP.REQ.HEADER("Request1").EQ("Callout Request").NOT.
2 <!--NeedCopy-->
```

Pol2 utilise la même expression de stratégie avancée, mais exclut l'opérateur .NOT afin que la stratégie évalue MyCallout1 lorsque l'appliance Citrix ADC l'analyse. Notez que MyCallout2 identifie son propre en-tête unique appelé « Request2 », et Pol2 inclut une expression de stratégie avancée pour empêcher MyCallout2 de s'appeler récursivement.

Exemple :

```
1  > add policy httpCallout myCallout1
2
3  Done
4
5  > set policy httpCallout myCallout1 -IPAddress 10.102.3.95 -port 80 -
       returnType TEXT -hostExpr
6   ""10.102.3.95"" -urlStemExpr ""/cgi-bin/check_clnt_from_database.pl""
       -headers Request1
7  ("Callout Request") -parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.
       RES.BODY(100)"
8
9  Done
10
11 > add responder policy Pol1 "HTTP.REQ.HEADER("Request1").EQ("Callout
       Request").NOT &&
12 SYS.HTTP_CALLOUT(myCallout1).CONTAINS("IP Matched")" RESET
13
14 Done
15
```



```
16 > bind responder global Pol1 100 END -type OVERRIDE
17
18 Done
19
20 > add policy httpCallout myCallout2
21
22 Done
23
24 > set policy httpCallout myCallout2 -IPAddress 10.102.3.96 -port 80 -
      returnType TEXT -hostExpr
25 ""10.102.3.96"" -urlStemExpr ""/cgi-bin/
      check_clnt_location_from_database.pl"" -headers Request2
26 ("Callout Request") -parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.
      RES.BODY(200)"
27
28  Done
29
30 > add responder policy Pol2 "HTTP.REQ.HEADER("Request2").EQ("Callout
      Request").NOT &&
31  HTTP.REQ.HEADER("Request1").EQ("Callout Request") && SYS.HTTP_CALLOUT(
       myCallout2).CONTAINS
32 ("APAC")" RESET
33
34  Done
35
36 > bind responder global Pol2 110 END -type OVERRIDE
37
38 Done
39 <!--NeedCopy-->
```

Éviter la récursion de légende HTTP

October 5, 2021

Même si l'appliance Citrix ADC ne vérifie pas la validité de la demande de légende HTTP, elle analyse la demande une fois avant d'envoyer la demande à l'agent de légende HTTP. Cette analyse permet à l'appliance de traiter la demande de légende comme n'importe quelle autre demande entrante, ce qui vous permet de configurer plusieurs fonctionnalités utiles de Citrix ADC (telles que la mise en cache intégrée) pour travailler sur la demande de légende.

Toutefois, au cours de cette analyse, la demande de légende HTTP peut sélectionner la même stratégie et donc s'invoquer de manière récursive. La solution matérielle-logicielle détecte l'appel récursif et

déclenche une condition undefined (UNDEF). Toutefois, l'appel récursif entraîne l'incrémentation des compteurs de sélection de stratégie et de légende HTTP de deux points chacun au lieu d'un décompte chacun.

Pour empêcher qu'une légende ne s'appelle elle-même, vous devez identifier au moins une caractéristique unique de la demande de légende HTTP, puis exclure toutes les demandes avec cette caractéristique du traitement par la règle de stratégie qui appelle la légende. Pour ce faire, vous pouvez inclure une autre expression de stratégie avancée dans la règle de stratégie. L'expression doit précéder l' `SYS.HTTP_CALLOUT(<name>)` expression de sorte qu'elle soit évaluée avant l'évaluation de l'expression de légende. Par exemple :

```
<Expression that prevents callout recursion> OR SYS.HTTP_CALLOUT(<name
    >)
<!--NeedCopy-->
```

Lorsque vous configurez une règle de stratégie de cette manière, lorsque la solution matérielle-logicielle génère la demande et l'analyse, la règle composée prend la valeur FALSE, la légende n'est pas générée une deuxième fois et les compteurs de sélection sont incrémentés correctement.

Une façon d'attribuer une caractéristique unique à une demande de légende HTTP consiste à inclure un en-tête HTTP personnalisé unique lorsque vous configurez la légende. Voici un exemple d'une légende HTTP appelée « MyCallout ». « La légende génère une requête HTTP qui vérifie si l'adresse IP d'un client est présente dans une base de données d'adresses IP sur liste noire. La légende inclut un en-tête personnalisé appelé « Demande », qui est défini sur la valeur « Demande de légende ». « Une stratégie de répondeur globalement liée, « Pol1 », appelle la légende HTTP mais exclut toutes les demandes dont l'en-tête Request est défini sur cette valeur, empêchant ainsi un second appel de MyCallout. L'expression qui empêche un deuxième appel est HTTP.REQ.HEADER (« Request ») .EQ (« Callout Request ») .NOT.

Exemple :

```
> add policy httpCallout myCallout
 Done

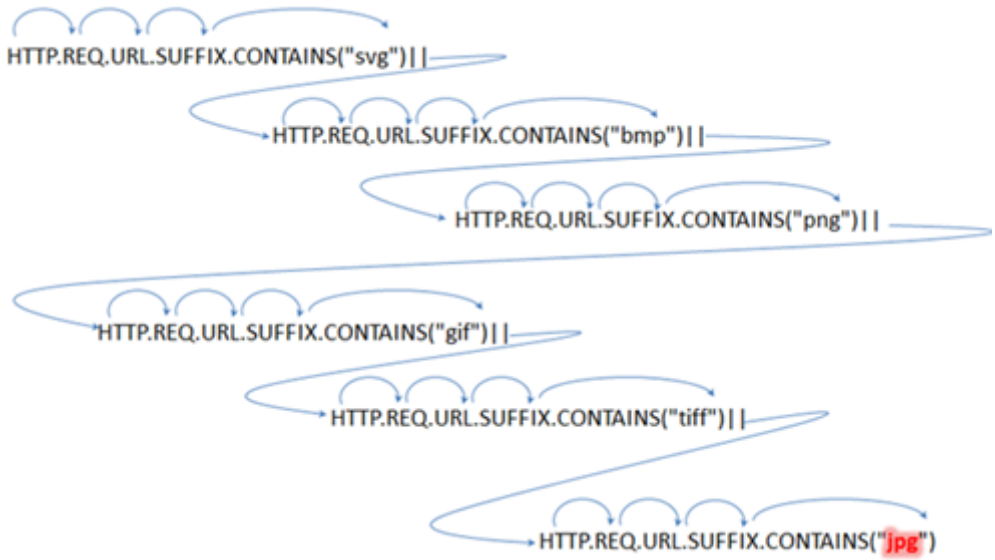
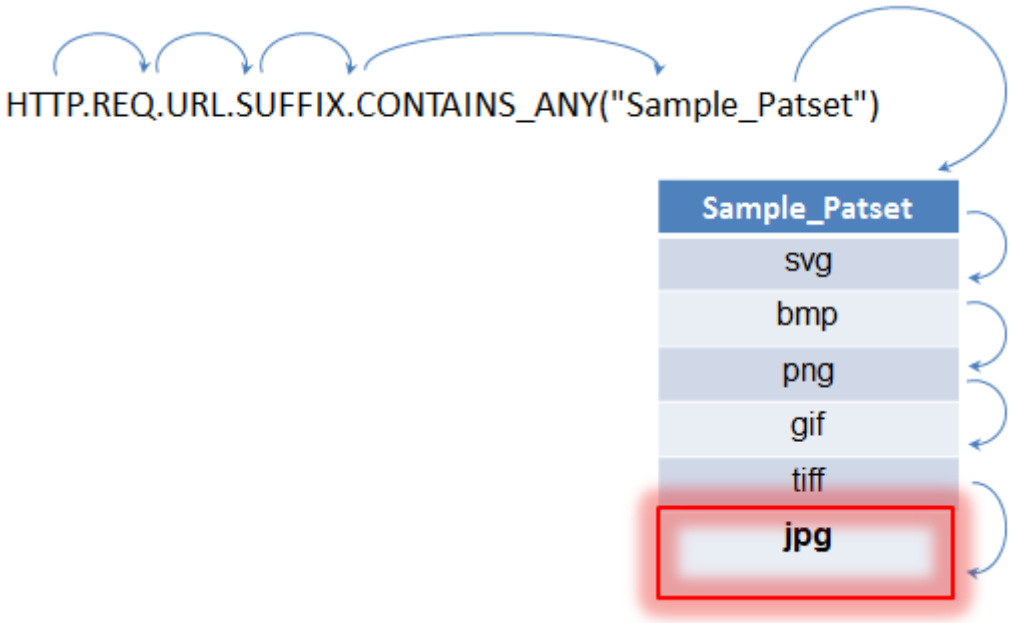
> set policy httpCallout myCallout -IPAddress 10.102.3.95 -port 80 -
    returnType TEXT -hostExpr ""10.102.3.95"" -urlStemExpr ""/cgi-bin/
    check_clnt_from_database.pl"" -headers Request("Callout Request") -
    parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.RES.BODY(100)"
Done

> add responder policy Pol1 "HTTP.REQ.HEADER("Request").EQ("Callout
    Request").NOT && SYS.HTTP_CALLOUT(myCallout).CONTAINS("IP Matched")"
     RESET
Done
```



```
9
10 > bind responder global Pol1 100 END -type OVERRIDE
11 Done
12 <!--NeedCopy-->
```

> **Remarque :**
> Vous pouvez également configurer une expression pour vérifier si l'URL de la demande inclut l'expression hampe configurée pour la légende HTTP. Pour implémenter la solution, assurez-vous que l'agent de légende HTTP ne peut répondre qu'aux appels HTTP et non aux autres requêtes dirigées via la solution matérielle-logicielle. Si l'agent de légende HTTP est une application ou un serveur Web qui répond à d'autres demandes client, une telle expression empêche la solution matérielle-logicielle de traiter ces demandes client. Utilisez plutôt un en-tête personnalisé unique comme décrit précédemment.

Mise en cache des réponses de légende HTTP

August 20, 2021

Pour améliorer les performances lors de l'utilisation des légendes, vous pouvez utiliser la fonction de mise en cache intégrée pour mettre en cache les réponses des légendes. Les réponses sont stockées dans un groupe de contenu de mise en cache intégré nommé CalloutContentGroup pour une durée spécifiée.

Remarque : Pour mettre en cache les réponses de légende, assurez-vous que la fonction de mise en cache intégrée est activée.

Pour définir la durée du cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set policy httpCallout <name> -cacheForSecs <secs>
```

Exemple :

```
1 > set httpcallout httpcallout1 -cacheForSecs 120
2 <!--NeedCopy-->
```

Pour définir la durée du cache à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert > Légendes HTTP**.

2. Dans le volet d'informations, sélectionnez la légende HTTP pour laquelle vous souhaitez définir la durée du cache et cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer la légende HTTP**, spécifiez l'**heure d'expiration du cache** .
4. Vérifiez que vous avez entré la durée correcte, puis cliquez sur **OK**.

Cas d'utilisation : filtrage des clients à l'aide d'une liste noire IP

October 5, 2021

Les appels HTTP peuvent être utilisés pour bloquer les demandes des clients qui sont mis sur liste noire par l'administrateur. La liste des clients peut être une liste noire connue du public, une liste noire que vous gérez pour votre organisation ou une combinaison des deux.

L'appliance Citrix ADC vérifie l'adresse IP du client par rapport à la liste noire préconfigurée et bloque la transaction si l'adresse IP a été mise sur liste noire. Si l'adresse IP ne figure pas dans la liste, la solution matérielle-logicielle traite la transaction.

Pour implémenter cette configuration, vous devez effectuer les tâches suivantes :

1. Activez le répondeur sur l'appliance Citrix ADC.
2. Créez une légende HTTP sur l'appliance Citrix ADC et configurez-la avec des détails sur le serveur externe et d'autres paramètres requis.
3. Configurez une stratégie de répondeur pour analyser la réponse à l'appel HTTP, puis liez la stratégie globalement.
4. Créez un agent de légende HTTP sur le serveur distant.

Activation du répondeur

Vous devez activer le répondeur avant de pouvoir l'utiliser.

Pour activer le répondeur à l'aide de l'interface graphique

1. Assurez-vous d'avoir installé la licence du répondeur.
2. Dans l'utilitaire de configuration, développez AppExpert, cliquez avec le bouton droit sur **Répondeur**, puis cliquez sur **Activer la fonctionnalité Répondeur** .

Création d'une légende HTTP sur l'appliance Citrix ADC

Créez une légende HTTP, HTTP_Callout, avec les paramètres indiqués dans le tableau suivant. Pour plus d'informations sur la création d'une légende HTTP, consultez Configuration d'une légende HTTP

PDF.

Configuration d'une stratégie de répondeur et liaison globale

Après avoir configuré la légende HTTP, vérifiez la configuration de la légende, puis configurez une stratégie de répondeur pour appeler la légende. Bien que vous puissiez créer une stratégie de répondeur dans le sous-nœud
Stratégies, puis la lier globalement à l'aide du
Responder Policy Manager, cette démonstration utilise le
Responder Policy Manager pour créer la stratégie de répondeur et la lier globalement.

Pour créer une stratégie de répondeur et la lier globalement à l'aide de

1. Accédez à **AppExpert** > **Répondeur**.
2. Dans le volet d'informations, sous **Gestionnaire de stratégies**, cliquez sur **Gestionnaire de stratégies**.
3. Dans la boîte de dialogue **Responder Policy Manager**, cliquez sur **Remplacer la stratégie globale**.
4. Cliquez sur **Insérer une stratégie**, puis, sous **Nom de la stratégie**, cliquez sur **Nouvelle stratégie**.
5. Dans la boîte de dialogue **Créer une stratégie de répondeur**, procédez comme suit :
   a) Dans Nom, saisissez **PolicyResponder1**.
   b) Dans **Action**, sélectionnez **RESET**.
   c) Dans Action de **résultat non défini, sélectionnez Actionglobale de résultat non défini** .
   d) Dans **Expression**, tapez l'expression de stratégie avancée suivante :

```
"HTTP.REQ.HEADER("Request").EQ("Callout Request").NOT && SYS.
   HTTP_CALLOUT(HTTP_Callout).CONTAINS("IP Matched")"
<!--NeedCopy-->
```

   e) Cliquez sur **Créer**, puis cliquez sur **Fermer**.
6. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Création d'un agent de légende HTTP sur le serveur distant

Vous devez maintenant créer un agent de légende HTTP sur le serveur d'appels distant qui recevra les demandes d'appel de l'appliance Citrix ADC et répondra de manière appropriée. L'agent de légende

HTTP est un script différent pour chaque déploiement et doit être écrit en tenant compte des spécifications du serveur, telles que le type de base de données et le langage de script pris en charge.

Voici un exemple d'agent de légende qui vérifie si l'adresse IP donnée fait partie d'une liste noire d'adresses IP. L'agent a été écrit dans le langage de script Perl et utilise une base de données MYSQL.

Le script CGI suivant vérifie la présence d'une adresse IP donnée sur le serveur de légendes.

```
#!/usr/bin/perl -w
print "Content-type: text/html\n\n";
        use DBI();
        use CGI qw(:standard);
#Take the Client IP address from the request query
        my $ip_to_check = param('cip');
# Where a MYSQL database is running
        my $dsn = 'DBI:mysql:BAD_CLIENT:localhost';
# Database username to connect with
        my $db_user_name =  'dbuser' ;
# Database password to connect with
        my $db_password = 'dbpassword';
        my ($id, $password);
# Connecting to the database
        my $dbh = DBI->connect($dsn, $db_user_name, $db_password);
        my $sth = $dbh->prepare(qq{
  select * from bad_clnt  }
 );
        $sth->execute();
        while (my ($ip_in_database) = $sth->fetchrow_array()) {

        chomp($ip_in_database);
# Check for IP match
        if ($ip_in_database eq $ip_to_check) {

              print "\n IP Matched\n";
                                                    $sth->finish();
                                               exit;
                 }

        }

       print "\n IP Failed\n";
       $sth->finish();
       exit;
<!--NeedCopy-->
```


Cas d'utilisation : prise en charge ESI pour la récupération et la mise à jour dynamique du contenu

October 5, 2021

Edge Side Includes (ESI) est un langage de balisage destiné à l'assemblage de contenu Web dynamique au niveau de la périphérie. Il aide à accélérer les applications Web dynamiques en définissant un langage de balisage simple pour décrire les composants de page Web pouvant être mis en cache et non mis en cache qui peuvent être agrégés, assemblés et fournis à la périphérie du réseau. En utilisant des légendes HTTP sur l'appliance Citrix ADC, vous pouvez lire les constructions ESI et agréger ou assembler le contenu de manière dynamique.

Pour implémenter cette configuration, vous devez effectuer les tâches suivantes :

1. Activez la réécriture sur l'appliance Citrix ADC.
2. Créez une légende HTTP sur la solution matérielle-logicielle et configurez-la avec des détails sur le serveur externe et d'autres paramètres requis.
3. Configurez une action de réécriture pour remplacer le contenu ESI par le corps de réponse de légende.
4. Configurez une stratégie de réécriture pour spécifier les conditions dans lesquelles l'action est exécutée, puis liez la stratégie de réécriture globalement.

Activation de la réécriture

La réécriture doit être activée avant d'être utilisée sur l'appliance Citrix ADC. La procédure suivante décrit les étapes à suivre pour activer la fonction de réécriture.

Pour activer la réécriture à l'aide de l'interface graphique

1. Assurez-vous d'avoir installé la licence de réécriture.
2. Dans l'utilitaire de configuration, développez AppExpert, cliquez avec le bouton droit de la souris sur Réécrire, puis cliquez sur Activer la fonction de réécriture.

Création d'une légende HTTP sur l'appliance Citrix ADC

Pour plus d'informations sur la création d'une légende HTTP, consultez Configuration d'une légende HTTP.
Pour plus d'informations sur les valeurs des paramètres, voir Paramètres et valeurs pour HTTP-Callout-2 pdf.

Configuration de l'action de réécriture

Créez une action de réécriture, Action-Rewrite-1, pour remplacer le contenu ESI par le corps de réponse de légende. Utilisez les paramètres affichés dans le tableau suivant.

Tableau 2. Paramètres et valeurs pour Action-Rewrite-1

Paramètre	Valeur
Nom	Action-Rewrite-1
Type	Remplacer
Expression pour choisir la référence du texte cible	« HTTP.RES.BODY (500) .AFTER_STR (<example>\ » \ ») .BEFORE_STR (\ »</example> \ ») »
Expression de chaîne pour le texte de remplacement	"SYS.HTTP_CALLOUT(HTTP-Callout-2)"

Pour configurer l'action de réécriture à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Réécrire** > **Actions**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action de réécriture**, dans Nom, tapez **Action-Rewrite-1**.
4. Dans Type, sélectionnez **REMPLACER**.
5. Dans **Expression** pour choisir une référence de texte cible, tapez l'expression de stratégie avancée suivante :

```
1 "HTTP.RES.BODY(500).AFTER_STR("<example>").BEFORE_STR("<example>")
     "
2 <!--NeedCopy-->
```

6. Dans l'expression String pour le texte de remplacement, tapez l'expression de chaîne suivante :

```
1 "SYS.HTTP_CALLOUT(HTTP-Callout-2)"
2 <!--NeedCopy-->
```

7. Cliquez sur **Créer**, puis cliquez sur **Fermer**.

Création de la stratégie de réécriture et liaison globale

Créez une stratégie de réécriture, Policy-Rewrite-1, avec les paramètres affichés dans le tableau suivant. Vous pouvez créer une stratégie de réécriture dans le sous-nœud
Policies, puis la lier globalement à l'aide du Gestionnaire de stratégies de
réécriture. Vous pouvez également utiliser le Gestionnaire de stratégies de
réécriture pour effectuer ces deux tâches simultanément. Cette démonstration utilise le Gestionnaire de stratégies de
réécriture pour effectuer les deux tâches.

Tableau 3. Paramètres et valeurs pour Policy-Rewrite-1

Paramètre	Valeur
Nom	Policy-Rewrite-1
Action	Action_Rewrite-1
Action de résultat non définie	-Global undefined-result action-
Expression.	"HTTP.REQ.HEADER("Name").CONTAINS ("Callout").NOT"

Pour configurer une stratégie de réécriture et la lier globalement à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Rewrite**.
2. Dans le volet d'informations, sous **Gestionnaire de stratégies**, cliquez sur **Réécrire le Gestionnaire de stratégies**.
3. Dans la boîte de dialogue **Gestionnaire de stratégies de réécriture**, cliquez sur **Remplacer la stratégie globale**.
4. Cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur **Nouvelle stratégie**.
5. Dans la boîte de dialogue **Créer une stratégie de réécriture**, procédez comme suit :
   1.Dans Nom, tapez Policy-Rewrite-1.
   a) Dans Action, sélectionnez Action-Rewrite-1.
   b) Dans Action de résultat non défini, sélectionnez Action globale de résultat non défini.
   c) Dans Expression, tapez l'expression de stratégie avancée suivante :

```
"HTTP.REQ.HEADER("Name").CONTAINS("Callout").NOT"
<!--NeedCopy-->
```

   a) Cliquez sur **Créer**, puis cliquez sur **Fermer**.
6. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Cas d'utilisation : Contrôle d'accès et authentification

August 20, 2021

Dans les zones à haute sécurité, il est obligatoire d'authentifier l'utilisateur de manière externe avant qu'une ressource soit accessible par les clients. Sur l'appliance Citrix ADC, vous pouvez utiliser des légendes HTTP pour authentifier l'utilisateur de manière externe en évaluant les informations d'identification fournies. Dans cet exemple, l'hypothèse est que le client envoie le nom d'utilisateur et le mot de passe via les en-têtes HTTP dans la requête. Cependant, les mêmes informations peuvent être récupérées à partir de l'URL ou du corps HTTP.

Pour implémenter cette configuration, vous devez effectuer les tâches suivantes :

1. Activez la fonctionnalité de répondeur sur l'appliance Citrix ADC.
2. Créez une légende HTTP sur l'appliance et configurez-la avec des détails sur le serveur externe et les autres paramètres requis.
3. Configurez une stratégie de répondeur pour analyser la réponse, puis liez la stratégie globalement.
4. Créez un agent de légende sur le serveur distant.

Activation du répondeur

La fonction de répondeur doit être activée avant d'être utilisée sur l'appliance Citrix ADC.

Pour activer le répondeur à l'aide de l'utilitaire de configuration

1. Assurez-vous que la licence de répondeur est installée.
2. Dans l'utilitaire de configuration, développez AppExpert, cliquez avec le bouton droit sur Répondeur, puis cliquez sur **Activer la fonctionnalité Répondeur**.

Création d'une légende HTTP sur l'appliance Citrix ADC

Créez une légende HTTP, HTTP-Callout-3, avec les paramètres indiqués dans le tableau suivant. Pour plus d'informations sur la création d'une légende HTTP, consultez Configuration d'une légende HTTP.

Tableau 1. Paramètres et valeurs pour HTTP-callout-3

Paramètre	Valeur	Nom
Nom	Policy-Responder-3	

Paramètre

Valeur

Nom

HTTP-Callout-3

Serveur pour recevoir une demande de légende :

Adresse IP

10.103.9.95

Port

80

Demande d'envoi au serveur :

Méthode

GET

Expression de l'hôte

10.102.3.95

Expression de la tige d'URL

« /cgi-bin/authenticate.pl »

En-têtes :

Nom

Demander

Expression de valeur

Demande de légende

Paramètres :

Nom

Nom d'utilisateur

Expression de valeur

HTTP.REQ.HEADER (« Nom d'utilisateur ») .VALUE (0)

Nom

Mot de passe

Expression de valeur

HTTP.REQ.HEADER (« Mot de passe ») .VALUE (0)

Réponse du serveur :

Type de retour

TEXTE

Expression pour extraire des données de la réponse

HTTP.RES.BODY (100)

Création d'une stratégie de répondeur pour analyser la réponse

Créez une stratégie de répondeur, Policy-Responder-3, qui vérifie la réponse du serveur de légendes et réinitialise la connexion si l'adresse IP source a été répertoriée sur la liste noire. Créez la stratégie avec les paramètres indiqués dans le tableau suivant. Bien que vous puissiez créer une stratégie de répondeur dans le sous-nœud
Stratégies, puis la lier globalement à l'aide du Gestionnaire de stratégies de
répondeur, cette démonstration utilise le Gestionnaire de stratégies de
répondeur pour créer la stratégie de répondeur et lier la stratégie globalement.

Tableau 2. Paramètres et valeurs pour Policy-Responder-3

Paramètre	Valeur
Nom	Policy-Responder-3
Action	RESET
Résultat indéfini - Action	-Action globale à résultat indéfini-
Expression.	"HTTP.REQ.HEADER(\"Request\").EQ(\"Callout Request\").NOT && SYS.HTTP_CALLOUT(HTTP-Callout-3).CONTAINS(\"Authentication Failed\")"

Pour créer une stratégie de répondeur et la lier globalement à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Répondeur**.
2. Dans le volet d'informations, sous **Gestionnaire de stratégies**, cliquez sur **Gestionnaire de stratégies de répondeur**.
3. Dans la boîte de dialogue **Gestionnaire de stratégies de répondeur**, cliquez sur **Remplacer global**.

4. Cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur **Nouvelle stratégie**.
5. Dans la boîte de dialogue **Créer une stratégie de répondeur**, procédez comme suit :
   a) Dans Nom, tapez Policy-Responder-3.
   b) Dans Action, sélectionnez **RÉINITIALISER**.
   c) Dans Action de résultat indéfini, sélectionnez Action globale de résultat indéfini.
   d) Dans la zone de texte Expression, tapez :

```
"HTTP.REQ.HEADER("Request").EQ("Callout Request").NOT && SYS.
   HTTP_CALLOUT(HTTP-Callout-3).CONTAINS("Authentication Failed")"
<!--NeedCopy-->
```

   a) Cliquez sur **Créer**, puis sur **Fermer**.
6. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Création d'un agent de légende HTTP sur le serveur distant

Vous devez maintenant créer un agent de légende HTTP sur le serveur de légende distant. L'agent de légende HTTP reçoit les demandes de légende de l'appliance Citrix ADC et répond de manière appropriée. L'agent de légende est un script différent pour chaque déploiement et doit être écrit en tenant compte des spécifications du serveur, telles que le type de base de données et le langage de script pris en charge.

Voici un exemple de pseudo-code de l'agent de légende qui vérifie si le nom d'utilisateur et le mot de passe fournis sont valides. L'agent peut être implémenté dans n'importe quel langage de programmation de votre choix. Le pseudo-code doit être utilisé uniquement comme guide pour le développement de l'agent de légende. Vous pouvez intégrer des fonctionnalités supplémentaires dans le programme.

Pour vérifier le nom d'utilisateur et le mot de passe fournis à l'aide d'un pseudo-code

1. Acceptez le nom d'utilisateur et le mot de passe fournis dans la demande et formatez-les de manière appropriée.
2. Connectez-vous à la base de données qui contient tous les noms d'utilisateur et mots de passe valides.
3. Vérifiez les informations d'identification fournies par rapport à votre base de données.
4. Formater la réponse comme requis par la légende HTTP.
5. Envoyez la réponse à l'appliance Citrix ADC.

Cas d'utilisation : filtrage du spam basé sur OWA

August 20, 2021

Le filtrage du spam est la capacité de bloquer dynamiquement les e-mails qui ne proviennent pas d'une source connue ou fiable ou qui ont un contenu inapproprié. Le filtrage du spam nécessite une logique métier associée qui indique qu'un type particulier de message est du spam. Lorsque l'appliance Citrix ADC traite des messages Outlook Web Access (OWA) en fonction du protocole HTTP, les légendes HTTP peuvent être utilisées pour filtrer le spam.

Vous pouvez utiliser des légendes HTTP pour extraire n'importe quelle partie du message entrant et vérifier avec un serveur de légendes externe configuré avec des règles destinées à déterminer si un message est légitime ou indésirable. En cas de courrier indésirable, pour des raisons de sécurité, l'appliance Citrix ADC n'informe pas l'expéditeur que l'e-mail est marqué comme spam.

L'exemple suivant effectue une vérification très basique pour divers mots-clés répertoriés dans l'objet de l'e-mail. Ces contrôles peuvent être plus complexes dans un environnement de production.

Pour implémenter cette configuration, vous devez effectuer les tâches suivantes :

1. Activez la fonctionnalité de répondeur sur l'appliance Citrix ADC.
2. Créez une légende HTTP sur l'appliance Citrix ADC et configurez-la avec des détails sur le serveur externe et d'autres paramètres requis.
3. Créez une stratégie de répondeur pour analyser la réponse, puis liez la stratégie globalement.
4. Créez un agent de légende sur le serveur distant.

Activation du répondeur

La fonction de répondeur doit être activée avant de pouvoir être utilisée sur l'appliance Citrix ADC.

Pour activer le répondeur à l'aide de l'interface graphique

1. Assurez-vous que la licence de répondeur est installée.
2. Dans l'utilitaire de configuration, développez AppExpert, cliquez avec le bouton droit sur **Répondeur**, puis cliquez sur **Activer la fonctionnalité Répondeur** .

Création d'une légende HTTP sur l'appliance Citrix ADC

Créez une légende HTTP, HTTP-Callout-4, avec les paramètres indiqués dans le tableau suivant. Pour plus d'informations sur la création d'une légende HTTP, consultez Configuration d'une légende HTTP.

Pour plus d'informations, voir Paramètres et valeurs pour HTTP-Callout-4 pdf.

Création d'une action de répondeur

Créez une action de répondeur, Action-Responder-4. Créez l'action avec les paramètres indiqués dans le tableau suivant.

Paramètre	Valeur
Nom	Action-Responder-4
Type	Répondez avec
Cible	""HTTP/1.1 200 OK\r\nServer: Microsoft-IIS/6.0\r\nX-Powered-By: ASP.NET\r\nContent-Length: 0\r\nMS-WebStorage: 6.5.6944\r\nCache-Control: no-cache\r\n\r\n""

Tableau 2. Paramètres et valeurs pour Action-Responder-4

Pour créer une action de répondeur à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Répondeur** > **Actions**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action de répondeur**, dans Nom, tapez **Action-Répondeur-4** .
4. Dans Type, cliquez sur **Répondre avec**.
5. Dans Target, tapez :

```
1 ""HTTP/1.1 200 OK\r\nServer: Microsoft-IIS/6.0\r\nX-Powered-By:
     ASP.NET\r\nContent-Length: 0\r\nMS-WebStorage: 6.5.6944\r\
     nCache-Control: no-cache\r\n\r\n""
2 <!--NeedCopy-->
```

6. Cliquez sur **Créer**, puis sur **Fermer**.

Création d'une stratégie de répondeur pour appeler la légende HTTP

Créez une stratégie de répondeur, Policy-Responder-4, qui vérifiera le corps de la requête et, si le corps contient le mot "
subject," invoquera la légende HTTP pour vérifier l'e-mail. Créez la stratégie avec les paramètres indiqués dans le tableau suivant. Bien que vous puissiez créer une stratégie de répondeur dans le sous-nœud

Stratégies, puis la lier globalement à l'aide du Gestionnaire de stratégies de répondeur, cette démonstration utilise le Gestionnaire de stratégies de répondeur pour créer la stratégie de répondeur et la lier globalement.

Paramètre	Valeur
Nom	Policy-Responder-4
Action	Action-Responder-4
Résultat indéfini - Action	-Action globale à résultat indéfini-
Expression.	"HTTP.REQ.BODY(1000).CONTAINS("urn:schemas:httpmail:su && SYS.HTTP_CALLOUT(HTTP-Callout-4)"

Pour créer une stratégie de répondeur à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Répondeur**.
2. Dans le volet d'informations, sous **Gestionnaire de stratégies**, cliquez sur Gestionnaire de **stratégies du répondeur**.
3. Dans la boîte de dialogue **Gestionnaire de stratégies de répondeur**, cliquez sur **Remplacer global**.
4. Cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur **Nouvelle stratégie**.
5. Dans la boîte de dialogue **Créer une stratégie de répondeur**, procédez comme suit :
   a) Dans Nom, tapez **Policy-Responder-4**.
   b) Dans Action, cliquez sur **Action-Responder-4**.
   c) Dans Action de résultat indéfini, cliquez sur Action **globale de résultat indéfini** .
   d) Dans la zone de texte **Expression**, tapez :

```
"HTTP.REQ.BODY(1000).CONTAINS("urn:schemas:httpmail:subject")
   && SYS.HTTP_CALLOUT(HTTP-Callout-4)"
<!--NeedCopy-->
```

   e) Cliquez sur **Créer**, puis sur **Fermer**.
6. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Création d'un agent de légende HTTP sur le serveur distant

Vous devez maintenant créer un agent de légende HTTP sur le serveur de légende distant. L'agent de légende HTTP reçoit les demandes de légende de l'appliance Citrix ADC et répond en conséquence. L'agent de légende est un script différent pour chaque déploiement et doit être écrit en tenant compte

des spécifications du serveur, telles que le type de base de données et le langage de script pris en charge.

Le pseudo-code suivant fournit des instructions pour créer un agent de légende qui vérifie une liste de mots généralement compris pour indiquer des courriers indésirables. L'agent peut être implémenté dans n'importe quel langage de programmation de votre choix. Le pseudo-code doit être utilisé uniquement comme guide pour le développement de l'agent de légende. Vous pouvez intégrer des fonctionnalités supplémentaires dans le programme.

Pour identifier le courrier indésirable à l'aide d'un pseudo-code

1. Acceptez le sujet de l'e-mail fourni par l'appliance Citrix ADC.
2. Connectez-vous à la base de données qui contient tous les termes par rapport auxquels l'objet de l'e-mail est vérifié.
3. Vérifiez les mots de l'objet de l'e-mail par rapport à la liste de mots spam.
4. Formater la réponse comme requis par la légende HTTP.
5. Envoyez la réponse à l'appliance Citrix ADC.

Cas d'utilisation : Commutation de contenu dynamique

August 20, 2021

Ce cas d'utilisation fournit un changement de contenu dynamique à l'aide d'une légende HTTP pour obtenir le nom du serveur virtuel d'équilibrage de charge vers lequel la demande est transférée.

1. Ajouter un serveur virtuel de commutation de contenu.

```
add cs vserver cs_vserver1 HTTP 10.102.29.196 80
<!--NeedCopy-->
```

2. Créez une légende HTTP.

```
add policy httpCallout http_callout1
<!--NeedCopy-->
```

3. Configurez la légende HTTP pour qu'elle réponde avec le nom du serveur virtuel d'équilibrage de charge à partir d'une requête contenant l'adresse IP du client dans l'en-tête HTTP « X-CLIENT-IP ».

```
> set policy httpCallout http_callout1 -IPAddress 10.217.14.23 -
    port 80 -returnType TEXT -hostExpr ""www.get-lbvip.com"" -
    urlStemExpr ""/index.html"" -headers X-CLIENT-IP(CLIENT.IP.SRC)
```



```
        -resultExpr "HTTP.RES.BODY(1000).AFTER_STR("<lbvip>").
      BEFORE_STR("<lbvip")"
2 <!--NeedCopy-->
```

4. Configurez l'action de commutation de contenu pour récupérer la réponse de légende.

```
1 add cs action cs_action1 -targetVserverExpr 'SYS.HTTP_CALLOUT(
     http_callout1)'
2 <!--NeedCopy-->
```

> Remarque :
>
> Vous devez lier un serveur virtuel d'équilibrage de charge au serveur virtuel de commutation de contenu pour tenir compte des éléments suivants :
>
> - Indisponibilité du serveur virtuel d'équilibrage de charge auquel la légende résout.
> - Condition UNDEF résultant de l'exécution de la légende.

```
1 > bind cs vserver cs_vserver1 -lbvserver default_lbvip
2 <!--NeedCopy-->
```

5. Configurez la stratégie de changement de contenu.

```
1 add cs policy cs_policy1 -rule true -action cs_action1
2 <!--NeedCopy-->
```

6. Liaison de la stratégie de commutation de contenu au serveur virtuel de commutation de contenu.

```
1 bind cs vserver cs_vserver1 -policyName cs_policy1 -priority 10
2 <!--NeedCopy-->
```

Jeux de motifs et jeux de données

October 5, 2021

Les expressions de stratégie pour les opérations de correspondance de chaînes sur un grand nombre de modèles de chaînes ont tendance à devenir longues et complexes. Les ressources consommées par l'évaluation de ces expressions complexes sont importantes en termes de cycles de traitement, de mémoire et de taille de configuration. Vous pouvez créer des expressions plus simples et moins gourmandes en ressources en utilisant la correspondance de motifs.

Selon le type de motifs que vous souhaitez faire correspondre, vous pouvez utiliser l'une des fonctions suivantes pour implémenter la correspondance de motifs :

- Un jeu de motifs est un tableau de modèles indexés utilisé pour la correspondance de chaînes lors de l'évaluation avancée des stratégies. Exemple de jeu de motifs : imagetypes {svg, bmp, png, gif, tiff, jpg}.
- Un ensemble de données est une forme spécialisée de jeu de motifs. Il s'agit d'un tableau de modèles de types nombre (entier), adresse IPv4 ou adresse IPv6.

Dans de nombreux cas, vous pouvez utiliser des jeux de modèles ou des jeux de données. Toutefois, dans les cas où vous souhaitez des correspondances spécifiques pour des données numériques ou des adresses IPv4 et IPv6, vous devez utiliser des jeux de données.

> **Remarque** :
>
> Les jeux de modèles et les jeux de données ne peuvent être utilisés que dans les stratégies avancées.

Pour utiliser des jeux de motifs ou des jeux de données, commencez par créer le jeu de motifs ou le jeu de données et liez-y des motifs. Ensuite, lorsque vous configurez une stratégie pour comparer une chaîne dans un paquet, utilisez un opérateur approprié et passez le nom du jeu de motifs ou de l'ensemble de données comme argument.

Fonctionnement de la correspondance de chaînes avec les jeux de motifs et les jeux de données

January 21, 2021

Un jeu de répétitions ou un ensemble de données contient un ensemble de répétitions, et chaque modèle reçoit un index unique. Lorsqu'une stratégie est appliquée à un paquet, une expression identifie une chaîne à évaluer et l'opérateur compare la chaîne aux modèles définis dans le jeu de motifs ou le jeu de données jusqu'à ce qu'une correspondance soit trouvée ou que tous les modèles aient été comparés. Ensuite, en fonction de sa fonction, l'opérateur renvoie soit une valeur booléenne qui indique si un motif correspondant a été trouvé ou non ou l'index du motif qui correspond à la chaîne.

Remarque : Cette rubrique explique le fonctionnement d'un jeu de motifs. Les ensembles de données fonctionnent de la même manière. La seule différence entre les jeux de répétitions et les jeux de données est le type de répétitions défini dans l'ensemble.

Considérez le cas d'utilisation suivant pour comprendre comment les modèles peuvent être utilisés pour la correspondance de chaînes.

Vous souhaitez déterminer si le suffixe URL (texte cible) contient l'une des extensions de fichier image. Sans utiliser de jeux de motifs, vous devrez définir une expression complexe, comme suit :

```
1 HTTP.REQ.URL.SUFFIX.CONTAINS("svg") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("
      bmp") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("png") ¦¦
```



```
2 HTTP.REQ.URL.SUFFIX.CONTAINS("gif") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("
    tiff") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("jpg")
3 <!--NeedCopy-->
```

Si l'URL a un suffixe « jpg », avec l'expression composée ci-dessus, l'appliance Citrix ADC doit parcourir l'ensemble de l'expression composée de manière séquentielle, d'une sous-expression à l'autre, pour déterminer que la requête fait référence à une image jpg. La figure suivante montre les étapes du processus.



Lorsqu'une expression composée comprend des centaines de sous-expressions, le processus ci-dessus nécessite beaucoup de ressources. Une meilleure alternative est une expression qui invoque un jeu de motifs, comme illustré dans la figure suivante.



Lors de l'évaluation de la stratégie, comme indiqué ci-dessus, l'opérateur (CONTAINS_ANY) compare la chaîne identifiée dans la requête avec les motifs définis dans le jeu de motifs jusqu'à ce qu'une correspondance soit trouvée. Avec l'expression Sample_Patset, les itérations multiples à travers six sous-expressions sont réduites à une seule.

En éliminant la nécessité de configurer des expressions composées qui effectuent la correspondance de chaînes avec plusieurs opérations OR, les jeux de motifs ou les jeux de données simplifient la configuration et accélèrent le traitement des demandes et des réponses.

Configuration d'un jeu de modèles

August 20, 2021

Pour configurer un jeu de motifs, vous devez spécifier les chaînes qui doivent servir de modèles. Vous pouvez attribuer manuellement une valeur d'index unique à chacun de ces modèles ou autoriser l'attribution automatique des valeurs d'index.

Remarque : Les jeux de motifs sont sensibles à la casse (sauf si vous spécifiez l'expression à ignorer la casse). Par conséquent, le modèle de chaîne « product1 », par exemple, n'est pas le même que le modèle de chaîne « Product1 ».

Points à retenir sur les valeurs d'index :

- Vous ne pouvez pas lier la même valeur d'index à plusieurs motifs.
- Une valeur d'index attribuée automatiquement est un nombre supérieur à la valeur d'index la plus élevée des modèles existants dans le jeu de motifs. Par exemple, si la valeur d'index la

plus élevée des modèles existants dans un jeu de répétitions est 104, la valeur d'index assignée automatiquement suivante est 105.

- Si vous ne spécifiez pas d'index pour le premier motif, la valeur d'index 1 est automatiquement affectée à ce modèle.
- Les valeurs d'index ne sont pas régénérées automatiquement si un ou plusieurs modèles sont supprimés ou modifiés. Par exemple, si l'ensemble contient cinq répétitions, avec des index compris entre 1 et 5, et si le motif avec un index de 3 est supprimé, les autres valeurs d'index du jeu de répétitions ne sont pas automatiquement régénérées pour produire des valeurs comprises entre 1 et 4.
- La valeur d'index maximale pouvant être affectée à un motif est 4294967290. Si cette valeur est déjà affectée à un motif dans l'ensemble, vous devez affecter manuellement des valeurs d'index à tous les modèles nouvellement ajoutés. Une valeur d'index inutilisée inférieure à une valeur actuellement utilisée ne peut pas être affectée automatiquement.

Pour configurer un jeu de motifs à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

1. Créez un jeu de motifs.

```
add policy patset <name>
```

Exemple :

```
add policy patset samplepatset
```

1. Liez des motifs à l'ensemble de motifs.

```
bind policy patset <name> <string> [-index <positive_integer>][-charset
 ( ASCII | UTF_8 )] [-comment <string>]
```

Exemple :

```
bind policy patset samplepatset product1 -index 1 -comment short description
 about the pattern bound to the pattern set
```

Remarque : Répétez cette étape pour tous les motifs que vous souhaitez lier au jeu de motifs.

1. Vérifiez la configuration.

```
show policy patset <name>
```

Pour configurer un jeu de motifs à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Jeux de motifs** .
2. Dans le volet d'informations, cliquez sur **Ajouter** pour ouvrir la boîte de dialogue **Créer un jeu de motifs** .

3. Spécifiez un nom pour le jeu de motifs dans la zone de texte Nom.
4. Sous Spécifier un motif, tapez le premier motif et, éventuellement, spécifiez des valeurs pour les paramètres suivants :
   - Traiter la barre oblique inverse comme caractère d'échappement : activez cette case à cocher pour spécifier que tous les caractères de barre oblique inverse que vous pourriez inclure dans le modèle doivent être traités comme des caractères d'échappement.
   - Indice : valeur d'index affectée par l'utilisateur, comprise entre 1 et 4294967290.
5. Vérifiez que vous avez entré les caractères corrects, puis cliquez sur **Ajouter**.
6. Répétez les étapes 4 et 5 pour ajouter d'autres motifs, puis cliquez sur **Créer**.

Configurer des jeux de modèles basés sur des fichiers

L'appliance Citrix ADC prend en charge les jeux de modèles basés sur des fichiers.

Pour configurer des jeux de modèles basés sur des fichiers à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes :

- Importez un nouveau fichier de jeu de modèles dans l'appliance Citrix ADC.

```
import policy patsetfile <src> <name> -delimiter <char> -charset
   <ASCII | UTF_8>
<!--NeedCopy-->
```

Exemple :

```
import policy patsetfile local:test.csv clientids_list -
   delimiter ,
<!--NeedCopy-->
```

Vous pouvez importer un fichier à partir d'un périphérique local, d'un serveur HTTP ou d'un serveur FTP. Pour ajouter le fichier à partir de votre périphérique local, le fichier doit être disponible à l' `/var/tmp` emplacement.

- Mettez à jour un fichier de jeu de modèles existant sur l'appliance Citrix ADC.

```
update policy -patsetfile <patset filename>
<!--NeedCopy-->
```

Exemple :

```
update policy -patsetfile clientids_list
<!--NeedCopy-->
```


- Ajoutez un fichier de jeu de motifs au moteur de paquets.

```
add policy -patsetfile <patset filename>
<!--NeedCopy-->
```

Exemple :

```
add policy -patsetfile clientids_list
<!--NeedCopy-->
```

- Liez des motifs à l'ensemble de motifs.

```
add policy patset <patset name> -patsetfile <patset filename>
<!--NeedCopy-->
```

Exemple :

```
add policy patset clientid_patset -patsetfile clientids_list
<!--NeedCopy-->
```

- Vérifiez la configuration.

```
show policy patsetfile clientids_list

Name: clientids_list
Patset Name: clientid_patset
Number of Imported Patterns: 8
Number of Bound Patterns: 8
(All the patterns bound successfully)

Done
<!--NeedCopy-->
```

Pour configurer des jeux de modèles basés sur des fichiers à l'aide de l'interface graphique

1. Accédez à **AppExpert > Fichiers de jeu de motifs**.
2. Dans le volet **Importé**, cliquez sur **Importer**.
3. Dans la page **Configurer le fichier de patchs de stratégie**, sélectionnez le fichier à importer, puis cliquez sur **OK**.
4. Sélectionnez le fichier importé, puis cliquez sur **Ajouter**.
5. Dans la page **Créer un fichier de patchs de stratégie**, entrez les détails, puis cliquez sur **Créer** pour ajouter un jeu de modèles de stratégie.

Configuration d'un ensemble de données

August 20, 2021

Pour configurer un jeu de données, vous devez spécifier les chaînes du serveur en tant que modèle, affecter un type (nombre, adresse IPv4 ou adresse IPv6) et configurer la plage du jeu de données. Vous pouvez attribuer manuellement une valeur d'index unique au modèle ou autoriser l'affectation automatique des valeurs d'index. Le jeu de données n'est pas lié à HTTP ou à un protocole de couche 7. Il fonctionne uniquement sur le texte ou la chaîne. Il existe différents types de jeux de données tels que NUM, ULONG, IPv4, IPv6, MAC, DOUBLE. Vous pouvez sélectionner un type et définir la plage du jeu de données en fonction du type spécifié.

> **Remarque :**
>
> Les jeux de données de stratégie sont sensibles à la casse (sauf si vous spécifiez l'expression à ignorer la casse). Par conséquent, l'adresse MAC ff:ff:ff:ff:ff:ff par exemple, n'est pas la même que l'adresse MAC FF:FF:FF:FF:FF:FF:FF:FF : FF.

Les règles appliquées aux valeurs d'index des ensembles de données sont similaires aux jeux de répétitifs. Pour plus d'informations sur les valeurs d'index, voir Configuration d'un jeu de modèles.

Pour configurer un jeu de données

Pour configurer un jeu de données, procédez comme suit :

1. Ajouter un jeu de données de stratégie
2. Lier un modèle à un jeu de données de stratégie
3. Ajouter une expression de stratégie
4. Vérifier la configuration de la stratégie

Ajouter un jeu de données de stratégie

À l'invite de commandes, procédez comme suit :

```
add policy dataset <name> <type>
```

Exemple :

```
add policy dataset ds1 ipv4 -comment numbers
```

Lier un motif à l'ensemble de données

À l'invite de commandes, tapez :


```
bind policy dataset <name> <value> [-index <positive_integer>] [-endRange <
string>] [-comment <string>]
```

Exemple :

```
bind policy dataset ds1 1.1.1.1 -endRange 1.1.1.10 -comment short description
 about the pattern bound to the data set
```

> **Remarque :**
>
> Vous devez répéter cette étape pour tous les modèles que vous souhaitez lier à l'ensemble de données. Vous ne pouvez lier qu'un maximum de 5000 motifs à un jeu de données.
>
> De plus, une plage de jeux de données ne doit pas se chevaucher avec d'autres plages liées à un jeu de données et ne peut pas inclure de valeurs uniques liées au jeu de données. Si vous liez un jeu de données avec une plage superposée entraîne une erreur.

Exemple :

```
1 add policy dataset ip_set ipv4
2  Done
3 bind policy dataset ip_set 2.2.2.25
4  Done
5 bind policy dataset ip_set 2.2.2.20 -endRange 2.2.2.30
6 ERROR: The range overlaps an existing range or includes a value bound
     to the dataset.
7 <!--NeedCopy-->
```

Une valeur est considérée comme étant dans l'ensemble de données si elle est égale à une valeur unique liée à l'ensemble de données ou se situe entre la valeur inférieure et la valeur supérieure (valeur inférieure <= valeur && valeur <- valeur supérieure), pour une plage liée à l'ensemble de données.

Utiliser l'expression de stratégie dans un jeu de données de stratégie

À l'invite de commandes, tapez :

```
add policy expression exp1 http.req.body(100).contains_any("ds1")
```

Où,
L'expression vérifie s'il y a un motif (ou motif dans la plage) lié au jeu de données ds1 est présent dans les 100 premiers octets du corps de la requête HTTP.

Vérifier la configuration du jeu de données

À l'invite de commandes, tapez :


```
show policy dataset ds1
> show policy dataset ds1
```

Exemple :

```
1         Dataset:        ds1
2          Type:   IPV4
3 1)       Bound Dataset Range from: 1.1.1.1       through: 1.1.1.10
            Index:  1
4 <!--NeedCopy-->
```

Pour configurer un ensemble de données à l'aide de l'utilitaire de configuration

Suivez les étapes ci-dessous pour configurer un jeu de données de stratégie :

1. Accédez à **AppExpert > Ensembles de données**.
2. Dans le volet d'informations, sous Ensembles de données, cliquez sur **Ajouter**.
3. Dans la page **Configurer le jeu de données**, définissez les paramètres suivants.
   a) Nom. Nom du jeu de données de stratégie.
   b) Type. Type de valeur à lier au jeu de données.

   Configuration d'un jeu de données
4. Cliquez sur **Insérer** pour lier la valeur du jeu de données d'un type spécifique.
   a) Valeur. Valeur du type spécifié associé au jeu de données.
   b) Index. Valeur d'index du jeu de données.
   c) Plage d'extrémité. Entrée du jeu de données. C'est une plage <value> à <end_range>.
   d) Commentaires. Une brève description de l'ensemble de données.

   liaison de jeu de données
5. Cliquez sur **Insérer** et **fermer**.
6. Saisissez des commentaires.
7. Cliquez sur **Créer** et **Fermer**.

Utilisation de jeux de motifs et de jeux de données

October 5, 2021

Les expressions de stratégie avancées qui prennent des jeux de modèles ou des jeux de données comme argument peuvent être utilisées pour effectuer des opérations de mise en correspondance de chaînes.

L'utilisation est la suivante :

```
<text>.<operator>("<name>")
<!--NeedCopy-->
```

où,

- <text> est l'expression qui identifie une chaîne dans un paquet. Exemple : HTTP.REQ.HEADER("Host").
- <operator> est l'un des opérateurs décrits dans le tableau Types de jeux de modèles pdf.

Pour connaître l'utilisation des échantillons, voir Utilisation de l'échantillon.

Exemple d'utilisation

August 20, 2021

Pour comprendre l'utilisation des jeux de motifs dans les expressions, considérez l'exemple d'un jeu de motifs nommé "imagetypes."

Modèles	Valeur de l'indice
svg	1
bmp	2
png	3
gif	4
Tiff	5
jpg	6

Tableau 1. Jeu de motifs « imagetypes »

Exemple 1 : Déterminez si le suffixe d'une requête HTTP est l'une des extensions de fichier définies dans le jeu de motifs « imagetypes ».

- **Expression.** HTTP.REQ.URL.SUFFIX.EQUALS_ANY("imagetypes")
- **Exemple d'URL.** http://www.example.com/homepageicon.jpg
- **Résultat.** VRAI

Exemple 2 : Déterminez si le suffixe d'une requête HTTP est l'une des extensions de fichier définies dans le jeu de motifs « imagetypes » et renvoyez l'index de ce modèle.

- **Expression.** HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes")

- **Exemple d'URL.** `http://www.example.com/mylogo.png`
- **Résultat.** 4 (La valeur d'index du motif « gif ».)

Exemple 3 : Utilisez la valeur d'index d'un modèle pour déterminer si le suffixe d'URL se trouve dans une plage de valeurs d'index spécifiée.

- **Expression.** HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes").GE(3) && HTTP.REQ.URL.SUFFIX.EQUALS
- **Exemple d'URL.** `http://www.example.com/mylogo.png`
- **Résultat.** TRUE (La valeur d'index des types de fichiers gif est 4.)

Exemple 4 : implémentez un ensemble de stratégies pour les extensions de fichiers bmp, jpg et png, et un autre ensemble de stratégies pour les fichiers gif, tiff et svg.

Une expression qui renvoie l'index d'un motif apparié peut être utilisée pour définir des sous-ensembles de trafic pour une application Web. Les deux expressions suivantes peuvent être utilisées dans les stratégies de commutation de contenu pour un serveur virtuel de commutation de contenu :

- HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes").LE(3)
- HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes").GE(4)

Variables

January 21, 2021

Les variables sont des objets nommés qui stockent des informations sous la forme de jetons. Ces jetons sont utilisés dans et entre différentes transactions sur l'appliance Citrix ADC pour le calcul interne et le traitement des stratégies.

L'appliance Citrix ADC prend en charge la création de variables des types suivants :

- **Variables singleton.** Peut avoir une valeur unique de l'un des types suivants : ulong et text (taille max-size). Le type ulong est un entier 64 bits non signé, le type de texte est une séquence d'octets et la taille max-size est le nombre maximal d'octets dans la séquence.
- **Mapper les variables.** Les cartes contiennent des valeurs associées aux clés : chaque paire clé-valeur est appelée entrée de carte. La clé de chaque entrée est unique dans la carte. Les cartes sont spécifiées comme suit :

  map (key_type, value_type, max-values).

  où,

  - *key_type* est le type de données de la clé. Il est de type texte (taille max-size).
  - *value_type* est le type de données des valeurs de la carte. Il peut être de type ulong ou texte (taille max-size).

- *valeurs max-value* est le nombre maximal d'entrées que la carte peut contenir. C'est de type ulong.

Les valeurs de ces variables sont définies à l'aide d'affectations qui doivent être invoquées lors des actions de stratégie.

> **Remarque** : les variables ne sont pas encore prises en charge dans une configuration haute disponibilité ou dans un cluster.

Champ d'application des variables

Une variable de carte ou une variable singleton peut avoir une portée globale. Alternativement, la portée d'une variable singleton peut être limitée à une seule transaction.

- **Variable de portée globale** : une variable avec portée globale (valeur par défaut) n'a qu'une seule instance, et cette instance a la ou les mêmes valeurs sur tous les cœurs d'une appliance Citrix ADC et sur tous les nœuds d'une configuration de cluster ou de HA. Les valeurs de variables globales existent jusqu'à ce qu'elles soient explicitement supprimées, jusqu'à leur expiration, ou jusqu'à ce qu'une appliance autonome soit redémarrée ou que tous les nœuds d'une configuration de cluster ou de HA soient redémarrés.
- **Variable d'étendue** de transaction : une variable avec étendue de transaction possède une instance distincte, avec sa propre valeur, pour chaque transaction traitée par l'appliance Citrix ADC. Lorsque le traitement de la transaction est terminé, la valeur de la variable de transaction est supprimée.

> **Remarque** : Les variables d'étendue de transaction sont disponibles dans Citrix ADC version 10.5.e ou ultérieure.

Configuration et utilisation de variables

January 21, 2021

Vous devez d'abord créer une variable, puis affecter une valeur ou spécifier l'opération qui doit être effectuée sur la variable. Après avoir effectué ces opérations, vous pouvez utiliser l'affectation comme action de stratégie.

Remarque : une fois configuré, les paramètres d'une variable ne peuvent pas être modifiés ou réinitialisés. Si la variable doit être modifiée, la variable et toutes les références à la variable (expressions et affectations) doivent être supprimées. La variable peut ensuite être rajoutée avec de nouveaux paramètres, et les références (expressions et affectations) peuvent être rajoutées.

Pour configurer des variables à l'aide de l'interface de ligne de commande

1. Créez une variable.

```
add ns variable <name> -type <string> [-scope global] [-ifFull ( undef
    | lru )] [-ifValueTooBig ( undef | truncate )] [-ifNoValue ( undef |
     init )] [-init <string>] [-expires <positive_integer>] [-comment <
    string>]
<!--NeedCopy-->
```

Remarque : Reportez-vous à la page man « man add ns variable » pour la description des paramètres de commande.

Exemple 1 : Créez une variable ulong nommée « my_counter » et initialisez-la à 1.

```
add ns variable my_counter  - type ulong -init 1
<!--NeedCopy-->
```

Exemple 2 : Créer une carte nommée « user_privilege_map ». La carte contiendra des clés d'une longueur maximale de 15 caractères et des valeurs de texte d'une longueur maximale de 10 caractères, avec un maximum de 10000 entrées.

```
add ns variable user_privilege_map -type map(text(15),text(10),10000)
<!--NeedCopy-->
```

Remarque : Si la carte contient 10000 entrées non expirées, les affectations pour les nouvelles clés réutilisent l'une des entrées les moins récemment utilisées. Par défaut, une expression essayant d'obtenir une valeur pour une clé inexistante initialisera une valeur de texte vide.

Affectez la valeur ou spécifiez l'opération à effectuer sur la variable. Cela se fait en créant une affectation.

```
add ns assignment <name> -variable <expression> [-set <expression> | -
    add <expression> | -sub <expression> | -append <expression> | -clear
    ] [-comment <string>]
<!--NeedCopy-->
```

Remarque : Une variable est référencée à l'aide du sélecteur de variable ($). Par conséquent, **$variable1** est utilisé pour faire référence à des variables de texte ou ulong. De même, **$variable2[key-expression]**est utilisée pour faire référence à des variables de carte.

Exemple 1 : Définissez une affectation nommée « inc_my_counter » qui ajoute automatiquement 1 à la variable « my_counter ».

```
add ns assignment inc_my_counter -variable $my_counter -add 1
<!--NeedCopy-->
```


Exemple 2 : Définissez une affectation nommée « set_user_privilege » qui ajoute à la variable « user_privilege_map » une entrée pour l'adresse IP du client avec la valeur renvoyée par la légende HTTP « get_user_privilege ».

```
1 add ns assignment set_user_privilege -variable $user_privilege_map[
     client.ip.src.typecast_text_t] -set sys.http.callout(
     get_user_privilege)
2 <!--NeedCopy-->
```

Remarque : Si une entrée pour cette clé existe déjà, la valeur sera remplacée. Sinon, une nouvelle entrée pour la clé et la valeur sera ajoutée. Sur la base de la déclaration précédente pour user_privilege_map, si la carte contient déjà 10000 entrées, l'une des entrées les moins récemment utilisées sera réutilisée pour la nouvelle clé et la nouvelle valeur.

1. Appelez l'affectation de variable dans une stratégie.

   Il existe deux fonctions qui peuvent fonctionner sur des variables de carte.

   - **$name.valueExists(key-expression).** Renvoie true s'il y a une valeur dans la carte sélectionnée par l'expression clé. Sinon renvoie false. Cette fonction met à jour les informations d'expiration et de LRU si l'entrée de carte existe, mais ne crée pas de nouvelle entrée de carte si la valeur n'existe pas.
   - **$name.valueCount.** Renvoie le nombre de valeurs actuellement détenues par la variable. Il s'agit du nombre d'entrées dans une carte. Pour une variable singleton, ceci est 0 si la variable n'est pas initialisée ou 1 autrement.

   Exemple : invoquez l'affectation nommée « set_user_privilege » avec une stratégie de compression.

```
1 add cmp policy set_user_privilege_pol -rule $user_privilege_map.
     valueExists(client.ip.src.typecast_text_t).not -resAction
     set_user_privilege
2 <!--NeedCopy-->
```

Cas d'utilisation pour insérer un en-tête HTTP dans le côté réponse

L'exemple suivant montre un exemple de variable singleton.

Ajoutez une variable singleton de type texte. Cette variable peut contenir un maximum de 100 octets de données.

```
1 add ns variable http_req_data -type text(100) -scope transaction
2 <!--NeedCopy-->
```


Ajoutez une action d'affectation, qui sera utilisée pour stocker les données de requête HTTP dans la variable.

```
add ns assignment set_http_req_data -variable $http_req_data -set http.
   req.body(100)
<!--NeedCopy-->
```

Ajoutez une action de réécriture pour insérer l'en-tête HTTP, dont la valeur sera récupérée à partir de la variable.

```
add rewrite action act_ins_header insert_http_header user_name
   $http_req_data.after_str("user_name").before_str("password")
<!--NeedCopy-->
```

Ajoutez une stratégie de réécriture qui évaluera dans l'heure de la requête et effectuera une action d'affectation pour stocker les données. Lorsque nous atteignons cette stratégie, nous allons prendre l'action d'affectation et stocker les données dans la variable ns (http_req_data)

```
add rewrite policy pol_set_variable true set_http_req_data

bind rewrite global pol_set_variable 10 -type req_dEFAULT
<!--NeedCopy-->
```

Ajoutez une stratégie de réécriture qui évaluera dans le temps de réponse, et ajoutez un en-tête HTTP dans la réponse.

```
add rewrite policy pol_ins_header true act_ins_header

bind rewrite global pol_ins_header 10 -type res_dEFAULT
<!--NeedCopy-->
```

Action d'affectation

Dans une appliance Citrix ADC, une action d'affectation liée à la stratégie est déclenchée lorsque la règle de stratégie est évaluée à true. L'action met à jour la valeur de la variable qui peut être utilisée dans les évaluations ultérieures des règles de stratégie. De cette façon, la même variable peut être mise à jour et utilisée pour des évaluations de stratégie ultérieures dans la même fonctionnalité. Auparavant, l'appliance exécutait des actions d'affectation uniquement après avoir évalué toutes les stratégies de la fonction lorsque les stratégies des actions d'affectation associées étaient évaluées à true. Par conséquent, la valeur de variable définie par l'action d'affectation ne peut pas être utilisée dans les évaluations de règles de stratégie suivantes au sein de la fonction.

Cette fonctionnalité peut être mieux comprise avec un cas d'utilisation qui contrôle la liste d'accès des clients sur une appliance Citrix ADC. La décision d'accès est fournie par un service Web distinct, avec la

demandeGET /client-access?<client-IP-address> qui renvoie une réponse avec « BLOCK » ou « Autoriser » dans le corps. La légende HTTP est configurée pour inclure l'adresse IP du client associée à une requête entrante. Lorsque l'appliance Citrix ADC reçoit une demande d'un client, l'appliance génère la demande de légende et l'envoie au serveur de légende, qui héberge une base de données d'adresses IP figurant sur la liste noire et un agent de légende HTTP qui vérifie si l'adresse IP du client est répertoriée dans la base de données. L'agent de légende HTTP reçoit la demande de légende, vérifie si l'adresse IP du client est répertoriée et envoie une réponse. La réponse est un code d'état, 200, 302 avec « BLOCK » ou « Autoriser » dans le corps. En fonction du code d'état, l'appliance effectue l'évaluation de la stratégie. Si l'évaluation de stratégie a la valeur true, l'action d'affectation est déclenchée immédiatement et l'action définit la valeur à la variable. L'appliance utilise et définit cette valeur de variable pour une évaluation ultérieure de stratégie dans le même module.

Cas d'utilisation pour configurer l'action d'affectation

Suivez les étapes ci-dessous pour configurer l'action d'affectation et utiliser la variable pour les stratégies suivantes :

1. La décision d'accès est fournie par un service Web séparé, avec la demande qui renvoie une réponse avec BLOCK ou Autoriser dans le corps.

   ```
   GET /url-service>/url-allowed?<URL path>
   ```

2. Configurez une variable de carte pour contenir les décisions d'accès pour les URL.

   ```
   add ns variable url_list_map -type 'map(text(1000),text(10),10000)'
   ```

3. Configurez une légende HTTP pour envoyer la demande d'accès au service Web.

   ```
   add policy httpCallout url_list_callout -vserver url_vs -returnType
   TEXT -urlStemExpr '"/url-allowed?" + HTTP.REQ.URL.PATH'-resultExpr '
   HTTP.RES.BODY(10)'
   ```

4. Configurez une action d'affectation pour appeler la légende pour obtenir la décision d'accès et l'affecter à l'entrée de mappage de l'URL.

   ```
   add ns assignment client_access_assn -variable '$client_access_map[
   CLIENT.IP.SRC.TYPECAST_TEXT_T]'-set SYS.HTTP_CALLOUT(client_access_callout
   )
   ```

5. Configurez une action de répondeur pour envoyer une réponse 403 si une requête d'URL est bloquée.

   ```
   add responder action url_list_block_act respondwith '"HTTP/1.1 403
   Forbidden\\r\\n\\r\\n"'
   ```

6. Configurez une stratégie de répondeur pour définir l'entrée de carte pour l'URL si elle n'est pas déjà définie. Avec l'amélioration de l'action immédiate, la valeur d'entrée de carte est définie

lors de l'évaluation de cette stratégie. Avant l'amélioration, l'affectation n'a pas été effectuée avant que toutes les stratégies des intervenants aient été évaluées décision est fournie par un service Web distinct.

```
add responder policy url_list_assn_pol '!$url_list_map.VALUEEXISTS(HTTP
.REQ.URL.PATH)'url_list_assn
```

7. Configurez une stratégie de répondeur pour bloquer l'accès à une URL si sa valeur d'entrée de carte est BLOCK. Avec l'amélioration de l'action immédiate, l'entrée de carte définie par la stratégie précédente peut être utilisée dans cette stratégie. Avant l'amélioration, l'entrée de carte n'est toujours pas définie à ce stade.

   ```
   add responder policy client_access_block_pol '$client_access_map[CLIENT
   .IP.SRC.TYPECAST_TEXT_T] == "BLOCK"'client_access_block_act
   ```

8. Liez les stratégies de répondeur au serveur virtuel. **Remarque** : Nous ne pouvons pas lier globalement les stratégies car nous ne voulons pas les exécuter pour la légende HTTP sur un serveur virtuel distinct.

   ```
   bind lb vserver vs -policyName client_access_assn_pol -priority 10 -
   gotoPriorityExpression NEXT -type REQUEST
   bind lb vserver vs -policyName client_access_block_pol -priority 20 -
   gotoPriorityExpression END -type REQUEST
   ```

Pour configurer des variables à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert > Variables NS**, pour créer une variable.
2. Accédez à **AppExpert > NS Assignments**, pour affecter des valeurs à la variable.
3. Accédez à la zone d'entités appropriée dans laquelle vous souhaitez configurer l'affectation en tant qu'action.

Cas d'utilisation : mise en cache des privilèges utilisateur

January 21, 2021

Dans ce cas d'utilisation, les privilèges utilisateur (« GOLD », « SILVER », etc.) doivent être récupérés à partir d'un service Web externe.

Pour réaliser ce cas d'utilisation, effectuez les opérations suivantes

Créez une légende HTTP pour récupérer les privilèges utilisateur à partir du service Web externe.


```
add policy httpcallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port <port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod ( GET | POST )] [-hostExpr <string>] [-urlStemExpr <string>] [-headers <name(value)> ...] [-parameters <name(value)> ...] [-bodyExpr <string>][-fullReqExpr <string>] [-scheme ( http | https )] [-resultExpr <string>] [-cacheForSecs <secs>] [-comment <string>]

add policy httpcallout get_user_privilege -ipaddress 10.217.193.84 -port 80 -returnType text -httpMethod GET -hostExpr '"/get_user_privilege"' -resultExpr 'http.res.body(5)'
<!--NeedCopy-->
```

Stockez les privilèges dans une variable.

```
add ns variable <name> -type <string> [-scope ( global | transaction )][-ifFull ( undef | lru )] [-ifValueTooBig ( undef | truncate )][-ifNoValue ( undef | init )] [-init <string>] [-expires <positive_integer>] [-comment <string>]

add ns variable user_privilege_map -type map(text(15),text(10),10000) -expires 1200

add ns assignment set_user_privilege -variable $user_privilege_map[client.ip.src] -set sys.http_callout(get_user_privilege)
<!--NeedCopy-->
```

Créez une stratégie pour vérifier s'il existe déjà une entrée mise en cache pour l'adresse IP du client ; sinon, il appelle la légende HTTP pour définir une entrée de mappage pour le client.

```
add cmp policy <name> -rule <expression> -resAction <string>

add cmp policy set_user_privilege_pol -rule $user_privilege_map.valueExists(client.ip.src).not -resAction set_user_privilege>
<!--NeedCopy-->
```

Créez une stratégie qui compresse si l'entrée de privilège mise en cache pour le client est « GOLD ».

```
add cmp policy <name> -rule <expression> -resAction <string>

add cmp policy compress_if_gold_privilege_pol -rule '$user_privilege_map[client.ip.src].eq("GOLD")' -resAction compress
<!--NeedCopy-->
```

Liez les stratégies de compression globalement.


```
bind cmp global <policyName> [-priority <positive_integer>] [-state (
    ENABLED | DISABLED )] [-gotoPriorityExpression <expression>] [-type
    <type>] [-invoke (<labelType> <labelName>) ]

bind cmp global set_user_privilege_pol -priority 10 NEXT

bind cmp global compress_if_gold_privilege_pol -priority 20 END
<!--NeedCopy-->
```

Cas d'utilisation : Limitation du nombre de sessions

January 21, 2021

Dans ce cas d'utilisation, il est nécessaire de limiter le nombre de sessions backend actives. Dans le déploiement, chaque connexion de session a une connexion dans l'URL et chaque déconnexion de session a une déconnexion dans l'URL. En cas de connexion réussie, le backend définit un cookie sessionid avec une valeur unique de 10 caractères.

Pour réaliser ce cas d'utilisation, effectuez les opérations suivantes :

1. Créez une variable de carte qui peut stocker chaque session active. La clé de la carte est le sessionid. La durée d'expiration de la variable est définie sur 600 secondes (10 minutes).

   ```
   > add ns variable session_map -type map(text(10),ulong,100) -
       expires 600
   <!--NeedCopy-->
   ```

2. Créez les affectations suivantes pour la variable de carte :

   - Créez une entrée pour le sessionid et définissez cette valeur sur 1 (cette valeur n'est pas réellement utilisée).

     ```
     > add ns assignment add_session -variable '$session_map[http.
         req.cookie.value("sessionid")]' -set 1
     <!--NeedCopy-->
     ```

   - Déplacez l'entrée d'un ID de session, qui décrémente implicitement le nombre de valeurs pour session_map.

     ```
     > add ns assignment delete_session -variable '$session_map[
         http.req.cookie.value("sessionid")]' -clear
     <!--NeedCopy-->
     ```


3. Créez des stratégies de répondeur pour les éléments suivants :

   - Pour vérifier si une entrée de mappage existe pour ce sessionid dans la requête HTTP. L'affectation add_session est exécutée si l'entrée de carte n'existe pas.

     ```
     1 > add responder policy add_session_pol 'http.req.url.contains
         ("twbkwbis.P_SabanciLogin") || $session_map.valueExists(
         http.req.cookie.value("netsuis"))' add_session
     2 <!--NeedCopy-->
     ```

     Remarque : La fonction
     valueExists () de la stratégie
     add_session_pol est considérée comme une référence à l'entrée de mappage de la session, de sorte que chaque requête réinitialise le délai d'expiration de sa session. Si aucune demande de session n'est reçue après 10 minutes, l'entrée de la session sera désallouée.

   - Pour vérifier si la session est déconnectée. L'affectation delete_session est exécutée.

     ```
     1 add responder policy delete_session_pol "http.req.url.
         contains("Logout")" delete_session
     2 <!--NeedCopy-->
     ```

   - Pour vérifier les demandes de connexion et si le nombre de sessions actives dépasse 100. Si ces conditions sont remplies, afin de limiter le nombre de sessions, l'utilisateur est redirigé vers une page indiquant que le serveur est occupé.

     ```
     1 add responder action redirect_too_busy redirect "/too_busy.
         html"
     2 add responder policy check_login_pol "http.req.url.contains("
         twbkwbis.P_SabanciLogin") && $session_map.valueCount > 100
         " redirect_too_busy
     3 <!--NeedCopy-->
     ```

4. Liez les stratégies de répondeur à l'échelle mondiale.

   ```
   1 bind responder global add_session_pol 30 next
   2 bind responder global delete_session_pol 10
   3 bind responder global check_login_pol 20
   4 <!--NeedCopy-->
   ```


Politiques et expressions

October 5, 2021

Les rubriques suivantes fournissent les informations conceptuelles et de référence dont vous avez besoin pour configurer des stratégies avancées sur l'appliance Citrix® ADC® Citrix®.

Pour en savoir plus sur toutes les expressions de stratégie avancées prises en charge sur l'appliance Citrix ADC, consultez Expressions de stratégie.

Introduction aux stratégies et expressions	Décrit l'objectif des expressions, des stratégies et des actions, ainsi que la façon dont les différentes applications Citrix ADC les utilisent.
Configuration des stratégies avancées	Décrit la structure des stratégies avancées et la façon de les configurer individuellement et en tant que banques de stratégies.

Configuration des expressions avancées : mise en route	Décrit la syntaxe et la sémantique des expressions, et explique brièvement comment configurer les expressions et les stratégies.
Expressions avancées : évaluation du texte	Décrit les expressions que vous configurez lorsque vous souhaitez utiliser du texte (par exemple, le corps d'une demande HTTP POST ou le contenu d'un certificat utilisateur).

Expressions avancées : utilisation des dates, des heures et des nombres	Décrit les expressions que vous configurez lorsque vous souhaitez utiliser n'importe quel type de données numériques (par exemple, la longueur d'une URL, l'adresse IP d'un client ou la date et l'heure d'envoi d'une demande HTTP).
Expressions avancées : analyse des données HTTP, TCP et UDP	Décrit les expressions d'analyse des adresses IP et IPv6, des adresses MAC et des données spécifiques au trafic HTTP et TCP.

Expressions avancées : analyse des certificats SSL	Explique comment configurer des expressions pour le trafic SSL et les certificats clients, par exemple, comment récupérer la date d'expiration d'un certificat ou de l'émetteur du certificat.

Expressions avancées : adresses IP et MAC, débit, ID VLAN	Décrit les expressions que vous pouvez utiliser pour travailler avec d'autres données liées au client ou au serveur qui ne sont pas abordées dans d'autres chapitres.	Typecasting Data	Décrit les expressions permettant de transformer des données d'un type en un autre.	Expressions régulières	Décrit comment transmettre des expressions régulières en tant qu'arguments aux opérateurs dans les expressions avancées.	Référence des
expressions	Une référence pour les arguments d'expression avancés.	Résumé des exemples d'expressions et de stratégies avancées	Exemples d'expressions et de stratégies avancées, au format de référence rapide et de didacticiel, que vous pouvez personnaliser pour votre propre usage.			

Tutoriel Exemples de stratégies avancées de réécriture	Exemples de stratégies avancées à utiliser dans la fonction de réécriture.
Tutoriel Exemples de stratégies	Exemples de stratégies pour les fonctionnal-ités de Citrix ADC telles que le pare-feu d'application et le protocole SSL.

Migration des règles Apache mod_rewrite vers des stratégies avancées	Exemples de fonctions écrites à l'aide du moteur mod_rewrite du serveur HTTP Apache, avec des exemples de ces fonctions après traduction en stratégies de réécriture et de répondeur sur Citrix ADC.

Introduction aux politiques et expressions

October 5, 2021

Pour de nombreuses fonctionnalités Citrix ADC, les stratégies contrôlent la façon dont une fonctionnalité évalue les données. Une stratégie utilise une expression logique, appelée en règle générale, pour évaluer les données et applique une ou plusieurs actions basées sur l'évaluation. Une stratégie peut également appliquer un profil, qui définit une action complexe.

Certaines fonctionnalités de Citrix ADC utilisent des stratégies avancées, qui offrent des fonctionnalités supérieures à celles des stratégies classiques plus anciennes. Si vous avez migré vers une version plus récente du logiciel Citrix ADC et que vous avez configuré des stratégies classiques pour les fonc-

tionnalités qui utilisent des stratégies avancées, vous devez migrer manuellement les stratégies vers une infrastructure de stratégies avancées.

Infrastructure de stratégie

October 5, 2021

> **Avertissement**
>
> Les expressions de stratégie classiques sont obsolètes à partir de Citrix ADC 12.0 build 56.20 et à titre d'alternative, Citrix vous recommande d'utiliser des stratégies avancées. Pour plus d'informations, consultez la section Stratégies avancées

L'infrastructure de stratégie avancée (PI) vous permet d'analyser davantage de données (par exemple, le corps d'une requête HTTP) et de configurer davantage d'opérations dans la règle de stratégie (par exemple, la transformation des données du corps d'une demande en en-tête HTTP).

Outre l'attribution d'une action ou d'un profil à une stratégie, vous la liez à un point particulier du traitement associé aux fonctionnalités de Citrix ADC. Le point de liaison est l'un des facteurs qui déterminent le moment où la stratégie sera évaluée.

Avantages de l'utilisation de stratégies avancées

Les stratégies de stratégie avancées utilisent un langage d'expression puissant basé sur un modèle d'objet de classe, et elles offrent plusieurs options qui améliorent votre capacité à configurer le comportement de diverses fonctionnalités de Citrix ADC. Avec l'infrastructure de stratégies avancées (PI), vous pouvez effectuer les opérations suivantes :

- Effectuer des analyses minces du trafic réseau des couches 2 à 7.
- Évaluez toute partie de l'en-tête ou du corps d'une requête ou réponse HTTP ou HTTPS.
- Liez les stratégies aux différents points de liaison pris en charge par l'infrastructure de stratégies avancées (PI) aux niveaux par défaut, de remplacement et de serveur virtuel.
- Utilisez les expressions goto pour transférer le contrôle vers d'autres stratégies et points de liaison, comme déterminé par le résultat de l'évaluation de l'expression.
- Utilisez des outils spéciaux tels que des jeux de motifs, des étiquettes de stratégie, des identificateurs de limite de débit et des légendes HTTP, qui vous permettent de configurer efficacement les stratégies pour des cas d'utilisation complexes.

En outre, l'utilitaire de configuration étend la prise en charge robuste de l'interface utilisateur graphique pour l'infrastructure de stratégie avancée (PI) et les expressions et permet aux utilisateurs qui ont une connaissance limitée des protocoles réseau de configurer rapidement et facilement des stratégies. L'utilitaire de configuration inclut également une fonctionnalité d'évaluation de

stratégie pour les stratégies avancées. Vous pouvez utiliser cette fonctionnalité pour évaluer une stratégie avancée et tester son comportement avant de la valider, réduisant ainsi le risque d'erreurs de configuration.

Composants de base d'une stratégie avancée

Voici quelques caractéristiques d'une stratégie avancée :

- Name. Chaque stratégie possède un nom unique.
- Rule. La règle est une expression logique qui permet à la fonctionnalité Citrix ADC d'évaluer un élément de trafic ou un autre objet. Par exemple, une règle peut permettre à Citrix ADC de déterminer si une requête HTTP provient d'une adresse IP particulière ou si un en-tête Cache-Control d'une requête HTTP a la valeur « No-Cache ».

Les stratégies avancées peuvent utiliser toutes les expressions disponibles dans une stratégie classique, à l'exception des expressions classiques pour le client VPN SSL. En outre, les stratégies avancées vous permettent de configurer des expressions plus complexes.

- Fixations. Pour vous assurer que Citrix ADC peut invoquer une stratégie lorsque cela est nécessaire, vous associez la stratégie, ou la liez, à un ou plusieurs points de liaison.

Vous pouvez lier une stratégie globalement ou à un serveur virtuel. Pour plus d'informations, voir À propos des liaisons de stratégies.

- Une action associée. Une action est une entité distincte d'une stratégie. L'évaluation des stratégies aboutit finalement à l'exécution d'une action par Citrix ADC.

Par exemple, une stratégie du cache intégré peut identifier les requêtes HTTP pour les fichiers .png ou .jpeg. Une action que vous associez à cette stratégie détermine que les réponses à ces types de demandes sont diffusées à partir du cache.

Pour certaines fonctionnalités, vous configurez des actions dans le cadre d'un ensemble d'instructions plus complexe appelé profil.

Utilisation des stratégies par différentes fonctionnalités de Citrix ADC

Citrix ADC prend en charge diverses fonctionnalités qui reposent sur des stratégies de fonctionnement. Le tableau suivant récapitule la façon dont les fonctionnalités Citrix ADC utilisent les stratégies.

Nom de la fonctionnalité	Type de stratégie	Utilisation des stratégies dans la fonctionnalité
Système	Classique	Pour la fonction Authentification, les stratégies contiennent des schémas d'authentification pour différentes méthodes d'authentification. Par exemple, vous pouvez configurer des schémas d'authentification LDAP et basés sur des certificats. Vous pouvez également configurer des stratégies dans la fonction Audit.
DNS	Advanced	Pour déterminer comment effectuer une résolution DNS pour les requêtes.
SSL	Classic et Advanced	Pour déterminer quand appliquer une fonction de chiffrement et ajouter des informations de certificat en texte clair. Pour assurer une sécurité de bout en bout, après le déchiffrement d'un message, la fonctionnalité SSL recrypte le texte en clair et utilise SSL pour communiquer avec les serveurs Web.
Compression SSL	Classic et Advanced	Pour déterminer le type de trafic qui est compressé.
Mise en cache intégrée	Advanced	Pour déterminer si les réponses HTTP peuvent être mises en cache.
Répondeur	Advanced	Pour configurer le comportement de la fonction Responder.

Nom de la fonctionnalité	Type de stratégie	Utilisation des stratégies dans la fonctionnalité
Caractéristiques de protection	Classique	Pour configurer le comportement des fonctions Filter, SureConnect et Priority Queuing.
Commutation de contenu	Classic et Advanced	Pour déterminer quel serveur ou groupe de serveurs est responsable du traitement des réponses, en fonction des caractéristiques d'une demande entrante. Les caractéristiques de la demande incluent le type de périphérique, la langue, les cookies, la méthode HTTP, le type de contenu et le serveur de cache associé.
AAA - Gestion du trafic	Classique. Exceptions : Les stratégies de trafic prennent uniquement en charge les infrastructures de stratégies avancées (PI) et les stratégies d'autorisation prennent en charge l'infrastructure de stratégie avancée (PI).	Pour vérifier la sécurité côté client avant que les utilisateurs se connectent et établissent une session. Les stratégies de trafic, qui déterminent si l'authentification unique (SSO) est requise, utilisent uniquement la stratégie Avancée. Les stratégies d'autorisation autorisent les utilisateurs et les groupes qui accèdent aux ressources intranet via l'appliance.
Redirection de cache	Classique	Pour déterminer si les réponses sont diffusées à partir d'un cache ou d'un serveur d'origine.

Nom de la fonctionnalité	Type de stratégie	Utilisation des stratégies dans la fonctionnalité
Réécrire	Advanced	Pour identifier les données HTTP que vous souhaitez modifier avant de les transmettre. Les stratégies fournissent des règles pour la modification des données. Par exemple, vous pouvez modifier les données HTTP pour rediriger une demande vers une nouvelle page d'accueil, un nouveau serveur ou un serveur sélectionné en fonction de l'adresse de la demande entrante, ou vous pouvez modifier les données pour masquer les informations du serveur dans une réponse à des fins de sécurité. La fonction URL Transformer identifie les URL dans les transactions HTTP et les fichiers texte afin de déterminer si une URL doit être transformée.
Pare-feu d'application	Classic et Advanced	Identifier les caractéristiques du trafic et des données qui doivent ou non être admis via le pare-feu.
Citrix Gateway, fonction d'accès sans client	Advanced	Pour définir des règles de réécriture pour l'accès Web général à l'aide de Citrix Gateway.

Nom de la fonctionnalité	Type de stratégie	Utilisation des stratégies dans la fonctionnalité
Citrix Gateway	Classique	Pour déterminer comment Citrix Gateway effectue l'authentification, l'autorisation, l'audit et d'autres fonctions.

À propos des actions et des profils

Les stratégies n'agissent pas elles-mêmes sur les données. Les stratégies fournissent une logique en lecture seule pour évaluer le trafic. Pour permettre à une fonctionnalité d'effectuer une opération basée sur une évaluation de stratégie, vous configurez des actions ou des profils et vous les associez à des stratégies.

Remarque : Les actions et les profils sont spécifiques à des fonctionnalités particulières. Pour plus d'informations sur l'affectation d'actions et de profils aux fonctionnalités, consultez la documentation relative aux fonctionnalités individuelles.

À propos des actions

Les actions sont des étapes prises par Citrix ADC, en fonction de l'évaluation de l'expression dans la stratégie. Par exemple, si une expression d'une stratégie correspond à une adresse IP source particulière dans une demande, l'action associée à cette stratégie détermine si la connexion est autorisée.

Les types d'actions que Citrix ADC peut effectuer sont spécifiques aux fonctionnalités. Par exemple, dans Réécrire, les actions peuvent remplacer le texte d'une demande, modifier l'URL de destination d'une demande, etc. Dans Integrated Caching, les actions déterminent si les réponses HTTP sont diffusées à partir du cache ou d'un serveur d'origine.

Dans certaines fonctionnalités de Citrix ADC, les actions sont prédéfinies et dans d'autres, elles sont configurables. Dans certains cas (par exemple, Réécrire), vous configurez les actions à l'aide des mêmes types d'expressions que ceux utilisés pour configurer la règle de stratégie associée.

À propos des profils

Certaines fonctionnalités de Citrix ADC vous permettent d'associer des profils, ou des actions et des profils, à une stratégie. Un profil est un ensemble de paramètres qui permettent à la fonctionnalité d'exécuter une fonction complexe. Par exemple, dans le pare-feu d'application, un profil de données XML peut effectuer plusieurs opérations de filtrage, telles que l'examen des données à la recherche d'une syntaxe XML illégale ou d'une preuve d'injection SQL.

Utilisation d'actions et de profils dans des fonctionnalités particulières

Le tableau suivant récapitule l'utilisation des actions et des profils dans différentes fonctionnalités de Citrix ADC. Le tableau n'est pas exhaustif. Pour plus d'informations sur les utilisations spécifiques des actions et des profils pour une fonctionnalité, consultez la documentation de cette fonctionnalité.

Fonctionnalité	Utilisation d'une action	Utilisation d'un profil
Pare-feu d'application	Synonyme de profil	Toutes les fonctionnalités du pare-feu d'application utilisent des profils pour définir des comportements complexes, y compris l'apprentissage basé sur des modèles. Vous ajoutez ces profils aux stratégies.
Citrix Gateway	Les fonctionnalités suivantes de Citrix Gateway utilisent des actions : Pré-authentification. Utilise les actions Autoriser et Refuser. Vous ajoutez ces actions à un profil., Autorisation. Utilise les actions Autoriser et Refuser. Vous ajoutez ces actions à une stratégie. Compression TCP. Utilise diverses actions. Vous ajoutez ces actions à une stratégie.	Les fonctionnalités suivantes utilisent un profil : pré-authentification, session, trafic et accès sans client. Après avoir configuré les profils, vous les ajoutez aux stratégies.
Réécrire	Vous configurez les actions de réécriture d'URL et vous les ajoutez à une stratégie.	Non utilisé.
Mise en cache intégrée	Vous configurez les actions de mise en cache et d'invalidation au sein d'une stratégie	Non utilisé.

Fonctionnalité	Utilisation d'une action	Utilisation d'un profil
AAA - Gestion du trafic	Vous sélectionnez un type d'authentification, définissez une action d'autorisation sur ALLOW ou DENY, ou définissez l'audit sur SYSLOG ou NSLOG.	Vous pouvez configurer des profils de session avec un délai d'expiration et une action d'autorisation par défaut.
Caractéristiques de protection	Vous configurez des actions au sein des stratégies pour les fonctions suivantes : Filtre, Compression, Répondeur et SureConnect.	Non utilisé.
SSL	Vous configurez des actions dans les stratégies SSL	Non utilisé.
Système	L'action est implicite. Pour la fonction Authentification, elle est soit Autoriser, soit Refuser. Pour l'audit, l'audit est activé ou Audit désactivé.	Non utilisé.
DNS	L'action est implicite. Il s'agit soit de Drop Packets, soit de l'emplacement d'un serveur DNS.	Non utilisé.
Déchargement SSL	L'action est implicite. Il est basé sur une stratégie que vous associez à un serveur virtuel SSL ou à un service.	Non utilisé.
Compression SSL	Déterminez le type de compression à appliquer aux données	Non utilisé.
Commutation de contenu	L'action est implicite. Si une demande correspond à la stratégie, elle est dirigée vers le serveur virtuel associé à la stratégie.	Non utilisé.

Fonctionnalité	Utilisation d'une action	Utilisation d'un profil
Redirection de cache	L'action est implicite. Si une demande correspond à la stratégie, elle est dirigée vers le serveur d'origine.	Non utilisé.

À propos des liaisons de stratégie

Une stratégie est associée ou liée à une entité qui permet d'appeler la stratégie. Par exemple, vous pouvez lier une stratégie à une évaluation au moment de la demande qui s'applique à tous les serveurs virtuels. Un ensemble de stratégies liées à un point de liaison particulier constitue une banque de stratégies.

Vous trouverez ci-dessous un aperçu des différents types de points de liaison pour une stratégie :

- Temps de demande global. Une stratégie peut être disponible pour tous les composants d'une fonctionnalité au moment de la demande.
- Temps de réponse global. Une stratégie peut être disponible pour tous les composants d'une fonctionnalité au moment de la réponse.
- Heure de la demande, spécifique au serveur virtuel.

Une stratégie peut être liée au traitement au moment de la demande pour un serveur virtuel particulier. Par exemple, vous pouvez lier une stratégie de temps de demande à un serveur virtuel de redirection de cache pour vous assurer que des demandes particulières sont transférées vers un serveur virtuel d'équilibrage de charge pour le cache, et que les autres demandes sont envoyées à un serveur virtuel d'équilibrage de charge pour l'origine.

- Temps de réponse, spécifique au serveur virtuel. Une stratégie peut également être liée au traitement du temps de réponse pour un serveur virtuel particulier.
- Étiquette de stratégie définie par l'utilisateur. Pour l'infrastructure de stratégies avancées (PI), vous pouvez configurer des groupes de stratégies personnalisés (banques de stratégies) en définissant une étiquette de stratégie et en collectant un ensemble de stratégies associées sous l'étiquette de stratégie.
- Autres points de liaison. La disponibilité de points de liaison supplémentaires dépend du type de stratégie avancée et des spécificités de la fonctionnalité Citrix ADC concernée.

Pour plus d'informations sur les liaisons de stratégie avancées, consultez la rubrique Liaison de stratégies qui utilisent la rubrique Stratégies avancées .

À propos de l'ordre d'évaluation des stratégies

Les groupes de stratégies et les stratégies d'un groupe sont évalués dans un ordre particulier, en fonction des éléments suivants :

- Point de liaison de la stratégie, par exemple, si la stratégie est liée au traitement du temps de demande pour un serveur virtuel ou au traitement du temps de réponse global. Par exemple, au moment de la demande, Citrix ADC évalue toutes les stratégies de temps de demande avant d'évaluer les stratégies spécifiques au serveur virtuel.
- Le niveau de priorité de la stratégie. Pour chaque point du processus d'évaluation, un niveau de priorité attribué à une stratégie détermine l'ordre d'évaluation par rapport aux autres stratégies qui partagent le même point de liaison. Par exemple, lorsque Citrix ADC évalue une banque de stratégies spécifiques au serveur virtuel au moment de la demande, il commence par la stratégie affectée à la valeur de priorité la plus faible. Dans les stratégies, les niveaux de priorité doivent être uniques sur tous les points de liaison.

Pour les stratégies avancées, Citrix ADC sélectionne un regroupement ou une banque de stratégies à un moment particulier du traitement global. Voici l'ordre d'évaluation des groupements de base, ou banques, des stratégies avancées :

1. Request-time global override
2. Heure de la demande, spécifique au serveur virtuel (un point de liaison par serveur virtuel)
3. Défaut global au moment de la demande
4. Response-time global override
5. Temps de réponse spécifique au serveur virtuel
6. Response-time global default

Toutefois, dans toutes les banques de politiques précédentes, l'ordre d'évaluation est plus souple que dans les politiques. Dans une banque de stratégies, vous pouvez pointer vers la prochaine stratégie à évaluer quel que soit le niveau de priorité, et vous pouvez appeler des banques de stratégies qui appartiennent à d'autres points de liaison et banques de stratégies définies par l'utilisateur.

Order of evaluation based on traffic flow

Au fur et à mesure que le trafic passe par Citrix ADC et est traité par diverses fonctionnalités, chaque fonctionnalité effectue une évaluation des stratégies. Chaque fois qu'une stratégie correspond au trafic, Citrix ADC stocke l'action et continue le traitement jusqu'à ce que les données soient sur le point de quitter Citrix ADC. À ce stade, Citrix ADC applique généralement toutes les actions correspondantes. La mise en cache intégrée, qui n'applique qu'une action finale Cache ou NoCache, est une exception.

Certaines politiques influent sur le résultat d'autres politiques. Voici des exemples :

- Si une réponse est fournie à partir du cache intégré, d'autres fonctionnalités de Citrix ADC ne traitent pas la réponse ou la demande qui l'a initiée.
- Si la fonctionnalité de filtrage du contenu empêche la diffusion d'une réponse, aucune fonctionnalité ultérieure n'évalue la réponse.

Si le pare-feu d'application rejette une demande entrante, aucune autre fonctionnalité ne peut la traiter.

Expressions de stratégie avancées

October 5, 2021

L'une des composantes les plus fondamentales d'une politique est sa règle. Une règle de stratégie est une expression logique qui permet à la stratégie d'analyser le trafic. La plupart des fonctionnalités de la stratégie sont dérivées de son expression.

Une expression met en correspondance les caractéristiques du trafic ou d'autres données avec un ou plusieurs paramètres et valeurs. Par exemple, une expression peut permettre à Citrix ADC d'effectuer les opérations suivantes :

- Déterminez si une demande contient un certificat.
- Déterminez l'adresse IP d'un client qui a envoyé une demande TCP.
- Identifiez les données contenues dans une requête HTTP (par exemple, une feuille de calcul populaire ou une application de traitement de texte).
- Calculez la longueur d'une requête HTTP.

À propos des expressions de stratégie avancées

Toute fonctionnalité qui utilise une infrastructure de stratégie avancée utilise également des expressions avancées. Pour plus d'informations sur les fonctionnalités qui utilisent des stratégies avancées, reportez-vous au tableau Citrix ADC Feature, Policy Type and Policy Usage.

Les expressions de stratégie avancées ont d'autres utilisations. Outre la configuration des expressions avancées dans les règles de stratégie, vous configurez les
expressions avancées dans les situations suivantes :

- Mise en cache intégrée :

  Vous utilisez des expressions de stratégie avancées pour configurer un sélecteur pour un groupe de contenus dans le cache intégré.

- Équilibrage de charge :

Vous utilisez des expressions de stratégie avancées pour configurer l'extraction de jetons pour un serveur virtuel d'équilibrage de charge qui utilise la méthode TOKEN pour l'équilibrage de charge.

- Réécriture :

  Vous utilisez des expressions de stratégie avancées pour configurer les actions de réécriture.

- Stratégies basées sur les taux :

  Vous utilisez des expressions de stratégie avancées pour configurer des sélecteurs de limite lorsque vous configurez une stratégie pour contrôler le taux de trafic vers différents serveurs.

Voici quelques exemples simples d'expressions de stratégie avancées :

- Une URL de requête HTTP ne contient pas plus de 500 caractères.

```
http.req.url.length \<= 500
```

- Une requête HTTP contient un cookie de moins de 500 caractères.

```
http.req.cookie.length \< 500
```

- Une URL de requête HTTP contient une chaîne de texte particulière.

```
http.req.url.contains(".html")
```

Conversion des expressions de stratégie à l'aide de l'outil NSPEPI

October 5, 2021

> **Remarque :**
>
> Vous pouvez télécharger l'outil de vérification NSPEPI et de pré-configuration depuis le GitHub public. Pour plus d'informations, consultez la page NEPEPI de GitHubet la page de préconfiguration de GitHub pour obtenir des instructions détaillées sur le téléchargement des outils. Nous recommandons aux clients d'utiliser les outils disponibles dans GitHub pour obtenir la version la plus complète et la plus récente.

Les fonctionnalités et fonctionnalités classiques basées sur des règles sont obsolètes à partir de NetScaler 12.0 build 56.20. Comme alternative, Citrix vous recommande d'utiliser l'infrastructure de stratégie avancée. Dans le cadre de cet effort, lorsque vous effectuez une mise à niveau vers Citrix ADC 12.1 version 56.20 ou ultérieure, vous devez remplacer les fonctionnalités et fonctionnalités basées sur des stratégies classiques par les fonctionnalités et fonctionnalités non obsolètes correspondantes. Vous devez également convertir les stratégies et expressions classiques en stratégies et expressions avancées. De plus, toutes les nouvelles fonctionnalités de Citrix ADC prennent uniquement en charge l'infrastructure de stratégie avancée.

L' `nspepi` outil peut effectuer les opérations suivantes :

1. Convertissez les expressions de stratégie classiques en expressions de stratégie avancées.
2. Convertissez certaines stratégies classiques et leurs liaisons d'entités en stratégies et liaisons avancées.
3. Convertissez quelques autres entités obsolètes en fonctionnalités non dépréciées correspondantes.
4. Convertissez les commandes de filtre classiques en commandes de filtrage avancées.

> **Remarque :**
>
> Une fois que l' `nspepi` outil a réussi à convertir le fichier de configuration ns.conf, il affiche le fichier converti sous la forme d'un nouveau fichier avec le préfixe « new_ ». Si le fichier de configuration converti contient des erreurs ou des avertissements, vous devez les corriger manuellement dans le cadre du processus de conversion. Une fois converti, vous devez tester le fichier dans l'environnement de test, puis l'utiliser pour remplacer le fichier de configuration ns.conf actuel. Après le test, vous devez redémarrer la solution matérielle-logicielle pour le fichier de configuration ns.conf nouvellement converti ou corrigé.

Les fonctionnalités qui ne prennent en charge que les stratégies ou expressions classiques sont obsolètes et peuvent être remplacées par les fonctionnalités non obsolètes correspondantes.

> **Remarque :**
>
> Les informations relatives à l'ancienne version de l' `nspepi` outil sont disponibles au format PDF. Pour plus d'informations, consultez la section Conversion de stratégie classique à l'aide de l'outil nspepi avant la version 12.1-51.16 PDF.

Avertissements de conversion et fichiers d'erreur

Avant d'utiliser l'outil pour votre conversion, il y a quelques avertissements à garder à l'esprit :

1. Tous les avertissements et erreurs sont affichés sur la console. Un fichier d'avertissement est créé dans lequel les fichiers de configuration sont stockés.
2. Le fichier d'avertissement et d'erreur porte le même nom que le fichier d'entrée, mais avec le préfixe « warn_ » ajouté au nom du fichier. Lors de la conversion d'expression (avec l'option -e), les avertissements apparaissent dans le répertoire courant sous le nom « warn_expr ».

> **Remarque :**
>
> Ce fichier est au format de fichier journal standard, avec horodatage et niveau de journalisation. Les instances précédentes du fichier sont conservées avec des suffixes tels que ".1", ".2", etc., car l'outil est exécuté plusieurs fois. Au plus 10 instances seront conservées.

Format de fichier converti

Lors de la conversion d'un fichier de configuration (en utilisant « -f »), le fichier converti est placé dans le même répertoire que celui où existe le fichier de configuration d'entrée portant le même nom mais avec le préfixe « new_ ».

Commandes ou fonctionnalités gérées par l'outil de conversion nspepi

Voici les commandes gérées pendant le processus de conversion automatique.

- Les stratégies classiques suivantes et leurs expressions sont converties en stratégies et expressions avancées. La conversion inclut les liaisons d'entités et les liaisons globales.

1. add appfw policy
2. add cmp policy
3. add cr policy
4. add cs policy
5. add tm sessionPolicy
6. add filter action
7. add filter policy
8. liaison de stratégie de filtre à l'équilibrage de charge, à la commutation de contenu, à la redirection du cache et à la stratégie globale.

> **Remarque :**
>
> Toutefois, pour « add tm SessionPolicy », vous ne pouvez pas vous lier au remplacement global dans les stratégies avancées.

- Le paramètre de règle configuré dans « ajouter un serveur virtuel lb » est converti de l'expression classique à l'expression avancée.
- Le paramètre SPDY configuré dans la commande « add ns HttpProfile » ou « set ns HttpProfile » est remplacé par « -http2 ENABLED ».
- Expressions nommées (commandes « ajouter une expression de stratégie »). Chaque expression de stratégie nommée Classic est convertie en son expression nommée Advanced correspondante avec « nspepi_adv_ » défini comme préfixe. En outre, l'utilisation des expressions nommées pour les expressions classiques converties est remplacée par les expressions nommées avancées correspondantes. De plus, chaque expression nommée comporte deux expressions nommées, l'une étant classique et l'autre avancée (comme illustré ci-dessous).
- La conversion Tunnel TrafficPolicy est prise en charge.
- Gestion des liaisons de stratégie classiques intégrées dans CMP, CR et Tunnel.
- La fonction Patclass est convertie en fonction Pat set.
- Le paramètre « -pattern » de la commande « add rewrite action » est converti pour utiliser le paramètre « -search ».

- SYS.EVAL_CLASSIC_EXPR est converti en expression avancée non obsolète équivalente. Ces expressions sont visibles dans toutes les commandes où les expressions avancées sont autorisées.
- Les préfixes Q et S des expressions avancées sont convertis en expressions avancées non obsolètes équivalentes. Ces expressions sont visibles dans toutes les commandes où les expressions avancées sont autorisées.

Par exemple :

```
add policy expression classic_expr ns_true
Converts to:
add policy expression classic_expr ns_true
add policy expression nspepi_adv_classic_expr TRUE
<!--NeedCopy-->
```

- Le paramètre PolicyType configuré dans la commande « set cmp parameter » est supprimé. Par défaut, le type de stratégie est « Avancé ».

Convertir les commandes de filtre classiques en commandes de filtrage avancées

L' outil `nspepi` peut convertir des commandes basées sur des actions de filtre classiques telles que l'ajout, la liaison, etc. en commandes de filtrage avancées.

Toutefois, l'outil nepepi ne prend pas en charge les commandes de filtre suivantes.

1. add filter action <`action Name`> FORWARD <`service name`>
2. add filter action <`action name`> ADD prebody
3. add filter action <`action name`> ADD postbody

> **Remarque :**
>
> 1. S'il existe des fonctionnalités de réécriture ou de répondeur dans ns.conf et que leurs stratégies sont liées globalement à l'expression `GOTO` en tant que `END` ou `USER_INVOCATION_RESULT` et que le type de liaison est `REQ_X` ou `RES_X` alors l'outil convertit partiellement les commandes de filtre de liaison et les commente. Un avertissement s'affiche pour mettre en œuvre un effort manuel.
> 2. S'il existe des fonctionnalités de réécriture ou de répondeur existantes et que leurs stratégies sont liées à des serveurs virtuels (par exemple, équilibrage de charge, changement de contenu ou redirection de cache) de type HTTPS avec `GOTO` - `END` ou `USER_INVOCATION_RESULT`, l'outil convertit partiellement les commandes de filtre de liaison, puis les commente. Un avertissement s'affiche pour mettre en œuvre un effort manuel.

Exemple

Voici un exemple d'entrée :

```
add lb vserver v1 http 1.1.1.1 80 -persistenceType NONE -cltTimeout
    9000
add cs vserver csv1 HTTP 1.1.1.2 80 -cltTimeout 180 -persistenceType
    NONE
add cr vserver crv1 HTTP 1.1.1.3 80 -cacheType FORWARD
add service svc1 1.1.1.4 http 80
add filter action fact_add add 'header:value'
add filter action fact_variable add 'H1:%%HTTP.TRANSID%%'
add filter action fact_prebody add prebody
add filter action fact_error_act1 ERRORCODE 200 "<HTML>Good URL</HTML>"
add filter action fact_forward_act1 FORWARD svc1
add filter policy fpol_add_res -rule ns_true -resAction fact_add
add filter policy fpol_error_res -rule ns_true -resAction
    fact_error_act1
add filter policy fpol_error_req -rule ns_true -reqAction
    fact_error_act1
add filter policy fpol_add_req -rule ns_true -reqAction fact_add
add filter policy fpol_variable_req -rule ns_true -reqAction
    fact_variable
add filter policy fpol_variable_res -rule ns_true -resAction
    fact_variable
add filter policy fpol_prebody_req -rule ns_true -reqAction
    fact_prebody
add filter policy fpol_prebody_res -rule ns_true -resAction
    fact_prebody
add filter policy fpol_forward_req -rule ns_true -reqAction
    fact_forward_act1
bind lb vserver v1 -policyName fpol_add_res
bind lb vserver v1 -policyName fpol_add_req
bind lb vserver v1 -policyName fpol_error_res
bind lb vserver v1 -policyName fpol_error_req
bind lb vserver v1 -policyName fpol_variable_res
bind lb vserver v1 -policyName fpol_variable_req
bind lb vserver v1 -policyName fpol_forward_req
bind cs vserver csv1 -policyName fpol_add_req
bind cs vserver csv1 -policyName fpol_add_res
bind cs vserver csv1 -policyName fpol_error_res
bind cs vserver csv1 -policyName fpol_error_req
bind cr vserver crv1 -policyName fpol_add_req
bind cr vserver crv1 -policyName fpol_add_res
bind cr vserver crv1 -policyName fpol_error_res
```



```
bind cr vserver crv1 -policyName fpol_error_req
bind cr vserver crv1 -policyName fpol_forward_req
bind filter global fpol_add_req
bind filter global fpol_add_res
bind filter global fpol_error_req
bind filter global fpol_error_res
bind filter global fpol_variable_req
bind filter global fpol_variable_res
bind filter global fpol_variable_res -state DISABLED
bind filter global fpol_prebody_req
bind filter global fpol_forward_req
After conversion, warning/error messages will be displayed for manual
    effort.
Warning files:
cat warn_<input file name>:
2019-11-07 17:13:34,724: ERROR - Conversion of [add filter action
    fact_prebody add prebody] not supported in this tool.
2019-11-07 17:13:34,739: ERROR - Conversion of [add filter action
    fact_forward_act1 FORWARD svc1] not supported in this tool.
2019-11-07 17:13:38,042: ERROR - Conversion of [add filter policy
    fpol_prebody_req -rule ns_true -reqAction fact_prebody] not
    supported in this tool.
2019-11-07 17:13:38,497: ERROR - Conversion of [add filter policy
    fpol_prebody_res -rule ns_true -resAction fact_prebody] not
    supported in this tool.
2019-11-07 17:13:39,035: ERROR - Conversion of [add filter policy
    fpol_forward_req -rule ns_true -reqAction fact_forward_act1] not
    supported in this tool.
2019-11-07 17:13:39,060: WARNING - Following bind command is commented
    out because state is disabled. Advanced expressions only have a
    fixed ordering of the types of bindings without interleaving, except
     that global bindings are allowed before all other bindings and
    after all bindings. If you have global bindings in the middle of non
    -global bindings or any other interleaving then you will need to
    reorder all your bindings for that feature and direction. Refer to
    nspepi documentation. If command is required please take a backup
    because comments will not be saved in ns.conf after triggering 'save
     ns config': bind filter global fpol_variable_res -state DISABLED


<!--NeedCopy-->
```

Voici un exemple de sortie. Toutes les commandes converties sont commentées.

```
cat new_<input file name>
```



```
add rewrite action fact_add insert_http_header header ""value""
add filter action fact_prebody add prebody
add filter action fact_forward_act1 FORWARD svc1
add filter policy fpol_prebody_req -rule ns_true -reqAction
    fact_prebody
add filter policy fpol_prebody_res -rule ns_true -resAction
    fact_prebody
add filter policy fpol_forward_req -rule ns_true -reqAction
    fact_forward_act1
bind lb vserver v1 -policyName fpol_forward_req
bind cr vserver crv1 -policyName fpol_forward_req
#bind filter global fpol_variable_res -state DISABLED
bind filter global fpol_prebody_req
bind filter global fpol_forward_req
add rewrite action nspepi_adv_fact_variable insert_http_header H1 HTTP.
    RES.TXID
add rewrite action fact_variable insert_http_header H1 HTTP.REQ.TXID
add responder action fact_error_act1 respondwith "HTTP.REQ.VERSION.
    APPEND(" 200 OK\r
nConnection: close\r
nContent-Length: 21\r\n\r
n<HTML>Good URL</HTML>")"
add rewrite action nspepi_adv_fact_error_act1 replace_http_res "HTTP.
    REQ.VERSION.APPEND(" 200 OK\r
nConnection: close\r
nContent-Length: 21\r\n\r
n<HTML>Good URL</HTML>")"
add rewrite policy fpol_add_res TRUE fact_add
add rewrite policy fpol_error_res TRUE nspepi_adv_fact_error_act1
add responder policy fpol_error_req TRUE fact_error_act1
add rewrite policy fpol_add_req TRUE fact_add
add rewrite policy fpol_variable_req TRUE fact_variable
add rewrite policy fpol_variable_res TRUE nspepi_adv_fact_variable
set cmp parameter -policyType ADVANCED
bind rewrite global fpol_add_req 100 NEXT -type REQ_DEFAULT
bind rewrite global fpol_variable_req 200 NEXT -type REQ_DEFAULT
bind rewrite global fpol_add_res 100 NEXT -type RES_DEFAULT
bind rewrite global fpol_error_res 200 NEXT -type RES_DEFAULT
bind rewrite global fpol_variable_res 300 NEXT -type RES_DEFAULT
bind responder global fpol_error_req 100 END -type REQ_DEFAULT
bind lb vserver v1 -policyName fpol_add_res -type RESPONSE -priority
    100 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_error_res -type RESPONSE -priority
    200 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_variable_res -type RESPONSE -
```



```
    priority 300 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_add_req -type REQUEST -priority 100
     -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_variable_req -type REQUEST -
    priority 200 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_error_req -type REQUEST -priority
    100 -gotoPriorityExpression END
bind cs vserver csv1 -policyName fpol_add_req -type REQUEST -priority
    100 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_add_res -type RESPONSE -priority
    100 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_error_res -type RESPONSE -
    priority 200 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_error_req -type REQUEST -priority
     100 -gotoPriorityExpression END
bind cr vserver crv1 -policyName fpol_add_req -type REQUEST -priority
    100 -gotoPriorityExpression NEXT
bind cr vserver crv1 -policyName fpol_add_res -type RESPONSE -priority
    100 -gotoPriorityExpression NEXT
bind cr vserver crv1 -policyName fpol_error_res -type RESPONSE -
    priority 200 -gotoPriorityExpression NEXT
bind cr vserver crv1 -policyName fpol_error_req -type REQUEST -priority
     100 -gotoPriorityExpression END

<!--NeedCopy-->
```

Convertir les commandes de filtre classiques en commandes de fonctionnalités avancées si les liaisons de stratégie de réécriture ou de répondeur existantes ont atteint l'expression END ou USE_INNVOCATION

Dans cette conversion, si une stratégie de réécriture est liée à un ou plusieurs serveurs virtuels et si le serveur possède END ou USE_INVOCATION_RESULT, l'outil commente les commandes.

Exemple

Voici un exemple de commande d'entrée :

```
COPY
add filter policy fpol1 -rule ns_true -resAction reset
add filter policy fpol2 -rule ns_true -reqAction reset
add rewrite policy pol1 true NOREWRITE
add rewrite policylabel pl http_res
bind rewrite policylabel pl pol1 1
```



```
bind rewrite global NOPOLICY 1 USE_INVOCATION_RESULT -type RES_DEFAULT
    -invoke policylabel pl
add responder policy pol2 true NOOP
add responder policylabel pl -policylabeltype HTTP
bind responder policylabel pl pol2 1
bind responder global NOPOLICY 1 USE_INVOCATION_RESULT -type
    REQ_DEFAULT -invoke policylabel pl
bind lb vserver v1_tcp -policyName pol1 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind cs vserver csv1_tcp -policyName pol1 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind lb vserver v1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cs vserver csv1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cr vserver crv1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind lb vserver v1_http -policyName fpol1
bind cs vserver csv1_http -policyName fpol1
bind lb vserver v2_http -policyName fpol2
bind cs vserver csv2_http -policyName fpol2
bind cr vserver crv2_http -policyName fpol2
bind filter global fpol1 -priority 100
bind filter global fpol2 -priority 100
<!--NeedCopy-->
```

Voici un exemple de commande de sortie :

```
COPY
add rewrite policy pol1 true NOREWRITE
add rewrite policylabel pl http_res
bind rewrite policylabel pl pol1 1
add responder policy pol2 true NOOP
add responder policylabel pl -policylabeltype HTTP
bind responder policylabel pl pol2 1
add rewrite policy fpol1 TRUE RESET
add responder policy fpol2 TRUE RESET
#bind lb vserver v1_http -policyName fpol1 -type RESPONSE
#bind cs vserver csv1_http -policyName fpol1 -type RESPONSE
#bind rewrite global fpol1 100 -type RES_DEFAULT
#bind lb vserver v2_http -policyName fpol2 -type REQUEST
#bind cs vserver csv2_http -policyName fpol2 -type REQUEST
#bind cr vserver crv2_http -policyName fpol2 -type REQUEST
#bind responder global fpol2 100 -type REQ_DEFAULT
bind rewrite global NOPOLICY 1 USE_INVOCATION_RESULT -type RES_DEFAULT
```



```
    -invoke policylabel pl
18 bind responder global NOPOLICY 1 USE_INVOCATION_RESULT -type
    REQ_DEFAULT -invoke policylabel pl
19 bind lb vserver v1_tcp -policyName pol1 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
20 bind lb vserver v1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
21 bind cs vserver csv1_tcp -policyName pol1 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
22 bind cs vserver csv1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
23 bind cr vserver crv1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST-
24
25 <!--NeedCopy-->
```

Commandes ou fonctionnalités non gérées par l'outil de conversion nspepi

Voici quelques commandes qui ne sont pas gérées dans le cadre du processus de conversion automatique.

- Certaines liaisons ne peuvent pas être converties s'il existe un certain entrelacement des priorités entre les points de liaison globaux et non globaux, entre les utilisateurs et les groupes, ainsi qu'entre les liaisons vers différentes entités. La configuration affectée est commentée et une erreur est générée. Ces configurations doivent être converties manuellement.
- Les stratégies Classic et Advanced peuvent être liées à cmp global. Dans de nombreux cas, la fonctionnalité change une fois que les stratégies classiques sont converties en stratégies avancées. Nous avons converti des commandes qui peuvent être résolues en commentant certaines stratégies. Certaines commandes ne peuvent cependant pas être converties. Dans ce cas, une erreur se produit et la conversion doit être effectuée manuellement.
- Les expressions nommées intégrées classiques ne sont pas toutes converties en expressions nommées Advanced équivalentes.
- Les expressions de sécurité client ne sont pas gérées.
- L'option « -precedence » pour les serveurs virtuels de commutation de contenu et de redirection de cache n'est pas gérée.
- SureConnect (SC)
- Priority Queuing (PQ)
- HTTP Denial of Service (HDOS)
- HTML Injection
- Authentication
- Authorization

- VPN
- Syslog
- Nslog
- Les expressions classiques basées sur des fichiers ne sont pas gérées.

> **Remarque :**
>
> Pour certaines fonctionnalités telles que PatClass/Filter, la syntaxe de la commande est modifiée. S'il existe des stratégies cmd, les stratégies cmd peuvent devoir être modifiées en fonction des besoins du client.

Problèmes connus

Les erreurs suivantes peuvent être produites par l'outil `nspepi`:

- En cas de problème lors de la conversion d'une expression.
- Si une expression de stratégie nommée utilise le paramètre -ClientSecurityMessage, car ce paramètre n'est pas pris en charge dans l'expression de stratégie avancée.

> **Remarque :**
>
> Toutes les liaisons de stratégie classiques avec l'option -state désactivée sont commentées. L'option -state n'est pas disponible pour les liaisons de stratégie avancées.

Exécution de l'outil nspepi

Voici un exemple de ligne de commande permettant d'exécuter l'outil `nspepi`. Cet outil est exécuté à partir de la ligne de commande du shell (vous devez taper la commande « shell » dans le « CLI » de NetScaler pour y accéder). « -f » ou « -e » doivent être spécifiés pour effectuer une conversion. L'utilisation de « -d » est destinée au personnel Citrix pour l'analyse à des fins de support.

```
1  usage: nspepi [-h] (-e <classic policy expression> | -f <path to ns
       config file>)[-d] [-v] [-V
2
3  Convert classic policy expressions to advanced policy expressions and
       deprecated commands to non-deprecated
4  commands.
5
6  optional arguments:
7  -h, --help show this help message and exit
8  -e <classic policy expression>, --expression <classic policy expression
       >
9  convert classic policy expression to advanced policy
10 expression (maximum length of 8191 allowed)
11 -f <path to ns config file>, --infile <path to ns config file>
```



```
convert netscaler config file
-d, --debug log debug output
-v, --verbose show verbose output
-V, --version show program's version number and exit
<!--NeedCopy-->
```

Exemples d'utilisation :

1. `nspepi -e "req.tcp.destport == 80"`
2. `nspepi -f ns.conf`

Voici quelques exemples d'exécution de l'outil `nspepi` à l'aide de l'interface de ligne de commande :

Exemple de sortie pour le paramètre —e :

```
root@ns# nspepi -e "req.http.header foo == "bar""
"HTTP.REQ.HEADER("foo").EQ("bar")"
<!--NeedCopy-->
```

Exemple de sortie pour le paramètre -f :

```
root@ns# cat sample.conf
add c\*\*Input\*\*r vserver cr_vs HTTP -cacheType TRANSPARENT -
   cltTimeout 180 -originUSIP OFF
add cr policy cr_pol1 -rule ns_true
bind cr vserver cr_vs -policyName cr_pol1
<!--NeedCopy-->
```

Exécution de nspepi avec le paramètre -f :

```
nspepi -f sample.conf
<!--NeedCopy-->
```

La configuration convertie est disponible dans un nouveau fichier `new_sample.conf`.
Recherchez dans le fichier `warn_sample.conf` les avertissements ou erreurs qui ont pu être générés.

Exemple de sortie du paramètre -f avec le paramètre -v

```
nspepi -f sample.conf -v
INFO - add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180
    -originUSIP OFF
INFO - add cr policy cr_pol1 -rule TRUE -action ORIGIN
INFO - bind cr vserver cr_vs -policyName cr_pol1 -priority 100 -
   gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```


La configuration convertie est disponible dans un nouveau fichier `new_sample.conf`.
Recherchez dans le fichier `warn_sample.conf` les avertissements ou erreurs qui ont pu être générés.

Fichier de configuration converti :

```
root@ns# cat new_sample.conf
add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180 -
    originUSIP OFF
add cr policy cr_pol1 -rule TRUE -action ORIGIN
set cmp parameter -policyType ADVANCED
bind cr vserver cr_vs -policyName cr_pol1 -priority 100 -
    gotoPriorityExpression END -type REQUEST

<!--NeedCopy-->
```

Exemple de sortie d'un exemple de configuration sans erreur ni avertissement :

```
nspepi -f sample_2.conf
<!--NeedCopy-->
```

La configuration convertie est disponible dans un nouveau fichier `new_sample_2.conf`.
Recherchez dans le fichier `warn_sample_2.conf` les avertissements ou erreurs qui ont pu être générés.

Exemple de sortie d'un exemple de configuration avec des avertissements :

```
root@ns# cat sample_2.conf
add policy expression security_expr "req.tcp.destport == 80" -
    clientSecurityMessage "Not allowed"
set cmp parameter -policyType CLASSIC
add cmp policy cmp_pol1 -rule ns_true -resAction COMPRESS
add cmp policy cmp_pol2 -rule ns_true -resAction COMPRESS
add cmp policy cmp_pol3 -rule TRUE -resAction COMPRESS
bind cmp global cmp_pol1
bind cmp global cmp_pol2 -state DISABLED
bind cmp global cmp_pol3 -priority 1 -gotoPriorityExpression END -type
    RES_DEFAULT
bind lb vserver lb_vs -policyName cmp_pol2
root@ns#
<!--NeedCopy-->
```

Exemple d'exécution de nspepi avec le paramètre -f :

```
root@ns# nspepi -f sample_2.conf
ERROR - Error in converting expression security_expr : conversion of
    clientSecurityMessage based expression is not supported.
```



```
3 WARNING - Following bind command is commented out because state is
    disabled. Advanced expressions only have a fixed ordering of the
    types of bindings without interleaving, except that global bindings
    are allowed before all other bindings and after all bindings. If you
     have global bindings in the middle of non-global bindings or any
    other interleaving then you will need to reorder all your bindings
    for that feature and direction. Refer to nspepi documentation. If
    command is required please take a backup because comments will not
    be saved in ns.conf after triggering 'save ns config': bind cmp
    global cmp_pol2 -state DISABLED
4 Warning - Bindings of advanced CMP policies to cmp global are commented
     out, because initial global cmp parameter is classic but advanced
    policies are bound. Now global cmp parameter policy type is set to
    advanced. If commands are required please take a backup because
    comments will not be saved in ns.conf after triggering 'save ns
    config'. Advanced expressions only have a fixed ordering of the
    types of bindings without interleaving, except that global bindings
    are allowed before all other bindings and after all bindings. If you
     have global bindings in the middle of non-global bindings or any
    other interleaving then you will need to reorder all your bindings
    for that feature and direction. Refer to nspepi documentation.
5 root@ns#
6 <!--NeedCopy-->
```

Fichier converti :

```
1  root@ns# cat new_sample_2.conf
2  add policy expression security_expr "req.tcp.destport == 80" -
       clientSecurityMessage "Not allowed"
3  set cmp parameter -policyType ADVANCED
4  add cmp policy cmp_pol1 -rule TRUE -resAction COMPRESS
5  add cmp policy cmp_pol2 -rule TRUE -resAction COMPRESS
6  add cmp policy cmp_pol3 -rule TRUE -resAction COMPRESS
7  #bind cmp global cmp_pol2 -state DISABLED
8  #bind cmp global cmp_pol3 -priority 1 -gotoPriorityExpression END -type
       RES_DEFAULT
9  bind cmp global cmp_pol1 -priority 100 -gotoPriorityExpression END -
       type RES_DEFAULT
10 bind lb vserver lb_vs -policyName cmp_pol2 -priority 100 -
       gotoPriorityExpression END -type RESPONSE
11 root@ns#
12 <!--NeedCopy-->
```

Fichier d'avertissement :


```
root@ns# cat warn_sample_2.conf
2019-02-28 06:20:10,590: ERROR - Error in converting expression
    security_expr : conversion of clientSecurityMessage based expression
     is not supported.
2019-02-28 06:20:12,187: WARNING - Following bind command is commented
    out because state is disabled. Advanced expressions only have a
    fixed ordering of the types of bindings without interleaving, except
     that global bindings are allowed before all other bindings and
    after all bindings. If you have global bindings in the middle of non
    -global bindings or any other interleaving then you will need to
    reorder all your bindings for that feature and direction. Refer to
    nspepi documentation. If command is required please take a backup
    because comments will not be saved in ns.conf after triggering 'save
     ns config': bind cmp global cmp_pol2 -state DISABLED
2019-02-28 06:20:12,191: WARNING - Bindings of advanced CMP policies to
     cmp global are commented out, because initial global cmp parameter
    is classic but advanced policies are bound. Now global cmp parameter
     policy type is set to advanced. If commands are required please
    take a backup because comments will not be saved in ns.conf after
    triggering 'save ns config'. Advanced expressions only have a fixed
    ordering of the types of bindings without interleaving, except that
    global bindings are allowed before all other bindings and after all
    bindings. If you have global bindings in the middle of non-global
    bindings or any other interleaving then you will need to reorder all
     your bindings for that feature and direction. Refer to nspepi
    documentation.
root@ns#
<!--NeedCopy-->
```

Priorités liées

Les stratégies avancées n'autorisent pas l'entrelacement arbitraire par priorité entre global et non global et entre différents types de liaison. Si vous vous fiez à un tel entrelacement des priorités de stratégie classique, vous devez ajuster les priorités pour qu'elles soient conformes aux règles de stratégie avancées et pour obtenir le comportement souhaité.
Les priorités des stratégies avancées sont locales à un point de liaison. Un point de liaison est une combinaison unique de protocole, de fonctionnalité, de direction et d'entité (les entités sont des serveurs virtuels spécifiques, des utilisateurs, des groupes, des services et soit un remplacement global, soit un défaut global). Les priorités politiques ne sont pas suivies à travers les points de liaison.

Pour un protocole, une fonctionnalité et une direction donnés, l'ordre d'évaluation des stratégies avancées est indiqué ci-dessous :

- REMPLACEMENT GLOBAL.
- Authentification, autorisation et audit de l'utilisateur (actuel).
- Groupes d'authentification, d'autorisation et d'audit (dont l'utilisateur est membre) par ordre de pondération - l'ordre n'est pas défini si deux groupes ou plus ont le même poids.
- Serveur virtuel LB sur lequel la demande a été reçue ou que Content Switching a sélectionné.
- Serveur virtuel de commutation de contenu, serveur virtuel de redirection de cache sur lequel la demande a été reçue.
- Service sélectionné par l'équilibrage de charge.
- Valeur par défaut globale.

Pour l'évaluation de la stratégie d'autorisation, l'ordre est le suivant :

- Les systèmes sont priorisés.
- Serveur virtuel d'équilibrage de charge sur lequel la demande a été reçue ou sur lequel CS a été sélectionné.
- Serveur virtuel de commutation de contenu sur lequel la demande a été reçue.
- Valeur par défaut du système.

Dans chaque point de liaison, les stratégies sont évaluées par ordre de priorité, du numéro le plus bas au numéro le plus élevé. Les stratégies ne sont évaluées que pour le protocole utilisé et la direction d'où le message a été reçu.

Liaisons de stratégie classiques nécessitant une redéfinition manuelle des priorités

Voici quelques types de liaisons de stratégie classiques qui nécessitent une redéfinition manuelle des priorités pour répondre à vos besoins. Tous ces éléments sont destinés à un trait donné et à la direction.

- Priorités classiques dont le numéro de priorité augmente en sens inverse de la direction des listes de types d'entités ci-dessus. Par exemple, une liaison de serveur virtuel de commutation de contenu inférieure à une liaison de serveur virtuel d'équilibrage de charge.
- Priorités classiques qui entrelacent les groupes d'authentification, d'autorisation et d'audit. Une partie d'un groupe se trouve avant un autre groupe et une autre partie se trouve après une partie de cet autre groupe.
- Priorités classiques qui augmentent en nombre autre que l'ordre de pondération des groupes d'authentification, d'autorisation et d'audit.
- Les priorités mondiales classiques qui sont inférieures à certaines priorités non mondiales et les mêmes priorités mondiales sont supérieures à d'autres priorités non mondiales (en d'autres termes, tout segment de priorités non mondiales, suivi d'une ou de plusieurs priorités mondiales, suivi d'une ou de plusieurs priorités non mondiales).

Outil de vérification de la préconfiguration

October 5, 2021

> **Remarque :**
>
> Vous pouvez télécharger l'outil de vérification NSPEPI et de pré-configuration à partir de GITHUB public. Pour plus d'informations, consultez la page NEPEPI de Github et la page de préconfiguration de Github pour obtenir des instructions détaillées sur le téléchargement des outils. Nous recommandons aux clients d'utiliser les outils disponibles dans GitHub pour obtenir la version la plus complète et la plus récente.

Un outil de pré-validation est disponible dans les versions Citrix ADC 12.1, 13.0 et 13.1 pour vérifier si des fonctionnalités non valides ou supprimées sont toujours utilisées dans une configuration de fonctionnalité. Les outils valident le `nsconfig` fichier s'il contient des commandes ou des paramètres dans une commande qui a été supprimée dans la version Citrix ADC 13.1. Si le résultat de la validation indique l'utilisation de commandes supprimées ou non valides, avant de mettre à niveau votre appliance, vous devez d'abord modifier la configuration en fonction de l'alternative recommandée par Citrix.

L'outil valide également l'utilisation des expressions de stratégie classiques utilisées dans la configuration des fonctionnalités qui ne prend pas en charge les stratégies classiques. Vous pouvez modifier manuellement ou utiliser l' `nspepi` outil.

L'outil valide l'utilisation suivante :

1. Expressions de stratégie classiques dans les fonctionnalités de commutation de contenu, de redirection de cache, d'AppFW, de SSL et de CMP.
2. Fonction de filtrage (également connue sous le nom de filtrage de contenu) : actions, stratégies et liaison
3. SPDY dans le profil HTTP, la connexion sûre (SC), la mise en file d'attente prioritaire (PQ), le déni de service HTTP (DoS) et les fonctionnalités d'injection HTML.
4. Expressions classiques dans les règles de persistance de l'équilibrage de charge.
5. Paramètres « Pattern » et « BypassSafetyCheck » dans les actions de réécriture.
6. « SYS.EVAL_CLASSIC_EXPR » dans les expressions avancées.
7. Entité de configuration « patclass ».
8. « HTTP.REQ.BODY » sans argument dans les expressions avancées.
9. Préfixes Q et S dans les expressions avancées.
10. Paramètre « PolicyType » pour le paramètre cmp.

Exécution de l'outil de pré-revalidation dans UNIX Shell

À l'invite de commandes, tapez :


```
check_invalid_config <config_file>
<!--NeedCopy-->
```

Exemple :

```
root@ns## check_invalid_config/nsconfig/ns.conf
```

Où, le fichier de configuration est le fichier de configuration Citrix ADC. Le fichier doit être issu d'une configuration enregistrée telle que `ns.conf`.

Exemple de sortie avec erreurs de validation

Voici un exemple de sortie du fichier de configuration contenant des erreurs dans Citrix ADC version 13.1 :

```
add policy expression x "sys.eval_classic_expr("ns_true")"
add cmp policy cmp_pol -rule ns_true -resAction GZIP
add cs policy cs_pol_2 -rule ns_true
add cs policy cs_pol_3 -domain www.abc.com
add cs policy cs_pol_4 -url "/abc"
add rewrite action act_1 replace_all "http.req.body(1000)" http.req.url
    -pattern abcd
add rewrite action act_123 replace_all http.req.url ""aaaa"" -pattern
   abcd
add responder action ract respondwith "Q.URL + Q.HEADER("abcd")"
add responder policy rsp_pol "sys.eval_classic_expr("ns_true")" DROP
add appfw policy aff_pol_1 "http.req.body.length.gt(10)" APPFW_BYPASS
add appfw policy aff_pol ns_true APPFW_BYPASS

<!--NeedCopy-->
```

Une fois ces erreurs détectées, vous pouvez utiliser l'outil de `nspepi` mise à niveau pour convertir votre configuration ou la convertir manuellement. Pour plus d'informations, consultez la rubrique de l'outil nspepi .

> **Remarque :**
>
> Vous pouvez exécuter l' `nspepi` outil uniquement sur Citrix ADC version 12.1, 13.0 et versions ultérieures.

Exemple de sortie sans erreur de validation

Voici un exemple de sortie du fichier de configuration sans configuration supprimée ou non valide :


```
root@ns# check_invalid_config /var/tmp/new_ns.conf
No issue detected with the configuration.
root@ns#
<!--NeedCopy-->
```

FAQ sur la dépréciation des stratégies classiques

October 5, 2021

- **Quelles sont les stratégies classiques obsolètes à partir de la version 12.0 de Citrix ADC ?**

  Toutes les fonctionnalités et fonctionnalités mentionnées dans le tableau des stratégies obsolètes sont obsolètes de Citrix ADC version 12.0 build 56.20. Citrix vous recommande de consulter les tableaux suivants (au format PDF) pour obtenir des détails sur les fonctionnalités et les stratégies obsolètes.

  - Tableau 1 pour les politiques dépréciées et leur alternative.
  - Tableau 2 pour les fonctionnalités Citrix ADC obsolètes et son alternative avec les détails de configuration.

- **Comment puis-je convertir les fonctionnalités et fonctionnalités basées sur des stratégies classiques en stratégie avancée ?**

  Vous pouvez utiliser l' `nspepi` outil propriétaire Citrix ADC pour convertir des commandes, des expressions et des configurations. `nspepi` permet de convertir toutes les expressions classiques de la configuration Citrix ADC en expressions de stratégie avancée. Pour plus d'informations sur `nspepi` cet outil, voir Conversion d'expressions de stratégie à l'aide de l'outil NSPEPI.

- **À partir de quelle version les fonctionnalités et fonctionnalités basées sur des stratégies classiques sont-elles obsolètes ?**

  Citrix ADC 12.0 build 56.20 et versions ultérieures.

- **À partir de quelle version les fonctionnalités et fonctionnalités classiques basées sur des stratégies obsolètes sont-elles supprimées de l'appliance Citrix ADC ?**

  Citrix ADC version 13.1 et suivantes. Pour plus d'informations, consultez la section Tableau des stratégies dépréciées .

- **Quelles sont les étapes à suivre lorsque je mets à niveau mon appliance vers une version qui ne prend pas en charge les fonctionnalités classiques basées sur des stratégies ?**

Citrix recommande d'utiliser des stratégies avancées avant de mettre à niveau votre appliance vers des versions ultérieures à Citrix ADC version 13.0. Pour plus d'informations, voir Stratégies avancées.

- **Combien de temps les fonctionnalités obsolètes seront-elles prises en charge sur une appliance Citrix ADC ?**

  Citrix ne prend pas en charge la stratégie classique et son utilisation dans les versions postérieures à Citrix ADC version 13.0.

- **Dois-je redémarrer mon appliance après avoir converti le fichier de configuration ?**

  Oui, vous devez redémarrer l'instance Citrix ADC après la conversion réussie du `ns.config` fichier.

Avant de continuer

October 5, 2021

Avant de configurer des expressions et des stratégies, assurez-vous de bien comprendre la fonctionnalité Citrix ADC pertinente et la structure de vos données, comme suit :

- Lisez la documentation sur la fonctionnalité concernée.
- Examinez le flux de données pour connaître le type de données que vous souhaitez configurer.

Vous souhaiterez peut-être exécuter un suivi sur le type de trafic ou de contenu que vous souhaitez configurer. Cela vous donnera une idée des paramètres et des valeurs, ainsi que des opérations sur ces paramètres et valeurs, que vous devez spécifier dans une expression.

Remarque : Citrix ADC prend en charge la stratégie avancée au sein d'une fonctionnalité. Les deux types ne peuvent pas figurer dans la même fonction. Au cours des dernières versions, certaines fonctionnalités de Citrix ADC sont passées de l'utilisation de stratégies et d'expressions à la stratégie et expressions avancées. Si une fonctionnalité qui vous intéresse est passée au format de stratégie Avancé, il se peut que vous deviez migrer manuellement les informations plus anciennes. Vous trouverez ci-dessous des instructions pour décider si vous devez migrer vos stratégies :

- Si vous avez configuré des stratégies classiques dans une version de la fonctionnalité de mise en cache intégrée avant la version 9.0, puis que vous effectuez une mise à niveau vers la version 9.0 ou ultérieure, cela n'a aucun impact. Toutes les stratégies héritées sont migrées vers le format de stratégie avancé.
- Pour les autres fonctionnalités, vous devez migrer manuellement les stratégies et expressions classiques vers la syntaxe Avancée si la fonctionnalité a migré vers la stratégie Avancée.

Configurer l'infrastructure de stratégie avancée

January 21, 2021

Vous pouvez créer des stratégies avancées pour diverses fonctionnalités de Citrix ADC, notamment DNS, Rewrite, Responder et Integrated Caching, et la fonction d'accès sans client dans Citrix Gateway. Les stratégies contrôlent le comportement de ces fonctionnalités.

Lorsque vous créez une stratégie, vous lui attribuez un nom, une règle (une expression), des attributs spécifiques à une entité et une action effectuée lorsque les données correspondent à la stratégie. Après avoir créé la stratégie, vous déterminez quand elle est appelée en la liant globalement ou au traitement en temps de demande ou de réponse pour un serveur virtuel.

Les stratégies qui partagent le même point de liaison sont appelées *banque de stratégies*. Par exemple, toutes les stratégies liées à un serveur virtuel constituent la banque de stratégies du serveur virtuel. Lors de la liaison de la stratégie, vous lui attribuez un niveau de priorité pour spécifier quand elle est appelée par rapport aux autres stratégies de la banque. Outre l'attribution d'un niveau de priorité, vous pouvez configurer un ordre d'évaluation arbitraire pour les stratégies d'une banque en spécifiant des expressions Goto.

Outre les banques de stratégies associées à un point de liaison intégré ou à un serveur virtuel, vous pouvez configurer des *étiquettes de stratégie*. Une étiquette de stratégie est une banque de stratégies identifiée par un nom arbitraire. Vous appelez une étiquette de stratégie et les stratégies qu'elle comporte à partir d'une banque de stratégies globale ou spécifique au serveur virtuel. Une étiquette de stratégie ou une banque de stratégies de serveur virtuel peut être invoquée à partir de plusieurs banques de stratégies.

Pour certaines fonctionnalités, vous pouvez utiliser le gestionnaire de stratégies pour configurer et lier des stratégies.

Règles pour les noms dans les identificateurs utilisés dans les stratégies

January 21, 2021

Les noms des identificateurs dans l'expression nommée, la légende HTTP, le jeu de motifs et les entités limitant la vitesse doivent commencer par un alphabet ASCII ou un trait de soulignement (_). Les caractères restants peuvent être des caractères alphanumériques ASCII ou des traits de soulignement (_).

Les noms de ces identificateurs ne doivent pas commencer par les mots réservés suivants :

- Les mots ALT, TRUE ou FALSE ou l'identificateur à un caractère Q ou S.

- Indicateur de syntaxe spéciale RE (pour les expressions régulières) ou XP (pour les expressions XPath).
- Préfixes d'expression, qui sont actuellement les suivants:
  - CLIENT
  - EXTEND
  - HTTP
  - SERVER
  - SYS
  - TARGET
  - TEXTE
  - URL
  - MYSQL
  - MSSQL

En outre, les noms de ces identificateurs ne peuvent pas être les mêmes que les noms des constantes d'énumération utilisées dans l'infrastructure de stratégies. Par exemple, le nom d'un identificateur ne peut pas être IGNORECASE, YEAR ou LATIN2_CZECH_CS (un jeu de caractères MySQL).

Remarque : l'appliance Citrix ADC effectue une comparaison insensible à la casse des identificateurs avec ces mots et constantes d'énumération. Par exemple, les noms des identificateurs ne peuvent pas commencer par TRUE, True ou True.

Créer ou modifier une stratégie

August 20, 2021

Toutes les stratégies comportent des éléments communs. La création d'une stratégie consiste, au minimum, à nommer la stratégie et à configurer une règle. Les outils de configuration de stratégie pour les différentes entités présentent des zones de chevauchement, mais aussi des différences. Pour plus d'informations sur la configuration d'une stratégie pour une fonction particulière, y compris l'association d'une action à la stratégie, reportez-vous à la documentation de la fonction.

Pour créer une stratégie, commencez par déterminer l'objet de la stratégie. Par exemple, vous pouvez définir une stratégie qui identifie les requêtes HTTP pour les fichiers image ou les demandes client qui contiennent un certificat SSL. En plus de connaître le type d'informations avec lequel vous souhaitez que la stratégie fonctionne, vous devez connaître le format des données analysées par la stratégie.

Ensuite, déterminez si la stratégie est applicable globalement ou si elle concerne un serveur virtuel particulier. Tenez également compte de l'effet que l'ordre dans lequel vos stratégies sont évaluées (qui sera déterminé par la façon dont vous les liez) aura sur la stratégie que vous êtes sur le point de configurer.

Créer une stratégie à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une stratégie et vérifier la configuration :

```
- add responder|dns|cs|rewrite|cache policy <policyName> -rule <
    expression> [<feature-specific information>]

- show rewrite policy <name>
<!--NeedCopy-->
```

Exemple 1 :

```
add rewrite policy "pol_remove-ae" true "act_remove-ae"
Done
> show rewrite policy pol_remove-ae
            Name: pol_remove-ae
            Rule: true
            RewriteAction: act_remove-ae
            UndefAction: Use Global
            Hits: 0
            Undef Hits: 0
            Bound to: GLOBAL RES_OVERRIDE
            Priority: 90
            GotoPriorityExpression: END
Done
<!--NeedCopy-->
```

Exemple 2 :

```
add cache policy BranchReportsCachePolicy -rule q{
 http.req.url.query.value("actionoverride").contains("branchReport s")
    }
  -action cache
Done
show cache policy BranchReportsCachePolicy
            Name: BranchReportsCachePolicy
            Rule: http.req.url.query.value("actionoverride").contains("
               branchReports")
            CacheAction: CACHE
            Stored in group: DEFAULT
            UndefAction: Use Global
            Hits: 0
            Undef Hits: 0
Done
<!--NeedCopy-->
```


Remarque : Sur la ligne de commande, les guillemets dans une règle de stratégie (l'expression) doivent être échappés ou délimités avec le délimiteur q. Pour plus d'informations, voir Configurer les expressions de stratégie avancées : Pour commencer.

Créer ou modifier une stratégie à l'aide de l'interface graphique

1. Dans le volet de navigation, développez le nom de la fonctionnalité pour laquelle vous souhaitez configurer une stratégie, puis cliquez sur **Stratégies**. Par exemple, vous pouvez sélectionner **Commutation de contenu, Mise en cache intégrée, DNS, Réécriture ou Répondeur**.
2. Dans le volet d'informations, cliquez sur **Ajouter**ou sélectionnez une stratégie existante et cliquez sur **Ouvrir**. Une boîte de dialogue de configuration de stratégie s'affiche.
3. Spécifiez des valeurs pour les paramètres suivants. (Un astérisque indique un paramètre obligatoire. Pour un terme entre parenthèses, voir le paramètre correspondant dans "Paramètres pour la création ou la modification d'une stratégie.")
4. Cliquez sur **Créer**, puis sur **Fermer**.
5. Cliquez sur **Enregistrer**. Une stratégie est ajoutée.
   Remarque : Après avoir créé une stratégie, vous pouvez afficher les détails de la stratégie en cliquant sur l'entrée de stratégie dans le volet de configuration. Les détails qui sont mis en surbrillance et soulignés sont des liens vers l'entité correspondante (par exemple, une expression nommée).

Exemples de configuration de stratégie

August 20, 2021

Ces exemples montrent comment les stratégies et les actions associées sont entrées dans l'interface de ligne de commande. Dans l'utilitaire de configuration, les expressions s'affichent dans la fenêtre Expression de la boîte de dialogue Configuration de l'entité pour la fonction de mise en cache ou de réécriture intégrée.

Voici un exemple de création d'une stratégie de mise en cache. Notez que les actions pour les stratégies de mise en cache sont intégrées, vous n'avez donc pas besoin de les configurer séparément de la stratégie.

```
1   add cache policy BranchReportsCachePolicy -rule q{
2  http.req.url.query.value("actionoverride").contains("branchReports") }
3   -action cache
4 <!--NeedCopy-->
```


Voici un exemple de stratégie et d'action de réécriture :

```
1  add rewrite action myAction1 INSERT_HTTP_HEADER "myHeader" "
      valueForMyHeader"
2  add rewrite policy myPolicy1 "http.req.url.contains("myURLstring")"
      myAction1
3  <!--NeedCopy-->
```

Remarque : Sur la ligne de commande, les guillemets dans une règle de stratégie (l'expression) doivent être échappés ou délimités avec le délimiteur q. Pour plus d'informations, voir Configurer les expressions de stratégie avancées : Pour commencer.

Configurer et lier des stratégies avec le gestionnaire de stratégies

October 5, 2021

> **Avertissement :**
>
> Les expressions de stratégie classiques ne sont plus prises en charge à partir de Citrix ADC 12.0 build 56.20 et à titre d'alternative, Citrix vous recommande d'utiliser des stratégies avancées. Pour plus d'informations, voir Stratégies avancées.

Certaines applications fournissent un gestionnaire de stratégies spécialisé dans l'utilitaire de configuration Citrix ADC pour simplifier la configuration des banques de stratégies. Il vous permet également de rechercher et de supprimer des stratégies et des actions qui ne sont pas utilisées.

Le Gestionnaire de stratégies est actuellement disponible pour les fonctionnalités de réécriture, de mise en cache intégrée, de répondeur et de compression.

Voici les équivalents clavier des procédures décrites dans cette section :

- Pour modifier une cellule dans le Gestionnaire de stratégies, vous pouvez accéder à la cellule et cliquer sur F2 ou appuyer sur la barre d'espace du clavier.
- Pour sélectionner une entrée dans un menu déroulant, vous pouvez accéder à l'entrée avec la touche de tabulation, appuyer sur la barre d'espace pour afficher le menu déroulant, utiliser les touches FLÉCHÉES HAUT et BAS pour accéder à l'entrée souhaitée, puis appuyer à nouveau sur la barre d'espace pour sélectionner l'entrée.
- Pour annuler une sélection dans un menu déroulant, appuyez sur la touche Echap.
- Pour insérer une stratégie, appuyez sur la touche de tabulation jusqu'à la ligne au-dessus du point d'insertion et appuyez sur CtrL+Insérer, ou cliquez sur Insérer une stratégie.

- Pour supprimer une stratégie, appuyez sur la touche de tabulation jusqu'à la ligne qui contient la stratégie, puis appuyez sur Supprimer.

Remarque : Notez que lorsque vous supprimez la stratégie, Citrix ADC recherche les valeurs Goto Expression des autres stratégies de la banque. Si l'une de ces valeurs Goto Expression correspond au niveau de priorité de la stratégie supprimée, elle est supprimée.

Configurez les liaisons de stratégie à l'aide du gestionnaire de stratégies

1. Dans le volet de navigation, cliquez sur la fonctionnalité pour laquelle vous souhaitez configurer des stratégies. Les choix sont Responder, Integrated Caching, Rewrite ou Compression.
2. Dans le volet d'informations, cliquez sur **Gestionnaire de stratégies**.
3. À tout moment avant de terminer la configuration des liaisons de stratégie, si vous souhaitez configurer les liaisons pour les stratégies qui utilisent la stratégie avancée, cliquez sur le bouton Basculer vers la stratégie avancée.
4. Pour les fonctionnalités autres que Responder, pour spécifier le point de liaison, cliquez sur Demande ou Réponse, puis sur l'un des points de liaison de temps de demande ou de réponse. Les options sont Override Global, LB Virtual Server, CS Virtual Server, Default Global ou Policy Label. Si vous configurez le répondeur, les types de flux Demande et Réponse ne sont pas disponibles.
5. Pour lier une stratégie à ce point de liaison, cliquez sur Insérer une stratégie, puis sélectionnez une stratégie précédemment configurée, une étiquette NOPOLICY ou l'option Nouvelle stratégie. Selon l'option que vous sélectionnez, vous avez les choix suivants :
   - **Nouvelle stratégie :** créez la stratégie comme décrit dans « Créer ou modifier une stratégie », puis configurez le niveau de priorité, l'expression GoTo et l'appel de stratégie comme décrit dans le tableau, « Format de chaque entrée d'une banque de stratégies. «
   - **Stratégie existante**, **NOPOLICY**ou `NOPOLICY\<feature name\>` : Configurez le niveau de priorité, l'expression GoTo et l'appel de stratégie comme décrit dans le tableau, « Format de chaque entrée d'une banque de stratégies. « Les options `NOPOLICY\<feature name \>` ou les options **NOPOLICY** ne sont disponibles que pour les stratégies qui utilisent des stratégies avancées.
6. Répétez les étapes précédentes pour ajouter des entrées à cette banque de stratégies.
7. Pour modifier le niveau de priorité d'une entrée, vous pouvez effectuer l'une des opérations suivantes :
   - Double-cliquez sur le champ Priorité d'une entrée et modifiez la valeur.
   - Cliquez sur une stratégie et faites-la glisser vers une autre ligne du tableau.
   - Cliquez sur Régénérer les priorités.

Dans les trois cas, les niveaux de priorité de toutes les autres politiques sont modifiés au besoin pour tenir compte de la nouvelle valeur. Les expressions Goto avec des valeurs entières sont également mises à jour automatiquement. Par exemple, si vous modifiez une valeur de priorité de 10 à 100, toutes les stratégies avec une valeur Goto Expression de 10 sont mises à jour avec la valeur 100.

8. Pour modifier l'appel de stratégie, d'action ou de banque de stratégies pour une ligne du tableau, cliquez sur la flèche vers le bas à droite de l'entrée et effectuez l'une des opérations suivantes :
   - Pour modifier la stratégie, sélectionnez un autre nom de stratégie ou sélectionnez Nouvelle stratégie et suivez les étapes de la section Créer ou modifier une stratégie.
   - Pour modifier l'expression Goto, sélectionnez Suivant, Fin, USE_INVOCATION_RESULT ou sélectionnez plus et entrez une expression dont le résultat renvoie le niveau de priorité d'une autre entrée de cette banque de stratégies.
   - Pour modifier un appel, sélectionnez une banque de stratégies existante ou cliquez sur Nouvelle étiquette de stratégie et suivez les étapes de la section Lier une stratégie à une étiquette de stratégie.
9. Pour dissocier une stratégie ou une invocation d'étiquette de stratégie de cette banque, cliquez sur n'importe quel champ de la ligne contenant l'étiquette de stratégie ou de stratégie, puis cliquez sur Annulation de la stratégie.
10. Lorsque vous avez terminé, cliquez sur Appliquer les modifications. Un message dans la barre d'état indique que la stratégie est liée avec succès.

Supprimer les stratégies inutilisées à l'aide du gestionnaire de stratégies

1. Dans le volet de navigation, cliquez sur la fonctionnalité pour laquelle vous souhaitez configurer la banque de stratégies. Les choix sont Responder, Integrated Caching ou Rewrite.
2. Dans le volet d'informations, cliquez sur Gestionnaire <Feature Name> de stratégies.
3. Dans la boîte de dialogue **Nom de la fonctionnalité** > **Gestion des stratégies**r, cliquez sur **Configuration du nettoyage**.
4. Dans la boîte de dialogue **Configuration du nettoyage**, sélectionnez les éléments que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
5. Dans la boîte de dialogue Supprimer, cliquez sur **Oui**.
6. Cliquez sur **Fermer**. Un message dans la barre d'état indique que la stratégie a été supprimée avec succès.

Dissocier une stratégie

August 20, 2021

Si vous souhaitez réaffecter une stratégie ou la supprimer, vous devez d'abord supprimer sa liaison.

Dissocier globalement une stratégie avancée de mise en cache, de réécriture ou de compression intégrée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier globalement une stratégie avancée de mise en cache, de réécriture ou de compression intégrée et vérifier la configuration :

```
1 -  unbind cache|rewrite|cmp global <policyName> [-type req_override|
     req_default|res_override|res_default] [-priority <positiveInteger>]
2
3 -  show cache|rewrite|cmp global
4 <!--NeedCopy-->
```

Exemple :

```
1 > unbind cache global_nonPostReq
2 Done
3 > show cache global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6
7     2)      Global bindpoint: RES_DEFAULT
8             Number of bound policies: 1
9
10 Done
11 <!--NeedCopy-->
```

La priorité n'est requise que pour la stratégie « factice » nommée NOPOLICY.

Dissocier globalement une stratégie de répondeur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier globalement une stratégie de répondeur et vérifier la configuration :

```
1 -  unbind responder global <policyName> [-type override|default] [-
     priority <positiveInteger>]
2
```



```
3 -  show responder global
4 <!--NeedCopy-->
```

Exemple :

```
1 > unbind responder global pol404Error
2 Done
3 > show responder global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6 Done
7 <!--NeedCopy-->
```

La priorité n'est requise que pour la stratégie « factice » nommée NOPOLICY.

Dissocier globalement une stratégie DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier globalement une stratégie DNS et vérifier la configuration :

```
1 -  unbind responder global <policyName>
2
3 -  unbind responder global
4 <!--NeedCopy-->
```

Exemple :

```
1 unbind dns global dfgdfg
2 Done
3 show dns global
4     Policy name : dfgdfggfhg
5             Priority : 100
6             Goto expression : END
7 Done
8 <!--NeedCopy-->
```

Dissocier une stratégie avancée d'un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier une stratégie avancée d'un serveur virtuel et vérifier la configuration :

```
1 -  unbind cs vserver <name> -policyName <policyName> [-priority <
     positiveInteger>] [-type REQUEST|RESPONSE]
```



```
2
3 -  show lb vserver <name>
4 <!--NeedCopy-->
```

Exemple :

```
1 unbind cs vserver vs-cont-switch  -policyName pol1
2 Done
3 > show cs vserver vs-cont-switch
4             vs-cont-switch (10.102.29.10:80) - HTTP Type: CONTENT
5             State: UP
6             Last state change was at Wed Aug 19 08:56:55 2009 (+18 ms)
7             Time since last state change: 0 days, 02:47:55.750
8             Client Idle Timeout: 180 sec
9             Down state flush: ENABLED
10            Disable Primary Vserver On Down : DISABLED
11            Port Rewrite : DISABLED
12            State Update: DISABLED
13            Default:        Content Precedence: RULE
14            Vserver IP and Port insertion: OFF
15            Case Sensitivity: ON
16            Push: DISABLED  Push VServer:
17            Push Label Rule: none
18 Done
19 <!--NeedCopy-->
```

La priorité n'est requise que pour la stratégie « factice » nommée NOPOLICY.

Dissocier globalement une stratégie avancée de mise en cache, répondeur, réécriture ou compression intégrée à l'aide de l'interface graphique

1. Dans le volet de navigation, cliquez sur l'entité avec la stratégie que vous souhaitez dissocier (par exemple, mise en cache intégrée).
2. Dans le volet d'informations, cliquez sur Gestionnaire de stratégies <Feature Name>.
3. Dans la boîte de dialogue **Gestionnaire de stratégies**, sélectionnez le point de liaison avec la stratégie à dissocier, par exemple Advanced Global.
4. Cliquez sur le nom de la stratégie que vous souhaitez dissocier, puis cliquez sur Dissocier la stratégie.
5. Cliquez sur **Appliquer les modifications**.
6. Cliquez sur **Fermer**. Un message dans la barre d'état indique que la stratégie n'est pas liée avec succès.

Dissocier globalement une stratégie DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **DNS** > **Stratégies**.
2. Dans le volet d'informations, cliquez sur **Liaisons globales**.
3. Dans la boîte de dialogue **Liaisons globales**, sélectionnez stratégie et cliquez sur **dissocier stratégie**.
4. Cliquez sur **OK**. Un message dans la barre d'état indique que la stratégie est dissociée avec succès.

Dissocier une stratégie avancée d'un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic,** développez Équilibrage de charge ou Changement de contenu, puis cliquez sur **Serveurs virtuels**.
2. Dans le volet d'informations, double-cliquez sur le serveur virtuel à partir duquel vous souhaitez dissocier la stratégie.
3. Sous l'onglet **Stratégies**, dans la colonne **Actif**, désactivez la case à cocher en regard de la stratégie à dissocier.
4. Cliquez sur **OK**. Un message dans la barre d'état indique que la stratégie est dissociée avec succès.

Créer des étiquettes de stratégie

August 20, 2021

Outre les points de liaison intégrés dans lesquels vous configurez des banques de stratégies, vous pouvez également configurer des étiquettes de stratégies définies par l'utilisateur et les associer.

Dans une étiquette de stratégie, vous liez des stratégies et spécifiez l'ordre d'évaluation de chaque stratégie par rapport aux autres dans la banque de stratégies de l'étiquette de stratégie. Citrix ADC vous permet également de définir un ordre d'évaluation arbitraire comme suit :

- Vous pouvez utiliser les expressions « goto » pour pointer vers l'entrée suivante dans la banque à évaluer après l'entrée actuelle.
- Vous pouvez utiliser une entrée dans une banque de stratégies pour appeler une autre banque.

Chaque entité détermine le type de stratégie que vous pouvez lier à une étiquette de stratégie, le type de serveur virtuel d'équilibrage de charge auquel vous pouvez lier l'étiquette et le type de serveur virtuel à partir duquel l'étiquette peut être invoquée. Par exemple, une étiquette de stratégie TCP ne peut être liée qu'à un serveur virtuel d'équilibrage de charge TCP. Vous ne pouvez pas lier les stratégies

HTTP à une étiquette de stratégie de ce type. Et vous pouvez appeler une étiquette de stratégie TCP uniquement à partir d'un serveur virtuel de commutation de contenu TCP.

Après avoir configuré une nouvelle étiquette de stratégie, vous pouvez l'appeler depuis une ou plusieurs banques pour les points de liaison intégrés.

Créer une étiquette de stratégie de mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une étiquette de stratégie de mise en cache et vérifier la configuration :

```
1 -  add cache policylabel <labelName> -evaluates req|res
2
3 -  show cache policylabel<labelName>
4 <!--NeedCopy-->
```

Exemple :

```
1 > add cache policylabel lbl-cache-pol -evaluates req
2 Done
3
4 > show cache policylabel lbl-cache-pol
5             Label Name: lbl-cache-pol
6             Evaluates: REQ
7             Number of bound policies: 0
8             Number of times invoked: 0
9 Done
10 <!--NeedCopy-->
```

Créer une étiquette de stratégie de changement de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une étiquette de stratégie Commutation de contenu et vérifier la configuration :

```
1 -  add cs policylabel <labelName> http|tcp|rtsp|ssl
2
3 -  show cs policylabel <labelName>
4 <!--NeedCopy-->
```

Exemple :


```
> add cs policylabel lbl-cs-pol http
Done
> show cs policylabel lbl-cs-pol
            Label Name: lbl-cs-pol
            Label Type: HTTP
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Créer une étiquette de stratégie de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une étiquette de stratégie Réécriture et vérifier la configuration :

```
-  add rewrite policylabel <labelName> http_req|http_res|url|text|
   clientless_vpn_req|clientless_vpn_res

-  show rewrite policylabel <labelName>
<!--NeedCopy-->
```

Exemple :

```
> add rewrite policylabel lbl-rewrt-pol http_req
Done

> show rewrite policylabel lbl-rewrt-pol
            Label Name: lbl-rewrt-pol
            Transform Name: http_req
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Créer une étiquette de stratégie de répondeur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une étiquette de stratégie Répondeur et vérifier la configuration :

```
-  add responder policylabel <labelName>
```



```
2
3 -  show responder policylabel <labelName>
4 <!--NeedCopy-->
```

Exemple :

```
1 > add responder policylabel lbl-respndr-pol
2 Done
3
4 > show responder policylabel lbl-respndr-pol
5             Label Name: lbl-respndr-pol
6             Number of bound policies: 0
7             Number of times invoked: 0
8 Done
9 <!--NeedCopy-->
```

Remarque : Invoquez cette étiquette de stratégie à partir d'une banque de stratégies. Pour plus d'informations, consultez la section « Liaison d'une stratégie à une étiquette de stratégie ».

Créer une étiquette de stratégie à l'aide de l'interface graphique

1. Dans le volet de navigation, développez la fonction pour laquelle vous souhaitez créer une étiquette de stratégie, puis cliquez sur **Étiquettes de stratégie**. Les options sont la mise en cache intégrée, la réécriture, la commutation de contenu ou le répondeur.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la zone Nom, entrez un nom unique pour cette étiquette de stratégie.
4. Entrez des informations spécifiques à l'entité pour l'étiquette de stratégie. Par exemple, pour la mise en cache intégrée, dans le menu déroulant Evaluates, vous devez sélectionner REQ si vous souhaitez que cette étiquette de stratégie contienne des stratégies request-time, ou sélectionner RES si vous souhaitez que cette étiquette de stratégie contienne des stratégies response-time. Pour Réécrire, vous devez sélectionner un nom de transformation.
5. Cliquez sur **Créer**.
6. Configurez l'une des banques de stratégies intégrées pour appeler cette étiquette de stratégie. Pour plus d'informations, consultez la section « Liaison d'une stratégie à une étiquette de stratégie ». Un message dans la barre d'état indique que l'étiquette de stratégie a été créée avec succès.

Lier une stratégie à une étiquette de stratégie

Comme pour les banques de stratégies liées aux points de liaison intégrés, chaque entrée d'une étiquette de stratégie est liée à l'étiquette de stratégie. Comme pour les stratégies qui sont liées globalement ou à un serveur vserver, chaque stratégie liée à l'étiquette de stratégie peut également appeler

une banque de stratégies ou une étiquette de stratégie qui est évaluée après le traitement de l'entrée en cours. Le tableau suivant récapitule les entrées d'une étiquette de stratégie.

- **Nom**. Le nom d'une stratégie ou, pour invoquer une autre banque de stratégies sans évaluer une stratégie, le nom de stratégie « fictif » NOPOLICY.

  Vous pouvez spécifier NOPOLICY plusieurs fois dans une banque de stratégies, mais vous ne pouvez spécifier une stratégie nommée qu'une seule fois.

- **Priorité**. Un entier. Ce paramètre peut fonctionner avec l'expression Goto.

- **Goto Expression**. Détermine la stratégie suivante à évaluer dans cette banque. Vous pouvez fournir l'une des valeurs suivantes :

  - **SUIVANT**. Passez à la stratégie avec la priorité supérieure suivante.
  - **FIN**. Arrêtez l'évaluation.
  - **USE_INVOCATION_RESULT**. Applicable si cette entrée fait appel à une autre banque de polices. Si le Goto final dans la banque invoquée a une valeur de END, l'évaluation s'arrête. Si le Goto final est autre chose que END, la banque de polices actuelle effectue un NEXT.
  - **Nombre positif :** numéro de priorité de la prochaine stratégie à évaluer.
  - **Expression numérique**. Expression qui produit le numéro de priorité de la stratégie suivante à évaluer.

  Le Goto ne peut aller de l'avant que dans une banque de polices.

  Si vous omettez l'expression Goto, c'est la même chose que de spécifier END.

- **Type d'invocation**. Désigne un type de banque de stratégies. La valeur peut être l'une des valeurs suivantes :

  - **Demande Vserver**. Appelle les stratégies de temps de demande associées à un serveur virtuel.
  - **Réponse Vserver**. Appelle les stratégies de temps de réponse associées à un serveur virtuel.
  - **Étiquette de stratégie**. Invoque une autre banque de stratégies, identifiée par l'étiquette de stratégie de la banque.

- **Nom de l'invocation**. Nom d'un serveur virtuel ou d'une étiquette de stratégie, en fonction de la valeur que vous avez spécifiée pour le type d'appel.

Configurer une étiquette de stratégie ou une banque de stratégies de serveur virtuel

August 20, 2021

Après avoir créé des stratégies et créé des banques de stratégies en les liant, vous pouvez effectuer une configuration supplémentaire des stratégies au sein d'une étiquette ou d'une banque de stratégies. Par exemple, avant de configurer l'invocation d'une banque de stratégies externe, vous pouvez attendre que vous ayez configuré cette banque de stratégies.

Cette rubrique comprend les sections suivantes :

- Configurer une étiquette de stratégie
- Configurer une banque de stratégies pour un serveur virtuel

Configurer une étiquette de stratégie

Une étiquette de stratégie consiste en un ensemble de stratégies et d'appels d'autres étiquettes de stratégie et de banques de stratégies spécifiques au serveur virtuel. Un paramètre Invoke vous permet d'appeler une étiquette de stratégie ou une banque de stratégies spécifique au serveur virtuel à partir de n'importe quelle autre banque de stratégies. Une entrée NoPolicy à usage spécial vous permet d'appeler une banque externe sans traiter d'expression (règle). L'entrée NoPolicy est une stratégie « factice » qui ne contient pas de règle.

Pour configurer les étiquettes de stratégie à partir de la ligne de commande Citrix ADC, notez les détails suivants de la syntaxe de commande :

- gotoPriorityExpression est configuré comme décrit dans le tableau 2. Format de chaque entrée dans une banque de politiques de la section « Entrées dans une banque de politiques » dans les stratégies de liaison utilisant une stratégie avancée.
- L'argument type est obligatoire. Cela n'est pas contraignant une stratégie conventionnelle, où cet argument est facultatif.
- Vous pouvez appeler la banque de stratégies liées à un serveur virtuel en utilisant la même méthode que celle utilisée pour appeler une étiquette de stratégie.

Configurer une étiquette de stratégie à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une étiquette de stratégie et vérifier la configuration :

```
1 - bind cache|rewrite|responder policylabel <policylabelName> -
    policyName <policyName> -priority <priority> [-
    gotoPriorityExpression <gotoprioritыExpression>] [-invoke reqvserver
    |resvserver|policylabel <policyLabelName>|<vserverName>]
2
3 - show cache|rewrite|responder policylabel <policylabelName>
4 <!--NeedCopy-->
```

Exemple :


```
bind cache policylabel _reqBuiltinDefaults -policyName  _nonGetReq -
    priority 100
Done
show cache policylabel _reqBuiltinDefaults
            Label Name: _reqBuiltinDefaults
            Evaluates: REQ
            Number of bound policies: 3
            Number of times invoked: 0
    1)      Policy Name: _nonGetReq
            Priority: 100
            GotoPriorityExpression: END
    2)      Policy Name: _advancedConditionalReq
            Priority: 200
            GotoPriorityExpression: END

    3)      Policy Name: _personalizedReq
            Priority: 300
            GotoPriorityExpression: END
Done
<!--NeedCopy-->
```

Invoquer une étiquette de stratégie à partir d'une banque de stratégies de réécriture avec une entrée NOPOLICY à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour appeler une étiquette de stratégie à partir d'une banque de stratégies de réécriture avec une entrée NOPOLICY et vérifiez la configuration :

```
-  bind rewrite global <policyName> <priority> <gotoPriorityExpression>
     -type REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke
    reqvserver|resvserver|policylabel <policyLabelName>|<vserverName>

-  show rewrite global
<!--NeedCopy-->
```

Exemple :

```
> bind rewrite global NOPOLICY 100 -type REQ_DEFAULT -invoke
    policylabel lbl-rewrt-pol
Done
> show rewrite global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 1
```



```
6
7      2)      Global bindpoint: REQ_OVERRIDE
8              Number of bound policies: 1
9  Done
10 <!--NeedCopy-->
```

Appeler une étiquette de stratégie à partir d'une banque de stratégies de mise en cache intégrée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour appeler une étiquette de stratégie à partir d'une banque de stratégies de mise en cache intégrée et vérifier la configuration :

```
1 -  bind cache global NOPOLICY -priority <priority> -
     gotoPriorityExpression <gotoprioritыExpression> -type REQ_OVERRIDE|
     REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke reqvserver|resvserver|
     policylabel <policyLabelName>|<vserverName>
2
3 -  show cache global
4 <!--NeedCopy-->
```

Exemple :

```
1 bind cache global NOPOLICY -priority 100 -gotoPriorityExpression END -
     type REQ_DEFAULT -invoke policylabel lbl-cache-pol
2 Done
3 > show cache global
4      1)      Global bindpoint: REQ_DEFAULT
5              Number of bound policies: 2
6
7      2)      Global bindpoint: RES_DEFAULT
8              Number of bound policies: 1
9
10 Done
11 <!--NeedCopy-->
```

Appeler une étiquette de stratégie à partir d'une banque de stratégies de répondeur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour appeler une étiquette de stratégie à partir d'une banque de stratégies Répondre et vérifier la configuration :


```
- bind responder global NOPOLICY <priority> <gotopriorityExpression> -
    type OVERRIDE|DEFAULT -invoke vserver|policylabel <policyLabelName
    >|<vserverName>

- show responder global
<!--NeedCopy-->
```

Exemple :

```
> bind responder global NOPOLICY 100 NEXT -type DEFAULT -invoke
    policylabel lbl-respndr-pol
Done
> show responder global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 2

Done
<!--NeedCopy-->
```

Configurer une étiquette de stratégie à l'aide de l'interface graphique

1. Dans le volet de navigation, développez la fonctionnalité pour laquelle vous souhaitez configurer une étiquette de stratégie, puis cliquez sur Étiquettes de stratégie. Les options sont la mise en cache intégrée, la réécriture ou le répondeur.
2. Dans le volet d'informations, double-cliquez sur l'étiquette que vous souhaitez configurer.
3. Si vous ajoutez une nouvelle stratégie à cette étiquette de stratégie, cliquez sur Insérer une stratégie et, dans le champ Nom de la stratégie, sélectionnez Nouvelle stratégie. Pour plus d'informations sur l'ajout d'une stratégie, voir Créer ou modifier une stratégie. Notez que si vous appelez une banque de stratégies et que vous ne souhaitez pas qu'une règle soit évaluée avant l'invocation, cliquez sur Insérer une stratégie, puis dans le champ Nom de la stratégie, sélectionnez NOPOLICY.
4. Pour chaque entrée de cette étiquette de stratégie, configurez les éléments suivants :
   - **Nom de la stratégie :**

     Ceci est déjà déterminé par le nom de la stratégie, la nouvelle stratégie ou l'entrée NOPOLICY que vous avez insérée dans cette banque.
   - **Priorité :**

     Valeur numérique qui détermine soit un ordre absolu d'évaluation au sein de la banque, soit est utilisée conjointement avec une expression Goto.

- **Expression :**

  Règle de stratégie. Les expressions de stratégie sont décrites en détail dans les chapitres suivants. Pour une introduction, reportez-vous à la section Configurer les expressions de stratégie avancées : Pour commencer.

- **Action :**

  Action à prendre si cette stratégie est évaluée à TRUE.

- **Expression Goto :**

  Facultatif. Utilisé pour augmenter le niveau de priorité afin de déterminer la prochaine stratégie ou banque de stratégies à évaluer. Pour plus d'informations sur les valeurs possibles d'une expression Goto, reportez-vous au tableau 2. Format de chaque entrée dans une banque de politiques de la section « Entrées dans une banque de politiques » dans les stratégies de liaison utilisant une stratégie avancée.

- **Invoquer :**

  Facultatif. Invoque une autre banque de stratégies.

5. Cliquez sur **OK**. Un message dans la barre d'état indique que l'étiquette de stratégie est correctement configurée.

Configurer une banque de stratégies pour un serveur virtuel

Vous pouvez configurer une banque de stratégies pour un serveur virtuel. La banque de stratégies peut contenir des stratégies individuelles et chaque entrée de la banque de stratégies peut éventuellement appeler une étiquette de stratégie ou une banque de stratégies que vous avez configurée pour un autre serveur virtuel. Si vous appelez une étiquette de stratégie ou une banque de stratégies, vous pouvez le faire sans déclencher une expression (une règle) en sélectionnant une entrée « factice » NOPOLICY au lieu d'un nom de stratégie.

Ajouter des stratégies à une banque de stratégies de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter des stratégies à une banque de stratégies de serveur virtuel et vérifier la configuration :

```
1 - bind lb|cs vserver <virtualServerName> <serviceType> [-policyName <
    policyName>] [-priority <positiveInteger>] [-gotoPriorityExpression
    <expression>] [-type REQUEST|RESPONSE]
2
3 - show lb|cs vserver <virtualServerName>
4 <!--NeedCopy-->
```


Exemple :

```
add lb vserver vs-cont-sw TCP
Done
show lb vserver vs-cont-sw
            vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
            State: DOWN
            Last state change was at Wed Aug 19 10:04:02 2009 (+279 ms)
            Time since last state change: 0 days, 00:02:14.420
            Effective State: DOWN
            Client Idle Timeout: 9000 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
            Connection Failover: DISABLED
Done
<!--NeedCopy-->
```

Appelez une étiquette de stratégie à partir d'une banque de stratégies de serveur virtuel avec une entrée NOPOLICY à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour appeler une étiquette de stratégie à partir d'une banque de stratégies de serveur virtuel avec une entrée NOPOLICY et vérifiez la configuration :

```
-  bind lb|cs vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
   NOPOLICY-CACHE|NOPOLICY-RESPONDER -priority <integer> -type REQUEST|
   RESPONSE -gotoPriorityExpression <gotoprioritыExpression> -invoke
   reqVserver|resVserver|policyLabel <vserverName>|<labelName>

-  show lb vserver
<!--NeedCopy-->
```

Exemple :

```
> bind lb vserver vs-cont-sw -policyname NOPOLICY-REWRITE -priority 200
    -type REQUEST -gotoPriorityExpression NEXT -invoke policyLabel lbl-
   rewrt-pol
Done
<!--NeedCopy-->
```


Configurer une banque de stratégies de serveur virtuel à l'aide de l'interface graphique

1. Dans le volet de navigation de gauche, développez ** **Gestion du trafic** > **Équilibrage de charge, Gestion du trafic** > **Commutation de contenu, Gestion du trafic** > **Déchargement SSL, Sécurité** > **AAA - Trafic d'application**, ou **Citrix Gateway**, le cas échéant, puis cliquez sur **Serveurs virtuels.**
2. Dans le volet d'informations, sélectionnez le serveur virtuel à configurer, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le serveur virtuel**, cliquez sur l'onglet **Stratégies**.
4. Pour créer une nouvelle stratégie dans cette banque, cliquez sur l'icône correspondant au type de stratégie ou d'étiquette de stratégie que vous souhaitez ajouter à la banque de stratégies du serveur virtuel, cliquez sur **Insérer une stratégie**. Notez que si vous souhaitez appeler une étiquette de stratégie sans évaluer de règle, sélectionnez la stratégie « factice » NOPOLICY.
5. Pour configurer une entrée existante dans cette banque de stratégies, entrez les éléments suivants :
   - **Priorité :**

     Valeur numérique qui détermine un ordre absolu d'évaluation au sein de la banque ou est utilisée conjointement avec une expression Goto.
   - **Expression :**

     Règle de stratégie. Les expressions de stratégie sont décrites en détail dans les chapitres suivants. Pour une introduction, reportez-vous à la section Configuration des expressions de stratégie avancées : mise en route.
   - **Action :**

     Action à prendre si cette stratégie est évaluée à TRUE.
   - **Expression Goto :**

     Facultatif. Détermine la prochaine évaluation de la stratégie ou de la banque de stratégies. Pour plus d'informations sur les valeurs possibles d'une expression Goto, reportez-vous à la section « Entrées dans une banque de stratégies » de la section Règles de liaison utilisant une stratégie avancée.
   - **Invoquer :**

     Facultatif. Pour appeler une autre banque de stratégies, sélectionnez le nom de l'étiquette de stratégie ou de la banque de stratégies de serveur virtuel que vous souhaitez appeler.
6. Cliquez sur **OK**. Un message dans la barre d'état indique que la stratégie est correctement configurée.

Appeler ou supprimer une étiquette de stratégie ou une banque de stratégies de serveur virtuel

August 20, 2021

Contrairement à une stratégie, qui ne peut être liée qu'une seule fois, vous pouvez utiliser une étiquette de stratégie ou la banque de stratégies d'un serveur virtuel à plusieurs reprises en l'appelant. L'invocation peut être effectuée à partir de deux endroits :

- À partir de la liaison d'une stratégie nommée dans une banque de stratégies.
- De la liaison pour une entrée « fictive » NOPOLICY dans une banque de polices.

En règle générale, l'étiquette de stratégie doit être du même type que la stratégie à partir de laquelle elle est invoquée. Par exemple, vous appelez une étiquette de stratégie de répondeur à partir d'une stratégie de répondeur.

Remarque : Lorsque vous liez ou déliez une entrée NOPOLICY globale dans une banque de stratégies sur la ligne de commande, vous spécifiez une priorité pour distinguer une entrée NOPOLICY d'une autre.

Invoquer une étiquette de stratégie de réécriture ou de mise en cache intégrée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour appeler une étiquette de stratégie de réécriture ou de mise en cache intégrée et vérifier la configuration :

```
1 -  bind cache global <policy> -priority <positive_integer> [-
     gotoPriorityExpression <expression>] -type REQ_OVERRIDE|REQ_DEFAULT|
     RES_OVERRIDE|RES_DEFAULT] -invoke reqvserver|resvserver|policylabel
     <label_name>
2
3 -  bind rewrite global<policy> -priority <positive_integer> [-
     gotoPriorityExpression <expression>] -type REQ_OVERRIDE|REQ_DEFAULT|
     RES_OVERRIDE|RES_DEFAULT] -invoke reqvserver|resvserver|policylabel
     <label_name>
4
5 -  show cache global|show rewrite global
6 <!--NeedCopy-->
```

Exemple :

```
1 > bind cache global _nonPostReq2 -priority 100 -type req_override -
     invoke
2     policylabel lbl-cache-pol
```



```
Done
> show cache global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 2

    2)      Global bindpoint: RES_DEFAULT
            Number of bound policies: 1

    3)      Global bindpoint: REQ_OVERRIDE
            Number of bound policies: 1

Done
<!--NeedCopy-->
```

Appeler une étiquette de stratégie de répondeur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour appeler une étiquette de stratégie de répondeur et vérifier la configuration :

```
-  bind responder global <policy_Name> <priority_as_positive_integer>
   [<gotoPriorityExpression>] -type REQ_OVERRIDE|REQ_DEFAULT|OVERRIDE|
   DEFAULT -invoke vserver|policylabel <label_name>

-  show responder global
<!--NeedCopy-->
```

Exemple :

```
> bind responder global pol404Error1 300 -invoke policylabel lbl-
   respndr-pol
Done
> show responder global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 2

Done
<!--NeedCopy-->
```


Appeler une banque de stratégies de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour appeler une banque de stratégies de serveur virtuel et vérifier la configuration :

```
1 -  bind lb vserver <vserver_name> -policyName <policy_Name> -priority <
     positive_integer> [-gotoPriorityExpression <expression>] -type
     REQUEST|RESPONSE -invoke reqvserver|resvserver|policylabel <
     policy_Label_Name>
2
3 -  bind lb vserver <vserver_name>
4 <!--NeedCopy-->
```

Exemple :

```
1  > bind lb vserver lbvip -policyName ns_cmp_msapp -priority 100
2  Done
3
4  > show lb vserver lbvip
5              lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
6              State: DOWN
7              Last state change was at Wed Jul 15 05:54:24 2009 (+166 ms)
8              Time since last state change: 28 days, 06:37:49.250
9              Effective State: DOWN
10             Client Idle Timeout: 180 sec
11             Down state flush: ENABLED
12             Disable Primary Vserver On Down : DISABLED
13             Port Rewrite : DISABLED
14             No. of Bound Services :  0 (Total)       0 (Active)
15             Configured Method: LEASTCONNECTION
16             Mode: IP
17             Persistence: NONE
18             Vserver IP and Port insertion: OFF
19             Push: DISABLED  Push VServer:
20             Push Multi Clients: NO
21             Push Label Rule: none
22
23     1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority:
           100   Hits: 0
24
25     2)      Policy : pol-ssl Priority:0
26     3)      Policy : ns_cmp_msapp Priority:100
27     4)      Policy : cf-pol Priority:1      Inherited
28 Done
```



```
29 <!--NeedCopy-->
```

Supprimer une étiquette de stratégie de mise en cache intégrée ou réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour supprimer une étiquette de stratégie de réécriture ou de mise en cache intégrée et vérifier la configuration :

```
1 - unbind rewrite global <policyName> -priority <positiveInteger> -type
     REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT
2
3 - unbind cache global <policyName> -priority <positiveInteger> -type
    REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT
4
5 - show rewrite global|show cache global
6 <!--NeedCopy-->
```

Exemple :

```
1 > unbind rewrite global NOPOLICY -priority 100 -type REQ_OVERRIDE
2 > show rewrite global
3 Done
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6
7 Done
8 <!--NeedCopy-->
```

Supprimer une étiquette de stratégie de répondeur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour supprimer une étiquette de stratégie de répondeur et vérifier la configuration :

```
1 - unbind responder global <policyName> -priority <positiveInteger> -
    type OVERRIDE|DEFAULT
2
3 - show responder global
4 <!--NeedCopy-->
```

Exemple :


```
> unbind responder global NOPOLICY -priority 100 -type REQ_DEFAULT
Done
> show responder global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 1

Done
<!--NeedCopy-->
```

Supprimer une étiquette de stratégie de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour supprimer une étiquette de stratégie de serveur virtuel et vérifier la configuration :

```
- unbind lb vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
  NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority <
  positiveInteger>

- unbind cs vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
  NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority <
  positiveInteger>

- show lb vserver|show cs vserver
<!--NeedCopy-->
```

Exemple :

```
> unbind lb vserver lbvip -policyName ns_cmp_msapp -priority 200
Done
> show lb vserver lbvip
            lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
            State: DOWN
            Last state change was at Wed Jul 15 05:54:24 2009 (+161 ms)
            Time since last state change: 28 days, 06:47:54.600
            Effective State: DOWN
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Port Rewrite : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
```



```
16              Persistence: NONE
17              Vserver IP and Port insertion: OFF
18              Push: DISABLED  Push VServer:
19              Push Multi Clients: NO
20              Push Label Rule: none
21
22      1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority:
            100   Hits: 0
23
24      1)      Policy : pol-ssl Priority:0
25      2)      Policy : cf-pol Priority:1      Inherited
26  Done
27  <!--NeedCopy-->
```

Appelez une étiquette de stratégie ou une banque de stratégies de serveur virtuel à l'aide de l'interface graphique

1. Liez une stratégie, comme décrit dans Lier une stratégie globalement, Lier une stratégie à un serveur virtuelou Lier une stratégie à une étiquette de stratégie. Vous pouvez également entrer une entrée « factice » NOPOLICY au lieu d'un nom de stratégie. Vous le faites si vous ne souhaitez pas évaluer une stratégie avant d'évaluer la banque de stratégies.
2. Dans le champ Invoquer, sélectionnez le nom de l'étiquette de stratégie ou de la banque de stratégies de serveur virtuel que vous souhaitez évaluer si le trafic correspond à la stratégie liée. Un message dans la barre d'état indique que l'étiquette de stratégie ou la banque de stratégies de serveur virtuel est appelée avec succès.

Supprimer une invocation d'étiquette de stratégie à l'aide de l'interface graphique

1. Ouvrez la stratégie et désactivez le champ Invoquer. La suppression de la liaison de la stratégie supprime également l'invocation de l'étiquette. Un message dans la barre d'état indique que l'étiquette de stratégie a été supprimée avec succès.

Configuration de l'expression de stratégie avancée : mise en route

January 21, 2021

Les stratégies avancées évaluent les données en fonction des informations que vous fournissez dans les expressions de stratégie avancées. Une expression de stratégie avancée analyse les éléments de données (par exemple, les en-têtes HTTP, les adresses IP source, l'heure système Citrix ADC et les données de corps POST). Outre la configuration d'une expression de stratégie avancée dans une stratégie,

dans certaines fonctionnalités de Citrix ADC, vous configurez l'expression de stratégie avancée en dehors du contexte d'une stratégie.

Pour créer une expression de stratégie avancée, vous sélectionnez un préfixe qui identifie un élément de données à analyser, puis vous spécifiez une opération à effectuer sur les données. Par exemple, une opération peut correspondre à un élément de données avec une chaîne de texte que vous spécifiez ou peut transformer une chaîne de texte en en-tête HTTP. D'autres opérations correspondent à une chaîne renvoyée avec un ensemble de chaînes ou un motif de chaîne. Vous configurez des expressions composées en spécifiant des opérateurs booléens et arithmétiques et en utilisant des parenthèses pour contrôler l'ordre d'évaluation.

L'expression de stratégie avancée peut également contenir des expressions classiques. Vous pouvez attribuer un nom à une expression fréquemment utilisée pour éviter d'avoir à créer l'expression à plusieurs reprises.

Les stratégies et quelques autres entités incluent des règles que Citrix ADC utilise pour évaluer un paquet dans le trafic qui le traverse, pour extraire des données du système Citrix ADC lui-même, pour envoyer une requête (une « légende ») à une application externe ou pour analyser un autre élément de données. Une règle prend la forme d'une expression logique qui est comparée au trafic et renvoie finalement les valeurs TRUE ou FALSE.

Les éléments de la règle peuvent eux-mêmes renvoyer des valeurs TRUE ou FALSE, chaîne ou numériques.

Avant de configurer une expression de stratégie avancée, vous devez comprendre les caractéristiques des données que la stratégie ou une autre entité doit évaluer. Par exemple, lorsque vous travaillez avec la fonctionnalité de mise en cache intégrée, une stratégie détermine quelles données peuvent être stockées dans le cache. Avec la mise en cache intégrée, vous devez connaître les URL, les en-têtes et les autres données dans les requêtes HTTP et les réponses reçues par Citrix ADC. Grâce à ces connaissances, vous pouvez configurer des stratégies qui correspondent aux données réelles et permettre à Citrix ADC de gérer la mise en cache du trafic HTTP. Ces informations vous aident à déterminer le type d'expression que vous devez configurer dans la stratégie.

Éléments de base d'une expression de stratégie avancée

August 20, 2021

Une expression de stratégie avancée se compose, au minimum, d'un préfixe (ou d'un seul élément utilisé à la place d'un préfixe). La plupart des expressions spécifient également une opération à effectuer sur les données identifiées par le préfixe. Vous formatez une expression de 1 499 caractères au maximum comme suit :

```
<prefix>.<operation> [<compound-operator> <prefix>.<operation>. . .]
```


où

- <prefix>

  est un point d'ancrage pour le démarrage d'une expression.

  Le préfixe est une clé délimitée par une période qui identifie une unité de données. Par exemple, le préfixe suivant examine les requêtes HTTP pour la présence d'un en-tête nommé Content-Type :

  http.req.header (« Content-Type »)

  Les préfixes peuvent également être utilisés seuls pour renvoyer la valeur de l'objet que le préfixe identifie.

- <operation>

  identifie une évaluation à effectuer sur les données identifiées par le préfixe.

  Par exemple, considérez l'expression suivante :

  http.req.header("Content-Type").eq("text/html")

  Dans cette expression, ce qui suit est le composant opérateur :

  eq("text/html")

  Cet opérateur fait en sorte que Citrix ADC évalue toutes les requêtes HTTP qui contiennent un en-tête Content-Type, et en particulier, détermine si la valeur de cet en-tête est égale à la chaîne "text/html". Pour plus d'informations, voir « Opérations ». «

- <compound-operator>

  est un opérateur booléen ou arithmétique qui forme une expression composée à partir de plusieurs éléments préfixes ou préfix.operation.

  Par exemple, considérez l'expression suivante :

  http.req.header("Content-Type").eq("text/html") && http.req.url.contains(".html")

Préfixes

Un préfixe d'expression représente une donnée discrète. Par exemple, un préfixe d'expression peut représenter une URL HTTP, un en-tête de cookie HTTP ou une chaîne dans le corps d'une requête HTTP POST. Un préfixe d'expression peut identifier et renvoyer une grande variété de types de données, notamment les suivants :

- Une adresse IP du client dans un paquet TCP/IP
- Heure système Citrix ADC
- Une légende externe sur HTTP
- Type d'enregistrement TCP ou UDP

Dans la plupart des cas, un préfixe d'expression commence par l'un des mots-clés suivants :

- CLIENT:
  - Identifie une caractéristique du client qui envoie une demande ou reçoit une réponse, comme dans les exemples suivants :
  - Le préfixe client.ip.dst désigne l'adresse IP de destination dans la requête ou la réponse.
  - Le préfixe client.ip.src désigne l'adresse IP source.
- HTTP:
  - Identifie un élément dans une requête HTTP ou une réponse, comme dans les exemples suivants :
  - Le préfixe http.req.body (integer) désigne le corps de la requête HTTP comme un objet texte multiligne, jusqu'à la position du caractère désignée dans un entier.
  - Le préfixe http.req.header (« header_name ») désigne un en-tête HTTP, comme spécifié dans header_name.
  - Le préfixe http.req.url désigne une URL HTTP au format URL.
- SERVER:

  Identifie un élément du serveur qui traite une demande ou envoie une réponse.
- SYS:

  Identifie une caractéristique de Citrix ADC qui traite le trafic.

  Remarque : Notez que les stratégies DNS prennent en charge uniquement les objets SYS, CLIENT et SERVER.

  En outre, dans Citrix Gateway, la fonction VPN sans client peut utiliser les types de préfixes suivants :
- TEXT:

  Identifie tout élément de texte dans une requête ou une réponse.
- CIBLE :

  Identifie la cible d'une connexion.
- URL :

  Identifie un élément dans la partie URL d'une requête ou d'une réponse HTTP.

En règle générale, tout préfixe d'expression peut être une expression autonome. Par exemple, le préfixe suivant est une expression complète qui renvoie le contenu de l'en-tête HTTP spécifié dans l'argument chaîne (entre guillemets) :

```
http.res.header.("myheader")
```


Ou vous pouvez combiner des préfixes avec des opérations simples pour déterminer les valeurs TRUE et FALSE. Par exemple, ce qui suit renvoie une valeur TRUE ou FALSE :

```
http.res.header.("myheader").exists
```

Vous pouvez également utiliser des opérations complexes sur des préfixes individuels et plusieurs préfixes au sein d'une expression, comme dans l'exemple suivant :

```
http.req.url.length + http.req.cookie.length <= 500
```

Les préfixes d'expression que vous pouvez spécifier dépendent de la fonctionnalité Citrix ADC. Le tableau suivant décrit les préfixes d'expression qui présentent un intérêt sur une base par entité

Fonctionnalité	Types de préfixe d'expression utilisés dans la fonction
DNS	SYS, CLIENT, SERVER
Répondeur dans les fonctions de protection	HTTP, SYS, CLIENT
Commutation de contenu	HTTP, SYS, CLIENT
Réécrire	HTTP, SYS, CLIENT, SERVER, URL, TEXT, TARGET, VPN
Mise en cache intégrée	HTTP, SYS, CLIENT, SERVER
Citrix Gateway, accès sans client	HTTP, SYS, CLIENT, SERVER, URL, TEXT, TARGET, VPN

Tableau 1. Types autorisés de préfixes d'expression dans diverses fonctionnalités de Citrix ADC

Remarque : Pour plus d'informations sur les préfixes d'expression autorisés dans une fonction, reportez-vous à la documentation de cette fonction.

Expressions à un seul élément

Le type le plus simple d'expression de stratégie avancée contient un seul élément. Cet élément peut être l'un des éléments suivants :

- C'est vrai. Une expression de stratégie avancée peut simplement consister en la valeur true. Ce type d'expression renvoie toujours une valeur TRUE. Il est utile pour chaîner des actions de stratégie et déclencher des expressions Goto.
- Faux. Une expression de stratégie avancée peut simplement consister en la valeur false. Ce type d'expression renvoie toujours une valeur FALSE.
- Préfixe d'une expression composée. Par exemple, le préfixe HTTP.REQ.HOSTNAME est une expression complète qui renvoie un nom d'hôte et HTTP.REQ.URL est une expression complète

qui renvoie une URL. Le préfixe peut également être utilisé conjointement avec des opérations et des préfixes supplémentaires pour former une expression composée.

Opérations

Dans la plupart des expressions, vous spécifiez également une opération sur les données identifiées par le préfixe. Par exemple, supposons que vous spécifiez le préfixe suivant :

```
http.req.url
```

Ce préfixe extrait les URL dans les requêtes HTTP. Ce préfixe d'expression ne nécessite pas l'utilisation d'opérateurs dans une expression. Toutefois, lorsque vous configurez une expression qui traite les URL de requête HTTP, vous pouvez spécifier des opérations qui analysent des caractéristiques particulières de l'URL. Voici quelques possibilités :

- Recherchez un nom d'hôte particulier dans l'URL.
- Recherchez un chemin particulier dans l'URL.
- Évaluez la longueur de l'URL.
- Recherchez une chaîne dans l'URL qui indique un horodatage et convertissez-la en GMT.

Voici un exemple de préfixe qui identifie un en-tête HTTP nommé Serveur et une opération qui recherche la chaîne IIS dans la valeur d'en-tête :

```
http.res.header("Server").contains("IIS")
```

Voici un exemple de préfixe qui identifie les noms d'hôtes et une opération qui recherche la chaîne « www.mycompany.com » comme valeur du nom :

```
http.req.hostname.eq("www.mycompany.com")
```

Opérations de base sur les préfixes d'expression

Le tableau suivant décrit quelques-unes des opérations de base qui peuvent être effectuées sur les préfixes d'expression.

Opération	Détermine si oui ou non
CONTAINS(<string>)	L'objet correspond <string>. Voici un exemple : http.req.header (« Cache-Control ») .contains (« no-cache »)
EXISTS	Un élément particulier est présent dans un objet. Voici un exemple : http.res.header (« myHDR ») .exists

Opération	Détermine si oui ou non
EQ(<text>)	Une valeur non numérique particulière est présente dans un objet. Voici un exemple : http.req.method.eq (post)
EQ(<integer>)	Une valeur numérique particulière est présente dans un objet. Voici un exemple : client.ip.dst.eq (10.100.10.100)
LT (<integer>)	La valeur d'un objet est inférieure à une valeur particulière. Voici un exemple : http.req.content_length.lt (5000)
GT (<integer>)	La valeur d'un objet est supérieure à une valeur particulière. Voici un exemple : http.req.content_length.gt (5)

Le tableau suivant résume quelques-uns des types d'opérations disponibles.

Type d'opération	Description
Opérations de texte	Faites correspondre des chaînes individuelles et des ensembles de chaînes avec n'importe quelle partie d'une cible. La cible peut être une chaîne entière, le début d'une chaîne ou n'importe quelle partie du texte entre le début et la fin de la chaîne. Par exemple, vous pouvez extraire la chaîne « XYZ » de « XYZSomeText ». Ou, vous pouvez comparer une valeur d'en-tête HTTP avec un tableau de chaînes différentes. Vous pouvez également transformer du texte en un autre type de données. Voici des exemples : Transformer une chaîne en une valeur entière, créer une liste à partir des chaînes de requête dans une URL et transformer une chaîne en une valeur de temps.

Type d'opération	Description
Opérations numériques	Les opérations numériques incluent l'application d'opérateurs arithmétiques, l'évaluation de la longueur du contenu, le nombre d'éléments dans une liste, les dates, les heures et les adresses IP.

Expressions de stratégie avancées composées

October 5, 2021

Vous pouvez configurer une expression de stratégie avancée avec des opérateurs booléens ou arithmétiques et des opérations atomiques. L'expression composée suivante a un AND booléen :

```
http.req.hostname.eq("mycompany.com")&& http.req.method.eq(post)
```

L'expression suivante ajoute la valeur de deux cibles et compare le résultat à une troisième valeur :

```
http.req.url.length + http.req.cookie.length \<= 500
```

Une expression composée peut comporter un certain nombre d'opérateurs logiques et arithmétiques.

L'expression suivante évalue la longueur d'une requête HTTP. Cette expression est basée sur l'URL et le cookie.
Cette expression évalue le texte de l'en-tête. De plus, un AND booléen fait sur ces deux résultats :

```
http.req.url.length + http.req.cookie.length \<= 500 && http.req.header.
contains("some text")
```

Vous pouvez utiliser des parenthèses pour contrôler l'ordre d'évaluation dans une expression composée.

Booléens dans les expressions composées

Vous configurez des expressions composées à l'aide des opérateurs suivants :

- &&.

  Cet opérateur est un AND logique. Pour que l'expression soit évaluée à TRUE, tous les composants doivent être évalués à TRUE.

  Exemple :

  http.req.url.hostname.eq("myHost") && http.req.header("myHeader").exists

- ||.

  Cet opérateur est un OR logique. Si un composant de l'expression est évalué à TRUE, l'expression entière est TRUE.

- !.

  P N'est pas logique sur l'expression.

Parfois, l'utilitaire de configuration Citrix ADC propose des opérateurs AND, NOT et OR dans la boîte de dialogue **Ajouter une expression** . Toutefois, ces expressions composées sont d'une utilité limitée. Citrix vous recommande d'utiliser les opérateurs &&, || et ! Pour configurer des expressions composées utilisant la logique booléenne.

Parenthèses dans les expressions composées

Vous pouvez utiliser des parenthèses pour contrôler l'ordre d'évaluation d'une expression. Voici un exemple :

```
http.req.url.contains("myCompany.com")|| (http.req.url.hostname.eq("myHost"
)&& http.req.header("myHeader").exists)
```

Voici un autre exemple :

```
(http.req.header("Content-Type").exists && http.req.header("Content-Type").
eq("text/html"))|| (http.req.header("Transfer-Encoding").exists || http.req
.header("Content-Length").exists)
```

Opérations composées pour les chaînes

Le tableau suivant décrit les opérateurs que vous pouvez utiliser pour configurer des opérations composées sur des données de chaîne.

Opérations produisant une valeur de chaîne	Description
str +	Concatène la valeur de l'expression à gauche de l'opérateur avec la valeur à droite. Exemple : http.req.hostname + http.req.url.protocol
str + num	Concatène la valeur de l'expression à gauche de l'opérateur avec une valeur numérique à droite. Exemple : http.req.hostname + http.req.url.content_length

Opérations produisant une valeur de chaîne	Description
num + str	Concatène la valeur numérique de l'expression sur le côté gauche de l'opérateur avec une valeur de chaîne sur la droite. Exemple : http.req.url.content_length + http.req.url.hostname
str + ip	Concatène la valeur de chaîne de l'expression sur le côté gauche de l'opérateur avec une valeur d'adresse IP sur la droite. Exemple : http.req.hostname + 10.00.000.00
IP + str	Concatène la valeur de l'adresse IP de l'expression située à gauche de l'opérateur avec une valeur de chaîne à droite. Exemple : client.ip.dst + http.req.url.hostname
str1 ALT str2	Utilise string2 si l'évaluation de string1 entraîne une exception undef ou si le résultat est une chaîne nulle. Sinon, utilise string1 et n'évalue jamais string2. Exemple : ttp.req.hostname alt client.ip.src

Opérations sur les chaînes qui produisent un résultat de TRUE ou FALSE	Description
str == str	Évalue si les chaînes de chaque côté de l'opérateur sont identiques. Voici un exemple : http.req.header("myheader") == http.res.header("myheader")
str <= str	Évalue si la chaîne située à gauche de l'opérateur est identique à la chaîne de droite ou si elle la précède dans l'ordre alphabétique.
str >= str	Évalue si la chaîne située à gauche de l'opérateur est identique à la chaîne de droite ou si elle la suit dans l'ordre alphabétique.
str < str	Évalue si la chaîne située à gauche de l'opérateur précède la chaîne de droite dans l'ordre alphabétique.

Opérations sur les chaînes qui produisent un résultat de TRUE ou FALSE	Description
str > str	Évalue si la chaîne située à gauche de l'opérateur suit la chaîne de droite dans l'ordre alphabétique.
str !!= str	Évalue si les chaînes de chaque côté de l'opérateur sont différentes.

Opérations logiques sur les chaînes	Description
bool && bool	Cet opérateur est un AND logique. Lors de l'évaluation des composants de l'expression composée, tous les composants qui sont joints par le AND doivent être évalués à TRUE. Voici un exemple : http.req.method.eq(GET) && http.req.url.query.contains("viewReport && my_pagelabel")
bool || bool	Cet opérateur est un OR logique. Lors de l'évaluation des composants de l'expression composée, si un composant de l'expression appartenant à OR est évalué à TRUE, l'expression entière est TRUE. Voici un exemple : http.req.url.contains(".js") || http.res.header.("Content-Type"). Contains("javascript")
Bool	Effectue une opération NOT logique sur l'expression.

Opérations composées pour les nombres

Vous pouvez configurer des expressions numériques composées. Par exemple, l'expression suivante renvoie une valeur numérique qui est la somme d'une longueur d'en-tête HTTP et d'une longueur d'URL :

```
http.req.header.length + http.req.url.length
```

Les tableaux suivants décrivent les opérateurs que vous pouvez utiliser pour configurer des expressions composées pour des données numériques.

Opérations arithmétiques sur les nombres	Description
num + num	Ajoutez la valeur de l'expression à gauche de l'opérateur à la valeur de l'expression de droite. Voici un exemple : http.req.content_length + http.req.url.length
num — num	Soustrayez la valeur de l'expression à droite de l'opérateur de la valeur de l'expression à gauche.
num*num	Multipliez la valeur de l'expression à gauche de l'opérateur par la valeur de l'expression à droite. Voici un exemple : client.interface.rxthroughput* 9
num / num	Divisez la valeur de l'expression à gauche de l'opérateur par la valeur de l'expression à droite.
num% num	Calculez le modulo, ou le reste numérique sur une division de la valeur de l'expression à gauche de l'opérateur par la valeur de l'expression à droite. Par exemple, les valeurs « 15 mod 4" sont égales à 3 et « 12 mod 4" sont égales à 0.
~number	Renvoie un nombre après avoir appliqué une négation logique bit à bit du nombre. L'exemple suivant suppose que numeric.expression renvoie 12 (binaire 1100) : ~numeric.expression. Le résultat de l'application de l'opérateur ~ est -11 (un binaire 1110011, 32 bits au total avec tous ceux à gauche). Notez que toutes les valeurs renvoyées de moins de 32 bits avant l'application de l'opérateur ont implicitement des zéros à gauche pour les rendre larges de 32 bits.

Opérations arithmétiques sur les nombres	Description
number ^ number	Compare deux modèles de bits de même longueur et effectue une opération XOR sur chaque paire de bits correspondants dans chaque argument numérique, renvoyant 1 si les bits sont différents et 0 s'ils sont identiques. Renvoie un nombre après avoir appliqué un XOR bit à bit à l'argument entier et à la valeur numérique courante. Si les valeurs de la comparaison bit à bit sont identiques, la valeur renvoyée est 0. L'exemple suivant suppose que numeric.expression1 renvoie 12 (binaire 1100) et numeric.expression2 renvoie 10 (binaire 1010) : numeric.expression1 ^ numeric.expression2Le résultat de l'application de l'opérateur ^ à l'ensemble de l'expression est 6 (binaire 0110). Notez que toutes les valeurs renvoyées de moins de 32 bits avant l'application de l'opérateur ont implicitement des zéros à gauche pour les rendre larges de 32 bits.
number | number	Renvoie un nombre après avoir appliqué un OR bit à bit aux valeurs numériques. Si l'une des valeurs de la comparaison bit à bit est 1, la valeur renvoyée est 1. L'exemple suivant suppose que numeric.expression1 renvoie 12 (binaire 1100) et numeric.expression2 renvoie 10 (binaire 1010) : numeric.expression1 | numeric.expression2 Le résultat de l'application de l'opérateur | à l'ensemble de l'expression est 14 (binaire 1110). Notez que toutes les valeurs renvoyées de moins de 32 bits avant l'application de l'opérateur ont implicitement des zéros à gauche pour les rendre larges de 32 bits.

Opérations arithmétiques sur les nombres	Description
number & number	Compare deux modèles de bits de même longueur et effectue une opération AND bit à bit sur chaque paire de bits correspondants, renvoyant 1 si les deux bits contiennent une valeur de 1, et 0 si l'un des bits est égal à 0. L'exemple suivant suppose que numeric.expression1 renvoie 12 (binaire 1100) et numeric.expression2 renvoie 10 (binaire 1010) : numeric.expression1 & numeric.expression2 L'expression entière est évaluée à 8 (binaire 1000). Notez que toutes les valeurs renvoyées de moins de 32 bits avant l'application de l'opérateur ont implicitement des zéros à gauche pour les rendre larges de 32 bits.
num « num	Renvoie un nombre après un décalage vers la gauche de la valeur de nombre par le nombre d'arguments de droite nombre de bits. Notez que le nombre de bits décalés est un entier modulo 32. L'exemple suivant suppose que numeric.expression1 renvoie 12 (binaire 1100) et numeric.expression2 renvoie 3 : numeric.expression1 « numeric.expression2 Le résultat de l'application de l'opérateur LSHIFT est 96 (un binaire 1100000) .Notez que toutes les valeurs renvoyées sont inférieures à 32 bits avant d'appliquer l'opérateur ont implicitement des zéros à gauche pour leur donner une largeur de 32 bits.

Opérations arithmétiques sur les nombres	Description
num » num	Retourne un nombre après un décalage vers la droite du bit de la valeur du nombre par le nombre entier d'argument de bits. Notez que le nombre de bits décalés est un entier modulo 32. L'exemple suivant suppose que numeric.expression1 renvoie 12 (binaire 1100) et numeric.expression2 renvoie 3 : numeric.expression1 » numeric.expression2 Le résultat de l'application de l'opérateur RSHIFT est 1 (un binaire 0001). Notez que toutes les valeurs renvoyées de moins de 32 bits avant l'application de l'opérateur ont implicitement des zéros à gauche pour les rendre larges de 32 bits.

Opérateurs numériques qui produisent un résultat de TRUE ou FALSE	Description
———–	———————————————————————————
num == num	Déterminez si la valeur de l'expression à gauche de l'opérateur est égale à la valeur de l'expression à droite.
num! = num	Déterminez si la valeur de l'expression située à gauche de l'opérateur n'est pas égale à la valeur de l'expression à droite.	
num > num	Déterminez si la valeur de l'expression située à gauche de l'opérateur est supérieure à la valeur de l'expression à droite.
num < num	Déterminez si la valeur de l'expression située à gauche de l'opérateur est inférieure à la valeur de l'expression à droite.
num >= num	Déterminez si la valeur de l'expression située à gauche de l'opérateur est supérieure ou égale à la valeur de l'expression à droite.
num <= num	Déterminez si la valeur de l'expression située à gauche de l'opérateur est inférieure ou égale à la valeur de l'expression à droite

Fonctions pour les types de données dans l'infrastructure de stratégie

L'infrastructure de stratégie Citrix ADC prend en charge les types de données numériques suivants :

- Entier (32 bits)
- Long non signé (64 bits)
- Double (64 bits)

Les expressions simples peuvent renvoyer tous ces types de données. Vous pouvez également créer des expressions composées qui utilisent des opérateurs arithmétiques et des opérateurs logiques pour évaluer ou renvoyer les valeurs de ces types de données. Vous pouvez également utiliser toutes ces valeurs dans des expressions de stratégie. Les constantes littérales de type unsigned long peuvent être spécifiées en ajoutant la chaîne ul au nombre. Les constantes littérales de type double contiennent un point (.), un exposant ou les deux.

Opérateurs arithmétiques, opérateurs logiques et promotion de type

Dans les expressions composées, les opérateurs arithmétiques et logiques standard suivants peuvent être utilisés pour les types de données longues doubles et non signées :

- +, -, * et/
- %, ~, ^, &, |, «, et » (ne s'appliquent pas au double)
- ==, ! =, >, <, >= et <=

Tous ces opérateurs ont la même signification que dans le langage de programmation C.

Dans tous les cas d'opérations mixtes entre des opérandes de type entier, long non signé et double. La promotion de type est effectuée pour effectuer l'opération sur les opérandes du même type. L'opération promeut un type de priorité inférieure à l'opérande ayant le type de priorité la plus élevée. L'ordre de priorité (supérieur à inférieur) est le suivant :

- Double
- Long non signé
- Nombre entier

Ainsi, une opération qui renvoie un résultat numérique renvoie un résultat du type le plus élevé impliqué dans l'opération.

Par exemple, si les opérandes sont de type entier et non signé long, l'opérande entier est automatiquement converti en type unsigned long. Cette conversion de type s'effectue dans des expressions simples. Le type de données identifié par le préfixe d'expression ne correspond pas au type de données transmises en tant qu'argument à la fonction. Dans l'opération HTTP.REQ.CONTENT_LENGTH.DIV (3ul), le préfixe HTTP.REQ.CONTENT_LENGTH.DIV renvoie un entier qui devient long non signé. Long non signé : le type de données transmis comme argument à la fonction DIV (), une division longue non signée est effectuée. De même, l'argument peut être promu dans une expression. Par exemple, HTTP.REQ.HEADER (« MyHeader ») .TYPECAST_DOUBLE_AT.DIV (5) promeut l'entier 5 à taper double et effectue une division à double précision.

Pour plus d'informations sur les expressions permettant de transférer des données d'un type vers des données d'un autre type, reportez-vous à la section Données de typage.

Spécifier le jeu de caractères dans les expressions

August 20, 2021

L'infrastructure de stratégie de l'appliance Citrix ADC prend en charge les jeux de caractères ASCII et UTF-8. Le jeu de caractères par défaut est ASCII. Si le trafic pour lequel vous configurez une expression se compose uniquement de caractères ASCII, vous n'avez pas besoin de spécifier le jeu de caractères dans l'expression. L'appliance autorise tous les littéraux de chaînes et de caractères qui incluent des caractères binaires. Cependant, les jeux de caractères UTF-8 nécessitent toujours que les littéraux de chaîne et de caractères soient un UTF-8 valide.

```
CLIENT.TCP.PAYLOAD(100).CONTAINS("\xff\x02")
```

Dans une expression, la fonction SET_CHAR_SET () doit être introduite au point de l'expression après quoi le traitement des données doit être effectué dans le jeu de caractères spécifié. Par exemple, dans l'expression HTTP.REQ.BODY(1000).AFTER_REGEX(re/following example/).BEFORE_REGEX(re/In the preceding example/).CONTAINS_ANY("Greek_ alphabet"), si les chaînes stockées dans le jeu de motifs "Greek_Alphabet" sont en UTF-8, vous devez inclure la fonction SET_CHAR_SET (UTF_8) immédiatement avant la fonction CONTAINS_ANY("<string>"), comme suit :

```
HTTP.REQ.BODY(1000).AFTER_REGEX(re/following example/).BEFORE_REGEX(re/In
the preceding example/).SET_CHAR_SET(UTF_8).CONTAINS_ANY("Greek_ alphabet")
```

La fonction SET_CHAR_SET () définit le jeu de caractères pour tout traitement ultérieur (c'est-à-dire pour toutes les fonctions suivantes) dans l'expression, à moins qu'il ne soit remplacé plus tard dans l'expression par une autre fonction SET_CHAR_SET () qui modifie le jeu de caractères. Par conséquent, si toutes les fonctions d'une expression simple donnée sont destinées à UTF-8, vous pouvez inclure la fonction SET_CHAR_SET (UTF_8) immédiatement après les fonctions qui identifient le texte (par exemple, les <name> <int> fonctions HEADER (» «) ou BODY ()). Dans le deuxième exemple qui suit le premier paragraphe ci-dessus, si les arguments ASCII transmis aux fonctions AFTER_REGEX () et BEFORE_REGEX () sont remplacés par des chaînes UTF-8, vous pouvez inclure la fonction SET_CHAR_SET (UTF_8) immédiatement après la fonction BODY (1000), comme suit :

```
HTTP.REQ.BODY(1000).SET_CHAR_SET(UTF_8).AFTER_REGEX(re/Bücher/).BEFORE_REGEX
(re/Wörterbuch/).CONTAINS_ANY("Greek_alphabet")
```

Le jeu de caractères UTF-8 est un surensemble du jeu de caractères ASCII, de sorte que les expressions configurées pour le jeu de caractères ASCII continuent de fonctionner comme prévu si vous modifiez le jeu de caractères en UTF-8.

Expressions composées avec différents jeux de caractères

Dans une expression composée, si un sous-ensemble d'expressions est configuré pour fonctionner avec des données du jeu de caractères ASCII et que le reste des expressions est configuré pour fonc-

tionner avec des données du jeu de caractères UTF-8, le jeu de caractères spécifié pour chaque expression individuelle est pris en compte lors de l'évaluation des expressions individuellement. Toutefois, lors du traitement de l'expression composée, juste avant le traitement des opérateurs, l'appliance promeut le jeu de caractères des valeurs ASCII renvoyées en UTF-8. Par exemple, dans l'expression composée suivante, la première expression simple évalue les données du jeu de caractères ASCII tandis que la seconde expression simple évalue les données du jeu de caractères UTF-8 :

```
HTTP.REQ.HEADER("MyHeader")== HTTP.REQ.BODY(10).SET_CHAR_SET(UTF_8)
```

Cependant, lors du traitement de l'expression composée, juste avant d'évaluer l'opérateur booléen « est égal à », l'appliance Citrix ADC promeut le jeu de caractères de la valeur renvoyée par HTTP.REQ.HEADER (« myHeader ») en UTF-8.

La première expression simple de l'exemple suivant évalue les données du jeu de caractères ASCII. Toutefois, lorsque l'appliance Citrix ADC traite l'expression composée, juste avant de concaténer les résultats des deux expressions simples, l'appliance promeut le jeu de caractères de la valeur renvoyée par HTTP.REQ.BODY (10) en UTF-8.

```
HTTP.REQ.BODY(10)+ HTTP.REQ.HEADER("MyHeader").SET_CHAR_SET(UTF_8)
```

Par conséquent, l'expression composée renvoie des données dans le jeu de caractères UTF-8.

Spécifier le jeu de caractères en fonction du jeu de caractères du trafic

Vous pouvez définir le jeu de caractères sur UTF-8 en fonction des caractéristiques de trafic. Si vous ne savez pas si le jeu de caractères du trafic évalué est UTF-8, vous pouvez configurer une expression composée dans laquelle la première expression vérifie le trafic UTF-8 et les expressions suivantes définissent le jeu de caractères à UTF-8. Voici un exemple d'expression composée qui vérifie d'abord la valeur de « charset » dans l'en-tête Content-Type de la requête pour « UTF-8" avant de vérifier si les 1000 premiers octets de la requête contiennent la chaîne UTF-8 Bücher :

```
HTTP.REQ.HEADER("Content-Type").SET_TEXT_MODE(IGNORECASE).TYPECAST_NVLIST_T
('=', '; ', '"').VALUE("charset").EQ("UTF-8")&& HTTP.REQ.BODY(1000).SET_CHAR_SET
(UTF_8).CONTAINS("Bücher")
```

Si vous êtes sûr que le jeu de caractères du trafic évalué est UTF-8, la deuxième expression de l'exemple est suffisante.

Littéraires de caractères et de chaîne dans les expressions

Lors de l'évaluation de l'expression, même si le jeu de caractères actuel est ASCII, les littéraux de caractères et les littéraux de chaîne, qui sont respectivement placés entre guillemets simples (‘’) et guillemets (« »), sont considérés comme des littéraux dans le jeu de caractères UTF-8. Dans une expression donnée, si une fonction fonctionne sur des littéraux de caractères ou de chaîne dans le jeu de caractères ASCII et que vous incluez un caractère non ASCII dans le littéral, une erreur est renvoyée.

> **Remarque** :
>
> Les littéraux de chaîne dans les expressions de stratégie avancées sont maintenant aussi longs que l'expression de stratégie. L'expression peut avoir une longueur de 1499 octets ou 8191 octets.

Valeurs en formats hexadécimaux et octaux

Lors de la configuration d'une expression, vous pouvez entrer des valeurs au format octal et hexadécimal. Cependant, chaque octet hexadécimal ou octal est considéré comme un octet UTF-8. Les octets UTF-8 non valides entraînent des erreurs, que la valeur soit saisie manuellement ou collée à partir du presse-papiers. Par exemple, "\xce\x20" est un caractère UTF-8 non valide car "c8" ne peut pas être suivi de "20" (chaque octet d'une chaîne UTF-8 multi-octets doit avoir le bit élevé). Un autre exemple de caractère UTF-8 non valide est "\xce \xa9", puisque les caractères hexadécimaux sont séparés par un caractère d'espace blanc.

Fonctions qui retournent des chaînes UTF-8

Seules les fonctions `text>.XPATH` et `<text>.XPATH_JSON` et renvoient toujours les chaînes UTF-8. Les routines MYSQL suivantes déterminent au moment de l'exécution le jeu de caractères à renvoyer, en fonction des données du protocole :

- `MYSQL_CLIENT_T.USER`
- `MYSQL_CLIENT_T.DATABASE`
- `MYSQL_REQ_QUERY_T.COMMAND`
- `MYSQL_REQ_QUERY_T.TEXT`
- `MYSQL_REQ_QUERY_T.TEXT(<unsigned int>)`
- `MYSQL_RES_ERROR_T.SQLSTATE`
- `MYSQL_RES_ERROR_T.MESSAGE`
- `MYSQL_RES_FIELD_T.CATALOG`
- `MYSQL_RES_FIELD_T.DB`
- `MYSQL_RES_FIELD_T.TABLE`
- `MSQL_RES_FIELD_T.ORIGINAL_TABLE`
- `MYSQL_RES_FIELD_T.NAME`
- `MYSQL_RES_FIELD_T.ORIGINAL_NAME`
- `MYSQL_RES_OK_T.MESSAGE`
- `MYSQL_RES_ROW_T.TEXT_ELEM(<unsigned int>)`

Paramètres de connexion du terminal pour UTF-8

Lorsque vous configurez une connexion à l'appliance Citrix ADC à l'aide d'une connexion de terminal (à l'aide de PuTTY, par exemple), vous devez définir le jeu de caractères pour la transmission des données

en UTF-8.

Fonctions minimales et maximales dans une expression de stratégie avancée

Les expressions de stratégie avancées prennent en charge les fonctions minimales et maximales ci-dessous.

1. (<expression1>.max(<expression2>) - renvoie le maximum des deux valeurs.
2. (<expression1>.min(<expression2>) - renvoie le minimum des deux valeurs.

Expressions classiques dans les expressions de stratégie avancées

August 20, 2021

> **Avertissement :**
>
> Les expressions de stratégie classiques ne sont plus prises en charge à partir de Citrix ADC 12.0 build 56.20 et à titre d'alternative, Citrix vous recommande d'utiliser des stratégies avancées. Pour plus d'informations, voir Configurer les expressions de stratégie avancées : Pour commencer.

Les expressions classiques décrivent les caractéristiques de base du trafic. Parfois, vous pouvez utiliser une expression classique dans une expression de stratégie avancée.

Voici la syntaxe de toutes les expressions de stratégie avancées qui utilisent une expression classique :

SYS.EVAL_CLASSIC_EXPR("expression")

> **Remarque :**
>
> La syntaxe et les métadonnées de l'expression SYS.EVAL_CLASSIC_EXPR sont obsolètes. Vous pouvez convertir manuellement ou utiliser l'outil nspepi pour convertir l'expression classique en expression avancée.

Voici des exemples de l'expression SYS.EVAL_CLASSIC_EXPR (« expression ») :

```
1 sys.eval_classic_expr("req.ssl.client.cipher.bits > 1000")
2 sys.eval_classic_expr("url contains abc")
3 sys.eval_classic_expr("req.ip.sourceip == 10.102.1.61 -netmask
     255.255.255.255")
4 sys.eval_classic_expr("time >= *:30:00GMT")
5 sys.eval_classic_expr("e1 || e2")
6 sys.eval_classic_expr("req.http.urllen > 50")
7 sys.eval_classic_expr("dayofweek == wedGMT")
8 <!--NeedCopy-->
```


> **Remarque :**
>
> Lorsque vous mettez à niveau Citrix ADC vers la version 9.0 ou ultérieure, les stratégies de mise en cache intégrée sont automatiquement mises à niveau vers des stratégies avancées et les expressions de ces stratégies sont mises à niveau vers les stratégies avancées.

Configuration des expressions de stratégie avancées dans une stratégie

October 5, 2021

Vous pouvez configurer une expression de stratégie avancée comportant jusqu'à 1 499 caractères dans une stratégie. L'interface utilisateur des expressions de stratégie avancées dépend dans une certaine mesure de la fonctionnalité pour laquelle vous configurez l'expression et de la configuration d'une expression pour une stratégie ou pour une autre utilisation.

Lorsque vous configurez des expressions sur la ligne de commande, vous les délimitez en utilisant des guillemets («.. » ou «.. »). Dans une expression, vous échappez les guillemets supplémentaires à l'aide d'une barre oblique inverse (). Par exemple, les méthodes standard suivantes permettent d'échapper les guillemets dans une expression :

```
"\"abc\""
```

```
'\"abc\"'
```

Vous devez également utiliser une barre oblique inverse pour échapper les points d'interrogation et autres barres obliques inverses sur la ligne de commande. Par exemple, l'expression http.req.url.contains (« ? ») nécessite une barre oblique inverse pour que le point d'interrogation soit analysé. Notez que la barre oblique inverse n'apparaîtra pas sur la ligne de commande après avoir tapé le point d'interrogation. En revanche, si vous échappez une barre oblique inverse (par exemple, dans l'expression 'http.req.url.contains (« \ \ http ») '), les caractères d'échappement sont repris en écho sur la ligne de commande.

Pour rendre une entrée plus lisible, vous pouvez échapper les guillemets pour une expression entière. Au début de l'expression, vous entrez la séquence d'échappement « q » plus l'un des caractères spéciaux suivants :/{<	~$^+=&%@' ?.

Vous n'entrez que le caractère spécial à la fin de l'expression, comme suit :

```
1 q@http.req.url.contains("sometext") && http.req.cookie.exists@
2
```



```
q~http.req.url.contains("sometext") && http.req.cookie.exists~
<!--NeedCopy-->
```

Notez qu'une expression qui utilise le délimiteur {est fermée par}.

Pour certaines fonctionnalités (par exemple, Integrated Caching and Responder), la boîte de dialogue de configuration de stratégie fournit une boîte de dialogue secondaire pour configurer les expressions. Cette boîte de dialogue vous permet de choisir parmi des listes déroulantes qui affichent les choix disponibles à chaque étape de la configuration de l'expression. Vous ne pouvez pas utiliser d'opérateurs arithmétiques lorsque vous utilisez ces boîtes de dialogue de configuration, mais la plupart des autres fonctionnalités avancées d'expression de stratégie sont disponibles. Pour utiliser des opérateurs arithmétiques, écrivez vos expressions au format libre.

Configurer une règle de syntaxe de stratégie avancée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une règle de stratégie avancée et vérifier la configuration :

1. `add cache|dns|rewrite|cs policyName **-rule** expression featureSpecificParameter **-action**`
2. `show cache|dns|rewrite|cs policyName`
   Voici un exemple de configuration d'une stratégie de mise en cache :

   Exemple :

```
> add cache policy pol-cache -rule http.req.content_length.le(5) -
    action INVAL
 Done

> show cache policy pol-cache
        Name: pol-cache
        Rule: http.req.content_length.le(5)
        CacheAction: INVAL
        Invalidate groups: DEFAULT
        UndefAction: Use Global
        Hits: 0
        Undef Hits: 0

 Done
<!--NeedCopy-->
```


Configurer une expression de stratégie avancée à l'aide de l'interface graphique

1. Dans le volet de navigation, cliquez sur le nom de l'entité pour laquelle vous souhaitez configurer une stratégie. Par exemple, vous pouvez sélectionner Mise en cache intégrée, Répondeur, DNS, Réécriture ou Changement de contenu, puis cliquez sur **Stratégies**.
2. Cliquez sur Ajouter.
3. Pour la plupart des fonctionnalités, cliquez sur dans le champ **Expression** . Pour le changement de contenu, cliquez sur **Configurer**.
4. Cliquez sur l'icône **Préfixe** (la maison) et sélectionnez le premier préfixe d'expression dans la liste déroulante. Par exemple, dans Responder, les options sont HTTP, SYS et CLIENT. Le prochain ensemble d'options applicables apparaît dans une liste déroulante.
5. Double-cliquez sur l'option suivante pour la sélectionner, puis tapez un point (.). Encore une fois, un ensemble d'options applicables apparaît dans une autre liste déroulante.
6. Continuez à sélectionner les options jusqu'à ce qu'un champ de saisie (signalé par des parenthèses) apparaisse. Lorsque vous voyez un champ de saisie, saisissez une valeur appropriée entre parenthèses. Par exemple, si vous sélectionnez GT (int) (format entier supérieur à), vous spécifiez un entier entre parenthèses. Les chaînes de texte sont délimitées par des guillemets. Voici un exemple :

   ```
   HTTP.REQ.BODY(1000).BETWEEN("this","that")
   ```

7. Pour insérer un opérateur entre deux parties d'une expression composée, cliquez sur l'icône Opérateurs (le sigma), puis sélectionnez le type d'opérateur. Voici un exemple d'expression configurée avec un OR booléen (signalé par des barres verticales doubles, ||) :

   ```
   HTTP.REQ.URL.EQ("www.mycompany.com")||HTTP.REQ.BODY(1000).BETWEEN("this
   ","that")
   ```

8. Pour insérer une expression nommée, cliquez sur la flèche vers le bas en regard de l'icône Ajouter (signe plus) et sélectionnez une expression nommée.
9. Pour configurer une expression à l'aide de menus déroulants et insérer des expressions intégrées, cliquez sur l'icône Ajouter (signe plus). La boîte de dialogue **Ajouter une expression** fonctionne de la même manière que la boîte de dialogue principale, mais elle fournit des listes déroulantes pour sélectionner des options et des champs de texte pour la saisie des données au lieu de parenthèses. Cette boîte de dialogue fournit également une liste déroulante Expressions fréquemment utilisées qui insère les expressions couramment utilisées. Lorsque vous avez terminé d'ajouter l'expression, cliquez sur **OK**.
10. Lorsque vous avez terminé, cliquez sur **Créer**. Un message dans la barre d'état indique que l'expression de stratégie est correctement configurée.

Test d'une expression de stratégie avancée à l'aide de l'interface graphique

1. Dans le volet de navigation, cliquez sur le nom de la fonctionnalité pour laquelle vous souhaitez configurer une stratégie (par exemple, vous pouvez sélectionner Mise en cache intégrée, Répondeur, DNS, Réécriture ou Changement de contenu), puis cliquez sur Stratégies.
2. Sélectionnez une stratégie, puis cliquez sur **Ouvrir**.
3. Pour tester l'expression, cliquez sur l'icône Evaluer (coche).
4. Dans la boîte de dialogue de l'évaluateur d'expression, sélectionnez le type de flux correspondant à l'expression.
5. Dans le champ **Données de demande HTTP** ou **Données de réponse HTTP**, collez la demande ou la réponse HTTP que vous souhaitez analyser avec l'expression, puis cliquez sur **Evaluer**. Notez que vous devez fournir une requête ou une réponse HTTP complète, et que l'en-tête et le corps doivent être séparés par une ligne vide. Certains programmes qui traquent les en-têtes HTTP ne traquent pas non plus la réponse. Si vous copiez et collez uniquement l'en-tête, insérez une ligne vide à la fin de l'en-tête pour former une requête ou une réponse HTTP complète.
6. Cliquez sur **Fermer** pour fermer cette boîte de dialogue.

Configuration des expressions de stratégie avancées nommées

October 5, 2021

Au lieu de retaper la même expression plusieurs fois dans plusieurs stratégies, vous pouvez configurer une expression nommée et faire référence au nom chaque fois que vous souhaitez utiliser l'expression dans une stratégie. Par exemple, vous pouvez créer les expressions nommées suivantes :

- Cette expression :

  ```
  http.req.body(100).contains("this")
  ```

- Cette expression :

  ```
  http.req.body(100).contains("that")
  ```

Vous pouvez ensuite utiliser ces expressions nommées dans une expression de stratégie. Par exemple, voici une expression juridique basée sur les exemples précédents :

Cette expression	Cette expression

Vous pouvez utiliser le nom d'une expression de stratégie avancée comme préfixe d'une fonction. L'expression nommée peut être une expression simple ou une expression composée. La fonction doit être capable d'opérer sur le type de données renvoyé par l'expression nommée.

Exemple 1 : expression nommée simple en tant que préfixe

L'expression nommée simple suivante, qui identifie une chaîne de texte, peut être utilisée comme préfixe de la <string>fonction AFTER_STR (» «), qui fonctionne avec des données de texte :

```
HTTP.REQ.BODY(1000)
```

Si le nom de l'expression est Top1Ko, vous pouvez utiliser Top1KB.after_str (« username ») au lieu de HTTP.REQ.BODY (1000) .AFTER_STR (« username »).

Exemple 2 : expression nommée composée en tant que préfixe

Vous pouvez créer une expression nommée composée appelée basic_header_value pour concaténer le nom d'utilisateur dans une requête, un signe deux-points (:) et le mot de passe de l'utilisateur, comme suit :

```
add policy expression basic_header_value "HTTP.REQ.USER.NAME + \":\" + HTTP
.REQ.USER.PASSWD"
```

Vous pouvez ensuite utiliser le nom de l'expression dans une action de réécriture, comme illustré dans l'exemple suivant :

```
add rewrite action insert_b64encoded_authorization insert_http_header
authorization '"Basic " + basic_header_value.b64encode'
```

Dans cet exemple, dans l'expression utilisée pour construire la valeur de l'en-tête personnalisé, l'algorithme de codage B64 est appliqué à la chaîne renvoyée par l'expression nommée composée.

Vous pouvez également utiliser une expression nommée (seule ou comme préfixe d'une fonction) pour créer l'expression de texte de la cible de remplacement lors d'une réécriture.

Configurez une expression de stratégie avancée nommée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une expression nommée et vérifier la configuration :

```
1 -  add policy expression <name><value>
2
3 -  show policy expression <name>
4 <!--NeedCopy-->
```

Exemple :

```
1 > add policy expression myExp "http.req.body(100).contains("the other")
     "
```



```
Done

> show policy expression myExp
    1)      Name: myExp  Expr: "http.req.body(100).contains("the other"
       )"  Hits: 0 Type : ADVANCED
Done
<!--NeedCopy-->
```

L'expression peut contenir jusqu'à 1 499 caractères.

Configurer une expression nommée à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **AppExpert**, puis cliquez sur **Expressions**.
2. Cliquez sur **Expressions avancées**.
3. Cliquez sur **Ajouter**.
4. Entrez un nom et une description pour l'expression.
5. Configurez l'expression à l'aide du processus décrit dans Configurer l'expression de stratégie avancée. Un message dans la barre d'état indique que l'expression de stratégie est correctement configurée.

Configurer des expressions de stratégie avancées en dehors du contexte d'une stratégie

August 20, 2021

Un certain nombre de fonctions, notamment les suivantes, peuvent nécessiter une expression de stratégie avancée qui ne fait pas partie d'une stratégie :

- Sélecteurs de mise en cache intégrés :

  Vous définissez plusieurs expressions non composées (sélections) dans la définition du sélecteur. Chaque sélecteur est dans une relation logique implicite ET avec les autres.

- Équilibrage de charge :

  Vous configurez une expression pour la méthode TOKEN d'équilibrage de charge pour un serveur virtuel d'équilibrage de charge.

- Actions de réécriture :

  Les expressions définissent l'emplacement de l'action de réécriture et le type de réécriture à effectuer, selon le type d'action de réécriture que vous configurez. Par exemple, une action

DELETE utilise uniquement une expression cible. Une action REPLACE utilise une expression cible et une expression pour configurer le texte de remplacement.

- Stratégies basées sur des taux :

  Vous utilisez des expressions de stratégie avancées pour configurer les sélecteurs de limite. Vous pouvez utiliser ces sélecteurs lors de la configuration de stratégies pour étrangler le débit de trafic vers différents serveurs. Vous définissez jusqu'à cinq expressions non composées (sélections) dans la définition du sélecteur. Chaque sélecteur est dans un ET logique implicite avec les autres.

Configurer une expression de stratégie avancée en dehors d'une stratégie à l'aide de l'interface de ligne de commande (exemple de sélection de cache)

À l'invite de commandes, tapez les commandes suivantes pour configurer une expression de stratégie avancée en dehors d'une stratégie et vérifier la configuration :

```
1 -  add cache selector <selectorName> <rule>
2 -  show cache selector <selectorName>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add cache selector mainpageSelector "http.req.cookie.value("ABC_def")
     "
2     "http.req.url.query.value("_ghi")"selector "mainpageSelector" added
3 Done
4 > show cache selector mainpageSelector
5             Name: mainpageSelector
6             Expressions:
7                     1) http.req.cookie.value("ABC_def")
8                     2) http.req.url.query.value("_ghi")
9 Done
10 <!--NeedCopy-->
```

Voici une commande équivalente qui utilise le délimiteur q le plus lisible, comme décrit dans Configurer les expressions de stratégie avancées dans une stratégie :

```
1 > add cache selector mainpageSelector2 q~http.req.cookie.value("ABC_def
     ")~
2     q~http.req.url.query.value("_ghi")~selector "mainpageSelector2"
        added
3 Done
4 > show cache selector mainpageSelector2
5             Name: mainpageSelector2
```



```
6               Expressions:
7                       1) http.req.cookie.value("ABC_def")
8                       2) http.req.url.query.value("_ghi")
9   Done
10  <!--NeedCopy-->
```

Expressions de stratégie avancées : évaluation du texte

January 21, 2021

Vous pouvez configurer une stratégie avec une expression de stratégie avancée qui évalue le texte d'une demande ou d'une réponse. Les expressions de texte de stratégie avancées peuvent aller des expressions simples qui effectuent la correspondance de chaînes dans les en-têtes HTTP aux expressions complexes qui encodent et décodent du texte. Vous pouvez configurer les expressions de texte pour qu'elles respectent la casse ou la casse et utiliser ou ignorer les espaces. Vous pouvez également configurer des expressions de texte complexes en combinant des expressions de texte avec des opérateurs booléens

Vous pouvez utiliser des préfixes d'expression et des opérateurs pour évaluer les requêtes HTTP, les réponses HTTP et les données VPN et VPN sans client. Toutefois, les préfixes d'expression de texte ne se limitent pas à évaluer ces éléments de votre trafic.

À propos des expressions de texte

October 5, 2021

Vous pouvez configurer diverses expressions pour travailler avec du texte qui passe par l'appliance Citrix ADC. Voici quelques exemples de la façon dont vous pouvez analyser du texte à l'aide d'une expression de stratégie avancée :

- Déterminez qu'il existe un en-tête HTTP particulier.

  Par exemple, vous pouvez souhaiter identifier les requêtes HTTP qui contiennent un en-tête Accept-Language particulier afin de diriger la demande vers un serveur particulier.

- Déterminez qu'une URL HTTP particulière contient une chaîne particulière.

  Par exemple, vous pouvez souhaiter bloquer les demandes pour des URL particulières. Notez que la chaîne peut apparaître au début, au milieu ou à la fin d'une autre chaîne.

- Identifiez une demande POST qui est dirigée vers une application particulière.

Par exemple, vous pouvez souhaiter identifier toutes les demandes POST qui sont dirigées vers une application de base de données dans le but d'actualiser les données d'application mises en cache.

Notez qu'il existe des outils spécialisés permettant de visualiser le flux de données des requêtes et réponses HTTP. Vous pouvez utiliser les outils pour afficher le flux de données.

À propos des opérations sur le texte

Une expression textuelle consiste en au moins un préfixe pour identifier un élément de données et généralement (mais pas toujours) une opération sur ce préfixe. Les opérations textuelles peuvent s'appliquer à n'importe quelle partie d'une demande ou d'une réponse. Les opérations de base sur le texte incluent différents types de correspondances de chaînes.

Par exemple, l'expression suivante compare une valeur d'en-tête à une chaîne :

```
http.req.header("myHeader").contains("some-text")
```

Les expressions suivantes sont des exemples de mise en correspondance d'un type de fichier dans une demande :

```
http.req.url.suffix.contains("jpeg")
```

```
http.req.url.suffix.eq("jpeg")
```

Dans les exemples précédents, l'opérateur contains autorise une correspondance partielle et l'opérateur eq recherche une correspondance exacte.

D'autres opérations sont disponibles pour formater la chaîne avant de l'évaluer. Par exemple, vous pouvez utiliser des opérations de texte pour supprimer les guillemets et les espaces blancs, pour convertir la chaîne en minuscules ou pour concaténer des chaînes.

> **Remarque** : Des opérations
>
> complexes sont disponibles pour effectuer des correspondances basées sur des motifs ou pour convertir un type de format de texte en un autre type.

Pour plus d'informations, consultez les rubriques suivantes :

- Jeux de modèles et jeux de données.
- Expressions régulières.
- Données de typographie.

Compilation et priorité dans les expressions de texte

Vous pouvez appliquer différents opérateurs pour combiner des préfixes de texte ou des expressions. Par exemple, l'expression suivante concatène les valeurs renvoyées pour chaque préfixe :


```
http.req.hostname + http.req.url
```

Voici un exemple d'expression de texte composé qui utilise un AND logique. Les deux composants de cette expression doivent avoir la valeur TRUE pour qu'une requête corresponde à l'expression :

```
http.req.method.eq(post)&& http.req.body(1024).startswith("destination=")
```

> **Remarque :**
>
> Pour plus d'informations sur les opérateurs de composition, voir Expressions avancées composées.

Catégories d'expressions de texte

Les principales catégories d'expressions de texte que vous pouvez configurer sont les suivantes :

- Informations dans les en-têtes HTTP, les URL HTTP et le corps POST dans les requêtes HTTP.

  Pour plus d'informations, voir Préfixes d'expression pour le texte dans les requêtes et réponses HTTP.

- Informations concernant un VPN ou un VPN sans client.

  Pour plus d'informations, consultez Préfixes d'expression pour les VPN et les VPN sans client.

- Informations sur la charge utile TCP.

  Pour plus d'informations sur les expressions de charge utile TCP, voir Expressions de stratégie avancées : analyse des données HTTP, TCP et UDP.

- Texte dans un certificat SSL (Secure Sockets Layer).

  Pour plus d'informations sur les expressions de texte pour les données de certificat SSL et SSL, voir Expressions de stratégie avancées : Analyse des certificats SSL et Expressions pour les dates de certificat SSL.

> **Remarque :**
>
> L'analyse d'un corps de document, tel que le corps d'une requête POST, peut affecter les performances. Vous pouvez tester l'impact sur les performances des stratégies qui évaluent le corps d'un document.

Instructions relatives aux expressions de texte

Du point de vue des performances, il est généralement préférable d'utiliser des fonctions prenant en charge le protocole dans une expression. Par exemple, l'expression suivante utilise une fonction prenant en charge le protocole :

```
HTTP.REQ.URL.QUERY
```


L'expression précédente fonctionne mieux que l'expression équivalente suivante, qui est basée sur l'analyse de chaînes :

```
HTTP.REQ.URL.AFTER_STR("?")
```

Dans le premier cas, l'expression se penche spécifiquement sur la requête URL. Dans le second cas, l'expression analyse les données à la recherche de la première occurrence d'un point d'interrogation.

Il y a également un avantage de performance de l'analyse structurée du texte, comme dans l'expression suivante :

```
HTTP.REQ.HEADER("Example").TYPECAST_LIST_T(',').GET(1)
```

(Pour plus d'informations sur la typographie, voir Données de typographie. L'expression de typecasting, qui recueille des données délimitées par des virgules et les structure en une liste, fonctionnerait généralement mieux que l'équivalent non structuré suivant :

```
HTTP.REQ.HEADER("Example").AFTER_STR(",").BEFORE_STR(",")
```

Enfin, les expressions textuelles non structurées présentent généralement de meilleures performances que les expressions régulières. Par exemple, voici une expression de texte non structurée :

```
HTTP.REQ.HEADER("Example").AFTER_STR("more")
```

L'expression précédente fournirait généralement de meilleures performances que l'équivalent suivant, qui utilise une expression régulière :

```
HTTP.REQ.HEADER("Example").AFTER_REGEX(re/more/)
```

Pour plus d'informations sur les expressions régulières, voir Expressions régulières.

Préfixes d'expression pour le texte dans les requêtes et réponses HTTP

August 20, 2021

Une requête ou une réponse HTTP contient généralement du texte, par exemple sous la forme d'en-têtes, de valeurs d'en-tête, d'URL et de corps de texte POST. Vous pouvez configurer des expressions pour qu'elles fonctionnent sur un ou plusieurs de ces éléments textuels dans une requête ou une réponse HTTP.

Reportez-vous au tableau Préfixe d'expression pour plus d'informations sur la configuration et l'extraction de texte à partir de différentes parties d'une requête ou d'une réponse HTTP.

Préfixes d'expression pour les VPN et les VPN sans client

August 20, 2021

Le moteur de stratégie avancé fournit des préfixes spécifiques à l'analyse des données VPN ou VPN sans client. Ces données comprennent les éléments suivants :

- Noms d'hôte, domaines et URL dans le trafic VPN.
- Protocoles dans le trafic VPN.
- Requêtes dans le trafic VPN.

Ces éléments de texte sont souvent des URL et des composants d'URL. En plus d'appliquer les opérations textuelles sur ces éléments, vous pouvez analyser ces éléments à l'aide d'opérations spécifiques à l'analyse des URL. Pour plus d'informations, voir Expressions pour extraire des segments d'URL.

Pour plus d'informations sur les préfixes d'expression VPN, reportez-vous au tableau des expressions VPN.

Opérations de base sur le texte

October 5, 2021

Les opérations de base sur le texte incluent les opérations de correspondance de chaînes, de calcul de la longueur d'une chaîne et de contrôle de la sensibilité à la casse. Vous pouvez inclure des espaces blancs dans une chaîne passée en tant qu'argument à une expression, mais la chaîne ne peut pas dépasser 255 caractères.

Fonctions de comparaison de chaînes

Le tableau suivant répertorie les opérations de correspondance de chaînes de base dans lesquelles les fonctions renvoient une valeur booléenne TRUE ou FALSE.

Fonction	Description
`<text>.CONTAINS(<string>)`	Renvoie une valeur booléenne TRUE si la cible contient `<string>`. Exemple : `http.req.url.contains(".jpeg")`
`<text>.EQ(<string>)`	Renvoie une valeur booléenne TRUE si la cible correspond exactement à `<string>`. Par exemple, l'expression suivante renvoie une valeur booléenne TRUE pour une URL dont le nom d'hôte est « myhostabc » : `http.req.url.hostname.eq("myhostabc")`

Fonction	Description
`<text>.STARTSWITH(<string>)`	Renvoie une valeur booléenne TRUE si la cible commence par `<string>`. Par exemple, l'expression suivante renvoie une valeur booléenne TRUE pour une URL dont le nom d'hôte est « myhostabc » : `http.req.url.hostname.startswith("myhost")`
`<text>.ENDSWITH(<string>)`	Renvoie une valeur booléenne TRUE si la cible se termine par<string>. Par exemple, l'expression suivante renvoie une valeur booléenne TRUE pour une URL dont le nom d'hôte est « myhostabc » : `http.req.url.hostname.endswith("abc")`
`<text>.NE(<string>)`	Renvoie une valeur booléenne TRUE si le préfixe n'est pas égal à l'argument de chaîne. Si le préfixe renvoie une valeur qui n'est pas une chaîne, l'argument de la fonction est comparé à la représentation sous forme de chaîne de la valeur renvoyée par le préfixe. Vous pouvez utiliser les fonctions avec `SET_TEXT_MODE(IGNORECASE)or SET_TEXT_MODE(NOIGNORECASE)` et avec les jeux de caractères ASCII et UTF-8.
`<text>.GT(<string>)`	Renvoie une valeur booléenne TRUE si le préfixe est alphabétiquement supérieur à l'argument de chaîne. Si le préfixe renvoie une valeur qui n'est pas une chaîne, l'argument de la fonction est comparé à la représentation sous forme de chaîne de la valeur renvoyée par le préfixe. Vous pouvez utiliser les fonctions avec `SET_TEXT_MODE(IGNORECASE)` ou `SET_TEXT_MODE(NOIGNORECASE)`, et avec les jeux de caractères ASCII et UTF-8.

Fonction	Description
`<text>.GE(<string>)`	Renvoie une valeur booléenne TRUE si le préfixe est alphabétiquement supérieur ou égal à l'argument de chaîne. Si le préfixe renvoie une valeur qui n'est pas une chaîne, l'argument de la fonction est comparé à la représentation sous forme de chaîne de la valeur renvoyée par le préfixe. Vous pouvez utiliser les fonctions avec `SET_TEXT_MODE(IGNORECASE)` ou `SET_TEXT_MODE(NOIGNORECASE)`, et avec les jeux de caractères ASCII et UTF-8.
`<text>.LT(<string>)`	Renvoie une valeur booléenne TRUE si le préfixe est alphabétiquement inférieur à l'argument chaîne. Si le préfixe renvoie une valeur qui n'est pas une chaîne, l'argument de la fonction est comparé à la représentation sous forme de chaîne de la valeur renvoyée par le préfixe. Vous pouvez utiliser les fonctions avec `SET_TEXT_MODE(IGNORECASE)` ou `SET_TEXT_MODE(NOIGNORECASE)`, et avec les jeux de caractères ASCII et UTF-8.
`<text>.LE(<string>)`	Renvoie une valeur booléenne TRUE si le préfixe est alphabétiquement inférieur ou égal à l'argument chaîne. Si le préfixe renvoie une valeur qui n'est pas une chaîne, l'argument de la fonction est comparé à la représentation sous forme de chaîne de la valeur renvoyée par le préfixe. Vous pouvez utiliser les fonctions avec `SET_TEXT_MODE(IGNORECASE)` ou `SET_TEXT_MODE(NOIGNORECASE)`, et avec les jeux de caractères ASCII et UTF-8.

Calculer la longueur d'une chaîne

L' `<text>.LENGTH` opération renvoie une valeur numérique égale au nombre de caractères (et non d'octets) d'une chaîne :


```
<text>.LENGTH
```

Par exemple, vous pouvez souhaiter identifier les URL de demande qui dépassent une longueur particulière. Voici une expression qui implémente cet exemple :

```
HTTP.REQ.URL.LENGTH < 500
```

Après avoir compté les caractères ou les éléments d'une chaîne, vous pouvez leur appliquer des opérations numériques. Pour plus d'informations, consultez Expressions de stratégie avancées : utilisation des dates, des heures et des nombres.

Considérez, ignorez et modifiez la casse du texte

Les fonctions suivantes fonctionnent sur la casse (majuscule ou minuscule) des caractères de la chaîne.

Fonction	Description	
<text>.SET_TEXT_MODE (IGNORECASE	NOIGNORECASE)	Cette fonction active ou désactive la sensibilité à la casse pour toutes les opérations de texte.
<text>.TO_LOWER	Convertit la cible en minuscules pour un bloc de texte d'une taille maximale de 2 kilo-octets (Ko). Renvoie UNDEF si la cible dépasse 2 Ko. Par exemple, la chaîne « abCD : » est convertie en « abcd : » .	
<text>.TO_UPPER	Convertit la cible en majuscules. Renvoie UNDEF si la cible dépasse 2 Ko. Par exemple, la chaîne « AbCD : » est convertie en « ABCD : » .	

Dépouille des caractères spécifiques d'une chaîne

Vous pouvez utiliser la fonction STRIP_CHARS (<string>) pour supprimer des caractères spécifiques du texte renvoyé par un préfixe d'expression de stratégie avancée (la chaîne d'entrée). Toutes les instances des caractères spécifiés dans l'argument sont retirées de la chaîne d'entrée. Vous pouvez

utiliser n'importe quelle méthode de texte sur la chaîne résultante, y compris les méthodes utilisées pour faire correspondre la chaîne à un jeu de motifs.

Par exemple, dans l'expression `CLIENT.UDP.DNS.DOMAIN.STRIP\\_CHARS(".-\\_")`, la fonction `STRIP\\_CHARS(<string>)` supprime tous les points (.), tirets (-) et traits de soulignement (_) du nom de domaine renvoyé par le préfixe CLIENT.UDP.DNS.DOMAIN. Si le nom de domaine renvoyé est « a.dom_ai_n-name », la fonction renvoie la chaîne « adomainname ».

Dans l'exemple suivant, la chaîne résultante est comparée à un jeu de motifs appelé « listofdomains » :

```
CLIENT.UDP.DNS.DOMAIN.STRIP_CHARS(".-_").CONTAINS_ANY("listofdomains")
```

Remarque : Vous ne pouvez pas effectuer de réécriture sur la chaîne renvoyée par la fonction `STRIP_CHARS(<string>)`.

Les fonctions suivantes enlève les caractères correspondants du début et de la fin d'une entrée de chaîne donnée.

Fonction	Description
`<text>.STRIP_START_CHARS(s)`	Enlève les caractères correspondants depuis le début de la chaîne d'entrée jusqu'à ce que le premier caractère non concordant soit trouvé et renvoie le reste de la chaîne. Vous devez spécifier les caractères que vous souhaitez supprimer sous la forme d'une chaîne unique entre guillemets. Par exemple, si le nom d'un en-tête est TestLang et que :*/en_us:est sa valeur, HTTP.RES.HEADER (« TestLang ») .STRIP_START_CHARS (« : «*) supprime les caractères spécifiés depuis le début de la valeur de l'en-tête jusqu'à ce que le premier caractère non correspondant e soit trouvé et renvoie sen_us : sous la forme d'un chaîne.

Fonction	Description
<text>.STRIP_END_CHARS(s)	Enlève les caractères correspondants depuis la fin de la chaîne d'entrée jusqu'au premier caractère non correspondant est trouvé et renvoie le reste de la chaîne. Vous devez spécifier les caractères que vous souhaitez supprimer sous la forme d'une chaîne unique entre guillemets. Par exemple, si le nom d'un en-tête est TestLang et que :/*en_us:is its value,HTTP.RES.HEADER("TestLang").STRIP_START_CHARS(":")* supprime les caractères spécifiés à partir de la fin de la valeur de l'en-tête jusqu'à ce que le premier caractère non correspondant s soit trouvé et renvoie : /_en_us sous forme de chaîne.

Ajouter une chaîne à une autre chaîne

Vous pouvez utiliser la fonction APPEND () pour ajouter la représentation sous forme de chaîne de l'argument à la représentation sous forme de chaîne de la valeur renvoyée par la fonction précédente. La fonction précédente peut être une fonction qui renvoie un nombre, un long non signé, un double, une valeur temporelle, une adresse IPv4 ou une adresse IPv6. L'argument peut être une chaîne de texte, un nombre, un long non signé, un double, une valeur temporelle, une adresse IPv4 ou une adresse IPv6. La valeur de chaîne résultante est la même valeur de chaîne que celle obtenue à l'aide de l'opérateur +.

Opérations complexes sur le texte

October 5, 2021

En plus de la simple correspondance de chaînes, vous pouvez configurer des expressions qui examinent la longueur des chaînes et les blocs de texte à la recherche de motifs plutôt que de chaînes spécifiques.

Pour toute opération basée sur du texte, prenez en compte les points suivants :

- Pour toute opération qui prend un argument de chaîne, la chaîne ne peut pas dépasser 255 caractères.

- Vous pouvez inclure des espaces blancs lorsque vous spécifiez une chaîne dans une expression.

Opérations sur la longueur d'une chaîne

Les opérations suivantes extraient les chaînes en fonction du nombre de caractères.

Opération de nombre de caractères	Description
<text>.TRUNCATE(<count>)	Renvoie une chaîne après avoir tronqué la fin de la cible du nombre de caractères dans <count>. Si la chaîne entière est plus courte que <count>, rien n'est renvoyé.
<text>.TRUNCATE(<character>, <count>)	Renvoie une chaîne après avoir tronqué le texte après <character> du nombre de caractères spécifié dans <count>.
<text>.PREFIX(<character>, <count>)	Sélectionne le préfixe le plus long de la cible dont le nombre d' <count> occurrences est le plus long <character>.
<text>.SUFFIX(<character>, <count>)	Sélectionne le suffixe le plus long de la cible dont le nombre d' <count> occurrences est le plus long <character>. Par exemple, considérez le corps de réponse suivant : JLewX. L'expression suivante renvoie la valeur « JlewX » : http.res.body (100) .suffix ('L',1) L'expression suivante renvoie « llewX » : http.res.body (100) .suffix ('L',2)
<text>.SUBSTR(<starting_offset>, <length>)	Sélectionnez une chaîne contenant <length>le nombre de caractères de l'objet cible. Commencez à extraire la chaîne après le <starting_offset>. Si le nombre de caractères après le décalage est inférieur à la valeur de l' <length> argument, sélectionnez tous les caractères restants.
<text>.SKIP(<character>, <count>)	Sélectionnez une chaîne dans la cible après avoir ignoré le préfixe le plus long qui a le plus d' <count> occurrences de <character>.

Opérations sur une partie d'une chaîne

Reportez-vous à la table Opérations de chaîne pour savoir comment extraire un sous-ensemble d'une chaîne plus grande à l'aide de l'une des opérations.

Opérations de comparaison de l'ordre alphanumérique de deux chaînes

L'opération COMPARE examine le premier caractère non concordant de deux chaînes différentes. Cette opération est basée sur l'ordre lexicographique, qui est la méthode utilisée pour trier les termes dans les dictionnaires.

Cette opération renvoie la différence arithmétique entre les valeurs ASCII des premiers caractères non concordants des chaînes comparées. Les différences suivantes sont des exemples :

- La différence entre « abc » et « and » est de -1 (basé sur la troisième comparaison de caractères par paire).
- La différence entre « @ » et « abc » est de -33.
- La différence entre « 1 » et « abc » est de -47.

Voici la syntaxe de l'opération COMPARE.

```
<text>.COMPARE(<string>)
```

Extraire un entier d'une chaîne d'octets représentant du texte

Reportez-vous à la table d'extraction Integer pour savoir comment traiter une chaîne d'octets représentant du texte comme une séquence d'octets, extraire 8 bits, 16 bits ou 32 bits de la séquence, puis convertir les bits extraits en entier.

Convertir le texte en une valeur de hachage

Vous pouvez convertir une chaîne de texte en valeur de hachage à l'aide de la fonction HASH. Cette fonction renvoie un entier positif de 31 bits à la suite de l'opération. Voici le format de l'expression :

```
<text>.HASH
```

Cette fonction ne tient pas compte de la casse et des espaces blancs. Par exemple, après l'opération, les deux chaînes Ab c et a bc produiraient la même valeur de hachage.

Encodez et décodez du texte en appliquant l'algorithme de codage Base64

Les deux fonctions suivantes encodent et décodent une chaîne de texte en appliquant l'algorithme de codage Base64.

Fonction	Description
text.B64ENCODE	Encode la chaîne de texte (désignée par texte) en appliquant l'algorithme de codage Base64.
text.B64DECODE	Décode la chaîne codée en Base64 (désignée par du texte) en appliquant l'algorithme de décodage Base64. L'opération déclenche un UNDEF si le texte n'est pas au format B64.

Affinez la recherche dans une action de réécriture à l'aide de la fonction EXTEND

La fonction EXTEND est utilisée dans les actions de réécriture qui spécifient des motifs ou des jeux de motifs et ciblent le corps des paquets HTTP. Lorsqu'une correspondance de motif est trouvée, la fonction EXTEND étend la portée de la recherche d'un nombre prédéfini d'octets des deux côtés de la chaîne correspondante. Une expression régulière peut ensuite être utilisée pour effectuer une réécriture sur les correspondances dans cette région étendue. Les actions de réécriture configurées avec la fonction EXTEND effectuent des réécritures plus rapidement que les actions de réécriture qui évaluent des corps HTTP entiers à l'aide d'expressions régulières uniquement.

Le format de la fonction EXTEND est EXTEND (m, n), où m et n sont le nombre d'octets par lesquels la portée de la recherche est étendue avant et après le motif correspondant, respectivement. Lorsqu'une correspondance est trouvée, la nouvelle portée de recherche comprend m octets qui précèdent immédiatement la chaîne correspondante, la chaîne elle-même et les n octets qui suivent la chaîne. Une expression régulière peut ensuite être utilisée pour effectuer une réécriture sur une partie de cette nouvelle chaîne.

La fonction EXTEND ne peut être utilisée que si l'action de réécriture dans laquelle elle est utilisée remplit les conditions suivantes :

- La recherche est effectuée à l'aide de motifs ou de jeux de motifs (et non d'expressions régulières)
- L'action de réécriture évalue uniquement le corps des paquets HTTP.

De plus, la fonction EXTEND ne peut être utilisée qu'avec les types d'actions de réécriture suivants :

- replace_all
- insert_after_all
- supprimer_tout
- insert_before_all

Par exemple, vous voudrez peut-être supprimer toutes les instances dehttp://exampleurl.com/"" ethttp://exampleurl.au/"" dans les 1000 premiers octets du corps. Pour ce faire, vous pouvez configurer une action de réécriture pour rechercher toutes les instances de la chaîne exampleurl,

étendre la portée de la recherche des deux côtés de la chaîne lorsqu'une correspondance est trouvée, puis utiliser une expression régulière pour effectuer la réécriture dans la région étendue. L'exemple suivant étend la portée de la recherche de 20 octets à gauche et de 50 octets à droite de la chaîne correspondante :

```
add rewrite action delurl_example delete_all 'HTTP.REQ.BODY(1000)'-search
exampleurl -refineSearch 'extend(20,50).regex_select(re##http://exampleurl
.(com|au)##)'
```

Convertir du texte au format hexadécimal

La fonction suivante convertit le texte au format hexadécimal et extrait la chaîne résultante :

```
<text>.BLOB_TO_HEX(<string>)
```

Par exemple, cette fonction convertit la chaîne d'octets « abc » en « 61:62:63 ».

Crypter et déchiffrer du texte

Dans les expressions de stratégie avancées, vous pouvez utiliser les fonctions CRYPTER et DECRYPT pour chiffrer et déchiffrer du texte. Les données chiffrées par la fonction ENCRYPT sur une appliance Citrix ADC ou une paire haute disponibilité (HA) donnée sont destinées au déchiffrement par la fonction DECRYPT sur la même appliance Citrix ADC ou la même paire HA. L'appliance prend en charge les méthodes de cryptage RC4, DES3, AES128, AES192 et AES256. La valeur de clé requise pour le chiffrement n'est pas spécifiable par l'utilisateur. Lorsqu'une méthode de chiffrement est définie, la solution matérielle-logicielle génère automatiquement une valeur de clé aléatoire adaptée à la méthode spécifiée. La méthode par défaut est le chiffrement AES256, qui est la méthode de cryptage la plus sécurisée et celle recommandée par Citrix.

Vous n'avez pas besoin de configurer le chiffrement, sauf si vous souhaitez modifier la méthode de chiffrement ou si vous souhaitez que la solution matérielle-logicielle génère une nouvelle valeur de clé pour la méthode de chiffrement actuelle.

Remarque : Vous pouvez également chiffrer et déchiffrer des charges utiles XML. Pour plus d'informations sur les fonctions de chiffrement et de déchiffrement des charges utiles XML, consultez Chiffrement et déchiffrement des charges utiles XML.

Configurer le chiffrement

Au démarrage, la solution matérielle-logicielle exécute la commande set ns EncryptionParams avec, par défaut, la méthode de cryptage AES256, et utilise une valeur de clé générée aléatoirement qui convient au chiffrement AES256. L'appliance chiffre également la valeur de la clé et enregistre la commande, avec la valeur de la clé chiffrée, dans le fichier de configuration Citrix ADC. Par conséquent,

la méthode de cryptage AES256 est activée par défaut pour les fonctions ENCRYPT et DECRYPT. La valeur de clé enregistrée dans le fichier de configuration persiste lors des redémarrages, même si la solution matérielle-logicielle exécute la commande chaque fois que vous la redémarrez.

Vous pouvez exécuter la commande set ns EncryptionParams manuellement ou utiliser l'utilitaire de configuration, si vous souhaitez modifier la méthode de chiffrement ou si vous souhaitez que la solution matérielle-logicielle génère une nouvelle valeur de clé pour la méthode de chiffrement actuelle. Pour utiliser l'interface de ligne de commande pour modifier la méthode de chiffrement, définissez uniquement le paramètre de méthode, comme indiqué dans « **Exemple 1 : Modification de la méthode de chiffrement** ». « Si vous souhaitez que la solution matérielle-logicielle génère une nouvelle valeur de clé pour la méthode de chiffrement actuelle, définissez le paramètre de méthode sur la méthode de chiffrement actuelle et le paramètre KeyValue sur une chaîne vide (« »), comme indiqué dans « **Exemple 2 : Génération d'une nouvelle valeur de clé pour la méthode de chiffrement actuelle**. « Après avoir généré une nouvelle valeur de clé, vous devez enregistrer la configuration. Si vous n'enregistrez pas la configuration, la solution matérielle-logicielle utilise la valeur de clé nouvellement générée uniquement jusqu'au prochain redémarrage, après quoi elle revient à la valeur de clé dans la configuration enregistrée.

Configurer le chiffrement à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans la zone **Paramètres**, cliquez sur **Modifier les paramètres de chiffrement** .
3. Dans la boîte de dialogue **Modifier les paramètres de chiffrement**, effectuez l'une des opérations suivantes :
   - Pour modifier la méthode de chiffrement, dans la liste Méthode, sélectionnez la méthode de chiffrement souhaitée.
   - Pour générer une nouvelle valeur de clé pour la méthode de chiffrement actuelle, cliquez sur Générer une nouvelle clé pour la méthode sélectionnée.
4. Cliquez sur **OK**.

Utilisez les fonctions ENCRYPT et DECRYPT

Vous pouvez utiliser les fonctions ENCRYPT et DECRYPT avec n'importe quel préfixe d'expression qui renvoie du texte. Par exemple, vous pouvez utiliser les fonctions CRYPTER et DECRYPT dans les stratégies de réécriture pour le chiffrement des cookie. Dans l'exemple suivant, les actions de réécriture chiffrent un cookie nommé MyCookie, qui est défini par un service principal, et décryptent le même cookie lorsqu'il est renvoyé par un client :

```
1 add rewrite action my-cookie-encrypt-action replace "HTTP.RES.
    SET_COOKIE.COOKIE("MyCookie").VALUE(0)" "HTTP.RES.SET_COOKIE.COOKIE(
    "MyCookie").VALUE(0).ENCRYPT"
```



```
2
3 add rewrite action my-cookie-decrypt-action replace "HTTP.REQ.COOKIE.
     VALUE("MyCookie")" "HTTP.REQ.COOKIE.VALUE("MyCookie").DECRYPT"
4 <!--NeedCopy-->
```

Après avoir configuré les stratégies de chiffrement et de déchiffrement, enregistrez la configuration pour que les stratégies entrent en vigueur.

Configuration de la clé de chiffrement pour le chiffrement

Dans les expressions de stratégie avancées, vous pouvez utiliser les fonctions CRYPTER et DECRYPT pour chiffrer et déchiffrer le texte d'une demande ou d'une réponse. Les données chiffrées par la fonction ENCRYPT sur une appliance (autonome, haute disponibilité ou cluster) sont destinées à être déchiffrées par la fonction DECRYPT par la même solution matérielle-logicielle. L'appliance prend en charge les méthodes de cryptage RC4, DES, Triple-DES, AES92 et AES256 et chacune de ces méthodes utilise une clé secrète pour le chiffrement et le déchiffrement des données. Vous pouvez utiliser l'une de ces méthodes pour chiffrer et déchiffrer les données de deux manières : l'autochiffrement et le cryptage tiers.

La fonctionnalité d'auto-chiffrement d'une appliance (autonome, haute disponibilité ou cluster) chiffre puis déchiffre les données en évaluant la valeur de l'en-tête. Un exemple pour comprendre cela est le cryptage des cookies HTTP. L'expression évalue l'en-tête, chiffre la valeur du cookie HTTP dans l'en-tête Set-Cookie dans la réponse sortante, puis déchiffre la valeur du cookie lorsqu'elle est renvoyée dans l'en-tête du cookie d'une demande entrante ultérieure du client. La valeur de la clé n'est pas configurable par l'utilisateur. En revanche, lorsqu'une méthode de chiffrement est configurée dans la commande set ns EncryptionParams, la solution matérielle-logicielle génère automatiquement une valeur de clé aléatoire pour la méthode configurée. Par défaut, la commande utilise la méthode de cryptage AES256, qui est la méthode hautement sécurisée, et Citrix recommande cette méthode.

La fonctionnalité de chiffrement tiers chiffre ou déchiffre les données avec une application tierce. Par exemple, un client peut chiffrer les données d'une demande et la solution matérielle-logicielle déchiffre les données avant de les envoyer au serveur principal ou vice versa. Pour ce faire, la solution matérielle-logicielle et l'application tierce doivent partager une clé secrète. Sur la solution matérielle-logicielle, vous pouvez configurer directement la clé secrète à l'aide d'un objet de clé de chiffrement et la valeur de clé est automatiquement générée par la solution matérielle-logicielle pour un chiffrement renforcé. La même clé est configurée manuellement sur l'appliance tierce afin que la solution matérielle-logicielle et l'application tierce puissent utiliser la même clé pour chiffrer et déchiffrer les données.

Remarque : En utilisant le chiffrement tiers, vous pouvez également chiffrer et déchiffrer les charges utiles XML. Pour plus d'informations sur les fonctions de chiffrement et de déchiffrement des charges

utiles XML, reportez-vous à la section « Cryptage et déchiffrement des charges de traitement XML.

Méthodes de chiffrement

Une méthode de chiffrement fournit deux fonctions : une fonction de chiffrement qui transforme une séquence d'octets de texte brut en une séquence d'octets de texte chiffré, et une fonction de déchiffrement qui transforme le texte chiffré en texte brut. Les méthodes de chiffrement utilisent des séquences d'octets appelées clés pour effectuer le chiffrement et le déchiffrement. Les méthodes de chiffrement qui utilisent la même clé pour le chiffrement et le déchiffrement sont appelées symétriques. Les méthodes de chiffrement qui utilisent des clés différentes pour le chiffrement et le déchiffrement sont asymétriques. Les exemples les plus notables de chiffrement asymétrique se trouvent dans la cryptographie à clé publique, qui utilise une clé publique accessible à tous pour le chiffrement et une clé privée connue uniquement du décrypteur.

Une bonne méthode de chiffrement rend impossible le déchiffrement (« craquer ») du texte chiffré si vous ne possédez pas la clé. « Infaisable » signifie vraiment que le déchiffrement du texte chiffré prendrait plus de temps et de ressources informatiques qu'il n'en vaut la peine. À mesure que les ordinateurs deviennent plus puissants et moins chers, les chiffrements qui étaient auparavant impossibles à déchiffrer deviennent de plus en plus réalisables. De plus, au fil du temps, des failles se retrouvent dans les méthodes de chiffrement (ou dans leurs implémentations), ce qui facilite le craquage. Les méthodes de chiffrement plus récentes sont donc préférées aux anciennes. En général, les clés de plus grande longueur offrent une meilleure sécurité que les clés plus courtes, au prix de temps de chiffrement et de déchiffrement plus longs.

Une méthode de chiffrement peut utiliser des chiffrements de flux ou des chiffrements par blocs. RC4 est le chiffrement de flux le plus sécurisé et il est utilisé uniquement pour les applications héritées. Les chiffrements par blocs peuvent inclure un remplissage.

Chiffrements de flux

Une méthode de chiffrement de flux fonctionne sur des octets individuels. Un seul chiffrement de flux est disponible sur les appliances Citrix ADC : RC4, qui utilise une longueur de clé de 128 bits (16 octets). Pour une clé donnée, RC4 génère une séquence pseudo-aléatoire d'octets, appelle un flux de clés, qui est oré X avec le texte brut pour produire le texte chiffré. RC4 n'est plus considéré comme sécurisé et ne doit être utilisé que si les applications héritées l'exigent.

Chirements par blocs

Une méthode de chiffrement par blocs fonctionne sur un bloc d'octets fixe. Une appliance Citrix ADC fournit deux chiffrements par blocs : Data Encryption Standard (DES) et Advanced Encryption Standard (AES). DES utilise une taille de bloc de 8 octets et (sur une appliance Citrix ADC) deux choix de

longueur de clé : 64 bits (8 octets), dont 56 bits de données et 8 bits de parité, et Triple-DES, une longueur de clé de 192 bits (24 octets). AES a une taille de bloc de 16 octets et (sur Citrix ADC) trois choix de longueur de clé : 128 bits (16 octets), 192 bits (24 octets) et 256 bits (32 octets).

Rembourrage

Si le texte brut d'un chiffrement par blocs n'est pas un nombre entier de blocs, un remplissage avec plus d'octets peut être nécessaire. Par exemple, supposons que le texte en clair soit « xyzzy » (hexadécimal 78797a7a79). Pour un bloc Triple-DES de 8 octets, cette valeur doit être complétée pour créer 8 octets. Le schéma de remplissage doit permettre à la fonction de déchiffrement de déterminer la longueur du texte brut original après le déchiffrement. Voici quelques schémas de remplissage actuellement utilisés (n est le nombre d'octets ajoutés) :

- PKCS7 : ajoute n octets de valeur n chacun. Par exemple, 78797a7a79030303. Il s'agit du schéma de remplissage utilisé par OpenSSL et la fonction de stratégie ENCRYPT(). Le schéma de remplissage PKCS5 est le même que celui de PKCS7.
- ANSI X.923 : Ajoute n-1 zéro octet et un octet final de valeur n. Par exemple, 78797a7a79000003.
- ISO 10126 : Ajoute n-1 octets aléatoires et un octet final de valeur n. Par exemple, 78797a7a79xxxx03, où xx peut être n'importe quelle valeur d'octet. La fonction de stratégie DECRYPT() accepte ce schéma de remplissage, ce qui lui permet également d'accepter les schémas PKCS7 et ANSI X.923.
- ISO/IEC 7816-4 : Ajoute un octet 0x80 et n-1 zéro octet. Par exemple, 78797a7a79800000. C'est aussi ce que l'on appelle le padding OneAndZeros.
- Zéro : ajoute n zéro octet. Exemple : 78797a7a79000000. Cette option ne peut être utilisée qu'avec du texte brut qui n'inclut pas d'octets NUL.

Si le remplissage est utilisé et que le texte en clair est un nombre entier de blocs, un bloc supplémentaire est généralement ajouté afin que la fonction de déchiffrement puisse déterminer sans ambiguïté la longueur du texte brut d'origine. Pour PCKS7 et bloc de 8 octets, il s'agirait de 0808080808080808.

Modes de fonctionnement

Il existe différents modes de fonctionnement pour les chiffrements par blocs, qui spécifient comment plusieurs blocs de texte brut sont chiffrés. Certains modes utilisent un vecteur d'initialisation (IV), un bloc de données en dehors du texte brut utilisé pour démarrer le processus de chiffrement. Il est recommandé d'utiliser un IV différent pour chaque cryptage, de sorte qu'un même texte en clair produise un texte chiffré différent. Le IV n'a pas besoin d'être secret, c'est pourquoi il est ajouté au texte chiffré. Les modes incluent :

- Electronic Codebook (ECB) : Chaque bloc de texte en clair est crypté indépendamment. Aucun IV n'est utilisé. Le remplissage est requis si le texte en clair n'est pas un multiple de la taille du bloc de chiffrement. Le même texte brut et la même clé produisent toujours le même texte

chiffré. Pour cette raison, la BCE est considérée comme moins sécurisée que les autres modes et ne doit être utilisée que pour les applications héritées.

- Cipher Block Chaining (CBC) : Chaque bloc de texte brut est codé avec le bloc de texte chiffré précédent, ou l'IV du premier bloc, avant d'être chiffré. Le remplissage est requis si le texte en clair n'est pas un multiple de la taille du bloc de chiffrement. Il s'agit du mode utilisé avec la méthode Citrix ADC EncryptionParams.
- Retour de chiffrement (CFB) : Le bloc de texte chiffré précédent, ou l'IV du premier bloc, est chiffré et la sortie est codée avec le bloc de texte brut actuel pour créer le bloc de texte chiffré actuel. La rétroaction peut être de 1 bit, 8 bits ou 128 bits. Comme le texte en clair est XORé avec le texte chiffré, le remplissage n'est pas nécessaire.
- Output Feedback (OFB) : Un flux de clés est généré en appliquant le chiffrement successivement au IV et en XoRing les blocs de flux de clés avec le texte brut. Le rembourrage n'est pas nécessaire.

Configuration des clés de chiffrement pour le chiffrement tiers

Voici les tâches de configuration effectuées lors de la configuration de la clé de chiffrement.

1. Ajout d'une clé de chiffrement. Configure une clé de chiffrement pour une méthode de chiffrement spécifiée avec une valeur de clé spécifiée.
2. Modification d'une clé de chiffrement. Vous pouvez modifier les paramètres d'une clé de chiffrement configurée.
3. Désinstallation d'une clé de chiffrement. Définit les paramètres d'une clé de chiffrement configurée sur leurs valeurs par défaut. Une valeur EncryptionKey portant le nom doit exister. Définit le remplissage sur DEFAULT (déterminé par la méthode), supprime un IV existant, ce qui provoque la génération d'une IV aléatoire par ENCRYPT (). Supprime un commentaire existant. La méthode et la valeur de la clé ne peuvent pas être réinitialisées.
4. Suppression d'une clé de chiffrement. Supprime une clé de chiffrement configurée. La clé ne peut pas comporter de référence.
5. Afficher une clé de chiffrement. Affiche les paramètres de la clé de chiffrement configurée ou de toutes les clés configurées. Si le nom est omis, la valeur de la clé n'est pas affichée.

Ajouter une clé de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ns encryptionKey <name> -method <method> [-keyValue <keyvalue>][-
padding (OFF | ON)] [-iv <hexstring>] -keyValue <keyvalue> [-comment <
string>]
```

Où,


```
<method> = ( NONE | RC4 | DES3 | AES128 | AES192 | AES256 | DES | DES-
    CBC | DES-CFB | DES-OFB | DES-ECB | DES3-CBC | DES3-CFB | DES3-OFB |
     DES3-ECB | AES128-CBC | AES128-CFB | AES128-OFB | AES128-ECB |
    AES192-CBC | AES192-CFB | AES192-OFB | AES192-ECB | AES256-CBC |
    AES256-CFB | AES256-OFB | AES256-ECB ) <hexstring> = hex-encoded
    byte sequence
<!--NeedCopy-->
```

Les méthodes de chiffrement ci-dessus spécifient le mode de fonctionnement avec CBC comme mode de fonctionnement par défaut. Par conséquent, les méthodes DES, DES2, AES128, AES192 et AES256 sont équivalentes aux méthodes DES-CBC, DES3-CBC, AES128-CBC, AES192-CBC et AES256-CBC.

Modifier une clé de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ns encryptionKey <name> [-method <method>] [-keyValue <keyvalue>] [-
padding ( OFF | ON )] [-iv <string>] [-comment <string>]
```

Désinstaller une clé de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unset ns encryptionKey <name> [-padding] [-iv] [-comment]
```

Supprimer une clé de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm ns encryptionKey <name>
```

Afficher une clé de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

Exemple :

```
show ns encryptionKey [<name>]

add ns encryptionKey my_key -method aes256 -keyValue 26
    ea5537b7e0746089476e5658f9327c0b10c3b4778c673a5b38cee182874711 -iv
    c2bf0b2e15c15004d6b14bcdc7e5e365
set ns encryptionKey my_key -keyValue
    b8742b163abcf62d639837bbee3cef9fb5842d82d00dfe6548831d2bd1d93476
unset ns encryptionKey my_key -iv
```



```
rm ns encryptionKey my_key
show ns encryptionKey my_key
Name: my_key
Method: AES256
Padding: DEFAULT
Key Value: (not disclosed)
<!--NeedCopy-->
```

Ajouter une clé de chiffrement à l'aide de l'interface graphique

Accédez à **Système** > **Clés de chiffrement**, puis cliquez sur **Ajouter** pour créer une clé de chiffrement.

Modifier une clé de chiffrement à l'aide de l'interface graphique

Accédez à **Système** > **Clés de chiffrement**, puis cliquez sur **Modifier** pour modifier les paramètres d'une clé de chiffrement configurée.

Supprimer une clé de chiffrement à l'aide de l'interface graphique

Accédez à **Système** > **Clés de chiffrement**, puis cliquez sur **Supprimer**.

Fonctions ENCRYPT et DECRYPT pour le chiffrement tiers

Voici la fonction ENCRYPT utilisée pour le chiffrement tiers.

```
ENCRYPT (encryptionKey, out_encoding)
```

Où,

Les données d'entrée de la solution matérielle-logicielle sont le texte à chiffrer

EncryptionKey : paramètre de chaîne facultatif qui spécifie l'objet clé de chiffrement configuré pour fournir la méthode de chiffrement, la valeur de la clé secrète et d'autres paramètres de chiffrement. Si elle n'est pas spécifiée, la méthode utilise la valeur de clé générée automatiquement associée à la commande set ns EncryptionParams.

out_encoding : Cette valeur spécifie le mode de codage de la sortie. S'il n'est pas spécifié, le codage BASE64 est utilisé.

Entrée :

```
BASE64: original PEM base64-encoding: 6 bits (0..63) encoded as one
    ASCII character:
                0..23 = 'A'..'Z', 24..51 = 'a'..'z', 52..61 = '0'..'9
                   ', 62 = '+', 63 = '/', '=' = pad byte.
```



```
3        BASE64URL:  URL and Filename safe base64-encoding: same as BASE64
             except 62 = '-', 63 = '_'
4        HEX_UPPER:  Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'A'..'F
             '.
5        HEX_LOWER:  Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'a'..'f
             '.
6        HEX_COLONS: Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'A'..'F
             '; ':' between each hex byte. Matches BLOB_TO_HEX() output
             format
7        HEX:  For input, accepts HEX_UPPER, HEX_LOWER, and HEX_COLONS
             format. For output, produces HEX_LOWER format
8  <!--NeedCopy-->
```

Sortie : La sortie est un texte chiffré à l'aide de la méthode et de la clé spécifiées et codé à l'aide d'un codage de sortie spécifié. Il insère une IV générée avant le texte chiffré pour les méthodes de bloc et les modes nécessitant une IV, et soit aucune IV n'est spécifiée pour la clé de chiffrement, soit la clé de chiffrement est omise.

Voici la fonction DECRYPT utilisée pour le déchiffrement tiers.

```
DECRYPT(encryptionKey, in_encoding)
```

Où,

Les données d'entrée sont un texte chiffré à l'aide de la méthode spécifiée et une clé codée à l'aide du codage d'entrée spécifié. Ce texte est censé inclure une IV générée avant le texte chiffré pour les méthodes et modes de blocs qui nécessitent une IV, et soit aucune IV n'est spécifiée pour la clé de chiffrement, soit la clé de chiffrement est omise.

EncryptionKey : paramètre de chaîne facultatif qui spécifie l'objet EncryptionKey configuré pour fournir la méthode de chiffrement, la clé secrète et d'autres paramètres de chiffrement. En cas d'omission, la méthode et la clé générée automatiquement associées au paramètre Encryption-Params seront utilisées

IN_ENCODING : paramètre d'énumération facultatif qui spécifie comment l'entrée doit être codée. Les valeurs sont les mêmes que l'encodage sortant de ENCRYPT. S'il n'est pas spécifié, le codage BASE64 est attendu.

Les données de sortie sont un texte déchiffré non codé.

Variantes et paramètres facultatifs

Voici les variantes de ces fonctions avec les paramètres facultatifs :

Variante	Description
ENCRYPT	Utilisez la commande EncryptionParams et le paramètre de codage de sortie BASE64.
ENCRYPT(out_encoding)	Utilisez EncryptionParams et le paramètre de codage de sortie spécifié.
ENCRYPT(encryptionKey)	Utilisez les paramètres de codage de sortie EncryptionKey et BASE64 spécifiés.
ENCRYPT(encryptionKey, out_encoding)	Utilisez la clé de chiffrement et le paramètre de codage de sortie spécifiés.
DECRYPT	Utilisez la commande EncryptionParams et le paramètre de codage d'entrée BASE64.
DECRYPT(out_encoding)	Utilisez la commande EncryptionParams et le paramètre de codage d'entrée spécifié.
DECRYPT(encryptionKey)	Utilisez les paramètres de codage d'entrée EncryptionKey et BASE64 spécifiés.
DECRYPT(encryptionKey, out_encoding)	Utilisez la clé de chiffrement et le paramètre de codage d'entrée spécifiés.

Configurer les clés HMAC

Les appliances Citrix ADC prennent en charge une fonction HMAC (Hashed Message Authentication Code) qui calcule une méthode de résumé ou un hachage du texte d'entrée à l'aide d'une clé secrète partagée entre l'expéditeur et le destinataire du message. La méthode de résumé (dérivée d'une technique RFC 2104) authentifie l'expéditeur et vérifie que le contenu du message n'a pas été modifié. Par exemple, lorsqu'un client envoie un message avec la clé HMAC partagée à une appliance Citrix ADC, les expressions de stratégie avancée (PI) utilisent la fonction HMAC pour calculer le code basé sur le hachage sur le texte sélectionné. Ensuite, lorsque le récepteur reçoit le message avec la clé secrète, il recalcule le HMAC en le comparant au HMAC d'origine pour déterminer si le message a été modifié. La fonction HMAC est prise en charge par les appliances autonomes et par les appliances dans une configuration haute disponibilité ou dans un cluster. Son utilisation est similaire à la configuration d'une clé de chiffrement.

Les commandes add ns hmackey et set ns hmackey incluent un paramètre qui spécifie la méthode de condensation et la clé secrète partagée à utiliser pour le calcul HMAC.

Pour configurer une clé HMAC, vous devez effectuer les opérations suivantes :

1. Ajout d'une clé HMAC. Configure une clé HMAC avec une valeur de clé spécifiée.

2. Modification d'une clé HMAC. Modifie les paramètres d'une clé HMAC configurée. La méthode de condensation peut être modifiée sans modifier la valeur de clé, car la longueur de la valeur de clé n'est pas déterminée par le condensé. Toutefois, il est conseillé de spécifier une nouvelle clé lors de la modification du résumé.
3. Désinstallation d'une clé HMAC. Définit les paramètres d'une clé HMAC configurée sur leurs valeurs par défaut. Un objet HMacKey portant le nom doit exister. Le seul paramètre qui peut être désactivé est le commentaire, qui est supprimé.
4. Suppression d'une clé HMAC. Supprime une clé configurée. La clé ne peut pas comporter de référence.
5. Afficher une clé HMAC. Affiche les paramètres de la clé AC HMAC configurée ou de toutes les clés configurées. Si le nom est omis, la valeur de la clé n'est pas affichée.

Configurer une clé HMAC unique et aléatoire

Vous pouvez générer automatiquement une clé HMAC unique. Si votre appliance est une configuration de cluster, la clé HMAC est générée au début du processus et distribuée à tous les nœuds et moteurs de paquets. Cela garantit que la clé HMAC est identique pour tous les moteurs de paquets et tous les nœuds du cluster.

À l'invite de commandes, tapez :

```
add ns hmacKey <your_key> -digest <digest> -keyValue <keyvalue>
```

Exemple :

```
add ns hmacKey <name> -digest sha1 -keyValue AUTO
```

Où,

- La syntaxe du nom est correcte et ne duplique pas le nom d'une clé existante.
- La valeur de clé « AUTO » peut être utilisée dans les commandes set pour générer de nouvelles clés pour les objets EncrytionKey et HMacKey existants.

> **Remarque :**
>
> La génération automatique de clés est utile si l'appliance Citrix ADC chiffre et déchiffre les données avec la clé, ou génère et vérifie une clé HMAC. Étant donné que la valeur de clé elle-même est déjà chiffrée lorsqu'elle est affichée, vous ne pouvez pas récupérer la valeur de clé générée à des fins d'utilisation par une autre partie.

Exemple :

```
add ns hmacKey my_hmac_key -digest sha1 -keyValue 0c753c6c5ef859189cacdf95b506d02c179
```

Les méthodes de chiffrement ci-dessus spécifient le mode de fonctionnement avec CBC comme mode de fonctionnement par défaut. Par conséquent, les méthodes DES, DES2, AES128, AES192 et AES256

sont équivalentes aux méthodes DES-CBC, DES3-CBC, AES128-CBC, AES192-CBC et AES256-CBC.

Modifier une clé HMAC à l'aide de l'interface de ligne de commande

Cette commande modifie les paramètres configurés pour une clé HMAC. Vous pouvez modifier le résumé sans modifier la valeur de la clé, car la longueur de la valeur de clé n'est pas déterminée par le résumé. Toutefois, il est conseillé de spécifier une nouvelle clé lors de la modification du résumé. À l'invite de commandes, tapez :

```
set ns hmacKey <name> [-digst <digest>] [-keyValue <keyvalue>]
[-comment <string>]

<!--NeedCopy-->
```

Désinstaller une clé HMAC à l'aide de l'interface de ligne de commande

Cette commande définit les paramètres configurés pour une clé HMAC avec leurs valeurs par défaut. Un objet HMacKey portant le nom doit exister. Le seul paramètre que vous pouvez annuler est l'option de commentaire, qui est supprimée. À l'invite de commandes, tapez :

```
unset ns hmacKey <name> -comment
```

Supprimer une clé HMAC à l'aide de l'interface de ligne de commande

Cette commande supprime la clé hmac configurée. La clé ne peut pas contenir de références. À l'invite de commandes, tapez :

```
rm ns hmacKey <name>
```

Afficher une clé HMAC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show ns encryptionKey [<name>]

add ns hmacKey my_hmac_key -digest sha1 -keyValue 0
    c753c6c5ef859189cacdf95b506d02c1797407d
set ns hmacKey my_hmac_key -keyValue
    f348c594341a840a1f641a1cf24aa24c15eb1317
rm ns hmacKey my_hmac_key
show ns hmacKey my_hmac_key
           Name: my_hmac_key
     Digest: SHA1
```



```
    Key Value: (not disclosed)
<!--NeedCopy-->
```

Expressions de stratégie avancées : utilisation des dates, des heures et des nombres

January 21, 2021

La plupart des données numériques traitées par l'appliance Citrix ADC sont constituées de dates et d'heures. En plus de travailler avec les dates et les heures, l'appliance traite d'autres données numériques, telles que la longueur des requêtes et des réponses HTTP. Pour traiter ces données, vous pouvez configurer des expressions de stratégie avancées qui traitent les numéros.

Une expression numérique consiste en un préfixe d'expression qui renvoie un nombre et parfois, mais pas toujours, un opérateur capable d'effectuer une opération sur le nombre. Exemples de préfixes d'expression qui renvoient des nombres sont `SYS.TIME.DAY` `HTTP.REQ.CONTENT_LENGTH` et les opérateurs `HTTP.RES.BODY.LENGTH`. `Numeric` peuvent travailler avec n'importe quelle expression de préfixe qui renvoie des données dans format numérique. L'opérateur `GT(<int>)` par exemple, peut être utilisé avec n'importe quelle expression de préfixe, telle que HTTP.REQ.CONTENT_LENGTH, qui renvoie un entier.

Format des dates et heures dans une expression

August 20, 2021

Lorsque vous configurez une expression de stratégie avancée dans une stratégie qui fonctionne avec des dates et des heures (par exemple, l'heure système Citrix ADC ou une date dans un certificat SSL), vous spécifiez un format d'heure comme suit :

```
GMT|LOCAL [<yyyy>] [<month>] [<d>] [<h>] [<m>] [<s>]
```

Où :

- <yyyy> est une année à quatre chiffres après GMT ou LOCAL.
- <month> est une abréviation à trois caractères pour le mois, par exemple, Jan, Déc.
- <d> est un jour de la semaine ou un entier pour la date.

  Vous ne pouvez pas spécifier le jour comme Lundi, Mardi, etc. Vous spécifiez un entier pour un jour spécifique du mois, ou vous spécifiez une date comme premier, deuxième, troisième jour de semaine du mois, etc. Voici des exemples de spécification d'un jour de la semaine :

  - Sun_1 est le premier dimanche du mois.
  - Sun_3 est le troisième dimanche du mois.
  - Wed_3 est le troisième mercredi du mois.
  - 30 est un exemple de date exacte dans un mois.

- <h> est l'heure, par exemple, 10h.
- <s> est le nombre de secondes, par exemple, 30s.

L'exemple d'expression suivant est vrai si la date est comprise entre 2008 Jan et 2009 Jan, basée sur GMT.

```
http.req.date.between(GMT 2008 Jan, GMT 2009 Jan)
```

L'exemple d'expression suivant est vrai pour Mars et tous les mois qui suivent Mars de l'année civile, en fonction de la GMT :

```
sys.time.ge(GMT 2008 Mar)
```

Lorsque vous spécifiez une date et une heure, notez que le format respecte la casse et doit de conserver le nombre exact d'espaces vides entre les entrées.

```
**Note:**

In an expression that requires two time values, both must use GMT or
    both must use LOCAL. You cannot mix the two in an expression.

Unlike when you use the SYS.TIME prefix in an advanced policy
    expression, if you specify SYS.TIME in a rewrite action, the Citrix
    ADC returns a string in conventional date format (for example, Sun,
    06 Nov 1994 08:49:37 GMT). For example, the following rewrite action
     replaces the http.res.date header with the Citrix ADC system time
    in a conventional date format:

add rewrite action sync_date replace http.res.date sys.time
```

Expressions pour l'heure système Citrix ADC

August 20, 2021

Le préfixe d'expression SYS.TIME extrait l'heure système Citrix ADC. Vous pouvez configurer des expressions qui déterminent si un événement particulier s'est produit à un moment donné ou dans une plage de temps spécifique en fonction de l'heure système Citrix ADC.

Le tableau suivant décrit les expressions que vous pouvez créer à l'aide du préfixe SYS.TIME.

- **SYS.TIME.BETWEEN(<time1>, <time2>):**

  Renvoie une valeur booléenne TRUE si la valeur renvoyée est postérieure <time1> et antérieure à <time2>.

  Vous formatez les <time1> <time2> arguments, comme suit :

  - Ils doivent tous les deux être GMT ou les deux LOCAL.
  - <time2>doit être plus tard que <time1>.

  Par exemple, si l'heure actuelle est GMT 2005 mai 1 10h 15m 30, et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit :

  - sys.time.between (GMT 2004, GMT 2006)
  - sys.time.between (GMT 2004 Jan, GMT 2006 Nov)
  - sys.time.between (GMT 2004 Jan, GMT 2006)
  - sys.time.between (GMT 2005 Mai Sun_1, GMT 2005 Mai Sun_3)
  - sys.time.between (GMT 2005 1er mai, GMT Mai 2005 1)
  - sys.time.between (LOCAL 2005 1er mai, LOCAL mai 2005 1)

- **SYS.TIME.DAY :**

  Renvoie le jour courant du mois sous la forme d'un nombre compris entre 1 et 31.

- **SYS.TIME.EQ(<time>):**

  Renvoie une valeur booléenne TRUE si l'heure actuelle est égale à l' <time> argument.

  Par exemple, si l'heure actuelle est GMT 2005 Mai 1 10h 15m 30, et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont affichés entre parenthèses) :

  - sys.time.eq (GMT 2005) (TRUE dans cet exemple.)
  - sys.time.eq (GMT 2005 Dec) (FALSE dans cet exemple.)
  - sys.time.eq (LOCAL 2005 May) (Value TRUE ou FALSE dans cet exemple, selon le fuseau horaire actuel.)
  - sys.time.eq (GMT 10h) (TRUE dans cet exemple.)
  - sys.time.eq (GMT 10h 30s) (TRUE dans cet exemple.)
  - sys.time.eq (GMT 10 mai) (TRUE dans cet exemple.)
  - sys.time.eq (GMT Sun) (TRUE dans cet exemple.)
  - sys.time.eq (GMT May Sun_1) (TRUE dans cet exemple.)

- **SYS.TIME.NE(<time>):**

  Renvoie une valeur booléenne TRUE si l'heure actuelle n'est pas égale à l' <time> argument.

- **SYS.TIME.GE(<time>):**

  Renvoie une valeur booléenne TRUE si l'heure actuelle est postérieure ou égale à <time>.

Par exemple, si l'heure actuelle est GMT 2005 Mai 1 10h 15m 30, et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont affichés entre parenthèses) :

- sys.time.ge (GMT 2004) (TRUE dans cet exemple.)
- sys.time.ge (GMT 2005 Jan) (TRUE dans cet exemple.)
- sys.time.ge (LOCAL 2005 May) (TRUE ou FALSE dans cet exemple, selon le fuseau horaire actuel.)
- sys.time.ge (GMT 8h) (TRUE dans cet exemple.)
- sys.time.ge (GMT 30m) (FALSE dans cet exemple.)
- sys.time.ge (GMT 10 mai) (TRUE dans cet exemple.)
- sys.time.ge (GMT 10 mai 0m) (VRAI dans cet exemple.)
- sys.time.ge (GMT Sun) (TRUE dans cet exemple.)
- sys.time.ge (GMT May Sun_1) (TRUE dans cet exemple.)

- **SYS.TIME.GT(<time>):**

  Renvoie une valeur booléenne TRUE si la valeur temporelle est postérieure à l' <time> argument.

  Par exemple, si l'heure actuelle est GMT 2005 Mai 1 10h 15m 30, et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont affichés entre parenthèses) :

  - sys.time.gt (GMT 2004) (TRUE dans cet exemple.)
  - sys.time.gt (GMT 2005 Jan) (TRUE dans cet exemple.)
  - sys.time.gt (LOCAL 2005 mai) (TRUE ou FALSE, selon le fuseau horaire actuel.)
  - sys.time.gt (GMT 8h) (TRUE dans cet exemple.)
  - sys.time.gt (GMT 30m) (FALSE dans cet exemple.)
  - sys.time.gt (GMT 10 mai) (FALSE dans cet exemple.)
  - sys.time.gt (GMT mai 10h 0m) (TRUE dans cet exemple.)
  - sys.time.gt (GMT Sun) (FALSE dans cet exemple.)
  - sys.time.gt (GMT May Sun_1) (FALSE dans cet exemple.)

- **SYS.TIME.HOURS:**

  Renvoie l'heure actuelle sous la forme d'un entier compris entre 0 et 23.

- **SYS.TIME.LE(<time>):**

  Renvoie une valeur booléenne TRUE si la valeur de temps actuelle précède ou est égale à l' <time> argument.

  Par exemple, si l'heure actuelle est GMT 2005 Mai 1 10h 15m 30, et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont affichés entre parenthèses) :

  - sys.time.le (GMT 2006) (TRUE dans cet exemple.)

- sys.time.le (GMT 2005 Dec) (TRUE dans cet exemple.)
- sys.time.le (LOCAL 2005 mai) (TRUE ou FALSE selon le fuseau horaire actuel.)
- sys.time.le (GMT 8h) (FALSE dans cet exemple.)
- sys.time.le (GMT 30m) (TRUE dans cet exemple.)
- sys.time.le (GMT 10 mai) (TRUE dans cet exemple.)
- sys.time.le (GMT Jun 11h) (VRAI dans cet exemple.)
- sys.time.le (GMT Wed) (TRUE dans cet exemple.)
- sys.time.le (GMT May Sun_1) (TRUE dans cet exemple.)

- **SYS.TIME.LT(<time>):**

  Renvoie une valeur booléenne TRUE si la valeur de temps actuelle précède l' <time> argument.

  Par exemple, si l'heure actuelle est GMT 2005 Mai 1 10h 15m 30, et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont affichés entre parenthèses) :

  - sys.time.lt (GMT 2006) (TRUE dans cet exemple.)
  - sys.time.lt.time.lt (GMT 2005 Dec) (TRUE dans cet exemple.)
  - sys.time.lt (LOCAL 2005 mai) (TRUE ou FALSE selon le fuseau horaire actuel.)
  - sys.time.lt (GMT 8h) (FALSE dans cet exemple.)
  - sys.time.lt (GMT 30m) (TRUE dans cet exemple.)
  - sys.time.lt (GMT 10 mai) (FALSE dans cet exemple.)
  - sys.time.lt (GMT Jun 11h) (TRUE dans cet exemple.)
  - sys.time.lt (GMT mer) (TRUE dans cet exemple.)
  - sys.time.lt (GMT May Sun_1) (FALSE dans cet exemple.)

- **SYS.TIME.MINUTES:**

  Renvoie la minute actuelle sous la forme d'un entier compris entre 0 et 59.

- **SYS.TIME.MONTH:**

  Extrait le mois en cours et renvoie un entier compris entre 1 (janvier) et 12 (décembre).

- **SYS.TIME.RELATIVE_BOOT:**

  Calcule le nombre de secondes du redémarrage précédent ou planifié le plus proche et renvoie un entier.

  Si l'heure de démarrage la plus proche est dans le passé, l'entier est négatif. Si c'est dans le futur, l'entier est positif.

- **SYS.TIME.RELATIVE_NOW:**

  Calcule le nombre de secondes entre l'heure système Citrix ADC courant et l'heure spécifiée, puis renvoie un entier indiquant la différence.

  Si l'heure désignée est dans le passé, l'entier est négatif ; s'il est dans le futur, l'entier est positif.

- **SYS.TIME.SECONDS:**

  Extrait les secondes de l'heure système Citrix ADC en cours et renvoie cette valeur sous la forme d'un entier compris entre 0 et 59.

- **SYS.TIME.WEEKDAY:**

  Renvoie le jour de la semaine en cours sous la forme d'une valeur comprise entre 0 (dimanche) et 6 (samedi).

- **SYS.TIME.WITHIN (<time1>, <time2>):**

  Si vous omettez un élément de temps dans <time1>, par exemple, le jour ou l'heure, il est supposé avoir la valeur la plus faible dans sa plage. Si vous omettez un élément dans <time2>, il est supposé avoir la valeur la plus élevée de sa plage.

  Les plages pour les éléments de temps sont les suivantes : mois 1-12, jour 1-31, jour de semaine 0-6, heure 0-23, minutes 0-59 et secondes 0-59. Si vous spécifiez l'année, vous devez le faire dans les deux <time1> et <time2>.

  Par exemple, si l'heure est GMT 2005 10 mai 10h 15m 30s, et que c'est le deuxième mardi du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont affichés entre parenthèses) :

  - sys.time.within (GMT 2004, GMT 2006) (TRUE dans cet exemple.)
  - sys.time.within (GMT 2004 Jan, GMT 2006 Mar) (FALSE, mai n'est pas compris entre janvier et mars.)
  - sys.time.within (GMT Feb, GMT) (VRAI, mai se situe entre février et décembre.)
  - sys.time.within (GMT Sun_1, GMT Sun_3) (TRUE, le deuxième mardi se situe entre le premier dimanche et le troisième dimanche).
  - sys.time.within (GMT 2005 mai 1 10h, GMT mai 2005 1 17h) (VRAI dans cet exemple.)
  - sys.time.within (LOCAL 2005 1er mai, LOCAL mai 2005 1) (TRUE ou FALSE, selon le fuseau horaire du système Citrix ADC.)

- **SYS.TIME.YEAR:**

  Extrait l'année de l'heure système actuelle et renvoie cette valeur sous la forme d'un entier à quatre chiffres.

Expressions pour les dates de certificat SSL

August 20, 2021

Vous pouvez déterminer la période de validité des certificats SSL en configurant une expression qui contient le préfixe suivant :

```
CLIENT.SSL.CLIENT_CERT
```


L'exemple d'expression suivant correspond à un délai d'expiration particulier avec les informations contenues dans le certificat :

```
client.ssl.client_cert.valid_not_after.eq(GMT 2009)
```

Le tableau suivant décrit les opérations basées sur le temps sur les certificats SSL. Pour obtenir l'expression souhaitée, remplacez le *certificat* dans l'expression de la première colonne par l'expression de préfixe « CLIENT.SSL.CLIENT_CERT ».

- `<certificate>.VALID_NOT_AFTER`:

  Renvoie le dernier jour avant l'expiration du certificat. Le format de retour est le nombre de secondes depuis le 1er janvier 1970 GMT (0 heures, 0 minutes, 0 secondes).

- **<certificate>.VALID_NOT_AFTER.BETWEEN(<time1>, <time2>):**

  Renvoie une valeur booléenne TRUE si la validité du certificat se situe entre les arguments <time1> et <time2>. <time1> et <time2> doivent être entièrement spécifiés. Voici des exemples :

  GMT 1995 Jan est entièrement spécifié.

  GMT Jan n'est pas entièrement spécifié

  GMT 1995 20 n'est pas entièrement spécifié.

  GMT Jan Mon_2 n'est pas entièrement spécifié.

  Les arguments <time1> et <time2> doivent être GMT ou tous les deux LOCAL, et <time2> doit être supérieur à <time1>.

  Par exemple, si c'est GMT 2005 mai 1 10h 15m 30, et le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont entre parenthèses).

  - . . .between(GMT 2004, GMT 2006) (TRUE)
  - . . .between(GMT 2004 Jan, GMT 2006 Nov) (TRUE)
  - . . .between(GMT 2004 Jan, GMT 2006) (TRUE)
  - . . .between(GMT 2005 May Sun_1, GMT 2005 May Sun_3) (TRUE)
  - . . .between(GMT 2005 May 1, GMT May 2005 1) (TRUE)
  - . . .between(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE ou FALSE, selon le fuseau horaire du système Citrix ADC.)

- **<certificate>.VALID_NOT_AFTER.DAY:**

  Extrait le dernier jour du mois pendant lequel le certificat est valide et renvoie un nombre compris entre 1 et 31, selon le cas pour la date.

- **<certificate>.VALID_NOT_AFTER.EQ(<time>):**

  Renvoie une valeur booléenne TRUE si la durée est égale à l' <time> argument.

Par exemple, si l'heure actuelle est GMT 2005 1er mai 10h 15m 30s et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats d'évaluation de cet exemple sont entre parenthèses) :

- . . .eq(GMT 2005) (TRUE)
- . . .eq(GMT 2005 Dec) (FALSE)
- . . .eq(LOCAL 2005 May) (TRUE ou FALSE, selon le fuseau horaire actuel)
- . . .eq(GMT May 10h) (TRUE)
- . . .eq(GMT 10h 30s) (TRUE)
- . . .eq(GMT May 10h) (TRUE)
- . . .eq(GMT Sun) (TRUE)
- . . .eq(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_AFTER.GE(<time>):**

  Renvoie une valeur booléenne TRUE si la valeur temporelle est supérieure ou égale à l'argument <time>.

  Par exemple, si la valeur d'heure est GMT 2005 1er mai 10h 15m 30s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats d'évaluation de cet exemple sont entre parenthèses) :

  - . . .ge(GMT 2004) (TRUE)
  - . . .ge(GMT 2005 Jan) (TRUE)
  - . . .ge(LOCAL 2005 May) (TRUE ou FALSE, selon le fuseau horaire actuel.)
  - . . .gt(GMT 8h) (TRUE)
  - . . .ge(GMT 30m) (FALSE)
  - . . .ge(GMT May 10h) (TRUE)
  - . . .ge(GMT May 10h 0m) (TRUE)
  - . . .ge(GMT Sun) (TRUE)
  - . . .ge(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_AFTER.GT(<time>):**

  Renvoie une valeur booléenne TRUE si la valeur temporelle est supérieure à l'argument <time>.

  Par exemple, si la valeur d'heure est GMT 2005 1er mai 10h 15m 30s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats d'évaluation de cet exemple sont entre parenthèses) :

  - . . .gt(GMT 2004) (TRUE)
  - . . .gt(GMT 2005 Jan) (TRUE)
  - . . .gt(LOCAL 2005 May) (TRUE ou FALSE, selon le fuseau horaire actuel.)
  - . . .gt(GMT 8h) (TRUE)
  - . . .gt(GMT 30m) (FALSE)

- . . .gt(GMT May 10h) (FALSE)
- . . .gt(GMT Sun) (FALSE)
- . . .gt(GMT May Sun_1) (FALSE)

- **<certificate>.VALID_NOT_AFTER.HOURS:**

  Extrait la dernière heure pendant laquelle le certificat est valide et renvoie cette valeur sous la forme d'un entier compris entre 0 et 23.

- **<certificate>.VALID_NOT_AFTER.LE(<time>):**

  Renvoie une valeur booléenne TRUE si l'heure précède ou est égale à l' <time> argument.

  Par exemple, si la valeur d'heure est GMT 2005 1er mai 10h 15m 30s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats d'évaluation de cet exemple sont entre parenthèses) :

  - . . .le(GMT 2006) (TRUE)
  - . . .le(GMT 2005 Dec) (TRUE)
  - . . .le(LOCAL 2005 May) (TRUE ou FALSE, selon le fuseau horaire actuel.)
  - . . .lt(GMT 8h) (FALSE)
  - . . .le(GMT 30m) (TRUE)
  - . . .le(GMT May 10h) (TRUE)
  - . . .le(GMT Jun 11h) (TRUE)
  - . . .le(GMT Wed) (TRUE)
  - . . .le(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_AFTER.LT(<time>):**

  Renvoie une valeur booléenne TRUE si l'heure précède l' <time> argument.

  Par exemple, si l'heure actuelle est GMT 2005 mai 1 10h 15m 30, et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit :

  - . . .lt(GMT 2006) (TRUE)
  - . . .lt(GMT 2005 Dec) (TRUE)
  - . . .lt(LOCAL 2005 May) (TRUE ou FALSE, selon le fuseau horaire actuel.)
  - . . .lt(GMT 8h) (FALSE)
  - . . .lt(GMT 30m) (TRUE)
  - . . .lt(GMT May 10h) (FALSE)
  - . . .lt(GMT Jun 11h) (TRUE)
  - . . .lt(GMT Wed) (TRUE)
  - . . .lt(GMT May Sun_1) (FALSE)

- **<certificate>.VALID_NOT_AFTER.MINUTES:**

  Extrait la dernière minute que le certificat est valide et renvoie cette valeur sous la forme d'un entier compris entre 0 et 59.

- **<certificate>.VALID_NOT_AFTER.MONTH:**

  Extrait le dernier mois pendant lequel le certificat est valide et renvoie cette valeur sous la forme d'un entier compris entre 1 (janvier) et 12 (décembre).

- **<certificate>.VALID_NOT_AFTER.RELATIVE_BOOT:**

  Calcule le nombre de secondes du redémarrage précédent ou planifié le plus proche et renvoie un entier. Si l'heure de démarrage la plus proche est dans le passé, l'entier est négatif. Si c'est dans le futur, l'entier est positif.

- **<certificate>.VALID_NOT_AFTER.RELATIVE_NOW;**

  Calcule le nombre de secondes entre l'heure système actuelle et l'heure spécifiée et renvoie un entier. Si le temps est dans le passé, l'entier est négatif ; s'il est dans le futur, l'entier est positif.

- **<certificate>.VALID_NOT_AFTER.SECONDS:**

  Extrait la dernière seconde que le certificat est valide et renvoie cette valeur sous la forme d'un entier compris entre 0 et 59.

- **<certificate>.VALID_NOT_AFTER.WEEKDAY:**

  Extrait le dernier jour de semaine pendant lequel le certificat est valide. Renvoie un nombre compris entre 0 (dimanche) et 6 (samedi) pour indiquer le jour de la semaine dans la valeur d'heure.

- **<certificate>.VALID_NOT_AFTER.WITHIN(<time1>, <time2>):**

  Renvoie une valeur booléenne TRUE si le temps se trouve dans toutes les plages définies par les éléments dans <time1> et <time2>.

  Si vous omettez un élément de temps de <time1>, il est supposé avoir la valeur la plus faible dans sa plage. Si vous omettez un élément de <time2>, il est supposé avoir la valeur la plus élevée de sa plage. Si vous spécifiez une année dans <time1>, vous devez la spécifier dans <time2>.

  Les plages pour les éléments de temps sont les suivantes : mois 1-12, jour 1-31, jour de semaine 0-6, heure 0-23, minutes 0-59 et secondes 0-59. Pour que le résultat soit TRUE, chaque élément dans le temps doit exister dans la plage correspondante que vous spécifiez dans <time1>, <time2>.

  Par exemple, si l'heure est GMT 2005 10 mai 10h 15m 30s et que c'est le deuxième mardi du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont entre parenthèses) :

  - . . .within(GMT 2004, GMT 2006) (TRUE)
  - . . .within(GMT 2004 Jan, GMT 2006 Mar) (FALSE, May n'est pas compris entre janvier et mars.)
  - . . .within(GMT Feb, GMT) (TRUE, May est dans la plage de février à décembre.)

- . . .within(GMT Sun_1, GMT Sun_3) (TRUE, le deuxième mardi se situe entre le premier dimanche et le troisième dimanche.)
- . . .within(GMT 2005 May 1 10h, GMT May 2005 1 17h) (TRUE)
- . . .within(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE ou FALSE, selon le fuseau horaire du système Citrix ADC)

- **<certificate>.VALID_NOT_AFTER.YEAR:**

  Extrait la dernière année pendant laquelle le certificat est valide et renvoie un entier à quatre chiffres.

- **<certificate>.VALID_NOT_BEFORE:**

  Renvoie la date à laquelle le certificat client devient valide.

  Le format de retour est le nombre de secondes depuis le 1er janvier 1970 GMT (0 heures, 0 minutes, 0 secondes).

- **<certificate>.VALID_NOT_BEFORE.BETWEEN(<time1>, <time2>):**

  Renvoie une valeur booléenne TRUE si la valeur de temps est comprise entre les deux arguments de temps. Les deux arguments <time1> et <time2> doivent être entièrement spécifiés.

  Voici des exemples :

  GMT 1995 Jan est entièrement spécifié.
  GMT Jan n'est pas entièrement spécifié.
  GMT 1995 20 n'est pas entièrement spécifié.
  GMT Jan Mon_2 n'est pas entièrement spécifié.
  Les arguments de temps doivent être GMT ou tous les deux LOCAL, et <time2> doit être supérieur à <time1>.

  Par exemple, si la valeur d'heure est GMT 2005 1er mai 10h 15m 30s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats d'évaluation de cet exemple sont entre parenthèses) :

  - . . .between(GMT 2004, GMT 2006) (TRUE)
  - . . .between(GMT 2004 Jan, GMT 2006 Nov) (TRUE)
  - . . .between(GMT 2004 Jan, GMT 2006) (TRUE)
  - . . .between(GMT 2005 May Sun_1, GMT 2005 May Sun_3) (TRUE)
  - . . .between(GMT 2005 May 1, GMT May 2005 1) (TRUE)
  - . . .between(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE ou FALSE, selon le fuseau horaire du système Citrix ADC.)

- **<certificate>.VALID_NOT_BEFORE.DAY:**

  Extrait le dernier jour du mois pendant lequel le certificat est valide et renvoie cette valeur sous la forme d'un nombre compris entre 1 et 31 représentant ce jour.

- **<certificate>.VALID_NOT_BEFORE.EQ(<time>):**

  Renvoie une valeur booléenne TRUE si la durée est égale à l' <time> argument.

  Par exemple, si la valeur d'heure est GMT 2005 1er mai 10h 15m 30s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats d'évaluation de cet exemple sont entre parenthèses) :

  - . . .eq(GMT 2005) (TRUE)
  - . . .eq(GMT 2005 Dec) (FALSE)
  - . . .eq(LOCAL 2005 May) (TRUE ou FALSE, selon le fuseau horaire actuel.)
  - . . .eq(GMT May 10h) (TRUE)
  - . . .eq(GMT 10h 30s) (TRUE)
  - . . .eq(GMT May 10h) (TRUE)
  - . . .eq(GMT Sun) (TRUE)
  - . . .eq(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_BEFORE.GE(<time>):**

  Renvoie une valeur booléenne TRUE si le temps est supérieur (après) ou égal à l' <time> argument.

  Par exemple, si la valeur d'heure est GMT 2005 1er mai 10h 15m 30s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont entre parenthèses) :

  - . . .ge(GMT 2004) (TRUE)
  - . . .ge(GMT 2005 Jan) (TRUE)
  - . . .ge(LOCAL 2005 May) (TRUE ou FALSE, selon le fuseau horaire actuel.)
  - . . .gt(GMT 8h) (TRUE)
  - . . .ge(GMT 30m) (FALSE)
  - . . .ge(GMT May 10h) (TRUE)
  - . . .ge(GMT May 10h 0m) (TRUE)
  - . . .ge(GMT Sun) (TRUE)
  - . . .ge(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_BEFORE.GT(<time>):**

  Renvoie une valeur booléenne TRUE si l'heure se produit après l' <time> argument.

  Par exemple, si la valeur d'heure est GMT 2005 1er mai 10h 15m 30s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont entre parenthèses) :

  - . . .gt(GMT 2004) (TRUE)
  - . . .gt(GMT 2005 Jan) (TRUE)
  - . . .gt(LOCAL 2005 May) (TRUE ou FALSE, selon le fuseau horaire actuel.)

- . . .gt(GMT 8h) (TRUE)
- . . .gt(GMT 30m) (FALSE)
- . . .gt(GMT May 10h) (FALSE)
- . . .gt(GMT May 10h 0m) (TRUE)
- . . .gt(GMT Sun) (FALSE)
- . . .gt(GMT May Sun_1) (FALSE)

- **<certificate>.VALID_NOT_BEFORE.HOURS:**

  Extrait la dernière heure pendant laquelle le certificat est valide et renvoie cette valeur sous la forme d'un entier compris entre 0 et 23.

- **<certificate>.VALID_NOT_BEFORE.LE (<time>)

  Renvoie une valeur booléenne TRUE si l'heure précède ou est égale à l' <time> argument.

  Par exemple, si la valeur d'heure est GMT 2005 1er mai 10h 15m 30s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats d'évaluation de cet exemple sont entre parenthèses) :

  - . . .le(GMT 2006) (TRUE)
  - . . .le(GMT 2005 Dec) (TRUE)
  - . . .le(LOCAL 2005 May) (TRUE ou FALSE, selon le fuseau horaire actuel.)
  - . . .le(GMT 8h) (FALSE)
    . - . .le(GMT 30m) (TRUE)
  - . . .le(GMT May 10h) (TRUE)
  - . . .le(GMT Jun 11h) (TRUE)
  - . . .le(GMT Wed) (TRUE)
  - . . .le(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_BEFORE.LT(<time>):**

  Renvoie une valeur booléenne TRUE si l'heure précède l' <time> argument.

  Par exemple, si la valeur d'heure est GMT 2005 1er mai 10h 15m 30s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats d'évaluation de cet exemple sont entre parenthèses) :

  - . . .lt(GMT 2006) (TRUE)
  - . . .lt(GMT 2005 Dec) (TRUE)
  - . . .lt(LOCAL 2005 May) (TRUE ou FALSE, selon le fuseau horaire actuel.)
  - . . .lt(GMT 8h) (FALSE)
  - . . .lt(GMT 30m) (TRUE)
  - . . .lt(GMT May 10h) (FALSE)
  - . . .lt(GMT Jun 11h) (TRUE)
  - . . .lt(GMT Wed) (TRUE)

- . . .lt(GMT May Sun_1) (FALSE)

- **<certificate>.VALID_NOT_BEFORE.MINUTES:**

  Extrait la dernière minute que le certificat est valide. Renvoie la minute actuelle sous la forme d'un entier compris entre 0 et 59.

- **<certificate>.VALID_NOT_BEFORE.MONTH:**

  Extrait le dernier mois de validité du certificat. Renvoie le mois courant sous la forme d'un entier compris entre 1 (janvier) et 12 (décembre).

- **<certificate>.VALID_NOT_BEFORE.RELATIVE_BOOT:**

  Calcule le nombre de secondes par rapport au redémarrage Citrix ADC N, puis renvoie un entier. Si l'heure de démarrage la plus proche est dans le passé, l'entier est négatif ; s'il est dans le futur, l'entier est positif.

- **<certificate>.VALID_NOT_BEFORE.RELATIVE_NOW:**

  Renvoie le nombre de secondes entre l'heure système Citrix ADC en cours et l'heure spécifiée sous forme d'entier. Si l'heure désignée est dans le passé, l'entier est négatif. Si c'est dans le futur, l'entier est positif.

- **<certificate>.VALID_NOT_BEFORE.SECONDS:**

  Extrait la dernière seconde que le certificat est valide. Retourne la seconde courante sous la forme d'un entier compris entre 0 et 59.

- **<certificate>.VALID_NOT_BEFORE.WEEKDAY:**

  Extrait le dernier jour de semaine pendant lequel le certificat est valide. Renvoie le jour de la semaine sous la forme d'un nombre compris entre 0 (dimanche) et 6 (samedi).

- **<certificate>.VALID_NOT_BEFORE.WITHIN(<time1>, <time2>):**

  Renvoie une valeur booléenne TRUE si chaque élément de temps existe dans la plage définie dans les <time1> <time2> arguments,.

  Si vous omettez un élément de temps de <time1>, il est supposé avoir la valeur la plus faible dans sa plage. Si vous omettez un élément de temps de <time2>, il est supposé avoir la valeur la plus élevée dans sa plage. Si vous spécifiez une année dans <time1>, il doit être spécifié dans <time2>. Les plages pour les éléments de temps sont les suivantes : mois 1-12, jour 1-31, jour de semaine 0-6, heure 0-23, minutes 0-59 et secondes 0-59.

  Par exemple, si l'heure est GMT 2005 10 mai 10h 15m 30s, et que c'est le deuxième mardi du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont entre parenthèses) :

  - . . .within(GMT 2004, GMT 2006) (TRUE)
  - . . .within(GMT 2004 Jan, GMT 2006 Mar) (FALSE, May n'est pas compris entre janvier et mars.)

  - . . .within(GMT Feb, GMT) (TRUE, May se situe entre février et décembre.)
  - . . .within(GMT Sun_1, GMT Sun_3) (TRUE, le deuxième mardi se situe entre le premier dimanche et le troisième dimanche.)
  - . . .within(GMT 2005 May 1 10h, GMT May 2005 1 17h) (TRUE)
  - . . .within(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE ou FALSE, selon le fuseau horaire du système Citrix ADC)

- **<certificate>.VALID_NOT_BEFORE.YEAR:**

  Extrait la dernière année de validité du certificat. Renvoie l'année en cours sous la forme d'un entier à quatre chiffres.

Expressions pour les dates de requête et de réponse HTTP

October 5, 2021

Les préfixes d'expression suivants renvoient le contenu de l'en-tête Date HTTP sous forme de texte ou d'objet date. Ces valeurs peuvent être évaluées comme suit :

- En tant que numéro. La valeur numérique d'un en-tête HTTP Date est renvoyée sous la forme du nombre de secondes écoulées depuis le 1er janvier 1970.

  Par exemple, l'expression http.req.date.mod (86400) renvoie le nombre de secondes écoulées depuis le début de la journée. Ces valeurs peuvent être évaluées en utilisant les mêmes opérations que d'autres données numériques non liées à la date. Pour plus d'informations, voir Préfixes d'expression pour les données numériques autres que la date et l'heure.

- En tant qu'en-tête HTTP. Les en-têtes de date peuvent être évalués en utilisant les mêmes opérations que les autres en-têtes HTTP.

  Pour plus d'informations, consultez Expressions de stratégie avancées : analyse des données HTTP, TCP et UDP.

- Comme texte. Les en-têtes de date peuvent être évalués en utilisant les mêmes opérations que les autres chaînes.

Pour plus d'informations, voir Expressions de stratégie avancées : évaluation du texte.

Prefix	Description
HTTP.REQ.DATE	Renvoie le contenu de l'en-tête HTTP Date sous forme de texte ou d'objet date. Les formats de date reconnus sont : RFC822. Dim, 06 Jan 1980 08:49:37 GMT, RFC 850. Dimanche, 06-Jan-80 09:49:37 GMT, et ASCTIME. Dim. 6 janv. 08:49:37 1980.
HTTP.RES.DATE	Renvoie le contenu de l'en-tête HTTP Date sous forme de texte ou d'objet date. Les formats de date reconnus sont : RFC822. Dim, 06 Jan 1980 8:49:37 GMT, RFC 850. Dimanche 6 janvier 80 9 : 49 : 37 GMT, et ASCTIME. Dim. 6 janv. 08:49:37 1980.

Générer le jour de la semaine, sous forme de chaîne, en formats courts et longs

January 21, 2021

Les fonctions,`WEEKDAY_STRING_SHORT` et`WEEKDAY_STRING`, génèrent le jour de la semaine, sous forme de chaîne, en formats courts et longs, respectivement. Les chaînes renvoyées sont toujours en anglais. Le préfixe utilisé avec ces fonctions doit renvoyer le jour de la semaine au format entier et la plage acceptable pour la valeur renvoyée par le préfixe est 0-6. Par conséquent, vous pouvez utiliser n'importe quel préfixe qui renvoie un entier dans la plage acceptable. Une condition UNDEF est déclenchée si la valeur renvoyée n'est pas dans cette plage ou si l'allocation de mémoire échoue.

Voici les descriptions des fonctions :

Fonction	Description
<prefix>.WEEKDAY_STRING_SHORT	Renvoie le jour de la semaine en format court. La forme abrégée est toujours de 3 caractères avec une majuscule initiale et les caractères restants en minuscules. Par exemple, SYS.TIME.WEEKDAY.WEEKDAY_STRING_SHORTrenvoie Sun si la valeur renvoyée par la fonction WEEKDAY est 0 et Sat si la valeur renvoyée par le préfixe est 6.
<prefix>.WEEKDAY_STRING	Renvoie le jour de la semaine en format long. La forme longue a toujours une majuscule initiale, avec les caractères restants en minuscules. Par exemple,SYS.TIME.WEEKDAY.WEEKDAY_STRING renvoie Sunday si la valeur renvoyée par la fonction WEEKDAY est 0 et Saturday si la valeur renvoyée par le préfixe est 6.

Préfixes d'expression pour les données numériques autres que la date et l'heure

August 20, 2021

Outre la configuration d'expressions fonctionnant à temps, vous pouvez configurer des expressions pour les types de données numériques suivants :

- La longueur des requêtes HTTP, le nombre d'en-têtes HTTP dans une requête, etc.

  Pour plus d'informations, consultez Expressions pour les données de charge utile HTTP numériques autres que les dates.

- Adresses IP et MAC.

  Pour plus d'informations, voir Expressions pour adresses IP et sous-réseauxIP.

- Données client et serveur en ce qui concerne les ID d'interface et le débit de transaction.

  Pour plus d'informations, voir Expressions pour données numériques client et serveur.

- Données numériques dans les certificats clients autres que les dates.

Pour plus d'informations sur ces préfixes, y compris le nombre de jours avant l'expiration du certificat et la taille de la clé de chiffrement, consultez Préfixes pour les données numériques dans les certificats SSL.

Conversion de nombres en texte

August 20, 2021

Les fonctions suivantes produisent des chaînes binaires à partir d'un nombre renvoyé par un préfixe d'expression. Ces fonctions sont particulièrement utiles dans la fonction de réécriture TCP en tant que chaînes de remplacement pour les données binaires. Pour plus d'informations sur la fonction de réécriture TCP, voir Réécriture.

Toutes les fonctions renvoient une valeur de type texte. L'endianness que certaines fonctions acceptent comme paramètre est LITTLE_ENDIAN ou BIG_ENDIAN.

Fonction	Description
<number>.SIGNED8_STRING	Produit une chaîne binaire signée de 8 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).GET_SIGNED8(16).SUB(3).SIGNED8_STR
<number>.UNSIGNED8_STRING	Produit une chaîne binaire non signée de 8 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).GET_UNSIGNED8(31).ADD(3).UNSIGNED
<number>.SIGNED16_STRING(<endianness>)	Produit une chaîne binaire signée de 16 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).SKIP(12).GET_SIGNED16(0, BIG_ENDIAN).SUB(4).SIGNED16_STRING(BIG_ENDIAN)

Fonction	Description
<number>.UNSIGNED16_STRING(<endianness>)	Produit une chaîne binaire non signée de 16 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).GET_UNSIGNED16(47, LIT-TLE_ENDIAN).ADD(7).UNSIGNED16_STRING(LITTLE_ENDIAN)
<number>.SIGNED32_STRING (<endianness>)	Produit une chaîne binaire signée 32 bits représentant le nombre. Exemple : HTTP.REQ.BODY(100).AFTER_STR(“delim”).GET_SIGNED32(0, BIG_ENDIAN).SUB(1).SIGNED32_STRING(BIG_ENDIAN)
<unsigned_long_number>.UNSIGNED8_STRING	Produit une chaîne binaire non signée de 8 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).GET_UNSIGNED8(24).TYPECAST_UNSIG
<unsigned_long_number>.UNSIGNED16_STRING	Produit une chaîne binaire non signée de 16 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).GET_UNSIGNED16(23, LIT-TLE_ENDIAN).TYPECAST_UNSIGNED_LONG_AT.ADD(10).UNSIG
<unsigned_long_number>.UNSIGNED32_STRING(<endianness>)	Produit une chaîne binaire non signée 32 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).AFTER_STR(“delim2”).GET_UNSIGNED3 BIG_ENDIAN).ADD(2).UNSIGNED32_STRING(BIG_ENDIAN)

Expressions basées sur un serveur virtuel

October 5, 2021

Le préfixe `SYS.VSERVER("<vserver-name>")` d’expression vous permet d’identifier un serveur

virtuel. Vous pouvez utiliser les fonctions suivantes avec ce préfixe pour récupérer des informations relatives au serveur virtuel spécifié :

- **DÉBIT.** Renvoie le débit du serveur virtuel en Mbps (mégabits par seconde). La valeur renvoyée est un nombre long non signé.

  Utilisation : SYS.VSERVER (« vserver ») .THROUGHPUT

- **CONNEXIONS.** Renvoie le nombre de connexions gérées par le serveur virtuel. La valeur renvoyée est un nombre long non signé.

  Utilisation : SYS.VSERVER (« vserver ») .CONNECTIONS

- **ÉTAT.** Renvoie l'état du serveur virtuel. La valeur renvoyée est UP, DOWN ou OUT_OF_SERVICE. L'une de ces valeurs peut donc être passée en argument à l'opérateur EQ () pour effectuer une comparaison qui aboutit à une valeur booléenne TRUE ou FALSE.

  Utilisation : SYS.VSERVER (« vserver ») .STATE

- **SANTÉ.** Renvoie le pourcentage de services en état UP pour le serveur virtuel spécifié. La valeur renvoyée est un nombre entier.

  Utilisation : SYS.VSERVER (« vserver ») .HEALTH

- **RESPTIME.** Renvoie le temps de réponse sous la forme d'un nombre entier représentant le nombre de microsecondes. Le temps de réponse est le TTFB (Time To First Byte) moyen de tous les services liés au serveur virtuel.

  Utilisation : SYS.VSERVER (« vserver ») .RESPTIME

- **SURGECOUNT.** Renvoie le nombre de demandes dans la file d'attente de surtension du serveur virtuel. La valeur renvoyée est un nombre entier.

  Utilisation : SYS.VSERVER (« vserver ») .SURGECOUNT

Exemple 1 :

La stratégie de réécriture suivante interrompt le traitement de réécriture si le nombre de connexions sur le serveur virtuel d'équilibrage de charge LBVServer dépasse 10 000 :

```
add rewrite policy norewrite_pol sys.vserver("LBvserver").connections.gt
(10000)norewrite
```

Exemple 2 :

L'action de réécriture suivante insère un en-tête personnalisé, TP, dont la valeur est le tout au long du serveur virtuel LBVServer :

```
add rewrite action tp_header insert_http_header TP SYS.VSERVER("LBvserver")
.THROUGHPUT
```

Exemple 3 :

L'action de message de journal d'audit suivante écrit le TTFB moyen des services liés à un serveur virtuel, dans le fichier journal newnslog :

```
add audit messageaction log_vserver_resptime_act INFORMATIONAL "\"NS
Response Time to Servers:\" + sys.vserver(\"ssllb\").resptime + \" millisec
\""-logtoNewnslog YES
```

Expressions de stratégie avancées : analyse des données HTTP, TCP et UDP

October 5, 2021

Vous pouvez configurer des expressions de stratégie avancées pour évaluer la charge utile dans une demande ou une réponse HTTP. La charge utile associée à une connexion HTTP inclut les en-têtes HTTP (en-têtes standard ou personnalisés), le corps et l'URL de connexion. Vous pouvez également évaluer et traiter la charge utile dans un paquet TCP ou UDP. Pour les connexions HTTP, par exemple, vous pouvez vérifier si un en-tête HTTP particulier est présent ou si l'URL inclut un paramètre de requête particulier.

Vous pouvez configurer des expressions pour transformer le codage URL et appliquer un codage HTML ou XML « sécurisé » pour une évaluation ultérieure. Vous pouvez également utiliser les préfixes XPATH et JSON pour évaluer la date dans les fichiers XML et JSON, respectivement.

Pour plus d'informations sur les expressions d'authentification telles que AAA.USER, AAA.LOGIN, voir Authentification, autorisation et audit de connexion et pour l'expression AAA.AUTHENTICATION, consultez Rubriques d'authentification utilisateur Citrix ADC AAA .

Vous pouvez également utiliser des expressions de stratégie avancées basées sur le texte et numériques pour évaluer les données de requête et de réponse HTTP. Pour plus d'informations, consultez les sections Expressions de stratégie avancées : évaluation du texte et Expressions de stratégie avancées : utilisation des dates, des heures et des nombres.

Expressions pour identifier le protocole dans un paquet IP entrant

August 20, 2021

Le tableau suivant répertorie les expressions que vous pouvez utiliser pour identifier le protocole dans un paquet entrant.

Expression.	Description
CLIENT.IP.PROTOCOL	Identifie le protocole dans les paquets IPv4 envoyés par les clients.
CLIENT.IPV6.PROTOCOL	Identifie le protocole dans les paquets IPv6 envoyés par les clients.
SERVER.IP.PROTOCOL	Identifie le protocole dans les paquets IPv4 envoyés par les serveurs.
SERVER.IPV6.PROTOCOL	Identifie le protocole dans les paquets IPv6 envoyés par les serveurs.

Arguments de la fonction PROTOCOL

Vous pouvez transmettre le numéro de protocole IANA (Internet Assigned Numbers Authority) à la fonction PROTOCOLE. Par exemple, si vous voulez déterminer si le protocole d'un paquet entrant est TCP, vous pouvez utiliser CLIENT .IP.PROTOCOL.EQ(6), où 6 est le numéro de protocole attribué à l'IANA pour TCP. Pour certains protocoles, vous pouvez passer une valeur d'énumération au lieu du numéro de protocole. Par exemple, au lieu de CLIENT.IP.PROTOCOL.EQ(6), vous pouvez utiliser CLIENT.IP.PROTOCOL.EQ (TCP). Le tableau suivant répertorie les protocoles pour lesquels vous pouvez utiliser des valeurs d'énumération et les valeurs d'énumération correspondantes à utiliser avec la fonction PROTOCOL.

Protocole	Valeur d'énumération
Protocole de contrôle de transmission (TCP)	TCP
Protocole de datagramme utilisateur (UDP)	UDP
Protocole ICMP (Internet Control Message Protocol)	ICMP
En-tête d'authentification IP (AH), pour fournir des services d'authentification dans IPv4 et IPv6	AH
Protocole ESP (encapsulation de la charge utile de sécurité)	ESP
Encapsulation générale de routage (GRE)	GRE
Protocole d'encapsulation IP dans IP	IPIP
Protocole de message de contrôle Internet pour IPv6 (ICMPv6)	ICMPv6

Protocole	Valeur d'énumération
En-tête de fragment pour IPv6	FRAGMENT

Scénarios de cas d'utilisation

Les expressions de protocole peuvent être utilisées à la fois dans les stratégies basées sur la demande et sur la réponse. Vous pouvez utiliser les expressions dans diverses fonctionnalités de Citrix ADC, telles que l'équilibrage de charge, l'optimisation du réseau étendu, la commutation de contenu, la réécriture et les stratégies d'écoute. Vous pouvez utiliser les expressions avec des fonctions telles que EQ () et NE (), pour identifier le protocole dans une stratégie et effectuer une action.

Voici quelques cas d'utilisation pour les expressions :

- Dans les configurations d'équilibrage de charge de Branch Repeater, vous pouvez utiliser les expressions dans une stratégie d'écoute pour le serveur virtuel générique. Par exemple, vous pouvez configurer le serveur virtuel générique avec la stratégie d'écoute CLIENT .IP.PROTOCOL.EQ (TCP) de sorte que le serveur virtuel traite uniquement le trafic TCP et ponts simplement tout le trafic non-TCP. Même si vous pouvez utiliser une liste de contrôle d'accès au lieu de la stratégie d'écoute, la stratégie d'écoute offre un meilleur contrôle sur le trafic traité.
- Pour les serveurs virtuels de commutation de contenu de type ANY, vous pouvez configurer des stratégies de commutation de contenu qui changent les demandes sur la base du protocole dans les paquets entrants. Par exemple, vous pouvez configurer des stratégies de commutation de contenu pour diriger tout le trafic TCP vers un serveur virtuel d'équilibrage de charge et tout le trafic non-TCP vers un autre serveur virtuel d'équilibrage de charge.
- Vous pouvez utiliser les expressions basées sur le client pour configurer la persistance en fonction du protocole. Par exemple, vous pouvez utiliser CLIENT.IP.PROTOCOL pour configurer la persistance sur la base des protocoles dans les paquets IPv4 entrants.

Expressions pour les en-têtes HTTP et de contrôle de cache

August 20, 2021

Une méthode courante d'évaluation du trafic HTTP consiste à examiner les en-têtes d'une requête ou d'une réponse. Un en-tête peut effectuer un certain nombre de fonctions, notamment les suivantes :

- Fournissez des cookies qui contiennent des données sur l'expéditeur.
- Identifiez le type de données transmises.
- Identifiez l'itinéraire parcouru par les données (en-tête Via).

> **Remarque**
>
> Si une opération est utilisée pour évaluer les données d'en-tête et de texte, l'opération basée sur l'en-tête remplace toujours l'opération basée sur le texte. Par exemple, l'opération AFTER_STR, lorsqu'elle est appliquée à un en-tête, remplace les opérations AFTER_STR basées sur le texte pour toutes les instances du type d'en-tête actuel.

Préfixes pour les en-têtes HTTP

Le tableau Préfixes pour les en-têtes HTTP pour les préfixes d'expression qui extrait les en-têtes HTTP.

Opérations pour les en-têtes HTTP

Le tableau Opérations pour en-têtes HTTP pour les opérations que vous pouvez spécifier avec les préfixes des en-têtes HTTP.

Préfixes pour les en-têtes de contrôle de cache

Les préfixes suivants s'appliquent spécifiquement aux en-têtes Cache-Control.

Préfixe d'en-tête HTTP	Description
HTTP.REQ.CACHE_CONTROL	Renvoie un en-tête Cache-Control dans une requête HTTP.
HTTP.RES.CACHE_CONTROL	Renvoie un en-tête Cache-Control dans une réponse HTTP.

Opérations pour les en-têtes de contrôle de cache

Vous pouvez appliquer n'importe quelle opération pour les en-têtes HTTP aux en-têtes Cache-Control.

En outre, les opérations suivantes identifient des types spécifiques d'en-têtes Cache-Control. Reportez-vous à la section RFC 2616 pour plus d'informations sur ces types d'en-tête.

Opération d'en-tête HTTP	Description
`Cache-Control header.NAME(<integer>)`	Renvoie sous forme de valeur de texte le nom de l'en-tête Cache-Control qui correspond au nième composant d'une liste nom-valeur, comme spécifié par`<integer>`. L'index du composant nom-valeur est basé sur 0. Si le `<integer>` qui est spécifié par l'argument entier est supérieur au nombre de composants dans la liste, un objet texte de longueur nulle est renvoyé. Voici un exemple : `http.req.cache_control.name(3).contains("some_text")`
Cache-Control header.IS_INVALID	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control n'est pas présent dans la requête ou la réponse. Voici un exemple : `http.req.cache_control.is_invalid`
`Cache-Control header.IS_PRIVATE`	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Private. Voici un exemple : `http.req.cache_control.is_private`
Cache-Control header.IS_PUBLIC	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Private. Voici un exemple : http.req.cache_control.is_public
Cache-Control header.IS_NO_STORE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur No-Store. Voici un exemple : http.req.cache_control.is_no_store
Cache-Control header.IS_NO_CACHE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur No-Cache. Voici un exemple : http.req.cache_control.is_no_cache
Cache-Control header.IS_MAX_AGE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Max-Age. Voici un exemple : http.req.cache_control.is_max_age
Cache-Control header.IS_MIN_FRESH	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Min-Fresh. Voici un exemple : http.req.cache_control.is_min_fresh

Opération d'en-tête HTTP	Description
Cache-Control header.IS_MAX_STALE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Max-Stale. Voici un exemple : http.req.cache_control.is_max_stale
Cache-Control header.IS_MUST_REVALIDATE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Doit-Revalidate. Voici un exemple : http.req.cache_control.is_must_revalidate
Cache-Control header.IS_NO_TRANSFORM	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur No-Transform. Voici un exemple : http.req.cache_control.is_no_transform
Cache-Control header.IS_ONLY_IF_CACHED	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Only-If-Cached. Voici un exemple : http.req.cache_control.is_only_if_cached
Cache-Control header.IS_PROXY_REVALIDATE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Proxy-Revalidate. Voici un exemple : http.req.cache_control.is_proxy_revalidate
Cache-Control header.IS_S_MAXAGE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur S-Maxage. Voici un exemple : http.req.cache_control.is_s_maxage
Cache-Control header.IS_UNKNOWN	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control est d'un type inconnu. Voici un exemple : http.req.cache_control.is_unknown
Cache-Control header.MAX_AGE	Renvoie la valeur de l'en-tête Cache-Control Max-Age. Si cet en-tête est absent ou non valide, 0 est renvoyé. Voici un exemple : http.req.cache_control.max_age.le(3)
Cache-Control header.MAX_STALE	Renvoie la valeur de l'en-tête Cache-Control Max-Stale. Si cet en-tête est absent ou non valide, 0 est renvoyé. Voici un exemple : http.req.cache_control.max_stale.le(3)

Opération d'en-tête HTTP	Description
Cache-Control header.MIN_FRESH	Renvoie la valeur de l'en-tête Cache-Control Min-Fresh. Si cet en-tête est absent ou non valide, 0 est renvoyé. Voici un exemple : http.req.cache_control.min_fresh.le (3)
Cache-Control header.S_MAXAGE	Renvoie la valeur de l'en-tête Cache-Control S-Maxage. Si cet en-tête est absent ou non valide, 0 est retourné.Folor est un exemple : http.req.cache_control.s_maxage.eq (2)

Expressions pour extraire des segments d'URL

August 20, 2021

Vous pouvez extraire des URL et des parties d'URL, telles que le nom d'hôte ou un segment du chemin d'URL. Par exemple, l'expression suivante identifie les requêtes HTTP pour les fichiers image en extrayant les suffixes de fichier image de l'URL :

```
http.req.url.suffix.eq("jpeg")|| http.req.url.suffix.eq("gif")
```

La plupart des expressions pour URL fonctionnent sur du texte et sont décrites dans Préfixes d'expression pour le texte dans les requêtes et réponses HTTP. Cette section traite de l'opération GET. L'opération GET extrait du texte lorsqu'elle est utilisée avec les préfixes suivants :

- HTTP.REQ.URL.PATH
- VPN.BASEURL.PATH
- VPN.CLIENTLESS_BASEURL.PATH

Le tableau suivant décrit les préfixes des URL HTTP.

Préfixe d'URL	Description
HTTP.REQ.URL.PATH.GET(<n>)	Renvoie une liste séparée par barre oblique (« / ») du chemin d'URL. Par exemple, considérez l'URL suivante :<http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1>. L'expression suivante renvoie dir1 à partir de cette URL :<http.req.url.path.get(1)>. L'expression suivante renvoie dir2 : http.req.url.path.get (2)
HTTP.REQ.URL.PATH.GET_REVERSE(<n>)	Retourne une liste slash- (« / ») séparée du chemin d'URL, à partir de la fin du chemin d'accès. Par exemple, considérez l'URL suivante :<http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1>. L'expression suivante renvoie index.html à partir de cette URL :<http.req.url.path.get_reverse(0)>. L'expression suivante renvoie dir3 : http.req.url.path.get_reverse(1)

Expressions pour les codes d'état HTTP et les données de charge utile HTTP numériques autres que les dates

January 21, 2021

Le tableau suivant décrit les préfixes pour les valeurs numériques dans les données HTTP autres que les dates.

Prefix	Description
HTTP.REQ.CONTENT_LENGTH	Renvoie la longueur d'une requête HTTP sous la forme d'un nombre. Voici un exemple : http.req.content_length < 500
HTTP.RES.CONTENT_LENGTH	Renvoie la longueur de la réponse HTTP sous la forme d'un nombre. Voici un exemple : http.res.content_length <= 1000
HTTP.RES.STATUS	Retourne le code d'état de la réponse

Prefix	Description
HTTP.RES.IS_REDIRECT	Renvoie une valeur booléenne TRUE si le code de réponse est associé à une redirection. Voici les codes de réponse de redirection : 300 (choix multiples), 301 (déplacement permanent), 302 (trouvé), 303 (voir autre), 305 (utilisation proxy) et 307 (redirection temporaire). Remarque : Le code d'état 304 n'est pas considéré comme un code d'état de la réponse HTTP de redirection. Le code d'état 306 n'est pas utilisé.

Opérations pour le codage HTTP, HTML et XML et caractères « sûrs »

August 20, 2021

Les opérations suivantes fonctionnent avec l'encodage des données HTML dans une requête ou une réponse et des données XML dans un corps POST.

- **<text>.HTML_XML_SAFE :**
  transforme les caractères spéciaux en format XML sécurisé, comme dans les exemples suivants :

  Un support d'angle pointant vers la gauche (<) est converti en <
  Un support d'angle pointant vers la droite (>) est converti en
  Une esperluette (&) est convertie en &
  Cette opération protège contre les attaques de script intersites. La longueur maximale du texte transformé est de 2048 octets. Il s'agit d'une opération en lecture seule.

  Après avoir appliqué la transformation, les opérateurs supplémentaires que vous spécifiez dans l'expression sont appliqués au texte sélectionné. Voici un exemple :

  http.req.url.query.html_xml_safe. contains("myQueryString")

- **<text>.HTTP_HEADER_SAFE :**
  Convertit tous les nouveaux caractères de ligne ('n') dans le texte d'entrée en '%0A' pour permettre à l'entrée d'être utilisée en toute sécurité dans les en-têtes HTTP.

  Cette opération protège contre les attaques qui séparent les interventions.

  La longueur maximale du texte transformé est de 2048 octets. Il s'agit d'une opération en lecture seule.

- **<text>.HTTP_URL_SAFE:**
  Convertit les caractères d'URL non sécurisés en valeurs '%xx', où "xx" est une représentation

hexagonale du caractère d'entrée. Par exemple, l'esperluette (&) est représentée comme%26 dans le codage sécurisé URL. La longueur maximale du texte transformé est de 2048 octets. Il s'agit d'une opération en lecture seule.

Voici les caractères sécurisés URL. Tous les autres sont dangereux :

- Caractères alphanumériques : a-z, A-Z, 0-9
- Astérix : « * »
- Esperluette : « & »
- Signe arobase : « @ »
- Deux-points : « : »
- Virgule : « , »
- Dollar : « $ »
- Dot: "."
- Egal à : « = »
- Point d'exclamation : « ! »
- Tiret : « - »
- Ouvrir et fermer les parenthèses : « (« , «) »
- Pourcentage : « % »
- Plus : « + »
- point-virgule : « ; »
- Citation simple : « ' »
- Barre oblique : « / »
- Point d'interrogation : « ? »
- Tilde : « ~ »
- Soulignement : « _ »

- **<text>.MARK_SAFE:**

  Marque le texte comme sûr sans appliquer aucun type de transformation de données.

- **<text>.SET_TEXT_MODE(URLENCODED|NOURLENCODED)**

  Transforme tout le codage %HH dans le flux d'octets. Cette opération fonctionne avec des caractères (pas des octets). Par défaut, un octet unique représente un caractère dans le codage ASCII. Toutefois, si vous spécifiez le mode URLENCODED, trois octets peuvent représenter un caractère.

  Dans l'exemple suivant, une opération PREFIX (3) sélectionne les 3 premiers caractères d'une cible.

  ```
  http.req.url.hostname.prefix(3)
  ```

  Dans l'exemple suivant, Citrix ADC peut sélectionner jusqu'à 9 octets de la cible :

  ```
  http.req.url.hostname.set_text_mode(urlencoded).prefix(3)
  ```


- **<text>.SET_TEXT_MODE(PLUS_AS_SPACE|NO_PLUS_AS_SPACE):**

  Spécifie comment traiter le caractère plus (+). L'option PLUS_AS_SPACE remplace un caractère plus par un espace blanc. Par exemple, le texte "hello+world" devient "hello world." L'option NO_PLUS_AS_SPACE laisse les caractères plus tels qu'ils sont.

- **<text>.SET_TEXT_MODE(BACKSLASH_ENCODED|NO_BACKSLASH_ENCODED):**

  Spécifie si le décodage de barre oblique inverse est effectué sur l'objet texte représenté par <text>.

  Si BACKSLASH_ENCODED est spécifié, l'opérateur SET_TEXT_MODE effectue les opérations suivantes sur l'objet texte :

  - Toutes les occurrences de "\XXX" seront remplacées par le caractère "Y" (où XXX représente un nombre dans le système octal et Y représente l'équivalent ASCII de XXX). La plage valide de valeurs octales pour ce type d'encodage est de 0 à 377. Par exemple, le texte codé "http\72//" et http\072//" seront tous les deux décodés sur <http://>, où le deux-points (:) est l'équivalent ASCII de la valeur octale "72".
  - Toutes les occurrences de "\xHH" seront remplacées par le caractère "Y" (HH représente un nombre dans le système hexadécimal et Y indique l'équivalent ASCII de HH. Par exemple, le texte codé "http\x3a//" sera décodé sur <http://>, où le deux-points (:) est l'équivalent ASCII de la valeur hexadécimale "3a".
  - Toutes les occurrences de "\uWWXX" seront remplacées par la séquence de caractères "YZ" (où WW et XX représentent deux valeurs hexadécimales distinctes et Y et Z représentent leurs équivalents ASCII de WW et XX respectivement. Par exemple, le texte codé "http%u3a2f/" et "http%u003a//" seront tous les deux décodés<http://>, où "3a" et "2f" sont deux valeurs hexadécimales et les deux-points (:) et la barre oblique ("/") représentent leurs équivalents ASCII respectivement.
  - Toutes les occurrences de "\b", "\n", "\t", "\f" et "\r" sont remplacées par les caractères ASCII correspondants.

  Si NO_BACKSLASH_ENCODED est spécifié, le décodage de la barre oblique inverse n'est pas effectué sur l'objet texte.

- **<text>.SET_TEXT_MODE(BAD_ENCODE_RAISE_UNDEF|NO_BAD_ENCODE_RAISE_UNDEF):**

  Effectue l'action non définie associée si le mode URLENCODED ou BACKSLASH_ENCODED est défini et si un codage incorrect correspondant au mode de codage spécifié est rencontré dans l'objet texte représenté par <text>.

  Si NO_BAD_ENCODE_RAISE_UNDEF est spécifié, l'action non définie associée ne sera pas exécutée lorsque le codage est incorrect dans l'objet texte représenté par <text>.

Expressions pour les données TCP, UDP et VLAN

August 20, 2021

Les données TCP et UDP prennent la forme d'une chaîne ou d'un nombre. Pour les préfixes d'expression qui renvoient des valeurs de chaîne pour les données TCP et UDP, vous pouvez appliquer toutes les opérations basées sur le texte. Pour plus d'informations, voir Expressions de stratégie avancées : évaluation du texte.

Pour les préfixes d'expression qui renvoient une valeur numérique, comme un port source, vous pouvez appliquer une opération arithmétique. Pour plus d'informations, voir Opérations de base sur les préfixes d'expression et Opérations composées pour les nombres.

Le tableau suivant décrit les préfixes qui extraient les données TCP et UDP.

Opération GET	Description
`CLIENT.TCP.PAYLOAD(<integer>)`	Retourne les données de charge utile TCP sous forme de chaîne, en commençant par le premier caractère de la charge utile et en continuant le nombre de caractères dans l'argument `<integer>`. Vous pouvez appliquer n'importe quelle opération de texte à ce préfixe.
CLIENT.TCP.SRCPORT	Renvoie l'ID du port source du paquet courant sous forme de nombre.
CLIENT.TCP.DSTPORT	Renvoie l'ID du port de destination du paquet courant sous forme de nombre.
CLIENT.TCP.OPTIONS	Renvoie les options TCP définies par le client. Exemples d'options TCP : Taille maximale de segment (MSS), Échelle de fenêtre, Accusés de réception sélectifs (SACK) et Option d'horodatage. Les opérateurs COUNT, TYPE(<type>) et TYPE_NAME(<m>) peuvent être utilisés avec ce préfixe. Pour connaître les options TCP définies par le serveur, consultez le préfixe SERVER.TCP.OPTIONS.
CLIENT.TCP.OPTIONS.COUNT	Renvoie le nombre d'options TCP définies par le client.

Opération GET	Description
CLIENT.TCP.OPTIONS.TYPE(<type>)	Renvoie la valeur de l'option TCP dont le type (ou type d'option) est spécifié comme argument. La valeur est renvoyée sous la forme d'une chaîne d'octets au format big endian (ou dans l'ordre des octets réseau). Paramètres : type - Valeur de type
CLIENT.TCP.OPTIONS.TYPE_NAME(<m>)	Renvoie la valeur de l'option TCP dont la constante d'énumération est spécifiée comme argument. Les constantes d'énumération que vous pouvez transmettre en tant qu'argument sont REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW et MAXSEG. Pour spécifier le type d'option TCP au lieu de ces constantes d'énumération, utilisez CLIENT.TCP.OPTIONS.TYPE (<type>). Pour les autres options TCP, vous devez utiliser CLIENT.TCP.OPTIONS.TYPE(<type>). Paramètres : m - Constante d'énumération d'option TCP
CLIENT.TCP.REPEATER_OPTION.EXISTS	Renvoie une valeur booléenne TRUE si les options TCP du répéteur existent.
CLIENT.TCP.REPEATER_OPTION.IP	Renvoie l'adresse IPv4 du répéteur de branche à partir des options TCP du répéteur.
CLIENT.TCP.REPEATER_OPTION.MAC	Renvoie l'adresse MAC du répéteur de branche à partir des options TCP du répéteur.
CLIENT.UDP.DNS.DOMAIN	Renvoie le nom de domaine DNS.
CLIENT.UDP.DNS.DOMAIN.EQ("<hostname>")	Renvoie une valeur booléenne TRUE si le nom de domaine correspond à l'<hostname> argument. La comparaison est insensible à la casse. Voici un exemple : client.udp.dns.domain.eq (« www.mycompany.com »)
CLIENT.UDP.DNS.IS_AAAAREC	Renvoie une valeur booléenne TRUE si le type d'enregistrement est AAAA. Ces types d'enregistrements indiquent une adresse IPv6 dans les recherches prospectives.

Opération GET	Description
CLIENT.UDP.DNS.IS_ANYREC	Renvoie une valeur booléenne TRUE si elle est de n'importe quel type d'enregistrement.
CLIENT.UDP.DNS.IS_AREC	Renvoie une valeur de type Boolean TRUE si l'enregistrement est de type A. Les enregistrements de type A fournissent l'adresse de l'hôte.
CLIENT.UDP.DNS.IS_CNAMEREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type CNAME. Dans les systèmes qui utilisent plusieurs noms pour identifier une ressource, il existe un nom canonique et un certain nombre d'alias. Le CNAME fournit le nom canonique.
CLIENT.UDP.DNS.IS_MXREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type MX (échangeur de messagerie). Cet enregistrement DNS décrit une priorité et un nom d'hôte. Les enregistrements MX pour le même nom de domaine spécifient les serveurs de messagerie dans le domaine et la priorité pour chaque serveur.
CLIENT.UDP.DNS.IS_NSREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type NS. Il s'agit d'un enregistrement de serveur de noms qui inclut un nom d'hôte associé à un enregistrement A. Cela permet de localiser le nom de domaine associé à l'enregistrement NS.
CLIENT.UDP.DNS.IS_PTRREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type PTR. Il s'agit d'un pointeur de nom de domaine et est souvent utilisé pour associer un nom de domaine à une adresse IPv4.
CLIENT.UDP.DNS.IS_SOAREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type SOA. C'est un début d'enregistrement d'autorité.

Opération GET	Description
CLIENT.UDP.DNS.IS_SRVREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type SRV. Ceci est une version plus générale de l'enregistrement MX.
CLIENT.UDP.DSTPORT	Renvoie l'ID numérique du port de destination UDP du paquet courant.
CLIENT.UDP.SRCPORT	Renvoie l'ID numérique du port source UDP du paquet courant.
CLIENT.UDP.RADIUS	Retourne les données RADIUS du paquet courant.
CLIENT.UDP.RADIUS.ATTR_TYPE(<type>)	Renvoie la valeur du type d'attribut spécifié comme argument.
CLIENT.UDP.RADIUS.USERNAME	Renvoie le nom d'utilisateur RADIUS.
CLIENT.TCP.MSS	Renvoie la taille maximale du segment (MSS) de la connexion en cours sous forme de nombre.
CLIENT.VLAN.ID	Renvoie l'ID numérique du VLAN via lequel le paquet courant est entré dans le Citrix ADC.
SERVER.TCP.DSTPORT	Renvoie l'ID numérique du port de destination du paquet courant.
SERVER.TCP.SRCPORT	Renvoie l'ID numérique du port source du paquet courant.
SERVER.TCP.OPTIONS	Renvoie les options TCP définies par le serveur. Exemples d'options TCP : Taille maximale de segment (MSS), Échelle de fenêtre, Accusés de réception sélectifs (SACK) et Option d'horodatage. Les opérateurs COUNT, TYPE(<type>) et TYPE_NAME(<m>) peuvent être utilisés avec ce préfixe. Pour connaître les options TCP définies par le client, consultez le préfixe CLIENT.TCP.OPTIONS.
SERVER.TCP.OPTIONS.COUNT	Renvoie le nombre d'options TCP définies par le serveur.

Opération GET	Description
SERVER.TCP.OPTIONS.TYPE(<type>)	Renvoie la valeur de l'option TCP dont le type (ou type d'option) est spécifié comme argument. La valeur est renvoyée sous la forme d'une chaîne d'octets au format big endian (ou dans l'ordre des octets réseau). Paramètres : type - Valeur de type
SERVER.TCP.OPTIONS.TYPE_NAME(<m>)	Renvoie la valeur de l'option TCP dont la constante d'énumération est spécifiée comme argument. Les constantes d'énumération que vous pouvez transmettre en tant qu'argument sont REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW et MAXSEG. Pour spécifier le type d'option TCP au lieu de ces constantes d'énumération, utilisez CLIENT.TCP.OPTIONS.TYPE (<type>). Pour les autres options TCP, vous devez utiliser CLIENT.TCP.OPTIONS.TYPE(<type>). Paramètres : m - Constante d'énumération d'option TCP
SERVER.VLAN	Fonctionne sur le VLAN via lequel le paquet courant est entré dans le Citrix ADC.
SERVER.VLAN.ID	Renvoie l'ID numérique du VLAN via lequel le paquet courant est entré dans le Citrix ADC.

Expressions pour évaluer un message DNS et identifier son protocole porteur

January 21, 2021

Vous pouvez évaluer les demandes DNS et les réponses à l'aide d'expressions commençant par DNS.REQ et DNS.RES respectivement. Vous pouvez également identifier le protocole de la couche de transport utilisé pour envoyer les messages DNS.

Les fonctions suivantes renvoient le contenu d'une requête DNS.

Fonction	Description
DNS.REQ.QUESTION.DOMAIN	Retourne le nom de domaine (la valeur du champ QNAME) dans la section question de la requête DNS. Le nom de domaine est renvoyé sous la forme d'une chaîne de texte, qui peut être transmise à EQ(), NE() et à toute autre fonction qui fonctionne avec du texte.
DNS.REQ.QUESTION.TYPE	Retourne le type de requête (la valeur du champ QTYPE) dans la requête DNS. Le champ indique le type d'enregistrement de ressource (par exemple, A, NS ou CNAME) pour lequel le serveur de noms est interrogé. La valeur renvoyée peut être comparée à l'une des valeurs suivantes à l'aide des fonctions EQ () et NE () : A, AAAA, NS, SRV, PTR, CNAME, SOA, MX et ANY. Remarque : Vous pouvez utiliser uniquement les fonctions EQ () et NE () avec la fonction TYPE. Exemple : DNS.REQ.QUESTION .TYPE.EQ (MX)

Les fonctions suivantes renvoient le contenu d'une réponse DNS.

Fonction	Description
DNS.RES.HEADER.RCODE	Retourne le code de réponse (la valeur du champ RCODE) dans la section d'en-tête de la réponse DNS. Vous pouvez utiliser uniquement les fonctions EQ() et NE() avec la fonction RCODE. Voici les valeurs possibles : NOERROR, FORMERR, SERVFAIL, NXDOMAIN, NOTIMP et REFUSED.
DNS.RES.QUESTION.DOMAIN	Retourne le nom de domaine (la valeur du champ QNAME) dans la section question de la réponse DNS. Le nom de domaine est renvoyé sous la forme d'une chaîne de texte, qui peut être transmise à EQ(), NE() et à toute autre fonction qui fonctionne avec du texte.

Fonction	Description
DNS.RES.QUESTION.TYPE	Retourne le type de requête (la valeur du champ QTYPE) dans la section question de la réponse DNS. Le champ indique le type d'enregistrement de ressource (par exemple, A, NS ou CNAME) contenu dans la réponse. La valeur renvoyée peut être comparée à l'une des valeurs suivantes à l'aide des fonctions EQ () et NE () : A, AAAA, NS, SRV, PTR, CNAME, SOA, MX et ANY. Vous pouvez utiliser uniquement les fonctions EQ () et NE () avec la fonction TYPE. Exemple : DNS.RES.QUESTION .TYPE.EQ(SOA)

Les fonctions suivantes renvoient le nom du protocole de la couche de transport.

Fonction	Description
DNS.REQ.TRANSPORT	Retourne le nom du protocole de la couche de transport utilisé pour envoyer la requête DNS. Les valeurs possibles renvoyées sont TCP et UDP. Vous pouvez utiliser uniquement les fonctions EQ() et NE() avec la fonction TRANSPORT. Exemple : DNS.REQ.TRANSPORT.EQ(TCP)
DNS.RES.TRANSPORT	Retourne le nom du protocole de couche de transport utilisé pour la réponse DNS. Les valeurs possibles renvoyées sont TCP et UDP. Vous pouvez utiliser uniquement les fonctions EQ() et NE() avec la fonction TRANSPORT. Exemple : DNS.RES.TRANSPORT.EQ(TCP)

Expressions XPath et HTML, XML ou JSON

August 20, 2021

L'infrastructure de stratégie avancée prend en charge les expressions permettant d'évaluer et de

récupérer des données à partir de fichiers JSON (HTML, XML et JavaScript Object Notation). Cela vous permet de rechercher des nœuds spécifiques dans un document HTML, XML ou JSON, de déterminer si un nœud existe dans le fichier, de localiser des nœuds dans des contextes XML (par exemple, des nœuds qui ont des parents spécifiques ou un attribut spécifique avec une valeur donnée) et de renvoyer le contenu de ces nœuds. En outre, vous pouvez utiliser les expressions XPath dans les expressions de réécriture.

L'implémentation de l'expression de stratégie avancée pour XPath comprend un préfixe d'expression de stratégie avancée (tel que « HTTP.REQ.BODY ») qui désigne du texte HTML ou XML, et l'opérateur XPATH qui prend l'expression XPath comme argument.

Les fichiers HTML sont une collection largement libre de balises et d'éléments de texte. Vous pouvez utiliser l'opérateur XPATH_HTML, qui prend une expression XPath comme argument, pour traiter les fichiers HTML. Les fichiers JSON sont soit une collection de paires nom/valeur, soit une liste ordonnée de valeurs. Vous pouvez utiliser l'opérateur XPATH_JSON, qui prend une expression XPath comme argument, pour traiter les fichiers JSON.

- **<text>.XPATH(xpathex):**

  Opérer sur un fichier XML et renvoyer une valeur booléenne.

  Par exemple, l'expression suivante renvoie une valeur booléenne TRUE si un nœud appelé « creator » existe sous le nœud « Book » dans les 1000 premiers octets du fichier XML.

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%boolean(//Book/creator)%)
  ```

  Paramètres :

  xpathex - Expression booléenne XPath

- **<text>.XPATH(xpathex):**

  Opérer sur un fichier XML et renvoyer une valeur de type de données “double.”

  Par exemple, l'expression suivante convertit la chaîne « 36” (une valeur de prix) en une valeur de type de données « double » si la chaîne se trouve dans les 1000 premiers octets du fichier XML :

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%number(/Book/price)%)
  ```

  Paramètres :

  xpathex - Expression numérique XPath

Exemple :

```
1     <Book>
2     <creator>
3         <Person>
4             <name>Milton</name>
5         </Person>
```



```
6      </creator>
7      <title>Paradise Lost</title>
8      </Book>
9  <!--NeedCopy-->
```

- **<text>.XPATH(xpathex):**

  Opérer sur un fichier XML et renvoyer un jeu de nœuds ou une chaîne. Les ensembles de nœuds sont convertis en chaînes correspondantes à l'aide de la routine de conversion de chaînes XPath standard.

  Par exemple, l'expression suivante sélectionne tous les nœuds qui sont entourés par « /book/creator » (un ensemble de nœuds) dans les 1000 premiers octets du corps :

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%/Book/creator%)
  ```

  Paramètres :

  xpathex - Expression XPath

- **<text>.XPATH_HTML(xpathex)**

  Fonctionnez sur un fichier HTML et renvoyez une valeur de texte.

  Par exemple, l'expression suivante fonctionne sur un fichier HTML et renvoie le texte enfermé dans les balises <title\></title\> si l'élément HTML titre se trouve dans les 1000 premiers octets :

  ```
  HTTP.REQ.BODY(1000).XPATH_HTML(xp%/html/head/title%)
  ```

  Paramètres :

  xpathex - Expression de texte XPath

- **<text>.XPATH_HTML_WITH_MARKUP(xpathex)**

  Fonctionnez sur un fichier HTML et renvoyez une chaîne contenant la totalité de la partie sélectionnée du document, y compris le balisage, par exemple l'inclusion des balises d'élément englobant.

  L'expression suivante fonctionne sur le fichier HTML et sélectionne tout le contenu de la balise <\title> balise, y compris le balisage.

  ```
  HTTP.REQ.BODY(1000).XPATH_HTML_WITH_MARKUP( xp%/html/head/title%)
  ```

  La partie du corps HTML sélectionnée par l'expression est marquée pour un traitement ultérieur.

  Paramètres :

  xpathex - Expression XPath

- **<text>.XPATH_JSON(xpathex)**

  Opérer sur un fichier JSON et renvoyer une valeur booléenne.

  Par exemple, considérez le fichier JSON suivant :

  { ”Book”:{ ”creator”:{ ”person”:{ ”name”:’<name>’ } }, ”title”:’<title>’ } }

  L’expression suivante fonctionne sur le fichier JSON et renvoie une valeur booléenne TRUE si le fichier JSON contient un nœud nommé « creator », dont le nœud parent est « Book », dans les 1000 premiers octets :

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%boolean(/Book/creator)%)
  ```

  Paramètres :

  xpathex - Expression booléenne XPath

- **<text>.XPATH_JSON(xpathex)**

  Opérer sur un fichier JSON et renvoyer une valeur de type de données “double.”

  Par exemple, considérez le fichier JSON suivant :

  { ”Book”:{ ”creator”:{ ”person”:{ ”name”:’<name>’ } }, ”title”:’<title>’, ”price”:”36” } }

  L’expression suivante fonctionne sur le fichier JSON et convertit la chaîne “36” en une valeur de type de données « double » si la chaîne est présente dans les 1000 premiers octets du fichier JSON.

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%number(/Book/price)%)
  ```

  Paramètres :

  xpathex - Expression numérique XPath

- **<text>.XPATH_JSON(xpathex)**

  Opérer sur un fichier JSON et renvoyer un jeu de nœuds ou une chaîne. Les ensembles de nœuds sont convertis en chaînes correspondantes à l’aide de la routine de conversion de chaînes XPath standard.

  Par exemple, considérez le fichier JSON suivant :

  { ”Book”:{ ”creator”:{ ”person”:{ ”name”:’<name>’ } }, ”title”:’<title>’ } }

  L’expression suivante sélectionne tous les nœuds qui sont entourés par « /Book » (un jeu de nœuds) dans les 1000 premiers octets du corps du fichier JSON et renvoie la valeur de chaîne correspondante, qui est »<name><title>”:

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%/Book%)
  ```

  Paramètres :

  xpathex - Expression XPath

- **<text>.XPATH_JSON_WITH_MARKUP (xpathex)**

  Fonctionnez sur un fichier XML et renvoyez une chaîne contenant toute la partie du document pour le nœud de résultat, y compris le balisage comme l'inclusion des balises d'élément englobant.

  Par exemple, considérez le fichier JSON suivant :

  {"Book":{ "creator":{ "person":{ "name":'<name>' } }, "title":'<title>' } }

  L'expression suivante fonctionne sur le fichier JSON et sélectionne tous les nœuds qui sont entourés par « /book/creator » dans les 1000 premiers octets du corps, qui est "creator:{ person:{ name:'<name>' } }."

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON_WITH_MARKUP(xp%/Book/creator%)
  ```

  La partie du corps JSON sélectionnée par l'expression est marquée pour un traitement ultérieur.

  Paramètres :

  xpathex - Expression XPath

- **<text>.XPATH_WITH_MARKUP (xpathex) :**

  Fonctionnez sur un fichier XML et renvoyez une chaîne contenant toute la partie du document pour le nœud de résultat, y compris le balisage comme l'inclusion des balises d'élément englobant.

  Par exemple, l'expression suivante fonctionne sur un fichier XML et sélectionne tous les nœuds entourés par « /book/creator » dans les 1000 premiers octets du corps.

  ```
  HTTP.REQ.BODY(1000).XPATH_WITH_MARKUP(xp%/Book/creator%)
  ```

  La partie du corps JSON sélectionnée par l'expression est marquée pour un traitement ultérieur.

  Paramètres :

  xpathex - Expression XPath

Crypter et décrypter les charges utiles XML

October 5, 2021

Vous pouvez utiliser les fonctions XML_ENCRYPT () et XML_DECRYPT () dans les expressions de stratégie avancées pour chiffrer et déchiffrer, respectivement, les données XML. Ces fonctions sont conformes à la norme W3C XML Encryption définie à l'adresse "http://www.w3.org/TR/2001/PR-xmldsig-core-20010820/. « XML_ENCRYPT () et XML_DECRYPT () prennent en charge un sous-ensemble de la spécification XML Encryption. Dans le sous-ensemble, le chiffrement des données

utilise une méthode de chiffrement en bloc (RC4, DES3, AES128, AES192 ou AES256), et une clé publique RSA est utilisée pour chiffrer la clé de chiffrement en bloc.

Remarque : Si vous souhaitez chiffrer et déchiffrer du texte dans une charge utile, vous devez utiliser les fonctions ENCRYPT et DECRYPT. Pour plus d'informations sur ces fonctions, voir Chiffrer et déchiffrer du texte.

Les fonctions XML_ENCRYPT () et XML_DECRYPT () ne dépendent pas du service de chiffrement et de déchiffrement utilisé par les commandes ENCRYPT et DECRYPT pour le texte. La méthode de chiffrement est spécifiée explicitement en tant qu'argument de la fonction XML_ENCRYPT (). La `XML_DECRYPT()` fonction obtient les informations relatives à la méthode de chiffrement spécifiée à partir de l' `<xenc:EncryptedData>` élément. Voici des synopsis des fonctions de chiffrement et de déchiffrement XML :

- `XML_ENCRYPT(<certKeyName>, <method> [, <flags>])**. Returns an <xenc:EncryptedData>` qui contient le texte d'entrée chiffré et la clé de chiffrement, qui est elle-même chiffrée à l'aide de RSA.
- `XML_DECRYPT(<certKeyName>)`. Renvoie le texte déchiffré de l' `<xenc:EncryptedData>` élément d'entrée, qui inclut la méthode de chiffrement et la clé chiffrée RSA.

Remarque : L' `<xenc:EncryptedData>` élément est défini dans la spécification W3C XML Encryption.

Voici une description des arguments :

- **CertKeyName :** sélectionne un certificat X.509 avec une clé publique RSA pour XML_ENCRYPT () ou une clé privée RSA pour XML_DECRYPT (). La clé de certificat doit avoir été créée au préalable par une `add ssl certKey` commande.
- **method :** spécifie la méthode de chiffrement à utiliser pour chiffrer les données XML. Valeurs possibles : RC4, DES3, AES128, AES192, AES256.
- **flags :** masque de bits spécifiant les informations clés facultatives suivantes (`<ds:KeyInfo>`) à inclure dans l' `<xenc:EncryptedData>` élément généré par `XML_ENCRYPT()` :
  - **1** - Incluez un élément KeyName avec le CertKeyName. L'élément est `<ds:KeyName>`.
  - **2** - Incluez un élément KeyValue avec la clé publique RSA du certificat. L'élément est `<ds:KeyValue>`.
  - **4** - Incluez un élément X509IssuerSerial avec le numéro de série du certificat et le nom unique de l'émetteur. L'élément est `<ds:X509IssuserSerial>`.
  - **8** - Inclut un élément X509SubjectName avec le nom unique de l'objet du certificat. L'élément est `<ds:X509SubjectName>`.
  - **16** - Incluez un élément X509Certificate avec l'intégralité du certificat. L'élément est `<ds:X509Certificate>`.

Utiliser les fonctions XML_ENCRYPT () et XML_DECRYPT () dans les expressions

La fonctionnalité de cryptage XML utilise des paires de clés de certificat SSL pour fournir des certificats X.509 (avec des clés publiques RSA) pour le chiffrement des clés et des clés privées RSA pour le déchiffrement des clés. Par conséquent, avant d'utiliser la fonction XML_ENCRYPT () dans une expression, vous devez créer une paire de clés de certificat SSL. La commande suivante crée une paire de clés de certificat SSL, my-certkey, avec le certificat X.509, my-cert.pem et le fichier de clé privée, my-key.pem.

```
add ssl certKey my-certkey -cert my-cert.pem -key my-key.pem -passcrypt
kxPeMRYnitY=
```

Les commandes CLI suivantes créent des actions de réécriture et des stratégies de chiffrement et de déchiffrement du contenu XML.

```
1  add rewrite action my-xml-encrypt-action replace "HTTP.RES.BODY(10000).
       XPATH_WITH_MARKUP(xp%/%)" "HTTP.RES.BODY(10000).XPATH_WITH_MARKUP(xp
       %/%).XML_ENCRYPT("my-certkey", AES256, 31)"
2
3  add rewrite action my-xml-decrypt-action replace "HTTP.REQ.BODY(10000).
       XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%)" "HTTP.REQ.BODY(10000).
       XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%).XML_DECRYPT("my-certkey"
       )"
4
5  add rewrite policy my-xml-encrypt-policy "HTTP.REQ.URL.CONTAINS("xml-
       encrypt")" my-xml-encrypt-action
6
7  add rewrite policy my-xml-decrypt-policy "HTTP.REQ.BODY(10000).XPATH(xp
       %boolean(//xenc:EncryptedData)%)" my-xml-decrypt-action
8
9  bind rewrite global my-xml-encrypt-policy 30
10
11 bind rewrite global my-xml-decrypt-policy 30
12 <!--NeedCopy-->
```

Dans l'exemple ci-dessus, l'action de réécriture my-xml-encrypt-action chiffre l'intégralité du document XML (XPATH_WITH_MARKUP (xp%/%)) dans la demande à l'aide de la méthode de chiffrement en bloc AES-256 et de la clé publique RSA de my-certkey pour chiffrer la clé de chiffrement en bloc. L'action remplace le document par un <xenc:EncryptedData> élément contenant les données chiffrées et une clé chiffrée. Les drapeaux représentés par 31 incluent tous les <ds:KeyInfo> éléments facultatifs.

L'action my-xml-decrypt-action déchiffre le premier <xenc:EncryptedData> élément de la réponse (XPATH_WITH_MARKUP (XP%//XENC:EncryptedData%)). Cela nécessite l'ajout préalable de l'espace de noms XML xenc à l'aide de la commande CLI suivante :


```
add ns xmlnamespace xenc http://www.w3.org/2001/04/xmlenc##
```

L'action my-xml-decrypt-action utilise la clé privée RSA dans my-certkey pour déchiffrer la clé chiffrée, puis utilise la méthode de chiffrement en bloc spécifiée dans l'élément pour déchiffrer le contenu chiffré. Enfin, l'action remplace l'élément de données chiffré par le contenu déchiffré.

La stratégie de réécriture my-xml-encrypt-policy applique my-xml-encrypt-action aux demandes d'URL contenant xml-encrypt. L'action chiffre l'intégralité de la réponse d'un service configuré sur l'appliance Citrix ADC.

La stratégie de réécriture my-xml-decrypt-policy applique my-xml-decrypt-action aux requêtes qui contiennent un <xenc:EncryptedData> élément (XPATH (XP%//XENC:EncryptedData%) renvoie une chaîne non vide). L'action déchiffre les données chiffrées dans les demandes liées à un service configuré sur l'appliance Citrix ADC.

Expressions de stratégie avancées : analyse SSL

August 20, 2021

Il existe des expressions de stratégie avancées pour analyser les certificats SSL et les messages de bonjour client SSL.

Analyser les certificats SSL

Vous pouvez utiliser des expressions de stratégie avancées pour évaluer les certificats client SSL (Secure Sockets Layer) X.509. Un certificat client est un document électronique qui peut être utilisé pour authentifier l'identité d'un utilisateur. Un certificat client contient (au minimum) des informations de version, un numéro de série, un ID d'algorithme de signature, un nom d'émetteur, une période de validité, un nom de sujet (utilisateur), une clé publique et des signatures.

Vous pouvez examiner à la fois les connexions SSL et les données dans les certificats clients. Par exemple, vous pouvez envoyer des requêtes SSL qui utilisent des chiffrements de faible puissance à une batterie de serveurs virtuels d'équilibrage de charge particulière. La commande suivante est un exemple de stratégie Commutation de contenu qui analyse la force de chiffrement dans une requête et correspond aux forces de chiffrement inférieures ou égales à 40 :

```
1 add cs policy p1 -rule "client.ssl.cipher_bits.le(40)"
2 <!--NeedCopy-->
```

Autre exemple, vous pouvez configurer une stratégie qui détermine si une demande contient un certificat client :


```
1 add cs policy p2 -rule "client.ssl.client_cert exists"
2 <!--NeedCopy-->
```

Vous pouvez également configurer une stratégie qui examine des informations particulières dans un certificat client. Par exemple, la stratégie suivante vérifie que le certificat a un ou plusieurs jours avant l'expiration :

```
1 add cs policy p2 -rule "client.ssl.client_cert exists && client.ssl.
     client_cert.days_to_expire.ge(1)"
2 <!--NeedCopy-->
```

> **Remarque**
>
> Pour plus d'informations sur l'analyse des dates et des heures dans un certificat, voir Format des dates et heures dans une expression et des expressions pour les dates de certificat SSL.

Préfixes pour les données SSL et de certificat basées sur le texte

Le tableau suivant décrit les préfixes d'expression qui identifient les éléments textuels dans les transactions SSL et les certificats clients.

Tableau 1. Préfixes renvoyant du texte ou des valeurs booléennes pour SSL et les données de certificat client

Prefix	Description
CLIENT.SSL.CLIENT_CERT	Renvoie le certificat client SSL dans la transaction SSL actuelle.
CLIENT.SSL.CLIENT_CERT.TO_PEM	Renvoie le certificat client SSL au format binaire.
CLIENT.SSL.CIPHER_EXPORTABLE	Renvoie une valeur booléenne TRUE si le chiffrement cryptographique SSL cryptographique SSL est exportable.
CLIENT.SSL.CIPHER_NAME	Renvoie le nom du chiffrement SSL s'il est invoqué à partir d'une connexion SSL, et une chaîne NULL s'il est invoqué à partir d'une connexion non SSL.
CLIENT.SSL.IS_SSL	Renvoie une valeur booléenne TRUE si la connexion actuelle est basée sur SSL.

Préfixes pour les données numériques dans les certificats SSL

Le tableau suivant décrit les préfixes qui évaluent des données numériques autres que les dates dans les certificats SSL. Ces préfixes peuvent être utilisés avec les opérations décrites dans Opérations de base sur les préfixes d'expression et Opérations composées pour les nombres.

Tableau 2. Préfixes qui évaluent des données numériques autres que les dates dans les certificats SSL

Prefix	Description
CLIENT.SSL.CLIENT_CERT.DAYS_TO_EXPIRE	Renvoie le nombre de jours pendant lesquels le certificat est valide ou renvoie -1 pour les certificats expirés.
CLIENT.SSL.CLIENT_CERT.PK_SIZE	Renvoie la taille de la clé publique utilisée dans le certificat.
CLIENT.SSL.CLIENT_CERT.VERSION	Renvoie le numéro de version du certificat. Si la connexion n'est pas basée sur SSL, renvoie zéro (0).
CLIENT.SSL.CIPHER_BITS	Renvoie le nombre de bits dans la clé cryptographique. Renvoie 0 si la connexion n'est pas basée sur SSL.
CLIENT.SSL.VERSION	Renvoie un nombre qui représente la version du protocole SSL, comme suit : 0. La transaction n'est pas basée sur SSL. ; 0x002. La transaction est SSLv2. ; 0x300. La transaction est SSLv3. ; 0x301. La transaction est TLSv1. ; 0x302. La transaction est TLS 1.1. ; 0x303. La transaction est TLS 1.2 ; 0x304. La transaction est TLS 1.3.

> **Remarque**
>
> Pour les expressions liées aux dates d'expiration d'un certificat, voir Expressions pour les dates de certificat SSL.

Expressions pour les certificats SSL

Vous pouvez analyser les certificats SSL en configurant les expressions qui utilisent le préfixe suivant :

CLIENT.SSL.CLIENT_CERT

Cette section décrit les expressions que vous pouvez configurer pour les certificats, à l'exception des

expressions qui examinent l'expiration du certificat. Les opérations temporelles sont décrites dans Expressions de stratégie avancées : utilisation des dates, des heures et des nombres.

Le tableau suivant décrit les opérations que vous pouvez spécifier pour le préfixe CLIENT.SSL.CLIENT_CERT.

Tableau 3. Opérations pouvant être spécifiées avec le préfixe CLIENT.SSL.CLIENT_CERT

Opération de certificat SSL	Description
`<certificate>.EXISTS`	Renvoie une valeur booléenne TRUE si le client possède un certificat SSL.
`<certificate>.ISSUER`	Renvoie le nom distinctif (DN) de l'émetteur dans le certificat sous forme de liste nom-valeur. Un signe égal (« = ») est le délimiteur du nom et de la valeur, et la barre oblique (« / ») est le délimiteur qui sépare les paires nom-valeur. Voici un exemple de DN renvoyé : `/C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycompany.com`
`<certificate>.ISSUER.IGNORE_EMPTY_ELEMENTS`	Renvoie l'émetteur et ignore les éléments vides dans une liste nom-valeur. Par exemple, considérez ce qui suit : Cert-Issuer: /c=in/st=kar//l=bangelore //o=mycompany/ou=sales/ /emailAddress=myuserid@mycompany.com. L'action Réécriture suivante renvoie un nombre de 6 en fonction de la définition précédente de l'émetteur : `sh rewrite action insert_ssl_header Name: insert_ssl Operation: insert_http_header Target:Cert-Issuer Value:CLIENT.SSL.CLIENT_CERT.ISSUER.COUNT`. Toutefois, si vous modifiez la valeur suivante, le nombre retourné est 9 :`CLIENT.SSL.CLIENT_CERT.ISSUER.IGNORE_EMPTY_ELEMENTS.COUNT`

Analyser le client SSL hello

Vous pouvez analyser le message Hello client SSL en configurant les expressions qui utilisent le préfixe suivant :

Prefix	Description
CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXC(	Correspond au code hexadécimal fourni dans l'expression avec les codes hexadécimaux des suites de chiffrement reçues dans le message de bonjour client.
CLIENT.SSL.CLIENT_HELLO.CLIENT_VERSION	Version reçue dans l'en-tête du message client Hello.
CLIENT.SSL.CLIENT_HELLO.IS_RENEGOTIATE	Renvoie true si un client ou un serveur initie la renégociation de session.
CLIENT.SSL.CLIENT_HELLO.IS_REUSE	Renvoie true si l'appliance réutilise la session SSL en fonction de l'ID de session non nul reçu dans le message client Hello.
CLIENT.SSL.CLIENT_HELLO.IS_SCSV	Renvoie true si la fonction Signalisation Cipher Suite Value (SCSV) est annoncée dans le message de bonjour client. Le code hexadécimal pour SCSV de secours est 0x5600.
CLIENT.SSL.CLIENT_HELLO.IS_SESSION_TICKET	Renvoie true si l'extension de ticket de session avec une longueur différente de zéro est annoncée dans le message client Hello.
CLIENT.SSL.CLIENT_HELLO.LENGTH	Longueur reçue dans l'en-tête du message Hello client.
CLIENT.SSL.CLIENT_HELLO.SNI	Renvoie le nom du serveur reçu dans l'extension Nom du serveur du message bonjour du client.
CLIENT.SSL.CLIENT_HELLO.ALPN.HAS_NEXTPRC	Renvoie true si le protocole d'application dans l'extension ALPN reçu dans le message bonjour client correspond au protocole fourni dans l'expression.

Ces expressions peuvent être utilisées au point de liaison CLIENTHELLO_REQ. Pour plus d'informations, voir Liaison de stratégie SSL.

Expressions de stratégie avancées : adresses IP et MAC, débit, ID VLAN

October 5, 2021

Vous pouvez utiliser des préfixes d'expression de stratégie avancée qui renvoient des adresses IPv4 et IPv6, des adresses MAC, des sous-réseaux IP, des données client et serveur utiles telles que les débits aux ports d'interface (Rx, Tx et RxTx) et les ID des VLAN via lesquels les paquets sont reçus. Vous pouvez ensuite utiliser différents opérateurs pour évaluer les données renvoyées par ces préfixes d'expression.

Expressions pour adresses IP et sous-réseaux IP

Vous pouvez utiliser des expressions de stratégie avancées pour évaluer les adresses et les sous-réseaux qui sont au format IPv4 (Internet Protocol version 4) ou IPv6 (Internet Protocol version 6). Les préfixes d'expression des adresses et sous-réseaux IPv6 incluent IPv6 dans le préfixe. Les préfixes d'expression des adresses et sous-réseaux IPv4 incluent l'adresse IP dans le préfixe. Voici un exemple d'expression qui identifie si une demande provient d'un sous-réseau IPv4 particulier.

```
client.ip.src.in_subnet(147.1.0.0/16)
<!--NeedCopy-->
```

Voici deux exemples de stratégies de réécriture qui examinent le sous-réseau à partir duquel le paquet est reçu et effectuent une action de réécriture sur l'en-tête Host. Une fois ces deux stratégies configurées, l'action de réécriture effectuée dépend du sous-réseau de la demande. Ces deux stratégies évaluent les adresses IP au format d'adresse IPv4.

```
- add rewrite action URL1-rewrite-action replace "http.req.header("Host
   ")" ""www.mycompany1.com""
- add rewrite policy URL1-rewrite-policy "http.req.header("Host").
   contains("www.test1.com") && client.ip.src.in_subnet(147.1.0.0/16)"
   URL1-rewrite-action
- add rewrite action URL2-rewrite-action replace "http.req.header("Host
   ")" ""www.mycompany2.com""
- add rewrite policy URL2-rewrite-policy "http.req.header("Host").
   contains("www.test2.com") && client.ip.src.in_subnet(10.202.0.0/16)"
    URL2-rewrite-action
<!--NeedCopy-->
```

> **Remarque**
>
> Les exemples précédents sont des commandes que vous tapez sur l'interface de ligne de commande (CLI) de Citrix ADC et, par conséquent, chaque guillemet doit être précédé d'une

> barre oblique inverse (\). Pour plus d'informations, voir Configuration d'expressions de stratégie avancées dans une stratégie."

Préfixes pour les adresses IPV4 et les sous-réseaux IP

Le tableau suivant décrit les préfixes qui renvoient des adresses et des sous-réseaux IPv4, ainsi que des segments d'adresses IPv4. Vous pouvez utiliser des opérateurs numériques et des opérateurs spécifiques aux adresses IPv4 avec ces préfixes. Pour plus d'informations sur les opérations numériques, voir « Opérations debase sur les préfixes d'expression » et « Opérations composées pour les nombres ».

Tableau 1. Préfixes qui évaluent les adresses IP et MAC

Prefix	Description
CLIENT.IP.SRC	Renvoie l'adresse IP source du paquet actuel sous forme d'adresse IP ou de numéro.
CLIENT.IP.DST	Renvoie l'adresse IP de destination du paquet actuel sous forme d'adresse IP ou de numéro.
SERVEUR.IP.SRC	Renvoie l'adresse IP source du paquet actuel sous forme d'adresse IP ou de numéro.
SERVEUR.IP.DST	Renvoie l'adresse IP de destination du paquet actuel sous forme d'adresse IP ou de numéro.

Opérations pour les adresses IPV4

Le tableau Prefix for IPV4 Operations décrit les opérateurs pouvant être utilisés avec des préfixes renvoyant une adresse IPv4.

A propos des expressions IPv6

Le format d'adresse IPv6 offre plus de flexibilité que l'ancien format IPv4. Les adresses IPv6 sont au format hexadécimal (RFC 2373). Dans les exemples suivants, l'exemple 1 est une adresse IPv6, l'exemple 2 est une URL qui inclut l'adresse IPv6 et l'exemple 3 inclut l'adresse IPv6 et un numéro de port.

Exemple 1 :

```
9901:0ab1:22a2:88a3:3333:4a4b:5555:6666
<!--NeedCopy-->
```

Exemple 2 :


```
http://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]/
<!--NeedCopy-->
```

Exemple 3 :

```
https://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]:8080/
<!--NeedCopy-->
```

Dans l'exemple 3, les crochets séparent l'adresse IP du numéro de port (8080).

Notez que vous ne pouvez utiliser l'opérateur « + » que pour combiner des expressions IPv6 avec d'autres expressions. La sortie est une concaténation des valeurs de chaîne renvoyées par les expressions individuelles. Vous ne pouvez pas utiliser d'autres opérateurs arithmétiques avec une expression IPv6. La syntaxe suivante est un exemple :

```
client.ipv6.src + server.ip.dst
<!--NeedCopy-->
```

Par exemple, si l'adresse IPv6 source du client est `ABCD:1234::ABCD`, et que l'adresse IPv4 de destination du serveur est `10.100.10.100`, l'expression précédente renvoie `"ABCD:1234::ABCD10.100.10.100"`.

Notez que lorsque l'appliance Citrix ADC reçoit un paquet IPv6, elle attribue une adresse IPv4 temporaire à partir d'une plage d'adresses IPv4 inutilisée et remplace l'adresse source du paquet par cette adresse temporaire. Au moment de la réponse, l'adresse source du paquet sortant est remplacée par l'adresse IPv6 d'origine.

> **Remarque**
>
> Vous pouvez combiner une expression IPv6 avec n'importe quelle autre expression, à l'exception d'une expression qui produit un résultat booléen.

Préfixes d'expression pour les adresses IPv6

Les adresses IPv6 renvoyées par les préfixes d'expression du tableau suivant peuvent être traitées comme des données textuelles. Par exemple, le préfixe client.ipv6.dst renvoie l'adresse IPv6 de destination sous la forme d'une chaîne pouvant être évaluée en tant que texte.

Le tableau suivant décrit les préfixes d'expression qui renvoient une adresse IPv6.

Tableau 3. Préfixes d'expression IPv6 qui renvoient du texte

Prefix	Description
CLIENT.IPV6	Fonctionne sur l'adresse IPv6 avec le paquet actuel.
CLIENT.IPV6.DST	Renvoie l'adresse IPv6 dans le champ de destination de l'en-tête IP.
CLIENT.IPV6.SRC	Renvoie l'adresse IPv6 dans le champ source de l'en-tête IP. Voici des exemples : `client.ipv6.src.in_subnet(2007::2008/64)` `client.ipv6.src.get1.le(2008)`
SERVEUR.IPV6	Fonctionne sur l'adresse IPv6 avec le paquet actuel.
SERVER.IPV6.DST	Renvoie l'adresse IPv6 dans le champ de destination de l'en-tête IP.
SERVER.IPV6.SRC	Renvoie l'adresse IPv6 dans le champ source de l'en-tête IP. Voici des exemples : `server.ipv6.src.in_subnet(2007::2008/64)` `server.ipv6.src.get1.le(2008)`

Opérations pour les préfixes IPv6

Le tableau suivant décrit les opérateurs qui peuvent être utilisés avec des préfixes qui renvoient une adresse IPv6 :

Tableau 4. Opérations qui évaluent les adresses IPv6

Fonctionnement IPv6	Description
`<ipv6>.EQ(<IPv6_address>`	Renvoie une valeur booléenne TRUE si la valeur de l'adresse IP est identique à celle de l' `<IPv6_address>` argument. Voici un exemple : `client.ipv6.dst.eq(ABCD:1234::ABCD)`

Fonctionnement IPv6	Description
<ipv6>.GET1. . .GET8	Renvoie un segment d'une adresse IPv6 sous la forme d'un nombre. Les exemples d'expressions suivants récupèrent des segments à partir de l'adresse ipv6 1000:1001:CD 10:0000:0000:89 AB:4567:CDEF : client.ipv6.dst.get5 extracts 0000, qui est le cinquième ensemble de bits de l'adresse. client.ipv6.dst.get6 extracts 89AB. client.ipv6.dst.get7 extracts 4567. Vous pouvez effectuer des opérations numériques sur ces segments. Notez que vous ne pouvez pas effectuer d'opérations numériques lorsque vous récupérez une adresse IPv6 complète. En effet, les expressions qui renvoient une adresse IPv6 complète, comme CLIENT.IPV6.SRC, renvoient l'adresse au format texte.
<ipv6>.IN_SUBNET(<subnet>)	Renvoie une valeur booléenne TRUE si la valeur de l'adresse IPv6 se trouve dans le sous-réseau spécifié par l' <subnet> argument. Voici un exemple : client.ipv6.dst.eq(1000:1001:CD10 :0000:0000:89AB:4567:CDEF/60)
<ipv6>.IS_IPV4	Retourne une valeur booléenne TRUE s'il s'agit d'un client IPv4, et renvoie une valeur booléenne FALSE si ce n'est pas le cas.
<ipv6>.SUBNET(<n>)	Renvoie l'adresse IPv6 après avoir appliqué le masque de sous-réseau spécifié comme argument. Le masque de sous-réseau peut prendre des valeurs comprises entre 0 et 128. Pa exemple : CLIENT.IPV6.SRC.SUBNET(24)

Expressions pour adresses MAC

Une adresse MAC est constituée de valeurs hexadécimales délimitées par deux points au format ## : ## : ## : ## : ## : ##, où chaque « # » représente soit un nombre compris entre 0 et 9, soit une lettre de A à F. Des préfixes et opérateurs d'expression de stratégie avancés sont disponibles pour évaluer les adresses MAC source et cible.

Préfixes des adresses MAC

Le tableau suivant décrit les préfixes qui renvoient des adresses MAC.

Tableau 5. Préfixes qui évaluent les adresses MAC

Prefix	Description
`client.ether.dstmac`	Renvoie l'adresse MAC dans le champ de destination de l'en-tête Ethernet.
`client.ether.srcmac`	Renvoie l'adresse MAC dans le champ source de l'en-tête Ethernet.

Opérations pour les adresses MAC

Le tableau suivant décrit les opérateurs qui peuvent être utilisés avec des préfixes qui renvoient une adresse MAC.

Tableau 6. Opérations sur les adresses MAC

Prefix	Description
`<mac address>.EQ(<address>)`	Renvoie une valeur booléenne TRUE si la valeur de l'adresse MAC est identique à celle de l' `<address>` argument.
`<mac address>.GET1. . .GET4`	Renvoie une valeur numérique extraite du segment de l'adresse MAC spécifié dans l'opération GET. Par exemple, si l'adresse MAC est 12:34:56:78:9 a:bc, la valeur suivante renvoie 34 : `client.ether.dstmac.get2`

Expressions pour les données numériques du client et du serveur

Le tableau suivant décrit les préfixes pour l'utilisation des données numériques du client et du serveur, notamment le débit, les numéros de port et les ID de VLAN.

Tableau 7. Préfixes qui évaluent les données numériques du client et du serveur

Prefix	Description
Débit client.interface.rx	Renvoie un entier représentant le débit brut du trafic reçu en kilo-octets par seconde (Kbps) pendant les sept secondes précédentes.
débit client.interface.tx	Renvoie un entier représentant le débit brut du trafic transmis en Kbps pendant les sept secondes précédentes.
Débit client.interface.rxtx	Renvoie un entier représentant le débit brut du trafic reçu et transmis en Kbps pendant les sept secondes précédentes.
débit server.interface.rx	Renvoie un entier représentant le débit brut du trafic reçu en Kbps pendant les sept secondes précédentes.
débit server.interface.tx	Renvoie un entier représentant le débit brut du trafic transmis en Kbps pendant les sept secondes précédentes.
débit server.interface.rxtx	Renvoie un entier représentant le débit brut du trafic reçu et transmis en Kbps pendant les sept secondes précédentes.
server.vlan.id	Renvoie un ID numérique du VLAN via lequel le paquet actuel est entré dans Citrix ADC.
client.vlan.id	Renvoie un ID numérique pour le VLAN via lequel le paquet courant est entré dans le Citrix ADC.

Expressions de stratégie avancées : fonctions d'analyse de flux

January 21, 2021

Les expressions Stream Analytics commencent par le préfixe ANALYTICS.STREAM(<identifier_name>)

. La liste suivante décrit les fonctions qui peuvent être utilisées avec ce préfixe.

- **COLLECT_STATS**

  Recueillir des données statistiques à partir des demandes évaluées par rapport à la stratégie et créer un enregistrement pour chaque demande.

- **REQUESTS**

  Retourne le nombre de requêtes existant pour le regroupement d'enregistrements spécifié. La valeur renvoyée est de type unsigned long.

- **BANDWIDTH**

  Retourne la statistique de bande passante pour le regroupement d'enregistrements spécifié. La valeur renvoyée est de type unsigned long.

- **RESPTIME**

  Renvoie la statistique de temps de réponse pour le regroupement d'enregistrements spécifié. La valeur renvoyée est de type unsigned long.

- **CONNECTIONS**

  Renvoie le nombre de connexions simultanées existant pour le regroupement d'enregistrements spécifié. La valeur renvoyée est de type unsigned long.

- **IS_TOP (n)**

  Renvoie une valeur booléenne TRUE si la valeur statistique du regroupement d'enregistrements spécifié est l'un des n groupes les plus importants. Sinon, renvoyez une valeur booléenne FALSE.

- **CHECK_LIMIT**

  Renvoie une valeur booléenne TRUE si la statistique du regroupement d'enregistrements spécifié a atteint la limite préconfigurée. Sinon, renvoyez une valeur booléenne FALSE.

Expressions de stratégie avancées : DataStream

August 20, 2021

L'infrastructure de stratégie de l'appliance Citrix ADC comprend des expressions que vous pouvez utiliser pour évaluer et traiter le trafic du serveur de base de données lorsque l'appliance est déployée entre une batterie de serveurs d'applications et leurs serveurs de base de données associés.

Cette rubrique comprend les sections suivantes :

- Expressions pour le protocole MySQL
- Expressions pour évaluer les connexions Microsoft SQL Server

Expressions pour le protocole MySQL

Les expressions suivantes évaluent le trafic associé aux serveurs de base de données MySQL. Vous pouvez utiliser les expressions basées sur la demande (expressions commençant par MYSQL.CLIENT et MYSQL.REQ) dans les stratégies pour prendre des décisions de changement de demande au point de liaison du serveur virtuel de commutation de contenu et les expressions basées sur la réponse (expressions commençant par MYSQL.RES) pour évaluer les réponses du serveur à l'utilisateur. moniteurs d'intégrité configurés.

- **MYSQL.CLIENT.** Fonctionne sur les propriétés client d'une connexion MySQL.
- **MYSQL.CLIENT.CAPABILITIES.** Renvoie le jeu d'indicateurs que le client a défini dans le champ capacités du paquet d'initialisation de la poignée de main pendant l'authentification. Les exemples d'indicateurs définis sont CLIENT_FOUND_ROWS, CLIENT_COMPRESS et CLIENT_SSL.
- **MYSQL.CLIENT.CHAR_SET.** Renvoie la constante d'énumération affectée au jeu de caractères utilisé par le client. Les opérateurs EQ(<m>) et NE(<m>), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec ce préfixe. Voici les constantes d'énumération de jeu de caractères :
  - LATIN2_CZECH_CS
  - DEC8_SWEDISH_CI
  - CP850_GENERAL_CI
  - GREEK_GENERAL_CI
  - LATIN1_GERMAN1_CI
  - HP8_ENGLISH_CI
  - KOI8R_GENERAL_CI
  - LATIN1_SWEDISH_CI
  - LATIN2_GENERAL_CI
  - SWE7_SWEDISH_CI
  - ASCII_GENERAL_CI
  - CP1251_BULGARIAN_CI
  - LATIN1_DANISH_CI
  - HEBREW_GENERAL_CI
  - LATIN7_ESTONIAN_CS
  - LATIN2_HUNGARIAN_CI
  - KOI8U_GENERAL_CI
  - CP1251_UKRAINIAN_CI
  - CP1250_GENERAL_CI
  - LATIN2_CROATIAN_CI
  - CP1257_LITHUANIAN_CI
  - LATIN5_TURKISH_CI
  - LATIN1_GERMAN2_CI

- ARMSCII8_GENERAL_CI
- UTF8_GENERAL_CI
- CP1250_CZECH_CS
- CP866_GENERAL_CI
- KEYBCS2_GENERAL_CI
- MACCE_GENERAL_CI
- MACROMAN_GENERAL_CI
- CP852_GENERAL_CI
- LATIN7_GENERAL_CI
- LATIN7_GENERAL_CS
- MACCE_BIN
- CP1250_CROATIAN_CI
- LATIN1_BIN
- LATIN1_GENERAL_CI
- LATIN1_GENERAL_CS
- CP1251_BIN
- CP1251_GENERAL_CI
- CP1251_GENERAL_CS
- MACROMAN_BIN
- CP1256_GENERAL_CI
- CP1257_BIN
- CP1257_GENERAL_CI
- ARMSCII8_BIN
- ASCII_BIN
- CP1250_BIN
- CP1256_BIN
- CP866_BIN
- DEC8_BIN
- GREEK_BIN
- HEBREW_BIN
- HP8_BIN
- KEYBCS2_BIN
- KOI8R_BIN
- KOI8U_BIN
- LATIN2_BIN
- LATIN5_BIN
- LATIN7_BIN
- CP850_BIN
- CP852_BIN

  - SWE7_BIN
  - UTF8_BIN
  - GEOSTD8_GENERAL_CI
  - GEOSTD8_BIN
  - LATIN1_SPANISH_CI
  - UTF8_UNICODE_CI
  - UTF8_ICELANDIC_CI
  - UTF8_LATVIAN_CI
  - UTF8_ROMANIAN_CI
  - UTF8_SLOVENIAN_CI
  - UTF8_POLISH_CI
  - UTF8_ESTONIAN_CI
  - UTF8_SPANISH_CI
  - UTF8_SWEDISH_CI
  - UTF8_TURKISH_CI
  - UTF8_CZECH_CI
  - UTF8_DANISH_CI
  - UTF8_LITHUANIAN_CI
  - UTF8_SLOVAK_CI
  - UTF8_SPANISH2_CI
  - UTF8_ROMAN_CI
  - UTF8_PERSIAN_CI
  - UTF8_ESPERANTO_CI
  - UTF8_HUNGARIAN_CI
  - INVAL_CHARSET

- **MYSQL.CLIENT.DATABASE.** Renvoie le nom de la base de données spécifiée dans le paquet d'authentification que le client envoie au serveur de base de données. Il s'agit de l'attribut databasename.
- MYSQL.CLIENT.USER. Renvoie le nom d'utilisateur (dans le paquet d'authentification) avec lequel le client tente de se connecter à la base de données. Il s'agit de l'attribut utilisateur.
- **MYSQL.REQ.** Fonctionne sur une requête MySQL.
- **MYSQL.REQ.COMMAND.** Identifie la constante d'énumération affectée au type de commande dans la demande. Les opérateurs EQ(<m>) et NE(<m>), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec ce préfixe. Voici les valeurs de constantes d'énumération :
  - SLEEP
  - QUIT
  - INIT_DB

  - QUERY
  - FIELD_LIST
  - CREATE_DB
  - DROP_DB
  - REFRESH
  - SHUTDOWN
  - STATISTICS
  - PROCESS_INFO
  - CONNECT
  - PROCESS_KILL
  - DEBUG
  - PING
  - TIME
  - DELAYED_INSERT
  - CHANGE_USER
  - BINLOG_DUMP
  - TABLE_DUMP
  - CONNECT_OUT
  - REGISTER_SLAVE
  - STMT_PREPARE
  - STMT_EXECUTE
  - STMT_SEND_LONG_DATA
  - STMT_CLOSE
  - STMT_RESET
  - SET_OPTION
  - STMT_FETCH

- **MYSQL.REQ.QUERY.** Identifie la requête dans la requête MySQL.
- **MYSQL.REQ.QUERY.COMMAND.** Renvoie le premier mot-clé de la requête MySQL.
- **MYSQL.REQ.QUERY.SIZE.** Renvoie la taille de la requête au format entier. La méthode SIZE est similaire à la méthode CONTENT_LENGTH qui renvoie la longueur d'une requête ou d'une réponse HTTP.
- **MYSQL.REQ.QUERY.TEXT.** Renvoie une chaîne couvrant l'ensemble de la requête.
- **MYSQL.REQ.QUERY.TEXT(<n>).** Renvoie les n premiers octets de la requête MySQL sous forme de chaîne. Ceci est similaire à HTTP.BODY (<n>).

  Paramètres :

  n - Nombre d'octets à renvoyer

- **MYSQL.RES.** Fonctionne sur une réponse MySQL.

- **MYSQL.RES.ATLEAST_ROWS_COUNT(<i>).** Vérifie si la réponse a au moins i nombre de lignes et renvoie une valeur booléenne TRUE ou FALSE pour indiquer le résultat.

  Paramètres :

  i - Nombre de lignes

- **MYSQL.RES.ERROR.** Identifie l'objet d'erreur MySQL. L'objet erreur inclut le numéro d'erreur et le message d'erreur.
- **MYSQL.RES.ERROR.MESSAGE.** Renvoie le message d'erreur qui est extrait de la réponse d'erreur du serveur.
- **MYSQL.RES.ERROR.NUM.** Renvoie le numéro d'erreur qui est extrait de la réponse d'erreur du serveur.
- **MYSQL.RES.ERROR.SQLSTATE.** Renvoie la valeur du champ SQLSTATE dans la réponse d'erreur du serveur. Le serveur MySQL convertit les valeurs de numéro d'erreur en valeurs SQLSTATE.
- **MYSQL.RES.FIELD(<i>).** Identifie le paquet qui correspond à^{la} champ individuel dans la réponse du serveur. Chaque paquet de champ décrit les propriétés de la colonne associée. Le nombre de paquets (i) commence à 0.

  Paramètres :

  i - Numéro de paquet

- **MYSQL.RES.FIELD(<i>).CATALOG.** Renvoie la propriété catalogue du paquet de champ.
- **MYSQL.RES.FIELD(<i>).CHAR_SET.** Renvoie le jeu de caractères de la colonne. Les opérateurs EQ(<m>) et NE(<m>), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec ce préfixe.
- **MYSQL.RES.FIELD(<i>).DATATYPE.** Renvoie une constante d'énumération qui représente le type de données de la colonne. Il s'agit de l'attribut type (également appelé enum_field_type) de la colonne. Les opérateurs EQ(<m>) et NE(<m>), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec ce préfixe. Les valeurs possibles pour les différents types de données sont les suivantes :
  - DECIMAL
  - TINY
  - SHORT
  - LONG
  - FLOAT
  - DOUBLE
  - NULL
  - TIMESTAMP

  - LONGLONG
  - INT24
  - DATE
  - TIME
  - DATETIME
  - YEAR
  - NEWDATE
  - VARCHAR (new in MySQL 5.0)
  - BIT (new in MySQL 5.0)
  - NEWDECIMAL (new in MySQL 5.0)
  - ENUM
  - SET
  - TINY_BLOB
  - MEDIUM_BLOB
  - LONG_BLOB
  - BLOB
  - VAR_STRING
  - STRING
  - GEOMETRY

- **MYSQL.RES.FIELD(<i>).DB.** Renvoie l'attribut identifiant de base de données (db) du paquet de champ.
- **MYSQL.RES.FIELD(<i>).DECIMALS.** Renvoie le nombre de positions après la virgule décimale si le type est DECIMAL ou NUMERIC. Il s'agit de l'attribut décimal du paquet de champ.
- **MYSQL.RES.FIELD(<i>).FLAGS.** Renvoie la propriété flags du paquet de champ. Voici les valeurs de drapeau hexadécimal possibles :
  - 0001: NOT_NULL_FLAG
  - 0002: PRI_KEY_FLAG
  - 0004: UNIQUE_KEY_FLAG
  - 0008: MULTIPLE_KEY_FLAG
  - 0010: BLOB_FLAG
  - 0020: UNSIGNED_FLAG
  - 0040: ZEROFILL_FLAG
  - 0080: BINARY_FLAG
  - 0100: ENUM_FLAG
  - 0200: AUTO_INCREMENT_FLAG
  - 0400: TIMESTAMP_FLAG
  - 0800: SET_FLAG
- **MYSQL.RES.FIELD(<i>).LENGTH.** Renvoie la longueur de la colonne. Il s'agit de la valeur de

l'attribut length du paquet de champ. La valeur renvoyée peut être supérieure à la valeur réelle. Par exemple, une instance d'une colonne VARCHAR (2) peut renvoyer une valeur de 2 même lorsqu'elle ne contient qu'un seul caractère.

- **MYSQL.RES.FIELD(<i>).NAME.** Renvoie l'identifiant de colonne (le nom après la clause AS, le cas échéant). Il s'agit de l'attribut name du paquet de champ.
- **MYSQL.RES.FIELD(<i>).ORIGINAL_NAME.** Renvoie l'identifiant de colonne d'origine (avant la clause AS, le cas échéant). Il s'agit de l'attribut org_name du paquet de champ.
- **MYSQL.RES.FIELD(<i>).ORIGINAL_TABLE.** Renvoie l'identifiant de table d'origine de la colonne (avant la clause AS, le cas échéant). Il s'agit de l'attribut org_table du paquet de champ.
- **MYSQL.RES.FIELD(<i>).TABLE.** Renvoie l'identificateur de table de la colonne (après la clause AS, le cas échéant). Il s'agit de l'attribut table du paquet de champ.
- **MYSQL.RES.FIELDS_COUNT.** Renvoie le nombre de paquets de champs dans la réponse (l'attribut field_count du paquet OK).
- **MYSQL.RES.OK.** Identifie le paquet OK envoyé par le serveur de base de données.
- **MYSQL.RES.OK.AFFECTED_ROWS.** Renvoie le nombre de lignes affectées par une requête INSERT, UPDATE ou DELETE. Il s'agit de la valeur de l'attribut affected_rows du paquet OK.
- **MYSQL.RES.OK.INSERT_ID.** Identifie l'attribut unique_id du paquet OK. Si une identité auto-incrément n'est pas générée par l'instruction ou la requête MySQL actuelle, la valeur de unique_id, et donc la valeur renvoyée par l'expression, est 0.
- **MYSQL.RES.OK.MESSAGE.** Renvoie la propriété message du paquet OK.
- **MYSQL.RES.OK.STATUS.** Identifie la chaîne de bits dans l'attribut server_status du paquet OK. Les clients peuvent utiliser l'état du serveur pour vérifier si la commande actuelle fait partie d'une transaction en cours d'exécution. Les bits de la chaîne de bits server_status correspondent aux champs suivants (dans l'ordre donné) :
  - IN TRANSACTION
  - AUTO_COMMIT
  - MORE RESULTS
  - MULTI QUERY
  - BAD INDEX USED
  - NO INDEX USED
  - CURSOR EXISTS
  - LAST ROW SEEN
  - DATABASE DROPPED
  - NO BACKSLASH ESCAPES

- **MYSQL.RES.OK.WARNING_COUNT.** Renvoie l'attribut warning_count du paquet OK.
- **MYSQL.RES.ROW(<i>).** Identifie le paquet qui correspond à^{la} ligne individuelle dans la réponse du serveur de base de données.

  Paramètres :

  i - Numéro de ligne
- **MYSQL.RES.ROW(<i>).DOUBLE_ELEM(<j>).** Vérifie si le jth colonne de^{la} la ligne de la table est NULL. Suivant les conventions C, les index i et j commencent à partir de 0. Par conséquent, la ligne i et la colonne j sont en fait le (i+1)th la ligne et le (j+1)th colonne, respectivement.

  Paramètres :

  i - Numéro de ligne

  j - Numéro de colonne
- **MYSQL.RES.ROW(<i>).IS_NULL_ELEM(j).** Vérifie si le jth colonne de^{la} la ligne de la table est NULL. Suivant les conventions C, les index i et j commencent à partir de 0. Par conséquent, la ligne i et la colonne j sont en fait le (i+1)th la ligne et le (j+1)th colonne, respectivement.

  Paramètres :

  i - Numéro de ligne

  j - Numéro de colonne
- **MYSQL.RES.ROW(<i>).NUM_ELEM(<j>).** Renvoie une valeur entière de la valeur jth colonne de^{la} rangée du tableau. Suivant les conventions C, les index i et j commencent à partir de 0. Par conséquent, la ligne i et la colonne j sont en fait le (i+1)th la ligne et le (j+1)th colonne, respectivement.

  Paramètres :

  i - Numéro de ligne

  j - Numéro de colonne
- **MYSQL.RES.ROW(<i>).TEXT_ELEM(j).** Renvoie une chaîne de caractères du jth colonne de^{la} rangée du tableau. Suivant les conventions C, les index i et j commencent à partir de 0. Par conséquent, la ligne i et la colonne j sont en fait le (i+1)th la ligne et le (j+1)th colonne, respectivement.

  Paramètres :

  i - Numéro de ligne

  j - Numéro de colonne

- **MYSQL.RES.TYPE.** Renvoie une constante d'énumération pour le type de réponse. Ses valeurs peuvent être ERROR, OK et RESULT_SET. Les opérateurs EQ(<m>) et NE(<m>), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec ce préfixe.

Expressions pour évaluer les connexions Microsoft SQL Server

Les expressions suivantes évaluent le trafic associé aux serveurs de base de données Microsoft SQL Server. Vous pouvez utiliser les expressions basées sur la demande (expressions commençant par MSSQL.CLIENT et MSSQL.REQ) dans les stratégies pour prendre des décisions de changement de demande au point de liaison du serveur virtuel de commutation de contenu et les expressions basées sur la réponse (expressions commençant par MSSQL.RES) pour évaluer les réponses du serveur à l'utilisateur. moniteurs d'intégrité configurés.

Expression.	Description
MSSQL.CLIENT.CAPABILITIES	Renvoie les champs OptionFlags1, OptionFlags2, OptionFlags3 et TypeFlags du paquet Login7Authentication, dans cet ordre, sous la forme d'un entier de 4 octets. Chaque champ a une longueur de 1 octet et spécifie un ensemble de fonctionnalités client.
MSSQL.CLIENT.DATABASE	Renvoie le nom de la base de données cliente. La valeur renvoyée est de type texte.
MSSQL.CLIENT.USER	Renvoie le nom d'utilisateur avec lequel le client s'est authentifié. La valeur renvoyée est de type texte.
MSSQL.REQ.COMMAND	Renvoie une constante d'énumération qui identifie le type de commande dans la requête envoyée à un serveur de base de données Microsoft SQL Server. La valeur renvoyée est de type texte. Les valeurs de la constante d'énumération sont QUERY, RESPONSE, RPC et ATTENTION. Les opérateurs EQ(<m>) et NE(<m>), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec cette expression.
MSSQL.REQ.QUERY.COMMAND	Renvoie le premier mot-clé de la requête SQL. La valeur renvoyée est de type texte.

Expression.	Description
MSSQL.REQ.QUERY.SIZE	Renvoie la taille de la requête SQL dans la requête. La valeur renvoyée est un nombre.
MSSQL.REQ.QUERY.TEXT	Renvoie l'intégralité de la requête SQL sous forme de chaîne. La valeur renvoyée est de type texte.
MSSQL.REQ.QUERY.TEXT(<n>)	Renvoie les n premiers octets de la requête SQL. La valeur renvoyée est de type texte. Paramètres : n - Nombre d'octets
MSSQL.REQ.RPC.NAME	Renvoie le nom de la procédure appelée dans une requête RPC (Remote Procedure Call). Le nom est renvoyé sous forme de chaîne.
MSSQL.REQ.RPC.IS_PROCID	Renvoie une valeur de type Boolean qui indique si la demande d'appel de procédure distante (RPC) contient un ID de procédure ou un nom de RPC. Une valeur de retour True indique que la demande contient un ID de procédure et une valeur de retour FALSE indique que la demande contient un nom RPC.
MSSQL.REQ.RPC.PROCID	Renvoie l'ID de procédure de la demande d'appel de procédure distante (RPC) sous forme d'entier.
MSSQL.REQ.RPC.BODY **Remarque :** Non disponible pour les versions antérieures à la version 10.1.	Renvoie le corps de la requête SQL sous forme de chaîne sous la forme de paramètres représentés par des clauses « a=b » séparées par des virgules, où « a » est le nom du paramètre RPC et « b » est sa valeur.
MSSQL.REQ.RPC.BODY (n) **Note :** Non disponible pour les versions antérieures à la version 10.1.	Renvoie une partie du corps de la requête SQL sous forme de chaîne sous la forme de paramètres représentés par des clauses « a=b » séparées par des virgules, où « a » est le nom du paramètre RPC et « b » est sa valeur. Les paramètres sont renvoyés uniquement à partir des premiers « n » octets de la requête, en ignorant l'en-tête SQL. Seules les paires nom-valeur complètes sont renvoyées.

Expression.	Description
MSSQL.RES.ATLEAST_ROWS_COUNT (i)	Vérifie si la réponse a au moins i nombre de lignes. La valeur renvoyée est une valeur booléenne TRUE ou FalseValue. Paramètres : i - Nombre de lignes
MSSQL.RES.DONE.ROWCOUNT	Renvoie le nombre de lignes affectées par une requête INSERT, UPDATE ou DELETE. La valeur renvoyée est de type unsigned long.
MSSQL.RES.DONE.STATUS	Renvoie le champ d'état à partir du jeton Done envoyé par un serveur de base de données Microsoft SQL Server. La valeur renvoyée est un nombre.
MSSQL.RES.ERROR.MESSAGE	Renvoie le message d'erreur du jeton ERROR envoyé par un serveur de base de données Microsoft SQL Server. Il s'agit de la valeur du champ MsgText dans le jeton ERREUR. La valeur renvoyée est de type texte.
MSSQL.RES.ERROR.NUM	Renvoie le numéro d'erreur du jeton ERROR envoyé par un serveur de base de données Microsoft SQL Server. Il s'agit de la valeur du champ Nombre dans le jeton ERREUR. La valeur renvoyée est un nombre.
MSSQL.RES.ERROR.STATE	Renvoie l'état d'erreur à partir du jeton ERROR envoyé par un serveur de base de données Microsoft SQL Server. Il s'agit de la valeur du champ État dans le jeton ERROR. La valeur renvoyée est un nombre.

Expression.	Description
MSSQL.RES.FIELD (<i>) .DATATYPE	Renvoie le type de données du ith champ dans la réponse du serveur. Les <m> <m> fonctions EQ () et NE (), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisées avec ce préfixe. Par exemple, l'expression suivante renvoie une valeur booléenne TRUE si la fonction DATATYPE renvoie une valeur de datetime pour le troisième champ de la réponse : MSSQL.RES.FIELD(<2>) .DATATYPE.EQ(datetime) Paramètres : i - Numéro de ligne
MSSQL.RES.FIELD (<i>). LONGUEUR	Renvoie la longueur maximale possible du ith champ dans la réponse du serveur. La valeur renvoyée est un nombre. Paramètres : i - Numéro de ligne
MSSQL.RES.FIELD (<i>) .NAME	Renvoie le nom du ith champ dans la réponse du serveur. La valeur renvoyée est de type texte. Paramètres : i - Numéro de ligne
MSSQL.RES.ROW (<i>) .DOUBLE_ELEM (<j>)	Renvoie une valeur de type double à partir de la m-ième colonne de la n-ième ligne de la table. Si la valeur n'est pas une double valeur, une condition UNDEF est déclenchée. Suivant les conventions C, les index i et j commencent à partir de 0 (zéro). Par conséquent, la ligne i et la colonne j sont en fait la (i + 1) ème ligne et la (j + 1) ème colonne, respectivement. Paramètres : i - Numéro de ligne j - Numéro de colonne

Expression.	Description
MSSQL.RES.ROW (<i>) .NUM_ELEM (j)	Renvoie une valeur entière de la jème colonne de la m-ième ligne de la table. Si la valeur n'est pas une valeur entière, une condition UNDEF est déclenchée. Suivant les conventions C, les index i et j commencent à partir de 0 (zéro). Par conséquent, la ligne i et la colonne j sont en fait la (i + 1) ème ligne et la (j + 1) ème colonne, respectivement. Paramètres : i - Numéro de ligne j - Numéro de colonne
MSSQL.RES.ROW (<i>) .IS_NULL_ELEM (j)	Vérifie si la jème colonne de la m-ième ligne de la table est NULL et renvoie une valeur booléenne TRUE ou FALSE pour indiquer le résultat. Suivant les conventions C, les index i et j commencent à partir de 0 (zéro). Par conséquent, la ligne i et la colonne j sont en fait la (i + 1) ème ligne et la (j + 1) ème colonne, respectivement. Paramètres : i - Numéro de ligne j - Numéro de colonne
MSSQL.RES.ROW (<i>) .TEXT_ELEM (j)	Renvoie une chaîne de texte de la jème colonne de la ième ligne de la table. Suivant les conventions C, les index i et j commencent à partir de 0 (zéro). Par conséquent, la ligne i et la colonne j sont en fait la (i + 1) ème ligne et la (j + 1) ème colonne, respectivement. Paramètres : i - Numéro de ligne j - Numéro de colonne
MSSQL.RES.TYPE	Renvoie une constante d'énumération qui identifie le type de réponse. Voici les valeurs de retour possibles : ERROR, OK et RESULT_SET. Les opérateurs EQ(<m>) et NE(<m>), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec cette expression.

Données de typecasting

August 20, 2021

Vous pouvez extraire des données d'un type (par exemple, du texte ou un entier) des demandes et des réponses et les transformer en données d'un autre type. Par exemple, vous pouvez extraire une chaîne et la transformer en format temporel. Vous pouvez également extraire une chaîne d'un corps de requête HTTP et la traiter comme un en-tête HTTP ou extraire une valeur d'un type d'en-tête de requête et l'insérer dans un en-tête de réponse d'un type différent.

Après avoir tapé les données, vous pouvez appliquer n'importe quelle opération appropriée au nouveau type de données. Par exemple, si vous tapez du texte dans un en-tête HTTP, vous pouvez appliquer toute opération applicable aux en-têtes HTTP à la valeur renvoyée.

Pour plus d'informations sur les données de typographie, consultez le fichier PDF Typecasting Operations .

Expressions régulières

October 5, 2021

Lorsque vous souhaitez effectuer des opérations de correspondance de chaînes plus complexes que celles effectuées avec les opérateurs CONTIENS ("<string>") ou EQ ("<string>"), vous utilisez des expressions régulières. L'infrastructure de stratégie de l'appliance Citrix® Citrix ADC® inclut des opérateurs auxquels vous pouvez transmettre des expressions régulières en tant qu'arguments pour la correspondance de texte. Les noms des opérateurs qui travaillent avec les expressions régulières incluent la chaîne REGEX. Les expressions régulières que vous transmettez en tant qu'arguments doivent être conformes à la syntaxe des expressions régulières décrite dans "<http://www.pcre.org/pcre.txt>." Pour en savoir plus sur les expressions régulières, consultez "<http://www.regular-expressions.info/quickstart.html>" et à "<http://www.silverstones.com/thebat/Regex.html>."

Le texte cible d'un opérateur qui travaille avec des expressions régulières peut être du texte ou la valeur d'un en-tête HTTP. Voici le format d'une expression de stratégie avancée qui utilise un opérateur d'expression régulière pour opérer sur du texte :

```
<text>.<regex_operator>(re<delimiter><regex_pattern><delimiter>)
```

La chaîne <text> représente le préfixe d'expression de stratégie avancée qui identifie une chaîne de texte dans un paquet (par exemple, HTTP.REQ.URL). La chaîne <regex_operator> représente l'opérateur d'expression régulière. L'expression régulière commence toujours par la chaîne re.

Une paire de délimiteurs correspondants, représentés par `<delimiter>`, entoure la chaîne `<regex_pattern>`, qui représente l'expression régulière.

L'exemple d'expression suivant vérifie si l'URL d'un paquet HTTP contient la chaîne `*.jpeg` (où * est un caractère générique) et renvoie une valeur booléenne TRUE ou FALSE pour indiquer le résultat. L'expression régulière est entourée d'une paire de barre oblique (/), qui servent de délimiteurs.

```
http.req.url.regex_match(re/.<asterisk>\.jpeg/)
```

Les opérateurs d'expression régulière peuvent être combinés pour définir ou affiner la portée d'une recherche. Par exemple, `<text>.AFTER_REGEX(reregex_pattern1).BEFORE_REGEX(reregex_pattern2)` spécifie que la cible de la correspondance de chaîne est le texte entre les motifs regex_pattern1 et regex_pattern2. Vous pouvez utiliser un opérateur de texte sur la portée définie par les opérateurs d'expression régulière. Par exemple, vous pouvez utiliser l'opérateur CONTAINS (`"<string>"`) pour vérifier si la portée définie contient la chaîne abc :

```
<text>.AFTER_REGEX(re/regex_pattern1).BEFORE_REGEX(re/regex_pattern2/).
CONTAINS("abc")
```

> **Remarque**
>
> Le processus d'évaluation d'une expression régulière prend plus de temps que celui d'un opérateur tel que CONtains (`"<string>"`) ou EQ (`"<string>"`), qui fonctionnent avec des arguments de chaîne simples. Vous devez utiliser des expressions régulières uniquement si votre exigence dépasse le champ d'application des autres opérateurs.

Caractéristiques de base des expressions régulières

January 21, 2021

Voici les caractéristiques notables des expressions régulières telles que définies sur l'appliance Citrix ADC :

- Une expression régulière commence toujours par la chaîne « re » suivie d'une paire de caractères de délimitation (appelés délimiteurs) qui entourent l'expression régulière que vous souhaitez utiliser.

Par exemple, re# <regex_pattern> # utilise le signe numérique (#) comme séparateur.

- Une expression régulière ne peut pas dépasser 1499 caractères.
- La correspondance des chiffres peut être effectuée en utilisant la chaîne d (une barre oblique inverse suivie de d).
- Les espaces blancs peuvent être représentés en utilisant s (une barre oblique inverse suivie de s).

- Une expression régulière peut contenir des espaces blancs.

Voici les différences entre la syntaxe Citrix ADC et la syntaxe PCRE :

- Citrix ADC n'autorise pas les références arrière dans les expressions régulières.
- Vous ne devez pas utiliser d'expressions régulières récursives.
- Le méta-caractère point correspond également au caractère de nouvelle ligne.
- Unicode n'est pas pris en charge.
- L'opération SET_TEXT_MODE(IGNORECASE) remplace le (?i) option interne dans l'expression régulière.

Opérations pour les expressions régulières

October 5, 2021

Le tableau suivant décrit les opérateurs qui utilisent des expressions régulières. L'opération effectuée par un opérateur d'expression régulière dans une expression de stratégie avancée donnée dépend du fait que le préfixe d'expression identifie du texte ou des en-têtes HTTP. Les opérations qui évaluent les en-têtes remplacent toutes les opérations textuelles pour toutes les instances du type d'en-tête spécifié. Lorsque vous utilisez un opérateur, remplacez-le <text>par le préfixe d'expression de stratégie avancée que vous souhaitez configurer pour identifier le texte.

Opération d'expression régulière	Description
<text>.BEFORE_REGEX (<regular expression>)	Sélectionne le texte qui précède la chaîne correspondant à l'<regular expression>argument. Si l'expression régulière ne correspond à aucune donnée de la cible, elle renvoie un objet texte de longueur 0. L'expression suivante sélectionne la chaîne « text » dans « text/plain ». http.res.header (« content-type ») .before_regex (re#/#)
<text>.AFTER_REGEX (<regular expression>)	Sélectionne le texte qui suit la chaîne qui correspond à l'<regular expression>argument. Si l'expression régulière ne correspond à aucun texte de la cible, elle renvoie un objet texte de longueur 0. L'expression suivante extrait « Example » de « MyExample » : http.req.header (« etag ») .after_regex (re/my/)

Opération d'expression régulière	Description
<text>.REGEX_SELECT (<regular expression>)	Sélectionne une chaîne qui correspond à l'<regular expression>argument. Si l'expression régulière ne correspond pas à la cible, un objet texte de longueur 0 est renvoyé. L'exemple suivant extrait la chaîne « NS-CACHE-9.0 : 90 » d'un en-tête Via : http.req.header (« via ») .regex_select (re ! NS-CACHE- \ d. \ d : \ s* \ d {1,3} !)

Opération d'expression régulière	Description
<text>.REGEX_MATCH (<regular expression>)	Renvoie TRUE si la cible correspond à un <regular expression>argument de 1499 caractères maximum. L'expression régulière doit avoir le format suivant : re <delimiter>expression régulière< delimiter> Les deux délimiteurs doivent être identiques. En outre, l'expression régulière doit être conforme à la syntaxe de la bibliothèque d'expressions rationnelles compatible PERL (PCRE). Pour plus d'informations, accédez à http://www.pcre.org/pcre.txt. En particulier, consultez la page de manuel pcrepattern. Toutefois, notez ce qui suit : Les références antécédentes ne sont pas autorisées. Les expressions régulières récursives ne sont pas recommandées. Le métacaractère de point correspond également au caractère de saut de ligne. Le jeu de caractères Unicode n'est pas pris en charge. SET_TEXT_MODE (IGNORECASE) remplace le (? i) option interne spécifiée dans l'expression régulière. Voici des exemples : http.req.hostname.regex_match (re/[[:alpha :]] + (abc) {2,3}/) et http.req.url.set_text_mode (code URL) .regex_match (re# (a*b*+c*) #) L'exemple suivant correspond à ab et aB : http.req.url.regex_match (re/a (re/a (re/a (? i) b/) L'exemple suivant correspond à ab, ab, Ab et AB : http.req.url.set_text_mode (ignorecase) .regex_match (re/ab/) L'exemple suivant effectue une correspondance multiligne insensible à la casse dans laquelle le méta-caractère du point correspond également à un caractère de saut de ligne : http.req.body.regex_match (re/ (? ixm) (^ab (.*) cd$)/)

Exemples récapitulatifs d'expressions de stratégie et de stratégies avancées

October 5, 2021

Le tableau suivant fournit des exemples d'expressions de stratégie avancées que vous pouvez utiliser comme base pour vos propres expressions de stratégie avancée.

Tableau 1. Exemples d'expressions de stratégie avancées

Type d'expression	Exemples d'expressions
Examinez la méthode utilisée dans la requête HTTP.	`http.req.method.eq(post)http.req.method.eq(get)`

Vérifiez la valeur de l'en-tête Cache-Control ou Pragma dans une requête HTTP (req) ou une réponse (res).	`http.req.header("Cache-Control").contains("no-store")`
	`http.req.header("Cache-Control").contains("no-cache")`
	`http.req.header("Pragma").contains("no-cache")`
	`http.res.header("Cache-Control").contains("private")`
	`http.res.header("Cache-Control").contains("public")`
	`http.res.header("Cache-Control").contains("must-revalidate")http.res.header("Cache-Control").contains ("proxy-revalidate")`
	`http.res.header("Cache-Control").contains("max-age")`

Vérifiez la présence d'un en-tête dans une requête (req) ou une réponse (res).	`http.req.header("myHeader").exists` `http.res.header("myHeader").exists`

Type d'expression	Exemples d'expressions
Recherchez un type de fichier particulier dans une requête HTTP en fonction de l'extension de fichier.	`http.req.url.contains(".html")http.req.url.contains(".cgi")http.req.url.contains(".asp")http.req.url.contains(".exe")http.req.url.contains(".cfm")http.req.url.contains(".ex")http.req.url.contains(".shtml")http.req.url.contains(".htx")http.req.url.contains("/cgi-bin/")http.req.url.contains("/exec/")http.req.url.contains("/bin/")`
Recherchez tout élément autre qu'un type de fichier particulier dans une requête HTTP.	`http.req.url.contains(".png").not; http.req.url.contains(".jpeg").not`
Vérifiez le type de fichier envoyé dans une réponse HTTP en fonction de l'en-tête Content-Type.	`http.res.header("Content-Type").contains("text")http.res.header("Content-Type").contains "application/msword")http.res.header("Content-Type").contains("vnd.ms-excel")http.res.header("Content-Type").contains("application/vnd.ms-powerpoint"); http.res.header("Content-Type").contains("text/css"); http.res.header("Content-Type").contains("text/xml"); http.res.header("Content-Type").contains("image/")`
Vérifiez si cette réponse contient un en-tête d'expiration.	`http.res.header("Expires").exists`
Recherchez un en-tête Set-Cookie dans une réponse.	`http.res.header("Set-Cookie").exists`
Vérifiez l'agent qui a envoyé la réponse.	`http.res.header("User-Agent").contains("Mozilla/4.7")http.res.header("User-Agent").contains("MSIE")`

Type d'expression	Exemples d'expressions
Vérifiez si les 1024 premiers octets du corps d'une requête commencent par la chaîne « du texte ».	`http.req.body(1024).contains("some text")`

Le tableau suivant présente des exemples de configurations de stratégie et de liaisons pour les fonctions couramment utilisées.

Tableau 2. Exemples d'expressions et de stratégies avancées

Objectif	Exemple
Utilisez la fonction de réécriture pour remplacer les occurrences de `http://with https://` dans le corps d'une réponse HTTP.	`add rewrite action httpRewriteAction replace_all http.res.body(50000)"\"https://\""-search http://add rewrite policy demo_rep34312 "http.res.body(50000).contains(\"http://\")" httpRewriteAction`
Remplacez toutes les occurrences de « abcd » par « 1234 » dans les 1000 premiers octets du corps HTTP.	`add rewrite action abcdTo1234Action replace_all "http.req.body(1000)""\"1234\""-search abcd add rewrite policy abcdTo1234Policy "http.req.body(1000).contains(\"abcd\")" abcdTo1234Action bind rewrite global abcdTo1234Policy 100 END -type REQ_OVERRIDE`
Réduisez la version HTTP vers la version 1.0 pour empêcher le serveur de répartir les réponses HTTP.	`add rewrite action downgradeTo1.0Action replace http.req.version.minor "\"0\""add rewrite policy downgradeTo1.0Policy "http.req.version.minor.eq(1)"downgradeTo1.0Action bind lb vserver myLBVserver -policyName downgradeTo1.0Policy -priority 100 -gotoPriorityExpression NEXT -type REQUEST`

Objectif	Exemple
Supprimez les références au protocole HTTP ou HTTPS dans toutes les réponses, de sorte que si la connexion de l'utilisateur est HTTP, le lien soit ouvert à l'aide de HTTP, et si la connexion de l'utilisateur est HTTPS, le lien soit ouvert à l'aide du protocole HTTPS.	`add rewrite action remove_http_https replace_all "http.res.body(1000000).set_text_mode(ignorecase)""\"//\""-search "re~https?://|HTTPS?://~"add rewrite policy remove_http_https true remove_http_https bind lb vserver test_vsvr -policyName remove_http_https -priority 20 -gotoPriorityExpression NEXT -type RESPONSE`
Réécrivez les instances de http : en https : dans toutes les URL.	`add responder action httpToHttpsAction redirect "\"https://\" + http.req.hostname + http.req.url"add responder policy httpToHttpsPolicy "!CLIENT.SSL.IS_SSL"httpToHttpsAction bind responder global httpToHttpsPolicy 1 END -type OVERRIDE`
Modifiez une URL pour rediriger de l'URL A vers l'URL B. Dans cet exemple, « file5.html » est ajouté au chemin d'accès.	`add responder action appendFile5Action redirect \"http://\" + http.req.hostname + http.req.url + \"/file5.html\""add responder policy appendFile5Policy "http.req.url.eq(\"/testsite\")" appendFile5Action bind responder global appendFile5Policy 1 END -type OVERRIDE`

Objectif	Exemple
Redirigez une URL externe vers une URL interne.	`add rewrite action act_external_to_internal REPLACE 'http.req.hostname.server'"www.my.host.com"'add rewrite policy pol_external_to_internal 'http.req.hostname.server.eq("www.external.host.com")'act_external_to_internal bind rewrite global pol_external_to_internal 100 END -type REQ_OVERRIDE`
Redirigez les demandes vers www.example.com qui ont une chaîne de requête vers www.webn.example.com. La valeur n est dérivée d'un paramètre de serveur dans la chaîne de requête, par exemple, server=5.	`add rewrite action act_redirect_query REPLACE q##http.req.header("Host").before_str(".example.com")'"Web"+ http.req.url.query.value("server")## add rewrite policy pol_redirect_query q##http.req.header("Host").eq("www.example.com")&& http.req.url.contains("?")'act_redirect_query##`
Limitez le nombre de demandes par seconde à partir d'une URL.	`add ns limitSelector ip_limit_selector http.req.url "client.ip.src"add ns limitIdentifier ip_limit_identifier -threshold 4 -timeSlice 3600 -mode request_rate -limitType smooth -selectorName ip_limit_selector add responder action my_Web_site_redirect_action redirect "\"http://www.mycompany.com/\""add responder policy ip_limit_responder_policy "http.req.url.contains(\"myasp.asp\")&& sys.check_limit (\"ip_limit_identifier\")"my_Web_site_redirect_action bind responder global ip_limit_responder_policy 100 END -type default`

Objectif	Exemple
Vérifiez l'adresse IP du client, mais transmettez la demande sans modifier la demande.	`add rewrite policy check_client_ip_policy 'HTTP.REQ. HEADER ("x-forwarded-for").EXISTS HTTP.REQ.HEADER ("client-ip"). EXISTS'NOREWRITE bind rewrite global check_client_ip_policy 100 END`
Supprimez les anciens en-têtes d'une demande et insérez un en-tête NS-Client.	`add rewrite action del_x_forwarded_for delete_http_header x-forwarded-for add rewrite action del_client_ip delete_http_header client-ip add rewrite policy check_x_forwarded_for_policy 'HTTP. REQ.HEADER("x-forwarded-for"). EXISTS'del_x_forwarded_for add rewrite policy check_client_ip_policy 'HTTP.REQ. HEADER("client-ip").EXISTS' del_client_ip add rewrite action insert_ns_client_header insert_http_header NS-Client ' CLIENT.IP.SRC'add rewrite policy insert_ns_client_policy 'HTTP.REQ. HEADER("x-forwarded-for").EXISTS HTTP.REQ.HEADER("client-ip").EXISTS 'insert_ns_client_header bind rewrite global check_x_forwarded_for_policy 100 200 bind rewrite global check_client_ip_policy 200 300 bind rewrite global insert_ns_client_policy 300 END`

Objectif	Exemple
Supprimez les anciens en-têtes d'une demande, insérez un en-tête NS-Client, puis modifiez l'action « insérer un en-tête » afin que la valeur de l'en-tête inséré contienne les valeurs IP du client des anciens en-têtes et de l'adresse IP de connexion de l'appliance Citrix ADC. Notez que cet exemple répète l'exemple précédent, à l'exception de l'action de réécriture du jeu final.	'ajouter une action de réécriture del_x_forwarded_for delete_http_header x-forwarded-for ajouter une action de réécriture del_client_ip delete_http_header client-ip ajouter une politique de réécriture check_x_forwarded_for_policy 'HTTP.REQ.HEADER (« x-forwarded-for ») .EXISTS' del_x_forwarded_for ajouter une politique de réécriture check_client_ip_policy 'HTTP.REQ. HEADER (« client-ip ») .EXISTS 'del_client_ip ajouter l'action de réécriture insert_ns_client_header insert_http_header NS-Client 'CLIENT.IP.SRC' ajouter la stratégie de réécriture insert_ns_client_policy 'HTTP.REQ.HEADER (« x-forwarded-for ») .EXISTS HTTP.REQ.HEADER (« client-ip ») .EXISTS' insert_ns_ns__client_ header bind rewrite global check_x_forwarded_for_policy 100 200 bind rewrite global check_client_ip_policy 200 300 bind rewrite global insert_ns_client_policy 300 FIN définir l'action de réécriture insert_ns_client_header -StringBuilderExpr 'HTTP.REQ.HEADER (« x-forwarded-for ») .VALUE (0) + "" + HTTP.REQ. EN-TÊTE (« client-ip ») .VALUE (0) + "" + CLIENT.IP.SRC'

Exemples de stratégies de stratégie avancées pour la réécriture

October 5, 2021

Avec la fonction de réécriture, vous pouvez modifier n'importe quelle partie d'un en-tête HTTP et, pour les réponses, vous pouvez modifier le corps HTTP. Vous pouvez utiliser cette fonctionnalité pour effectuer plusieurs tâches utiles, telles que la suppression d'en-têtes HTTP inutiles, le masquage d'URL internes, la redirection de pages Web et la redirection de requêtes ou de mots clés.

Dans les exemples suivants, vous créez d'abord une action de réécriture et une stratégie de réécriture.

Ensuite, vous liez la stratégie à l'échelle mondiale.

Ce document comprend les détails suivants :

- Redirection d'une URL externe vers une URL interne
- Redirection d'une requête
- Réécriture d'HTTP en HTTPS
- Suppression des en-têtes indésirables
- Réduction des redirections de serveur Web
- Masquage de l'en-tête du serveur
- Conversion de texte brut en chaîne codée par URL et de la manière inverse

Pour plus d'informations sur les commandes et les descriptions de syntaxe, consultez la page Réécriture de la référence des commandes .

Redirection d'une URL externe vers une URL interne

Cet exemple décrit comment créer une action de réécriture et une stratégie de réécriture qui redirige une URL externe vers une URL interne. Vous créez une action, appelée act_external_to_internal, qui effectue la réécriture. Ensuite, vous créez une stratégie appelée pol_external_to_internal.

Pour rediriger une URL externe vers une URL interne à l'aide de l'interface de ligne de commande

- Pour créer l'action de réécriture, à l'invite de commandes, tapez :

```
add rewrite action act_external_to_internal REPLACE "http.req.hostname.
server" "\" host_name_of_internal_Web_server\" "
```

- Pour créer la stratégie de réécriture, à l'invite de commandes Citrix ADC, tapez :

```
add rewrite policy pol_external_to_internal "http.req.hostname.server.eq(\"
host_name_of_external_Web_server\")"act_external_to_internal
```

- Liez la stratégie à l'échelle mondiale.

Pour rediriger une URL externe vers une URL interne à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Réécrire** > **Actions**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action de réécriture**, entrez le nom act_external_to_internal.
4. Pour remplacer le nom d'hôte du serveur HTTP par le nom du serveur interne, choisissez **Remplacer** dans la zone de liste Type.
5. Dans le champ Nom de l'en-tête, tapez **Hôte**.

6. Dans l'expression chaîne d'un champ de texte de remplacement, saisissez le nom d'hôte interne de votre serveur Web.
7. Cliquez sur **Create**, puis cliquez sur **Close**.
8. Dans le volet de navigation, cliquez sur **Stratégies**.
9. Dans le volet d'informations, cliquez sur **Ajouter**.
10. Dans le champ Nom, tapez pol_external_to_internal. Cette stratégie détecte les connexions au serveur Web.
11. Dans le menu déroulant **Action**, choisissez l'action act_external_to_internal.
12. Dans l'éditeur d'expressions, construisez l'expression suivante :

```
HTTP.REQ.HOSTNAME.SERVER.EQ("www.example.com")
<!--NeedCopy-->
```

1. Liez votre nouvelle stratégie à l'échelle mondiale.

Redirection d'une requête

Cet exemple décrit comment créer une action de réécriture et une stratégie de réécriture qui redirige une requête vers l'URL appropriée. L'exemple suppose que la demande contient un en-tête Host défini **sur www.example.com** et une méthode GET avec la **chaîne /query.cgi ? serveur=5**. La redirection extrait le nom de domaine de l'en-tête de l'hôte et le numéro de la chaîne de requête, puis redirige la requête de l'utilisateur vers le serveur **Web5.example.com**, où le reste de la requête de l'utilisateur est traité.

> **Remarque :**
>
> Bien que les commandes suivantes apparaissent sur plusieurs lignes, vous devez les saisir sur une seule ligne sans sauts de ligne.

Pour rediriger une requête vers l'URL appropriée à l'aide de l'interface de ligne de commande

- Pour créer une action de réécriture nommée act_redirect_query qui remplace le nom d'hôte du serveur HTTP par le nom du serveur interne, tapez :

```
add rewrite action act_redirect_query REPLACE http.req.header("Host").
before_str(".example.com")'"Web" + http.req.url.query.value("server")'
```

- Pour créer une stratégie de réécriture nommée pol_redirect_query, tapez les commandes suivantes à l'invite de commandes Citrix ADC. Cette stratégie détecte les connexions au serveur Web qui contiennent une chaîne de requête. N'appliquez pas cette stratégie aux connexions qui ne contiennent pas de chaîne de requête :

```
add rewrite policy pol_redirect_query 'http.req.header("Host").eq(www.
example.com)&& http.req.url.contains("?")'act_redirect_query
```


- Liez votre nouvelle stratégie à l'échelle mondiale.

Étant donné que cette stratégie de réécriture est très spécifique et doit être exécutée avant toute autre stratégie de réécriture, il est conseillé de lui attribuer une priorité élevée. Si vous lui attribuez une priorité de 1, elle est évaluée en premier.

Réécriture d'HTTP en HTTPS

Cet exemple explique comment réécrire les réponses du serveur Web pour rechercher toutes les URL commençant par la chaîne « HTTP » et remplacer cette chaîne par « https ». Vous pouvez l'utiliser pour éviter de devoir mettre à jour des pages Web après avoir déplacé un serveur de HTTP vers HTTPS.

Pour rediriger les URL HTTP vers HTTPS à l'aide de l'interface de ligne de commande

- Pour créer une action de réécriture nommée act_replace_http_with_https qui remplace toutes les instances de la chaîne « HTTP » par la chaîne « https », entrez la commande suivante :

```
add rewrite action act_replace_http_with_https replace_all 'http.res.body
(100)''"https"'-search http
```

- Pour créer une stratégie de réécriture nommée pol_replace_http_with_https qui détecte les connexions au serveur Web, entrez la commande suivante :

```
add rewrite policy pol_replace_http_with_https TRUE act_replace_http_with_https
 NOREWRITE
```

- Liez votre nouvelle stratégie à l'échelle mondiale.

Pour résoudre cette opération de réécriture, reportez-vous à la section « Étude de cas : Politique de réécriture pour la conversion des liens HTTP en HTTPS ne fonctionne pas. «

Suppression des en-têtes indésirables

Cet exemple explique comment utiliser une stratégie de réécriture pour supprimer les en-têtes indésirables. Plus précisément, l'exemple montre comment supprimer les en-têtes suivants :

- **Acceptez l'en-tête Encoding.** La suppression de l'en-tête Accept Encoding des réponses HTTP empêche la compression de la réponse.
- **En-tête Emplacement du contenu.** La suppression de l'en-tête Content Location des réponses HTTP empêche votre serveur de fournir à un pirate des informations susceptibles de permettre une faille de sécurité.

Pour supprimer des en-têtes des réponses HTTP, vous créez une action de réécriture et une stratégie de réécriture, et vous liez la stratégie globalement.

Pour créer l'action de réécriture appropriée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour supprimer l'en-tête Accepter l'encodage et empêcher la compression des réponses ou supprimer l'en-tête Emplacement de contenu :

- `add rewrite action "act_remove-ae"delete_http_header "Accept-Encoding"`
- `add rewrite action "act_remove-cl"delete_http_header "Content-Location"`

Pour créer la stratégie de réécriture appropriée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour supprimer l'en-tête Accepter l'encodage ou l'en-tête Emplacement de contenu :

- `add rewrite policy "pol_remove-ae"true "act_remove-ae"`
- `add rewrite policy "pol_remove-cl"true "act_remove-cl"`

Pour lier la stratégie globalement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes, le cas échéant, pour lier globalement la stratégie que vous avez créée :

- `bind rewrite global pol_remove_ae 100`
- `bind rewrite global pol_remove_cl 200`

Réduction des redirections de serveur Web

Cet exemple explique comment utiliser une stratégie de réécriture pour modifier les connexions à votre page d'accueil et à d'autres URL qui se terminent par une barre oblique (/) vers la page d'index par défaut de votre serveur, empêchant les redirections et réduisant la charge sur votre serveur.

Pour modifier les requêtes HTTP au niveau du répertoire afin d'inclure la page d'accueil par défaut à l'aide de l'interface de ligne de commande

- Pour créer une action de réécriture nommée action-default-homepage qui modifie les URL qui se terminent par une barre oblique pour inclure la page d'accueil par défaut index.html, tapez :

```
add rewrite action "action-default-homepage"replace http.req.url.path "\"/
index.html\""
```

- Pour créer une stratégie de réécriture nommée policy-default-homepage qui détecte les connexions à votre page d'accueil et applique votre nouvelle action, tapez :

```
add rewrite policy "policy-default-homepage"q\##http.req.url.path.EQ("/")"
action-default-homepage"\##
```


- Liez globalement votre nouvelle politique pour la mettre en œuvre.

Masquage de l'en-tête du serveur

Cet exemple explique comment utiliser une stratégie de réécriture pour masquer les informations contenues dans l'en-tête du serveur dans les réponses HTTP de votre serveur Web. Cet en-tête contient des informations que les pirates peuvent utiliser pour compromettre votre site Web. Bien que le masquage de l'en-tête n'empêche pas un hacker qualifié de trouver des informations sur votre serveur, cela rend le piratage de votre serveur Web plus difficile et encourage les pirates à choisir des cibles moins protégées.

Pour masquer l'en-tête du serveur dans les réponses de l'interface de ligne de commande

1. Pour créer une action de réécriture nommée act_mask-server qui remplace le contenu de l'en-tête Server par une chaîne non informative, tapez :

```
add rewrite action "act_mask-server"replace "http.RES.HEADER(\"Server\")""
\"Web Server 1.0\""
```

1. Pour créer une stratégie de réécriture nommée pol_mask-server qui détecte toutes les connexions, tapez :

```
add rewrite policy "pol_mask-server"true "act_mask-server"
```

1. Liez globalement votre nouvelle politique pour la mettre en œuvre.

Comment convertir du texte brut en chaîne encodée par URL et de la manière inverse

Les expressions suivantes convertissent le texte brut en chaîne encodée par URL et de la manière inverse :

1. URL_RESERVED_CHARS_SAFE (chaîne vers URL ENCODED).

Exemple :

```
("abc def&123").URL_RESERVED_CHARS_SAFE
Output will be
 “abc%20def%26123”  which is url encoded.
<!--NeedCopy-->
```

1. SET_TEXT_MODE (URLENCODED) .DECODE_USING_TEXT_MODE. (URL ENCODÉE en chaîne)

Exemple :

```
("abc%20def%26123").SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE
Output will be
```



```
 “abc def&123”
<!--NeedCopy-->
```

Exemples de stratégies de réécriture et de répondeur

October 5, 2021

Voici quelques exemples de stratégies de réécriture et de répondeur :

Exemple 1 : Pour ajouter un en-tête Client-IP local à l’aide de l’interface de ligne de commande

```
add rewrite action act_ins_client insert_http_header NS-Client 'CLIENT.
   IP.SRC'
add rewrite policy pol_ins_client http.req.is_valid act_ins_client
bind rewrite global pol_ins_client 300 END

namem@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Date: Tue, 10 Nov 2020 10:06:48 GMT
* Server Apache/2.2.15 (CentOS) is not blacklisted
< Server: Apache/2.2.15 (CentOS)
< Last-Modified: Thu, 20 Jun 2019 07:16:04 GMT
< ETag: "816c5-5-58bbc1e73cdd3"
< Accept-Ranges: bytes
< Content-Length: 5
< Content-Type: text/html; charset=UTF-8
< NS-Client: 10.102.1.98
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_namem@obelix:~$

<!--NeedCopy-->
```


Exemple 2 : masquer le type de serveur HTTP

```
add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER("Server") ""Web Server 1.0""
add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
namem@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Date: Tue, 10 Nov 2020 10:15:42 GMT
* Server Web Server 1.0 is not blacklisted
< Server: Web Server 1.0
< Last-Modified: Thu, 20 Jun 2019 07:16:04 GMT
< ETag: "816c5-5-58bbc1e73cdd3"
< Accept-Ranges: bytes
< Content-Length: 5
< Content-Type: text/html; charset=UTF-8
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_namem@obelix:~$
<!--NeedCopy-->
```

Exemple 3 : Répondez en redirigeant vers une autre URL lorsqu'une URL est reçue

```
> add responder action act1 redirect ""www.google.com""
 Done
> add responder policy pol1 'HTTP.REQ.URL.CONTAINS("file")' act1
 Done
> bind responder global pol1 1
 Done
>

name:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
```



```
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 302 Found : Moved Temporarily
< Location: www.google.com
< Connection: close
< Cache-Control: no-cache
< Pragma: no-cache
<
* Closing connection 0
name@obelix:~$
<!--NeedCopy-->
```

Exemple 4 : Répondez avec un message qui peut être n'importe quelle expression ou un texte

```
add responder action act123 respondwith ""Please reach out to
   administrator""
add responder policy pol1 "HTTP.REQ.URL.CONTAINS("file")" act123
bind responder global pol1 100 END

name@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10..Responder Action and Policy:

>add responder action Redirect-Action redirect ""https://xyz.abc.com/
   dispatcher/SAML2AuthService?siteurl=wmav"" -responseStatusCode 302

>add responder policy Redirect-Policy "HTTP.REQ.HOSTNAME.CONTAINS("abc"
   )" Redirect-Action

Binding to LB Virtual Server:

>bind lb vserver Test1_SF -policyName Redirect-Policy -priority 100 -
   gotoPriorityExpression END -type REQUEST.
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
* Connection #0 to host 10.10.10.10 left intact
```



```
Please reach out to administratort_name@obelix:~$
<!--NeedCopy-->
```

Exemple 5 : répondre avec une page HTML importée

```
import responder htmlpage http://10.10.10.10)/testsite/file5.html
   page112
add responder action act1 respondwithHtmlpage page1
add responder policy pol1 true act1
bind responder global pol1 100

name@obelix:~$ curl -v http://10.10.10.10)/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10)) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.102.58.140
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Content-Length: 5
< Content-Type: text/html
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_name@obelix:~$
<!--NeedCopy-->
```

Exemple 6 : URL de redirection basée sur HOSTNAME à l'aide de la stratégie de répondeur

```
Responder Action and Policy:

>add responder action Redirect-Action redirect ""https://xyz.abc.com/
   dispatcher/SAML2AuthService?siteurl=wmav"" -responseStatusCode 302

>add responder policy Redirect-Policy "HTTP.REQ.HOSTNAME.CONTAINS("abc"
   )" Redirect-Action

Binding to LB Virtual Server:

```



```
>bind lb vserver Test1_SF -policyName Redirect-Policy -priority 100 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Limitation de débit

October 5, 2021

La fonctionnalité de limitation de débit vous permet de définir la charge maximale pour une entité réseau ou une entité virtuelle donnée sur l'appliance Citrix ADC. Cette fonctionnalité vous permet de configurer la solution matérielle-logicielle pour surveiller le taux de trafic associé à l'entité et prendre des mesures préventives, en temps réel, en fonction du taux de trafic. Cette fonctionnalité est particulièrement utile lorsque le réseau est attaqué par un client hostile qui envoie un flot de requêtes à la solution matérielle-logicielle. Vous pouvez atténuer les risques qui affectent la disponibilité des ressources pour les clients et améliorer la fiabilité du réseau et des ressources que l'appliance gère.

Vous pouvez surveiller et contrôler le taux de trafic associé aux entités virtuelles et définies par l'utilisateur, y compris les serveurs virtuels, les URL, les domaines et les combinaisons d'URL et de domaines. Vous pouvez limiter le taux de trafic s'il est trop élevé, baser la mise en cache des informations sur le débit de trafic et rediriger le trafic vers un serveur virtuel d'équilibrage de charge donné si le débit de trafic dépasse une limite prédéfinie. Vous pouvez appliquer une surveillance basée sur le débit aux requêtes HTTP, TCP et DNS.

Pour surveiller le taux de trafic pour un scénario donné, vous devez configurer un *identificateur de limite de débit*. Un identificateur de limite de débit spécifie des seuils numériques tels que le nombre maximal de demandes ou de connexions (d'un type particulier) autorisées dans une période spécifiée appelée *tranche de temps*.

Vous pouvez également configurer des filtres, appelés *sélecteurs de flux*, et les associer à des identificateurs de limite de débit lorsque vous configurez les identificateurs. Après avoir configuré le sélecteur de flux facultatif et l'identificateur de limite, vous devez appeler l'identificateur de limite à partir d'une stratégie avancée. Vous pouvez appeler des identificateurs à partir de n'importe quelle fonctionnalité dans laquelle l'identifiant peut être utile, y compris la réécriture, le répondeur, le DNS et la mise en cache intégrée.

Vous pouvez activer et désactiver globalement les interruptions SNMP pour les identificateurs de limite de débit. Chaque interruption contient des données cumulatives pour l'intervalle de collecte de données configuré de l'identificateur de limite de débit (tranche de temps), sauf si vous avez spécifié plusieurs interruptions à générer par tranche de temps. Pour plus d'informations sur la configuration des interruptions et des gestionnaires SNMP, consultez SNMP.

Configuration d'un sélecteur de flux

October 5, 2021

Un sélecteur de flux de trafic est un filtre facultatif permettant d'identifier une entité pour laquelle vous souhaitez limiter l'accès. Le sélecteur est appliqué à une demande ou à une réponse et sélectionne des points de données (clés) qui peuvent être analysés par un identifiant de flux de débit. Ces points de données peuvent être basés sur presque toutes les caractéristiques du trafic, y compris les adresses IP, les sous-réseaux, les noms de domaine, les identifiants TCP ou UDP, et des chaînes ou extensions particulières dans les URL.

Un sélecteur de flux se compose d'expressions de stratégie avancées individuelles appelées selectlets. Chaque selectlet est une expression de stratégie avancée non composée. Un sélecteur de flux de trafic peut contenir jusqu'à cinq expressions non composées appelées selectlets. Chaque selectlet est considéré comme étant en relation AND avec les autres expressions. Voici quelques exemples de selectlets :

```
1 http.req.url
2 http.res.body(1000>after_str("car_model").before_str("made_in")"
3 "client.ip.src.subnet(24)"
4 <!--NeedCopy-->
```

L'ordre dans lequel vous spécifiez les paramètres est significatif. Par exemple, si vous configurez une adresse IP et un domaine (dans cet ordre) dans un sélecteur, puis que vous spécifiez le domaine et l'adresse IP (dans l'ordre inverse) dans un autre sélecteur, Citrix ADC considère ces valeurs comme uniques. Cela peut entraîner le comptage deux fois de la même transaction. De plus, si plusieurs stratégies invoquent le même sélecteur, Citrix ADC peut, là encore, compter la même transaction plusieurs fois.

Remarque : Si vous modifiez une expression dans un sélecteur de flux, une erreur peut s'afficher si une stratégie qui l'appelle est liée à une nouvelle étiquette de stratégie ou à un nouveau point de liaison. Par exemple, supposons que vous créiez un sélecteur de flux nommé MyStreamSelector1, que vous l'appeliez à partir de MyLimitid1 et que vous invoquez l'identificateur à partir d'une stratégie DNS nommée DNSRateLimit1. Si vous modifiez l'expression dans MyStreamSelector1, vous risquez de recevoir une erreur lors de la liaison de DNSRateLimit1 à un nouveau point de liaison. La solution de contournement consiste à modifier ces expressions avant de créer les stratégies qui les invoquent.

Pour configurer un sélecteur de flux de trafic à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
add stream selector <name> <rule> ...
<!--NeedCopy-->
```

Exemple :

```
add stream selector myStreamSel HTTP.REQ.URL CLIENT.IP.SRC
<!--NeedCopy-->
```

Pour configurer un sélecteur de flux à l'aide de l'utilitaire de configuration

Accédez à AppExpert > Limitation de débit > Sélecteurs, cliquez sur Ajouter et spécifiez les détails pertinents.

Configuration d'un identificateur de limite de débit de trafic

October 5, 2021

Un identificateur de limite de débit vérifie si la quantité de trafic dépasse une valeur spécifiée, dans un intervalle de temps particulier. L'identificateur renvoie un « Boolean TRUE » si la quantité de trafic dépasse une limite dans un intervalle de temps particulier. Lorsque vous incluez un identificateur de limite dans l'expression de stratégie DAvanced composée d'une règle de stratégie, vous devez inclure un sélecteur de flux. Si vous ne le spécifiez pas, l'identificateur de limite est appliqué à toutes les demandes ou réponses identifiées par les expressions composées.

> **Remarque :**
>
> La longueur maximale de stockage des résultats de chaîne (par exemple, HTTP.REQ.URL) est de 60 caractères. Si la chaîne (par exemple, URL) comporte 1 000 caractères, dont 50 sont suffisants pour identifier une chaîne de manière unique, vous pouvez utiliser une expression pour extraire les 50 caractères requis.

Pour configurer un identificateur de limite de trafic à partir de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ns limitIdentifier <limitIdentifier> -threshold <positive_integer>
    -timeSlice <positive_integer> -mode <mode> -limitType ( BURSTY |
    SMOOTH ) -selectorName <string> -maxBandwidth <positive_integer> -
    trapsInTimeSlice <positive_integer>
<!--NeedCopy-->
```


Description de l'argument

Identificateur de limite. Nom d'un identificateur de limite de taux. Doit commencer par une lettre ASCII ou un caractère de soulignement (_) et ne doit être composé que de caractères alphanumériques ou de soulignement ASCII. Les mots réservés ne doivent pas être utilisés. Il s'agit d'un argument obligatoire. Longueur maximale : 31

seuil. Nombre maximal de demandes autorisées dans la tranche de temps donnée lorsque les demandes (le mode est défini sur REQUEST_RATE) sont suivies par tranche de temps. Lorsque les connexions (le mode est défini sur CONNECTION) sont suivies, il s'agit du nombre total de connexions qui seraient laissées passer. Valeur par défaut : 1 Valeur minimale : 1 Valeur maximale : 4294967295

TimeSlice. Intervalle de temps, en millisecondes, spécifié en multiples de 10, pendant lequel les demandes sont suivies pour vérifier si elles dépassent le seuil. Cet argument n'est nécessaire que lorsque le mode est défini sur REQUEST_RATE. Valeur par défaut : 1000 Valeur minimale : 10 Valeur maximale : 4294967295

mode. Définit le type de trafic à suivre.

1. REQUEST_RATE. Effectue le suivi des demandes/tranche de temps.
2. CONNEXION. Suivi des transactions actives.

LimitType. Type de demande lisse ou éclatante.

NomSelector. Nom du sélecteur de limite de taux. Si cet argument est NULL, la limitation de débit sera appliquée à tout le trafic reçu par le serveur virtuel ou Citrix ADC (selon que l'identificateur de limite est lié à un serveur virtuel ou globalement) sans aucun **filtrage. Longueur maximale : 31**

Bande passante maximale. Bande passante maximale autorisée, en kbps. Valeur minimale : 0 Valeur maximale : 4294967287

Exemple :

Configuration de l'identificateur de limite de débit de trafic en mode BURSTY :

```
1 add ns limitIdentifier 100_request_limit -threshold 100 -timeSlice 1000
      -mode REQUEST_RATE -limitType BURSTY -selectorName
     limit_100_requests_selector -trapsInTimeSlice 30
2 <!--NeedCopy-->
```

Configuration de l'identificateur de limite de débit de trafic en mode SMOOTH :

```
1 add ns limitidentifier limit_req -mode request_rate -limitType smooth -
     timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200
2 <!--NeedCopy-->
```


Pour configurer un identificateur de limite de trafic à l'aide de l'utilitaire de configuration

Accédez à AppExpert > Limitation de débit > Identificateurs de limite, cliquez sur Ajouter et spécifiez les détails pertinents.

Configuration et liaison d'une stratégie de débit de trafic

October 5, 2021

Vous implémentez un comportement d'application basé sur le débit en configurant une stratégie dans une fonctionnalité Citrix ADC appropriée. La fonctionnalité doit prendre en charge les stratégies avancées. L'expression de stratégie doit contenir le préfixe d'expression suivant pour permettre à la fonctionnalité d'analyser le taux de trafic :

```
sys.check_limit(<limit_identifier>)
<!--NeedCopy-->
```

Où limit_identifier est le nom d'un identificateur de limite.

L'expression de stratégie doit être une expression composée qui contient au moins deux composants :

- Expression qui identifie le trafic auquel l'identificateur de limite de débit est appliqué. Par exemple :

```
    http.req.url.contains("my_aspx.aspx").
<!--NeedCopy-->
```

- Expression qui identifie un identificateur de limite de taux, par exemple, sys.check_limit (« my_limit_identifier »). Il doit s'agir de la dernière expression de l'expression de stratégie.

Pour configurer une stratégie basée sur les taux à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour configurer une stratégie basée sur les taux et vérifier la configuration :

```
add cache|dns|rewrite|responder policy <policy_name> -rule expression
    && sys.check_limit("<LimitIdentifierName>") [<feature-specific
    information>]
<!--NeedCopy-->
```


Voici un exemple complet de règle de stratégie basée sur le taux. Notez que cet exemple suppose que vous avez configuré l'action du répondeur, send_direct_url, qui est associée à la stratégie. Notez que le paramètre sys.check_limit doit être le dernier élément de l'expression de stratégie :

```
1 add responder policy responder_threshold_policy "http.req.url.contains(
     "myindex.html") && sys.check_limit("my_limit_identifier")"
     send_direct_url
2 <!--NeedCopy-->
```

Pour plus d'informations sur la liaison d'une stratégie globalement ou à un serveur virtuel, reportez-vous à la section « Liaison de stratégies avancées ». «

Pour configurer une stratégie basée sur les taux à l'aide de l'utilitaire de configuration

1. Dans le volet de navigation, développez la fonctionnalité dans laquelle vous souhaitez configurer une stratégie (par exemple, Mise en cache intégrée, Réécriture ou Répondeur), puis cliquez sur Stratégies.
2. Dans le volet d'informations, cliquez sur Ajouter. Dans Nom, saisissez un nom unique pour la stratégie.
3. Sous Expression, entrez la règle de stratégie et assurez-vous d'inclure le paramètre sys.check_limit en tant que composant final de l'expression. Par exemple :

   ```
   1 http.req.url.contains("my_aspx.aspx") && sys.check_limit("
        my_limit_identifier")
   2 <!--NeedCopy-->
   ```

4. Saisissez des informations spécifiques à la fonctionnalité concernant la stratégie.

   Par exemple, vous devrez peut-être associer la stratégie à une action ou à un profil. Pour plus d'informations, consultez la documentation spécifique aux fonctionnalités.
5. Cliquez sur Créer, puis cliquez sur Fermer.
6. Cliquez sur Enregistrer.

Affichage du débit de trafic

August 20, 2021

Si le trafic via un ou plusieurs serveurs virtuels correspond à une stratégie basée sur les taux, vous pouvez afficher le débit de ce trafic. Les statistiques de taux sont conservées dans l'identificateur de limite que vous avez nommé dans la règle pour la stratégie basée sur le taux. Si plusieurs stratégies

utilisent le même identificateur de limite, vous pouvez afficher le taux de trafic tel que défini par les accès à toutes les stratégies qui utilisent cet identificateur de limite particulier.

Pour afficher le débit de trafic à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour afficher le débit de trafic :

```
show ns limitSessions <limitIdentifier>
<!--NeedCopy-->
```

Exemple :

```
sh limitsession myLimitSession
<!--NeedCopy-->
```

Pour afficher le débit de trafic à l'aide de l'utilitaire de configuration

1. Accédez à AppExpert > Limitation de débit > Identificateurs de limite.
2. Sélectionnez un identificateur de limite dont vous souhaitez afficher le taux de trafic.
3. Cliquez sur le bouton Afficher les sessions. Si le trafic via un ou plusieurs serveurs virtuels correspond à une stratégie de limitation de débit qui utilise cet identificateur de limite (et que les accès se trouvent dans la tranche de temps configurée pour cet identificateur), la boîte de dialogue Détails de la session apparaît. Sinon, vous recevez un message « Aucune session n'existe ».

Test d'une stratégie basée sur le débit

January 21, 2021

Pour tester une stratégie basée sur le taux, vous pouvez envoyer du trafic vers n'importe quel serveur virtuel auquel une stratégie basée sur le taux est liée.

Vue d'ensemble des tâches : Test d'une stratégie basée sur le taux

1. Configurez un sélecteur de flux (facultatif) et un identificateur de limite de débit (obligatoire). Par exemple :

```
add stream selector sel_subnet Q.URL "CLIENT.IP.SRC.SUBNET(24)"
add ns limitIdentifier k_subnet -Threshold 4 -timeSlice 3600 -mode
    REQUEST_RATE  -limittype smooth  -selectorName sel_subnet  -
   trapsInTimeSlice 8
<!--NeedCopy-->
```


2. Configurez l'action que vous souhaitez associer à la stratégie qui utilise l'identificateur de limite de débit. Par exemple :

```
add responder action resp_redirect redirect ""http://response_site.com/""
<!--NeedCopy-->
```

3. Configurez une stratégie qui utilise le préfixe d'expression sys.check_limit pour appeler l'identificateur de limite de débit. Par exemple, la stratégie peut appliquer un identificateur de limite de débit à toutes les demandes provenant d'un sous-réseau particulier, comme suit :

```
add responder policy resp_subnet "SYS.CHECK_LIMIT("k_subnet")" resp_redirect
<!--NeedCopy-->
```

4. Liez la stratégie globalement ou à un serveur virtuel. Par exemple :

```
bind responder global resp_subnet 6 END -type DEFAULT
<!--NeedCopy-->
```

5. Dans une barre d'adresse du navigateur, envoyez une requête HTTP test à un serveur virtuel. Par exemple :

```
http://<IP of a vserver>/testsite/test.txt
<!--NeedCopy-->
```

6. À l'invite de commandes Citrix ADC, tapez :

```
show ns limitSessions <limitIdentifier>
<!--NeedCopy-->
```

Exemple

```
> sh limitsession k_subnet
1)      Time Remaining:       98 secs  Hits: 2
                            Action Taken: 0
        Total Hash:    1718618  Hash String: /test.txt
        IPs gathered:
                1) 10.217.253.0
        Active Transactions: 0
 Done
>
<!--NeedCopy-->
```


7. Répétez la requête et vérifiez à nouveau les statistiques de l'identificateur de limite pour vérifier que les statistiques sont mises à jour correctement.

Exemples de politiques basées sur les taux

October 5, 2021

Le tableau suivant présente des exemples de stratégies basées sur les taux.

Table 1. Examples of Rate-Based Policies

Purpose	Example

Limit the number of requests per second from a URL	`add stream selector ipStreamSelector http.req.url "client.ip.src"`
	`add ns limitIdentifier ipLimitIdentifier -threshold 4 -timeSlice 1000`
	`-mode request_rate -limitType smooth -selectorName ipStreamSelector`
	
	`add responder action myWebSiteRedirectAction redirect`
	`"\"http://www.mycompany.com/\""`
	
	`add responder policy ipLimitResponderPolicy "http.req.url.contains(\"myasp.asp\")`
	`&& sys.check_limit(\"ipLimitIdentifier\")" myWebSiteRedirectAction`
	
	`bind responder global ipLimitResponderPolicy 100 END -type default`

Cache a response if the request URL rate exceeds 5 per 20000 milliseconds	`add stream selector cacheStreamSelector http.req.url`
	`add ns limitidentifier cacheRateLimitIdentifier -threshold 5 -timeSlice 2000`
	`-selectorName cacheStreamSelector`
	
	`add cache policy cacheRateLimitPolicy -rule "http.req.method.eq(get)`
	`&& sys.check_limit(\"cacheRateLimitIdentifier\")" -action cache`
	
	`bind cache global cacheRateLimitPolicy -priority 10`

Drop a connection on the basis of cookies received in requests from www.yourcompany.com if the requests exceed the rate limit	`add stream selector reqCookieStreamSelector "http.req.cookie`
	`.value(\"mycookie\")" "client.ip.src.subnet(24)"`
	
	`add ns limitIdentifier myLimitIdentifier -Threshold 2 -timeSlice 3000`
	`-selectorName reqCookieStreamSelector`
	
	`add responder action sendRedirectUrl redirect '\"http://www.mycompany.com\"`
	`+ http.req.url' -bypassSafetyCheck YES`
	
	`add responder policy rateLimitCookiePolicy`
	`"http.req.url.contains(\"www.yourcompany.com\")`
	`&& sys.check_limit(\"myLimitIdentifier\")" sendRedirectUrl`

Drop a DNS packet if the requests from a particular client IP address and DNS domain exceed the rate limit	`add stream selector dropDNSStreamSelector client.udp.dns.domain client.ip.src`
	`add ns limitIdentifier dropDNSRateIdentifier -timeslice 20000 -mode request_rate`
	`-selectorName dropDNSStreamSelector -maxBandwidth 1 -trapsintimeslice 20`
	
	`add dns policy dnsDropOnClientRatePolicy "sys.check_limit`
	`(\"dropDNSRateIdentifier\")" -drop yes`

Limit the number of HTTP requests that arrive from the same host (with a subnet mask of 32) and that have the same destination IP address.	`add stream selector ipv6_sel "CLIENT.IPv6.src.subnet(32)" CLIENT.IPv6.dst Q.URL`
	`add ns limitIdentifier ipv6_id -imeSlice 20000 -selectorName ipv6_sel`
	`add lb vserver ipv6_vip HTTP 3ffe::209 80 -persistenceType NONE -cltTimeout 180`
	`add responder action redirect_page redirect "\"http://redirectpage.com/\""`
	`add responder policy ipv6_resp_pol "SYS.CHECK_LIMIT(\"ipv6_id\")" redirect_page`
	`bind responder global ipv6_resp_pol 5 END -type DEFAULT`

Exemples de cas d'utilisation pour les stratégies basées sur le débit

January 21, 2021

Les scénarios suivants décrivent deux utilisations des stratégies basées sur le taux dans l'équilibrage de charge du serveur global (GSLB) :

- Le premier scénario décrit l'utilisation d'une stratégie basée sur le taux qui envoie du trafic vers un nouveau centre de données si le taux de demandes DNS dépasse 1000 par seconde.
- Dans le second scénario, si plus de cinq demandes DNS arrivent pour un client DNS local (LDNS) au cours d'une période donnée, les demandes supplémentaires sont supprimées.

Redirection du trafic en fonction du tarif de trafic

Dans ce scénario, vous configurez une méthode d'équilibrage de charge basée sur la proximité et une stratégie de limitation de débit qui identifie les demandes DNS pour une région particulière. Dans la stratégie de limitation de débit, vous spécifiez un seuil de 1000 demandes DNS par seconde. Une stratégie DNS applique la stratégie de limitation des tarifs aux demandes DNS pour la région "Europe.gb.17.london.uk-east.isp-uk." Dans la stratégie DNS, les demandes DNS qui dépassent le seuil de limitation de débit, commençant par la demande 1001 et se poursuivant jusqu'à la fin de l'intervalle d'une seconde, doivent être transmises aux adresses IP associées à la région "North America.us.tx.dallas.us-east.isp-US."

La configuration suivante illustre ce scénario :

```
1 add stream selector DNSSelector1 client.udp.dns.domain
2
3 add ns limitIdentifier DNSLimitIdentifier1 -threshold 5 -timeSlice 1000
      -selectorName DNSSelector1
4
5 add dns policy DNSLimitPolicy1 "client.ip.src.matches_location("Europe.
    GB.17.London.\*.\*") &&
6 sys.check_limit("DNSLimitIdentifier1")" -preferredLocation "North
    America.US.TX.Dallas.\*.\*"
7
8 bind dns global DNSLimitPolicy1 5
9 <!--NeedCopy-->
```

Abandon des demandes DNS sur la base du tarif de trafic

Dans l'exemple suivant d'équilibrage de charge de serveur global, vous configurez une stratégie de limitation de débit qui permet de rediriger un maximum de cinq requêtes DNS dans un intervalle par-

ticulier, par domaine, vers un client LDNS pour résolution. Toutes les demandes qui dépassent ce taux sont supprimées. Ce type de stratégie peut aider à protéger Citrix ADC contre l'exploitation des ressources. Par exemple, dans ce scénario, si la durée de vie (TTL) d'une connexion est de cinq secondes, cette stratégie empêche le LDNS de demander un domaine. Au lieu de cela, il utilise des données mises en cache sur Citrix ADC.

```
add stream selector LDNSSelector1 client.udp.dns.domain client.ip.src

add ns limitIdentifier LDNSLimitIdentifier1 -threshold 5 -timeSlice
    1000 -selectorName LDNSSelector1

add dns policy LDNSPolicy1 "client.udp.dns.domain.contains(".") && sys.
    check_limit("LDNSLimitIdentifier1")" -drop YES

bind dns global LDNSPolicy1 6

show gslb vserver gvip

gvip - HTTP     State: UP
Last state change was at Mon Sep  8 11:50:48 2008 (+711 ms)
Time since last state change: 1 days, 02:55:08.830
Configured Method: STATICPROXIMITY
BackupMethod: ROUNDROBIN
No. of Bound Services :  3 (Total)       3 (Active)
Persistence: NONE       Persistence ID: 100
Disable Primary Vserver on Down: DISABLED       Site Persistence: NONE
Backup Session Timeout: 0
Empty Down Response: DISABLED
Multi IP Response: DISABLED Dynamic Weights: DISABLED
Cname Flag: DISABLED
Effective State Considered: NONE
1.     site11_svc(10.100.00.00: 80)- HTTP State: UP    Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: Europe.GB.17.London.UK-East.ISP-UK
2.      site12_svc(10.101.00.100: 80)- HTTP State: UP   Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: North America.US.TX.Dallas.US-East.ISP-US
3.      site13_svc(10.102.00.200: 80)- HTTP State: UP   Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
```



```
Threshold : BELOW
Location: North America.US.NJ.Salem.US-Mid.ISP-US
4.      www.gslbindia.com        TTL: 5 secn
Cookie Timeout: 0 min   Site domain TTL: 3600 sec
Done
<!--NeedCopy-->
```

Limitation du débit pour les domaines de trafic

January 21, 2021

Vous pouvez configurer la limitation de débit pour les domaines de trafic. L'expression suivante dans le langage des expressions Citrix ADC pour identifie le trafic associé aux domaines de trafic.

- client.traffic_domaine.id

Vous pouvez configurer la limitation de débit pour le trafic associé à un domaine de trafic particulier, à un ensemble de domaines de trafic ou à tous les domaines de trafic.

Pour configurer la limitation de débit pour les domaines de trafic, effectuez les opérations suivantes sur une appliance Citrix ADC à l'aide de l'utilitaire de configuration ou de la ligne de commande Citrix ADC :

1. Configurez un sélecteur de flux qui utilise l'expression client.traffic_domain.id pour identifier le trafic, associé aux domaines de trafic, afin d'être limité à la vitesse.
2. Configurez un identificateur de limite de débit qui spécifie des paramètres tels que le seuil maximal pour que le trafic soit limité. Vous associez également un sélecteur de flux au limiteur de débit dans cette étape.
3. Configurez une action que vous souhaitez associer à la stratégie qui utilise l'identificateur de limite de débit.
4. Configurez une stratégie qui utilise le préfixe d'expression sys.check_limit pour appeler l'identificateur de limite de débit et associez l'action à cette stratégie.
5. Liez la stratégie à l'échelle mondiale.

Prenons un exemple dans lequel deux domaines de trafic, avec les ID 10 et 20, sont configurés sur Citrix ADC NS1. Sur le domaine de trafic 10, LB1-TD-1 est configuré pour équilibrer la charge des serveurs S1 et S2 ; LB2-TD1 est configuré pour équilibrer la charge des serveurs S3 et S4.

Sur le domaine de trafic 20, LB1-TD-2 est configuré pour équilibrer la charge des serveurs S5 et S6 ; LB2-TD2 est configuré pour équilibrer la charge des serveurs S7 et S8.

Le tableau suivant répertorie quelques exemples de stratégies de limitation de débit pour les domaines de trafic dans l'exemple de configuration.

Objectif	Commandes CLI
Limitez le nombre de requêtes à 10 par seconde pour chacun des domaines de trafic.	add stream selector tdratelimit-1 CLIENT.TRAFFIC_DOMAIN.ID add ns limitIdentifier limitidf-1 -threshold 10 -selectorName tdratelimit-1 -trapsInTimeSlice 0 add responder policy ratelimit-pol “sys.check_limit(\“limitidf-1\”)” DROP bind responder global ratelimit-pol 1
Limitez le nombre de requêtes à 5 par client et par seconde pour chacun des domaines de trafic.	add stream selector tdandclientip CLIENT.IP.SRC,CLIENT.TRAFFIC_DOMAIN.ID add ns limitIdentifier td_limitidf -threshold 5 -selectorName tdandclientip -trapsInTimeSlice 5 add responder policy tdratelimit-pol “sys.check_limit(\“td_limitidf\”)” DROP bind responder global tdratelimit-pol 2
Limitez le nombre de requêtes envoyées pour un domaine de trafic particulier (par exemple le domaine de trafic 10) à 30 requêtes toutes les 3 secondes.	add stream selector tdratelimit CLIENT.TRAFFIC_DOMAIN.ID add ns limitIdentifier td10_limitidf -threshold 30 -timeSlice 3000 -selectorName tdratelimit -trapsInTimeSlice 5 add responder policy td10ratelimit “client.traffic_domain.id==10 && sys.check_limit(\“td10_limitidf\”)” DROP bind responder global td10ratelimit 3
Limitez le nombre de connexions à 5 par client et par seconde pour un domaine de trafic particulier (par exemple le domaine de trafic 20).	add stream selector tdandclientip CLIENT.IP.SRC CLIENT.TRAFFIC_DOMAIN.ID add ns limitIdentifier td20_limitidf -threshold 5 -mode CONNECTION -selectorName tdandclientip -trapsInTimeSlice 5 add responder policy td20_ratelimit “client.traffic_domain.id==20 && sys.check_limit(\“td20_limitidf\”)” DROP bind responder global td20_ratelimit 4

Configurer la limite de débit au niveau des paquets

August 20, 2021

Vous pouvez configurer un sélecteur de flux et une stratégie de répondeur pour collecter des statistiques au niveau des paquets circulant à travers toutes les connexions identifiées par le sélecteur. Si le nombre de paquets par seconde dépasse le seuil configuré, la stratégie applique l'action configurée (RESET ou DROP). Vous pouvez configurer ces stratégies pour tous les types de serveurs virtuels. Les paquets de toutes tailles sont considérés.

Pour configurer la limitation de débit au niveau des paquets, effectuez les tâches suivantes

1. Activer l'équilibrage de charge
2. Ajouter un sélecteur de flux
3. Ajouter un identificateur de flux
4. Ajouter une stratégie de répondeur
5. Ajouter un serveur virtuel d'équilibrage de charge
6. Politique de répondeur de liaison

Pour activer la fonction d'équilibrage de charge

À l'invite de commandes, tapez :

```
enable ns feature lb
<!--NeedCopy-->
```

Pour ajouter un sélecteur de flux

À l'invite de commandes, tapez :

```
add stream selector packetlimitselector client.ip.src client.tcp.
   srcport client.ip.dst client.tcp.dstport
<!--NeedCopy-->
```

Pour ajouter un identificateur de flux

À l'invite de commandes, tapez :

```
add stream identifier packetlimitidentifier packetlimitselector -
   interval 1
<!--NeedCopy-->
```


Pour activer le suivi des paquets ACK uniquement

À l'invite de commandes, tapez :

```
set stream identifier packetlimitidentifier  -trackAckOnlyPackets
    ENABLED
<!--NeedCopy-->
```

Pour ajouter une stratégie de répondeur

À l'invite de commandes, tapez :

```
add responder policy packet_rate_sessionpolicy "ANALYTICS.STREAM("
    packetlimitidentifier").COLLECT_STATS("PACKET_LIMIT", <
    max_threshold_PPS>, ACTION, 0/1)" NOOP
<!--NeedCopy-->
```

Où,

- <max_threshold_PPS>est le nombre maximal de paquets autorisés par la connexion par seconde.
- ACTION peut être DROP ou RESET.
- 0 ou 1 représente le type limite ; 0 représente le type limite BURSTY et 1 représente le type de limite SMOOTH.

Exemple :

```
add responder policy packet_rate_sessionpolicy "ANALYTICS.STREAM("
    packetlimitidentifier").COLLECT_STATS("PACKET_LIMIT", 40, RESET, 0)"
     NOOP
<!--NeedCopy-->
```

Pour ajouter un serveur virtuel d'équilibrage de charge

À l'invite de commandes, tapez :

```
add lb vserver <name> <serviceType> <ip> <port>

add lb vserver Vserver-lb-1 HTTP 10.102.20.200 80
<!--NeedCopy-->
```


Pour lier une stratégie de répondeur

Une fois le sélecteur et la stratégie de répondeur configurés, la stratégie peut être liée globalement ou au serveur virtuel spécifique.

À l'invite de commandes, tapez l'une des commandes suivantes :

```
bind responder global <policyName> <priority> [<gotoPriorityExpression
    >] [-type <type>] [-invoke  (<labelType>  <labelName>) ]
<!--NeedCopy-->
```

OU

```
bind lb vserver <name>@  (-policyName <string>@ [-priority <
    positive_integer>]
<!--NeedCopy-->
```

Exemples :

```
bind responder global packet_rate_sessionpolicy 101 END -type
    REQ_DEFAULT

bind responder global packet_rate_sessionpolicy 102 END -type

bind lb vserver v1 -policyname packet_rate_sessionpolicy -priority 10
<!--NeedCopy-->
```

Répondeur

January 21, 2021

> **Avertissement**
>
> Les fonctionnalités de filtrage utilisant des stratégies classiques sont obsolètes et Citrix vous recommande d'utiliser les fonctionnalités de réécriture et de répondeur avec une infrastructure de stratégie avancée.

Les configurations Web complexes d'aujourd'hui nécessitent souvent des réponses différentes aux requêtes HTTP qui apparaissent, à la surface, comme similaires. Lorsque les utilisateurs demandent une page Web, vous pouvez fournir une page différente en fonction de l'emplacement géographique de l'utilisateur, de la spécification du navigateur ou des langues acceptées par le navigateur et de l'ordre de préférence. Vous pouvez supprimer la connexion si la demande provient d'une plage d'adresses IP qui a généré des attaques DDoS ou lancé des tentatives de piratage.

Le répondeur prend en charge les protocoles tels que TCP, DNS (UDP) et HTTP. Lorsque le répondeur est activé sur votre appliance, les réponses du serveur peuvent être basées sur la personne qui envoie la demande, l'endroit d'où elle est envoyée et d'autres critères ayant des implications en matière de sécurité et de gestion du système. La fonctionnalité est simple et rapide à utiliser. En évitant l'invocation de fonctionnalités plus complexes, il réduit les cycles CPU et le temps passé à traiter les demandes qui ne nécessitent pas de traitement complexe.

Pour le traitement de données sensibles telles que les informations financières, si vous souhaitez vous assurer que le client utilise une connexion sécurisée pour naviguer sur un site, vous pouvez rediriger la demande vers une connexion sécurisée en utilisant `https://` plutôt que `http://`.

Pour utiliser un répondeur, procédez comme suit :

- Activez une fonction de répondeur sur l'appliance.
- Configurez une action de répondeur. L'action peut être de générer une réponse personnalisée, de rediriger une requête vers une autre page Web ou de réinitialiser une connexion.
- Configurez une stratégie de répondeur. La stratégie détermine les demandes (trafic) sur lesquelles une action doit être effectuée.
- Liez chaque stratégie à un point de liaison mettez-la en vigueur. Un point de liaison fait référence à une entité à partir de laquelle l'appliance Citrix ADC examine le trafic pour voir s'il correspond à une stratégie. Par exemple, un point de liaison peut être un serveur virtuel d'équilibrage de charge.

Vous pouvez spécifier une action par défaut pour les demandes qui ne correspondent à aucune stratégie, et vous pouvez contourner la vérification de sécurité pour les actions qui, autrement, généreraient des messages d'erreur.

La fonctionnalité Réécriture de Citrix ADC aide à réécrire certaines informations dans les demandes ou réponses traitées par Citrix ADC. La section suivante montre quelques différences entre les deux fonctionnalités.

Comparaison entre les options Réécriture et Répondeur

La principale différence entre la fonction de réécriture et la fonction de répondeur est la suivante :

Le répondeur ne peut pas être utilisé pour les expressions de réponse ou basées sur le serveur. Le répondeur ne peut être utilisé que pour les scénarios suivants en fonction des paramètres du client :

- Redirection d'une requête HTTP vers de nouveaux sites Web ou pages Web
- Répondre avec une réponse personnalisée
- Retrait ou réinitialisation d'une connexion au niveau de la demande

S'il existe une stratégie de répondeur, Citrix ADC examine la demande du client, effectue des actions en fonction des stratégies applicables, envoie la réponse au client et ferme la connexion avec le client.

S'il existe une stratégie de réécriture, Citrix ADC examine la demande du client ou la réponse du serveur, prend des mesures en fonction des stratégies applicables et transfère le trafic au client ou au serveur.

En général, il est recommandé d'utiliser un répondeur si vous souhaitez que l'appliance réinitialise ou supporte une connexion en fonction d'un paramètre basé sur une demande. Utilisez un répondeur pour rediriger le trafic ou répondre avec des messages personnalisés. Utilisez la réécriture pour manipuler les données des requêtes et réponses HTTP.

Activation de la fonction Responder

October 5, 2021

Pour utiliser la fonction Répondeur, vous devez d'abord l'activer.

Pour activer la fonctionnalité de répondeur à l'aide de l'interface de ligne de commande Citrix ADC :

À l'invite de commandes, tapez les commandes suivantes pour activer la fonction de répondeur et vérifier la configuration :

- `enable ns feature <feature>`
- `show ns feature`

Exemple :

```
enable ns feature Responder
 Done
> show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   ON
 2)     Surge Protection                SP                   ON
 .
 .
 .
 19)     Responder                       RESPONDER            ON
 20)     Citrix ADC Push                 push                 OFF
 Done
>
<!--NeedCopy-->
```

Pour activer la fonctionnalité de répondeur à l'aide de l'interface graphique :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.

2. Dans le volet d'informations, sous **Modes** et **fonctionnalités**, cliquez sur **Modifier les fonctionnalités avancées**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, activez la case à cocher **Répondeur**, puis cliquez sur **OK**.
4. Dans la ou les **fonctions Activer/Désactiver ?**, cliquez sur **OUI**. Un message apparaît dans la barre d'état indiquant que la fonction a été activée.

Configurer l'action du répondeur

October 5, 2021

Après avoir activé la fonction de répondeur, vous devez configurer une ou plusieurs actions de traitement des demandes. Le répondeur prend en charge les types d'actions suivants :

- **Répondez avec**. Envoie la réponse définie par l'expression Target sans transférer la demande à un serveur Web. (L'appliance Citrix ADC se substitue à un serveur Web et agit en tant que serveur Web.) Utilisez ce type d'action pour définir manuellement une réponse HTML simple. Normalement, le texte d'une action Répondre avec consiste en un code d'erreur de serveur Web et une brève page HTML.
- **Répondez avec SQL OK**. Envoie la réponse SQL OK désignée définie par l'expression Target. Utilisez ce type d'action pour envoyer une réponse SQL OK à une requête SQL.
- **Répondez avec une erreur SQL**. Envoie la réponse d'erreur SQL désignée définie par l'expression Target. Utilisez ce type d'action pour envoyer une réponse d'erreur SQL à une requête SQL.
- **Répondez avec une page HTML**. Envoie la page HTML désignée en tant que réponse. Vous pouvez choisir dans une liste déroulante de pages HTML précédemment chargées ou charger une nouvelle page HTML. Utilisez ce type d'action pour envoyer une page HTML importée en tant que réponse. La solution matérielle-logicielle répond avec un en-tête personnalisé dans l'action Responder responsewithhtmlpage. Vous pouvez configurer jusqu'à huit en-têtes personnalisés.
- **Redirection**. Redirige la demande vers une autre page Web ou un autre serveur Web. Une action de redirection peut rediriger les demandes initialement envoyées vers un site Web « fictif » qui existe dans le DNS, mais pour lequel il n'existe pas de serveur Web réel, vers un site Web réel. Il peut également rediriger les demandes de recherche vers une URL appropriée. Normalement, la cible de redirection d'une action de redirection consiste en une URL complète.

Pour configurer une action de répondeur à l'aide de la ligne de commande Citrix ADC :

Affiche les paramètres actuels de l'action de répondeur spécifiée. Si aucun nom d'action n'est fourni, affichez la liste de toutes les actions de répondeur actuellement configurées sur l'appliance Citrix ADC, avec des paramètres abrégés.

À l'invite de commandes, tapez les commandes suivantes pour configurer une action de répondeur et vérifier la configuration :

- `add responder action <name> <type> <target>`
- `show responder action`

Paramètres :

- **Nom**. Nom de l'action du répondeur. Longueur maximale : 127
- **type**. Type d'action du répondeur. Il peut s'agir de : (répondez avec).
- **cible**. Expression spécifiant les éléments de réponse
- **htmlpage**. Option spécifiant de répondre avec une page HTML
- **hits**. Le nombre de fois où l'action a été effectuée.
- **Nombre de références**. Nombre de références à l'action.
- **UndefHits**. Le nombre de fois où l'action a abouti au FNUD.
- **commentaire**. Tout type d'informations concernant cette action de répondeur.
- **intégré**. Indicateur permettant de déterminer si l'action du répondeur est intégrée ou non

Exemple :

```
To create a responder action that displays a "Not Found" error page for URLs that do not exist:

> add responder action act404Error respondWith '"HTTP/1.1 404 Not Found \r\n\r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."'
Done

> show responder action

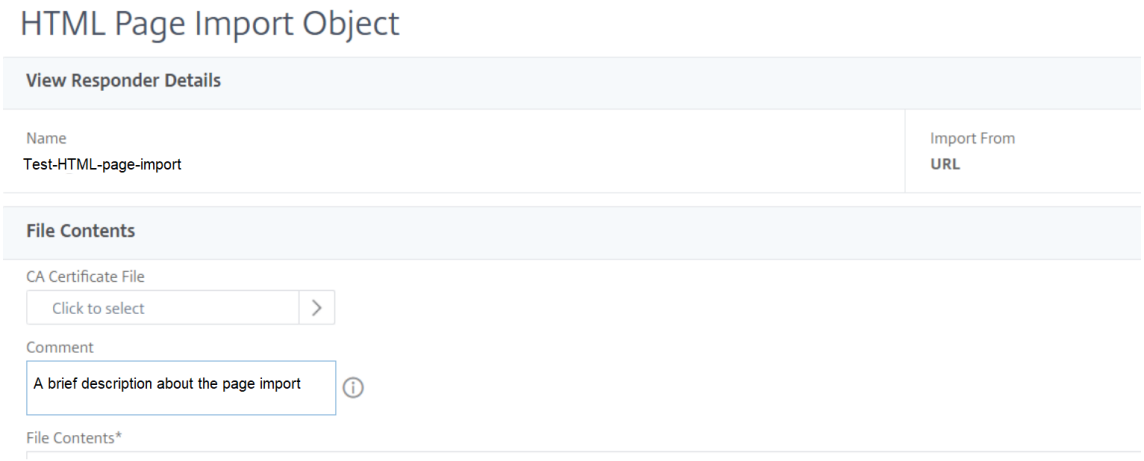
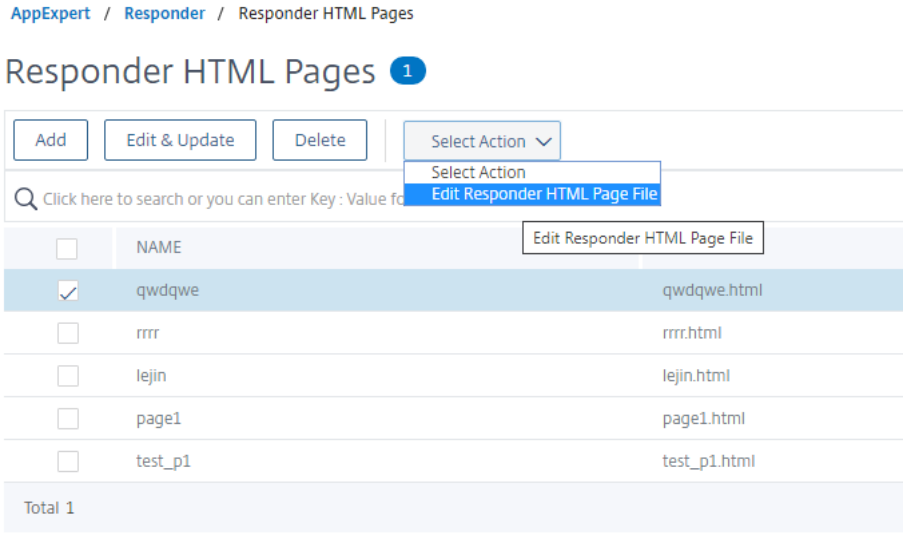
1) Name: act404Error
Operation: respondwith
Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

To create a responder action that displays a "Not Found" error page for URLs that do not exist:

```



```
add responder action act404Error respondWith '"HTTP/1.1 404 Not Found\r\n\r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."'
Done
> show responder action

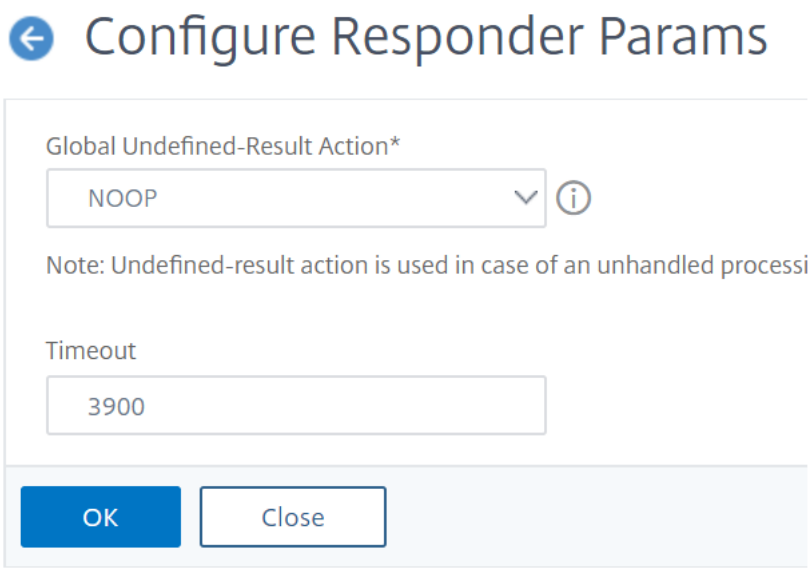
1) Name: act404Error
Operation: respondwith
Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
<!--NeedCopy-->
```

Pour modifier une action de répondeur existante à l'aide de la ligne de commande Citrix ADC :

À l'invite de commandes, tapez la commande suivante pour modifier une action de répondeur existante et vérifier la configuration :

- `set responder action <name> -target <string>`
- `show responder action`

Exemple :

```
set responder action act404Error  -target '"HTTP/1.1 404 Not Found\r\n\r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."'
 Done
> show responder action

1)      Name: act404Error
        Operation: respondwith
        Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."
        Hits: 0
        Undef Hits: 0
        Action Reference Count: 0
 Done
<!--NeedCopy-->
```

Pour supprimer une action de répondeur à l'aide de la ligne de commande Citrix ADC, procédez comme suit :

À l'invite de commandes, tapez la commande suivante pour supprimer une action de répondeur et

vérifier la configuration :

- `rm responder action <name>`
- `show responder action`

Exemple :

```
rm responder action act404Error
 Done

> show responder action
 Done
<!--NeedCopy-->
```

Pour ajouter des en-têtes personnalisés dans l'action responsewithhtmlpage responder à l'aide de la ligne de commande Citrix ADC :

Une appliance Citrix ADC peut désormais répondre avec des en-têtes personnalisés dans l'action répondeur responsewithhtmlpage. Vous pouvez configurer jusqu'à huit en-têtes personnalisés. Auparavant, la solution matérielle-logicielle répondait uniquement avec `Content-type:text/html` des en-têtes `Content-Length:<value>` statiques et.

> **Remarque :**
>
> Dans la configuration d'en-tête personnalisée, vous pouvez également écraser la valeur de l'en-tête « Content-Type ».

À l'invite de commandes, tapez la commande suivante :

```
add responder action <name> <type> (<target> | <htmlpage>)[-comment <string
>] [-responseStatusCode <positive_integer>] [-reasonPhrase <expression>] [-
headers <name(value)> ...]
```

Où,

de l'utilisateur. Nom de l'action du répondeur. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), le hachage (#), l'espace (), à (@), égal (=), deux-points (:) et les caractères de soulignement. Peut être modifié après l'ajout de la stratégie de répondeur.

Tapez. Type d'action du répondeur. Les paramètres disponibles fonctionnent comme suit :

1. respondwith `<target>` - Répond à la demande avec l'expression spécifiée comme cible.
2. respondwithhtmlpage - Répond à la demande avec l'objet de page HTML téléchargé spécifié comme cible.
3. redirect - Redirige la demande vers l'URL spécifiée comme cible.
4. sqlresponse_ok - Envoie une réponse SQL OK.

5. sqlresponse_error - Envoie une réponse SQL ERROR. Il s'agit d'un argument obligatoire. Valeurs possibles : noop, respondwith, redirect, respondwith htmlpage, sqlresponse_ok, sqlresponse_error

Cible. Expression spécifiant les éléments de réponse. En général, une URL pour les stratégies de redirection ou une expression de syntaxe par défaut. Outre les expressions de syntaxe par défaut de Citrix ADC qui font référence aux informations de la demande, une expression stringbuilder peut contenir du texte et du code HTML, ainsi que de simples codes d'échappement qui définissent de nouvelles lignes et paragraphes. Encadrez chaque élément d'expression stringbuilder (une expression de syntaxe par défaut Citrix ADC ou une chaîne) entre guillemets doubles. Utilisez le signe plus (+) pour joindre les éléments.

htmlpage. Pour les stratégies respondwithhtmlpage, nom de l'objet de page HTML à utiliser comme réponse. Vous devez d'abord importer l'objet de page. Longueur maximale : 31

Comment. Tout type d'informations concernant cette action de répondeur. Longueur maximale : 255

Code de statut de réponse. Code d'état de réponse HTTP, par exemple 200, 302, 404, etc. La valeur par défaut pour le type d'action de redirection est 302 et pour respondwithhtmlpage est 200 Valeur minimale : 100 Valeur maximale : 599

Phrase de raison. Expression spécifiant la phrase de motif de la réponse HTTP. La phrase de raison peut être un littéral de chaîne avec des guillemets ou une expression PI. Par exemple : « URL non valide :" + HTTP.REQ.URL Longueur maximale : 8191

en-têtes. Un ou plusieurs en-têtes à insérer dans la réponse HTTP. Chaque en-tête est spécifié sous la forme « name (expr) », où expr est une expression qui est évaluée au moment de l'exécution pour fournir la valeur de l'en-tête nommé. Vous pouvez configurer un maximum de huit en-têtes pour une action de répondeur.

Pour configurer une action de répondeur à l'aide de l'interface graphique :

1. Accédez à **AppExpert > Répondeur > Actions**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une action, cliquez sur **Ajouter**.
   - Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Ouvrir**.
3. Cliquez sur **Créer** ou sur **OK**, selon que vous créez une action ou modifiez une action existante.
4. Cliquez sur **Fermer**. Un message apparaît dans la barre d'état indiquant que la fonction a été activée.
5. Pour supprimer une action de répondeur, sélectionnez-la, puis cliquez sur **Supprimer**. Un message apparaît dans la barre d'état, indiquant que la fonctionnalité a été désactivée.

Pour ajouter une expression à l'aide de la boîte de dialogue **Ajouter une expression**

1. Dans la boîte de dialogue **Créer une action de répondeur** ou **Configurer une action** de répondeur, cliquez sur **Ajouter**.

2. Dans la boîte de dialogue **Ajouter une expression**, dans la première zone de liste, choisissez le premier terme de votre expression.

   - HTTP. Le protocole HTTP. Choisissez cette option si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole HTTP.
   - SYS. Un ou plusieurs sites Web protégés. Sélectionnez cette option si vous souhaitez examiner certains aspects de la demande qui concernent le destinataire de la demande.
   - CLIENT. L'ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'expéditeur de la demande.
   - ANALYTICS. Les données analytiques associées à la demande. Sélectionnez cette option si vous souhaitez examiner les métadonnées de la demande.
   - SIP. Une demande SIP. Choisissez cette option si vous souhaitez examiner certains aspects d'une demande SIP. Lorsque vous faites votre choix, la zone de liste la plus à droite répertorie les termes appropriés pour la partie suivante de votre expression.

3. Dans la deuxième zone de liste, choisissez le deuxième terme de votre expression. Les choix dépendent du choix que vous avez effectué à l'étape précédente et sont adaptés au contexte. Une fois que vous avez fait votre deuxième choix, la fenêtre d'aide située sous la fenêtre Construire une expression (qui était vide) affiche de l'aide décrivant le but et l'utilisation du terme que vous venez de choisir.

4. Continuez à choisir des termes dans les zones de liste qui apparaissent à droite de la zone de liste précédente, ou à taper des chaînes ou des nombres dans les zones de texte qui s'affichent pour vous inviter à entrer une valeur, jusqu'à ce que votre expression soit terminée.

Configuration de l'action HTTP globale

Vous pouvez configurer l'action HTTP globale pour qu'elle invoque une action de répondeur lorsqu'une requête HTTP arrive à son heure d'attente. Pour configurer cette fonctionnalité, vous devez d'abord créer l'action de répondeur que vous souhaitez appeler. Ensuite, vous configurez l'action de délai d'expiration HTTP global pour répondre à un délai d'expiration avec cette action de répondeur.

Pour configurer l'action HTTP globale à l'aide de la ligne de commande Citrix ADC, procédez comme suit :

À l'invite de commandes, tapez la commande suivante :

- `set ns httpProfile -reqTimeoutAction <responder action name>`
- `save ns config`

Par `<responder action name>`, remplacez le nom de l'action du répondeur.

Configurer l'importation de pages HTML

Lorsqu'une appliance Citrix ADC répond par un message personnalisé, nous pouvons répondre avec un fichier HTML. Vous pouvez importer le fichier à l'aide de la commande `import responder htmlpage`, puis utiliser ce fichier dans la commande `add responder action <act name> respondwithhtmlpage <file name>`. Vous pouvez également importer le fichier via l'interface graphique Citrix ADC. Vous pouvez importer la page HTML souhaitée dans le dossier de la solution matérielle-logicielle et la télécharger pendant l'exécution du répondeur.

Importer une page HTML à l'aide de la CLI

À l'invite de commandes, tapez :

```
import responder htmlpage [<src>] <name> [-comment <string>] [-overwrite][-CAcertFile <string>]
```

Exemple :

```
import responder htmlpage http://www.example.com/page.html my-responder-page -CAcertFile my_root_ca_cert
```

Où, le certificat de l'autorité de
certification est utilisé pour vérifier le certificat client. Le certificat doit être importé à l'aide de la commande CLI « import ssl certfile » ou équivalente via l'API ou l'interface graphique. Si le nom du certificat n'est pas configuré, les certificats d'autorité de certification racine par défaut sont utilisés pour la vérification du certificat.

Importer une page HTML à l'aide de l'interface graphique Citrix ADC

1. Accédez à **AppExpert** > **Répondeur** > **Importations de pages HTML**.
2. Dans le volet de détails **Importations HTML du répondeur**, cliquez sur **Ajouter**.
3. Dans la **page Objet d'importation de page HTML**, définissez les paramètres suivants :
    a) Name. Nom de la page HTML.
    b) Importer depuis. Importé à partir d'un fichier, d'un texte ou d'un texte.
    c) URL. Sélectionnez cette option pour entrer l'emplacement URL du fichier HTML.
    d) Dossier. Sélectionnez le fichier HTML dans le répertoire de la solution matérielle-logicielle.
    e) Texte. Sélectionnez le fichier HTML sous forme de texte.
4. Cliquez sur **Continuer**.
5. Vérifiez les détails de la page HTML du répondeur.
6. Cliquez sur **Terminé**.



Pour modifier une page HTML, vous pouvez sélectionner un fichier et cliquer sur **Modifier le fichier de page HTML du répondeur** dans la liste déroulante **Sélectionner une action** .



Configuration d'une stratégie de répondeur

October 5, 2021

Après avoir configuré une action de répondeur, vous devez ensuite configurer une stratégie de répondeur pour sélectionner les demandes auxquelles l'appliance Citrix ADC doit répondre. Une stratégie de répondeur est basée sur une règle, qui consiste en une ou plusieurs expressions. La règle est associée à une action, qui est exécutée si une demande correspond à la règle.

Remarque : Pour la création et la gestion des stratégies de répondeur, l'interface graphique fournit une assistance qui n'est pas disponible à l'invite de commande Citrix ADC.

Pour configurer une stratégie de répondeur à l'aide de la ligne de commande Citrix ADC, procédez comme suit :

À l'invite de commandes, tapez :

- `add responder policy <name> <expression> <action> [<undefaction>]-appFlowaction <actionName>`
- `show responder policy <name>`

Exemple :

```
> add responder policyThree "CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)"
   RESET
 Done
> show responder policyThree

        Name: policyThree
        Rule: CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)
        Responder Action: RESET
        UndefAction: Use Global
        Hits: 0
        Undef Hits: 0
 Done
<!--NeedCopy-->
```

Pour modifier une stratégie de répondeur existante à l'aide de la ligne de commande Citrix ADC :

À l'invite de commandes, tapez :

- `set responder policy <name> [-rule <expression>] [-action <string>] [-undefAction <string>]`
- `show responder policy <name>`

Pour supprimer une stratégie de répondeur à l'aide de la ligne de commande Citrix ADC, procédez comme suit :

À l'invite de commandes, tapez :

- `rm responder policy <name>`
- `show responder policy`

Exemple :

```
>rm responder policy pol404Error
 Done

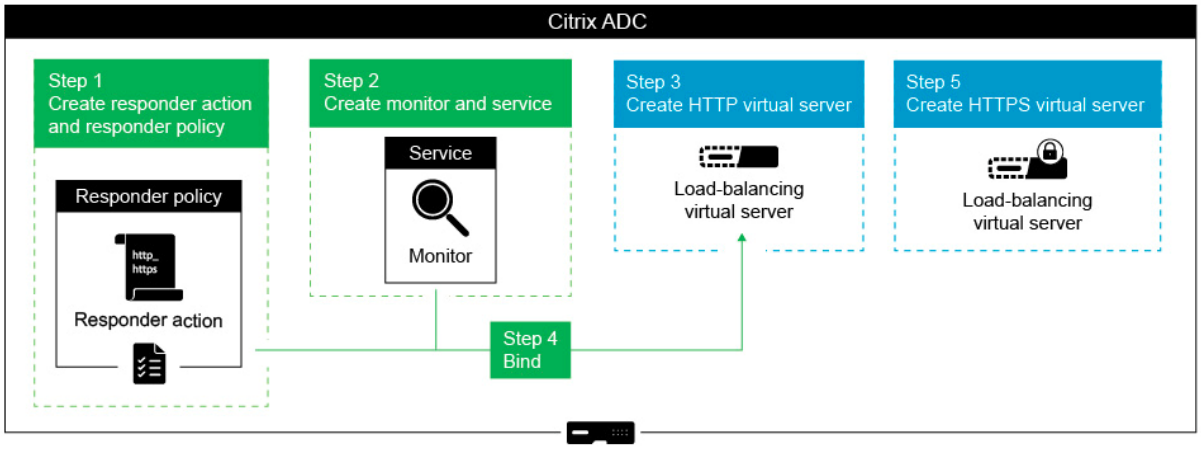
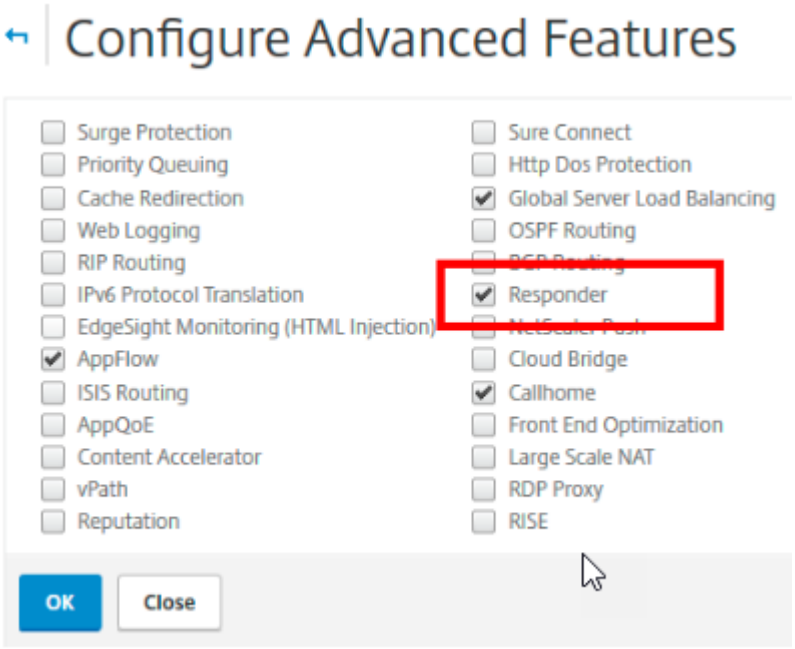
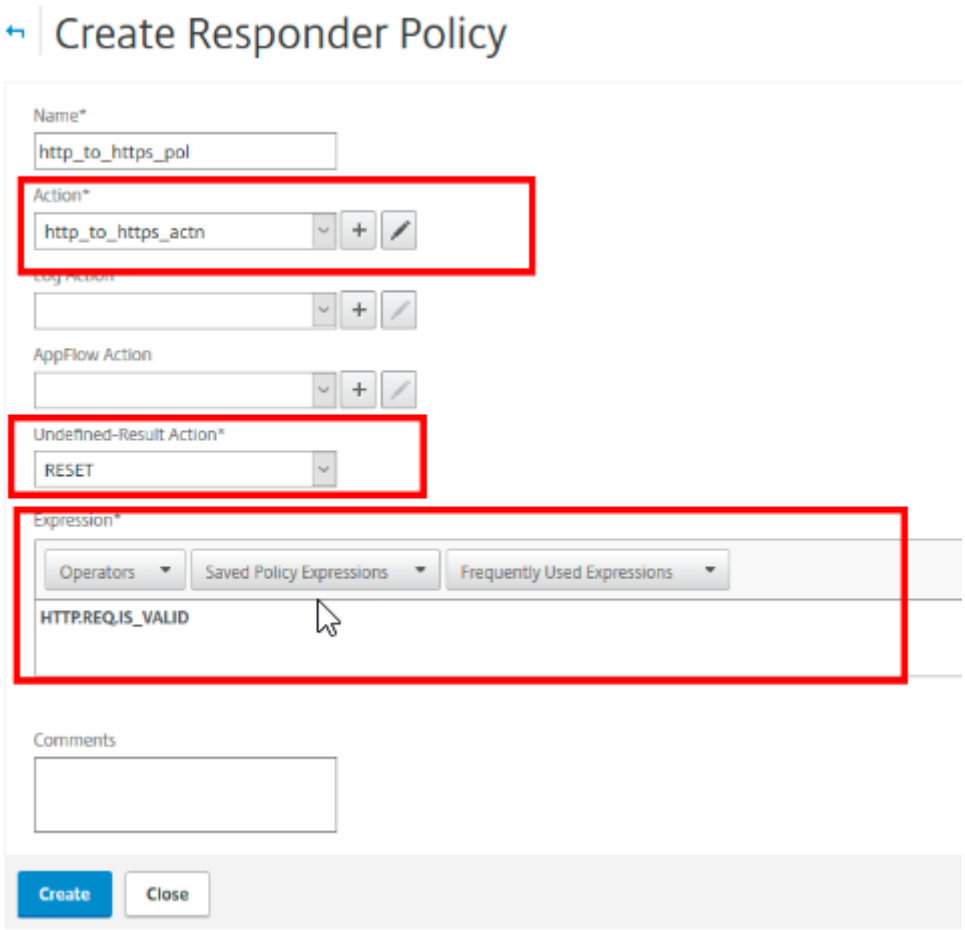
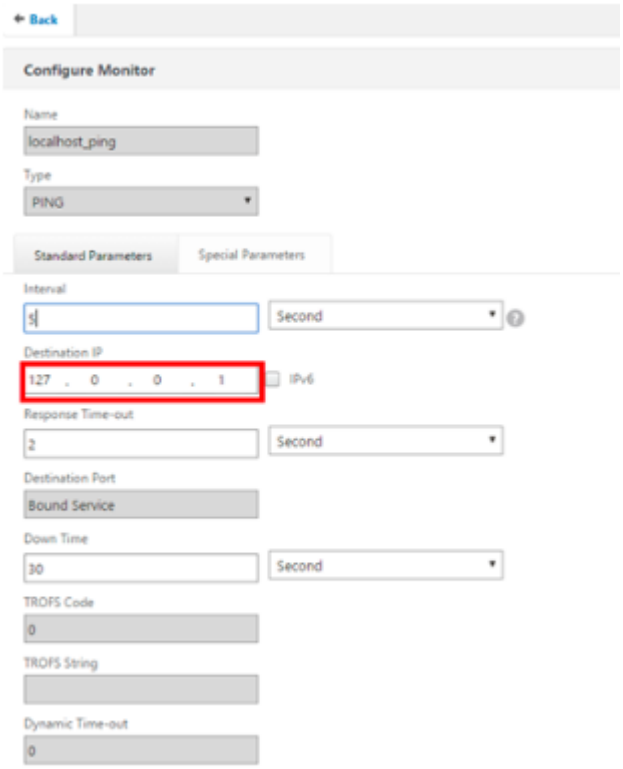
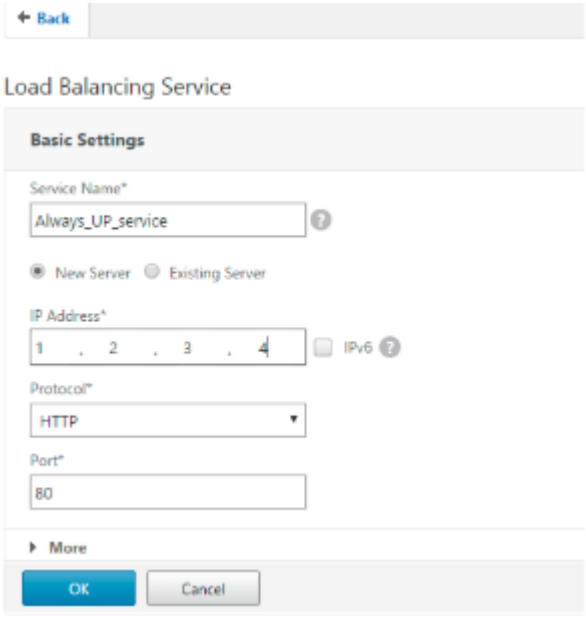
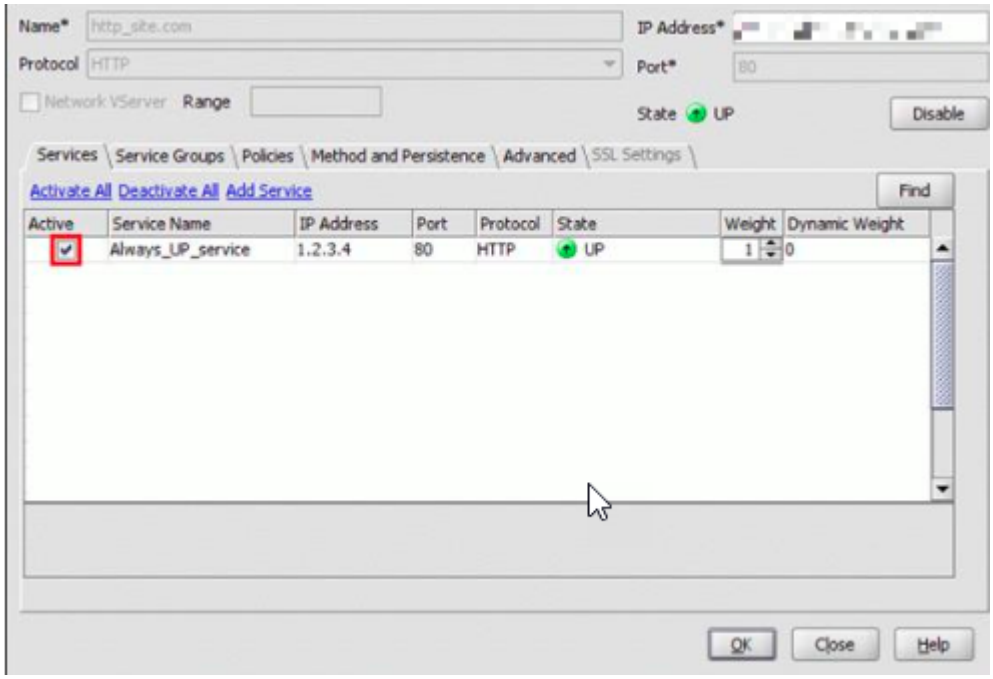
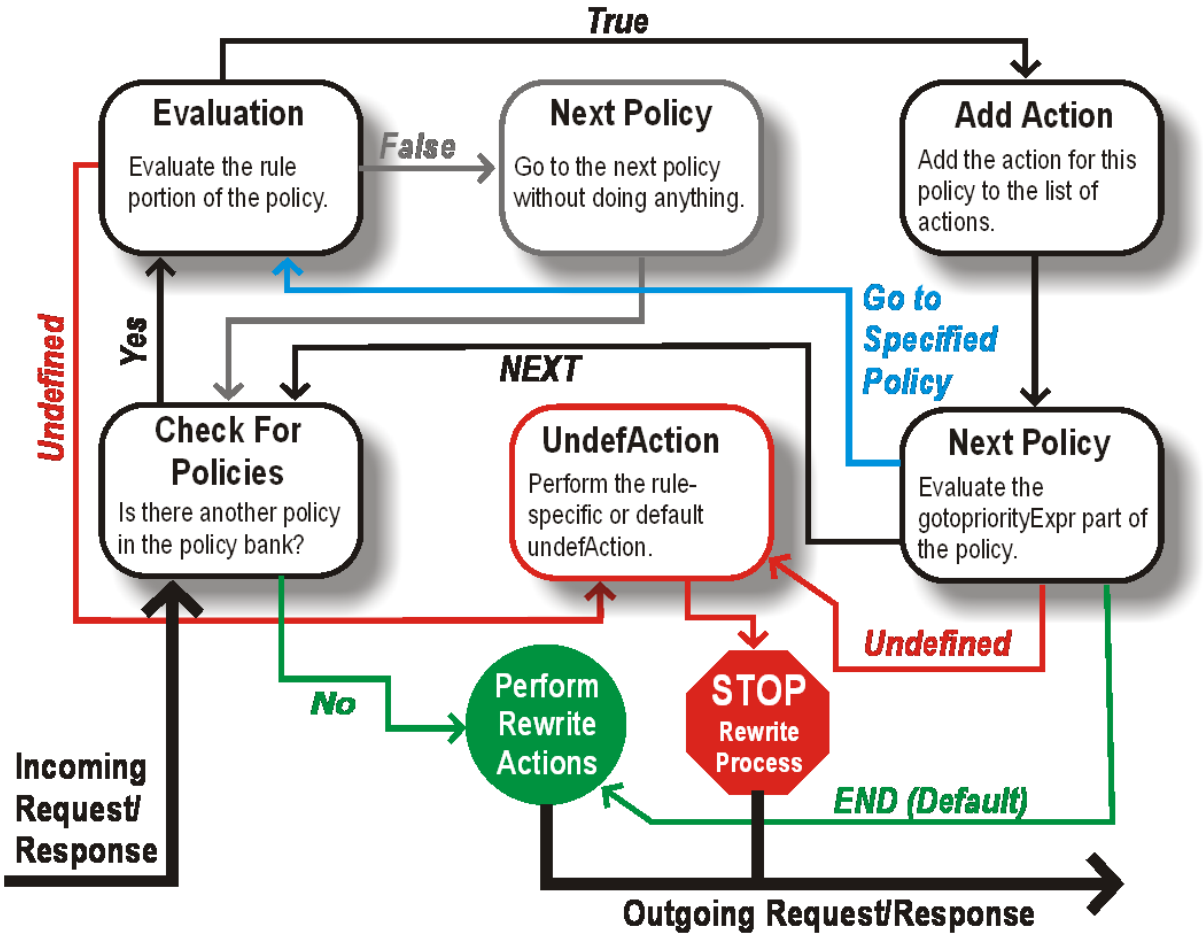
> show responder policy
 Done
```



```
<!--NeedCopy-->
```

Pour configurer une stratégie de répondeur à l'aide de l'interface graphique :

1. Accédez à **AppExpert > Répondeur > Stratégies**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle stratégie, cliquez sur **Ajouter**.
   - Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Ouvrir**.
3. Cliquez sur **Créer** ou sur **OK**, selon que vous créez une nouvelle stratégie ou modifiez une stratégie existante.
4. Cliquez sur **Fermer**. Un message apparaît dans la barre d'état indiquant que la fonction a été configurée.

Liaison d'une stratégie de répondeur

August 20, 2021

Pour mettre une stratégie en vigueur, vous devez la lier soit globalement, de sorte qu'elle s'applique à tout le trafic qui circule via Citrix ADC, soit à un serveur virtuel spécifique, de sorte que la stratégie ne s'applique qu'aux demandes dont l'adresse IP de destination est le VIP de ce serveur virtuel.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel entier positif.

Dans le système d'exploitation Citrix ADC, les priorités de stratégie fonctionnent dans l'ordre inverse : plus le nombre est élevé, plus la priorité est faible. Par exemple, si vous avez trois stratégies avec des priorités de 10, 100 et 1000, la stratégie affectée d'une priorité de 10 est exécutée en premier, puis la stratégie affectée d'une priorité de 100 et enfin la stratégie affectée d'un ordre de 1000. La fonction de répondeur implémente uniquement la première stratégie correspondant à une demande, et non les stratégies supplémentaires qu'elle pourrait également correspondre. Par conséquent, la priorité de stratégie est importante pour obtenir les résultats que vous souhaitez obtenir.

Vous pouvez vous laisser beaucoup de place pour ajouter d'autres stratégies dans n'importe quel ordre, tout en les définissant pour les évaluer dans l'ordre souhaité, en définissant des priorités avec des intervalles de 50 ou 100 entre chaque stratégie lorsque vous la liez globalement. Vous pouvez ensuite ajouter des stratégies supplémentaires à tout moment sans avoir à réaffecter la priorité d'une stratégie existante.

Pour plus d'informations sur les stratégies de liaison sur Citrix ADC, consultez Politiques et expressions.

> **Remarque :**
>
> Les stratégies de répondeur sont liées aux serveurs virtuels basés sur TCP.

Pour lier globalement une stratégie de répondeur à l'aide de la ligne de commande Citrix ADC :

À l'invite de commandes, tapez la commande suivante pour lier globalement une stratégie de répondeur et vérifier la configuration :

- `bind responder global <policyName> <priority> [<gotoPriorityExpression> [-type <type>] [-invoke (<labelType> <labelName>)]`
- `show responder global`

Exemple :

```
> bind responder global poliError 100
 Done
> show responder global
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 1

 Done
<!--NeedCopy-->
```

Pour lier une stratégie de répondeur à un serveur virtuel spécifique à l'aide de la ligne de commande Citrix ADC :

À l'invite de commandes, tapez :

- `bind lb vserver <name> -policyname <policy_name> -priority <priority>`
- `sh lb vserver <name>`

Exemple :

```
> bind lb vserver vs-loadbal -policyName policyTwo -priority 100
 Done
> show lb vserver
1)      vs-loadbal (10.102.29.20:80) - HTTP     Type: ADDRESS
        State: OUT OF SERVICE
        Last state change was at Wed Aug 19 09:05:47 2009 (+211 ms)
        Time since last state change: 2 days, 00:58:03.260
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
```



```
15          Mode: IP
16          Persistence: NONE
17          Vserver IP and Port insertion: OFF
18          Push: DISABLED  Push VServer:
19          Push Multi Clients: NO
20          Push Label Rule: none
21  2)      vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
22          State: DOWN
23          Last state change was at Wed Aug 19 10:03:46 2009 (+213 ms)
24          Time since last state change: 2 days, 00:00:04.260
25          Effective State: DOWN
26          Client Idle Timeout: 9000 sec
27          Down state flush: ENABLED
28          Disable Primary Vserver On Down : DISABLED
29          No. of Bound Services :  0 (Total)       0 (Active)
30          Configured Method: LEASTCONNECTION
31          Mode: IP
32          Persistence: NONE
33          Connection Failover: DISABLED
34   Done
35  <!--NeedCopy-->
```

Pour lier globalement une stratégie de répondeur à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Répondeur** > **Stratégies**.
2. Dans la page **Stratégies de répondeur**, sélectionnez une stratégie de répondeur, puis cliquez sur **Gestionnaire de stratégies** .
3. Dans la boîte de dialogue **Gestionnaire de stratégies de répondeur**, menu Points de liaison, sélectionnez Global par défaut.
4. Cliquez sur **Insérer une stratégie** pour insérer une nouvelle ligne et afficher une liste déroulante de toutes les stratégies de répondeur indépendant.
5. Cliquez sur l'une des stratégies de la liste. Cette stratégie est insérée dans la liste des stratégies de répondeur liées globalement.
6. Cliquez sur **Appliquer les modifications**.
7. Cliquez sur **Fermer**. Un message s'affiche dans la barre d'état indiquant que la configuration a été terminée avec succès.

Pour lier une stratégie de répondeur à un serveur virtuel spécifique à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans la page **Serveurs virtuels d'équilibrage** de charge, sélectionnez le serveur virtuel auquel vous souhaitez lier la stratégie de répondeur, puis cliquez sur **Ouvrir** .
3. Dans la boîte de dialogue **Configurer le serveur virtuel** (équilibrage de charge), sélectionnez l'onglet **Stratégies**, qui affiche la liste de toutes les stratégies configurées sur votre appliance

Citrix ADC.

4. Activez la case à cocher en regard du nom de la stratégie que vous souhaitez lier à ce serveur virtuel.
5. Cliquez sur **OK**. Un message s'affiche dans la barre d'état indiquant que la configuration a été terminée avec succès.

Définition de l'action par défaut pour une stratégie de répondeur

August 20, 2021

L'appliance Citrix ADC génère un événement non défini (événement UNDEF) lorsqu'une demande ne correspond pas à une stratégie de répondeur. L'appliance exécute ensuite l'action par défaut affectée aux événements non définis. Par défaut, l'action transmet la requête à la fonction suivante, telle que l'équilibrage de charge, le filtrage du contenu, etc. Ce comportement par défaut garantit que les demandes ne nécessitent pas d'action spécifique de répondeur à vos serveurs Web. En outre, les clients ont accès au contenu qu'ils ont demandé.

Si un ou plusieurs sites Web que votre appliance Citrix ADC protège reçoivent un nombre important de demandes non valides ou malveillantes, cependant, vous pouvez modifier l'action par défaut pour réinitialiser la connexion client ou supprimer la demande. Dans ce type de configuration, vous devez écrire une ou plusieurs stratégies de répondeur qui correspondraient à toutes les demandes légitimes, et simplement rediriger ces demandes vers leurs destinations d'origine. Votre appliance Citrix ADC bloque ensuite toutes les autres demandes, comme spécifié par l'action par défaut que vous avez configurée.

Vous pouvez affecter l'une des actions suivantes à un événement non défini :

- **NOOP**. L'action NOOP interrompt le traitement du répondeur mais ne modifie pas le flux de paquets. Pour que l'appliance continue de traiter les demandes qui ne correspondent à aucune stratégie de répondeur et les transfère finalement à l'URL demandée, sauf si une autre fonctionnalité intervient et bloque ou redirige la demande. Cette action est appropriée pour les demandes normales adressées à vos serveurs Web et est le paramètre par défaut.
- **RESET**. Si l'action non définie est définie sur RESET, l'appliance réinitialise la connexion client, informant le client qu'elle doit rétablir sa session avec le serveur Web. L'action est appropriée pour les demandes répétées de pages Web qui n'existent pas ou pour les connexions qui peuvent être des tentatives de piratage ou de sonde de vos sites Web protégés.
- **DROP**. Si l'action non définie est définie sur DROP, l'appliance abandonne silencieusement la demande sans répondre au client de quelque manière que ce soit. Cette action est appropriée pour les demandes qui semblent faire partie d'une attaque DDoS ou d'une autre attaque soutenue sur vos serveurs.

Note : Les événements UNDEF ne sont déclenchés que pour les demandes des clients. Aucun événement UNDEF n'est déclenché pour les réponses.

Pour définir l'action non définie à l'aide de la ligne de commande Citrix ADC :

À l'invite de commandes, tapez la commande suivante pour définir l'action non définie et vérifier la configuration :

- `set responder param -undefAction (RESET|DROP|NOOP)[-timeout <msecs>]`
- `show responder param`

Où,

timeout - Durée maximale en millisecondes pour permettre le traitement de toutes les stratégies et de leurs actions sélectionnées sans interruption. Si le délai d'expiration est atteint, l'évaluation entraîne une hausse du UNDEF et aucun traitement ultérieur n'est effectué.

Valeur minimale : 1

Valeur maximale : 5000

Exemple :

```
>set responder param -undefAction RESET -timeout 3900
 Done
> show responder param
Action Name: RESET
Timeout: 3900
 Done
>
<!--NeedCopy-->
```

Définir l'action indéfinie à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Répondeur**, puis sous **Paramètres**, cliquez sur le lien **Modifier les paramètres du répondeur** .
2. Dans la page **Définir les paramètres de répondeur**, définissez les paramètres suivants :
   a) Action globale de résultat indéfini. L'action de résultat non défini est préférée dans une exception de traitement non gérée dans les stratégies et actions du répondeur. Sélectionnez **NOOP**, **RESET**ou **DROP**.
   b) Délai d'expiration. Durée maximale en millisecondes pour permettre le traitement sans interruption de toutes les stratégies et leurs actions sélectionnées. Si le délai d'expiration est atteint, l'évaluation entraîne une hausse du UNDEF et aucun traitement ultérieur n'est effectué.
3. Cliquez sur **OK**.



Exemples d'actions et de stratégies d'intervenants

August 20, 2021

Les actions et les stratégies du répondeur sont puissantes et complexes, mais vous pouvez commencer avec des applications relativement simples.

Exemple : Blocage de l'accès à partir d'adresses IP spécifiées

Les procédures suivantes bloquent l'accès à vos sites Web protégés par les clients provenant du CIDR 222.222.0.0/16. Le répondeur envoie un message d'erreur indiquant que le client n'est pas autorisé à accéder à l'URL demandée.

Pour bloquer l'accès à l'aide de la ligne de commande Citrix ADC :

À l'invite de commandes, tapez les commandes suivantes pour bloquer l'accès :

- add responder action act_unauthorized respond with "HTTP/1.1 403 Forbidden\r\n\r\n" + "Client: " + CLIENT.IP.SRC + " is not authorized to access URL:" + "HTTP.REQ.URL.HTTP_URL_SAFE"'
- add responder policy pol_un "CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)" act_unauthorized
- bind responder global pol_un 10

Pour bloquer l'accès à l'aide de l'interface graphique :

1. Dans le volet de navigation, développez **Répondeur**, puis cliquez sur **Actions**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action du répondeur**, procédez comme suit :

a) Dans la zone de texte **Nom**, tapez act_unauthorized.
b) Sous Type, sélectionnez Répondre avec.
c) Dans la zone de texte cible, tapez la chaîne suivante : “HTTP/1.1 200 OK\r\n\r\n” + “Client: “ + CLIENT.IP.SRC + “ is not authorized to access URL:” + HTTP.REQ.URL.HTTP_URL_SAFE
d) Cliquez sur **Créer**, puis sur **Fermer**.
L’action du répondeur que vous avez configurée, nommée act_unauthorized, apparaît désormais dans la page **Actions du répondeur** .

4. Dans le volet de navigation, cliquez sur **Stratégies**.
5. Dans le volet d’informations, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Créer une stratégie de répondeur**, procédez comme suit :
a) Dans la zone de texte Nom, tapez pol_unauthorized.
b) Sous **Action**, sélectionnez act_unauthorized.
c) Dans la fenêtre **Expression**, tapez la règle suivante : CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)
d) Cliquez sur **Créer**, puis sur **Fermer**.
La stratégie de répondeur que vous avez configurée, nommée pol_unauthorized, apparaît désormais dans la page **Stratégies de répondeur** .
7. Liez globalement votre nouvelle stratégie, pol_unauthorized, comme décrit dans Liaison d’une stratégie de répondeur.

Exemple : Redirection d’un client vers une nouvelle URL

Les procédures suivantes redirigent les clients qui accèdent à vos sites Web protégés depuis le CIDR 222.222.0.0/16 vers une URL spécifiée.

Pour rediriger des clients à l’aide de la ligne de commande Citrix ADC :

À l’invite de commandes, tapez les commandes suivantes pour rediriger les clients et vérifier la configuration :

- ajouter l’action du répondeur act_redirect redirection"<http://www.example.com/404.html>"
- Afficher l’action du répondeur act_redirect
- add responder policy pol_redirect “CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)” act_redirect
- show responder policy pol_redirect
- bind responder global pol_redirect 10

Exemple :

```
1 > add responder action act_redirect redirect `" http ://www.example.com
    /404.html "`
2 Done
3
```



```
4 > add responder policy pol_redirect "CLIENT.IP.SRC.IN_SUBNET
     (222.222.0.0/16)" act_redirect
5 Done
6 <!--NeedCopy-->
```

Pour rediriger les clients à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Répondeur** > **Actions**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action du répondeur**, procédez comme suit :
   a) Dans la zone de texte **Nom**, tapez act_redirect.
   b) Sous Type, sélectionnez **Rediriger**.
   c) Dans la zone de texte **Cible**, tapez la chaîne suivante : `"<http://www.example.com/404.html>"`
   d) Cliquez sur **Créer**, puis sur **Fermer**.
   L'action du répondeur que vous avez configurée, nommée act_redirect, apparaît désormais dans la page **Actions du répondeur** .
4. Dans le volet de navigation, cliquez sur **Stratégies**.
5. Dans le volet d'informations, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Créer une stratégie de répondeur**, procédez comme suit :
   a) Dans la zone de texte **Nom**, tapez pol_redirect.
   b) Sous **Action**, sélectionnez act_redirect.
   c) Dans la fenêtre **Expression**, tapez la règle suivante : CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)
   d) Cliquez sur **Créer**, puis sur **Fermer**.
   La stratégie de répondeur que vous avez configurée, nommée pol_redirect, apparaît désormais dans la page **Stratégies de répondeur** .
7. Liez globalement votre nouvelle stratégie, pol_redirect, comme décrit dans Liaison d'une stratégie de répondeur.

Prise en charge de Diameter pour répondeur

August 20, 2021

La fonction Répondeur prend désormais en charge le protocole Diameter. Vous pouvez configurer Responder pour répondre aux requêtes Diameter comme il le fait les requêtes HTTP et TCP. Par exemple, vous pouvez configurer Responder pour répondre aux demandes provenant d'une origine Diameter spécifique avec une redirection vers une page Web améliorée pour les appareils mobiles. Un certain nombre d'expressions Citrix ADC ont été ajoutées qui prennent en charge l'examen de l'en-tête Diameter et des paires attribute-valeur (AVP). Ces expressions prennent en charge la recherche de AVP spécifiques par index, ID ou nom, examinent les informations dans chaque AVP et envoient une réponse

appropriée.

Pour configurer Répondeur pour qu'il réponde à une demande de Diameter :

À l'invite de commandes, tapez les commandes suivantes :

- `add responder action <actname> RESPONDWITH "DIAMETER.NEW_REDIRECT(\"aaa://host.example.com\")"`

  Pour <actname>, remplacez un nom pour votre nouvelle action. Le nom peut se composer d'un à 127 caractères, et peut contenir des lettres, des chiffres et des tirets (-) et des traits de soulignement (_). Pour,aaa://host.example.com remplacez l'URL de l'hôte de Diameter vers lequel vous souhaitez rediriger les connexions.

- add responder policy <polname> "diameter.req.avp(264).value.eq("host1.example.net")" <actname>

  Pour <polname>, remplacez un nom pour votre nouvelle stratégie. Comme c'est le cas< actname>, le nom peut comporter entre un et 127 caractères, et peut contenir des lettres, des chiffres et des tirets (-) et des traits de soulignement (_). Pour host1.example.net, remplacez le nom de l'hôte d'origine des requêtes que vous souhaitez rediriger. Pour <actname>, remplacez le nom de l'action que vous venez de créer.

- `bind lb vserver <vservername> -policyName <polname> -priority <priority> -type REQUEST`

  Pour,<vservername> remplacez le nom du serveur virtuel d'équilibrage de charge auquel vous souhaitez lier la stratégie. Pour,<polname> remplacez le nom de la stratégie que vous venez de créer. Pour,<priority> substituez une priorité à la stratégie.

Exemple :

Pour créer une action et une stratégie Répondeur pour répondre aux demandes de Diameter provenant de « host1.example.net » avec une redirection vers « host.example.com », vous pouvez ajouter l'action et la stratégie suivantes et lier la stratégie comme indiqué.

```
1 > add responder action act_resp-dm-redirect RESPONDWITH "DIAMETER.
     NEW_REDIRECT("aaa://host.example.com")"
2 Done
3
4 > add responder pol_resp-dm-redirect "diameter.req.avp(264).value.eq("
     host1.example.net")" act_resp-dm-redirect
5 Done
6
7 > bind lb vserver vs1 -policyName pol_resp-dm-redirect -priority 10 -
     type REQUEST
8 Done
9 <!--NeedCopy-->
```


Prise en charge de RADIUS pour le répondeur

August 20, 2021

Le langage des expressions Citrix ADC contient des expressions qui peuvent extraire des informations des requêtes RADIUS et les manipuler. Ces expressions vous permettent d'utiliser la fonction Responder pour répondre aux demandes RADIUS. Vos stratégies et actions de répondeur peuvent utiliser n'importe quelle expression appropriée ou pertinente à une requête RADIUS. Les expressions disponibles vous permettent d'identifier le type de message RADIUS, d'extraire toute paire attribute-valeur (AVP) de la connexion et d'envoyer différentes réponses sur la base de ces informations. Vous pouvez également créer des étiquettes de stratégie qui appellent toutes les stratégies de répondeur pour les connexions RADIUS.

Vous pouvez utiliser les expressions RADIUS pour créer des réponses simples qui ne nécessitent pas de communication avec le serveur RADIUS auquel la demande a été envoyée. Lorsqu'une stratégie de répondeur correspond à une connexion, Citrix ADC construit et envoie la réponse RADIUS appropriée sans contacter le serveur d'authentification RADIUS. Par exemple, si l'adresse IP source d'une requête RADIUS provient d'un sous-réseau spécifié dans la stratégie de répondeur, Citrix ADC peut répondre à cette demande avec un message de rejet d'accès ou peut simplement supprimer la demande.

Vous pouvez également créer des étiquettes de stratégie pour acheminer des types spécifiques de demandes RADIUS via une série de stratégies appropriées à ces demandes.

Remarque : Les expressions RADIUS actuelles ne fonctionnent pas avec les attributs RADIUS IPv6.

La documentation Citrix ADC pour les expressions prenant en charge RADIUS suppose une familiarité avec la structure de base et le but des communications RADIUS. Si vous avez besoin de plus d'informations sur RADIUS, consultez la documentation de votre serveur RADIUS ou recherchez en ligne une introduction au protocole RADIUS.

Configuration des stratégies de répondeur pour RADIUS

La procédure suivante utilise la ligne de commande Citrix ADC pour configurer une action et une stratégie de répondeur et lier la stratégie à un point de liaison global spécifique à RADIUS.

Pour configurer une action et une stratégie de répondeur et lier la stratégie :

À l'invite de commandes, tapez les commandes suivantes :

- `add responder action <actName> <actType>`
- `add responder policy <polName> <rule> <actName>`
- `bind responder policy <polName> <priority> <nextExpr> -type <bindPoint>` où`<bindPoint>` représente l'un des points de liaison globaux spécifiques à Radius.

Expressions RADIUS pour le répondeur

Dans une configuration de répondeur, vous pouvez utiliser les expressions Citrix ADC suivantes pour faire référence à diverses parties d'une requête RADIUS.

Identification du type de connexion :

- RADIUS.IS_CLIENT. Renvoie TRUE si la connexion est un message client RADIUS (demande).
- RADIUS.IS_SERVER. Renvoie TRUE si la connexion est un message de réponse du serveur RADIUS.

Expressions de requête :

- `RADIUS.REQ.CODE`. Renvoie le nombre correspondant au type de requête RADIUS. Un dérivé de la classe num_at. Par exemple, une demande d'accès RADIUS renvoie 1 (un). Une demande de comptabilité RADIUS retournerait 4.
- `RADIUS.REQ.LENGTH`. Renvoie la longueur de la requête RADIUS, y compris l'en-tête. Un dérivé de la classe num_at.
- `RADIUS.REQ.IDENTIFIER`. Renvoie l'identificateur de demande RADIUS, un numéro attribué à chaque demande qui permet de faire correspondre la demande à la réponse correspondante. Un dérivé de la classe num_at.
- `RADIUS.REQ.AVP(<AVP Code No>).VALUE`. Renvoie la valeur de la première occurrence de cet AVP sous la forme d'une chaîne de type text_t.
- `RADIUS.REQ.AVP(<AVP code no>).INSTANCE(instance number)`. Renvoie l'instance spécifiée de l'AVP sous la forme d'une chaîne de type RAVP_t. Un AVP RADIUS spécifique peut se produire plusieurs fois dans un message RADIUS. INSTANCE (0) renvoie la première instance, INSTANCE (1) renvoie la deuxième instance, et ainsi de suite, jusqu'à seize instances.
- `RADIUS.REQ.AVP(<AVP code no>).VALUE(instance number)`. Renvoie la valeur de l'instance spécifiée de l'AVP sous la forme d'une chaîne de type text_t.
- `RADIUS.REQ.AVP(<AVP code no>).COUNT`. Renvoie le nombre d'instances d'un AVP spécifique dans une connexion RADIUS, sous forme d'entier.
- `RADIUS.REQ.AVP(<AVP code no>).EXISTS`. Renvoie TRUE si le type d'AVP spécifié existe dans le message, ou FALSE si ce n'est pas le cas.

Expressions de réponse :

Les expressions de réponse RADIUS sont identiques aux expressions de demande RADIUS, sauf que RES remplace REQ.

Typecasts des valeurs AVP :

L'ADC prend en charge les expressions permettant de taper les valeurs AVP RADIUS dans les types de données texte, entier, entier non signé, long, adresse ipv4, adresse ipv6, préfixe ipv6 et heure. La syntaxe est la même que pour les autres expressions de typecast Citrix ADC.

Exemple :

L'ADC prend en charge les expressions permettant de taper les valeurs AVP RADIUS dans les types de données texte, entier, entier non signé, long, adresse ipv4, adresse ipv6, préfixe ipv6 et heure. La syntaxe est la même que pour les autres expressions de typecast Citrix ADC.

```
RADIUS.REQ.AVP(8).VALUE(0).typecast_ip_address_at
<!--NeedCopy-->
```

Expressions de type AVP :

Citrix ADC prend en charge les expressions pour extraire les valeurs RADIUS AVP à l'aide des codes entiers assignés décrits dans RFC2865 et RFC2866. Vous pouvez également utiliser des alias de texte pour accomplir la même tâche. Voici quelques exemples.

- RADIUS.REQ.AVP (1).VALUE or RADIUS.REQ.USERNAME.value. Extrait la valeur du nom d'utilisateur RADIUS.
- RADIUS.REQ.AVP (4). VALUE ou RADIUS.REQ. ACCT_SESSION_ID.value. Extrait Acct-Session-ID AVP (code 44) du message.
- RADIUS.REQ.AVP (26). VALUE ou RADIUS.REQ.VENDOR_SPECIFIC.VALUE. Extrait la valeur spécifique au fournisseur.

Les valeurs des AVP RADIUS les plus couramment utilisés peuvent être extraites de la même manière.

Points de liaison RADIUS :

Quatre points de liaison globaux sont disponibles pour les stratégies qui contiennent des expressions RADIUS.

- RADIUS_REQ_OVERRIDE. Priorité/Remplacer la file d'attente de stratégie de demande.
- RADIUS_REQ_DEFAULT. File d'attente de stratégie de demande standard.
- RADIUS_RES_OVERRIDE. Priorité/Remplacer la file d'attente de stratégie de réponse.
- RADIUS_RES_DEFAULT. File d'attente de stratégie de réponse standard.

Expressions spécifiques au répondeur RADIUS :

- RADIUS_RESPONDWITH. Répondez avec la réponse RADIUS spécifiée. La réponse est créée avec les expressions Citrix ADC, à la fois les expressions RADIUS et toutes les autres expressions applicables.
- RADIUS.NEW_ANSWER. Envoie une nouvelle réponse RADIUS à l'utilisateur.
- RADIUS.NEW_ACCESSREJECT. Rejette la demande RADIUS.
- RADIUS.NEW_AVP. Ajoute le nouvel AVP spécifié à la réponse.

Cas d'utilisation

Voici des cas d'utilisation pour RADIUS avec répondeur.

Blocage des demandes RADIUS à partir d'un réseau spécifique

Pour configurer la fonctionnalité de répondeur pour bloquer les demandes d'authentification à partir d'un réseau spécifique, commencez par créer une action de répondeur qui rejette les demandes. Utilisez l'action d'une stratégie qui sélectionne les demandes des réseaux que vous souhaitez bloquer. Liez la stratégie de répondeur à un point de liaison global spécifique à RADIUS, en spécifiant :

- La priorité
- END comme valeur NextExpr, pour s'assurer que l'évaluation de la stratégie s'arrête lorsque cette stratégie est appariée
- RADIUS_REQ_OVERRIDE en tant que file d'attente à laquelle vous affectez la stratégie, de sorte qu'elle soit évaluée avant que les stratégies ne soient affectées à la file d'attente par défaut

Pour configurer Répondeur pour bloquer les ouvertures de session à partir d'un réseau spécifique**

- `add responder action <actName> <actType>`
- `add responder policy <polName> <rule> <actName>`
- `bind responder global <polName> <priority> <nextExpr> -type <bindPoint>`

Exemple :

```
1 > add responder action rspActRadiusReject respondwith radius.
     new_accessreject
2 Done
3
4 > add responder policy rspPolRadiusReject client.ip.src.in_subnet
     (10.224.85.0/24) rspActRadiusReject
5 Done
6
7 > bind responder global rspPolRadiusReject 1 END -type
     RADIUS_REQ_OVERRIDE
8 <!--NeedCopy-->
```

Prise en charge DNS de la fonction de répondeur

January 21, 2021

Vous pouvez configurer la fonctionnalité de répondeur pour répondre aux demandes DNS comme aux requêtes HTTP et TCP. Par exemple, vous pouvez le configurer pour envoyer des réponses DNS via UDP et vous assurer que les demandes DNS du client sont envoyées via TCP. Un certain nombre d'expressions Citrix ADC prennent en charge l'examen de l'en-tête DNS dans la requête. Ces expressions examinent des champs d'en-tête spécifiques et envoient une réponse appropriée.

- **Expressions DNS**. Dans une configuration de répondeur, vous pouvez utiliser les expressions Citrix ADC suivantes pour faire référence à diverses parties d'une requête DNS :

Expressions	Description
DNS.NEW_RESPONSE	Crée une nouvelle réponse DNS vide en fonction de la demande.
DNS.NEW_RESPONSE <AA, TC, rcode>	Crée une nouvelle réponse DNS basée sur les paramètres spécifiés.

- **Points de liaison DNS**. Les points de liaison globaux suivants sont disponibles pour les stratégies qui contiennent des expressions DNS.

Points de liaison	Description
DNS_REQ_OVERRIDE	Priorité/Remplacer la file d'attente de stratégie de demande.
DNS_REQ_DEFAULT	File d'attente de stratégie de demande standard.

  En plus des points de liaison par défaut, vous pouvez créer des étiquettes de stratégie de type DNS et y lier des stratégies DNS.

Configuration des stratégies de répondeur pour DNS

La procédure suivante utilise la ligne de commande Citrix ADC pour configurer une action et une stratégie de répondeur et lier la stratégie à un point de liaison global spécifique au répondeur.

Pour configurer Répondeur pour répondre à une demande DNS :

À l'invite de commandes, tapez les commandes suivantes :

1. `add responder action <actName> <actType>`

   Pour <actname>, remplacez un nom pour votre nouvelle action. Le nom peut contenir de 1 à 127 caractères et peut contenir des lettres, des chiffres, des tirets (-) et des traits de soulignement (_). Pour <actType>, remplacez un type d'action répondant, *RespondWith*.

2. `add responder policy <polName> <rule> <actName>`

   Pour <polname>, remplacez un nom pour votre nouvelle stratégie. Pour <actname>, le nom peut contenir de 1 à 127 caractères et peut contenir des lettres, des chiffres, des tirets (-) et des

traits de soulignement (_). Pour <actname>, remplacez le nom de l'action que vous venez de créer.

3. bind responder policy <polName> <priority> <nextExpr> -type <bindPoint>

   Pour <bindPoint>, spécifiez l'un des points de liaison globaux spécifiques du répondeur. Pour <polName>, remplacez le nom de la stratégie que vous venez de créer. Pour <priority>, spécifiez la priorité de la stratégie.

Exemple de configuration - Appliquer toutes les requêtes DNS sur TCP :

Pour appliquer toutes les requêtes DNS sur TCP, créez une action de répondeur qui définira le bit TC et rcode comme NOERROR.

```
1 > add responder action resp_act_set_tc_bit respondwith DNS.NEW_RESPONSE
     (true, true, NOERROR)
2 Done
3
4 > add responder policy enforce_tcp  dns.REQ.TRANSPORT.EQ(udp)
     resp_act_set_tc_bit
5 Done
6
7 >bind lb vserver dns_udp  - policyName  enforce_tcp   -type request  -
     priority 100
8 Done
9 <!--NeedCopy-->
```

Prise en charge de MQTT pour le répondeur

August 20, 2021

La fonctionnalité Répondeur prend en charge le protocole MQTT. Vous pouvez configurer les stratégies de répondeur pour qu'elles prennent une action basée sur les paramètres du message MQTT entrant.

L'action répond avec l'un des éléments suivants à une nouvelle connexion :

- DROP
- RESET
- NOOP
- Une action de l'intervenant pour lancer une nouvelle réponse MQTT CONNACK.

Configuration des stratégies de répondeur pour MQTT

Après avoir activé la fonctionnalité de répondeur, vous devez configurer une ou plusieurs actions pour gérer les demandes MQTT. Ensuite, configurez une stratégie de répondeur. Vous pouvez lier les stratégies de répondeur globalement, ou à un serveur virtuel d'équilibrage de charge spécifique ou à un serveur virtuel de commutation de contenu spécifique.

Les points de liaison suivants sont disponibles pour lier les stratégies de répondeur globalement :

- MQTT_REQ_DEFAULT
- MQTT_REQ_OVERRIDE
- MQTT_JUMBO_REQ_DEFAULT
- MQTT_JUMBO_REQ_OVERRIDE

Les points de liaison suivants sont disponibles pour lier les stratégies de répondeur à un serveur virtuel de commutation de contenu ou d'équilibrage de charge :

- REQUEST
- MQTT_JUMBO_REQ (ce point de liaison est utilisé uniquement pour les paquets Jumbo)

Pour configurer le répondeur pour répondre à une requête MQTT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

Configurez une action de répondeur.

```
add responder action <actName> <actType>
<!--NeedCopy-->
```

- Pour `actname`, remplacez un nom pour votre nouvelle action. Le nom peut contenir de 1 à 127 caractères et peut contenir des lettres, des chiffres, des tirets (-) et des symboles de trait de soulignement (_).
- Pour `actType`, substituer un type d'action de répondeur, respondwith.

Exemple :

```
add responder action mqtt_connack_unsup_ver respondwith MQTT.
   NEW_CONNACK(132)
<!--NeedCopy-->
```

Configurez une stratégie de répondeur. L'appliance Citrix ADC répond aux demandes MQTT sélectionnées par cette stratégie de répondeur.

```
add responder policy <polName> <rule> <actname>
<!--NeedCopy-->
```


- Pour `polname`, remplacez un nom pour votre nouvelle stratégie.
- Pour `actname`, remplacez le nom de l'action que vous avez créée.

Exemple :

```
add responder policy reject_lower_version "MQTT.HEADER.COMMAND.EQ(
    CONNECT) && MQTT.VERSION.LT(3)" mqtt_connack_unsup_ver
<!--NeedCopy-->
```

Liez la stratégie de répondeur à un serveur virtuel d'équilibrage de charge spécifique ou à un serveur virtuel de commutation de contenu spécifique. La stratégie s'applique uniquement aux requêtes MQTT dont l'adresse IP de destination est la VIP de ce serveur virtuel.

```
bind lb vserver <name> -policyName <policy_name> -priority <priority>

bind cs vserver <name> -policyName <policy_name> -priority <priority>
<!--NeedCopy-->
```

- Pour `policy_name`, remplacez le nom de la stratégie que vous avez créée.
- Pour `priority`, spécifiez la priorité de la stratégie.

Exemple :

```
bind lb vserver lb1 -policyName reject_lower_version -priority 50

bind cs vserver mqtt_frontend_cs -policyName reject_lower_version -
    priority 5
<!--NeedCopy-->
```

Cas d'utilisation 1 : filtrer les clients en fonction du nom d'utilisateur ou de l'ID client

L'administrateur peut configurer une stratégie de répondeur MQTT pour rejeter la connexion en fonction du nom d'utilisateur ou de l'ID client dans le message MQTT CONNECT.

Exemple de configuration pour filtrer les clients en fonction de l'ID client

```
add policy patset filter_clients
bind policy patset filter_clients client1

add responder action mqtt_connack_invalid_client respondwith MQTT.
    NEW_CONNACK(2)

```



```
6 add responder policy reject_clients "MQTT.HEADER.COMMAND.EQ(CONNECT) &&
      mqtt.connect.clientid.equals_any("filter_clients")"
     mqtt_connack_invalid_client
7
8 bind cs vserver mqtt_frontend_cs -policyName reject_clients -priority 5
9 <!--NeedCopy-->
```

Cas d'utilisation 2 : Limiter la longueur maximale des messages MQTT pour gérer les paquets jumbo

L'administrateur peut configurer une stratégie de répondeur MQTT pour supprimer la connexion client si la longueur du message dépasse un certain seuil, ou prendre les mesures nécessaires en fonction de l'exigence.

Pour gérer les paquets jumbo, les stratégies de répondeur avec l'un des modèles de règles suivants sont liées au point de liaison jumbo :

- MQTT.MESSAGE_LENGTH
- MQTT.COMMAND
- MQTT.FROM_CLIENT
- MQTT.FROM_SERVER

Les stratégies liées aux points de liaison jumbo sont évaluées uniquement pour les paquets jumbo.

Exemple de configuration pour limiter la longueur maximale des messages MQTT

```
1 set lb parameter -dropmqttjumbomessage no
2
3 add responder policy drop_large_message MQTT.MESSAGE_LENGTH.GT(100000)
     reset
4
5 bind cs vserver mqtt_frontend_cs -policyName drop_large_message -
     priority 10
6 <!--NeedCopy-->
```

Dans cet exemple, le `dropmqttjumbomessage` paramètre est défini sur NO. Par conséquent, l'appliance ADC traite les messages dont la longueur est supérieure à 64 000 octets et inférieure à 100 000 octets. Les messages d'une longueur supérieure à 100 000 octets sont réinitialisés.

Comment rediriger une requête HTTP vers HTTPS en utilisant le répondeur

August 20, 2021

Cet article explique comment configurer la fonctionnalité de répondeur avec un équilibrage de charge adresses IP de serveur virtuel et rediriger les requêtes client de HTTP vers HTTPS.

Considérez un scénario dans lequel un utilisateur peut tenter d'accéder à un site Web sécurisé en envoyant une requête HTTP. Au lieu de supprimer la demande, vous pouvez rediriger la demande vers un site Web sécurisé. Vous pouvez utiliser la fonctionnalité de répondeur pour rediriger la demande vers le site Web sécurisé sans modifier le chemin d'accès et la requête URL auxquelles l'utilisateur tente d'accéder.

Comment le répondeur Citrix ADC redirige une requête de HTTP vers HTTPS

L'illustration suivante présente un flux étape par étape de la manière dont l'appliance redirige une demande.



> **Remarque** : Les chemins de navigation et les captures d'écran sont dérivés de NetScaler 11.0.

Pour configurer la fonctionnalité Répondeur ainsi que les adresses VIP d'équilibrage de charge d'une appliance NetScaler afin de rediriger les demandes client du HTTP vers HTTPS, procédez comme suit.

1. Activez la fonction de répondeur sur l'appliance. Accédez à **Système** > **Paramètres** > **Configurer les fonctionnalités avancées** > **Répondeur** .



2. Créez une action de répondeur et spécifiez un nom approprié, tel que http_to_https_actn, dans le champ Nom.
3. Pour créer une action de répondeur, dans le volet de navigation, développez **AppExpert** > **Répondeur**, cliquez sur **Actions**, puis cliquez sur **Ajouter** .
4. Sélectionnez Rediriger en tant que Type.
5. Dans le champ **Expression**, tapez l'expression suivante :

   ```
   "https://"+ HTTP.REQ.HOSTNAME.HTTP_URL_SAFE + HTTP.REQ.URL.PATH_AND_QUERY
   .HTTP_URL_SAFE.
   ```

6. Dans NetScaler version 9.0 et 10.0, assurez-vous que l'option **Contourner la vérification de sécurité** est désactivée.

   Remarque : cette option n'est pas présente à partir de NetScaler 11.0.
7. Créez une **stratégie de répondeur** et spécifiez un nom approprié, tel que http_to_https_pol, dans le champ Nom.
8. Pour créer une stratégie de répondeur, dans le volet de navigation, développez **AppExpert** > **Répondeur**, cliquez sur **Stratégies**, puis cliquez sur **Ajouter** .
9. Dans la liste Action, sélectionnez le nom de l'action que vous avez créée.
10. Dans la liste Action non définie, sélectionnez RESET.
11. Tapez l'expression **HTTP.REQ.IS_VALID** dans le champ **Expression**, comme indiqué dans la capture d'écran suivante.



1. Créez un moniteur pour lequel l'état est toujours marqué comme UP et spécifiez un nom approprié, tel que localhost_ping, dans le champ Nom.
2. Pour créer un moniteur, dans le volet de navigation, développez **Équilibrage de la charge**, cliquez sur **Moniteurs**, puis cliquez sur **Ajouter**.
3. Dans le champ **IP de destination**, spécifiez l'adresse IP 127.0.0.1, comme indiqué dans la capture d'écran suivante.



4. Créez un service et spécifiez un nom approprié, tel que Always_up_Service, dans le champ **Nom** .
5. Pour créer un service, dans le volet de navigation, développez **Équilibrage de la charge**, cliquez sur **Services**, puis cliquez sur **Ajouter**.
6. Spécifiez une adresse IP inexistante dans le champ **Serveur** .



7. Spécifiez 80 dans le champ **Port** .
8. Ajoutez le moniteur créé à partir de la liste **Moniteurs disponibles** .
9. Créez un serveur virtuel d'équilibrage de charge et spécifiez un nom approprié dans le champ **Nom** .
10. Pour créer un serveur virtuel d'équilibrage de charge, dans le volet de navigation, développez **Équilibrage de charge**, cliquez sur **Services**, puis cliquez sur **Ajouter**.
11. Spécifiez l'adresse IP du site Web dans le champ Adresse IP.
12. Sélectionnez HTTP dans la liste Protocol.
13. Tapez 80 dans le champ Port.
14. Sur NetScaler version 9.0 et 10.0, sélectionnez l'option Actif pour le service que vous avez créé dans l'onglet Services, comme indiqué dans la capture d'écran suivante. Cette option est obsolète dans NetScaler version 11.0.



15. Cliquez sur l'onglet **Stratégies**.
16. Liez la stratégie Répondeur que vous avez créée à l'adresse VIP d'équilibrage de la charge HTTP du site Web.
17. Créez un serveur virtuel d'équilibrage de charge sécurisé dont l'adresse IP du site Web et le port sont 443.

Pour créer une configuration similaire à la procédure précédente à partir de l'interface de ligne de commande de l'appliance, exécutez les commandes suivantes :

```
1  enable ns feature responder
2  add responder action http_to_https_actn redirect ""https://" + http.req
       .hostname.HTTP_URL_SAFE + http.REQ.URL.PATH_AND_QUERY.HTTP_URL_SAFE"
3  add responder policy http_to_https_pol HTTP.REQ.IS_VALID
       http_to_https_actn RESET
4  add lb monitor localhost_ping PING -LRTM ENABLED -destIP 127.0.0.1
5  add service Always_UP_service 1.2.3.4 HTTP 80 -gslb NONE -maxClient 0 -
       maxReq 0 -cip ENABLED dummy -usip NO -sp OFF -cltTimeout 180 -
       svrTimeout 360 -CKA NO -TCPB NO -CMP YES
6  bind lb monitor localhost_ping Always_UP_service
7  add lb vserver http_site.com HTTP 10.217.96.238 80 -persistenceType
       COOKIEINSERT -timeout 0 -cltTimeout 180
8  bind lb vserver http_site.com Always_UP_service
9  bind lb vserver http_site.com -policyName http_to_https_pol -priority 1
        -gotoPriorityExpression END
10 <!--NeedCopy-->
```


Remarques :

- L'état du serveur virtuel Redirection d'équilibrage de charge du port 80 doit être UP pour que la redirection fonctionne.
- Les navigateurs Web peuvent ne pas rediriger correctement si le serveur virtuel HTTPS n'est pas actif.
- Cette configuration de redirection permet des situations où plusieurs domaines sont liés à la même adresse IP.
- Si le client envoie une requête HTTP non valide au serveur virtuel de redirection, l'appliance envoie un code de message RESET.

Résolution des problèmes

January 21, 2021

Si la fonctionnalité de répondeur ne fonctionne pas comme prévu après l'avoir configurée, vous pouvez utiliser certains outils courants pour accéder aux ressources Citrix ADC et diagnostiquer le problème.

Ressources pour le dépannage

Pour obtenir de meilleurs résultats, utilisez les ressources suivantes pour résoudre un problème de cache intégré sur une appliance Citrix ADC :

- Le fichier ns.conf
- Les fichiers de suivi pertinents du client et de l'appliance Citrix ADC

En plus des ressources ci-dessus, les outils suivants permettent d'accélérer le dépannage :

- Les iehttpheaders ou un utilitaire similaire
- L'application Wireshark personnalisée pour les fichiers de trace Citrix ADC

Résolution des problèmes liés au répondeur

- **Problème**

  La fonctionnalité Répondeur est configurée, mais l'action Répondeur ne fonctionne pas.

  Résolution

  - Vérifiez que la fonctionnalité est activée.
  - Vérifiez les compteurs d'accès de l'une des stratégies pour voir si les compteurs sont incrémentés.

- Vérifiez que les stratégies et les actions sont correctement configurées.
- Vérifiez que les actions et les stratégies sont liées de manière appropriée.
- Enregistrez les traces de paquets sur le client et l'appliance Citrix ADC et analysez-les pour obtenir un pointeur sur le problème.
- Enregistrez les traces de paquets IEHttpHeaters sur le client et vérifiez les requêtes HTTP et les réponses pour obtenir un pointeur sur le problème.

- **Problème**

  Vous devez créer une page de maintenance.

  Résolution

1. Configurez les services et le serveur virtuel.
2. Configurez un serveur virtuel de sauvegarde avec un service qui lui est lié. Cela garantit que l'état du site Web est toujours affiché comme UP.
3. Configurez le serveur virtuel principal pour qu'il utilise le serveur virtuel de sauvegarde comme sauvegarde.
4. Créez une action de répondeur avec une cible appropriée. Voici un exemple pour votre référence :

   ```
   add responder action sorry_page respondwith q{ "HTTP/1.0 200 OK"+"\r\n\
   r\n"+ "<html><body>Sorry, this page is not available\</body>\</html>"+
   "\r\n"}
   ```

5. Créez une stratégie de répondeur et liez l'action à celle-ci.
6. Liez la stratégie de répondeur au serveur virtuel de sauvegarde.

Réécrire

October 5, 2021

> **Avertissement :**
>
> Les fonctionnalités de filtrage utilisant des stratégies classiques sont obsolètes et Citrix vous recommande d'utiliser les fonctionnalités de réécriture et de répondeur avec une infrastructure de stratégie avancée.

Réécriture fait référence à la réécriture de certaines informations dans les demandes ou réponses traitées par l'appliance Citrix ADC. La réécriture peut aider à fournir l'accès au contenu demandé sans exposer des détails inutiles sur la configuration réelle du site Web. Voici quelques situations dans lesquelles la fonction de réécriture est utile :

- Pour améliorer la sécurité, Citrix ADC peut réécrire tous les éléments `https://` dans `http://` `links` le corps de la réponse.
- Dans le déploiement de déchargement SSL, les liens non sécurisés de la réponse doivent être convertis en liens sécurisés. À l'aide de l'option de réécriture, vous pouvez réécrire tous les `https://` éléments `http://links` pour vous assurer que les réponses sortantes de Citrix ADC vers le client disposent des liens sécurisés.
- Si un site Web doit afficher une page d'erreur, vous pouvez afficher une page d'erreur personnalisée au lieu de la page d'erreur 404 par défaut. Par exemple, si vous affichez la page d'accueil ou le plan du site Web au lieu d'une page d'erreur, le visiteur reste sur le site au lieu de s'éloigner du site Web.
- Si vous souhaitez lancer un nouveau site Web, mais utiliser l'ancienne URL, vous pouvez utiliser l'option Réécrire.
- Lorsqu'une rubrique d'un site comporte une URL compliquée, vous pouvez la réécrire avec une URL simple et facile à retenir (également appelée « URL cool »).
- Vous pouvez ajouter le nom de page par défaut à l'URL d'un site Web. Par exemple, si la page par défaut du site Web d'une entreprise est `http://www.abc.com/index.php`, lorsque l'utilisateur tape « abc.com » dans la barre d'adresse du navigateur, vous pouvez réécrire l'URL en « abc.com/index.php ».

Lorsque vous activez la fonctionnalité de réécriture, Citrix ADC peut modifier les en-têtes et le corps des requêtes et réponses HTTP.

Pour réécrire les demandes et réponses HTTP, vous pouvez utiliser des expressions de stratégie Citrix ADC prenant en charge le protocole dans les stratégies de réécriture que vous configurez. Les serveurs virtuels qui gèrent les demandes et réponses HTTP doivent être de type
HTTP ou
SSL. Dans le trafic HTTP, vous pouvez effectuer les actions suivantes :

- Modifier l'URL d'une demande
- Ajouter, modifier ou supprimer des en-têtes
- Ajoutez, remplacez ou supprimez une chaîne spécifique dans le corps ou les en-têtes.

Pour réécrire des charges utiles TCP, considérez la charge utile comme un flux brut d'octets. Chacun des serveurs virtuels qui gèrent les connexions TCP doit être de type TCP ou SSL_TCP. Le terme réécriture TCP est utilisé pour désigner la réécriture de charges utiles TCP qui ne sont pas des données HTTP. Dans le trafic TCP, vous pouvez ajouter, modifier ou supprimer n'importe quelle partie de la charge utile TCP.

Pour obtenir des exemples d'utilisation de la fonction de réécriture, consultez Exemples d'actions de réécriture et de stratégie.

Comparaison entre les options Réécriture et Répondeur

La principale différence entre la fonction de réécriture et la fonction répondeur est la suivante :

Le répondeur ne peut pas être utilisé pour les expressions de réponse ou basées sur le serveur. Le répondeur ne peut être utilisé que pour les scénarios suivants, en fonction des paramètres du client :

- Redirection d'une requête HTTP vers de nouveaux sites Web ou pages Web
- Répondre avec une réponse personnalisée
- Dépose ou réinitialisation d'une connexion au niveau de la demande

S'il existe une stratégie de répondeur, Citrix ADC examine la demande du client, prend des mesures conformément aux stratégies applicables, envoie la réponse au client et ferme la connexion avec le client.

S'il existe une stratégie de réécriture, Citrix ADC examine la demande du client ou la réponse du serveur, prend des mesures en fonction des stratégies applicables et transfère le trafic au client ou au serveur.

En général, il est recommandé d'utiliser un répondeur si vous souhaitez que Citrix ADC réinitialise ou abandonne une connexion en fonction d'un client ou d'un paramètre basé sur une demande. Utilisez le répondeur pour rediriger le trafic ou répondez avec des messages personnalisés. Utilisez la réécriture pour manipuler les données des requêtes et réponses HTTP.

Comment fonctionne la réécriture

Une stratégie de réécriture consiste en une règle et une action. La règle détermine le trafic sur lequel la réécriture est appliquée et l'action détermine l'action à entreprendre par Citrix ADC. Vous pouvez définir plusieurs stratégies de réécriture. Pour chaque stratégie, spécifiez le point de liaison et la priorité.

Un point de liaison fait référence à un point du flux de trafic auquel Citrix ADC examine le trafic pour vérifier si une stratégie de réécriture peut lui être appliquée. Vous pouvez lier une stratégie à un serveur virtuel d'équilibrage de charge ou de commutation de contenu spécifique, ou rendre la stratégie globale si vous souhaitez que la stratégie soit appliquée à l'ensemble du trafic géré par Citrix ADC. Ces stratégies sont appelées stratégies globales.

Outre les stratégies définies par l'utilisateur, Citrix ADC dispose de certaines stratégies par défaut. Vous ne pouvez pas modifier ou supprimer une stratégie par défaut.

Pour évaluer les stratégies, Citrix ADC respecte l'ordre suivant :

- Politiques mondiales
- Stratégies liées à des serveurs virtuels spécifiques
- Stratégies par défaut

> **Remarque :**
>
> Citrix ADC peut appliquer une stratégie de réécriture uniquement lorsqu'elle est liée à un point.

Citrix ADC implémente la fonctionnalité de réécriture dans les étapes suivantes :

- L'appliance Citrix ADC recherche des stratégies globales, puis vérifie les stratégies au niveau des points de liaison individuels.
- Si plusieurs stratégies sont liées à un point de liaison, Citrix ADC évalue les stratégies dans l'ordre de leur priorité. La stratégie ayant la priorité la plus élevée est évaluée en premier. Après avoir évalué chaque stratégie, si la stratégie est évaluée à TRUE, elle ajoute l'action associée à la stratégie à laquelle l'action associée est exécutée. Une correspondance se produit lorsque les caractéristiques spécifiées dans la règle de stratégie correspondent aux caractéristiques de la demande ou de la réponse en cours d'évaluation.
- Pour n'importe quelle stratégie, en plus de l'action, vous pouvez spécifier la stratégie qui doit être évaluée après l'évaluation de la stratégie actuelle. Cette politique est appelée « Aller à l'expression ». Pour n'importe quelle stratégie, si une option Aller à l'expression (GoToPriorityExpr) est spécifiée, Citrix ADC évalue la stratégie Aller à l'expression. Il ne tient pas compte de la stratégie qui a la priorité la plus élevée.

  Vous pouvez spécifier la priorité de la stratégie pour indiquer la stratégie Atteindre l'expression. Vous ne pouvez pas utiliser le nom de la stratégie. Si vous souhaitez que Citrix ADC arrête d'évaluer d'autres stratégies après avoir évalué une stratégie particulière, vous pouvez définir l'option Aller à l'expression sur « FIN ».
- Une fois toutes les stratégies évaluées ou lorsqu'une stratégie a l'option Aller à l'expression définie comme END, Citrix ADC commence à exécuter les actions en fonction de la liste des actions.

Pour plus d'informations sur la configuration des stratégies de réécriture, voir Configuration d'une stratégie de réécriture et sur la liaison des stratégies de réécriture, voir Liaison d'une stratégie de réécriture.

La figure suivante illustre la façon dont Citrix ADC traite une demande ou une réponse lorsque la fonction de réécriture est utilisée.

Figure 1. Le processus de réécriture



Évaluation des politiques

La stratégie ayant la priorité la plus élevée est évaluée en premier. Citrix ADC n'arrête pas l'évaluation des stratégies de réécriture lorsqu'il trouve une correspondance. Il évalue toutes les stratégies de réécriture configurées sur Citrix ADC.

- Si une stratégie est évaluée à TRUE, Citrix ADC suit la procédure ci-dessous :
  - Si la stratégie Atteindre l'expression est définie sur END, Citrix ADC arrête d'évaluer toutes les autres stratégies et commence à effectuer la réécriture.
  - L'expression GoToPriorityExpression peut être définie sur « NEXT », « END », un nombre entier ou « INVOCATION_LIST ». La valeur détermine la stratégie avec la priorité suivante. Le tableau suivant présente l'action entreprise par Citrix ADC pour chaque valeur de l'expression.

Valeur de l'expression	Action
SUIVANT	La stratégie avec la priorité suivante est évaluée.
END	L'évaluation des politiques s'arrête.
<an integer>	La stratégie avec une priorité spécifiée est évaluée.
INVOCATION_LIST	Goto NEXT ou END est appliqué en fonction du résultat de la liste d'appels.

- Si une stratégie est évaluée à FALSE, Citrix ADC poursuit l'évaluation dans l'ordre de priorité.
- Si une stratégie est évaluée sur UNDEFINED (ne peut pas être évaluée sur le trafic reçu en raison d'une erreur), Citrix ADC exécute l'action affectée à la condition UNDEFINED (appelée UnDefaction) et arrête l'évaluation ultérieure des stratégies.

Citrix ADC démarre la réécriture proprement dite une fois l'évaluation terminée. Il fait référence à la liste des actions identifiées par les stratégies évaluées à TRUE et démarre la réécriture. Après avoir implémenté toutes les actions de la liste, Citrix ADC transfère le trafic selon les besoins.

> **Remarque :**
>
> Assurez-vous que les stratégies ne spécifient pas d'actions conflictuelles ou superposées sur la même partie de l'en-tête ou du corps HTTP, ou de la charge utile TCP. Lorsqu'un tel conflit se produit, Citrix ADC rencontre une situation indéfinie et interrompt la réécriture.

Actions de réécriture

Sur l'appliance Citrix ADC, spécifiez les actions à effectuer, telles que l'ajout, le remplacement ou la suppression de texte dans le corps, ou l'ajout, la modification ou la suppression d'en-têtes, ou toute modification de la charge utile TCP en tant qu'actions de réécriture. Pour plus d'informations sur les actions de réécriture, voir Configuration d'une action de réécriture.

Le tableau suivant décrit les étapes que peut prendre Citrix ADC lorsqu'une stratégie évalue la valeur TRUE.

Action	Résultats
Inser	L'action de réécriture spécifiée pour la stratégie est exécutée.
NOREWRITE	La demande ou la réponse n'est pas réécrite. Citrix ADC transfère le trafic sans réécrire aucune partie du message.

Action	Résultats
RÉINITIALISER	La connexion est interrompue au niveau TCP.
FAIRE TOMBER	Le message est supprimé.

> **Remarque** :
>
> Pour n'importe quelle stratégie, vous pouvez configurer la sous-action (action à effectuer lorsque la stratégie est évaluée à UNDEFINED) en tant que NOREWRITE, RESET ou DROP.

Pour utiliser la fonction de
réécriture, procédez comme suit :

- Activez la fonctionnalité sur Citrix ADC.
- Définissez les actions de réécriture.
- Définissez des stratégies de réécriture.
- Liez les stratégies à un point de liaison pour mettre en œuvre une stratégie.

Activer la réécriture

Activez la fonction de réécriture sur l'appliance Citrix ADC si vous souhaitez réécrire les demandes ou réponses HTTP ou TCP. Si la fonctionnalité est activée, Citrix ADC prend l'action de réécriture en fonction des stratégies spécifiées. Pour plus d'informations, voir Comment fonctionne la réécriture.

Pour activer la fonction de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer la fonction de réécriture et vérifier la configuration :

- enable ns feature REWRITE
- show ns feature

Exemple :

```
> enable ns feature REWRITE
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 .
 .
 .
```



```
 1)     Rewrite                          REWRITE              ON
 .
 .
 1)     Citrix ADC Push                   push                 OFF
 Done
<!--NeedCopy-->
```

Pour activer la fonction de réécriture à l'aide de l'interface graphique

1. Dans le volet de navigation, cliquez sur **Système**, puis sur **Paramètres**.
2. Dans le volet d'informations, sous Modes et fonctionnalités, cliquez sur **Configurer les fonctionnalités de base**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités de base**, activez la case à cocher Réécrire, puis cliquez sur **OK**.
4. Dans la boîte de dialogue **Activer/Désactiver les fonctionnalités**, cliquez sur **Oui**. Un message apparaît dans la barre d'état, indiquant que la fonctionnalité sélectionnée a été activée.

Configuration d'une action de réécriture

> **Avertissement**
>
> La fonction Pattern dans une action de réécriture est obsolète à partir de Citrix ADC 12.0 build 56.20 et, comme alternative, Citrix vous recommande d'utiliser le paramètre Search rewrite action.

Une action de réécriture indique les modifications apportées à une demande ou à une réponse avant de l'envoyer à un serveur ou à un client.

Les expressions définissent les éléments suivants :

- Type d'action de réécriture.
- Emplacement de l'action de réécriture.
- Type de configuration de l'action de réécriture.

Par exemple, une action DELETE utilise uniquement une expression cible. Une action REMPLACER utilise une expression cible et une expression pour configurer le texte de remplacement.

Après avoir activé la fonction de réécriture, vous devez configurer une ou plusieurs actions, à moins qu'une action de réécriture intégrée ne soit suffisante. Toutes les actions intégrées ont des noms commençant par la chaîne ns_cvpn, suivie d'une chaîne de lettres et de caractères de soulignement. Les actions intégrées effectuent des tâches utiles et complexes telles que le décodage de parties d'une demande ou d'une réponse VPN sans client ou la modification de données JavaScript ou XML. Les actions intégrées peuvent être affichées, activées et désactivées, mais elles ne peuvent pas être modifiées ou supprimées.

> Remarque :
>
> Les types d'action qui peuvent être utilisés uniquement pour la réécriture HTTP sont identifiés dans la colonne **Type d'action de réécriture** .

Pour plus d'informations, consultez la section **Paramètre de type**.

Créer une action de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une action de réécriture et vérifier la configuration :

- `add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-search <expression>] [refineSearch <expression>] [-comment<string>]`
- `show rewrite action <name>`

Pour plus d'informations, consultez le tableau Types d'actions de réécriture et leurs arguments .

La fonction de réécriture comporte les actions intégrées suivantes :

- NoRewrite-envoie la demande ou la réponse à l'utilisateur sans la réécrire.
- RESET - Réinitialise la connexion et informe le navigateur de l'utilisateur, afin que l'utilisateur puisse renvoyer la demande.
- DROP - Permet de supprimer la connexion sans envoyer de réponse à l'utilisateur.

L'un des types de flux suivants est implicitement associé à chaque action :

- Demande - L'action s'applique à la demande.
- Réponse - L'action s'applique à la réponse.
- Neutre - L'action s'applique à la fois aux demandes et aux réponses.

Nom

Nom de l'action de réécriture définie par l'utilisateur. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), le hachage (#), l'espace (), à (@), égal (=), deux-points (:) et les caractères de soulignement. Peut être modifié après l'ajout de la stratégie de réécriture.

Paramètre de type

Le paramètre **Type** indique le type d'action de réécriture définie par l'utilisateur.

Voici les valeurs du paramètre **Type** :

- REPLACE <target> <string_builder_expr>. Remplace la chaîne par l'expression string-builder.

Exemple :

```
> add rewrite action replace_http_act replace http.res.body(100) '"
    new_replaced_data"'
Done
> sh rewrite action replace_http_act
Name: replace_http_act
Operation: replace
Target:http.res.body(100)
Value:"new_replaced_data"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_ALL <target> <string_builder_expr1> -(search)<string_builder_expr2>. Dans la demande ou la réponse spécifiée par <target>, remplace toutes les occurrences de la chaîne définie <string_builder_expr1> par par la chaîne définie par <string_builder_expr2>. Vous pouvez utiliser la fonction de recherche pour trouver les chaînes à remplacer.

Exemple :

```
> add policy patset pat_list_2
Done
> bind policy patset pat_list_2 "www.abc.com"
Done
> bind policy patset pat_list_2 "www.def.com"
Done
> add rewrite action refineSearch_act_31 replace_all "HTTP.RES.BODY
    (100000)" ""https://""-search "patset("pat_list_2")" -refineSearch "
    EXTEND(7,0).REGEX_SELECT(re#http://#)"
Done

> sh rewrite action refineSearch_act_31
Name: refineSearch_act_31
Operation: replace_all
Target:HTTP.RES.BODY(100000)
Refine Search:EXTEND(7,0).REGEX_SELECT(re#http://#)
Value:"https://"
Search: patset("pat_list_2")
```



```
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_HTTP_RES <string_builder_expr>. Remplace la réponse HTTP complète par la chaîne définie par l'expression string-builder.

Exemple :

```
> add rewrite action replace_http_res_act replace_http_res '"HTTP/1.1
   200 OK\r\n\r\nSending from ADC"'
 Done
> sh rewrite action replace_http_res_act
Name: replace_http_res_act
Operation: replace_http_res
Target:"HTTP/1.1 200 OK
Sending from ADC"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_SIP_RES <target>. Remplace la réponse SIP complète par la chaîne spécifiée par <target>.

Exemple :

```
> add rewrite action replace_sip_res_act replace_sip_res '"HTTP/1.1 200
    OK\r\n\r\nSending from ADC"'
Done
> sh rewrite action replace_sip_res_act
Name: replace_sip_res_act
Operation: replace_sip_res
Target:"HTTP/1.1 200 OK
Sending from ADC"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```


- INSERT_HTTP_HEADER <header_string_builder_expr> <contents_string_builder_expr>. Insère l'en-tête HTTP spécifié par <header_string_builder_expr> et le contenu de l'en-tête spécifié par <contents_string_builder_expr>.

Exemple :

```
> add rewrite action ins_cip_header insert_http_header "CIP" "CLIENT.IP.SRC"
Done
> sh rewrite action ins_cip_header
Name: ins_cip_header
Operation: insert_http_header
Target:CIP
Value:CLIENT.IP.SRC
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE_HTTP_HEADER <target>. Supprime l'en-tête HTTP spécifié par <target>

Exemple :

```
> add rewrite action del_true_client_ip_header delete_http_header "True-Client-IP"
Done
> sh rewrite action del_true_client_ip_header
Name: del_true_client_ip_header
Operation: delete_http_header
Target:True-Client-IP
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CORRUPT_HTTP_HEADER <target>. Remplace le nom d'en-tête de toutes les occurrences de l'en-tête HTTP spécifié <target> par un nom corrompu, de sorte qu'il ne soit pas reconnu par le destinataire Exemple : MY_HEADER est remplacé par MHEY_ADER.

Exemple :


```
> add rewrite action corrupt_content_length_hdr corrupt_http_header "
    Content-Length"
Done
> sh rewrite action corrupt_content_length_hdr
Name: corrupt_content_length_hdr
Operation: corrupt_http_header
Target:Content-Length
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_BEFORE <string_builder_expr1> <string_builder_expr1>. Recherche la chaîne spécifiée dans <string_builder_expr1> et insère la chaîne <string_builder_expr2 > avant.

```
> add rewrite action insert_before_ex_act insert_before http.res.body
    (100) '"Add this string in the starting"'
Done
> sh rewrite action insert_before_ex_act
Name: insert_before_ex_act
Operation: insert_before
Target:http.res.body(100)
Value:"Add this string in the starting"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_BEFORE_ALL <target> <string_builder_expr1> -(search)<string_builder_expr2 >. Dans la requête ou la réponse spécifiée par <target>, localise toutes les occurrences de la chaîne spécifiée dans <string_builder_expr1> et insère la chaîne spécifiée < string_builder_expr2> avant celle-ci. Vous pouvez utiliser la fonction de recherche pour trouver les chaînes.

Exemple :

```
> add policy patset pat
 Done
> bind policy patset pat abcd
 Done
```



```
> add rewrite action refineSearch_act_1 insert_before_all http.res.body
    (10) 'target.prefix(10) + "refineSearch_testing"' -search patset("
    pat") -refineSearch extend(10,10)
 Done
> sh rewrite action refineSearch_act_1
Name: refineSearch_act_1
Operation: insert_before_all
Target:http.res.body(10)
Refine Search:extend(10,10)
Value:target.prefix(10) + "refineSearch_testing"
Search: patset("pat")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_AFTER <string_builder_expr1> <string_builder_expr2>. Recherche la chaîne spécifiée dans <string_builder_expr1>, puis insère la chaîne spécifiée dans <string_builder_expr2> après ça.

Exemple :

```
> add rewrite action insert_after_act insert_after http.req.body(100) '
    "add this string after 100 bytes"'
Done
> sh rewrite action insert_after_act
Name: insert_after_act
Operation: insert_after
Target:http.req.body(100)
Value:"add this string after 100 bytes"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_AFTER_ALL <target> <string_builder_expr1> -(search)<string_builder_expr>. Dans la demande ou la réponse spécifiée par <target>, localise toutes les occurrences de la chaîne spécifiée par <string_builder_expr1> et insère la chaîne spécifiée par <string_builder_expr2> après chaque. Vous pouvez utiliser la fonction de recherche pour trouver les chaînes.

Exemple :

```
> add rewrite action refineSearch_act_2 insert_after_all http.res.body
   (100) '"refineSearch_testing"' -search text("abc") -refineSearch
   extend(0, 10)
Done
> sh rewrite action refineSearch_act_2
Name: refineSearch_act_2
Operation: insert_after_all
Target:http.res.body(100)
Refine Search:extend(0, 10)
Value:"refineSearch_testing"
Search: text("abc")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `DELETE <target>`. Recherche et supprime la cible spécifiée.

Exemple :

```
> add rewrite action delete_ex_act delete http.req.header("HDR")
Done
> sh rewrite action delete_ex_act
Name: delete_ex_act
Operation: delete
Target:http.req.header("HDR")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `DELETE_ALL <target> -(search)<string_builder_expr>`. Dans la demande ou la réponse spécifiée par `<target>`, recherche et supprime toutes les occurrences de la chaîne spécifiée par `<string_builder_expr>`. Vous pouvez utiliser la fonction de recherche pour trouver les chaînes.

Exemple :

```
>add rewrite action refineSearch_act_4 delete_all "HTTP.RES.BODY(50000)
   " -search text("Windows Desktops") -refineSearch "EXTEND(40,40).
```



```
    REGEX_SELECT(re#\s`\*`<AppData>.`\*`\s`\*`<\\/AppData>#)"
Done
> show REWRITE action refineSearch_act_4
Name: refineSearch_act_4
Operation: delete_all
Target:HTTP.RES.BODY(50000)
Refine Search:EXTEND(40,40).REGEX_SELECT(re#\s`\*`<AppData>.`\*`\s
    `\*`</AppData>#)
Search: text("Windows Desktops")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `REPLACE_DIAMETER_HEADER_FIELD <target> <field value>`. Dans la ou les réponses, modifiez le champ d'en-tête spécifié par `<target>`. Utilisez `Diameter.req.flags.SET (<flag>)` ou `Diameter.req.flags.UNSET<flag>` comme `stringbuilderexpression` pour définir ou annuler les indicateurs.

Exemple :

```
> add rewrite action replace_diameter_field_ex_act
    replace_diameter_header_field diameter.req.flags diameter.req.flags.
    set(PROXIABLE)
Done
> sh rewrite action replace_diameter_field_ex_act
Name: replace_diameter_field_ex_act
Operation: replace_diameter_header_field
Target:diameter.req.flags
Value:diameter.req.flags.set(PROXIABLE)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `REPLACE_DNS_HEADER_FIELD <target>`. Dans la demande ou la réponse, modifie le champ d'en-tête spécifié par `<target>`.

Exemple :

```
> add rewrite action replace_dns_hdr_act replace_dns_header_field dns.
    req.header.flags.set(AA)
```



```
Done
> sh rewrite action replace_dns_hdr_act
Name: replace_dns_hdr_act
Operation: replace_dns_header_field
Target:dns.req.header.flags.set(AA)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_DNS_ANSWER_SECTION <target>. Remplacez la section de réponse DNS dans la réponse. Cela s'applique uniquement aux enregistrements A et AAAA. Utilisez DNS.NEW_RRSET_A les NS.NEW_RRSET_AAAA expressions et pour configurer la nouvelle section de réponses.

Exemple :

```
> add rewrite action replace_dns_ans_act replace_dns_answer_section
   DNS.NEW_RRSET_A("1.1.1.1", 10)
Done
> sh rewrite action replace_dns_ans_act
Name: replace_dns_ans_act
Operation: replace_dns_answer_section
Target:DNS.NEW_RRSET_A("1.1.1.1", 10)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CLIENTLESS_VPN_DECODE<target>. Décode le modèle spécifié par la cible au format VPN sans client.

Exemple :

```
> add rewrite action cvpn_decode_act_1 clientless_vpn_decode http.req.
   body(100)
Done
> sh rewrite action cvpn_decode_act_1
Name: cvpn_decode_act_1
Operation: clientless_vpn_decode
Target:http.req.body(100)
```



```
7  Hits: 0
8  Undef Hits: 0
9  Action Reference Count: 0
10 Done
11
12 <!--NeedCopy-->
```

- CLIENTLESS_VPN_DECODE_ALL<target>-search<expression>. Décode TOUS les modèles spécifiés par le paramètre de recherche au format VPN sans client.

Exemple :

```
1  > add rewrite action act1 clientless_vpn_decode_all http.req.body(100)
      -search text("abcd")
2  Done
3  > sh rewrite action act1
4  Name: act1
5  Operation: clientless_vpn_decode_all
6  Target:http.req.body(100)
7  Search: text("abcd")
8  Hits: 0
9  Undef Hits: 0
10 Action Reference Count: 0
11 Done
12
13 <!--NeedCopy-->
```

- CLIENTLESS_VPN_ENCODE<target>. Encode le modèle spécifié par la cible au format VPN sans client.

Exemple :

```
1  > add rewrite action cvpn_encode_act_1 clientless_vpn_encode http.req.
      body(100)
2  Done
3  > sh rewrite action cvpn_encode_act_1
4  Name: cvpn_encode_act_1
5  Operation: clientless_vpn_encode
6  Target:http.req.body(100)
7  Hits: 0
8  Undef Hits: 0
9  Action Reference Count: 0
10 Done
11
12 <!--NeedCopy-->
```


- CLIENTLESS_VPN_ENCODE_ALL<target>-search<expression>. Encode TOUS les paramètres de recherche spécifiés dans le format VPN sans client.

Exemple :

```
> add rewrite action act2 clientless_vpn_encode_all http.req.body(100)
   -search text("abcd")
Done
> sh rewrite action act2
Name: act1
Operation: clientless_vpn_encode_all
Target:http.req.body(100)
Search: text("abcd")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CORRUPT_SIP_HEADER<target>. Remplace le nom d'en-tête de toutes les occurrences de l'en-tête SIP spécifié par <target> par un nom corrompu, de sorte que le destinataire ne le reconnaisse pas.

Exemple :

```
> add rewrite action corrupt_sip_hdr_act corrupt_sip_header SIP_HDR
Done
> sh rewrite action corrupt_sip_hdr_act
Name: corrupt_sip_hdr_act
Operation: corrupt_sip_header
Target:SIP_HDR
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_SIP_HEADER <header_string_builder_expr> <contents_string_builder_expr>. Insère l'en-tête SIP spécifié par <header_string_builder_expr> et le contenu de l'en-tête spécifié par <contents_string_builder_expr>.

Exemple :


```
> add rewrite action insert_sip_hdr_act insert_sip_header SIP_HDR '"
    inserting_sip_header"'
 Done
>sh rewrite action insert_sip_hdr_act
Name: insert_sip_hdr_act
Operation: insert_sip_header
Target:SIP_HDR
Value:"inserting_sip_header"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE_SIP_HEADER<target>. Supprime l'en-tête SIP spécifié par <target>

Exemple :

```
> add rewrite action delete_sip_hdr delete_sip_header  SIP_HDR
Done
> sh rewrite action delete_sip_hdr
Name: delete_sip_hdr
Operation: delete_sip_header
Target:SIP_HDR
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Paramètre Target

Le paramètre Target est une expression qui spécifie la partie de la demande ou de la réponse à réécrire.

StringBuilderExpr

StringBuilderExpr est une expression qui spécifie le contenu qui doit être inséré dans la demande ou la réponse à l'emplacement spécifié. Cette expression remplace une chaîne spécifiée.

Exemple 1. Insertion d'un en-tête HTTP avec l'adresse IP du client :

```
> add rewrite action insertact INSERT_HTTP_HEADER "client-IP" CLIENT.IP
    .SRC
```



```
Done
> show rewrite action insertact
Name: insertact
Operation: insert_http_header
Target:Client-IP
Value:CLIENT.IP.SRC
BypassSafetyCheck : NO
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Exemple 2. Remplacement des chaînes dans une charge utile TCP (réécriture TCP) :

```
> add rewrite action client_tcp_payload_replace_all REPLACE_ALL
  'client.tcp.payload(1000)' '"new-string"' -search text("old-string")
Done
> show rewrite action client_tcp_payload_replace_all
Name: client_tcp_payload_replace_all
Operation: replace_all
Target:client.tcp.payload(1000)
Value:"new-string"
Search: text("old-string")
BypassSafetyCheck : NO
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Rechercher une partie de la demande ou de la réponse à réécrire

La fonctionnalité de recherche permet de trouver toutes les instances du modèle requis dans la demande ou la réponse.

La fonctionnalité de recherche doit être utilisée dans les types d'action suivants :

- INSERT_BEFORE_ALL
- INSERT_AFTER_ALL
- REPLACE_ALL
- DELETE_ALL

- CLIENTLESS_VPN_ENCODE_ALL
- CLIENTLESS_VPN_DECODE_ALL

La fonctionnalité de recherche ne peut pas être utilisée avec les types d'action suivants :

- INSERT_HTTP_HEADER
- INSERT_BEFORE
- INSERT_AFTER
- REMPLACER
- SUPPRIMER
- DELETE_HTTP_HEADER
- CORRUPT_HTTP_HEADER
- REPLACE_HTTP_RES
- CLIENTLESS_VPN_ENCODE
- CLIENTLESS_VPN_DECODE
- INSERT_SIP_HEADER
- DELETE_SIP_HEADER
- CORRUPT_SIP_HEADER
- REPLACE_DIAMETER_HEADER_FIELD
- REPLACE_DNS_ANSWER_SECTION
- REPLACE_DNS_HEADER_FIELD
- REPLACE_SIP_RES

Les types de recherche suivants sont pris en charge :

- Texte - une chaîne littérale
  Exemple recherche de texte (« bonjour »)
- Expression régulière - modèle utilisé pour faire correspondre plusieurs chaînes dans la requête ou la réponse
  Exemple search regex (re~^bonjour*~)
- XPATH - Expression XPATH pour effectuer une recherche XML.
  Exemple search xpath (xp%/a/b%)
- JSON : expression XPATH permettant de rechercher JSON.
  Exemple search xpath_json (xp%/a/b%)
  HTML - Une expression XPATH pour rechercher du HTML
  Exemple search xpath_html (xp%/html/body%)
  Patset - Ceci recherche tous les motifs liés à l'entité patset.
  Exemple -search patset("patset1")
- Jeu de données - Cette option recherche tous les modèles liés à l'entité du jeu de données.
  Exemple : -search dataset("dataset1")
- AVP - Numéro AVP utilisé pour faire correspondre plusieurs AVP dans un message Diameter/Radius

Exemple ⊠search avp (999)

Affiner les résultats de la recherche

Vous pouvez utiliser la fonctionnalité Affiner la recherche pour spécifier les critères supplémentaires permettant d'affiner les résultats de la recherche. La fonctionnalité Affiner la recherche ne peut être utilisée que si la fonctionnalité de recherche est utilisée.
Le paramètre Affiner la recherche commence toujours par l'opération « extend (m, n) », où 'm' indique quelques octets à gauche du résultat de la recherche et 'n' indique plusieurs octets à droite du résultat de la recherche pour étendre la zone sélectionnée.

Si l'action de réécriture configurée est la suivante :

```
> add rewrite action test_refine_search replace_all http.res.body(10) '
    " testing_refine_search" ' -search text("abc") -refineSearch extend
    (1,1)
And the HTTP response body is abcxxxx456.

<!--NeedCopy-->
```

Ensuite, le paramètre de recherche trouve le motif « abc » et puisque le paramètre RefineSearch est également configuré pour vérifier un octet supplémentaire à gauche et un octet supplémentaire à droite du motif correspondant. Le texte remplacé qui en résulte est : abcx. Le résultat de cette action est donc `testing_refine_searchxxx456`.

Exemple 1 : Utilisation de la fonctionnalité Affiner la recherche dans le type d'action INSERT_BEFORE_ALL.

```
> add policy patset pat
Done
> bind policy patset pat abcd
Done
> add rewrite action refineSearch_act_1 insert_before_all http.res.body
    (10) 'target.prefix(10) + "refineSearch_testing"' -search patset("
    pat") -refineSearch extend(10,10)
Done
> sh rewrite action refineSearch_act_1
Name: refineSearch_act_1
Operation: insert_before_all
Target:http.res.body(10)
Refine Search:extend(10,10)
Value:target.prefix(10) + "refineSearch_testing"
Search: patset("pat")
Hits: 0
Undef Hits: 0
```



```
Action Reference Count: 0
Done

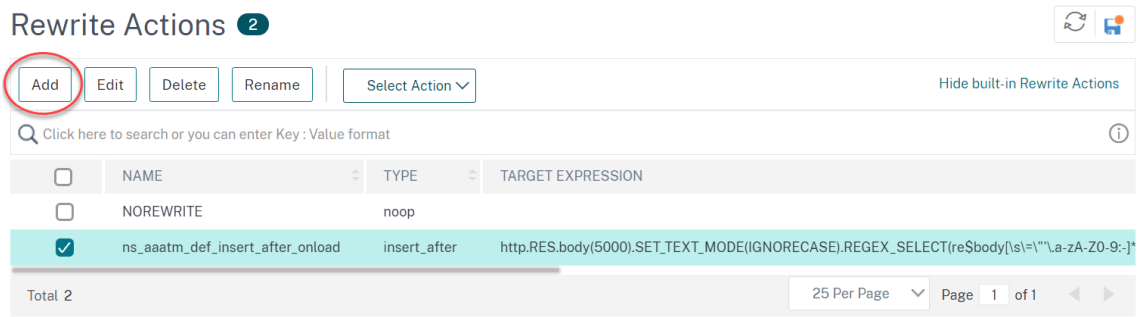
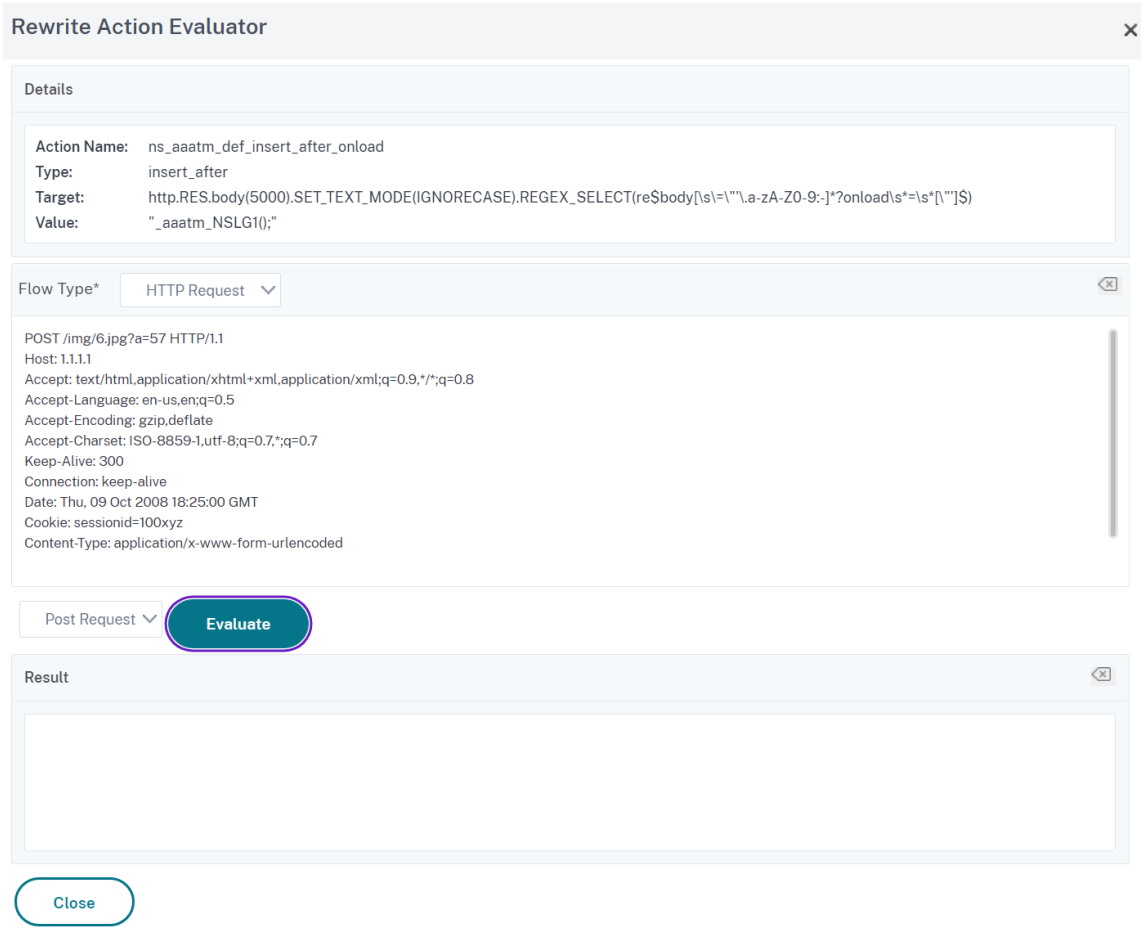
<!--NeedCopy-->
```

Exemple 2 : utilisation de la fonctionnalité Affiner la recherche dans le type d'action INSERT_AFTER_ALL.

```
> add rewrite action refineSearch_act_2 insert_after_all http.res.body
   (100) '"refineSearch_testing"' -search text("abc") -refineSearch
   extend(0, 10)
Done
> sh rewrite action refineSearch_act_2
Name: refineSearch_act_2
Operation: insert_after_all
Target:http.res.body(100)
Refine Search:extend(0, 10)
Value:"refineSearch_testing"
Search: text("abc")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Exemple 3 : utilisation de la fonctionnalité Affiner la recherche dans le type d'action REPLACE_ALL.

```
> add policy patset pat_list_2
Done
> bind policy patset pat_list_2 "www.abc.com"
Done
> bind policy patset pat_list_2 "www.def.com"
Done
> add rewrite action refineSearch_act_31 replace_all "HTTP.RES.BODY
   (100000)" ""https://"" -search "patset("pat_list_2")" -refineSearch
   "EXTEND(7,0).REGEX_SELECT(re#http://#)"
Done
> sh rewrite action refineSearch_act_31
Name: refineSearch_act_31
Operation: replace_all
Target:HTTP.RES.BODY(100000)
Refine Search:EXTEND(7,0).REGEX_SELECT(re#http://#)
Value:"https://"
```



```
Search: patset("pat_list_2")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Exemple 4 : utilisation de la fonctionnalité Affiner la recherche dans le type d'action DELETE_ALL.

```
>add rewrite action refineSearch_act_4 delete_all "HTTP.RES.BODY(50000)
   " -search text("Windows Desktops") -refineSearch "EXTEND(40,40).
   REGEX_SELECT(re#\s*<AppData>.\*\s\*<\\/AppData>#)"
> show REWRITE action refineSearch_act_4
Name: refineSearch_act_4
Operation: delete_all
Target:HTTP.RES.BODY(50000)
Refine Search:EXTEND(40,40).REGEX_SELECT(re#\s*<AppData>.\*\s\*</
   AppData>#)
Search: text("Windows Desktops")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Exemple 5 : utilisation de la fonctionnalité Affiner la recherche dans le type d'action CLIENTLESS_VPN_ENCODE_ALL.

"'

> ajout de l'action de réécriture act2 clientless_vpn_encode_all http.req.body (100) -search text (« abcd »)
> Effectuée action de réécriture
> sh act2
> Nom : act1
> Opération : clientless_vpn_encode_all
> Cible : http.req.body (100)
> Recherche : text (« abcd »)
> Hits : 0
> Undef Hits : 0
> Action Nombre de références : 0

> Terminé
>
> ”’

Exemple 6 : utilisation de la fonctionnalité Affiner la recherche dans le type d’action CLIENTLESS_VPN_DECODE_ALL.

```
> add rewrite action act1 clientless_vpn_decode_all http.req.body(100)
   -search text("abcd")
Done
> sh rewrite action act1
Name: act1
Operation: clientless_vpn_decode_all
Target:http.req.body(100)
Search: text("abcd")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Modifier une action de réécriture existante à l’aide de l’interface de ligne de commande

À l’invite de commandes, tapez les commandes suivantes pour modifier une action de réécriture existante et vérifier la configuration :

- `set rewrite action <name> [-target <expression>] [-stringBuilderExpr <expression>] [-search <expression>] [-refineSearch <expression>] [-comment <string>]`

À l’invite de commandes, tapez les commandes suivantes pour vérifier la configuration modifiée

- `show rewrite action <name>`

Exemple :

```
> set rewrite action insertact -target "Client-IP"
 Done
> show rewrite action insertact

Name: insertact
Operation: insert_http_header   Target:Client-IP
Value:CLIENT.IP.SRC
Hits: 0
```



```
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Supprimer une action de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour supprimer une action de réécriture :

```
rm rewrite action <name>
```

Exemple :

```
> rm rewrite action insertact
Done

<!--NeedCopy-->
```

Configurez une action de réécriture à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert > Rewrite > Actions**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une action, cliquez sur **Ajouter**.
   - Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Modifier**.
3. Cliquez sur **Créer** ou **sur OK**. Un message apparaît dans la barre d'état, indiquant que l'action a été correctement configurée.
4. Répétez les étapes 2 à 4 pour créer ou modifier autant d'actions de réécriture que vous le souhaitez.
5. Cliquez sur **Fermer**.



Ajouter une expression à l'aide de la boîte de dialogue Ajouter une expression

1. Dans la boîte de dialogue **Créer une action** de **réécriture ou Configurer une action** de réécriture, sous la zone de texte de l'argument de type que vous souhaitez entrer, cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Ajouter une expression**, dans la première zone de liste, choisissez le premier terme de votre expression.
   - HTTP. Le protocole HTTP. Choisissez cette option si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole HTTP.
   - SYS. Les sites Web protégés. Sélectionnez cette option si vous souhaitez examiner certains aspects de la demande qui concernent le destinataire de la demande.
   - CLIENT. L'ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'expéditeur de la demande.

Lorsque vous faites votre choix, la zone de liste la plus à droite répertorie les termes appropriés pour la partie suivante de votre expression.

1. Dans la deuxième zone de liste, choisissez le deuxième terme de votre expression. Les choix dépendent du choix que vous avez effectué à l'étape précédente et sont adaptés au contexte. Une fois que vous avez fait votre deuxième choix, la fenêtre d'aide située sous la fenêtre Construire une expression (qui était vide) affiche de l'aide décrivant le but et l'utilisation du terme que vous venez de choisir.
2. Continuez à choisir des termes dans les zones de liste qui apparaissent à droite de la zone de liste précédente, ou à taper des chaînes ou des nombres dans les zones de texte qui s'affichent pour vous inviter à entrer une valeur, jusqu'à ce que votre expression soit terminée.
   Pour plus d'informations sur le langage des expressions PI et la création d'expressions pour les stratégies de répondeur, voir « Policies and Expressions ». «

Si vous souhaitez tester l'effet d'une action de réécriture lorsqu'elle est utilisée sur des exemples de données HTTP, vous pouvez utiliser l'évaluateur de réécriture d'expression.

Réécriture des charges utiles TCP

Les expressions cibles des actions de réécriture TCP doivent commencer par l'un des préfixes d'expression suivants :

- **CLIENT.TCP.PAYLOAD.** Pour réécrire les charges utiles TCP dans les demandes des clients. Par exemple, CLIENT.TCP.PAYLOAD (10000) .AFTER_STR (« string1").
- **SERVER.TCP.PAYLOAD.** Pour réécrire les charges utiles TCP dans les réponses du serveur. Par exemple, SERVER.TCP.PAYLOAD (1000) .B64DECODE.BWEEN (« string1", "string2").

Évaluez une action de réécriture à l'aide de la boîte de dialogue Evaluateur d'actions de réécriture

1. Dans le volet de détails **Actions de réécriture**, sélectionnez l'action de réécriture que vous souhaitez évaluer, puis cliquez sur **Evaluer**.
2. Dans la boîte de dialogue Rewrite Expression Evaluator, spécifiez les valeurs des paramètres suivants. (Un astérisque indique un paramètre obligatoire.)

   Action de réécriture : si l'action de réécriture que vous souhaitez évaluer n'est pas déjà sélectionnée, sélectionnez-la dans la liste déroulante. Une fois que vous avez sélectionné une action de réécriture, la section Détails affiche les détails de l'action de réécriture sélectionnée.
   Nouveau : sélectionnez Nouveau pour ouvrir la boîte de dialogue Créer une action de réécriture et créer une action de réécriture.
   Modifier : sélectionnez Modifier pour ouvrir la boîte de dialogue Configurer l'action de réécriture et modifier l'action de réécriture sélectionnée.
   Type de flux : spécifie si l'action de réécriture sélectionnée doit être testée avec des données de demande HTTP ou de réponse HTTP. La valeur par défaut est Request. Si vous souhaitez effectuer un test avec les données de réponse, sélectionnez Réponse.
   Données de requête/réponse HTTP* : fournit un espace vous permettant de fournir les données HTTP que l'évaluateur d'action de réécriture est utilisé pour tester. Vous pouvez coller les données directement dans la fenêtre ou cliquer sur Exemple pour insérer des exemples d'en-têtes HTTP.
   Afficher la fin de ligne : spécifie si les caractères de fin de ligne de style UNIX (\ n) doivent être affichés à la fin de chaque ligne d'exemple de données HTTP.
   Exemple : insère des données HTTP d'exemple dans la fenêtre Données de requête/réponse HTTP. Vous pouvez choisir les données GET ou POST.
   Parcourir (Browse) : ouvre une fenêtre de navigation locale qui vous permet de choisir un fichier contenant des exemples de données HTTP à partir d'un emplacement local ou réseau.

Effacer (Clear) : efface les exemples de données HTTP actuels de la fenêtre Données de requête/réponse HTTP.

3. Cliquez sur Evaluer. L' **évaluateur d'action de réécriture** évalue l'effet de l'action Réécrire sur les données d'exemple que vous avez choisies et affiche les résultats tels que modifiés par l'action de **réécriture** sélectionnée dans la fenêtre **Résultats** . Les ajouts et suppressions sont mis en surbrillance comme indiqué dans la légende dans le coin inférieur gauche de la boîte de dialogue.
4. Continuez à évaluer les actions de réécriture jusqu'à ce que vous ayez déterminé que toutes vos actions ont l'effet souhaité.
    - Vous pouvez modifier l'action de réécriture sélectionnée et tester la version modifiée en cliquant sur **Modifier** pour ouvrir la boîte de dialogue **Configurer l'action de réécriture**, en effectuant et en enregistrant vos modifications, puis en cliquant à nouveau sur Evaluer.
    - Vous pouvez évaluer une action de réécriture différente à l'aide des mêmes données de demande ou de réponse en la sélectionnant dans la liste déroulante **Action de réécriture**, puis en cliquant à nouveau sur **Evaluer** .
5. Cliquez sur **Fermer** pour fermer l' **évaluateur d'expression de réécriture** et revenir au volet **Actions de réécriture** .
6. Pour supprimer une action de réécriture, sélectionnez l'action de réécriture à supprimer, puis cliquez sur **Supprimer** et, lorsque vous y êtes invité, confirmez votre choix en cliquant sur **OK**.



Configurer la stratégie de réécriture

Après avoir créé les actions de réécriture nécessaires, vous devez créer au moins une stratégie de réécriture pour sélectionner les demandes que l'appliance Citrix ADC doit réécrire.

Une stratégie de réécriture se compose d'une règle, elle-même composée d'une ou de plusieurs expressions, et d'une action associée qui est exécutée si une demande ou une réponse correspond à la règle. Les règles de stratégie d'évaluation des requêtes et réponses HTTP peuvent être basées sur presque n'importe quelle partie d'une demande ou d'une réponse.

Même si vous ne pouvez pas utiliser les actions de réécriture TCP pour réécrire des données autres que la charge utile TCP, vous pouvez baser les règles de stratégie pour les stratégies de réécriture TCP sur les informations de la couche de transport et des couches situées sous la couche de transport.

Si une règle configurée correspond à une demande ou à une réponse, la stratégie correspondante est déclenchée et l'action qui lui est associée est exécutée.

> **Remarque :**
>
> Vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique pour créer et

> configurer des stratégies de réécriture. Les utilisateurs qui ne connaissent pas parfaitement l'interface de ligne de commande et le langage d'expression de stratégie Citrix ADC trouveront généralement l'utilisation de l'interface graphique beaucoup plus facile.

Pour ajouter une nouvelle stratégie de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter une nouvelle stratégie de réécriture et vérifier la configuration :

- `<add rewrite policy <name> <expression> <action> [<undefaction>]`
- `<show rewrite policy <name>`

Exemple 1. Réécriture du contenu HTTP

```
> add rewrite policyNew "HTTP.RES.IS_VALID" insertact NOREWRITE
 Done
> show rewrite policyNew
        Name: policyNew
        Rule: HTTP.RES.IS_VALID
        RewriteAction: insertact
        UndefAction: NOREWRITE
        Hits: 0
        Undef Hits: 0

 Done
<!--NeedCopy-->
```

Exemple 2. Réécriture d'une charge utile TCP (réécriture TCP) :

```
> add rewrite policy client_tcp_payload_policy CLIENT.IP.SRC.EQ
   (172.168.12.232) client_tcp_payload_replace_all
 Done
> show rewrite policy client_tcp_payload_policy
        Name: client_tcp_payload_policy
        Rule: CLIENT.IP.SRC.EQ(172.168.12.232)
        RewriteAction: client_tcp_payload_replace_all
        UndefAction: Use Global
        LogAction: Use Global
        Hits: 0
        Undef Hits: 0

 Done
>
<!--NeedCopy-->
```

Pour modifier une stratégie de réécriture existante à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour modifier une stratégie de réécriture existante et vérifier la configuration :

- `<set rewrite policy <name> -rule <expression> -action <action> [<undefaction>]`
- `<show rewrite policy <name>`

Exemple :

```
> set rewrite policyNew -rule "HTTP.RES.IS_VALID" -action insertaction
 Done

> show rewrite policyNew
        Name: policyNew
        Rule: HTTP.RES.IS_VALID
        RewriteAction: insertaction
        UndefAction: NOREWRITE
        Hits: 0
        Undef Hits: 0

 Done
<!--NeedCopy-->
```

Pour supprimer une stratégie de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour supprimer une stratégie de réécriture :

```
rm rewrite policy <name>
```

Exemple :

```
> rm rewrite policyNew
Done
<!--NeedCopy-->
```

Pour configurer une stratégie de réécriture à l'aide de l'interface graphique

1. Accédez à **AppExpert > Rewrite > Policies**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une stratégie, cliquez sur Ajouter.
   - Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur Ouvrir.
3. Cliquez sur **Créer** ou **sur OK**. Un message apparaît dans la barre d'état indiquant que la stratégie a été configurée avec succès.
4. Répétez les étapes 2 à 4 pour créer ou modifier autant d'actions de réécriture que vous le souhaitez.

5. Cliquez sur **Fermer**. Pour supprimer une stratégie de réécriture, sélectionnez la stratégie de réécriture à supprimer, puis cliquez sur **Supprimer** et, lorsque vous y êtes invité, confirmez votre choix en cliquant sur **OK**.

Lier la stratégie de réécriture

Après avoir créé une stratégie de réécriture, vous devez la lier pour la mettre en œuvre. Vous pouvez lier votre stratégie à Global si vous souhaitez l'appliquer à tout le trafic qui passe par votre Citrix ADC, ou vous pouvez lier votre stratégie à un serveur virtuel ou à un point de liaison spécifique pour diriger uniquement ce serveur virtuel ou lier le trafic entrant du point à cette stratégie. Si une demande entrante correspond à une stratégie de réécriture, l'action associée à cette stratégie est exécutée.

Les stratégies de réécriture pour l'évaluation des requêtes et réponses HTTP peuvent être liées à des serveurs virtuels de type HTTP ou SSL, ou elles peuvent être liées aux points de liaison REQ_OVERRIDE,
REQ_DEFAULT, RES_OVERRIDE et RES_DEFAULT. Les stratégies de réécriture pour la réécriture TCP peuvent être liées uniquement aux serveurs virtuels de type TCP ou SSL_TCP, ou aux points de liaison OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE et OTHERTCP_RES_DEFAULT.

> **Remarque :**
>
> Le terme OTHERTCP est utilisé dans le contexte de l'appliance Citrix ADC pour désigner toutes les demandes et réponses TCP ou SSL_TCP que vous souhaitez traiter comme un flux brut d'octets, quels que soient les protocoles encapsulés par les paquets TCP.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel nombre entier positif.

Dans le système d'exploitation Citrix ADC, les priorités de stratégie fonctionnent dans l'ordre inverse : plus le nombre est élevé, plus la priorité est faible. Par exemple, si vous avez trois stratégies avec des priorités de 10, 100 et 1000, la stratégie affectée d'une priorité de 10 est appliquée en premier, puis la stratégie affectée une priorité de 100 et enfin la stratégie affectée d'un ordre de 1000.

Contrairement à la plupart des autres fonctionnalités du système d'exploitation Citrix ADC, la fonctionnalité de réécriture continue d'évaluer et d'implémenter des stratégies une fois qu'une demande correspond à une stratégie. Toutefois, l'effet d'une stratégie d'action particulière sur une demande ou une réponse sera souvent différent selon qu'elle est exécutée avant ou après une autre action. La priorité est importante pour obtenir les résultats escomptés.

Vous pouvez vous laisser suffisamment de place pour ajouter d'autres stratégies dans n'importe quel ordre, tout en les définissant pour qu'elles soient évaluées dans l'ordre souhaité, en définissant des priorités avec des intervalles de 50 ou 100 entre chaque stratégie lorsque vous la liez. Dans ce cas, vous

pouvez ajouter d'autres stratégies à tout moment sans avoir à réattribuer la priorité d'une stratégie existante.

Lorsque vous liez une stratégie de réécriture, vous avez également la possibilité d'affecter une expression goto (GoToPriorityExpression) à la stratégie. Une expression goto peut être n'importe quel entier positif correspondant à la priorité attribuée à une autre stratégie dont la priorité est supérieure à celle qui contient l'expression goto. Si vous affectez une expression goto à une stratégie et qu'une demande ou une réponse correspond à la stratégie, Citrix ADC va immédiatement accéder à la stratégie dont la priorité correspond à l'expression goto. Il ignore toutes les stratégies dont les numéros de priorité sont inférieurs à ceux de la stratégie actuelle, mais supérieurs au numéro de priorité de l'expression goto, et n'évalue pas ces stratégies.

Pour lier globalement une stratégie de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier globalement une stratégie de réécriture et vérifier la configuration :

- `bind rewrite global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>] [-invoke (<labelType> <labelName>)]`
- `show rewrite global`

Exemple :

```
>bind rewrite global policyNew 10
 Done

> show rewrite global
1)      Global bindpoint: RES_DEFAULT
        Number of bound policies: 1

2)      Global bindpoint: REQ_OVERRIDE
        Number of bound policies: 1

 Done
<!--NeedCopy-->
```

Pour lier la stratégie de réécriture à un serveur virtuel spécifique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier la stratégie de réécriture à un serveur virtuel spécifique et vérifier la configuration :

- `bind lb vserver <name>@ (<serviceName>@ [-weight <positive_integer>])| <serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>)] )`

- show lb vserver <name>

Exemple :

```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 50
 Done
>
> show lb vserver lbvip
        lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jul 15 05:54:24 2009 (+226 ms)
        Time since last state change: 28 days, 01:57:26.350
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1)      Policy : ns_cmp_msapp Priority:50
2)      Policy : cf-pol Priority:1      Inherited
 Done
<!--NeedCopy-->
```

Pour lier une stratégie de réécriture à un point de liaison à l'aide de l'interface graphique

1. Accédez à **AppExpert** >**Réécriture** > **Stratégies**.
2. Dans le volet d'informations, sélectionnez la stratégie de réécriture que vous souhaitez lier globalement, puis cliquez sur **Gestionnaire de stratégies**.
3. Dans la boîte de dialogue **Gestionnaire de stratégies de réécriture**, dans le menu **Points de liaison**, effectuez l'une des opérations suivantes :
   a) Si vous souhaitez configurer des liaisons pour les stratégies de réécriture HTTP, cliquez sur **HTTP**, puis sur **Demande** ou **Réponse**, selon que vous souhaitez configurer des stratégies de réécriture basées sur les demandes ou des stratégies de réécriture basées sur les réponses.
   b) Si vous souhaitez configurer des liaisons pour les stratégies de réécriture TCP, cliquez sur **TCP**, puis sur **Client** ou **Serveur**, selon que vous souhaitez configurer des stratégies de

réécriture TCP côté client ou des stratégies de réécriture TCP côté serveur.

4. Cliquez sur le point de liaison auquel vous souhaitez lier la stratégie de réécriture. La boîte de dialogue **Gestionnaire de stratégies** de réécriture affiche toutes les stratégies de réécriture liées au point de liaison sélectionné.
5. Cliquez sur **Insérer une stratégie** pour insérer une nouvelle ligne et afficher une liste déroulante contenant toutes les stratégies de réécriture disponibles et non liées.
6. Cliquez sur la stratégie que vous souhaitez lier au point de liaison. La stratégie est insérée dans la liste des stratégies de réécriture liées au point de liaison.
7. Dans la colonne **Priorité**, vous pouvez modifier la priorité par n'importe quel entier positif. Pour plus d'informations sur ce paramètre, reportez-vous à la section Priorité dans « Paramètres de liaison d'une stratégie de réécriture. «
8. Si vous souhaitez ignorer les stratégies et accéder directement à une stratégie spécifique si la stratégie actuelle est appariée, modifiez la valeur de la colonne Goto Expression pour qu'elle corresponde à la priorité de la prochaine stratégie à appliquer. Pour plus d'informations sur ce paramètre, consultez GoToPriorityExpression dans « Paramètres de liaison d'une stratégie de réécriture ». «
9. Pour modifier une stratégie, cliquez sur la stratégie, puis cliquez sur **Modifier la stratégie**.
10. Pour délier une stratégie, cliquez sur la stratégie, puis cliquez sur **Délier la stratégie**.
11. Pour modifier une action, dans la colonne Action, cliquez sur l'action que vous souhaitez modifier, puis cliquez sur **Modifier l'action**.
12. Pour modifier une étiquette d'appel, dans la colonne **Invoke**, cliquez sur l'étiquette d'appel que vous souhaitez modifier, puis cliquez sur **Modifier le libellé d'appel**.
13. Pour régénérer les priorités de toutes les stratégies liées au point de liaison que vous configurez actuellement, cliquez sur **Régénérer les priorités**. Les politiques conservent leurs priorités existantes par rapport aux autres politiques, mais les priorités sont renumérotées par multiples de 10.
14. Cliquez sur **Appliquer les modifications**.
15. Cliquez sur **Fermer**. Un message apparaît dans la barre d'état indiquant que la stratégie a été configurée avec succès.

Pour lier une stratégie de réécriture à un serveur virtuel spécifique à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans la liste des serveurs virtuels du volet d'informations, sélectionnez le serveur virtuel auquel vous souhaitez lier la stratégie de réécriture, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le serveur virtuel (équilibrage de charge)**, sélectionnez l'onglet **Stratégies** . Toutes les stratégies configurées sur votre Citrix ADC apparaissent dans la liste.
4. Cochez la case en regard du nom de la stratégie que vous souhaitez lier à ce serveur virtuel.
5. Cliquez sur **OK**. Un message apparaît dans la barre d'état indiquant que la stratégie a été configurée avec succès.

Configuration des étiquettes de stratégie de réécriture

Si vous souhaitez créer une structure de stratégie plus complexe que celle prise en charge par des stratégies uniques, vous pouvez créer des étiquettes de stratégie, puis les lier comme vous le feriez pour les stratégies. Une étiquette de stratégie est un point défini par l'utilisateur auquel les stratégies sont liées. Lorsqu'une étiquette de stratégie est appelée, toutes les stratégies qui lui sont liées sont évaluées dans l'ordre de priorité que vous avez configuré. Un libellé de stratégie peut inclure une ou plusieurs stratégies, chacune pouvant se voir attribuer son propre résultat. Une correspondance sur une stratégie dans l'étiquette de stratégie peut entraîner la poursuite de la stratégie suivante, l'appel d'un autre libellé de stratégie ou d'une ressource appropriée, ou la fin immédiate de l'évaluation de la stratégie et le retour du contrôle à la stratégie qui a appelé l'étiquette de stratégie.

Une étiquette de stratégie de réécriture se compose d'un nom, d'un nom de transformation qui décrit le type de stratégie inclus dans l'étiquette de stratégie et d'une liste de stratégies liées à l'étiquette de stratégie. Chaque stratégie liée à l'étiquette de stratégie contient tous les éléments décrits dans Configuration d'une stratégie de réécriture.

Remarque : Vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique pour créer et configurer des étiquettes de stratégie de réécriture. Les utilisateurs qui ne connaissent pas parfaitement l'interface de ligne de commande et le langage Citrix ADC Policy Infrastructure (PI) trouvent généralement l'interface graphique beaucoup plus facile.

Pour configurer une étiquette de stratégie de réécriture à l'aide de l'interface de ligne de commande

Pour ajouter une étiquette de stratégie de réécriture, à l'invite de commandes, tapez la commande suivante :

```
add rewrite policylabel <labelName> <transform>
```

Par exemple, pour ajouter une étiquette de stratégie de réécriture nommée PollabelHttpResponses afin de regrouper toutes les stratégies qui fonctionnent sur les réponses HTTP, vous devez taper ce qui suit :

```
add rewrite policy label polLabelHTTPResponses http_res
```

Pour modifier une étiquette de stratégie de réécriture existante, à l'invite de commandes **Citrix ADC**, tapez la commande suivante :

```
set rewrite policy <name> <transform>
```

> **Remarque :**
>
> La commande set rewrite policy utilise les mêmes options que la commande add rewrite policy.

Pour supprimer une étiquette de stratégie de réécriture, à l'invite de commandes **Citrix ADC**, tapez la commande suivante :

```
rm rewrite policy<name>
```


Par exemple, pour supprimer une étiquette de stratégie de réécriture nommée PollabelHttpResponses, vous devez taper ce qui suit :

```
rm rewrite policy polLabelHTTPResponses
```

Pour configurer une étiquette de stratégie de réécriture à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Réécriture** > **Étiquettes de stratégie**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une étiquette de stratégie, cliquez sur **Ajouter**.
   - Pour modifier une étiquette de stratégie existante, sélectionnez la stratégie, puis cliquez sur **Ouvrir**.
3. Ajoutez ou supprimez des stratégies de la liste liée à l'étiquette de stratégie.
   - Pour ajouter une stratégie à la liste, cliquez sur **Insérer une stratégie**, puis choisissez une stratégie dans la liste déroulante. Vous pouvez créer une stratégie et l'ajouter à la liste en choisissant Nouvelle stratégie dans la liste, puis en suivant les instructions de la section Configuration d'une stratégie de réécriture.
   - Pour supprimer une stratégie de la liste, sélectionnez-la, puis cliquez sur Annuler la stratégie.
4. Modifiez la priorité de chaque stratégie en modifiant le nombre dans la colonne Priorité.
   Vous pouvez également renuméroter automatiquement les stratégies en cliquant sur Régénérer les priorités.
5. Cliquez sur **Créer** ou sur **OK**, puis cliquez sur **Fermer**.
   Pour supprimer une étiquette de stratégie, sélectionnez-la, puis cliquez sur **Supprimer**. Pour renommer une étiquette de stratégie, sélectionnez-la, puis cliquez sur **Renommer**. Modifiez le nom de la stratégie, puis cliquez sur **OK** pour enregistrer vos modifications.

Réécrire des exemples d'action et de stratégie

January 21, 2021

Les exemples de cette section montrent comment configurer la réécriture pour effectuer diverses tâches utiles. Ces exemples se trouvent dans la salle des serveurs d'Example Manufacturing Inc., une entreprise de fabrication de taille moyenne qui utilise son site Web pour gérer une partie considérable de ses ventes, de ses livraisons et de son support client.

Exemple de fabrication comporte deux domaines : example.com pour son site Web et le courrier électronique aux clients, et exemple.net pour son intranet. Les clients utilisent le site Web Exemple pour passer des commandes, demander des devis, rechercher des produits et contacter le service à la clientèle et le support technique.

En tant que partie importante du flux de revenus d'Example, le site Web doit répondre rapidement et

préserver la confidentialité des données des clients. Exemple a donc plusieurs serveurs Web et utilise les appliances Citrix ADC pour équilibrer la charge du site Web et gérer le trafic à destination et en provenance de ses serveurs Web.

Les administrateurs système Exemple utilisent les fonctionnalités de réécriture pour effectuer les tâches suivantes :

Exemple 1 : Supprimer les anciens en-têtes X-Forwarded-For et client-IP

Example Inc. supprime les anciens en-têtes HTTP X-Forwarded-For et Client-IP des requêtes entrantes.

Exemple 2 : Ajout d'un en-tête IP client local

Example Inc. ajoute un nouvel en-tête local Client-IP aux requêtes entrantes.

Exemple 3 : Marquage des connexions sécurisées et non sécurisées

Exemple Inc. marque les demandes entrantes avec un en-tête indiquant si la connexion est une connexion sécurisée.

Exemple 4 : Masquer le type de serveur HTTP

Example Inc. modifie l'en-tête HTTP Server : afin que les utilisateurs non autorisés et le code malveillant ne puissent pas utiliser cet en-tête pour déterminer le logiciel du serveur HTTP qu'il utilise.

Exemple 5 : Rediriger une URL externe vers une URL interne

Example Inc. cache aux utilisateurs des informations sur les noms réels de ses serveurs Web et la configuration de sa salle de serveurs, afin de raccourcir et de faciliter la mémorisation des URL de son site Web et d'améliorer la sécurité de son site.

Exemple 6 : Migration des règles du module de réécriture Apache

Example Inc. a déplacé ses règles de réécriture Apache vers une appliance Citrix ADC, traduisant la syntaxe de script Apache Perl en syntaxe de règle de réécriture Citrix ADC.

Exemple 7 : Redirection de mots-clés marketing

Le service marketing d'Example Inc. met en place des URL simplifiées pour certaines recherches de mots clés prédéfinies sur le site Web de l'entreprise.

Exemple 8 : Rediriger les requêtes vers le serveur interrogé.

Example Inc. redirige certaines requêtes de requête vers le serveur approprié.

Exemple 9 : Redirection de la page d'accueil

Example Inc. a récemment acquis un concurrent plus petit, et elle redirige maintenant les demandes vers la page d'accueil de l'entreprise acquise vers une page de son propre site Web.

Exemple 10 : chiffrement RSA basé sur des règles

Example Inc. crypte le contenu d'en-tête ou de corps HTTP prédéfini et défini par l'utilisateur à l'aide de la clé publique PEM RSA.

Chacune de ces tâches nécessite que les administrateurs système créent des actions et des stratégies de réécriture et les lient à un point de liaison valide sur Citrix ADC.

Exemple 1 : supprimer les anciens en-têtes X-Forwarded-For et client-IP

August 20, 2021

Example Inc. souhaite supprimer les anciens en-têtes HTTP X-Forwarded-For et Client-IP des requêtes entrantes, de sorte que les seuls en-têtes X-Forwarded-For qui apparaissent soient ceux ajoutés par le serveur local. Cette configuration peut être effectuée via la ligne de commande Citrix ADC ou l'utilitaire de configuration. L'administrateur système Example Inc. est un ingénieur réseau ancien et préfère utiliser une interface CLI dans la mesure du possible, mais veut s'assurer qu'il comprend l'interface de l'utilitaire de configuration afin qu'il puisse montrer aux nouveaux administrateurs système de l'équipe comment l'utiliser.

Les exemples ci-dessous montrent comment effectuer chaque configuration avec l'interface de ligne de commande et l'utilitaire de configuration. Les procédures sont abrégées en supposant que les utilisateurs connaissent déjà les bases de la création d'actions de réécriture, de la création de stratégies de réécriture et des stratégies de liaison.

- Pour plus d'informations sur la création d'actions de réécriture, voir Configuration d'une action de réécriture.
- Pour plus d'informations sur la création de stratégies de réécriture, voir Configuration d'une stratégie de réécriture.
- Pour plus d'informations sur les stratégies de réécriture de liaison, voir Liaison d'une stratégie de réécriture.

Pour supprimer les anciens en-têtes X-Forwarded et Client-IP d'une requête à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes dans l'ordre indiqué :

```
1 add rewrite action act_del_xfor delete_http_header x-forwarded-for
2 add rewrite action act_del_cip delete_http_header client-ip
3 add rewrite policy pol_check_xfor 'HTTP.REQ.HEADER("x-forwarded-for").
     EXISTS' act_del_xfor
4 add rewrite policy pol_check_cip 'HTTP.REQ.HEADER("client-ip").EXISTS'
     act_del_cip
5 bind rewrite global pol_check_xfor 100 200
```



```
6 bind rewrite global pol_check_cip 200 300
7 <!--NeedCopy-->
```

Pour supprimer les anciens en-têtes X-Forwarded et Client-IP d'une requête à l'aide de l'utilitaire de configuration

Dans la boîte de dialogue Créer une action de réécriture, créez deux actions de réécriture avec les descriptions suivantes.

Nom	Type	Argument(s)
act_del_xfor	delete_http_header	x-transmet-pour
act_del_cip	delete_http_header	client-ip

Dans la boîte de dialogue Créer une stratégie de réécriture, créez deux stratégies de réécriture avec les descriptions suivantes.

Nom	Expression.	Action
pol_check_xfor	'HTTP.REQ.HEADER("x-forwarded-for").EXISTS'	act_del_xfor
pol_check_cip	'HTTP.REQ.HEADER("client-ip").EXISTS'	act_del_cip

Liez les deux stratégies à global, en attribuant les priorités et les valeurs d'expression goto indiquées ci-dessous.

Nom	Priority	Goto Expression
pol_check_xfor	100	200
pol_check_cip	200	300

Tous les anciens en-têtes HTTP X-Forwarded-For et Client-IP sont maintenant supprimés des requêtes entrantes.

Exemple 2 : Ajout d'un en-tête IP client local

August 20, 2021

Example Inc. souhaite ajouter un en-tête HTTP Client-IP local aux requêtes entrantes. Cet exemple contient deux versions légèrement différentes de la même tâche de base.

Pour ajouter un en-tête Client-IP local à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes dans l'ordre indiqué :

```
1 add rewrite action act_ins_client insert_http_header NS-Client 'CLIENT.
     IP.SRC'
2 add rewrite policy pol_ins_client 'HTTP.REQ.HEADER("x-forwarded-for").
     EXISTS || HTTP.REQ.HEADER("client-ip").EXISTS' act_ins_client
3 bind rewrite global pol_ins_client 300 END
4 <!--NeedCopy-->
```

Pour ajouter un en-tête Client-IP local à l'aide de l'utilitaire de configuration

Dans la boîte de dialogue Créer une action de réécriture, créez une action de réécriture avec la description suivante.

Nom	Type	Argument(s)
act_ins_client	insert_http_header	NS-Client 'CLIENT .IP.SRC'

Dans la boîte de dialogue Créer une stratégie de réécriture, créez une stratégie de réécriture avec la description suivante.

Nom	Expression.	Action
pol_ins_client	'HTTP.REQ.HEADER (« x-forwarded-for ») .EXISTS || HTTP.REQ.HEADER (« client-ip ») .EXISTS'	act_ins_client

Liez la stratégie à globale, en affectant les priorités et les valeurs d'expression goto indiquées ci-dessous.

Nom	Priority	Goto Expression
pol_ins_client	100	Suivant

Exemple 3 : Marquage des connexions sécurisées et non sécurisées

August 20, 2021

Example Inc. souhaite marquer les demandes entrantes avec un en-tête indiquant si la connexion est une connexion sécurisée ou non. Cela permet au serveur de suivre les connexions sécurisées après que le Citrix ADC a déchiffré les connexions.

Pour implémenter cette configuration, vous devez commencer par créer des actions de réécriture avec les valeurs indiquées dans les tableaux suivants. Ces actions étiquettent les connexions au port 80 comme des connexions non sécurisées et les connexions au port 443 comme des connexions sécurisées.

Nom de l'action	Type d'action de réécriture	Nom de l'en-tête	Valeur
Action-Rewrite-SSL_YES	INSERT_HTTP_HEADER	SSL	OUI

Nom de l'action	Type d'action de réécriture	Nom de l'en-tête	Valeur
Action-Rewrite-SSL_NO	INSERT_HTTP_HEADER	SSL	NON

Vous devez ensuite créer une stratégie de réécriture avec les valeurs indiquées dans les tableaux suivants. Ces stratégies vérifient les demandes entrantes pour déterminer quelles sont les demandes dirigées vers le port 80 et celles dirigées vers le port 443. Les stratégies ajoutent ensuite l'en-tête SSL correct.

Nom de la stratégie	Nom de l'action	Action non définie	Expression.
Policy-Rewrite-SSL_YES	Action-Rewrite-SSL_YES	NOREWRITE	CLIENT.TCP.DSTPORT.EQ (443)

Nom de la stratégie	Nom de l'action	Action non définie	Expression.
Policy-Rewrite-SSL_NO	Action-Rewrite-SSL_NO	NOREWRITE	CLIENT.TCP.DSTPORT.EQ(80)

Enfin, vous devez lier les stratégies de réécriture à Citrix ADC, en attribuant à la première stratégie une priorité de 200 et à la seconde une priorité de 300, et en définissant l'expression goto des deux stratégies sur END.

Chaque connexion entrante au port 80 a maintenant un en-tête HTTP SSL:NO ajouté et chaque connexion entrante au port 443 a un en-tête HTTP SSL:YES ajouté.

Exemple 4 : masquer le type de serveur HTTP

October 5, 2021

Example Inc. souhaite modifier l'en-tête HTTP Server : afin que les utilisateurs non autorisés et le code malveillant ne puissent pas utiliser cet en-tête pour identifier le logiciel utilisé par le serveur HTTP.

Pour modifier l'en-tête HTTP Server :, vous devez créer une action de réécriture et une stratégie de réécriture avec les valeurs des tableaux suivants.

Nom de l'action	Type d'action de réécriture	Expression pour choisir la référence cible	Expression de chaîne pour le texte de remplacement
Masque_serveur Action-Réécriture	REMPLACER	HTTP.RES.HEADER (« Serveur »)	« Serveur Web 1.0 »

Nom de la stratégie	Nom de l'action	Action non définie	Expression.
Policy-Rewrite-Server_Mask	Masque_serveur Action-Réécriture	NOREWRITE	HTTP.RES.IS_VALID

Exemples de commandes :

```
> add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER("
Server")"\"Web Server 1.0\""
```

```
> add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-
```


`Server_Mask NOREWRITE`

Vous liez ensuite globalement la stratégie de réécriture, en attribuant une priorité de 100 et en définissant l'expression de priorité Goto de la stratégie sur END.

L'en-tête HTTP Server : est maintenant modifié pour lire « Web Server 1.0 », masquant le logiciel de serveur HTTP utilisé par le site Web Example Inc.

Exemple 5 : rediriger une URL externe vers une URL interne

October 5, 2021

Example Inc. souhaite masquer la configuration de sa salle de serveurs aux utilisateurs afin d'améliorer la sécurité de ses serveurs Web.

Pour ce faire, vous devez créer une action de réécriture avec les valeurs indiquées dans les tableaux suivants. Pour les en-têtes de demande, l'action de la table est modifiée `www.example.com` en web.hq.example.net. Pour les en-têtes de réponse, l'action fait l'inverse, en se traduisant par `web.hq.example.netwww.example.com`.

Nom de l'action	Type d'action de réécriture	Expression pour choisir la référence cible	Expression de chaîne pour le texte de remplacement
Action-Réécriture-Request_Server_Repla	REMPLACER	HTTP.REQ.HOSTNAME.S	« Web.HQ.Example.net »
Action-Réécriture-Response_Server_Replace	REMPLACER	HTTP.RES.HEADER (« Serveur »)	« www.example.com »

La première stratégie vérifie les demandes entrantes pour voir si elles sont valides, et si elles le sont, elle exécute l'action Action-Rewrite-Request_Server_Replace. La deuxième stratégie vérifie les réponses pour vérifier si elles proviennent du serveur `web.hq.example.net`. Si tel est le cas, il exécute l'action Action-Rewrite-Response_Server_Replace.

Exemples d'actions de réécriture et de stratégie de redirection d'une URL externe.

```
add rewrite action Action-Rewrite-Request_Server_Replace REPLACE HTTP.REQ.
HOSTNAME.SERVER '"Web.hq.example.net"
```

```
add rewrite action Action-Rewrite-Response_Server_Replace REPLACE HTTP.RES.
HEADER("Server")'"www.example.com"'
```

```
add rewrite policy-Rewrite-Request_Server_Replace HTTP.REQ.HOSTNAME.SERVER.
```



```
EQ("www.example.com")Action-Rewrite-Request_Server_Replace NOREWRITE

add rewrite policy-Rewrite-Response_Server_Replace HTTP.REQ.HEADER("Server"
).EQ("Web.hq.example.net")Action-Rewrite-Response_Server_Replace
```

Enfin, vous liez les stratégies de réécriture, en attribuant à chacune une priorité de 500, car elles se trouvent dans des banques de stratégies différentes et ne sont donc pas en conflit. Vous devez définir l'expression goto sur NEXT pour les deux liaisons.

```
bind rewrite global Policy-Rewrite-Request_Server_Replace 500 END -type
REQ_DEFAULT

bind rewrite global Policy-Rewrite-Response_Server_Replace 500 END -type
RES_DEFAULT
```

Toutes les instances de `www.example.com` dans les en-têtes de requête sont désormais remplacées par `web.hq.example.net`, et toutes les instances `web.hq.example.net` des en-têtes de réponse sont désormais remplacées par `www.example.com`.

Exemple 6 : Migration des règles du module de réécriture Apache

October 5, 2021

Example Inc., utilise actuellement le module de réécriture Apache pour traiter les demandes de recherche envoyées à ses serveurs Web et les rediriger vers le serveur approprié sur la base des informations contenues dans l'URL de la requête. Example Inc. souhaite simplifier sa configuration en migrant ces règles sur la plate-forme Citrix ADC.

Plusieurs règles de réécriture Apache que Example utilise actuellement sont présentées ci-dessous. Ces règles redirigent les demandes de recherche vers une page de résultats spéciale si elles n'ont pas de chaîne SiteID ou si elles ont une chaîne SiteID égale à zéro (0), ou vers la page de résultats standard si ces conditions ne s'appliquent pas.

Voici les règles de réécriture Apache actuelles :

- RewriteCond% {REQUEST_FILENAME} ^/recherche$ [NC]
- RewriteCond% {QUERY_STRING} ! SiteID = [OU]
- RewriteCond %{QUERY_STRING} SiteId=0
- RewriteCond %{QUERY_STRING} CallName=DisplayResults [NC]
- RewriteRule ^.*$ results2.html [PL,]
- RewriteCond %{REQUEST_FILENAME} ^/search$ [NC]
- RewriteCond %{QUERY_STRING} CallName=DisplayResults [NC]
- RewriteRule ^.*$ /results.html [PL,]

Pour implémenter ces règles de réécriture Apache sur Citrix ADC, vous devez créer des actions de réécriture avec les valeurs indiquées dans les tableaux suivants.

Nom de l'action	Type d'action de réécriture	Expression pour choisir la référence cible	Expression de chaîne pour le texte de remplacement
Action-Rewrite-Display_Results_NulSit	REPLACE	HTTP.REQ.URL	"/results2.html"
Action-Rewrite-Display_Results	REPLACE	HTTP.REQ.URL	"/results2.html"

Vous devez ensuite créer des stratégies de réécriture avec les valeurs indiquées dans les tableaux ci-dessous.

Nom de la stratégie	Nom de l'action	Action non définie	Expression.
Policy-Rewrite-Display_Re	Action-Rewrite-Display_Re	NOREWRITI	HTTP.REQ.l && (!HTTP.REQ HTTP.REQ.l HTTP.REQ.URL.QUERY.S
Politique_Réécriture-Display_Results	Action-Rewrite-Display_Results	NOREWRITE	HTTP.REQ.URL.PATH.SET_TEXT_MODE(IGNORECASE).REPLACE_ALL("/results.html" "/results2.html").HTTP.REQ.URL.SET_TEXT_MODE(IGNORE

Enfin, vous devez lier les stratégies de réécriture, en attribuant à la première une priorité de 600 et à la seconde une priorité de 700, puis définir l'expression goto sur NEXT pour les deux liaisons.

Citrix ADC gère désormais ces requêtes de recherche exactement comme le serveur Web l'a fait avant la migration des règles du module de réécriture Apache.

Exemple 7 : Redirection de mots-clés marketing

August 20, 2021

Le service marketing d'Example Inc. souhaite mettre en place des URL simplifiées pour certaines recherches de mots clés prédéfinies sur le site Web de l'entreprise. Pour ces mots-clés, il veut redéfinir l'URL comme indiqué ci-dessous.

- URL externe :

```
http://www.example.com/\<marketingkeyword\>
```

- URL interne :

```
http://www.example.com/go/kwsearch.asp?keyword=\<marketingkeyword\>
```

Pour configurer la redirection pour les mots-clés marketing, vous devez créer une action de réécriture avec les valeurs du tableau suivant.

Nom de l'action	Type d'action de réécriture	Expression pour choisir l'emplacement cible	Expression de chaîne pour le texte de remplacement
Action-réécriture-modify_URL	INSERT_BEFORE	HTTP.REQ.URL.PATH.GE (1)	””go/kwsearch.aspkeyword=”l”

Vous devez ensuite créer une stratégie de réécriture avec les valeurs du tableau suivant.

Nom de la stratégie	Nom de l'action	Action non définie	Expression.
Policy-Rewrite-Modify_URL	Action-réécriture-modify_URL	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ(“v

Enfin, vous devez lier la stratégie de réécriture, en lui attribuant une priorité de 800. Contrairement aux stratégies de réécriture précédentes, cette stratégie doit être la dernière à appliquer à une demande qui correspond à ses critères. Pour cette raison, l'administrateur Citrix ADC définit son expression de priorité Goto sur END.

Toute demande utilisant un mot clé marketing est redirigée vers la page CGI de recherche par mot clé, après quoi une recherche est effectuée et toutes les stratégies restantes sont ignorées.

Exemple 8 : Redirection des requêtes vers le serveur interrogé

October 5, 2021

Example Inc. souhaite rediriger les demandes de requête vers le serveur approprié, comme illustré ici.

- <Request: GET /query.cgi?server=5HOST: www.example.com
- <Redirect URL: <http://web-5.example.com/>

Pour implémenter cette redirection, vous devez d'abord créer une action de réécriture avec les valeurs du tableau suivant.

Nom de l'action	Type d'action de réécriture	Expression pour choisir la référence cible	Expression de chaîne pour le texte de remplacement
Action-Réécriture-Replace_Hostheader	REMPLACER	HTTP.REQ.HEADER (« Hôte ») .BEFORE_STR (« .example.com »)	« serveur- » + HTTP.REQ.URL.QUERY.VALUE (« web »)

Vous devez ensuite créer une stratégie de réécriture avec les valeurs du tableau suivant.

Nom de la stratégie	Nom de l'action	Action non définie	Expression.
`Policy-Rewrite-Replace_Hostheader`	`Action-Rewrite-Replace_Hostheader`	NOREWRITE	`HTTP.REQ.HEADER("Host").EQ("www.example.com")`

Exemples de commandes :

```
> add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER("Server")"\"Web Server 1.0\""
Done
```

```
> add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
Done
```

Enfin, vous liez la stratégie de réécriture en lui attribuant une priorité de 900. Comme cette stratégie doit être la dernière stratégie appliquée à une demande qui correspond à ses critères, vous définissez l'expression goto sur END.

Les demandes entrantes vers n'importe quelle URL commençant par `<http://www.example.com/query.cgi?server>=` sont redirigées vers le numéro de serveur figurant dans la requête.

Exemple 9 : Redirection de la page d'accueil

August 20, 2021

New Company, Inc. a récemment acquis un concurrent plus petit, Acheté Company, et souhaite rediriger la page d'accueil de la société Acheté vers une nouvelle page de son propre site Web, comme indiqué ici.

- Ancienne URL :http://www.purchasedcompany.com/*
- Nouvelle URL :http://www.newcompany.com/products/page.htm

Pour rediriger les demandes vers la page d'accueil Entreprise achetée, vous devez créer des actions de réécriture avec les valeurs du tableau suivant.

Nom de l'action	Type d'action de réécriture	Expression pour choisir la référence cible	Expression de chaîne pour le texte de remplacement
Action-Rewrite-Replace_URLr	REPLACE	HTTP.REQ.URL.PATH_A	"/products/page.htm"
Action-Rewrite-Replace_Host	REPLACE	HTTP.REQ.HOSTNAME	« www.newcompany.com »

Vous devez ensuite créer des stratégies de réécriture avec les valeurs du tableau suivant.

Nom de la stratégie	Nom de l'action	Action non définie	Expression.
Policy-Rewrite-Replace-None	Action-Rewrite-Replace-None	NOREWRITE	!HTTP.REQ.HOSTNAME.SERVER.EQ("
Policy-Rewrite-Replace-Host	Action-Rewrite-Replace_Host	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ("v
Policy-Rewrite-Replace-URL	Action-Rewrite-Replace_URL	NOREWRITE	HTTP.REQ.IS_VALID

Enfin, vous devez lier globalement les stratégies de réécriture, en attribuant à la première une priorité de 100, à la seconde une priorité de 200 et à la troisième une priorité de 300. Ces stratégies doivent être les dernières stratégies appliquées à une demande qui correspond aux critères. Pour cette raison, définissez l'expression goto sur END pour les première et troisième stratégies, et sur 300 pour la deuxième stratégie. Cela garantit que toutes les demandes restantes sont traitées correctement.

Les demandes adressées à l'ancien site Web de l'entreprise acquise sont maintenant redirigées vers la bonne page de la page d'accueil de la nouvelle société.

Exemple 10 : chiffrement RSA basé sur des règles

August 20, 2021

L'algorithme RSA utilise la fonction PKEY_ENCRYPT_PEM () pour chiffrer le contenu d'en-tête ou de corps HTTP prédéfini et défini par l'utilisateur. La fonction accepte uniquement les clés publiques RSA (pas les clés privées) et les données chiffrées ne peuvent pas dépasser la longueur de la clé publique. Lorsque les données chiffrées sont plus courtes que la longueur de la clé, l'algorithme utilise la méthode de remplissage RSA_PKCS1.

Dans un exemple de scénario, la fonction peut être utilisée avec la fonction B64ENCODE () dans une action de réécriture pour remplacer une valeur d'en-tête HTTP par une valeur chiffrée par une clé publique RSA. Les données chiffrées sont ensuite déchiffrées par le destinataire à l'aide de la clé privée RSA.

Vous pouvez implémenter la fonctionnalité à l'aide d'une stratégie de réécriture. Pour ce faire, vous devez effectuer les tâches suivantes :

1. Ajoutez une clé publique RSA en tant qu'expression de stratégie.
2. Créer une action de réécriture.
3. Créer une stratégie de réécriture.
4. Lier la stratégie de réécriture comme globale.
5. Vérifier le chiffrement RSA

Chiffrement RSA basé sur des règles à l'aide de l'interface de commande Citrix ADC

Effectuez les tâches suivantes pour configurer le chiffrement RSA basé sur des stratégies à l'aide de l'interface de commande Citrix ADC.

Pour ajouter une clé publique RSA en tant qu'expression de stratégie à l'aide de l'interface de commande Citrix ADC :

```
1 add policy expression pubkey '"-----BEGIN RSA PUBLIC KEY-----
     MIGJAoGBAKl5vgQEj73Kxp+9
     yn1v5gPR1pnc4oLM2a0kaWwBOsB6rzCIy6znwnvwCY1xRvQhRlJSAyJbloL7wZFIJ2FOR8Cz
     +8ZQWXU2syG+udi4EnWqLgFYowF9zK+o79az597eNPAjsHZ/C2oL/+6qY5a/
     f1z8bQPrHC4GpFfAEJhh/+NnAgMBAAE=-----END RSA PUBLIC KEY-----"'
2 <!--NeedCopy-->
```

Pour ajouter réécrire une action pour chiffrer une requête d'en-tête HTTP à l'aide de l'interface de commande Citrix ADC :

```
add rewrite action encrypt_act insert_http_header encrypted_data

HTTP.REQ.HEADER("data_to_encrypt").PKEY_ENCRYPT_PEM(pubkey).B64ENCODE
```


Pour ajouter une stratégie de réécriture à l'aide de l'interface de commande Citrix ADC :

```
add rewrite policy encrypt_pol 'HTTP.REQ.HEADER("data_to_encrypt").
   EXISTS' encrypt_act
<!--NeedCopy-->
```

Pour lier la stratégie de réécriture globale à l'aide de l'interface de commande Citrix ADC :

```
bind rewrite global encrypt_pol 10 -type RES_DEFAULT
```

Pour vérifier le chiffrement RSA à l'aide de l'interface de commande Citrix ADC :

```
>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/`

* About to connect() to 10.217.24.7 port 80 (#0)

*  Trying 10.217.24.7...

*  connected

*  Connected to 10.217.24.7 (10.217.24.7) port 80 (#0)

> GET / HTTP/1.1
> User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0
   OpenSSL/0.9.8y zlib/1.2.3
> Host: 10.217.24.7
> Accept: \*/\*
> data_to_encrypt: Now is the time that tries men's souls
>
< HTTP/1.1 200 OK
< Date: Mon, 09 Oct 2017 05:22:37 GMT
< Server: Apache/2.2.24 (FreeBSD) mod_ssl/2.2.24 OpenSSL/0.9.8y DAV/2
< Last-Modified: Thu, 20 Feb 2014 20:29:06 GMT
< ETag: "6bd9f2-2c-4f2dc5b570880"
< Accept-Ranges: bytes
< Content-Length: 44
< Content-Type: text/html
< encrypted_data: UliegKBJqZd7JdaC49XMLEK1+eQN2rEfevypW91gKvBVlaKM9N9/
   C2BKuztS99SE0xQaisidzN5IgeIcpQMn+
   CiKYVlLzPG1RuhGaqHYzIt6C8A842da7xE4OlV5SHwScqkqZ5aVrXc3EwtUksna7jOLr40aLeXnnB
   /DB11pUAE=
<
* Connection #0 to host 10.217.24.7 left intact
<html><body><h1>It works!</h1></body></html>* Closing connection #0

```



```
<!--NeedCopy-->
```

L'exécution ultérieure de cette commande curl avec les mêmes données à chiffrer montre que les données chiffrées sont différentes à chaque exécution. Cela est dû au fait que le remplissage insère des octets aléatoires au début des données à chiffrer, ce qui provoque des données chiffrées différentes à chaque fois.

```
>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/`

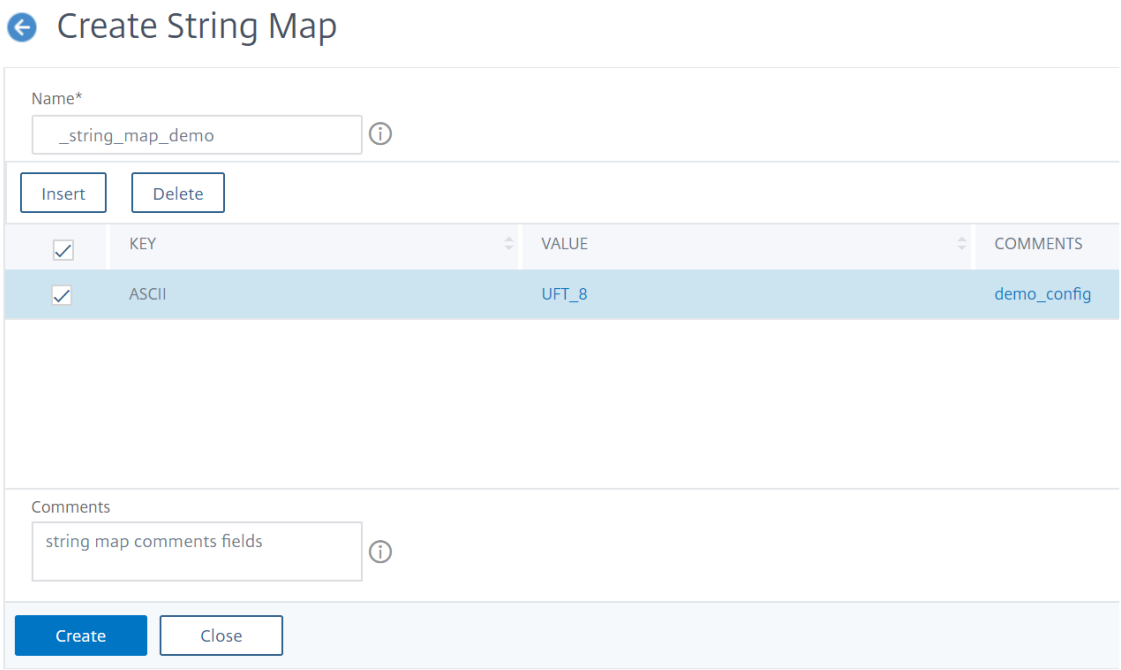
< encrypted_data:
   DaOjtl1Pl4DlQKf58MMeL4cFwFvZwhjMqv5aUYM5Iyzk4UpwIYhpRvgTNu2lXEVc1H0tcR1EGC
   /ViQncLc4EbTurCWLbzjce3+fknnMmzF0lRT6ZZXWbMvsNFOxDA1SnuAgwxWXy/
   ooe9Wy6SYsL2oi1sr5wTG+RihDd9zP+P14=

>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/

. . .

< encrypted_data: eej6YbGP68yHn48qFUvi+fkG+OiO8j3yYLScrRBU+
   TPQ8WeDVaWnDNAVLvL0ZYHHAU1W2YDRYb+8
   cdKHLpW36QbI6Q5FfBuWKZSI2hSyUvypTpCoAYcHXFv0ns+tRtg0EPNNj+
   lyGjKQWtFi6K8IXXISoDy42FblKIlaA7gEriY=
<!--NeedCopy-->
```

Chiffrement RSA basé sur des règles à l'aide de l'interface graphique

L'interface graphique vous permet d'effectuer les tâches suivantes :

Pour ajouter une clé publique RSA en tant qu'expression de stratégie à l'aide de l'interface graphique :

1. Connectez-vous à l'appliance Citrix ADC et accédez à **Configurations** > **AppExpert** > **Expressions avancées**.
2. Dans le volet d'informations, cliquez sur **Ajouter** pour définir une clé publique RSA en tant qu'expression de stratégie avancée.
3. Dans la page Créer une expression, définissez les paramètres suivants :
   a) Nom de l'expression. Nom de l'expression avancée.
   b) Expression. Définissez la clé publique RSA en tant qu'expression avancée à l'aide de l'Éditeur d'expression.
   c) Commentaires. Une brève description de l'expression.
4. Cliquez sur **Créer**.

Pour ajouter réécrire une action pour chiffrer une requête d'en-tête HTTP à l'aide de l'interface graphique :

1. Connectez-vous à l'appliance Citrix ADC et accédez à **Configurations** > **AppExpert** > **Réécriture** > **Actions**.
2. Dans le volet d'informations, cliquez sur **Ajouter** pour ajouter une action de réécriture.
3. Dans l'écran **Créer une action de réécriture**, définissez les paramètres suivants :
   a) Nom. Nom de l'action de réécriture.
   b) Type. Sélectionnez le type d'action comme INSERT_HTTP_HEADER.
   c) Utilisez le type d'action pour insérer un en-tête. Entrez le nom de l'en-tête HTTP qui doit être réécrit.
   d) Expression. Nom de l'expression de stratégie avancée associée à l'action.
   e) Commentaires. Une brève description de l'action de réécriture.
4. Cliquez sur **Créer**.

Pour ajouter une stratégie avancée de réécriture à l'aide de l'interface graphique :

1. Connectez-vous à l'appliance Citrix ADC et accédez à **Configurations** > **AppExpert** > **Réécriture** > **Stratégies**.
2. Dans la page **Réécrire les stratégies**, cliquez sur **Ajouter** pour ajouter une stratégie de réécriture.
3. Dans la page **Créer une stratégie de réécriture**, définissez les paramètres suivants :
   a) Nom. Nom de la stratégie de réécriture.
   b) Action. Nom de l'action de réécriture à effectuer si la demande ou la réponse correspond à cette stratégie de réécriture.
   c) Actions de journalisation. Nom de l'action du journal des messages à utiliser lorsqu'une demande correspond à cette stratégie.
   d) Action à résultat indéfini. Action à effectuer si le résultat de l'évaluation de la stratégie n'est pas défini.
   e) Expression. Nom de l'expression de stratégie avancée qui déclenche l'action.
   f) Commentaires. Une brève description de l'action de réécriture.
4. Cliquez sur **Créer**.

Pour lier la stratégie de réécriture globale à l'aide de l'interface graphique :

1. Connectez-vous à l'appliance Citrix ADC et accédez à **Configurations** > **AppExpert** > **Réécriture** > **Stratégies**.
2. Dans l'écran **Stratégies de réécriture**, sélectionnez une stratégie de réécriture à lier, puis cliquez sur **Gestionnaire de stratégies** .
3. Dans la page Réécrire le Gestionnaire de stratégies, dans la section Points de liaison, définissez les paramètres suivants :
   a) Point de liaison. Sélectionnez le point de liaison comme Global par défaut.
   b) Protocole. Sélectionnez le type de protocole HTTP.

c) Type de connexion. Sélectionnez le type de connexion en tant que Demande.
d) Cliquez sur **Continuer** pour afficher la section **Liaison de stratégie** .
e) Dans la section **Liaison de stratégie**, sélectionnez la stratégie de réécriture et définissez les paramètres de liaison.

4. Cliquez sur **Bind**.

Exemple 11 : chiffrement RSA basé sur des règles sans opération de remplissage

August 20, 2021

La fonction de stratégie PKEY_ENCRYPT_PEM_NO_PADDING () utilise l'algorithme RSA sans opération de remplissage avant d'effectuer le chiffrement RSA. La fonction de stratégie fonctionne comme la fonction PKEY_ENCRYPT_PEM (), sauf qu'elle utilise la méthode RSA_NO_PADDING au lieu de RSA_PKCS1_PADDING. Le paramètre pkey est une chaîne de texte avec une clé publique RSA codée au format PEM. Semblable à PKEY_ENCRYPT_PEM (), vous pouvez utiliser une expression de stratégie pour la clé.

Vous pouvez implémenter la fonctionnalité à l'aide d'une stratégie de réécriture. Pour ce faire, vous devez effectuer les tâches suivantes :

1. Ajoutez une clé publique RSA en tant qu'expression de stratégie.
2. Créer une action de réécriture.

Chiffrement RSA basé sur des règles à l'aide de l'interface de commande Citrix ADC

Effectuez les tâches suivantes pour configurer le chiffrement RSA basé sur des stratégies à l'aide de l'interface de commande Citrix ADC.

Pour ajouter une clé publique RSA sans expression de stratégie de remplissage à l'aide de l'interface de commande Citrix ADC :

```
add expression rsa_pub_key_4096 '"-----BEGIN RSA PUBLIC KEY-----" + "
    MIICCgKCAgEArrwBldKd48xrpOSRPMrg+eNAO0ODU6t5b/WYQLdElqNv7WpefBrA" +
    "nwI2s619gEU1r4zoLqL7l5ALtt5Z+F0JBYfOzBzOky0GtEJ5iX5GP4QxT65J3nHH" +
     "4MTF3acmjvXxclmaKXEFlaVIzW7FTr3Luw/CnOjflAB403Q6F9VBVvQmOVYWnqoI"
    + "+0q1VIg6Q1pAcvdKBiOf85BBofE5EIbZ/1Jt0CdbsV568l+8ve7BnSUncFHoRR3O"
     + "/VfSsDuNWZf7n3RNMzxEuIA72UGPzNYFQzvcPOdzd0aN7jAXw0mgC/NSvKzGKHlo
    " + "mUYYBzlVQdDMZWnd6jSzsBRXSXxsNEy/
    RuXwplrA5epo7JdCoMkfeI4vUXm6MNr8" + "
    TQdFqIc1pdnOsbRf9ec62XbcfR7P8CDTsmLSaagx3rjenPdB+LTWKw2VUF+YONIg" +
    "jM3fyFef9ovVhLhS5HvMqFGs8P75W+d7BOIbIu3EngACiEJOpYSsETD4WgPK6Iyv" +
```



```
        "j6cxsLeYMtElTb0fBIIqysCHdmjF3M1lqdqp4dKs3+W798GJZYM5MxZKUzrBi0Xu"
       + "e7GtSh2aimsfQureUD+0z0RN2umeDsYcA1ghXMclDP+jLS1lnrv0Yvo+TKcm9b8G"
        + "uR/drbCrCsGyWFW+bsAu3AWz9S6TePurP5unRmNNvXpH5DRgsYl3d50CAwEAAQ
       ==" + "-----END RSA PUBLIC KEY-----"
2 <!--NeedCopy-->
```

Pour ajouter une action de réécriture sans expression de stratégie de remplissage à l'aide de l'interface de commande Citrix ADC :

```
add rewrite action rsa_encrypt_act insertHttpHeader encrypted 'HTTP.REQ.
HEADER("plaintext").PKEY_ENCRYPT_PEM_NO_PADDING(rsa_pub_key_4096)
```

Chiffrement RSA basé sur des règles sans option de remplissage à l'aide de l'interface graphique

L'interface graphique vous permet d'effectuer les tâches suivantes :

Pour ajouter une clé publique RSA sans opération de remplissage en tant qu'expression de stratégie à l'aide de l'interface graphique :

1. Connectez-vous à l'appliance Citrix ADC et accédez à **Configurations** > **AppExpert** > **Expressions avancées**.
2. Dans le volet d'informations, cliquez sur **Ajouter** pour définir une clé publique RSA en tant qu'expression de stratégie avancée.
3. Dans la page Créer une expression, définissez les paramètres suivants :
   a) Nom de l'expression. Nom de l'expression avancée.
   b) Expression. Définissez la clé publique RSA en tant qu'expression avancée à l'aide de l'Éditeur d'expression.
   Remarque : La longueur de chaîne maximale est de 255 caractères dans une expression de stratégie. Pour toute clé de plus de 1024 bits, vous devez casser la clé en petits morceaux et concaténer les morceaux ensemble comme « chunk1" + « chunk2" +…
   c) Commentaires. Une brève description de l'expression.
4. Cliquez sur **Créer**.

Pour ajouter réécrire une action à l'aide de l'interface graphique :

1. Connectez-vous à l'appliance Citrix ADC et accédez à **Configurations** > **AppExpert** > **Réécriture** > **Actions**.
2. Dans le volet d'informations, cliquez sur **Ajouter** pour ajouter une action de réécriture.
3. Dans l'écran **Créer une action de réécriture**, définissez les paramètres suivants :
   a) Nom. Nom de l'action de réécriture.
   b) Type. Sélectionnez le type d'action comme INSERT_HTTP_HEADER.
   c) Utilisez le type d'action pour insérer un en-tête. Entrez le nom de l'en-tête HTTP qui doit être réécrit.

d) Expression. Nom de l'expression de stratégie avancée associée à l'action.
e) Commentaires. Une brève description de l'action de réécriture.

4. Cliquez sur **Créer**.

Exemple 12 : Configurer la réécriture pour modifier le nom d'hôte et l'URL dans la demande du client sur l'appliance Citrix ADC

January 21, 2021

La fonctionnalité de réécriture sur une appliance Citrix ADC est utilisée pour convertir l'URL disponible dans la demande du client en une autre URL que le serveur principal peut comprendre. Vous pouvez obtenir les avantages suivants en utilisant la fonction de réécriture :

- Améliore la sécurité en masquant l'URL réelle de la ressource, demandée par le client.
- Empêche l'accès non autorisé de l'utilisateur d'accéder aux ressources réseau.

Prenons un exemple où votre organisation actuelle est acquise par une autre organisation. Il devient difficile pour les administrateurs d'informer sur la nouvelle adresse Web à chaque utilisateur de l'organisation acquise. Dans ce scénario, l'utilisation de la fonction de réécriture devient pratique pour modifier le nom d'hôte et l'URL dans les demandes client pour le site Web de l'organisation acquise. Vous pouvez utiliser la réécriture pour modifier temporairement les URL de la demande du client lorsque le site Web est en cours de maintenance.

La section suivante décrit la procédure de modification du nom d'hôte et de l'URL dans une demande client à l'aide de la fonction de réécriture.

Prenons un exemple où l'utilisateur entre une `http://www.example.com` URL dans le navigateur Web. L'administrateur du site Web souhaite que l'appliance Citrix ADC convertisse l'URL précédente dans la demande client en tant que `http://myexample.example.net.in/resource/inventory/s?t=112`.

Dans l'exemple précédent, l'administrateur du site Web souhaite que l'appliance Citrix ADC remplace le nom de domaine « example.com » par « myexample.exemple.net.in » et l'URL par « ressource/inventory/s ?t=112".

Effectuez les opérations suivantes à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'appliance Citrix ADC à l'aide de SSH.
2. Ajouter des actions de réécriture.
    - `add rewrite action rewrite_host_hdr_act replace "HTTP.REQ.HEADER(\"Host\")""\"myexample.example.net.in\""`

- `add rewrite action rewrite_url_act replace HTTP.REQ.URL.PATH_AND_QUERY "\"/resource/inventory/s?t=112\""`

3. Ajoutez des stratégies de réécriture pour les actions de réécriture.
   - `add rewrite policy rewrite_host_hdr_pol "HTTP.REQ.HEADER(\"Host\").CONTAINS(\"www.example.com\")"rewrite_host_hdr_act`
   - `add rewrite policy rewrite_url_pol "HTTP.REQ.HEADER(\"Host\").CONTAINS(\"www.example.com\")"rewrite_url_act`
4. Liez les stratégies de réécriture à un serveur virtuel.
   - `bind lb vserver rewrite_LB -policyName rewrite_host_hdr_pol -priority 10 -gotoPriorityExpression 20 -type REQUEST`
   - `bind lb vserver rewrite_LB -policyName rewrite_url_pol -priority 20 -gotoPriorityExpression END -type REQUEST`

Transformation d'URL

August 20, 2021

La fonction de transformation d'URL fournit une méthode pour modifier toutes les URL des demandes désignées à partir d'une version externe vue par des utilisateurs externes vers une URL interne visible uniquement par vos serveurs Web et votre personnel informatique. Vous pouvez rediriger les demandes des utilisateurs de manière transparente, sans exposer la structure de votre réseau aux utilisateurs. Vous pouvez également modifier des URL internes complexes dont les utilisateurs peuvent avoir du mal à se souvenir en URL externes plus simples et plus facilement mémorisées.

> **Remarque**
>
> Avant de pouvoir utiliser la fonction de transformation d'URL, vous devez activer la fonction Réécriture. Pour activer la fonction de réécriture, reportez-vous à la section Activation de la fonction de réécriture.
>
> La fonction de transformation d'URL réécrit les URL dans le corps de réponse HTML et n'est pas appliquée à JavaScript et à d'autres variables.

Pour commencer à configurer la transformation d'URL, vous créez des profils, chacun décrivant une transformation spécifique. Dans chaque profil, vous créez une ou plusieurs actions décrivant en détail la transformation. Ensuite, vous créez des stratégies, chacune identifiant un type de requête HTTP à transformer, et vous associez chaque stratégie à un profil approprié. Enfin, vous liez globalement chaque stratégie pour la mettre en œuvre.

Configuration des profils de transformation d'URL

August 20, 2021

Un profil décrit une transformation d'URL spécifique sous la forme d'une série d'actions. Le profil fonctionne principalement comme un conteneur pour les actions, déterminant l'ordre dans lequel les actions sont effectuées. La plupart des transformations transforment un nom d'hôte externe et un chemin optionnel en un nom d'hôte et un chemin d'accès internes différents. La plupart des transformations utiles sont simples et ne nécessitent qu'une seule action, mais vous pouvez utiliser plusieurs actions pour effectuer des transformations complexes.

Vous ne pouvez pas créer d'actions, puis les ajouter à un profil. Vous devez d'abord créer le profil, puis y ajouter des actions. Dans l'interface de ligne de commande, la création d'une action et la configuration de l'action sont des étapes distinctes. La création d'un profil et la configuration du profil sont des étapes distinctes dans l'interface de ligne de commande et dans l'utilitaire de configuration.

Pour créer un profil de transformation d'URL à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC, tapez les commandes suivantes, dans l'ordre indiqué, pour créer un profil de transformation d'URL et vérifier la configuration. Vous pouvez ensuite répéter les deuxième et troisième commandes pour configurer des actions supplémentaires :

- `add transform profile <profileName> -type URL [-onlyTransformAbsURLinBody (ON|OFF)] \[-comment <comment>]`
- `add transform action <name> <profileName> <priority>`
- `set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainFrom <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment "<string>"]`
- `show transform profile <name>`

Exemple :

```
1 > add transform profile shoppingcart -type URL
2  Done
3 > add transform action actshopping shoppingcart 1000
4  Done
5 > set transform action actshopping -priority 1000 -reqUrlFrom 'shopping
     .example.com' -reqUrlInto 'www.example.net/shopping' -resUrlFrom '
     www.example.net/shopping' -resUrlInto 'shopping.example.com' -
     cookieDomainFrom 'example.com' -cookieDomainInto 'example.net' -
     state ENABLED -comment 'URL transformation for shopping cart.'
```



```
 Done
> show transform profile shoppingcart
        Name: shoppingcart
                Type: URL       onlyTransformAbsURLinBody: OFF
        Comment:
        Actions:

1)              Priority 1000   Name: actshopping       ENABLED
 Done
<!--NeedCopy-->
```

Pour modifier un profil ou une action de transformation d'URL existant à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC, tapez les commandes suivantes pour modifier un profil ou une action de transformation d'URL existant et vérifier la configuration :

Remarque : Utilisez respectivement une commande set transform profile ou set transform action. La commande set transform profile prend les mêmes arguments que la commande add transform profile, et l'action set transform est la même commande que celle utilisée pour la configuration initiale.

- `set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment "<string>"]`
- `show transform profile <name>`

Exemple :

```
> set transform action actshopping -priority 1000 -reqUrlFrom '
   searching.example.net' -reqUrlInto 'www.example.net/searching' -
   resUrlFrom 'www.example.net/searching' -resUrlInto 'searching.
   example.com' -cookieDomainInto 'example.net' -state ENABLED -comment
    'URL transformation for searching cart.'
 Done
> show transform profile shoppingcart
        Name: shoppingcart
                Type: URL       onlyTransformAbsURLinBody: OFF
        Comment:
        Actions:

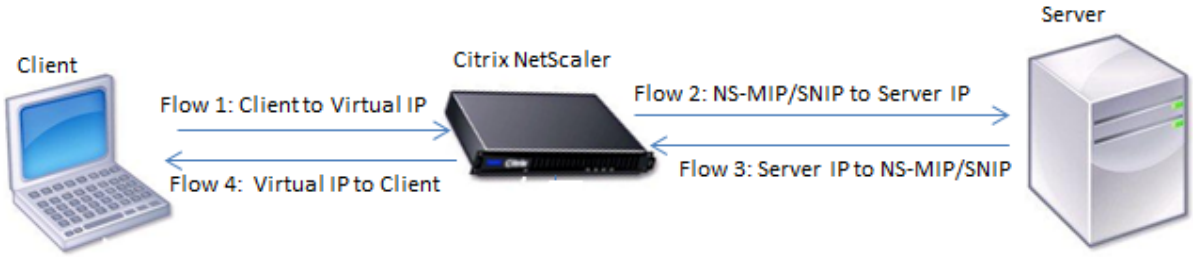
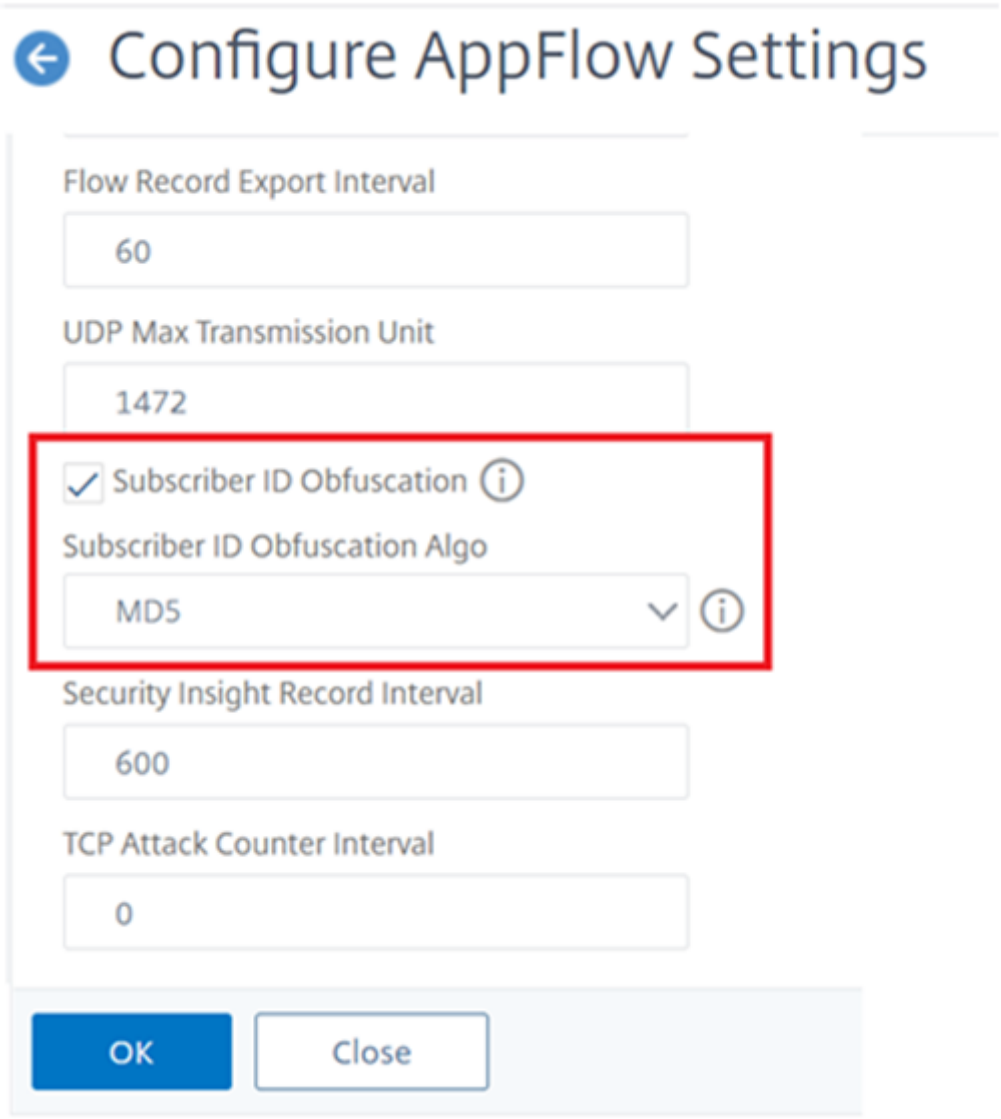
1)              Priority 1000   Name: actshopping       ENABLED
 Done
<!--NeedCopy-->
```


Pour supprimer un profil de transformation d'URL et des actions à l'aide de la ligne de commande Citrix ADC

Supprimez d'abord toutes les actions associées à ce profil en tapant la commande suivante une fois pour chaque action :

- rm transform action <name> Après avoir supprimé toutes les actions associées à un profil, supprimez le profil comme indiqué ci-dessous.
- rm transform profile <name>

Pour créer un profil de transformation d'URL à l'aide de l'utilitaire de configuration

1. Dans le volet de navigation, développez **Réécrire**, Transformation d'URL, puis cliquez sur **Profils**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un profil de transformation d'URL**, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres pour la configuration des profils de transformation d'URL » comme suit (un astérisque indique un paramètre requis) :
   - Nom* : nom
   - Commentaire—Commentaire
   - Transformer uniquement les URL absolues dans le corps de réponse : OnlyTransformAbsurlinBody
4. Cliquez sur **Créer**, puis sur **Fermer**. Un message apparaît dans la barre d'état indiquant que le profil a été configuré avec succès.

Pour configurer un profil de transformation d'URL et des actions à l'aide de l'utilitaire de configuration

1. Dans le volet de navigation, développez **Réécrire**, Transformation d'URL, puis cliquez sur **Profils**.
2. Dans le volet d'informations, sélectionnez le profil à configurer, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le profil de transformation d'URL**, effectuez l'une des opérations suivantes.
   - Pour créer une action, cliquez sur **Ajouter**.
   - Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Ouvrir**.
4. Renseignez la boîte de dialogue **Créer une action de transformation d'URL** ou **Modifier une action de transformation d'URL** en saisissant ou en sélectionnant des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres pour la configuration des profils de transformation d'URL » comme suit (un astérisque indique un paramètre requis) :

- Nom de l'action* : nom
- Commentaires—Commentaire
- Priorité*—Priorité
- URL de la requête de—RequrlFrom
- URL de la requête dans—RequrlInto
- URL de réponse de—ResURLFrom
- URL de réponse dans—ResURLInto
- Cookie Domain de—CookieDomainFrom
- Domaine de cookie dans—CookieDomainInto
- Activé : état

5. Enregistrez vos modifications.
   - Si vous créez une action, cliquez sur **Créer**, puis sur **Fermer**.
   - Si vous modifiez une action existante, cliquez sur **OK**.
     Un message apparaît dans la barre d'état indiquant que le profil a été configuré avec succès.
6. Répétez les étapes 3 à 5 pour créer ou modifier des actions supplémentaires.
7. Pour supprimer une action, sélectionnez-la, puis cliquez sur Supprimer. Lorsque vous y êtes invité, cliquez sur OK pour confirmer la suppression.
8. Cliquez sur **OK** pour enregistrer vos modifications et fermer la boîte de dialogue Modifier le profil de transformation d'URL.
9. Pour supprimer un profil, sélectionnez le profil dans le volet d'informations, puis cliquez sur **Supprimer**. Lorsque vous y êtes invité, cliquez sur **OK** pour confirmer la suppression.

Configuration de stratégies de transformation d'URL

August 20, 2021

Après avoir créé un profil de transformation d'URL, vous créez ensuite une stratégie de transformation d'URL pour sélectionner les demandes et réponses que Citrix ADC doit transformer à l'aide du profil. La transformation d'URL considère chaque demande et sa réponse comme une seule unité, de sorte que les stratégies de transformation d'URL ne sont évaluées que lorsqu'une demande est reçue. Si une stratégie correspond, Citrix ADC transforme à la fois la demande et la réponse.

Remarque : les fonctions de transformation et de réécriture d'URL ne peuvent pas toutes les deux fonctionner sur le même en-tête HTTP pendant le traitement de la demande. Pour cette raison, si vous souhaitez appliquer une transformation d'URL à une requête, vous devez vous assurer qu'aucun des en-têtes HTTP qu'elle modifiera n'est manipulé par une action de réécriture.

Pour configurer une stratégie de transformation d'URL à l'aide de la ligne de commande Citrix ADC

Vous devez créer une nouvelle stratégie. Sur la ligne de commande, une stratégie existante ne peut être supprimée que. À l'invite de commandes Citrix ADC, tapez les commandes suivantes pour configurer une stratégie de transformation d'URL et vérifier la configuration :

- `<add transform policy <name> <rule> <profileName>`
- `<show transform policy <name>`

Exemple :

```
1  > add transform policy polsearch  HTTP.REQ.URL.SUFFIX.EQ("Searching")
       prosearching
2   Done
3  > show transform policy polsearch
4  1)      Name: polsearch
5          Rule: HTTP.REQ.URL.SUFFIX.EQ("Searching")
6          Profile: prosearching
7          Priority: 0
8          Hits: 0
9   Done
10 <!--NeedCopy-->
```

Pour supprimer une stratégie de transformation d'URL à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC, tapez la commande suivante pour supprimer une stratégie de transformation d'URL :

```
rm transform policy <name>
```

Exemple :

```
1  > rm transform policy polsearch
2  Done
3  <!--NeedCopy-->
```

Pour configurer une stratégie de transformation d'URL à l'aide de l'utilitaire de configuration

1. Dans le volet de navigation, développez **Réécrire**, Transformation d'URL, puis cliquez sur **Stratégies**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :

- Pour créer une stratégie, cliquez sur **Ajouter**.
- Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Ouvrir**.

3. Dans la boîte de dialogue **Créer une stratégie de transformation d'URL** ou **Configurer une stratégie de transformation d'URL**, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres pour la configuration des stratégies de transformation d'URL » comme suit (un astérisque indique un paramètre requis) :

   - nom* : nom (Impossible de modifier une stratégie précédemment configurée.)
   - Profile*—Nom du profil
   - Expression : règle

   Si vous souhaitez obtenir de l'aide pour créer une expression pour une nouvelle stratégie, vous pouvez soit maintenir la touche CTRL enfoncée et appuyer sur la barre d'espace lorsque le curseur se trouve dans la zone de texte Expression. Pour créer l'expression, vous pouvez la taper directement comme décrit ci-dessous, ou vous pouvez utiliser la boîte de dialogue Ajouter une expression.

4. Cliquez sur **Préfixe**, puis choisissez le préfixe de votre expression.

   Vos choix sont les suivants :

   - HTTP : protocole HTTP. Choisissez cette option si vous souhaitez examiner un aspect de la demande qui concerne le protocole HTTP.
   - SYS : site (s) Web protégé (s). Choisissez cette option si vous souhaitez examiner un aspect de la demande qui concerne le destinataire de la demande.
   - Client : ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner un aspect de l'expéditeur de la demande.
   - Serveur : ordinateur auquel la demande a été envoyée. Choisissez cette option si vous souhaitez examiner un aspect du destinataire de la demande.
   - URL : URL de la demande. Choisissez cette option si vous souhaitez examiner un aspect de l'URL à laquelle la demande a été envoyée.
   - text : n'importe quelle chaîne de texte de la requête. Choisissez cette option si vous souhaitez examiner une chaîne de texte dans la requête.
   - target : cible de la demande. Choisissez cette option si vous souhaitez examiner un aspect de la cible de la demande.

   Après avoir choisi un préfixe, le Citrix ADC affiche une fenêtre d'invite en deux parties qui affiche les choix suivants possibles en haut et une brève explication de ce que signifie le choix sélectionné en bas. Les choix dépendent du préfixe que vous avez choisi.

5. Sélectionnez votre prochain mandat.

Si vous avez choisi HTTP comme préfixe, vos choix sont REQ, qui spécifie les requêtes HTTP, et RES, qui spécifie les réponses HTTP. Si vous avez choisi un autre préfixe, vos choix sont plus variés. Pour obtenir de l'aide sur un choix spécifique, cliquez une fois sur ce choix pour afficher des informations à ce sujet dans la fenêtre d'invite inférieure.

Lorsque vous êtes certain du choix souhaité, double-cliquez dessus pour l'insérer dans la fenêtre Expression.

1. Tapez un point, puis continuez à sélectionner des termes dans les zones de liste qui apparaissent à droite de la zone de liste précédente. Vous tapez les chaînes de texte ou les nombres appropriés dans les zones de texte qui s'affichent pour vous inviter à entrer une valeur, jusqu'à ce que votre expression soit terminée.
2. Cliquez sur **Créer** ou sur **OK**, selon que vous créez une stratégie ou modifiez une stratégie existante.
3. Cliquez sur **Fermer**. Un message apparaît dans la barre d'état indiquant que la stratégie a été configurée avec succès.

Pour ajouter une expression à l'aide de la boîte de dialogue Ajouter une expression

1. Dans la boîte de dialogue **Créer une action du répondeur** ou **Configurer une action du répondeur**, cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Ajouter une expression**, dans la première zone de liste, choisissez le premier terme de votre expression.
    - HTTP. Le protocole HTTP. Choisissez cette option si vous souhaitez examiner un aspect de la demande qui concerne le protocole HTTP.
    - SYS. Le(s) site(s) protégé(s). Choisissez cette option si vous souhaitez examiner un aspect de la demande qui concerne le destinataire de la demande.
    - CLIENT. Ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner un aspect de l'expéditeur de la demande.
    - SERVER. Ordinateur auquel la demande a été envoyée. Choisissez cette option si vous souhaitez examiner un aspect du destinataire de la demande.
    - URL. URL de la demande. Choisissez cette option si vous souhaitez examiner un aspect de l'URL à laquelle la demande a été envoyée.
    - TEXTE. Toute chaîne de texte dans la requête. Choisissez cette option si vous souhaitez examiner une chaîne de texte dans la requête.
    - CIBLE. La cible de la demande. Choisissez cette option si vous souhaitez examiner un aspect de la cible de la demande.
      Lorsque vous faites votre choix, la zone de liste la plus à droite répertorie les termes appropriés pour la partie suivante de votre expression.

3. Dans la deuxième zone de liste, choisissez le deuxième terme pour votre expression. Les choix dépendent du choix que vous avez fait à l'étape précédente et sont adaptés au contexte. Après avoir fait votre deuxième choix, la fenêtre d'aide située sous la fenêtre Construire une expression (qui était vide) affiche de l'aide décrivant le but et l'utilisation du terme que vous venez de choisir.
4. Continuez à choisir des termes dans les zones de liste qui apparaissent à droite de la zone de liste précédente, ou à taper des chaînes ou des nombres dans les zones de texte qui s'affichent pour vous inviter à entrer une valeur, jusqu'à ce que votre expression soit terminée.

Stratégies de transformation d'URL de liaison globale

August 20, 2021

Après avoir configuré vos stratégies de transformation d'URL, vous les liez à Global ou à un point de liaison pour les mettre en œuvre. Après la liaison, toute requête ou réponse qui correspond à une stratégie de transformation d'URL est transformée par le profil associé à cette stratégie.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel entier positif. Dans le système d'exploitation Citrix ADC, les priorités de stratégie fonctionnent dans l'ordre inverse - plus le nombre est élevé, plus la priorité est faible.

Étant donné que la fonction de transformation d'URL implémente uniquement la première stratégie correspondant à une demande, et non les stratégies supplémentaires qu'elle pourrait également correspondre, la priorité de stratégie est importante pour obtenir les résultats que vous souhaitez obtenir. Si vous attribuez à votre première stratégie une priorité faible (par exemple 1000), vous demandez à Citrix ADC de l'exécuter uniquement si d'autres stratégies avec une priorité supérieure ne correspondent pas à une demande. Si vous attribuez à votre première stratégie une priorité élevée (par exemple 1), vous indiquez à Citrix ADC de l'exécuter en premier et ignorez toutes les autres stratégies qui pourraient également correspondre. Vous pouvez vous laisser beaucoup de place pour ajouter d'autres stratégies dans n'importe quel ordre, sans avoir à réaffecter des priorités, en définissant des priorités avec des intervalles de 50 ou 100 entre chaque stratégie lorsque vous liez globalement vos stratégies.

Remarque : les stratégies de transformation d'URL ne peuvent pas être liées à des serveurs virtuels basés sur TCP.

Pour lier une stratégie de transformation d'URL à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC, tapez les commandes suivantes pour lier globalement une stratégie de transformation d'URL et vérifier la configuration :

- `bind transform global <policyName> <priority>`
- `show transform global`

Exemple :

```
1 > bind transform global polisearching 100
2  Done
3 > show transform global
4 1)      Policy Name: polisearching
5         Priority: 100
6
7  Done
8 <!--NeedCopy-->
```

Pour lier une stratégie de transformation d'URL à l'aide de l'utilitaire de configuration

1. Dans le volet de navigation, développez Réécrire, puis Transformation d'URL, puis cliquez sur **Stratégies.
2. Dans le volet d'informations, cliquez sur **Gestionnaire de stratégies**.
3. Dans la boîte de **dialogue Transformer le Gestionnaire** de stratégies, choisissez le point de liaison auquel vous souhaitez lier la stratégie**. Les choix sont les suivants :
   - **Remplacer Global.** Les stratégies liées à ce point de liaison traitent tout le trafic provenant de toutes les interfaces de l'appliance Citrix ADC et sont appliquées avant toute autre stratégie.
   - **Serveur virtuel LB.** Les stratégies liées à un serveur virtuel d'équilibrage de charge sont appliquées uniquement au trafic traité par ce serveur virtuel d'équilibrage de charge et sont appliquées avant toute stratégie globale par défaut. Après avoir sélectionné Serveur virtuel LB, vous devez également sélectionner le serveur virtuel d'équilibrage de charge spécifique auquel vous souhaitez lier cette stratégie.
   - **Serveur virtuel CS.** Les stratégies liées à un serveur virtuel de commutation de contenu sont appliquées uniquement au trafic traité par ce serveur virtuel de commutation de contenu et sont appliquées avant toute stratégie globale par défaut. Après avoir sélectionné CS Virtual Server, vous devez également sélectionner le serveur virtuel de commutation de contenu spécifique auquel vous souhaitez lier cette stratégie.
   - **Global par défaut.** Les stratégies liées à ce point de liaison traitent tout le trafic provenant de toutes les interfaces de l'appliance Citrix ADC.

- **Étiquette de stratégie.** Les stratégies liées à un trafic de traitement d'étiquette de stratégie que l'étiquette de stratégie leur achemine. L'étiquette de stratégie contrôle l'ordre dans lequel les stratégies sont appliquées à ce trafic.

4. Sélectionnez Insérer une stratégie pour insérer une nouvelle ligne et afficher une liste déroulante contenant toutes les stratégies de transformation d'URL non liées disponibles.
5. Sélectionnez la stratégie à lier ou sélectionnez Nouvelle stratégie pour créer une stratégie. La stratégie que vous avez sélectionnée ou créée est insérée dans la liste des stratégies de transformation d'URL liées globalement.
6. Effectuez des ajustements supplémentaires à la liaison.
   - Pour modifier la priorité de stratégie, cliquez sur le champ pour l'activer, puis tapez une nouvelle priorité. Vous pouvez également sélectionner Régénérer les priorités pour renuméroter les priorités uniformément.
   - Pour modifier l'expression de stratégie, double-cliquez sur ce champ pour ouvrir la boîte de dialogue Configurer la stratégie de transformation, dans laquelle vous pouvez modifier l'expression de stratégie.
   - Pour définir l'expression Goto, double-cliquez sur le champ dans l'en-tête de colonne Optimer l'expression pour afficher la liste déroulante, dans laquelle vous pouvez choisir une expression.
   - Pour définir l'option Invoquer, double-cliquez sur le champ dans l'en-tête de colonne Invoquer pour afficher la liste déroulante, dans laquelle vous pouvez choisir une expression.
7. Répétez les étapes 3 à 6 pour ajouter des stratégies de transformation d'URL supplémentaires que vous souhaitez lier globalement.
8. Cliquez sur **OK** pour enregistrer vos modifications. Un message apparaît dans la barre d'état indiquant que la stratégie a été configurée avec succès.

Prise en charge de RADIUS pour la fonction de réécriture

August 20, 2021

Le langage des expressions Citrix ADC inclut des expressions qui peuvent extraire des informations à partir des messages RADIUS et les manipuler dans les requêtes et les réponses. Ces expressions vous permettent d'utiliser la fonction de réécriture pour modifier des portions d'un message RADIUS avant de l'envoyer à sa destination. Vos stratégies et actions de réécriture peuvent utiliser n'importe quelle expression appropriée ou pertinente à un message RADIUS. Les expressions disponibles vous permettent d'identifier le type de message RADIUS, d'extraire toute paire attribute-valeur (AVP) de la connexion et de modifier les AVP RADIUS. Vous pouvez également créer des étiquettes de stratégie pour les connexions RADIUS.

Vous pouvez utiliser les nouvelles expressions RADIUS dans les règles de réécriture à plusieurs fins.

Par exemple, vous pouvez :

- Supprimez la partie domaine du nom d'utilisateur RADIUS AVP pour simplifier l'authentification unique (SSO).
- Insérez un AVP spécifique au fournisseur, tel que le champ MISSDN utilisé dans les opérations de la compagnie de téléphone pour contenir des informations sur l'abonné.

Vous pouvez également créer des étiquettes de stratégie pour acheminer des types spécifiques de demandes RADIUS via une série de stratégies appropriées à ces demandes.

> **Remarque** :
>
> RADIUS for Rewrite a les limitations suivantes :

- Citrix ADC ne résigne pas les demandes ou réponses RADIUS réécrites. Si le serveur d'authentification RADIUS nécessite des messages RADIUS signés, l'authentification échoue.
- Les expressions RADIUS actuellement disponibles ne fonctionnent pas avec les attributs RADIUS IPv6.

La documentation Citrix ADC pour les expressions prenant en charge RADIUS suppose une familiarité avec la structure de base et le but des communications RADIUS. Si vous avez besoin de plus d'informations sur RADIUS, consultez la documentation de votre serveur RADIUS ou recherchez en ligne une introduction au protocole RADIUS.

Configuration des stratégies de réécriture pour RADIUS

La procédure suivante utilise la ligne de commande Citrix ADC pour configurer une action et une stratégie de réécriture et lier la stratégie à un point de liaison global spécifique à la réécriture.

Pour configurer une action et une stratégie de réécriture et lier la stratégie :

À l'invite de commandes, tapez les commandes suivantes :

- `add rewrite action <actName> <actType>`
- `add rewrite policy <polName> <rule> <actName>`
- `bind rewrite policy <polName> <priority> <nextExpr> -type <bindPoint>` où`<bindPoint>` représente l'un des points de liaison globaux spécifiques à la réécriture.

Expressions RADIUS pour la réécriture

Dans une configuration de réécriture, vous pouvez utiliser les expressions Citrix ADC suivantes pour faire référence à diverses parties d'une requête ou d'une réponse RADIUS.

Identification du type de connexion :

- `RADIUS.IS_CLIENT`

  Renvoie TRUE si la connexion est un message client RADIUS (demande).

- `RADIUS.IS_SERVER`

  Renvoie TRUE si la connexion est un message de réponse du serveur RADIUS.

Expressions de demande :

- `RADIUS.REQ.CODE`

  Renvoie le nombre correspondant au type de requête RADIUS. Un dérivé de la classe num_at. Par exemple, une demande d'accès RADIUS renvoie 1 (un). Une demande de comptabilité RADIUS retournerait 4.

- `RADIUS.REQ.LENGTH`

  Renvoie la longueur de la requête RADIUS, y compris l'en-tête. Un dérivé de la classe num_at.

- `RADIUS.REQ.IDENTIFIER`

  Renvoie l'identificateur de demande RADIUS, un numéro attribué à chaque demande qui permet de faire correspondre la demande à la réponse correspondante. Un dérivé de la classe num_at.

- `RADIUS.REQ.AVP(<AVP Code No>).VALUE`

  Renvoie la valeur de la première occurrence de cet AVP sous la forme d'une chaîne de type text_t.

- `RADIUS.REQ.AVP(<AVP code no>).INSTANCE(instance number)`

  Renvoie l'instance spécifiée de l'AVP sous la forme d'une chaîne de type RAVP_t. Un AVP RADIUS spécifique peut se produire plusieurs fois dans un message RADIUS. INSTANCE (0) renvoie la première instance, INSTANCE (1) renvoie la deuxième instance, et ainsi de suite, jusqu'à seize instances.

- `RADIUS.REQ.AVP(<AVP code no>).VALUE(instance number)`

  Renvoie la valeur de l'instance spécifiée de l'AVP sous la forme d'une chaîne de type text_t.

- `RADIUS.REQ.AVP(<AVP code no>).COUNT`

  Renvoie le nombre d'instances d'un AVP spécifique dans une connexion RADIUS, sous forme d'entier.

- `RADIUS.REQ.AVP(<AVP code no>).EXISTS`

  Renvoie TRUE si le type d'AVP spécifié existe dans le message, ou FALSE si ce n'est pas le cas.

Expressions de réponse :

Les expressions de réponse RADIUS sont identiques aux expressions de demande RADIUS, sauf que RES remplace REQ.

Typecasts des valeurs AVP :

L'ADC prend en charge les expressions permettant de taper les valeurs AVP RADIUS dans les types de données texte, entier, entier non signé, long, adresse ipv4, adresse ipv6, préfixe ipv6 et heure. La syntaxe est la même que pour les autres expressions de typecast Citrix ADC.

Exemple :

L'ADC prend en charge les expressions permettant de taper les valeurs AVP RADIUS dans les types de données texte, entier, entier non signé, long, adresse ipv4, adresse ipv6, préfixe ipv6 et heure. La syntaxe est la même que pour les autres expressions de typecast Citrix ADC.

```
RADIUS.REQ.AVP(8).VALUE(0).typecast_ip_address_at
<!--NeedCopy-->
```

Expressions de type AVP :

Citrix ADC prend en charge les expressions pour extraire les valeurs RADIUS AVP à l'aide des codes entiers assignés décrits dans RFC2865 et RFC2866. Vous pouvez également utiliser des alias de texte pour accomplir la même tâche. Voici quelques exemples.

- `RADIUS.REQ.AVP (1).VALUE or RADIUS.REQ.USERNAME.value`

  Extrait la valeur du nom d'utilisateur RADIUS.

- `RADIUS.REQ.AVP (4). VALUE or RADIUS.REQ. ACCT\\_SESSION\\_ID.value`

  Extrait Acct-Session-ID AVP (code 44) du message.

- `RADIUS.REQ.AVP (26). VALUE or RADIUS.REQ.VENDOR\\_SPECIFIC.VALUE`

  Extrait la valeur spécifique au fournisseur.

Les valeurs des AVP RADIUS les plus couramment utilisés peuvent être extraites de la même manière.

Points de liaison RADIUS :

Quatre points de liaison globaux sont disponibles pour les stratégies qui contiennent des expressions RADIUS.

- `RADIUS_REQ_OVERRIDE`

  Priorité/Remplacer la file d'attente de stratégie de demande.

- `RADIUS_REQ_DEFAULT`

  File d'attente de stratégie de demande standard.

- `RADIUS_RES_OVERRIDE`

  Priorité/Remplacer la file d'attente de stratégie de réponse.

- RADIUS_RES_DEFAULT

  File d'attente de stratégie de réponse standard.

Expressions spécifiques à la réécriture RADIUS :

- RADIUS.NEW_AVP

  Renvoie le RADIUS AVP spécifié sous forme de chaîne.

- RADIUS.NEW_AVP_INTEGER32

  Renvoie le RADIUS AVP spécifié sous forme d'entier.

- RADIUS.NEW_AVP_UNSIGNED32

  Renvoie le RADIUS AVP spécifié sous la forme d'un entier non signé.

- RADIUS.NEW_VENDOR_SPEC_AVP(<ID>, <definition>)

  Ajoute les AVP spécifiques au fournisseur étendus spécifiés à la connexion. Pour<ID>, remplacez un nombre long. Pour<definition>, remplacez une chaîne contenant les données de l'AVP.

- RADIUS.REQ.AVP_START

  Renvoie l'emplacement entre la fin de l'en-tête RADIUS et le début des AVP. Utilisé dans les actions de réécriture.

  Exemple :

```
1     add rewrite action insert1 insert_after radius.req.avp_start radius
          .new_avp(33, "NEW AVP")
2 <!--NeedCopy-->
```

- RADIUS.REQ.AVP_END

  Renvoie l'emplacement à la fin du message de rayon (ou, en d'autres termes, la fin de tous les AVP) dans le message de rayon. Utilisé lors de l'exécution d'actions de réécriture.

  Exemple :

```
1     add rewrite action insert2 insert_before radius.req.avp_end "radius
          .new_avp(33, "NEW AVP")"
2 <!--NeedCopy-->
```

- RADIUS.REQ.AVP_LIST

  Renvoie l'emplacement au début des AVP dans un message RADIUS et la longueur du message RADIUS, à l'exclusion de l'en-tête. En d'autres termes, renvoie tous les AVP d'un message RADIUS. Utilisé pour effectuer des actions de réécriture.

  Exemple :


```
1     add rewrite action insert3 insert_before_all radius.req.avp_list "
         radius.new_avp(33, "NEW AVP")" -search "avp(33)"
2  <!--NeedCopy-->
```

Types d'action de réécriture valides pour RADIUS :

Les types d'action Réécriture qui peuvent être utilisés avec les expressions RADIUS sont les suivants :

- INSERT_AFTER
- INSERT_BEFORE
- INSERT_AFTER_ALL
- INSERT_BEFORE_ALL
- SUPPRIMER
- DELETE_ALL
- REPLACE
- REPLACE_ALL

Tout `INSERT_ actions` peut être utilisé pour insérer un RADIUS AVP dans une connexion RADIUS.

Cas d'utilisation

Voici des cas d'utilisation pour RADIUS avec réécriture.

Réécriture du nom d'utilisateur AVP

Pour configurer la fonction de réécriture pour supprimer la chaîne de domaine du nom d'utilisateur RADIUS AVP, commencez par créer une action de réécriture REPLACE comme indiqué dans l'exemple ci-dessous. Utilisez l'action d'une stratégie de réécriture qui sélectionne toutes les requêtes RADIUS. Liez la stratégie à un point de liaison global. Lorsque vous le faites, définissez la priorité au niveau approprié pour autoriser les stratégies de blocage ou de rejet à prendre effet en premier, mais assurez-vous que toutes les demandes qui ne sont pas bloquées ou rejetées sont réécrites. Définissez l'expression Goto (GotoRiorityExpr) sur NEXT pour continuer l'évaluation de la stratégie et attachez-la à la file d'attente RADIUS_REQ_DEFAULT.

Exemple :

```
1  add rewrite action rwActRadiusDomainDel replace radius.req.user_name q/
      RADIUS.NEW_AVP(1,RADIUS.REQ.USER_NAME.VALUE.AFTER_STR(" "))/
2  add rewrite policy RadiusRemoveDomainPol true rwActRadiusDomainDel
3  <!--NeedCopy-->
```


> **Remarque** :
>
> La stratégie de réécriture pour RADIUS n'est pas applicable à un serveur virtuel de Gateway. Si un serveur virtuel de Gateway est utilisé un équilibrage de charge, RADIUS doit être configuré et la stratégie de réécriture doit être liée à un serveur virtuel d'équilibrage de charge RADIUS.

Insertion d'un AVP spécifique au fournisseur

Pour configurer l'action Réécriture pour insérer un AVP spécifique au fournisseur contenant le contenu du champ MISSDN, commencez par créer une action INSERT réécriture qui insère le champ MISSDN dans la demande. Utilisez l'action d'une stratégie de réécriture qui sélectionne toutes les requêtes RADIUS. Liez la stratégie à global, en définissant la priorité sur un niveau approprié et les autres paramètres, comme illustré dans l'exemple suivant.

Exemple :

```
add rewrite action rwActRadiusInsMSISDN insert_after radius.req.
    avp_start RADIUS.NEW_VENDOR_SPEC_AVP(<VENDOR ID>, "RADIUS.NEW_AVP(<
    Attribute Code>, <MSISDN>)")
add rewrite policy rwPolRadiusInsMSISDN true rwActRadiusInsMSISDN
bind rewrite global rwPolRadiusInsMSISDN 100 NEXT -type
    RADIUS_REQ_DEFAULT
<!--NeedCopy-->
```

Support de Diameter pour la réécriture

August 20, 2021

La fonction Réécriture prend désormais en charge le protocole Diameter. Vous pouvez configurer Rewrite pour modifier les demandes et les réponses de Diameter comme vous le feriez pour HTTP ou TCP requêtes et réponses, ce qui vous permet d'utiliser Rewrite pour gérer le flux des demandes de Diameter et apporter les modifications nécessaires. Par exemple, si la valeur « Origin-Host » dans une requête Diameter n'est pas appropriée, vous pouvez utiliser Rewrite pour la remplacer par une valeur acceptable pour le serveur Diameter.

Pour configurer Réécriture pour modifier une demande de Diameter

Pour configurer la fonction Réécriture pour remplacer l'hôte Origin-dans une demande de Diameter par une valeur différente, à l'invite de commandes, tapez les commandes suivantes :

- <add rewrite action <actname> replace “DIAMETER.REQ.AVP(264,\“Citrix ADC.example.net\”)” Pour <actname>, remplacez un nom pour votre nouvelle action. Le nom peut se composer d’un à 127 caractères, et peut contenir des lettres, des chiffres et des tirets (-) et des traits de soulignement (_). Pour Citrix Adc.example.net, remplacez l’hôte Origin que vous souhaitez utiliser au lieu du nom d’hôte d’origine.
- add rewrite policy <polname> “diameter.req.avp(264).value.eq(\“host.example.com\”)” <actname>
  Pour <polname>, remplacez un nom pour votre nouvelle stratégie. Comme c’est <actname> le cas, le nom peut comporter entre un et 127 caractères, et peut contenir des lettres, des chiffres et des tirets (-) et des traits de soulignement (_). Pour host.example.com, remplacez le nom de l’origine hôte que vous souhaitez modifier. Pour <actname>, remplacez le nom de l’action que vous venez de créer.
- bind lb vserver <vservername> -policyName <polname> -priority <priority> -type REQUEST
  For <vservername>, remplacez le nom du serveur virtuel d’équilibrage de charge auquel vous souhaitez lier la stratégie. Pour <polname>, remplacez le nom de la stratégie que vous venez de créer. Pour <priority>, substituer une priorité à la stratégie.

Exemple :

Pour créer une action et une stratégie de réécriture afin de modifier toutes les origines de l’hôte de Diameter de « host.example.com » en « Citrix Adc.example.net », vous pouvez ajouter l’action et la stratégie suivantes et lier la stratégie comme illustré.

```
1 > add rewrite action rw_act_replace_avp replace "diameter.req.avp(264)"
     "diameter.new.avp(264,"Citrix ADC.example.net")"
2 > add rewrite policy rw_diam_pol "diameter.req.avp(264).value.eq("
    client.realm2.net")" rw_act_replace_avp
3 > bind lb vserver vs1 -policyName rw_diam_pol -priority 10 -type
    REQUEST
4
5 Done
6 <!--NeedCopy-->
```

Prise en charge de DNS pour la fonction de réécriture

August 20, 2021

Vous pouvez configurer la fonction de réécriture pour modifier les requêtes et réponses DNS, comme vous le feriez pour les requêtes et réponses HTTP ou TCP. Vous pouvez utiliser la réécriture pour gérer le flux des requêtes DNS et apporter les modifications nécessaires dans l’en-tête ou dans la section

des réponses. Par exemple, si la réponse DNS n'a pas le bit AA défini dans l'indicateur d'en-tête, vous pouvez utiliser réécriture pour définir le bit AA dans la réponse DNS et l'envoyer au client.

Expressions DNS

Dans une configuration de réécriture, vous pouvez utiliser les expressions Citrix ADC suivantes pour faire référence à diverses parties d'une requête ou d'une réponse DNS :

Voir Expressions et descriptions

Points de liaison DNS

Les points de liaison globaux suivants sont disponibles pour les stratégies qui contiennent des expressions DNS.

Points de liaison	Description
DNS_REQ_OVERRIDE	Remplacer la file d'attente des stratégies de demande.
DNS_REQ_DEFAULT	File d'attente de stratégie de demande standard.
DNS_RES_OVERRIDE	Remplacer la file d'attente des stratégies de réponse.
DNS_RES_DEFAULT	File d'attente de stratégie de réponse standard.

En plus des points de liaison par défaut, vous pouvez créer des étiquettes de stratégie de type DNS_REQ ou DNS_RES et y lier des stratégies DNS.

Réécrire les types d'action pour DNS

- **replace_dns_answer_section**—Cette action remplace la section des réponses DNS par l'expression définie dans la stratégie DNS.
- **replace_dns_header_field**—Vérifie le type opcode dans la requête DNS. Renvoie True ou False, indiquant si le type opcode dans la requête DNS correspond au type opcode spécifié. Cette action remplace la section d'en-tête DNS par l'expression définie dans la stratégie DNS.

Configuration des stratégies de réécriture pour DNS

La procédure suivante utilise la ligne de commande Citrix ADC pour configurer une action et une stratégie de réécriture et lier la stratégie à un point de liaison global spécifique à la réécriture.

Configurer l'action et la stratégie de réécriture et lier la stratégie pour DNS

À l'invite de commandes, tapez les commandes suivantes :

1. `add rewrite action <actName> <actType>`

   Pour <actname>, remplacez un nom pour votre nouvelle action. Le nom peut contenir de 1 à 127 caractères et peut contenir des lettres, des chiffres, des tirets (-) et des traits de soulignement (_). Pour <actType>, spécifiez les types d'action de réécriture fournis pour les expressions DNS.

2. `add rewrite policy <polName> <rule> <actName>`

   Pour <polname>, remplacez un nom pour votre nouvelle stratégie. Pour <actname>, le nom peut contenir de 1 à 127 caractères et peut contenir des lettres, des chiffres, des tirets (-) et des traits de soulignement (_). Pour <actname>, remplacez le nom de l'action que vous venez de créer.

3. `bind rewrite global <polName> <priority> <gotoPriorityExpression> -type <bindPoint>`

   Pour <polName>, remplacez le nom de la stratégie que vous venez de créer. Pour <priority>, spécifiez la priorité de la stratégie. Pour <bindPoint>, remplacez l'un des points de liaison globaux spécifiques à la réécriture.

Exemple :

Définissez le bit AA de la demande DNS pour équilibrer la charge du serveur virtuel.

Les commandes suivantes configurent l'appliance Citrix ADC pour qu'elle agisse en tant que serveur DNS faisant autorité pour toutes les requêtes qu'elle sert.

```
1 add rewrite action set_aa replace_dns_header_field dns.req.header.flags
     .set(aa)
2 add rewrite policy pol !dns.req.header.flags.is_set(aa)  set_aa
3 bind rewrite global  pol  100  -type dns_res_override
4 <!--NeedCopy-->
```

Modifiez la réponse et la section d'en-tête.

Si le serveur répond avec un domaine NX, vous pouvez définir l'action de réécriture pour remplacer la réponse par l'adresse IP spécifiée. NOPOLICY-REWRITE vous permet d'appeler une banque externe sans traiter une expression (une règle). Cette entrée est une stratégie fictive qui ne contient pas de règle mais dirige l'entrée vers une étiquette de stratégie ou des banques de stratégies spécifiques au serveur virtuel.

```
1 add rewrite action set_aa_res replace_dns_header_field "dns.res.header.
     flags.set(aa)"
```



```
2 add rewrite action modify_nxdomain_res replace_dns_answer_section "dns.
     new_rrset_a("10.102.218.160",300)"
3 add rewrite policy set_res_aa true set_aa_res
4 add add rewrite policy modify_answer "dns.RES.HEADER.RCODE.EQ(nxdomain)
      && dns.RES.QUESTION.TYPE.EQ(A)"
5 modify_nxdomain_res
6 add rewrite policylabel MODIFY_NODATA dns_res
7 bind rewrite policylabel MODIFY_NODATA modify_answer 10 END
8 bind rewrite policylabel MODIFY_NODATA set_res_aa 11 END
9 bind lb vserver v1 -policyName NOPOLICY-REWRITE -priority 11 -
     gotoPriorityExpression END -type
10 RESPONSE -invoke policylabel MODIFY_NODATA
11 <!--NeedCopy-->
```

Limitations :

- Les stratégies de réécriture sont évaluées uniquement si l'appliance Citrix ADC est configurée en tant que serveur proxy DNS et qu'il y a un défaut de cache.
- Si l'indicateur Récursion disponible (RA) dans l'en-tête est défini sur YES, l'indicateur RA ne sera pas modifié dans les réécritures.
- Si l'indicateur RA dans l'en-tête est défini sur YES, l'indicateur CD dans l'en-tête est modifié indépendamment de toute action de réécriture.

Cartes à cordes

October 5, 2021

Vous pouvez utiliser des mappages de chaînes pour effectuer une correspondance de modèles dans toutes les fonctionnalités de Citrix ADC qui utilisent la syntaxe de stratégie par défaut. Une carte de chaînes est une entité Citrix ADC composée de paires clé-valeur. Les clés et les valeurs sont des chaînes au format ASCII ou UTF-8. La comparaison de chaînes utilise deux nouvelles fonctions, `MAP_STRING (<string_map_name>)` et `IS_STRINGMAP_KEY(<string_map_name>)`.

Une configuration de stratégie qui utilise des mappages de chaînes fonctionne mieux qu'une configuration qui effectue une correspondance de chaînes via des expressions de stratégie, et vous avez besoin de moins de stratégies pour effectuer une correspondance de chaînes avec un grand nombre de paires clé-valeur. Les String Maps sont également intuitifs, simples à configurer et se traduisent par une configuration plus petite.

Fonctionnent les String Maps

Les mappages de chaînes ont une structure similaire aux jeux de motifs (un jeu de motifs définit un mappage des valeurs d'index avec des chaînes ; un mappage de chaînes définit un mappage de chaînes avec des chaînes de caractères) et les commandes de configuration des mappages de chaînes (commandes telles que add, bind, unbind, remove et show) sont syntaxiquement similaires à la configuration commandes pour les jeux de motifs. De plus, comme pour les valeurs d'index d'un jeu de motifs, chaque clé d'une carte de chaînes doit être unique sur la carte. Le tableau suivant illustre un mappage de chaînes appelé url_string_map, qui contient des URL sous forme de clés et de valeurs.

Key	Valeur
/url_1.html	http://www.redirect_url_1.com/url_1.html
/url_2.html	http://www.redirect_url_2.com/url_2.html
/url_3.html	http://www.redirect_url_1.com/url_1.html

Tableau 1. String Map « url_string_map »

Le tableau suivant décrit les deux fonctions qui ont été introduites pour activer la correspondance de chaînes avec des clés dans un mappage de chaînes. La correspondance des chaînes est toujours effectuée avec les clés. En outre, les fonctions suivantes effectuent une comparaison entre les clés du mappage de chaînes et la chaîne complète renvoyée par le préfixe d'expression. Les exemples dans les descriptions se réfèrent à l'exemple précédent.

Pour obtenir des informations complètes sur les deux fonctions introduites pour activer la correspondance de chaînes avec des clés dans une carte de chaînes, reportez-vous au tableau des fonctions de carte de chaînes pdf.

Configuration d'un mappage de chaînes

Vous créez d'abord une carte de chaînes, puis vous y liez des paires clé-valeur. Vous pouvez créer un mappage de chaînes à partir de l'interface de ligne de commande (CLI) ou de l'utilitaire de configuration.

Pour configurer un mappage de chaînes à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

1. Créez une carte de chaînes.

```
add policy stringmap <name> -comment <string>
```


1. Liez une paire clé-valeur à la carte de chaînes.

```
bind policy stringmap <name> <key> <value> [-comment <string>]
```

Exemple :

```
1 bind policy stringmap url_string_map1 "/url_1.html" "http://www.
     redirect_url_1.com/url_1.html"
2 <!--NeedCopy-->
```

Pour configurer un mappage de chaînes à l'aide de l'interface graphique Citrix ADC

Accédez à **AppExpert** > **String Maps**, cliquez sur **Ajouter** et spécifiez les détails pertinents.

Exemple : stratégie de répondeur avec une action de redirection

Le cas d'utilisation suivant implique une stratégie de répondeur avec une action de redirection. Dans l'exemple ci-dessous, les quatre premières commandes créent la carte de chaînes url_string_map et lient les trois paires clé-valeur utilisées dans l'exemple précédent. Après avoir créé la carte et lié les paires clé-valeur, vous créez une action de répondeur (act_url_redirects) qui redirige le client vers l'URL correspondante dans la carte de chaînes ou vers www.default.com. Vous configurez également une stratégie de répondeur (pol_url_redirects) qui vérifie si les URL demandées correspondent à l'une des clés de url_string_map, puis exécute l'action configurée. Enfin, vous liez la stratégie de répondeur au serveur virtuel de commutation de contenu qui reçoit les demandes des clients qui doivent être évaluées.

```
add stringmap url_string_map
```

```
bind stringmap url_string_map /url_1.html http://www.redirect_url_1.com/
url_1.html
```

```
bind stringmap url_string_map /url_2.html http://www.redirect_url_2.com/
url_2.html
```

```
bind stringmap url_string_map /url_3.html http://www.redirect_url_1.com/
url_1.html
```

'Ajouter l'action du répondeur act_url_redirects rediriger 'HTTP.REQ.URL.MAP_STRING (« url_string_map ») ALT « www.default.com"'

```
add responder policy pol_url_redirects TRUE act_url_redirects
```

```
bind cs vserver csw_redirect -policyname pol_url_redirects -priority 1 -
type request
```


Pour configurer un mappage de chaînes à l'aide de l'interface graphique Citrix ADC

Suivez la procédure ci-dessous pour configurer un mappage de chaînes.

1. Dans le volet de navigation, développez **AppExpert** et cliquez sur **String Maps**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Create String Map**, définissez les paramètres suivants :
   - Name. Nom de la carte de chaînes.
   - Configurez la valeur de clé. Entrée de valeur de clé ASCII liée au mappage de chaînes
   - Commentaires. Une brève description des valeurs clés liées à la carte de chaînes.
4. Cliquez sur **Créer** et **Fermer**.



Jeux d'URL

January 21, 2021

Cette fonctionnalité vous permet de mettre en liste noire un million d'URL. La section comprend les rubriques suivantes :

- Mise en route
- Utilisation des expressions de stratégie avancées pour l'évaluation d'URL
- Configuration d'un jeu d'URL
- Sémantique des modèles d'URL

- Catégories d'URL sur la liste noire

Mise en route

January 21, 2021

Pour empêcher l'accès aux sites Web restreints, une appliance Citrix ADC utilise un algorithme de correspondance d'URL spécialisé. L'algorithme utilise un jeu d'URL qui peut contenir une liste d'URL jusqu'à 1 million (1 000 000) entrées sur liste noire. Chaque entrée peut inclure des métadonnées qui définissent les catégories d'URL et les groupes de catégories en tant que modèles indexés. L'appliance peut également télécharger périodiquement des URL de jeux d'URL hautement sensibles gérés par des organismes d'application de la loi sur Internet (avec des sites Web gouvernementaux) ou des organisations Internet. Une fois l'ensemble d'URL téléchargé à partir d'un site Web et importé dans l'appliance, l'appliance crypte les ensembles d'URL (selon les besoins de ces agences) et ils restent confidentiels et les entrées ne sont pas altérées.

L'appliance Citrix ADC utilise des stratégies avancées pour déterminer si une URL entrante doit être bloquée, autorisée ou redirigée. Ces stratégies utilisent des expressions avancées pour évaluer les URL entrantes par rapport aux entrées sur la liste noire. Une entrée peut inclure des métadonnées. Pour les entrées sans métadonnées, vous pouvez utiliser une expression qui évalue l'URL en fonction d'une correspondance exacte de chaîne. Pour les autres URL, vous pouvez utiliser une expression qui évalue les métadonnées de l'URL, en plus d'une expression qui vérifie la correspondance exacte de chaîne.

Utilisation des stratégies d'accès Internet sécurisé pour les FSI et les entreprises de télécommunication

Un jeu d'URL permet à un FAI (FAI) ou à un client de télécommunications d'appliquer les politiques d'accès Internet sécurisé prescrites par le gouvernement, telles que :

1. Bloquer l'accès aux sites Internet illégaux (abus d'enfants, drogues, etc.)
2. Navigation sécurisée pour les enfants

Une appliance Citrix ADC vous permet de télécharger périodiquement des ensembles d'URL gérés par des agences d'application Internet ou des organisations Internet indépendantes. L'appliance télécharge périodiquement la liste et la met à jour en toute sécurité. La liste est stockée en tant que jeux d'URL confidentiels afin qu'elle ne soit pas falsifiée ou lisible par l'homme. Le jeu d'URL téléchargé périodiquement fonctionne comme un jeu de liste noire à des fins d'évaluation d'URL.

Si vous disposez d'une URL privée et que le contenu de la liste reste confidentiel et que l'administrateur réseau ne connaît pas les URL de liste noire présentes dans la liste. Pour vous

assurer que la stratégie est correctement configurée et que la liste correcte est référencée, vous devez configurer l'URL Canary et l'ajouter au jeu d'URL. À l'aide de l'URL Canary, l'administrateur peut demander via l'appliance utilise l'URL privée définie pour s'assurer qu'elle est recherchée pour chaque requête d'URL.

Expressions de stratégie avancées pour l'évaluation d'URL

August 20, 2021

Le tableau suivant décrit les expressions que vous pouvez utiliser pour évaluer les URL entrantes avec des entrées dans un jeu d'URL.

Remarque : HTTP.REQ.URL est généralisé pour être utilisé comme <URL expression>

Expression.	Opération
<URL expression>.URLSET_MATCHES_ANY	Value TRUE si l'URL correspond exactement à n'importe quelle entrée du jeu d'URL.
<URL expression> .GET_URLSET_METADATA(<URLSET>)	L'expression GET_URLSET_METADATA() renvoie les métadonnées associées si l'URL correspond exactement à n'importe quel motif dans le jeu d'URL. Une chaîne vide est renvoyée s'il n'y avait pas de correspondance.
<URL expression> .GET_URLSET_METADATA(<URLSET>).EQ(<METADATA>	Evalue à TRUE si les métadonnées correspondantes sont égales à <METADATA>.
<URL expression> .GET_URLSET_METADATA(<URLSET>).TYPECAST_LIST_T(',').GET(0).EQ(<CATEGORY>)	Value TRUE si les métadonnées correspondantes sont au début de la catégorie. Ce modèle peut être utilisé pour encoder des champs distincts dans les métadonnées, mais correspondre uniquement au 1er champ.
HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL)	Joigne les paramètres hôte et URL, qui peuvent ensuite être utilisés comme un <URL expression> pour la correspondance.

Configuration du jeu d'URL

October 5, 2021

Vous pouvez effectuer les tâches suivantes pour configurer un jeu d'URL et restreindre les URL sur une plate-forme Citrix ADC :

1. Importez un jeu d'URL (téléchargez-le et chiffrez-le). L'importation d'un ensemble d'URL dans une appliance Citrix ADC vous permet de :

- Pour télécharger le fichier URL.
- Pour ajouter le fichier à la solution matérielle-logicielle.
- Pour chiffrer le fichier.
  Tant que vous n'avez pas ajouté l'URL définie au système, elle n'est pas visible par l'utilisateur.

Vous pouvez télécharger un ensemble de la manière suivante :

- Téléchargez un ensemble d'URL une fois à partir d'un serveur distant et spécifiez-le comme `http://myserver.com/file_with_urlset.csv`
- ajoutez un fichier sous le `/var/tmp/` chemin d'accès dans ADC et utilisez la commande, comme dans l'exemple :

```
1 > shell cat /var/tmp/test_urlset.csv
2 example.com
3 google.com
4 > import policy urlset top10
5 k -url local:test_urlset.csv -delimiter "," -rowSeparator "n" -interval
      10 -privateSet -canaryUrl http://www.in.gr
6 Done
7
8 <!--NeedCopy-->
```

Le jeu d'URL importé est également classé en différentes catégories et groupes de catégories dans la base de données. Cette option n'est valable que si des catégories existent dans les métadonnées du fichier de jeu d'URL.

Remarque : Il est possible que vous ayez des modèles d'URL sans métadonnées.

Une fois que vous avez importé le fichier, vous pouvez mettre à jour, supprimer ou afficher les propriétés du fichier. Une fois le fichier inséré dans l'appliance, vous pouvez modifier les entrées en ajoutant des lignes supplémentaires.

L'ensemble importé est ensuite stocké dans un format de fichier chiffré dans le répertoire Citrix ADC. La liste importée contient des millions d'entrées d'URL. Pour ce qui suit : « La liste importée peut contenir jusqu'à 1 million d'entrées d'URL. Sinon, l'appliance renvoie un message d'erreur indiquant

que la valeur dépasse la limite. Si le jeu d'URL importé contient des entrées sur liste noire avec des métadonnées, les métadonnées détectées par l'appliance lors de son importation.

Une fois que vous avez importé un ensemble d'URL et que vous l'avez ajouté à l'appliance, le jeu d'URL est disponible pour les stratégies avancées afin d'identifier le jeu d'URL correct lors de l'évaluation d'URL entrante. `HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY(<URL set name>)`

1. Mise à jour d'un ensemble d'URL sur l'appliance Citrix ADC. Une fois que vous avez inséré le fichier dans l'appliance, à cet intervalle, vous pouvez mettre à jour manuellement un fichier URL à l'aide de l'interface de ligne de commande.
2. Exportation d'un jeu d'URL. Si vous préférez une sauvegarde du jeu d'URL, vous pouvez exporter la liste des modèles d'URL et en enregistrer une copie vers une URL de destination. Avant d'exporter, vérifiez si le jeu d'URL est marqué comme privé. S'il est marqué comme privé, le jeu d'URL ne peut pas être exporté. La fonctionnalité d'exportation ne fonctionne pas avec un ensemble privé. Un nouveau jeu d'URL `myurl` serait donc importé sans définir de jeu privé, puis exporté vers un autre fichier dans un chemin local, comme ci-dessous :

```
> shell touch /var/tmp/test_urlset_export.csv
Done
> shell cat /var/tmp/test_urlset_export.csv
Done
> shell cat /var/tmp/test_urlset.csv
example.com
google.com
Done
> export urlset myurl -url local:test_urlset_export.csv

> import urlset myurl -url local:test_urlset.csv
Done
(a non-private urlset is imported)

<!--NeedCopy-->
```

1. Suppression d'un jeu d'URL. Si vous souhaitez supprimer un ensemble d'URL d'entrées sur liste noire, vous pouvez utiliser la commande remove pour supprimer le jeu d'URL de l'appliance Citrix ADC.
2. Affichage d'un jeu d'URL. Vous pouvez afficher les propriétés d'un ensemble d'URL à l'aide de la commande show.

> **Remarque :** Les URL contenant une partie de requête sont supprimées lors de l'importation.

Exemple :


```
show urlset
Name: top100 PatternCount: 100 Delimiter:  RowSeparator: Interval: 0
Done
<!--NeedCopy-->
```

Importer un ensemble d'URL avec méta à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
import urlset <name> [-overwrite] [ - delimiter <character>] [-
   rowSeparator <character>] [-url] <url> [-interval <seconds>] [-
   privateSet] [-canaryUrl <URL>]
<!--NeedCopy-->
```

Où,

Delimiter est un enregistrement de fichier CSV dont la valeur par défaut est 44.

RowSeparator est un séparateur de lignes de fichiers CSV dont la valeur par défaut est 10.

L'intervalle est l'intervalle de temps en secondes, arrondi aux 15 minutes les plus proches au cours desquelles la mise à jour du jeu d'URL a lieu.

CanaryURL est une URL utilisée pour tester lorsque le contenu du jeu d'URL reste confidentiel.

Exemple

```
import policy urlset -url local:test_urlset.csv -delimiter ","-rowSeparator
 "n"-interval 10 -privateSet -canaryUrl http://www.in.gr
```

Effectuer une correspondance explicite de sous-domaines pour un ensemble d'URL importé

Vous pouvez désormais effectuer une correspondance explicite de sous-domaines pour un jeu d'URL importé. Un nouveau paramètre, « SubDomainExactMatch », est ajouté à la commande « Import policy URLSet ». Lorsque vous activez le paramètre, l'algorithme de filtrage d'URL effectue une correspondance explicite de sous-domaines. Par exemple, si l'URL entrante est « news.exemple.com » et si l'entrée du jeu d'URL est « exemple.com », l'algorithme ne correspond pas aux URL.

À l'invite de commandes, tapez :

```
import policy urlset <name> [-overwrite] [-delimiter <character>][-rowSeparator
 <character>] -url [-interval <secs>] [-privateSet][-subdomainExactMatch]
[-canaryUrl <URL>]
```

Exemple :

```
import policy urlset forth_urlset -url local:test_urlset.csv -interval 3600
 -subdomainExactMatch
```


Pour afficher l'URL définie à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show urlset <name>
```

Exemple :

À l'invite de commandes, tapez :

```
1          URLset     Count
2          ------     -----
3 1)       top1k      100
4  Done
5
6 > show urlset top1k
7          Count      Delimiter  Interval   RowSeparator
8          -----      ---------  --------   ------------
9          100              ,        0         0x0a
10  Done
11 >
12
13 <!--NeedCopy-->
```

Pour afficher le jeu d'URL importé à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show urlset -imported
```

Exemple :

À l'invite de commandes, tapez :

```
1          URLset
2          ------
3 1)       top1k
4  Done
5 <!--NeedCopy-->
```

Pour afficher le jeu d'URL <urlset_name> à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show urlset <name>
```


Pour exporter un ensemble d'URL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
export urlset <name> <url>
```

Pour ajouter un ensemble d'URL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add urlset <urlset_name>
```

Pour mettre à jour un ensemble d'URL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
update urlset <name>
```

Pour supprimer une commande de jeu d'URL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
remove urlset <name>
```

Exemple :

> Remarque :
>
> Avant d'importer ou d'exporter un ensemble d'URL, vous devez vous assurer que les `test_urlset.csv` fichiers `test_urlset_export.csv` et sont créés et disponibles dans le `/var/tmp` répertoire.

```
1  import policy urlset -url local:test_urlset.csv -delimiter "," -
       rowSeparator "n" -interval 10 -privateSet -overwrite  - canaryUrl
       http://www.in.gr
2
3  add policy urlset top10k
4
5  update policy urlset top10k
6
7  sh policy urlset
8
9  sh policy urlset top10k
10
11 export policy urlset urlset1 -url local:test_urlset_export.csv
12
```



```
import policy urlset top10k -url local:test_urlset.csv  - privateSet

add policy urlset top10k

update policy urlset top10k

show policy urlset top10k
<!--NeedCopy-->
```

Afficher les jeux d'URL importés

Vous pouvez désormais afficher des jeux d'URL importés en plus des jeux d'URL ajoutés. Pour ce faire, un nouveau paramètre « importé » est ajouté à la commande « show url set ». Si vous activez cette option, l'appliance affiche tous les jeux d'URL importés et distingue les jeux d'URL importés des jeux d'URL ajoutés.

À l'invite de commandes, tapez :

```
show policy urlset [<name>] [-imported]
```

Exemple :

```
show policy urlset -imported
```

Pour importer un ensemble d'URL à l'aide de l'interface graphique

Accédez à **AppExpert** > **Jeux d'URL**, cliquez sur **Importer** pour télécharger le jeu d'URL.

Pour ajouter un ensemble d'URL à l'aide de l'interface graphique

Accédez à **AppExpert** > **Jeux d'URL**, cliquez sur **Ajouter** pour créer un fichier de jeu d'URL pour le jeu d'URL téléchargé.

Pour modifier un ensemble d'URL à l'aide de l'interface graphique

Accédez à **AppExpert** > **Jeux d'URL**, sélectionnez un jeu d'URL et cliquez sur **Modifier** pour modifier.

Pour mettre à jour un ensemble d'URL à l'aide de l'interface graphique

Accédez à **AppExpert** > **Jeux d'URL,** sélectionnez un jeu d'URL et cliquez sur **Mettre à jour le jeu** d'URL pour mettre à jour le jeu d'URL avec les dernières modifications apportées au fichier.

Pour exporter un ensemble d'URL à l'aide de l'interface graphique

Accédez à **AppExpert > Jeux d'URL**, sélectionnez un jeu d'URL, puis cliquez sur **Exporter le jeu** d'URL pour exporter les modèles d'URL d'un ensemble vers une URL de destination et l'enregistrer à cet emplacement.

Sémantique des modèles d'URL

August 20, 2021

Le tableau suivant présente les modèles d'URL utilisés pour spécifier la liste des pages que vous souhaitez filtrer. Par exemple, le modèle d'URL `http://www.example.com/bar` correspond à une seule page `http://www.example.com/bar`. Pour couvrir toutes les pages où l'URL commence par www.example.com/bar, vous devez ajouter explicitement un « * » à la fin.

Pour plus d'informations, voir Tableau de mappage des métadonnées de modèle d'URL .

Catégories d'URL

August 20, 2021

Voici une liste des catégories sur la liste noire.

S.non	Catégories sur la liste noire
1	Activités illégales
2	Drogues illicites
3	Médicaments
4	Marijuana
5	Terrorisme/extrémistes
6	Armes
7	Haine/calomnie
8	Violence/suicide
9	Défense d'intérêts en général
10	Adulte/pornographie
11	Nudité

S.non	Catégories sur la liste noire
12	Services sexuels
13	Recherche/liens pour adultes
14	Piratage/décodage
15	Malware
16	Proxies distants
17	Caches du moteur de recherche
18	Traducteurs
19	Rencontres
20	Mariage
21	Taux du marché
22	Négoce en ligne
23	Assurance
24	Produits financiers
25	Jeux d’argent en général
26	Loterie
27	Jeux en ligne
28	Jeux
29	Enchères
30	Shopping/vente au détail
31	Immobilier
32	Achats informatiques en ligne
33	Chat en ligne
34	Messages instantanés
35	Courrier basé sur le Web
36	Abonnements par e-Mail
37	Bulletins électroniques
38	Bulletins informatiques
39	Pages Web personnelles/blogs
40	Téléchargements

S.non	Catégories sur la liste noire
41	Téléchargements de programmes
42	Services de stockage
43	Streaming de multimédia
44	Emploi
45	Avancement professionnel
46	Activités parallèles
47	Grotesque
48	Événements spéciaux
49	Sujets populaires
50	Magazine/actualités pour adultes
51	Fumer
52	Boissons
53	Produits alcoolisés
54	Fétiche
55	Expression sexuelle (texte)
56	Costume/divertissement
57	Occulte
58	Maison et famille
59	Sports professionnels
60	Sports en général
61	Événements de la vie
62	Voyage et tourisme
63	Agence publique de tourisme
64	Transport public
65	Hébergement
66	Musique
67	Horoscope /astrologie/voyance
68	Artiste/célébrité
69	Restaurant/gastronomie

S.non	Catégories sur la liste noire
70	Divertissements/lieux/activités
71	Religions traditionnelles
72	Religions
73	Politique
74	Publicités/bannières
75	Concours/prix
76	SPAM
77	Actualités
78	Automobile
79	Affaires et Commercial
80	Informatique et Internet
81	Éducation
82	Gouvernement
83	Intégrité
84	Téléphonie Internet
85	Militaire
86	Peer to Peer/Torrents
87	Loisirs et hobbies
88	Référence
89	Moteurs de recherche et portails
90	Éducation sexuelle
91	Services de SMS et de téléphonie mobile
92	Applications mobiles et éditeurs
93	Spyware
94	Réseaux de distribution de contenu et infrastructure
95	Sites pour enfants
96	Maillots de bain et lingerie
97	Événements artistiques et culturels

S.non	Catégories sur la liste noire
98	Sites d’hébergement
99	Organisations philanthropiques à but non lucratif
100	Sites de recherche et de partage de photos
101	Sonneries
102	Mode et beauté
103	App Stores pour mobiles
104	Domaines parqués
105	Émoticônes
106	Opérateurs mobiles
107	Botnets
108	Sites infectés
109	Sites de phishing
110	Keyloggers
111	Malware sur mobiles
112	Aucun contenu
113	Agriculture
114	Architecture
115	Associations/groupements d’affiliation/syndicats
116	Livres/eBooks
117	Bot de type rappel (phone home)
118	DDNS
119	URL non prise en charge
120	Loi
121	Communautés locales
122	Divers
123	Magazines en ligne
124	Animaux/vétérinaire

S.non	Catégories sur la liste noire
125	Piratage et usurpation de droits d'auteur
126	Adresses IP privées
127	Recyclage/environnement
128	Science
129	Société et culture
130	Services de transport et de fret
131	Photographie et film
132	Musées et histoire
133	Formation en ligne
134	Réseaux sociaux en général
135	Facebook
136	Facebook : Publication
137	Facebook : Commenter
138	Facebook : Amis
139	Facebook : Charger des photos
140	Facebook : Événements
141	Facebook : Applications
142	Facebook : Chat
143	Facebook : Questions
144	Facebook : Chargement de vidéos
145	Facebook : Groupes
146	Facebook : Jeux
147	LinkedIn
148	LinkedIn : Mises à jour
149	LinkedIn : Messages
150	LinkedIn : Connexions
151	LinkedIn : Emplois
152	Twitter
153	Twitter : Publication

S.non	Catégories sur la liste noire
154	Twitter : Messages
155	Twitter : Suivre
156	Youtube
157	YouTube : Commenter
158	YouTube : Chargement de vidéos
159	YouTube : Partage
160	Instagram
161	Instagram : Charger
162	Instagram : Commenter
163	Instagram : Message privé
164	Tumblr
165	Tumblr : Publication
166	Tumblr : Commenter
167	Tumblr : Chargement de photos ou de vidéos
168	Google+
169	Google+ : Publication
170	Google+ : Commenter
171	Google+ : Chargement de photos
172	Google+ : Chargement de vidéos
173	Google+ : chat vidéo
174	Pinterest
175	Pinterest : Code PIN
176	Vine : Charger
177	Vine : Commenter
178	Vine : Message
179	Ask.fm
180	Ask.fm : Demander
181	Ask.fm : Répondre
182	YikYak

S.non	Catégories sur la liste noire
183	YikYak : Publication
184	YikYak : Commenter
185	Wordpress
186	Wordpress : Publication
187	Wordpress : Charger

AppFlow

October 5, 2021

L'appliance Citrix ADC est un point de contrôle central pour tout le trafic des applications dans le centre de données. Il collecte des informations de flux et de session utilisateur utiles pour la surveillance des performances des applications, l'analyse et les applications de Business Intelligence. Il collecte également des données sur les performances des pages Web et des informations de base de données. AppFlow transmet les informations en utilisant le format IPFIX (Internet Protocol Flow Information Export), qui est une norme ouverte de l'Internet Engineering Task Force (IETF) définie dans la RFC 5101. IPFIX (la version normalisée de NetFlow de Cisco) est largement utilisé pour surveiller les informations de flux réseau. AppFlow définit de nouveaux éléments d'information pour représenter des informations au niveau de l'application, des données de performances de page Web et des informations de base de données.

En utilisant UDP comme protocole de transport, AppFlow transmet les données collectées, appelées *enregistrements de flux*, à un ou plusieurs collecteurs IPv4. Les collecteurs regroupent les enregistrements de flux et génèrent des rapports en temps réel ou historiques.

AppFlow offre une visibilité au niveau des transactions pour les flux HTTP, SSL, TCP, SSL_TCP et HDX Insight. Vous pouvez échantillonner et filtrer les types de flux que vous souhaitez surveiller.

> **Remarque**
>
> Pour plus d'informations sur HDX Insight, consultez HDX Insight.

AppFlow utilise des actions et des stratégies pour envoyer des enregistrements pour un flux sélectionné à un ensemble de collecteurs spécifique. Une action AppFlow spécifie quel ensemble de collecteurs reçoit les enregistrements AppFlow. Les stratégies basées sur des expressions avancées peuvent être configurées pour sélectionner les flux pour lesquels des enregistrements de flux sont envoyés aux collecteurs spécifiés par l'action AppFlow associée.

Pour limiter les types de flux, vous pouvez activer AppFlow pour un serveur virtuel. AppFlow peut également fournir des statistiques pour le serveur virtuel.

Vous pouvez également activer AppFlow pour un service spécifique, représentant un serveur d'applications, et surveiller le trafic vers ce serveur d'applications.

Remarque : Cette fonctionnalité n'est prise en charge que sur les versions Citrix ADC nCore.

Fonctionnement d'AppFlow

Dans le scénario de déploiement le plus courant, le trafic entrant circule vers une adresse IP virtuelle (VIP) sur l'appliance Citrix ADC et est équilibré en charge sur un serveur. Le trafic sortant circule du serveur vers une adresse IP mappée ou de sous-réseau sur Citrix ADC et de l'adresse IP VIP vers le client. Un flux est un ensemble unidirectionnel de paquets IP identifiés par les cinq n-uplets suivants : SourceIP, SourcePort, DEStip, DestPort et protocole.

La figure suivante décrit le fonctionnement de la fonctionnalité AppFlow.

Figure 1. Séquence de flux Citrix ADC



Comme le montre la figure, les identificateurs de flux réseau pour chaque segment d'une transaction dépendent de la direction du trafic.

Les différents flux qui forment un enregistrement de flux sont les suivants :

Flux 1 : <Client-IP, Client-Port, VIP-IP, VIP-port, Protocol>

Débit 2 : <NS-MIP/SNIP, NS-port, Server-IP, Server-Port, Protocol>

Flux 3 : <Server-IP, Server-Port, NS-MIP/SNIP, NS-Port, Protocol>

Flux 4 : <VIP-IP, VIP-port, Client-IP, Client-Port, Protocol>

Pour aider le collecteur à lier les quatre flux d'une transaction, AppFlow ajoute un élément TransactionID personnalisé à chaque flux. Pour la commutation de contenu au niveau de l'application, telle que HTTP, il est possible d'équilibrer la charge d'une connexion TCP client unique sur différentes connexions TCP dorsales pour chaque demande. AppFlow fournit un ensemble d'enregistrements pour chaque transaction.

Enregistrements de flux

Les enregistrements AppFlow contiennent des informations NetFlow ou IPFIX standard, telles que les horodatages pour le début et la fin d'un flux, le nombre de paquets et le nombre d'octets. Les enregistrements AppFlow contiennent également des informations au niveau de l'application (telles que les URL HTTP, les méthodes de requête HTTP et les codes d'état de réponse, le temps de réponse du serveur et la latence). Données de performances de la page Web (telles que le temps de chargement de la page, le temps de rendu de la page et le temps passé sur la page). Et les informations de base de données (telles que le protocole de base de données, l'état de la réponse de base de données et la taille de la réponse Les enregistrements de flux IPFIX sont basés sur des modèles qui doivent être envoyés avant d'envoyer des enregistrements de flux.

Modèles

AppFlow définit un ensemble de modèles, un pour chaque type de flux. Chaque modèle contient un ensemble d'éléments d'information (IE) standard et d'éléments d'information spécifiques à l'entreprise (EIE). Les modèles IPFIX définissent l'ordre et la taille des éléments d'information (Internet Explorer) dans l'enregistrement de flux. Les modèles sont envoyés aux collecteurs à intervalles réguliers, comme décrit dans la RFC 5101.

Un modèle peut inclure les EIE suivants :

- transactionID

  Numéro 32 bits non signé identifiant une transaction au niveau de l'application. Pour HTTP, il correspond à une paire requêtes et réponses. Tous les enregistrements de flux qui correspondent à cette paire demande et réponse ont le même ID de transaction. Dans le cas le plus courant, quatre `uniflow` enregistrements correspondent à cette transaction. Si Citrix ADC génère la réponse par lui-même (servie à partir du cache intégré ou par une stratégie de sécurité), il peut y avoir seulement deux enregistrements de flux pour cette transaction.

- connectionID

  Numéro 32 bits non signé identifiant une connexion de couche 4 (TCP ou UDP). Les flux Citrix ADC sont bidirectionnels, avec deux enregistrements de flux distincts pour chaque direction du flux. Cet élément d'information peut être utilisé pour relier les deux flux.

  Pour Citrix ADC, un ID de connexion est un identificateur de la structure de données de connexion permettant de suivre la progression d'une connexion. Dans une transaction HTTP, par exemple, un ConnectionID donné peut comporter plusieurs éléments TransactionID correspondant à plusieurs requêtes effectuées sur cette connexion.

- TCPRTT

  Temps aller-retour, en millisecondes, mesuré sur la connexion TCP. Il peut être utilisé comme mesure pour déterminer la latence du client ou du serveur sur le réseau.

- httpRequestMethod

  Numéro 8 bits indiquant la méthode HTTP utilisée dans la transaction. Un modèle d'options avec le mappage number-to-method est envoyé avec le modèle.

- httpRequestSize

  Numéro 32 bits non signé indiquant la taille de la charge utile de la demande.

- httpRequestURL

  URL HTTP demandée par le client.

- httpUserAgent

  Source des demandes entrantes adressées au serveur Web.

- httpResponseStatus

  Numéro 32 bits non signé indiquant le code d'état de la réponse.

- httpResponseSize

  Un numéro 32 bits non signé indiquant la taille de la réponse.

- httpResponseTimeToFirstByte

  Un numéro 32 bits non signé indiquant le temps nécessaire à la réception du premier octet de la réponse.

- httpResponseTimeToLastByte

  Numéro 32 bits non signé indiquant le temps nécessaire à la réception du dernier octet de la réponse.

- flowFlags

  Indicateur 64 bits non signé utilisé pour indiquer différentes conditions de flux.

EIE pour les données de performance des pages Web

- clientInteractionStartTime

  Heure à laquelle le navigateur reçoit le premier octet de la réponse pour charger les objets de la page tels que les images, les scripts et les feuilles de style.

- clientInteractionEndTime

  Heure à laquelle le navigateur a reçu le dernier octet de réponse pour charger tous les objets de la page tels que les images, les scripts et les feuilles de style.

- clientRenderStartTime

  Heure à laquelle le navigateur commence à afficher la page.

- clientRenderEndTime

  Heure à laquelle un navigateur a terminé le rendu de la page entière, y compris les objets incorporés.

EIE pour les informations de base de données

- dbProtocolName

  Numéro 8 bits non signé indiquant le protocole de base de données. Les valeurs valides sont 1 pour MS SQL et 2 pour MySQL.

- dbReqType

  Numéro 8 bits non signé indiquant la méthode de demande de base de données utilisée dans la transaction. Pour MS SQL, les valeurs valides sont 1 pour QUERY, 2 pour TRANSACTION et 3 pour RPC. Pour connaître les valeurs valides pour MySQL, consultez la documentation MySQL.

- dbReqString

  Indique la chaîne de requête de base de données sans l'en-tête.

- dbRespStatus

  Numéro 64 bits non signé indiquant l'état de la réponse de base de données reçue du serveur Web.

- dbRespLength

  Nombre 64 bits non signé indiquant la taille de la réponse.

- dbRespStatString

  Chaîne d'état de réponse reçue du serveur Web.

Configuration de la fonctionnalité AppFlow

August 20, 2021

Vous configurez AppFlow de la même manière que la plupart des autres fonctionnalités basées sur des stratégies. Tout d'abord, vous activez la fonctionnalité AppFlow. Ensuite, vous spécifiez les collecteurs auxquels les enregistrements de flux sont envoyés. Après cela, vous définissez des actions, qui sont des ensembles de collecteurs configurés. Ensuite, vous configurez une ou plusieurs stratégies et associez une action à chaque stratégie. La stratégie indique à l'appliance Citrix ADC de sélectionner les demandes dont les enregistrements de flux sont envoyés à l'action associée. Enfin, vous liez chaque stratégie globalement ou au serveur virtuel spécifique pour la mettre en œuvre.

Vous pouvez définir davantage les paramètres AppFlow pour spécifier l'intervalle d'actualisation du modèle et activer l'exportation des informations HttpURL, HttpCookie et HttPreferer. Sur chaque collecteur, vous devez spécifier l'adresse IP Citrix ADC comme adresse de l'exportateur.

> **Remarque**
>
> Pour plus d'informations sur la configuration de Citrix ADC en tant qu'exportateur sur le collecteur, consultez la documentation du collecteur spécifique.

L'utilitaire de configuration fournit des outils qui aident les utilisateurs à définir les stratégies et les actions. Il détermine exactement comment l'appliance Citrix ADC exporte les enregistrements d'un flux particulier vers un ensemble de collecteurs (action). L'interface de ligne de commande fournit un ensemble correspondant de commandes basées sur l'API pour les utilisateurs expérimentés qui préfèrent une ligne de commande.

Activation d'AppFlow

Pour pouvoir utiliser la fonctionnalité AppFlow, vous devez d'abord l'activer.

> **Remarque**
>
> AppFlow peut être activé uniquement sur les appliances NCore Citrix ADC.

Pour activer la fonctionnalité AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
enable ns feature AppFlow
<!--NeedCopy-->
```

Pour activer la fonctionnalité AppFlow à l'aide de l'utilitaire de configuration

Accédez à **Système > Paramètres**, cliquez sur **Configurer les fonctionnalités avancées**, puis sélectionnez l'option **AppFlow** .

Spécification d'un collecteur

Un collecteur reçoit les enregistrements AppFlow générés par l'appliance Citrix ADC. Pour envoyer les enregistrements AppFlow, vous devez spécifier au moins un collecteur. Par défaut, le collecteur écoute les messages IPFIX sur le port UDP 4739. Vous pouvez modifier le port par défaut lors de la configuration du collecteur. De même, par défaut, NSIP est utilisé comme adresse IP source pour le trafic AppFlow. Vous pouvez modifier cette adresse IP source par défaut en une adresse SNIP lors de la configuration d'un collecteur. Vous pouvez également supprimer les collecteurs inutilisés.

Pour spécifier un collecteur à l'aide de l'interface de ligne de commande

> **Important**
>
> À partir de Citrix ADC version 12.1 build 55.13, vous pouvez spécifier le type de collecteur que vous souhaitez utiliser. Un nouveau paramètre « Transport » est introduit dans la `add appflow collector` commande. Par défaut, le collecteur écoute les messages IPFIX. Vous pouvez modifier le type de collecteur `logstreamipfix` ou de repos en utilisant le paramètre « Transport ». Pour plus d'informations sur la configuration, consultez l'exemple.

À l'invite de commandes, tapez les commandes suivantes pour ajouter un collecteur et vérifier la configuration :

```
1 -  add appflow collector <name> -IPAddress <ipaddress> -port <
     port_number> -netprofile <netprofile_name> -Transport <Transport>
2
3 -  show appflow collector <name>
4 <!--NeedCopy-->
```

Exemple

```
1 add appflow collector col1 -IPaddress 10.102.29.251 -port 8000 -
     netprofile n2 -Transport ipfix
2 <!--NeedCopy-->
```

Pour spécifier plusieurs collecteurs à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter et envoyer les mêmes données à plusieurs collecteurs :

```
1  add appflow collector <collector1> -IPAddress <IP>
2
3  add appflow collector <collector2> -IPAddress <IP>
4
5  add appflow action <action> -collectors <collector1> <collector2>
6
7  add appflow policy <policy> true <action>
8
9  bind lbvserver <lbvserver> -policy <policy> -priority <priority>
10 <!--NeedCopy-->
```


Pour spécifier un ou plusieurs collecteurs à l'aide de l'utilitaire de configuration

Accédez à **Système > AppFlow > Collecteurs**et créez le collecteur AppFlow.

Configuration d'une action AppFlow

Une action AppFlow est un collecteur de jeux, auquel les enregistrements de flux sont envoyés si la stratégie AppFlow associée correspond.

Pour configurer une action AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une action AppFlow et vérifier la configuration :

```
1 add appflow action <name> --collectors <string> ... [-
     clientSideMeasurements (Enabled|Disabled) ] [-comment <string>]
2
3 show appflow action
4 <!--NeedCopy-->
```

Exemple

```
1 add appflow action apfl-act-collector-1-and-3 -collectors collector-1
     collecter-3
2 <!--NeedCopy-->
```

Pour configurer une action AppFlow à l'aide de l'utilitaire de configuration

Accédez à **Système > AppFlow > Actions**, puis créez l'action AppFlow.

Configuration d'une stratégie AppFlow

Après avoir configuré une action AppFlow, vous devez ensuite configurer une stratégie AppFlow. Une stratégie AppFlow est basée sur une règle, qui consiste en une ou plusieurs expressions.

> **Remarque**
>
> Pour créer et gérer des stratégies AppFlow, l'utilitaire de configuration fournit une assistance qui n'est pas disponible sur l'interface de ligne de commande.

Pour configurer une stratégie AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour ajouter une stratégie AppFlow et vérifier la configuration :

```
1 add appflow policy <name> <rule> <action>
2
3 show appflow policy <name>
4 <!--NeedCopy-->
```

Exemple

```
1 add appflow policy apfl-pol-tcp-dsprt client.TCP.DSTPORT.EQ(22) apfl-
     act-collector-1-and-3
2 <!--NeedCopy-->
```

Pour configurer une stratégie AppFlow à l'aide de l'utilitaire de configuration

Accédez à **Système > AppFlow > Stratégies**et créez la stratégie AppFlow.

Pour ajouter une expression à l'aide de la boîte de dialogue Ajouter une expression

1. Dans la boîte de dialogue Ajouter une expression, dans la première zone de liste, choisissez le premier terme de votre expression.
   - HTTP
     Protocole HTTP. Choisissez l'option si vous souhaitez examiner certains aspects de la requête qui se rapportent au protocole HTTP.
   - SSL

     Les sites Web protégés. Choisissez l'option si vous souhaitez examiner un aspect de la demande qui concerne le destinataire de la demande.
   - CLIENT

     Ordinateur qui a envoyé la demande. Choisissez l'option si vous souhaitez examiner certains aspects de l'expéditeur de la demande.
     Lorsque vous faites votre choix, la zone de liste la plus à droite répertorie les termes appropriés pour la partie suivante de votre expression.
2. Dans la deuxième zone de liste, choisissez le deuxième terme pour votre expression. Les choix dépendent du choix que vous avez fait à l'étape précédente et sont adaptés au contexte. Après

avoir fait votre deuxième choix, la fenêtre d'aide située sous la fenêtre Construire une expression (qui était vide) affiche de l'aide décrivant le but et l'utilisation du terme que vous venez de choisir.

3. Continuez à choisir des termes dans les zones de liste qui apparaissent à droite de la zone de liste précédente, ou à taper des chaînes ou des nombres dans les zones de texte qui s'affichent pour vous inviter à entrer une valeur, jusqu'à ce que votre expression soit terminée.

Liaison d'une stratégie AppFlow

Pour mettre une stratégie en œuvre, vous devez la lier globalement, de sorte qu'elle s'applique à tout le trafic qui circule via Citrix ADC, ou à un serveur virtuel spécifique, de sorte que la stratégie ne s'applique qu'au trafic lié à ce serveur virtuel.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel entier positif.

Dans le système d'exploitation Citrix ADC, les priorités de stratégie fonctionnent dans l'ordre inverse : plus le nombre est élevé, plus la priorité est faible. Par exemple, si vous disposez de trois stratégies dont les priorités sont de 10, 100 et 1000, la stratégie attribuée à une priorité de 10 est exécutée en premier. Plus tard, la stratégie affectée avec une priorité de 100, et enfin la stratégie a attribué un ordre de 1000.

Vous pouvez vous laisser suffisamment d'espace pour ajouter d'autres stratégies dans n'importe quel ordre, et toujours les définir pour les évaluer dans l'ordre souhaité. Vous pouvez y parvenir en définissant des priorités avec des intervalles de 50 ou 100 entre chaque stratégie lorsque vous la liez globalement. Vous pouvez ensuite ajouter d'autres stratégies à tout moment sans avoir à modifier la priorité d'une stratégie existante.

Pour lier globalement une stratégie AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour lier globalement une stratégie AppFlow et vérifier la configuration :

```
1 bind appflow global <policyName> <priority> [<gotoPriorityExpression [-
     type <type>] [-invoke (<labelType> <labelName>)]
2
3 show appflow global
4 <!--NeedCopy-->
```

Exemple


```
bind appflow global af_policy_lb1_10.102.71.190 1 NEXT -type
   REQ_OVERRIDE -invoke vserver google
<!--NeedCopy-->
```

Pour lier une stratégie AppFlow à un serveur virtuel spécifique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour lier une stratégie AppFlow à un serveur virtuel spécifique et vérifiez la configuration :

```
bind lb vserver <name> -policyname <policy_name> -priority <priority>
<!--NeedCopy-->
```

Exemple

```
bind lb vserver google -policyname af_policy_google_10.102.19.179 -
   priority 251
<!--NeedCopy-->
```

Pour lier globalement une stratégie AppFlow à l'aide de l'utilitaire de configuration

Accédez à **Système > AppFlow**, cliquez sur **Gestionnaire de stratégies AppFlow**, puis sélectionnez le point de liaison (global par défaut) et le type de connexion, puis liez la stratégie AppFlow.

Pour lier une stratégie AppFlow à un serveur virtuel spécifique à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, sélectionnez le serveur virtuel, cliquez sur **Stratégies**, puis liez la stratégie AppFlow.

Activation d'AppFlow pour les serveurs virtuels

Si vous souhaitez surveiller uniquement le trafic via certains serveurs virtuels, activez AppFlow spécifiquement pour ces serveurs virtuels. Vous pouvez activer AppFlow pour l'équilibrage de charge, la commutation de contenu, la redirection de cache, le VPN SSL, le GSLB et l'authentification des serveurs virtuels.

Pour activer AppFlow pour un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cs vserver <name> <protocol> <IPAddress> <port> -appflowLog ENABLED
<!--NeedCopy-->
```

Exemple

```
set cs vserver Vserver-CS-1 HTTP 10.102.29.161 80 -appflowLog ENABLED
<!--NeedCopy-->
```

Pour activer AppFlow pour un serveur virtuel à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Changement de contenu > Serveurs virtuels**, sélectionnez le serveur virtuel et activez l'option de journalisation AppFlow.

Activation d'AppFlow pour un service

Vous pouvez activer AppFlow pour les services qui doivent être liés aux serveurs virtuels d'équilibrage de charge.

Pour activer AppFlow pour un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -appflowLog ENABLED
<!--NeedCopy-->
```

Exemple

```
set service ser -appflowLog ENABLED
<!--NeedCopy-->
```

Pour activer AppFlow pour un service à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services**, sélectionnez le service et activez l'option Journalisation AppFlow.

Définition des paramètres AppFlow

Vous pouvez définir des paramètres AppFlow pour personnaliser l'exportation des données vers les collecteurs.

Pour définir les paramètres AppFlow à l'aide de l'interface de ligne de commande

> **Important**
>
> - À partir de Citrix ADC version 12.1 build 55.13, vous pouvez utiliser le NSIP pour envoyer `Logstream` des enregistrements au lieu du SNIP. Un nouveau paramètre « LogStreaMovern-SIP » est introduit dans la `set appflow param` commande. Par défaut, le paramètre « LogStreamoVernSip » est DÉSACTIVÉ, vous devez « ACTIVER ». Pour plus d'informations sur la configuration, consultez l'exemple.
> - À partir de Citrix ADC version 13.0 build 58.x, vous pouvez activer l'option d'application Web SaaS dans la fonctionnalité AppFlow. Il peut être activé pour recevoir l'utilisation des données des applications Web ou SaaS à partir du service Citrix Gateway. Pour plus d'informations sur la configuration, consultez l'exemple.

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres AppFlow et vérifier les paramètres :

```
1 -  set appflow param [-templateRefresh <secs>] [-appnameRefresh <secs>]
      [-flowRecordInterval <secs>] [-udpPmtu <positive_integer>] [-
     httpUrl ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-httpCookie ( \*\*
     ENABLED\*\* | \*\*DISABLED\*\* )] [-httpReferer ( \*\*ENABLED\*\* |
     \*\*DISABLED\*\* )] [-httpMethod ( \*\*ENABLED\*\* | \*\*DISABLED
     \*\* )] [-httpHost ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
     httpUserAgent ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
     httpXForwardedFor ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )][-
     clientTrafficOnly ( \*\*YES\*\* | \*\*NO\*\*)] [-
     webSaaSAppUsageReporting ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
     logstreamOverNSIP ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )]
2
3 -  show appflow Param
4 <!--NeedCopy-->
```

Exemple

```
1 set appflow Param -templateRefresh 240 -udpPmtu 128 -httpUrl enabled -
     webSaaSAppUsageReporting ENABLED -logstreamOverNSIP ENABLED
2 <!--NeedCopy-->
```


Pour définir les paramètres AppFlow à l'aide de l'utilitaire de configuration

Accédez à **Système > AppFlow**, cliquez sur **Modifier les paramètres AppFlow**et spécifiez les paramètres AppFlow pertinents.

Prise en charge de l'obfuscation de l'ID d'abonné

À partir de Citrix ADC version 13.0 build 35.xx, la configuration AppFlow est améliorée pour prendre en charge l'algorithme « SubscriberIdObfuscation » pour obscurcir MSISDN dans les enregistrements AppFlow de couche 4 ou 7. Toutefois, avant de configurer l'algorithme en tant que MD5 ou SHA256, vous devez d'abord l'activer en tant que paramètre AppFlow. Le paramètre est désactivé par défaut.

Pour configurer l'algorithme d'obfuscation de l'ID d'abonné à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set appflow param [-subscriberIdObfuscation ( ENABLED | DISABLED )  [-
   subscriberIdObfuscationAlgo ( MD5 | SHA256 )]]
<!--NeedCopy-->
```

Exemple

```
set appflow param  - subscriberIdObfuscation ENABLED  -
   subscriberIdObfuscationAlgo SHA256
<!--NeedCopy-->
```

Pour configurer l'algorithme d'obfuscation de l'ID d'abonné à l'aide de l'interface graphique

1. Accédez à **Système > AppFlow**.
2. Dans le volet détaillé AppFlow, cliquez sur **Modifier le paramètre AppFlow** sous **Paramètres**.
3. Dans la page Configurer les paramètres AppFlow, définissez les paramètres suivants :
   - **Obfuscation de l'ID d'abonné.** Activez l'option d'obfuscation MSISDN dans les enregistrements AppFlow L4/L7.
   - **Identifiant d'abonné Obfuscation Algo.** Sélectionnez le type d'algorithme comme MD5 ou SHA256.
4. Cliquez sur **OK** et **Fermer**.



Exemple : Configuration d'AppFlow pour DataStream

L'exemple suivant illustre la procédure de configuration d'AppFlow for DataStream à l'aide de l'interface de ligne de commande.

```
enable feature appflow

add db user sa password freebsd

add lbvserver lb0 MSSQL 10.102.147.97 1433 -appflowLog ENABLED

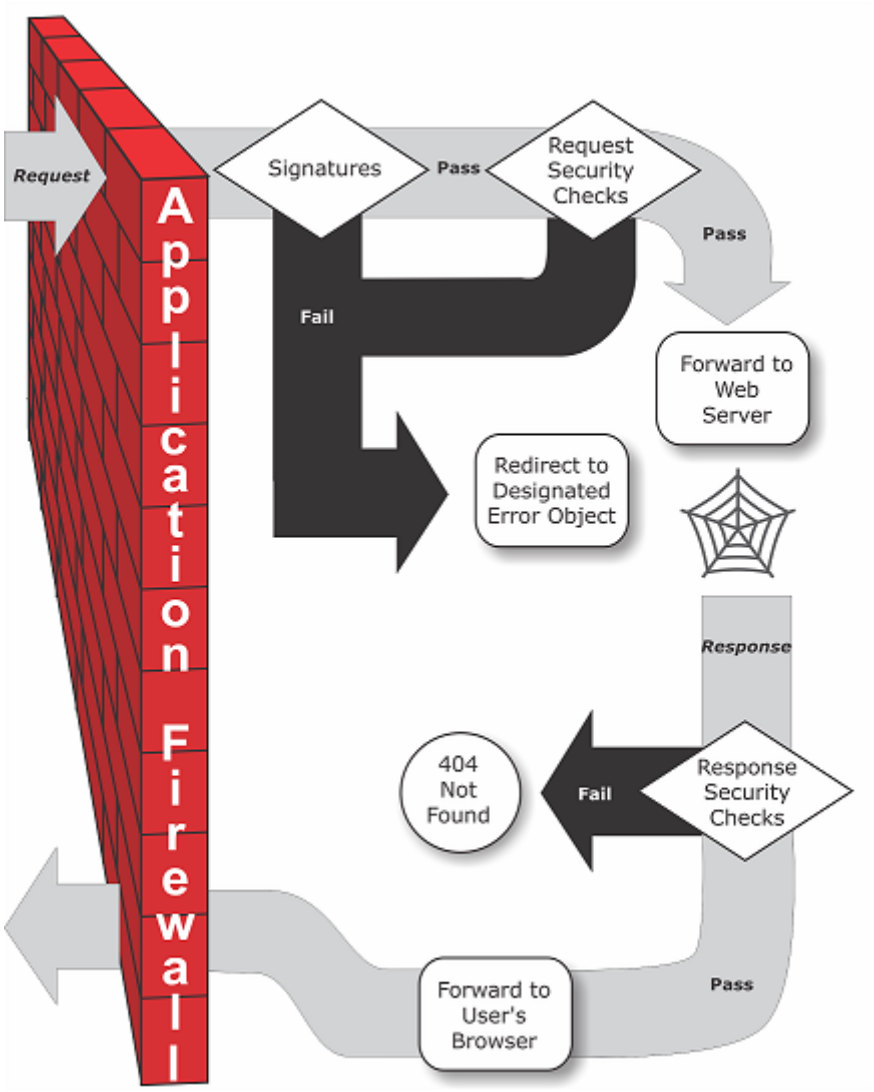
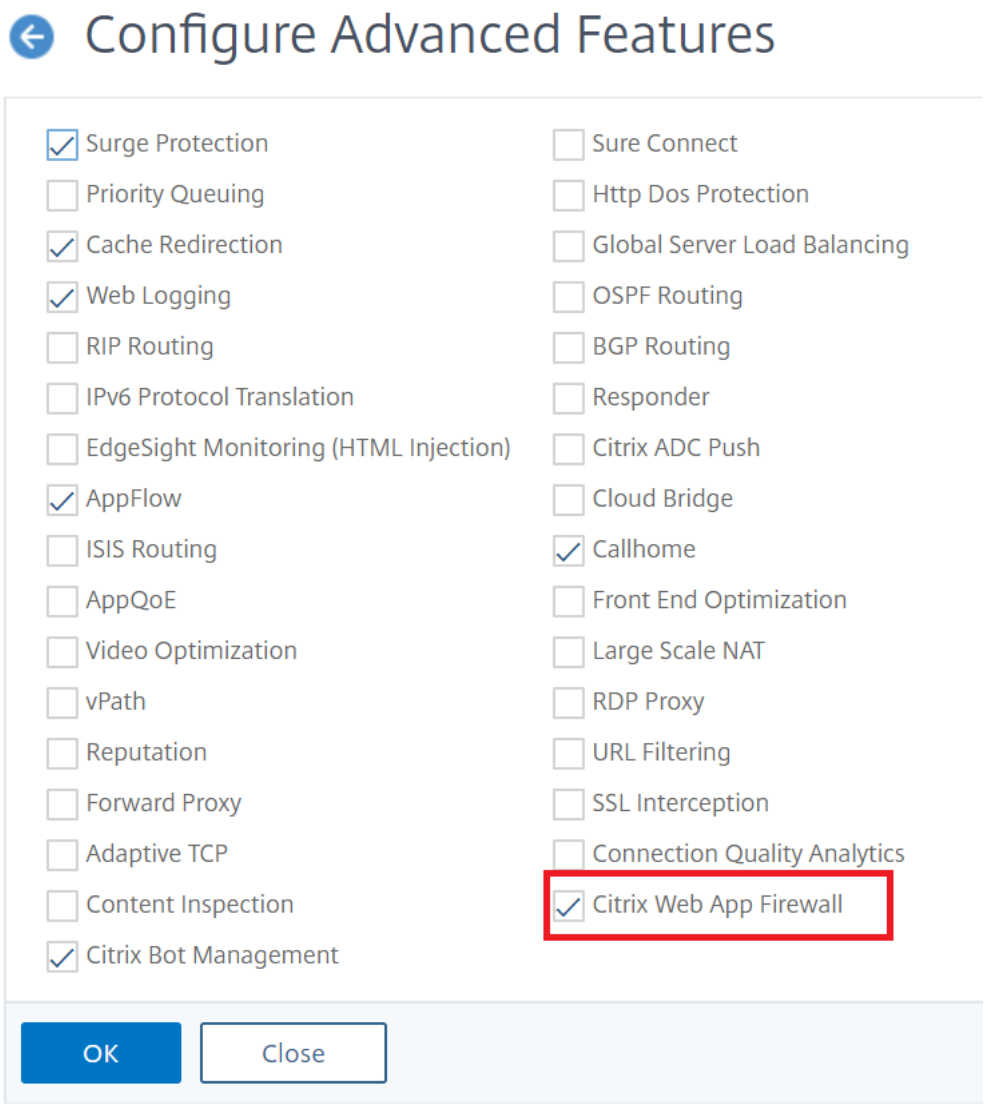
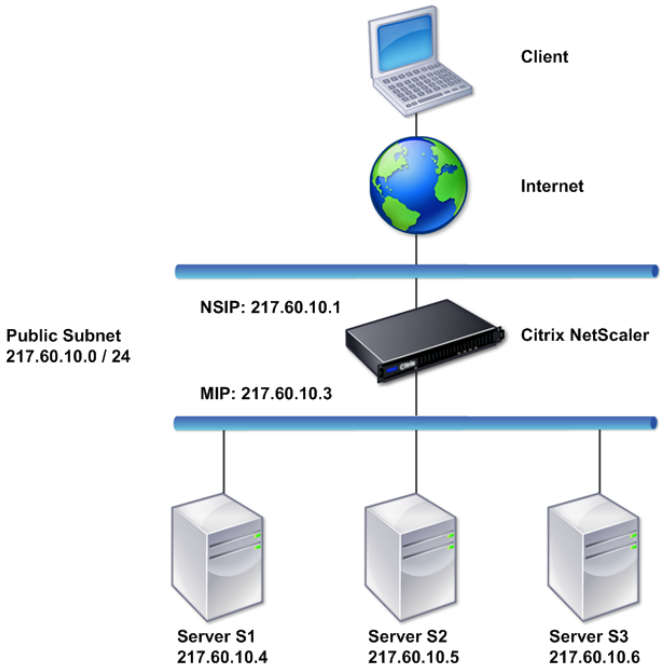
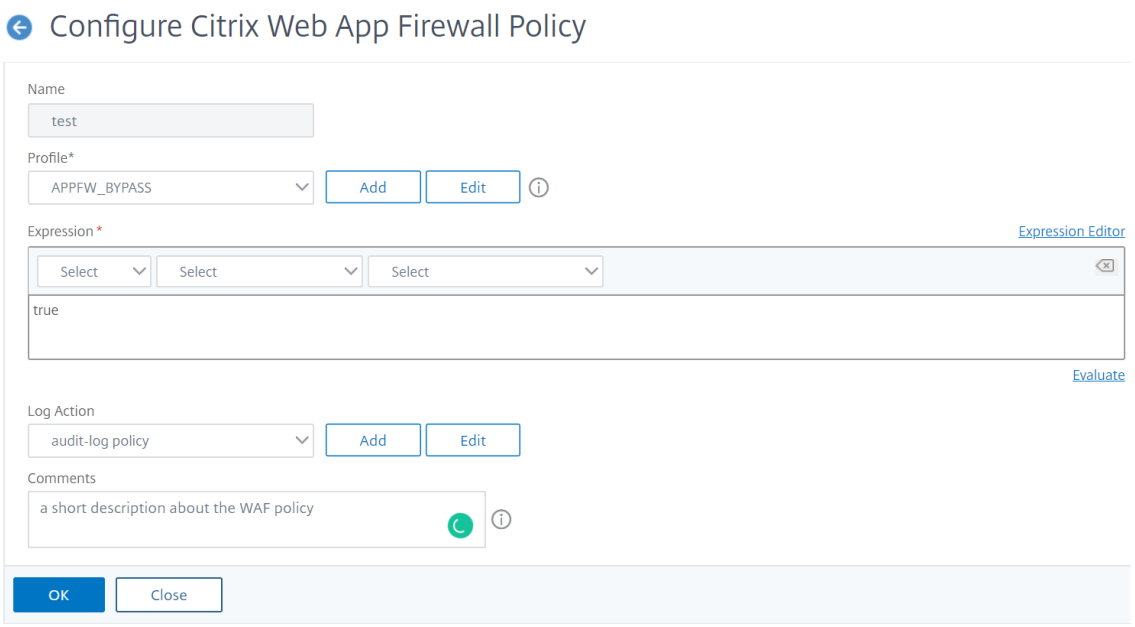
add service sv0 10.103.24.132 MSSQL 1433 -appflowLog ENABLED

```



```
bind lbvserver lb0 sv0

add appflow collector col0 -IPAddress 10.102.147.90

add appflow action act0 -collectors col0

add appflow policy pol0 "mssql.req.query.text.contains("select")" act0

bind lbvserver lb0 -policyName pol0 -priority 10
<!--NeedCopy-->
```

Lorsque l'appliance Citrix ADC reçoit une demande de base de données, l'appliance évalue la demande par rapport à une stratégie configurée. Si une correspondance est trouvée, les détails sont envoyés au collecteur AppFlow configuré dans la stratégie.

Exportation des données de performances des pages Web vers AppFlow Collector

August 20, 2021

L'application EdgeSight Monitoring fournit des données de surveillance des pages Web avec lesquelles vous pouvez surveiller les performances de diverses applications Web desservies dans un environnement Citrix ADC. Vous pouvez désormais exporter ces données vers des collecteurs AppFlow pour obtenir une analyse approfondie des applications de page Web. AppFlow, basé sur la norme IPFIX, fournit des informations plus spécifiques sur les performances des applications Web que la seule surveillance EdgeSight.

Vous pouvez configurer des serveurs virtuels d'équilibrage de charge et de commutation de contenu pour exporter des données EdgeSight Monitoring vers des collecteurs AppFlow. Avant de configurer un serveur virtuel pour l'exportation AppFlow, associez une action AppFlow à la stratégie de réponse EdgeSight Monitoring.

Les données de performances de la page Web suivantes sont exportées vers AppFlow :

- **Temps de chargement de la page**. Temps écoulé, en millisecondes, à partir du moment où le navigateur commence à recevoir le premier octet d'une réponse jusqu'à ce que l'utilisateur commence à interagir avec la page. À ce stade, tout le contenu de la page peut ne pas être chargé.
- **Heure de rendu de la page**. Temps écoulé, en millisecondes, entre le moment où le navigateur reçoit le premier octet de réponse jusqu'à ce que tout le contenu de la page ait été rendu ou que l'action de chargement de page ait expiré.

- **Temps passé sur la page**. Temps passé par les utilisateurs sur une page. Représente le temps écouler entre une demande de page et la suivante.

AppFlow transmet les données de performances à l'aide du format IPFIX (Internet Protocol Flow Information Export), qui est un standard ouvert Internet Engineering Task Force (IETF) défini dans la RFC 5101. Les modèles AppFlow utilisent les éléments d'information spécifiques à l'entreprise (EIE) suivants pour exporter les informations :

- **Heure de fin du chargement du client**. Heure à laquelle le navigateur a reçu le dernier octet d'une réponse pour charger tous les objets de la page tels que les images, les scripts et les feuilles de style.
- **Heure de début du chargement du client**. Heure à laquelle le navigateur reçoit le premier octet de la réponse pour charger tous les objets de la page tels que des images, des scripts et des feuilles de style.
- **Heure de fin du rendu client**. Heure à laquelle un navigateur a terminé le rendu de la page entière, y compris les objets incorporés.
- **Heure de début du rendu client**. Heure à laquelle le navigateur a commencé à rendre la page.

Conditions préalables à l'exportation des données de performances des pages Web vers des collecteurs AppFlow

Avant d'associer l'action AppFlow à la stratégie AppFlow, vérifiez que les conditions préalables suivantes ont été remplies :

- La fonctionnalité AppFlow a été activée et configurée.
- La fonction Répondeur a été activée.
- La fonction EdgeSight Monitoring a été activée.
- La surveillance EdgeSight a été activée sur les serveurs virtuels d'équilibrage de charge ou de commutation de contenu liés aux services des applications pour lesquelles vous souhaitez collecter les données de performances.

Association d'une action AppFlow à la stratégie de réponse EdgeSight monitoring

Pour exporter les données de performances de la page Web vers le collecteur AppFlow, vous devez associer une action AppFlow à la stratégie de réponse EdgeSight Monitoring. Une action AppFlow spécifie quel ensemble de collecteurs reçoit le trafic.

Pour associer une action AppFlow à la stratégie EdgeSight Monitoring Responder à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set responder policy <name> -appflowAction <action_Name>
<!--NeedCopy-->
```

Exemple

```
set responder policy pol -appflowAction actn
<!--NeedCopy-->
```

Pour associer une action AppFlow à la stratégie EdgeSight Monitoring Responder à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Répondeur** > **Stratégies**.
2. Dans le volet d'informations, sélectionnez une stratégie de répondeur EdgeSight Monitoring, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer la stratégie de répondeur**, dans la liste déroulante **Action AppFlow**, sélectionnez l'action AppFlow associée aux collecteurs auxquels vous souhaitez envoyer les données de performances de la page Web.
4. Cliquez sur **OK**.

Configuration d'un serveur virtuel pour exporter les statistiques EdgeSight vers des collecteurs AppFlow

Pour exporter les informations statistiques EdgeSight d'un serveur virtuel vers le collecteur AppFlow, vous devez associer une action AppFlow au serveur virtuel.

Pour associer une action AppFlow à un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**. Vous pouvez également accéder à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels** .
2. Dans le volet d'informations, sélectionnez un serveur virtuel ou plusieurs serveurs virtuels, puis cliquez sur **Activer la surveillance EdgeSight**.
3. Dans la boîte de dialogue Activer la surveillance EdgeSight, activez la case à cocher **Exporter les statistiques EdgeSight vers Appflow** .
4. Dans la liste déroulante Action AppFlow, sélectionnez l'action **AppFlow** . L'action AppFlow définit la liste des collecteurs AppFlow vers lesquels elle exporte les statistiques EdgeSight Monitoring. Si vous avez sélectionné plusieurs serveurs virtuels d'équilibrage de charge, la même

action AppFlow est associée aux stratégies de répondeur qui leur sont liées. Vous pouvez modifier ultérieurement l'action AppFlow configurée pour chacun des serveurs virtuels d'équilibrage de charge sélectionné individuellement, si nécessaire.

5. Cliquez sur **OK**.

Fiabilité de session sur la paire haute disponibilité Citrix ADC

August 20, 2021

Lorsqu'une interruption réseau ou un basculement de périphérique se produit au cours d'une session ICA, la reconnexion de session peut utiliser l'un des deux mécanismes : la fiabilité de session ou la reconnexion automatique du client.

Fiabilité de session. Le mode préféré, est une expérience fluide pour l'utilisateur. La perturbation est à peine perceptible pour de brèves interruptions de réseau.

Reconnexion automatique des clients. L'option de secours implique le redémarrage du client. Ce mécanisme perturbe l'utilisateur et n'est pas toujours pris en charge.

Les récepteurs peuvent reconnecter leurs sessions ICA en toute transparence à l'aide de la fonctionnalité de fiabilité de session ICA, lorsque HDX Insight est activé.
Cette fonctionnalité fonctionne à la fois en mode autonome et dans une configuration de paire Citrix ADC HA, et même lorsqu'un basculement sur incident Citrix ADC se produit.

> **Remarque :**
>
> - Les appliances Citrix ADC doivent être exécutées sur la version 11.1 de la version 49.16 ou ultérieure du logiciel.
> - Vous ne devez pas activer ou désactiver le mode de fiabilité de session lorsque les appliances Citrix ADC disposent de connexions actives.
> - L'activation ou la désactivation de la fonctionnalité lorsque les connexions sont toujours actives, HDX Insight arrête l'analyse de ces sessions après un basculement. Cela entraîne la perte d'informations sur les sessions.
> - La fiabilité de session sur une configuration haute disponibilité est désactivée par défaut pour le logiciel Citrix ADC version 11.1 49.16 ou ultérieure. La fiabilité de session est prise en charge sur une configuration haute disponibilité uniquement si les deux nœuds de l'installation exécutent la même version (par exemple, version 11.1 build 53). En d'autres termes, la fiabilité de session n'est pas prise en charge sur une configuration haute disponibilité si les deux nœuds exécutent des versions différentes (par exemple, un nœud a la version 11.1 build 53 alors que l'autre a la version 11.1 build 56). La fiabilité de session pour SSL VDA est prise en charge si les conditions suivantes sont remplies :

> - The "EnableSRonHAFailover" parameter in the `set ica parameter` command must be YES.
> - The HTTPS must be used instead of HTTP while configuring the virtual server.
>
> • Lorsque HDX Insight est activé, les applications de chiffrement de base et les postes de travail se reconnectent après basculement haute disponibilité, même si le paramètre EnableSronhaFailover est désactivé.

Pour configurer la fiabilité de session à l'aide de la CLI :

1. Sur la ligne de commande, utilisez les informations d'identification de l'administrateur système par défaut pour ouvrir une session sur le système.
2. Pour activer la fiabilité de session en cas de basculement HA, à l'invite, tapez : `set ica parameter EnableSRonHAFailover YES`
3. Pour désactiver la fiabilité de session en cas de basculement HA, à l'invite, tapez : `set ica parameter EnableSRonHAFailover NO`

Pour activer la fiabilité de session en cas de basculement HA à l'aide de l'interface graphique :

1. Dans un navigateur Web, tapez l'adresse IP de l'instance principale de Citrix ADC dans la paire HA (par exemple, http://192.168.100.1).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Sous l'onglet **Configuration**, accédez à **Système** > **Paramètres**, puis cliquez sur **Modifier les paramètres ICA** .
4. Dans la section **Modifier les paramètres ICA**, sélectionnez **Fiabilité de session sur basculement HA**.
5. Cliquez sur **OK**.

Limitations

- L'activation de cette fonctionnalité entraîne une augmentation de la consommation de bande passante due à la désactivation de la compression ICA par la fonction. Et le trafic supplémentaire entre les nœuds principal et secondaire pour les garder synchronisés.
- Cette fonctionnalité est prise en charge en mode Active-Passif uniquement. Le mode actif n'est pas actuellement pris en charge.
- Lorsque HDX Insight est activé et que la fiabilité de session sur le bouton HA est définie sur NO, seul le mode de reconnexion ACR est pris en charge dans le scénario de basculement haute disponibilité Citrix ADC. Le bouton HA ne désactive pas la fiabilité de session si HDX Insight est désactivé.

La table **Sémantique de reconnexion** de session est la suivante :

Session reconnecte la sémantique

État	EnableSRonHAFailover Oui	EnableSRonHAFailover Non (valeur par défaut)
HDX Insight activé	Reconnexion de session pour les sessions ICA fonctionne	La reconnexion de session pour les sessions ICA ne fonctionne pas
HDX Insight désactivé	Reconnexion de session pour les sessions ICA fonctionne	Reconnexion de session pour ICA Sessions fonctionne

Points à noter

- La fiabilité de session pour les sessions ICA fonctionne très bien avec Citrix Gateway.
- La fiabilité de session pour les sessions ICA ne fonctionne pas UNIQUEMENT lorsque les deux conditions suivantes sont remplies :
  - HDX Insight est activé
  - EnableSronhaFailover est défini sur NO
- La définition du bouton EnableSronhaFaiLover sur YES ou NO ne fait aucune différence lorsque HDX Insight est désactivé.

Citrix Web App Firewall

August 20, 2021

Les rubriques suivantes couvrent les détails d'installation et de configuration de la fonctionnalité Citrix Web App Firewall.

Introduction	Vue d'ensemble de la sécurité Web et du fonctionnement du Web App Firewall.
Configuration	Comment configurer le Web App Firewall pour protéger un site Web, un service Web ou un site Web 2.0.
Signatures	Description détaillée des signatures et comment les configurer à partir d'un outil d'analyse des vulnérabilités pris en charge, et définir vos propres signatures, avec des exemples.

Vue d'ensemble des contrôles de sécurité	Description détaillée des vérifications de sécurité du Web App Firewall, avec des informations de configuration et des exemples.
Profils	Description de la façon dont les profils sont configurés et utilisés dans le Web App Firewall.
Stratégies	Description de la façon dont les stratégies sont utilisées lors de la configuration du Web App Firewall, avec des exemples de stratégies utiles.
Importations	Description de la façon dont le Web App Firewall utilise différents types de fichiers importés et comment importer et exporter des fichiers.
Configuration globale	Description des fonctionnalités du Web App Firewall qui s'appliquent à tous les profils et comment les configurer.
Cas d'utilisation	Exemples étendus qui montrent comment configurer le Web App Firewall pour protéger au mieux des types spécifiques de sites Web et de services Web plus complexes.
Journaux, statistiques et rapports	Comment accéder et utiliser les journaux du Web App Firewall, les statistiques et les rapports pour vous aider à configurer le pare-feu Web App.

Le Citrix Web App Firewall offre des options faciles à configurer pour répondre à un large éventail d'exigences en matière de sécurité des applications. Les profils de Web App Firewall, qui consistent en des ensembles de contrôles de sécurité, peuvent être utilisés pour protéger à la fois les demandes et les réponses en fournissant des inspections approfondies au niveau des paquets. Chaque profil inclut une option permettant de sélectionner des protections de base ou des protections avancées. Certaines protections peuvent nécessiter l'utilisation d'autres fichiers. Par exemple, les vérifications de validation xml peuvent nécessiter des fichiers WSDL ou de schéma. Les profils peuvent également utiliser d'autres fichiers, tels que des signatures ou des objets d'erreur. Ces fichiers peuvent être ajoutés localement ou importés à l'avance et enregistrés sur l'appliance pour une utilisation ultérieure.

Chaque stratégie identifie un type de trafic et ce trafic est inspecté pour détecter les violations de contrôle de sécurité spécifiées dans le profil associé à la stratégie. Les stratégies peuvent avoir différents points de liaison, qui déterminent la portée de la stratégie. Par exemple, une stratégie liée à un serveur virtuel spécifique est appelée et évaluée uniquement pour le trafic circulant à travers ce serveur virtuel. Les stratégies sont évaluées dans l'ordre de leurs priorités désignées, et la première qui correspond à la demande ou à la réponse est appliquée.

- Déploiement rapide de la protection par Web App Firewall

  Vous pouvez utiliser la procédure suivante pour un déploiement rapide de la sécurité du Web App Firewall :

  1. Ajoutez un profil Web App Firewall et sélectionnez le type approprié (html, xml, JSON) pour les exigences de sécurité de l'application.
  2. Sélectionnez le niveau de sécurité requis (de base ou avancé).
  3. Ajoutez ou importez les fichiers requis, tels que les signatures ou WSDL.
  4. Configurez le profil pour qu'il utilise les fichiers et apportez les autres modifications nécessaires aux paramètres par défaut.
  5. Ajoutez une stratégie de Web App Firewall pour ce profil.
  6. Liez la stratégie au point de liaison cible et spécifiez la priorité.

- Entités de Web App Firewall

  Profil : un profil Web App Firewall spécifie ce qu'il faut rechercher et ce qu'il faut faire. Il examine à la fois la demande et la réponse afin de déterminer quelles violations potentielles de sécurité doivent être vérifiées et quelles mesures doivent être prises lors du traitement d'une transaction. Un profil peut protéger une charge utile HTML, XML ou HTML et XML. Selon les exigences de sécurité de l'application, vous pouvez créer un profil de base ou un profil avancé. Un profil de base peut protéger contre les attaques connues. Si une sécurité plus élevée est requise, vous pouvez déployer un profil avancé pour permettre un accès contrôlé aux ressources de l'application, bloquant les attaques zéro jour. Cependant, un profil de base peut être modifié pour offrir des protections avancées, et inversement. Plusieurs options d'action (par exemple, bloc, journal, apprentissage et transformation) sont disponibles. Les contrôles de sécurité avancés peuvent utiliser des cookies de session et des balises de formulaire cachées pour contrôler et surveiller les connexions client. Les profils de Web App Firewall peuvent apprendre les violations déclenchées et suggérer les règles de relaxation.

  Protections de base : un profil de base inclut un ensemble préconfiguré de règles de relaxation d'URL de démarrage et de refus d'URL. Ces règles d'assouplissement déterminent quelles demandes doivent être autorisées et celles qui doivent être refusées. Les demandes entrantes sont mises en correspondance avec ces listes et les actions configurées sont appliquées. Cela permet à l'utilisateur de sécuriser les applications avec une configuration minimale pour les règles de relaxation. Les règles d'URL de démarrage protègent contre la navigation forcée. Les vulnérabilités connues des serveurs Web exploitées par les pirates peuvent être détectées et

bloquées en activant un ensemble de règles d'URL de refus par défaut. Les attaques lancées couramment, telles que Buffer Overflow, SQL ou cross-site scripting peuvent également être facilement détectées.

Protections avancées : comme son nom l'indique, les protections avancées sont utilisées pour les applications qui présentent des exigences de sécurité plus élevées. Les règles de relaxation sont configurées pour autoriser l'accès à des données spécifiques et bloquer le reste. Ce modèle de sécurité positif atténue les attaques inconnues, qui peuvent ne pas être détectées par les contrôles de sécurité de base. En plus de toutes les protections de base, un profil avancé assure le suivi d'une session utilisateur en contrôlant la navigation, en vérifiant les cookies, en spécifiant les exigences d'entrée pour différents champs de formulaire et en protégeant contre la falsification de formulaires ou les attaques de falsification de requêtes intersites. L'apprentissage, qui observe le trafic et déploie les relaxations appropriées, est activé par défaut pour de nombreuses vérifications de sécurité. Bien que faciles à utiliser, les protections avancées nécessitent une attention particulière, car elles offrent une sécurité plus étroite, mais nécessitent également plus de traitement et ne permettent pas l'utilisation de la mise en cache, ce qui peut affecter les performances.

Importer—La fonctionnalité d'importation est utile lorsque les profils Web App Firewall doivent utiliser des fichiers externes, c'est-à-dire des fichiers hébergés sur un serveur Web externe ou interne, ou qui doivent être copiés à partir d'une machine locale. Il est utile d'importer un fichier et de le stocker sur l'appliance, en particulier dans les situations où vous devez contrôler l'accès à des sites Web externes, ou lorsque la compilation prend beaucoup de temps, que des fichiers volumineux doivent être synchronisés sur des déploiements HA ou vous pouvez réutiliser un fichier en le copiant sur plusieurs périphériques. Par exemple :

- Les WSDL hébergées sur des serveurs Web externes peuvent être importées localement avant de bloquer l'accès aux sites Web externes.
- Les fichiers de signatures volumineux générés par un outil d'analyse externe tel que Cenzic peuvent être importés et précompilés à l'aide d'un schéma sur l'appliance Citrix.
- Une page d'erreur HTML ou XML personnalisée peut être importée à partir d'un serveur Web externe ou copiée à partir d'un fichier local.

Signatures—Les signatures sont puissantes, car elles utilisent la correspondance de motifs pour détecter les attaques malveillantes et peuvent être configurées pour vérifier à la fois la demande et la réponse d'une transaction. Ils sont une option privilégiée lorsqu'une solution de sécurité personnalisable est nécessaire. Plusieurs choix (par exemple, bloc, journal, apprentissage et transformation) sont disponibles pour l'action à effectuer lorsqu'une correspondance de signature est détectée. Le Web App Firewall dispose d'un objet de signature par défaut intégré composé de plus de 1 300 règles de signature, avec une option permettant d'obtenir les dernières règles à l'aide de la fonctionnalité de mise à jour automatique. Les règles créées par d'autres outils d'analyse peuvent également être importées. L'objet signature peut être per-

sonnalisé en ajoutant de nouvelles règles, qui peuvent fonctionner avec les autres contrôles de sécurité spécifiés dans le profil Web App Firewall. Une règle de signature peut avoir plusieurs modèles et ne peut marquer une violation que lorsque tous les modèles sont appariés, évitant ainsi les faux positifs. Une sélection minutieuse d'un `fastmatch` motif littéral pour une règle peut considérablement optimiser le temps de traitement.

Stratégies—Les stratégies de pare-feu Web App sont utilisées pour filtrer et séparer le trafic en différents types. Cela offre la flexibilité nécessaire pour implémenter différents niveaux de protection de sécurité pour les données de l'application. L'accès aux données hautement sensibles peut être dirigé vers des inspections de sécurité avancées, tandis que les données moins sensibles sont protégées par des inspections de sécurité de base. Les stratégies peuvent également être configurées pour contourner l'inspection de contrôle de sécurité pour un trafic inoffensif. Une sécurité plus élevée nécessite plus de traitement, de sorte que la conception soignée des stratégies peut fournir la sécurité souhaitée ainsi que des performances optimisées. La priorité de la stratégie détermine l'ordre dans lequel elle est évaluée, et son point de liaison détermine la portée de son application.

Résumé

1. Possibilité de sécuriser un large éventail d'applications en protégeant différents types de données, en mettant en œuvre le bon niveau de sécurité pour différentes ressources et en obtenant des performances maximales.
2. Flexibilité pour ajouter ou modifier une configuration de sécurité. Vous pouvez resserrer ou relâcher les contrôles de sécurité en activant ou en désactivant les protections de base et avancées.
3. Option permettant de convertir un profil HTML en profil XML ou Web2.0 (HTML+XML) et inversement, offrant la flexibilité d'ajouter la sécurité pour différents types de charge utile.
4. Des actions facilement déployées pour bloquer les attaques, les surveiller dans les journaux, collecter des statistiques ou même transformer certaines chaînes d'attaque pour les rendre inoffensives.
5. Capacité à détecter les attaques en inspectant les demandes entrantes et à prévenir les fuites de données sensibles en inspectant les réponses envoyées par les serveurs.
6. Possibilité d'apprendre du modèle de trafic pour obtenir des recommandations pour des règles de relaxation facilement modifiables qui peuvent être déployées pour autoriser les exceptions.
7. Modèle de sécurité hybride qui applique la puissance des signatures personnalisables pour bloquer les attaques qui correspondent à des modèles spécifiés, et qui offre la flexibilité d'utiliser les contrôles positifs du modèle de sécurité pour les protections de sécurité de base ou avancées.
8. Disponibilité de rapports de configuration complets, y compris des informations sur la conformité PCI-DSS.

FAQ et guide de déploiement

October 5, 2021

Q : Pourquoi Citrix Web App Firewall est-il le choix privilégié pour sécuriser les applications ?

Avec les fonctionnalités suivantes, le Citrix Web App Firewall offre une solution de sécurité complète :

- **Modèle de sécurité hybride :** le modèle de sécurité hybride Citrix ADC vous permet de tirer parti à la fois d'un modèle de sécurité positif et d'un modèle de sécurité négatif pour proposer une configuration parfaitement adaptée à vos applications.
  - Le**modèle de sécurité positif** protège contre le Buffer Overflow, la manipulation de paramètres CGI-BIN, la manipulation de formulaires et de champs cachés, la navigation forcée, l'empoisonnement des cookies ou des sessions, les listes de contrôle d'accès brisées, les scripts intersites (script intersite), l'injection de commandes, l'injection SQL, le déclenchement d'erreur sensible Fuite d'informations, utilisation non sécurisée de la cryptographie, mauvaise configuration du serveur, portes dérobées et options de débogage, application de la politique basée sur les taux, vulnérabilités bien connues de la plate-forme, exploits zero-day, falsification des demandes intersites (CSRF) et fuite de cartes de crédit et d'autres données sensibles.
  - **Le modèle de sécurité négatif** utilise un ensemble de signatures enrichies pour se protéger contre les vulnérabilités des applications L7 et HTTP. Le Web App Firewall est intégré à plusieurs outils d'analyse tiers, tels que ceux proposés par Cenzic, Qualys, Whitehat et IBM. Les fichiers XSLT intégrés permettent d'importer facilement des règles, qui peuvent être utilisées conjointement avec les règles Snort au format natif. Une fonctionnalité de mise à jour automatique obtient les dernières mises à jour des nouvelles vulnérabilités.

Le modèle de sécurité positif peut être le choix privilégié pour protéger les applications qui ont un besoin élevé de sécurité, car il vous donne la possibilité de contrôler entièrement qui peut accéder à quelles données. Vous n'autorisez que ce que vous voulez et bloquez le reste. Ce modèle inclut une configuration de vérification de sécurité intégrée, qui peut être déployée en quelques clics. Cependant, gardez à l'esprit que plus la sécurité est renforcée, plus la surcharge de traitement est importante.

Le modèle de sécurité négative peut être préférable pour les applications personnalisées. Les signatures vous permettent de combiner plusieurs conditions, et une correspondance et l'action spécifiée sont déclenchées uniquement lorsque toutes les conditions sont remplies. Vous ne bloquez que ce que vous ne voulez pas et vous autorisez le reste. Un modèle de correspondance rapide spécifique dans un emplacement spécifié peut réduire considérablement la surcharge de traitement afin d'optimiser les performances. La possibilité d'ajouter vos propres règles de signature, en fonction

des besoins de sécurité spécifiques de vos applications, vous donne la possibilité de concevoir vos propres solutions de sécurité personnalisées.

- **Détection et protection côté demande et réponse :** Vous pouvez inspecter les demandes entrantes pour détecter tout comportement suspect et prendre les mesures appropriées, et vous pouvez vérifier les réponses pour détecter et protéger contre les fuites de données sensibles.
- **Ensemble complet de protections intégrées pour les charges utiles HTML, XML et JSON :** le Web App Firewall offre 19 contrôles de sécurité différents. Six d'entre eux (tels que Start URL et Deny URL) s'appliquent aux données HTML et XML. Cinq vérifications (telles que la cohérence des champs et le format des champs) sont spécifiques au HTML, et huit (telles que le format XML et l'interopérabilité des services Web) sont spécifiques aux charges utiles XML. Cette fonctionnalité inclut un ensemble complet d'actions et d'options. Par exemple, la fermeture d'URL vous permet de contrôler et d'optimiser la navigation sur votre site Web, pour vous protéger contre une navigation forcée sans avoir à configurer des règles de relaxation pour autoriser chaque URL légitime. Vous avez la possibilité de supprimer ou de supprimer les données sensibles, telles que les numéros de carte de crédit, dans la réponse. Que ce soit la protection contre les attaques SOAP Array, le déni de service XML (XDoS), la prévention de l' analyse WSDL, la vérification des pièces jointes ou tout autre type d'attaques XML, vous avez le confort de savoir que vous disposez d'un bouclier inébranlable protégeant vos données lorsque vos applications sont protégées par le Web App Firewall. Les signatures vous permettent de configurer des règles à l'aide d'expressions XPath pour détecter les violations dans le corps ainsi que dans l'en-tête d'une charge utile JSON.
- **GWT :** prise en charge de la protection des applications Google Web Toolkit pour se protéger contre les violations de SQL, de script intersite et de vérification de la cohérence des champs de formulaire.
- **Interface utilisateur graphique (GUI) conviviale et sans Java : Une interface** graphique intuitive et des contrôles de sécurité préconfigurés facilitent le déploiement de la sécurité en cliquant sur quelques boutons. Un assistant vous invite et vous guide pour créer les éléments requis, tels que des profils, des stratégies, des signatures et des liaisons. L'interface graphique basée sur HTML5 est exempte de toute dépendance Java. Les performances sont nettement supérieures à celles des anciennes versions Java.
- **CLI facile à utiliser et automatisable :** La plupart des options de configuration disponibles dans l'interface graphique sont également disponibles dans l'interface de ligne de commande (CLI). Les commandes CLI peuvent être exécutées par un fichier de commandes et sont faciles à automatiser.
- **Prise en charge de l'API REST :** Le protocole Citrix ADC NITRO prend en charge un ensemble complet d'API REST pour automatiser la configuration du Web App Firewall et collecter des statistiques pertinentes pour la surveillance continue des violations de sécurité.

- **Apprentissage :** La capacité du Web App Firewall à apprendre en surveillant le trafic pour affiner la sécurité est très conviviale. Le moteur d'apprentissage recommande des règles, ce qui facilite le déploiement de relaxations sans maîtrise des expressions régulières.
- **Prise en charge de l'éditeur RegEx :** Les expressions régulières offrent une solution élégante au dilemme de la volonté de consolider les règles tout en optimisant la recherche. Vous pouvez tirer parti de la puissance des expressions régulières pour configurer des URL, des noms de champs, des modèles de signature, etc. L'éditeur RegEx intégré riche vous offre une référence rapide pour les expressions et fournit un moyen pratique de valider et de tester la précision de votre RegEx.
- **Page d'erreur personnalisée :** les demandes bloquées peuvent être redirigées vers une URL d'erreur. Vous avez également la possibilité d'afficher un objet d'erreur personnalisé qui utilise des variables prises en charge et une stratégie Citrix Advanced (expressions PI avancées) pour intégrer des informations de dépannage pour le client.
- Rapports**PCI-DSS, statistiques et autres rapports de violation :** le riche ensemble de rapports facilite le respect des exigences de conformité PCI-DSS, la collecte de statistiques sur les compteurs de trafic et l'affichage des rapports de violation pour tous les profils ou un seul profil.
- **Logging and click-to-rule from log :** La journalisation détaillée est prise en charge pour les formats natif et CEF. Le Web App Firewall vous offre la possibilité de filtrer les messages de journal ciblés dans la visionneuse Syslog. Vous pouvez sélectionner un message de journal et déployer une règle de relaxation correspondante en cliquant simplement sur un bouton. Vous avez la flexibilité de personnaliser les messages de journal et également la prise en charge de la génération de journaux Web. Pour plus d'informations, consultez la rubrique Journaux du Web App Firewall.
- **Inclure les journaux de violation dans les enregistrements de trace :** la possibilité d'inclure des messages de journal dans les enregistrements de trace facilite le débogage d'un comportement inattendu tel que la réinitialisation et le blocage.
- **Clonage :** L'option de profil d'importation/exportation utile vous permet de cloner la configuration de sécurité d'une appliance Citrix ADC vers d'autres. Les options d'exportation des données apprises facilitent l'exportation des règles apprises vers un fichier Excel. Vous pouvez ensuite les faire examiner et approuver par le propriétaire de l'application avant de les appliquer.
- **Un modèle AppExpert** (un ensemble de paramètres de configuration) peut être conçu pour fournir une protection appropriée à vos sites Web. Vous pouvez simplifier et accélérer le déploiement d'une protection similaire sur d'autres appliances en exportant ces modèles de découpe vers un modèle.

Pour plus de détails, consultez la rubrique sur le modèle AppExpert.

- **Vérifications de sécurité sans session :** le déploiement de vérifications de sécurité sans session peut vous aider à réduire l'empreinte mémoire et à accélérer le traitement.

- **Interopérabilité avec les autres fonctionnalités de Citrix ADC :** le Web App Firewall fonctionne de manière transparente avec les autres fonctionnalités de Citrix ADC, telles que la réécriture, la transformation d'URL, la mise en cache intégrée, le CVPN et la limitation du débit.
- **Prise en charge des expressions PI dans les stratégies :** vous pouvez tirer parti de la puissance des expressions PI avancées pour concevoir des stratégies afin d'implémenter différents niveaux de sécurité pour différentes parties de votre application.
- **Prise en charge d'IPv6 :** le Web App Firewall prend en charge les protocoles IPv4 et IPv6.
- **Protection de sécurité basée sur la géolocalisation :** vous avez la flexibilité d'utiliser la stratégie Citrix Advanced (PI Expressions) pour configurer des stratégies basées sur l'emplacement, qui peuvent être utilisées conjointement avec une base de données d'emplacements intégrée pour personnaliser la protection par pare-feu. Vous pouvez identifier les emplacements d'où proviennent les demandes malveillantes et appliquer le niveau d'inspection de sécurité souhaité pour les demandes provenant d'un emplacement géographique spécifique.
- **Performances :** la **diffusion en continu** côté demande améliore considérablement les performances. Dès qu'un champ est traité, les données résultantes sont transférées vers le back-end tandis que l'évaluation se poursuit pour les champs restants. L'amélioration du temps de traitement est particulièrement importante lorsque l'on manipule de gros poteaux.
- **Autres fonctionnalités de sécurité :** Le Web App Firewall comporte plusieurs autres paramètres de sécurité qui peuvent contribuer à assurer la sécurité de vos données. Par exemple, le **champ confidentiel** vous permet de bloquer les fuites d'informations sensibles dans les messages de journal, et **Strip HTML Comment** vous permet de supprimer les commentaires HTML de la réponse avant de la transmettre au client. **Les types de champs** peuvent être utilisés pour spécifier les entrées autorisées dans les formulaires envoyés à votre application.

Q : Que dois-je faire pour configurer le Web App Firewall ?

Procédez comme suit :

- Ajoutez un profil de Web App Firewall et sélectionnez le type approprié (html, xml, web2.0) pour les exigences de sécurité de l'application.
- Sélectionnez le niveau de sécurité requis (de base ou avancé).
- Ajoutez ou importez les fichiers requis, tels que des signatures ou WSDL.
- Configurez le profil pour qu'il utilise les fichiers et apportez toute autre modification nécessaire aux paramètres par défaut.
- Ajoutez une stratégie de Web App Firewall pour ce profil.
- Liez la stratégie au point de liaison cible et spécifiez la priorité.

Q : Comment savoir quel type de profil choisir ?

Le profil Web App Firewall offre une protection pour les charges utiles HTML et XML. Selon les besoins de votre application, vous pouvez choisir un profil HTML ou un profil XML. Si votre application prend en charge les données HTML et XML, vous pouvez choisir un profil Web2.0.

Q : Quelle est la différence entre un profil de base et un profil avancé ? Comment puis-je choisir celui dont j'ai besoin ?

La décision d'utiliser un profil de base ou un profil avancé dépend des besoins de sécurité de votre application. Un profil de base inclut un ensemble préconfiguré de règles de relaxation URL de démarrage et Refuser l'URL. Ces règles de relaxation déterminent quelles demandes sont autorisées et lesquelles sont refusées. Les demandes entrantes sont mises en correspondance avec les règles préconfigurées et les actions configurées sont appliquées. L'utilisateur peut sécuriser les applications avec une configuration minimale des règles de relaxation. Les règles d'URL de démarrage protègent contre la navigation forcée. Les vulnérabilités connues des serveurs Web exploitées par des pirates peuvent être détectées et bloquées en activant un ensemble de règles de refus d'URL par défaut. Les attaques couramment lancées, telles que Buffer Overflow, SQL ou Cross-Site Scripting, peuvent également être facilement détectées.

Comme son nom l'indique, les protections avancées sont destinées aux applications qui ont des exigences de sécurité plus élevées. Les règles de relaxation sont configurées pour autoriser l'accès à des données spécifiques et bloquer le reste. Ce modèle de sécurité positif atténue les attaques inconnues, qui peuvent ne pas être détectées par les contrôles de sécurité de base. En plus de toutes les protections de base, un profil avancé assure le suivi d'une session utilisateur en contrôlant la navigation, en vérifiant les cookies, en spécifiant les exigences de saisie pour divers champs de formulaire et en protégeant contre la falsification des formulaires ou les attaques Cross-Site Request Forgery. L'apprentissage, qui observe le trafic et recommande les assouplissements appropriés, est activé par défaut pour de nombreux contrôles de sécurité. Bien qu'elles soient faciles à utiliser, les protections avancées nécessitent une attention particulière, car elles offrent une sécurité plus stricte mais nécessitent également un traitement plus important. Certaines vérifications de sécurité avancées n'autorisent pas l'utilisation de la mise en cache, ce qui peut affecter les performances.

Gardez à l'esprit les points suivants lorsque vous décidez d'utiliser des profils de base ou avancés :

- Les profils de base et avancés ne font que commencer les modèles. Vous pouvez toujours modifier le profil de base pour déployer des fonctionnalités de sécurité avancées, et vice versa.
- Les contrôles de sécurité avancés nécessitent davantage de traitement et peuvent affecter les performances. À moins que votre application n'ait besoin d'une sécurité avancée, vous pouvez commencer par un profil de base et resserrer la sécurité selon les besoins de votre application.
- Vous ne souhaitez pas activer toutes les vérifications de sécurité, sauf si votre application en a besoin.

Q : Qu'est-ce qu'une politique ? Comment sélectionner le point de liaison et définir la priorité ?

Les stratégies de Web App Firewall peuvent vous aider à trier votre trafic en groupes logiques afin de configurer différents niveaux de mise en œuvre de la sécurité. Sélectionnez soigneusement les points de liaison des stratégies afin de déterminer quel trafic est mis en correspondance avec quelle stratégie. Par exemple, si vous souhaitez que chaque requête entrante soit vérifiée pour détecter les attaques de script SQL/intersite, vous pouvez créer une stratégie générique et la lier globalement. Si vous souhaitez appliquer des contrôles de sécurité plus stricts au trafic d'un serveur virtuel hébergeant des applications contenant des données sensibles, vous pouvez lier une stratégie à ce serveur virtuel.

Une affectation minutieuse des priorités peut améliorer le traitement du trafic. Vous souhaitez attribuer des priorités plus élevées à des stratégies plus spécifiques et des priorités plus faibles aux stratégies génériques. Notez que plus le nombre est élevé, plus la priorité est faible. Une stratégie avec une priorité de 10 est évaluée avant une stratégie qui a une priorité de 15.

Vous pouvez appliquer différents niveaux de sécurité pour différents types de contenus, par exemple les demandes d'objets statiques tels que les images et le texte peuvent être contournées à l'aide d'une stratégie et les demandes pour d'autres contenus sensibles peuvent être soumises à un contrôle très rigoureux à l'aide d'une deuxième stratégie.

Q : Comment puis-je configurer les règles pour sécuriser mon application ?

Le Web App Firewall permet de concevoir très facilement le niveau de sécurité approprié pour votre site Web. Vous pouvez avoir plusieurs stratégies de Web App Firewall, liées à différents profils de Web App Firewall, afin de mettre en œuvre différents niveaux d'inspections de vérification de sécurité pour vos applications. Vous pouvez d'abord surveiller les journaux pour savoir quelles menaces de sécurité sont détectées et quelles violations sont déclenchées. Vous pouvez ajouter manuellement les règles de relaxation ou tirer parti des règles apprises recommandées par le Web App Firewall pour déployer les assouplissements requis afin d'éviter les faux positifs.

Le Citrix Web App Firewall prend en charge les **visualiseurs** dans l'interface graphique, ce qui facilite grandement la gestion des règles. Vous pouvez facilement afficher toutes les données sur un seul écran et agir sur plusieurs règles en un seul clic. Le plus grand avantage du visualiseur est qu'il recommande des expressions régulières pour consolider plusieurs règles. Vous pouvez sélectionner un sous-ensemble de règles, en vous basant sur le délimiteur et l'URL de l'action. La prise en charge de Visualizer est disponible pour visualiser 1) les règles apprises et 2) les règles de relaxation.

1. Le visualiseur des règles apprises offre la possibilité de modifier les règles et de les déployer sous forme d'assouplissements. Vous pouvez également ignorer (ignorer) les règles.
2. Le visualiseur des relaxations déployées vous offre la possibilité d'ajouter une nouvelle règle ou de modifier une règle existante. Vous pouvez également activer ou désactiver un groupe de

règles en sélectionnant un nœud et en cliquant sur le bouton **Activer** ou **Désactiver** dans le visualiseur de relaxation.

Q : Que sont les signatures ? Comment savoir quelles signatures utiliser ?

Une signature est un objet qui peut comporter plusieurs règles. Chaque règle se compose d'un ou de plusieurs modèles pouvant être associés à un ensemble d'actions spécifié. Le Web App Firewall comporte un objet de signature par défaut intégré composé de plus de 1 300 règles de signature, avec une option permettant d'obtenir les dernières règles à l'aide de la fonctionnalité de **mise à jour automatique** pour obtenir une protection contre les nouvelles vulnérabilités. Les règles créées par d'autres outils d'analyse peuvent également être importées.

Les signatures sont très puissantes car elles utilisent la correspondance de motifs pour détecter les attaques malveillantes et peuvent être configurées pour vérifier à la fois la demande et la réponse d'une transaction. Ils sont une option privilégiée lorsqu'une solution de sécurité personnalisable est nécessaire. Plusieurs choix d'actions (par exemple, bloquer, consigner, apprendre et transformer) sont disponibles lorsqu'une correspondance de signature est détectée. Les signatures par défaut couvrent les règles pour protéger différents types d'applications, telles que web-cgi, web-coldfusion, web-frontpage, web-iis, web-php, web-client, web-activex, web-shell-shock et web-struts. Pour répondre aux besoins de votre application, vous pouvez sélectionner et déployer les règles appartenant à une catégorie spécifique.

Conseils d'utilisation des signatures :

- Vous pouvez simplement créer une copie de l'objet de signature par défaut et le modifier pour activer les règles dont vous avez besoin et configurer les actions souhaitées.
- L'objet de signature peut être personnalisé en ajoutant de nouvelles règles, qui peuvent fonctionner conjointement avec d'autres règles de signature.
- Les règles de signature peuvent également être configurées pour fonctionner conjointement avec les vérifications de sécurité spécifiées dans le profil de Web App Firewall. Si une correspondance indiquant une violation est détectée par une signature et un contrôle de sécurité, l'action la plus restrictive est celle qui est appliquée.
- Une règle de signature peut comporter plusieurs modèles et être configurée pour signaler une violation uniquement lorsque tous les modèles sont appariés, évitant ainsi les faux positifs.
- La sélection rigoureuse d'un modèle de correspondance rapide littéral pour une règle peut considérablement optimiser le temps de traitement.

Q : Le Web App Firewall fonctionne-t-il avec d'autres fonctionnalités de Citrix ADC ?

Le Web App Firewall est entièrement intégré à l'appliance Citrix ADC et fonctionne de manière transparente avec d'autres fonctionnalités. Vous pouvez configurer une sécurité maximale pour votre application en utilisant d'autres fonctionnalités de sécurité Citrix ADC conjointement avec le Web App

Firewall. Par exemple, **AAA-TM** peut être utilisé pour authentifier l'utilisateur, vérifier l'autorisation de l'utilisateur à accéder au contenu et consigner les accès, y compris les tentatives de connexion non valides. La**réécriture** peut être utilisée pour modifier l'URL ou pour ajouter, modifier ou supprimer des en-têtes, et **Responder** peut être utilisé pour fournir du contenu personnalisé à différents utilisateurs. Vous pouvez définir la charge maximale de votre site Web en utilisant la **limitation de débit** pour surveiller le trafic et limiter le taux s'il est trop élevé. La protection par**déni de service (DoS) HTTP** peut aider à faire la distinction entre les clients HTTP réels et les clients DoS malveillants. Vous pouvez réduire la portée de l'inspection de vérification de sécurité en liant les stratégies de Web App Firewall aux serveurs virtuels, tout en optimisant l'expérience utilisateur en utilisant la fonctionnalité d' **équilibrage de charge** pour gérer les applications très utilisées. Les demandes d'objets statiques tels que des images ou du texte peuvent contourner l'inspection des contrôles de sécurité, en tirant parti de la **mise en cache intégrée** ou de la **compression** pour optimiser l'utilisation de la bande passante pour ce contenu.

Q : Comment la charge utile est-elle traitée par le Web App Firewall et les autres fonctionnalités de Citrix ADC ?

Un diagramme montrant les détails du flux de paquets L7 dans une appliance Citrix ADC est disponible dans la section Ordre de traitement des fonctionnalités .

Q : Quel est le flux de travail recommandé pour le déploiement du Web App Firewall ?

Maintenant que vous connaissez les avantages de l'utilisation des protections de sécurité de pointe du Citrix Web App Firewall, vous souhaiterez peut-être collecter des informations supplémentaires qui peuvent vous aider à concevoir la solution optimale pour vos besoins de sécurité. Citrix vous recommande d'effectuer les opérations suivantes :

- **Connaître votre environnement :** La connaissance de votre environnement vous aidera à identifier la meilleure solution de protection de sécurité (signatures, contrôles de sécurité ou les deux) pour vos besoins. Avant de commencer la configuration, vous devez collecter les informations suivantes.
  - Système d'**exploitation :** Quel type de système d'exploitation (MS Windows, Linux, BSD, Unix, autres) avez-vous ?
  - **Serveur Web :** Quel serveur Web (IIS, Apache ou Citrix ADC Enterprise Server) exécutez-vous ?
  - **Application :** Quels types d'applications sont en cours d'exécution sur votre serveur d'applications (par exemple, ASP.NET, PHP, Cold Fusion, ActiveX, FrontPage, Struts, CGI, Apache Tomcat, Domino et WebLogic) ?
  - Avez-vous des applications personnalisées ou des applications prêtes à l'emploi (par exemple, Oracle, SAP) ? Quelle version utilisez-vous ?

  - **SSL :** Avez-vous besoin de SSL ? Dans l'affirmative, quelle taille de clé (512, 1024, 2048, 4096) est utilisée pour la signature des certificats ?
  - **Volume du trafic :** Quel est le taux de trafic moyen via vos applications ? Avez-vous des pics de trafic saisonniers ou temporels ?
  - **Ferme de serveurs :** Combien de serveurs disposez-vous ? Avez-vous besoin d'utiliser l'équilibrage de charge ?
  - **Base de données :** Quel type de base de données (MS-SQL, MySQL, Oracle, Postgres, SQLite, nosql, Sybase, Informix, etc.) utilisez-vous ?
  - **Connectivité DB :** Quel type de connectivité de base de données disposez-vous (DSN, chaîne de connexion par fichier, chaîne de connexion à un seul fichier) et quels pilotes sont utilisés ?
- **Identifiez vos besoins en matière de sécurité :** Vous voudrez peut-être évaluer quelles applications ou données spécifiques nécessitent une protection de sécurité maximale, lesquelles sont les moins vulnérables et celles pour lesquelles l'inspection de sécurité peut être contournée en toute sécurité. Cela vous aidera à trouver une configuration optimale et à concevoir des stratégies et des points de liaison appropriés pour séparer le trafic. Par exemple, vous pouvez configurer une stratégie pour contourner l'inspection de sécurité des demandes de contenu Web statique, tels que des images, des fichiers MP3 et des films, et configurer une autre stratégie pour appliquer des contrôles de sécurité avancés aux demandes de contenu dynamique. Vous pouvez utiliser plusieurs stratégies et profils pour protéger différents contenus d'une même application.
- **Exigences de licence :** Citrix offre une solution unifiée pour optimiser les performances de votre application en tirant parti d'un ensemble complet de fonctionnalités telles que l'équilibrage de charge, la commutation de contenu, la mise en cache, la compression, le répondeur, la réécriture et le filtrage de contenu, pour n'en nommer que quelques-unes. L'identification des fonctionnalités souhaitées peut vous aider à choisir la licence dont vous avez besoin.
- **Installez et baseline une appliance Citrix ADC :** créez un serveur virtuel et exécutez le trafic de test à travers celui-ci pour avoir une idée du débit et de la quantité de trafic circulant dans votre système. Ces informations vous aideront à identifier vos besoins en capacité et à sélectionner le bon matériel (VPX, MPX ou SDX).
- **Déployer le pare-feu des applications Web :** utilisez l'assistant Web App Firewall pour procéder à une configuration de sécurité simple. L'Assistant vous guide à travers plusieurs écrans et vous invite à ajouter un profil, une stratégie, une signature et des vérifications de sécurité.
  - **Profil :** sélectionnez un nom significatif et le type approprié (HTML, XML ou WEB 2.0) pour votre profil. La stratégie et les signatures seront générées automatiquement sous le même nom.
  - **Stratégie :** La stratégie générée automatiquement possède l'expression par défaut (true), qui sélectionne tout le trafic et est liée globalement. C'est un bon point de départ, sauf si

vous avez en tête une politique spécifique que vous souhaitez utiliser.

- **Protections :** l'assistant vous aide à tirer parti du modèle de sécurité hybride, dans lequel vous pouvez utiliser les signatures par défaut offrant un ensemble complet de règles pour protéger différents types d'applications. Le mode d'édition**simple** vous permet de visualiser les différentes catégories (CGI, Cold Fusion, PHP, etc.). Vous pouvez sélectionner une ou plusieurs catégories pour identifier un ensemble spécifique de règles applicables à votre application. Utilisez l'option **Action** pour activer toutes les règles de signature dans les catégories sélectionnées. Assurez-vous que le blocage est désactivé afin de pouvoir surveiller le trafic avant de renforcer la sécurité. Cliquez sur **Continuer**. Dans le volet **Spécifier les protections approfondies**, vous pouvez apporter les modifications nécessaires pour déployer les protections de vérification de sécurité. Dans la plupart des cas, les protections de base sont suffisantes pour la configuration initiale de la sécurité. Exécutez le trafic pendant un certain temps pour collecter un échantillon représentatif des données d'inspection de sécurité.
- **Renforcer la sécurité :** après avoir déployé Web App Firewall et observé le trafic pendant un certain temps, vous pouvez commencer à renforcer la sécurité de vos applications en déployant des assouplissements, puis en activant le blocage. Les règles **Learning**, **Visualizer** et **Click to deploy** sont des fonctionnalités utiles qui facilitent la modification de votre configuration pour trouver le bon niveau de relaxation. À ce stade, vous pouvez également modifier l'expression de la stratégie et/ou configurer des stratégies et des profils supplémentaires pour mettre en œuvre les niveaux de sécurité souhaités pour différents types de contenu.
- **Débogage :** si vous constatez un comportement inattendu de votre application, le Web App Firewall offre différentes options pour faciliter le débogage :
  * **Journal**. Si des demandes légitimes sont bloquées, la première étape consiste à vérifier le fichier ns.log pour voir si une violation inattendue des contrôles de sécurité est déclenchée.
  * **Désactiver la fonction.** Si vous ne constatez aucune violation, mais que vous constatez toujours un comportement inattendu, comme la réinitialisation d'une application ou l'envoi de réponses partielles, vous pouvez désactiver la fonctionnalité Web App Firewall pour le débogage. Si le problème persiste, il exclut le Web App Firewall en tant que suspect.
  * **Trace les enregistrements avec des messages de journal.** Si le problème semble être lié au Web App Firewall et doit être examiné de plus près, vous avez la possibilité d'inclure des messages de violation de sécurité dans une nstrace. Vous pouvez utiliser « Suivre le flux TCP » dans la trace pour afficher les détails de la transaction individuelle, y compris les en-têtes, la charge utile et le message de journal correspondant, ensemble sur le même écran. Des détails sur l'utilisation de cette fonctionnalité sont disponibles dans les annexes.

Présentation du pare-feu Citrix Web Application

August 20, 2021

Le Citrix Web App Firewall empêche les failles de sécurité, la perte de données et les éventuelles modifications non autorisées des sites Web qui accèdent aux informations sensibles de l'entreprise ou des clients. Il le fait en filtrant les demandes et les réponses, en les examinant à la recherche de preuves d'activités malveillantes et en bloquant les demandes qui démontrent une telle activité. Votre site est protégé non seulement contre les types d'attaques courants, mais aussi contre les attaques nouvelles, encore inconnues. En plus de protéger les serveurs Web et les sites Web contre les accès non autorisés, le Web App Firewall protège contre les vulnérabilités des codes ou scripts CGI existants, des frameworks Web, des logiciels de serveur Web et d'autres systèmes d'exploitation sous-jacents.

Citrix Web App Firewall est disponible en tant qu'appliance autonome ou en tant que fonctionnalité sur un dispositif virtuel Citrix ADC (VPX). Dans la documentation du Web App Firewall, le terme Citrix ADC fait référence à la plate-forme sur laquelle le Web App Firewall est exécuté, que cette plate-forme soit un dispositif de pare-feu dédié, un Citrix ADC sur lequel d'autres fonctionnalités ont également été configurées ou un Citrix ADC VPX.

Pour utiliser le Web App Firewall, vous devez créer au moins une configuration de sécurité pour bloquer les connexions qui enfreignent les règles que vous définissez pour vos sites Web protégés. Le nombre de configurations de sécurité que vous souhaitez créer dépend de la complexité de votre site Web. Parfois, une seule configuration est suffisante. Dans d'autres cas, en particulier ceux qui incluent des sites Web interactifs, des sites Web qui accèdent à des serveurs de base de données, des magasins en ligne avec des paniers d'achat, vous pourriez avoir besoin de plusieurs configurations différentes pour protéger au mieux les données sensibles sans gaspiller d'efforts importants sur le contenu qui n'est pas vulnérable à certains types de attaques. Vous pouvez souvent laisser les valeurs par défaut des paramètres globaux, qui affectent toutes les configurations de sécurité, inchangées. Toutefois, vous pouvez modifier les paramètres globaux s'ils sont en conflit avec d'autres parties de votre configuration ou si vous préférez les personnaliser.

Sécurité des applications Web

La sécurité des applications Web est la sécurité du réseau pour les ordinateurs et les programmes qui communiquent à l'aide des protocoles HTTP et HTTPS. Il s'agit d'un vaste domaine dans lequel les failles et les faiblesses en matière de sécurité abondent. Les systèmes d'exploitation des serveurs et des clients présentent des problèmes de sécurité et sont vulnérables aux attaques. Les logiciels de serveur Web et les technologies d'activation de sites Web comme CGI, Java, JavaScript, PERL et PHP présentent des vulnérabilités sous-jacentes. Les navigateurs et autres applications clientes qui communiquent avec des applications web présentent également des vulnérabilités. Les sites Web qui

utilisent n'importe quelle technologie, mais le HTML le plus simple, y compris tout site qui permet l'interaction avec les visiteurs, ont souvent des vulnérabilités propres.

Dans le passé, une atteinte à la sécurité n'était souvent qu'une gêne, mais aujourd'hui c'est rarement le cas. Par exemple, les attaques au cours desquelles un pirate a accédé à un serveur Web et apporté des modifications non autorisées à un site Web (défacé) étaient courantes. Ils étaient généralement lancés par des pirates qui n'avaient aucune motivation que de démontrer leurs compétences à d'autres pirates ou de gêner la personne ou l'entreprise visée. Cependant, la plupart des manquements actuels à la sécurité sont motivés par un désir d'argent. La majorité tente d'atteindre l'un ou l'autre des objectifs suivants : obtenir des renseignements confidentiels et potentiellement utiles, ou obtenir un accès non autorisé à un site Web ou un serveur Web et à le contrôler.

Certaines formes d'attaques sur le Web visent à obtenir des informations privées. Ces attaques sont souvent possibles même contre des sites Web suffisamment sécurisés pour empêcher un attaquant de prendre le contrôle total. Les informations qu'un attaquant peut obtenir à partir d'un site Web peuvent inclure les noms, adresses, numéros de téléphone, numéros de sécurité sociale, numéros de carte de crédit, dossiers médicaux et autres informations privées. L'attaquant peut alors utiliser ces informations ou les vendre à d'autres. Une grande partie de l'information obtenue par de telles attaques est protégée par la loi, et tout cela par la coutume et l'attente. Une violation de ce type peut avoir de graves conséquences pour les clients dont les informations privées sont compromises. Au mieux, ces clients doivent faire preuve de vigilance pour empêcher les autres d'abuser de leurs cartes de crédit, d'ouvrir des comptes de crédit non autorisés à leur nom ou de s'approprier leur identité pure et simple (usurpation d'identité). Au pire, les clients peuvent faire face à des notations de crédit ruines ou même être blâmés pour des activités criminelles auxquelles ils n'ont pas participé.

D'autres attaques Web visent à obtenir le contrôle (ou *compromettre*) un site Web ou le serveur sur lequel il opère, ou les deux. Un pirate qui prend le contrôle d'un site Web ou d'un serveur peut l'utiliser pour héberger du contenu non autorisé, agir comme proxy pour le contenu hébergé sur un autre serveur Web, fournir des services SMTP pour envoyer des courriels non sollicités en masse ou fournir des services DNS pour prendre en charge de telles activités sur d'autres serveurs Web compromis. La plupart des sites Web hébergés sur des serveurs Web compromis favorisent des entreprises douteuses ou carrément frauduleuses. Par exemple, la plupart des sites Web d'hameçonnage et des sites d'exploitation des enfants sont hébergés sur des serveurs Web compromis.

La protection de vos sites Web et services Web contre ces attaques nécessite une défense multicouche capable à la fois de bloquer les attaques connues avec des caractéristiques identifiables et de protéger contre les attaques inconnues, qui peuvent souvent être détectées parce qu'elles ont un aspect différent du trafic normal vers vos sites Web et Web services.

Attaques Web connues

La première ligne de défense de vos sites Web est la protection contre le grand nombre d'attaques connues et observées et analysées par des experts en sécurité web. Les types courants d'attaques contre les sites Web HTML sont les suivants :

- **Attaques par débordement de tampon.** L'envoi d'une longue URL, d'un cookie long ou de longues informations à un serveur Web entraîne le blocage, le blocage ou l'accès non autorisé au système d'exploitation sous-jacent. Une attaque par débordement de tampon peut être utilisée pour accéder à des informations non autorisées, compromettre un serveur Web, ou les deux.
- **Attaques de sécurité des cookies.** Envoi d'un cookie modifié à un serveur Web, généralement dans l'espoir d'obtenir l'accès à un contenu non autorisé en utilisant des informations d'identification falsifiées.
- **Navigation puissante.** Accéder directement aux URL d'un site Web, sans accéder aux URL contenant des hyperliens sur la page d'accueil ou d'autres URL de démarrage courantes sur le site Web. Des cas individuels de navigation forcée peuvent indiquer un utilisateur qui a marqué une page sur votre site Web, mais les tentatives répétées d'accès à du contenu inexistant, ou à du contenu auquel les utilisateurs ne doivent jamais accéder directement, représentent souvent une atteinte à la sécurité du site Web. La navigation forcée est normalement utilisée pour accéder à des informations non autorisées, mais peut également être combinée à une attaque par débordement de tampon dans le but de compromettre votre serveur.
- **Attaques de sécurité des formulaires Web.** Envoi de contenu inapproprié à votre site Web dans un formulaire Web. Le contenu inapproprié peut inclure des champs masqués modifiés, du code HTML ou du code dans un champ destiné uniquement aux données alphanumériques, une chaîne trop longue dans un champ qui n'accepte qu'une chaîne courte, une chaîne alphanumérique dans un champ qui n'accepte qu'un entier et une grande variété d'autres données que votre site Web ne contient pas attendez à recevoir dans ce formulaire Web. Une attaque de sécurité de formulaire Web peut être utilisée soit pour obtenir des informations non autorisées de votre site Web, soit pour compromettre le site Web, généralement lorsqu'elle est associée à une attaque de débordement de tampon.

Deux types spécialisés d'attaques contre la sécurité des formulaires Web méritent une mention spéciale :

- **Attaques par injection SQL.** Envoi d'une ou de plusieurs commandes SQL actives dans un formulaire Web ou dans le cadre d'une URL, dans le but d'amener une base de données SQL à exécuter la ou les commandes. Les attaques par injection SQL sont normalement utilisées pour obtenir des informations non autorisées.
- **Attaques de scripts intersites.** Utilisation d'une URL ou d'un script sur une page Web pour enfreindre la stratégie de même origine, qui interdit à tout script d'obtenir des propriétés à partir d'un autre site Web ou de modifier un contenu sur un autre site Web. Étant donné que les scripts peuvent obtenir des informations et modifier des fichiers sur votre site Web, autoriser un script

à accéder au contenu d'un autre site Web peut fournir à un attaquant le moyen d'obtenir des informations non autorisées, de compromettre un serveur web, ou les deux.

Les attaques contre les services Web XML relèvent normalement d'au moins une des deux catégories suivantes : tentatives d'envoi de contenu inapproprié à un service Web ou tentatives de violation de la sécurité sur un service Web. Les types d'attaques les plus courants contre les services Web XML sont les suivants :

- **Code ou objets malveillants.** Demandes XML contenant du code ou des objets qui peuvent obtenir directement des informations sensibles ou donner à un attaquant le contrôle du service Web ou du serveur sous-jacent.
- **Demandes XML mal formées.** Demandes XML qui ne sont pas conformes à la spécification XML du W3C et qui peuvent donc enfreindre la sécurité sur un service Web non sécurisé
- **Attaques par déni de service (DoS).** Demandes XML envoyées à plusieurs reprises et en volume élevé, dans le but d'accabler le service Web ciblé et de refuser aux utilisateurs légitimes l'accès au service Web.

Outre les attaques basées sur XML standard, les services Web XML et les sites Web 2.0 sont également vulnérables aux attaques par injection SQL et par script intersite, comme décrit ci-dessous :

- **Attaques par injection SQL.** Envoi d'une ou de plusieurs commandes SQL actives dans une requête XML, dans le but d'amener une base de données SQL à exécuter cette ou ces commandes. Comme pour les attaques par injection HTML SQL, les attaques par injection XML SQL sont normalement utilisées pour obtenir des informations non autorisées.
- **Attaques de scripts intersites.** Utilisation d'un script inclus dans une application XML pour enfreindre la stratégie de même origine, ce qui ne permet à aucun script d'obtenir des propriétés à partir d'une application différente ou de modifier un contenu. Étant donné que les scripts peuvent obtenir des informations et modifier des fichiers à l'aide de votre application XML, permettre à un script d'accéder au contenu appartenant à une autre application peut donner à un attaquant les moyens d'obtenir des informations non autorisées, de compromettre l'application, ou les deux

Les attaques Web connues peuvent généralement être arrêtées en filtrant le trafic du site Web pour des caractéristiques spécifiques (signatures) qui apparaissent toujours pour une attaque spécifique et ne doivent jamais apparaître dans le trafic légitime. Cette approche présente l'avantage d'exiger relativement peu de ressources et de présenter relativement peu de risques de faux positifs. Par conséquent, il s'agit d'un outil précieux pour lutter contre les attaques sur les sites Web et les services Web, et pour configurer la protection de base des signatures.

Attaques Web inconnues

La plus grande menace contre les sites Web et les applications ne provient pas d'attaques connues, mais d'attaques inconnues. La plupart des attaques inconnues appartiennent à l'une des deux caté-

gories suivantes : les attaques nouvellement lancées pour lesquelles les entreprises de sécurité n'ont pas encore développé de défense efficace (attaques « jour zéro »), et les attaques ciblées avec soin sur un site Web ou un service Web spécifique plutôt que sur de nombreux sites Web ou services Web (attaques lancées). Ces attaques, comme les attaques connues, ont pour but d'obtenir des informations confidentielles sensibles, de compromettre le site Web ou le service Web et de les utiliser pour d'autres attaques, ou les deux objectifs.

Les attaques Zero Day constituent une menace majeure pour tous les utilisateurs. Ces attaques sont généralement du même type que les attaques connues ; les attaques « jour zéro » impliquent souvent du SQL injecté, un script intersite, une falsification de requête intersite ou un autre type d'attaque similaire aux attaques connues. Généralement, ils ciblent des vulnérabilités que les développeurs du logiciel, du site Web ou du service Web ciblé ignorent ou ont appris. Les entreprises de sécurité n'ont donc pas développé de défenses contre ces attaques, et même si elles l'ont fait, les utilisateurs n'ont pas obtenu et installé les correctifs ni effectué les solutions de contournement nécessaires pour se protéger contre ces attaques. Le temps entre la découverte d'une attaque « jour zéro » et la disponibilité d'une défense (la fenêtre de vulnérabilité) diminue, mais les auteurs peuvent toujours compter sur des heures, voire des jours pendant lesquels de nombreux sites Web et services Web ne disposent pas d'une protection spécifique contre l'attaque.

Les attaques de lance constituent une menace majeure, mais pour un groupe d'utilisateurs plus sélect. Un type commun d'attaque de lance, un hameçonnage de lance, est ciblé sur les clients d'une banque ou d'une institution financière spécifique, ou (moins souvent) sur les employés d'une entreprise ou d'une organisation spécifique. Contrairement à d'autres hameçons, qui sont souvent des faux écrits grossièrement qu'un utilisateur connaissant les communications réelles de cette banque ou institution financière peut reconnaître, les phishing de lance sont lettre parfaite et convaincante. Ils peuvent contenir des renseignements spécifiques à la personne qu'aucun étranger ne doit connaître ou être en mesure d'obtenir à première vue. Le spécialiste de l'hameçonnage est donc en mesure de convaincre la cible de fournir les informations demandées, que le phisher peut ensuite utiliser pour piller des comptes, traiter de l'argent obtenu illégitimement d'autres sources ou accéder à d'autres informations encore plus sensibles.

Ces deux types d'attaque ont certaines caractéristiques qui peuvent généralement être détectées, mais pas en utilisant des modèles statiques qui recherchent des caractéristiques spécifiques, comme le font les signatures standard. La détection de ces types d'attaques nécessite des approches plus sophistiquées et plus gourmandes en ressources, telles que le filtrage heuristique et les systèmes de modèles de sécurité positifs. Les regards de filtrage heuristique, non pas pour des modèles spécifiques, mais pour des modèles de comportements. Les systèmes de modèles de sécurité positifs modélisent le comportement normal du site Web ou du service Web qu'ils protègent, puis bloquent les connexions qui ne correspondent pas à ce modèle d'utilisation normale. Les contrôles de sécurité basés sur des URL et des formulaires Web permettent de déterminer le profil de l'utilisation normale de vos sites Web, puis de contrôler la façon dont les utilisateurs interagissent avec vos sites Web, en utilisant à la fois des heuristiques et une sécurité positive pour bloquer le trafic anormal ou inattendu.

Une sécurité heuristique et positive, bien conçue et déployée, peut détecter la plupart des attaques que les signatures manquent. Cependant, ils nécessitent beaucoup plus de ressources que les signatures, et vous devez passer du temps à les configurer correctement pour éviter les faux positifs. Ils sont donc utilisés, non pas comme ligne de défense principale, mais comme sauvegarde des signatures ou d'autres approches moins gourmandes en ressources.

En configurant ces protections avancées en plus des signatures, vous créez un modèle de sécurité hybride qui permet au Web App Firewall de fournir une protection complète contre les attaques connues et inconnues.

Fonctionnement de Citrix Web Application Firewall

Lorsque vous installez le Web App Firewall, vous créez une configuration de sécurité initiale, qui se compose d'une stratégie, d'un profil et d'un objet signatures. La stratégie est une règle qui identifie le trafic à filtrer et le profil identifie les modèles et les types de comportement à autoriser ou à bloquer lorsque le trafic est filtré. Les modèles les plus simples, appelés signatures, ne sont pas spécifiés dans le profil, mais dans un objet signatures associé au profil.

Une signature est une chaîne ou un motif qui correspond à un type d'attaque connu. Le Web App Firewall contient plus d'un millier de signatures dans sept catégories, chacune dirigée contre des attaques contre des types spécifiques de serveurs Web et de contenu Web. Citrix met à jour la liste avec de nouvelles signatures au fur et à mesure que de nouvelles menaces sont identifiées. Au cours de la configuration, vous spécifiez les catégories de signature appropriées pour les serveurs Web et le contenu que vous devez protéger. Les signatures offrent une bonne protection de base avec de faibles frais de traitement. Si vos applications présentent des vulnérabilités spéciales ou si vous détectez une attaque contre elles pour laquelle aucune signature n'existe, vous pouvez ajouter vos propres signatures.

Les protections les plus avancées sont appelées contrôles de sécurité. Une vérification de sécurité est une inspection algorithmique plus rigoureuse d'une demande de modèles ou de comportements spécifiques qui pourraient indiquer une attaque ou constituer une menace pour vos sites Web et services Web protégés. Il peut, par exemple, identifier une demande qui tente d'effectuer un certain type d'opération susceptible de violer la sécurité, ou une réponse qui inclut des informations confidentielles sensibles telles qu'un numéro de sécurité sociale ou un numéro de carte de crédit. Lors de la configuration, vous spécifiez les vérifications de sécurité appropriées pour les serveurs Web et le contenu que vous devez protéger. Les contrôles de sécurité sont restrictifs. Beaucoup d'entre eux peuvent bloquer les demandes et réponses légitimes si vous n'ajoutez pas les exceptions appropriées (relaxations) lors de leur configuration. Identifier les exceptions nécessaires n'est pas difficile si vous utilisez la fonction d'apprentissage adaptatif, qui observe l'utilisation normale de votre site Web et crée des exceptions recommandées.

Le Web App Firewall peut être installé en tant que périphérique réseau de couche 3 ou pont réseau

de couche 2 entre vos serveurs et vos utilisateurs, généralement derrière le routeur ou le pare-feu de votre entreprise. Il doit être installé à un endroit où il peut intercepter le trafic entre les serveurs Web que vous souhaitez protéger et le concentrateur ou basculer par lequel les utilisateurs accèdent à ces serveurs Web. Vous configurez ensuite le réseau pour qu'il envoie des demandes au Web App Firewall plutôt que directement à vos serveurs Web, et des réponses au Web App Firewall plutôt que directement à vos utilisateurs. Le Web App Firewall filtre ce trafic avant de le transférer vers sa destination finale, en utilisant à la fois son jeu de règles interne et vos ajouts et modifications. Il bloque ou rend inoffensif toute activité qu'il détecte comme nuisible, puis transfère le trafic restant au serveur Web. La figure suivante donne une vue d'ensemble du processus de filtrage.

> **Remarque :**
>
> La figure omet l'application d'une stratégie au trafic entrant. Il illustre une configuration de sécurité dans laquelle la stratégie est de traiter toutes les demandes. De plus, dans cette configuration, un objet signatures a été configuré et associé au profil, et des vérifications de sécurité ont été configurées dans le profil.

Figure 1. Diagramme de flux du filtrage du Web App Firewall



Comme l'illustre la figure, lorsqu'un utilisateur demande une URL sur un site Web protégé, le Web App Firewall examine d'abord la demande pour s'assurer qu'elle ne correspond pas à une signature. Si la demande correspond à une signature, Citrix Web Application Firewall affiche l'objet d'erreur (une page Web située sur le dispositif de Web App Firewall et que vous pouvez configurer à l'aide de la fonctionnalité d'importation) ou transfère la demande à l'URL d'erreur désignée (la page d'erreur). Les signatures ne nécessitent pas autant de ressources que les vérifications de sécurité. La détection et l'arrêt des attaques détectées par une signature avant d'exécuter l'une des vérifications de sécurité réduisent la charge sur le serveur.

Si une demande réussit l'inspection des signatures, le Web App Firewall applique les vérifications de sécurité des demandes qui ont été activées. Les contrôles de sécurité de la demande permettent de vérifier que la demande est appropriée pour votre site Web ou service Web et qu'elle ne contient pas de matériel susceptible de constituer une menace. Par exemple, les vérifications de sécurité examinent la demande pour détecter des signes indiquant qu'elle peut être d'un type inattendu, deman-

der du contenu inattendu ou contenir des données de formulaire Web, des commandes SQL ou des scripts inattendus et éventuellement malveillants. Si la demande échoue une vérification de sécurité, le Web App Firewall nettoie la demande, puis la renvoie à l'appliance Citrix ADC (ou à l'appliance virtuelle Citrix ADC), ou affiche l'objet d'erreur. Si la demande réussit les vérifications de sécurité, elle est renvoyée à l'appliance Citrix ADC, qui termine tout autre traitement et transfère la demande au serveur Web protégé.

Lorsque le site Web ou le service Web envoie une réponse à l'utilisateur, le Web App Firewall applique les vérifications de sécurité de réponse qui ont été activées. Les contrôles de sécurité des réponses examinent la réponse à la présence de fuites d'informations confidentielles sensibles, de signes de défacement du site Web ou d'autres contenus qui ne doivent pas être présents. Si la réponse échoue une vérification de sécurité, le Web App Firewall supprime le contenu qui ne doit pas être présent ou bloque la réponse. Si la réponse réussit les vérifications de sécurité, elle est renvoyée à l'appliance Citrix ADC, qui la transmet à l'utilisateur.

Fonctionnalités du pare-feu Citrix Web Application

Les fonctionnalités de base du Web App Firewall sont les stratégies, les profils et les signatures, qui fournissent un modèle de sécurité hybride tel que décrit dans Attaques Web connues, Attaques Web inconnueset Fonctionnement du pare-feu Web App. Il convient de noter la fonctionnalité d'apprentissage, qui observe le trafic vers vos applications protégées et recommande les paramètres de configuration appropriés pour certaines vérifications de sécurité.

La fonctionnalité d'importation gère les fichiers que vous téléchargez vers le Web App Firewall. Ces fichiers sont ensuite utilisés par le Web App Firewall dans divers contrôles de sécurité ou lors de la réponse à une connexion qui correspond à une vérification de sécurité.

Vous pouvez utiliser les fonctions de journaux, de statistiques et de rapports pour évaluer les performances du Web App Firewall et identifier les besoins possibles pour davantage de protections.

Comment Citrix Web Application Firewall modifie le trafic des applications

Citrix Web Application Firewall affecte le comportement d'une application Web qu'il protège en modifiant les éléments suivants :

- Cookies
- En-têtes HTTP
- Formulaires/Données

Cookie de session Citrix Web Application Firewall

Pour maintenir l'état de la session, Citrix ADC Web App Firewall génère son propre cookie de session. Ce cookie est transmis uniquement entre le navigateur Web et le pare-feu Citrix ADC Web Application

et non au serveur Web. Si un pirate tente de modifier le cookie de session, le pare-feu d'application supprime le cookie avant de transférer la demande au serveur et traite la demande comme une nouvelle session utilisateur. Le cookie de session est présent tant que le navigateur Web est ouvert. Lorsque le navigateur Web est fermé, le cookie de session Application Firewall devient plus valide. L'état de la session conserve les informations des URL et formulaires visités par le client.

Le cookie de session de Web App Firewall configurable est `citrix_ns_id`.

À partir de Citrix ADC build 12.1 54 et 13.0, la cohérence des cookies est sans session et n'applique pas le cookie de session d'ajout `citrix_ns_id` généré par l'appliance.

Cookies Citrix Web App Firewall

De nombreuses applications Web génèrent des cookies pour suivre les informations spécifiques à l'utilisateur ou à la session. Ces informations peuvent être des préférences de l'utilisateur ou des articles de panier. Un cookie d'application Web peut être l'un des deux types suivants :

- **Cookies persistants** - Ces cookies sont stockés localement sur l'ordinateur et utilisés à nouveau la prochaine fois que vous visitez le site. Ce type de cookie contient généralement des informations sur l'utilisateur, telles que l'ouverture de session, le mot de passe ou les préférences.
- **Cookies de session ou transitoires** - Ces cookies ne sont utilisés que pendant la session et sont détruits après la fin de la session. Ce type de cookie contient des informations sur l'état de l'application, telles que les éléments du panier d'achat ou les informations d'identification de session.

Les pirates peuvent tenter de modifier ou de voler des cookies d'application pour détourner une session utilisateur ou se masquer en tant qu'utilisateur. Le pare-feu d'application empêche de telles tentatives en hachant les cookies de l'application, puis en ajoutant plus de cookies avec les signatures numériques. En traçant les cookies, le Pare-feu d'application garantit que les cookies ne sont pas modifiés ou compromis entre le navigateur client et le pare-feu d'application. Le Pare-feu d'application ne modifie pas les cookies de l'application.

Citrix Web Application Firewall génère les cookies par défaut suivants pour suivre les cookies d'application :

- **Cookies persistants** : `citrix_ns_id_wlf`. Note : wlf signifie vivra éternellement.
- **Cookies de session ou transitoires** : `citrix_ns_id_wat`. Note : wat signifie agir de façon transitoire.
  Pour suivre les cookies de l'application, le Pare-feu d'application regroupe les cookies persistants ou de session de l'application, puis hacher et signer tous les cookies ensemble. Ainsi, le Pare-feu d'application génère un `wlf` cookie pour suivre tous les cookies d'application persistants et un `wat` cookie pour suivre tous les cookies de session d'application.

Le tableau suivant indique le nombre et les types de cookies générés par l'Application Firewall sur la base des cookies générés par l'application web :

Avant Citrix ADC Web App Firewall	À
Un cookie persistant	Cookie persistant : `citix_ns_id_wlf`
Un cookie transitoire	Cookie transitoire : `citix_ns_id_wat`
Cookies persistants multiples, Cookies transitoires multiples	Un cookie persistant : `citrix_ns_id_wlf`, Un cookie transitoire : `citix_ns_id_wat`

Citrix Web App Firewall permet de chiffrer le cookie d'application. Application Firewall offre également une option pour proxy le cookie de session envoyé par l'application, en le stockant avec le reste des données de session Application Firewall et en ne l'envoyant pas au client. Lorsqu'un client envoie une requête à l'application qui inclut un cookie de session Application Firewall, Application Firewall insère le cookie envoyé de nouveau dans la demande avant d'envoyer la demande à l'application d'origine. Application Firewall permet également d'ajouter les indicateurs HttpOnly et/ou Secure aux cookies.

Comment le pare-feu de l'application affecte les en-têtes HTTP

Les requêtes HTTPS et les réponses HTTPS utilisent des en-têtes pour envoyer des informations sur un ou plusieurs messages Https. Un en-tête est une série de lignes avec chaque ligne contenant un nom suivi d'un deux-points, d'un espace et d'une valeur. Par exemple, l'en-tête Host a le format suivant :

```
Host: www.citrix.com
```

Certains champs d'en-tête sont utilisés dans les en-têtes de requête et de réponse, tandis que d'autres ne conviennent qu'à une demande ou à une réponse. Le pare-feu d'application peut ajouter, modifier ou supprimer certains en-têtes dans une ou plusieurs requêtes HTTPS ou réponse afin de maintenir la sécurité de l'application.

En-têtes de requête supprimés par Citrix Web Application Firewall

La plupart des en-têtes de requête liés à la mise en cache sont supprimés pour afficher chaque requête dans le contexte d'une session. De même, si la demande inclut un en-tête de codage permettant au serveur Web d'envoyer des réponses compressées, le pare-feu d'application supprime cet en-tête de sorte que le contenu de la réponse du serveur non compressé soit inspecté par le Web App Firewall pour éviter toute fuite de données sensibles vers le client.

Le pare-feu d'application supprime les en-têtes de requête suivants :

- Range : permet de récupérer à partir d'un transfert de fichiers en échec ou partiel.
- If-Range — Permet à un client de récupérer un objet partiel lorsqu'il contient déjà une partie de cet objet dans son cache (GET conditionnel).

- If-Modified-Since — Si l'objet demandé n'est pas modifié depuis l'heure spécifiée dans ce champ, une entité n'est pas renvoyée par le serveur. Vous obtenez une erreur HTTP 304 non modifiée.
- If-Non-Match — Permet des mises à jour efficaces des informations mises en cache avec un minimum de frais généraux.
- Accept-Encoding — Quelles méthodes d'encodage sont autorisées pour un objet particulier, tel que gzip.

En-tête de demande modifié par Citrix Web Application Firewall

Si un navigateur Web utilise les protocoles HTTP/1.0 ou antérieurs, le navigateur ouvre et ferme continuellement la connexion socket TCP après avoir reçu chaque réponse. Cela ajoute une surcharge au serveur Web et empêche le maintien de l'état de session. Le protocole HTTP/1.1 permet à la connexion de rester ouverte pendant la session. Le pare-feu d'application modifie l'en-tête de requête suivant pour utiliser HTTP/1.1 entre le pare-feu d'application et le serveur Web, quel que soit le protocole utilisé par le navigateur Web :
Connexion : keep-alive

En-têtes de requête ajoutés par Citrix Web Application Firewall

Le Pare-feu d'application agit comme un proxy inverse et remplace l'adresse IP source d'origine de la session par l'adresse IP du pare-feu d'application. Par conséquent, toutes les demandes enregistrées dans le journal du serveur Web indiquent que les demandes sont envoyées à partir du pare-feu d'application.

En-tête de réponse supprimé par Citrix Web Application Firewall

Le Pare-feu d'application peut bloquer ou modifier du contenu, comme la suppression des numéros de carte de crédit ou la suppression de commentaires, ce qui peut entraîner une inadéquation de la taille. Pour éviter un tel scénario, le pare-feu d'application supprime l'en-tête suivant :

Content-Length — Indique la taille du message envoyé au destinataire.
En-têtes de réponse modifiés par le pare-feu d'application

La plupart des en-têtes de réponse modifiés par le pare-feu Application sont liés à la mise en cache. Les en-têtes de mise en cache dans les réponses HTTP (S) doivent être modifiés pour forcer le navigateur Web à toujours envoyer une requête au serveur Web pour obtenir les données les plus récentes et à ne pas utiliser le cache local. Toutefois, certaines applications ASP utilisent des plug-ins distincts pour afficher des contenus dynamiques et peuvent nécessiter la possibilité de mettre en cache temporairement les données dans le navigateur. Pour autoriser la mise en cache temporaire des données lorsque des protections avancées de sécurité telles que FFC, fermeture d'URL ou vérifications CSRF

sont activées, Application Firewall ajoute ou modifie les en-têtes de contrôle de cache dans la réponse du serveur à l'aide de la logique suivante :

- Si Server envoie Pragma : no-cache, le pare-feu d'application n'effectue aucune modification.
- Si la requête client est HTTP 1.0, Application Firewall insère Pragma : no-cache.
- Si la requête client est HTTP 1.1 et a Cache-Control : no-store, Application Firewall n'apporte aucune modification.
- Si la requête client est HTTP 1.1 et que Server Response a un en-tête Cache-Control sans magasin ou aucune directive de cache, Application Firewall n'apporte aucune modification.
- Si la requête client est HTTP 1.1 et que la réponse du serveur n'a pas d'en-tête de contrôle Cache-Control ou l'en-tête Cache-Control n'a pas de directive magasin ou sans cache, le pare-feu d'application effectue les tâches suivantes :

1. Inserts Cache-control: max-age=3, must-revalidate,private.
2. Inserts X-Cache-Control-orig = Original value of Cache-Control Header.
3. Supprime l'en-tête Dernière modification.
4. Remplace Etag.
5. Insère X-Expires-Orig=Valeur d'origine de l'en-tête Expire envoyé par le serveur.
6. Modifie l'en-tête Expire et définit la date d'expiration de la page Web sur le passé, de sorte qu'elle est toujours récupérée à nouveau.
7. Modifie les plages Accept-Plages et la définit sur aucun.

Pour remplacer les données temporairement mises en cache dans le navigateur client lorsque Application Firewall modifie la réponse (par exemple, pour StripComments, X-out/Remove SafeObject, xout ou suppression de carte de crédit ou transformation d'URL), Application Firewall effectue les actions suivantes :

1. Supprime la dernière modification du serveur avant le transfert vers le client.
2. Remplace Etag par une valeur déterminée par Application Firewall.

En-têtes de réponse ajoutés par Citrix Web App Firewall

- `Transfer-Encoding` : Chunked. Cet en-tête transmet les informations à un client sans avoir à connaître la longueur totale de la réponse avant d'envoyer la réponse. Cet en-tête est obligatoire car l'en-tête de longueur de contenu est supprimé.
- `Set-Cookie` : les cookies ajoutés par le pare-feu d'application.
- `Xet-Cookie` : si la session est valide et si la réponse n'a pas expiré dans le cache, vous pouvez servir à partir du cache et n'avez pas à envoyer de nouveau cookie car la session est toujours valide. Dans un tel scénario, le Set-Cookie est changé en Xet-Cookie. Pour le navigateur Web.

Comment les données de formulaire sont affectées

Le pare-feu d'application protège contre les attaques qui tentent de modifier le contenu du formulaire original envoyé par le serveur. Il peut également se protéger contre les attaques de falsification de requête inter-site. Le pare-feu d'application effectue en insérant la balise de formulaire masquée as_fid dans la page.

Exemple : `<input type="hidden"name="as_fid"value="VRgWq0I196Jmg/+LOY7C"/>`

Le champ masqué as_fid est utilisé pour la cohérence des champs. Ce champ est utilisé par Application Firewall pour suivre tous les champs du formulaire, y compris les paires nom/valeur des champs masqués et pour s'assurer qu'aucun des champs du formulaire envoyé par le serveur n'est modifié du côté client. La vérification CSRF utilise également cette balise de formulaire unique as_fid pour s'assurer que les formulaires soumis par l'utilisateur ont été servis à l'utilisateur dans cette session et qu'aucun pirate ne tente de détourner la session utilisateur.

Vérification du formulaire sans session

Application Firewall offre également une option pour protéger les données de formulaire en utilisant une cohérence de champ sans session. Ceci est utile pour les applications où les formulaires peuvent avoir un grand nombre de champs masqués dynamiques qui conduisent à une allocation de mémoire élevée par session par le pare-feu d'application. Le contrôle de cohérence des champs sans session est effectué en insérant un autre champ masqué as_ffc_field pour uniquement les requêtes POST ou pour les requêtes GET et POST en fonction du paramètre configuré. Le pare-feu d'application change la méthode GET en POST lorsqu'il transfère le formulaire au client. L'appliance rétablit ensuite la méthode GET lorsqu'elle est renvoyée au serveur. La valeur as_ffc_field peut être volumineuse car elle contient le résumé chiffré du formulaire servi. Voici un exemple de vérification de formulaire sans session :

```
1 <input type="hidden" name="as_ffc_field" value="CwAAAAVIGLD/
     luRRi1Wu1rbYrFYargEDcO5xVAxsEnMP1megXuQfiDTGbwk0fpgndMHqfMbzfAFdjwR+
     TOm1oT
2 +u+Svo9+NuloPhtnbkxGtNe7gB/o8GlxEcK9ZkIIVv3oIL/
     nIPSRWJljgpWgafzVx7wtugNwnn8/
     GdnhneLCJTaYU7ScnC6LexJDLisI1xsEeONWt8Zm
3 +vJTa3mTebDY6LVyhDpDQfBgI1XLgfLTexAUzSNWHYyloqPruGYfnRPw+
     DIGf6gGwn1BYLEsRHKNbjJBrKpOJo9JzhEqdtZ1g3bMzEF9PocPvM1Hpvi5T6VB
4 /YFunUFM4f+bD7EAVcugdhovzb71CsSQX5+qcC1B8WjQ==" />
5 <!--NeedCopy-->
```

Décapage des commentaires HTML

Le pare-feu d'application offre également une option pour supprimer tous les commentaires HTML dans les réponses avant de les envoyer au client. Cela affecte non seulement les formulaires, mais toutes les pages de réponses. Le Pare-feu d'application localise et supprime tout texte incorporé entre les balises de commentaire "<!-" et "->". Les balises restent pour indiquer qu'un commentaire existait à cet emplacement du code source HTML. Tout texte incorporé dans d'autres balises HTML ou JavaScript est ignoré.
Certaines applications peuvent ne pas fonctionner correctement si JavaScript est incorrectement incorporé dans les balises de commentaire. Une comparaison du code source de la page avant et après que les commentaires ont été supprimés par Application Firewall peut aider à identifier si l'un des commentaires supprimés comportait le JavaScript requis intégré dans ces commentaires.

Protection des cartes de crédit

Le pare-feu d'application offre une option pour inspecter les en-têtes et le corps de la réponse et supprime ou élimine les numéros de carte de crédit avant de transférer la réponse au client. Actuellement Application Firewall offre une protection pour les principales cartes de crédit suivantes : American Express, Diners Club, Discover, JCB, MasterCard et Visa. L'action X-out fonctionne indépendamment de l'action Bloquer.

Protection sécurisée des objets

Comme pour les numéros de carte de crédit, la fuite d'autres données sensibles peut également être évitée en utilisant la vérification de sécurité Application Firewall Safe Object pour supprimer ou supprimer le contenu sensible dans la réponse.

Le script inter-site transforme l'action

Lorsque la transformation est activée pour le script intersite, le Web App Firewall change `"<"into "%26lt;"and ">"into "%26gt;"` dans les requêtes. Si le paramètre CheckRequestHeaders dans le Web App Firewall est activé, le pare-feu Web App inspecte les en-têtes de requête et transforme ces caractères dans En-tête et cookies également. L'action de transformation ne bloque ni ne transforme pas les valeurs initialement envoyées par le serveur. Il existe un ensemble d'attributs et de balises par défaut pour les scripts inter-sites que le Web App Firewall permet. Une liste par défaut des modèles de script intersite refusés est également fournie. Vous pouvez les personnaliser en sélectionnant l'objet signatures et en cliquant sur la boîte de **dialogue Gérer les modèles de script SQL/inter-site** dans l'interface graphique.

Transformation des caractères spéciaux SQL

Application Firewall possède les règles de transformation par défaut suivantes pour les caractères spéciaux SQL :

De	À	Transformation
‘(guillemet unique qui est, %27)	”	Un autre guillemet
\ (barre oblique inverse qui est %5c)	|Une autre barre oblique inverse ajoutée	
; (point-virgule qui est %3B)		Abandonné

Lorsque la transformation des caractères spéciaux est activée et que le checkRequestHeaders est défini sur ON, la transformation des caractères spéciaux se produit également dans les en-têtes et les cookies.
Remarque : Certains en-têtes de requête tels que User-Agent, Accept-Encoding contiennent généralement des points-virgules et peuvent être affectés par la transformation SQL.

Comportement Citrix Web Application Firewall dans lequel il corrompt l’en-tête EXPECT

1. Chaque fois que NetScaler reçoit une requête HTTP avec l’en-tête EXPECT, NetScaler envoie la réponse EXPECT: 100 -continue au client au nom du serveur back-end.
2. Ce problème est dû au fait que les protections du pare-feu d’application doivent être exécutées sur l’ensemble de la demande avant de transférer la demande au serveur, NetScaler doit obtenir la demande entière du client.
3. À la réception d’une `100 continue` réponse, le client envoie la partie restante de la demande qui complète la demande.
4. NetScaler exécute ensuite toutes les protections, puis transmet la requête au serveur.
5. Maintenant que NetScaler transfère la requête complète, l’en-tête EXPECT qui provient de la requête initiale devient obsolète, ce qui entraîne l’altération de cet en-tête par Netscaler qui l’envoie au serveur.
6. Serveur à la réception de la demande ignore tout en-tête corrompu.

Configuration de Web App Firewall

August 20, 2021

Vous pouvez configurer le pare-feu Citrix Web App (pare-feu Web App) à l’aide de l’une des méthodes suivantes :

- **Assistant Web App Firewall.** Boîte de dialogue composée d’une série d’écrans qui vous guident tout au long du processus de configuration.

- **Modèle AppExpert Interface Web Citrix.** Modèle AppExpert (un ensemble de paramètres de configuration) conçus pour fournir une protection appropriée aux sites Web. Ce modèle AppExpert contient les paramètres de configuration du Web App Firewall appropriés pour protéger de nombreux sites Web.
- **GUI Citrix ADC.** Interface de configuration basée sur le Web.
- **Interface de ligne de commande Citrix ADC.** Interface de configuration de ligne de commande.

Citrix vous recommande d'utiliser l'Assistant Web App Firewall. La plupart des utilisateurs trouveront qu'il s'agit de la méthode la plus simple pour configurer le Web App Firewall, et il est conçu pour éviter les erreurs. Si vous disposez d'un nouveau Citrix ADC ou VPX que vous utiliserez principalement pour protéger des sites Web, le modèle AppExpert Interface Web peut être une meilleure option car il fournit une bonne configuration par défaut, non seulement pour le Web App Firewall, mais pour l'ensemble de l'appliance. L'interface graphique et l'interface de ligne de commande sont toutes deux destinées aux utilisateurs expérimentés, principalement pour modifier une configuration existante ou utiliser des options avancées.

Assistant Web App Firewall

L'Assistant Web App Firewall est une boîte de dialogue composée de plusieurs écrans qui vous invitent à configurer chaque partie d'une configuration simple. Le Web App Firewall crée ensuite les éléments de configuration appropriés à partir des informations que vous lui fournissez. C'est le moyen le plus simple et, à la plupart des fins, le meilleur pour configurer le Web App Firewall.

Pour utiliser l'assistant, connectez-vous à l'interface graphique avec le navigateur de votre choix. Lorsque la connexion est établie, vérifiez que le Web App Firewall est activé, puis exécutez l'Assistant Web App Firewall, qui vous invite à fournir des informations de configuration. Vous n'avez pas à fournir toutes les informations demandées la première fois que vous utilisez l'Assistant. Au lieu de cela, vous pouvez accepter les paramètres par défaut, effectuer quelques tâches de configuration relativement simples pour activer des fonctionnalités importantes, puis autoriser le Web App Firewall à collecter des informations importantes pour vous aider à terminer la configuration.

Par exemple, lorsque l'Assistant vous invite à spécifier une règle pour sélectionner le trafic à traiter, vous pouvez accepter la valeur par défaut, qui sélectionne tout le trafic. Lorsqu'il vous présente une liste de signatures, vous pouvez activer les catégories de signatures appropriées et activer la collecte de statistiques pour ces signatures. Pour cette configuration initiale, vous pouvez ignorer les protections avancées (vérifications de sécurité). L'Assistant crée automatiquement la stratégie, l'objet signatures et le profil appropriés (collectivement, la configuration de sécurité) et lie la stratégie à globale. Le Web App Firewall commence alors à filtrer les connexions à vos sites Web protégés, à enregistrer toutes les connexions qui correspondent à une ou plusieurs des signatures que vous avez activées et à collecter des statistiques sur les connexions correspondant à chaque signature. Une fois que le Web App Firewall traite un certain trafic, vous pouvez exécuter à nouveau l'Assistant et examiner les

journaux et les statistiques pour voir si l'une des signatures que vous avez activées correspond au trafic légitime. Après avoir déterminé quelles signatures identifient le trafic que vous souhaitez bloquer, vous pouvez activer le blocage de ces signatures. Si votre site Web ou service Web n'est pas complexe, n'utilise pas SQL et n'a pas accès à des informations confidentielles, cette configuration de sécurité de base offrira probablement une protection adéquate.

Vous pourriez avoir besoin d'une protection supplémentaire si, par exemple, votre site Web est dynamique. Le contenu qui utilise des scripts peut avoir besoin d'une protection contre les attaques de scripts intersites. Le contenu Web qui utilise SQL (par exemple les paniers d'achat, de nombreux blogs et la plupart des systèmes de gestion de contenu) peut nécessiter une protection contre les attaques par injection SQL. Les sites Web et les services Web qui recueillent des informations confidentielles telles que les numéros de sécurité sociale ou les numéros de carte de crédit peuvent nécessiter une protection contre l'exposition involontaire de ces informations. Certains types de logiciels serveur Web ou serveur XML peuvent nécessiter une protection contre les types d'attaques adaptés à ce logiciel. Une autre considération est que certains éléments de vos sites Web ou services Web peuvent nécessiter une protection différente de celle d'autres éléments. L'examen des journaux et des statistiques du Web App Firewall peut vous aider à identifier les protections supplémentaires dont vous pourriez avoir besoin.

Après avoir décidé quelles protections avancées sont nécessaires pour vos sites Web et services Web, vous pouvez exécuter à nouveau l'Assistant pour configurer ces protections. Certaines vérifications de sécurité exigent que vous saisissiez des exceptions (relaxations) pour empêcher la vérification de bloquer le trafic légitime. Vous pouvez le faire manuellement, mais il est généralement plus facile d'activer la fonction d'apprentissage adaptatif et de lui permettre de recommander la relaxation nécessaire. Vous pouvez utiliser l'Assistant autant de fois que nécessaire pour améliorer votre configuration de sécurité de base et/ou créer des configurations de sécurité supplémentaires.

L'Assistant automatise certaines tâches que vous devrez effectuer manuellement si vous n'avez pas utilisé l'Assistant. Il crée automatiquement une stratégie, un objet signatures et un profil, et leur attribue le nom que vous avez fourni lorsque vous êtes invité à entrer le nom de votre configuration. L'Assistant ajoute également vos paramètres de protection avancée au profil, lie l'objet signatures au profil, associe le profil à la stratégie et met la stratégie en vigueur en le liant à Global.

Quelques tâches ne peuvent pas être exécutées dans l'Assistant. Vous ne pouvez pas utiliser l'Assistant pour lier une stratégie à un point de liaison autre que Global. Si vous souhaitez que le profil s'applique uniquement à une partie spécifique de votre configuration, vous devez configurer manuellement la liaison. Vous ne pouvez pas configurer les paramètres du moteur ou certaines autres options de configuration globales dans l'Assistant. Bien que vous puissiez configurer l'un des paramètres de protection avancés de l'Assistant, si vous souhaitez modifier un paramètre spécifique dans une seule vérification de sécurité, il peut être plus facile de le faire sur les écrans de configuration manuelle de l'interface graphique.

Pour plus d'informations sur l'utilisation de l'assistant Web App Firewall Wizard, consultez l'assistant

Web App Firewall Wizard.

Modèle AppExpert Interface Web Citrix

Les modèles AppExpert sont une approche différente et plus simple pour configurer et gérer des applications d'entreprise complexes. L'affichage AppExpert dans l'interface graphique est constitué d'une table. Les applications sont répertoriées dans la colonne la plus à gauche, les fonctionnalités de Citrix ADC applicables à cette application apparaissant chacune dans sa propre colonne à droite. (Dans l'interface AppExpert, les fonctionnalités associées à une application sont appelées *unités d'application*.) Dans l'interface AppExpert, vous configurez le trafic intéressant pour chaque application et activez les règles de compression, de mise en cache, de réécriture, de filtrage, de répondeur et de Web App Firewall, au lieu d'avoir à configurer chaque fonctionnalité individuellement.

Le modèle AppExpert Interface Web contient des règles pour les signatures de Web App Firewall et les vérifications de sécurité suivantes :

- **Refuser la vérification d'URL.** Détecte les connexions au contenu qui pose un risque de sécurité ou à toute autre URL que vous désignez.
- **Vérification du dépassement de tampon.** Détecte les tentatives de provoquer un dépassement de tampon sur un serveur Web protégé.
- **Vérification de la cohérence des cookies.** Détecte les modifications malveillantes des cookies définis par un site Web protégé.
- **Vérification de la cohérence des champs de formulaire.** Détecte les modifications apportées à la structure d'un formulaire Web sur un site Web protégé.
- **Vérification du marquage de formulaire CSRF.** Détecte les attaques de falsification de requêtes intersites.
- **Vérification des formats de champ.** Détecte les informations inappropriées téléchargées dans les formulaires Web sur un site Web protégé.
- **Vérification HTML SQL Injection.** Détecte les tentatives d'injection de code SQL non autorisé.
- **Contrôle HTML Cross-Site Scripting.** Détecte les attaques de script inter-sites.

Pour plus d'informations sur l'installation et l'utilisation d'un modèle AppExpert, consultez Applications et modèles AppExpert.

L'interface graphique Citrix

L'interface graphique est une interface Web qui permet d'accéder à toutes les options de configuration de la fonctionnalité de pare-feu de l'application Web, y compris les options de configuration et de gestion avancées qui ne sont disponibles à partir d'aucun autre outil ou interface de configuration. Plus précisément, de nombreuses options de signatures avancées peuvent être configurées uniquement dans l'interface graphique. Vous ne pouvez consulter les recommandations générées par la fonction-

nalité d'apprentissage que dans l'interface graphique. Vous pouvez lier des stratégies à un point de liaison autre que Global uniquement dans l'interface graphique.

Pour obtenir une description de l'interface graphique, reportez-vous à la section Interfaces de configuration du Web App Firewall. Pour plus d'informations sur l'utilisation de l'interface graphique pour configurer le Web App Firewall, voir Configuration manuelle à l'aide de l'interface graphique.

Pour obtenir des instructions sur la configuration du Web App Firewall à l'aide de l'interface graphique, voir Configuration manuelle à l'aide de l'interface graphique. Pour plus d'informations sur l'interface graphique de citrix-adc, reportez-vous à la section Interfaces de configuration du Web App Firewall.

Interface de ligne de commande Citrix ADC

L'interface de ligne de commande Citrix ADC est un shell UNIX modifié basé sur le shell bash FreeBSD. Pour configurer le Web App Firewall à partir de l'interface de ligne de commande, tapez des commandes à l'invite et appuyez sur la touche Entrée, comme vous le faites avec tout autre shell Unix. Vous pouvez configurer la plupart des paramètres et options pour le Web App Firewall à l'aide de la ligne de commande NetScaler. Les exceptions sont la fonctionnalité de signatures, dont la plupart des options peuvent être configurées uniquement à l'aide de l'interface graphique ou de l'assistant de Web App Firewall, et la fonctionnalité d'apprentissage, dont les recommandations ne peuvent être examinées que dans l'interface graphique.

Pour obtenir des instructions sur la configuration du Web App Firewall à l'aide de la ligne de commande Citrix ADC, reportez-vous à la section Configuration manuelle à l'aide de l'interface de ligne de commande.

Activer le Citrix Web App Firewall

August 20, 2021

Avant de pouvoir créer une configuration de sécurité, vous devez activer la fonctionnalité Citrix Web App Firewall sur l'appliance.

Points à retenir

- Si vous configurez une appliance Citrix Web App Firewall dédiée ou que vous mettez à niveau une appliance existante, la fonctionnalité est déjà activée. Vous n'avez pas à effectuer l'une ou l'autre des procédures décrites ici.
- Si vous disposez d'un nouveau Citrix ADC ou VPX, vous devez activer la fonctionnalité Citrix Web App Firewall avant de la configurer.

- Si vous mettez à niveau un Citrix ADC ou VPX à partir d'une version précédente, vous devez d'abord activer la fonctionnalité Citrix Web App Firewall avant de la configurer.

> **Remarque :**
>
> Si vous mettez à niveau un Citrix ADC ou VPX à partir d'une version précédente, vous devrez peut-être mettre à jour les licences de votre appliance avant d'activer Citrix Web App Firewall. Vérifiez auprès de votre représentant ou revendeur Citrix pour obtenir la licence correcte.

Activer Citrix Web App Firewall à l'aide de l'interface de commande

À l'invite de commandes, tapez la commande suivante :

```
enable ns feature AppFW
```

Activer le Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans le volet d'informations, cliquez sur **Configurer les fonctionnalités avancées**.
3. Dans la page **Configurer les fonctionnalités avancées**, sélectionnez **Citrix Web App Firewall**.
4. Cliquez sur **OK**.



Assistant Web App Firewall

August 20, 2021

Contrairement à la plupart des assistants, l'Assistant Citrix Web App Firewall est conçu non seulement pour simplifier le processus de configuration initiale, mais également pour modifier les configurations précédemment créées et pour maintenir la configuration de votre pare-feu Web App. Un utilisateur typique exécute l'Assistant plusieurs fois, ignorant certains écrans à chaque fois.

L'Assistant Web App Firewall crée automatiquement des profils, des stratégies et des signatures.

Ouverture de l'assistant

Pour exécuter l'Assistant Web App Firewall, ouvrez l'interface graphique et procédez comme suit :

1. Accédez à **Sécurité** > **Pare-feu d'application**.
2. Dans le volet d'informations, sous **Mise en route**, cliquez sur **Assistant Pare-feu d'application**. L'Assistant s'ouvre.

Pour plus d'informations sur l'interface graphique, voir « Interfaces de configuration du Web App Firewall. «

Les écrans de l'Assistant

L'Assistant Web App Firewall affiche les écrans suivants sur une page tabulaire :

1. Spécifier le nom : sur cet écran, lors de la création d'une nouvelle configuration de sécurité, spécifiez un nom significatif et le type approprié (HTML, XML ou WEB 2.0) pour votre profil. La stratégie par défaut et les signatures sont générées automatiquement en utilisant le même nom.

Nom du profil

Le nom peut commencer par une lettre, un nombre ou le symbole de trait de soulignement, et peut être composé de 1 à 31 lettres, chiffres et le tiret (-), point (.) livre (#), espace (), at (@), égal (=), deux-points (:) et soulignement (_). Choisissez un nom qui facilite l'affichage du contenu protégé par votre nouvelle configuration de sécurité.

> **Remarque :**
>
> Étant donné que l'Assistant utilise ce nom à la fois pour la stratégie et le profil, il est limité à 31 caractères. Les stratégies créées manuellement peuvent contenir des noms pouvant atteindre 127 caractères.

Lorsque vous modifiez une configuration existante, sélectionnez Modifier la configuration existante, puis, dans la liste déroulante Nom, sélectionnez le nom de la configuration existante à modifier.

> **Remarque :**
>
> Seules les stratégies liées à un point global ou à un point de liaison apparaissent dans cette liste ; vous ne pouvez pas modifier une stratégie non liée à l'aide de l'Assistant Pare-feu d'application. Vous devez soit le lier manuellement à Global ou à un point de liaison, soit le modifier manuellement. (Pour une modification manuelle, dans l'interface graphique) **Application Pare-feu** > **Stratégies** > Volet **Pare-feu**, sélectionnez la stratégie et cliquez sur **Ouvrir**.

Type de profil

Vous sélectionnez également un type de profil sur cet écran. Le type de profil détermine les types de protection avancée (vérifications de sécurité) qui peuvent être configurés. Étant donné que certains types de contenu ne sont pas vulnérables à certains types de menaces de sécurité, la restriction de la

liste des vérifications disponibles permet d'économiser du temps pendant la configuration. Les types de profils de Web App Firewall sont les suivants :

- Application Web (HTML). Tout site Web HTML qui n'utilise pas les technologies XML ou Web 2.0.
- Application XML (XML, SOAP). Tout service Web basé sur XML.
- Application Web 2.0 (HTML, XML, REST). Tout site Web 2.0 qui combine du contenu HTML et XML, tel qu'un site basé sur ATOM, un blog, un flux RSS ou un wiki.

Remarque : Si vous ne savez pas quel type de contenu est utilisé sur votre site Web, vous pouvez choisir Application Web 2.0 pour vous assurer de protéger tous les types de contenu d'application Web.

2. Spécifier la règle : sur cet écran, vous spécifiez la règle de stratégie (expression) qui définit le trafic examiné par la configuration actuelle. Si vous créez une configuration initiale pour protéger vos sites Web et services Web, vous pouvez accepter la valeur par défaut, **true**, qui sélectionne tout le trafic Web.

Si vous souhaitez que cette configuration de sécurité examine, non pas tout le trafic HTTP acheminé via l'appliance, mais le trafic spécifique, vous pouvez écrire une règle de stratégie spécifiant le trafic que vous souhaitez examiner. Les règles sont écrites dans le langage d'expressions Citrix ADC, qui est un langage de programmation orienté objet entièrement fonctionnel.

Remarque : Outre la syntaxe des expressions par défaut, pour des raisons de rétrocompatibilité, le système d'exploitation Citrix ADC prend en charge la syntaxe des expressions classiques Citrix ADC sur les appliances Citrix ADC Classic et NCore et les appliances virtuelles. Les expressions classiques ne sont pas prises en charge sur les appliances Citrix ADC Cluster et les appliances virtuelles. Les utilisateurs actuels qui souhaitent migrer leurs configurations existantes vers le cluster Citrix ADC doivent migrer toutes les stratégies contenant des expressions classiques vers la syntaxe des expressions par défaut.

- Pour obtenir une description simple de l'utilisation de la syntaxe des expressions Citrix ADC pour créer des règles de Web App Firewall et une liste de règles utiles, voir Stratégies de pare-feu.
- Pour obtenir une explication détaillée de la création de règles de stratégie dans la syntaxe des expressions Citrix ADC, consultez Politiques et expressions.

4. Sélectionnez Signatures : sur cet écran, vous sélectionnez les catégories de signatures que vous souhaitez utiliser pour protéger vos sites Web et services Web.

Cette étape n'est pas obligatoire, et vous pouvez l'ignorer si vous le souhaitez et aller à l'écran **Spécifier les protections profondes**. Si l'écran Sélectionner les signatures est ignoré, seuls un profil et les stratégies associées sont créés et les signatures ne sont pas créées.

Vous pouvez sélectionner **Créer une nouvelle signature** ou **Sélectionner une signature existante**.

Si vous créez une configuration de sécurité, les catégories de signature que vous sélectionnez sont

activées et, par défaut, elles sont enregistrées dans un nouvel objet signatures. Le nouvel objet signatures se voit attribuer le même nom que celui que vous avez entré sur l'écran Spécifier le nom que le nom de la configuration de sécurité.

Si vous avez déjà configuré des objets signatures et que vous souhaitez en utiliser l'un comme objet signatures associé à la configuration de sécurité que vous créez, cliquez sur **Sélectionner une signature existante** et sélectionnez un objet signatures dans la liste Signatures.

Si vous modifiez une configuration de sécurité existante, vous pouvez cliquer sur Sélectionner une signature existante et affecter un objet signatures différent à la configuration de sécurité.

Si vous cliquez sur Créer une nouvelle signature, vous pouvez choisir le mode d'édition comme **Simple** ou **Avancé**.

1. **Spécifier les protections de signature (mode simple)**

Le mode simple permet de configurer facilement la signature, avec une liste prédéfinie de définitions de protection pour les applications courantes telles que IIS (Internet Information Server), PHP et ActiveX. Les catégories par défaut en mode Simple sont :

- CGI. Protection contre les attaques contre les sites Web qui utilisent des scripts CGI dans n'importe quelle langue, y compris les scripts PERL, les scripts shell Unix et les scripts Python.
- Fusion froide. Protection contre les attaques contre les sites Web utilisant la plateforme de développement Web Adobe Systems® ColdFusion®.
- Page frontale. Protection contre les attaques contre les sites Web qui utilisent la plateforme de développement Web Microsoft® FrontPage®.
- PHP. Protection contre les attaques sur les sites Web utilisant le langage de script de développement Web open-source PHP.
- Côté client. Protection contre les attaques contre les outils côté client utilisés pour accéder à vos sites Web protégés, tels que Microsoft Internet Explorer, Mozilla Firefox, le navigateur Opera et Adobe Acrobat Reader.
- Microsoft IIS. Protection contre les attaques sur les sites Web exécutant Microsoft Internet Information Server (IIS)
- Divers. Protection contre les attaques sur d'autres outils côté serveur, tels que les serveurs Web et les serveurs de base de données.

Sur cet écran, vous sélectionnez les actions associées aux catégories de signatures sélectionnées dans l'écran Sélectionner les signatures. Les actions que vous pouvez configurer sont les suivantes :

- Bloquer
- Journal
- Statistiques

Par défaut, les actions Journal et Statistiques sont activées, mais pas l'action Bloquer. Pour configurer des actions, cliquez sur **Paramètres**. Vous pouvez modifier les paramètres d'action de toutes les catégories sélectionnées à l'aide de la liste déroulante **Action**.

1. **Spécifier les protections de signature (mode avancé)**

Le mode avancé permet un contrôle plus granulaire sur les définitions de signature et fournit beaucoup plus d'informations. Utilisez le mode avancé si vous souhaitez contrôler complètement la définition de signature.

Le contenu de cet écran est identique au contenu de la boîte de dialogue Modifier un objet Signatures, comme décrit dans Configuration ou modification d'un objet Signatures. Dans cet écran, vous pouvez configurer des actions en cliquant sur la liste déroulante **Actions** ou sur le menu Actions, qui apparaît sous la forme d'un cercle avec trois points.

7. Spécifiez des protections profondes : sur cet écran, vous choisissez les protections avancées (également appelées contrôles de sécurité ou simplement vérifications) que vous souhaitez utiliser pour protéger vos sites Web et services Web. Les vérifications disponibles dépendent du type de profil que vous avez choisi dans l'écran Spécifier le nom. Toutes les vérifications sont disponibles pour les profils d'application Web 2.0.

Pour plus d'informations, voir Vue d'ensemble des contrôles de sécuritéet voir Contrôles avancés de protection des formulaires.

Vous configurez les actions pour les protections avancées que vous avez activées.Les actions que vous pouvez configurer sont les suivantes :

- Bloque : bloque les connexions qui correspondent à la signature. Désactivé par défaut.
- Journal : enregistre les connexions qui correspondent à la signature pour une analyse ultérieure. Activé par défaut.
- Statistiques : gère des statistiques, pour chaque signature, qui indiquent le nombre de connexions correspondant et fournissent d'autres informations sur les types de connexions bloquées. Désactivé par défaut.
- Apprendre. Observez le trafic vers ce site Web ou service Web et utilisez des connexions qui violent à plusieurs reprises cette vérification pour générer des exceptions recommandées à la vérification ou de nouvelles règles pour la vérification. Disponible uniquement pour certains chèques. Pour plus d'informations sur la fonctionnalité d'apprentissage, voir Configuration et utilisation de la fonctionnalité d'apprentissage, et comment l'apprentissage fonctionne et comment configurer des exceptions (relaxations) ou déployer des règles apprises pour une vérification, voir Configuration manuelle à l'aide de l'interface graphique.

Pour configurer des actions, activez la protection en cochant la case à cocher, puis cliquez sur **Paramètres d'action** pour sélectionner les actions requises. Sélectionnez d'autres paramètres, si nécessaire, puis cliquez sur **OK** pour fermer la fenêtre Paramètres d'action.

Pour afficher tous les journaux d'une vérification spécifique, sélectionnez-la, puis cliquez sur **Journaux** pour afficher la visionneuse Syslog, comme décrit dans Journaux du Web App Firewall. Si une vérification de sécurité bloque l'accès légitime à votre site Web ou service Web protégé, vous pouvez créer et implémenter une relaxation pour cette vérification de sécurité en sélectionnant un journal affichant le blocage indésirable, puis en cliquant sur **Déployer**.

Après avoir spécifié les paramètres d'action, cliquez sur **Terminer** pour terminer l'Assistant.

Voici quatre procédures qui montrent comment effectuer des types de configuration spécifiques à l'aide de l'assistant de Web App Firewall.

Créer une nouvelle configuration

Procédez comme suit pour créer une configuration de pare-feu et des objets de signature, à l'aide de l'assistant de pare-feu Applicaiton.

1. Accédez à **Sécurité** > **Pare-feu d'application**.
2. Dans le volet d'informations, sous **Mise en route**, cliquez sur Pare-feu **d'application. L'Assistant s'ouvre.



3. Dans l'écran **Spécifier un nom**, sélectionnez **Créer une nouvelle configuration.
4. Dans le champ **Nom**, tapez un nom, puis cliquez sur **Suivant**.

5. Dans l'écran **Spécifier une règle**, cliquez à nouveau sur **Suivant**.
6. Dans l'écran **Sélectionner les signatures**, sélectionnez **Créer une nouvelle signature** et **Simple** comme mode de modification, puis cliquez sur **Suivant**.
7. Dans l'écran **Spécifier les protections de signature**, configurez les paramètres requis. Pour plus d'informations sur les signatures à prendre en compte pour le blocage et comment déterminer quand vous pouvez activer le blocage d'une signature en toute sécurité, voir Signatures.
8. Dans l'écran **Spécifier les protections approfondies**, configurez les actions et les paramètres requis dans **Paramètres d'action**.
9. Lorsque vous avez terminé, cliquez sur **Terminer** pour fermer l'Assistant Pare-feu d'application.

Modifier une configuration existante

Procédez comme suit pour modifier une configuration existante et des catégories de signatures existantes.

1. Accédez à **Sécurité** > **Pare-feu d'application**.
2. Dans le volet d'informations, sous **Mise en route**, cliquez sur **Assistant Pare-feu d'application**. L'Assistant s'ouvre.
3. Dans l'écran **Spécifier le nom**, sélectionnez Modifier la configuration existante et, dans la liste déroulante **Nom**, choisissez la configuration de sécurité que vous avez créée lors de la nouvelle configuration, puis cliquez sur **Suivant**.
4. Dans l'écran **Spécifier la règle**, cliquez sur Suivant pour conserver la valeur par défaut « true ». Si vous souhaitez modifier la règle, suivez les étapes décrites dans Configurer une expression de stratégie personnalisée.
5. Dans l'écran **Sélectionner les signatures**, cliquez sur **Sélectionner une signature existante**. Dans la liste déroulante **Signature existante**, sélectionnez l'option appropriée, puis cliquez sur **Suivant**. L'écran de protection avancée des signatures apparaît.
   Remarque : Si vous sélectionnez une signature existante, le mode d'édition par défaut pour la signature protégée est avancé.
6. Dans l'écran Spécifier les protections de signature, configurez les paramètres requis et cliquez sur **Suivant**. Pour plus d'informations sur les signatures à prendre en compte pour le blocage et comment déterminer quand vous pouvez activer le blocage d'une signature en toute sécurité, voir Signatures.
7. Dans l'écran **Spécifier les protections profondes**, configurez les paramètres et cliquez sur **Suivant**.
8. Une fois que vous avez terminé, cliquez sur **Terminer** pour fermer l'**Assistant Web App Firewall**.

Créer une nouvelle configuration sans signatures

Procédez comme suit pour utiliser l'Assistant Pare-feu d'application pour ignorer l'écran Sélectionner les signatures et créer une nouvelle configuration avec uniquement le profil et les stratégies associées, mais sans signatures.

1. Accédez à **Sécurité** > **Pare-feu d'application**.
2. Dans le volet d'informations, sous **Mise en route**, cliquez sur **Assistant Pare-feu d'application**. L'Assistant s'ouvre.
3. Sur l'écran **Spécifier le nom**, sélectionnez **Créer une nouvelle configuration**.
4. Dans le champ **Nom**, tapez un nom, puis cliquez sur **Suivant**.
5. **Dans l'écran**Spécifier une règle**, cliquez à nouveau sur Suivant.**
6. Dans l'écran **Sélectionner les signatures**, cliquez sur **Ignorer.**
7. Dans l'écran **Spécifier les protections approfondies**, configurez les actions et les paramètres requis dans **Paramètres d'action**.
8. Lorsque vous avez terminé, cliquez sur **Terminer** pour fermer l'Assistant Pare-feu d'application.

Configurer une expression de stratégie personnalisée

Procédez comme suit pour utiliser l'Assistant Pare-feu d'application pour créer une configuration de sécurité spécialisée afin de protéger uniquement le contenu spécifique. Dans ce cas, vous créez une nouvelle configuration de sécurité au lieu de modifier la configuration initiale. Ce type de configuration de sécurité nécessite une règle personnalisée, de sorte que la stratégie applique la configuration uniquement au trafic Web sélectionné.

1. Accédez à **Sécurité** > **Pare-feu d'application**.
2. Dans le volet d'informations, sous **Mise en route**, cliquez sur **Assistant Pare-feu d'application**.
3. Dans l'écran Spécifier un nom, tapez un nom pour votre nouvelle configuration de sécurité dans la zone de texte Nom, sélectionnez le type de configuration de sécurité dans la liste déroulante Type, puis cliquez sur **Suivant**.
4. Dans l'écran **Spécifier une règle**, entrez une règle qui correspond uniquement au contenu que vous souhaitez que cette application Web protège. Utilisez la liste déroulante **Expressions fréquemment utilisées** et l'**éditeur d'**expressions pour créer une expression personnalisée. Lorsque vous avez terminé, cliquez sur **Suivant**.
5. Dans l'écran **Sélectionner les signatures**, sélectionnez le mode de modification, puis cliquez sur **Suivant**.
6. Dans l'écran **Spécifier les protections de signature**, configurez les paramètres requis.
7. Dans l'écran **Spécifier les protections approfondies**, configurez les actions et les paramètres requis dans **Paramètres d'action**.
8. Lorsque vous avez terminé, cliquez sur **Terminer** pour fermer l' **Assistant Pare-feu d'application**.

Configuration manuelle

August 20, 2021

Si vous souhaitez lier un profil à un point de liaison autre que Global, vous devez configurer manuellement la liaison. En outre, certaines vérifications de sécurité exigent que vous saisissez manuellement les exceptions nécessaires ou que la fonctionnalité d'apprentissage génère les exceptions dont vos sites Web et services Web ont besoin. Certaines de ces tâches ne peuvent pas être effectuées à l'aide de l'Assistant Web App Firewall.

Si vous connaissez bien le fonctionnement du Web App Firewall et que vous préférez une configuration manuelle, vous pouvez configurer manuellement un objet signatures et un profil, associer l'objet signatures au profil, créer une stratégie avec une règle qui correspond au trafic Web que vous souhaitez configurer et associer la stratégie avec le profil. Vous liez ensuite la stratégie à Global, ou à un point de liaison, pour la mettre en œuvre, et vous avez créé une configuration de sécurité complète.

Pour la configuration manuelle, vous pouvez utiliser l'interface graphique (interface graphique) ou la ligne de commande. Citrix vous recommande d'utiliser l'interface graphique. Toutes les tâches de configuration ne peuvent pas être exécutées sur la ligne de commande. Certaines tâches, telles que l'activation des signatures et l'examen des données apprises, doivent être effectuées dans l'interface graphique. La plupart des autres tâches sont plus faciles à effectuer dans l'interface graphique.

Réplication de la configuration

Lorsque vous utilisez l'interface graphique (GUI) ou l'interface de ligne de commande (CLI) pour configurer manuellement le Web App Firewall, la configuration est enregistrée dans le fichier /nsconfig/ns.conf. Vous pouvez utiliser les commandes de ce fichier pour répliquer la configuration sur une autre appliance. Vous pouvez couper et coller les commandes dans l'interface de ligne de commande une par une, ou enregistrer plusieurs commandes dans un fichier texte dans le dossier /var/tmp et les exécuter en tant que fichier batch. Voici un exemple d'exécution d'un fichier batch contenant des commandes copiées à partir du fichier /nsconfig/ns.conf d'une autre appliance :

```
> batch -f /var/tmp/appfw_add.txt
```

> **Avertissement :**
>
> Les commandes d'importation ne sont pas enregistrées dans le fichier ns.conf. Avant d'exécuter des commandes à partir du fichier ns.conf pour répliquer la configuration sur une autre appliance, vous devez importer tous les objets utilisés dans la configuration (par exemple, signatures, page d'erreur, WSDL et schéma) vers l'appliance sur laquelle vous répliquez la configuration. La commande add permettant d'ajouter un profil Web App Firewall enregistré dans un fichier ns.conf peut inclure le nom d'un objet importé, mais cette commande peut échouer lorsqu'elle

> est exécutée sur une autre appliance si l'objet référencé n'existe pas sur cette appliance.

Pour plus d'informations sur les détails d'importation ou d'exportation pour la réplication de la configuration, consultez les rubriques Exportation de signatureset Export d'importation commune .

Configuration manuelle à l'aide de l'interface graphique Citrix ADC

August 20, 2021

Si vous devez configurer manuellement la fonctionnalité de Web App Firewall, Citrix vous recommande d'utiliser la procédure GUI Citrix ADC.

Pour créer et configurer un objet de signatures

Avant de pouvoir configurer les signatures, vous devez créer un objet signatures à partir du modèle d'objet signatures par défaut approprié. Attribuez un nouveau nom à la copie, puis configurez la copie. Vous ne pouvez pas configurer ou modifier directement les objets de signatures par défaut. La procédure suivante fournit des instructions de base pour configurer un objet signatures. Pour obtenir des instructions plus détaillées, voir Configuration manuelle de la fonctionnalité Signatures.

1. Accédez à **Sécurité > Citrix Web App Firewall > Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures que vous souhaitez utiliser comme modèle, puis cliquez sur **Ajouter**.

   Vos choix sont les suivants :

   - **Signatures par défaut.** Contient les règles de signatures, les règles d'injection SQL et les règles de script intersite.
   - **Injection XPath.** Contient tous les éléments des signatures par défaut et contient en outre les règles d'injection XPath.
3. Dans la boîte de dialogue **Ajouter un objet Signatures**, tapez un nom pour votre nouvel objet signatures, cliquez sur OK, puis cliquez sur **Fermer**. Le nom peut commencer par une lettre, un nombre ou le symbole de trait de soulignement, et peut être composé de 1 à 31 lettres, chiffres et le tiret (-), point (.) livre (#), espace (), arobase (@), égal (=) et soulignement (_).
4. Sélectionnez l'objet signatures que vous avez créé, puis cliquez sur **Ouvrir**.
5. Dans la boîte de dialogue **Modifier l'objet Signatures**, définissez les options **Afficher les critères de filtre** à gauche pour afficher les éléments de filtre que vous souhaitez configurer.

   Lorsque vous modifiez ces options, les résultats que vous spécifiez sont affichés dans la fenêtre Résultats filtrés située à droite. Pour plus d'informations sur les catégories de signatures, voir Signatures.

6. Dans la zone **Résultats filtrés**, configurez les paramètres d'une signature en cochant et en désactivant les cases à cocher appropriées.
7. Lorsque vous avez terminé, cliquez sur **Fermer**.

Pour créer un profil Web App Firewall à l'aide de l'interface graphique

La création d'un profil Web App Firewall nécessite que vous ne spécifiez que quelques détails de configuration.

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un profil de Web App Firewall**, tapez un nom pour votre profil.

   Le nom peut commencer par une lettre, un nombre ou le symbole de trait de soulignement, et peut être composé de 1 à 31 lettres, chiffres et le tiret (-), point (.) livre (#), espace (), arobase (@), égal (=), deux-points (:) et soulignement (_).
4. Choisissez le type de profil dans la liste déroulante.
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour configurer un profil de Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez le profil à configurer, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Configurer le profil du Web App Firewall**, sous l'onglet **Vérifications de sécurité**, configurez les vérifications de sécurité.
   - Pour activer ou désactiver une action pour une vérification, dans la liste, activez ou désactivez la case à cocher correspondant à cette action.
   - Pour configurer d'autres paramètres pour les vérifications qui en ont, dans la liste, cliquez sur le chevron bleu à l'extrême droite de cette vérification. Dans la boîte de dialogue qui s'affiche, configurez les paramètres. Ceux-ci varient d'une vérification à l'autre.

     Vous pouvez également sélectionner une coche et, en bas de la boîte de dialogue, cliquez sur Ouvrir pour afficher la boîte de dialogue Configurer la relaxation ou Configurer la règle pour cette vérification. Ces boîtes de dialogue varient également d'une vérification à l'autre. La plupart d'entre eux comprennent un onglet Vérifications et un onglet Général. Si la vérification prend en charge les relaxations ou les règles définies par l'utilisateur, l'onglet Vérifications inclut un bouton Ajouter, qui ouvre une nouvelle boîte de dialogue, dans laquelle vous pouvez spécifier une relaxation ou une règle pour la vérification. (Un

assouplissement est une règle permettant d'exempter le trafic spécifié du contrôle.) Si les relaxations ont déjà été configurées, vous pouvez en sélectionner une et cliquer sur Ouvrir pour la modifier.

- Pour consulter les exceptions ou les règles apprises pour une vérification, sélectionnez la vérification, puis cliquez sur Violations apprises. Dans la boîte de dialogue Gérer les règles apprises, sélectionnez successivement chaque exception ou règle apprise.
  - Pour modifier l'exception ou la règle, puis l'ajouter à la liste, cliquez sur **Modifier et déployer**.
  - Pour accepter l'exception ou la règle sans modification, cliquez sur **Déployer**.
  - Pour supprimer l'exception ou la règle de la liste, cliquez sur **Ignorer**.
- Pour actualiser la liste des exceptions ou des règles à réviser, cliquez sur **Actualiser**.
- Pour ouvrir le **visualiseur d'apprentissage** et l'utiliser pour consulter les règles apprises, cliquez sur **Visualizer**.
- Pour vérifier les entrées de journal des connexions correspondant à une vérification, sélectionnez la vérification, puis cliquez sur **Journaux**. Vous pouvez utiliser ces informations pour déterminer quelles vérifications correspondent aux attaques afin d'activer le blocage de ces vérifications. Vous pouvez également utiliser ces informations pour déterminer quelles vérifications correspondent au trafic légitime, de sorte que vous pouvez configurer une exemption appropriée pour autoriser ces connexions légitimes. Pour plus d'informations sur les journaux, consultez Journaux, statistiques et rapports.
- Pour désactiver complètement une coche, dans la liste, désactivez toutes les cases à droite de cette coche.

4. Sous l'onglet **Paramètres**, configurez les paramètres du profil.
   - Pour associer le profil à l'ensemble de signatures que vous avez précédemment créé et configuré, sous **Paramètres communs**, sélectionnez cet ensemble de signatures dans la liste déroulante Signatures.

     > **Remarque :**
     >
     > Vous pouvez utiliser la barre de défilement située à droite de la boîte de dialogue pour afficher la section Paramètres communs.

   - Pour configurer un objet Erreur HTML ou XML, sélectionnez l'objet dans la liste déroulante appropriée.

     > **Remarque :**
     >
     > Vous devez d'abord charger l'objet d'erreur que vous souhaitez utiliser dans le volet Importer.

- Pour configurer le type de contenu XML par défaut, tapez la chaîne de type de contenu directement dans les zones de texte Demande par défaut et Réponse par défaut, ou cliquez sur Gérer les types de contenu autorisés pour gérer la liste des types de contenu autorisés.

5. Si vous souhaitez utiliser la fonctionnalité d'apprentissage, cliquez sur Formation et configurez les paramètres d'apprentissage du profil. Pour plus d'informations, voir Fonctionnalité Configurer et apprendre.
6. Cliquez sur **OK** pour enregistrer vos modifications et revenir au volet Profils.

Configuration d'une règle ou d'une relaxation Web App Firewall

Vous configurez deux types d'informations différents dans cette boîte de dialogue, selon le contrôle de sécurité que vous configurez. Dans la plupart des cas, vous configurez une exception (ou relaxation) à la vérification de sécurité. Si vous configurez la vérification Refuser URL ou la vérification Formats de champ, vous configurez une addition (ou une règle). Le processus pour l'un ou l'autre d'entre eux est le même.

Pour configurer une règle de relaxation à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité** > **Citrix Web App Firewall** > **Profils**.
2. Dans le volet **Profils**, sélectionnez le profil à configurer, puis cliquez sur **Modifier**.
3. Dans la page **Configurer le profil du Web App Firewall**, cliquez sur **Règle de relaxation** à partir de la section **Paramètres avancés**. La section **Règle de relaxation** contient la liste complète des règles de relaxation du Web App Firewall.
4. Cliquez sur une règle de sécurité que vous souhaitez configurer, puis cliquez sur **Modifier**.
5. La page Règles de relaxation d'URL contient une liste d'actions que vous pouvez configurer pour cette règle ainsi qu'une liste de relaxations ou de règles existantes. La liste peut être vide si vous n'avez pas ajouté manuellement de relaxations ou approuvé les relaxations recommandées par le moteur d'apprentissage. Sous la liste se trouve une rangée de boutons qui vous permettent d'ajouter, de modifier, de supprimer, d'activer ou de désactiver les relaxations de la liste.
6. Pour ajouter ou modifier une relaxation ou une règle, effectuez l'une des opérations suivantes :

   - Pour ajouter une nouvelle relaxation, cliquez sur **Ajouter**.
   - Pour modifier une relaxation existante, sélectionnez la relaxation à modifier, puis cliquez sur **Ouvrir**.

   La page **Démarrer la règle de relaxation d'URL** s'affiche. À l'exception du titre, ces boîtes de dialogue sont identiques.

7. Remplissez la boîte de dialogue comme décrit ci-dessous. Les boîtes de dialogue de chaque coche sont différentes. La liste ci-dessous couvre tous les éléments susceptibles d'apparaître dans n'importe quelle boîte de dialogue.

   - **Case à cocher Activé** : activez cette option pour placer cette relaxation ou cette règle en cours d'utilisation ; désactivez cette option pour la désactiver.
   - **Type de contenu de pièce jointe** : attribut Content-Type d'une pièce jointe XML. Dans la zone de texte, entrez une expression régulière qui correspond à l'attribut Content-Type des pièces jointes XML à autoriser.
   - **URL d'action**—Dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL vers laquelle les données saisies dans le formulaire Web sont livrées.
   - **Cookie**—Dans la zone de texte, entrez une expression régulière au format PCRE qui définit le cookie.
   - **Nom de champ** : un élément de nom de champ de formulaire Web peut être étiqueté Nom de champ, Champ de formulaire ou un autre nom similaire. Dans la zone de texte, entrez une expression régulière au format PCRE qui définit le nom du champ de formulaire.
   - **URL de l'origine** : dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL qui héberge le formulaire Web.
   - **URL de l'action** : dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL à laquelle les données saisies dans le formulaire Web sont envoyées.
   - **Name —Nom**d'élément XML ou d'attribut. Dans la zone de texte, entrez une expression régulière au format PCRE qui définit le nom de l'élément ou de l'attribut.
   - **URL** : un élément URL peut être étiqueté URL d'action, URL de refus, URL d'action de formulaire, URL d'origine du formulaire, URL de démarrage ou simplement URL. Dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL.
   - **Format** : la section Format contient plusieurs paramètres qui incluent des zones de liste et des zones de texte. L'un des éléments suivants peut apparaître :
     - **Type** : sélectionnez un type de champ dans la liste déroulante Type. Pour ajouter une nouvelle définition de type de champ, cliquez sur Gérer —
     - **Minimum Length** : saisissez un entier positif qui représente la longueur minimale en caractères si vous souhaitez forcer les utilisateurs à remplir ce champ. Par défaut : 0 (permet de laisser le champ vide.)
     - **Longueur maximale** : pour limiter la longueur des données dans ce champ, tapez un entier positif qui représente la longueur maximale en caractères. Par défaut : 65535
   - **Location**—Choisissez l'élément de la demande auquel votre relaxation s'applique dans la liste déroulante. Pour les vérifications de sécurité HTML, les choix sont les suivants :

- FORMFIELD : champs de formulaire dans les formulaires Web.
- HEADER : demande des en-têtes.
- COOKIE : En-têtes de cookie.

Pour les vérifications de sécurité XML, les choix sont les suivants :

- ELEMENT : élément XML.
- ATTRIBUTE : attribut XML.

- **Taille maximale de la pièce jointe** : taille maximale en octets autorisée pour une pièce jointe XML.
- **Commentaires** : dans la zone de texte, tapez un commentaire. Facultatif.

Remarque : Pour tout élément nécessitant une expression régulière, vous pouvez taper l'expression régulière, utiliser le menu Jetons regex pour insérer des éléments et des symboles d'expression régulière directement dans la zone de texte, ou cliquer sur **Éditeur de regex** pour ouvrir la boîte de dialogue **Ajouter une expression régulière**, et utilisez-le pour construire l'expression.

8. Pour supprimer une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Supprimer**.
9. Pour activer une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Activer**.
10. Pour désactiver une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Désactiver**.
11. Pour configurer les paramètres et les relations de toutes les relaxations existantes dans un affichage graphique interactif intégré, cliquez sur **Visualizer**et utilisez les outils d'affichage.

> **Remarque :**
>
> Le bouton **Visualiseur** n'apparaît pas dans toutes les boîtes de dialogue de relaxation de vérification.

12. Pour consulter les règles apprises pour cette vérification, cliquez sur Apprentissage et effectuez les étapes de la section Pour configurer et utiliser la fonctionnalité d'apprentissage.
13. Cliquez sur **OK**.

Pour configurer les règles apprises à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité** > **Citrix Web App Firewall** > **Profils**.
2. Dans le volet **Profils**, sélectionnez le profil, puis cliquez sur **Modifier**.
3. Dans la page **Profil du Citrix Web App Firewall**, cliquez sur **Règles apprises** à partir des **paramètres avancés**. Dans la section **Règles apprises**, vous pouvez voir la liste des vérifications de sécurité disponibles dans le profil actuel et qui prennent en charge la fonctionnalité d'apprentissage.

4. Pour configurer les seuils d'apprentissage, sélectionnez une vérification de sécurité, puis cliquez sur **Paramètres**.
5. Dans la page **Paramètres des règles de profilage dynamique et d'apprentissage**, vous pouvez définir les paramètres. Pour plus d'informations, voir Paramètres de profil dynamique.
   - **Seuil de nombre minimum.** Selon les paramètres d'apprentissage de la vérification de sécurité que vous configurez, le seuil de nombre minimum peut faire référence au nombre minimum de sessions utilisateur totales à observer, au nombre minimum de demandes à observer ou au nombre minimum de fois qu'un champ de formulaire spécifique doit être observé, avant qu'une relaxation apprise ne soit générée. Par défaut : 1
   - **Pourcentage du seuil de durée.** Selon les paramètres d'apprentissage de la vérification de sécurité que vous configurez, le pourcentage de seuil de durée peut faire référence au pourcentage du nombre total de sessions utilisateur observées qui ont enfreint la vérification de sécurité, au pourcentage de demandes ou au pourcentage de fois qu'un champ de formulaire correspond à un type de champ particulier, avant qu'un une relaxation apprise est générée. Par défaut : 0
6. Pour supprimer toutes les données apprises et réinitialiser la fonction d'apprentissage afin qu'elle redémarre ses observations dès le début, sélectionnez l'action **Supprimer toutes les données apprises**.

   > **Remarque :**
   >
   > Ce bouton supprime uniquement les recommandations apprises qui n'ont pas été examinées et approuvées ou ignorées. Il ne supprime pas les relaxations apprises qui ont été acceptées et déployées.

7. Pour limiter le moteur de formation au trafic provenant d'un ensemble spécifique d'adresses IP, cliquez sur **Clients d'apprentissage approuvés**, puis ajoutez les adresses IP que vous souhaitez utiliser à la liste.
   a) Pour ajouter une adresse IP ou une plage d'adresses IP à la liste Clients d'apprentissage approuvés, cliquez sur **Ajouter**.
   b) Dans la page **Profil AppFirewall to Trusted Clint Binding**, cliquez sur **Ajouter**.
   c) **Activez la case à cocher Activé pour activer la fonction.**
   d) Dans la** zone Client d'apprentissage approuvé, tapez l'adresse IP ou une plage d'adresses IP au format CIDR.
   e) Dans la zone de texte **Commentaires**, tapez un commentaire qui décrit cette adresse IP ou cette plage.
   f) Cliquez sur **Créer** et **Fermer**.
8. Pour modifier une adresse IP existante ou une plage, cliquez sur l'adresse IP ou la plage, puis cliquez sur **Modifier**. À l'exception du nom, la boîte de dialogue qui s'affiche est identique à la boîte de dialogue Ajouter des clients d'apprentissage approuvés.

9. Pour désactiver ou activer une adresse IP ou une plage, mais la laisser dans la liste, cliquez sur l'adresse IP ou la plage, puis cliquez sur **Désactiver** ou **Activer**, selon le cas.
10. Pour supprimer complètement une adresse IP ou une plage, cliquez sur l'adresse IP ou la plage, puis cliquez sur **Supprimer**.
11. Cliquez sur **Fermer** pour revenir à la page **Profil du Citrix Web App Firewall**.

Pour créer une stratégie Citrix Web App Firewall à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité** > **Pare-feu Citrix Web App** > **Stratégies**.
2. Dans la page **Stratégies**, cliquez sur le lien **Stratégie de Citrix Web App Firewall**.
3. Dans la page Stratégies de Citrix Web App Firewall, cliquez sur **Ajouter**.
4. Dans la page Créer une stratégie de Citrix Web App Firewall, définissez les paramètres suivants.
    a) Nom. Le nom peut commencer par une lettre, un nombre ou le symbole de trait de soulignement et peut être composé de 1 à 128 lettres, chiffres et le trait d'union (-), point (.) livre (#), espace (), at (@), égal (=), deux-points (:) et soulignement (_).
    b) Profil. Sélectionnez le profil à associer à cette stratégie dans la liste déroulante Profil. Vous pouvez créer un profil à associer à votre stratégie en cliquant sur Nouveau, puis modifier un profil existant en cliquant sur **Modifier**.
    c) Expression. Dans la zone de texte Expression, créez une règle pour votre stratégie.
    d) Actions de journalisation. Ajoutez une action de journalisation ou vous pouvez modifier une action de journal existante.
    e) Commentaires. Une brève description de la politique.
5. Cliquez sur **Créer** ou **OK**, puis cliquez sur **Fermer**.



Pour créer ou configurer une règle de Web App Firewall (expression)

La règle de stratégie, également appelée *expression*, définit le trafic Web que le Web App Firewall filtre à l'aide du profil associé à la stratégie. Comme les autres règles de stratégie ADC Citrix (ou *expressions*), les règles de Web App Firewall utilisent la syntaxe des expressions Citrix ADC. Cette syntaxe est puissante, flexible et extensible. Il est trop complexe pour décrire complètement dans cet ensemble d'instructions. Vous pouvez utiliser la procédure suivante pour créer une règle de stratégie de pare-feu simple ou la lire comme une vue d'ensemble du processus de création de stratégie.

1. Si vous ne l'avez pas encore fait, accédez à l'emplacement approprié dans l'Assistant Web App Firewall ou dans l'interface graphique Citrix ADC pour créer votre règle de stratégie :
   - Si vous configurez une stratégie dans l'Assistant Pare-feu Web App, dans le volet de navigation, cliquez sur **Assistant Citrix Web App Firewall**, puis dans le volet d'informations, cliquez sur **Assistant Citrix Web App Firewall**, puis accédez à l'onglet **Spécifier une règle** .
   - Dans la page **Spécifier une règle**, choisissez le préfixe de votre expression dans la liste déroulante. Vos choix sont les suivants :
   - **HTTP.** Le protocole HTTP. Choisissez cette option si vous souhaitez examiner un aspect de la demande qui concerne le protocole HTTP.
   - **SYS.** Un ou plusieurs sites Web protégés. Choisissez cette option si vous souhaitez examiner un aspect de la demande qui concerne le destinataire de la demande.
   - **CLIENT.** Ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner un aspect de l'expéditeur de la demande.

- **SERVER.** Ordinateur auquel la demande a été envoyée. Choisissez cette option si vous souhaitez examiner un aspect du destinataire de la demande.

Après avoir choisi un préfixe, le Web App Firewall affiche une fenêtre d'invite en deux parties qui affiche les options suivantes possibles en haut et une brève explication de ce que signifie le choix sélectionné en bas.

2. Choisissez votre terme suivant.

   Si vous avez choisi HTTP comme préfixe, votre seul choix est REQ, qui spécifie la paire Request/Réponse. (Le Web App Firewall fonctionne sur la demande et la réponse en tant qu'unité plutôt que sur chacune séparément.) Si vous avez choisi un autre préfixe, vos choix sont plus variés. Pour obtenir de l'aide sur un choix spécifique, cliquez une fois sur ce choix pour afficher des informations à ce sujet dans la fenêtre d'invite inférieure.

   Lorsque vous avez décidé du terme souhaité, double-cliquez dessus pour l'insérer dans la fenêtre Expression.

3. Tapez un point après le terme que vous venez de choisir. Vous êtes alors invité à choisir votre prochain terme, comme décrit à l'étape précédente. Lorsqu'un terme nécessite que vous saisissiez une valeur, saisissez la valeur appropriée. Par exemple, si vous choisissez HTTP.REQ.HEADER(“”), tapez le nom de l'en-tête entre guillemets.

4. Continuez à choisir des termes dans les invites et à remplir toutes les valeurs nécessaires, jusqu'à ce que votre expression soit terminée.

   Voici quelques exemples d'expressions à des fins spécifiques.

   - **Hôte Web spécifique.** Pour faire correspondre le trafic provenant d'un hôte Web particulier :

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

Pour shopping.example.com, remplacez le nom de l'hôte Web que vous souhaitez faire correspondre.

- **Dossier Web ou répertoire spécifique.** Pour faire correspondre le trafic provenant d'un dossier ou d'un répertoire particulier sur un hôte Web :

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")
```

Pour www.example.com, remplacez le nom de l'hôte Web. Pour le dossier, remplacez le dossier ou le chemin d'accès au contenu que vous souhaitez faire correspondre. Par exemple, si votre panier se trouve dans un dossier appelé /solutions/orders, vous remplacez cette chaîne par dossier.

- **Type de contenu spécifique : images GIF.** Pour faire correspondre les images au format GIF :

```
HTTP.REQ.URL.ENDSWITH(".png")
```

Pour correspondre à d'autres images de format, remplacez une autre chaîne à la place de .png.

- **Type de contenu spécifique : scripts.** Pour faire correspondre tous les scripts CGI situés dans le répertoire CGI-BIN :

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")
```

Pour faire correspondre tous les Javascripts avec les extensions .js :

```
HTTP.REQ.URL.ENDSWITH(".js")
```

Pour plus d'informations sur la création d'expressions de stratégie, voir Stratégies et expressions.

> **Remarque :**
>
> Si vous utilisez la ligne de commande pour configurer une stratégie, n'oubliez pas d'échapper aux guillemets doubles dans les expressions Citrix ADC. Par exemple, l'expression suivante est correcte si elle est entrée dans l'interface graphique :

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

Si vous entrez dans la ligne de commande, cependant, vous devez taper ceci à la place :

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

```
1 ![Policy expression configuration](/en-us/citrix-adc/media/waf-rule.png
     )
```

Pour ajouter une règle de pare-feu (expression) à l'aide de la boîte de dialogue Ajouter une expression

La boîte de dialogue **Ajouter une expression** (également appelée Éditeur d'expression) aide les utilisateurs qui ne connaissent pas le langage d'expressions Citrix ADC à construire une stratégie qui correspond au trafic qu'ils souhaitent filtrer.

1. Si vous ne l'avez pas déjà fait, accédez à l'emplacement approprié dans l'Assistant Web App Firewall ou dans l'interface graphique Citrix ADC :
   - Si vous configurez une stratégie dans l'Assistant **Web App Firewall**, dans le volet de navigation, cliquez sur **Pare-feu Web App**, puis dans le volet de détails sur Assistant **Pare-feu Web App**, puis accédez à l'écran **Spécifier une règle**.
   - Si vous configurez une stratégie manuellement, dans le volet de navigation, développez **Web App Firewall**, **Stratégies**, puis **Pare-feu**. Dans le volet d'informations, pour créer une stratégie, cliquez sur **Ajouter**. Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Ouvrir**.
2. Dans l'écran **Spécifier une règle**, dans la boîte de dialogue **Créer un profil de Web App Firewall** ou dans la boîte de dialogue **Configurer le profil de pare-feu d'application Web**, cliquez sur **Ajouter**.

3. Dans la boîte de dialogue **Ajouter une expression**, dans la zone Construire une expression, dans la première zone de liste, choisissez l'un des préfixes suivants :
   - **HTTP.** Le protocole HTTP. Choisissez cette option si vous souhaitez examiner un aspect de la demande qui concerne le protocole HTTP. Le choix par défaut.
   - **SYS.** Un ou plusieurs sites Web protégés. Choisissez cette option si vous souhaitez examiner un aspect de la demande qui concerne le destinataire de la demande.
   - **CLIENT.** Ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner un aspect de l'expéditeur de la demande.
   - **SERVER.** Ordinateur auquel la demande a été envoyée. Choisissez cette option si vous souhaitez examiner un aspect du destinataire de la demande.
4. Dans la deuxième zone de liste, choisissez votre prochain terme. Les termes disponibles diffèrent selon le choix que vous avez fait à l'étape précédente, car la boîte de dialogue ajuste automatiquement la liste pour ne contenir que les termes valides pour le contexte. Par exemple, si vous avez sélectionné HTTP dans la zone de liste précédente, le seul choix est REQ, pour les demandes. Étant donné que le Web App Firewall traite les demandes et les réponses associées comme une seule unité et filtre les deux, vous n'avez pas besoin de réponses spécifiques séparément. Après avoir choisi votre deuxième terme, une troisième zone de liste apparaît à droite du second. La fenêtre Aide affiche une description du deuxième terme et la fenêtre Aperçu de l'expression affiche votre expression.
5. Dans la troisième zone de liste, choisissez le terme suivant. Une nouvelle zone de liste apparaît à droite et la fenêtre d'aide change pour afficher une description du nouveau terme. La fenêtre Aperçu de l'expression est mise à jour pour afficher l'expression telle que vous l'avez spécifiée à ce point.
6. Continuez à choisir des termes, et lorsque vous y êtes invité à remplir des arguments, jusqu'à ce que votre expression soit terminée. Si vous faites une erreur ou souhaitez modifier votre expression après avoir déjà sélectionné un terme, vous pouvez simplement choisir un autre terme. L'expression est modifiée et tous les arguments ou autres termes que vous avez ajoutés après le terme que vous avez modifié sont effacés.
7. Lorsque vous avez terminé de construire votre expression, cliquez sur OK pour fermer la boîte de dialogue Ajouter une expression. Votre expression est insérée dans la zone de texte Expression.

Pour lier une stratégie de Web App Firewall à l'aide de l'interface graphique Citrix ADC

1. Procédez comme suit :
   - Accédez à **Sécurité** > **Web App Firewall**, puis dans le volet d'informations, cliquez sur **Gestionnaire de stratégies de pare-feu d'application**.
   - Accédez à **Sécurité** > **Citrix Web App Firewall** > **Stratégies** > **Pare-feu**, puis dans le volet « Stratégies de Citrix Web App Firewall », cliquez sur **Gestionnaire de stratégies**.
2. Dans la boîte de dialogue **Application Firewall Policy Manager**, choisissez le point de liaison auquel vous souhaitez lier la stratégie dans la liste déroulante. Les choix sont les suivants :

- **Remplacer Global.** Les stratégies liées à ce point de liaison traitent tout le trafic provenant de toutes les interfaces de l'appliance Citrix ADC et sont appliquées avant toute autre stratégie.
- **Serveur virtuel LB.** Les stratégies liées à un serveur virtuel d'équilibrage de charge sont appliquées uniquement au trafic traité par ce serveur virtuel d'équilibrage de charge et sont appliquées avant toute stratégie globale par défaut. Après avoir sélectionné Serveur virtuel LB, vous devez également sélectionner le serveur virtuel d'équilibrage de charge spécifique auquel vous souhaitez lier cette stratégie.
- **Serveur virtuel CS.** Les stratégies liées à un serveur virtuel de commutation de contenu sont appliquées uniquement au trafic traité par ce serveur virtuel de commutation de contenu et sont appliquées avant toute stratégie globale par défaut. Après avoir sélectionné CS Virtual Server, vous devez également sélectionner le serveur virtuel de commutation de contenu spécifique auquel vous souhaitez lier cette stratégie.
- **Global par défaut.** Les stratégies liées à ce point de liaison traitent tout le trafic provenant de toutes les interfaces de l'appliance Citrix ADC.
- **Étiquette de stratégie.** Les stratégies liées à un trafic de traitement d'étiquette de stratégie que l'étiquette de stratégie leur achemine. L'étiquette de stratégie contrôle l'ordre dans lequel les stratégies sont appliquées à ce trafic.
- **Aucun.** Ne liez pas la stratégie à un point de liaison.

3. Cliquez sur **Continuer**. Une liste des stratégies de Web App Firewall existantes s'affiche.
4. Sélectionnez la stratégie que vous souhaitez lier en cliquant dessus.
5. Effectuez des ajustements supplémentaires à la liaison.
   - Pour modifier la priorité de stratégie, cliquez sur le champ pour l'activer, puis tapez une nouvelle priorité. Vous pouvez également sélectionner **Régénérer les priorités** pour renuméroter les priorités uniformément.
   - Pour modifier l'expression de stratégie, double-cliquez sur ce champ pour ouvrir la boîte de dialogue **Configurer la stratégie de Web App Firewall**, dans laquelle vous pouvez modifier l'expression de stratégie.
   - Pour définir l'expression Goto, double-cliquez sur le champ de l'en-tête **de colonne Optimer l'expression** pour afficher la liste déroulante, dans laquelle vous pouvez choisir une expression.
   - Pour définir l'option Invoke, double-cliquez sur le champ dans l'en-tête de colonne Invoquer pour afficher la liste déroulante, dans laquelle vous pouvez choisir une expression.
6. Répétez les étapes 3 à 6 pour ajouter toutes les stratégies de Web App Firewall supplémentaires que vous souhaitez lier globalement.
7. Cliquez sur **OK**. Un message apparaît dans la barre d'état indiquant que la stratégie a été liée avec succès.

Configuration manuelle À l'aide de l'interface de ligne de commande

August 20, 2021

> **Remarque :**
>
> Si vous devez configurer manuellement la fonctionnalité de Web App Firewall, Citrix vous recommande d'utiliser la procédure GUI Citrix ADC.

Vous pouvez configurer les fonctionnalités du Web App Firewall à partir de l'interface de commande **Citrix ADC**. Cependant, il existe d'importantes exceptions. Vous ne pouvez pas activer les signatures à partir de l'interface de commande. Il y a environ 1 000 signatures par défaut dans sept catégories et la tâche est trop complexe pour l'interface de commande. Vous pouvez activer ou désactiver des fonctionnalités et configurer des paramètres à partir de la ligne de commande, mais vous ne pouvez pas configurer des relaxations manuelles. Bien que vous puissiez configurer la fonction d'apprentissage adaptatif et activer l'apprentissage à partir de la ligne de commande, vous ne pouvez pas passer en revue les relaxations apprises ou les règles apprises et les approuver ou les ignorer. L'interface de ligne de commande est destinée aux utilisateurs avancés qui connaissent bien l'utilisation de l'appliance Citrix ADC et du Web App Firewall.

Pour configurer manuellement le Web App Firewall à l'aide de la ligne de commande Citrix ADC, utilisez un client telnet ou shell sécurisé de votre choix pour vous connecter à la ligne de commande Citrix ADC.

Pour créer un profil à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw profile <name> [-defaults ( basic | advanced )]`
- `set appfw profile <name> -type ( HTML | XML | HTML XML )`
- `save ns config`

Exemple

L'exemple suivant montre comment ajouter un profil nommé pr-basic, avec des valeurs par défaut de base, et affecter un type de profil HTML. Il s'agit de la configuration initiale appropriée pour un profil afin de protéger un site Web HTML.

```
1 add appfw profile pr-basic -defaults basic
2 set appfw profile pr-basic -type HTML
3 save ns config
4 <!--NeedCopy-->
```


Pour configurer un profil à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw profile <name> <arg1> [<arg2> ...]` où `<arg1>` représente un paramètre et `<arg2>` représente un autre paramètre ou la valeur à affecter au paramètre représenté par `<arg1>`. Pour obtenir des descriptions des paramètres à utiliser lors de la configuration de contrôles de sécurité spécifiques, consultez Protections avancées et ses sous-rubriques. Pour obtenir une description des autres paramètres, reportez-vous à la section « Paramètres pour la création d'un profil ».
- `save ns config`

Exemple

L'exemple suivant montre comment configurer un profil HTML créé avec des valeurs par défaut de base pour commencer à protéger un site Web HTML simple. Cet exemple montre comment activer la journalisation et la maintenance des statistiques pour la plupart des contrôles de sécurité, mais n'active le blocage que pour les contrôles dont les taux de faux positifs sont faibles et qui ne nécessitent aucune configuration particulière. Il active également la transformation de HTML dangereux et SQL dangereux, ce qui empêche les attaques mais ne bloque pas les requêtes vers vos sites Web. Lorsque la journalisation et les statistiques sont activées, vous pouvez examiner ultérieurement les journaux pour déterminer s'il faut activer le blocage pour une vérification de sécurité spécifique.

```
set appfw profile -startURLAction log stats
set appfw profile -denyURLAction block log stats
set appfw profile -cookieConsistencyAction log stats
set appfw profile -crossSiteScriptingAction log stats
set appfw profile -crossSiteScriptingTransformUnsafeHTML ON
set appfw profile -fieldConsistencyAction log stats
set appfw profile -SQLInjectionAction log stats
set appfw profile -SQLInjectionTransformSpecialChars ON
set appfw profile -SQLInjectionOnlyCheckFieldsWithSQLChars ON
set appfw profile -SQLInjectionParseComments checkall
set appfw profile -fieldFormatAction log stats
set appfw profile -bufferOverflowAction block log stats
set appfw profile -CSRFtagAction log stats
save ns config
<!--NeedCopy-->
```

Pour créer et configurer une stratégie

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw policy <name> <rule> <profile>`
- `save ns config`

Exemple

L'exemple suivant montre comment ajouter une stratégie nommée pl-blog, avec une règle qui intercepte tout le trafic à destination ou en provenance de l'hôte blog.example.com et associe cette stratégie au profil pr-blog.

```
1 add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com
     ")" pr-blog
2 <!--NeedCopy-->
```

Pour lier une stratégie de Web App Firewall

À l'invite de commandes, tapez les commandes suivantes :

- `bind appfw global <policyName> <priority>`
- `save ns config`

Exemple

L'exemple suivant lie la stratégie nommée pl-blog et lui attribue une priorité de 10.

```
1 bind appfw global pl-blog 10
2 save ns config
3 <!--NeedCopy-->
```

Pour configurer la limite de session par PE

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw settings <session limit>`

Exemple

L'exemple suivant configure la limite de session par PE.

```
1 > set appfw settings -sessionLimit 500000`
2
3 Done
4
5 Default value:100000   Max value:500000 per PE
```



```
<!--NeedCopy-->
```

Signatures

August 20, 2021

Les signatures du Web App Firewall fournissent des règles spécifiques et configurables pour simplifier la tâche de protection de vos sites Web contre les attaques connues. Une signature représente un modèle qui est un composant d'une attaque connue contre un système d'exploitation, un serveur Web, un site Web, un service Web XML ou une autre ressource. Un ensemble riche de règles préconfigurées intégrées ou natives du Web App Firewall offre une solution de sécurité facile à utiliser, en appliquant la puissance de la correspondance de modèles pour détecter les attaques et protéger contre les vulnérabilités des applications.

Vous pouvez créer vos propres signatures ou utiliser des signatures dans les modèles intégrés. Le Web App Firewall comporte deux modèles intégrés :

- **Signatures par défaut** : ce modèle contient une liste préconfigurée de plus de 1 300 signatures, en plus d'une liste complète de mots-clés d'injection SQL, de chaînes spéciales SQL, de règles de transformation SQL et de caractères génériques SQL. Il contient également des modèles refusés pour les scripts intersites, ainsi que des attributs et des balises autorisés pour les scripts intersites. Il s'agit d'un modèle en lecture seule. Vous pouvez afficher le contenu, mais vous ne pouvez pas ajouter, modifier ou supprimer quoi que ce soit dans ce modèle. Pour l'utiliser, vous devez en faire une copie. Dans votre propre copie, vous pouvez activer les règles de signature que vous souhaitez appliquer à votre trafic et spécifier les actions à entreprendre lorsque les règles de signature correspondent au trafic.

Les signatures du Web App Firewall sont dérivées des règles publiées par Snort, un système open source de prévention des intrusions capable d'effectuer une analyse du trafic en temps réel pour détecter diverses attaques et sondes.

- ***Xpath Injection Patterns** : Ce modèle contient un ensemble préconfiguré de mots-clés littéraux et PCRE et des chaînes spéciales qui sont utilisés pour détecter les attaques d'injection XPath (XML Path Language).

Signatures vides : en plus de faire une copie du modèle *Signatures par défaut intégré, vous pouvez utiliser un modèle de signatures vides pour créer un objet signature. L'objet de signature que vous créez avec l'option Signatures vides ne possède pas de règles de signature natives, mais, tout comme le modèle *Par défaut, il possède toutes les entités intégrées de script SQL/cross-site.

Signatures de format externe : Le Web App Firewall prend également en charge les signatures de format externe. Vous pouvez importer le rapport d'analyse tiers à l'aide des fichiers XSLT pris en charge

par le Citrix Web App Firewall. Un ensemble de fichiers XSLT intégrés est disponible pour les outils d'analyse suivants pour traduire les fichiers de format externe au format natif :

- Cenzic
- Sécurité profonde pour les applications Web
- IBM AppScan Enterprise
- IBM AppScan Standard.
- Qualys
- Qualys Cloud
- Whitehat
- Hewlett Packard Enterprise WebInspect
- Rapid7 Appspider
- Acunetix

Protection de sécurité pour votre application

Une sécurité plus serrée augmente les frais de traitement. Les signatures fournissent les options de déploiement suivantes pour vous aider à optimiser la protection de vos applications :

- **Modèle de sécurité négatif** : avec le modèle de sécurité négatif, vous utilisez un ensemble riche de règles de signature préconfigurées pour appliquer la puissance de la correspondance de motifs afin de détecter les attaques et de protéger contre les vulnérabilités des applications. Vous ne bloquez que ce que vous ne voulez pas et permettez le reste. Vous pouvez ajouter vos propres règles de signature, en fonction des besoins de sécurité spécifiques de vos applications, afin de concevoir vos propres solutions de sécurité personnalisées.
- **Modèle de sécurité hybride** : en plus d'utiliser des signatures, vous pouvez utiliser des contrôles de sécurité positifs pour créer une configuration parfaitement adaptée à vos applications. Utilisez des signatures pour bloquer ce que vous ne voulez pas, et utilisez des contrôles de sécurité positifs pour appliquer ce qui est autorisé.

Pour protéger votre application à l'aide de signatures, vous devez configurer un ou plusieurs profils pour utiliser votre objet signatures. Dans une configuration de sécurité hybride, les modèles d'injection SQL et de script inter-site, ainsi que les règles de transformation SQL, dans votre objet signatures sont utilisés non seulement par les règles de signature, mais aussi par les contrôles de sécurité positifs configurés dans le profil Web App Firewall qui utilise l'objet signatures.

Le Web App Firewall examine le trafic vers vos sites Web et services Web protégés pour détecter le trafic correspondant à une signature. Une correspondance n'est déclenchée que lorsque chaque motif de la règle correspond au trafic. Lorsqu'une correspondance se produit, les actions spécifiées pour la règle sont appelées. Vous pouvez afficher une page d'erreur ou un objet d'erreur lorsqu'une demande est bloquée. Les messages de journalisation peuvent vous aider à identifier les attaques lancées contre votre application. Si vous activez les statistiques, le Web App Firewall conserve les données rela-

tives aux demandes qui correspondent à une signature ou à une vérification de sécurité du pare-feu d'application Web.

Si le trafic correspond à la fois à une signature et à un contrôle de sécurité positif, la plus restrictive des deux actions est appliquée. Par exemple, si une demande correspond à une règle de signature pour laquelle l'action de blocage est désactivée, mais que la demande correspond également à une vérification de sécurité positive SQL Injection pour laquelle l'action est bloquée, la demande est bloquée. Dans ce cas, la violation de signature peut être enregistrée comme<not blocked>, bien que la demande soit bloquée par la vérification d'injection SQL.

Personnalisation : si nécessaire, vous pouvez ajouter vos propres règles à un objet signatures. Vous pouvez également personnaliser les modèles de script SQL/cross-site. L'option d'ajouter vos propres règles de signature, en fonction des besoins de sécurité spécifiques de vos applications, vous offre la flexibilité nécessaire pour concevoir vos propres solutions de sécurité personnalisées. Vous ne bloquez que ce que vous ne voulez pas et permettez le reste. Un modèle de correspondance rapide spécifique à un emplacement spécifique peut réduire considérablement les frais de traitement afin d'optimiser les performances. Vous pouvez ajouter, modifier ou supprimer des modèles d'injection SQL et de script intersite. Les éditeurs RegEx et d'expression intégrés vous aident à configurer vos modèles et à vérifier leur exactitude.

Mise à jour automatique : vous pouvez mettre à jour manuellement l'objet de signature pour obtenir les dernières règles de signature, ou appliquer la fonctionnalité de mise à jour automatique afin que le Web App Firewall puisse mettre à jour automatiquement les signatures à partir du service de mises à jour du pare-feu Web App basé sur un nuage.

> **Remarque :**
>
> Si de nouvelles règles de signature sont ajoutées lors de la mise à jour automatique, elles sont désactivées par défaut. Vous devez examiner périodiquement les signatures mises à jour et activer les règles nouvellement ajoutées qui sont pertinentes pour protéger vos applications.
>
> Vous devez configurer CORS pour héberger les signatures sur les serveurs IIS.
>
> La fonctionnalité de mise à jour automatique de signature ne fonctionne pas sur le serveur Web local lorsque vous accédez à l'URL à partir de l'interface graphique Citrix ADC.

Mise en route

L'utilisation des signatures Citrix pour protéger votre application est facile et peut être réalisée en quelques étapes simples :

1. Ajoutez un objet signature.

   - Vous pouvez utiliser l'Assistant qui vous invite à créer l'intégralité de la configuration du Web App Firewall, notamment en ajoutant le profil et la stratégie, en sélectionnant et en activant

les signatures et en spécifiant des actions pour les signatures et les vérifications de sécurité positives. L'objet signatures est créé automatiquement.

- Vous pouvez créer une copie de l'objet signatures à partir du modèle *Signatures par défaut, utiliser un modèle vide pour créer une signature avec vos propres règles personnalisées ou ajouter une signature de format externe. Activez les règles et configurez les actions à appliquer.

1. Configurez le profil de Web App Firewall cible pour utiliser cet objet signatures.
2. Envoyer du trafic pour valider la fonctionnalité

Résumé

- L'objet Signatures par défaut est un modèle. Il ne peut pas être modifié ou supprimé. Pour l'utiliser, vous devez créer une copie. Dans votre propre copie, vous pouvez activer les règles et l'action souhaitée pour chaque règle selon les besoins de votre application. Pour protéger l'application, vous devez configurer le profil cible pour qu'il utilise cette signature.
- Le traitement des modèles de signature a des frais généraux. Essayez d'activer uniquement les signatures applicables à la protection de votre application, plutôt que d'activer toutes les règles de signature.
- Chaque motif de la règle doit correspondre pour déclencher une correspondance de signature.
- Vous pouvez ajouter vos propres règles personnalisées pour inspecter les requêtes entrantes afin de détecter différents types d'attaques, telles que les attaques par injection SQL ou par script intersite. Vous pouvez également ajouter des règles pour inspecter les réponses afin de détecter et de bloquer les fuites d'informations sensibles telles que les numéros de carte de crédit.
- Vous pouvez faire une copie d'un objet de signature existant et le modifier, en ajoutant ou en modifiant des règles et des modèles de script SQL/cross-site, afin de protéger une autre application.
- Vous pouvez utiliser la mise à jour automatique pour télécharger la dernière version des règles par défaut du Web App Firewall sans avoir besoin d'une surveillance continue pour vérifier la disponibilité de la nouvelle mise à jour.
- Un objet signature peut être utilisé par plusieurs profils. Même après avoir configuré un ou plusieurs profils pour utiliser un objet signature, vous pouvez toujours activer ou désactiver les signatures ou modifier les paramètres d'action. Vous pouvez créer et modifier manuellement vos propres règles de signature personnalisées. Les modifications s'appliquent à tous les profils actuellement configurés pour utiliser cet objet de signature.
- Vous pouvez configurer les signatures pour détecter les violations dans différents types de charges utiles, tels que HTML, XML, JSON et GWT.
- Vous pouvez exporter un objet signatures configuré et l'importer dans un autre dispositif Citrix ADC pour faciliter la réplication de vos règles de signature personnalisées.

Les signatures sont des modèles associés à une vulnérabilité connue. Vous pouvez utiliser la pro-

tection des signatures pour identifier le trafic qui tente d'exploiter ces vulnérabilités et prendre des mesures spécifiques.

Les signatures sont organisées en catégories. Vous pouvez optimiser les performances et réduire les frais de traitement en activant uniquement les règles dans les catégories appropriées à la protection de votre application.

Configuration manuelle de la fonction de signatures

August 20, 2021

Pour utiliser des signatures pour protéger vos sites Web, vous devez examiner les règles et activer et configurer celles que vous souhaitez appliquer. Les règles sont désactivées par défaut. Citrix vous recommande d'activer toutes les règles applicables au type de contenu utilisé par votre site Web.

Pour configurer manuellement la fonction de signatures, utilisez un navigateur pour vous connecter à l'interface graphique. Ensuite, créez un objet signatures à partir d'un modèle intégré, d'un objet signatures existant ou en important un fichier. Ensuite, configurez le nouvel objet signatures comme expliqué dans Configuration ou modification d'un objet Signatures.

Ajout ou suppression d'un objet signature

January 21, 2021

Vous pouvez ajouter un nouvel objet signature au Web App Firewall en :

- Copie d'un modèle intégré.
- Copie d'un objet signatures existant.
- Importation d'un objet signatures à partir d'un fichier externe.

Le fichier de signature inclut l'utilisation de l'UC, la dernière année applicable et les détails du niveau de gravité. Vous pouvez voir l'utilisation de l'UC, l'année dernière et le niveau de gravité CVE chaque fois qu'un fichier de signature est modifié et téléchargé périodiquement. Après avoir observé ces valeurs, vous pouvez décider d'activer ou de désactiver la signature sur l'appliance.

Vous devez utiliser l'interface graphique pour copier un modèle ou un objet signatures existant. Vous pouvez utiliser l'interface graphique ou la ligne de commande pour importer un objet signatures. Vous pouvez également utiliser l'interface graphique ou la ligne de commande pour supprimer un objet signatures.

Pour créer un objet signatures à partir d'un modèle

1. Accédez à **Sécurité > Citrix Web App Firewall > Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures que vous souhaitez utiliser comme modèle.

   Vos choix sont les suivants :

   - **Signatures par défaut.** Contient les règles de signatures, les règles d'injection SQL et les règles de script intersite.
   - **Injection XPath.** Contient les modèles d'injection XPath.
   - **Tout objet de signatures existant.**

   > **Attention :**
   >
   > Si vous ne choisissez pas de type de signature à utiliser comme modèle, le Web App Firewall vous invite à créer des signatures à partir de zéro.

3. Cliquez sur **Ajouter**.
4. Dans la boîte de dialogue Ajouter un objet de signatures, tapez un nom pour votre nouvel objet de signatures, puis cliquez sur OK. Le nom peut commencer par une lettre, un nombre ou le symbole de trait de soulignement, et peut être composé de 1 à 31 lettres, chiffres et le tiret (-), point (.) livre (#), espace (), arobase (@), égal (=) et soulignement (_).
5. Cliquez sur **Fermer**.

Pour créer un objet signatures en important un fichier

1. Accédez à **Sécurité > Citrix Web App Firewall > Signatures**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un objet de signatures**, sélectionnez le format des signatures à importer.
   - Pour importer un fichier de signatures au format Citrix ADC, sélectionnez l'onglet **Format natif**.
   - Pour importer un fichier de format de signatures externes, sélectionnez l'onglet **Format externe**.
4. Choisissez le fichier que vous souhaitez utiliser pour créer votre objet signatures.
   - Pour importer un fichier de signatures au format Citrix ADC natif, dans la section Importer, sélectionnez Importer à partir d'un fichier local ou Importer à partir d'une URL, puis tapez ou accédez au chemin d'accès ou à l'URL du fichier.
   - Pour importer un fichier au format Cenzic, IBM AppScan, Qualys ou Whitehat, dans la section XSLT, sélectionnez Utiliser le fichier XSLT intégré, Utiliser le fichier local ou Référence à partir de l'URL. Ensuite, si vous avez choisi Utiliser le fichier XSLT intégré, sélectionnez

le format de fichier approprié dans la liste. Si vous avez choisi Utiliser le fichier local ou Référence à partir de l'URL, tapez ou recherchez le chemin d'accès ou l'URL du fichier.

5. Cliquez sur **Ajouter**, puis sur **Fermer**.

Pour créer un objet signatures en important un fichier à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `import appfw signatures <src> <name> [-xslt <string>] [-comment <string>] [-overwrite] [-merge] [-sha1 <string>]`
- `save ns config`

Exemple #1

L'exemple suivant crée un objet signatures à partir d'un fichier nommé signatures.xml et lui attribue le nom mySignatures.

```
1 import appfw signatures signatures.xml MySignatures
2 save ns config
3 <!--NeedCopy-->
```

Pour supprimer un objet signatures à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Web App Firewall > Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures à supprimer.
3. Cliquez sur **Supprimer**.

Pour supprimer un objet signatures à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `rm appfw signatures <name>`
- `save ns config`

Configuration ou modification d'un objet signatures

August 20, 2021

Vous configurez un objet signatures après l'avoir créé, ou modifiez un objet signatures existant, pour activer ou désactiver des catégories de signatures ou des signatures spécifiques, et configurez la façon dont le Web App Firewall répond lorsqu'une signature correspond à une connexion.

Pour configurer ou modifier un objet signatures

1. Accédez à **Sécurité > Citrix Web App Firewall > Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures à configurer, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Modifier l'objet Signatures**, définissez les options **Afficher les critères de filtre** à gauche pour afficher les éléments de filtre que vous souhaitez configurer.

   Lorsque vous modifiez ces options, les résultats que vous avez demandés sont affichés dans la fenêtre Résultats filtrés à droite.

   - Pour afficher uniquement les catégories de signatures sélectionnées, cochez ou désactivez les cases à cocher Catégorie de signature appropriées. Les catégories de signature sont les suivantes :

Nom	Type d'attaque contre laquelle cette signature protège
Effets spéciaux	Scripts CGI. Inclut les scripts shell Perl et UNIX.
client	Navigateurs et autres clients.
coldfusion	qui utilisent le serveur d'applications Adobe Systems ColdFusion.
frontpage	qui utilisent le serveur FrontPage de Microsoft.
iis	qui utilisent Microsoft Internet Information Server (IIS).
Divers	Attaques diverses.
php	sites Web qui utilisent PHP
web-activex	qui contiennent des contrôles ActiveX.
web-struts	qui contiennent des struts Apache, qui sont des applets basés sur java-ee.

   - Pour afficher uniquement les signatures pour lesquelles des actions de vérification spécifiques sont activées, activez la case à cocher Activé pour chacune de ces actions, désactivez les cases à cocher Activé pour les autres actions et désactivez toutes les cases à cocher Désactivé. Pour afficher uniquement les signatures pour lesquelles une action de

vérification spécifique est désactivée, activez leurs cases à cocher OFF respectives et désactivez toutes les cases à cocher ON. Pour afficher les signatures, qu'une action de vérification soit activée ou désactivée, activez ou désactivez les cases à cocher ON et OFF pour cette action. Les actions de vérification sont les suivantes :

Critère	Description
Activé	La signature est activée. Le Web App Firewall vérifie uniquement les signatures activées lorsqu'il traite le trafic.
Bloquer	Les connexions qui correspondent à cette signature sont bloquées.
Journal	Une entrée de journal est générée pour toute connexion qui correspond à cette signature.
Statistiques	Le Web App Firewall inclut toute connexion qui correspond à cette signature dans les statistiques qu'il génère pour cette vérification.

- Pour afficher uniquement les signatures contenant une chaîne spécifique, tapez la chaîne dans la zone de texte sous les critères de filtre, puis cliquez sur Rechercher.
- Pour réinitialiser tous les critères de filtre d'affichage aux paramètres par défaut et afficher toutes les signatures, cliquez sur Afficher tout.

4. Pour plus d'informations sur une signature spécifique, sélectionnez la signature, puis cliquez sur la double flèche bleue dans le champ Plus. La boîte de message Détail de la vulnérabilité de règle de signature s'affiche. Il contient des informations sur l'objet de la signature et fournit des liens vers des informations Web externes sur la vulnérabilité ou les vulnérabilités que cette signature corrige. Pour accéder à un lien externe, cliquez sur la double flèche bleue située à gauche de la description de ce lien.
5. Configurez les paramètres d'une signature en cochant les cases appropriées.
6. Si vous souhaitez ajouter une règle de signature locale à l'objet signatures ou modifier une règle de signature locale existante, consultez The Signatures Editor.
7. Si vous n'avez pas besoin d'injection SQL, de script intersite ou de modèles d'injection Xpath, cliquez sur OK, puis sur Fermer. Sinon, dans le coin inférieur gauche du volet d'informations, cliquez sur Gérer les modèles de script SQL/inter-site.
8. Dans la boîte de dialogue Gérer les modèles de script SQL/inter-sites, fenêtre Résultats filtrés, accédez à la catégorie et au modèle de répétition que vous souhaitez configurer. Pour plus d'informations sur les modèles d'injection SQL, reportez-vous à la section Vérification des in-

jections HTML SQL. Pour plus d'informations sur les modèles de script intersite, consultez Vérification des scripts intersites HTML.

9. Pour ajouter un nouveau motif :
   a) Sélectionnez la branche à laquelle vous souhaitez ajouter le nouveau motif.
   b) Cliquez sur le bouton **Ajouter** directement sous la section inférieure de la fenêtre **Résultats filtrés**.
   c) Dans la boîte de dialogue Créer un élément de signature, remplissez la zone de texte Elément avec le motif que vous souhaitez ajouter. Si vous ajoutez un motif de transformation à la branche Règles de transformation, sous Eléments, remplissez la zone de texte De avec le motif à modifier et la zone de texte À avec le motif auquel vous souhaitez modifier le motif précédent.
   d) Cliquez sur **OK**.
10. Pour modifier une répétition existante :
    a) Dans la fenêtre **Résultats filtrés**, sélectionnez la branche qui contient le motif à modifier.
    b) Dans la fenêtre de détail située sous la fenêtre **Résultats filtrés**, sélectionnez la répétition à modifier.
    c) Cliquez sur **Modifier**.
    d) Dans la boîte de dialogue **Modifier l'élément de signature, zone de texte Élément**, modifiez le motif. Si vous modifiez une répétition de transformation, vous pouvez modifier l'une ou l'autre des répétitions sous Eléments, dans les zones de texte De et À.
    e) Cliquez sur **OK**.
11. Pour supprimer une répétition, sélectionnez la répétition à supprimer, puis cliquez sur le bouton **Supprimer** sous le volet d'informations sous la fenêtre **Résultats filtrés**. Lorsque vous y êtes invité, confirmez votre choix en cliquant sur **Fermer**.
12. Pour ajouter la catégorie de motifs à la branche de script inter-site :
    a) Sélectionnez la branche à laquelle vous souhaitez ajouter la catégorie de motifs.
    b) Cliquez sur le bouton **Ajouter** directement sous la fenêtre **Résultats filtrés**.

       > **Remarque :** Actuellement, vous ne pouvez ajouter qu'une seule catégorie, les modèles nommés, à la branche de script inter-site. Par conséquent, après avoir cliqué sur **Ajouter**, vous devez accepter le choix par défaut, à savoir les modèles.

    c) Cliquez sur **OK**.
13. Pour supprimer une branche, sélectionnez cette branche, puis cliquez sur le bouton Supprimer directement sous la fenêtre **Résultats filtrés**. Lorsque vous y êtes invité, confirmez votre choix en cliquant sur **OK**.

> **Remarque :** Si vous supprimez une branche par défaut, vous supprimez tous les motifs de cette branche. Cela peut désactiver les contrôles de sécurité qui utilisent ces informations.

14. Lorsque vous avez terminé de modifier les modèles d'injection SQL, de script intersite et d'injection XPath, cliquez sur **OK**, puis sur **Fermer**pour revenir à la boîte de dialogue **Modifier l'objet signatures**.
15. Cliquez sur **OK** à tout moment pour enregistrer vos modifications et lorsque vous avez terminé de configurer l'objet signatures, cliquez sur **Fermer**.

Protection des applications JSON à l'aide de signatures

August 20, 2021

JavaScript Object Notation (JSON) est un standard ouvert basé sur le texte dérivé du langage de script JavaScript. JSON est préféré pour la représentation lisible par l'homme de structures de données simples et de tableaux associatifs, appelés objets. Il sert d'alternative au XML et est principalement utilisé pour transmettre des structures de données sérialisées pour communiquer avec des applications Web. Les fichiers JSON sont généralement enregistrés avec une extension .json.

La charge utile JSON est généralement envoyée avec le type MIME spécifié comme **application/json**. Les autres types de contenu « standard » pour JSON sont :

- **application/x-javascript**
- **text/javascript**
- **text/x-javascript**
- **text/x-json**

Utilisation des signatures du Citrix Web App Firewall pour protéger les applications JSON

Pour autoriser les requêtes JSON, l'appliance est préconfigurée avec le type de contenu JSON, comme indiqué dans la sortie show-command suivante :

```
1 > sh appfw jsonContentType
2 1)      JSONContenttypevalue:  "^application/json$" IsRegex:  REGEX
3 Done
4 <!--NeedCopy-->
```

Le Citrix Web App Firewall traite le corps de publication pour les types de contenu suivants uniquement :

- **application/x-www-form-urlencoded**

- **multipart/form-data**
- **text/x-gwt-rpc**

Les demandes reçues avec d'autres en-têtes de type contenu, y compris application/json (ou tout autre type de contenu autorisé), sont transmises au backend après l'inspection des en-têtes. Le corps de la publication dans ces requêtes n'est pas inspecté pour détecter les violations des contrôles de sécurité même lorsque les vérifications de sécurité du profil, telles que SQL ou le script inter-site, sont activées.

Afin de protéger les applications JSON et de détecter les violations, les signatures de Web App Firewall peuvent être utilisées. Toutes les demandes qui contiennent l'en-tête de type de contenu autorisé sont traitées par le Web App Firewall pour la correspondance de signature. Vous pouvez ajouter vos propres règles de signature personnalisées pour traiter la charge utile JSON pour effectuer diverses inspections de vérification de sécurité (par exemple, script inter-site, SQL et cohérence des champs), détecter les violations dans les en-têtes ainsi que dans le corps de la publication, et prendre des actions spécifiées.

> **Conseil**
>
> Contrairement aux autres valeurs par défaut intégrées, le type de contenu JSON préconfiguré peut être modifié ou supprimé à l'aide de l'interface de ligne de commande ou de l'interface graphique (GUI). Si des requêtes légitimes pour des applications JSON sont bloquées et déclenchent des violations de type de contenu, vérifiez que la valeur du type de contenu est configurée avec précision. Pour plus d'informations sur la façon dont Web App Firewall traite l'en-tête de type de contenu, voir Protection du type de contenu.

Pour ajouter ou supprimer le type de contenu JSON à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
add appfw jsonContentType ^application/json$ IsRegEx REGEX
```

```
rm appfw JSONContentType "^application/json$"
```

Pour gérer les types de contenu JSON à l'aide de l'interface graphique

Accédez à **Sécurité** > **Web App Firewall** et, dans la section **Paramètres**, sélectionnez **Gérer les types de contenu JSON**.

Dans le panneau **Configurer le type de contenu JSON du Web App Firewall**, ajoutez, modifiez ou supprimez des types de contenu JSON pour répondre aux besoins de vos applications.

Configuration de la protection des signatures pour détecter les attaques dans la charge utile JSON

En plus d'un type de contenu JSON valide, vous devez configurer les signatures pour spécifier le ou les modèles qui, lorsqu'ils sont détectés dans une requête JSON, indiquent une violation de sécurité. Les actions spécifiées, telles que bloc et journal, sont effectuées lorsqu'une demande entrante déclenche une correspondance pour tous les modèles cibles dans la règle de signature.

Pour ajouter une règle de signature personnalisée, Citrix vous recommande d'utiliser l'interface graphique. Accédez à **Système** > **Sécurité** > **Web App Firewall** > **Signatures**. Double-cliquez sur l'objet de signature cible pour accéder au panneau **Modifier les signatures du Web App Firewall**. Cliquez sur le bouton **Ajouter** pour configurer les actions, la catégorie, la chaîne de journal, les modèles de règles, etc. Bien que le Web App Firewall inspecte toutes les charges utiles de type de contenu autorisées pour la correspondance de signature, vous pouvez optimiser le traitement en spécifiant l'expression JSON dans la règle. Lorsque vous **ajoutez** un nouveau modèle de règle, sélectionnez **Expression** dans les options de liste déroulante pour **Match** et fournissez l'expression de correspondance cible à partir de votre charge utile JSON pour identifier les requêtes spécifiques qui doivent être inspectées. Une expression doit commencer par un **TEXT.** préfixe. Vous pouvez ajouter d'autres modèles de règles pour spécifier des modèles de correspondance supplémentaires afin d'identifier l'attaque.

L'exemple suivant montre une règle de signature. Si une balise de script inter-site est détectée dans le corps POST de la charge utile JSON correspondant à l'expression XPATH_JSON spécifiée, une correspondance de signature est déclenchée.

Exemple de signature pour détecter des scripts inter-sites dans la charge utile JSON

```
<SignatureRule actions="log,stats" category="JSON" enabled="ON" id="
    1000001" severity="" source="" type="" version="1">

  <PatternList>

    <RequestPatterns>

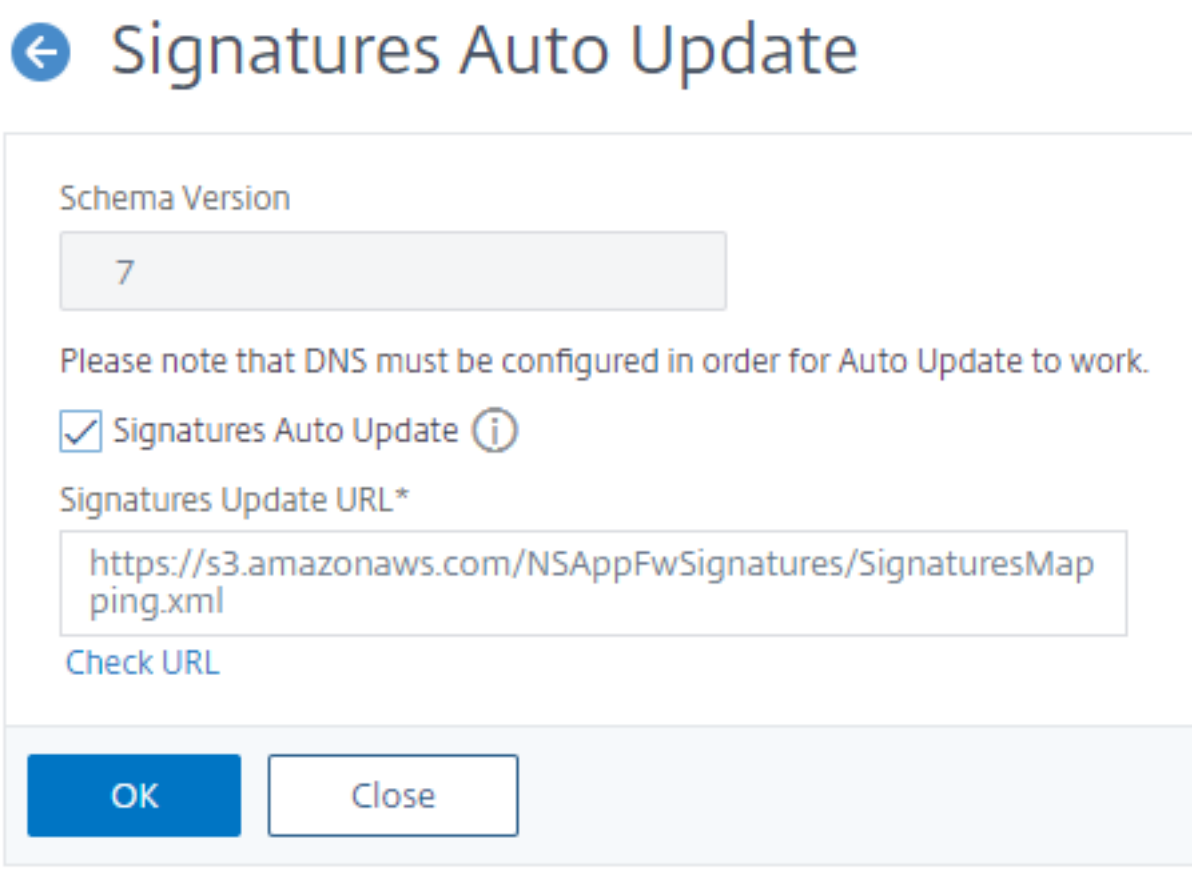
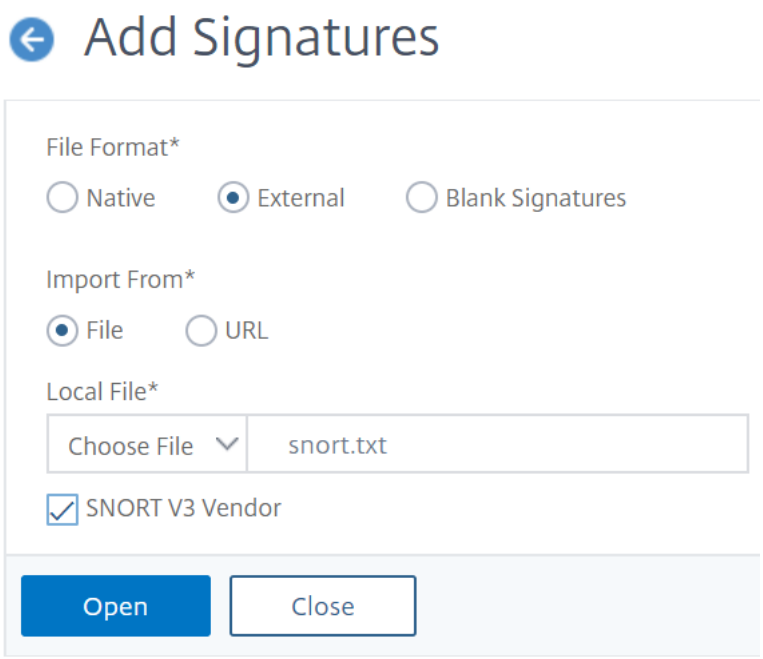
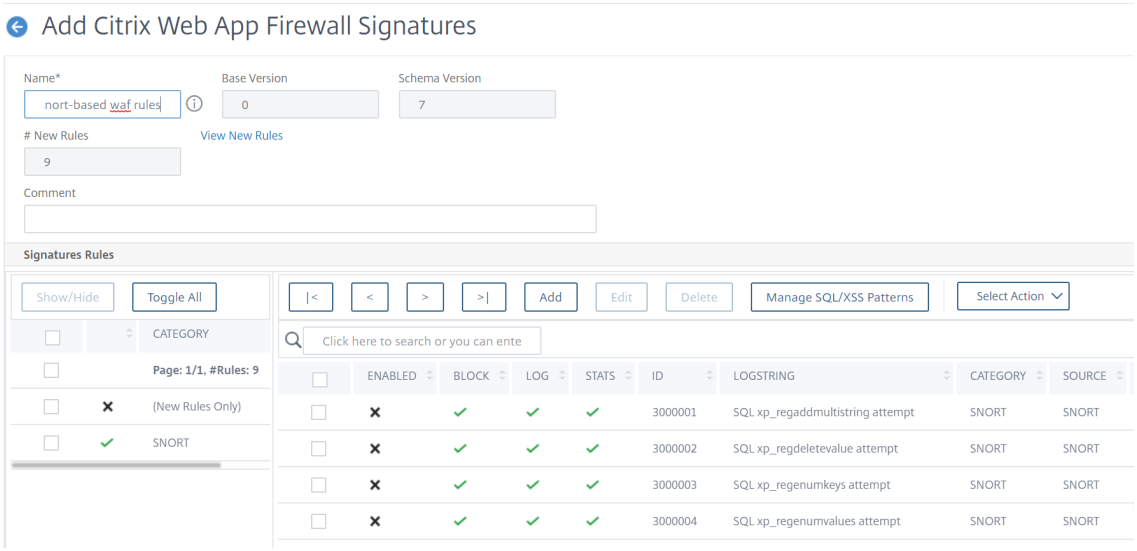
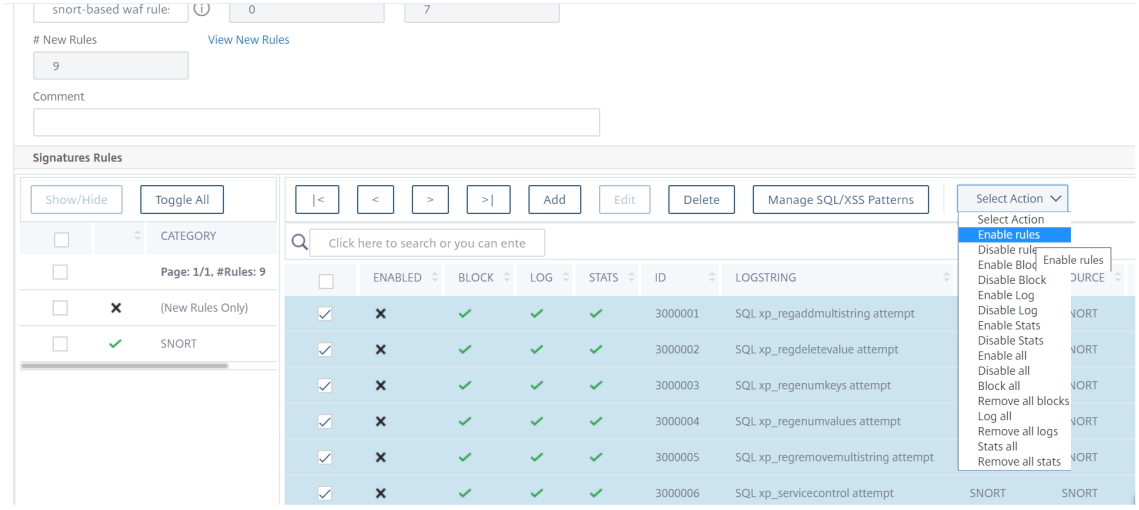
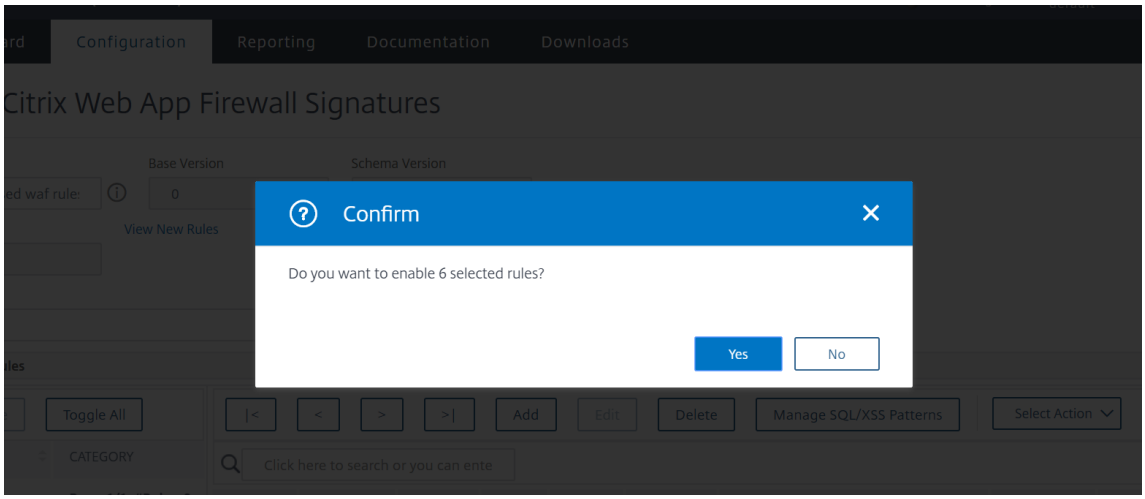
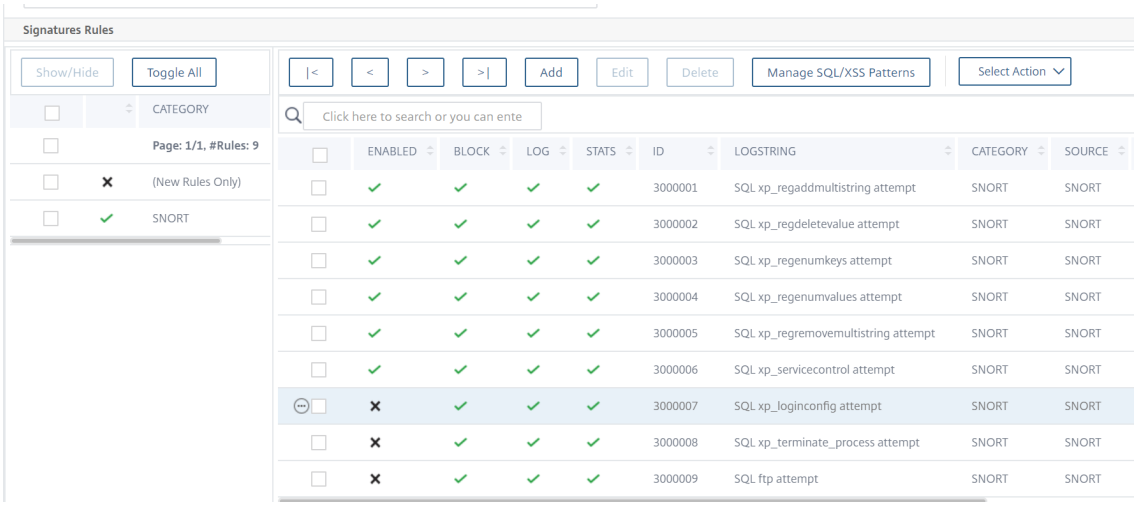
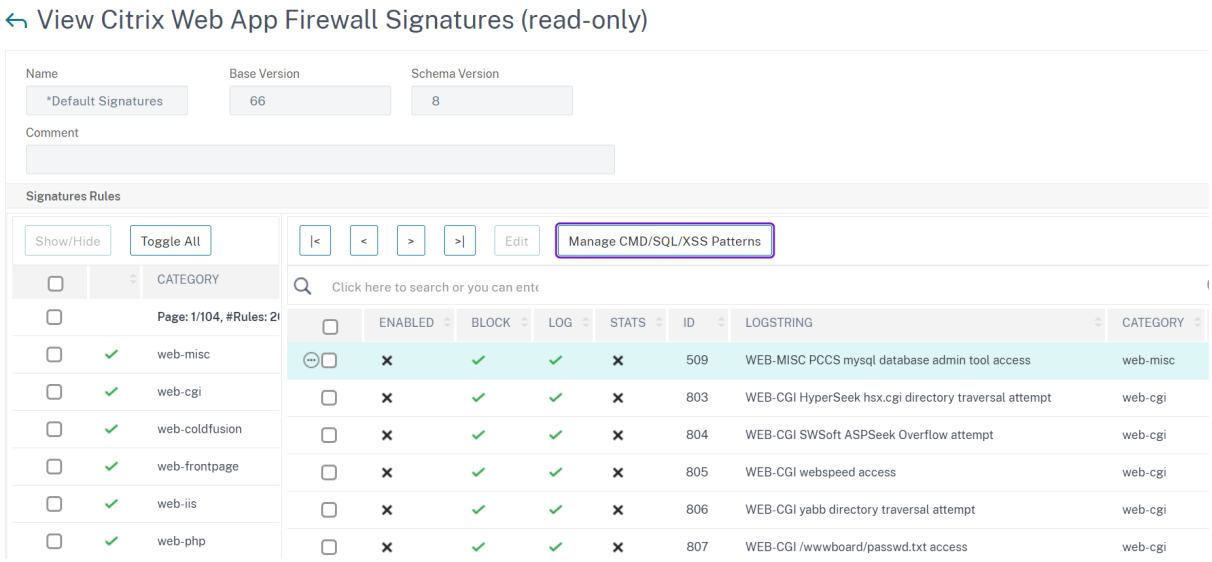
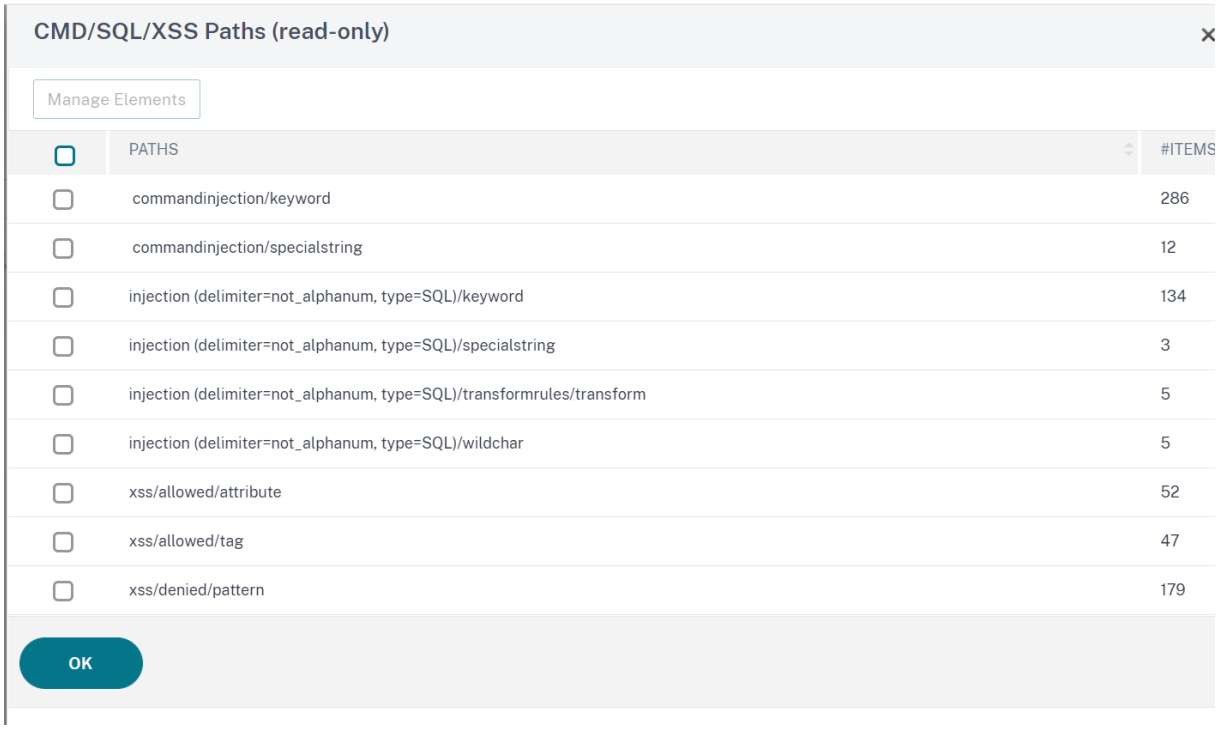
      <Pattern>

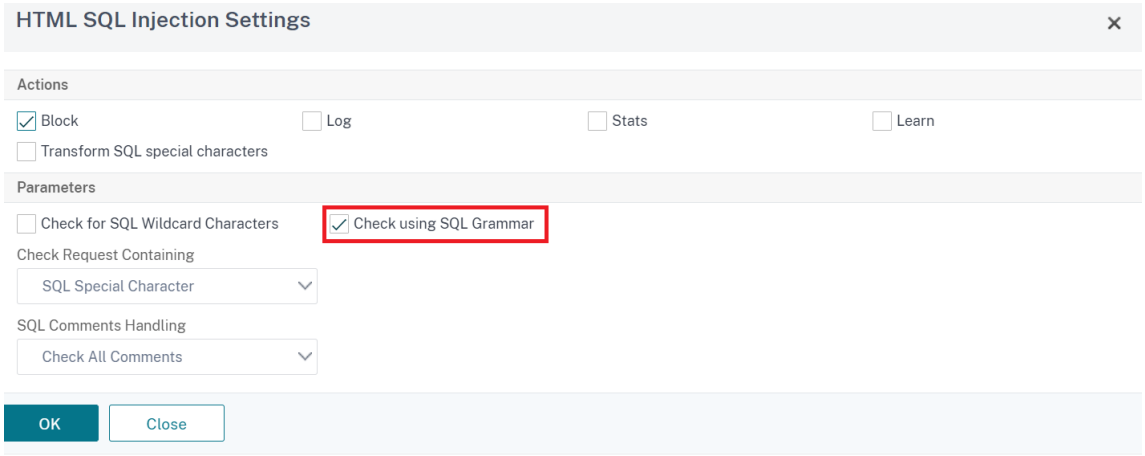
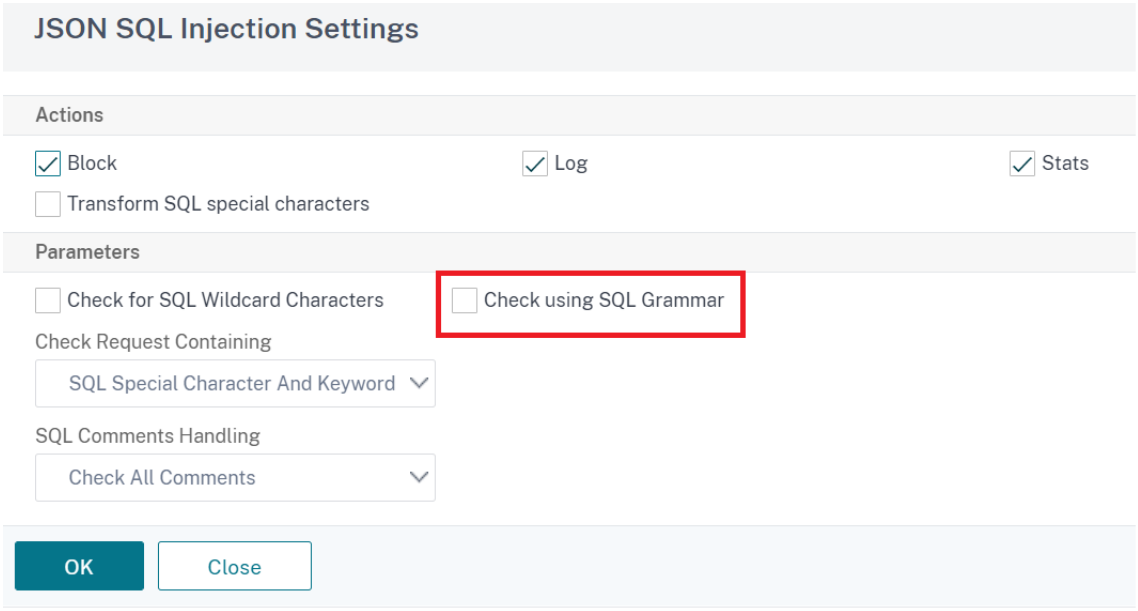
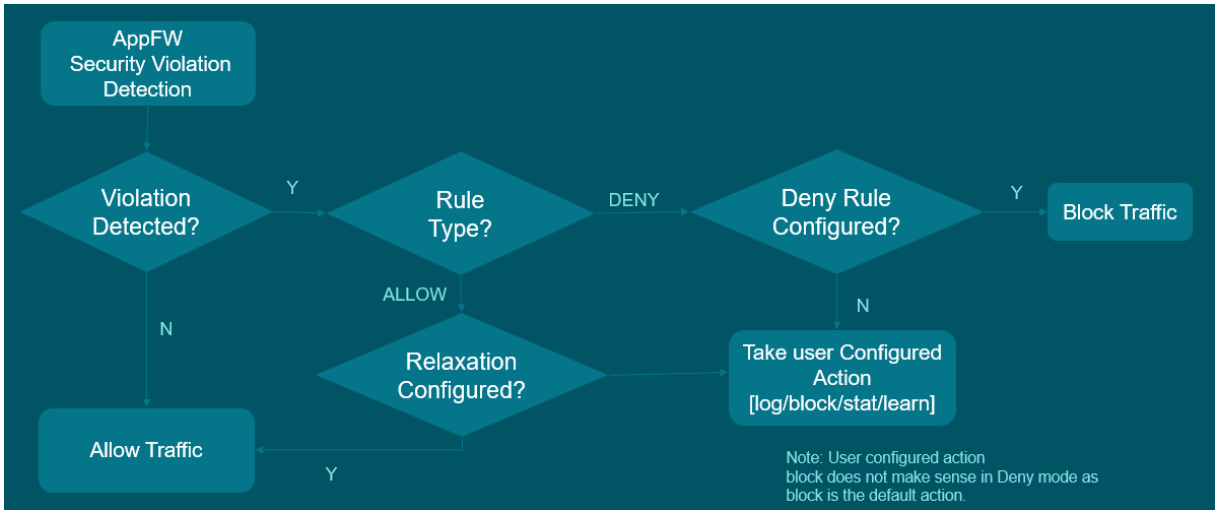
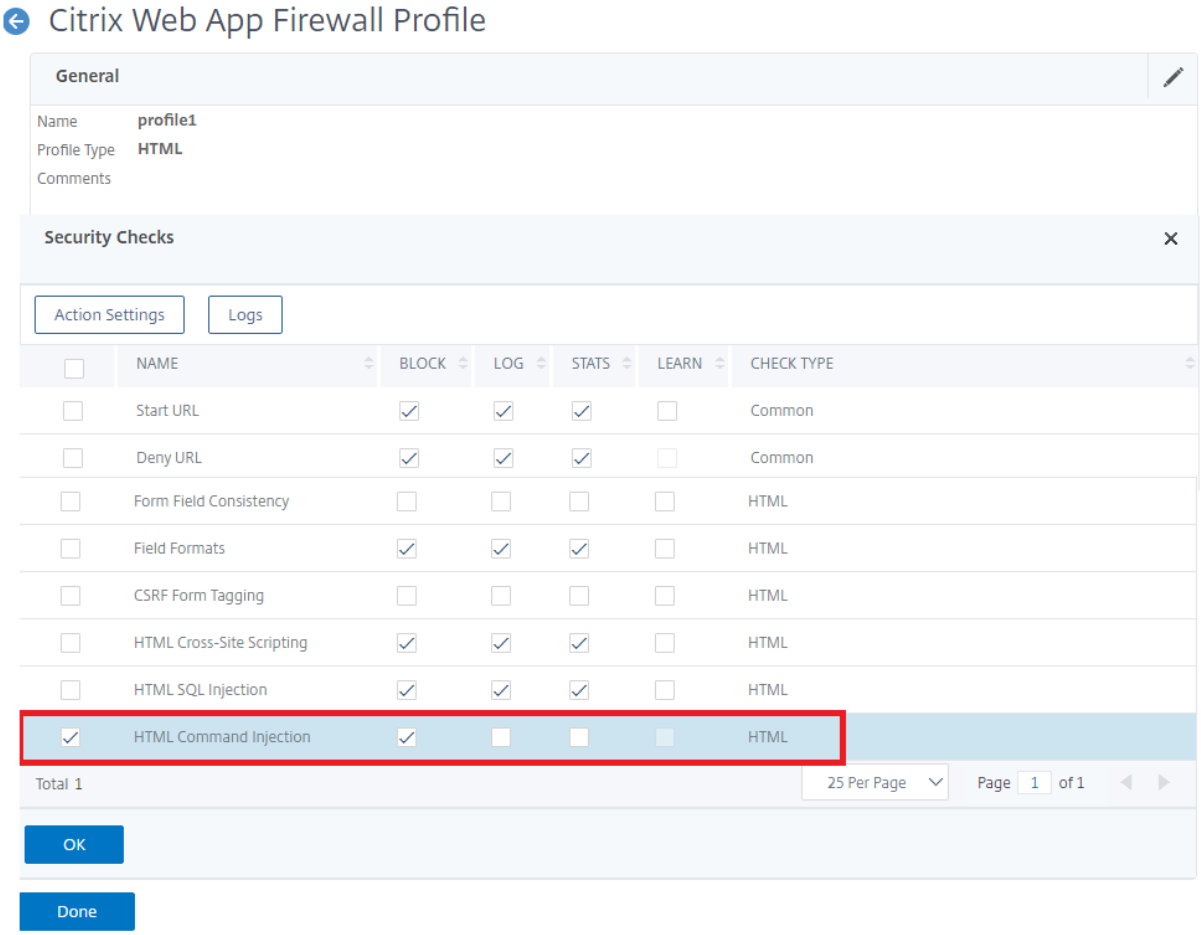
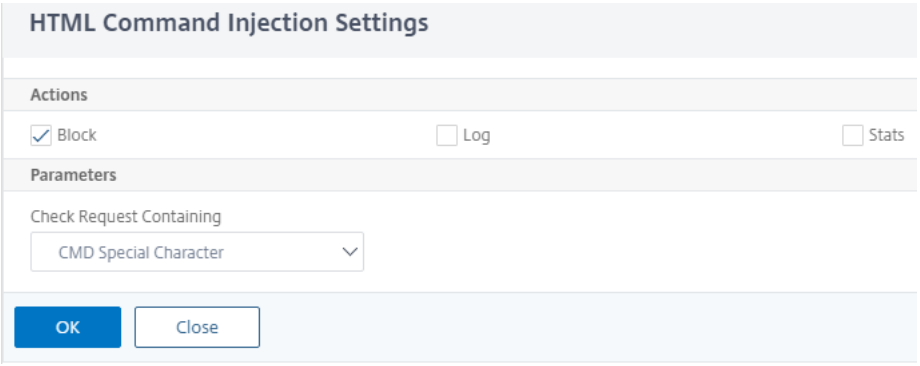
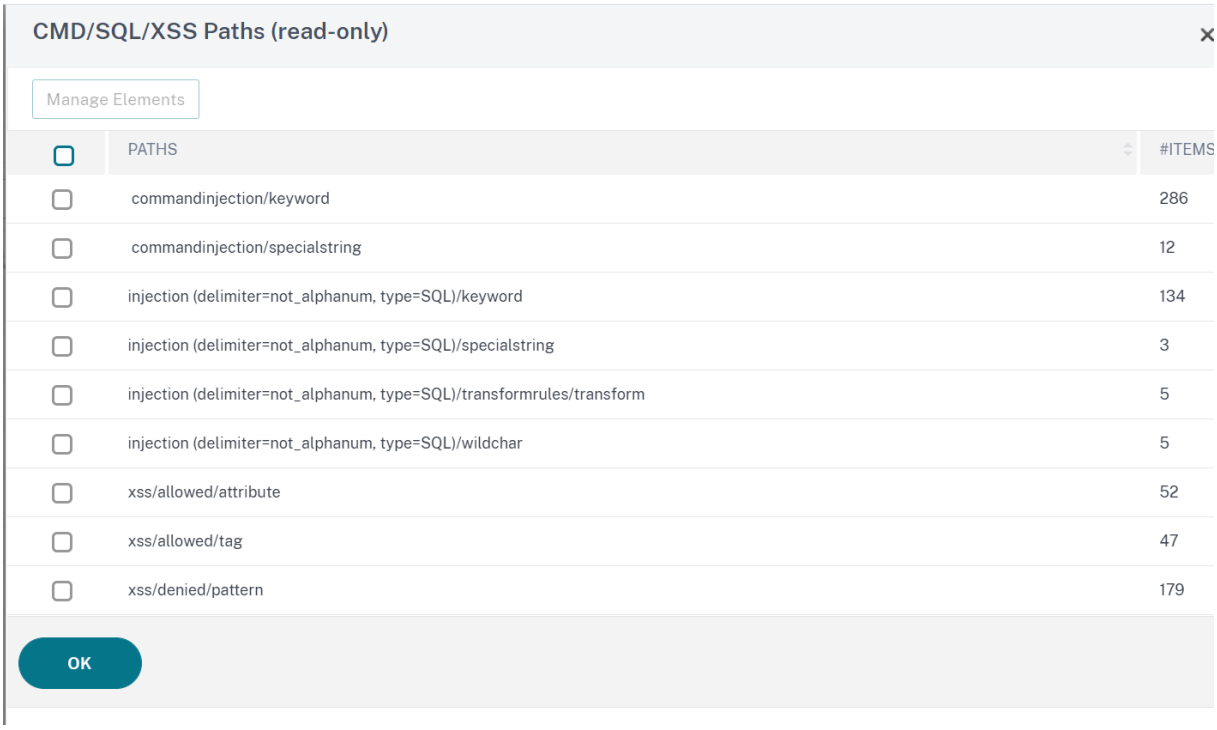
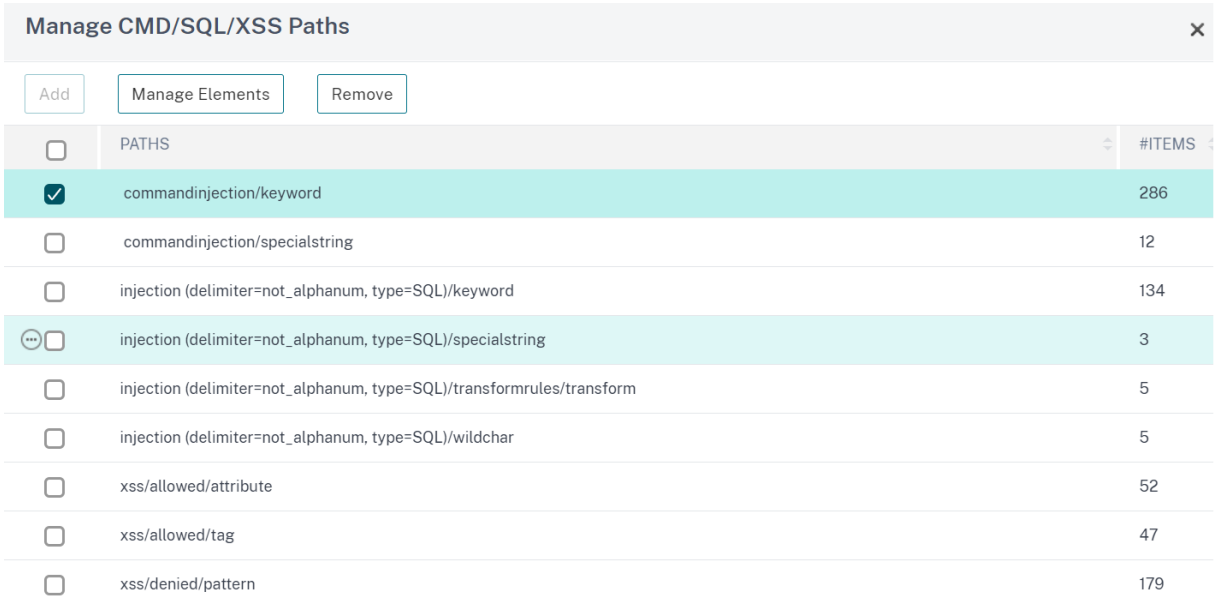
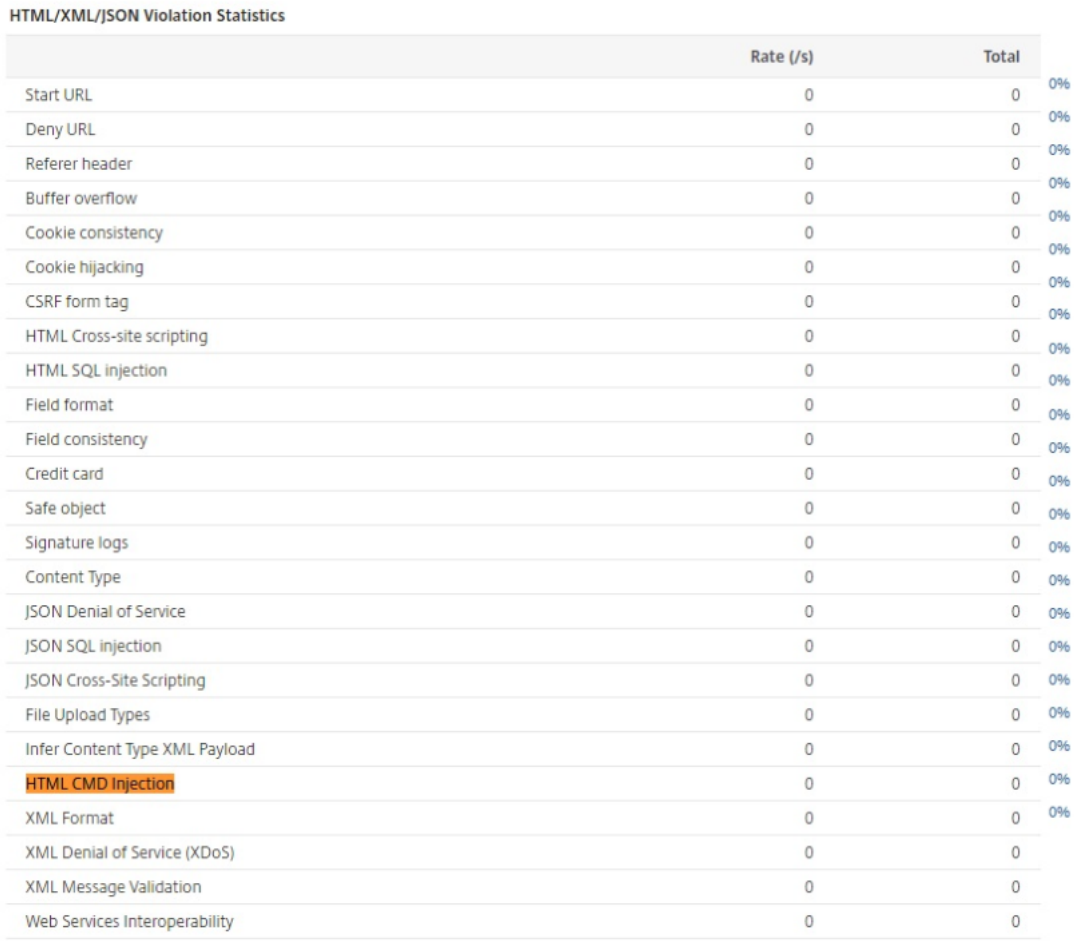
        <Location area="HTTP_POST_BODY"/>

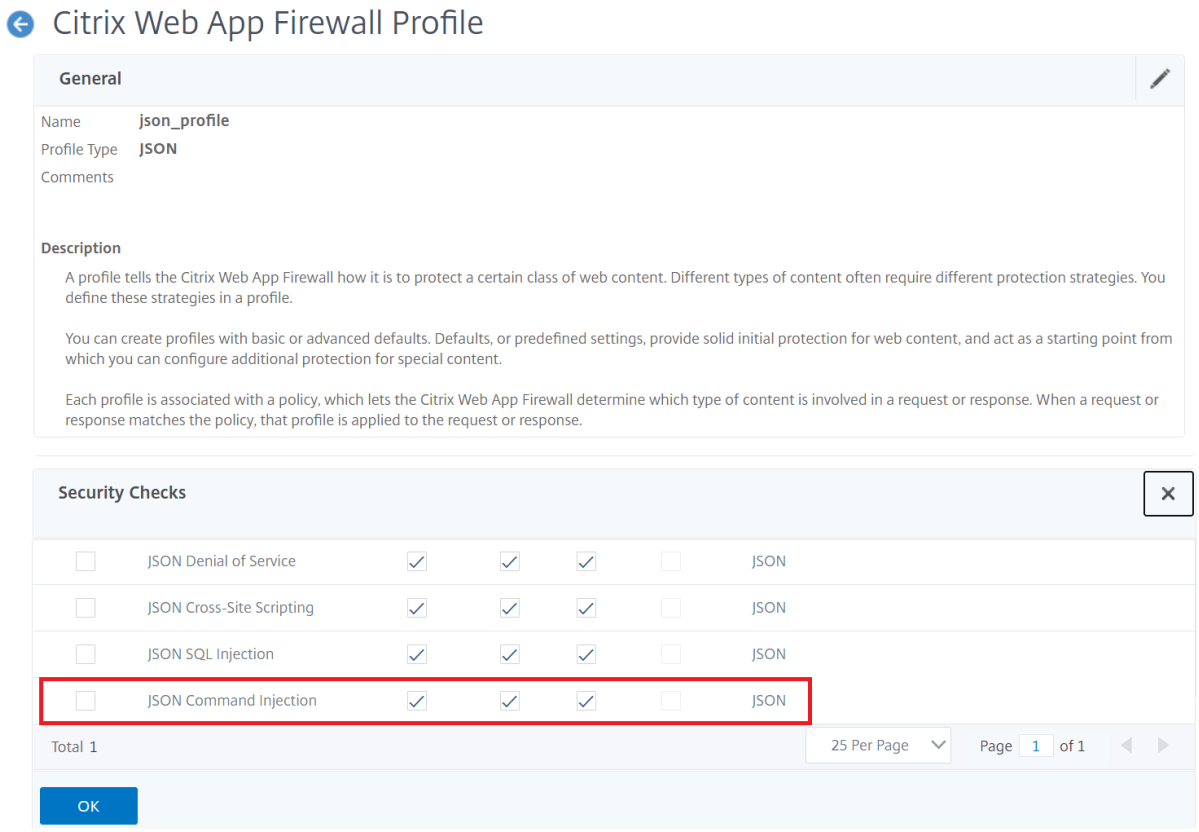
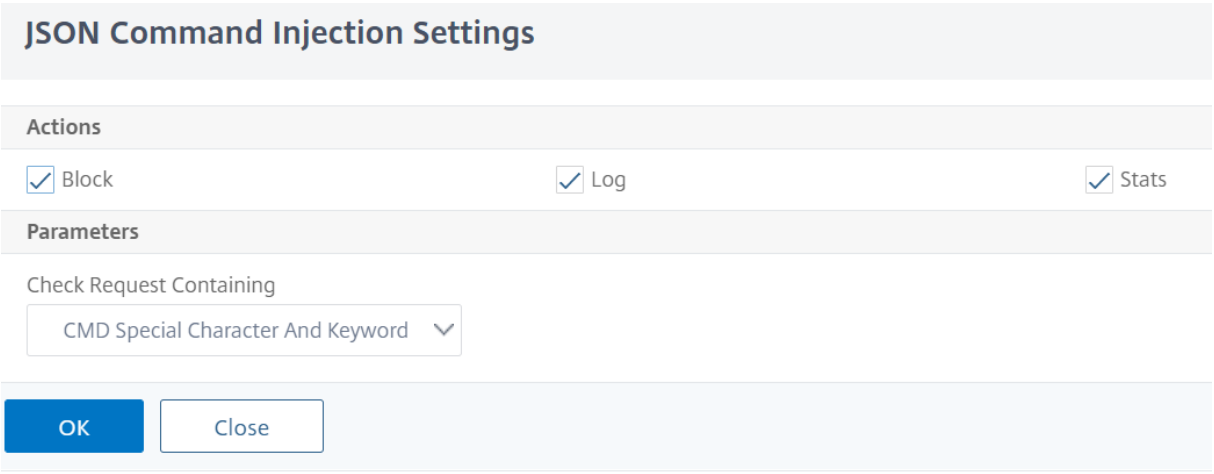
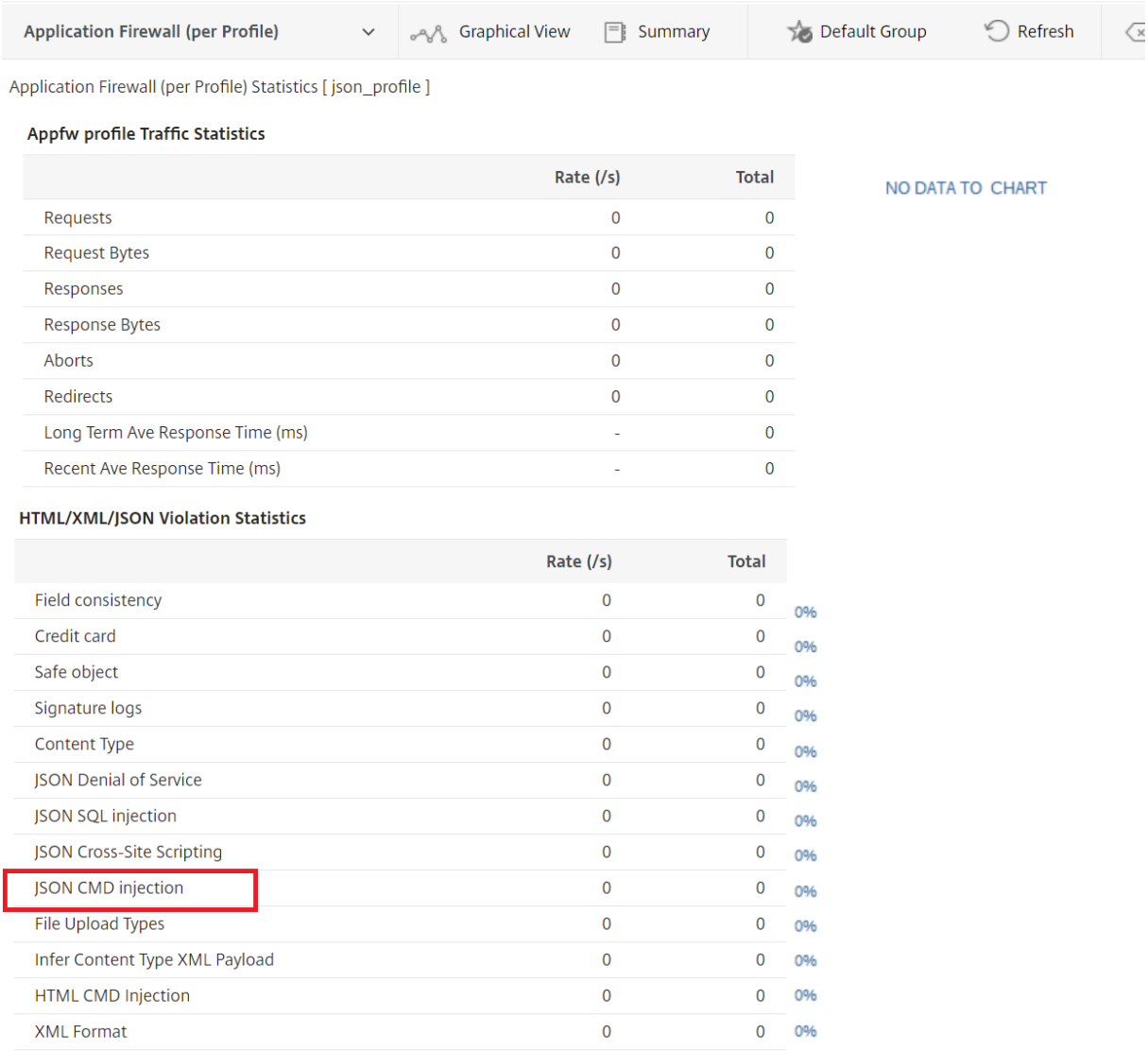
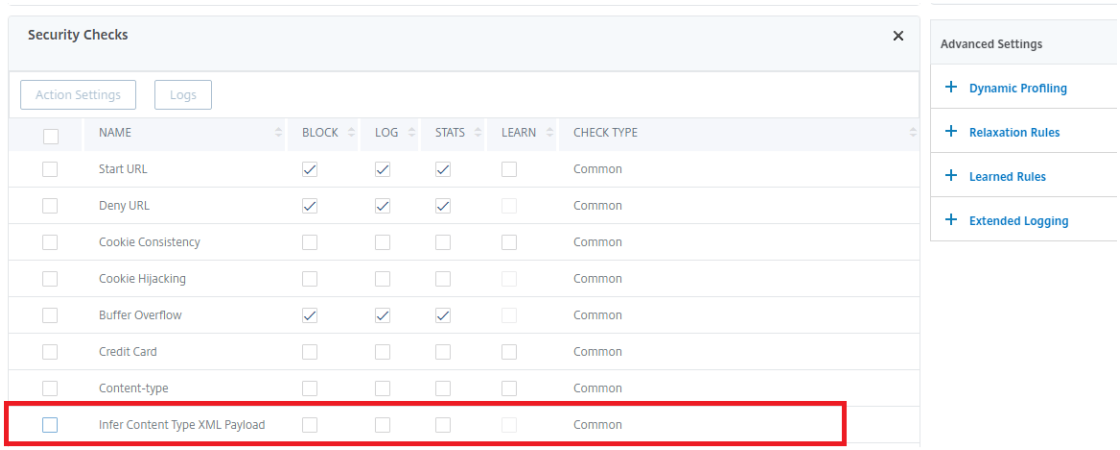
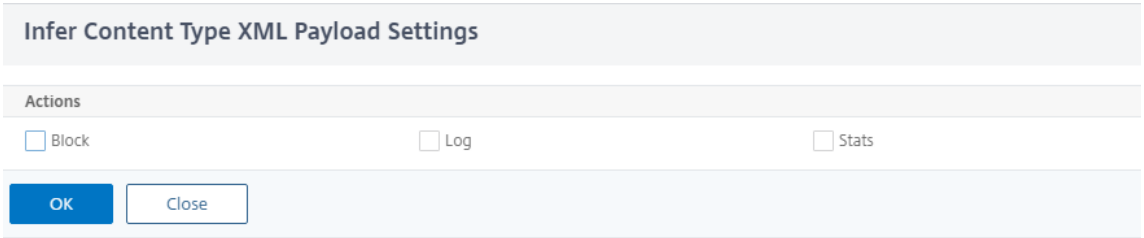
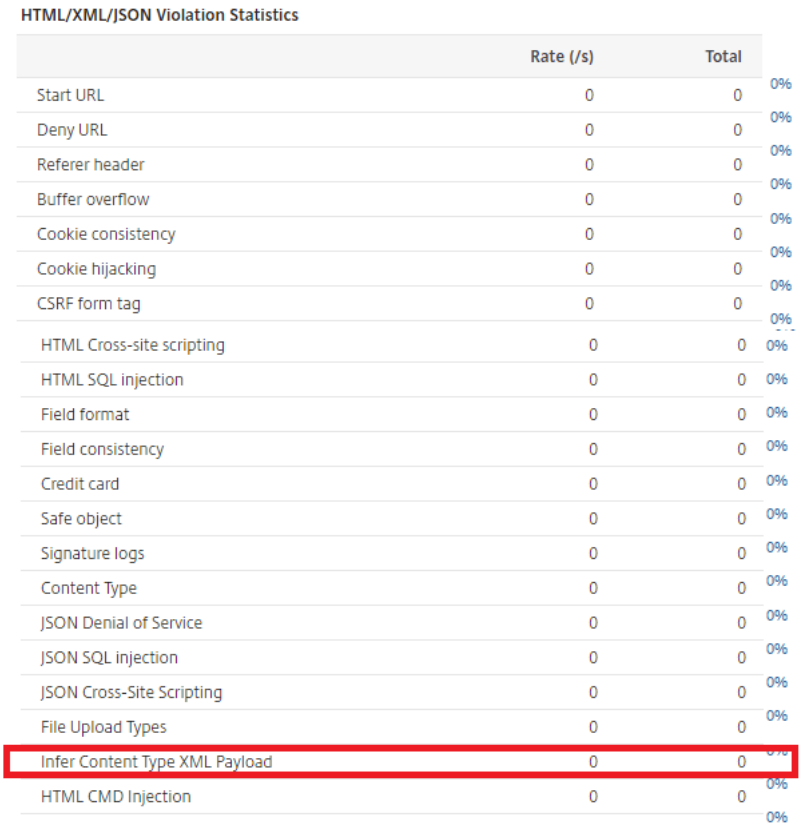
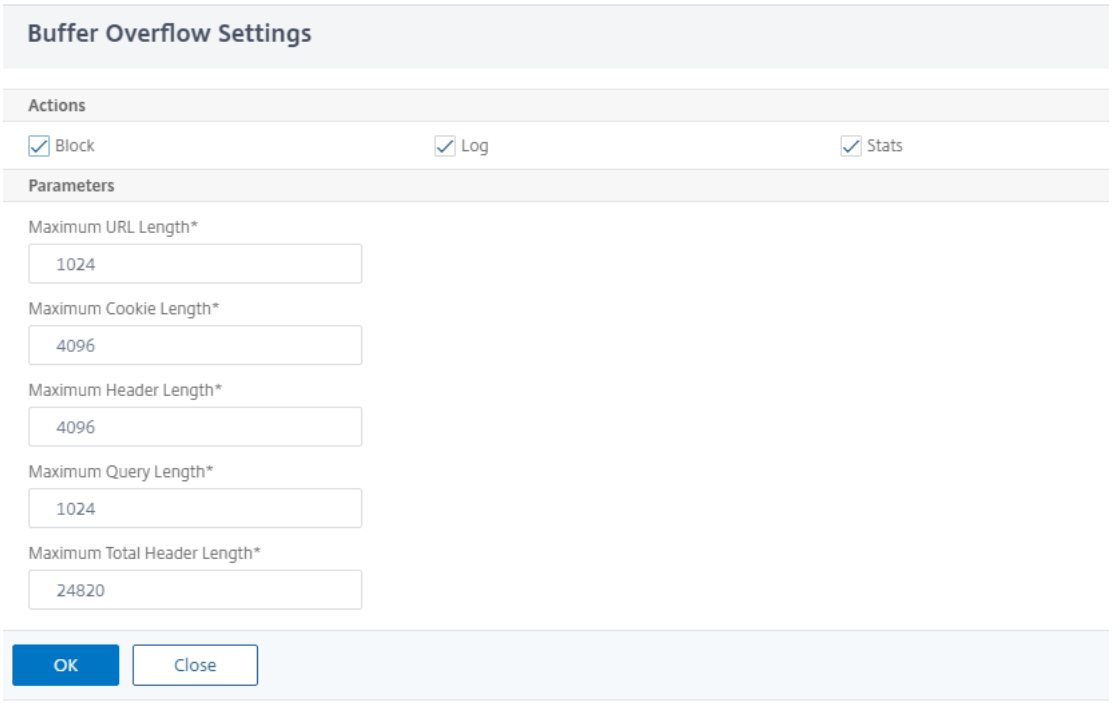
        <Match type="Expression">TEXT.XPATH_JSON(xp%/glossary/title%).
            CONTAINS("example glossary")</Match>

      </Pattern>

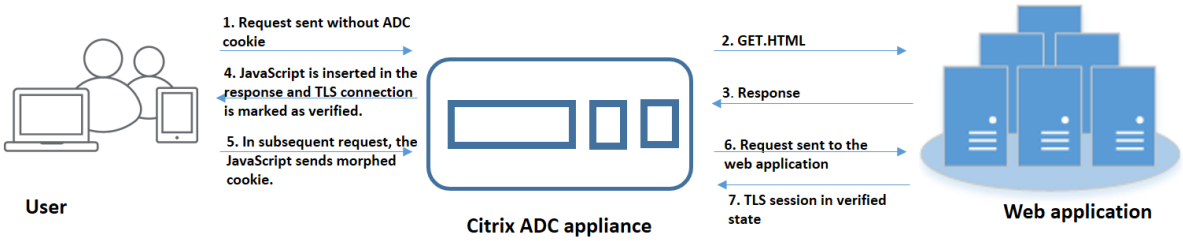
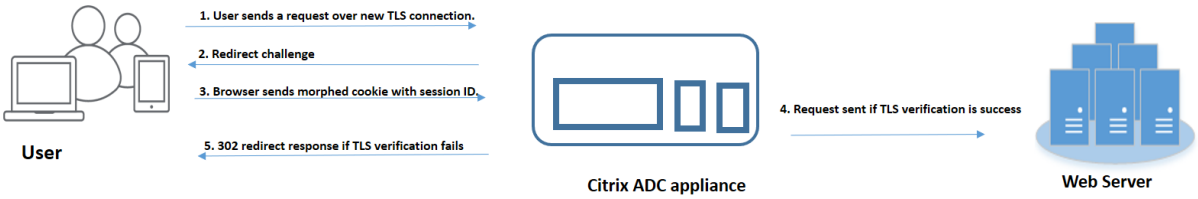
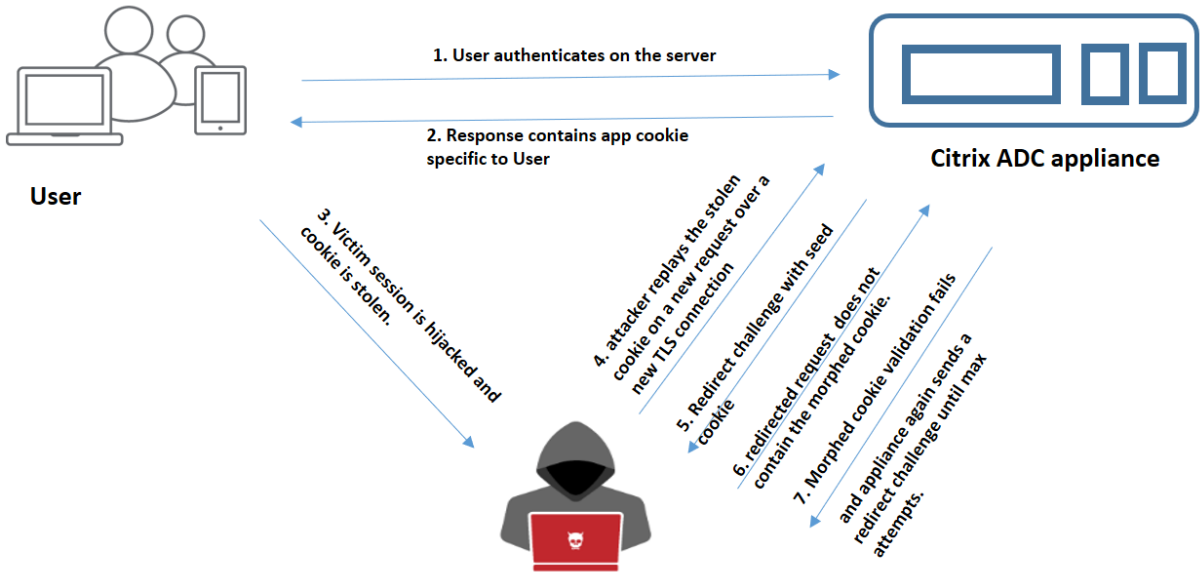
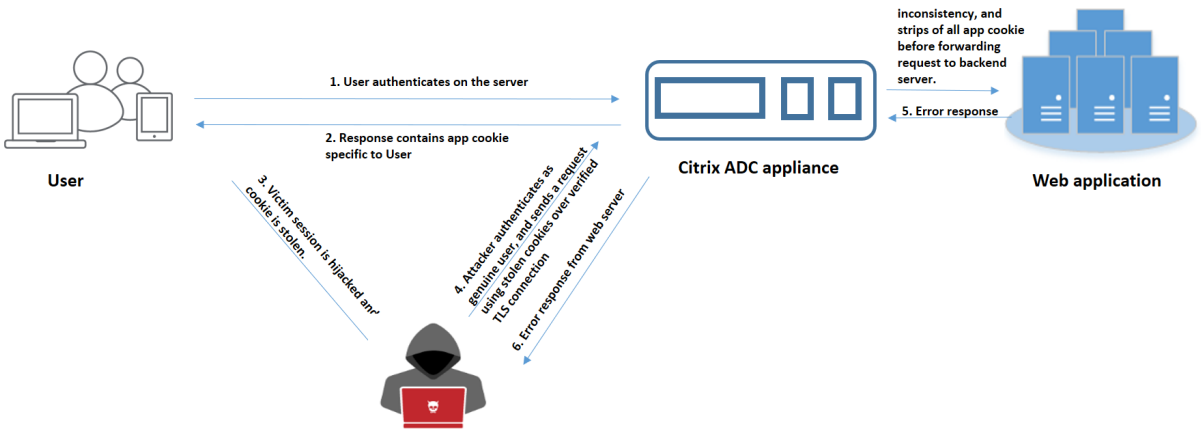
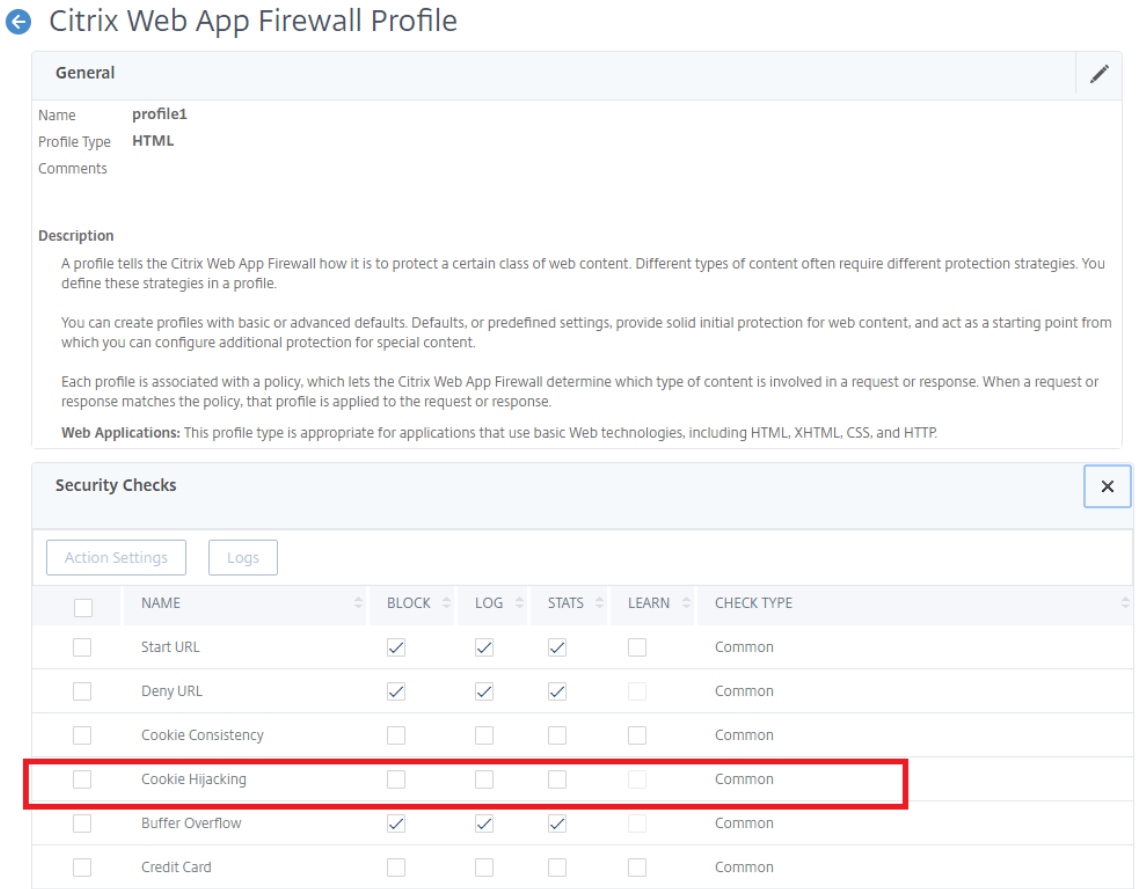
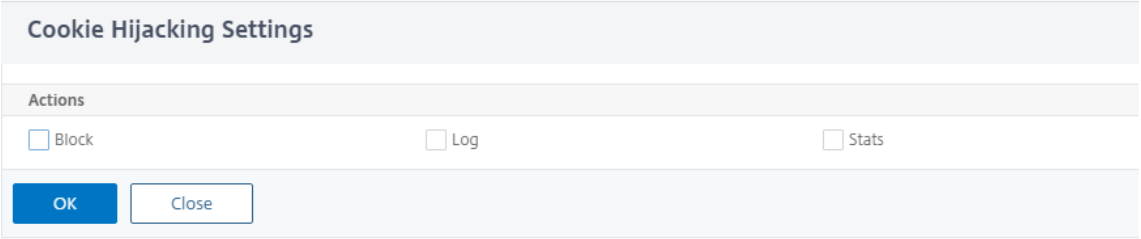
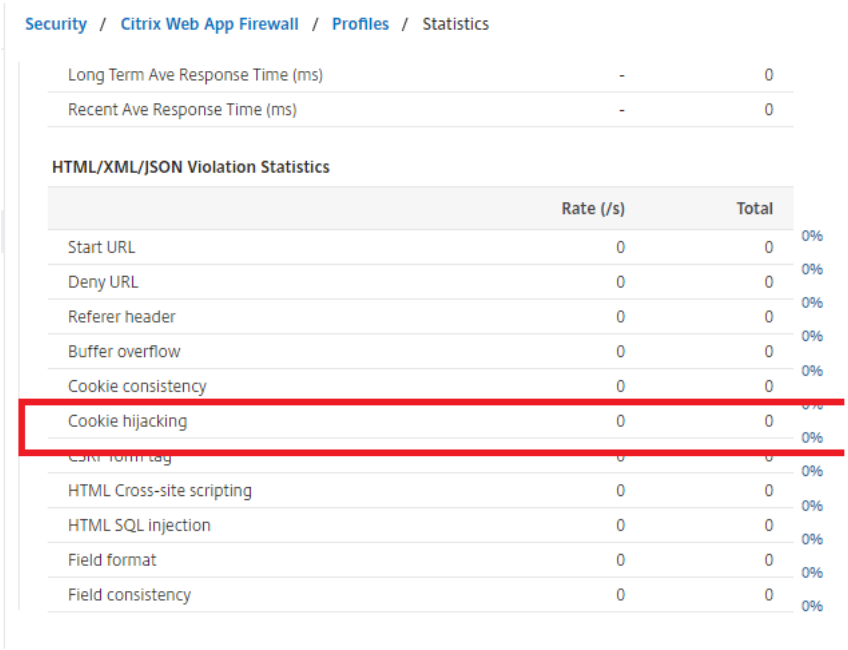
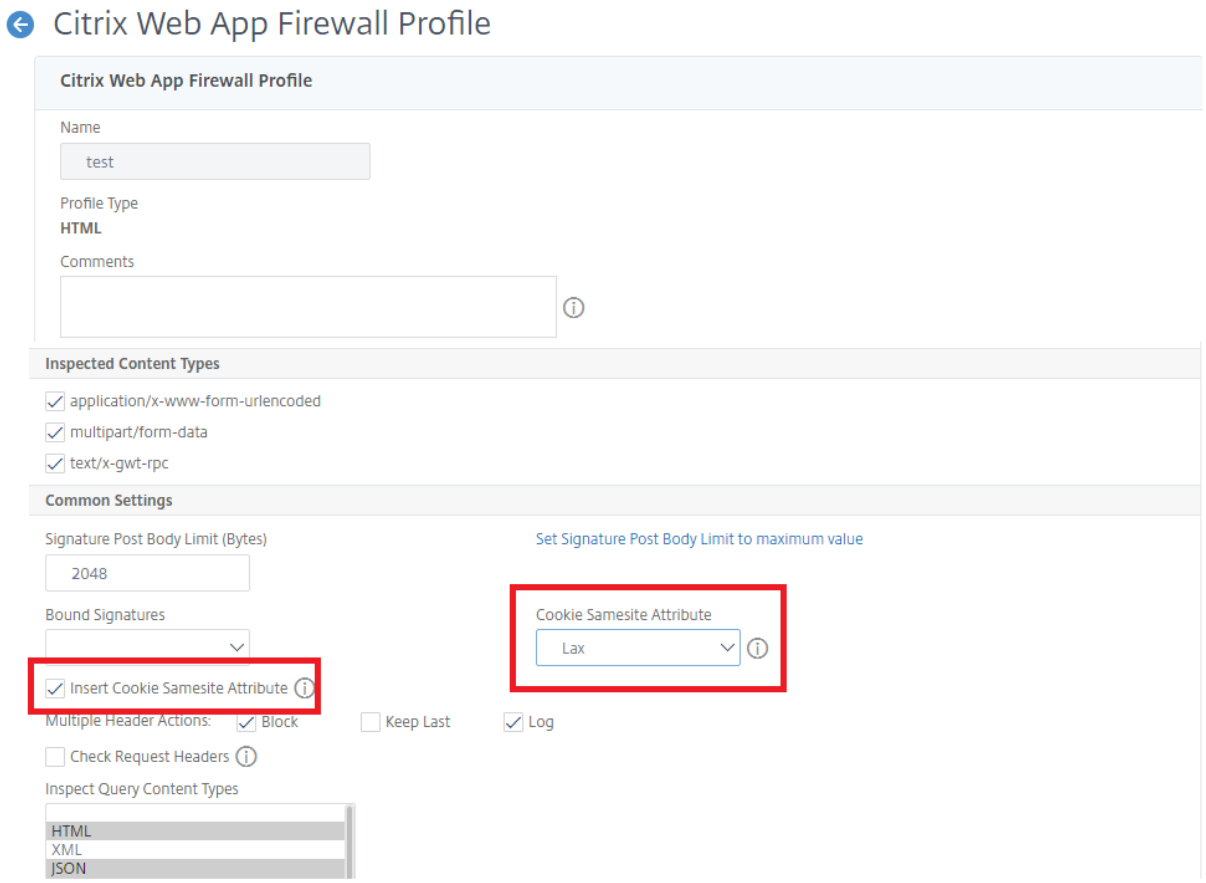
```



```
15        <Pattern>
16
17          <Location area="HTTP_METHOD"/>
18
19          <Match type="LITERAL">POST</Match>
20
21        </Pattern>
22
23        <Pattern>
24
25          <Location area="HTTP_POST_BODY"/>
26
27          <Match type="CrossSiteScripting"/>
28
29         </Pattern>
30
31      </RequestPatterns>
32
33    </PatternList>
34
35    <LogString>Cross-site scripting violation detected in json payload</
         LogString>
36
37    <Comment/>
38
39 </SignatureRule>
40 <!--NeedCopy-->
```

Exemple de la charge utile

La charge utile suivante déclenche la correspondance de signature, car elle inclut la balise de script cross-site **<Gotcha!! >**.

```
1 {
2  "glossary": {
3  "title": "example glossary","GlossDiv": {
4  "title": "S","GlossList": {
5  "GlossEntry": {
6  "ID": "SGML","SortAs": "SGML","GlossTerm": "Standard Generalized
      Markup Language","Acronym": "SGML","Abbrev": "ISO 8879:1986","
      GlossDef": {
7  "para": "A meta-markup language, used to create markup languages \*\*<
      Gotcha!!>\*\* such as DocBook.","GlossSeeAlso": ["GML", "XML"] }
8  ,"GlossSee": "markup" }
```



```
9    }
10   }
11   }
12   }
13
14 <!--NeedCopy-->
```

Exemple de message de journal

```
1 Aug 21 12:21:42 <local0.info> 10.217.31.239 08/21/2015:23:21:42 GMT ns
     0-PPE-1 : APPFW APPFW_SIGNATURE_MATCH 1471 0 :  10.217.253.62 990-
     PPE0 NtJnVMNnvPeQJnaUzXYW/GTvAQsA010 prof1 http://10.217.31.212/FFC/
     login_post.php Signature violation rule ID 1000001: cross-site
     scripting violation detected in json payload  <not blocked>
2 <!--NeedCopy-->
```

> **Remarque**
>
> Si vous envoyez la même charge utile après avoir supprimé la balise de script inter-site (**<Gotcha!!>**), la correspondance de règle de signature n'est pas déclenchée.

Résumé

- Pour protéger la charge utile JSON, utilisez les signatures du Web App Firewall pour détecter les scripts intersites, SQL et autres violations.
- Vérifiez que le type de contenu JSON est configuré sur l'appliance en tant que type de contenu autorisé.
- Assurez-vous que le type de contenu dans la charge utile correspond au type de contenu JSON configuré.
- Assurez-vous que tous les modèles configurés dans la règle de signature correspondent à la violation de signature à déclencher.
- Lorsque vous ajoutez une règle de signature, elle DOIT avoir au moins un modèle de règle pour correspondre à l'expression dans la charge utile JSON. Toutes les expressions PI dans les règles de signature doivent commencer par le préfixe TEXT. et doivent être booléens.

Protégez l'application ou le type de contenu JSON avec SQL et la charge utile codée par script inter-site à l'aide de stratégies et de signatures

Citrix Web App Firewall peut protéger l'application ou le type de contenu JSON à l'aide de stratégies et de signatures.

Inspecter l'application ou le type de contenu JSON pour une injection SQL à l'aide de stratégies

Vous devez ajouter les stratégies suivantes et les lier au serveur virtuel globalement pour prendre en charge l'injection SQL.

```
add appfw policy sqli_1 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_])))(select|insert|delete|update|drop|create|alter|grant
|revoke|commit|rollback|shutdown|union|intersect|minus|case|decode|where
|group|begin|join|exists|distinct|add|modify|constraint|null|like|exec|
execute|char|or|and|sp_sdidebug)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK
```

```
add appfw policy sqli_2 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_])))(xp_availablemedia|xp_cmdshell|xp_deletemail|xp_dirtree
|xp_dropwebtask|xp_dsninfo|xp_enumdsn|xp_enumerrorlogs|xp_enumgroups|
xp_enumqueuedtasks|xp_eventlog|xp_findnextmsg|xp_fixeddrives|xp_getfiledetails
|xp_getnetname|xp_grantlogin|xp_logevent|xp_loginconfig|xp_logininfo|
xp_makewebtask|xp_msver|xp_regread|xp_perfend|xp_perfmonitor|xp_perfsample
|xp_perfstart|xp_readerrorlog|xp_readmail|xp_revokelogin|xp_runwebtask|
xp_schedulersignal|xp_sendmail|xp_servicecontrol|xp_snmp_getstate|xp_snmp_raisetrap
|xp_sprintf|xp_sqlinventory|xp_sqlregister|xp_sqltrace|xp_sscanf|xp_startmail
|xp_stopmail|xp_subdirs|xp_unc_to_drive)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK
```

```
add appfw policy sqli_3 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_])))(sysobjects|syscolumns|MSysACEs|MSysObjects|MSysQueries
|MSysRelationships)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK
```

```
add appfw policy sqli_4 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A
)|(?<=[^a-zA-Z0-9_])))(SYS\.USER_OBJECTS|SYS\.TAB|SYS\.USER_TABLES|SYS\.
USER_VIEWS|SYS\.ALL_TABLES|SYS\.USER_TAB_COLUMNS|SYS\.USER_CONSTRAINTS|SYS
\.USER_TRIGGERS|SYS\.USER_CATALOG|SYS\.ALL_CATALOG|SYS\.ALL_CONSTRAINTS|SYS
\.ALL_OBJECTS|SYS\.ALL_TAB_COLUMNS|SYS\.ALL_TAB_PRIVS|SYS\.ALL_TRIGGERS|SYS
\.ALL_USERS|SYS\.ALL_VIEWS|SYS\.USER_ROLE_PRIVS|SYS\.USER_SYS_PRIVS|SYS\.
USER_TAB_PRIVS)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK
```

Inspecter l'application ou le type de contenu JSON à l'aide de signatures

Vous pouvez ajouter les règles de signature suivantes à l'objet signature dans le profil de pare-feu de l'application pour prendre en charge l'injection SQL pour le type de contenu JSON.

> **Remarque :**
>
> Les signatures postérieures sont gourmandes en CPU.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2013-2018 Citrix Systems, Inc. All rights reserved. -->
<SignaturesFile schema_version="6" version="0" minor_schema_version="0"
    >
     <Signatures>
         <SignatureRule id="4000000" enabled="ON" actions="log,block"
            category="sql" source="" severity="" type="" version="1"
            sourceid="" harmscore="">
             <PatternList>
                 <RequestPatterns>
                     <Pattern>
                         <Location area="HTTP_POST_BODY"/>
                         <Match type="Expression">TEXT.SET_TEXT_MODE(
                            IGNORECASE).SET_TEXT_MODE(URLENCODED).
                            DECODE_USING_TEXT_MODE.REGEX_MATCH(re#(((\A)
                            |(?<=[^a-zA-Z0-9_])))(select|insert|delete|
                            update|drop|create|alter|grant|revoke|commit
                            |rollback|shutdown|union|intersect|minus|
                            case|decode|where|group|begin|join|exists|
                            distinct|add|modify|constraint|null|like|
                            exec|execute|char|or|and|sp_sdidebug)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                     </Pattern>
                     <Pattern type="fastmatch">
                         <Location area="HTTP_METHOD"/>
                         <Match type="LITERAL">T</Match>
                     </Pattern>
                 </RequestPatterns>
             </PatternList>
             <LogString>sql Injection</LogString>
             <Comment/>
         </SignatureRule>
         <SignatureRule id="4000001" enabled="ON" actions="log,block"
            category="sql" source="" severity="" type="" version="1"
            sourceid="" harmscore="">
             <PatternList>
                 <RequestPatterns>
                     <Pattern>
                         <Location area="HTTP_POST_BODY"/>
                         <Match type="Expression">TEXT.SET_TEXT_MODE(
                            IGNORECASE).SET_TEXT_MODE(URLENCODED).
```



```
                                DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                                |(?<=[^a-zA-Z0-9_]))(xp_availablemedia|
                                xp_cmdshell|xp_deletemail|xp_dirtree|
                                xp_dropwebtask|xp_dsninfo|xp_enumdsn|
                                xp_enumerrorlogs|xp_enumgroups|
                                xp_enumqueuedtasks|xp_eventlog|
                                xp_findnextmsg|xp_fixeddrives|
                                xp_getfiledetails|xp_getnetname|
                                xp_grantlogin|xp_logevent|xp_loginconfig|
                                xp_logininfo|xp_makewebtask|xp_msver|
                                xp_regread|xp_perfend|xp_perfmonitor|
                                xp_perfsample|xp_perfstart|xp_readerrorlog|
                                xp_readmail|xp_revokelogin|xp_runwebtask|
                                xp_schedulersignal|xp_sendmail|
                                xp_servicecontrol|xp_snmp_getstate|
                                xp_snmp_raisetrap|xp_sprintf|xp_sqlinventory
                                |xp_sqlregister|xp_sqltrace|xp_sscanf|
                                xp_startmail|xp_stopmail|xp_subdirs|
                                xp_unc_to_drive)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                        </Pattern>
                        <Pattern type="fastmatch">
                            <Location area="HTTP_METHOD"/>
                            <Match type="LITERAL">T</Match>
                        </Pattern>
                    </RequestPatterns>
                </PatternList>
                <LogString>sql Injection</LogString>
                <Comment/>
            </SignatureRule>
            <SignatureRule id="4000002" enabled="ON" actions="log,block"
               category="sql" source="" severity="" type="" version="1"
               sourceid="" harmscore="">
                <PatternList>
                    <RequestPatterns>
                        <Pattern>
                            <Location area="HTTP_POST_BODY"/>
                            <Match type="Expression">TEXT.SET_TEXT_MODE(
                               IGNORECASE).SET_TEXT_MODE(URLENCODED).
                               DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                               |(?<=[^a-zA-Z0-9_]))(sysobjects|syscolumns|
                               MSysACEs|MSysObjects|MSysQueries|
                               MSysRelationships)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                        </Pattern>
```



```
                    <Pattern type="fastmatch">
                        <Location area="HTTP_METHOD"/>
                        <Match type="LITERAL">T</Match>
                    </Pattern>
                </RequestPatterns>
            </PatternList>
            <LogString>sql Injection</LogString>
            <Comment/>
        </SignatureRule>
        <SignatureRule id="4000003" enabled="ON" actions="log,block"
           category="sql" source="" severity="" type="" version="1"
           sourceid="" harmscore="">
            <PatternList>
                <RequestPatterns>
                    <Pattern>
                        <Location area="HTTP_POST_BODY"/>
                        <Match type="Expression">TEXT.SET_TEXT_MODE(
                           IGNORECASE).SET_TEXT_MODE(URLENCODED).
                           DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                           |(?<=[^a-zA-Z0-9_]))(SYS.USER_OBJECTS|SYS.
                           TAB|SYS.USER_TABLES|SYS.USER_VIEWS|SYS.
                           ALL_TABLES|SYS.USER_TAB_COLUMNS|SYS.
                           USER_CONSTRAINTS|SYS.USER_TRIGGERS|SYS.
                           USER_CATALOG|SYS.ALL_CATALOG|SYS.
                           ALL_CONSTRAINTS|SYS.ALL_OBJECTS|SYS.
                           ALL_TAB_COLUMNS|SYS.ALL_TAB_PRIVS|SYS.
                           ALL_TRIGGERS|SYS.ALL_USERS|SYS.ALL_VIEWS|SYS
                           .USER_ROLE_PRIVS|SYS.USER_SYS_PRIVS|SYS.
                           USER_TAB_PRIVS)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                    </Pattern>
                    <Pattern type="fastmatch">
                        <Location area="HTTP_METHOD"/>
                        <Match type="LITERAL">T</Match>
                    </Pattern>
                </RequestPatterns>
            </PatternList>
            <LogString>sql Injection</LogString>
            <Comment/>
        </SignatureRule>
    </Signatures>
</SignaturesFile>

<!--NeedCopy-->
```


Mise à jour d'un objet de signature

August 20, 2021

Vous devez mettre à jour vos objets signatures fréquemment pour vous assurer que votre Web App Firewall offre une protection contre les menaces actuelles. Vous devez mettre à jour régulièrement les signatures de Web App Firewall par défaut et toutes les signatures que vous importez à partir d'un outil d'analyse des vulnérabilités pris en charge.

Citrix met régulièrement à jour les signatures par défaut du Web App Firewall. Vous pouvez mettre à jour les signatures par défaut manuellement ou automatiquement. Dans les deux cas, demandez à votre représentant Citrix ou revendeur Citrix l'URL pour accéder aux mises à jour. Vous pouvez activer les mises à jour automatiques des signatures de format natif Citrix dans les boîtes de dialogue « Paramètres du moteur » et « Paramètres de mise à jour automatique des signatures ».

La plupart des fabricants d'outils d'analyse des vulnérabilités mettent régulièrement à jour les outils. La plupart des sites Web changent également fréquemment. Vous devez mettre à jour votre outil et ré-analyse régulièrement vos sites Web, exporter les signatures résultantes dans un fichier et les importer dans votre configuration de Web App Firewall.

> **Conseil**
>
> Lorsque vous mettez à jour les signatures du Web App Firewall à partir de la ligne de commande Citrix ADC, vous devez d'abord mettre à jour les signatures par défaut, puis émettre d'autres commandes de mise à jour pour mettre à jour chaque fichier de signatures personnalisées basé sur les signatures par défaut. Si vous ne mettez pas d'abord à jour les signatures par défaut, une erreur d'incompatibilité de version empêche la mise à jour des fichiers de signatures personnalisés.
>
> **Remarque**
>
> Les dispositions suivantes s'appliquent à la fusion d'un objet de signature tiers avec un objet de signature défini par l'utilisateur avec des règles natives et des règles ajoutées par l'utilisateur :
>
> Lorsqu'une signature de version 0 est fusionnée avec un nouveau fichier importé, les signatures résultantes restent en tant que version 0.
>
> Cela signifie que toutes les règles natives (ou intégrées) du fichier importé seront ignorées après la fusion. Ceci permet de s'assurer que les signatures de la version 0 sont conservées telles qu'elles sont après une fusion.
>
> Pour inclure les règles natives dans le fichier importé pour la fusion, vous devez d'abord mettre à jour les signatures existantes de la version 0 avant la fusion. Cela signifie que vous devez abandonner la version 0 des signatures existantes.

> Lorsqu'il y a une mise à niveau de la version Citrix ADC, le fichier "default_signatures.xml" est ajouté à la nouvelle version et le fichier "updated_signature.xml" est supprimé de l'ancienne version. Après la mise à niveau, si la fonctionnalité de mise à jour automatique de signature est activée, l'appliance met à jour la signature existante vers la dernière version de la version et génère le fichier "updated_signature.xml".

Pour mettre à jour les signatures du Web App Firewall à partir de la source à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `update appfw signatures <name> [-mergedefault]`
- `save ns config`

Exemple

L'exemple suivant met à jour l'objet signatures nommé mySignatures à partir de l'objet signatures par défaut, en fusionnant les nouvelles signatures de l'objet signatures par défaut avec les signatures existantes. Cette commande n'écrase pas les signatures créées par l'utilisateur ou les signatures importées à partir d'une autre source, par exemple un outil d'analyse des vulnérabilités approuvé.

```
1 update appfw signatures MySignatures -mergedefault
2 save ns config
3 <!--NeedCopy-->
```

Mise à jour d'un objet signatures à partir d'un fichier au format Citrix

Citrix met régulièrement à jour les signatures du Web App Firewall. Vous devez régulièrement mettre à jour les signatures de votre Web App Firewall pour vous assurer que votre pare-feu Web App utilise la liste la plus récente. Demandez à votre représentant Citrix ou revendeur Citrix l'URL pour accéder aux mises à jour.

Pour mettre à jour un objet signatures à partir d'un fichier au format Citrix à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `update appfw signatures <name> [-mergeDefault]`
- `save ns config`

Pour mettre à jour un objet signatures à partir d'un fichier au format Citrix à l'aide de l'interface graphique graphique

1. Accédez à **Sécurité** > **Web App Firewall** > **Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures à mettre à jour.
3. Dans la liste déroulante **Action**, sélectionnez **Fusionner**.
4. Dans la boîte de dialogue **Mettre à jour l'objet des signatures**, choisissez l'une des options suivantes.
   - **Importer à partir de l'URL** : choisissez cette option si vous téléchargez des mises à jour de signature à partir d'une URL Web.
   - **Importer à partir d'un fichier local** : choisissez cette option si vous importez des mises à jour de signature à partir d'un fichier sur votre disque dur local, votre disque dur réseau ou tout autre périphérique de stockage.
5. Dans la zone de texte, tapez l'URL, ou tapez ou recherchez le fichier local.
6. Cliquez sur **Update**. Le fichier de mise à jour est importé et la boîte de dialogue Mettre à jour les signatures passe à un format presque identique à celui de la boîte de dialogue **Modifier l'objet Signatures**. La boîte de dialogue **Mettre à jour les signatures d'objet** affiche toutes les branches avec des règles de signature nouvelles ou modifiées, des modèles de script d'injection SQL ou intersite et des modèles d'injection XPath, le cas échéant.
7. Vérifiez et configurez les signatures nouvelles et modifiées.
8. Lorsque vous avez terminé, cliquez sur **OK**, puis sur **Fermer**.

Mise à jour d'un objet signatures à partir d'un outil d'analyse des vulnérabilités pris en charge

> **Remarque :**
>
> Avant de mettre à jour un objet signatures à partir d'un fichier, vous devez le créer en exportant des signatures à partir de l'outil d'analyse des vulnérabilités.

Pour importer et mettre à jour des signatures à partir d'un outil d'analyse des vulnérabilités

1. Accédez à **Sécurité** > **Web App Firewall** > **Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures à mettre à jour, puis cliquez sur **Fusionner**.
3. Dans la boîte de dialogue **Mettre à jour l'objet signatures**, sous l'onglet **Format externe**, section Importer, sélectionnez l'une des options suivantes.
   - **Importer à partir de l'URL** : choisissez cette option si vous téléchargez des mises à jour de signature à partir d'une URL Web.
   - **Importer à partir d'un fichier local** : choisissez cette option si vous importez des mises à jour de signature à partir d'un fichier situé sur votre disque dur local ou réseau ou un autre

périphérique de stockage.

4. Dans la zone de texte, tapez l'URL, ou parcourez ou tapez le chemin d'accès au fichier local.
5. Dans la section XSLT, choisissez l'une des options suivantes.
   - **Utiliser le fichier XSLT intégré** : choisissez cette option si vous souhaitez utiliser un fichier XSLT intégré.
   - **Utiliser le fichier XSLT local** : choisissez cette option pour utiliser un fichier XSLT sur votre ordinateur local.
   - **Référence XSLT à partir de l'URL** : choisissez cette option pour importer un fichier XSLT à partir d'une URL Web.
6. Si vous avez choisi Utiliser le fichier XSLT intégré, dans la liste déroulante XSLT intégré, sélectionnez le fichier que vous souhaitez utiliser parmi les options suivantes :
   - **Cenzic.**
   - **Deep_Security_for_Web_Apps.**
   - **Hewlett_Packard_Enterprise_WebInspect.**
   - **IBM-AppScan-Enterprise.**
   - **IBM-AppScan-Standard.**
   - **Qualys.**
   - **Whitehat.**
7. Cliquez sur **Update**. Le fichier de mise à jour est importé et la boîte de dialogue Mettre à jour les signatures passe à un format presque identique à celui de la boîte de dialogue Modifier un objet Signatures, décrite dans Configuration ou modification d'un objet Signatures. La boîte de dialogue **Mettre à jour les signatures d'objet** affiche toutes les branches avec des règles de signature nouvelles ou modifiées, des modèles de script d'injection SQL ou intersite et des modèles d'injection XPath, le cas échéant.
8. Vérifiez et configurez les signatures nouvelles et modifiées.
9. Lorsque vous avez terminé, cliquez sur **OK**, puis sur **Fermer**.

Mise à jour automatique de signature

September 8, 2021

La fonctionnalité Signature Auto Update du pare-feu d'application Web permet à l'utilisateur d'obtenir les dernières signatures pour protéger l'application Web contre les nouvelles vulnérabilités. La fonction de mise à jour automatique offre une meilleure protection sans intervention manuelle continue pour obtenir les dernières mises à jour.

Les signatures sont mises à jour automatiquement toutes les heures et ne nécessitent pas de vérification régulière de la disponibilité de la dernière mise à jour. Une fois que vous avez activé la mise à jour automatique de signature, l'appliance Citrix ADC se connecte au serveur hébergeant les signa-

tures pour vérifier si une version plus récente est disponible.

Emplacement personnalisable

Les dernières signatures d'Application Firewall sont hébergées sur Amazon, qui est configurée comme URL de signature par défaut pour vérifier la dernière mise à jour.

Toutefois, l'utilisateur a la possibilité de télécharger ces fichiers de mappage de signatures sur son serveur interne. L'utilisateur peut ensuite configurer un chemin d'URL de signature différent pour télécharger les fichiers de mappage de signatures à partir d'un serveur local. Pour que la fonctionnalité de mise à jour automatique fonctionne, vous devrez peut-être configurer le serveur DNS pour accéder au site externe.

Signatures de

Tous les objets de signature définis par l'utilisateur qui sont créés à l'aide de l'objet signature par défaut appfw ont une version supérieure à zéro. Si vous activez la mise à jour automatique des signatures, toutes les signatures sont automatiquement mises à jour.

Si l'utilisateur a importé des signatures au format externe tel que Cenzic ou Qualys, les signatures sont importées avec la version zéro. De même, si l'utilisateur a créé un objet signature à l'aide du modèle vide, il est créé en tant que signature de version zéro. Ces signatures ne sont pas automatiquement mises à jour, car l'utilisateur peut ne pas être intéressé par la surcharge de gestion des signatures par défaut qui ne sont pas utilisées.

Toutefois, le pare-feu d'application Web permet également à l'utilisateur de sélectionner manuellement ces signatures et de les mettre à jour pour ajouter les règles de signature par défaut aux règles existantes. Une fois les signatures mises à jour manuellement, la version change, puis les signatures seront automatiquement mises à jour avec les autres signatures.

Configurer la mise à jour automatique des signatures

Pour configurer la fonctionnalité de mise à jour automatique des signatures à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 set appfw settings SignatureAutoUpdate on
2 set appfw settings SignatureUrl https://s3.amazonaws.com/
     NSAppFwSignatures/SignaturesMapping.xml
3 <!--NeedCopy-->
```

Pour configurer la mise à jour automatique des signatures à l'aide de l'interface graphique :

1. Développez le nœud Sécurité.
2. Développez le nœud Application Firewall.
3. Sélectionnez le nœud Signatures.
4. Sélectionnez **Paramètres de mise à jour automatique** dans **Action**.
5. Activez l'option **Mise à jour automatique des signatures** .
6. Vous pouvez spécifier un chemin personnalisé pour l'URL de mise à jour de la signature, si nécessaire. Cliquez sur **Réinitialiser** pour réinitialiser la valeur par défaut `s3.amazonaws.com server`.
7. Cliquez sur **OK**.



Mettre à jour manuellement les signatures

Pour mettre à jour manuellement une signature de version zéro ou toute autre signature définie par l'utilisateur, vous devez d'abord obtenir la dernière mise à jour des signatures par défaut, puis l'utiliser pour mettre à jour la signature définie par l'utilisateur cible.

Exécutez les commandes suivantes à partir de l'interface de ligne de commande pour mettre à jour un fichier de signatures :

```
update appfw signatures "*Default Signatures"
```



```
update appfw signatures cenzic  - mergedefault
<!--NeedCopy-->
```

> **Remarque :**
>
> `Default Signatures` Il est sensible à la casse. Cenzic dans la commande précédente est le nom du fichier de signatures mis à jour.

Importer des signatures par défaut sans accès Internet

Il est recommandé de configurer un serveur proxy pour qu'il pointe vers le serveur Amazon (AWS) pour obtenir la dernière mise à jour. Toutefois, si l'appliance NetScaler n'a pas de connexion Internet vers les sites externes, l'utilisateur peut stocker les fichiers de signatures mis à jour sur un serveur local. L'appliance peut ensuite télécharger les signatures à partir du serveur local. Dans ce scénario, l'utilisateur doit constamment vérifier le **site Amazon** pour obtenir les dernières mises à jour. Vous pouvez télécharger et vérifier le fichier de signature par rapport au fichier sha1 correspondant créé à l'aide de la clé **publique Citrix** pour vous protéger contre la falsification.

Pour copier les fichiers Signatures sur un serveur local, procédez comme suit :

1. Créez un répertoire local tel que <`MySignatures`> sur un serveur local.
2. Ouvrez le site AWS.
3. Copiez le `SignaturesMapping.xml` fichier <`MySignatures`> dans le dossier.

Si vous ouvrez le `SignaturesMapping.xml` fichier, vous pouvez voir tous les fichiers XML pour les signatures et leurs fichiers sha1 correspondants pour les différentes versions prises en charge. Une de ces paires est mise en surbrillance dans la capture d'écran suivante :

1. Créez un sous-répertoire <`sigs`> dans le <`MySignatures`> dossier.
2. Copiez toutes les paires de `*.xml files listed in the` <`file`> balises et les `*.xml.sha1` fichiers répertoriés dans les <`sha1`> balises correspondantes du `SignaturesMapping.xml` fichier dans le <`sigs`> dossier. Voici quelques exemples de fichiers copiés <`sigs`> dans le dossier :

```
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b86v3s3.xml
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b86v3s3.xml.sha1
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b0v3s2.xml
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b0v3s2.xml.sha1
```

> **Remarque :**
>
> Vous pouvez donner n'importe quel nom au <`MySignatures`> dossier et il peut se trouver à n'importe quel emplacement, mais le sous-répertoire <`sigs`> doit être un sous-répertoire du <`MySignatures`> dossier dans lequel le fichier de mappage est copié. En outre, assurez-vous

> que, comme indiqué dans le fichier SignaturesMapping.xml, le nom du sous-répertoire <sigs> doit porter le nom exact et est sensible à la casse. Tous les fichiers Signature et leurs fichiers sha1 correspondants doivent être copiés <sigs> dans ce répertoire.

Après avoir mis en miroir le contenu du serveur Web Amazon hébergé vers le serveur local, modifiez le chemin d'accès au nouveau serveur Web local pour le définir comme URL de signature pour la mise à jour automatique. Par exemple, exécutez la commande suivante à partir de l'interface de ligne de commande de l'appliance :

```
1 set appfw settings SignatureUrl https://myserver.example.net/
     MySignatures/SignaturesMapping.xml
2 <!--NeedCopy-->
```

L'opération de mise à jour peut prendre plusieurs minutes, en fonction du nombre de signatures à mettre à jour. Prévoyez suffisamment de temps pour que l'opération de mise à jour soit terminée.

Si vous rencontrez une erreur « Erreur lors de l'accès à l'URL ! « Lors de la configuration, suivez les étapes pour le résoudre.

1. Ajoutez l'URL https://myserver.example.net pour /netscaler/ns_gui/admin_ui/php/application/controllers/common/utils.php que la sécurité CSP (Content Security Policy) ne bloque pas l'accès à l'URL. Veuillez noter que ces paramètres ne persistent pas lors d'une mise à niveau. L'utilisateur doit l'ajouter à nouveau après la mise à niveau.

```
1 $configuration_view_connect_src = "connect-src 'self' https://app.pendo
     .io https://s3.amazonaws.comhttps://myserver.example.net;";
2 <!--NeedCopy-->
```

1. L'utilisateur doit configurer le serveur Web de https://myserver.example.net manière à ce qu'il réponde aux en-têtes CORS suivants pour https://myserver.example.net/MySignatures/SignaturesMapping.xml

```
1 Access-Control-Allow-Methods: GET
2 Access-Control-Allow-Origin: *
3 Access-Control-Max-Age: 3000
4 <!--NeedCopy-->
```

Directives pour mettre à jour les signatures

Les directives suivantes sont utilisées lors de la mise à jour des signatures :

- Les signatures sont mises à jour lorsque l'URL de mise à jour Signature comporte un objet Signature ayant la même version ou une version plus récente.

- Chaque règle de signature est associée à un ID de règle et à un numéro de version. Pa exemple : `<SignatureRule id="803"version="16"···>`
- La règle de signature du fichier Signatures entrantes portant le même ID et le même numéro de version que le fichier existant est ignorée même si elle comporte des modèles ou une chaîne de journal différents.
- Une règle de signature avec un nouvel identifiant est ajoutée. Toutes les actions et l'indicateur activé sont utilisés à partir du nouveau fichier.

  > **Remarque :**
  >
  > Il se peut que vous deviez toujours revoir régulièrement les signatures mises à jour pour activer ces nouvelles règles ajoutées et modifier d'autres paramètres d'action conformément aux exigences de l'application.

- Les règles portant le même ID mais avec un numéro de version plus récent remplacent celui existant. Toutes les actions et l'indicateur activé de la règle existante sont conservés.

> **Conseil :**
>
> Lorsque vous mettez à jour les signatures de l'interface de ligne de commande, vous devez d'abord mettre à jour les signatures par défaut. Vous devez ensuite ajouter des commandes de mise à jour pour mettre à jour chaque fichier de signatures personnalisé basé sur les signatures par défaut. Si vous ne mettez pas à jour les signatures par défaut en premier, une erreur de non-correspondance de version empêche la mise à jour du fichier de signatures personnalisées.

Intégration des règles Snort

August 20, 2021

Avec les attaques malveillantes sur les applications Web, il est important de protéger votre réseau interne. Les données malveillantes affectent non seulement vos applications Web au niveau de l'interface, mais les paquets malveillants atteignent également la couche d'application. Pour surmonter ces attaques, il est important de configurer un système de détection et de prévention des intrusions qui examine votre réseau interne.

Les règles Snort sont intégrées dans l'appliance pour examiner les attaques malveillantes dans les paquets de données au niveau de la couche d'application. Vous pouvez télécharger les règles de snort et les convertir en règles de signature WAF. Les signatures ont une configuration basée sur des règles qui peut détecter les activités malveillantes telles que les attaques DOS, les dépassements de tampon, les analyses de ports furtifs, les attaques CGI, les sondes SMB et les tentatives d'empreintes digitales du système d'exploitation. En intégrant les règles Snort, vous pouvez renforcer votre solution de sécurité au niveau de l'interface et au niveau de l'application.

Configurer les règles de snort

La configuration commence par télécharger d'abord les règles Snort, puis les importer dans les règles de signature WAF. Une fois les règles converties en signatures WAF, elles peuvent être utilisées comme contrôles de sécurité WAF. Les règles de signature basées sur le snort examinent le paquet de données entrant pour détecter s'il y a des attaques malveillantes sur votre réseau.

Un nouveau paramètre, « VendorType » est ajouté à la commande import pour convertir les règles Snort en signatures WAF.

Le paramètre « VendorType » est défini sur SNORT uniquement pour les règles Snort.

Télécharger les règles de snort à l'aide de l'interface de commande

Vous pouvez télécharger les règles Snort en tant que fichier texte à partir de l'URL ci-dessous :

```
https://www.snort.org/downloads/community/snort3-community-rules.tar.gz
```

Importer des règles de snort à l'aide de l'interface de commande

Après avoir téléchargé, vous pouvez importer les règles Snort dans votre appliance.

À l'invite de commandes, tapez :

```
import appfw signatures <src> <name> [-xslt <string>] [-comment <string>]
[-overwrite] [-merge [-preservedefactions]] [-sha1 <string>] [-VendorType
Snort]
```

Exemple :

```
import appfw signatures http://www.example.com/ns/signatures.xml sig-snort -
comment "signatures from snort rules" -VendorType snort
```

Arguments :

Src. URL (protocole, hôte, chemin d'accès et nom de fichier) pour l'emplacement où stocker l'objet signatures importé.

> **Remarque :**
>
> L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS qui nécessite l'authentification de certificat client pour l'accès. Argument obligatoire de longueur maximale : 2047

Nom. Nom à attribuer à l'objet signatures sur Citrix ADC. Argument obligatoire de longueur maximale : 31

Commentaire. Description de la façon de conserver les informations sur l'objet signatures. Longueur maximale : 255
écrasement. Remplacer tout objet signatures existant du même nom.

Fusionner. Fusionne la signature existante avec de nouvelles règles de signature.

Preservedefactions. Conserve les actions de déf des règles de signature.

VendorType. Fournisseur tiers pour générer les signatures WAF. Valeurs possibles : Snort.

Configurer les règles de snort à l'aide de l'interface graphique Citrix ADC

La configuration de l'interface graphique pour les règles Snort est similaire à la configuration d'autres scanners d'applications Web externes comme Cenzic, Qualys, Whitehat.

Suivez les étapes ci-dessous pour configurer Snort :

1. Accédez à **Configuration > Sécurité > Citrix Web App Firewall > Signatures**.
2. Dans la page **Signatures**, cliquez sur **Ajouter**.
3. Dans la page **Ajouter des signatures**, définissez les paramètres suivants pour configurer les règles Snort.
    a) File format. Sélectionnez le format de fichier comme externe.
    b) Importer à partir de. Sélectionnez l'option d'importation en tant que fichier Snort ou URL pour entrer l'URL.
    c) Snort V3 Vendor. Activez la case à cocher pour importer les règles Snort à partir d'un fichier ou d'une URL.
4. Cliquez sur **Ouvrir**.



L'appliance importe les règles Snort en tant que règles de signature WAF basées sur le snort.



Il est recommandé d'utiliser des actions de filtrage pour activer les règles de reniement que vous préférez importer en tant que règles de signature WAF sur l'appliance.



5. Pour confirmer, cliquez sur **Yes**.



6. Les règles sélectionnées sont activées sur l'appliance.



7. Cliquez sur **OK**.

Exportation d'un objet signatures dans un fichier

January 21, 2021

Vous exportez un objet signatures dans un fichier afin de pouvoir l'importer dans un autre Citrix ADC.

Pour exporter un objet signatures vers un fichier

1. Accédez à **Sécurité > Citrix Web App Firewall > Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures que vous souhaitez configurer.
3. Dans la liste déroulante **Actions**, sélectionnez **Exporter**.
4. Dans la boîte de dialogue **Exporter l'objet signatures**, zone de texte **Fichier local**, tapez le chemin d'accès et le nom du fichier vers lequel vous souhaitez exporter l'objet signatures, ou utilisez la boîte de dialogue **Parcourir** pour désigner un chemin d'accès et un nom.
5. Cliquez sur **OK**.

Editeur de signatures

August 20, 2021

Vous pouvez utiliser l'éditeur de signatures pour ajouter ou modifier une règle de signature définie par l'utilisateur (locale) à un objet signatures existant. Une règle de signature locale possède les mêmes attributs qu'une règle de signature par défaut de Citrix, et elle fonctionne de la même manière. Vous l'activez ou la désactivez et configurez les actions de signature pour elle, comme vous le faites pour une signature par défaut.

Ajoutez une règle locale si vous devez protéger vos sites Web et services contre une attaque connue que les signatures existantes ne correspondent pas. Par exemple, vous pouvez découvrir un nouveau type d'attaque et déterminer ses caractéristiques en examinant les journaux de votre serveur Web, ou vous pouvez obtenir des informations tierces sur un nouveau type d'attaque.

Au cœur d'une règle de signature se trouvent les *modèles*de règle, qui décrivent collectivement les caractéristiques de l'attaque que la règle est conçue pour correspondre. Chaque modèle peut être constitué d'une chaîne simple, d'une expression régulière au format PCRE ou d'une injection SQL intégrée ou de modèles de script intersite.

Vous pouvez modifier une règle de signature en ajoutant un nouveau modèle ou en modifiant un modèle existant pour correspondre à une attaque. Par exemple, vous pouvez vous renseigner sur les modifications apportées à une attaque, ou vous pouvez déterminer un meilleur modèle en examinant les journaux de votre serveur Web ou à partir d'informations tierces.

Pour ajouter ou modifier une règle de signature locale à l'aide de l'éditeur de signatures

1. Accédez à **Sécurité > Citrix Web App Firewall > Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures à modifier, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Modifier l'objet Signatures**, au milieu de l'écran sous la fenêtre **Résultats filtrés**, effectuez l'une des opérations suivantes :
   - Pour ajouter une nouvelle règle de signature locale, cliquez sur Ajouter.
   - Pour modifier une règle de signature locale existante, sélectionnez cette règle, puis cliquez sur **Ouvrir**.
4. Dans la boîte de dialogue **Ajouter une règle** de **signature locale ou Modifier une règle** de signature locale, configurez les actions d'une signature en cochant les cases appropriées.
   - **Activé.** Active la nouvelle règle de signature. Si vous ne sélectionnez pas cette option, cette nouvelle règle de signature est ajoutée à votre configuration, mais elle est inactive.
   - **Bloc.** Bloque les connexions qui violent cette règle de signature.
   - **Journal.** Consigne les violations de cette règle de signature dans le journal Citrix ADC.
   - **Stat.** Inclut les violations de cette règle de signature dans les statistiques.
   - **Remove.** Supprime les informations correspondant à la règle de signature de la réponse. (S'applique uniquement aux règles de réponse.)
   - **X-Out.** Masque les informations correspondant à la règle de signature avec la lettre X. (S'applique uniquement aux règles de réponse)
   - **Autoriser les doublons.** Autorise les doublons de cette règle de signature dans cet objet signatures.
5. Choisissez une catégorie pour la nouvelle règle de signature dans la liste déroulante **Catégorie**.

   Vous pouvez également créer une catégorie en cliquant sur l'icône située à droite de la liste et en utilisant la boîte de dialogue Ajouter une catégorie de règle de signature pour ajouter une nouvelle catégorie à la liste. La règle que vous modifiez est automatiquement ajoutée à la nouvelle catégorie. Pour obtenir des instructions, reportez-vous à la section Pour ajouter une catégorie de règles de signature.
6. Dans la zone de texte **LogString**, tapez une brève description de la règle de signature à utiliser dans les journaux.
7. Dans la zone de texte **Commentaire**, tapez un commentaire. (Facultatif)
8. Cliquez sur Plus… et modifiez les options avancées.
   a) Pour supprimer les commentaires HTML avant d'appliquer cette règle de signature, dans la liste déroulante Slot Commentaires, choisissez Tout ou Exclure la balise de script.

b) Pour définir la vérification des en-têtes de référencement CSRF, dans le tableau de boutons radio Vérification de l'en-tête du référent CSRF, sélectionnez le bouton radio Si présent ou Toujours.
c) Pour modifier manuellement l'ID de règle affecté à cette règle de signature locale, modifiez le numéro dans la zone de texte ID de règle. L'ID doit être un nombre entier positif compris entre 1000000 et 1999999 qui n'a pas déjà été attribué à une règle de signature locale.
d) Pour affecter un numéro de version à la nouvelle règle de signature, modifiez le numéro dans la zone de texte Numéro de version.
e) Pour affecter un ID source, modifiez la chaîne dans la zone de texte ID source.
f) Pour spécifier la source, choisissez Local ou Snort dans la liste déroulante Source, ou cliquez sur l'icône Ajouter à droite de la liste et ajoutez une nouvelle source.
g) Pour affecter un score de préjudice aux violations de cette règle de signature locale, tapez un nombre compris entre 1 et 10 dans la zone de texte Score de préjudice.
h) Pour affecter une cote de gravité à cette règle de signature locale, dans la liste déroulante Gravité, choisissez Élevée, Moyenne ou Faible, ou cliquez sur l'icône Ajouter à droite de la liste et ajoutez une nouvelle cote de gravité.
i) Pour affecter un type de violation à cette règle de signature locale, dans la liste déroulante Type, choisissez Vulnérable ou Avertissement, ou cliquez sur l'icône Ajouter à droite de la liste et ajoutez un nouveau type de violation.

9. Dans la liste **Motifs**, ajoutez ou modifiez un motif.

   - Pour ajouter un motif, cliquez sur **Ajouter**. Dans la boîte de dialogue **Créer un modèle de règle de signature**, ajoutez un ou plusieurs modèles pour votre règle de signature, puis cliquez sur **OK**.
   - Pour modifier un motif, sélectionnez-le, puis cliquez sur **Ouvrir**. Dans la boîte de dialogue **Modifier le modèle de règle de signature**, modifiez le modèle, puis cliquez sur **OK**.

   Pour plus d'informations sur l'ajout ou la modification de modèles, voir Modèles de règles de signature.

10. Cliquez sur **OK**.

Pour ajouter une catégorie de règle de signature

January 21, 2021

L'intégration de règles de signature dans une catégorie vous permet de configurer les actions pour un groupe de signatures plutôt que pour chaque signature individuelle. Vous pouvez le faire pour les raisons suivantes :

- **Facilité de sélection.** Par exemple, supposons que toutes les règles de signature d'un groupe

particulier protègent contre les attaques contre un type spécifique de logiciel ou de technologie de serveur Web. Si vos sites Web protégés utilisent ce logiciel ou cette technologie, vous souhaitez tous les activer. Si ce n'est pas le cas, vous ne voulez en activer aucun.

- **Facilité de configuration initiale.** Il est plus facile de définir des valeurs par défaut pour un groupe de signatures en tant que catégorie, au lieu d'une par une. Vous pouvez ensuite apporter les modifications nécessaires aux signatures individuelles.
- **Facilité de configuration continue.** Il est plus facile de configurer les signatures si vous ne pouvez afficher que celles qui répondent à des critères spécifiques, tels que l'appartenance à une catégorie spécifique.

1. Accédez à **Sécurité** > **Web App Firewall** > **Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures que vous souhaitez configurer, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Modifier l'objet Signatures**, au milieu de l'écran, sous la fenêtre **Résultats filtrés**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Ajouter une règle de signature locale**, cliquez sur l'icône située à droite de la liste déroulante Catégorie.
5. Dans la boîte de dialogue **Ajouter une catégorie de règle de signature**, zone de texte **Nouvelle catégorie**, tapez un nom pour votre nouvelle catégorie de signature. Le nom peut se composer d'un à 64 caractères.
6. Cliquez sur **OK**.

Modèles de règles de signature

August 20, 2021

Vous pouvez ajouter un motif ou modifier un motif existant pour spécifier une chaîne ou une expression qui caractérise une attaque si la signature correspond. Pour détecter les motifs d'une attaque, vous pouvez examiner les journaux sur votre serveur Web. Vous pouvez utiliser un outil pour observer les données de connexion en temps réel, ou obtenir la chaîne ou l'expression à partir d'un rapport tiers sur l'attaque.

> **Attention :**
>
> Tout nouveau modèle que vous ajoutez à une règle de signature se trouve dans une relation AND avec les modèles existants. N'ajoutez pas de modèle à une règle de signature existante si vous ne souhaitez pas qu'une attaque potentielle puisse correspondre à tous les modèles pour correspondre à la signature.

Chaque modèle peut être constitué d'une chaîne simple, d'une expression régulière au format PCRE ou d'une injection SQL intégrée ou d'un modèle de script intersite. Avant d'essayer d'ajouter un motif

basé sur une expression régulière, vous devez vous assurer que vous comprenez les expressions régulières au format PCRE. Les expressions PCRE sont complexes et puissantes. Si vous ne comprenez pas comment ils fonctionnent, vous pouvez involontairement créer un motif qui correspond à quelque chose que vous ne vouliez pas (un *faux positif*) ou qui ne correspond pas à quelque chose que vous vouliez (un *faux négatif*).

Modèle de signature personnalisé pour les types de contenu autres que par défaut

Le Citrix ADC Web App Firewall (WAF) prend désormais en charge un nouvel emplacement pour inspecter le contenu canonicalisé. Par défaut, WAF ne bloque pas la charge utile codée avec des types de contenu autres que par défaut. Lorsque ces types de contenu sont mis en liste blanche et qu'aucune action configurée n'est appliquée, la vérification de protection par script SQL et intersite ne filtrent pas les attaques de script SQL ou intersite dans les charges utiles codées. Pour résoudre le problème, un utilisateur peut créer une règle de signature personnalisée avec ce nouvel emplacement (HTTP_CANON_POST_BODY) qui examine les charges utiles codées pour les types de contenu autres que par défaut et s'il y a une attaque de script SQL ou intersite, il bloque le trafic après canonicalisation du corps de la publication.

> **Remarque :**
>
> Cette prise en charge n'est applicable que pour les requêtes HTTP.

Si vous n'êtes pas déjà familier avec les expressions régulières au format PCRE, vous pouvez utiliser les ressources suivantes pour apprendre les bases ou pour obtenir de l'aide sur un problème spécifique :

- « Maîtriser les expressions régulières », Troisième édition. Copyright (c) 2006 par Jeffrey Friedl. O'Reilly Media, ISBN : 9780596528126.
- « Regular Expressions Cookbook ». Copyright (c) 2009 par Jan Goyvaerts et Steven Levithan. O'Reilly Media, ISBN : 9780596520687
- **Page de manuel PCRE/spécification** (texte/officiel) : http://www.pcre.org/pcre.txt
- **Page d'accueil/spécification PCRE**

http://www.gammon.com.au/pcre/index.html

- **Entrée Wikipédia PCRE** : http://en.wikipedia.org/wiki/PCRE
- **Liste de diffusion PCRE PCRE-Dev**
  - Développement PCRE

Si vous devez encoder des caractères non ASCII dans une expression régulière au format PCRE, la plateforme Citrix ADC prend en charge le codage des codes hexadécimaux UTF-8. Pour plus d'informations, voir Format de codage de caractères PCRE.

Pour configurer un modèle de règle de signature

1. Accédez à **Sécurité > Citrix Web App Firewall > Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures que vous souhaitez configurer, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Modifier l'objet Signatures**, au milieu de l'écran, sous la fenêtre **Résultats filtrés**, cliquez sur **Ajouter** pour créer une règle de signature, ou sélectionnez une règle de signature existante et cliquez sur **Ouvrir**.

   > **Remarque :**
   >
   > Vous ne pouvez modifier que les règles de signature que vous avez ajoutées. Vous ne pouvez pas modifier les règles de signature par défaut.

   Selon votre action, la boîte de dialogue Ajouter une règle de signature locale ou Modifier une règle de signature locale s'affiche. Les deux boîtes de dialogue ont le même contenu.
4. Dans la **fenêtre Motifs** de la boîte de dialogue, cliquez sur **Ajouter** pour ajouter un nouveau motif ou sélectionnez un motif existant dans la liste située sous le bouton **Ajouter**, puis cliquez sur **Ouvrir**. Selon votre action, la boîte de dialogue **Créer un modèle de règle de signature** ou **Modifier le modèle de règle de signature** s'affiche. Les deux boîtes de dialogue ont le même contenu.
5. Dans la liste déroulante **Type de motif**, choisissez le type de connexion auquel le motif doit correspondre.
   - Si le modèle est conçu pour correspondre à des éléments ou des fonctionnalités de requête, tels que du code SQL injecté, des attaques sur des formulaires Web, des scripts intersites ou des URL inappropriées, choisissez **Request**.
   - Si le motif est conçu pour correspondre à des éléments ou des fonctions de réponse, tels que des numéros de carte de crédit ou des objets sûrs, choisissez **Réponse**.
6. Dans la zone Emplacement, définissez les éléments à examiner avec ce motif.
   La zone Emplacement décrit les éléments de la requête ou de la réponse HTTP à examiner pour ce modèle. Les choix qui apparaissent dans la zone Emplacement dépendent du type de répétition choisi. Si vous avez choisi Request comme type de motif, les éléments pertinents pour les requêtes HTTP apparaissent. Si vous avez choisi Réponse, les éléments pertinents pour les réponses HTTP apparaissent.
   En outre, lorsque vous choisissez une valeur dans la liste déroulante Zone, les parties restantes de la zone Emplacement changent de manière interactive. Voici tous les éléments de configuration qui peuvent apparaître dans cette section.
   - Zone. Liste déroulante des éléments qui décrivent une partie particulière de la connexion HTTP. Les choix sont les suivants :

- **HTTP_ANY**. Toutes les parties de la connexion HTTP.
- **HTTP_COOKIE**. Tous les cookies dans les en-têtes de requête HTTP après toute transformation de cookie est effectuée.
  Remarque : Ne recherche pas les en-têtes de réponse HTTP “Set-Cookie:”.
- **HTTP_FORM_FIELD**. Champs de formulaire et leur contenu, après décodage d’URL, décodage de pourcentage et suppression des espaces excédentaires. Vous pouvez utiliser la<Location> balise pour restreindre davantage la liste des noms de champs de formulaire à rechercher.
- **HTTP_HEADER**. Les parties de valeur de l’en-tête HTTP après toute transformation de script intersite ou de décodage d’URL.
- **HTTP_METHOD**. Méthode de requête HTTP.
- **HTTP_ORIGIN_URL**. URL d’origine d’un formulaire Web.
- **HTTP_POST_BODY**. Corps de publication HTTP et données de formulaire Web qu’il contient.
- **HTTP_RAW_COOKIE**. Tous les cookies de requête HTTP, y compris la partie nom « Cookie : ».
  Remarque : Ne recherche pas les en-têtes de réponse HTTP “Set-Cookie:”.
- **HTTP_RAW_HEADER**. En-tête HTTP entier, avec des en-têtes individuels séparés par des caractères de saut de ligne (n) ou des chaînes de retour chariot/saut de ligne (rn).
- **HTTP_RAW_RESP_HEADER**. L’ensemble de l’en-tête de réponse, y compris les parties de nom et de valeur de l’en-tête de réponse après la transformation de l’URL, ainsi que l’état de la réponse complète. Comme pour HTTP_RAW_HEADER, les en-têtes individuels sont séparés par des caractères de saut de ligne (n) ou des chaînes de retour chariot/saut de ligne (rn).
- **HTTP_RAW_SET_COOKIE**. L’en-tête Set-Cookie entier après toutes les transformations d’URL ont été effectuées
  Remarque : la transformation d’URL peut modifier à la fois les parties domaine et chemin de l’en-tête Set-Cookie.
- **HTTP_RAW_URL**. Toute l’URL de la requête avant toute transformation d’URL est effectuée, y compris les parties de requête ou de fragment.
- **HTTP_RESP_HEADER**. La partie valeur des en-têtes de réponse complète après toute transformation d’URL a été effectuée.
- **HTTP_RESP_BODY**. Le corps de la réponse HTTP
- **HTTP_SET_COOKIE**. Tous les en-têtes « Set-Cookie » dans les en-têtes de réponse HTTP.
- **HTTP_STATUS_CODE**. Code d’état HTTP.
- **HTTP_STATUS_MESSAGE**. Message d’état HTTP.
- **HTTP_URL**. La partie valeur de l’URL dans les en-têtes HTTP, à l’exclusion des ports de requête ou de fragment, après conversion au jeu de caractères UTF-*, décodage

d'URL, suppression des espaces et conversion des URL relatives en absolues. N'inclut pas le décodage d'entité HTML.
- URL. Examine toutes les URL trouvées dans les éléments spécifiés par le paramètre Area. Sélectionnez l'un des paramètres suivants.
- **Any.** Vérifie toutes les URL.
- Littéral. Vérifie les URL qui contiennent une chaîne littérale. Une fois que vous avez sélectionné Littéral, une zone de texte s'affiche. Tapez la chaîne littérale souhaitée dans la zone de texte.
- PCRE. Vérifie les URL qui correspondent à une expression régulière au format PCRE. Après avoir sélectionné ce choix, la fenêtre d'expression régulière s'affiche. Tapez l'expression régulière dans la fenêtre. Vous pouvez utiliser les **jetons Regex** pour insérer des éléments d'expression régulière communs au niveau du curseur, ou vous pouvez cliquer sur Éditeur Regex pour afficher la boîte de dialogue Éditeur d'expression régulière, qui fournit plus d'aide pour la construction de l'expression régulière souhaitée.
- Expression. Vérifie les URL qui correspondent à une expression par défaut de Citrix ADC.
- Nom du champ. Examine tous les noms de champs de formulaire trouvés dans les éléments spécifiés par la sélection
  Zone. **Any.** Vérifie toutes les URL.
- Littéral. Vérifie les URL qui contiennent une chaîne littérale. Une fois que vous avez sélectionné Littéral, une zone de texte s'affiche. Tapez la chaîne littérale souhaitée dans la zone de texte.
- PCRE. Vérifie les URL qui correspondent à une expression régulière au format PCRE. Après avoir sélectionné ce choix, la fenêtre d'expression régulière s'affiche. Tapez l'expression régulière dans la fenêtre. Vous pouvez utiliser les **jetons Regex** pour insérer des éléments d'expression rationnelle communs ou vous pouvez utiliser l'éditeur de regex pour vous aider à construire une expression rationnelle que vous voulez.
- Expression. Vérifie les URL qui correspondent à une expression par défaut de Citrix ADC.

7. Dans la zone Motif, définissez la répétition. Un motif est une chaîne littérale ou une expression régulière au format PCRE qui définit le motif que vous souhaitez faire correspondre. La zone Pattern contient les éléments suivants :
   - Correspondance. Liste déroulante des méthodes de recherche que vous pouvez utiliser pour la signature. Cette liste diffère selon que le type de motif est Request ou Réponse.

   Types de correspondance de demande
   PCRE. Expression régulière au format PCRE.

> **Remarque :**
>
> Lorsque vous choisissez PCRE, les outils d'expression régulière situés sous la fenêtre Motif sont activés. Ces outils ne sont pas utiles pour la plupart des autres types de modèles.

- **Injection**. Indique au Web App Firewall de rechercher le SQL injecté à l'emplacement spécifié. La fenêtre Motif disparaît, car le Web App Firewall possède déjà les modèles pour l'injection SQL.
- **CrossSitescripting**. Indique au pare-feu de l'application Web de rechercher des scripts intersites à l'emplacement spécifié. La fenêtre Motif disparaît, car le Web App Firewall possède déjà les modèles pour les scripts intersites.
- **Expression**. Une expression dans le langage d'expressions par défaut Citrix ADC est le même langage d'expression pour la création de stratégies de Web App Firewall sur l'appliance Citrix ADC. Bien que le langage d'expressions Citrix ADC ait été initialement développé pour les règles de stratégie, il s'agit d'un langage à usage général hautement flexible qui peut également être utilisé pour définir un modèle de signature.

Lorsque vous choisissez Expression, l'éditeur Citrix ADC Expression s'affiche sous la fenêtre Motif. Pour plus d'informations sur l'éditeur d'expression et des instructions sur son utilisation, reportez-vous à la section Pour ajouter une règle de pare-feu (expression) à l'aide de la boîte de dialogue Ajouter une expression.

Types de correspondance de réponse :

```
1 -  Literal. A literal string
2 -  PCRE. A PCRE-format regular expression.
```

> Remarque
>
> Lorsque vous choisissez PCRE, les outils d'expression régulière situés sous la fenêtre Motif sont activés. Ces outils ne sont pas utiles pour la plupart des autres types de modèles.

- **Carte de crédit**. Modèle intégré pour correspondre à l'un des six types de numéro de carte de crédit pris en charge.

> Remarque :
>
> Le type de correspondance Expression n'est pas disponible pour les signatures côté réponse.

- Fenêtre de répétition (sans étiquette)

Dans cette fenêtre, tapez le motif que vous souhaitez faire correspondre et remplissez toutes les données supplémentaires.

- Littéral. Tapez la chaîne à rechercher dans la zone de texte.

- CRE. Tapez l'expression régulière dans la zone de texte. Utilisez l'éditeur Regex pour obtenir plus d'aide dans la construction de l'expression régulière souhaitée, ou les jetons Regex pour insérer des éléments d'expression régulière communs au curseur. Pour activer les caractères UTF-8, cliquez sur UTF-8.
- Expression. Tapez l'expression avancée Citrix ADC dans la zone de texte. Utilisez Préfixe pour choisir le premier terme dans votre expression ou Opérateur pour insérer des opérateurs communs au curseur. Cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajouter une expression pour obtenir plus d'aide dans la construction de l'expression régulière souhaitée. Cliquez sur Evaluer pour ouvrir Advanced Expression Evaluator afin de déterminer l'effet de votre expression.
- Décalage. Nombre de caractères à ignorer avant de commencer à correspondre sur ce modèle. Vous utilisez ce champ pour commencer à examiner une chaîne à un moment autre que le premier caractère.
- Profondeur. Combien de caractères à partir du point de départ à examiner pour les correspondances. Vous utilisez ce champ pour limiter les recherches d'une chaîne volumineuse à un nombre spécifique de caractères.
- Mini-longueur. La chaîne à rechercher doit avoir au moins le nombre d'octets spécifié en longueur. Les chaînes plus courtes ne sont pas appariées.
- Longueur maximale. La chaîne à rechercher ne doit pas dépasser le nombre d'octets spécifié. Les chaînes plus longues ne sont pas appariées.
- Méthode de recherche. Une case à cocher intitulée Fastmatch. Vous pouvez activer fastmatch uniquement pour un motif littéral, afin d'améliorer les performances.

8. Cliquez sur **OK**.
9. Répétez les quatre étapes précédentes pour ajouter ou modifier d'autres motifs.
10. Lorsque vous avez terminé d'ajouter ou de modifier des modèles, cliquez sur **OK** pour enregistrer vos modifications et revenir au volet Signatures.

> **Attention :**
>
> Tant que vous n'avez pas cliqué sur **OK** dans la boîte de dialogue **Ajouter une règle** de **signature locale ou Modifier une règle** de signature locale, vos modifications ne sont pas enregistrées. Ne fermez aucune de ces boîtes de dialogue sans cliquer sur **OK**, sauf si vous souhaitez ignorer vos modifications.

Pour importer et fusionner des règles

August 20, 2021

Lorsque vous utilisez l'éditeur de signatures pour effectuer une opération d'importation et de fusion

à partir de l'interface graphique, vous pouvez désormais voir les règles nouvelles, mises à jour, dupliquées et non valides.

L'éditeur de signatures affiche les quatre nouvelles lignes suivantes :

1. Nouvelles règles
2. Règles mises à jour
3. Règles en double
4. Règles non valides

La sortie des filtres Nouvelles règles uniquement et Règles mises à jour uniquement apparaît également dans le volet Filtre Catégorie de la fenêtre Modifier dans l'éditeur de signatures.

Vous devrez importer les fichiers de l'interface graphique pour voir les liens correspondants pour les règles nouvelles, dupliquées, invalides et mises à jour.

Procédure d'importation des règles de signature :

1. Dans l'interface graphique Web Citrix ADC, accédez à **Configuration > Sécurité > Signatures de Citrix Web App Firewall**. Dans la fenêtre Signatures, cliquez sur **Ajouter**. Ensuite, sélectionnez **Format de fichier** > **Natif**, **Importer de** > **URL** et dans le champ URL, ajoutez le lien ci-dessus. Si vous ne parvenez pas à accéder à l'URL, vous pouvez télécharger les données XML dans un format de fichier texte.
2. Après avoir cliqué sur **Ouvrir**, le fichier de signature s'ouvre et vous pouvez voir des liens pour la nouvelle règle et les règles non valides.
3. Si vous importez une règle de signature de3rd partie, vous pouvez voir 90 nouvelles règles et 9 règles en double dans le fichier .xml importé. Si vous ne parvenez pas à accéder à l'URL, vous pouvez télécharger les données XML dans un format de fichier texte.

Mises à jour de signature dans le déploiement et les mises à niveau de génération haute disponibilité

January 21, 2021

La mise à jour de signature se produit sur le nœud principal. Pendant que les signatures sont mises à jour sur le nœud principal, les fichiers mis à jour sont simultanément synchronisés avec le nœud secondaire.

La signature par défaut est toujours mise à jour en premier, puis le reste des signatures définies par l'utilisateur est mis à jour.

Connexion à Amazon AWS

La route par défaut NSIP est utilisée pour se connecter à Amazon AWS. S'il existe un scénario d'utilisation spécifique dans lequel SNIP est utilisé, et s'il existe plusieurs SNIP, le premier à recevoir la réponse ARP du site d'hébergement contiendra l'itinéraire.

Mises à jour de signature pendant les mises à niveau de version

Dans le cas d'une mise à niveau, si le NS dispose d'une version de base plus ancienne pour les signatures, *La signature par défaut est automatiquement mise à jour si une version de signature plus récente est disponible.

Si le schéma a changé, la version de schéma de tous les objets de signature est mise à jour lors de la mise à niveau de la version.

Toutefois, pour la version de base des signatures définies par l'utilisateur, le comportement est différent dans la version 10.5 par rapport à la version 11.0.

Dans la version 10.5, seule la signature par défaut a été mise à jour et la version de base du reste des signatures est restée inchangée après la mise à niveau de génération.

Dans la version 11.0, ce comportement a changé. Lorsque l'appliance est mise à niveau pour installer une nouvelle version, non seulement l'objet signature *Default, mais toutes les autres signatures définies par l'utilisateur qui existent actuellement dans l'appliance sont également mises à jour et auront la même version après la mise à niveau de la version.

Dans les versions 10.5 et 11.0, si la mise à jour automatique est configurée, les signatures *Default ainsi que toutes les signatures de version non nulle sont automatiquement mises à jour vers la dernière version de signature publiée et auront la même version de base.

Vue d'ensemble des contrôles de sécurité

August 20, 2021

Les protections avancées du pare-feu Web App Firewall (contrôles de sécurité) sont un ensemble de filtres conçus pour détecter les attaques complexes ou inconnues sur vos sites Web et services Web protégés. Les contrôles de sécurité utilisent des techniques heuristiques, une sécurité positive et d'autres techniques pour détecter les attaques qui ne peuvent pas être détectées uniquement par les signatures. Vous configurez les vérifications de sécurité en créant et en configurant un profil de Web App Firewall, qui est un ensemble de paramètres définis par l'utilisateur qui indiquent au pare-feu Web App les vérifications de sécurité à utiliser et comment gérer une demande ou une réponse qui échoue une vérification de sécurité. Un profil est associé à un objet signatures et à une stratégie pour créer une configuration de sécurité.

Le pare-feu des applications Web fournit vingt contrôles de sécurité, qui diffèrent considérablement par le type d'attaque qu'ils ciblent et la complexité de leur configuration. Les contrôles de sécurité sont organisés selon les catégories suivantes :

- **Contrôles de sécurité communs.** Les contrôles qui s'appliquent à tout aspect de la sécurité Web qui n'implique pas de contenu ou s'appliquent également à tous les types de contenu.
- **Vérifications de sécurité HTML.** Vérifications qui examinent les demandes et les réponses HTML. Ces vérifications s'appliquent aux sites Web HTML et aux parties HTML des sites Web 2.0, qui contiennent des contenus HTML et XML mixtes.
- **Vérifications de sécurité XML.** Vérifications qui examinent les demandes et les réponses XML. Ces vérifications s'appliquent aux services Web XML et aux parties XML des sites Web 2.0.

Les contrôles de sécurité protègent contre un large éventail de types d'attaques, y compris les attaques contre les vulnérabilités logicielles du système d'exploitation et du serveur Web, les vulnérabilités de base de données SQL, les erreurs dans la conception et le codage des sites Web et des services Web, et les échecs de sites sécurisés qui hébergent ou peuvent accéder à des informations sensibles.

Toutes les vérifications de sécurité ont un ensemble d'options de configuration, les actions de vérification, qui contrôlent la façon dont le Web App Firewall gère une connexion correspondant à une vérification. Trois actions de vérification sont disponibles pour toutes les vérifications de sécurité. Ils sont :

- **Bloc.** Bloquer les connexions qui correspondent à la signature. Désactivé par défaut.
- **Journal.** Enregistrer les connexions qui correspondent à la signature, pour une analyse ultérieure. Activé par défaut.
- **Statistiques.** Tenir à jour des statistiques, pour chaque signature, indiquant le nombre de connexions correspondant et fournissant d'autres informations sur les types de connexions bloquées. Désactivé par défaut.

Une quatrième action de vérification, **Apprendre**, est disponible pour plus de la moitié des actions de vérification. Il observe le trafic vers un site Web protégé ou un service Web et utilise des connexions qui violent à plusieurs reprises la vérification de sécurité pour générer des exceptions recommandées (relaxations) à la vérification, ou de nouvelles règles pour la vérification. Outre les actions de vérification, certaines vérifications de sécurité ont des paramètres qui contrôlent les règles utilisées par la vérification pour déterminer quelles connexions ne respectent pas cette vérification ou qui configurent la réponse du pare-feu Web App aux connexions qui violent la vérification. Ces paramètres sont différents pour chaque vérification, et ils sont décrits dans la documentation de chaque vérification.

Pour configurer les contrôles de sécurité, vous pouvez utiliser l'assistant Web App Firewall, comme décrit dans l'Assistant Web App Firewall, ou vous pouvez configurer les contrôles de sécurité manuellement, comme décrit dans Configuration manuelle à l'aide de l'interface graphique. Certaines tâches, telles que la saisie manuelle de relaxations ou de règles ou l'examen des données apprises, ne peuvent être effectuées qu'à l'aide de l'interface graphique, et non de la ligne de commande. L'utilisation de

l'assistant est généralement la meilleure méthode de configuration, mais dans certains cas, la configuration manuelle peut être plus facile si vous êtes bien familier avec lui et que vous voulez simplement ajuster la configuration pour une seule vérification de sécurité.

Quelle que soit la méthode que vous utilisez pour configurer les vérifications de sécurité, chaque vérification de sécurité nécessite l'exécution de certaines tâches. De nombreuses vérifications nécessitent que vous spécifiez des exceptions (relaxations) pour empêcher le blocage du trafic légitime avant d'activer le blocage pour cette vérification de sécurité. Vous pouvez le faire manuellement, en observant les entrées du journal après un certain volume de trafic a été filtré, puis en créant les exceptions nécessaires. Cependant, il est généralement beaucoup plus facile d'activer la fonctionnalité d'apprentissage et de la laisser observer le trafic et recommander les exceptions nécessaires.

Le Web App Firewall utilise des moteurs de paquets (PE) pendant le traitement des transactions. Chaque moteur de paquets a une limite de 100 000 sessions, ce qui est suffisant pour la plupart des scénarios de déploiement. Toutefois, lorsque le Web App Firewall traite un trafic important et que le délai d'expiration de session est configuré à une valeur plus élevée, les sessions peuvent être accumulées. Si le nombre de sessions actives de Web App Firewall dépasse la limite de 100 000 par PE, les violations de vérification de sécurité du pare-feu Web App peuvent ne pas être envoyées à l'appliance Security Insight. La réduction du délai d'expiration de session à une valeur plus petite, ou l'utilisation du mode sans session pour les vérifications de sécurité avec fermeture d'URL sans session ou cohérence de champ sans session peut aider à empêcher l'accumulation des sessions. Si cette option n'est pas viable dans les scénarios où les transactions peuvent nécessiter des sessions plus longues, la mise à niveau vers une plate-forme supérieure avec plus de moteur de paquets est recommandée.

La prise en charge de AppFirewall mis en cache est ajoutée, et le paramètre de session maximale via l'interface de ligne de commande par cœur est défini sur 50 000 sessions.

Protections de haut niveau

January 21, 2021

Quatre des protections de Web App Firewall sont particulièrement efficaces contre les types courants d'attaques Web et sont donc plus couramment utilisées que les autres. Ils sont :

- **Scripting inter-site HTML.** Examine les demandes et réponses pour les scripts qui tentent d'accéder ou de modifier du contenu sur un site Web différent de celui sur lequel se trouve le script. Lorsque cette vérification détecte un tel script, elle le rend inoffensif avant de transférer la requête ou la réponse à sa destination, ou elle bloque la connexion.
- **Injection HTML SQL.** Examine les demandes qui contiennent des données de champ de formulaire pour les tentatives d'injection de commandes SQL dans une base de données SQL. Lorsque

cette vérification détecte du code SQL injecté, elle bloque la requête ou rend le code SQL injecté inoffensif avant de transférer la demande au serveur Web.

Remarque : Si les deux conditions suivantes s'appliquent à votre configuration, vous devez vous assurer que votre Web App Firewall est correctement configuré :

- Si vous activez la vérification HTML Cross-Site Scripting ou la vérification HTML SQL Injection (ou les deux), et
- Vos sites Web protégés acceptent les téléchargements de fichiers ou contiennent des formulaires Web qui peuvent contenir des données corporelles POST volumineuses.

Pour plus d'informations sur la configuration du Web App Firewall pour gérer ce cas, reportez-vous à la section Configuration du pare-feu d'application.

- **Dépassement de tampon.** Examine les demandes de détection des tentatives de provoquer un dépassement de mémoire tampon sur le serveur Web.
- **Cohérence des cookies.** Examine les cookies renvoyés avec les demandes des utilisateurs pour vérifier qu'ils correspondent aux cookies que votre serveur Web a définis pour cet utilisateur. Si un cookie modifié est trouvé, il est retiré de la demande avant que la demande soit transférée au serveur Web.

La vérification de débordement de tampon est simple ; vous pouvez généralement activer le blocage immédiatement. Les trois autres contrôles de niveau supérieur sont beaucoup plus complexes et nécessitent une configuration avant de pouvoir les utiliser en toute sécurité pour bloquer le trafic. Citrix recommande vivement que, plutôt que de tenter de configurer ces vérifications manuellement, vous activez la fonctionnalité d'apprentissage et lui permettez de générer les exceptions nécessaires.

Vérification des scripts inter-sites HTML

August 20, 2021

La vérification HTML Cross-Site Scripting (script inter-site) examine à la fois les en-têtes et les corps POST des requêtes utilisateur pour détecter d'éventuelles attaques de script inter-sites. S'il trouve un script intersite, il modifie (*transforme*) la requête pour rendre l'attaque inoffensive, ou bloque la requête.

> **Remarque :**
>
> La vérification de script inter-site HTML (script inter-site) ne fonctionne que pour le type de contenu, la longueur du contenu, etc. Cela ne fonctionne pas pour le cookie. Assurez-vous également que l'option « CheckRequestheAders » est activée dans votre profil de pare-feu d'application Web.

Vous pouvez empêcher l'utilisation abusive des scripts sur vos sites Web protégés en utilisant les scripts de script inter-site HTML qui enfreignent la *même règle d'origine*, qui stipule que les scripts ne doivent ni accéder ni modifier du contenu sur un serveur, sauf le serveur sur lequel ils se trouvent. Tout script qui enfreint la même règle d'origine est appelé script intersite, et la pratique consistant à utiliser des scripts pour accéder ou modifier du contenu sur un autre serveur est appelée script inter-site. La raison pour laquelle le script inter-site est un problème de sécurité est qu'un serveur Web qui autorise le script inter-site peut être attaqué avec un script qui ne se trouve pas sur ce serveur Web, mais sur un autre serveur Web, tel qu'un serveur détenu et contrôlé par l'attaquant.

Malheureusement, de nombreuses entreprises disposent d'une grande base installée de contenu Web amélioré par Javascript-qui viole la même règle d'origine. Si vous activez la vérification HTML Cross-Site Scripting sur un tel site, vous devez générer les exceptions appropriées afin que la vérification ne bloque pas l'activité légitime.

Le Web App Firewall offre diverses options d'action pour implémenter la protection HTML cross-site Scripting. En plus des actions **Block**, **Log**, **Stats**et **Apprendre**, vous avez également la possibilité de **transformer des scripts intersites**pour rendre une attaque inoffensive en codant les balises de script dans la demande soumise. Vous pouvez configurer Vérifier les URL complètes pour le paramètre de script inter-site pour spécifier si vous souhaitez inspecter non seulement les paramètres de requête, mais l'URL entière pour détecter les attaques de script inter-sites. Vous pouvez configurer le paramètre **InspectQueryContentTypes** pour inspecter la partie requête de requête pour l'attaque de script inter-site pour les types de contenu spécifiques.

Vous pouvez déployer des relaxations pour éviter les faux positifs. Le moteur d'apprentissage du Web App Firewall peut fournir des recommandations pour la configuration des règles de relaxation.

Pour configurer une protection optimisée par script multisite HTML pour votre application, configurez l'une des actions suivantes :

- **Bloc**—Si vous activez le bloc, l'action de blocage est déclenchée si les balises de script intersite sont détectées dans la requête.
- **Journal** : si vous activez la fonction de journal, le contrôle HTML Cross-Site Scripting génère des messages de journal indiquant les actions qu'il effectue. Si le bloc est désactivé, un message de journal distinct est généré pour chaque en-tête ou champ de formulaire dans lequel la violation de script intersite a été détectée. Toutefois, un seul message est généré lorsque la demande est bloquée. De même, un message de journal par requête est généré pour l'opération de transformation, même lorsque les balises de script intersite sont transformées en plusieurs champs. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.
- **Statistiques** : si cette option est activée, la fonction de statistiques recueille des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si les demandes légitimes sont bloquées, vous

devrez peut-être revoir la configuration pour voir si vous devez configurer de nouvelles règles de relaxation ou modifier les règles existantes.

- **Learn**—Si vous n'êtes pas sûr des règles de relaxation qui conviennent parfaitement à votre application, vous pouvez utiliser la fonctionnalité d'apprentissage pour générer des recommandations de règles de script inter-site HTML basées sur les données apprises. Le moteur d'apprentissage du Web App Firewall surveille le trafic et fournit des recommandations d'apprentissage basées sur les valeurs observées. Pour obtenir un avantage optimal sans compromettre les performances, vous pouvez activer l'option d'apprentissage pendant une courte période afin d'obtenir un échantillon représentatif des règles, puis déployer les règles et désactiver l'apprentissage.
- **Transformer les scripts intersites** : si cette option est activée, le Web App Firewall apporte les modifications suivantes aux demandes qui correspondent à la vérification de script inter-site HTML :
  - Crochet d'angle gauche (<) à l'équivalent d'entité de caractères HTML (<)
  - Angle droit (>) à l'équivalent d'entité de caractères HTML (>)

Cela garantit que les navigateurs n'interprètent pas les balises html dangereuses, telles que `<script>`, et exécutent ainsi du code malveillant. Si vous activez à la fois la vérification et la transformation de l'en-tête de demande, tous les caractères spéciaux trouvés dans les en-têtes de requête sont également modifiés. Si les scripts de votre site Web protégé contiennent des fonctionnalités de script intersite, mais que votre site Web ne s'appuie pas sur ces scripts pour fonctionner correctement, vous pouvez désactiver le blocage et activer la transformation en toute sécurité. Cette configuration garantit qu'aucun trafic Web légitime n'est bloqué, tout en arrêtant toute attaque de script intersite potentielle.

- **Vérifiez les URL complètes pour les scripts inter-sites**. Si la vérification des URL complètes est activée, le Web App Firewall examine des URL entières pour les attaques de script inter-sites HTML au lieu de vérifier uniquement les parties de requête des URL.
- **Cochez les en-têtes de requête**. Si la vérification des en-têtes de requête est activée, le Web App Firewall examine les en-têtes des requêtes pour les attaques de script inter-sites HTML, au lieu de se contenter d'URL. Si vous utilisez l'interface graphique, vous pouvez activer ce paramètre dans l'onglet Paramètres du profil Pare-feu de l'application Web.
- **InspectQueryContentTypes**. Si l'inspection des requêtes de requête est configurée, le pare-feu d'application examine la requête des demandes d'attaques de script intersite pour les types de contenu spécifiques. Si vous utilisez l'interface graphique, vous pouvez configurer ce paramètre dans l'onglet Paramètres du profil Pare-feu de l'application.

> **Important :**
>
> Dans le cadre des modifications de diffusion en continu, le traitement du Web App Firewall des balises de script inter-site a changé. Cette modification s'applique aux versions 11.0 ultérieures.

> Cette modification est également pertinente pour les versions d'amélioration de 10.5.e qui prennent en charge le streaming côté demande. Dans les versions antérieures, la présence de crochets ouverts (<), or close bracket (>) ou de crochets ouverts et fermés (<>) était marquée comme violation de script inter-site. Le comportement a changé dans les versions qui incluent la prise en charge de la diffusion côté demande. Seul le caractère rapproché (>) n'est plus considéré comme une attaque. Les requêtes sont bloquées même lorsqu'un caractère entre crochets ouverts (<) est présent et est considéré comme une attaque. L'attaque de script inter-site est signalée.

Scripting inter-site Relaxations à grain fin

Le Web App Firewall vous permet d'exempter un champ de formulaire, un en-tête ou un cookie spécifique de la vérification de l'inspection des scripts intersites. Vous pouvez contourner complètement l'inspection d'un ou plusieurs de ces champs en configurant des règles de relaxation.

Le Web App Firewall vous permet d'implémenter une sécurité plus stricte en affinant les règles de relaxation. Une application peut nécessiter la flexibilité nécessaire pour autoriser des modèles spécifiques, mais la configuration d'une règle de relaxation pour contourner l'inspection de sécurité peut rendre l'application vulnérable aux attaques, car le champ cible est exempté de l'inspection pour tout modèle d'attaque de script intersite. La relaxation fine de script inter-site permet d'autoriser des attributs, des balises et des motifs spécifiques. Les autres attributs, balises et motifs sont bloqués. Par exemple, le Web App Firewall dispose actuellement d'un ensemble par défaut de plus de 125 modèles refusés. Étant donné que les pirates peuvent utiliser ces modèles dans des attaques de script intersites, le Web App Firewall les signale comme des menaces potentielles. Vous pouvez vous détendre un ou plusieurs modèles considérés comme sûrs pour l'emplacement spécifique. Le reste des modèles de script inter-sites potentiellement dangereux sont toujours vérifiés pour l'emplacement cible et continuent à déclencher les violations des contrôles de sécurité. Vous avez maintenant un contrôle beaucoup plus serré.

Les commandes utilisées dans les relaxations ont des paramètres facultatifs pour **Type de valeur** et **Expression de valeur**. Le type de valeur peut être laissé vide ou vous avez la possibilité de sélectionner **Balise**, **Attribut** ou **Motif**. Si vous laissez le type de valeur vide, le champ configuré de l'URL spécifiée est exempté de l'inspection de vérification de script inter-site. Si vous sélectionnez un type de valeur, vous devez fournir une expression de valeur. Vous pouvez spécifier si l'expression de valeur est une expression régulière ou une chaîne littérale. Lorsque l'entrée est mise en correspondance avec la liste autorisée et refusée, seules les expressions spécifiées configurées dans les règles de relaxation sont exemptées.

Le Web App Firewall comporte les listes intégrées suivantes de scripts inter-sites :

1. **script inter-site Attributs autorisés** : Il existe 52 attributs autorisés par défaut, tels que, **abbr**, **accesskey**, **align**, **alt**, **axis**, **bgcolor**, **border**, **cell padding**, **cell spacing**, **char**, **charoff**, **charset** et ainsi de suite

2. **script inter-site balises autorisées** : Il y a 47 balises autorisées par défaut, telles que, **address**, **basefont**, **bgsound**, **big**, **blockquote**, **bg**, **br**, **légende**, **center**, ****cite,** ****dd**, **del** et ainsi de suite
3. **Script inter-site Refusé Patterns** : Il y a 129 modèles refusés par défaut, tels que, **FSCommand**, **javascript :**, **OnAbort**, **OnActivate** et ainsi de suite

> **Avertissement**
>
> Les URL d'action du Web App Firewall sont des expressions régulières. Lorsque vous configurez des règles de relaxation de script inter-site HTML, vous pouvez spécifier **Nom**et **Expression de valeur**comme étant littérale ou RegEx. Les expressions régulières sont puissantes. Surtout si vous n'êtes pas familier avec les expressions régulières au format PCRE, vérifiez les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement la règle que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation négligente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (.*), peut avoir des résultats que vous ne voulez pas, comme bloquer l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification de script inter-site HTML aurait autrement bloquée.

Points à considérer :

- L'expression de valeur est un argument facultatif. Un nom de champ peut ne pas avoir d'expression de valeur.
- Un nom de champ peut être lié à plusieurs expressions de valeur.
- Un type de valeur doit être affecté aux expressions de valeur. Le type de valeur de script inter-site peut être : 1) Tag, 2) Attribut ou 3) Pattern.
- Vous pouvez avoir plusieurs règles de relaxation par combinaison nom/URL de champ
- Les noms des champs de formulaire et les URL d'action ne sont pas sensibles à la casse.

Utilisation de la ligne de commande pour configurer la vérification HTML cross-site Scripting

Pour configurer les actions de vérification HTML Cross-Site Scripting et d'autres paramètres à l'aide de la ligne de commande

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer les commandes suivantes pour configurer la vérification de script inter-site HTML :

- set appfw profile « Descriptions des paramètres fournies en bas de la page. «)
- `<name> -crossSiteScriptingAction (([block] [learn] [log] [stats])| [** none**])`
- set appfw profile « Descriptions des paramètres fournies en bas de la page. «)
- `<name> **-crossSiteScriptingTransformUnsafeHTML** (ON | OFF)`
- Définissez le profil appfw Descriptions des paramètres fournies en bas de la page.

- <name> -crossSiteScriptingCheckCompleteURLs (ON | OFF)
- Définissez le profil appfw Descriptions des paramètres fournies en bas de la page.
- <name> - checkRequestHeaders (ON | OFF) Description des paramètres fournie en bas de la page."
- <name> - CheckRequestQueryNonHtml (ON | OFF) Description des paramètres fournie en bas de la page."

Pour configurer une règle de relaxation de script inter-site HTML à l'aide de la ligne de commande

Utilisez la commande bind ou unbind pour ajouter ou supprimer une liaison, comme suit :

- bind appfw profile <name> -crossSiteScripting <String> [isRegex (REGEX | NOTREGEX)] <formActionURL> [-location <location>] [-valueType (Tag|Attribute|Pattern)[<valueExpression>] [-isValueRegex (REGEX | NOTREGEX)]]
- unbind appfw profile <name> -crossSiteScripting <String> <formActionURL> [-location <location>] [-valueType (Tag |Attribute|Pattern)[<valueExpression>]]

Utilisation de l'interface graphique pour configurer la vérification des scripts entre sites HTML

Dans l'interface graphique, vous pouvez configurer la vérification HTML Cross-Site Scripting dans le volet du profil associé à votre application.

Pour configurer ou modifier la vérification HTML Cross-Site Scripting à l'aide de l'interface graphique

1. Accédez à **Application Pare-feu** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Vérifications de sécurité**.

La table de vérification de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Vous avez 2 options de configuration :

a. Si vous souhaitez activer ou désactiver les actions de **blocage**, de **journal**, de **statistiques**et d' **apprentissage** pour le script inter-site HTML, vous pouvez cocher ou désactiver les cases à cocher dans le tableau, cliquez sur **OK**, puis cliquez sur **Enregistrer et fermer** pour fermer le **Volet de vérification de la sécurité**.

b. Si vous souhaitez configurer d'autres options pour cette vérification de sécurité, double-cliquez sur **HTML Inter-Site Scripting**ou sélectionnez la ligne et cliquez sur **Paramètres d'action**pour afficher les options suivantes :

Transformer des scripts intersites—Transformer des balises de script non sécurisées.

Vérifier les URL complètes pour les scripts inter-sites : au lieu de vérifier uniquement la partie requête de l'URL, vérifiez l'URL complète pour les violations de script inter-sites.

Après avoir modifié l'un des paramètres ci-dessus, cliquez sur **OK** pour enregistrer les modifications et revenir au tableau Vérifications de sécurité. Vous pouvez procéder à la configuration d'autres vérifications de sécurité si nécessaire. Cliquez sur **OK** pour enregistrer toutes les modifications que vous avez apportées dans la section Contrôles de sécurité, puis cliquez sur **Enregistrer et fermer pour fermer** le volet de vérification de la sécurité.

Pour activer ou désactiver le paramètre **Vérifier l'en-tête de demande**, dans le volet **Paramètres avancés**, cliquez sur **Paramètres du profil**. Dans **Paramètres communs**, activez ou désactivez la case à **cocher Vérifier les en-têtes de demande**. Cliquez sur **OK**. Vous pouvez utiliser l'icône X en haut à droite du volet Paramètres du profil pour fermer cette section ou, si vous avez terminé la configuration de ce profil, vous pouvez cliquer sur **Terminé** pour revenir à **Application Pare-feu** > **Profil**.

Pour activer ou désactiver le paramètre **Vérifier la requête Requête non HTML**, dans le volet **Paramètres avancés**, cliquez sur **Paramètres du profil**. Dans **Paramètres communs**, Activez ou désactivez la **case à cocher Requête non HTML de requête**. Cliquez sur **OK**. Vous pouvez utiliser l'icône X en haut à droite du volet **Paramètres du profil** pour fermer cette section ou, si vous avez terminé de configurer ce profil, vous pouvez cliquer sur **Terminé** pour revenir au **pare-feu de l'application > Profil**.

Pour configurer une règle de relaxation de script inter-site HTML à l'aide de l'interface graphique

1. Accédez à **Application Pare-feu** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
3. Dans le tableau Règles de relaxation, double-cliquez sur l'entrée **HTML Cross-Site Scripting**, ou sélectionnez-la et cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Règles de relaxation de script inter-site HTML**, effectuez les opérations **Ajouter**, **Modifier**, **Supprimer**, **Activer** ou **Désactiver** pour les règles de relaxation.

> **Remarque**
>
> Lorsque vous ajoutez une nouvelle règle, le champ **Expression de valeur** n'est pas affiché, sauf si vous sélectionnez l'option **Balise** ou **Attribut** ou **Modèle** dans le champ **Type de valeur**.

Pour gérer les règles de relaxation HTML Cross-Site Scripting à l'aide du visualiseur

Pour obtenir une vue consolidée de toutes les règles de relaxation, vous pouvez mettre en surbrillance la ligne **HTML Cross-Site Scripting** dans le tableau Règles de relaxation, puis cliquer sur **Visualiseur**. Le visualiseur pour les relaxations déployées vous offre la possibilité d' **ajouter** une nouvelle règle ou de **modifier** une règle existante. Vous pouvez également **activer** ou **désactiver** un groupe de règles en sélectionnant un nœud et en cliquant sur les boutons correspondants dans le visualiseur de relaxation.

Pour afficher ou personnaliser les modèles de script inter-site à l'aide de l'interface graphique

Vous pouvez utiliser l'interface graphique pour afficher ou personnaliser la liste par défaut des at-

tributs autorisés de script intersite ou des balises autorisées. Vous pouvez également afficher ou personnaliser la liste par défaut des motifs refusés de script inter-site.

Les listes par défaut sont spécifiées dans **Application Firewall** > **Signatures > Signaturespar défaut**. Si vous ne liez aucun objet signature à votre profil, la liste de scripts intersites par défaut autorisée et refusée spécifiée dans l'objet Signatures par défaut sera utilisée par le profil pour le traitement du contrôle de sécurité Cross-Site Scripting. Les balises, attributs et motifs, spécifiés dans l'objet signatures par défaut, sont en lecture seule. Vous ne pouvez pas les modifier ou les modifier. Si vous souhaitez les modifier ou les modifier, effectuez une copie de l'objet Signatures par défaut pour créer un objet signature définie par l'utilisateur. Modifiez les listes autorisées ou refusées dans le nouvel objet de signature défini par l'utilisateur et utilisez cet objet de signature dans votre profil qui traite le trafic pour lequel vous souhaitez utiliser ces listes personnalisées autorisées et refusées.

1. Pour afficher les modèles de script intersite par défaut :

a. Accédez à **Application Pare-feu** > **Signatures**, sélectionnez **Signatures par défaut**, puis cliquez sur **Modifier**. Ensuite, cliquez sur **Gérer les modèles de script SQL/inter-site**.

Le tableau **Gérer les chemins de script SQL/inter-site** présente les trois lignes suivantes relatives au script inter-site :

`xss/allowed/attribute`

`xss/allowed/tag`

`xss/denied/pattern`

b. Sélectionnez une ligne et cliquez sur **Gérer les éléments** pour afficher les éléments de script intersite correspondants (balise, attribut, motif) utilisés par la vérification de **script inter-site du** Web App Firewall.

1. **Pour personnaliser des éléments de script inter-sites** : vous pouvez modifier l'objet de signature défini par l'utilisateur pour personnaliser la balise autorisée, les attributs autorisés et les motifs refusés. Vous pouvez ajouter de nouvelles entrées ou supprimer celles qui existent déjà.

a. Accédez à **Application Pare-feu** > **Signatures**, mettez en surbrillance la signature définie par l'utilisateur cible, puis cliquez sur **Modifier**. Cliquez sur **Gérer les modèles de script SQL/inter-sites** pour afficher la table **Gérer les chemins de script SQL/inter-site**.

b. Sélectionnez la ligne cible de script inter-site.

i. Cliquez sur **Gérer les éléments**pour **ajouter**, **modifier** ou **supprimer** l'élément de script inter-site correspondant.

ii. Cliquez sur **Supprimer** pour supprimer la ligne sélectionnée.

> **Avertissement :**
>
> Vous devez être prudent avant de supprimer ou de modifier tout élément de script inter-site par

> défaut, ou de supprimer le chemin de script inter-site pour supprimer la ligne entière. Les règles de signature et le contrôle de sécurité des scripts inter-sites reposent sur ces éléments pour détecter les attaques afin de protéger vos applications. La personnalisation du script inter-site Elements peut rendre votre application vulnérable aux attaques de script inter-site si le modèle requis est supprimé lors de la modification.

Utilisation de la fonctionnalité d'apprentissage avec la vérification de script inter-site HTML

Lorsque l'action « apprendre » est activée, le moteur d'apprentissage Citrix Web App Firewall surveille le trafic et apprend les violations des URL de script inter-sites. Vous pouvez inspecter périodiquement les règles d'URL de script intersite et les déployer pour détecter les scénarios de faux positifs.

> **Remarque :**
>
> Dans une configuration de cluster, tous les nœuds doivent être de la même version pour déployer les règles d'URL de script inter-site.

Amélioration de l'apprentissage des scripts inter-sites HTML. Une amélioration de l'apprentissage du Web App Firewall a été introduite dans la version 11.0 du logiciel Citrix ADC. Pour déployer une relaxation de script cross-site HTML à grain fin, le Web App Firewall offre un apprentissage de script cross-site HTML à grain fin. Le moteur d'apprentissage formule des recommandations concernant le type de valeur observé (balise, attribut, modèle) et l'expression de valeur correspondante observée dans les champs de saisie. En plus de vérifier les demandes bloquées pour déterminer si la règle actuelle est trop restrictive et doit être assouplie, vous pouvez consulter les règles générées par le moteur d'apprentissage pour déterminer quels types de valeur et expressions de valeur déclenchent des violations et doivent être traitées dans les règles de relaxation.

> **Remarque :**
>
> Le moteur d'apprentissage de Web App Firewall ne peut distinguer que les 128 premiers octets du nom. Si un formulaire comporte plusieurs champs dont les noms correspondent aux 128 premiers octets, le moteur d'apprentissage peut ne pas être en mesure de les distinguer. De même, la règle de relaxation déployée peut par inadvertance relâcher tous ces champs de l'inspection HTML Cross-Site Scripting.
> **Conseil**
>
> Les balises de script inter-sites qui contiennent plus de 12 caractères ne sont pas apprises ou enregistrées correctement.
>
> Si vous avez besoin d'une plus grande longueur de balise pour l'apprentissage, vous pouvez ajouter une grande balise n'apparaissant pas dans **AS_Cross-Site Scripting_Allowed_tags_list** pour la longueur 'x'.

Pour afficher ou utiliser les données apprises à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `show appfw learningdata <profilename> crossSiteScripting`
- `rm appfw learningdata <profilename> -crossSiteScripting <string> <formActionURL> [<location>] [<valueType> <valueExpression>]`
- `export appfw learningdata <profilename> **crossSiteScripting*`

Pour afficher ou utiliser les données apprises à l'aide de l'interface graphique

1. Accédez à **Application Pare-feu** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles apprises**. Vous pouvez sélectionner l'entrée **HTML Cross-Site Scripting** dans le tableau Règles apprises et double-cliquer dessus pour accéder aux règles apprises. Le tableau affiche les colonnes **Nom du champ**,**URL A ction**, **Type**de **valeur, Valeur**et **Hits** . Vous pouvez déployer les règles apprises ou modifier une règle avant de la déployer en tant que règle de relaxation. Pour ignorer une règle, vous pouvez la sélectionner et cliquer sur le bouton **Ignorer**. Vous ne pouvez modifier qu'une seule règle à la fois, mais vous pouvez sélectionner plusieurs règles à déployer ou à ignorer.

Vous avez également la possibilité d'afficher une vue résumée des relaxations apprises en sélectionnant l'entrée **HTML Cross-Site Scripting** dans le tableau Règles apprises et en cliquant sur **Visualiseur** pour obtenir une vue consolidée de toutes les violations apprises. Le visualiseur facilite la gestion des règles apprises. Il présente une vue complète des données sur un seul écran et facilite l'action sur un groupe de règles en un seul clic. Le plus grand avantage du visualiseur est qu'il recommande des expressions régulières pour consolider plusieurs règles. Vous pouvez sélectionner un sous-ensemble de ces règles, en fonction du délimiteur et de l'URL Action. Vous pouvez afficher 25, 50 ou 75 règles dans le visualiseur, en sélectionnant le nombre dans une liste déroulante. Le visualiseur des règles apprises offre la possibilité de modifier les règles et de les déployer en tant que relaxations. Ou vous pouvez ignorer les règles pour les ignorer.

Utilisation de la fonctionnalité de journal avec la vérification des scripts inter-sites HTML

Lorsque l'action de journalisation est activée, les violations de vérification de sécurité des scripts inter-sites HTML sont enregistrées dans le journal d'audit en tant que violations de **script AppFW_Cross-site**. Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur syslog distant.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Basculez vers l'interpréteur de commandes et queue les ns.logs dans le `/var/log/` dossier pour accéder aux messages de journal relatifs aux violations de script inter-site HTML :


```
Shell
tail -f /var/log/ns.log | grep APPFW_cross-site scripting
```

Exemple d'un message de journal des violations de vérification de sécurité de script inter-site au format de journal CEF :

```
1 Jul 11 00:45:51 <local0.info> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
     .0|APPFW|\*\*APPFW_cross-site scripting\*\*|6|src=10.217.253.62
     geolocation=Unknown spt=4840 method=GET request=http://aaron.
     stratum8.net/FFC/CreditCardMind.html?abc=%3Cdef%3E msg=\*\*Cross-
     site script check failed for field abc="Bad tag: def"\*\* cn1=133
     cn2=294 cs1=pr_ffc cs2=PPE1 cs3=eUljypvLa0BbabwfGVE52Sewg9U0001 cs4=
     ALERT cs5=2015 act=\*\*not blocked\*\*
2 <!--NeedCopy-->
```

Exemple d'un message de journal de violation de vérification de sécurité Cross-Site Scripting au format journal natif montrant une action de transformation

```
1 Jul 11 01:00:28 <local0.info> 10.217.31.98 07/11/2015:01:00:28 GMT ns
     0-PPE-0 : default APPFW \*\*APPFW_cross-site scripting\*\* 132 0 :
     10.217.253.62 392-PPE0 eUljypvLa0BbabwfGVE52Sewg9U0001 pr_ffc http:
     //aaron.stratum8.net/FFC/login.php?login_name=%3CBOB%3E&passwd=&
     drinking_pref=on &text_area=&loginButton=ClickToLogin&as_sfid=
     AAAAAAVFqmYL68IGvkrcn2pzehjfIkm5E6EZ9FL8YLvIW_41AvAATuKYe9N7uGThSpEAxbb0iBx55j
     -FC4llF \*\*Cross-site script special characters seen in fields <
     transformed>\*\*
2 <!--NeedCopy-->
```

Accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique Citrix inclut un outil utile (Syslog Viewer) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez au **pare-feu des applications** > **Profils**, sélectionnez le profil cible et cliquez sur **Vérifications de sécurité**. Mettez en surbrillance la ligne **HTML Cross-Site Scripting**, puis cliquez sur **Journaux**. Lorsque vous accédez aux journaux directement à partir de la vérification HTML Cross-Site Scripting du profil, l'interface graphique filtre les messages de journal et affiche uniquement les journaux relatifs à ces violations de vérification de sécurité.
- Vous pouvez également accéder à la visionneuse Syslog en accédant à **Citrix ADC** > **Système** > **Audit**. Dans la section **Messages d'audit**, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation des contrôles de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de vérification de sécurité peuvent être déclenchées pendant le traitement de la demande.

- Accédez à **Application Firewall** > **Stratégies** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation des contrôles de sécurité.

La visionneuse Syslog basée sur HTML fournit diverses options de filtre pour sélectionner uniquement les messages de journal qui vous intéressent. Pour sélectionner les messages de journalisation pour la vérification de **script inter-site HTML**, filtrez en sélectionnant **APPFW** dans les options de la liste déroulante pour **Module**. La liste **Type d'événement** offre un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous activez la case à cocher **AppFW_Inter-Site Script** et que vous cliquez sur le bouton **Appliquer**, seuls les messages relatifs aux violations de vérification de sécurité des scripts inter-sites HTML apparaissent dans la visionneuse Syslog.

Si vous placez le curseur dans la ligne d'un message de journal spécifique, plusieurs options, telles que **Module**, **Type d'événement**, **ID d'événement**, **adresse IP du client**, etc., apparaissent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans le message de journal.

Cliquez sur pour Déployer la fonctionnalité est disponible uniquement dans l'interface graphique. Vous pouvez utiliser la visionneuse Syslog non seulement pour afficher les journaux, mais aussi pour déployer des règles de relaxation HTML Cross-Site Scripting basées sur les messages de journal pour les violations de vérification de sécurité du Web App Firewall. Les messages de journal doivent être au format de journal CEF pour cette opération. Cliquez pour déployer la fonctionnalité est disponible uniquement pour les messages de journal générés par l'action Bloquer (ou non bloquer). Vous ne pouvez pas déployer une règle de relaxation pour un message de journal concernant l'opération de transformation.

Pour déployer une règle de relaxation à partir de la visionneuse Syslog, sélectionnez le message de journal. Une case à cocher s'affiche dans le coin supérieur droit de la case Visionneuse Syslog de la ligne sélectionnée. Activez la case à cocher, puis sélectionnez une option dans la liste **Action** pour déployer la règle de relaxation. **Modifier et déployer**, **déployer**et **déployer tout**sont disponibles en tant qu'options **Action**.

Les règles de script inter-site HTML déployées à l'aide de l'option **Cliquez pour déployer** n'incluent pas les recommandations de relaxation du grain fin.

Configurer le clic pour déployer la fonctionnalité à l'aide de l'interface graphique

1. Dans la visionneuse Syslog, sélectionnez **APPFW** dans les options du **module** .
2. Sélectionnez le **script App_cross-site** comme **Type d'événement** pour filtrer les messages de journal correspondants.
3. Activez la case à cocher pour identifier la règle à déployer.
4. Utilisez la liste déroulante d'options **Action** pour déployer la règle de relaxation.
5. Vérifiez que la règle apparaît dans la section Règle de relaxation correspondante.

Statistiques pour les violations de script inter-site HTML

Lorsque l'action des statistiques est activée, le compteur de la vérification HTML Cross-Site Scripting est incrémenté lorsque le Web App Firewall prend une action pour cette vérification de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. La taille d'un incrément du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, la demande d'une page contenant 3 violations de script inter-site HTML incrémente le compteur de statistiques d'un, car la page est bloquée dès que la première violation est détectée. Toutefois, si le bloc est désactivé, le traitement de la même demande incrémente le compteur de statistiques pour les violations et les journaux de trois, car chaque violation génère un message de journal distinct.

Pour afficher HTML Cross-Site Scripting, vérifiez les statistiques à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
> sh appfw stats
```

Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
> **stat appfw profile** <profile name>
```

Afficher les statistiques de script inter-sites HTML à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Pare-feu d'application > Profils > Statistiques**.
2. Dans le volet droit, accédez au lien **Statistiques**.
3. Utilisez la barre de défilement pour afficher les statistiques sur les violations et les journaux de script inter-site HTML. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Résumé

- Prise en**charge intégrée de la protection contre les attaques par script inter-site HTML** : Citrix Web App Firewall protège contre les attaques de script inter-site en surveillant une combinaison d'attributs et de balises autorisés et de modèles refusés dans la charge utile reçue. Toutes les balises autorisées par défaut intégrées, les attributs autorisés et les motifs refusés utilisés par la vérification des scripts inter-sites sont spécifiés dans le fichier /netscaler/default_custom_settings.xml.
- **Personnalisation** : vous pouvez modifier la liste par défaut de balises, d'attributs et de modèles pour personnaliser l'inspection de vérification de sécurité des scripts inter-site en fonction des besoins spécifiques de votre application. Effectuez une copie de l'objet signature par défaut, modifiez les entrées existantes ou ajoutez de nouvelles entrées. Liez cet objet signature à votre profil pour utiliser la configuration personnalisée.

- **Modèle de sécurité hybride** : les signatures et les protections de sécurité profondes utilisent les modèles de script SQL/cross-site spécifiés dans l'objet signature lié au profil. Si aucun objet de signature n'est lié au profil, les modèles de script SQL/cross-site présents dans l'objet signature par défaut sont utilisés.
- **Transform**—Notez ce qui suit à propos de l'opération de transformation :

L'opération de transformation fonctionne indépendamment des autres paramètres d'action de script inter-site. Si la transformation est activée et que le bloc, le journal, les statistiques et l'apprentissage sont tous désactivés, les balises de script intersite sont transformées.

Si l'action de blocage est activée, elle a priorité sur l'action de transformation.

- **Relaxation et apprentissage à grains fins**. Affinez la règle de relaxation pour relâcher un sous-ensemble d'éléments de script intersite de l'inspection de vérification de sécurité, mais détectez le reste. Le moteur d'apprentissage recommande un type de valeur spécifique et des expressions de valeur basées sur les données observées.
- **Cliquez pour déployer** : sélectionnez un ou plusieurs messages de journal des violations de script intersite dans la visionneuse syslog et déployez-les en tant que règles de relaxation.
- **Charset**—Le jeu de caractères par défaut du profil doit être défini en fonction des besoins de l'application. Par défaut, le jeu de caractères de profil est défini sur Anglais US (ISO-8859-1). Si une demande est reçue sans le jeu de caractères spécifié, le Web App Firewall traite la demande comme si elle était ISO-8859-1. Le caractère ouvert (<) or the close bracket character (>) ne sera pas interprété comme des balises de script inter-sites si ces caractères sont codés dans d'autres jeux de caractères. Par exemple, si une requête contient une chaîne de caractères UTF-8 "%uff1cscript%uff1e**"**mais que le jeu de caractères n'est pas spécifié sur la page de requête, la violation de script intersite peut ne pas être déclenchée sauf si le jeu de caractères par défaut du profil est spécifié comme Unicode.

Vérification par injection HTML SQL

August 20, 2021

De nombreuses applications Web ont des formulaires Web qui utilisent SQL pour communiquer avec des serveurs de bases de données relationnelles. Un code malveillant ou un pirate peut utiliser un formulaire Web non sécurisé pour envoyer des commandes SQL au serveur Web. La vérification HTML SQL Injection du Web App Firewall fournit des défenses spéciales contre l'injection de code SQL non autorisé qui pourrait briser la sécurité. Si le Web App Firewall détecte du code SQL non autorisé dans une demande utilisateur, il transforme la demande, rend le code SQL inactif ou bloque la demande. Le Web App Firewall examine la charge utile de la requête pour le code SQL injecté à trois emplacements : 1) corps POST, 2) en-têtes et 3) cookies. Pour examiner une partie de requête dans les demandes de

code SQL injecté, configurez un paramètre de profil de pare-feu d'application « InspectQueryContent-Types » pour les types de contenu spécifiques.

Un ensemble par défaut de mots-clés et de caractères spéciaux fournit des mots-clés connus et des caractères spéciaux couramment utilisés pour lancer des attaques SQL. Vous pouvez ajouter de nouveaux modèles et modifier le jeu par défaut pour personnaliser l'inspection de vérification SQL. Le Web App Firewall offre diverses options d'action pour implémenter la protection SQL Injection. En plus des actions **Block**, **Log**, **Stats**et **Learn**, le profil Web App Firewall offre également la possibilité de **transformer des caractères spéciaux SQL**pour rendre une attaque inoffensive.

En plus des actions, il existe plusieurs paramètres qui peuvent être configurés pour le traitement par injection SQL. Vous pouvez vérifier les **caractères génériques SQL**. Vous pouvez modifier le type d'injection SQL et sélectionner l'une des 4 options (**SQLKeyword**, **SQLSplChar**, **SQLSplCharAND-Keyword**, **SQLSplCharORKeyword**) pour indiquer comment évaluer les mots-clés SQL et les caractères spéciaux SQL lors du traitement de la charge utile. Le **paramètre SQL Comments Handling** vous permet de spécifier le type de commentaires qui doivent être inspectés ou exemptés lors de la détection SQL Injection.

Vous pouvez déployer des relaxations pour éviter les faux positifs. Le moteur d'apprentissage du Web App Firewall peut fournir des recommandations pour la configuration des règles de relaxation.

Les options suivantes sont disponibles pour configurer une protection SQL Injection optimisée pour votre application :

Block—L'action de bloc n'est déclenchée que si l'entrée correspond à la spécification de type d'injection SQL. Par exemple, si **SQLSplCharANDKeyword** est configuré comme type d'injection SQL, une requête n'est pas bloquée si elle ne contient pas de mots-clés, même si des caractères spéciaux SQL sont détectés dans l'entrée. Une telle requête est bloquée si le type d'injection SQL est défini sur **SQLSplChar**ou **SQLSplCharORKeyword**.

Log—Si vous activez la fonction de journal, la vérification SQL Injection génère des messages de journal indiquant les actions qu'elle effectue. Si l'action de blocage est désactivée, un message de journal distinct est généré pour chaque champ de saisie dans lequel la violation SQL a été détectée. Toutefois, un seul message est généré lorsque la demande est bloquée. De même, un message de journal par requête est généré pour l'opération de transformation, même lorsque des caractères spéciaux SQL sont transformés dans plusieurs champs. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.

Statistiques : si cette option est activée, la fonction de statistiques recueille des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si des demandes légitimes sont bloquées, vous devrez peut-être revoir la configuration pour voir si vous devez configurer de nouvelles règles de relaxation ou modifier celles existantes.

Learn—Si vous n'êtes pas sûr des règles de relaxation SQL qui conviennent parfaitement à votre application, vous pouvez utiliser la fonctionnalité learn pour générer des recommandations basées sur les données apprises. Le moteur d'apprentissage du Web App Firewall surveille le trafic et fournit des recommandations d'apprentissage SQL basées sur les valeurs observées. Pour obtenir un avantage optimal sans compromettre les performances, vous pouvez activer l'option d'apprentissage pendant une courte période afin d'obtenir un échantillon représentatif des règles, puis déployer les règles et désactiver l'apprentissage.

Transformer les caractères spéciaux SQL : le Web App Firewall considère trois caractères : guillemets simples (‘), barre oblique inverse () et point-virgule (;) comme caractères spéciaux pour le traitement des vérifications de sécurité SQL. La fonction de transformation SQL modifie le code d'injection SQL dans une requête HTML pour s'assurer que la requête est rendue inoffensive. La requête HTML modifiée est ensuite envoyée au serveur. Toutes les règles de transformation par défaut sont spécifiées dans le fichier /netscaler/default_custom_settings.xml.

L'opération de transformation rend le code SQL inactif en apportant les modifications suivantes à la demande :

- Citation simple (‘) à double citation droite (“).
- Inversible () à double barre oblique inverse ().
- Le point-virgule (;) est supprimé complètement.

Ces trois caractères (chaînes spéciales) sont nécessaires pour émettre des commandes à un serveur SQL. À moins qu'une commande SQL ne soit précédée d'une chaîne spéciale, la plupart des serveurs SQL ignorent cette commande. Par conséquent, les modifications effectuées par le Web App Firewall lorsque la transformation est activée empêchent un attaquant d'injecter du SQL actif. Une fois ces modifications apportées, la demande peut être transmise en toute sécurité à votre site Web protégé. Lorsque les formulaires Web de votre site Web protégé peuvent légitimement contenir des chaînes spéciales SQL, mais que les formulaires Web ne dépendent pas des chaînes spéciales pour fonctionner correctement, vous pouvez désactiver le blocage et activer la transformation pour empêcher le blocage des données de formulaire Web légitimes sans réduire la protection que l'application Web Le pare-feu fournit à vos sites Web protégés.

L'opération de transformation fonctionne indépendamment du paramètre **SQL Injection Type** . Si la transformation est activée et que le type d'injection SQL est spécifié comme mot-clé SQL, les caractères spéciaux SQL sont transformés même si la requête ne contient aucun mot-clé.

> **Conseil**
>
> Vous activez normalement la transformation ou le blocage, mais pas les deux. Si l'action de blocage est activée, elle a priorité sur l'action de transformation. Si le blocage est activé, l'activation de la transformation est redondante.

Vérifier les caractères génériques SQL —Lescaractères génériques peuvent être utilisés pour élargir les sélections d'une instruction SQL (SQL-SELECT). Ces opérateurs de caractères génériques

peuvent être utilisés avec des opérateurs **LIKEet NOT** LIKE pour comparer une valeur à des valeurs similaires. Le pourcentage (%) et le trait de soulignement (_) sont fréquemment utilisés comme caractères génériques. Le signe de pourcentage est analogue au caractère générique astérisque (*) utilisé avec MS-DOS et correspond à zéro, un ou plusieurs caractères dans un champ. Le trait de soulignement est similaire au point d'interrogation MS-DOS (?) caractère générique. Il correspond à un nombre ou un caractère unique dans une expression.

Par exemple, vous pouvez utiliser la requête suivante pour effectuer une recherche de chaîne pour rechercher tous les clients dont les noms contiennent le caractère D.

SELECT * from customer WHERE name like "%D%":

L'exemple suivant combine les opérateurs pour rechercher les valeurs de salaire qui ont 0 en deuxième et troisième place.

SELECT * from customer WHERE salary like '_00%':

Différents fournisseurs de SGBD ont étendu les caractères génériques en ajoutant des opérateurs supplémentaires. Le Citrix Web App Firewall peut se protéger contre les attaques lancées en injectant ces caractères génériques. Les 5 caractères génériques par défaut sont le pourcentage (%), le trait de soulignement (_), le caret (^), le crochet d'ouverture ([) et le crochet de fermeture (]). Cette protection s'applique aux profils HTML et XML.

Les caractères génériques par défaut sont une liste de littéraux spécifiés dans ***Signatures par défaut** :

- `<wildchar type=" LITERAL" >%</wildchar>`
- `<wildchar type=" LITERAL" >_</wildchar>`
- `<wildchar type=" LITERAL" >^</wildchar>`
- `<wildchar type=" LITERAL" >[</wildchar>`
- `<wildchar type=" LITERAL" >]</wildchar>`

Les caractères génériques d'une attaque peuvent être PCRE, comme [^A-F]. Le Web App Firewall prend également en charge les caractères génériques PCRE, mais les caractères génériques littéraux ci-dessus sont suffisants pour bloquer la plupart des attaques.

> **Remarque :**
>
> La vérification des caractères génériques SQL est différente de la vérification des caractères spéciaux SQL. Cette option doit être utilisée avec prudence pour éviter les faux positifs.

Check Request Contenant le type d'injection SQL : le Web App Firewall fournit 4 options pour implémenter le niveau de rigueur souhaité pour l'inspection SQL Injection, en fonction des besoins individuels de l'application. La demande est vérifiée par rapport à la spécification de type d'injection pour détecter les violations SQL. Les 4 options de type d'injection SQL sont les suivantes :

- **Caractère spécial SQL et mot-clé** : un mot-clé SQL et un caractère spécial SQL doivent être

présents dans l'entrée pour déclencher une violation SQL. Ce paramètre le moins restrictif est également le paramètre par défaut.

- **Caractère spécial SQL** : au moins un des caractères spéciaux doit être présent dans l'entrée pour déclencher la violation SQL.
- **Mot-clé SQL**—Au moins un des mots-clés SQL spécifiés doit être présent dans l'entrée pour déclencher une violation SQL. Ne sélectionnez pas cette option sans considération. Pour éviter les faux positifs, assurez-vous qu'aucun des mots-clés n'est attendu dans les entrées.
- **Caractère spécial SQL ou mot-clé** : le mot clé ou la chaîne de caractères spéciaux doit être présent dans l'entrée pour déclencher la violation de vérification de sécurité.

> **Conseil :**
>
> Si vous configurez le Web App Firewall pour rechercher les entrées contenant un caractère spécial SQL, le pare-feu Web App ignore les champs de formulaire Web qui ne contiennent pas de caractères spéciaux. Étant donné que la plupart des serveurs SQL ne traitent pas les commandes SQL qui ne sont pas précédées d'un caractère spécial, l'activation de cette option peut réduire considérablement la charge sur le Web App Firewall et accélérer le traitement sans mettre vos sites Web protégés en danger.

Gestion des commentaires SQL : par défaut, le Web App Firewall vérifie tous les commentaires SQL pour les commandes SQL injectées. De nombreux serveurs SQL ignorent quoi que ce soit dans un commentaire, même s'ils sont précédés d'un caractère spécial SQL. Pour un traitement plus rapide, si votre serveur SQL ignore les commentaires, vous pouvez configurer le Web App Firewall pour ignorer les commentaires lors de l'examen des demandes de SQL injecté. Les options de gestion des commentaires SQL sont les suivantes :

- **ANSI**—Ignorer les commentaires SQL au format ANSI, qui sont normalement utilisés par les bases de données SQL UNIX. Par exemple :
  - — (Deux traits d'union) - Il s'agit d'un commentaire qui commence par deux traits d'union et se termine par la fin de la ligne.
  - {} - Accolades (Les accolades enferment le commentaire. La { précède le commentaire, et la } le suit. Les accolades peuvent délimiter les commentaires à une ou plusieurs lignes, mais les commentaires ne peuvent pas être imbriqués)
  - `/**/: C style comments (Does not allow nested comments). Please note /*! <comment that begin with slash followed by asterisk and exclamation mark is not a comment > */`
  - MySQL Server prend en charge certaines variantes de commentaires de style C. Ceux-ci vous permettent d'écrire du code qui inclut des extensions MySQL, mais qui est toujours portable, en utilisant les commentaires de la forme suivante : `/*! MySQL-specific code */`
  - . # : Commentaires Mysql : Il s'agit d'un commentaire qui commence par # caractère.
- **Imbriqué**—Ignorer les commentaires SQL imbriqués, qui sont normalement utilisés par

Microsoft SQL Server. Par exemple ; — (Deux traits d'union) et **/* */** (Autorise les commentaires imbriqués)

- **ANSI/imbriqué**—Ignorer les commentaires qui respectent les normes ANSI et SQL de commentaires imbriqués. Les commentaires qui correspondent uniquement à la norme ANSI, ou uniquement à la norme imbriquée, sont toujours vérifiés pour le SQL injecté.
- **Check all Comments**—Vérifiez l'intégralité de la requête pour SQL injecté sans sauter quoi que ce soit. C'est le réglage par défaut.

> **Conseil**
>
> Habituellement, vous ne devez pas choisir l'option imbriquée ou l'option ANSI/imbriquée, sauf si votre base de données principale s'exécute sur Microsoft SQL Server. La plupart des autres types de logiciels SQL Server ne reconnaissent pas les commentaires imbriqués. Si des commentaires imbriqués apparaissent dans une requête dirigée vers un autre type de serveur SQL, ils peuvent indiquer une tentative de violation de la sécurité sur ce serveur.

Vérifier les en-têtes de demande : activez cette option si, en plus d'examiner l'entrée dans les champs de formulaire, vous souhaitez examiner les en-têtes de demande pour les attaques HTML SQL Injection. Si vous utilisez l'interface graphique, vous pouvez activer ce paramètre dans le volet **Paramètres avancés -> Paramètres** de **profil** du profil Pare-feu de l'application Web.

> **Remarque :**
>
> Si vous activez l'indicateur d'en-tête Check Request, vous devrez peut-être configurer une règle de relaxation pour l'en-tête **User-Agent** . La présence du mot-clé SQL **like** et du caractère spécial SQL point-virgule (**;**) peut déclencher des requêtes fausses positives et bloquer qui contiennent cet en-tête.
>
> **Avertissement**
>
> Si vous activez à la fois la vérification et la transformation des en-têtes de requête, tous les caractères spéciaux SQL présents dans les en-têtes sont également transformés. Les en-têtes Accept, Accept-Charset, Accept-Encoding, Accept-Language, Expect et User-Agent contiennent normalement des points-virgules (;). L'activation simultanée de la vérification des en-têtes de demande et de la transformation peut entraîner des erreurs.

InspectQueryContentTypes : configurez cette option si vous souhaitez examiner la partie requête pour les attaques SQL Injection pour les types de contenu spécifiques. Si vous utilisez l'interface graphique, vous pouvez configurer ce paramètre dans le volet **Paramètres avancés -> Paramètres** du **profil** du profil Pare-feu de l'application.

SQL Relaxations à grain fin

Le Web App Firewall vous permet d'exempter un champ de formulaire, un en-tête ou un cookie spécifique de la vérification d'inspection SQL Injection. Vous pouvez complètement contourner

l'inspection d'un ou de plusieurs de ces champs en configurant les règles de relaxation pour la vérification SQL Injection.

Le Web App Firewall vous permet d'implémenter une sécurité plus stricte en affinant les règles de relaxation. Une application peut nécessiter la flexibilité nécessaire pour autoriser des modèles spécifiques, mais la configuration d'une règle de relaxation pour contourner l'inspection de sécurité peut rendre l'application vulnérable aux attaques, car le champ cible est exempté de l'inspection pour tout modèle d'attaque SQL. La relaxation à grain fin SQL fournit la possibilité d'autoriser des motifs spécifiques et de bloquer le reste. Par exemple, le Web App Firewall dispose actuellement d'un ensemble par défaut de plus de 100 mots-clés SQL. Étant donné que les pirates peuvent utiliser ces mots-clés dans des attaques SQL Injection, le Web App Firewall les signale comme des menaces potentielles. Vous pouvez détendre un ou plusieurs mots-clés considérés comme sûrs pour un emplacement spécifique. Le reste des mots-clés SQL potentiellement dangereux sont toujours vérifiés pour l'emplacement cible et continuent de déclencher les violations de vérification de sécurité. Vous avez maintenant un contrôle beaucoup plus serré.

Les commandes utilisées dans les relaxations ont des paramètres facultatifs pour **Type de valeur** et **Expression de valeur**. Vous pouvez spécifier si l'expression de valeur est une expression régulière ou une chaîne littérale. Le type de valeur peut être laissé vide ou vous avez une option pour sélectionner **Mot-clé** ou **SpecialString** ou **WildChar**.

> **Avertissement :**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas familier avec les expressions régulières au format PCRE, vérifiez les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement l'URL que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation imprudente des caractères génériques, et en particulier du métacaractère d'astérisque de points (.*) ou de la combinaison de caractères génériques, peut avoir des résultats que vous ne souhaitez pas, tels que le blocage de l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification d'injection HTML SQL aurait autrement bloquée.

Points à considérer :

- L'expression de valeur est un argument facultatif. Un nom de champ peut ne pas avoir d'expression de valeur.
- Un nom de champ peut être lié à plusieurs expressions de valeur.
- Un type de valeur doit être affecté aux expressions de valeur. Le type de valeur SQL peut être : 1) Mot-clé, 2) SpecialString ou 3) WildChar.
- Vous pouvez avoir plusieurs règles de relaxation par combinaison nom/URL de champ.

Utilisation de la ligne de commande pour configurer la vérification d'injection SQL

Pour configurer des actions SQL Injection et d'autres paramètres à l'aide de la ligne de commande :

Dans l'interface de ligne de commande, vous pouvez utiliser la commande **set appfw profile** ou la commande **add appfw profile** pour configurer les protections SQL Injection. Vous pouvez activer les actions de blocage, d'apprentissage, de journalisation et de statistiques et spécifier si vous souhaitez transformer les caractères spéciaux utilisés dans les chaînes d'attaque SQL Injection pour désactiver l'attaque. Sélectionnez le type de modèle d'attaque SQL (mots-clés, caractères génériques, chaînes spéciales) que vous souhaitez détecter dans les charges utiles et indiquez si vous souhaitez que le Web App Firewall inspecte également les en-têtes de requête pour les violations SQL Injection. Utilisez la commande **unset appfw profile** pour rétablir les paramètres configurés à leurs valeurs par défaut. Chacune des commandes suivantes ne définit qu'un seul paramètre, mais vous pouvez inclure plusieurs paramètres dans une seule commande :

- définir le profil du pare-feu d'application « Descriptions des paramètres fournies au bas de la page. «
- `<name> -SQLInjectionAction ([block] [learn] [log] [stats])| [none])`
- définir le profil du pare-feu d'application « Descriptions des paramètres fournies au bas de la page. «
- `<name> -SQLInjectionTransformSpecialChars (**ON** | OFF)`
- définir le profil du pare-feu d'application « Descriptions des paramètres fournies au bas de la page. «
- `<name> -**SQLInjectionCheckSQLWildChars** (**ON** |**OFF**)`
- définir le profil du pare-feu d'application « Descriptions des paramètres fournies au bas de la page. «
- `**<name> -**SQLInjectionType** ([**SQLKeyword**] | [**SQLSplChar**] | [**SQLSplCharANDKeyword**] | [**SQLSplCharORKeyword**])`
- **définir le profil du pare-feu d'application** « Descriptions des paramètres fournies au bas de la page. «
- `<name> -**SQLInjectionParseComments** ([**checkall**] | [**ansi|nested **] | [**ansinested**])`
- **définir le profil du pare-feu d'application « Descriptions des paramètres fournies au bas de la page. «
- `<name> -CheckRequestHeaders (ON | OFF)` Les descriptions des paramètres sont fournies en bas de la page.
- `<name> - CheckRequestQueryNonHtml (ON | OFF)` Les descriptions des paramètres sont fournies en bas de la page.

Pour configurer une règle de relaxation SQL Injection à l'aide de l'interface de commande

Utilisez la commande bind ou unbind pour ajouter ou supprimer une liaison, comme suit :

- `bind appfw profile <name> -SQLInjection <String> [isRegex(REGEX| NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor |SpecialString|Wildchar)[<valueExpression>][-isValueRegex (REGEX |`


```
NOTREGEX)]]
```

- `unbind appfw profile <name> -SQLInjection <String> <formActionURL> [-location <location>] [-valueTyp (Keyword|SpecialString|Wildchar)[<valueExpression>]]`

> **Remarque :**
>
> Vous pouvez trouver la liste des mots-clés SQL à partir du contenu du fichier de signatures par défaut en affichant l'objet de signature de vue, qui contient la liste des mots-clés SQL et des caractères spéciaux SQL.

Utilisation de l'interface graphique pour configurer la vérification de sécurité SQL Injection

Dans l'interface graphique, vous pouvez configurer le contrôle de sécurité SQL Injection dans le volet pour le profil associé à votre application.

Pour configurer ou modifier la vérification SQL Injection à l'aide de l'interface graphique

1. Accédez à **Application Firewall > Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Vérifications de sécurité**.

La table de vérification de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Vous avez 2 options de configuration :

a. Si vous souhaitez activer ou désactiver les actions Block, Log, Stats et Learn pour HTML SQL Injection, vous pouvez sélectionner ou désactiver des cases à cocher dans le tableau, cliquer sur **OK**, puis cliquer sur **Enregistrer et fermer** pour fermer le volet de **contrôle de sécurité** .

b. Si vous souhaitez configurer d'autres options pour cette vérification de sécurité, double-cliquez sur Injection HTML SQL, ou sélectionnez la ligne et cliquez sur **Paramètres d'action**, pour afficher les options suivantes :

Transformer le caractère spécial SQL—Transformez tous les caractères spéciaux SQL dans la requête.

Rechercher les caractères génériques SQL—Considérez les caractères génériques SQL dans la charge utile comme des modèles d'attaque.

Vérifier la requête contenant—Type d'injection SQL (SQLKeyWord, SQLSplChar, SQLSplChar, SQLSplChArdKeyword ou SQLSplCharorKeyword) à vérifier.

Gestion des commentaires SQL : type de commentaires (Vérifier tous les commentaires, ANSI, imbriqué ou ANSI/imbriqué) à vérifier.

Après avoir modifié l'un des paramètres ci-dessus, cliquez sur **OK** pour enregistrer les modifications et revenir au tableau Vérifications de sécurité. Vous pouvez procéder à la configuration d'autres vérifications de sécurité si nécessaire. Cliquez sur **OK** pour enregistrer toutes les modifications que vous avez apportées dans la section Contrôles de sécurité, puis cliquez sur **Enregistrer et fermer pour fermer** le volet de vérification de la sécurité.

Pour configurer une règle de relaxation SQL Injection à l'aide de l'interface graphique

- Accédez à **Application Pare-feu** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
- Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
- Dans le tableau Règles de relaxation, double-cliquez sur l'entrée **HTML SQL Injection** ou sélectionnez-la et cliquez sur **Modifier**.
- Dans la boîte de dialogue **Règles de relaxation HTML Injection SQL**, effectuez les opérations **Ajouter**, **Modifier**, **Supprimer**, **Activer** ou **Désactiver** pour les règles de relaxation.

> **Remarque**
>
> Lorsque vous ajoutez une nouvelle règle, le champ **Expression de la valeur** n'est pas affiché, sauf si vous sélectionnez l'option **Mot-clé** ou **SpecialString** ou **WildChar** dans le champ **Type de valeur**.

Pour gérer les règles de relaxation par injection SQL à l'aide du visualiseur

Pour obtenir une vue consolidée de toutes les règles de relaxation, vous pouvez mettre en surbrillance la ligne **HTML SQL Injection** et cliquer sur **Visualizer**. Le visualiseur pour les relaxations déployées vous offre la possibilité d' **ajouter** une nouvelle règle ou de **modifier** une règle existante. Vous pouvez également **activer** ou **désactiver** un groupe de règles en sélectionnant un nœud et en cliquant sur les boutons correspondants dans le visualiseur de relaxation.

Afficher ou personnaliser les modèles d'injection à l'aide de l'interface graphique

Vous pouvez utiliser l'interface graphique pour afficher ou personnaliser les modèles d'injection.

Les modèles SQL par défaut sont spécifiés dans le fichier de signatures par défaut. Si vous ne liez aucun objet signature à votre profil, les modèles d'injection par défaut spécifiés dans l'objet signatures par défaut seront utilisés par le profil pour le traitement du contrôle de sécurité par injection de commandes. Les règles et les motifs, spécifiés dans l'objet signatures par défaut, sont en lecture seule. Vous ne pouvez pas les modifier ou les modifier. Si vous souhaitez modifier ou modifier ces modèles, effectuez une copie de l'objet SSignatures par défaut pour créer un objet Signature défini par l'utilisateur. Apportez des modifications aux modèles d'injection de commandes dans le nouvel objet Signature défini par l'utilisateur et utilisez cet objet signature dans votre profil qui traite le trafic pour lequel vous souhaitez utiliser ces modèles personnalisés.

Pour plus d'informations, voir Signatures.

Pour afficher les schémas d'injection par défaut à l'aide de l'interface graphique :

1. Accédez à **Application Firewall > Signatures**, sélectionnez ***Signatures par défaut**, puis cliquez sur **Modifier**.



1. Cliquez sur **Gérer les modèles CMD/SQL/XSS**. Le tableau **Gérer les chemins de script SQL/inter-sites** affiche les modèles relatifs à l'injection CMD/SQL/XS :



1. Sélectionnez une ligne et cliquez sur **Gérer les éléments** pour afficher les modèles d'injection correspondants (mots-clés, chaînes spéciales, règles de transformation ou caractères génériques) utilisés par la vérification d'injection de la commande Web App Firewall.

Utilisation de la fonctionnalité d'apprentissage avec la vérification d'injection SQL

Lorsque l'action d'apprentissage est activée, le moteur d'apprentissage du Web App Firewall surveille le trafic et apprend les violations déclenchées. Vous pouvez inspecter périodiquement ces règles apprises. Après avoir dûment pris en considération, vous pouvez déployer la règle apprise en tant que règle de relaxation SQL Injection.

Amélioration de l'apprentissage par injection SQL : une amélioration de l'apprentissage du Web App Firewall a été introduite dans la version 11.0 du logiciel Citrix ADC. Pour déployer une relaxation SQL Injection fine, le Web App Firewall offre un apprentissage SQL Injection à grain fin. Le moteur d'apprentissage formule des recommandations concernant le type de valeur observé (mot-clé, SpecialString, Wildchar) et l'expression de valeur correspondante observée dans les champs d'entrée. En plus de vérifier les demandes bloquées pour déterminer si la règle actuelle est trop restrictive et doit être assouplie, vous pouvez consulter les règles générées par le moteur d'apprentissage pour déterminer quels types de valeur et expressions de valeur déclenchent des violations et doivent être traitées dans les règles de relaxation.

> **Important**
>
> Le moteur d'apprentissage du pare-feu Web App Firewall ne peut distinguer que les 128 premiers octets du nom. Si un formulaire comporte plusieurs champs dont les noms correspondent aux 128 premiers octets, le moteur d'apprentissage peut ne pas être en mesure de les distinguer. De même, la règle de relaxation déployée peut par inadvertance relâcher tous ces champs de l'inspection SQL Injection.
>
> **Remarque** Pour contourner l'enregistrement SQL de l'en-tête User-Agent, utilisez la règle de relaxation suivante :
>
> ```
> bind appfw profile your_profile_name -SQLInjection User-Agent ".*"-
> location HEADER
> ```

Pour afficher ou utiliser les données apprises à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `show appfw learningdata <profilename> SQLInjection`
- `rm appfw learningdata <profilename> -SQLInjection <string> <formActionURL > [<location>] [<valueType> <valueExpression>]`
- `export appfw learningdata <profilename> SQLInjection`

Pour afficher ou utiliser les données apprises à l'aide de l'interface graphique

1. Accédez à **Application Firewall > Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles apprises**. Vous pouvez sélectionner l'entrée **HTML SQL Injection** dans le tableau Règles apprises et double-cliquer dessus pour ac-

céder aux règles apprises. Vous pouvez déployer les règles apprises ou modifier une règle avant de la déployer en tant que règle de relaxation. Pour ignorer une règle, vous pouvez la sélectionner et cliquer sur le bouton **Ignorer**. Vous ne pouvez modifier qu'une seule règle à la fois, mais vous pouvez sélectionner plusieurs règles à déployer ou à ignorer.

Vous avez également la possibilité d'afficher une vue résumée des relaxations apprises en sélectionnant l'entrée **HTML SQL Injection** dans le tableau Règles apprises et en cliquant sur **Visualizer** pour obtenir une vue consolidée de toutes les violations apprises. Le visualiseur facilite la gestion des règles apprises. Il présente une vue complète des données sur un seul écran et facilite l'action sur un groupe de règles en un seul clic. Le plus grand avantage du visualiseur est qu'il recommande des expressions régulières pour consolider plusieurs règles. Vous pouvez sélectionner un sous-ensemble de ces règles, en fonction du délimiteur et de l'URL Action. Vous pouvez afficher 25, 50 ou 75 règles dans le visualiseur, en sélectionnant le nombre dans une liste déroulante. Le visualiseur des règles apprises offre la possibilité de modifier les règles et de les déployer en tant que relaxations. Ou vous pouvez ignorer les règles pour les ignorer.

Utilisation de la fonction de journal avec la vérification d'injection SQL

Lorsque l'action du journal est activée, les violations de vérification de sécurité HTML SQL Injection sont enregistrées dans le journal d'audit en tant que violations **APPFW_SQL**. Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur syslog distant.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Passez à l'interpréteur de commandes et repérez ns.logs dans le dossier **/var/log/** pour accéder aux messages de journal relatifs aux violations SQL Injection :

```
> Shell

## tail -f /var/log/ns.log | grep APPFW_SQL
```

Exemple de message de journal HTML SQL Injection lorsque la demande est transformée

```
1 Jun 26 21:08:41 <local0.info> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
    .0|APPFW|APPFW_SQL|6|src=10.217.253.62 geolocation=Unknown spt=54001
     method=GET request=http://aaron.stratum8.net/FFC/login.php?
    login_name=%27+or&passwd=and+%3B&drinking_pref=on&text_area=select
    +*+from+%5C+%3B&loginButton=ClickToLogin&as_sfid=AAAAAAXjnGN5gLH-
    hvhTOpIySEIqES7BjFRs5Mq0fwPp-3ZHDi5yWlRWByj0cVbMyy-
    Ens2vaaiULKOcUri4OD4kbXWwSY5s7I3QkDsrvIgCYMC9BMvBwY2wbNcSqCwk52lfE0k
    %3D&as_fid=feeec8758b41740eedeeb6b35b85dfd3d5def30c msg= Special
    characters seen in fields cn1=74 cn2=762 cs1=pr_ffc cs2=PPE1 cs3=9
    ztIlf9p1H7p6Xtzn6NMygTv/QM0002 cs4=ALERT cs5=2015 act=transformed
2 <!--NeedCopy-->
```


Exemple de message de journal HTML SQL Injection lorsque la demande de publication est bloquée

```
Jun 26 21:30:34 <local0.info> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
    .0|APPFW|APPFW_SQL|6|src=10.217.253.62 geolocation=Unknown spt=9459
    method=POST request=http://aaron.stratum8.net/FFC/login_post.php msg
    =SQL Keyword check failed for field text_area="(')" cn1=78 cn2=834
    cs1=pr_ffc cs2=PPE1 cs3=eVJMMPtZ2XgylGrHjkx3rZLfBCI0002 cs4=ALERT
    cs5=2015 act=blocked
<!--NeedCopy-->
```

> **Remarque**
>
> Dans le cadre des modifications apportées au streaming dans la version 10.5.e (versions d'amélioration) et la version 11.0 ultérieure, nous traitons maintenant les données d'entrée en blocs. La correspondance de motifs RegEx est désormais limitée à 4K pour la correspondance de chaînes de caractères contiguës. Avec cette modification, les messages du journal des violations SQL peuvent inclure des informations différentes par rapport aux versions précédentes. Le mot-clé et le caractère spécial de l'entrée peuvent être séparés par de nombreux octets. Nous gardons maintenant une trace des mots-clés SQL et des chaînes spéciales lors du traitement des données, au lieu de mettre en mémoire tampon toute la valeur d'entrée. Outre le nom du champ, le message de journal inclut désormais le mot-clé SQL ou le caractère spécial SQL, ou à la fois le mot-clé SQL et le caractère spécial SQL, comme déterminé par le paramètre configuré. Le reste de l'entrée n'est plus inclus dans le message de journal, comme illustré dans l'exemple suivant :
>
> **Exemple :**
>
> Dans 10.5, lorsque le Web App Firewall détecte la violation SQL, la chaîne d'entrée entière peut être incluse dans le message de journal, comme indiqué ci-dessous :
>
> ```
> SQL Keyword check failed for field text=\"select a name from testbed1
> ;(;)\".*<blocked>
> ```
>
> Dans les versions d'amélioration de 10.5.e prenant en charge le streaming côté demande et la version 11.0 ultérieure, nous consignons uniquement le nom du champ, le mot-clé et le caractère spécial (le cas échéant) dans le message de journal, comme indiqué ci-dessous :
>
> ```
> SQL Keyword check failed for field **text="select(;)"<blocked>
> ```
>
> Cette modification s'applique aux demandes qui contiennent des types de contenu application/x-www-form-urlencoded, multipart/form-dataou text/x-gwt-rpc . Les messages de journal générés lors du traitement des charges utiles **JSON** ou **XML** ne sont pas affectés par cette modification.

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique Citrix inclut un outil utile (**Syslog Viewer**) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez au **pare-feu des applications** > **Profils**, sélectionnez le profil cible et cliquez sur **Vérifications de sécurité**. Mettez en surbrillance la ligne **HTML SQL Injection** et cliquez sur **Journaux**. Lorsque vous accédez aux journaux directement à partir de la vérification HTML SQL Injection du profil, l'interface graphique filtre les messages de journal et affiche uniquement les journaux relatifs à ces violations de vérification de sécurité.
- Vous pouvez également accéder à la visionneuse Syslog en accédant à **Citrix ADC** > **Système** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation des contrôles de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de vérification de sécurité peuvent être déclenchées pendant le traitement de la demande.
- Accédez à **Application Firewall** > **Stratégies** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation des contrôles de sécurité.

La visionneuse Syslog basée sur HTML fournit diverses options de filtre pour sélectionner uniquement les messages de journal qui vous intéressent. Pour sélectionner les messages de journal pour la vérification **HTML SQL Injection**, filtrez en sélectionnant **APPFW** dans la liste déroulante Options du **module**. La liste **Type d'événement** offre un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous activez la case à cocher **APPFW_SQL** et cliquez sur le bouton **Appliquer**, seuls les messages de journal relatifs aux violations de vérification de sécurité **SQL Injection** apparaissent dans la visionneuse Syslog.

Si vous placez le curseur dans la ligne d'un message de journal spécifique, plusieurs options, telles que **Module**, **Type d'événement**, **ID d'événement**, **adresse IP du client**, etc. s'affichent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans le message de journal.

Cliquez sur pour Déployer la fonctionnalité est disponible uniquement dans l'interface graphique. Vous pouvez utiliser la visionneuse Syslog non seulement pour afficher les journaux, mais aussi pour déployer des règles de relaxation HTML SQL Injection basées sur les messages de journal pour les violations de vérification de sécurité du Web App Firewall. Les messages de journal doivent être au format de journal CEF pour cette opération. Cliquez pour déployer la fonctionnalité est disponible uniquement pour les messages de journal générés par l'action Bloquer (ou non bloquer). Vous ne pouvez pas déployer une règle de relaxation pour un message de journal concernant l'opération de transformation.

Pour déployer une règle de relaxation à partir de la visionneuse Syslog, sélectionnez le message de journal. Une case à cocher apparaît dans le coin supérieur droit de la case **Syslog Viewer** de la ligne sélectionnée. Activez la case à cocher, puis sélectionnez une option dans la liste Action pour déployer la règle de relaxation. **Modifier et déployer**, **déployer**et **déployer tout**sont disponibles en tant qu'options **Action**.

Les règles d'injection SQL déployées à l'aide de l'option Cliquez pour déployer n'incluent pas les

recommandations de relaxation du grain fin.

Pour utiliser la fonctionnalité Cliquez pour déployer dans l'interface graphique :

1. Dans la visionneuse Syslog, sélectionnez **Application Firewall** dans les options du **module**.
2. Sélectionnez **APP_SQL** comme **type d'événement** pour filtrer les messages de journal correspondants.
3. Activez la case à cocher pour identifier la règle à déployer.
4. Utilisez la liste déroulante d'options **Action** pour déployer la règle de relaxation.
5. Vérifiez que la règle apparaît dans la section Règle de relaxation correspondante.

Statistiques pour les violations SQL Injection

Lorsque l'action des statistiques est activée, le compteur pour la vérification Injection SQL est incrémenté lorsque le Web App Firewall prend une action pour cette vérification de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. La taille d'un incrément du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, la demande d'une page contenant 3 violations SQL Injection incrémente le compteur de statistiques d'un, car la page est bloquée dès que la première violation est détectée. Toutefois, si le bloc est désactivé, le traitement de la même demande incrémente de trois le compteur de statistiques pour les violations et les journaux, car chaque violation génère un message de journal distinct.

Pour afficher les statistiques de vérification SQL Injection à l'aide de la ligne de commande :

À l'invite de commandes, tapez :

> **statistiques sh appfw**

Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
> stat appfw profile <profile name>
```

Pour afficher les statistiques HTML SQL Injection à l'aide de l'interface graphique

1. Accédez à **Système** > **Sécurité** > **Pare-feu d'application**.
2. Dans le volet droit, accédez au lien **Statistiques**.
3. Utilisez la barre de défilement pour afficher les statistiques sur les violations HTML SQL Injection et les journaux. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Résumé

Notez les points suivants à propos de la vérification SQL Injection :

- **Prise en charge intégrée de la protection par injection SQL** : Citrix Web App Firewall protège contre l'injection SQL en surveillant une combinaison de mots clés SQL et de caractères spéciaux dans les paramètres du formulaire. Tous les mots-clés SQL, caractères spéciaux, caractères génériques et règles de transformation par défaut sont spécifiés dans le fichier /netscaler/default_custom_settings.xml.
- **Personnalisation** : vous pouvez modifier les mots-clés, les caractères spéciaux, les caractères génériques et les règles de transformation par défaut pour personnaliser l'inspection du contrôle de sécurité SQL en fonction des besoins spécifiques de votre application. Effectuez une copie de l'objet signature par défaut, modifiez les entrées existantes ou ajoutez de nouvelles entrées. Liez cet objet signature à votre profil pour utiliser la configuration personnalisée.
- **Modèle de sécurité hybride** : les signatures et les protections de sécurité profondes utilisent les modèles de script SQL/cross-site spécifiés dans l'objet signature lié au profil. Si aucun objet de signature n'est lié au profil, les modèles de script SQL/cross-site présents dans l'objet signature par défaut sont utilisés.
- **Transform**—Notez ce qui suit à propos de l'opération de transformation :
  - L'opération de transformation fonctionne indépendamment des autres paramètres d'action SQL Injection. Si la transformation est activée et que le bloc, le journal, les statistiques et l'apprentissage sont tous désactivés, les caractères spéciaux SQL sont transformés.
  - Lorsque la transformation SQL est activée, les demandes des utilisateurs sont envoyées aux serveurs principaux après la transformation des caractères spéciaux SQL en mode non bloqué. Si l'action de blocage est activée, elle a priorité sur l'action de transformation. Si le type d'injection est spécifié en tant que caractère spécial SQL et que le bloc est activé, la demande est bloquée malgré l'action de transformation.
- **Relaxation et apprentissage à grains fins** : affinez la règle de relaxation pour détendre un sous-ensemble d'éléments SQL de l'inspection des contrôles de sécurité, mais détecter le reste. Le moteur d'apprentissage recommande un type de valeur spécifique et des expressions de valeur basées sur les données observées.
- **Cliquez pour déployer** : sélectionnez un ou plusieurs messages de journal des violations SQL dans la visionneuse syslog et déployez-les en tant que règles de relaxation.

Protection basée sur la grammaire SQL pour les charges utiles HTML et JSON

August 20, 2021

Citrix Web App Firewall utilise une approche de correspondance de modèles pour détecter les attaques par injection SQL dans `HTTP` et les `JSON` charges utiles. L'approche utilise un ensemble de

mots-clés prédéfinis et (ou) de caractères spéciaux pour détecter une attaque et la signaler comme une violation. Bien que cette approche soit efficace, elle peut entraîner de nombreux faux positifs, entraînant l'ajout d'une ou de plusieurs règles de relaxation. Surtout lorsque des mots couramment utilisés tels que « Sélectionner » et « De » sont utilisés dans une requête HTTP ou JSON. Nous pouvons réduire les faux positifs en implémentant la vérification de la protection de la grammaire SQL `HTML` et la `JSON` charge utile.

Dans l'approche de correspondance de modèles existante, une attaque par injection SQL est identifiée si un mot-clé prédéfini et/ou un caractère spécial sont présents dans une requête HTTP. Dans ce cas, il n'est pas nécessaire que l'instruction soit une instruction SQL valide. Toutefois, dans l'approche basée sur la grammaire, une attaque par injection SQL n'est détectée que si un mot-clé ou un caractère spécial est présent dans une instruction SQL ou fait partie d'une instruction SQL, réduisant ainsi les scénarios faux positifs.

scénario d'utilisation de la protection basée sur la grammaire SQL

Considérez une déclaration intitulée « Sélectionnez mes billets et rencontrons à la station Union » présente dans une demande HTTP. Bien que l'instruction ne soit pas une instruction SQL valide, l'approche de correspondance de modèle existante détecte la demande comme une attaque par injection SQL car l'instruction utilise des mots-clés tels que « Select », « and » et « Union ». Toutefois, dans le cas de l'approche grammaire SQL, l'instruction n'est pas détectée comme une attaque de violation car les mots-clés ne sont pas présents dans une instruction SQL valide ou ne font pas partie d'une instruction SQL valide.

L'approche basée sur la grammaire peut également être configurée pour détecter les attaques par injection SQL dans les `JSON` charges utiles. Pour ajouter une règle de relaxation, vous pouvez réutiliser les règles de relaxation existantes. Les règles de relaxation à grains fins sont également applicables à la grammaire SQL, aux règles avec « mot clé » « ValueType ». Dans la grammaire `JSON` SQL, la méthode basée sur URL existante peut être réutilisée.

Configurez la protection basée sur la grammaire SQL à l'aide de l'interface de ligne

Pour implémenter la détection basée sur la grammaire SQL, vous devez configurer le paramètre « SQLInjectionGrammar » dans le profil Web App Firewall. Par défaut, le paramètre est désactivé. Toutes les actions SQL Injection existantes sont prises en charge, sauf l'apprentissage. Tout nouveau profil créé après une mise à niveau prend en charge la grammaire d'injection SQL et le type par défaut reste « caractère spécial ou mot-clé » et il doit être explicitement activé.

À l'invite de commandes, tapez :

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
     SQLInjectionGrammar ON/OFF
```



```
2 <!--NeedCopy-->
```

Exemple :

```
add appfw profile profile1 -SQLInjectionAction Block -SQLInjectionGrammar ON
```

Configurer la protection de correspondance de motifs SQL et la protection basée sur la grammaire à l'aide de l'interface de ligne de commande

Si vous avez activé les approches grammaticales et les approches de correspondance de modèle, l'appliance effectue d'abord une détection grammaire et s'il existe une détection par injection SQL avec le type d'action défini sur bloquer, la demande est bloquée (sans vérifier la détection à l'aide de la correspondance de modèle).

À l'invite de commandes, tapez :

```
1 add appfw profile <profile-name> - SQLInjectionAction <action-name> -
     SQLInjectionGrammar ON - SQLInjectionType <Any action other than ‘
     None’ : SQLSplCharANDKeyword/ SQLSplCharORKeyword/ SQLSplChar/
     SQLKeyword>
2 <!--NeedCopy-->
```

Exemple :

```
add appfw profile p1 -SQLInjectionAction block - SQLInjectionGrammar ON -
SQLInjectionType SQLSplChar
```

Configurer la vérification SQL Injection uniquement avec une protection grammaire à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add appfw profile <profile-name> - SQLInjectionAction <action-name> -
     SQLInjectionGrammar ON - SQLInjectionType None
2 <!--NeedCopy-->
```

Exemple :

```
add appfw profile p1 -SQLInjectionAction block - SQLInjectionGrammar ON -
SQLInjectionType None
```


Liez les règles de relaxation pour la protection basée sur la grammaire SQL à l'aide de l'interface de ligne de commande

Si votre application exige que vous contourniez le contrôle d' SQL injection pour un « ELEMENT » ou un « ATTRIBUT » spécifique dans la charge utile, vous devez configurer une règle de relaxation.

> **Remarque :**
>
> Les règles de relaxation avec « mot-clé » ValueType sont évaluées uniquement lorsque l'appliance effectue une détection à l'aide de la SQL grammaire.

La SQL commande Règles de relaxation de l'inspection par injection a la syntaxe suivante. À l'invite de commandes, tapez :

```
1 bind appfw profile <name> -SQLInjection <String> [isRegex(REGEX|
      NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor
      |SpecialString|Wildchar) [<valueExpression>][-isValueRegex (REGEX |
      NOTREGEX) ]]
2 <!--NeedCopy-->
```

Exemple :

```
bind appfw profile p1 -sqlinjection abc http://10.10.10.10/
bind appfw profile p1 -sqlinjection 'abc[0-9]+'http://10.10.10.10/ -isregex
regEX
bind appfw profile p1 -sqlinjection 'name'http://10.10.10.10/ -valueType
Keyword 'selec[a-z]+' -isvalueRegex regEX
```

Configurer la protection basée sur la grammaire SQL pour la charge utile JSON à l'aide de l'interface de ligne de commande

Pour implémenter la détection basée sur la grammaire SQL pour la charge utile JSON, vous devez configurer le paramètre « JSONSQLInjectionGrammar » dans le profil Web App Firewall. Par défaut, le paramètre est désactivé. Toutes les actions SQL Injection existantes sont prises en charge, sauf l'apprentissage. Tout nouveau profil créé après une mise à niveau prend en charge la grammaire d'injection SQL et le type par défaut reste « caractère spécial ou mot-clé » et vous devez l'activer explicitement.

À l'invite de commandes, tapez :

```
1 add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
      action-name> -JSONSQLInjectionGrammar ON/OFF
2 <!--NeedCopy-->
```

Exemple :


```
add appfw profile profile1 -type JSON -JSONSQLInjectionAction Block -JSONSQLInjectionG
 ON
```

Configurer la protection de correspondance de motifs SQL et la protection grammaire à l'aide de l'interface de ligne de commande

Si vous avez activé les vérifications de grammaire et de correspondance de modèle, l'appliance effectue d'abord une détection grammaire et s'il existe une détection par injection SQL avec le type d'action bloqué, la demande est bloquée (sans vérifier la détection à l'aide de la correspondance de modèle).

> **Remarque :**
>
> Les règles de relaxation avec « mot-clé » ValueType sont évaluées uniquement lorsque l'appliance effectue une détection à l'aide de la grammaire SQL.

À l'invite de commandes, tapez :

```
1 add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
     action-name> -JSONSQLInjectionGrammar ON  - JSONSQLInjectionType <Any
      action other than  'None' : SQLSplCharANDKeyword/
     SQLSplCharORKeyword/ SQLSplChar/ SQLKeyword>
2 <!--NeedCopy-->
```

Exemple :

```
add appfw profile p1 -type JSON -JSONSQLInjectionAction block - JSONSQLInjectionGramma
 ON -JSONSQLInjectionType SQLSplChar
```

Configurer la protection basée sur la grammaire SQL pour la charge utile JSON à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
     action-name> -JSONSQLInjectionGrammar ON  - JSONSQLInjectionType None
     `\
2 <!--NeedCopy-->
```

Exemple :

```
add appfw profile p1 -type JSON -JSONSQLInjectionAction block - JSONSQLInjectionGramma
 ON -JSONSQLInjectionType None
```


Lier des règles de relaxation basées sur des URL pour une protection grammaire JSON SQL à l'aide de l'interface de ligne de commande

Si votre application exige que vous contourniez l'inspection par injection de JSON commandes pour un « ELEMENT » ou « ATTRIBUTE » spécifique dans la charge utile, vous pouvez configurer une règle de relaxation.
La JSON commande Règles de relaxation de l'inspection par injection a la syntaxe suivante. À l'invite de commandes, tapez :

```
1 bind appfw profile <profile name>  - JSONCMDURL <expression> -comment <
      string> -isAutoDeployed ( AUTODEPLOYED | NOTAUTODEPLOYED ) -state (
      ENABLED | DISABLED )
2 <!--NeedCopy-->
```

Exemple :

```
bind appfw profile p1 -sqlinjection abc http://10.10.10.10/
bind appfw profile p1 -sqlinjection 'abc[0-9]+'http://10.10.10.10/ -isregex
regEX
bind appfw profile p1 -sqlinjection 'name'http://10.10.10.10/ -valueType
Keyword 'selec[a-z]+' -isvalueRegex regEX
```

Configurer la protection basée sur la grammaire SQL à l'aide de l'interface graphique

Effectuez la procédure GUI pour configurer la détection d'injection HTML SQL basée sur la grammaire.

1. Dans le volet de navigation, accédez à **Sécurité > Profils**.
2. Dans la page **Profils**, cliquez sur **Ajouter**.
3. Sur la page **Profil Citrix Web App Firewall**, cliquez sur **Contrôles de sécurité** sous **Paramètres avancés**.
4. Dans la section **Vérification de sécurité**, accédez aux paramètres **HTML SQL Injection** .
5. Cliquez sur l'icône exécutable située près de la case à cocher.
6. Cliquez sur **Paramètres d'action** pour accéder à la page **Paramètres d'injection SQL HMTL** .



7. Activez la **case à cocher Vérifier l'utilisation de la grammaire SQL** .
8. Cliquez sur **OK**.

Configurer la protection basée sur la grammaire SQL pour la charge utile JSON à l'aide de l'interface graphique

Effectuez la procédure GUI pour configurer la détection d'injection JSON SQL basée sur la grammaire.

1. Dans le volet de navigation, accédez à **Sécurité > Profils**.
2. Dans la page **Profils**, cliquez sur **Ajouter**.
3. Sur la page **Profil Citrix Web App Firewall**, cliquez sur **Contrôles de sécurité** sous **Paramètres avancés**.
4. Dans la section **Vérifications de sécurité**, accédez aux paramètres **JSON SQL Injection**.
5. Cliquez sur l'icône exécutable située près de la case à cocher.
6. Cliquez sur **Paramètres d'action** pour accéder à la page **Paramètres d'injection JSON SQL**.
7. Activez la **case à cocher Vérifier l'utilisation de la grammaire SQL** .
8. Cliquez sur **OK**.



Règles de relaxation et de refus pour gérer les attaques par injection HTML SQL

August 20, 2021

En cas de trafic entrant, la logique de détection des violations vérifie les violations de la circulation. Si aucune attaque par injection HTML SQL n'est détectée, le trafic est autorisé à passer. Mais si une violation est détectée, les règles de relaxation (autorisation) et de refus définissent comment gérer les violations. Si le contrôle de sécurité est configuré en mode Autoriser (mode par défaut), la violation détectée est bloquée à moins que l'utilisateur n'ait explicitement configuré une règle de relaxation ou d'autorisation.

En plus du mode Autoriser, le contrôle de sécurité peut également être configuré en mode Refuser et utiliser des règles de refus pour gérer les violations. Si le contrôle de sécurité est configuré dans ce mode, les violations détectées sont bloquées si un utilisateur a explicitement configuré une règle de refus. Si aucune règle de refus n'est configurée, l'action configurée par l'utilisateur est appliquée.

L'illustration suivante explique comment autoriser et refuser les modes de fonctionnement :



1. Lorsqu'une violation est détectée, les règles de relaxation (autorisation) et de refus définissent la façon de gérer les violations.
2. Si le contrôle de sécurité est configuré en mode Refuser (s'il est configuré en mode Autoriser, passez à l'étape 5), la violation est bloquée sauf si vous avez explicitement configuré une règle de refus.
3. Si la violation correspond à une règle de refus, l'appliance bloque le trafic.
4. Si la violation du trafic ne correspond pas à une règle, l'appliance applique une action définie par l'utilisateur (bloquer, réinitialiser ou supprimer).
5. Si le contrôle de sécurité est configuré en mode Autoriser, le module Web App Firewall vérifie si une règle d'autorisation est configurée.
6. Si la violation correspond à une règle d'autorisation, l'appliance autorise le trafic à contourner autrement, il est bloqué.

Configurer le mode de relaxation et d'application de l'enregistrement de sécurité

À l'invite de commandes, tapez :

```
set appfw profile <name>   - SQLInjectionAction [block stats learn]  -
    SQLInjectionRuleType [ALLOW DENY]
<!--NeedCopy-->
```

Exemple :

```
set appfw profile prof1 sqlInjectionAction block -sqlInjectionRuleType
ALLOW DENY
```

Lier les règles de relaxation et d'application au profil Web Application Firewall

À l'invite de commandes, tapez :


```
1 bind appfw profile <name> -SQLInjection <string> <formActionURL>
2 <!--NeedCopy-->
```

Exemple :

```
bind appfw profile p1 -SQLInjection field_f1 "/login.php"-RuleType ALLOW
bind appfw profile p2 -SQLInjection field_f1 "/login.php"-RuleType ALLOW
```

Contrôle de la protection par injection de commande HTML

October 4, 2021

La vérification d'injection de commandes **HTML** examine si le trafic entrant comporte des commandes non autorisées qui enfreignent la sécurité du système ou modifient le système. Si le trafic comporte des commandes malveillantes lorsqu'il est détecté, l'appliance bloque la demande ou exécute l'action configurée.

Le profil Citrix Web App Firewall est désormais amélioré avec une nouvelle vérification de sécurité pour les attaques par injection de commandes. Lorsque le contrôle de sécurité par injection de commande examine le trafic et détecte des commandes malveillantes, l'appliance bloque la demande ou exécute l'action configurée.

Dans une attaque par injection de commandes, l'attaquant vise à exécuter des commandes non autorisées sur le système d'exploitation Citrix ADC. Pour ce faire, l'attaquant injecte des commandes du système d'exploitation à l'aide d'une application vulnérable. Une appliance Citrix ADC est vulnérable aux attaques par injection si l'application transmet des données non sécurisées (formulaires, cookies ou en-tête) à l'interpréteur de commandes système.

Fonctionnement de la protection par injection de commande

1. Pour une requête entrante, WAF examine le trafic pour les mots clés ou les caractères spéciaux. Si la demande entrante n'a aucun motif correspondant à l'un des mots-clés ou caractères spéciaux refusés, la demande est autorisée. Sinon, la demande est bloquée, supprimée ou redirigée en fonction de l'action configurée.
2. Si vous préférez exempter un mot clé ou un caractère spécial de la liste, vous pouvez appliquer une règle de relaxation pour contourner le contrôle de sécurité dans des conditions spécifiques.
3. Vous pouvez activer la journalisation pour générer des messages de journal. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.

4. Vous pouvez également activer la fonction de statistiques pour collecter des données statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si les demandes légitimes sont bloquées, vous devrez peut-être revoir la configuration pour voir si vous devez configurer la nouvelle règle de relaxation ou modifier la règle existante.

Mots clés et caractères spéciaux refusés pour la vérification de l'injection de commande

Pour détecter et bloquer les attaques par injection de commandes, l'appliance dispose d'un ensemble de motifs (mots-clés et caractères spéciaux) définis dans le fichier de signature par défaut. Voici une liste de mots-clés bloqués lors de la détection d'injection de commande.

```
    <commandinjection>
      <keyword type="LITERAL" builtin="ON">7z</keyword>
      <keyword type="LITERAL" builtin="ON">7za</keyword>
      <keyword type="LITERAL" builtin="ON">7zr</keyword>
…
</commandinjection>
<!--NeedCopy-->
```

Les caractères spéciaux définis dans le fichier de signature sont les suivants :
`| ; & $ > < '\ ! >> ##`

Configuration de la vérification de l'injection de commande à l'aide de la CLI

Dans l'interface de ligne de commande, vous pouvez utiliser la commande set the profile ou add the profile pour configurer les paramètres d'injection de commande. Vous pouvez activer les actions de blocage, de journal et de statistiques. Vous devez également définir les mots-clés et les caractères de chaîne que vous souhaitez détecter dans les charges utiles.

À l'invite de commandes, tapez :

```
set appfw profile <profile-name> -cmdInjectionAction <action-name> -CMDInjectionType
 <CMDInjectionType>]
```

> **Remarque :**
>
> Par défaut, l'action d'injection de commande est définie sur « Aucune ». En outre, le type d'injection de commande par défaut est défini comme `CmdSplCharANDKeyWord`.

Exemple :

```
set appfw profile profile1 -cmdInjectionAction block -CMDInjectionType
CmdSplChar
```


Où, les actions d'injection de commande disponibles sont :

- Aucun - Désactivez la protection par injection de commandes.
- Journal - Consigner les violations d'injection de commande pour le contrôle de sécurité.
- Bloquer - bloque le trafic qui viole le contrôle de sécurité de l'injection de commande.
- Stats - Génère des statistiques pour les violations de sécurité par injection de commande.

Où, les types d'injection de commandes disponibles sont :

- Cmd SplChar. Vérifie les caractères spéciaux
- CmdKeyWord. Vérifie les mots-clés d'injection
- CmdSplCharANDKeyWord. Vérifie les caractères spéciaux et l'injection de commandes. Mots clés et blocs uniquement si les deux sont présents.
- CmdSplCharORKeyWord. Vérifie les caractères spéciaux et l'injection de commande Mots-clés et blocs si l'un d'eux est trouvé.

Configuration des règles de relaxation pour la vérification de la protection par injection de commandes

Si votre application exige que vous contourniez l'inspection par injection de commande pour un ELEMENT ou un ATTRIBUT spécifique dans la charge utile, vous pouvez configurer une règle de relaxation.

La commande Injection inspection Relaxation rules ont la syntaxe suivante :

```
bind appfw profile <profile name> -cmdInjection <string> <URL> -isregex <
REGEX/NOTREGEX>
```

Exemple de règle de relaxation pour Regex dans l'en-tête

```
bind appfw profile sample -CMDInjection hdr "http://10.10.10.10/"-location
heaDER -valueType Keyword '[a-z]+grep'-isvalueRegex REGEX
```

Par conséquent, l'injection exempte la vérification d'injection de commande autorise l'en-tête `hdr` contenant des variantes de « grep ». «

Exemple de règle de relaxation avec ValueType en tant que regex dans le cookie

```
bind appfw profile sample -CMDInjection ck_login "http://10.10.10.10/"-
location cookie -valueType Keyword 'pkg[a-z]+'-isvalueRegex REGEX
```

Configuration de la vérification de l'injection de commandes à l'aide de Citrix ADC GUI

Procédez comme suit pour configurer la vérification de l'injection de commande.

1. Accédez à **Sécurité > Citrix Web App Firewall and Profils**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page **Profil du Citrix Web App Firewall**, accédez à la section **Paramètres avancés** et cliquez sur **Vérifications de sécurité**.



1. Dans la section **Vérifications de sécurité**, sélectionnez **Injection de commandes HTML** et cliquez sur Paramètres **d'action**.
2. Dans la page **Paramètres d'injection de commandes HTML**, définissez les paramètres suivants :
   a) Actions. Sélectionnez une ou plusieurs actions à effectuer pour le contrôle de sécurité de l'injection de commande.
   b) Vérifiez la requête contenant. Sélectionnez un modèle d'injection de commande pour vérifier si la requête entrante a le modèle.
3. Cliquez sur **OK**.



Afficher ou personnaliser les modèles d'injection de commandes à l'aide de l'interface graphique

Vous pouvez utiliser l'interface graphique pour afficher ou personnaliser les modèles d'injection de commandes **HTML** .

Les modèles d'injection de commandes par défaut sont spécifiés dans le fichier de signatures par défaut. Si vous ne liez aucun objet signature à votre profil, les modèles d'injection de commandes HTML par défaut spécifiés dans l'objet signatures par défaut seront utilisés par le profil pour le traitement du contrôle de sécurité des injections de commandes. Les règles et les motifs, spécifiés dans l'objet signatures par défaut, sont en lecture seule. Vous ne pouvez pas les modifier ou les modifier. Si vous souhaitez modifier ou modifier ces modèles, effectuez une copie de l'objet SSignatures par défaut pour créer un objet Signature défini par l'utilisateur. Apportez des modifications aux modèles d'injection de commandes dans le nouvel objet Signature défini par l'utilisateur et utilisez cet objet signature dans votre profil qui traite le trafic pour lequel vous souhaitez utiliser ces modèles personnalisés.

Pour plus d'informations, voir Signatures.

Pour afficher les modèles d'injection de commandes par défaut à l'aide de l'interface graphique :

1. Accédez à **Application Firewall > Signatures**, sélectionnez ***Signatures par défaut**, puis cliquez sur **Modifier**.

1. Cliquez sur **Gérer les modèles CMD/SQL/XSS**. Le tableau **Chemins CMD/SQL/XSS (lecture seule)** présente les schémas relatifs à l' `CMD` / `SQL` / `XSS` injection :



1. Sélectionnez une ligne et cliquez sur **Gérer les éléments** pour afficher les modèles d'injection de commandes correspondants (mots-clés, chaînes spéciales, règles de transformation ou caractères génériques) utilisés par la vérification d'injection de commande Web App Firewall.

Pour personnaliser un modèle d'injection de commandes à l'aide de l'interface graphique

Vous pouvez modifier l'objet signature défini par l'utilisateur pour personnaliser les mots-clés **CMD**, les chaînes spéciales et les caractères génériques. Vous pouvez ajouter de nouvelles entrées ou sup-

primer celles qui existent déjà. Vous pouvez modifier les règles de transformation des chaînes spéciales d'injection de commandes.

1. **Accédez à Application Firewall > Signatures**, mettez en surbrillance la signature définie par l'utilisateur cible, puis cliquez sur **Ajouter**. Cliquez sur **Gérer les modèles CMD/SQL/XSS**.
2. Dans la page **Gérer les chemins CMD/SQL/XSS**, sélectionnez la ligne d'injection CMD cible.
3. Cliquez sur **Gérer les éléments**, **Ajouter**ou **supprimer** un élément d'injection de commande.

> **Avertissement :**
>
> Vous devez être prudent avant de supprimer ou de modifier un élément d'injection de commande par défaut, ou de supprimer le chemin CMD pour supprimer la ligne entière. Les règles de signature et le contrôle de sécurité de l'injection de commandes reposent sur ces éléments pour détecter les attaques par injection de commandes afin de protéger vos applications. La personnalisation des modèles SQL peut rendre votre application vulnérable aux attaques par injection de commandes si le modèle requis est supprimé pendant la mise à jour.



Affichage des statistiques sur le trafic d'injection de commandes et les violations

La page **Statistiques du Citrix Web App Firewall** affiche les détails du trafic de sécurité et des violations de sécurité sous forme de tableau ou de graphique.

Pour afficher les statistiques de sécurité à l'aide de l'interface de commande.

À l'invite de commandes, tapez :

```
stat appfw profile profile1
```


Statistiques de trafic du profil Appfw	Taux (/s)	Total :
Demandes	0	0
Octets des demandes	0	0
Réponses	0	0
Octets des réponses	0	0
Abandonner	0	0
Redirections	0	0
Temps de réponse moyen à long terme (ms)	–	0
Temps de réponse moyen récent (ms)	–	0

Statistiques sur les violations HTML/XML/JSON	Taux (/s)	Total :
URL de démarrage	0	0
Refuser URL	0	0
En-tête Référer	0	0
Dépassement de tampon	0	0
Cohérence des cookies	0	0
Détournement de cookies	0	0
Balise de formulaire CSRF	0	0
Script inter-sites HTML	0	0
Injection SQL HTML	0	0
Format de champ	0	0
Cohérence des champs	0	0
Carte de crédit	0	0
Objet sécurisé	0	0
Violations des	0	0
Type de contenu	0	0
Déni de service JSON	0	0

Statistiques sur les violations HTML/XML/JSON	Taux (/s)	Total :
Injection JSON SQL	0	0
Script inter-site JSON	0	0
Types de téléchargement de fichiers	0	0
Induire Type de contenu Charge utile XML	0	0
Injection CMD HTML	0	0
Format XML	0	0
Déni de service XML (xDoS)	0	0
Validation des messages XML	0	0
Interopérabilité des services Web	0	0
Injection SQL XML	0	0
Script multisite XML	0	0
Pièce jointe XML	0	0
Violations de pannes SOAP	0	0
Violations génériques XML	0	0
Total des violations	0	0

Statistiques du journal HTML/XML/JSON	Taux (/s)	Total :
Journaux des URL de démarrage	0	0
Journaux des URL refusées	0	0
Journaux d’en-tête référer	0	0
Journaux de débordement de	0	0
journaux de cohérence des cookies	0	0
Bûches de détournement de cookies	0	0

Statistiques du journal HTML/XML/JSON	Taux (/s)	Total :
CSRF à partir des journaux des balises	0	0
Journaux de script inter-sites HTML	0	0
Journaux de transformation de script inter-site HTML	0	0
Journaux d'injection SQL HTML	0	0
Journaux de transformation HTML SQL	0	0
Journaux de format de	0	0
Journaux d'uniformité	0	0
Cartes de crédit	0	0
Logs de transformation des cartes de crédit	0	0
Journaux d'objets sûrs	0	0
Journaux signature	0	0
Journaux types de contenu	0	0
JSON Journaux de déni de service	0	0
Journaux d'injection JSON SQL	0	0
JSON Journaux de script inter-sites	0	0
Journaux des types de téléchargement	0	0
Induire le type de contenu XML Charge utile L	0	0
Journaux d'injection de commandes HTML	0	0
Journaux de format XML	0	0

Statistiques du journal HTML/XML/JSON	Taux (/s)	Total :
Journaux de déni de service XML (XDoS)	0	0
Journaux de validation des messages XML	0	0
Journaux WSI	0	0
Journaux d'injection SQL XML	0	0
Journaux de script inter-sites XML	0	0
journaux des pièces jointes XML	0	0
Journaux des défaillances SOAP	0	0
Journaux génériques XML	0	0
Nombre total de messages du journal	0	0

Taux de statistiques de réponse aux erreurs du serveur (/s) > Total			
Erreurs client HTTP (4xx Resp)	0	0	Erreurs serveur
HTTP (5xx Resp)	0	0	

Affichage des statistiques d'injection de commandes HTML à l'aide de l'interface graphique Citrix ADC

Procédez comme suit pour afficher les statistiques d'injection de commandes :

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez un profil de Web App Firewall et cliquez sur **Statistiques**.
3. La page **Statistiques du Citrix Web App Firewall** affiche le trafic d'injection de commandes

HTML et les détails de violation.

4. Vous pouvez sélectionner **Vue tabulaire** ou passer à la **vue graphique** pour afficher les données sous forme de tableau ou graphique.

Statistiques du trafic d'injection de commandes HTML

HTML SQL Injection logs	0	0
HTML SQL transform logs	0	0
Field format logs	0	0
Field consistency logs	0	0
Credit cards	0	0
Credit card transform logs	0	0
Safe object logs	0	0
Signature logs	0	0
Content Type logs	0	0
JSON Denial of Service logs	0	0
JSON SQL injection logs	0	0
JSON Cross-Site Scripting logs	0	0
File upload types logs	0	0
Infer Content Type XML Payload Logs	0	0
HTML Command Injection logs	0	0
XML Format logs	0	0
XML Denial of Service(XDoS) logs	0	0
XML Message Validation logs	0	0
WSI logs	0	0
XML SQL Injection logs	0	0
XML XSS logs	0	0
XML Attachment logs	0	0

Statistiques de violation d'injection de commande HTML



HTML/XML/JSON Violation Statistics

	Rate (/s)	Total	
Start URL	0	0	0%
Deny URL	0	0	0%
Referer header	0	0	0%
Buffer overflow	0	0	0%
Cookie consistency	0	0	0%
Cookie hijacking	0	0	0%
CSRF form tag	0	0	0%
HTML Cross-site scripting	0	0	0%
HTML SQL injection	0	0	0%
Field format	0	0	0%
Field consistency	0	0	0%
Credit card	0	0	0%
Safe object	0	0	0%
Signature logs	0	0	0%
Content Type	0	0	0%
JSON Denial of Service	0	0	0%
JSON SQL injection	0	0	0%
JSON Cross-Site Scripting	0	0	0%
File Upload Types	0	0	0%
Infer Content Type XML Payload	0	0	0%
HTML CMD Injection	0	0	0%
XML Format	0	0	0%
XML Denial of Service (XDoS)	0	0	
XML Message Validation	0	0	
Web Services Interoperability	0	0	

Vérification de la protection par injection de commande JSON

October 4, 2021

Le contrôle d'injection de commande JSON examine le trafic JSON entrant pour détecter les commandes non autorisées qui cassent la sécurité du système ou modifient le système. Lors de l'examen du trafic, si des commandes malveillantes sont détectées, l'appliance bloque la demande ou exécute l'action configurée.

Dans une attaque par injection de commandes, l'attaquant vise à exécuter des commandes non autorisées sur le système d'exploitation Citrix ADC ou le serveur principal. Pour ce faire, l'attaquant injecte des commandes du système d'exploitation à l'aide d'une application vulnérable. L'application back-end est vulnérable aux attaques par injection si l'appliance transmet simplement une requête sans aucune vérification de sécurité. Par conséquent, il est extrêmement important de configurer une vérification de sécurité afin que l'appliance Citrix ADC puisse protéger votre application Web en bloquant les données dangereuses.

Fonctionnement de la protection par injection de commande

1. Pour une requête JSON entrante, WAF examine le trafic pour les mots clés ou les caractères spéciaux. Si la requête JSON n'a aucun motif correspondant à l'un des mots-clés ou caractères spéciaux refusés, la demande est autorisée. Sinon, la demande est bloquée, supprimée ou redirigée en fonction de l'action configurée.
2. Si vous préférez exempter un mot clé ou un caractère spécial de la liste, vous pouvez créer une règle de relaxation pour contourner le contrôle de sécurité dans des conditions spécifiques.
3. Vous pouvez activer la journalisation pour générer des messages de journal. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.
4. Vous pouvez également activer la fonction de statistiques pour collecter des données statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si les demandes légitimes sont bloquées, vous devrez peut-être revoir la configuration pour voir si vous devez configurer la nouvelle règle de relaxation ou modifier la règle existante.

Mots clés et caractères spéciaux refusés pour la vérification de l'injection de commande

Pour détecter et bloquer les attaques par injection de commandes JSON, l'appliance dispose d'un ensemble de motifs (mots-clés et caractères spéciaux) définis dans le fichier de signature par défaut. Voici une liste de mots-clés bloqués lors de la détection d'injection de commande.

```
<commandinjection>
      <keyword type="LITERAL" builtin="ON">7z</keyword>
      <keyword type="LITERAL" builtin="ON">7za</keyword>
      <keyword type="LITERAL" builtin="ON">7zr</keyword>
…
</commandinjection>

<!--NeedCopy-->
```

Les caractères spéciaux définis dans le fichier de signature sont les suivants :
`| ; & $ > < '\ ! >> ##`

Configuration de la vérification d'injection de commande JSON à l'aide de l'interface de ligne de commande

Dans l'interface de ligne de commande, vous pouvez utiliser la commande set appfw profile ou ajouter une commande appfw profile pour configurer les paramètres d'injection de commande JSON. Vous

pouvez activer les actions de blocage, de journal et de statistiques. Vous devez également définir le type d'injection de commande, tel que les mots clés et les caractères de chaîne que vous souhaitez détecter dans les charges utiles.

À l'invite de commandes, tapez :

```
set appfw profile <profile-name> -cmdInjectionAction <action-name> -CMDInjectionType
 <CMDInjectionType>]
```

> **Remarque :**
>
> Par défaut, l'action d'injection de commande est définie comme « blocage des statistiques du journal ». En outre, le type d'injection de commande par défaut est défini comme `CmdSplCharANDKeyWord`. Après une mise à niveau, les profils Pare-feu de l'application Web existants ont l'action définie sur « Aucun ».

Exemple :

```
set appfw profile profile1 -JSONCMDInjectionAction block -JSONCMDInjectionType
 CmdSplChar
```

Où, les actions d'injection de commande JSON disponibles sont :

Aucun - Désactivez la protection par injection de commandes.
Journal - Consigner les violations d'injection de commande pour le contrôle de sécurité.
Bloquer - bloque le trafic qui viole le contrôle de sécurité de l'injection de commande.
Stats - Génère des statistiques pour les violations de sécurité par injection de commande.

Où, les types d'injection de commande JSON disponibles sont :

`Cmd SplChar` - Vérifie les caractères spéciaux
`CmdKeyWord` - Vérifie l'injection de la commande Mots-clés
`CmdSplCharANDKeyWord` - Ceci est l'action par défaut. L'action vérifie les caractères spéciaux et l'injection de commande. Mots clés et blocs uniquement si les deux sont présents.
`CmdSplCharORKeyWord` - Vérifie les caractères spéciaux et l'injection de commande Mots-clés et blocs si l'un d'eux est trouvé.

Configuration des règles de relaxation pour la vérification de la protection par injection de commande JSON

Si votre application exige que vous contourniez l'inspection par injection de commande JSON pour un ELEMENT ou un ATTRIBUT spécifique dans la charge utile, vous pouvez configurer une règle de relaxation.

Les règles de relaxation d'inspection par injection de commande JSON ont la syntaxe suivante.


```
bind appfw profile <profile name> -JSONCMDURL <expression> -comment <string
> -isAutoDeployed ( AUTODEPLOYED | NOTAUTODEPLOYED )-state ( ENABLED |
DISABLED )
```

Exemple de règle de relaxation pour Regex dans l'en-tête

```
bind appfw profile abc_json -jsoncmDURL http://1.1.1.1/hello.html
```

Attendu que, ce qui suit assouplit les requêtes de toutes les URL hébergées sur 1.1.1.1 :

```
bind appfw profile abc_json -jsoncmDURL http://1.1.1.1/*"
```

Pour supprimer la relaxation, utilisez 'unbin'.

```
unbind appfw profile abc_json -jsoncmDURL  " http://1.1.1.1/*"
```

Configurer la vérification de l'injection de commande JSON à l'aide de l'interface graphique

Procédez comme suit pour configurer la vérification d'injection de commande JSON.

1. Accédez à **Sécurité > Citrix Web App Firewall and Profils**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page **Profil du Citrix Web App Firewall**, accédez à la section **Paramètres avancés** et cliquez sur **Vérifications de sécurité**.



1. Dans **la section Vérifications de sécurité**, sélectionnez **Injection de commandes JSON** et cliquez sur Paramètres **d'action**.
2. Dans la page **Paramètres d'injection de commandes JSON**, définissez les paramètres suivants
   a) Actions. Sélectionnez une ou plusieurs actions à effectuer pour le contrôle de sécurité par injection de commande JSON.
   b) Vérifiez la requête contenant. Sélectionnez un modèle d'injection de commande pour vérifier si la requête entrante a le modèle.
3. Cliquez sur **OK**.



Affichage des statistiques sur le trafic d'injection de commandes et les violations

La page **Statistiques du Citrix Web App Firewall** affiche les détails du trafic de sécurité et des violations de sécurité sous forme de tableau ou de graphique.

Pour afficher les statistiques de sécurité à l'aide de l'interface de commande.

À l'invite de commandes, tapez :

```
stat appfw profile profile1
```

Statistiques de trafic du profil Appfw	Taux (/s)	Total :
Demandes	0	0
Octets des demandes	0	0
Réponses	0	0
Octets des réponses	0	0
Abandonner	0	0
Redirections	0	0
Temps de réponse moyen à long terme (ms)	–	0
Temps de réponse moyen récent (ms)	–	0

Statistiques sur les violations HTML/XML/JSON	Taux (/s)	Total :
URL de démarrage	0	0
Refuser URL	0	0
En-tête Référer	0	0
Dépassement de tampon	0	0
Cohérence des cookies	0	0
Détournement de cookies	0	0
Balise de formulaire CSRF	0	0
Script inter-sites HTML	0	0
Injection SQL HTML	0	0
Format de champ	0	0
Cohérence des champs	0	0
Carte de crédit	0	0
Objet sécurisé	0	0
Violations des	0	0
Type de contenu	0	0
Déni de service JSON	0	0
Injection JSON SQL	0	0
Script inter-site JSON	0	0
Types de téléchargement de fichiers	0	0
Induire Type de contenu Charge utile XML	0	0
Injection CMD HTML	0	0
Format XML	0	0
Déni de service XML (xDoS)	0	0
Validation des messages XML	0	0
Interopérabilité des services Web	0	0
Injection SQL XML	0	0

Statistiques sur les violations HTML/XML/JSON	Taux (/s)	Total :
Script multisite XML	0	0
Pièce jointe XML	0	0
Violations de pannes SOAP	0	0
Violations génériques XML	0	0
Total des violations	0	0

Statistiques du journal HTML/XML/JSON	Taux (/s)	Total :
Journaux des URL de démarrage	0	0
Journaux des URL refusées	0	0
Journaux d'en-tête référer	0	0
Journaux de débordement de	0	0
journaux de cohérence des cookies	0	0
Bûches de détournement de cookies	0	0
CSRF à partir des journaux des balises	0	0
Journaux de script inter-sites HTML	0	0
Journaux de transformation de script inter-site HTML	0	0
Journaux d'injection SQL HTML	0	0
Journaux de transformation HTML SQL	0	0
Journaux de format de	0	0
Journaux d'uniformité	0	0
Cartes de crédit	0	0

Statistiques du journal HTML/XML/JSON	Taux (/s)	Total :
Logs de transformation des cartes de crédit	0	0
Journaux d'objets sûrs	0	0
Journaux signature	0	0
Journaux types de contenu	0	0
JSON Journaux de déni de service	0	0
Journaux d'injection JSON SQL	0	0
JSON Journaux de script inter-sites	0	0
Journaux des types de téléchargement	0	0
Induire le type de contenu XML Charge utile L	0	0
JSON CMD Injection	0	0
Journaux d'injection de commandes HTML	0	0
Journaux de format XML	0	0
Journaux de déni de service XML (XDoS)	0	0
Journaux de validation des messages XML	0	0
Journaux WSI	0	0
Journaux d'injection SQL XML	0	0
Journaux de script inter-sites XML	0	0
journaux des pièces jointes XML	0	0
Journaux des défaillances SOAP	0	0
Journaux génériques XML	0	0

Statistiques du journal HTML/XML/JSON	Taux (/s)	Total :
Nombre total de messages du journal	0	0

Taux de statistiques de réponse d'erreur serveur (/s)	Total :		
Erreurs client HTTP (4xx Resp)	0	0	Erreurs serveur
HTTP (5xx Resp)	0	0	

Statistiques du journal HTML/XML/JSON	Taux (/s)	Total :
JSON Journaux d'injection de commandes	0	0
Journaux de format XML	0	0

Affichage des statistiques d'injection de commandes JSON à l'aide de l'interface graphique Citrix ADC

Procédez comme suit pour afficher les statistiques d'injection de commandes :

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez un profil de Web App Firewall et cliquez sur **Statistiques**.
3. La page **Statistiques du Citrix Web App Firewall** affiche le trafic d'injection de commandes JSON et les détails de violation.
4. Vous pouvez sélectionner **Vue tabulaire** ou passer à la **vue graphique** pour afficher les données sous forme de tableau ou graphique.

Statistiques du trafic d'injection de commande JSON

HTML/XML/JSON Log Statistics

	Rate (/s)	Total
Start URL logs	0	0
Deny URL logs	0	0
Field consistency logs	0	0
Credit cards	0	0
Credit card transform logs	0	0
Safe object logs	0	0
Signature logs	0	0
Content Type logs	0	0
JSON Denial of Service logs	0	0
JSON SQL injection logs	0	0
JSON Cross-Site Scripting logs	0	0
JSON CMD injection logs	0	0
File upload types logs	0	0
Infer Content Type XML Payload Logs	0	0

JSON CMD injection logs: X
Number of JSON Command Injection security check log messages generated by the Application Firewall.

Statistiques de violation d’injection de commande JSON



Protection contre les attaques des entités externes XML (XXE)

August 20, 2021

La protection contre les attaques des entités externes XML (XXE) examine si une charge utile entrante contient des entrées XML non autorisées concernant des entités en dehors du domaine approuvé où réside l'application Web. L'attaque XXE se produit si vous avez un analyseur XML faible qui analyse une charge utile XML avec une entrée contenant des références à des entités externes.

Dans une appliance Citrix ADC, si l'analyseur XML n'est pas correctement configuré, l'exploitation de la vulnérabilité peut avoir un impact dangereux. Il permet à un attaquant de lire des données sensibles sur le serveur Web. Effectuez l'attaque par déni de service, etc. Par conséquent, il est important de pro-

téger l'appliance contre les attaques XXE. Web Application Firewall est capable de protéger l'appliance contre les attaques XXE tant que le type de contenu est identifié comme XML. Pour empêcher un utilisateur malveillant de contourner ce mécanisme de protection, WAF bloque une demande entrante si le type de contenu « inféré » dans les en-têtes HTTP ne correspond pas au type de contenu du corps. Ce mécanisme empêche le contournement de la protection contre les attaques XXE lorsqu'un type de contenu par défaut ou non par défaut est utilisé sur liste blanche.

Voici quelques-unes des menaces XXE potentielles qui affectent une appliance Citrix ADC :

- Fuites de données confidentielles
- Attaques par déni de service (DOS)
- Requêtes de falsification côté serveur
- Analyse des ports

Configurer la protection par injection d'entités externes XML (XXE)

Pour configurer les entités externes XML (XXE), vérifiez à l'aide de l'interface de commande :
Dans l'interface de ligne de commande, vous pouvez ajouter ou modifier la commande de profil de pare-feu d'application pour configurer les paramètres **XXE** . Vous pouvez activer les actions de blocage, de journal et de statistiques.

À l'invite de commandes, tapez :

```
set appfw profile <name> [-inferContentTypeXmlPayloadAction <inferContentTypeXmlPaylo
 <block | log | stats | none>]
```

> Remarque :
>
> Par défaut, l'action XXE est définie comme « aucun. «

Exemple :

```
set appfw profile profile1 -inferContentTypeXmlPayloadAction Block
```

Où, les types d'action sont :

Bloc : La requête est bloquée sans exception aux URL de la requête.

Journal : si une incompatibilité entre le type de contenu dans un en-tête de requête HTTP et la charge utile se produit, les informations sur la demande violée doivent figurer dans le message de journal.

Statistiques : Si une incompatibilité entre les types de contenu est détectée, les statistiques correspondantes pour ce type de violation sont incrémentées.

Aucun : aucune action n'est prise si une inadéquation dans les types de contenu est détectée. Aucun ne peut être combiné avec un autre type d'action. L'action par défaut est définie sur Aucun.

Configurer la vérification de l'injection XXE à l'aide de l'interface graphique Citrix ADC

Procédez comme suit pour configurer la vérification de l'injection XXE.

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page **Profil du Citrix Web App Firewall**, accédez à la section **Paramètres avancés** et cliquez sur **Vérifications de sécurité**.



4. Dans la section **Vérifications de sécurité**, sélectionnez **Induire le type de contenu XML Charge utile** et cliquez sur Paramètres **d'action**.
5. Dans la page Infer Content Type XML Payload Settings, définissez les paramètres suivants :
   a) Actions. Sélectionnez une ou plusieurs actions à effectuer pour le contrôle de sécurité de l'injection XXE.
6. Cliquez sur **OK**.



Affichage des statistiques sur le trafic d'injection XXE et les violations

La page Statistiques du Citrix Web App Firewall affiche les détails du trafic de sécurité et des violations de sécurité dans un format tabulaire ou graphique.

Pour afficher les statistiques de sécurité à l'aide de l'interface de commande.

À l'invite de commandes, tapez :


```
stat appfw profile profile1
```

Affichage des statistiques d'injection XXE à l'aide de l'interface graphique Citrix ADC

Procédez comme suit pour afficher les statistiques d'injection XXE :

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez un profil de Web App Firewall et cliquez sur **Statistiques**.
3. La page **Statistiques du Citrix Web App Firewall** affiche le trafic d'injection de commandes XXE et les détails de violation.
4. Vous pouvez sélectionner **Vue tabulaire** ou passer à la **vue graphique** pour afficher les données sous forme de tableau ou graphique.



Vérification du débordement de tampon

August 20, 2021

La vérification de débordement de la mémoire tampon détecte les tentatives de provoquer un débordement de la mémoire tampon sur le serveur Web. Si le Web App Firewall détecte que l'URL, les cookies ou l'en-tête sont plus longs que la longueur configurée, il bloque la demande car elle peut provoquer un dépassement de tampon.

La vérification de débordement de la mémoire tampon empêche les attaques contre les logiciels non sécurisés du système d'exploitation ou du serveur Web qui peuvent se bloquer ou se comporter de manière imprévisible lorsqu'il reçoit une chaîne de données plus grande qu'elle ne peut gérer. Des techniques de programmation appropriées empêchent les débordements de tampon en vérifiant les données entrantes et en rejetant ou en tronquant les chaînes trop longues. De nombreux programmes, cependant, ne vérifient pas toutes les données entrantes et sont donc vulnérables aux débordements de tampon. Ce problème affecte particulièrement les anciennes versions des logiciels et des systèmes d'exploitation de serveurs Web, dont beaucoup sont encore en cours d'utilisation.

La vérification de sécurité Buffer Overflow vous permet de configurer les actions **Bloquer**, **Log**et **Stats**. En outre, vous pouvez également configurer les paramètres suivants :

- **Longueur maximale de l'URL**. Longueur maximale autorisée par le Web App Firewall dans une URL demandée. Les demandes avec des URL plus longues sont bloquées. **Valeurs possibles** : 0—65535. **Par défaut** : 1024
- **Longueur maximale du cookie**. La longueur maximale autorisée par le Web App Firewall pour tous les cookies d'une demande. Les demandes avec des cookies plus longs déclenchent les violations. **Valeurs possibles** : 0—65535. **Par défaut** : 4096
- **Longueur maximale de l'en-tête**. Longueur maximale autorisée par le Web App Firewall pour les en-têtes HTTP. Les demandes avec des en-têtes plus longs sont bloquées. **Valeurs possibles** : 0—65535. **Par défaut** : 4096
- **Longueur de chaîne de requête**. Longueur maximale autorisée pour la chaîne de requête dans une requête entrante. Les requêtes avec des requêtes plus longues sont bloquées. Valeurs possibles : 0—65535. Par défaut : 1024
- **Longueur totale de la demande**. Longueur maximale de demande autorisée pour une demande entrante. Les demandes de plus longue durée sont bloquées. Valeurs possibles : 0—65535. Par défaut : 24820

Utilisation de la ligne de commande pour configurer la vérification de sécurité Buffer Overflow

Pour configurer les actions de vérification de sécurité de Buffer Overflow et d'autres paramètres à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
add appfw profile <name> -bufferOverflowMaxURLLength <positive_integer> -
bufferOverflowMaxHeaderLength <positive_integer> - bufferOverflowMaxCookieLength
```



```
 <positive_integer> -bufferOverflowMaxQueryLength <positive_integer> -
bufferOverflowMaxTotalHeaderLength <positive_integer>
```

Exemple :

```
add appfw profile profile1 -bufferOverflowMaxURLLength 7000 -bufferOverflowMaxHeaderLe
 7250 - bufferOverflowMaxCookieLength 7100 -bufferOverflowMaxQueryLength
7300 -bufferOverflowMaxTotalHeaderLength 7300
```

Configurer la vérification de la sécurité de débordement de tampon à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité** > **Pare-feu et**profils**d'applications Web**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page **Profil du Citrix Web App Firewall**, accédez à la section **Paramètres avancés** et cliquez sur **Vérifications de sécurité**.
4. Dans **la section Vérifications de sécurité**, sélectionnez **Dépassement de tampon** et cliquez sur **Paramètres d'action**.
5. Dans la page **Paramètres de dépassement de tampon**, définissez les paramètres suivants.
   a. Actions. Sélectionnez une ou plusieurs actions à effectuer pour le contrôle de sécurité de l'injection de commande.
   b. Longueur maximale de l'URL. Longueur maximale, en caractères, des URL sur vos sites Web protégés. Les demandes avec des URL plus longues sont bloquées.
   c. Longueur maximale des cookies. Longueur maximale, en caractères, des cookies envoyés à vos sites Web protégés. Les demandes avec des cookies plus longs sont bloquées.
   d. Longueur maximale de l'en-tête. Longueur maximale, en caractères, des en-têtes HTTP dans les requêtes envoyées à vos sites Web protégés. Les demandes avec des en-têtes plus longs sont bloquées.
   e. Longueur maximale de la requête. Longueur maximale, en octets, pour la chaîne de requête envoyée à vos sites Web protégés. Les demandes avec des chaînes de requête plus longues sont bloquées.
   f. Longueur totale maximale de l'en-tête. Longueur maximale, en octets, de la longueur totale d'en-tête HTTP dans les requêtes envoyées à vos sites Web protégés. La valeur minimale de ceci et MaxHeaderLen dans HttpProfile sera utilisée. Les demandes de plus longue durée sont bloquées.
6. Cliquez sur **OK** et **Fermer**.



Utilisation de la fonction de journal avec la vérification de sécurité de débordement de tampon

Lorsque l'action du journal est activée, les violations de vérification de sécurité **Buffer Overflow sont enregistrées dans le journal d'audit en tant que violations APPFW_BUFFEROVERFLOW_URL**, **APPFW_BUFFEROVERFLOW_COOKIE**et **APPFW_BUFFEROVERFLOW_HDR**. Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur syslog distant.

Si vous utilisez l'interface graphique pour consulter les journaux, vous pouvez utiliser la fonctionnalité de clic pour déployer pour appliquer les relaxations indiquées par les journaux.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Passez à l'interpréteur de commandes et queue les ns.logs dans le dossier **/var/log/** pour accéder aux messages du journal relatifs aux violations de débordement de tampon :

```
1 > \*\*Shell\*\*
2 > \*\*tail -f /var/log/ns.log | grep APPFW_BUFFEROVERFLOW\*\*
3 <!--NeedCopy-->
```

Exemple de message de journal CEF montrant une violation BufferOverflowMaxCookieLength en mode non-bloc


```
Oct 22 17:35:20 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|\*\*APPFW_BUFFEROVERFLOW_COOKIE\*\*|6|src=10.217.253.62
    geolocation=Unknown spt=41198 method=GET request=http://aaron.
    stratum8.net/FFC/sc11.html \*\*msg=Cookie header length(43) is
    greater than maximum allowed(16).\*\* cn1=119 cn2=465 cs1=
    owa_profile cs2=PPE1 cs3=wvOOOb+cJ2ZRbstZpyeNXIqLj7Y0001 cs4=ALERT
    cs5=2015 \*\*act=not blocked\*\*
<!--NeedCopy-->
```

Exemple de message de journal CEF montrant une violation BufferOverflowMaxUrllEngth en mode non-bloc

```
Oct 22 18:39:56 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|\*\*APPFW_BUFFEROVERFLOW_URL\*\*|6|src=10.217.253.62
    geolocation=Unknown spt=19171 method=GET request=http://aaron.
    stratum8.net/FFC/sc11.html \*\*msg=URL length(39) is greater than
    maximum allowed(20).\*\* cn1=707 cn2=402 cs1=owa_profile cs2=PPE0
    cs3=kW49GcKbnwKByByi3+jeNzfgWa80000 cs4=ALERT cs5=2015 \*\*act=not
    blocked\*\*
<!--NeedCopy-->
```

Exemple de message de journal de format natif montrant une violation BufferOverflowMaxHeader-Length en mode bloc

```
Oct 22 18:44:00 <local0.info> 10.217.31.98 10/22/2015:18:44:00 GMT ns
    0-PPE-2 : default APPFW \*\*APPFW_BUFFEROVERFLOW_HDR\*\* 155 0 :
    10.217.253.62 374-PPE2 khhBEeY4DB8V2D3H2sMLkXmfWnA0002 owa_profile
    \*\*Header(User-Agent) length(82) is greater than maximum allowed
    (10)\*\* : http://aaron.stratum8.net/ \*\*<blocked>\*\*
<!--NeedCopy-->
```

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique Citrix inclut un outil utile (**Syslog Viewer**) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez au **pare-feu des applications** > **Profils**, sélectionnez le profil cible et cliquez sur **Vérifications de sécurité**. Mettez en **surbrillance la ligne Buffer Overflow** et cliquez sur **Journaux**. Lorsque vous accédez aux journaux directement à partir de la vérification de sécurité de débordement de tampon du profil, l'interface graphique filtre les messages de journal et affiche uniquement les journaux relatifs à ces violations de vérification de sécurité.
- Vous pouvez également accéder à la visionneuse Syslog en accédant à **NetScaler** > **Système** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de

violation des contrôles de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de vérification de sécurité peuvent être déclenchées pendant le traitement de la demande.

- Accédez à **Application Firewall** > **Stratégies** > **Audit**. Dans la section **Messages d'audit**, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation des contrôles de sécurité.

La visionneuse Syslog basée sur XML fournit diverses options de filtre pour sélectionner uniquement les messages de journal qui vous intéressent. Pour sélectionner les messages de journal pour la vérification **Dépassement de tampon**, filtrez en sélectionnant **APPFW** dans les options de la liste déroulante pour **Module**. La liste **Type d'événement** offre trois options, **APPFW_BUFFEROVERFLOW_URL**, **APPFW_BUFFEROVERFLOW_COOKIE** et A**PPFW_BUFFEROVERFLOW_HDR**, pour afficher tous les messages de journal relatifs à la vérification de sécurité de débordement de tampon. Vous pouvez sélectionner une ou plusieurs options pour affiner votre sélection. Par exemple, si vous activez la case à cocher **APPFW_BUFFEROVERFLOW_COOKIE** et que vous cliquez sur le bouton **Appliquer**, seuls les messages relatifs aux violations de contrôle de **sécurité de dépassement de tampon** pour l'en-tête Cookie apparaissent dans la visionneuse Syslog. Si vous placez le curseur dans la ligne d'un message de journal spécifique, plusieurs options, telles que **Module**, **Type d'événement**, **ID d'événement**et **IP du client**, apparaissent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans le message de journal.

Click-to-Deploy : l'interface graphique fournit une fonctionnalité de click-to-Deploy, qui est actuellement prise en charge uniquement pour les messages du journal de débordement de tampon relatifs aux violations de **longueur d'URL**. Vous pouvez utiliser la visionneuse Syslog non seulement pour afficher les violations déclenchées, mais aussi pour exécuter des décisions éclairées en fonction des longueurs observées des messages bloqués. Si la valeur actuelle est trop restrictive et déclenche des faux positifs, vous pouvez sélectionner un message et le déployer pour remplacer la valeur actuelle par la valeur de longueur d'URL affichée dans le message. Les messages de journal doivent être au format de journal CEF pour cette opération. Si la relaxation peut être déployée pour un message de journal, une case à cocher apparaît sur le bord droit de la case **Visualiseur Syslog** de la ligne. Activez la case à cocher, puis sélectionnez une option dans la liste **Action** pour déployer la relaxation. **Modifier et déployer**, **déployer**et **déployer tout**sont disponibles en tant qu'options **Action**. Vous pouvez utiliser le filtre **APPFW_BUFFEROVERFLOW_URL** pour isoler tous les messages de journal relatifs aux violations de longueur d'URL configurées.

Si vous sélectionnez un message de journal individuel, les trois options d'action **Modifier et**déployer**, Déployer**et **Déployer tout**sont disponibles. Si vous sélectionnez **Modifier et déployer**, la boîte de dialogue **Paramètres de débordement de la mémoire tampon**s'affiche. La nouvelle longueur d'URL observée dans la requête est insérée dans le champ **d'entrée Longueur d'URL maximale**. Si vous cliquez sur **Fermer** sans aucune modification, les valeurs configurées actuelles restent inchangées. Si vous cliquez sur le bouton **OK**, la nouvelle valeur de la longueur maximale de l'URL remplace la

valeur précédente.

> **Remarque**
>
> Les cases à cocher **Bloquer**, **Journal**et **Statistiques**ne sont pas cochées dans la boîte de dialogue **Paramètres de débordement de la mémoire tampon**affichée et doivent être reconfigurées si vous sélectionnez l'option **Modifier et déployer**. Assurez-vous d'activer ces cases à cocher avant de cliquer sur **OK**, sinon la nouvelle longueur de l'URL est configurée mais les actions sont définies sur **aucune**.

Si vous activez les cases à cocher pour plusieurs messages de journal, vous pouvez utiliser l'option **Déployer** ou **Déployer tout**. Si les messages de journal déployés ont des longueurs d'URL différentes, la valeur configurée est remplacée par la valeur de longueur d'URL la plus élevée observée dans les messages sélectionnés. Le déploiement de la règle entraîne uniquement la modification de la valeur **BufferOverflowMaxUrllEngth**. Les actions configurées sont conservées et restent inchangées.

Pour utiliser la fonctionnalité Click-to-Deploy dans l'interface graphique

1. Dans la visionneuse Syslog, sélectionnez **APPFW** dans les options du **module** .
2. Activez la case à cocher **APPFW_BUFFEROVERFLOW_URL** en tant que **Type d'événement** pour filtrer les messages de journal correspondants.
3. Activez la case à cocher pour sélectionner la règle.
4. Utilisez la liste déroulante **Action** pour déployer la relaxation.
5. Accédez à **Application Pare-feu** > **Profils**, sélectionnez le profil cible et cliquez sur **Vérifications de sécurité** pour accéder au volet Paramètres de **débordement de la mémoire tampon** pour vérifier que la valeur **Longueur d'URL maximale** est mise à jour.

Statistiques relatives aux violations de débordement de tampon

Lorsque l'action des statistiques est activée, le compteur pour la vérification de sécurité de débordement de la mémoire tampon est incrémenté lorsque le Web App Firewall prend une action pour cette vérification de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. La taille d'un incrément du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, une demande pour une page contenant trois violations de débordement de tampon incrémente le compteur de statistiques d'un, car la page est bloquée lorsque la première violation est détectée. Toutefois, si le bloc est désactivé, le traitement de la même demande incrémente le compteur statistique pour les violations car chaque violation génère un message de journal distinct.

Pour afficher les statistiques de vérification de sécurité par débordement de tampon à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
> sh appfw stats
```


Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
> stat appfw profile <profile name>
```

Pour afficher les statistiques de débordement de tampon à l'aide de l'interface graphique

1. Accédez à **Système** > **Sécurité** > **Pare-feu d'application**.
2. Dans le volet droit, accédez au lien **Statistiques**.
3. Utilisez la barre de défilement pour afficher les statistiques sur les violations de débordement de tampon et les journaux. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Résumé

- Le contrôle de sécurité de débordement de tampon vous permet de configurer des limites pour appliquer la longueur maximale des URL, des cookies et des en-têtes autorisés.
- **Les actions**Block**,**Log**et Stats**vous permettent de surveiller le trafic et de configurer une protection optimale pour votre application.
- La visionneuse Syslog vous permet de filtrer et d'afficher tous les messages de journal relatifs aux violations de débordement de tampon.
- La fonctionnalité**Click-to-Deploy** est prise en charge pour les violations **BufferOverflow-MaxUrllEnGth**. Vous pouvez sélectionner et déployer une règle individuelle, ou sélectionner plusieurs messages de journal pour ajuster et relâcher la valeur configurée actuelle de la longueur maximale autorisée de l'URL. La valeur la plus élevée de l'URL du groupe sélectionné est définie comme nouvelle valeur, pour autoriser toutes ces demandes qui sont actuellement signalées comme des violations.
- Le Web App Firewall évalue désormais les cookies individuels lors de l'inspection de la demande entrante. Si la longueur d'un cookie reçu dans l'en-tête Cookie dépasse la valeur **BufferOverflowMaxCookieLength**configurée, la violation Buffer Overflow est déclenchée.

> **Important**
>
> Dans la version 10.5.e (dans quelques améliorations intermédiaires antérieures à la version 59.13xx.e) et dans la version 11.0 (dans les versions antérieures à 65.x), le traitement du Web App Firewall de l'en-tête Cookie a été modifié. Dans ces versions, chaque cookie est évalué individuellement, et si la longueur d'un cookie reçu dans l'en-tête Cookie dépasse le BufferOverflowMaxCookieLength configuré, la violation Buffer Overflow est déclenchée. À la suite de cette modification, les requêtes qui ont été bloquées dans les versions 10.5 et antérieures peuvent être autorisées, car la longueur de l'en-tête du cookie entier n'est pas calculée pour déterminer la longueur du cookie. ** Dans certains cas, la taille totale des cookie transférés au serveur peut être supérieure à la valeur acceptée, et le serveur peut répondre par « 400 mauvaises

> demandes ».
>
> Ce changement a été rétabli. Le comportement dans les versions 10.5.e ->59.13xx.e et 10.5.e ultérieures en plus de la version 11.0 65.x et les versions ultérieures est maintenant similaire à celui des versions non améliorées de la version 10.5. L'en-tête de Cookie brut entier est maintenant pris en compte lors du calcul de la longueur du cookie. Les espaces environnants et les point-virgule (;) séparant les paires nom-valeur sont également inclus dans la détermination de la longueur du cookie.

Prise en charge Web App Firewall pour Google Web Toolkit

January 21, 2021

Remarque : Cette fonctionnalité est disponible dans Citrix ADC version 10.5.e.

Les serveurs Web suivant les mécanismes RPC (Remote Procedure Call) de Google Web Toolkit (GWT) peuvent être sécurisés par le Citrix Web App Firewall sans nécessiter de configuration spécifique pour activer la prise en charge de GWT.

Qu'est-ce que GWT

Le GWT est utilisé pour créer et optimiser des applications Web hautes performances complexes par des personnes qui n'ont pas d'expertise dans XMLHttpRequest et JavaScript. Cette boîte à outils de développement libre et open source est largement utilisée pour développer des applications à petite et grande échelle et est assez fréquemment utilisée pour afficher des données basées sur le navigateur telles que les résultats de recherche pour les vols, les hôtels, etc. Le GWT fournit un ensemble de base d'API Java et de widgets pour écrire des scripts JavaScript optimisés qui peuvent s'exécuter sur la plupart des navigateurs et des appareils mobiles. Le framework RPC GWT facilite l'échange d'objets Java sur HTTP pour les composants client et serveur de l'application Web. Les services RPC GWT ne sont pas les mêmes que les services Web basés sur SOAP ou REST. Ils sont simplement une méthode légère pour transférer des données entre le serveur et l'application GWT sur le client. GWT gère la sérialisation des objets Java en échangeant les arguments dans les appels de méthode et la valeur de retour.

Pour connaître les sites Web populaires qui utilisent GWT, voir

https://www.quora.com/What-web-applications-use-Google-Web-Toolkit-%28GWT%29

Fonctionnement d'une requête GWT

La requête RPC GWT est délimitée par un canal et a un nombre variable d'arguments. Il est porté comme une charge utile de HTTP POST et a les valeurs suivantes :

1. Type de contenu = text/x-gwt-rpc. Charset peut être n'importe quelle valeur.
2. Méthode = POST.

Les requêtes HTTP GET et POST sont toutes deux considérées comme des requêtes GWT valides si le type de contenu est « text/x-gwt-rpc ». Les chaînes de requête sont désormais prises en charge dans le cadre des requêtes GWT. Configurez le paramètre « InspectQueryContentTypes » du profil du pare-feu de l'application sur « Other » pour examiner la partie requête pour le type conent-type « text/x-gwt-rpc ».

L'exemple suivant montre une charge utile valide pour une requête GWT :

```
5|0|8|http://localhost:8080/test/|16878339F02B83818D264AE430C20468| com
    .test.client.TestService|testMethod|java.lang.String|java.lang.
    Integer| myInput1|java.lang.Integer/3438268394|1|2|3|4|2|5|6|7|8|1|
<!--NeedCopy-->
```

La demande peut être divisée en trois parties :

a)Header: 5|0|8|

Les 3 premiers chiffres `5|0|8|` de la requête ci-dessus représentent respectivement « version, sub-version et taille du tableau ». Ceux-ci doivent être des entiers positifs.

b) Table de chaînes :

```
http://localhost:8080/test/|16878339F02B83818D264AE430C20468| com.test.
client.TestService|testMethod|java.lang.String|java.lang.Integer|myInput1|
java.lang.Integer/3438268394|
```

Les membres de la table de chaîne délimitée par le tuyau ci-dessus contiennent les entrées fournies par l'utilisateur. Ces entrées sont analysées pour les vérifications du Web App Firewall et sont identifiées comme suit :

- 1er :`http://localhost:8080/test/`

  Il s'agit de l'URL de la demande.

- 2ème : `16878339F02B83818D264AE430C20468`

  Identifiant HEX unique. Une requête est considérée comme mal formée si cette chaîne a des caractères non hexadécimaux.

- 3ème : `com.test.client.TestService`

  Nom de la classe de service

- 4e : `testMethod`

  Nom de la méthode de service

- 5ème à partir : `java.lang.String|java.lang.Integer|myInput1|java.lang.Integer/3438268394`

  Types de données et données. Les types de données non primitifs sont spécifiés comme

  `<container>.<sub-cntnr>.name/<integer><identifier>`

c)`Payload`: `1|2|3|4|2|5|6|7|8|1|`

La charge utile consiste en des références aux éléments de la table de chaînes. Ces valeurs entières ne peuvent pas être supérieures au nombre d'éléments dans la table de chaînes.

Protection Web App Firewall pour les applications GWT

Le Web App Firewall comprend et interprète les requêtes RPC GWT, inspecte la charge utile pour détecter les violations de contrôle de sécurité et prend les actions spécifiées.

Les en-têtes et les contrôles des cookies du Web App Firewall pour les requêtes GWT sont similaires à ceux des autres formats de requête. Après le décodage d'URL et la conversion de jeu de caractères appropriés, tous les paramètres de la table de chaînes sont inspectés. Le corps de la requête GWT ne contient pas de noms de champs, seulement les valeurs de champs. Les valeurs d'entrée peuvent être validées par rapport au format spécifié à l'aide de la vérification Format de champ du Web App Firewall, qui peut également être utilisée pour contrôler la longueur de l'entrée. Les attaques **de script inter-site** et **d'injection SQL** dans les entrées peuvent être facilement détectées et contrecarrées par le Web App Firewall.

Règles d'apprentissage et de relaxation : L'apprentissage et le déploiement des règles de relaxation sont pris en charge pour les demandes GWT. Les règles du pare-feu des applications Web se présentent sous la forme de mappage <actionURL> <fieldName>. Le format de requête GWT n'a pas les noms de champs et nécessite donc un traitement spécial. Le Web App Firewall insère des noms de champs factices dans les règles apprises qui peuvent être déployés en tant que règles de relaxation. L'indicateur -isRegex fonctionne comme il le fait pour les règles non-GWT.

- URL de l'action :

  Plusieurs services répondant à un RPC peuvent être configurés sur le même serveur Web. La requête HTTP a l'URL du serveur Web, et non du service qui gère le RPC. Par conséquent, la relaxation n'est pas appliquée sur la base de l'URL de requête HTTP, car cela relâcherait tous les services sur cette URL pour le champ cible. Pour les requêtes GWT, le Web App Firewall utilise l'URL du service réel trouvé dans la charge utile GWT, dans le quatrième champ de la table de chaînes.

- Nom du champ :

  Étant donné que le corps de requête GWT contient uniquement des valeurs de champ, le Web App Firewall insère des noms de champ factices tels que 1, 2, etc. lors de la recommandation de règles apprises.

Exemple d'une règle d'apprentissage GWT

```
POST /abcd/def/gh HTTP/1.1
Content-type: text/x-gwt-rpc
Host: 10.217.222.75
Content-length: 157

5|0|8|http://localhost:8080/acdtest/|16878339
   F02Baf83818D264AE430C20468|
com.test.client.TestService|testMethod|java.lang.String%3b|java.
   lang.Integer|onblur|

  The learn data will be as follows:
> sh learningdata pr1 crossSiteScripting
Profile: pr1    SecurityCheck: crossSiteScripting
1)  Url:    http://localhost:8080/acdtest/  >> From GWT Payload.
    Field:  10
    Hits:   1
 Done
<!--NeedCopy-->
```

Exemple de règle de relaxation GWT

```
bind appfw profile pr1 -crossSiteScripting 1 abcd -isregex NOTREGEX
```

Messages de journal : le Web App Firewall génère des messages de journal pour les violations de vérification de sécurité détectées dans les requêtes GWT. Un message de journal généré par une requête GWT mal formée contient la chaîne « GWT » pour une identification facile.

Exemple de message de journal pour une requête GWT mal formée :

```
Dec 5 21:48:02 <local0.notice> 10.217.31.247 12/05/2014:21:48:02 GMT ns
0-PPE-0 : APPFW Message 696 0 : "GWT RPC request with malformed payload. <
blocked>"
```

Différence dans le traitement des demandes GWT par rapport aux demandes non GWT :

La même charge utile peut déclencher différentes violations de vérification de sécurité du Web App Firewall pour différents types de contenu. Prenons l'exemple suivant :

```
5|0|8|http://localhost:8080/acdtest/|16878339F02Baf83818D264AE430C20468|com
.test.client.TestService|testMethod|java.lang.String%3b|java.lang.Integer|
select|
```

Type de contenu : application/x-www-form-urlencoded :

Une requête envoyée avec ce type de contenu entraîne une violation SQL si le Type d'injection SQL est configuré pour utiliser l'une des quatre options disponibles : SQLSplCharANDKeyword,

SQLSplCharORKeyword, SQLKeyword ou SQLSplChar. Le Web App Firewall considère '&' comme le séparateur de champ et '=' comme le séparateur nom-valeur lors du traitement de la charge utile ci-dessus. Comme aucun de ces caractères n'apparaît dans le corps de la publication, le contenu entier est traité comme un seul nom de champ. Le nom du champ dans cette requête contient à la fois un caractère spécial SQL (;) et un mot-clé SQL (select). Par conséquent, les violations sont interceptées pour les quatre options de type Injection SQL.

Type de contenu : text/x-gwt-rpc :

Une demande envoyée avec ce type de contenu déclenche une violation SQL uniquement si le type d'injection SQL est défini sur l'une des trois options suivantes : SQLSplCharorKeyword, SQLKeyWord ou SQLSplChar. Aucune violation n'est déclenchée si le type d'injection SQL est défini sur SQLSplCharANDKeyword, qui est l'option par défaut. Le Web App Firewall considère que la barre | verticale est le séparateur de champ pour la charge utile ci-dessus dans la requête GWT. Par conséquent, le corps postérieur est divisé en différentes valeurs de champ de formulaire, et des noms de champ de formulaire sont ajoutés (conformément à la convention décrite plus haut). En raison de ce fractionnement, le caractère spécial SQL et le mot-clé SQL deviennent des parties de champs de formulaire distincts.

Champ du formulaire 8 : `java.lang.String%3b -\> %3b is the (;)char`

Champ du formulaire 10 : `select`

Par conséquent, lorsque Type d'injection SQL est défini sur **SQLSplchar**, le champ 8 indique la violation SQL. Pour **SQLKeyword**, le champ 10 indique la violation. L'un de ces deux champs peut indiquer une violation si le type SQL Inject est configuré avec l'option **SQLSplCharORKeyword**, qui recherche la présence d'un mot-clé ou d'un caractère spécial. Aucune violation n'est détectée pour l'option **SQLSplCharANDKeyword** par défaut, car il n'y a pas de champ unique qui contient à la fois **SQLSplChar** et **SQLKeyword** ensemble.

Conseils :

- Aucune configuration spéciale de Web App Firewall n'est nécessaire pour activer la prise en charge de GWT.
- Le type de contenu doit être text/x-gwt-rpc.
- L'apprentissage et le déploiement des règles de relaxation pour toutes les vérifications de sécurité pertinentes du Web App Firewall appliquées à la charge utile GWT fonctionnent de la même manière que pour les autres types de contenu pris en charge.
- Seules les demandes POST sont considérées comme valides pour GWT. Toutes les autres méthodes de requête sont bloquées si le type de contenu est text/x-gwt-rpc.
- Les requêtes GWT sont soumises à la limite de corps POST configurée du profil.
- Le paramètre sans session pour les vérifications de sécurité n'est pas applicable et sera ignoré.
- Le format de journal CEF est pris en charge pour les messages de journal GWT.

Protection contre les cookies

August 20, 2021

Cookie est un petit paquet de données envoyées d'un serveur Web à un navigateur client. Les cookies transportent des données sensibles telles que des mots de passe, des informations d'authentification de l'utilisateur et des informations d'identification via une connexion HTTP et stockées dans un navigateur Web. Il est donc très important de protéger les cookies contre les pirates qui volent des informations.

Vérification de la cohérence des cookies : Examine les cookies renvoyés avec les demandes des utilisateurs afin de vérifier qu'ils correspondent aux cookies définis par votre serveur Web pour cet utilisateur. Si un cookie modifié est trouvé, il est retiré de la demande avant que la demande soit transférée au serveur Web. Pour plus d'informations, consultez la rubrique Vérification de la cohérence des cookies .

Protection contre le détournement de cookies : Le détournement désigne une situation où un attaquant obtient un accès non autorisé aux cookies. Pour protéger les cookies contre l'accès autorisé, le pare-feu WAF (Web App Firewall) Citrix ADC conteste la connexion TLS du client ainsi que la validation de cohérence des cookies WAF. Pour chaque nouvelle demande client, l'appliance valide la connexion TLS et vérifie également la cohérence des cookies d'application et de session dans la requête. Pour plus d'informations, consultez la rubrique Protection contre le détournement des cookies .

Attribut de cookie Samesite : L' `SameSite` attribut de la réponse HTTP Set-Cookie vous permet de déclarer si votre cookie doit être limité à un contexte de première partie ou de même site. Le paramètre de cookie atténue les attaques et fournit une communication Web sécurisée. Pour plus d'informations, consultez la rubrique Attribut de cookie SameSite .

Vérification de la cohérence des cookies

August 20, 2021

Le contrôle de cohérence des cookies examine les cookies renvoyés par les utilisateurs, afin de vérifier qu'ils correspondent aux cookies que votre site Web a définis pour cet utilisateur. Si un cookie modifié est trouvé, il est retiré de la demande avant que la demande soit transmise au serveur Web. Vous pouvez également configurer la vérification de la cohérence des cookies pour transformer tous les cookies du serveur qu'il traite, en cryptant les cookies, en les transmettant par proxy ou en ajoutant des indicateurs aux cookies. Cette vérification s'applique aux demandes et aux réponses.

Un attaquant modifierait normalement un cookie pour accéder à des informations confidentielles sensibles en se posant comme un utilisateur précédemment authentifié, ou pour provoquer un débor-

dement de tampon. La vérification Dépassement de tampon protège contre les tentatives de dépassement de tampon à l'aide d'un cookie long. La vérification de cohérence des cookies se concentre sur le premier scénario.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue
Modifier la cohérence des cookies, sous l'onglet
Général, vous pouvez activer ou désactiver les actions suivantes :

- Bloquer
- Journal
- Apprendre
- Statistiques
- Transformez. Si elle est activée, l'action Transformer modifie tous les cookies comme spécifié dans les paramètres suivants :
  - **Chiffrer les cookies du serveur.** Chiffrer les cookies définis par votre serveur Web, à l'exception de ceux énumérés dans la liste de relaxation de vérification de la cohérence des cookies, avant de transmettre la réponse au client. Les cookies cryptés sont décryptés lorsque le client envoie une demande ultérieure, et les cookies déchiffrés sont réinsérés dans la demande avant d'être transmis au serveur Web protégé. Spécifiez l'un des types de chiffrement suivants :
    * **Aucun.** Ne pas chiffrer ou déchiffrer les cookies. Valeur par défaut.
    * **Décrypter uniquement.** Décrypter uniquement les cookies cryptés. Ne chiffrez pas les cookies.
    * **Chiffrer la session uniquement.** Chiffrer les cookies de session uniquement. Ne chiffrez pas les cookies persistants. Décrypter tous les cookies cryptés.
    * **Chiffrer tout.** Chiffrer les cookies de session et les cookies persistants. Décrypter tous les cookies cryptés.

      Remarque : lors du chiffrement des cookies, le Web App Firewall ajoute l'indicateur **HttpOnly**au cookie. Cet indicateur empêche les scripts d'accéder et d'analyser le cookie. L'indicateur empêche donc un virus basé sur des scripts ou un cheval de Troie d'accéder à un cookie déchiffré et d'utiliser ces informations pour enfreindre la sécurité. Cela est fait indépendamment des paramètres Indicateurs à ajouter dans les cookies, qui sont gérés indépendamment des paramètres de chiffrement des cookies du serveur.
- **Cookies du serveur proxy.** Proxy tous les cookies non persistants (session) définis par votre serveur Web, à l'exception de ceux répertoriés dans la liste de relaxation de vérification de la cohérence des cookies. Les cookies sont transmis par proxy à l'aide du cookie de session Web App Firewall existant. Le Web App Firewall supprime les cookies de session définis par le serveur Web protégé et les enregistre localement avant de transférer la réponse au client. Lorsque le client envoie une demande ultérieure, le Web App Firewall réinsère les cookies de session dans la demande avant de les transférer au serveur Web protégé. Spécifiez l'un des paramètres suiv-

ants :

- **Aucun.** Ne pas utiliser de cookies proxy. Valeur par défaut.
- **Session uniquement.** Cookies de session proxy uniquement. Ne pas utiliser de proxy de cookies persistants
  Remarque : Si vous désactivez le proxy des cookies après l'avoir activé (définissez cette valeur sur Aucun après avoir été défini sur Session uniquement), le proxy des cookies est maintenu pour les sessions qui ont été établies avant que vous ne l'ayez désactivé. Vous pouvez donc désactiver cette fonctionnalité en toute sécurité pendant que le Web App Firewall traite les sessions utilisateur.

- **Indicateurs à ajouter dans les cookies**. Ajouter des indicateurs aux cookies pendant la transformation. Spécifiez l'un des paramètres suivants :
  - **Aucun.** N'ajoutez pas de drapeaux aux cookies. Valeur par défaut.
  - **HTTP uniquement.** Ajoutez l'indicateur HttpOnly à tous les cookies. Les navigateurs qui prennent en charge l'indicateur HttpOnly n'autorisent pas les scripts à accéder aux cookies dont cet indicateur est défini.
  - **Sécurisé**. Ajoutez l'indicateur Secure aux cookies qui doivent être envoyés uniquement via une connexion SSL. Les navigateurs qui prennent en charge l'indicateur Secure n'envoient pas les cookies marqués sur une connexion non sécurisée.
  - **Tous.** Ajoutez l'indicateur HttpOnly à tous les cookies et l'indicateur Secure aux cookies qui doivent être envoyés uniquement via une connexion SSL.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer les commandes suivantes pour configurer la vérification de cohérence des cookies :

- `set appfw profile <name> -cookieConsistencyAction [**block**] [**learn**] [**log**] [**stats**] [**none**]`
- `set appfw profile <name> -cookieTransforms ([**ON**] | [**OFF**])`
- `set appfw profile <name> -cookieEncryption ([**none**] | [**decryptOnly**] | [**encryptSession**] | [**encryptAll**])`
- `set appfw profile <name> -cookieProxying ([**none**] | [**sessionOnly**])`
- `set appfw profile <name> -addCookieFlags ([**none**] | [**httpOnly**] | [**secure**] | [**all**])`

Pour spécifier des relaxations pour la vérification de cohérence des cookies, vous devez utiliser l'interface graphique. Sous l'onglet Vérifications de la boîte de dialogue Modifier le contrôle de cohérence des cookies, cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajouter la relaxation du contrôle de cohérence des cookies, ou sélectionnez une relaxation existante et cliquez sur Ouvrir pour ouvrir la boîte de dialogue Modifier la relaxation du contrôle de cohérence des cookies. L'une ou l'autre des boîtes de dialogue fournit les mêmes options pour configurer une relaxation.

Voici des exemples de relaxations de vérification de cohérence des cookies :

- **Champs d'ouverture de session.** L'expression suivante exempte tous les noms de cookies commençant par la chaîne logon_ suivie d'une chaîne de lettres ou de chiffres qui comporte au moins deux caractères et au plus quinze caractères :

```
^logon_[0-9A-Za-z]{
2,15 }
$
<!--NeedCopy-->
```

- **Champs d'ouverture de session (caractères spéciaux).** L'expression suivante exempte tous les noms de cookies commençant par la chaîne türkçe-logon_ suivie d'une chaîne de lettres ou de chiffres d'au moins deux caractères et d'au plus quinze caractères :

```
^txC3xBCrkxC3xA7e-logon_[0-9A-Za-z]{
2,15 }
$
<!--NeedCopy-->
```

- **Chaînes arbitraires.** Autoriser les cookies contenant la chaîne sc-item_, suivis de l'ID d'un article que l'utilisateur a ajouté à son panier ([0-9a-za-z]+), d'un deuxième soulignement (_) et enfin du nombre de ces articles qu'il souhaite ([1-9][0-9] ?) , pour être modifiable par l'utilisateur :

```
^sc-item_[0-9A-Za-z]+_[1-9][0-9]?$
<!--NeedCopy-->
```

Attention : Les expressions régulières sont puissantes. Surtout si vous n'êtes pas familier avec les expressions régulières au format PCRE, vérifiez les expressions régulières que vous écrivez. Assurez-vous qu'elles définissent exactement l'URL que vous voulez ajouter en tant qu'exception, et rien d'autre. L'utilisation négligente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (.*), peut avoir des résultats que vous ne voulez pas ou attendez pas, comme bloquer l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification de la cohérence des cookies aurait autrement bloqué.

> **Important**
>
> Dans la version 10.5.e (dans quelques versions d'amélioration provisoires antérieures à 59.13xx.e) ainsi que dans la version 11.0 (dans les versions antérieures à 65.x), le traitement de l'en-tête Cookie par Web App Firewall a été modifié. Dans ces versions, chaque cookie est évalué individuellement, et si la longueur d'un cookie reçu dans l'en-tête Cookie dépasse le BufferOverflowMaxCookieLength configuré, la violation Buffer Overflow est déclenchée. À la suite de cette modification, les requêtes qui ont été bloquées dans les versions 10.5 et antérieures peuvent être autorisées, car la longueur de l'en-tête du cookie entier n'est pas calculée pour déterminer la longueur du cookie. Dans certains cas, la taille totale des cookies

transférés au serveur peut être supérieure à la valeur acceptée, et le serveur peut répondre par « 400 Bad Request ».

Notez que cette modification a été annulée. Le comportement dans les versions 10.5.e ->59.13xx.e et 10.5.e ultérieures ainsi que dans la version 11.0 65.x et les versions ultérieures est maintenant similaire à celui des versions non améliorées de la version 10.5. L'en-tête de Cookie brut entier est maintenant pris en compte lors du calcul de la longueur du cookie. Les espaces environnants et les point-virgule (;) séparant les paires nom-valeur sont également inclus dans la détermination de la longueur du cookie.**

Remarque

Cohérence des cookies sans session : le comportement de cohérence des cookies a changé dans la version 11.0. Dans les versions antérieures, le contrôle de cohérence des cookies appelle la sessionisation. Les cookies sont stockés dans la session et signés. Un suffixe « wlt_» est ajouté aux cookies transitoires et un suffixe « wlf_ » est ajouté aux cookies persistants avant qu'ils ne soient transférés au client. Même si le client ne renvoie pas ces cookies wlf/wlt signés, le Web App Firewall utilise les cookies stockés dans la session pour effectuer le contrôle de cohérence des cookies.

Dans la version 11.0, la vérification de cohérence des cookies est sans session. Le Web App Firewall ajoute désormais un cookie qui est un hachage de tous les cookies suivis par le Web App Firewall. Si ce cookie de hachage ou tout autre cookie suivi est manquant ou altéré, le Web App Firewall supprime les cookies avant de transférer la demande au serveur back-end et déclenche une violation de cohérence des cookies. Le serveur traite la demande comme une nouvelle requête et envoie de nouveaux en-têtes Set-Cookie. La vérification de cohérence des cookies dans Citrix ADC version 13.0, 12.1 et NetScaler 12.0 et 11.1 n'a pas d'option sans session.

Protection contre le détournement de cookies

August 20, 2021

La protection contre le détournement de cookies atténue les attaques de pirates informatiques. Dans l'attaque de sécurité, un attaquant prend en charge une session utilisateur pour obtenir un accès non autorisé à une application Web. Lorsqu'un utilisateur navigue sur un site Web, par exemple une application bancaire, le site Web établit une session avec le navigateur. Pendant la session, l'application enregistre les détails de l'utilisateur tels que les informations d'identification de connexion, les visites de page dans un fichier cookie. Le fichier cookie est ensuite envoyé au navigateur client dans la réponse. Le navigateur stocke les cookies pour maintenir les sessions actives. L'attaquant peut voler ces cookies manuellement à partir du magasin de cookies du navigateur ou via une extension de navigateur rouge. L'attaquant utilise ensuite ces cookies pour accéder aux sessions d'application Web de

l'utilisateur.

Pour atténuer les attaques de cookies, le pare-feu WAF (Web App Firewall) Citrix ADC remet en question la connexion TLS du client ainsi que la validation de la cohérence des cookies WAF. Pour chaque nouvelle demande client, l'appliance valide la connexion TLS et vérifie également la cohérence des cookies d'application et de session dans la requête. Si un attaquant tente de mélanger et de faire correspondre les cookies d'application et les cookies de session volés à la victime, la validation de la cohérence des cookies échoue et l'action de détournement de cookie configurée est appliquée. Pour plus d'informations sur la cohérence des cookie, consultez la rubrique Vérification de la cohérence des cookies .

> **Remarque :**
>
> La fonction de détournement de cookies prend en charge la journalisation et les interruptions SNMP. Pour plus d'informations sur la journalisation, consultez la rubrique ADM et pour plus d'informations sur la configuration SNMP, consultez la rubrique SNMP.

Limitations

- JavaScript doit être activé dans le navigateur client.
- La protection contre le détournement de cookies n'est pas prise en charge sur TLS version 1.3.
- Prise en charge limitée du navigateur Internet Explorer (IE) car le navigateur ne réutilise pas les connexions SSL. Il en résulte plusieurs redirections envoyées pour une demande, entraînant éventuellement une erreur « REDIRECTIONS MAXIMALES EXCÉDÉES » dans le navigateur IE.

Comment fonctionne la protection contre le détournement de cookies

Les scénarios suivants expliquent comment la protection contre le détournement de cookies fonctionne dans une appliance Citrix ADC.

Scénario 1 : Utilisateur accédant à la première page Web sans cookie de session



1. L'utilisateur tente de s'authentifier dans une application Web et commence à accéder à la première page Web sans aucun cookie de session ADC dans la demande.
2. Lorsque la demande est reçue, l'appliance crée une session Application Firewall avec un ID de cookie de session.
3. Cela initie une connexion TLS pour la session. Comme le JavaScript n'est pas envoyé et exécuté sur le navigateur client, l'appliance marque la connexion TLS comme validée et aucune contestation n'est requise.

   > **Remarque :**
   >
   > Même si un attaquant tente d'envoyer tous les identifiants de cookies d'application d'une victime sans envoyer le cookie de session, l'appliance détecte le problème et supprime tous les cookies d'application dans la demande avant de transférer la demande au serveur principal. Le serveur back-end considère cette demande sans aucun cookie d'application et prend nécessaire selon sa configuration.

4. Lorsque le serveur principal envoie une réponse, l'appliance reçoit la réponse et la transmet avec un jeton de session JavaScript et un cookie de démarrage. L'appliance marque ensuite la connexion TLS comme vérifiée.
5. Lorsque le navigateur client reçoit la réponse, le navigateur exécute le JavaScript et génère un ID de cookie modifié à l'aide du jeton de session et du cookie de démarrage.
6. Lorsqu'un utilisateur envoie une requête ultérieure via la connexion TLS, l'appliance contourne la validation du cookie morphé. En effet, la connexion TLS est déjà validée.

Scénario 2 : Utilisateur accédant à des pages Web successives via une nouvelle connexion TLS avec un cookie de session



1. Lorsqu'un utilisateur envoie une requête HTTP pour des pages successives via une nouvelle connexion TLS, le navigateur envoie l'ID de cookie de session et l'ID de cookie morphed.
2. Comme il s'agit d'une nouvelle connexion TLS, l'appliance détecte la connexion TLS et défie le client avec une réponse de redirection avec le cookie de démarrage.
3. À la réception de la réponse de l'ADC, le client calcule le cookie morphé en utilisant le jeton de la session et le nouveau cookie de semence.

4. Le client envoie ensuite ce cookie morphé nouvellement calculé avec un ID de session.
5. Si le cookie morphé calculé au sein de l'appliance ADC et celui envoyé via la requête correspond, la connexion TLS est marquée comme vérifiée.
6. Si le cookie morphé calculé diffère de celui présent dans la demande du client, la validation échoue. Après quoi, l'appliance renvoie le défi au client, pour envoyer un cookie morphé approprié.

Scénario 3 : Un attaquant emprunte d'identité en tant qu'utilisateur non authentifié



1. Lorsqu'un utilisateur s'authentifie dans l'application Web, l'attaquant utilise différentes techniques pour voler les cookies et les rejouer.
2. Comme il s'agit d'une nouvelle connexion TLS de l'attaquant, l'ADC envoie un défi de redirection avec un nouveau cookie de démarrage.
3. Comme l'attaquant n'a pas JavaScript en cours d'exécution, la réponse de l'attaquant pour la demande redirigée ne contient pas le cookie morphé.
4. Il en résulte un échec de validation des cookies modifiés du côté de l'appliance ADC. L'appliance envoie à nouveau un défi de redirection au client.
5. Si le nombre de tentatives de validation des cookies modifiés dépasse la limite de seuil, l'appliance signale l'état du détournement de cookies.
6. Si l'attaquant tente de mélanger et de faire correspondre les cookies d'application et les cookies de session volés à la victime, la vérification de cohérence des cookies échoue et l'appliance applique l'action de détournement de cookies configurée.

Scénario 4 : Un attaquant emprunte d'identité en tant qu'utilisateur authentifié



1. Les attaquants peuvent également tenter de s'authentifier dans une application Web en tant qu'utilisateur authentique et rejouer les cookies de la victime pour accéder à la session Web.
2. L'appliance ADC détecte également ces attaquants usurpés. Bien qu'une connexion TLS vérifiée soit utilisée par l'attaquant lors de la relecture du cookie d'une victime, l'appliance ADC vérifie toujours si le cookie de session et le cookie d'application dans la requête sont cohérents. L'appliance vérifie la cohérence d'un cookie d'application à l'aide du cookie de session dans la requête. Étant donné que la requête contient un cookie de session d'un attaquant et un cookie d'application de la victime, la validation de cohérence des cookies échoue.
3. Par conséquent, l'appliance applique l'action de détournement de cookies configurée. Si l'action configurée est définie comme « bloc », l'appliance supprime tous les cookies de l'application et envoie la demande au serveur principal.
4. Le serveur back-end reçoit une requête sans cookie d'application et répond donc à une réponse d'erreur à l'attaquant, telle que « Utilisateur non connecté ».

Configurer le détournement de cookies à l'aide de l'interface de ligne de commande

Vous pouvez sélectionner un profil de pare-feu d'application spécifique et définir une ou plusieurs actions qui empêchent le détournement de cookies.

À l'invite de commandes, tapez :

```
set appfw profile <name> [-cookieHijackingAction <action-name> <block | log
 | stats | none>]
```

> **Remarque :**
>
> Par défaut, l'action est définie sur « none ».

Exemple :

```
set appfw profile profile1 - cookieHijackingAction Block
```


Où, les types d'action sont :

Bloquer : Bloquez les connexions qui ne respectent pas cette vérification de sécurité.
Journal : Consigner les violations de cette vérification de sécurité.
Statistiques : générez des statistiques pour cette vérification de sécurité.
Aucun : désactivez toutes les actions de cette vérification de sécurité.

Configurer le détournement de cookies à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page **Profil du Citrix Web App Firewall**, accédez à la section **Paramètres avancés** et cliquez sur **Vérifications de sécurité**.



4. Dans la section **Vérifications de sécurité**, sélectionnez **Détournement de cookies**, puis cliquez sur Paramètres **d'action**.
5. Dans la page **Paramètres de piratage des cookies**, sélectionnez une ou plusieurs actions pour empêcher le détournement de cookies.

6. Cliquez sur **OK**.



Ajouter une règle de relaxation pour la validation de la cohérence des cookies à l'aide de l'interface graphique Citrix ADC

Pour gérer les faux positifs dans la validation de la cohérence des cookies, vous pouvez ajouter une règle de relaxation pour les cookies qui peuvent être exemptés de la validation des cookies.

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page **Profil du Citrix Web App Firewall**, accédez à la section **Paramètres avancés** et cliquez sur **Règles de relaxation**.
4. Dans la section **Règles de relaxation**, sélectionnez **Cohérence des cookies** et cliquez sur **Action**.
5. Dans la page **Règle de relaxation de cohérence des cookies**, définissez les paramètres suivants.
   a) Activé. Sélectionnez si vous souhaitez activer la règle de relaxation.
   b) C'est le nom de cookie Regex. Sélectionnez si le nom du cookie est une expression régulière.
   c) Nom du cookie. Entrez le nom du cookie qui peut être exempté de la validation des cookies.
   d) Éditeur de regex. Cliquez sur cette option pour fournir les détails de l'expression régulière.
   e) Commentaires. Une brève description du cookie.
6. Cliquez sur **Créer** et **Fermer**.

Afficher les statistiques de trafic de détournement de cookies et de violations à l'aide de l'interface de ligne de commande

Affichez les détails du trafic de sécurité et des violations de sécurité dans un format tabulaire ou graphique.

Pour afficher les statistiques de sécurité :

À l'invite de commandes, tapez :

```
stat appfw profile profile1
```

Statistiques de trafic du profil Appfw	Taux (/s)	Total :
Demandes	0	0
Octets des demandes	0	0
Réponses	0	0
Octets des réponses	0	0
Abandonner	0	0
Redirections	0	0
Temps de réponse moyen à long terme (ms)	–	0
Temps de réponse moyen récent (ms)	–	0

Statistiques de violation HTML/XML/JSON	Taux (/s)	Total :
URL de démarrage	0	0
Refuser URL	0	0
En-tête Référer	0	0
Dépassement de tampon	0	0
Cohérence des cookies	0	0
Détournement de cookies	0	0
Balise de formulaire CSRF	0	0
Script inter-sites HTML	0	0
Injection SQL HTML	0	0
Format de champ	0	0
Cohérence des champs	0	0
Carte de crédit	0	0
Objet sécurisé	0	0
Violations des	0	0

Statistiques de violation HTML/XML/JSON	Taux (/s)	Total :
Type de contenu	0	0
Déni de service JSON	0	0
Injection JSON SQL	0	0
Script inter-site JSON	0	0
Types de téléchargement de fichiers	0	0
Induire Type de contenu Charge utile XML	0	0
Injection CMD HTML	0	0
Format XML	0	0
Déni de service XML (xDoS)	0	0
Validation des messages XML	0	0
Interopérabilité des services Web	0	0
Injection SQL XML	0	0
Script multisite XML	0	0
Pièce jointe XML	0	0
Violations de pannes SOAP	0	0
Violations génériques XML	0	0
Total des violations	0	0

Statistiques du journal HTML/XML/JSON	Taux (/s)	Total :
Journaux des URL de démarrage	0	0
Journaux des URL refusées	0	0
Journaux d’en-tête référer	0	0
Journaux de débordement de	0	0
Journaux de débordement de	0	0

Statistiques du journal HTML/XML/JSON	Taux (/s)	Total :
journaux de cohérence des cookies	0	0
Bûches de détournement de cookies	0	0
Journaux des balises de formulaire CSRF	0	0
Journaux de script inter-sites HTML	0	0
Journaux de transformation de script inter-site HTML	0	0
Journaux d'injection SQL HTML	0	0
Journaux de transformation HTML SQL	0	0
Journaux de format de	0	0
Journaux d'uniformité	0	0
Cartes de crédit	0	0
Logs de transformation des cartes de crédit	0	0
Journaux d'objets sûrs	0	0
Journaux signature	0	0
Journaux types de contenu	0	0
JSON Journaux de déni de service	0	0
Journaux d'injection JSON SQL	0	0
JSON Journaux de script inter-sites	0	0
Journaux des types de téléchargement	0	0
Induire le type de contenu XML Charge utile L	0	0

Statistiques du journal HTML/XML/JSON	Taux (/s)	Total :
Journaux d'injection de commandes HTML	0	0
Journaux de format XML	0	0
Journaux de déni de service XML (XDoS)	0	0
Journaux de validation des messages XML	0	0
Journaux WSI	0	0
Journaux d'injection SQL XML	0	0
Journaux de script inter-sites XML	0	0
journaux des pièces jointes XML	0	0
Journaux des défaillances SOAP	0	0
Journaux génériques XML	0	0
Nombre total de messages du journal	0	0

Statistiques de réponse aux erreurs du serveur	Taux (/s)	Total :
Erreurs client HTTP (4xx resp)	0	0
Erreurs du serveur HTTP (5xx)	0	0

Afficher les statistiques de trafic de détournement de cookies et de violations à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez un profil **Web App Firewall** et cliquez sur **Statistiques**.
3. La page **Statistiques du Citrix Web App Firewall** affiche le trafic de piratage de cookies et les détails de violation.

4. Vous pouvez sélectionner **Vue tabulaire** ou passer à la **vue graphique** pour afficher les données sous forme de tableau ou graphique.



Attribut cookie SameSite

August 20, 2021

Pour des communications Web sécurisées, Google a imposé l'utilisation de l'attribut `SameSite` cookie. En se conformant à la nouvelle `SameSite` stratégie de Google Chrome, l'appliance Citrix ADC peut gérer les cookies tiers avec l' `SameSite` attribut défini dans l' `set-cookie` en-tête. Le paramètre de cookie atténue les attaques et fournit une communication Web sécurisée.

Jusqu'en février 2020, l' `SameSite` attribut n'était pas explicitement défini dans le cookie. Le navigateur a pris la valeur par défaut comme « Aucun ». Cependant, avec certaines mises à niveau du navigateur, telles que Google Chrome 80, il y a un changement dans le comportement par défaut entre domaines dans les cookies.

Définition de la valeur de l'attribut cookie

L' `SameSite` attribut est défini sur l'une des valeurs suivantes et pour le navigateur Google Chrome, la valeur par défaut est définie comme « Lax ».

Aucune. Indique que le navigateur doit utiliser le cookie pour les requêtes dans le contexte intersite uniquement sur les connexions sécurisées.

Lax. Indique le navigateur à utiliser le cookie pour les requêtes dans le contexte du même site. Dans le contexte inter-site, seules les méthodes HTTP sûres comme la requête GET peuvent utiliser le cookie.

Strict. Utilisez le cookie uniquement lorsque l'utilisateur demande explicitement le domaine.

> **Remarque :**
>
> Si les cookies set-cookies (y compris les cookies de session de pare-feu) ont l' `SameSite` `addcookiesamesite` attribut et si l'indicateur d'attribut est activé dans le profil Pare-feu d'application Web, l' `SameSite` attribut est remplacé en fonction de la valeur configurée dans le profil.

Configurer l'attribut Samesite dans le profil Web App Firewall à l'aide de l'interface de ligne de commande

Pour configurer l' `SameSite` attribut, vous devez effectuer les étapes suivantes :

1. Activez l'attribut `SameSite` cookie.
2. Définissez l'attribut cookie pour les cookies de session appfw.

Activer l'attribut cookie « Samesite »

À l'invite de commandes, tapez :

```
set appfw profile <profile-name> -insertCookieSameSiteAttribute ( ON | OFF)
```

Exemple :

```
set appfw profile p1 -insertCookieSameSiteAttribute ON
```

Définir la même valeur d'attribut cookie de site pour les cookies de session du pare-feu d'application Web

À l'invite de commandes, tapez :

```
set appfw profile <profile-name> - cookieSameSiteAttribute ( LAX | NONE |
STRICT )
```

Exemple :

```
set appfw profile p1 - cookieSameSiteAttribute LAX
```

Où sont les types d'attributs,

Aucune. L'attribut Cookie SameSite est défini sur « none » et marqué sécurisé pour tous les cookies WAF et application.

Lax. L'attribut Cookie SameSite est défini sur « Lax » pour tous les cookies WAF et application.

Strict. L'attribut Cookie SameSite est défini sur « Lax » pour tous les cookies WAF et application.

Configurer l'attribut de cookie Samesite dans le profil Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez un profil et cliquez sur **Modifier**.
3. Dans la page **Profil du Citrix Web App Firewall**, cliquez sur **Paramètres du profil** sous **Paramètres avancés**.
4. Dans la section **Paramètres du profil**, définissez les paramètres suivants :

   a. Insérez l'`Samesite` attribut cookie. Activez la case à cocher pour activer l'`Samesite` attribut cookie.
   b. Attribut Samesite des cookies. Sélectionnez une option dans la liste déroulante pour définir la valeur du `Samesite` cookie.

5. Cliquez sur **OK** et **Terminé**.



Vérification de la prévention des fuites de données

January 21, 2021

Les contrôles de prévention des fuites de données filtrent les réponses pour éviter les fuites d'informations sensibles, telles que les numéros de carte de crédit et les numéros de sécurité sociale, à des destinataires non autorisés.

Vérification par carte de crédit

August 20, 2021

Si vous disposez d'une application qui accepte les cartes de crédit ou si vos sites Web ont accès à des serveurs de base de données qui stockent les numéros de carte de crédit, vous devez utiliser les mesures de prévention des fuites de données (DLP) et configurer la protection pour chaque type de carte de crédit que vous acceptez.

La vérification de la carte de crédit Citrix Web App Firewall empêche les pirates d'exploiter les défauts de prévention des fuites de données pour obtenir les numéros de carte de crédit de vos clients. En suivant des étapes de configuration simples, vous pouvez appliquer la protection d'une ou de plusieurs des cartes de crédit suivantes : 1) Visa, 2) Master Card, 3) Discover, 4) American Express (Amex), 5) JCB et 6) Diners Club.

La vérification de sécurité de la carte de crédit examine les réponses du serveur pour identifier les instances des numéros de carte de crédit cible et applique une action spécifiée lorsqu'un tel numéro est trouvé. L'action peut être de transformer la réponse en X'ing tous les chiffres sauf le dernier groupe de chiffres dans le numéro de carte de crédit, ou de bloquer la réponse si elle contient plus d'un nombre spécifié de numéros de carte de crédit. Si vous spécifiez les deux, l'action de blocage a priorité. Le paramètre Nombre maximal de cartes de crédit autorisées par page détermine le moment où l'action de blocage est invoquée. Le paramètre par défaut, 0 (aucun numéro de carte de crédit n'est autorisé sur la page), est le plus sûr, mais vous pouvez autoriser jusqu'à 255. Selon l'endroit où la violation est détectée dans la réponse et où l'action de blocage est déclenchée, vous pouvez obtenir moins que le nombre maximal autorisé de cartes de crédit dans la réponse.

Pour éviter les faux positifs, vous pouvez appliquer des relaxations pour exempter des numéros spécifiques du chèque de carte de crédit. Par exemple, un numéro de sécurité sociale, un numéro de bon de commande ou un numéro de compte Google peut être similaire à un numéro de carte de crédit. Vous pouvez spécifier des nombres individuels ou utiliser une expression régulière pour indiquer la chaîne de chiffres à contourner lors du traitement de l'URL de réponse pour l'inspection de carte de crédit.

Si vous n'êtes pas sûr des numéros de carte de crédit à exempter, vous pouvez utiliser la fonctionnalité d'apprentissage pour générer des recommandations basées sur les données apprises. Pour obtenir un avantage optimal sans compromettre les performances, vous pouvez activer cette option pendant une courte période pour obtenir un échantillon représentatif des règles, puis déployer les relaxations et désactiver l'apprentissage.

Si vous activez la fonction de journal, la vérification de carte de crédit génère des messages de journal indiquant les actions qu'elle prend. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives contrecarrées d'accès. Par défaut, le paramètre doSecureCreditCardLogging est ON, de sorte que le numéro de carte de crédit n'est pas inclus dans le message de journal généré par la violation de commerce sécurisé (carte de crédit).

La fonctionnalité des statistiques rassemble des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée.

Pour configurer la vérification de sécurité de la carte de crédit pour protéger votre application, configurez le profil qui régit l'inspection du trafic à destination et en provenance de cette application.

> **Remarque** :
>
> Un site Web qui n'accède pas à une base de données SQL n'a généralement pas accès à des informations confidentielles telles que les numéros de carte de crédit.

Utilisation de la ligne de commande pour configurer la vérification de carte de crédit

Dans l'interface de ligne de commande, vous pouvez utiliser la commande set appfw profile ou la commande add appfw profile pour activer la vérification de carte de crédit et spécifier les actions à effectuer. Vous pouvez utiliser la commande unset appfw profile pour revenir aux paramètres par défaut. Pour spécifier des relaxations, utilisez la commande bind appfw pour lier les numéros de carte de crédit au profil.

Pour configurer une vérification de carte de crédit à l'aide de la ligne de commande

Utilisez soit la commande set appfw profile, soit la commande add appfw profile, comme suit :

- `set appfw profile <name> -creditCardAction ( ([block][learn] [log][ stats])| [none])`
- `set appfw profile <name> -creditCard (VISA | MASTERCARD | DISCOVER | AMEX | JCB | DINERSCLUB)`
- `set appfw profile <name> -creditCardMaxAllowed <integer>`
- `set appfw profile <name> -creditCardXOut ([ON] | [OFF])<name> -doSecureCreditCard ([ON] | [OFF])`

- Pour configurer une règle de relaxation de carte de crédit à l'aide de la ligne de commande

  Utilisez la commande bind pour lier le numéro de carte de crédit au profil. Pour supprimer un numéro de carte de crédit d'un profil, utilisez la commande unbind, avec les mêmes arguments que vous avez utilisés pour la commande bind. Vous pouvez utiliser la commande show pour afficher les numéros de carte de crédit liés à un profil.

- Pour lier un numéro de carte de crédit un profil

  ```
  bind appfw profile <profile-name> -creditCardNumber <any number/regex>
  "<url>"
  ```

  Exemple : bind appfw profil test_profile -CreditCardNumber 378282246310005 `http://www.example.com/credit\\_card\\_test.html`

  - Pour dissocier un numéro de carte de crédit d'un profil

    ```
    unbind appfw profile <profile-name> -creditCardNumber <credit card
    number / regex> <url>
    ```

  - Pour afficher la liste des numéros de carte de crédit liés à un profil.

    ```
    show appfw profile <profile>
    ```

Utilisation de l'interface graphique pour configurer la vérification de carte de crédit

Dans l'interface graphique, vous configurez le contrôle de sécurité de la carte de crédit dans le volet pour le profil associé à votre application.

Pour ajouter ou modifier le contrôle de sécurité de la carte de crédit à l'aide de l'interface graphique

1. Accédez à **Web App Firewall** > **Profils, mettez en surbrillance** le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Vérifications de sécurité**.

   La table de vérification de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Vous avez 2 options de configuration :

   a) Si vous souhaitez simplement activer ou désactiver les actions Bloquer, Journaliser, Statistiques et Apprendre pour Carte de crédit, vous pouvez activer ou désactiver les cases à cocher dans le tableau, cliquez sur **OK**, puis cliquez sur **Enregistrer**et **fermer**pour fermer le volet **Contrôle de sécurité**.

   b) Si vous souhaitez configurer des options supplémentaires pour ce contrôle de sécurité, double-cliquez sur Carte de crédit ou sélectionnez la ligne et cliquez sur **Paramètres d'action** pour afficher les options supplémentaires suivantes :

      - Out : masquez tout numéro de carte de crédit détecté dans une réponse en remplaçant chaque chiffre, à l'exception des chiffres du groupe final, par la lettre « X.

- Nombre maximal de cartes de crédit autorisées par page : spécifiez le nombre de cartes de crédit pouvant être transférées au client sans déclencher une action de blocage.
- Cartes de crédit protégées. Activez ou désactivez une case à cocher pour activer ou désactiver la protection pour chaque type de carte de crédit.
- Vous pouvez également modifier les actions Bloquer, Journaliser, Statistiques et Apprendre dans le volet Paramètres de carte de crédit.

  Après avoir effectué l'une des modifications ci-dessus, cliquez sur OK pour enregistrer les modifications et revenir au tableau Vérifications de sécurité. Vous pouvez procéder à la configuration d'autres vérifications de sécurité si nécessaire. Cliquez sur OK pour enregistrer toutes les modifications apportées dans la section Vérifications de sécurité, puis cliquez sur Enregistrer et fermer pour fermer le volet Vérification de sécurité.

3. Dans le volet **Paramètres avancés**, cliquez sur **Paramètres du profil**. Pour activer ou désactiver l'enregistrement sécurisé des numéros de carte de crédit, activez ou désactivez la case à cocher **Sécuriser l'enregistrement des cartes de crédit**. (Par défaut, il est sélectionné).

   Cliquez sur **OK** pour enregistrer les modifications.

- Pour configurer une règle de relaxation de carte de crédit à l'aide de l'interface graphique

  1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
  2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**. Le tableau Règles de relaxation comporte une entrée par carte de crédit. Vous pouvez double-cliquer ou sélectionner cette ligne et cliquer sur **Modifier** pour accéder à la boîte de dialogue **Règles de relaxation de la carte de crédit**. Vous pouvez effectuer des opérations Ajouter, Modifier, Supprimer, Activer ou Désactiver pour les règles de relaxation.

Utilisation de la fonction d'apprentissage avec le chèque de carte de crédit

Lorsque l'action d'apprentissage est activée, le moteur d'apprentissage du Web App Firewall surveille le trafic et apprend les violations déclenchées. Vous pouvez inspecter périodiquement ces règles apprises. Après avoir dûment pris en considération, si vous souhaitez exempter une chaîne de chiffres spécifique du contrôle de sécurité de la carte de crédit, vous pouvez déployer la règle apprise en tant que règle de relaxation.

- Pour afficher ou utiliser les données apprises à l'aide de l'interface de ligne de commande

```
show appfw learningdata <profilename> creditCardNumber

rm appfw learningdata <profilename> -creditcardNumber <credit card
number> "<url>"
```



```
export appfw learningdata <profilename> creditCardNumber
```

- Pour afficher ou utiliser les données apprises à l'aide de l'interface graphique

  1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
  2. Dans le volet **Paramètres avancés**, cliquez sur **Règles apprises**. Vous pouvez sélectionner l'entrée Carte de crédit dans le tableau Règles apprises et double-cliquer dessus pour accéder aux règles apprises. Vous pouvez déployer les règles apprises ou modifier une règle avant de la déployer en tant que règle de relaxation. Pour ignorer une règle, vous pouvez la sélectionner et cliquer sur le bouton **Ignorer**. Vous ne pouvez modifier qu'une seule règle à la fois, mais vous pouvez sélectionner plusieurs règles à déployer ou à ignorer.

  Vous avez également la possibilité d'afficher une vue récapitulative des relaxations apprises en sélectionnant l'entrée Carte de crédit dans le tableau Règles apprises et en cliquant sur Visualizer pour obtenir une vue consolidée de toutes les violations apprises. Le visualiseur facilite la gestion des règles apprises. Il présente une vue complète des données sur un seul écran et facilite l'action sur un groupe de règles en un seul clic. Le plus grand avantage du visualiseur est qu'il recommande des expressions régulières pour consolider plusieurs règles. Vous pouvez sélectionner un sous-ensemble de ces règles, en fonction du délimiteur et de l'URL Action. Vous pouvez afficher 25, 50 ou 75 règles dans le visualiseur, en sélectionnant le nombre dans une liste déroulante. Le visualiseur des règles apprises offre la possibilité de modifier les règles et de les déployer en tant que relaxations. Ou vous pouvez ignorer les règles pour les ignorer.

Utilisation de la fonction de journal avec la vérification de carte de crédit

Lorsque l'action du journal est activée, les violations de vérification de sécurité de la carte de crédit sont enregistrées dans le journal d'audit en tant que violations APPFW_SAFECOMMERCE ou APPFW_SAFECOMMERCE_XFORM. Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur syslog distant.

Le paramètre par défaut de doSecureCreditCardLogging est ON. Si vous le remplacez par OFF, le numéro et le type de carte de crédit sont inclus dans le message de journal.

Selon les paramètres configurés pour les vérifications de carte de crédit, les messages de journal générés par le pare-feu applicatif peuvent inclure les informations suivantes :

- La réponse a été bloquée ou non bloquée.
- Les numéros de carte de crédit ont été transformés (X'd out). Un message de journal distinct est généré pour chaque numéro de carte de crédit transformé, de sorte que plusieurs messages de journal peuvent être générés lors du traitement d'une seule réponse.
- La réponse contenait le nombre maximal de numéros de carte de crédit potentiels.
- Numéros de carte de crédit et leurs types correspondants.

- Pour accéder aux messages du journal à l'aide de la ligne de commande

  Basculez vers le shell et recherchez les fichiers ns.logs dans le dossier /var/log/ pour accéder aux messages de journal relatifs aux violations de la carte de crédit :

  - Shell
  - queue -f /var/log/ns.log | grep SAFECOMMERCE

- Pour accéder aux messages du journal à l'aide de l'interface graphique

  1. L'interface utilisateur graphique Citrix inclut un outil très utile (Syslog Viewer) pour analyser les messages du journal. Vous disposez de quelques options pour accéder à la visionneuse Syslog : accédez au **profil cible** > **Vérifications de sécurité**. Mettez en surbrillance la ligne Carte de crédit et cliquez sur Journaux. Lorsque vous accédez aux journaux directement à partir de la vérification de sécurité de la carte de crédit du profil, il filtre les messages de journal et affiche uniquement les journaux relatifs à ces violations de contrôle de sécurité.

  2. Vous pouvez également accéder à la visionneuse Syslog en accédant à **NetScaler** > **Système** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation des contrôles de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de vérification de sécurité peuvent être déclenchées pendant le traitement de la demande.

     La visionneuse Syslog basée sur HTML fournit diverses options de filtre pour sélectionner uniquement les messages de journal qui vous intéressent. Pour accéder aux messages du journal des violations de vérification de sécurité de la carte de crédit, filtrez en sélectionnant APPFW dans les options déroulantes du module. Le type d'événement affiche un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous activez les cases à cocher APPFW_SAFECOMMERCE et APPFW_SAFECOMMERCE_XFORM et que vous cliquez sur le bouton Appliquer, seuls les messages relatifs aux violations de vérification de sécurité de la carte de crédit apparaissent dans la visionneuse Syslog.

     Si vous placez le curseur dans la ligne d'un message de journal spécifique, plusieurs options, telles que Module et EventType, apparaissent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans les journaux.

Exemple de message de journal au format natif lorsque la réponse n'est pas bloquée

```
1 May 29 01:26:31 <local0.info> 10.217.31.98 05/29/2015:01:26:31 GMT ns
     0-PPE-0 :
2 default APPFW APPFW_SAFECOMMERCE 2181 0 :  10.217.253.62 1098-PPE0
3 4erNfkaHy0IeGP+nv2S9Rsdu77I0000 pr_ffc http://aaron.stratum8.net/FFC/
     CreditCardMind.html
```



```
4 Maximum number of potential credit card numbers seen <not blocked>
5 <!--NeedCopy-->
```

Exemple de message de journal au format CEF lorsque la réponse est transformée

```
1 May 28 23:42:48 <local0.info> 10.217.31.98
2 CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_SAFECOMMERCE_XFORM|6|src
     =10.217.253.62
3 spt=25314 method=GET request=http://aaron.stratum8.net/FFC/
     CreditCardMind.html
4 msg=Transformed (xout) potential credit card numbers seen in server
     response
5 cn1=66 cn2=1095 cs1=pr_ffc cs2=PPE2 cs3=xzE7M0g9bovAtG/zLCrLd2zkVl80002
6 cs4=ALERT cs5=2015 act=transformed
7 <!--NeedCopy-->
```

Exemple de message de journal au format CEF lorsque la réponse est bloquée. Le numéro et le type de carte de crédit peuvent être vus dans le journal, car le paramètre doSecureCreditCardLogging est désactivé.

```
1 May 28 23:42:48 <local0.info> 10.217.31.98
2 CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_SAFECOMMERCE|6|src
     =10.217.253.62
3 spt=25314 method=GET request=http://aaron.stratum8.net/FFC/
     CreditCardMind.html
4 msg=Credit Card number 4505050504030302 of type Visa is seen in
     response cn1=68
5 cn2=1095 cs1=pr_ffc cs2=PPE2 cs3=xzE7M0g9bovAtG/zLCrLd2zkVl80002 cs4=
     ALERT cs5=2015
6 act=blocked
7 <!--NeedCopy-->
```

Statistiques pour les violations de la carte de crédit

Lorsque l'action des statistiques est activée, le compteur correspondant pour la vérification de carte de crédit est incrémenté lorsque le Web App Firewall prend une action pour cette vérification de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. L'incrémentation du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée et que le paramètre de carte de crédit max autorisé est 0, la demande d'une page contenant 20 numéros de carte de crédit incrémente le compteur de statistiques d'un lorsque la page est bloquée dès que le premier numéro de carte de crédit est détecté. Toutefois, si le bloc est désactivé et que la transformation est activée, le traitement de la même

demande incrémente le compteur de statistiques pour les journaux de 20, car chaque transformation de carte de crédit génère un message de journal distinct.

- Pour afficher les statistiques de carte de crédit à l'aide de la ligne de commande

  À l'invite de commandes, tapez :

  ```
  sh appfw stats
  ```

  Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

  ```
  stat appfw profile <profile name>
  ```

  Pour afficher les statistiques de carte de crédit à l'aide de l'interface graphique

  1. Accédez à **Système** > **Sécurité** > **Web App Firewall**.
  2. Dans le volet droit, accédez au lien **Statistiques**.
  3. Utilisez la barre de défilement pour afficher les statistiques sur les violations des cartes de crédit et les journaux. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Résumé

Notez les points suivants concernant le contrôle de sécurité de la carte de crédit :

- Le Web App Firewall vous permet de protéger les informations de carte de crédit et de détecter toute tentative d'accès à ces données sensibles.
- Pour utiliser la vérification de protection par carte de crédit, vous devez spécifier au moins un type de carte de crédit et une action. La vérification est ensuite appliquée aux profils HTML, XML et Web 2.0.
- Vous pouvez diriger la sortie de la commande sh appfw profile et grep for CreditCard pour voir toute la configuration spécifique à la carte de crédit. Par exemple, sh appfw profile my_profile | grep CreditCard affiche les paramètres configurés de différents paramètres ainsi que les règles de relaxation relatives à la vérification de carte de crédit pour le profil de Web App Firewall nommé my_profile.
- Vous pouvez exclure des numéros spécifiques de l'inspection par carte de crédit sans contourner l'inspection de contrôle de sécurité pour le reste des numéros de carte de crédit.
- La détente est disponible pour tous les modèles de cartes de crédit protégés par le Web App Firewall. Dans l'interface graphique, vous pouvez utiliser le visualiseur pour spécifier les opérations Ajouter, Modifier, Supprimer, Activer ou Désactiver sur les règles de relaxation.
- Le moteur d'apprentissage du Web App Firewall peut surveiller le trafic sortant pour recommander des règles basées sur les violations observées. La prise en charge de Visualizer est également disponible pour gérer les règles de carte de crédit apprises dans l'interface graphique. Vous pouvez modifier et déployer les règles apprises, ou les ignorer après une inspection minutieuse.

- Le paramètre du nombre de cartes de crédit autorisées s'applique à chaque réponse. Il ne concerne pas le total cumulé des numéros de carte de crédit observés pendant toute la session utilisateur.
- Le nombre de X chiffres sortis dépend de la longueur des numéros de carte de crédit. Dix chiffres sont X pour les cartes de crédit qui ont 13 à 15 chiffres. Douze chiffres sont X pour les cartes de crédit qui ont 16 chiffres. Si votre application ne nécessite pas l'envoi du numéro complet de carte de crédit dans la réponse, Citrix vous recommande d'activer cette action pour masquer les chiffres des numéros de carte de crédit.
- L'opération X-out transforme toutes les cartes de crédit et fonctionne indépendamment des paramètres configurés pour le nombre maximal de cartes de crédit autorisées. Par exemple, si la réponse contient 4 cartes de crédit et que le paramètre CreditCardMaxAllowed est défini sur 10, toutes les 4 cartes de crédit sont X'd-out, mais elles ne sont pas bloquées. Si les numéros de carte de crédit sont répartis dans le document, une réponse partielle avec des numéros X'd-out peut être envoyée au client avant que la réponse ne soit bloquée.
- Ne désactivez pas le paramètre doSecureCreditCardLogging avant d'en tenir compte. Lorsque ce paramètre est désactivé, les numéros de carte de crédit sont affichés et sont accessibles dans les messages du journal. Ces nombres ne sont pas masqués dans les journaux, même si l'action X-out est activée. Si vous envoyez des journaux à un serveur syslog distant et que les journaux sont compromis, les numéros de carte de crédit peuvent être exposés.
- Lorsque la page de réponse est bloquée en raison d'une violation de carte de crédit, le Web App Firewall ne redirige pas vers la page d'erreur.

Vérification de l'objet sécurisé

August 20, 2021

La vérification de l'objet sécurisé offre une protection configurable par l'utilisateur pour les informations commerciales sensibles, telles que les numéros de client, les numéros de commande, les numéros de téléphone ou les codes postaux spécifiques à un pays ou à une région. Une expression régulière ou un plug-in personnalisé défini par l'utilisateur indique au Web App Firewall le format de ces informations et définit les règles à utiliser pour les protéger. Si une chaîne dans une demande utilisateur correspond à une définition d'objet sécurisé, le Web App Firewall bloque la réponse, masque les informations protégées ou supprime les informations protégées de la réponse avant de les envoyer à l'utilisateur, selon la façon dont vous avez configuré cette règle d'objet sécurisé particulière.

La vérification de l'objet sécurisé empêche les attaquants d'exploiter un défaut de sécurité dans votre logiciel serveur Web ou sur votre site Web pour obtenir des informations confidentielles sensibles, telles que les numéros de carte de crédit d'entreprise ou les numéros de sécurité sociale. Si vos sites Web n'ont pas accès à ces types d'informations, vous n'avez pas besoin de configurer cette vérification.

Si vous disposez d'un panier d'achat ou d'une autre application pouvant accéder à ces informations, ou si vos sites Web ont accès à des serveurs de base de données contenant ces informations, vous devez configurer la protection de chaque type d'informations privées sensibles que vous manipulez et stockez.

> **Remarque :**
>
> Un site Web qui n'accède pas à une base de données SQL n'a généralement pas accès à des informations confidentielles sensibles.

La boîte de dialogue Vérification d'objet sécurisée est différente de celle de toute autre vérification. Chaque expression d'objet sécurisé que vous créez est l'équivalent d'une vérification de sécurité distincte, similaire à la vérification de carte de crédit, pour ce type d'informations. Si vous utilisez l'assistant ou l'interface graphique, vous ajoutez une nouvelle expression en cliquant sur Ajouter et en configurant l'expression dans la boîte de dialogue Ajouter un objet sécurisé. Vous modifiez une expression existante en la sélectionnant, puis en cliquant sur Ouvrir, puis en configurant l'expression dans la boîte de dialogue Modifier un objet sécurisé.

Dans la boîte de dialogue Objet sécurisé pour chaque expression d'objet sécurisé, vous pouvez configurer les éléments suivants :

- **Nom d'objet sécurisé.** Un nom pour votre nouvel objet sécurisé. Le nom peut commencer par une lettre, un nombre ou le symbole de trait de soulignement, et peut être composé de un à 255 lettres, chiffres et le tiret (-), point (.) livre (#), espace (), signe (@), égal (=), deux-points (:) et soulignement (_).
- **Actions.** Activez ou désactivez les actions Bloquer, Journal et Statistiques, ainsi que les actions suivantes :
  - **X-Out.** Masquez toute information correspondant à l'expression de l'objet sécurisé par la lettre « X ».
  - **Remove.** Supprimez toutes les informations correspondant à l'expression d'objet sécurisé.
- **Expression régulière.** Entrez une expression régulière compatible PCRE qui définit l'objet sécurisé. Vous pouvez créer l'expression régulière de l'une des trois façons suivantes : en tapant l'expression régulière directement dans la zone de texte, en utilisant le menu **Jetons Regex** pour entrer des éléments d'expression régulière et des symboles directement dans la zone de texte, ou en ouvrant l'éditeur d'expressions régulières et en l'utilisant pour construire l'expression. L'expression régulière doit être composée de caractères ASCII uniquement. Ne coupez pas et collez les caractères qui ne font pas partie du jeu ASCII de base de 128 caractères. Si vous souhaitez inclure des caractères non ASCII, vous devez taper manuellement ces caractères au format de codage de caractères hexadécimaux PCRE.
  Remarque : N'utilisez pas les ancres de départ (^) au début des expressions d'objet sécurisé, ni les ancres de fin ($) à la fin des expressions d'objet sécurisé. Ces entités PCRE ne sont pas prises

en charge dans les expressions d'objet sécurisé et, si elles sont utilisées, votre expression ne correspondra pas à ce qu'elle était destinée à correspondre.

- **Longueur maximale de correspondance.** Entrez un entier positif qui représente la longueur maximale de la chaîne que vous souhaitez faire correspondre. Par exemple, si vous souhaitez faire correspondre les numéros de sécurité sociale américains, saisissez le numéro onze (11) dans ce champ. Cela permet à votre expression régulière de correspondre à une chaîne avec neuf chiffres et deux traits d'union. Si vous souhaitez correspondre aux numéros de permis de conduire de la Californie, entrez le numéro huit (8).

  > **Attention :**
  >
  > Si vous n'entrez pas de longueur de correspondance maximale dans ce champ, le pare-feu d'application Web utilise la valeur par défaut un (1) lors du filtrage des chaînes correspondant à vos expressions d'objet sécurisées. Par conséquent, la plupart des expressions d'objet sûres ne parviennent pas à correspondre à leurs chaînes cibles.

Vous ne pouvez pas utiliser l'interface de ligne de commande pour configurer la vérification de l'objet sécurisé. Vous devez le configurer à l'aide de l'Assistant Web App Firewall ou de l'interface graphique.

Voici des exemples d'expressions régulières de vérification d'objet sécurisé :

- Recherchez les chaînes qui semblent être des numéros de sécurité sociale américains, qui se composent de trois chiffres (dont le premier ne doit pas être zéro), suivi d'un trait d'union, suivi de deux chiffres supplémentaires, suivi d'un second tiret, et se terminant par une chaîne de quatre chiffres supplémentaires :

```
[1-9][0-9]{
3,3 }
-[0-9]{
2,2 }
-[0-9]{
4,4 }

<!--NeedCopy-->
```

- Recherchez les chaînes qui semblent être des ID de permis de conduire californiens, qui commencent par une lettre et sont suivies d'une chaîne de sept chiffres exactement :

```
[A-Za-z][0-9]{
7,7 }

<!--NeedCopy-->
```

- Recherchez les chaînes qui semblent être des ID client qui se composent d'une chaîne de cinq caractères hexadécimaux (tous les chiffres et les lettres A à F), suivies d'un trait d'union, suivi

d'un code à trois lettres, suivi d'un second trait d'union et se terminant par une chaîne de dix chiffres :

```
[0-9A-Fa-f]{
5,5 }
-[A-Za-z]{
3,3 }
-[0-9]{
10,10 }

<!--NeedCopy-->
```

> **Attention :**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas parfaitement familier avec les expressions régulières au format PCRE, vérifiez toutes les expressions régulières que vous écrivez pour vous assurer qu'elles définissent exactement le type de chaîne que vous voulez ajouter en tant que définition d'objet sécurisé, et rien d'autre. L'utilisation imprudente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (.*), peut avoir des résultats que vous ne vouliez pas ou n'attendez pas, tels que le blocage de l'accès au contenu Web que vous n'aviez pas l'intention de bloquer.

Vérification avancée de la protection des formulaires

August 20, 2021

Les contrôles avancés de protection des formulaires examinent les données des formulaires Web pour empêcher les pirates de compromettre votre système en modifiant les formulaires Web sur vos sites Web ou en envoyant des types et quantités inattendus de données à votre site Web sous un formulaire.

> **Remarque**
>
> Les contrôles de protection SQL, de script inter-sites, FFC et FieldFormat sont appliqués si l'option **Exclure le téléchargement de fichiers des vérifications de sécurité** n'est pas définie.

Un téléchargement de fichier est également un élément de formulaire qui a champ **nom** de contrôle qui est soumis dans le cadre de la soumission de formulaire.

Pour plus d'informations, reportez-vous à cette page : Formulaires

Vérification des formats de champ

August 20, 2021

La vérification Formats de champ vérifie les données que les utilisateurs envoient à vos sites Web dans des formulaires Web. Il examine à la fois la longueur et le type de données pour s'assurer qu'elles conviennent au champ de formulaire dans lequel elles apparaissent. Si le Web App Firewall détecte des données de formulaire Web inappropriées dans une demande utilisateur, il bloque la demande.

En empêchant un attaquant d'envoyer des données de formulaire Web inappropriées à votre site Web, la vérification Formats de champ empêche certains types d'attaques sur votre site Web et vos serveurs de base de données. Par exemple, si un champ particulier s'attend à ce que l'utilisateur saisisse un numéro de téléphone, la vérification Formats de champ examine l'entrée soumise par l'utilisateur pour s'assurer que les données correspondent au format d'un numéro de téléphone. Si un champ particulier attend un prénom, la vérification Formats de champ garantit que les données de ce champ sont d'un type et d'une longueur appropriés pour un prénom. Il fait la même chose pour chaque champ de formulaire que vous le configurez pour protéger.

Cette vérification s'applique uniquement aux requêtes HTML. Il ne s'applique pas aux requêtes XML. Vous pouvez configurer les vérifications de format de champ dans les profils HTML ou Web 2.0 pour inspecter la charge utile HTML pour protéger vos applications. Le Web App Firewall prend également en charge la protection Field Format Check pour les applications Google Web Toolkit (GWT).

La vérification Formats des champs nécessite l'activation d'une ou de plusieurs actions. Le Web App Firewall examine les entrées soumises et applique les actions spécifiées.

> **Remarque**
>
> Les règles de format de champ sont des règles de resserrement. Les ajouter à la liste de relaxation à partir de données apprises agit comme une règle de blocage.
>
> Pour relâcher les règles de format de champ, supprimez « fieldname » de la liste des relaxations de format de champ.

Vous avez la possibilité de définir les formats de champ par défaut pour spécifier le type de champ et la longueur minimale et maximale des données attendues dans chaque champ de formulaire de chaque formulaire Web que vous souhaitez protéger. Vous pouvez déployer des règles de relaxation pour configurer un format de champ pour un champ individuel d'un formulaire spécifique. Plusieurs règles peuvent être ajoutées pour spécifier le nom du champ, l'URL de l'action et les formats de champ. Spécifiez Formats de champ pour accepter différents types d'entrées dans différents champs de formulaire. La fonction d'apprentissage peut fournir des recommandations pour les règles de relaxation.

Actions de format de champ : vous pouvez activer les actions Bloquer, Log, Statistiques et Apprendre. Au moins une de ces actions doit être activée pour activer la protection Contrôle du format de champ.

- **Bloc**. Si vous activez le bloc, l'action de blocage est déclenchée si l'entrée n'est pas conforme au format de champ spécifié. Si une règle a été configurée pour le champ cible, l'entrée est vérifiée par rapport à la règle spécifiée. Sinon, il est vérifié par rapport à la spécification de format de champ par défaut. Toute incompatibilité dans le type de champ ou la spécification de longueur min/max entraîne le blocage de la demande.
- **Bûche**. Si vous activez la fonction de journal, la vérification Format de champ génère des messages de journal indiquant les actions qu'elle effectue. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives malveillantes de lancer une attaque.
- **Stats**. Si elle est activée, la fonction de statistiques recueille des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée, ou vous devrez peut-être revoir la configuration pour voir si le format de champ spécifié est trop restrictif.
- **Apprendre**. Si vous n'êtes pas sûr des types de champs ou des valeurs de longueur minimale et maximale qui conviennent parfaitement à votre application, vous pouvez utiliser la fonctionnalité d'apprentissage pour générer des recommandations basées sur les données apprises. Le moteur d'apprentissage du Web App Firewall surveille le trafic et fournit des recommandations de format de champ basées sur les valeurs observées. Pour obtenir un avantage optimal sans compromettre les performances, vous pouvez activer l'option d'apprentissage pendant une courte période afin d'obtenir un échantillon représentatif des règles, puis déployer les règles et désactiver l'apprentissage.
  Remarque : le moteur d'apprentissage du pare-feu Web App ne peut distinguer que les 128 premiers octets du nom. Si un formulaire comporte plusieurs champs dont les noms correspondent aux 128 premiers octets, le moteur d'apprentissage peut ne pas être en mesure de les distinguer. De même, la règle de relaxation déployée pourrait, par inadvertance, modérer tous ces champs.

Format de champ par défaut : en plus de configurer les actions, vous pouvez configurer le format de champ par défaut pour spécifier le type de données attendu dans tous les champs de formulaire de votre application. Un type de champ peut être sélectionné comme type de format de champ. Les paramètres de longueur minimale et longueur maximale peuvent être utilisés pour spécifier la longueur des entrées autorisées. Comme alternative à Types de champs, vous pouvez utiliser les mappages de caractères pour spécifier ce qui est autorisé dans un champ (sauf dans les déploiements de cluster).

- **Type de champ** : les types de champ sont nommés expression à laquelle vous affectez des valeurs de priorité. Les expressions Type de champ spécifient les entrées autorisées et sont mises en correspondance avec les données soumises pour déterminer si les valeurs reçues sont cohérentes avec les valeurs autorisées. Les Types de champs sont vérifiés dans l'ordre de leurs numéros de priorité. Un nombre inférieur indique une priorité plus élevée. Le pare-feu de

l'application Web vous permet d'ajouter vos propres types de champs et de leur attribuer les priorités que vous souhaitez. La valeur de priorité peut varier de 0 à 64000. Les types de champs intégrés suivants sont fournis pour simplifier le processus de configuration :

```
> sh appfw fieldtype
1)      Name:  integer          Regex:  "^[+-]?[0-9]+$"
                Priority:  30           Comment:  Integer
                Builtin:  IMMUTABLE
2)      Name:  alpha            Regex:  "^[a-zA-Z]+$"
                Priority:  40           Comment:  "Alpha
                   characters"
             Builtin:  IMMUTABLE
3)      Name:  alphanum         Regex:  "^[a-zA-Z0-9]+$"
                Priority:  50           Comment:  "Alpha-numeric
                    characters"
                Builtin:  IMMUTABLE
4)      Name:  nohtml           Regex:  "^[^&<>]\*$"
                Priority:  60           Comment:  "Not HTML"
                Builtin:  IMMUTABLE
5)      Name:  any              Regex:  "^.\*$"
             Priority:  70           Comment:  Anything
                Builtin:  IMMUTABLE
    Done
>
<!--NeedCopy-->
```

> **Remarque :** Les types de champs intégrés sont IMMUABLES. Ils ne peuvent pas être modifiés ou supprimés. Tous les types de champs que vous ajoutez sont MODIFIABLES. Vous pouvez les modifier ou les supprimer.

La configuration d'un type de champ comme format de champ par défaut peut s'avérer utile lorsque vous disposez d'une expression PCRE qui peut identifier les entrées valides dans tous les champs de formulaire ou la plupart des champs de formulaire de votre application et exclure les entrées non valides. Par exemple, si toutes les entrées de vos formulaires de demande doivent contenir uniquement des chiffres et des lettres, vous pouvez utiliser le type de champ alphanum intégré comme type de champ par défaut. Tout caractère non alphanumérique tel qu'une barre oblique inverse () ou un point-virgule ; dans l'entrée déclenchera une violation. Vous pouvez également ajouter vos propres Types de champs personnalisés et les utiliser pour configurer les Formats de champs par défaut. Par exemple, si vous souhaitez que les minuscules « x », « y » et « z » soient les seuls caractères alpha autorisés, vous pouvez configurer un type de champ personnalisé avec l'expression régulière « ^[x-z]+$ ». Vous pouvez lui attribuer une priorité plus élevée (numéro de priorité inférieure) que les Types de champs intégrés et l'utiliser comme Type de champ par défaut.

- **Longueur minimale : longueur** minimale des données par défaut affectée aux champs de formulaire dans les formulaires Web qui n'ont pas de paramètre explicite. Ce paramètre est défini sur 0 par défaut, ce qui permet à l'utilisateur de laisser le champ vide. Tout paramètre supérieur oblige les utilisateurs à remplir le champ.

  Attention : Si la valeur de longueur minimale est 0 mais que le type de champ est entier, alpha ou alphanum, une demande est bloquée si un champ de saisie est laissé vide, malgré le paramètre de longueur minimale. En effet, la valeur RegEx pour ces types de champs contient un caractère +, ce qui signifie un ou plusieurs caractères. Pour distinguer un entier d'un caractère alpha, il faut au moins un caractère.

- **Longueur maximale : longueur**maximale des données par défaut attribuée aux champs de formulaire dans les formulaires Web qui n'ont pas de paramètre explicite. Ce paramètre est défini sur 65535 par défaut.

  > **Note :** Caractères par rapport aux octets. Les longueurs minimale et maximale des formats de champ représentent le nombre d'octets et non le nombre de caractères. Les langues qui ont une représentation de caractères supérieure à un octet peuvent entraîner le dépassement de la limite avec moins de caractères que le nombre configuré pour la valeur maximale. Par exemple, avec une représentation de caractères sur deux octets, la valeur maximale de 9 ne permet pas plus de 4 caractères.
  > **Astuce :** L'interface graphique vous permet de couper et de coller des caractères UTF-8 directement dans l'interface graphique sans avoir à les convertir en hexadécimal.

- **Cartes de caractères** : En plus de recommander les types de champs, le moteur d'apprentissage du Web App Firewall vous offre une option supplémentaire, Utiliser les cartes de caractères, pour déployer les règles de vérification du format. Une carte de caractères est un ensemble de tous les caractères autorisés dans un champ de formulaire particulier. Vous pouvez affiner la spécification de format de champ pour autoriser ou interdire des caractères spécifiques à l'aide de cartes de caractères. Une carte de caractères distincte est générée pour chaque champ de formulaire. Les caractères alpha et numériques sont traités différemment dans les cartes de caractères. Si un caractère alpha est visible dans l'entrée, tous les caractères [alpha de A à Z] seront autorisés par l'expression PCRE recommandée dans la carte de caractères. De même, si un chiffre est inclus, tous les chiffres [0 à 9] seront autorisés. Les caractères non imprimables sont spécifiés à l'aide de la construction x. Seuls les caractères octets dont les valeurs se situent entre 0 et 255 sont pris en compte pour les recommandations de la carte de caractères.

  Une carte de caractères peut être plus spécifique que la recommandation de type de champ correspondante. Dans certaines situations, les cartes de caractères peuvent être une meilleure option, car elles vous donnent un contrôle plus strict sur l'ensemble des caractères autorisés comme entrées. Les cartes de caractères déployées sont affichées sous forme de chaînes commençant par le préfixe « CM » suivi de chiffres. La priorité pour les cartes de caractères commence à 10000. Comme pour les Types de champs ajoutés par l'utilisateur, vous pouvez ajouter,

modifier ou supprimer un mappage de caractères. Les cartes de caractères actuellement utilisées dans les règles déployées ne peuvent pas être modifiées ou supprimées.

Remarque : Les cartes de caractères ne sont pas prises en charge dans les déploiements de cluster.

> **Remarque**
>
> Lorsque vous ajoutez une règle de formats de champ avec n'importe quel type de champ intégré et utilisez le mappage de caractères au lieu de Type de champ et que vous l'enregistrez, les modifications ne sont pas enregistrées et la règle s'affiche toujours avec Type de champ.
>
> Lorsque la carte de caractères correspond à l'un des types prédéfinis, le type de champ est réutilisé au lieu de créer une nouvelle carte de caractères.

Utilisation de la ligne de commande pour configurer la vérification du format de champ

Dans l'interface de ligne de commande, vous pouvez utiliser la commande add appfw fieldtype pour ajouter un nouveau type de champ. Vous pouvez utiliser la commande set appfw profile ou la commande add appfw profile pour configurer la vérification Format de champ et spécifier les actions à effectuer. Vous pouvez utiliser la commande unset appfw profile pour rétablir les paramètres configurés à leurs valeurs par défaut. Pour spécifier une règle de format de champ, utilisez la commande bind appfw pour lier un type de champ à un champ de formulaire et à l'URL d'action, ainsi que les spécifications de longueur minimale et maximale.

Pour ajouter, supprimer ou afficher un type de champ à l'aide de la ligne de commande :

Utilisez la commande add pour ajouter un type de champ. Vous devez spécifier le nom, l'expression régulière et la priorité lors de l'ajout d'un nouveau type de champ. Vous avez également la possibilité d'ajouter un commentaire. Vous pouvez utiliser la commande show pour afficher les Types de champs configurés. Vous pouvez également supprimer un type de champ à l'aide de la commande remove, qui requiert uniquement le nom du type de champ.

```
add [appfw] fieldType <name> <regex> <priority> [-comment <string>]
```

où :

<regex> est une expression régulière

<priority> est un entier positive_entier

Exemple :

```
1 add fieldtype "Cust_Zipcode" "^[0-9]{
2  5 }
3  [-][0-9]{
4  4 }
```



```
 $" 4

-  show [appfw] fieldType [<name>]

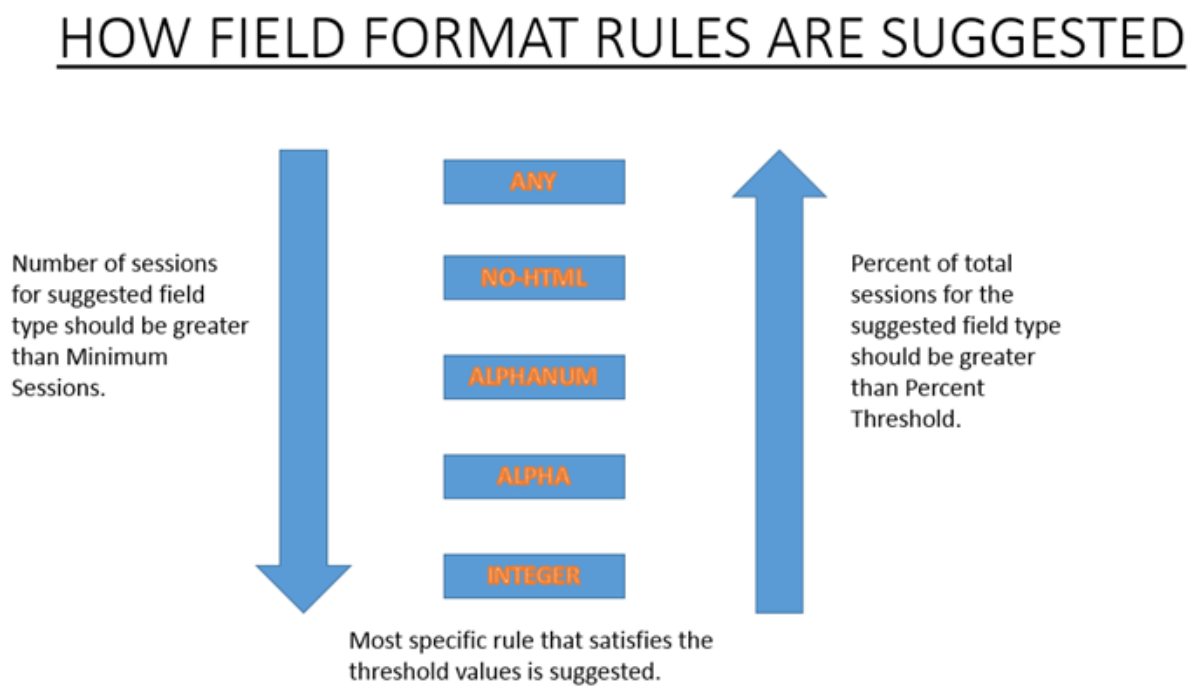
    Example: sh fieldtype

    sh appfw fieldtype

    sh appfw fieldtype cust_zipcode

-  `rm [appfw] fieldType <name>`

    Example: rm fieldtype cusT_ziPcode

    `rm appfw fieldtype cusT_ziPcode`
<!--NeedCopy-->
```

> **Remarque :** Comme indiqué ci-dessus, l'utilisation de « appfw » dans la commande est facultative. Par exemple, « Add FieldType » ou « Add appfw FieldType » sont deux options valides. Les noms des types de champ sont insensibles à la casse en raison de la normalisation. Comme indiqué dans les exemples ci-dessus, Cust_Zipcode, cust_zipcode et Cust_ZipCode font référence au même type de champ.

Pour configurer une vérification de format de champ à l'aide de la ligne de commande

Utilisez soit la commande set appfw profile, soit la commande add appfw profile, comme suit :

- `set appfw profile <name> -fieldFormatAction (([block] [learn] [log] [ stats])| [none])`
- `set appfw profile <name>-defaultFieldFormatType <string>`
- `set appfw profile <name> -defaultFieldFormatMinLength <integer>`
- `set appfw profile <name> -defaultFieldFormatMaxLength <integer>`

Pour configurer une règle de relaxation Format de champ à l'aide de la ligne de commande

```
bind appfw profile <name> (-fieldFormat <string> <formActionURL>  <
    fieldType>
[-fieldFormatMinLength <positive_integer>]  [-fieldFormatMaxLength <
    positive_integer>]
[-isRegex ( REGEX | NOTREGEX )])
<!--NeedCopy-->
```

Exemple :

```
bind appfw profile pr_ffc -fieldFormat "login_name" ".*/login.php"
    integer -fieldformatMinLength 3 -FieldformatMaxlength 6
```



```
<!--NeedCopy-->
```

Utilisation de l'interface graphique pour configurer le contrôle de sécurité des formats de champ

Dans l'interface graphique, vous pouvez gérer les Types de champs. Vous pouvez également configurer la vérification de sécurité Formats de champ dans le volet pour le profil associé à votre application.

Pour ajouter, modifier ou supprimer un type de champ à l'aide de l'interface graphique

1. Accédez au nœud Application Firewall. Dans les paramètres, cliquez sur **Gérer les types de champs** pour afficher la boîte de dialogue Configurer le type de champ du pare-feu d'application.
2. Cliquez sur **Ajouter** pour ajouter un nouveau type de champ. Suivez les instructions de ce volet et cliquez sur Créer. Vous pouvez également modifier ou supprimer tout type de champ ajouté par l'utilisateur s'il n'est pas utilisé par une règle déployée.

Pour ajouter ou modifier la vérification de sécurité Formats de champ à l'aide de l'interface graphique

1. Accédez à **Application Pare-feu** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Vérifications de sécurité**.

   La table de vérification de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Vous avez 2 options de configuration :

   a) Si vous souhaitez simplement activer ou désactiver les actions **Bloquer**, **Journaliser**, **Statistiques**et **Apprendre**pour les formats de champ, vous pouvez activer ou désactiver les cases à cocher dans le tableau, cliquez sur **OK**, puis cliquez sur **Enregistrer et fermer**pour fermer le Volet à cocher.

   b) Si vous souhaitez configurer des options supplémentaires pour cette vérification de sécurité, double-cliquez sur Formats de champ, ou sélectionnez la ligne et cliquez sur Paramètres d'action, pour afficher les options suivantes pour **Format de champ par défaut** :

   - **Type de champ** : sélectionnez le type de champ que vous souhaitez configurer comme type de champ par défaut. Vous pouvez sélectionner les types de champs intégrés et définis par l'utilisateur. Les cartes de caractères déployées sont également incluses dans la liste et peuvent être sélectionnées.
   - **Minimum Length** : spécifiez le nombre minimum de caractères devant figurer dans chaque champ. Valeurs possibles : 0-65535.
   - **Longueur maximale**(Maximum Length) : spécifiez le nombre maximal de caractères devant figurer dans chaque champ. Valeurs possibles : 1-65535.

Vous pouvez également modifier les actions **Bloquer**, **Journaliser**, **Statistiques**et **Apprendre**dans le volet Paramètres des formats de champ.

Après avoir effectué l'une des modifications ci-dessus, cliquez sur **OK** pour enregistrer les modifications et revenir au tableau Vérifications de sécurité. Vous pouvez procéder à la configuration d'autres vérifications de sécurité si nécessaire. Cliquez sur **OK** pour enregistrer toutes les modifications que vous avez apportées dans la section Contrôles de sécurité, puis cliquez sur **Enregistrer et fermer pour fermer** le volet de vérification de la sécurité.

Pour configurer une règle de relaxation Formats de champ à l'aide de l'interface graphique

1. Accédez à **Application Pare-feu** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**. La table Règles de relaxation comporte une entrée Formats de champ. Vous pouvez double-cliquer, ou sélectionner cette ligne et cliquer sur le bouton Modifier, pour accéder à la boîte de dialogue Règles de relaxation Formats de champ. Vous pouvez effectuer des opérations **Ajouter**, **Modifier**, **Supprimer**, **Activer**ou **Désactiver** pour les règles de relaxation.

Pour obtenir une vue consolidée de toutes les règles de relaxation, vous pouvez mettre en surbrillance la ligne Formats de champ et cliquer sur Visualizer. Le visualiseur pour les relaxations déployées vous offre la possibilité d' ajouter une nouvelle règle ou de modifier une règle existante. Vous pouvez également activer ou désactiver un groupe de règles en sélectionnant un nœud et en cliquant sur les boutons correspondants dans le visualiseur de relaxation.

Utilisation de la fonction d'apprentissage avec la vérification des formats de champ

Lorsque l'action d'apprentissage est activée, le moteur d'apprentissage du Web App Firewall surveille le trafic et apprend les violations déclenchées. Vous pouvez inspecter périodiquement ces règles apprises. Après avoir dûment pris en considération, vous pouvez déployer la règle apprise en tant que règle de relaxation Format de champ.

Amélioration de**l'apprentissage des formats de champ : une amélioration**de l'apprentissage du Web App Firewall a été introduite dans la version 11.0. Dans les versions précédentes, une fois que la recommandation de format de champ appris est déployée, le moteur d'apprentissage du Web App Firewall cesse de surveiller les demandes valides afin de recommander de nouvelles règles sur la base des nouveaux points de données. Cela limite la protection de sécurité configurée, car la base de données d'apprentissage n'inclut aucune représentation des nouvelles données vues dans les demandes valides traitées par le contrôle de sécurité.

Les violations ne sont plus associées à l'apprentissage. Le moteur d'apprentissage apprend et fait des recommandations pour les formats de champ quelles que soient les violations. En plus de vérifier les demandes bloquées pour déterminer si le format de champ actuel est trop restrictif et doit être

assouplie, le moteur d'apprentissage surveille également les demandes autorisées pour déterminer si le format de champ actuel est trop permissif et permet d'élever la sécurité en déployant un règle restrictive.

Voici un résumé du comportement d'apprentissage Formats de champ :

Aucun format de champ n'est lié : le comportement reste inchangé dans ce scénario. Toutes les données d'apprentissage sont envoyées au moteur aslearn. Le moteur d'apprentissage suggère une règle de format de champ basée sur l'ensemble de données.

Le**format de champ est lié** : dans les versions précédentes, les données observées sont envoyées au moteur aslearn uniquement en cas de violation. Le moteur d'apprentissage suggère une règle de format de champ basée sur l'ensemble de données. Dans la version 11.0, toutes les données sont envoyées à aslearn engine même si aucune violation n'est déclenchée. Le moteur d'apprentissage suggère une règle de format de champ basée sur l'ensemble de données de toutes les entrées reçues.

Cas d'utilisation pour l'amélioration de l'apprentissage :

Si les règles de mise en forme initiale des champs sont basées sur un petit échantillon de données, quelques valeurs non typiques peuvent donner lieu à une recommandation trop indulgente pour le champ cible. L'apprentissage continu permet au Web App Firewall d'observer les points de données de chaque demande afin de recueillir un échantillon représentatif des recommandations apprises. Ceci est utile pour renforcer encore la sécurité afin de déployer le format d'entrée optimal avec une valeur de plage adéquate.



La formation au format de champ utilise la priorité des Types de champ ainsi que les paramètres configurés des seuils d'apprentissage suivants :

- **FieldFormatminThreshold**—Nombre minimum de fois qu'un champ de formulaire spécifique doit être observé avant de générer une relaxation apprise. Par défaut : 1.
- **FieldFormatPercentThreshold**—Pourcentage de fois qu'un champ de formulaire correspond à un type de champ particulier, avant qu'une relaxation apprise ne soit générée. Par défaut : 0.

Les recommandations de règle de format de champ sont basées sur les critères suivants :

- **Recommandations de type**de champ : les recommandations de type de champ sont déterminées par les priorités attribuées aux types de champ existants et les seuils de format de champ spécifiés. Les priorités déterminent l'ordre dans lequel les Types de champs sont comparés aux entrées. Un nombre inférieur spécifie une priorité plus élevée. Par exemple, le type de champ entier a la priorité la plus élevée (30) et est donc évalué avant le type de champ alphanum (50). Les seuils déterminent le nombre d'entrées évaluées afin de recueillir un échantillon représentatif pour le point de données. L'attribution de la priorité appropriée aux Types de champ configurés et la configuration d'une valeur de **paramètre d'apprentissage** appropriée pour les paramètres **FieldFormatPercentThreshold** et **FieldFormatminThreshold** sont essentiels pour obtenir la recommandation de format de champ correcte. Le type de champ avec la priorité la plus élevée, basé sur les seuils configurés, est mis en correspondance d'abord avec les entrées. S'il y a une correspondance, ce type de champ est suggéré sans tenir compte des autres types de champ. Par exemple, trois types de champs par défaut, entier, alphanum et any correspondent si toutes les entrées contiennent uniquement des nombres. Cependant, l'entier sera recommandé car il a la priorité la plus élevée.
- **Recommandations de longueur minimale et maximale** : les calculs des longueurs minimale et maximale du format de champ sont effectués indépendamment de la détermination du type de champ. Les calculs de longueur de format de champ sont basés sur la longueur moyenne de toutes les entrées observées. La moitié de cette moyenne calculée est suggérée comme valeur min, et deux fois la valeur de cette moyenne est suggérée comme valeur maximale. La plage pour la longueur minimale est 0-65535 et la plage pour la longueur maximale est 1-65535. La valeur configurée pour la longueur minimale ne peut pas dépasser la longueur maximale.
- **Manipulation du caractère d'espace** : la vérification Format de champ compte tous les caractères d'espace lors de la vérification de la longueur Formats de champ. Les espaces de début ou de fin ne sont pas supprimés, et plusieurs espaces consécutifs au milieu de la chaîne d'entrée ne sont plus consolidés en un seul espace pendant le traitement d'entrée.

Exemple pour illustrer les recommandations du format de champ :

```
Total requests: 100
Number of Req with Field Type:
Int : 22            (22 int values)  -  22%
Alpha : 44                   (44 alpha values)  -  44%
Alphanum: 14            (14 + 44 + 22 = 80 alphanum values) = 80%
noHTML: 10              (80 + 10 = 90 noHTML values) = 90%
any : 10                     (90 + 10 = 100 any values) = 100%
```



```
8
9  % threshold                              Suggested Field Type
10 0-22                 int
11 23-44                alpha
12 45-80                alphanum
13 81-90                noHTML
14 91-100               any
15 <!--NeedCopy-->
```

Pour afficher ou utiliser les données apprises à l'aide de l'interface de ligne de commande

```
1 show appfw learningdata <profilename> FieldFormat
2 rm appfw learningdata <profilename> -fieldFormat <string>  <
     formActionURL>
3 export appfw learningdata <profilename> FieldFormat
4 <!--NeedCopy-->
```

Pour afficher ou utiliser les données apprises à l'aide de l'interface graphique

1. Accédez à **Application Pare-feu** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles apprises**. Vous pouvez sélectionner l'entrée Formats de champ dans le tableau Règles apprises et double-cliquer dessus pour accéder aux règles apprises. Vous pouvez déployer les règles apprises ou modifier une règle avant de la déployer en tant que règle de relaxation. Pour ignorer une règle, vous pouvez la sélectionner et cliquer sur le bouton **Ignorer**. Vous ne pouvez modifier qu'une seule règle à la fois, mais vous pouvez sélectionner plusieurs règles à déployer ou à ignorer.

   Vous avez également la possibilité d'afficher une vue résumée des relaxations apprises en sélectionnant l'entrée Formats de champ dans le tableau Règles apprises et en cliquant sur Visualiseur pour obtenir une vue consolidée de toutes les violations apprises. Le visualiseur facilite la gestion des règles apprises. Il présente une vue complète des données sur un seul écran et facilite l'action sur un groupe de règles en un seul clic. Le plus grand avantage du visualiseur est qu'il recommande des expressions régulières pour consolider plusieurs règles. Vous pouvez sélectionner un sous-ensemble de ces règles, en fonction du délimiteur et de l'URL Action. Vous pouvez afficher 25, 50 ou 75 règles dans le visualiseur, en sélectionnant le nombre dans une liste déroulante. Le visualiseur des règles apprises offre la possibilité de modifier les règles et de les déployer en tant que relaxations. Ou vous pouvez ignorer les règles pour les ignorer.

Utilisation de la fonction de journal avec les formats de champ, vérifiez

Lorsque l'action du journal est activée, les violations de vérification de sécurité Formats de champ sont enregistrées dans le journal d'audit en tant que violations APPFW_FIELDFORMAT. Le Web App

Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur syslog distant.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Basculez vers le shell et recherchez les fichiers ns.logs dans le dossier /var/log/ pour accéder aux messages de journal relatifs aux violations Formats de champ :

- `Shell`
- `tail -f /var/log/ns.log | grep APPFW_FIELDFORMAT`

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface utilisateur graphique Citrix inclut un outil très utile (Syslog Viewer) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez au **pare-feu des applications** > **Profils**, sélectionnez le profil cible et cliquez sur **Vérifications de sécurité**. Mettez en surbrillance la ligne Formats de champ et cliquez sur **Journaux**. Lorsque vous accédez aux journaux directement à partir de la vérification de **sécurité Formats de champ** du profil, il filtre les messages de journal et affiche uniquement les journaux relatifs à ces violations de contrôle de sécurité.
- Vous pouvez également accéder à la visionneuse Syslog en accédant à **Citrix ADC** > **Système** > **Audit**. Dans la section **Messages d'audit**, cliquez sur le lien **Messages Syslog** pour afficher la **visionneuse Syslog**, qui affiche tous les messages de journal, y compris les autres journaux de violation des contrôles de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de vérification de sécurité peuvent être déclenchées pendant le traitement de la demande.
- Accédez à **Application Firewall** > **Stratégies** > **Audit**. Dans la section **Messages d'audit**, cliquez sur le lien Messages Syslog pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation des contrôles de sécurité.

  La visionneuse Syslog basée sur HTML fournit diverses options de filtre pour sélectionner uniquement les messages de journal qui vous intéressent. Pour accéder aux messages du journal des violations de vérification de sécurité Formats de champ, filtrez en sélectionnant APPFW dans les options déroulantes du module. Le type d'événement affiche un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous activez la case à cocher **APPFW_FIELDFORMAT** et que vous cliquez sur le bouton **Appliquer**, seuls les messages relatifs aux violations de vérification de sécurité Formats de champ apparaissent dans la visionneuse Syslog.

Si vous placez le curseur dans la ligne d'un message de journal spécifique, plusieurs options, telles que Module et EventType, apparaissent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans les journaux.

Exemple de message de journal au format natif lorsque la demande n'est pas bloquée


```
Jun 10 22:32:26 <local0.info> 10.217.31.98 06/10/2015:22:32:26 GMT ns
    0-PPE-0 :
default APPFW APPFW_FIELDFORMAT 97 0 :  10.217.253.62 562-PPE0
x1MV+YnNGzQFM3Bsy2wti4bhXio0001 pr_ffc http://aaron.stratum8.net/FFC/
    login_post.php
Field format check failed for field passwd="65568888sz-*_" <not blocked
    >
Example of a CEF format log message when the request is blocked
Jun 11 00:03:51 <local0.info> 10.217.31.98
CEF:0|Citrix|Citrix ADC|NS11.0|APPFW|APPFW_FIELDFORMAT|6|src
    =10.217.253.62 spt=27076
method=POST requet=http://aaron.stratum8.net/FFC/maxlen_post.php msg=
    Field format check
failed for field text_area="" cn1=108 cn2=644 cs1=pr_ffc cs2=PPE0
cs3=GaUROfl1Nx1jJTvja5twH5BBqI0000 cs4=ALERT cs5=2015 act=blocked
<!--NeedCopy-->
```

Statistiques pour les violations de formats de champ

Lorsque l'action des statistiques est activée, le compteur correspondant pour la vérification Formats de champ est incrémenté lorsque le Web App Firewall prend une action pour cette vérification de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. L'incrémentation du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, la demande d'une page contenant 3 violations de format de champ incrémente le compteur de statistiques d'un, car la page est bloquée dès que la première violation Formats de champ est détectée. Toutefois, si le bloc est désactivé, le traitement de la même demande incrémente le compteur de statistiques pour les violations et les journaux de 3, car chaque violation Formats de champ génère un message de journal distinct.

Pour afficher les statistiques Formats de champ à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
sh appfw stats
```

Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
stat appfw profile <profile name>
```

Pour afficher les statistiques Formats de champ à l'aide de l'interface graphique

1. Accédez à **Système** > **Sécurité** > **Pare-feu d'application**.
2. Dans le volet droit, accédez au lien Statistiques.
3. Utilisez la barre de défilement pour afficher les statistiques sur les violations et les journaux des formats de champ. Le tableau des statistiques fournit des données en temps réel et est mis à

jour toutes les 7 secondes.

Conseil de déploiement

- Activer le journal des actions de format de champ, d'apprentissage et de statistiques.
- Après avoir exécuté un échantillon représentatif du trafic vers votre application, passez en revue les recommandations apprises.
- Si un type de champ est recommandé par la plupart des règles apprises, configurez ce type de champ comme type de champ par défaut. Pour les longueurs minimales et maximales, utilisez la plage la plus large suggérée par ces règles.
- Déployer des règles pour d'autres champs pour lesquels différents types de champs ou différentes longueurs minimum/maximales sont mieux adaptés.
- Activer le blocage et désactiver l'apprentissage.
- Surveiller les statistiques et les journaux. Si un nombre important de violations sont toujours déclenchées, vous pouvez consulter les messages du journal pour confirmer que les violations représentent des demandes malveillantes qui doivent avoir été bloquées. Si des demandes valides sont signalées comme des violations, vous pouvez soit modifier la règle de format de champ configurée pour la relâcher davantage ou activer à nouveau l'apprentissage pour obtenir des recommandations basées sur les nouveaux points de données.

> **Remarque :** Vous pouvez affiner votre configuration en obtenant de nouvelles recommandations d'apprentissage.

Résumé

Notez les points suivants à propos de la vérification de sécurité Field Format :

- **Protection** : en configurant des règles de format de champ optimales, vous pouvez vous protéger contre de nombreuses attaques. Par exemple, si vous spécifiez qu'un champ ne peut avoir que des entiers, les pirates ne pourront pas lancer des attaques par injection SQL ou des attaques de script inter-sites à l'aide de ce champ, car les entrées requises pour lancer de telles attaques ne répondent pas aux exigences de format de champ configuré.
- **Performances** : vous pouvez limiter la longueur minimale et la longueur maximale autorisée pour les entrées dans les règles de format de champ. Cela peut empêcher un utilisateur malveillant d'entrer des chaînes d'entrée excessivement volumineuses dans le but d'ajouter des frais de traitement au serveur, ou pire, provoquer le vidage du noyau du serveur en raison d'un débordement de pile. En limitant la taille d'entrée, vous pouvez raccourcir le temps nécessaire au traitement des demandes légitimes.
- **Configuration des formats de champ** : vous devez activer l'une des actions (bloc, journal, statistiques, apprentissage) pour activer la protection de format de champ. Vous pouvez également spécifier les règles de format de champ pour identifier les entrées autorisées dans vos

champs de formulaire.

- **Sélection de cartes de caractères par rapport à Types de champs** : les mappages de caractères et les types de champs utilisent des expressions régulières. Cependant, une carte de caractères fournit une expression plus spécifique en limitant la liste des caractères autorisés. Par exemple, pour une entrée telle que janedoe@citrix.com, le moteur d'apprentissage peut recommander le type de champ nohtml mais la carte de caractères [. @-za-Z] peut être plus spécifique, car il réduit l'ensemble autorisé de caractères non alpha. L'option Character Map permet, en plus des caractères alpha, seulement deux caractères non alpha : point (.) et at (@).
- **Apprentissage continu** : le Web App Firewall surveille et prend en compte toutes les données entrantes (violations et entrées autorisées) afin de créer une table d'apprentissage pour recommander des règles. Les règles sont révisées et mises à jour au fur et à mesure que de nouvelles données entrantes arrivent. De nouvelles règles de format de champ sont suggérées pour un champ même s'il a déjà une règle de format de champ lié. Si les formats de champ configurés sont trop restrictifs et bloquent les demandes valides, vous pouvez déployer un format de champ plus détendu. De même, si les formats de champ actuels sont trop génériques, vous pouvez affiner et renforcer la sécurité en déployant un format de champ plus restrictif.
- **Règles d'écrasement** : si une règle a déjà été déployée pour une combinaison champ/URL, l'interface graphique permet à l'utilisateur de mettre à jour le format de champ. Une boîte de dialogue demande une confirmation pour remplacer la règle existante. Si vous utilisez l'interface de ligne de commande, vous devez dissocier explicitement la liaison précédente, puis lier la nouvelle règle.
- **Correspondance multiple** : si plusieurs formats de champ correspondent à un nom de champ donné et à son URL d'action, le Web App Firewall sélectionne arbitrairement l'un d'entre eux à appliquer.
- **Limite de la mémoire tampon** : si une valeur de champ s'étend sur plusieurs tampons de streaming et que le format de ces deux parties de la valeur du champ est différent, un format de champ correspondant à « any » est envoyé à la base de données d'apprentissage.
- Format**de champ par rapport à Vérification de la cohérence**des champs : la vérification du format des champs et la vérification de la cohérence des champs sont des vérifications de protection basées sur un formulaire. La vérification Formats de champ offre un type de protection différent de celui de la vérification de cohérence des champs de formulaire. La vérification de cohérence des champs de formulaire vérifie que la structure des formulaires Web renvoyés par les utilisateurs est intacte, que les restrictions de format de données configurées dans le code HTML sont respectées et que les données des champs masqués n'ont pas été modifiées. Il peut le faire sans aucune connaissance spécifique sur vos formulaires Web autre que ce qu'il dérive du formulaire Web lui-même. La vérification Formats de champ vérifie que les données de chaque champ de formulaire correspondent aux restrictions de mise en forme spécifiques que vous avez configurées manuellement ou que la fonctionnalité d'apprentissage générée et approuvée. En d'autres termes, la vérification de cohérence des champs de formulaire applique

la sécurité générale des formulaires Web, tandis que la vérification Formats de champ applique les règles spécifiques pour les entrées autorisées pour vos formulaires Web.

Contrôle de cohérence des champs de formulaire

August 20, 2021

La vérification de cohérence des champs de formulaire examine les formulaires Web renvoyés par les utilisateurs de votre site Web et vérifie que les formulaires Web n'ont pas été modifiés de façon inappropriée par le client. Cette vérification s'applique uniquement aux demandes HTML qui contiennent un formulaire Web, avec ou sans données. Il ne s'applique pas aux requêtes XML.

La vérification de cohérence des champs de formulaire empêche les clients d'apporter des modifications non autorisées à la structure des formulaires Web de votre site Web lorsqu'ils remplissent et soumettent un formulaire. Il garantit également que les données soumises par un utilisateur respectent les restrictions HTML pour la longueur et le type, et que les données des champs masqués ne sont pas modifiées. Cela empêche un attaquant de falsifier un formulaire Web et d'utiliser le formulaire modifié pour obtenir un accès non autorisé au site Web, rediriger la sortie d'un formulaire de contact qui utilise un script non sécurisé et envoyant ainsi des courriels non sollicités en masse, ou d'exploiter une vulnérabilité dans votre logiciel de serveur Web pour prendre le contrôle du Web ou le système d'exploitation sous-jacent. Les formulaires Web constituent un maillon faible sur de nombreux sites Web et attirent un large éventail d'attaques.

La vérification de cohérence des champs de formulaire vérifie tous les éléments suivants :

- Si un champ est envoyé à l'utilisateur, la vérification garantit qu'il est renvoyé par l'utilisateur.
- La vérification applique les longueurs et les types de champs HTML.

> **Remarque :**
>
> – La vérification de cohérence des champs de formulaire applique des restrictions HTML sur le type et la longueur des données, mais ne valide pas autrement les données dans les formulaires Web. Vous pouvez utiliser la vérification Formats de champ pour configurer des règles qui valident les données renvoyées dans des champs de formulaire spécifiques de vos formulaires Web.
>
> – La protection de cohérence des champs de formulaire insère un champ masqué « as_fid » dans les formulaires de réponse envoyés au client. Le même champ masqué sera effacé par ADC lorsque le client soumet le formulaire. S'il y a un javascript côté client effectuant un calcul de somme de contrôle sur les champs du formulaire et la vérification de la même somme de contrôle sur le backend peut provoquer une rupture de l'application. Dans ce scénario, Il est recommandé de détendre le champ

> caché de la cohérence du champ de pare-feu d'application champ caché « as_fid » à partir du calcul de somme de contrôle javascript côté client.

- Si votre serveur Web n'envoie pas de champ à l'utilisateur, la vérification ne permet pas à l'utilisateur d'ajouter ce champ et d'y retourner des données.
- Si un champ est en lecture seule ou masqué, la vérification vérifie que les données n'ont pas changé.
- Si un champ est une zone de liste ou un champ de bouton radio, la vérification vérifie que les données de la réponse correspondent à l'une des valeurs de ce champ.

Si un formulaire Web renvoyé par un utilisateur viole un ou plusieurs contrôles de cohérence du champ de formulaire et que vous n'avez pas configuré le pare-feu de l'application Web pour autoriser ce formulaire Web à enfreindre les contrôles de cohérence du champ de formulaire, la demande est bloquée.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier le contrôle de cohérence des champs de formulaire, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Journaliser, Apprendre et Statistiques.

Vous configurez également la cohérence des champs sans session dans l'onglet Général. Si Cohérence des champs sans session est activée, le Web App Firewall vérifie uniquement la structure du formulaire Web, en supprimant les parties de la vérification de cohérence des champs de formulaire qui dépendent de la tenue à jour des informations de session. Cela peut accélérer la vérification de la cohérence des champs de formulaire avec peu de pénalité de sécurité pour les sites Web qui utilisent de nombreux formulaires. Pour utiliser la cohérence des champs sans session sur tous les formulaires Web, sélectionnez Activer. Pour l'utiliser uniquement pour les formulaires soumis avec la méthode HTTP POST, sélectionnez PostOnly

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer le contrôle de cohérence des champs de formulaire :

- `set appfw profile <name> -fieldConsistencyAction [**block**] [**learn**] [**log**] [**stats**] [**none**]`

Pour spécifier des relaxations pour la vérification de cohérence des champs de formulaire, vous devez utiliser l'interface graphique. Sous l'onglet Vérifications de la boîte de dialogue Modifier le contrôle de cohérence des champs de formulaire, cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajouter une relaxation du contrôle de cohérence des champs de formulaire ou sélectionnez une relaxation existante et cliquez sur Ouvrir pour ouvrir la boîte de dialogue Modifier la relaxation du contrôle de cohérence des champs de formulaire. L'une ou l'autre des boîtes de dialogue offre les mêmes options de configuration d'une relaxation, comme décrit dans Configuration manuelle à l'aide de l'interface graphique.

Voici des exemples d'assouplissements de vérification de cohérence des champs de formulaire :

Noms des champs de formulaire :

- Choisissez les champs de formulaire avec le nom UserType :

```
^UserType$
<!--NeedCopy-->
```

- Choisissez des champs de formulaire dont les noms commencent par UserType_ et sont suivis d'une chaîne qui commence par une lettre ou un chiffre et se compose de une à vingt et un lettres, des chiffres ou de l'apostrophe ou du trait d'union :

```
^UserType_[0-9A-Za-z][0-9A-Za-z'-]{
0,20 }
$
<!--NeedCopy-->
```

- Choisissez des champs de formulaire avec des noms commençant par Turkish-userType_ et qui sont autrement les mêmes que l'expression précédente, sauf qu'ils peuvent contenir des caractères spéciaux turcs dans l'ensemble :

```
^T\xC3\xBCrk\xC3\xA7e-UserType_([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa
   -f])+$
<!--NeedCopy-->
```

> **Remarque :**
>
> Voir Format de codage de caractères PCRE pour une description complète des caractères spéciaux pris en charge et comment les encoder correctement.

- Choisissez des noms de champs de formulaire qui commencent par une lettre ou un chiffre, qui sont constitués d'une combinaison de lettres et/ou de chiffres uniquement et qui contiennent la chaîne Num n'importe où dans la chaîne :

```
^[0-9A-Za-z]\*Num[0-9A-Za-z]\*$
<!--NeedCopy-->
```

URL d'action du champ de formulaire :

- Choisissez les URL commençant par`http://www.example.com/search.pl?` et contenant une chaîne après la requête, à l'exception d'une nouvelle requête :

```
^http://www[.]example[.]com/search[.]pl?[^?]*$
<!--NeedCopy-->
```

- Choisissez les URL commençant par `http://www.example-español.com` et dont les chemins d'accès et les noms de fichiers sont constitués de majuscules et minuscules, de

chiffres, de caractères spéciaux non ASCII et de symboles sélectionnés dans le chemin d'accès. Le caractère ñ et tous les autres caractères spéciaux sont représentés sous la forme de chaînes UTF-8 codées contenant le code hexadécimal attribué à chaque caractère spécial dans le jeu de caractères UTF-8 :

```
^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

- Choisissez toutes les URL qui contiennent la chaîne /search.cgi?:

```
^[^?<>]\*/search[.]cgi?[^?<>]\*$
<!--NeedCopy-->
```

> **Attention :**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas familier avec les expressions régulières au format PCRE, vérifiez les expressions régulières que vous écrivez. Assurez-vous qu'elles définissent exactement l'URL que vous voulez ajouter en tant qu'exception, et rien d'autre. L'utilisation négligente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (.*), peut avoir des résultats que vous ne voulez pas ou attendez pas, comme bloquer l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification de la cohérence des cookies aurait autrement bloqué.

Vérification du marquage des formulaires CSRF

August 20, 2021

La vérification de balisage de formulaire CSRF (Cross Site Request Request Fallgery) balises chaque formulaire Web envoyé par un site Web protégé aux utilisateurs avec un FormID unique et imprévisible, puis examine les formulaires Web renvoyés par les utilisateurs pour s'assurer que le formulaire fourni est correct. Cette vérification protège contre les attaques de falsification de requêtes intersites. Cette vérification s'applique uniquement aux demandes HTML qui contiennent un formulaire Web, avec ou sans données. Il ne s'applique pas aux requêtes XML.

La vérification du marquage des formulaires CSRF empêche les attaquants d'utiliser leurs propres formulaires Web pour envoyer des réponses de formulaire en volume élevé avec des données à vos

sites Web protégés. Ce contrôle nécessite relativement peu de capacité de traitement de l'UC par rapport à certains autres contrôles de sécurité qui analysent les formulaires Web en profondeur. Il est donc capable de gérer des attaques de volume élevé sans dégrader sérieusement les performances du site Web protégé ou du Web App Firewall lui-même.

Avant d'activer la vérification du balisage de formulaire CSRF, vous devez être conscient des éléments suivants :

- Vous devez activer le balisage des formulaires. La vérification CSRF dépend de l'étiquetage des formulaires et ne fonctionne pas sans elle.
- Vous devez désactiver la fonctionnalité de mise en cache intégrée Citrix ADC pour toutes les pages Web contenant des formulaires qui sont protégés par ce profil. La fonctionnalité de mise en cache intégrée et le balisage de formulaire CSRF ne sont pas compatibles.
- Vous devez envisager d'activer la vérification des référents. La vérification des référents fait partie de la vérification de l'URL de démarrage, mais elle empêche les falsification des requêtes intersites, et non les violations de l'URL de démarrage. La vérification des référents met également moins de charge sur l'UC que la vérification du marquage des formulaires CSRF. Si une demande ne respecte pas la vérification des référents, elle est immédiatement bloquée, de sorte que la vérification de marquage des formulaires CSRF n'est pas invoquée.
- La vérification de marquage des formulaires CSRF ne fonctionne pas avec les formulaires Web qui utilisent différents domaines dans l'URL d'origine du formulaire et l'URL d'action du formulaire. Par exemple, le balisage de formulaire CSRF ne peut pas protéger un formulaire Web avec une URL d'origine de formulaire `http://www.example.com` et une URL d'action de formulaire de `http://www.example.org/form`.pl, car example.com et example.org sont des domaines différents.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification du balisage de formulaire CSRF, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Journaliser, Apprendre et Statistiques.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification du balisage de formulaire CSRF :

- `set appfw profile <name> -CSRFtagAction [**block**] [**log**] [**learn**] [**stats**] [**none**]`

Pour spécifier des relaxations pour la vérification de marquage de formulaire CSRF, vous devez utiliser l'interface graphique. Sous l'onglet Vérifications de la boîte de dialogue Modifier le contrôle du marquage du formulaire CSRF, cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajouter la relaxation du contrôle du marquage du formulaire CSRF ou sélectionnez une relaxation existante et cliquez sur Ouvrir pour ouvrir la boîte de dialogue Modifier la relaxation du contrôle du marquage du formulaire CSRF. L'une ou l'autre des boîtes de dialogue fournit les mêmes options pour configurer une relaxation.

Une alerte est générée lorsque vous définissez la limite de session Citrix Web App Firewall sur une valeur inférieure ou égale à 0, car un tel paramètre affecte la fonctionnalité de vérification de la protection avancée qui nécessite une session de pare-feu Web App qui fonctionne correctement.

Voici des exemples d'assouplissements de vérification du marquage des formulaires CSRF :

Remarque : Les expressions suivantes sont des expressions d'URL qui peuvent être utilisées à la fois dans les rôles URL d'origine du formulaire et URL d'action de formulaire.

- Choisissez les URL commençant par`http://www.example.com/search.pl?` et contenant une chaîne après la requête, à l'exception d'une nouvelle requête :

```
^http://www[.]example[.]com/search[.]pl?[^?]*$
<!--NeedCopy-->
```

- Choisissez les URL commençant par `http://www.example-español.com` et dont les chemins d'accès et les noms de fichiers sont constitués de majuscules et minuscules, de chiffres, de caractères spéciaux non ASCII et de symboles sélectionnés dans le chemin d'accès. Le caractère ñ et tous les autres caractères spéciaux sont représentés sous la forme de chaînes UTF-8 codées contenant le code hexadécimal attribué à chaque caractère spécial dans le jeu de caractères UTF-8 :

```
^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\x[0-9A-Fa
   -f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|\x[0-9A-Fa-f
   ][0-9A-Fa-f])([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|
   php|s?html?)$
<!--NeedCopy-->
```

- Choisissez toutes les URL qui contiennent la chaîne /search.cgi?:

```
^[^?<>]\*/search[.]cgi?[^?<>]\*$
<!--NeedCopy-->
```

> **Important**
>
> Les expressions régulières sont puissantes. Si vous n'êtes pas très familier avec les expressions régulières au format PCRE, vérifiez les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement l'URL que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation négligente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (.*), peut avoir des résultats que vous ne voulez pas, comme bloquer l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification aurait autrement bloquée.
>
> **Conseil**

> Lorsque l'en-tête de référence enableValidate est activé sous l'action d'URL de démarrage, assurez-vous que l'URL d'en-tête de référence est également ajoutée à StartURL.
>
> **Remarque**
>
> Lorsque Citrix ADC atteint la limite appfw_session_limit et que les vérifications CSRF sont activées, l'application Web se bloque.
>
> Pour éviter le gel des applications Web, réduisez le délai d'expiration de session et augmentez la limite de session à l'aide des commandes suivantes :
>
> À partir de la CLI : > définir les paramètres appfw —sessiontimeout 300
> De shell : root @ns # nsapimgr_wr.sh -s appfw_session_limit=200000
>
> La journalisation et la génération d'alarmes SNMP lorsque appfw_session_limit est atteinte vous aident à résoudre les problèmes et à déboguer.

Gestion des relaxations de vérification du marquage des formulaires CSRF

August 20, 2021

Vous configurez une exception (ou une relaxation) à la vérification de sécurité du balisage de formulaire CSRF dans la boîte de dialogue Ajout de la relaxation de la vérification de la vérification de la vérification de la modification de la demande de falsification de la demande de contrefaçon de la boîte de dialogue Relaxation de la vérification de l'étiquetage.

Pour configurer une relaxation de contrôle de marquage de formulaire CSRF à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet **Profils**, sélectionnez le profil à configurer, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le profil du Web App Firewall**, cliquez sur l'onglet **Vérifications de sécurité**. L'onglet **Vérifications de sécurité** contient la liste des vérifications de sécurité du Web App Firewall.
4. Pour ajouter ou modifier une relaxation CSRF, effectuez l'une des opérations suivantes :
   - Pour ajouter une nouvelle relaxation, cliquez sur Ajouter.
   - Pour modifier une relaxation existante, sélectionnez la relaxation à modifier, puis cliquez sur **Ouvrir**.

La boîte de dialogue **Ajouter une demande de falsification de la vérification de l'étiquetage Relaxation** ou **Modifier la demande de contrefaçon de la modification de la relaxation du contrôle de l'étiquetage de la demande croisée** s'affiche. À l'exception du titre, ces boîtes de dialogue sont identiques.

5. Remplissez la boîte de dialogue comme décrit ci-dessous.
   - **Case à cocher Activé** : activez cette option pour placer cette relaxation ou cette règle en cours d'utilisation ; désactivez cette option pour la désactiver.
   - **URL d'origine du formulaire** : dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL qui héberge le formulaire.
   - **URL d'action de formulaire** : dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL vers laquelle les données saisies dans le formulaire sont livrées.
   - **Commentaires** : dans la zone de texte, tapez un commentaire. Facultatif.

   > **Remarque :**
   >
   > Pour tout élément nécessitant une expression régulière, vous pouvez taper l'expression régulière, utiliser le menu **Jetons Regex** pour insérer des éléments et des symboles d'expression régulière directement dans la zone de texte, ou cliquer sur **Éditeur Regex** pour ouvrir la boîte de dialogue **Ajouter une expression régulière**, et l'utiliser pour construire l'expression.

6. Cliquez sur **OK**. La boîte de dialogue **Add cross-site Request Tagging Check Relaxation** ou **Modify Cross-site Request Faux Tagging Check Relaxation** se ferme et vous revenez à la boîte de dialogue **Modifier le Tagging Faux Request Cross-site Tagging Check**.
7. Pour supprimer une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Supprimer**.
8. Pour activer une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Activer**.
9. Pour désactiver une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Désactiver**.
10. Pour configurer les paramètres et les relations de toutes les relaxations existantes dans un affichage graphique interactif intégré, cliquez sur **Visualizer**et utilisez les outils d'affichage.
11. Pour vérifier et configurer les règles apprises pour la vérification CSRF, cliquez sur **Apprentissage** et effectuez les étapes de la section Pour configurer et utiliser la fonctionnalité d'apprentissage.
12. Cliquez sur **OK**.

Vérifications de la protection des URL

January 21, 2021

Les contrôles de protection des URL examinent les URL de requête pour empêcher les pirates de tenter agressivement d'accéder à plusieurs URL (navigation forcée) ou d'utiliser une URL pour déclencher une vulnérabilité de sécurité connue dans les logiciels de serveur Web ou les scripts de site Web.

Démarrer la vérification de l'URL

August 20, 2021

La vérification de l'URL de démarrage examine les URL dans les demandes entrantes et bloque la tentative de connexion si l'URL ne répond pas aux critères spécifiés. Pour répondre aux critères, l'URL doit correspondre à une entrée de la liste URL de démarrage, sauf si le paramètre Imposer la fermeture de l'URL est activé. Si vous activez ce paramètre, un utilisateur qui clique sur un lien sur votre site Web est connecté à la cible de ce lien.

Le but principal de la vérification de l'URL de démarrage est d'empêcher les tentatives répétées d'accès aux URL aléatoires sur un site Web (navigation forcée) par le biais de signets, de liens externes, ou de sauter vers des pages en saisissant manuellement les URL pour ignorer les pages requises pour accéder à cette partie du site Web. Une navigation forcée peut être utilisée pour déclencher un dépassement de tampon, trouver du contenu auquel les utilisateurs n'étaient pas censés accéder directement, ou trouver une porte dérobée dans les zones sécurisées de votre serveur Web. Le Web App Firewall applique la traversée ou le chemin logique donné d'un site Web en autorisant uniquement l'accès aux URL configurées en tant qu'URL de démarrage.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification de l'URL de démarrage, sous l'onglet Général, vous pouvez activer ou désactiver Bloquer, Journal, Statistiques, Actions d'apprentissage et les paramètres suivants :

- **Imposer la fermeture de l'URL.** Permettez aux utilisateurs d'accéder à n'importe quelle page web de votre site Web en cliquant sur un lien hypertexte sur n'importe quelle autre page de votre site Web. Les utilisateurs peuvent accéder à n'importe quelle page de votre site Web accessible à partir de la page d'accueil ou de toute page de démarrage désignée en cliquant sur des hyperliens.
  Remarque : La fonction de fermeture d'URL permet à toute chaîne de requête d'être ajoutée et envoyée avec l'URL d'action d'un formulaire Web soumis à l'aide de la méthode HTTP GET. Si vos sites Web protégés utilisent des formulaires pour accéder à une base de données SQL, assurez-vous que la vérification d'injection SQL est activée et correctement configurée.
- **Fermeture d'URL sans session.** Du point de vue du client, ce type de fermeture d'URL fonctionne exactement de la même manière que la fermeture d'URL standard, sensible à la session, mais utilise un jeton intégré dans l'URL au lieu d'un cookie pour suivre l'activité de l'utilisateur, ce qui consomme beaucoup moins de ressources. Lorsque la fermeture d'URL sans session est

activée, le Web App Firewall ajoute une balise « as_url_id » à toutes les URL qui sont en fermeture d'URL.

Remarque : Lorsque vous activez la fermeture d'URL sans session (Fermeture d'URL sans session), vous devez également activer la fermeture d'URL régulière (
Forcer la fermeture d'URL) ou la fermeture d'URL sans session ne fonctionne pas.

- **Valider l'en-tête du référent.** Vérifiez que l'en-tête Referer dans une demande contenant des données de formulaire Web provenant de votre site Web protégé au lieu d'un autre site Web. Cette action vérifie que votre site Web, et non un attaquant extérieur, est la source du formulaire Web. Cela protège contre les falsifications de requêtes inter-sites (CSRF) sans nécessiter le balisage de formulaire, ce qui nécessite plus de CPU que les vérifications d'en-tête. Le Web App Firewall peut gérer l'en-tête HTTP Referer de l'une des quatre manières suivantes, selon l'option sélectionnée dans la liste déroulante :
  - **Off**—Ne pas valider l'en-tête Referer.
  - **If-Present**—Valide l'en-tête Referer si un en-tête Referer existe. Si un en-tête Referer non valide est trouvé, la demande génère une violation d'en-tête référent-référent. Si aucun en-tête Referer n'existe, la demande ne génère pas de violation d'en-tête référent-référent. Cette option permet au Web App Firewall d'effectuer la validation de l'en-tête Referer sur les demandes qui contiennent un en-tête Referer, mais ne bloque pas les demandes des utilisateurs dont le navigateur ne définit pas l'en-tête Referer ou qui utilisent des proxy Web ou des filtres qui suppriment cet en-tête.
  - **URL Always Except Start** : validez toujours l'en-tête Referer. S'il n'y a pas d'en-tête Referer et que l'URL demandée n'est pas exemptée par la règle de relaxation StarTURL, la demande génère une violation d'en-tête référent-référent. Si l'en-tête Referer est présent mais qu'il n'est pas valide, la requête génère une violation d'en-tête référent-référent.
  - **Always Except First Request**—Validez toujours l'en-tête du référent. S'il n'y a pas d'en-tête référent, seule l'URL qui est accédé en premier est autorisée. Toutes les autres URL sont bloquées sans en-tête référent valide. Si l'en-tête Referer est présent mais qu'il n'est pas valide, la requête génère une violation d'en-tête référent-référent.

Un paramètre d'URL de démarrage, **Exempter les URL de fermeture des vérifications de sécurité**, n'est pas configuré dans la boîte de dialogue Modifier la vérification d'URL de démarrage, mais est configuré dans l'onglet Paramètres du profil. Si cette option est activée, ce paramètre indique au Web App Firewall de ne pas exécuter d'autres vérifications basées sur le formulaire (telles que le script inter-site et l'inspection SQL Injection) sur les URL qui répondent aux critères de fermeture d'URL.

> **Remarque**
>
> Bien que la vérification de l'en-tête du référent et la vérification de sécurité de l'URL de démarrage partagent les mêmes paramètres d'action, il est possible de violer la vérification de l'en-tête du référent sans violer la vérification de l'URL de démarrage. La différence est visible dans les journaux, qui les violations de vérification de l'en-tête du référent de journal séparément des

> violations de vérification de l'URL de démarrage.

Les paramètres d'en-tête Referer (OFF, IF-Present, AlwaysExceptStartURLs et AlwaysExceptFirstRequest) sont organisés dans l'ordre le moins restrictif à le plus restrictif et fonctionnent comme suit :

OFF :

- En-tête du référent non coché.

If-Present :

- La requête n'a pas d'en-tête référent -> La requête est autorisée.
- La requête a l'en-tête du référent et l'URL du référent est dans la fermeture de l'URL -> La requête est autorisée.
- La requête a l'en-tête du référent et l'URL du référent **n'est pas** dans la fermeture de l'URL -> La requête est bloquée.

AlwaysExceptStartURLs :

- La requête n'a pas d'en-tête référent et l'URL de la requête est une URL de démarrage -> La requête est autorisée.
- La demande n'a pas d'en-tête référent et l'URL de la demande n'est pas une URL de démarrage ->La demande est bloquée.
- La requête a l'en-tête du référent et l'URL du référent est dans la fermeture de l'URL -> La requête est autorisée.
- La requête a l'en-tête du référent et l'URL du référent **n'est pas** dans la fermeture de l'URL -> La requête est bloquée.

AlwaysExceptFirstRequest :

- Request n'a pas d'en-tête référent et est la première URL de requête de la session -> Request is allowed.
- La requête n'a pas d'en-tête référent et **n'est pas** la première URL de requête de la session -> La requête est bloquée.
- Request a l'en-tête référent et est soit la première URL de requête de la session, soit est en fermeture d'URL -> Request is allowed.
- La requête a l'en-tête référent et n'est ni la première URL de requête de la session ni est en fermeture d'URL -> La requête est bloquée.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer les commandes suivantes pour configurer la vérification de l'URL de démarrage :

- `set appfw profile <name> -startURLAction [block] [learn] [log] [stats] [none]`
- `set appfw profile <name> -startURLClosure ([ON] | [OFF])`
- `set appfw profile <name> -sessionlessURLClosure ([ON] | [OFF])`

- `set appfw profile <name> -exemptClosureURLsFromSecurityChecks ([ON] | [OFF)`
- `set appfw profile <name> -RefererHeaderCheck ([OFF] | [if-present] | [AlwaysExceptStartURLs] | [AlwaysExceptFirstRequest])`

Pour spécifier des relaxations pour la vérification de l'URL de démarrage, vous devez utiliser l'interface graphique. Sous l'onglet Vérifications de la boîte de dialogue Modifier la vérification de l'URL de début, cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajouter la relaxation de la vérification de l'URL de début ou sélectionnez une relaxation existante et cliquez sur Ouvrir pour ouvrir la boîte de dialogue Modifier la relaxation de la vérification de l'URL de début. L'une ou l'autre des boîtes de dialogue fournit les mêmes options pour configurer une relaxation.

Voici des exemples de relaxations de vérification de l'URL de démarrage :

- Autoriser les utilisateurs à accéder à la page d'accueil à l'adresse www.example.com :

```
1 ^http://www[.]example[.]com$
2 <!--NeedCopy-->
```

- Autoriser les utilisateurs à accéder à toutes les pages Web au format HTML statique (.htm et .html), HTML analysé par serveur (.htp et .shtml), PHP (.php) et Microsoft ASP (.asp) à l'adresse www.example.com :

```
1 ^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
2 [0-9A-Za-z][0-9A-Za-z_.-]*[.](asp|htp|php|s?html?)$
3 <!--NeedCopy-->
```

- Autoriser les utilisateurs à accéder aux pages Web avec des noms de chemin d'accès ou des noms de fichiers contenant des caractères non ASCII sur www.example-español.com :

```
1 ^http://www[.]example-espaxC3xB1ol[.]com/(([0-9A-Za-z]|x[0-9A-Fa-
     f][0-9A-Fa-f])([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*
2 ([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|x[0-9A-Fa-f
     ][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
3 <!--NeedCopy-->
```

Remarque : Dans l'expression ci-dessus, chaque classe de caractères a été regroupée avec la chaîne
x[0-9a-fa-F][0-9A-Fa-f], qui correspond à toutes les chaînes de codage de caractères correctement construites, mais n'autorise pas les barres obliques inverse errantes qui ne sont pas associées à une chaîne de codage de caractères UTF-8. La double barre oblique inverse () est une barre oblique inverse échappée, qui indique au Web App Firewall de l'interpréter comme une barre oblique inverse littérale. Si vous n'incluez qu'une barre oblique inverse, le Web App Firewall interpréterait à la place le crochet gauche suivant ([) comme un caractère littéral au lieu de

l'ouverture d'une classe de caractères, ce qui romprait l'expression.

- Autoriser les utilisateurs à accéder à tous les graphiques au format GIF (.png), JPEG (.jpg et .jpeg) et PNG (.png) à l'adresse www.example.com :

```
^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
[0-9A-Za-z][0-9A-Za-z_.-]*[.](gif|jpe?g|png)$
<!--NeedCopy-->
```

- Autoriser les utilisateurs à accéder aux scripts CGI (.cgi) et PERL (.pl), mais uniquement dans le répertoire CGI-BIN :

```
^http://www[.]example[.]com/CGI-BIN/[0-9A-Za-z][0-9A-Za-z_
   .-]*[.](cgi|pl)$
<!--NeedCopy-->
```

- Autoriser les utilisateurs à accéder à Microsoft Office et à d'autres fichiers de documents dans le répertoire docsarchive :

```
^http://www[.]example[.]com/docsarchive/[0-9A-Za-z][0-9A-Za-z_
   -.]*[.](doc|xls|pdf|ppt)$
<!--NeedCopy-->
```

> **Remarque**
>
> Par défaut, toutes les URL du Web App Firewall sont considérées comme des expressions régulières.

Attention : Les expressions régulières sont puissantes. Surtout si vous n'êtes pas familier avec les expressions régulières au format PCRE, vérifiez les expressions régulières que vous écrivez. Assurez-vous qu'elles définissent exactement l'URL que vous voulez ajouter en tant qu'exception, et rien d'autre. L'utilisation négligente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (
.*), peut avoir des résultats que vous ne voulez pas, comme bloquer l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification de l'URL de démarrage aurait autrement bloquée.

> **Conseil**
>
> Vous pouvez ajouter le *-and-* à la liste autorisée de mots-clés SQL pour le schéma d'attribution de noms d'URL. Par exemple, https://FQDN/bread-and-butter.

Refuser la vérification de l'URL

August 20, 2021

La vérification de l'URL refusée examine et bloque les connexions aux URL auxquelles les pirates et les codes malveillants accèdent couramment. Cette vérification contient une liste d'URL qui sont des cibles communes de pirates ou de code malveillant et qui apparaissent rarement, voire jamais, dans des requêtes légitimes. Vous pouvez également ajouter des URL ou des motifs d'URL à la liste. La vérification Refuser l'URL empêche les attaques contre diverses faiblesses de sécurité connues dans les logiciels de serveur Web ou sur de nombreux sites Web.

La vérification de l'URL Refuser est prioritaire sur la vérification de l'URL de démarrage et refuse ainsi toute tentative de connexion malveillante même si une relaxation de l'URL de démarrage permet normalement à une demande de poursuivre.

Dans la boîte de dialogue Modifier la vérification de l'URL refusée, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Journal et Statistiques.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification de l'URL Refuser :

- `set appfw profile <name> -denyURLAction [**block**] [**log**] [**stats**] [**none**]`

Pour créer et configurer vos propres URL de refus, vous devez utiliser l'interface graphique. Sous l'onglet Vérifications de la boîte de dialogue Modifier la vérification de l'URL de refus, cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajouter une URL de refus ou sélectionnez une URL de refus définie par l'utilisateur et cliquez sur Ouvrir pour ouvrir la boîte de dialogue Modifier l'URL de refus. L'une ou l'autre des boîtes de dialogue fournit les mêmes options pour créer et configurer une URL de refus.

Voici des exemples d'expressions d'URL Deny :

- N'autorisez pas les utilisateurs à accéder directement au serveur d'images sur images.example.com :

```
1 ^http://images[.]example[.]com$
2 <!--NeedCopy-->
```

- N'autorisez pas les utilisateurs à accéder directement aux scripts CGI (.cgi) ou PERL (.pl) :

```
1 ^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
2 [0-9A-Za-z][0-9A-Za-z_.-]*[.](cgi|pl)$
3 <!--NeedCopy-->
```

- Voici la même URL de refus, modifiée pour prendre en charge les caractères non-ASCII :


```
^http://www[.]example[.]com/(([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])*[.](cgi|pl)$
<!--NeedCopy-->
```

> **Attention :**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas familier avec les expressions régulières au format PCRE, vérifiez les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement l'URL ou le motif que vous voulez bloquer, et rien d'autre. L'utilisation négligente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (.*), peut avoir des résultats que vous ne voulez pas, tels que le blocage de l'accès au contenu Web que vous n'aviez pas l'intention de bloquer.

Vérifications de protection XML

January 21, 2021

Les contrôles XML Protection examinent les demandes d'attaques basées sur XML de tous types.

> **Attention :**
>
> Les vérifications de sécurité XML s'appliquent uniquement au contenu envoyé avec un en-tête de type de contenu HTTP text/xml. Si l'en-tête de type de contenu est manquant ou est défini sur une valeur différente, toutes les vérifications de sécurité XML sont contournées. Si vous envisagez de protéger les applications Web XML ou Web 2.0, les webmasters de chaque serveur Web hébergeant ces applications doivent s'assurer que l'en-tête de type de contenu HTTP approprié est envoyé.

Vérification du format XML

January 21, 2021

La vérification Format XML examine le format XML des demandes entrantes et bloque les demandes qui ne sont pas bien formées ou qui ne répondent pas aux critères de la spécification XML pour les documents XML correctement formés. Certains de ces critères sont les suivants :

- Un document XML doit contenir uniquement des caractères Unicode codés correctement qui correspondent à la spécification Unicode.
- Aucun caractère de syntaxe XML spécial, tel que <, > et &, ne peut être inclus dans le document, sauf lorsqu'il est utilisé dans le balisage XML.
- Toutes les balises de début, de fin et d'élément vide doivent être imbriquées correctement, sans qu'il soit manquant ou superposé.
- Les balises d'éléments XML sont sensibles à la casse. Toutes les balises de début et de fin doivent correspondre exactement.
- Un seul élément racine doit contenir tous les autres éléments du document XML.

Un document qui ne répond pas aux critères d'un XML bien formé ne répond pas à la définition d'un document XML. Strictement parlant, ce n'est pas XML. Cependant, toutes les applications XML et les services Web n'appliquent pas la norme XML bien formée, et tous ne gèrent pas correctement les XML mal formés ou non valides. Une manipulation inappropriée d'un document XML mal formé peut entraîner des failles de sécurité. Le but de la vérification du format XML est d'empêcher un utilisateur malveillant d'utiliser une requête XML mal formée pour enfreindre la sécurité de votre application XML ou service Web.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification du format XML, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Journal et Statistiques.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification du format XML :

- `set appfw profile <name> -xmlFormatAction [**block**] [**log**] [**stats**] [**none**]`

Vous ne pouvez pas configurer les exceptions à la vérification Format XML. Vous ne pouvez l'activer ou le désactiver que.

Vérification par déni de service XML

August 20, 2021

La vérification du déni de service XML (XML DoS ou XDoS) examine les demandes XML entrantes pour déterminer si elles correspondent aux caractéristiques d'une attaque par déni de service (DoS). S'il y a une correspondance, bloque ces requêtes. Le but de la vérification XML DoS est d'empêcher un attaquant d'utiliser des requêtes XML pour lancer une attaque par déni de service sur votre serveur Web ou site Web.

Si vous utilisez l'Assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification du déni de service XML, sous l'onglet **Général**, vous pouvez activer ou désactiver les actions Bloquer,

Journal, Statistiques et Learn :

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification de déni de service XML :

- `set appfw profile <name> -xmlDoSAction [**block**] [**log**] [**learn**] [**stats**] [**none**]`

Pour configurer des règles de déni de service XML individuelles, vous devez utiliser l'interface graphique. Sous l'onglet **Vérifications** de la boîte de dialogue **Modifier la vérification du déni de service XML**, sélectionnez une règle et cliquez sur **Ouvrir** pour ouvrir la boîte de dialogue **Modifier le déni de service XML** pour cette règle. Les boîtes de dialogue individuelles diffèrent selon les règles mais sont simples. Certains vous permettent uniquement d'activer ou de désactiver la règle ; d'autres vous permettent de modifier un nombre en tapant une nouvelle valeur dans une zone de texte.

> **Remarque :**
>
> Le comportement attendu du moteur d'apprentissage pour les attaques par déni de service est basé sur l'action configurée. Si l'action est définie comme « Bloquer », le moteur apprend la valeur de liaison configurée +1 et l'analyse XML s'arrête en cas de violation. Si l'action configurée n'est pas définie comme « Bloquer », le moteur apprend la valeur réelle de longueur de violation entrante.

Les règles de déni de service XML individuelles sont les suivantes :

- Profondeur maximale de l'élément. Limitez le nombre maximal de niveaux imbriqués dans chaque élément individuel à 256. Si cette règle est activée et que le Web App Firewall détecte une demande XML avec un élément dont le nombre maximal de niveaux autorisés est supérieur au nombre maximal, il bloque la demande. Vous pouvez modifier le nombre maximal de niveaux à n'importe quelle valeur de un (1) à 65 535.
- Longueur maximale du nom de l'élément. Limitez la longueur maximale de chaque nom d'élément à 128 caractères. Cela inclut le nom dans l'espace de noms développé, qui inclut le chemin d'accès XML et le nom de l'élément dans le format suivant :

```
1 {
2 http://prefix.example.com/path/ }
3 target_page.xml
4 <!--NeedCopy-->
```

L'utilisateur peut modifier la longueur maximale du nom à n'importe quelle valeur comprise entre un (1) caractère et 65 535.

- Nombre maximum d'éléments. Limitez le nombre maximal d'un type d'élément par document XML à 65 535. Vous pouvez modifier le nombre maximal d'éléments à n'importe quelle valeur comprise entre un (1) et 65 535.

- Nombre maximum d'enfants d'élément. Limitez le nombre maximal d'enfants (y compris les autres éléments, les informations de caractère et les commentaires) que chaque élément individuel est autorisé à avoir à 65 535. Vous pouvez modifier le nombre maximal d'enfants d'élément à n'importe quelle valeur comprise entre un (1) et 65 535.
- Nombre maximum d'attributs. Restreindre le nombre maximal d'attributs que chaque élément individuel est autorisé à avoir à 256. Vous pouvez modifier le nombre maximal d'attributs à n'importe quelle valeur comprise entre un (1) et 256.
- Longueur maximale du nom d'attribut. Limitez la longueur maximale de chaque nom d'attribut à 128 caractères. Vous pouvez modifier la longueur maximale du nom d'attribut à n'importe quelle valeur comprise entre un (1) et 2,048.
- Longueur maximale de la valeur d'attribut. Limitez la longueur maximale de chaque valeur d'attribut à 2048 caractères. Vous pouvez modifier la longueur maximale du nom d'attribut à n'importe quelle valeur comprise entre un (1) et 2,048.
- Longueur maximale des données de caractère. Limitez la longueur maximale des données de caractères pour chaque élément à 65 535. Vous pouvez modifier la longueur à n'importe quelle valeur comprise entre un (1) et 65 535.
- Taille maximale du fichier. Limitez la taille de chaque fichier à 20 Mo. Vous pouvez modifier la taille maximale du fichier à n'importe quelle valeur.
- Taille minimale du fichier. Exiger que chaque fichier ait une longueur minimale de 9 octets. Vous pouvez modifier la taille minimale du fichier à n'importe quel entier positif représentant différents octets.
- Nombre maximal d'extensions d'entités. Limitez le nombre d'extensions d'entités autorisées au nombre spécifié. Par défaut : 1024.
- Profondeur maximale d'extension de l'entité. Limitez le nombre maximal d'expansions d'entités imbriquées au nombre spécifié. Par défaut : 32.
- Nombre maximum d'espaces de noms. Limitez le nombre de déclarations d'espace de noms dans un document XML au maximum au nombre spécifié. Par défaut : 16.
- Longueur maximale de l'URI d'espace de noms. Limitez la longueur d'URL de chaque déclaration d'espace de noms au maximum le nombre de caractères spécifié. Par défaut : 256.
- Instructions de traitement des blocs. Bloquer toutes les instructions spéciales de traitement incluses dans la demande. Cette règle ne comporte aucune valeur modifiable par l'utilisateur.
- Bloquer la DTD. Bloquer toutes les définitions de type de document (DTD) incluses dans la demande. Cette règle ne comporte aucune valeur modifiable par l'utilisateur.
- Bloquer les entités externes. Bloquer toutes les références aux entités externes dans la demande. Cette règle ne comporte aucune valeur modifiable par l'utilisateur.

- Vérification de la baie SOAP. Activez ou désactivez les vérifications de tableau SOAP suivantes :
  - **Taille maximale du tableau SOAP.** Taille totale maximale de toutes les baies SOAP dans une requête XML avant que la connexion ne soit bloquée. Vous pouvez modifier cette valeur. Par défaut : 20000000.
  - **Rang maximum du tableau SOAP.** Rang ou dimensions maximum d'un tableau SOAP unique dans une requête XML avant que la connexion ne soit bloquée. Vous pouvez modifier cette valeur. Par défaut : 16.

Vérification des scripts inter-sites XML

August 20, 2021

La vérification XML cross-site Scripting examine les demandes des utilisateurs pour d'éventuelles attaques de script intersite dans la charge utile XML. S'il détecte une attaque de script intersite possible, il bloque la demande.

Pour éviter l'utilisation abusive des scripts sur vos services Web protégés afin d'enfreindre la sécurité de vos services Web, la vérification XML cross-site scripting bloque les scripts qui enfreignent la même règle d'origine, qui indique que les scripts ne doivent ni accéder ni modifier du contenu sur un serveur, sauf le serveur sur lequel ils se trouvent. Tout script qui enfreint la même règle d'origine est appelé script intersite, et la pratique consistant à utiliser des scripts pour accéder ou modifier du contenu sur un autre serveur est appelée script intersite. La raison pour laquelle le script inter-site est un problème de sécurité est qu'un serveur Web qui autorise le script inter-site peut être attaqué avec un script qui ne se trouve pas sur ce serveur Web, mais sur un autre serveur Web, tel qu'un serveur détenu et contrôlé par l'attaquant.

Le Web App Firewall offre diverses options d'action pour implémenter la protection XML cross-site Scripting. Vous avez la possibilité de configurer les actions **Bloquer**, **Log**et **Stats**.

La vérification des scripts inter-sites XML du Web App Firewall est effectuée sur la charge utile des demandes entrantes et les chaînes d'attaque sont identifiées même si elles sont réparties sur plusieurs lignes. La vérification recherche les chaînes d'attaque de script inter-site dans l' **élément** et les valeurs **d'attribut**. Vous pouvez appliquer des relaxations pour contourner l'inspection de contrôle de sécurité dans des conditions spécifiées. Les journaux et les statistiques peuvent vous aider à identifier les relaxations nécessaires.

La section CDATA de la charge utile XML peut être un domaine d'intérêt intéressant pour les pirates car les scripts ne sont pas exécutables en dehors de la section CDATA. Une section CDATA est utilisée pour le contenu qui doit être traité entièrement comme des données de caractère. Les délimiteurs de balise HTML marquent **<**, **>**et **/>**n'entraîneront pas l'analyseur à interpréter le code comme des

éléments HTML. L'exemple suivant montre une section CDATA avec une chaîne d'attaque de script inter-site :

```
1      <![CDATA[rn
2      <script language="Javascript" type="text/javascript">alert ("Got
          you")</script>rn
3      ]]>
4  <!--NeedCopy-->
```

Options d'action

Une action est appliquée lorsque la vérification de script inter-site XML détecte une attaque de script intersite dans la requête. Les options suivantes sont disponibles pour optimiser la protection XML cross-site Scripting pour votre application :

- **Bloquer**—L'action de blocage est déclenchée si les balises de script inter-sites sont détectées dans la requête.
- **Log**—Générer des messages de journal indiquant les actions effectuées par la vérification de script inter-site XML. Si le bloc est désactivé, un message de journal distinct est généré pour chaque emplacement (ELEMENT, ATTRIBUTE) dans lequel la violation de script intersite est détectée. Toutefois, un seul message est généré lorsque la demande est bloquée. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.
- **Statistiques** : collecte des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si des demandes légitimes sont bloquées, vous devrez peut-être revoir la configuration pour voir si vous devez configurer de nouvelles règles de relaxation ou modifier celles existantes.

Règles de relaxation

Si votre application exige que vous contourniez la vérification de script inter-site pour un ELEMENT ou un ATTRIBUTE spécifique dans la charge utile XML, vous pouvez configurer une règle de relaxation. Les règles de relaxation de vérification de script inter-site XML ont les paramètres suivants :

- **Name**—Vous pouvez utiliser des chaînes littérales ou des expressions régulières pour configurer le nom de l'ELEMENT ou de l'attribut. L'expression suivante exempte tous les ELEMENTS commençant par la chaîne name_ suivie d'une chaîne de lettres majuscules ou minuscules, ou de chiffres, qui comporte au moins deux et pas plus de quinze caractères :

  ```
  ^name_[0-9A-Za-z]{ 2,15 } $
  ```


> **Remarque**
>
> Les noms sont sensibles à la casse. Les entrées en double ne sont pas autorisées, mais vous pouvez utiliser la majuscule des noms et des différences d'emplacement pour créer des entrées similaires. Par exemple, chacune des règles de relaxation suivantes est unique :
>
> 1. `XMLcross-site scripting: ABC IsRegex: NOTREGEX Location: ATTRIBUTE State: ENABLED`
> 2. `XMLcross-site scripting: ABC IsRegex: NOTREGEX Location: ELEMENT State: ENABLED`
> 3. `XMLcross-site scripting: abc IsRegex: NOTREGEX Location: ELEMENT State: ENABLED`
> 4. `XMLcross-site scripting: abc IsRegex: NOTREGEX Location: ATTRIBUTE State: ENABLED`

- **Emplacement** : vous pouvez spécifier l'emplacement de l'exception Vérification de script inter-site dans votre charge utile XML. L'option ELEMENT est sélectionnée par défaut. Vous pouvez le modifier en ATTRIBUTE.
- **Commentaire**—Il s'agit d'un champ facultatif. Vous pouvez utiliser une chaîne de 255 caractères maximum pour décrire l'objectif de cette règle de relaxation.

> **Avertissement**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas familier avec les expressions régulières au format PCRE, vérifiez les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement le nom que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation négligente des expressions régulières peut avoir des résultats que vous ne voulez pas, comme bloquer l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification de script inter-site XML aurait autrement bloquée.

Utilisation de la ligne de commande pour configurer la vérification XML cross-site Scripting

Pour configurer des actions de vérification de script inter-site XML et d'autres paramètres à l'aide de la ligne de commande

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer les commandes suivantes pour configurer la vérification de script inter-site XML :

```
> set appfw profile <name> -XMLcross-site scriptingAction (([block] [log] [
stats])| [none])
```


Pour configurer une règle de relaxation XML Cross-Site Scripting, vérifiez à l'aide de la ligne de commande

Vous pouvez ajouter des règles de relaxation pour contourner l'inspection de l'inspection d'attaque par script intersite dans un emplacement spécifique. Utilisez la commande bind ou unbind pour ajouter ou supprimer la liaison de règle de relaxation, comme suit :

```
> bind appfw profile <name> -XMLcross-site scripting <string> [isRegex ( REGEX | NOTREGEX)] [-location ( ELEMENT | ATTRIBUTE )] -comment <string> [-state ( ENABLED | DISABLED )]

> unbind appfw profile <name> -XMLcross-site scripting <String>
```

Exemple :

```
> bind appfw profile test_pr -XMLcross-site scripting ABC
```

Après l'exécution de la commande ci-dessus, la règle de relaxation suivante est configurée. La règle est activée, le nom est traité comme un littéral (NOTREGEX), et ELEMENT est sélectionné comme emplacement par défaut :

```
1)      XMLcross-site scripting:  ABC             IsRegex:  NOTREGEX

        Location:  ELEMENT       State:  ENABLED

`> unbind appfw profile test_pr -XMLcross-site scripting abc`

ERROR: No such XMLcross-site scripting check

`> unbind appfw profile test_pr -XMLcross-site scripting ABC`

 Done
<!--NeedCopy-->
```

Utilisation de l'interface graphique pour configurer la vérification de script inter-site XML

Dans l'interface graphique, vous pouvez configurer la vérification de script inter-site XML dans le volet pour le profil associé à votre application.

Pour configurer ou modifier la vérification XML cross-Site Scripting à l'aide de l'interface graphique

1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet Paramètres avancés, cliquez sur **Contrôles de sécurité**.

La table de vérification de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Vous avez 2 options de configuration :

a) Si vous souhaitez simplement activer ou désactiver les actions **Bloquer**, **Log**et **Stats**pour la **vérification de script inter-site XML**, vous pouvez activer ou désactiver les cases à cocher dans le tableau, cliquez sur **OK**, puis cliquez sur Enregistrer et fermer pour fermer le fichier de sécurité Volet à cocher.

b) Vous pouvez double-cliquer sur **XML Cross-Site Scripting**, ou sélectionner la ligne et cliquer sur **Paramètres d'action**, pour afficher les options d'action. Après avoir modifié l'un des paramètres d'action, cliquez sur **OK** pour enregistrer les modifications et revenir au tableau Vérifications de sécurité.

Vous pouvez procéder à la configuration d'autres vérifications de sécurité si nécessaire. Cliquez sur **OK** pour enregistrer toutes les modifications que vous avez apportées dans la section Contrôles de sécurité, puis cliquez sur **Enregistrer et fermer pour fermer** le volet de vérification de la sécurité.

Pour configurer une règle de relaxation XML cross-Site Scripting à l'aide de l'interface graphique

1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
3. Dans le tableau Règles de relaxation, double-cliquez sur l'entrée **XML Cross-Site Scripting**, ou sélectionnez-la et cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Règles de relaxation de script inter-site XML**, effectuez les opérations **Ajouter**, **Modifier**, **Supprimer**, **Activer** ou **Désactiver** pour les règles de relaxation.

Pour gérer les règles de relaxation XML Cross-Site Scripting à l'aide du visualiseur

Pour obtenir une vue consolidée de toutes les règles de relaxation, vous pouvez mettre en surbrillance la ligne **XML cross-site Scripting** dans le tableau Règles de relaxation, puis cliquer sur **Visualiseur**. Le visualiseur pour les relaxations déployées vous offre la possibilité d' **ajouter** une nouvelle règle ou de **modifier** une règle existante. Vous pouvez également **activer** ou **désactiver** un groupe de règles en sélectionnant un nœud et en cliquant sur les boutons correspondants dans le visualiseur de relaxation.

Pour afficher ou personnaliser les modèles de script inter-site à l'aide de l'interface graphique

Vous pouvez utiliser l'interface graphique pour afficher ou personnaliser la liste par défaut des attributs autorisés de script intersite ou des balises autorisées. Vous pouvez également afficher ou personnaliser la liste par défaut des motifs refusés de script inter-site.

Les listes par défaut sont spécifiées dans le **Web App Firewall** > **Signatures > Signaturespar défaut**. Si vous ne liez aucun objet signature à votre profil, la liste des scripts intersites par défaut autorisée et refusée spécifiée dans l'objet Signatures par défaut sera utilisée par le profil pour le traitement du contrôle de sécurité Inter-Site Scripting. Les balises, attributs et motifs, spécifiés dans l'objet signatures par défaut, sont en lecture seule. Vous ne pouvez pas les modifier ou les modifier. Si vous souhaitez

les modifier ou les modifier, effectuez une copie de l'objet Signatures par défaut pour créer un objet signature définie par l'utilisateur. Modifiez les listes Autorisé ou Refusé dans le nouvel objet signature défini par l'utilisateur et utilisez cet objet signature dans le profil qui traite le trafic pour lequel vous souhaitez utiliser ces listes personnalisées autorisées et refusées.

Pour plus d'informations sur les signatures, reportez-vous à la section http://support.citrix.com/proddocs/topic/ns-security-10-map/appfw-signatures-con.html.

Pour afficher les modèles de script intersite par défaut :

1. Accédez à **Web App Firewall** > **Signatures**, sélectionnez ***Signatures par défaut**, puis cliquez sur **Modifier**. Ensuite, cliquez sur **Gérer les modèles de script SQL/inter-site**.

Le tableau **Gérer les chemins de script SQL/inter-site** présente les trois lignes suivantes relatives au script inter-site :

```
1             xss/allowed/attribute
2
3             xss/allowed/tag
4
5             xss/denied/pattern
6 <!--NeedCopy-->
```

Sélectionnez une ligne et cliquez sur **Gérer les éléments** pour afficher les éléments de script intersite correspondants (balise, attribut, motif) utilisés par la vérification de **script inter-site du** pare-feu Web App Firewall.

Pour personnaliser des éléments de script inter-sites : vous pouvez modifier l'objet signature défini par l'utilisateur pour personnaliser la balise autorisée, les attributs autorisés et les motifs refusés. Vous pouvez ajouter de nouvelles entrées ou supprimer celles qui existent déjà.

1. **Accédez à Web App Firewall** > **Signatures**, mettez en surbrillance la signature définie par l'utilisateur cible, puis cliquez sur **Modifier**. Cliquez sur **Gérer les modèles de script SQL/inter-sites** pour afficher la table **Gérer les chemins de script SQL/inter-site**.
2. Sélectionnez la ligne cible de script inter-site.

a) Cliquez sur **Gérer les éléments**pour **ajouter**, **modifier** ou **supprimer** l'élément de script inter-site correspondant.

b) Cliquez sur **Supprimer** pour supprimer la ligne sélectionnée.

> **Avertissement**
>
> Soyez très prudent lorsque vous supprimez ou modifiez un élément de script inter-site par défaut, ou supprimez le chemin de script inter-site pour supprimer la ligne entière. Les signatures, la vérification de sécurité HTML Cross-Site Scripting et la vérification de sécurité XML cross-Site Scripting s'appuient sur ces éléments pour détecter les attaques visant à protéger vos applica-

> tions. La personnalisation du script inter-site Elements peut rendre votre application vulnérable aux attaques de script inter-site si le modèle requis est supprimé lors de la modification.

Utilisation de la fonction de journal avec la vérification de script inter-site XML

Lorsque l'action de journalisation est activée, les violations de vérification de sécurité XML cross-site Scripting sont enregistrées dans le journal d'audit en tant que violations de **script AppFW_XML_Cross-Sites**. Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur syslog distant.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Basculez vers le shell et recherchez les fichiers ns.logs dans le dossier /var/log/ pour accéder aux messages de journal relatifs aux violations de script inter-site XML :

```
> \*\*Shell\*\*

> \*\*tail -f /var/log/ns.log | grep APPFW_XML_cross-site scripting\*\*
<!--NeedCopy-->
```

Exemple d'un message de journal de violation de vérification de sécurité XML cross-site Scripting au format journal natif montrant<blocked> l'action

```
Oct  7 01:44:34 <local0.warn> 10.217.31.98 10/07/2015:01:44:34 GMT ns
    0-PPE-1 : default APPFW APPFW_XML_cross-site scripting 1154 0 :
    10.217.253.69 3466-PPE1 - owa_profile http://10.217.31.101/FFC/login
    .html Cross-site script check failed for field script="Bad tag:
    script" <\*\*blocked\*\*>
<!--NeedCopy-->
```

Exemple d'un message de journal de violation de vérification de sécurité XML cross-site Scripting au format de journal CEF montrant<not blocked> l'action

```
Oct  7 01:46:52 <local0.warn> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
    .0|APPFW|APPFW_XML_cross-site scripting|4|src=10.217.30.17
    geolocation=Unknown spt=33141 method=GET request=http://
    10.217.31.101/FFC/login.html msg=Cross-site script check failed for
    field script="Bad tag: script" cn1=1607 cn2=3538 cs1=owa_profile cs2
    =PPE0 cs4=ERROR cs5=2015 act=\*\*not blocked\*\*
<!--NeedCopy-->
```

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique Citrix inclut un outil utile (**Syslog Viewer**) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez au **Web App Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Vérifications de sécurité**. Mettez en surbrillance la ligne **XML cross-site Scripting**, puis cliquez sur **Journaux** . Lorsque vous accédez aux journaux directement à partir de la vérification de script inter-site XML du profil, l'interface graphique filtre les messages de journal et affiche uniquement les journaux relatifs à ces violations de vérification de sécurité.
- Vous pouvez également accéder à la visionneuse Syslog en accédant à **Citrix ADC** > **Système** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien Messages Syslog pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation de vérification de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de vérification de sécurité peuvent être déclenchées pendant le traitement de la demande.
- Accédez à **Web App Firewall** > **Stratégies** > **Audit**. Dans la section **Messages d'audit**, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation des contrôles de sécurité.

La visionneuse Syslog basée sur XML fournit diverses options de filtre pour sélectionner uniquement les messages de journal qui vous intéressent. Pour sélectionner les messages de journalisation pour la vérification **XML Cross-Site Scripting**, filtrez en sélectionnant **APPFW** dans les options déroulantes du **module**. La liste **Type d'événement** offre un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous activez la case à cocher **AppFW_XML_Inter-Site Script** et que vous cliquez sur le bouton **Appliquer**, seuls les messages relatifs aux violations de vérification de sécurité des scripts intersites XML apparaissent dans la visionneuse Syslog.

Si vous placez le curseur dans la ligne d'un message de journal spécifique, plusieurs options, telles que **Module**, **Type d'événement**, **ID d'événement**, **adresse IP du client**, etc. s'affichent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans le message de journal.

Statistiques relatives aux violations de script inter-site XML

Lorsque l'action des statistiques est activée, le compteur de la vérification de script inter-site XML est incrémenté lorsque le Web App Firewall prend une action pour cette vérification de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. La taille d'un incrément du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, une demande d'une page contenant trois violations de script inter-site XML incrémente le compteur de statistiques d'un, car la page est bloquée dès que la première violation est détectée. Toutefois, si le bloc est désactivé, le traitement de la même demande incrémente le compteur de statistiques pour les violations et les journaux de trois, car chaque violation génère un message de journal distinct.

Pour afficher les statistiques XML cross-Site Scripting, vérifiez les statistiques à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
> **sh appfw stats**
```

Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
> **stat appfw profile** <profile name>
```

Pour afficher les statistiques de script inter-site XML à l'aide de l'interface graphique

1. Accédez à **Système** > **Sécurité** > **Web App Firewall**.
2. Dans le volet droit, accédez au lien **Statistiques**.
3. Utilisez la barre de défilement pour afficher les statistiques sur les violations et les journaux de script inter-site XML. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Vérification de l'injection SQL XML

August 20, 2021

La vérification de l'injection SQL XML examine les demandes des utilisateurs pour d'éventuelles attaques par injection SQL XML. S'il trouve du SQL injecté dans des charges utiles XML, il bloque les requêtes.

Une attaque SQL XML peut injecter du code source dans une application Web de sorte qu'il puisse être interprété et exécuté comme une requête SQL valide pour effectuer une opération de base de données avec une intention malveillante. Par exemple, des attaques XML SQL peuvent être lancées pour obtenir un accès non autorisé au contenu d'une base de données ou pour manipuler les données stockées. Les attaques XML SQL Injection ne sont pas seulement courantes, mais peuvent également être très dangereuses et coûteuses.

Le cloisonnement des privilèges des utilisateurs de la base de données peut aider à protéger la base de données dans une certaine mesure. Tous les utilisateurs de base de données doivent disposer uniquement des privilèges requis pour effectuer les tâches prévues, de sorte qu'ils ne peuvent pas exécuter des requêtes SQL pour effectuer d'autres tâches. Par exemple, un utilisateur en lecture seule ne doit pas être autorisé à écrire ou manipuler des tables de données. La vérification SQL Injection XML du Web App Firewall inspecte toutes les demandes XML afin de fournir des défenses spéciales contre l'injection de code SQL non autorisé qui pourrait compromettre la sécurité. Si le Web App Firewall détecte du code SQL non autorisé dans une requête XML d'un utilisateur, il peut bloquer la demande.

Citrix Web App Firewall inspecte la présence de mots-clés SQL et de caractères spéciaux pour identifier l'attaque par injection SQL XML. Un ensemble par défaut de mots-clés et de caractères spéciaux fournit des mots-clés connus et des caractères spéciaux couramment utilisés pour lancer des at-

taques XML SQL. Le Web App Firewall considère trois caractères, un guillemet droit simple (‘), une barre oblique inverse () et un point-virgule (;) comme des caractères spéciaux pour le traitement des vérifications de sécurité SQL. Vous pouvez ajouter de nouveaux modèles et modifier le jeu par défaut pour personnaliser l’inspection de vérification XML SQL.

Le Web App Firewall offre diverses options d’action pour implémenter la protection XML SQL Injection. Vous pouvez **bloquer** la demande, **consigner** un message dans le fichier ns.log avec des détails concernant les violations observées, et collecter des **statistiques** pour garder une trace du nombre d’attaques observées.

En plus des actions, il existe plusieurs paramètres qui peuvent être configurés pour le traitement par injection XML SQL. Vous pouvez vérifier les **caractères génériques SQL**. Vous pouvez modifier le type d’injection SQL XML et sélectionner l’une des 4 options (**SQLKeyword**, **SQLSplChar**, **SQLSplCharANDKeyword**, **SQLSplCharORKeyword**) pour indiquer comment évaluer les mots-clés SQL et les caractères spéciaux SQL lors du traitement du fichier XML charge utile. Le paramètre XML **SQL Comments Handling** vous permet de spécifier le type de commentaires qui doivent être inspectés ou exemptés lors de la détection XML SQL Injection.

Vous pouvez déployer des relaxations pour éviter les faux positifs. La vérification XML XML du Web App Firewall est effectuée sur la charge utile des requêtes entrantes, et les chaînes d’attaque sont identifiées même si elles sont réparties sur plusieurs lignes. La vérification recherche les chaînes d’injection SQL dans l’**élément** et les valeurs **d’attribut** . Vous pouvez appliquer des relaxations pour contourner l’inspection de contrôle de sécurité dans des conditions spécifiées. Les journaux et les statistiques peuvent vous aider à identifier les relaxations nécessaires.

Options d’action

Une action est appliquée lorsque le contrôle Injection SQL XML détecte une chaîne d’attaque SQL Injection dans la requête. Les actions suivantes sont disponibles pour configurer une protection XML SQL Injection optimisée pour votre application :

Block : si vous activez block, l’action block n’est déclenchée que si l’entrée correspond à la spécification de type d’injection SQL XML. Par exemple, si **SQLSplCharANDKeyword** est configuré comme type d’injection SQL XML, une requête n’est pas bloquée si elle ne contient aucun mot clé, même si des caractères spéciaux SQL sont détectés dans la charge utile. Une telle demande est bloquée si le type d’injection SQL XML est défini sur **SQLSplChar**ou **SQLSplCharORKeyword**.

Journal : si vous activez la fonction de journal, la vérification XML SQL Injection génère des messages de journal indiquant les actions qu’elle effectue. Si bloc est désactivé, un message de journal distinct est généré pour chaque emplacement (**ELEMENT**, **ATTRIBUTE**) dans lequel la violation XML SQL a été détectée. Toutefois, un seul message est généré lorsque la demande est bloquée. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une

forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.

Statistiques : si cette option est activée, la fonction de statistiques recueille des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si des demandes légitimes sont bloquées, vous devrez peut-être revoir la configuration pour voir si vous devez configurer de nouvelles règles de relaxation ou modifier celles existantes.

Paramètres XML SQL

En plus des actions de blocage, de journal et de statistiques, vous pouvez configurer les paramètres suivants pour la vérification XML SQL Injection :

Check for XML SQL caractères génériques —Lescaractères génériques peuvent être utilisés pour élargir les sélections d'une instruction SQL-SELECT (langage de requête structuré). Ces opérateurs de carte génériques peuvent être utilisés en conjonction avec les opérateurs **LIKE** et **NOT LIKE** pour comparer une valeur à des valeurs similaires. Le pourcentage (%) et le trait de soulignement (_) sont fréquemment utilisés comme caractères génériques. Le signe de pourcentage est analogue au caractère générique astérisque (*) utilisé avec MS-DOS et correspond à zéro, un ou plusieurs caractères dans un champ. Le trait de soulignement est similaire au point d'interrogation MS-DOS (?) caractère générique. Il correspond à un nombre ou un caractère unique dans une expression.

Par exemple, vous pouvez utiliser la requête suivante pour effectuer une recherche de chaîne pour rechercher tous les clients dont les noms contiennent le caractère D.

```
SELECT * from customer WHERE name like "%D%"
```

L'exemple suivant combine les opérateurs pour rechercher les valeurs de salaire qui ont 0 comme deuxième et troisième caractères.

```
SELECT * from customer WHERE salary like '_00%
```

Différents fournisseurs de SGBD ont étendu les caractères génériques en ajoutant des opérateurs supplémentaires. Le Citrix Web App Firewall peut se protéger contre les attaques lancées en injectant ces caractères génériques. Les 5 caractères génériques par défaut sont le pourcentage (%), le trait de soulignement (_), le caret (^), l'ouverture du crochet ([) et le crochet carré de fermeture (]). Cette protection s'applique aux profils HTML et XML.

Les caractères génériques par défaut sont une liste de littéraux spécifiés dans ***Signatures par défaut** :

```
1 -  <wildchar type=" LITERAL" >%</wildchar>
2 -  <wildchar type=" LITERAL" >_</wildchar>
3 -  <wildchar type=" LITERAL" >^</wildchar>
4 -  <wildchar type=" LITERAL" >[</wildchar>
```



```
5 -  <wildchar type=" LITERAL" >]</wildchar>
6 <!--NeedCopy-->
```

Les caractères génériques d'une attaque peuvent être PCRE, comme [^A-F]. Le Web App Firewall prend également en charge les caractères génériques PCRE, mais les caractères génériques littéraux ci-dessus sont suffisants pour bloquer la plupart des attaques.

> **Remarque**
>
> La vérification des **caractères génériques** XML SQL est différente de la vérification des **caractères spéciaux** XML SQL. Cette option doit être utilisée avec prudence pour éviter les faux positifs.

Check Request Contenant le type d'injection SQL : le Web App Firewall fournit 4 options pour implémenter le niveau de rigueur souhaité pour l'inspection SQL Injection, en fonction des besoins individuels de l'application. La demande est vérifiée par rapport à la spécification de type d'injection pour détecter les violations SQL. Les 4 options de type d'injection SQL sont les suivantes :

- **Caractère spécial SQL et mot-clé** : un mot-clé SQL et un caractère spécial SQL doivent être présents à l'emplacement inspecté pour déclencher une violation SQL. Ce paramètre le moins restrictif est également le paramètre par défaut.
- **Caractère spécial SQL** : au moins un des caractères spéciaux doit être présent dans la chaîne de charge utile traitée pour déclencher une violation SQL.
- **Mot-clé SQL**—Au moins un des mots-clés SQL spécifiés doit être présent dans la chaîne de charge utile traitée pour déclencher une violation SQL. Ne sélectionnez pas cette option sans considération. Pour éviter les faux positifs, assurez-vous qu'aucun des mots-clés n'est attendu dans les entrées.
- **Caractère spécial SQL ou mot-clé** : le mot-clé ou la chaîne de caractères spéciaux doit être présent dans la charge utile pour déclencher la violation de vérification de sécurité.

> **Conseil**
>
> Si vous sélectionnez l'option Caractère spécial SQL, le Web App Firewall ignore les chaînes qui ne contiennent pas de caractères spéciaux. Étant donné que la plupart des serveurs SQL ne traitent pas les commandes SQL qui ne sont pas précédées d'un caractère spécial, l'activation de cette option peut réduire considérablement la charge sur le Web App Firewall et accélérer le traitement sans mettre vos sites Web protégés en danger.

Gestion des commentaires SQL : par défaut, le Web App Firewall analyse et vérifie tous les commentaires des données XML à la recherche de commandes SQL injectées. De nombreux serveurs SQL ignorent quoi que ce soit dans un commentaire, même s'ils sont précédés d'un caractère spécial SQL. Pour un traitement plus rapide, si votre serveur SQL XML ignore les commentaires, vous pouvez configurer le Web App Firewall pour ignorer les commentaires lors de l'examen des demandes de SQL injecté. Les options de gestion des commentaires SQL XML sont les suivantes :

- **ANSI**—Ignorer les commentaires SQL au format ANSI, qui sont normalement utilisés par les bases de données SQL UNIX.
- **Imbriqué**—Ignorer les commentaires SQL imbriqués, qui sont normalement utilisés par Microsoft SQL Server.
- **ANSI/imbriqué**—Ignorer les commentaires qui respectent les normes ANSI et SQL de commentaires imbriqués. Les commentaires qui correspondent uniquement à la norme ANSI, ou uniquement à la norme imbriquée, sont toujours vérifiés pour le SQL injecté.
- **Check all Comments**—Vérifiez l'intégralité de la requête pour SQL injecté, sans sauter quoi que ce soit. C'est le réglage par défaut.

> **Conseil**
>
> Dans la plupart des cas, vous ne devez pas choisir l'option imbriquée ou ANSI/imbriquée sauf si votre base de données back-end s'exécute sur Microsoft SQL Server. La plupart des autres types de logiciels SQL Server ne reconnaissent pas les commentaires imbriqués. Si des commentaires imbriqués apparaissent dans une requête dirigée vers un autre type de serveur SQL, ils peuvent indiquer une tentative de violation de la sécurité sur ce serveur.

Règles de relaxation

Si votre application exige que vous contourniez l'inspection XML SQL Injection pour un ELEMENT ou un ATTRIBUTE spécifique dans la charge utile XML, vous pouvez configurer une règle de relaxation. Les règles de relaxation de l'inspection XML SQL Injection ont les paramètres suivants :

- **Nom :** Vous pouvez utiliser des chaînes littérales ou des expressions régulières pour configurer le nom de l'**ELEMENT** ou de l'**ATTRIBUTE**. L'expression suivante exempte tous les **ELEMENTS** commençant par la chaîne **PurchaseOrder_** suivie d'une chaîne de nombres qui comporte au moins deux et pas plus de dix caractères :

  Commentaire : « Exempter XML SQL Check for Purchase Elements »

```
1     XMLSQLInjection:  "PurchaseOrder_[0-9A-Za-z]{
2  2,10 }
3  "
4
5     IsRegex:  REGEX          Location:  ELEMENT
6
7     State:  ENABLED
8  <!--NeedCopy-->
```

Remarque : Les noms sont sensibles à la casse. Les entrées en double ne sont pas autorisées, mais vous pouvez utiliser la majuscule des noms et des différences d'emplacement pour créer des entrées similaires. Par exemple, chacune des règles de relaxation suivantes est unique :


```
1)      XMLSQLInjection:  XYZ    IsRegex:  NOTREGEX

        Location:  ELEMENT       State:  ENABLED

2)      XMLSQLInjection:  xyz    IsRegex:  NOTREGEX

        Location:  ELEMENT       State:  ENABLED

3)      XMLSQLInjection:  xyz    IsRegex:  NOTREGEX

        Location:  ATTRIBUTE     State:  ENABLED

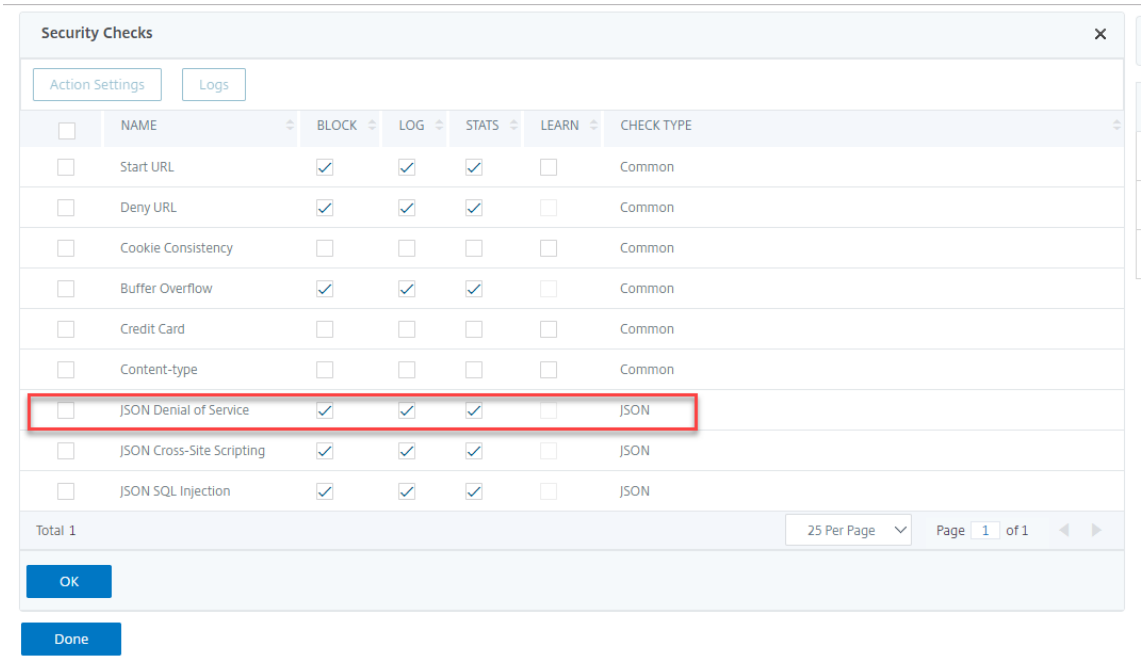
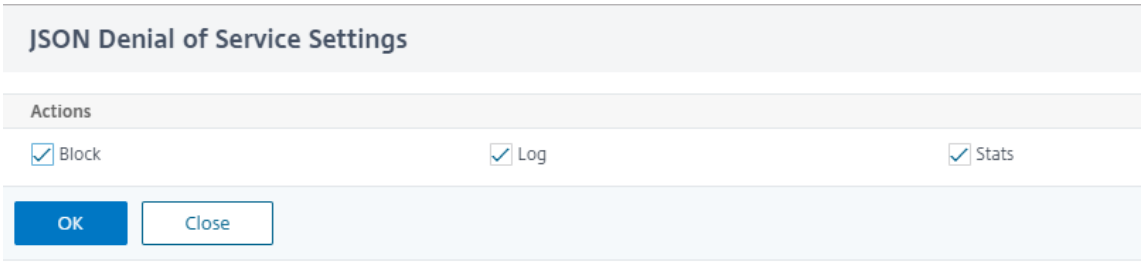
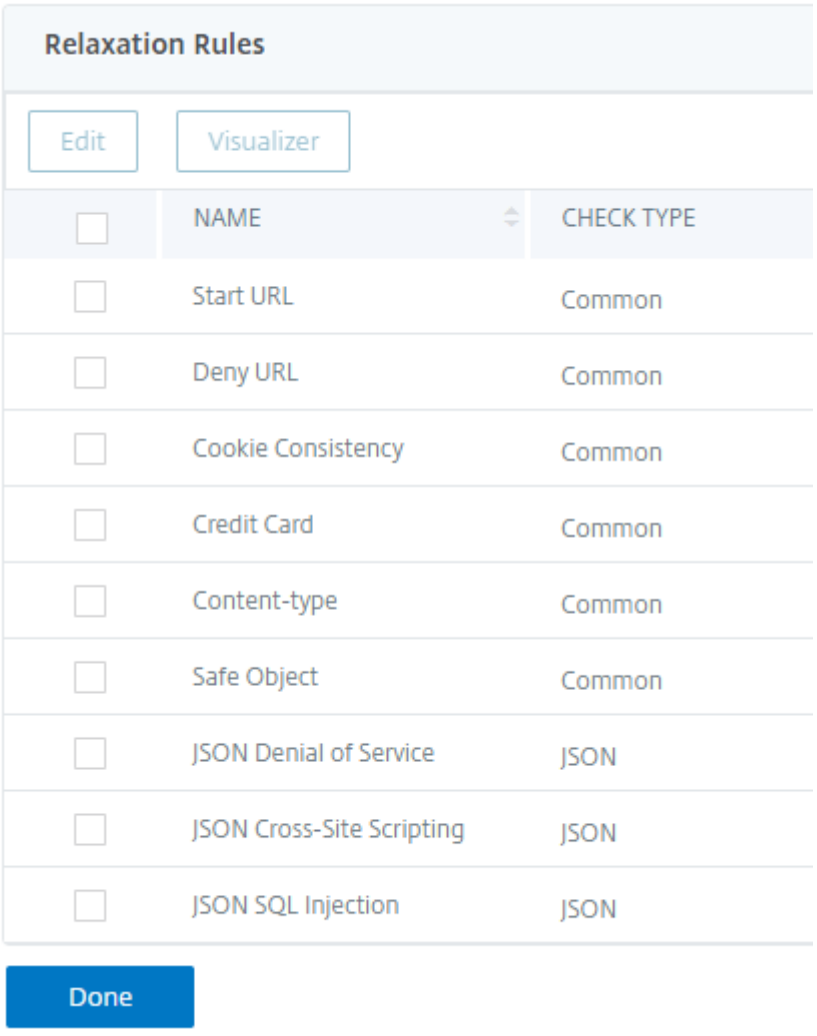
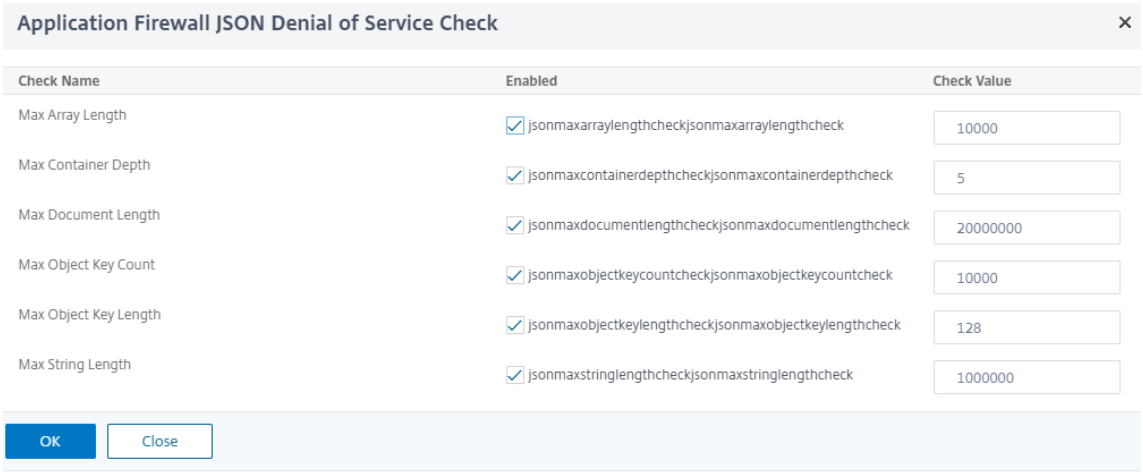
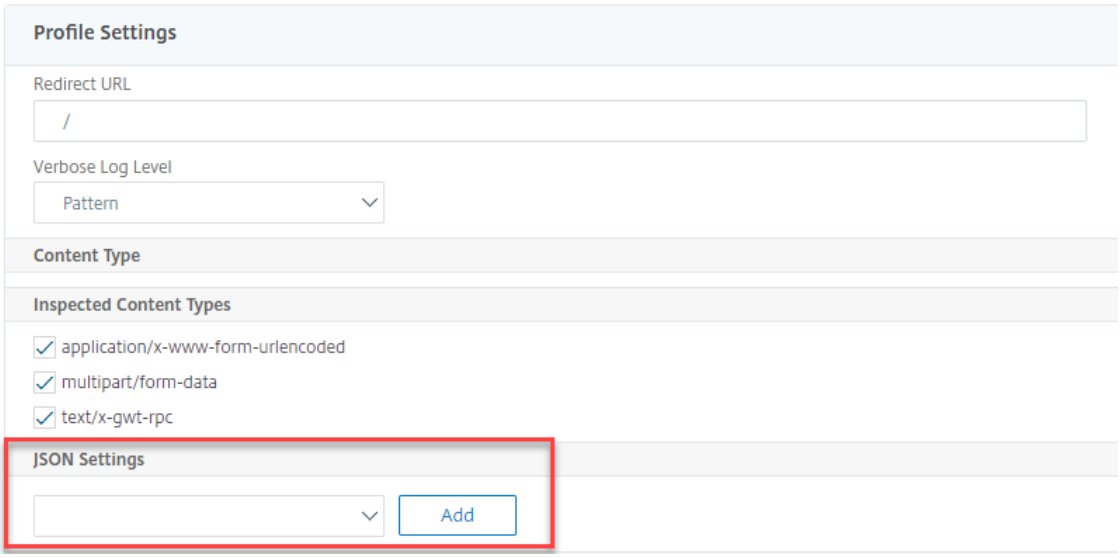
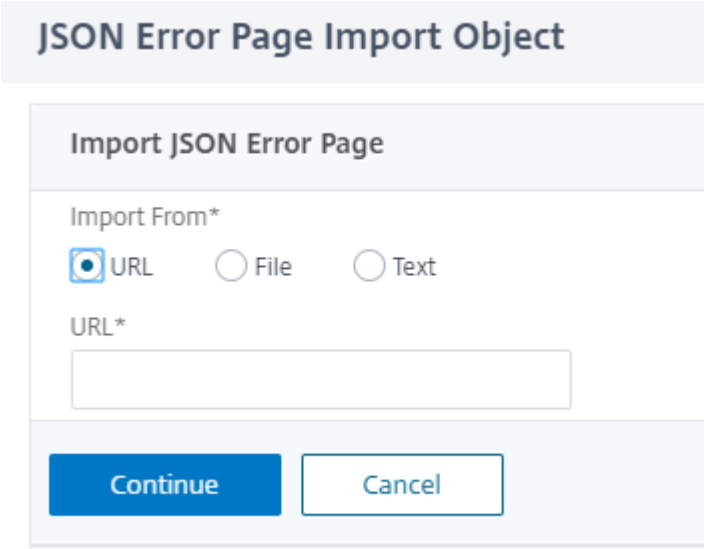
4)      XMLSQLInjection:  XYZ    IsRegex:  NOTREGEX

        Location:  ATTRIBUTE     State:  ENABLED
<!--NeedCopy-->
```

- **Emplacement** : vous pouvez spécifier l'emplacement de l'exception XML SQL Inspection dans votre charge utile XML. L'option **ELEMENT** est sélectionnée par défaut. Vous pouvez le modifier en **ATTRIBUTE**.
- **Commentaire** : Il s'agit d'un champ facultatif. Vous pouvez utiliser une chaîne de 255 caractères maximum pour décrire l'objectif de cette règle de relaxation.

> **Avertissement**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas familier avec les expressions régulières au format PCRE, vérifiez les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement le nom que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation négligente des expressions régulières peut avoir des résultats que vous ne voulez pas, comme bloquer l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que l'inspection XML SQL Injection aurait autrement bloquée.

Utilisation de la ligne de commande pour configurer la vérification d'injection SQL XML

Pour configurer des actions XML SQL Injection et d'autres paramètres à l'aide de la ligne de commande :

Dans l'interface de ligne de commande, vous pouvez utiliser la commande **set appfw profile** ou la commande **add appfw profile** pour configurer les protections XML SQL Injection. Vous pouvez activer les actions de blocage, de journalisation et de statistiques. Sélectionnez le type de modèle d'attaque SQL (mots-clés, caractères génériques, chaînes spéciales) que vous souhaitez détecter dans les charges utiles. Utilisez la commande **unset appfw profile** pour rétablir les paramètres configurés

à leurs valeurs par défaut. Chacune des commandes suivantes ne définit qu'un seul paramètre, mais vous pouvez inclure plusieurs paramètres dans une seule commande :

- set appfw profile <name> **-XMLSQLInjectionAction** (([block] [log] [stats])| [none])
- set appfw profile <name> -XMLSQLInjectionCheckSQLWildChars (ON |OFF)
- set appfw profile <name> -XMLSQLInjectionType ([SQLKeyword] | [SQLSplChar] | [SQLSplCharANDKeyword] | [SQLSplCharORKeyword])
- set appfw profile <name> -XMLSQLInjectionParseComments ([checkall] | [ansi|nested] | [ansinested])

Pour configurer une règle de relaxation SQL Injection à l'aide de la ligne de commande

Utilisez la commande bind ou unbind pour ajouter ou supprimer des règles de relaxation, comme suit :

```
1 -  bind appfw profile <name> -XMLSQLInjection <string> [isRegex (REGEX
     | NOTREGEX)] [-location ( ELEMENT | ATTRIBUTE )]  - comment <string>
     [-state ( ENABLED | DISABLED )]
2 -  unbind appfw profile <name> -XMLSQLInjection <String>
3 <!--NeedCopy-->
```

Exemple :

```
1 > bind appfw profile test_profile -XMLSQLInjection "PurchaseOrder_[0-9A
     -Za-z]{
2  2,15 }
3  " -isregex REGEX -location ATTRIBUTE
4
5 > unbind appfw profile test_profile  - XMLSQLInjection "PurchaseOrder_
     [0-9A-Za-z]{
6  2,15 }
7  " -location ATTRIBUTE
8 <!--NeedCopy-->
```

Utilisation de l'interface graphique pour configurer la vérification de sécurité par injection XMLSQL

Dans l'interface graphique, vous pouvez configurer le contrôle de sécurité XML SQL Injection dans le volet pour le profil associé à votre application.

Pour configurer ou modifier la vérification XML SQL Injection à l'aide de l'interface graphique

1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.

2. Dans le volet Paramètres avancés, cliquez sur **Contrôles de sécurité**.

La table de vérification de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Vous avez 2 options de configuration :

a. Si vous souhaitez simplement activer ou désactiver les actions Bloquer, Journal et Statistiques pour XML SQL Injection, vous pouvez activer ou désactiver les cases à cocher dans le tableau, cliquez sur OK, puis cliquez sur Enregistrer et fermer pour fermer le volet Contrôle de sécurité.

b. Si vous souhaitez configurer des options supplémentaires pour cette vérification de sécurité, double-cliquez sur XML SQL Injection ou sélectionnez la ligne et cliquez sur **Paramètres d'action**, pour afficher les options suivantes :

Rechercher les caractères génériques SQL—Considérez les caractères génériques SQL dans la charge utile comme des modèles d'attaque.

Vérifier la requête contenant—Type d'injection SQL (SQLKeyWord, SQLSplChar, SQLSplChar, SQLSplChArdKeyword ou SQLSplCharorKeyword) à vérifier.

Gestion des commentaires SQL : type de commentaires (Vérifier tous les commentaires, ANSI, imbriqué ou ANSI/imbriqué) à vérifier.

Après avoir modifié l'un des paramètres ci-dessus, cliquez sur **OK** pour enregistrer les modifications et revenir au tableau Vérifications de sécurité. Vous pouvez procéder à la configuration d'autres vérifications de sécurité si nécessaire. Cliquez sur **OK** pour enregistrer toutes les modifications que vous avez apportées dans la section Contrôles de sécurité, puis cliquez sur **Enregistrer** et **fermer** pour fermer le volet Vérification de sécurité.

Pour configurer une règle de relaxation XML Injection à l'aide de l'interface graphique

1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
3. Dans le tableau Règles de relaxation, double-cliquez sur l'entrée **XML SQL Injection** ou sélectionnez-la et cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Règles de relaxation d'injection SQL XML**, effectuez les opérations **Ajouter**, **Modifier**, **Supprimer**, **Activer** ou **Désactiver** pour les règles de relaxation.

Pour gérer les règles de relaxation XML Injection à l'aide du visualiseur

Pour obtenir une vue consolidée de toutes les règles de relaxation, vous pouvez mettre en surbrillance la ligne **Injection SQL XML** dans le tableau Règles de relaxation, puis cliquer sur **Visualiseur**. Le visualiseur pour les relaxations déployées vous offre la possibilité d' **ajouter** une nouvelle règle ou de **modifier** une règle existante. Vous pouvez également **activer** ou **désactiver** un groupe de règles en sélectionnant un nœud et en cliquant sur les boutons correspondants dans le visualiseur de relaxation.

Pour afficher ou personnaliser les modèles d'injection SQL à l'aide de l'interface graphique :

Vous pouvez utiliser l'interface graphique pour afficher ou personnaliser les modèles SQL.

Les modèles SQL par défaut sont spécifiés dans le **Web App Firewall** > **Signatures** > ***Signatures par défaut**. Si vous ne liez aucun objet de signature à votre profil, les modèles SQL par défaut spécifiés dans l'objet Signatures par défaut seront utilisés par le profil pour le traitement des vérifications de sécurité XML SQL Injection. Les règles et les motifs de l'objet Signatures par défaut sont en lecture seule. Vous ne pouvez pas les modifier ou les modifier. Si vous souhaitez modifier ou modifier ces modèles, créez un objet signature défini par l'utilisateur en créant une copie de l'objet Signatures par défaut et en modifiant les modèles SQL. Utilisez l'objet signature défini par l'utilisateur dans le profil qui traite le trafic pour lequel vous souhaitez utiliser ces modèles SQL personnalisés.

Pour plus d'informations, voir Signatures.

Pour afficher les modèles SQL par défaut :

a. Accédez à **Web App Firewall** > **Signatures**, sélectionnez ***Signatures par défaut**, puis cliquez sur **Modifier**. Ensuite, cliquez sur **Gérer les modèles de script SQL/inter-site**.

Le tableau Gérer les chemins de script SQL/inter-site affiche les quatre lignes suivantes relatives à l'injection SQL :

```
Injection (not_alphanum, SQL)/ Keyword

Injection (not_alphanum, SQL)/ specialstring

Injection (not_alphanum, SQL)/ transformrules/transform

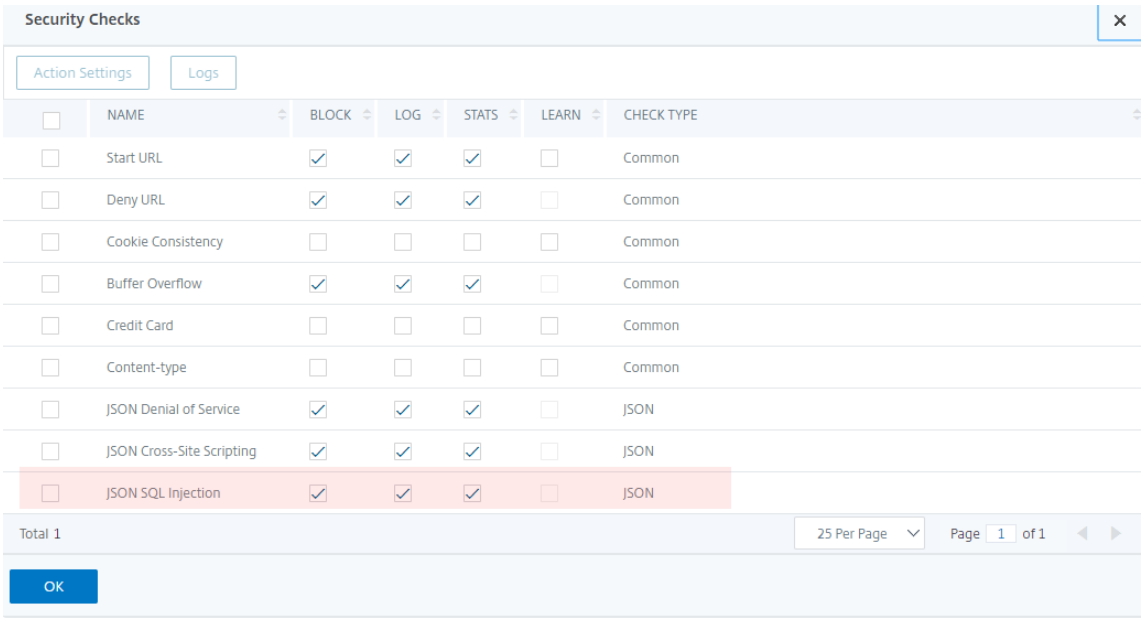
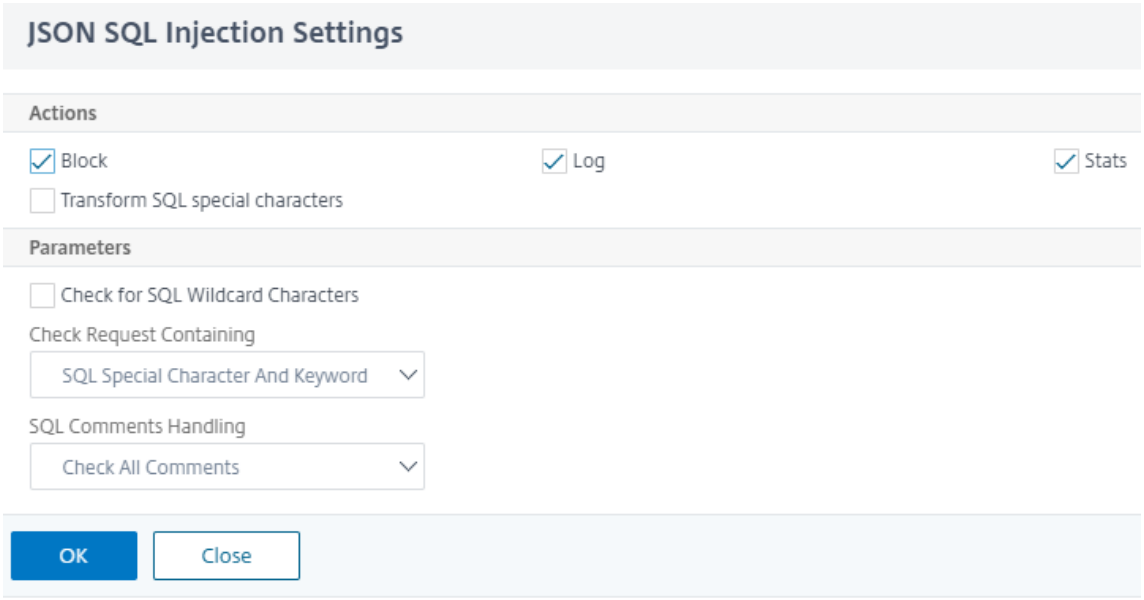
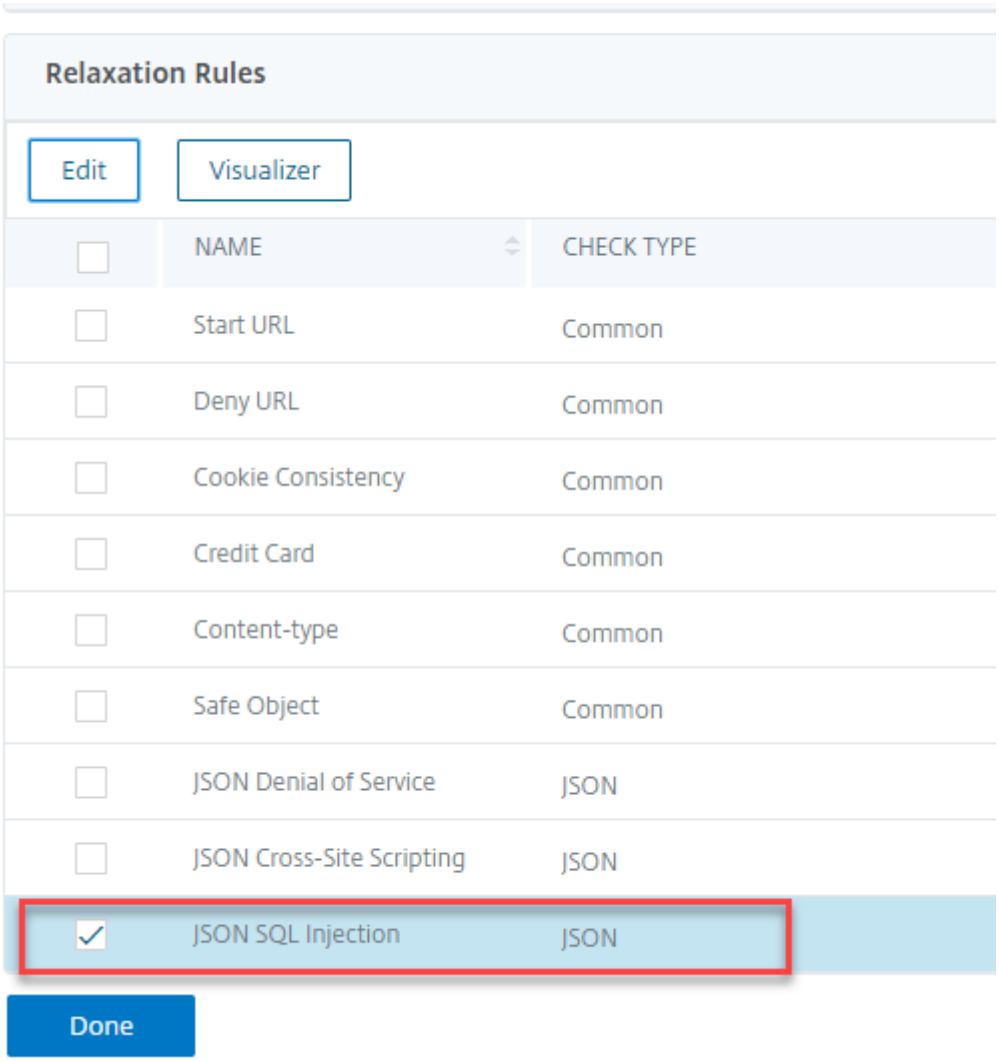
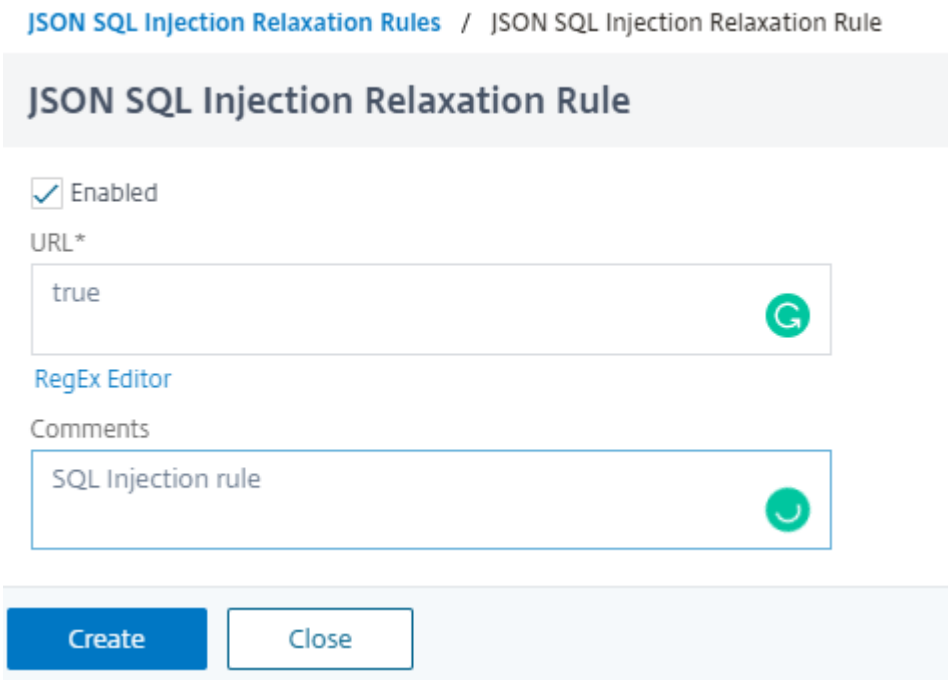
Injection (not_alphanum, SQL)/ wildchar
<!--NeedCopy-->
```

b. Sélectionnez une ligne et cliquez sur **Gérer les éléments** pour afficher les modèles SQL correspondants (mots-clés, chaînes spéciales, règles de transformation ou caractères génériques) utilisés par la vérification d'injection SQL du Web App Firewall.

Pour personnaliser les modèles SQL : vous pouvez modifier un objet signature défini par l'utilisateur pour personnaliser les mots-clés SQL, les chaînes spéciales et les caractères génériques. Vous pouvez ajouter de nouvelles entrées ou supprimer celles qui existent déjà. Vous pouvez modifier les règles de transformation des chaînes spéciales SQL.

a. Accédez à **Web App Firewall** > **Signatures**, mettez en surbrillance la signature définie par l'utilisateur cible, puis cliquez sur **Modifier**. Cliquez sur **Gérer les modèles de script SQL/inter-sites** pour afficher la table **Gérer les chemins de script SQL/inter-site**.

b. Sélectionnez la ligne SQL cible.

i. Cliquez sur **Gérer les éléments**pour **ajouter**, **modifier**ou **supprimer**l'élément SQL correspondant.

ii. Cliquez sur **Supprimer** pour supprimer la ligne sélectionnée.

> **Avertissement**
>
> Vous devez être très prudent lorsque vous supprimez ou modifiez un élément SQL par défaut ou supprimez le chemin SQL pour supprimer toute la ligne. Les règles de signature ainsi que la vérification de sécurité XML SQL Injection s'appuient sur ces éléments pour détecter les attaques SQL Injection afin de protéger vos applications. La personnalisation des modèles SQL peut rendre votre application vulnérable aux attaques XML SQL si le modèle requis est supprimé lors de la modification.

Utilisation de la fonction de journal avec la vérification d'injection SQL XML

Lorsque l'action du journal est activée, les violations de vérification de sécurité **XML SQL Injection** sont enregistrées dans le journal d'audit en tant que violations **APPFW_XML_SQL** . Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur syslog distant.

Pour accéder aux messages du journal à l'aide de la ligne de commande :

Basculez vers le shell et recherchez les fichiers ns.logs dans le dossier /var/log/ pour accéder aux messages de journal relatifs aux violations de script inter-site XML :

```
> Shell

> tail -f /var/log/ns.log | grep APPFW_XML_SQL
<!--NeedCopy-->
```

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique Citrix inclut un outil utile (Syslog Viewer) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez à **Web App Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Vérifications de sécurité**. Mettez en surbrillance la ligne **XML SQL Injection** et cliquez sur **Journaux**. Lorsque vous accédez aux journaux directement à partir de la vérification XML SQL Injection du profil, l'interface graphique filtre les messages de journal et affiche uniquement les journaux relatifs à ces violations de vérification de sécurité.
- Vous pouvez également accéder à la visionneuse Syslog en accédant à **Système** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation des contrôles de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de vérification de sécurité peuvent être déclenchées pendant le traitement de la demande.

- Accédez à **Web App Firewall** > **Stratégies** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien **Messages Syslog** pour afficher la **visionneuse Syslog**, qui affiche tous les messages de journal, y compris les autres journaux de violation de vérification de sécurité.

La visionneuse Syslog basée sur XML fournit diverses options de filtre pour sélectionner uniquement les messages de journal qui vous intéressent. Pour sélectionner les messages de journal pour la vérification **XML SQL Injection**, filtrez en sélectionnant **APPFW** dans les options déroulantes du **module**. La liste **Type d'événement** offre un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous activez la case à cocher **APPFW_XML_SQL** et cliquez sur le bouton **Appliquer**, seuls les messages de journalisation relatifs aux violations de vérification de sécurité **XML SQL Injection** apparaissent dans la visionneuse Syslog.

Si vous placez le curseur dans la ligne d'un message de journal spécifique, plusieurs options, telles que **Module**, **Type d'événement**, **ID d'événement**et **IP du client**apparaissent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans le message de journal.

Statistiques relatives aux violations d'injection SQL XML

Lorsque l'action des statistiques est activée, le compteur pour la vérification **XML SQL Injection** est incrémenté lorsque le Web App Firewall prend une action pour cette vérification de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. La taille d'un incrément du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, une demande d'une page contenant trois violations **SQL Injection XML** incrémente le compteur de statistiques d'un, car la page est bloquée dès que la première violation est détectée. Toutefois, si le bloc est désactivé, le traitement de la même demande incrémente le compteur de statistiques pour les violations et les journaux de trois, car chaque violation génère un message de journal distinct.

Pour afficher les statistiques de vérification XML SQL Injection à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
> sh appfw stats
```

Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
> stat appfw profile <profile name>
```

Pour afficher les statistiques XML SQL Injection à l'aide de l'interface graphique

1. Accédez à **Système** > **Sécurité** > **Web App Firewall**.
2. Dans le volet droit, accédez au lien **Statistiques**.
3. Utilisez la barre de défilement pour afficher les statistiques sur les violations **XML SQL Injection** et les journaux. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Vérification des pièces jointes XML

January 21, 2021

La vérification des pièces jointes XML examine les demandes entrantes de pièces jointes malveillantes et bloque celles qui contiennent des pièces jointes susceptibles d'enfreindre la sécurité des applications. Le but de la vérification des pièces jointes XML est d'empêcher un attaquant d'utiliser une pièce jointe XML pour enfreindre la sécurité de votre serveur.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification des pièces jointes XML, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Apprendre, Journaliser, Statistiques et Apprendre :

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification des pièces jointes XML :

- `set appfw profile <name> -xmlAttachmentAction [block] [learn] [log] [stats] [none]`

Vous devez configurer les autres paramètres de vérification des pièces jointes XML dans l'interface graphique. Dans la boîte de dialogue `Modify XML Attachment` Vérifier, sous l'onglet Vérifications, vous pouvez configurer les paramètres suivants :

- **Taille maximale de la pièce jointe.** Autorisez les pièces jointes qui ne sont pas supérieures à la taille maximale que vous spécifiez. Pour activer cette option, activez d'abord la case à cocher Activé, puis tapez la taille maximale de la pièce jointe en octets dans la zone de texte `Size`.
- **Type de contenu de pièce jointe.** Autoriser les pièces jointes du type de contenu spécifié. Pour activer cette option, activez d'abord la case à cocher Activé, puis entrez une expression régulière qui correspond à l'attribut Content-Type des pièces jointes que vous souhaitez autoriser.
  - Vous pouvez taper l'expression URL directement dans la fenêtre de texte. Si vous le faites, vous pouvez utiliser le menu `Regex Tokens` pour entrer un certain nombre d'expressions régulières utiles au niveau du curseur au lieu de les taper manuellement.
  - Vous pouvez cliquer sur Regex Editor pour ouvrir la`Add Regular Expression` boîte de dialogue et l'utiliser pour construire l'expression URL.

Contrôle de l'interopérabilité des services Web

January 21, 2021

La vérification de l'interopérabilité des services Web (WS-I) examine à la fois les demandes et les réponses pour vérifier la conformité à la norme WS-I et bloque les demandes et réponses qui ne respectent pas cette norme. Le but de la vérification WS-I est de bloquer les requêtes qui pourraient ne

pas interagir avec d'autres XML de manière appropriée. Un attaquant peut utiliser des incohérences dans l'interopérabilité pour lancer une attaque sur votre application XML.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier le contrôle de l'interopérabilité des services Web, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Journal, Statistiques et Apprendre.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification d'interopérabilité des services Web :

- `set appfw profile <name> -xmlWSIAction [block] ][log] [learn] [stats] [ none]`

Pour configurer des règles d'interopérabilité des services Web individuelles, vous devez utiliser l'interface graphique. Sous l'onglet Vérifications de la boîte de dialogue Modifier le contrôle de l'interopérabilité des services Web, sélectionnez une règle et cliquez sur Activer ou Désactiver pour activer ou désactiver la règle. Vous pouvez également cliquer sur Ouvrir pour ouvrir la boîte de message Détail de l'interopérabilité des services Web pour cette règle. La boîte de message affiche des informations en lecture seule sur la règle. Vous ne pouvez pas modifier ou apporter d'autres modifications de configuration à l'une de ces règles.

La vérification WS-I utilise les règles répertoriées dans WS-I Basic Profile 1.0. WS-I propose les meilleures pratiques pour le développement de solutions de services Web interopérables. Les vérifications WS-I sont effectuées uniquement sur les messages SOAP.

La description de chaque règle standard WSI est fournie ci-dessous :

Règle	Description
BP1201	Le corps du message doit être un soap:envelope avec espace de noms.
R1000	Lorsqu'une ENVELOPE est une erreur, l'élément SOAP:Fault NE DOIT PAS avoir des enfants d'élément autres que faultcode, faultstring, faultactor et detail.
R1001	Lorsqu'une ENVELOPE est une erreur, les enfants de l'élément SOAP:Fault DOIVENT être non qualifiés.

Règle	Description
R1003	UN RÉCEPTEUR DOIT accepter les messages d'erreur qui comportent un certain nombre d'attributs qualifiés ou non qualifiés, y compris zéro, apparaissant sur l'élément de détail. L'espace de noms des attributs qualifiés peut être autre que l'espace de noms de l'élément de document qualifié Envelope.
R1004	Lorsqu'une ENVELOPE contient un élément de code faultcode, le contenu de cet élément doit être soit l'un des codes d'erreur définis dans SOAP 1.1 (fournissant des informations supplémentaires si nécessaire dans l'élément detail), soit un Qname dont l'espace de noms est contrôlé par l'autorité de spécification de la faute (dans cet ordre de préférence).
R1005	Une ENVELOPE NE DOIT PAS contenir l'attribut SOAP:encodingStyle sur l'un des éléments dont l'espace de noms est le même que l'espace de noms de l'élément de document qualifié Envelope.
R1006	Une ENVELOPE NE DOIT PAS contenir les attributs SOAP:EncodingStyle sur un élément qui est un enfant de SOAP:Body.
R1007	Une ENVELOPE décrite dans une liaison littérale rpc-NE DOIT PAS contenir l'attribut SOAP:encodingStyle sur un élément qui est un petit-fils de Soap:body.
R1011	Une ENVELOPE NE DOIT PAS avoir d'enfant élément de SOAP:Envelope suivant l'élément SOAP:Body.
R1012	Un MESSAGE DOIT être sérialisé en UTF-8 ou UTF-16.
R1013	Une ENVELOPE contenant un attribut SOAP:MustUnderderderit DOIT utiliser uniquement les formes lexicales 0 et 1.

Règle	Description
R1014	Les enfants de l'élément SOAP:body dans une ENVELOPE DOIVENT être qualifiés d'espace de noms.
R1015	Un RECEPTEUR DOIT générer une erreur s'il rencontre une enveloppe dont l'élément de document n'est pas SOAP:Envelope.
R1031	Lorsqu'une ENVELOPE contient un élément de code faultcode, le contenu de cet élément ne doit PAS utiliser la notation des points SOAP 1.1 pour affiner la signification de la faute.
R1032	Les éléments SOAP:envelope, SOAP:header et SOAP:body d'une ENVELOPE NE DOIVENT PAS avoir des attributs dans le même espace de noms que celui de l'élément de document qualifié Envelope
R1033	Une ENVELOPE NE DEVRAIT PAS contenir la déclaration d'espace de noms :`xmlns:xml=http://www.w3.org/XML/1998/namespace.`
R1109	La valeur du champ d'en-tête HTTP SoapAction dans une requête HTTP MESSAGE DOIT être une chaîne entre guillemets.
R1111	Une INSTANCE DEVRAIT utiliser un code d'état HTTP 200 OK sur un message de réponse contenant une enveloppe qui n'est pas une erreur.
R1126	Une INSTANCE DOIT renvoyer un code d'état HTTP d'erreur serveur interne 500 si l'enveloppe de réponse est une erreur.
R1132	Une requête HTTP MESSAGE DOIT utiliser la méthode HTTP POST.
R1140	UN MESSAGE DEVRAIT être envoyé en utilisant HTTP/1.1.
R1141	Un MESSAGE DOIT être envoyé en utilisant HTTP/1.1 ou HTTP/1.0.

Règle	Description
R2113	Une ENVELOPE NE DOIT PAS inclure l'attribut SOAPENC:ArrayType.
R2211	Une ENVELOPE décrite avec une liaison littérale rpc-NE DOIT PAS avoir l'attribut xsi:nil avec une valeur de 1 ou true sur les accesseurs de pièce.
R2714	Pour les opérations à sens unique, une INSTANCE NE DOIT PAS renvoyer une réponse HTTP contenant une enveloppe. Plus précisément, l'entité de réponse HTTP doit être vide.
R2729	Une ENVELOPE décrite avec une liaison littérale rpc-qui est une réponse DOIT avoir un élément wrapper dont le nom est le nom wsdl:operation correspondant suffixé avec StringResponse.
R2735	Une ENVELOPE décrite avec une liaison littérale rpc-DOIT placer les éléments d'accesseur de pièce pour les paramètres et renvoyer la valeur dans aucun espace de noms.
R2738	Une ENVELOPE DOIT inclure tous les soapbind:headers spécifiés sur un wsdl:input ou wsdl:output d'un wsdl:operation d'un wsdl:binding qui le décrit.
R2740	Un wsdl:binding dans une DESCRIPTION DEVRAIT contenir un soapbind:fault décrivant chaque défaut connu.
R2744	Une requête HTTP MESSAGE DOIT contenir un champ d'en-tête HTTP SoapAction avec une valeur entre guillemets égale à la valeur de l'attribut SoapAction de soapbind:operation, s'il est présent dans la description WSDL correspondante.

Vérification de validation des messages XML

August 20, 2021

La vérification de validation des messages XML examine les demandes contenant des messages XML pour s'assurer qu'elles sont valides. Si une demande contient un message XML non valide, le Web App Firewall bloque la demande. Le but de la vérification de validation XML est d'empêcher un attaquant d'utiliser des messages XML invalides spécialement conçus pour enfreindre la sécurité de votre application.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification de validation des messages XML, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Journal et Statistiques.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification de validation des messages XML :

- `set appfw profile <name> -xmlValidationAction [**block**] [**log**] [**stats**] [**none**]`

Vous devez utiliser l'interface graphique pour configurer les autres paramètres de vérification de validation XML. Dans la boîte de dialogue
Modifier la vérification de validation des messages XML, sous l'onglet
Vérifications, vous pouvez configurer les paramètres suivants :

- **Validation des messages XML.** Utilisez l'une des options suivantes pour valider le message XML :
  - **Enveloppe SOAP.** Valider uniquement l'enveloppe SOAP des messages XML.
  - **WSDL.** Valider les messages XML à l'aide d'un XML SOAP WSDL. Si vous choisissez la validation WSDL, dans la liste déroulante Objet WSDL, vous devez choisir un WSDL. Si vous souhaitez valider un fichier WSDL qui n'a pas encore été importé dans le Web App Firewall, vous pouvez cliquer sur le bouton Importer pour ouvrir la boîte de dialogue Gérer les importations WSDL et importer votre fichier WSDL. Voir WSDL pour plus d'informations.
    * Si vous souhaitez valider l'URL entière, laissez le bouton radio Absolute dans le tableau de boutons Vérification du point de terminaison sélectionné. Si vous souhaitez valider uniquement la partie de l'URL après l'hôte, sélectionnez le bouton radio Relative.
    * Si vous souhaitez que le Web App Firewall applique strictement le WSDL et qu'il n'autorise pas d'en-têtes XML supplémentaires non définis dans le WSDL, vous devez désactiver la case à cocher Autoriser les en-têtes supplémentaires non définis dans le WSDL.
      Attention : Si vous décochez la case
      Autoriser les en-têtes supplémentaires non définis dans le WSDL et que votre WSDL

ne définit pas tous les en-têtes XML que votre application XML protégée ou Web 2.0 attend ou qu'un client envoie, vous pouvez bloquer l'accès légitime à votre service protégé.

  - **Schéma XML.** Valider les messages XML à l'aide d'un schéma XML. Si vous choisissez la validation de schéma XML, dans la liste déroulante Objet de schéma XML, vous devez choisir un schéma XML. Si vous souhaitez valider un schéma XML qui n'a pas encore été importé dans le Web App Firewall, vous pouvez cliquer sur le bouton Importer pour ouvrir la boîte de dialogue Gérer les importations de schéma XML et importer votre WSDL. Voir WSDL pour plus d'informations.

- **Validation des réponses.** Par défaut, le Web App Firewall ne tente pas de valider les réponses. Si vous souhaitez valider les réponses de votre application protégée ou de votre site Web 2.0, activez la case à cocher Valider la réponse. Lorsque vous le faites, la case à cocher Réutiliser le schéma XML spécifié dans la validation de la demande et la liste déroulante Objet de schéma XML sont activées.
  - Cochez la case Réutiliser le schéma XML pour utiliser le schéma que vous avez spécifié pour la validation de la demande pour effectuer également la validation de la réponse. Remarque : Si vous cochez cette case, la liste déroulante Objet de schéma XML est grisée.
  - Si vous souhaitez utiliser un schéma XML différent pour la validation de réponse, utilisez la liste déroulante Objet de schéma XML pour sélectionner ou télécharger ce schéma XML.

Vérification du filtrage des erreurs XML SOAP

January 21, 2021

La vérification de filtrage des erreurs XML SOAP examine les réponses de vos services Web protégés et filtre les erreurs XML SOAP. Cela empêche les fuites d'informations sensibles aux attaquants.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier le contrôle du filtrage des erreurs SOAP XML, sous l'onglet **Général**, vous pouvez activer ou désactiver les actions Bloquer, Journal et Statistiques et Supprimer, qui supprime les erreurs SOAP avant de transférer la réponse à l'utilisateur.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification du filtrage des erreurs XML SOAP :

```
set appfw profile <name> -XMLSOAPFaultAction [block] [log] [stats] [none]
```

Vous ne pouvez pas configurer des exceptions à la vérification XML SOAP Fault Filtering. Vous ne pouvez l'activer ou le désactiver que.

Vérifications de protection JSON

August 20, 2021

Citrix Web App Firewall protège vos applications JSON contre les attaques DoS au niveau du contenu, SQL ou par script intersite. Lorsqu'une requête JSON comporte une attaque DoS, SQL ou par script intersite, vous devez protéger votre application en configurant des limites sur les structures JSON telles que les tableaux et les chaînes.

> **Remarque :**
>
> Les vérifications de sécurité JSON s'appliquent uniquement au contenu envoyé avec un en-tête de type de contenu JSON. Si l'en-tête de type de contenu est manquant ou est défini sur une valeur différente, toutes les vérifications de sécurité JSON sont contournées. Si vous souhaitez protéger vos applications JSON, les webmasters de chaque serveur Web qui héberge ces applications doivent s'assurer qu'un en-tête de type de contenu JSON approprié est envoyé.
>
> La fonctionnalité d'apprentissage n'est pas prise en charge pour JSON SQL, les scripts inter-sites, les types de contenu DOS.

Vérification de la protection par déni de service JSON

August 20, 2021

La vérification JSON par déni de service (DoS) examine une requête JSON entrante et valide s'il existe des données correspondant aux caractéristiques d'une attaque DoS. Si la requête présentait des violations JSON, l'appliance bloque la demande, consigne les données, envoie une alerte SNMP et affiche également une page d'erreur JSON. Le but de la vérification DoS JSON est d'empêcher un attaquant d'envoyer une requête JSON pour lancer des attaques DoS sur vos applications JSON ou site Web.

Lorsqu'un client envoie une requête à une appliance Citrix ADC, l'analyseur JSON analyse la charge utile de la requête et, si une violation est observée, l'appliance applique des contraintes sur la structure JSON. La contrainte applique une limite de taille sur la requête JSON. Par conséquent, si une violation JSON a été observée, l'appliance applique une action et répond avec la page d'erreur JSON.

Règles DoS JSON

Lorsque l'appliance reçoit une demande JSON, la protection DOS JSON applique la limite de taille aux paramètres DoS suivants dans la charge utile de la requête.

1. profondeur maximale : imbrication maximale (profondeur) du document JSON. Cette vérification protège contre les documents dont la hiérarchie est excessive.

2. longueur maximale du document : longueur maximale du document JSON.
3. longueur maximale du tableau : longueur maximale du tableau dans l'un des objets JSON. Cette vérification protège contre les baies ayant de grandes longueurs.
4. longueur de chaîne maximale : longueur de chaîne maximale dans le JSON. Cette vérification protège contre les chaînes de grande longueur.
5. Nombre maximum de touches d'objet : Nombre maximum de touches dans l'un des objets JSON. Cette vérification protège contre les objets qui ont un grand nombre de clés.
6. longueur maximale de la clé d'objet : longueur maximale de la clé dans l'un des objets JSON. Cette vérification protège contre les objets qui ont de grandes clés.

Voici une liste des règles DoS JSON validées lors de l'analyse JSON.

1. JsonMaxContainerDepth. Cette vérification peut être activée en configurant la vérification JSONMaxContainerDepth et par défaut l'option est OFF.

2. JsonMaxContainerDepth. Cette vérification peut être active/désactivée par l'option configurable JsonMaxContainerDepthCheck et la valeur par défaut peut être modifiée par l'option JsonMaxContainerDepth. Toutefois, vous pouvez faire varier les niveaux maximum à une valeur comprise entre 1 et 127. Valeur par défaut : 5, Valeur minimale : 1, Valeur maximale : 127

3. JSONMaxDocumentLength. Cette vérification peut être activée en configurant la vérification JsonMaxDocumentLength et l'option par défaut est OFF.

4. JSONMaxDocumentLength. Cette vérification peut être activée en configurant la vérification JsonMaxDocumentLength et la longueur par défaut est définie sur 20000000 octets. Valeur minimale : 1, Valeur maximale : 2147483647

5. JSONMaxObjectKeyCount. La règle valide si la vérification du nombre maximal de clés d'objet JSON est activée ou désactivée. Valeurs possibles : ON, OFF, Valeur par défaut : OFF

6. JSONMaxObjectKeyCount. Cette vérification peut être activée en configurant la vérification JsonMaxObjectKeyCount. La vérification protège contre les objets qui ont un grand nombre de clés et la valeur par défaut est définie sur 1000 octets. Valeur minimale : 0, Valeur maximale : 2147483647

7. JSONMaxObjectKeyLength. Cette vérification peut être activée en configurant la vérification JSONMaxObjectKeyLength. La règle valide si la vérification de la longueur maximale de la clé d'objet JSON est activée ou désactivée. Par défaut, il est désactivé.

8. JSONMaxObjectKeyLength. Le contrôle protège contre les objets qui ont une grande longueur de clé. Valeur par défaut : 128. Valeur minimale : 1, Valeur maximale : 2147483647

9. JSONMaxArrayLength. La règle valide si la vérification de la longueur maximale du tableau JSON est ON ou OFF. Par défaut, il est désactivé.

10. JSONMaxArrayLength. La vérification protège contre les baies qui ont de grandes longueurs. Par défaut, la valeur est définie sur 10000. Valeur minimale : 1, Valeur maximale : 2147483647

11. JSONMaxStringLength. Cette vérification peut être activée en configurant la vérification JsonMaxStringLength. La vérification valide si la longueur maximale de chaîne JSON est ON ou OFF. Par défaut, il est désactivé.
12. JSONMaxStringLength. Le contrôle protège contre les chaînes de grande longueur. Par défaut, il est défini sur 1000000. Valeur minimale : 1, Valeur maximale : 2147483647

Configurer la vérification de la protection DoS JSON

Pour configurer la protection DoS JSON, vous devez effectuer les étapes suivantes :

1. Ajouter un profil de pare-feu d'application pour JSON.
2. Définissez le profil de pare-feu d'application pour les paramètres de DoS JSON.
3. Configurez les variables DoS JSON en liant le profil de pare-feu de l'application.

Ajouter un profil de pare-feu d'application pour la protection DoS JSON

Vous devez d'abord créer un profil qui spécifie comment le pare-feu d'application doit protéger votre contenu Web JSON contre les attaques DoS JSON.
À l'invite de commandes, tapez :

```
add appfw profile <name> -type (HTML | XML | JSON)
```

> *Remarque* :
>
> Lorsque vous définissez le type de profil comme JSON, d'autres vérifications telles que HTML ou XML ne s'appliquent pas.

Exemple

```
add appfw profile profile1 -type JSON
```

Définir le profil de pare-feu d'application pour la protection DoS JSON

Vous devez configurer le profil pour une ou plusieurs actions DOS JSON et objet d'erreur DOS JSON à définir sur le profil de pare-feu de l'application.
À l'invite de commandes, tapez :

```
set appfw profile <name> -JSONDoSAction [block] | [log] | [stats] | [none]
```

Bloquer - Bloquer les connexions qui violent cette vérification de sécurité.
Journal - Consigner les violations de cette vérification de sécurité.
Stats - Générez des statistiques pour cette vérification de sécurité.
Aucun - Désactivez toutes les actions pour cette vérification de sécurité.

> *Remarque* :
>
> Pour activer une ou plusieurs actions, tapez “set appfw profile -JSONDoSAction” suivi des actions à activer.

Exemple

```
set appfw profile profile1 -JSONDoSAction block log stat
```

Configurer les variables DoS en liant le profil de pare-feu d’application

Pour fournir une protection DoS JSON, vous devez lier le profil de pare-feu de l’application aux paramètres DoS JSON.
À l’invite de commandes, tapez :

```
bind appfw profile <name> -JSONDoSURL <expression> [-JSONMaxContainerDepthCheck
 ( ON | OFF )[-JSONMaxContainerDepth <positive_integer>]] [-JSONMaxDocumentLengthCheck
 ( ON | OFF )[-JSONMaxDocumentLength <positive_integer>]] [-JSONMaxObjectKeyCountCheck
 ( ON | OFF )[-SONMaxObjectKeyCount <positive_integer>]] [-JSONMaxObjectKeyLengthCheck
 ( ON | OFF )[-JSONMaxObjectKeyLength <positive_integer>]] [-JSONMaxArrayLengthCheck
 ( ON | OFF )[-JSONMaxArrayLength <positive_integer>]] [-JSONMaxStringLengthCheck
 ( ON | OFF )[-JSONMaxStringLength <positive_integer>]]
```

Exemple

```
bind appfw profile profile1 -JSONDoSURL  ".*"  -JSONMaxContainerDepthCheck ON
```

> *Remarque* :
>
> Les vérifications DoS JSON ne s’appliquent que si le type de profil est sélectionné comme JSON. En outre, le SQL, le script inter-site, le format de champ et les signatures de champ Formulaire sont appliqués aux paramètres de requête dans les cas de profil JSON.

Page d’erreur d’importation JSON

Si une demande entrante a subi une attaque DoS et lorsque vous bloquez la demande, l’appliance affiche un message d’erreur. Pour ce faire, vous devez importer la page d’erreur JSON.
À l’invite de commandes, tapez :

```
import appfw jsonerrorpage <src> <name> [-comment <string>] [-overwrite]
```

Où,

src. URL (protocole, hôte, chemin d’accès et nom) pour l’emplacement où stocker l’objet d’erreur JSON importé.

> *Remarque* :
>
> L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS qui nécessite l'authentification de certificat client pour l'accès. Il s'agit d'un argument obligatoire. Longueur maximale : 2047.

Nom. Nom à affecter à l'objet d'erreur JSON sur Citrix ADC. Il s'agit d'un argument obligatoire. Longueur maximale : 31

Commentaire. Tout commentaire pour conserver les informations sur l'objet d'erreur JSON. Longueur maximale : 255

Remplacer. Remplacer tout objet d'erreur JSON existant du même nom.

Exemple de configuration

```
Add appfw prof profjson - type JSON
Bind appfw prof profjson - JSONDoSURL ".*" -
    JSONMaxDocumentLengthCheck ON -JSONMaxDocumentLength 30 -
    JSONMaxContainerDepthCheck ON -JSONMaxContainerDepth 3
    JSONMaxObjectKeyCountCheck ON -JSONMaxObjectKeyCount 4 -
    JSONMaxObjectKeyLengthCheck ON -JSONMaxObjectKeyLength 10 -
    JSONMaxArrayLengthCheck ON -JSONMaxArrayLength 5 -
    JSONMaxStringLengthCheck ON -JSONMaxStringLength 30
<!--NeedCopy-->
```

Exemples de charges utiles, de messages de journal et de compteurs :

Violation JSONMaxDocumentLength

JSONMaxDocumentLength: 30

Payload: {"a":"A","b":"B","c":"C","d":"D","e":"E"}

Message du journal :

```
Document Length exceeds 20000000 May 29 20:23:32 <local0.info>
    10.217.31.243 05/29/2019:20:23:32 GMT 0-PPE-0 : default APPFW
    APPFW_JSON_DOS_MAX_DOCUMENT_LENGTH 136 0 : 10.217.32.134 114-PPE0 -
    profjson http://10.217.30.120/forms/login.html Document exceeds
    maximum document length (30). cn1=30467 cn2=115 cs1=profjson cs2=
    PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Compteurs :

```
1 0 6 as_viol_json_dos
2 0 3 as_viol_json_dos_max_document_length
```



```
3 0 6 as_log_json_dos
4 0 3 as_log_json_dos_max_document_length
5 0 6 as_viol_json_dos_profile appfw__(profile1)
6 0 3 as_viol_json_dos_max_document_length_profile appfw__(profile1)
7 0 6 as_log_json_dos_profile appfw__(profile1)
8 0 3 as_log_json_dos_max_document_length_profile appfw__(profile1)
9 <!--NeedCopy-->
```

Violation JSONMaxContainerDepth

JSONMaxContainerDepth: 3
Payload: {“a”: {”b”: {“c”: {“d”: { ”e” : “f” }}}}}

Message du journal :

```
1 May 29 19:33:59 <local0.info> 10.217.31.243 05/29/2019:19:33:59 GMT 0-
     PPE-1 : default APPFW APPFW_JSON_DOS_MAX_CONTAINER_DEPTH 4626 0 :
     10.217.31.247 22-PPE1 - profjson http://10.217.30.120/forms/login.
     html Document at offset (15) exceeds maximum container depth (3).
     cn1=30466 cn2=113 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=
     blocked
2 <!--NeedCopy-->
```

Compteurs :

```
1 36 20999 7 1 0 as_viol_json_dos
2 37 0 6 1 0 as_viol_json_dos_max_container_depth
3 38 0 7 1 0 as_log_json_dos
4 39 0 6 1 0 as_log_json_dos_max_container_depth
5 40 0 7 1 0 as_viol_json_dos_profile appfw__(profile1)
6 41 0 6 1 0 as_viol_json_dos_max_container_depth_profile appfw__(
     profile1)
7 42 0 7 1 0 as_log_json_dos_profile appfw__(profile1)
8 43 0 6 1 0 as_log_json_dos_max_container_depth_profile appfw__(profile1
     )
9 <!--NeedCopy-->
```

Violation JSONMaxObjectKeyCount

JSONMaxObjectKeyCount: 4

Payload: {“a”: ”A”, “b”: “B”, “c”:“C”, “d” :“D”, ”e” : “E” }

Message du journal :


```
May 30 19:42:41 <local0.info> 10.217.31.243 05/30/2019:19:42:41 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_OBJECT_KEY_COUNT 457 0 : 10.217.32.134 219-PPE1 - profjson http://10.217.30.120/forms/login.html Object at offset (41) that exceeds maximum key count (4). cn1=30468 cn2=118 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Compteurs :

```
94 119105 15 1 0 as_viol_json_dos
95 0 4 1 0 as_viol_json_dos_max_object_key_count
96 0 15 1 0 as_log_json_dos
97 0 4 1 0 as_log_json_dos_max_object_key_count
98 0 15 1 0 as_viol_json_dos_profile appfw__(profile1)
99 0 4 1 0 as_viol_json_dos_max_object_key_count_profile appfw__(profile1)
100 0 15 1 0 as_log_json_dos_profile appfw__(profile1)
101 0 4 1 0 as_log_json_dos_max_object_key_count_profile appfw__(profile1)
<!--NeedCopy-->
```

Violation JSONMaxObjectKeyLength

JSONMaxObjectKeyLength: 10
Payload: {“a”: ”A”, “b1234567890”: “B”, “c”:“C”, “d” :“D”, ”e” : “E” }

Message du journal :

```
May 31 20:26:10 <local0.info> 10.217.31.243 05/31/2019:20:26:10 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_OBJECT_KEY_LENGTH 102 0 : 10.217.32.134 89-PPE1 - profjson http://10.217.30.120/forms/login.html Object key(b1234567890) at offset (12) exceeds maximum key length (10). cn1=30469 cn2=118 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Compteurs :

```
242172 6 1 0 as_viol_json_dos
0 1 1 0 as_viol_json_dos_max_object_key_length
10 0 5 1 0 as_log_json_dos
11 0 1 1 0 as_log_json_dos_max_object_key_length
12 0 6 1 0 as_viol_json_dos_profile appfw__(profile1)
```



```
13 0 1 1 0 as_viol_json_dos_max_object_key_length_profile appfw__(
    profile1)
14 0 5 1 0 as_log_json_dos_profile appfw__(profile1)
15 0 1 1 0 as_log_json_dos_max_object_key_length_profile appfw__(
    profile1)
<!--NeedCopy-->
```

Violation JSONMaxArrayLength

JSONMaxArrayLength : 5

Charge utile : {« a » : » A », « c [» : » d », » e », » f », » g », » h »], » e » :[« E », » e »]}

Message du journal :

```
May 29 20:58:39 <local0.info> 10.217.31.243 05/29/2019:20:58:39 GMT 0-
    PPE-1 : default APPFW APPFW_JSON_DOS_MAX_ARRAY_LENGTH 4650 0 :
    10.217.32.134 153-PPE1 -profjson http://10.217.30.120/forms/login.
    html Array at offset (37) that exceeds maximum array length (5). cn1
    =30469 cn2=120 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Compteurs :

```
36 182293 10 1 0 as_viol_json_dos
37 0 1 1 0 as_viol_json_dos_max_array_length
38 0 10 1 0 as_log_json_dos 39 0 1 1 0 as_log_json_dos_max_array_length
40 0 10 1 0 as_viol_json_dos_profile appfw__(profile1)
41 0 1 1 0 as_viol_json_dos_max_array_length_profile appfw__(profile1)
42 0 10 1 0 as_log_json_dos_profile appfw__(profile1)
43 0 1 1 0 as_log_json_dos_max_array_length_profile appfw__(profile1))
<!--NeedCopy-->
```

Violation JSONMaxStringLength

JSONMaxStringLength : 10

Payload: {“a”: ”A”, “c”:”CcCcCcCcCcCcCcCcCc”,”e”:[« E », » e »]}

Message du journal :

```
May 29 20:05:02 <local0.info> 10.217.31.243 05/29/2019:20:05:02 GMT 0-
    PPE-0 : default APPFW APPFW_JSON_DOS_MAX_STRING_LENGTH 134 0 :
    10.217.32.134 80-PPE0 - profjson http://10.217.30.120/forms/login.
    html String(CcCcCcCcCcCcCc) at offset (27) that exceeds maximum
    string length (10). n1=30470 cn2=122 cs1=profjson cs2=PPE0 cs4=ALERT
     cs5=2019 act=blocked
```



```
<!--NeedCopy-->
```

Compteurs :

```
44 91079 3 1 0 as_viol_json_dos
45 0 1 1 0 as_viol_json_dos_max_string_length
46 0 3 1 0 as_log_json_dos
47 0 1 1 0 as_log_json_dos_max_string_length
48 0 3 1 0 as_viol_json_dos_profile appfw__(profile1)
49 0 1 1 0 as_viol_json_dos_max_string_length_profile appfw__(profile1)
50 0 3 1 0 as_log_json_dos_profile appfw__(profile1)
51 0 1 1 0 as_log_json_dos_max_string_length_profile appfw__(profile1
<!--NeedCopy-->
```

Configurer la protection DoS JSON à l'aide de l'interface graphique Citrix

Suivez la procédure ci-dessous pour définir les paramètres de protection DOS JSON.

1. Dans le volet de navigation, accédez à **Sécurité** > **Profils**.
2. Dans la page **Profils**, cliquez sur **Ajouter**.
3. Dans la page **Profil du Citrix Web App Firewall**, cliquez sur **Vérifications de sécurité sous Paramètres avancés**.
4. Dans la section **Vérifications de sécurité**, accédez aux paramètres de **déni de service JSON**.
5. Cliquez sur l'icône exécutable située près de la case à cocher.



6. Cliquez sur **Paramètres d'action** pour accéder à la page **Paramètres de déni de service JSON**.
7. Sélectionnez l'action DoS JSON.
8. Cliquez sur **OK**.



9. Dans la page **Profil du Citrix Web App Firewall**, cliquez sur **Règles de relaxation** sous **Paramètres avancés**.
10. Dans la section **Règles de relaxation**, sélectionnez Paramètres de **déni de service JSON** et cliquez sur **Modifier**.



11. Dans le **pare-feu d'application JSON Denial of Service Check**, définissez les valeurs de validation DOS JSON.
12. Cliquez sur **OK**.



13. Dans la page **Profil du Citrix Web App Firewall**, cliquez sur **Paramètres du profil** sous **Paramètres avancés**.
14. Dans la section **Paramètres du profil**, accédez à la sous-section **Paramètres d'erreur JSON** pour définir la page **d'erreur DoS JSON**.



15. Dans la **page Error Page Importer un objet JSON**, définissez les paramètres suivants :
    a) Importer à partir de. Importez la page d'erreur en tant que texte, fichier ou URL.
    b) URL. URL pour rediriger l'utilisateur vers la page d'erreur.
    1 Dossier. Sélectionnez un fichier à importer en tant que fichier d'erreur DoS JSON.
    c) Texte. Entrez le contenu du fichier JSON.
    d) Cliquez sur Continuer.

e) Dossier. Entrez le nom du fichier.
f) Contenu du fichier. Ajoutez le contenu du fichier d'erreur.
g) Cliquez sur **OK**.



16. Cliquez sur **OK**.
17. Cliquez sur **Terminé**.

Vérification de la protection JSON SQL Injection

August 20, 2021

Une requête JSON entrante peut avoir une injection SQL sous la forme de chaînes de requête SQL partielles ou de commandes non autorisées dans le code. Cela conduit au vol de données de la base de données JSON de vos serveurs Web. À la réception d'une telle demande, l'appliance bloque cette demande pour protéger vos données.

Considérons un scénario où un client envoie une requête SQL JSON à une appliance Citrix ADC, l'analyseur JSON analyse la charge utile de la requête et, si une injection SQL est observée, l'appliance applique des contraintes sur le contenu SQL JSON. La contrainte impose une limite de taille sur la requête SQL JSON. Par conséquent, si une injection JSON SQL est observée, l'appliance applique une action et répond avec la page d'erreur JSON SQL.

Configurer la protection JSON SQL Injection

Pour configurer la protection JSON SQL, vous devez effectuer les étapes suivantes :

1. Ajouter un profil de pare-feu d'application en tant que JSON.
2. Définir le profil de pare-feu d'application pour les paramètres de JSON SQL Injection
3. Configurez l'action SQL JSON en liant le profil de pare-feu de l'application.

Ajouter un profil de pare-feu d'application de type JSON

Vous devez d'abord créer un profil qui spécifie comment le pare-feu d'application doit protéger votre contenu Web JSON contre l'attaque JSON SQL Injection.
À l'invite de commandes, tapez :

```
add appfw profile <name> -type (HTML | XML | JSON)
```

> *Remarque* :
>
> Lorsque vous définissez le type de profil comme JSON, d'autres vérifications telles que HTML ou XML ne s'appliquent pas.

Exemple

```
add appfw profile profile1 -type JSON
```

Configurer l'action JSON SQL Injection

Vous devez configurer une ou plusieurs actions JSON SQL Injection pour protéger votre application contre les attaques par injection JSON SQL.
À l'invite de commandes, tapez :

```
set appfw profile <name> - JSONSQLInjectionAction [block] [log] [stats] [
none]
```

Les actions d'injection SQL sont les suivantes :
Bloquer - Bloquer les connexions qui violent cette vérification de sécurité.
Journal - Consigner les violations de cette vérification de sécurité.
Stats - Générez des statistiques pour cette vérification de sécurité.
Aucun - Désactivez toutes les actions pour cette vérification de sécurité.

Configurer le type d'injection SQL JSON

Pour configurer le type JSON SQL Injection sur un profil de pare-feu d'application, à l'invite de commandes, tapez :

```
set appfw profile <name> - JSONSQLInjectionType <JSONSQLInjectionType>
```


Exemple

```
set appfw profile profile1 -JSONSQLInjectionType SQLKeyword
```

Où sont les types d'injection SQL
disponibles : Types d'injection SQL disponibles.
SQLSplChar. Vérifie les caractères spéciaux SQL,
SQLKeyword. Vérifie les mots-clés SQL.
SQLSplCharANDKeyword. Vérifie les deux et les blocs s'ils sont trouvés.
SQLSplCharORKeyword. . Bloque si un caractère spécial SQL ou un mot-clé spl est trouvé.
Valeurs possibles : SQLSplChar, SQLKeyword, SQLSplCharORKeyword, SQLSplCharANDKeyword.

> *Remarque* :
> Pour activer une ou plusieurs actions, tapez « set appfw profile - JsonSQLinjectionAction » suivi des actions à activer.

Exemple

```
set appfw profile profile1 -JSONSQLInjectionAction block log stat
```

L'exemple suivant montre un exemple de charge utile, son message de journal et ses compteurs de statistiques correspondants :

```
Payload:
=======
{

  "test": "data",
  "username": "waf",
  "password": "select * from t1;",
  "details": {

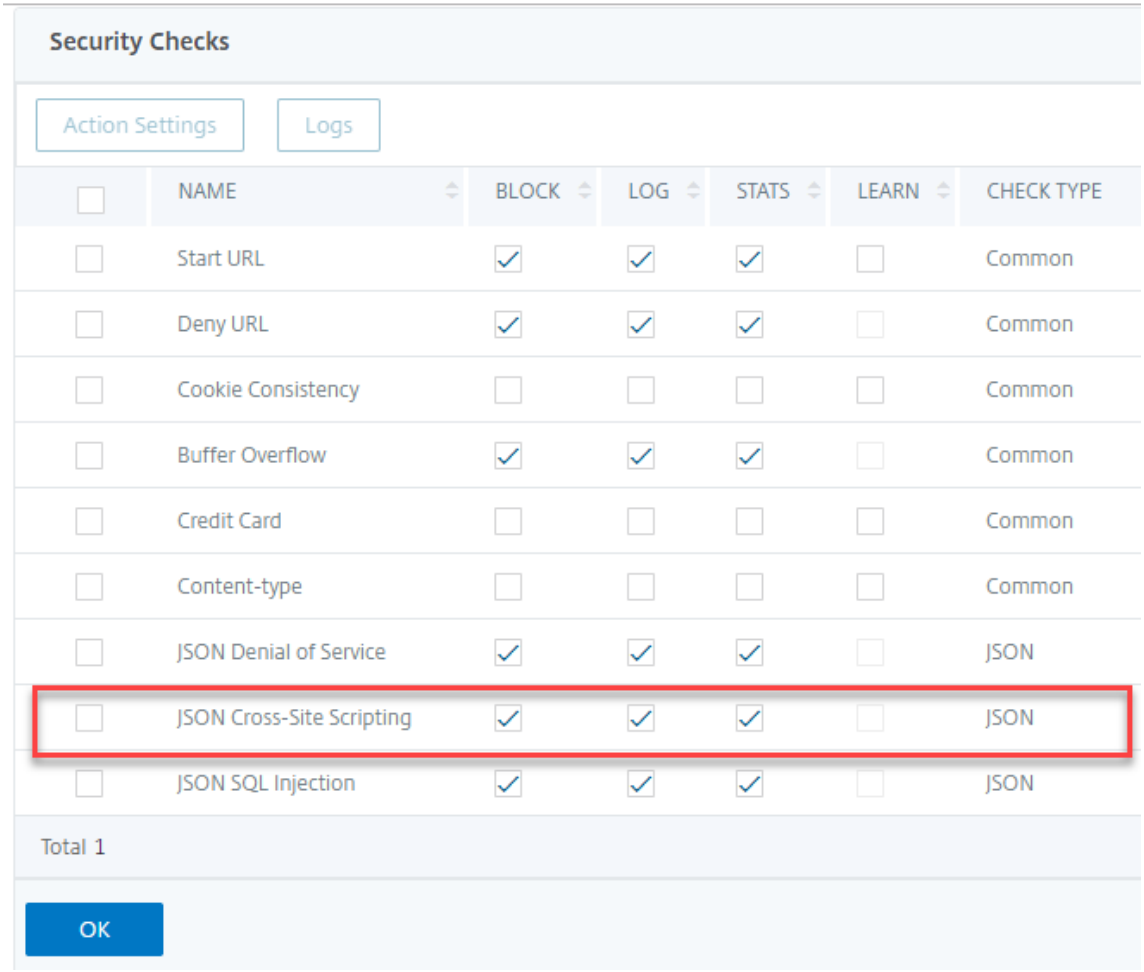
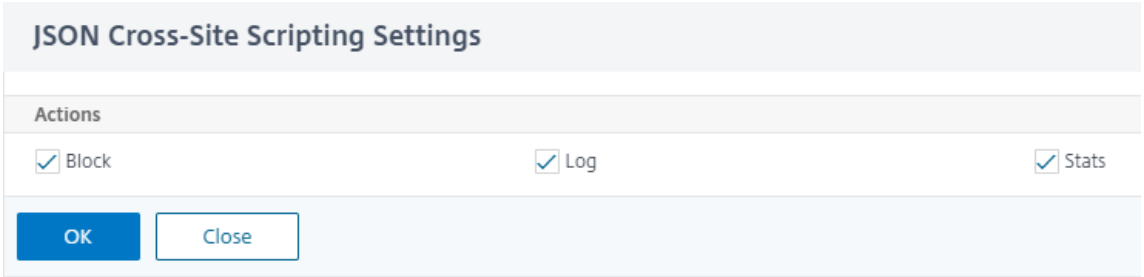
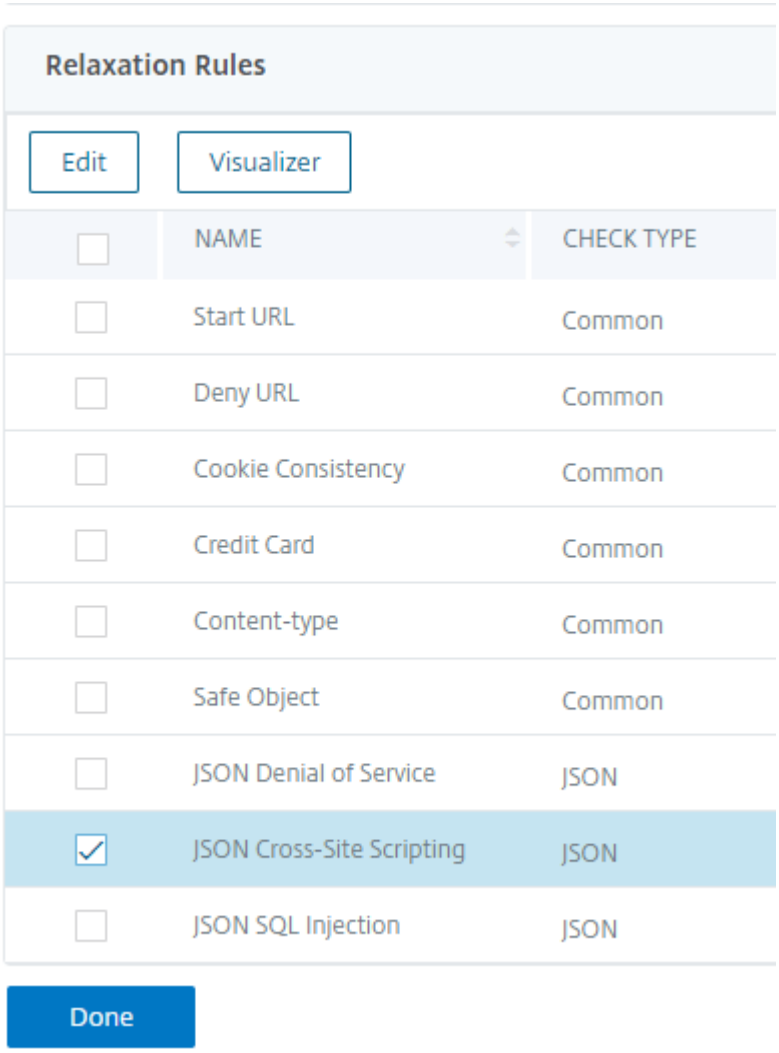
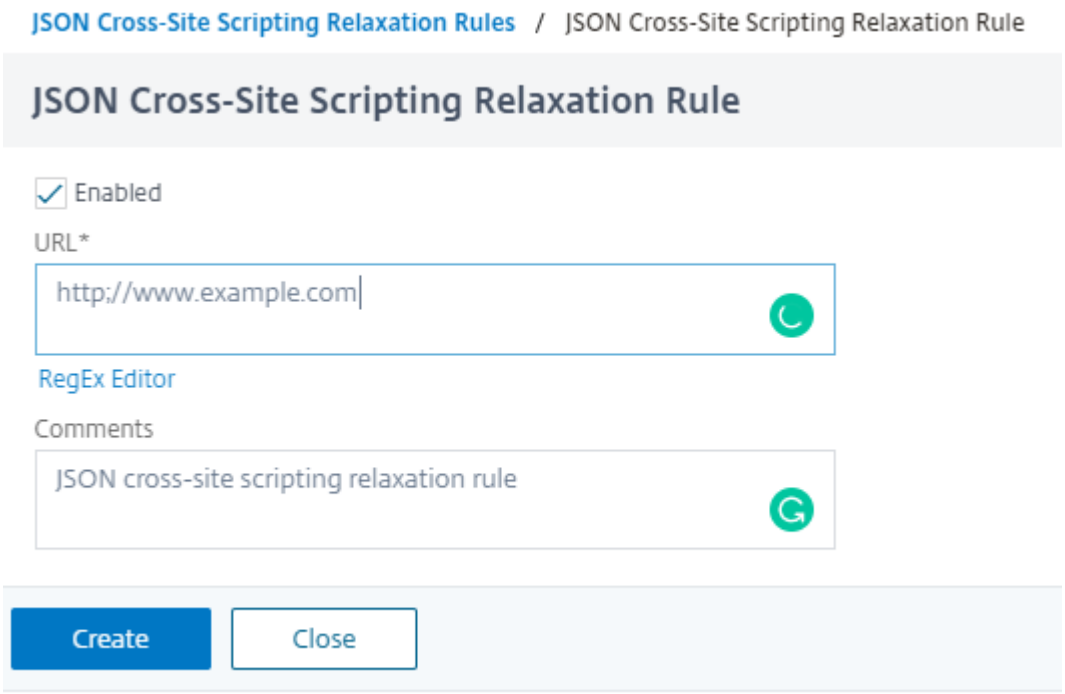
    "surname": "test",
    "age": "23"
   }

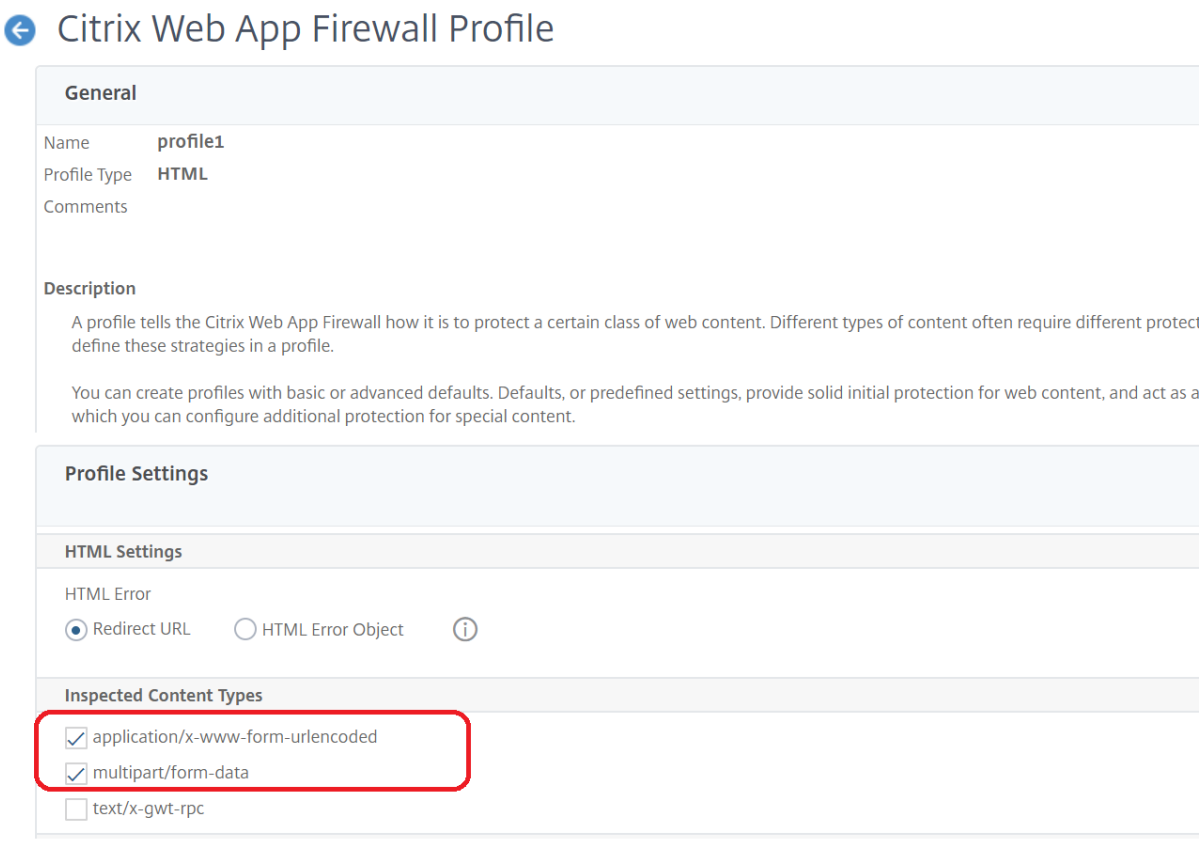
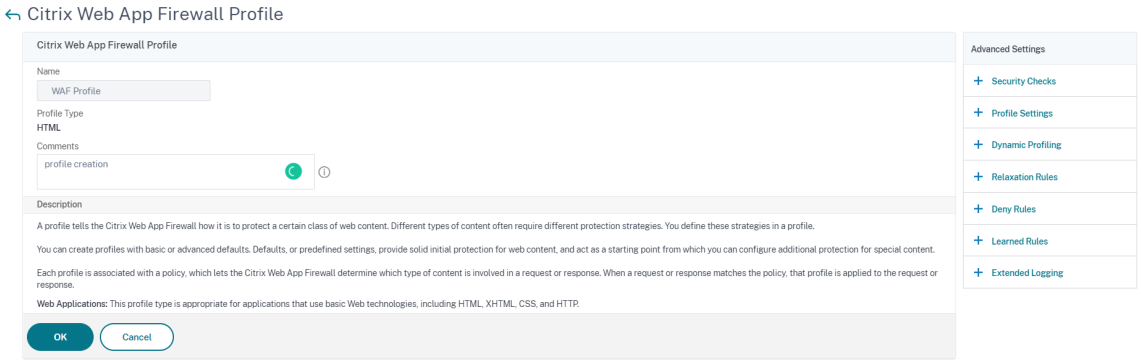
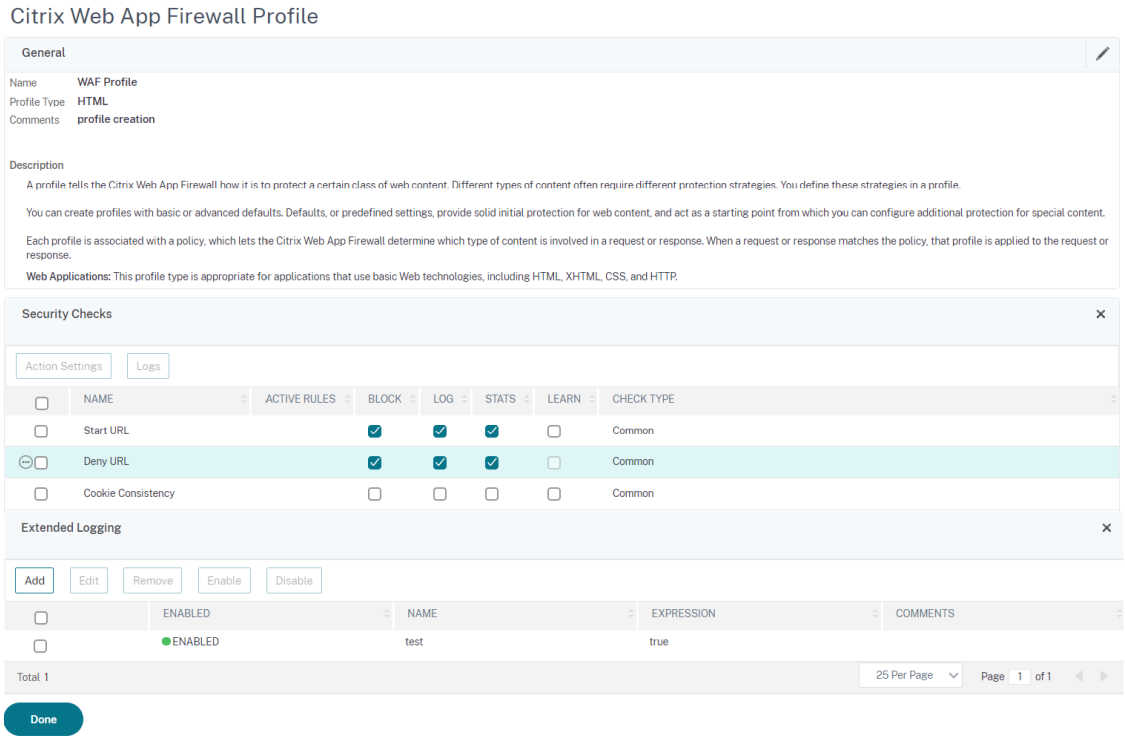
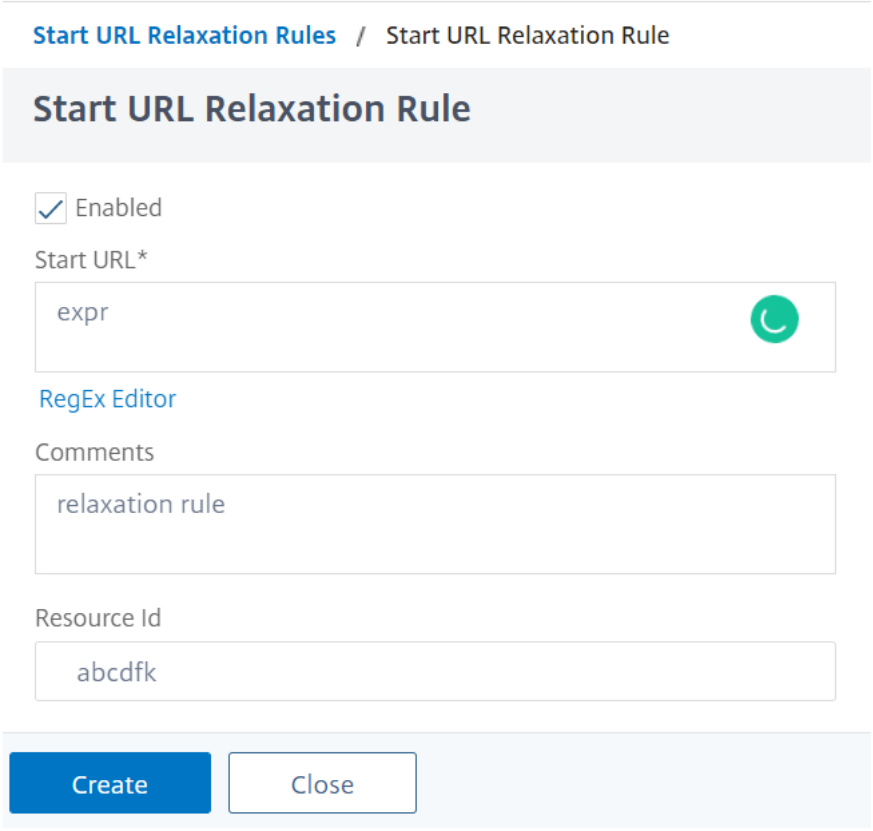
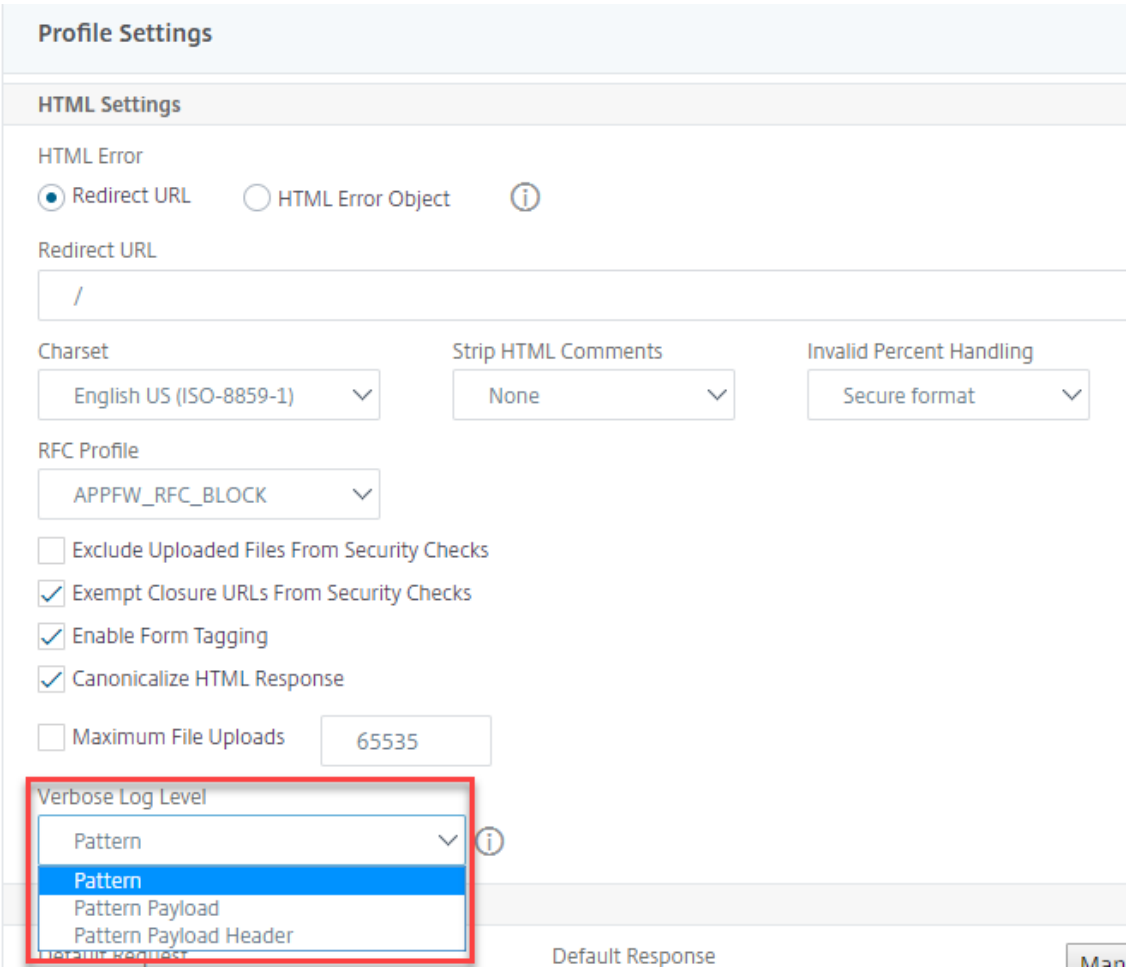
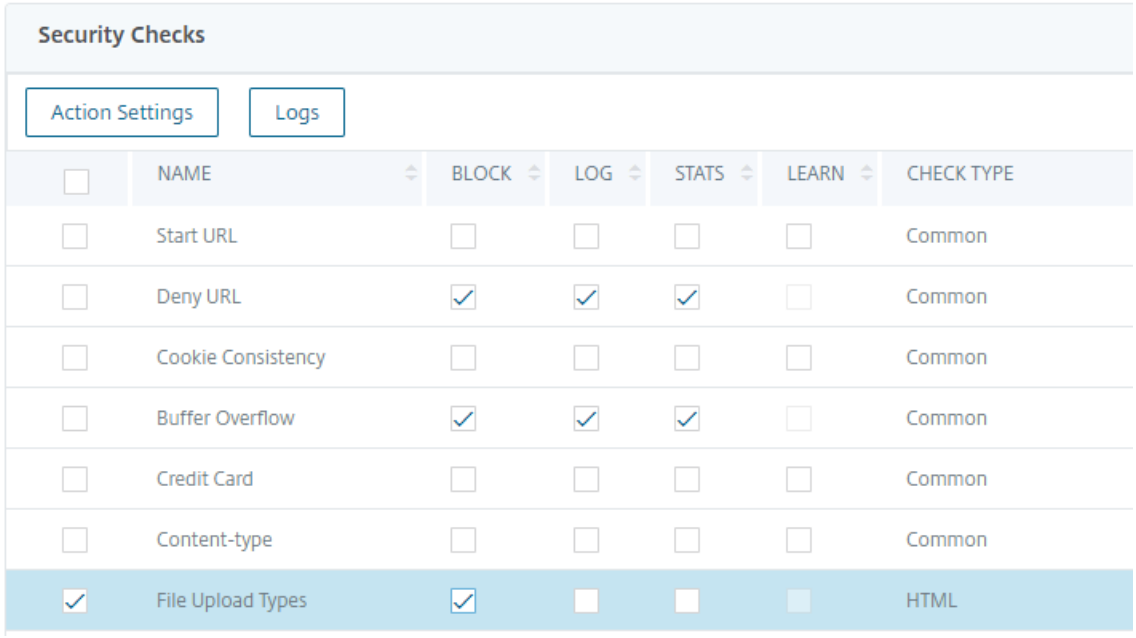
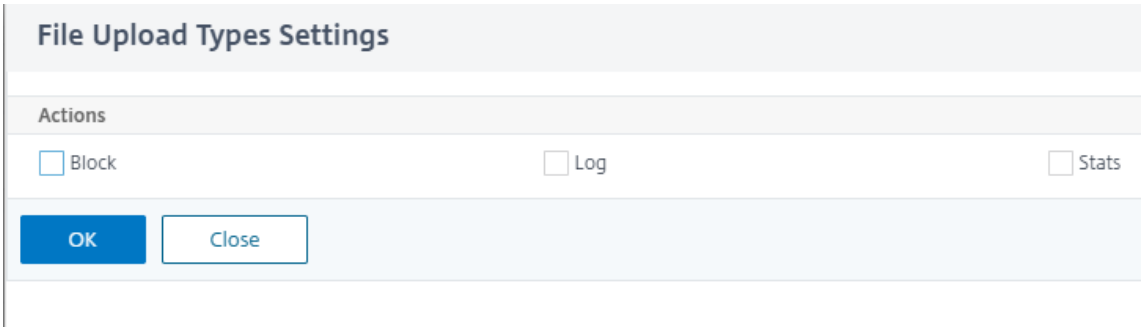
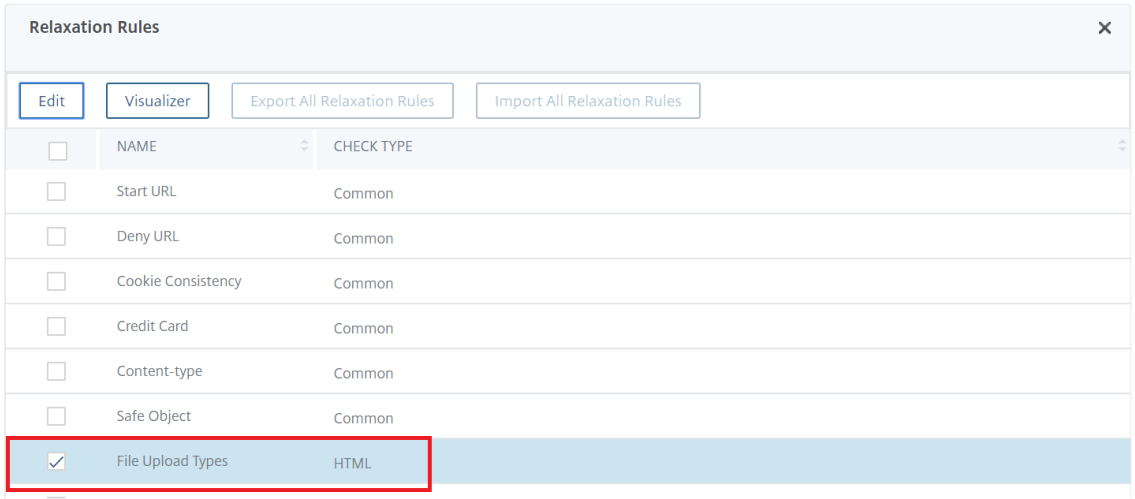
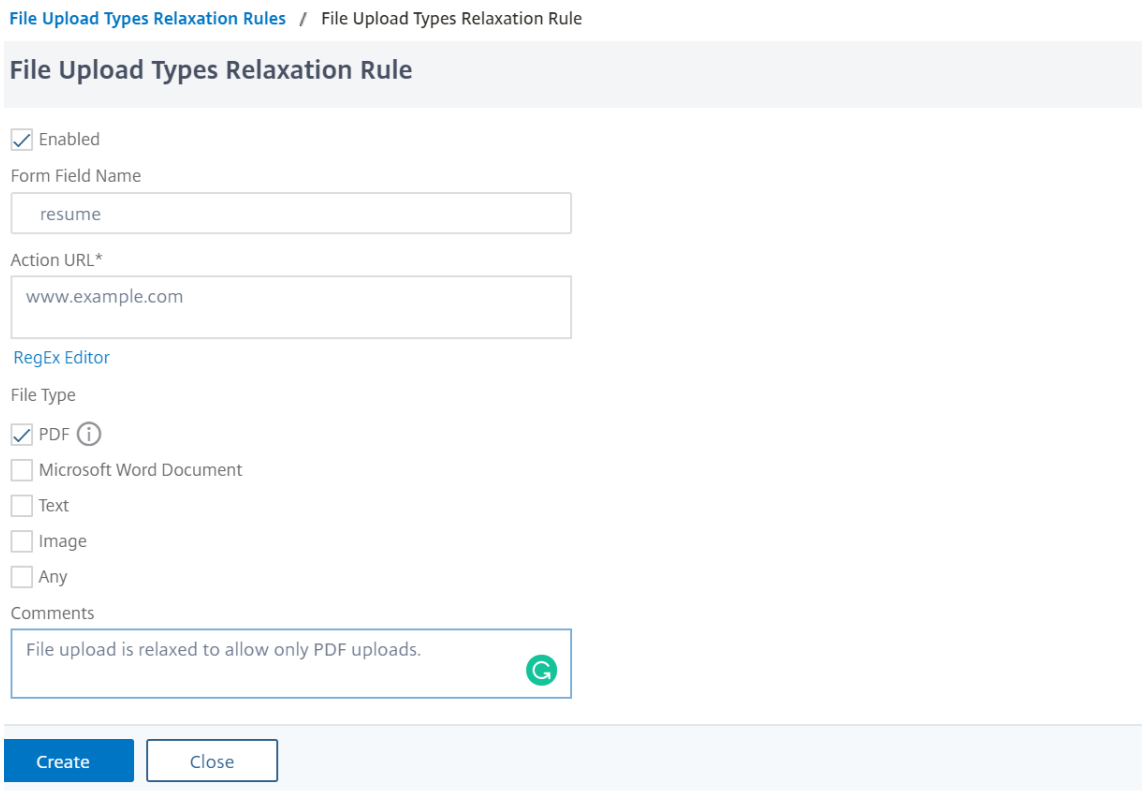
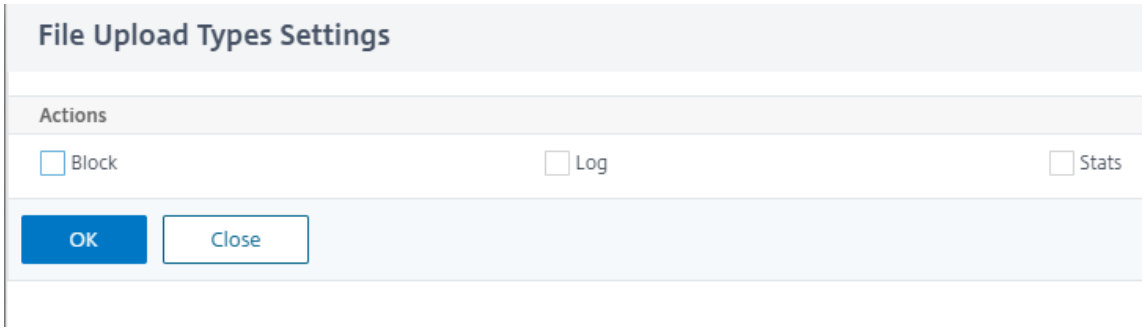
 }


Log Message:
===========
08/19/2019:08:49:46 GMT pegasus121 Informational 0-PPE-0 : default
   APPFW APPFW_JSON_SQL 6656 0 :  10.217.32.165 18402-PPE0 - profjson
   http://10.217.32.147/test.html SQL Keyword check failed for object
   value(with violation="select(;)") starting at offset(52) <blocked>
```



```
Counters:
========
   1  441083             1 as_viol_json_sql
   3       0             1 as_log_json_sql
   5       0             1 as_viol_json_sql_profile appfw__(profjson)
   7       0             1 as_log_json_sql_profile appfw__(profjson)
<!--NeedCopy-->
```

Configurer la protection JSON SQL Injection à l'aide de l'interface graphique Citrix

Suivez la procédure ci-dessous pour définir les paramètres de protection JSON SQL Injection.

1. Dans le volet de navigation, accédez à **Sécurité** > **Profils**.
2. Dans la page **Profils**, cliquez sur **Ajouter**.
3. Sur la page **Profil Citrix Web App Firewall**, cliquez sur **Contrôles de sécurité** sous **Paramètres avancés**.
4. Dans la section **Vérifications de sécurité**, accédez aux paramètres **JSON SQL Injection**.
5. Cliquez sur l'icône exécutable située près de la case à cocher.



6. Cliquez sur **Paramètres d'action** pour accéder à la page **Paramètres d'injection JSON SQL**.
7. Sélectionnez les actions **JSON SQL Injection**.
8. Cliquez sur **OK**.



9. Dans la page **Profil du Citrix Web App Firewall**, cliquez sur **Règles de relaxation** sous **Paramètres avancés**.
10. Dans la section **Règles de relaxation**, sélectionnez Paramètres **d'injection SQL JSON** et cliquez sur **Modifier**.



11. Dans la page Règle de relaxation JSON SQL Injection, entrez l'URL à laquelle la demande doit être envoyée. Toutes les demandes envoyées à cette URL ne seront pas bloquées.
12. Cliquez sur **Créer**.



Vérification de la protection des scripts inter-site JSON

August 20, 2021

Si une charge utile JSON entrante contient des données de script intersite malveillantes, WAF bloque la demande. Les procédures suivantes expliquent comment vous pouvez configurer cela via des interfaces CLI et GUI.

Configurer la protection des scripts inter-sites JSON

Pour configurer la protection des scripts inter-sites JSON, vous devez effectuer les étapes suivantes :

1. Ajouter un profil de pare-feu d'application en tant que JSON.
2. Configurer l'action de script inter-site JSON pour bloquer la charge utile malveillante de script inter-site

Ajouter un profil de pare-feu d'application de type JSON

Vous devez d'abord créer un profil qui spécifie comment le pare-feu d'application doit protéger votre contenu Web JSON contre les attaques de script inter-sites JSON.

À l'invite de commandes, tapez :

```
add appfw profile <name> -type (HTML | XML | JSON)
```


> **Remarque** :
>
> Lorsque vous définissez le type de profil comme JSON, d'autres vérifications telles que HTML ou XML ne s'appliquent pas.

Exemple

```
add appfw profile profile1 -type JSON
```

Exemple de sortie pour violation de script inter-site JSON

```
JSONcross-site scriptingAction: block log stats
Payload: {
 "username":"<a href="jAvAsCrIpT:alert(1)">X</a>","password":"xyz" }


Log message: Aug 19 06:57:33 <local0.info> 10.106.102.21
    08/19/2019:06:57:33 GMT  0-PPE-0 : default APPFW APPFW_JSON_cross-
    site scripting 58 0 :  10.102.1.98 12-PPE0 - profjson http://
    10.106.102.24/ Cross-site script check failed for object value(with
    violation="Bad URL: jAvAsCrIpT:alert(1)") starting at offset(12). <
    blocked>

Counters
    1  357000                  1 as_viol_json_xss
    3  0                       1 as_log_json_xss
    5  0                       1 as_viol_json_xss_profile appfw__(
       profjson)
    7  0                       1 as_log_json_xss_profile appfw__(
       profjson)

<!--NeedCopy-->
```

Configurer l'action de script inter-site JSON

Vous devez configurer une ou plusieurs actions de script JSON inter-site pour protéger votre application contre les attaques de script inter-site JSON.
À l'invite de commandes, tapez :

```
set appfw profile <name> - JSONcross-site scriptingAction [block] [log] [
stats] [none]
```


Exemple

```
set appfw profile profile1 -JSONcross-site scriptingAction block
```

Les actions de script inter-site disponibles sont les suivantes :
Bloquer - Bloquer les connexions qui violent cette vérification de sécurité.
Journal - Consigner les violations de cette vérification de sécurité.
Stats - Générez des statistiques pour cette vérification de sécurité.
Aucun - Désactivez toutes les actions pour cette vérification de sécurité.

> **Remarque** :
> Pour activer une ou plusieurs actions, tapez « set appfw profile - JSONCross-Site ScriptingAction » suivi des actions à activer.

Exemple

```
set appfw profile profile1 -JSONSQLInjectionAction block log stat
```

Configurer la protection JSON Cross Site Scripting (script inter-site) à l'aide de l'interface graphique Citrix

Suivez la procédure ci-dessous pour définir les paramètres de protection Cross Site Scripting (cross-site scripting).

1. Dans le volet de navigation, accédez à **Sécurité** > **Profils**.
2. Dans la page **Profils**, cliquez sur **Ajouter**.
3. Sur la page **Profil Citrix Web App Firewall**, cliquez sur **Contrôles de sécurité** sous **Paramètres avancés**.
4. Dans la section **Vérifications de sécurité**, accédez aux paramètres **JSON Inter-Site Scripting (cross-site scripting)**.
5. Cliquez sur l'icône exécutable située près de la case à cocher.



6. Cliquez sur **Paramètres d'action** pour accéder à la page **Paramètres de script inter-site JSON**.
7. Sélectionnez les actions de script inter-site JSON.
8. Cliquez sur **OK**.



9. Dans la page **Profil du Citrix Web App Firewall**, cliquez sur **Règles de relaxation** sous **Paramètres avancés**.
10. Dans la section **Règles de relaxation**, sélectionnez Paramètres JSON Cross-Site Scripting et cliquez sur **Modifier**.



11. Dans la page **JSON Cross-Site Scripting Relaxation Rule**, cliquez sur **Ajouter** pour ajouter une règle de relaxation JSON Cross-Site Scripting.
12. Entrez l'URL à laquelle la demande doit être envoyée. Toutes les demandes envoyées à cette URL ne seront pas bloquées.
13. Cliquez sur **Créer**.



Gestion des types de contenu

August 20, 2021

Les serveurs Web ajoutent un en-tête Content-Type avec une définition MIME/Type pour chaque type de contenu. Les serveurs Web servent de nombreux types de contenu différents. Par exemple, le code HTML standard est attribué au type MIME « text/html ». Les images JPG sont affectées au type de contenu « image/jpeg » ou « image/jpg ». Un serveur Web normal peut servir différents types de contenu, tous définis dans l'en-tête Type de contenu par le MIME/type attribué.

De nombreuses règles de filtrage du Web App Firewall sont conçues pour filtrer un type de contenu spécifique. Les règles de filtrage s'appliquent à un type de contenu tel que HTML et sont souvent inappropriées lors du filtrage d'un autre type de contenu (comme les images). Par conséquent, le Web App Firewall tente de déterminer le type de contenu des demandes et des réponses avant de les filtrer. Si un serveur Web ou un navigateur n'ajoute pas d'en-tête Content-Type à une requête ou à une réponse, le Web App Firewall applique un type de contenu par défaut et filtre le contenu en conséquence.

Le type de contenu par défaut est généralement « application/octet-stream » avec la définition MIME/-type la plus générique. Le MIME/type est approprié pour tout type de contenu qu'un serveur Web est susceptible de servir. Mais ne fournit pas beaucoup d'informations au Web App Firewall pour lui permettre de choisir le filtrage approprié. Si un serveur Web protégé est configuré pour ajouter des

en-têtes de type de contenu précis, vous pouvez créer un profil pour le serveur Web et lui attribuer un type de contenu par défaut. Ceci est fait pour améliorer à la fois la vitesse et la précision du filtrage.

Vous pouvez également configurer une liste de types de contenu de requête autorisés pour un profil spécifique. Lorsque cette fonctionnalité est configurée, si le Web App Firewall filtre une demande qui ne correspond pas à l'un des types de contenu autorisés, il bloque la demande. Après la mise à niveau de la version 10.5 vers la version 11.0, les types de contenu inconnus qui ne sont pas dans la liste des types de contenu autorisés par défaut ne se lient pas. Vous pouvez ajouter d'autres types de contenu que vous voulez être autorisés aux règles assouplies.

Les requêtes doivent toujours être des types « application/x-www-form-urlencoded », « multipart/form-data » ou « text/x-gwt-rpc ». Le Web App Firewall bloque toute demande ayant un autre type de contenu désigné.

> **Remarque**
>
> Vous ne pouvez pas inclure les types de contenu « application/x-www-form-urlencoded » ou « multipart/form-data » dans la liste des types de contenu de réponse autorisés.

Pour définir le type de contenu de la requête par défaut à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw profile <name> -requestContentType <type>`
- `save ns config`

Exemple

L'exemple suivant définit le type de contenu "text/html" comme valeur par défaut pour le profil spécifié :

```
1 set appfw profile profile1 -requestContentType "text/html"
2 save ns config
3 <!--NeedCopy-->
```

Pour supprimer le type de contenu de requête par défaut défini par l'utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `unset appfw profile <name> -requestContentType <type>`
- `save ns config`

Exemple

L'exemple suivant désactive le type de contenu par défaut "text/html" pour le profil spécifié, ce qui permet au type de revenir à "application/octet-stream" :

```
unset appfw profile profile1 -requestContentType "text/html"
save ns config
<!--NeedCopy-->
```

> **Remarque**
>
> Utilisez toujours le dernier en-tête de type de contenu pour le traitement et supprimez les en-têtes de type de contenu restants, le cas échéant, ce qui garantit que le serveur principal reçoit une requête avec un seul type de contenu.
>
> Pour bloquer les requêtes qui peuvent être contournées, ajoutez une stratégie de Web App Firewall avec la règle HTTP.REQ.HEADER ("content-type").COUNT.GT(1)' et le profil comme *appfw_block*.
>
> Si une demande est reçue sans en-tête Content-Type ou si la demande possède un en-tête Content-Type sans valeur, le Web App Firewall applique la valeur **RequestContentType** configurée et traite la demande en conséquence.

Pour définir le type de contenu de réponse par défaut à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw profile <name> -responseContentType <type>`
- `save ns config`

Exemple

L'exemple suivant définit le type de contenu "text/html" comme valeur par défaut pour le profil spécifié :

```
set appfw profile profile1 -responseContentType "text/html"
save ns config
<!--NeedCopy-->
```

Pour supprimer le type de contenu de réponse par défaut défini par l'utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `unset appfw profile <name> -responseContentType <type>`
- `save ns config`

Exemple

L'exemple suivant désactive le type de contenu par défaut "text/html" pour le profil spécifié, ce qui permet au type de revenir à "application/octet-stream" :

```
unset appfw profile profile1 -responseContentType "text/html"
save ns config
<!--NeedCopy-->
```

Pour ajouter un type de contenu à la liste des types de contenu autorisés à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `bind appfw profile <name> -ContentType <contentTypeName>`
- `save ns config`

Exemple

L'exemple suivant ajoute le type de contenu « text/shtml » à la liste des types de contenu autorisés pour le profil spécifié :

```
bind appfw profile profile1 -contentType "text/shtml"
save ns config
<!--NeedCopy-->
```

Pour supprimer un type de contenu de la liste des types de contenu autorisés à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `unbind appfw profile <name> -ContentType <contentTypeName>`
- `save ns config`

Exemple

L'exemple suivant supprime le type de contenu « text/shtml » de la liste des types de contenu autorisés pour le profil spécifié :


```
unbind appfw profile profile1 -contentType "text/shtml"
save ns config
<!--NeedCopy-->
```

Gérer les types de contenu urlencoded et multipart-form

Le pare-feu Citrix ADC Web App vous permet désormais de configurer les types de contenu Urlencoded et Multipart-Form pour les formulaires. La configuration du type de contenu est similaire à la liste XML et JSON. En fonction de la configuration, le Web App Firewall classe les demandes et vérifie le type de contenu urlencoded ou multipart-form.

Pour configurer le profil de Web App Firewall avec les types de contenu urlencoded et multipart-form À l'invite de commandes, tapez :

```
bind appfw profile p2 -contentType <string>
```

Exemple :

```
bind appfw profile p2 -contentType UrlencodedFormContentType

bind appfw profile p2 -ContentType appfwmultipartform
```

Pour gérer les types de contenu par défaut et autorisés à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Web App Firewall** > **Profils**.
2. Dans le volet d'informations, sélectionnez le profil à configurer, puis cliquez sur **Modifier**. La boîte de dialogue **Configurer le profil du Web App Firewall** s'affiche.
3. La boîte de dialogue **Configurer le profil du Web App Firewall**, cliquez sur l'onglet **Paramètres**.
4. Sous l'onglet **Paramètres**, faites défiler vers le bas à mi-chemin jusqu'à la zone Type de contenu.
5. Dans la zone Type de contenu, configurez le type de contenu de la demande ou de la réponse par défaut :
   - Pour configurer le type de contenu de la demande par défaut, tapez la définition MIME/-type du type de contenu que vous souhaitez utiliser dans la zone de texte Demande par défaut.
   - Pour configurer le type de contenu de réponse par défaut, tapez la définition MIME/type du type de contenu à utiliser dans la zone de texte Réponse par défaut.
   - Pour créer un nouveau type de contenu autorisé, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un type de contenu autorisé** s'affiche.
   - Pour modifier un type de contenu autorisé existant, sélectionnez ce type de contenu, puis cliquez sur **Ouvrir**. La boîte de dialogue **Modifier le type de contenu autorisé** s'affiche.

6. Pour gérer les types de contenu autorisés, cliquez sur Gérer les types de contenu autorisés.
7. Pour ajouter un nouveau type de contenu ou modifier un type de contenu existant, cliquez sur Ajouter ou Ouvrir et, dans la boîte de dialogue **Ajouter un type** de **contenu autorisé ou Modifier un type** de contenu autorisé, procédez comme suit.
   a) Active/désactivez la case à cocher Activé pour inclure le type de contenu dans la liste des types de contenu autorisés ou l'exclure de celle-ci.
   b) Dans la zone de texte Type de contenu, tapez une expression régulière qui décrit le type de contenu à ajouter ou modifiez l'expression régulière de type de contenu existante.
   Les types de contenu sont formatés exactement comme les descriptions de type MIME.

      Remarque :
      Vous pouvez inclure n'importe quel type MIME valide dans la liste des types de contenu autorisés. Étant donné que de nombreux types de document peuvent contenir du contenu actif et donc potentiellement contenir du contenu malveillant, vous devez faire preuve de prudence lorsque vous ajoutez des types MIME à cette liste.

   c) Fournissez une brève description expliquant la raison pour laquelle ce type MIME particulier a été ajouté à la liste des types de contenu autorisés.
   d) Cliquez sur **Créer** ou sur **OK** pour enregistrer vos modifications.
8. Cliquez sur **Fermer** pour fermer la boîte de dialogue Gérer les types de contenu autorisés et revenir à l'onglet **Paramètres**.
9. Cliquez sur **OK** pour enregistrer vos modifications.

Pour gérer les types de contenu Urlencoded ou Multipart-form à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité** > **Web App Firewall** > **Profils**.
2. Dans le volet d'informations, sélectionnez le profil à configurer, puis cliquez sur **Modifier**.
3. Dans la page **Configurer le profil du Web App Firewall**, sélectionnez les **paramètres du profil** dans la section **Paramètres avancés**.
4. Sous la section **Type de contenu inspecté**, définissez les paramètres suivants :
   a) application/x-www-form-urlencoded. Cochez la case pour inspecter le type de contenu Urlencoded.
   b) multipart/form-data. Sélectionnez la coche pour inspecter le type de contenu Multipart-form.
5. Cliquez sur **OK**.



Profils

August 20, 2021

Un profil est un ensemble de paramètres de sécurité qui sont utilisés pour protéger des types spécifiques de contenu Web ou des parties spécifiques de votre site Web. Dans un profil, vous déterminez comment le Web App Firewall applique chacun de ses filtres (ou vérifications) aux demandes adressées à vos sites Web, ainsi que les réponses de ceux-ci. Le Web App Firewall prend en charge deux types de profils : quatre profils intégrés (par défaut) qui ne nécessitent pas de configuration supplémentaire, et les profils définis par l'utilisateur qui nécessitent une configuration supplémentaire.

Profilés intégrés

Les quatre profils intégrés du Web App Firewall offrent une protection simple pour les applications et sites Web qui ne nécessitent pas de protection ou qui ne doivent pas être directement accessibles par les utilisateurs. Ces types de profils sont les suivants :

- **APPFW_BYPASS.** Ignore tout le filtrage du Web App Firewall et envoie le trafic non modifié à

l'application ou au site Web protégé, ou au client.
- **APPFW_RESET.** Réinitialise la connexion, exigeant que le client rétablisse sa session en visitant une page de démarrage désignée.
- **APPFW_DROP.** Supprime tout trafic vers ou depuis l'application ou le site Web protégé, et n'envoie aucune réponse d'aucune sorte au client.
- **APPFW_BLOCK.** Bloque le trafic vers ou en provenance de l'application ou du site Web protégé.

Vous utilisez les profils intégrés exactement comme vous le faites, en configurant une stratégie qui sélectionne le trafic auquel vous souhaitez appliquer le profil, puis en associant le profil à votre stratégie. Comme vous n'avez pas besoin de configurer une stratégie intégrée, elle fournit un moyen rapide d'autoriser ou de bloquer certains types de trafic ou de trafic qui sont envoyés à des applications ou à des sites Web spécifiques.

Profils définis par l'utilisateur

Les profils définis par l'utilisateur sont des profils créés et configurés par les utilisateurs. Contrairement aux profils par défaut, vous devez configurer un profil défini par l'utilisateur avant qu'il ne puisse être utilisé pour filtrer le trafic à destination et en provenance de vos applications protégées.

Il existe trois types de profils définis par l'utilisateur :

- **HTML.** Protège les pages Web HTML.
- **XML.** Protège les services Web basés sur XML et les sites Web.
- **Web 2.0.** Protège le contenu Web 2.0 qui combine des contenus HTML et XML, tels que les flux ATOM, les blogs et les flux RSS.

Le Web App Firewall comporte un certain nombre de contrôles de sécurité, qui peuvent tous être activés ou désactivés, et configurés de différentes manières dans chaque profil. Chaque profil possède également un certain nombre de paramètres qui contrôlent la façon dont il gère différents types de contenu. Enfin, plutôt que de configurer manuellement tous les contrôles de sécurité, vous pouvez activer et configurer la fonctionnalité d'apprentissage. Cette fonctionnalité observe le trafic normal vers vos sites Web protégés pendant un certain temps et utilise ces observations pour vous fournir une liste personnalisée des exceptions recommandées (*assouplissements*) à certains contrôles de sécurité, ainsi que des règles supplémentaires pour d'autres contrôles de sécurité.

Lors de la configuration initiale, que ce soit à l'aide de l'Assistant Web App Firewall ou manuellement, vous créez normalement un profil à usage général pour protéger tout le contenu de vos sites Web qui n'est pas couvert par un profil plus spécifique. Après cela, vous pouvez créer autant de profils spécifiques que vous le souhaitez pour protéger un contenu plus spécialisé.

Le volet Profils est constitué d'un tableau qui contient les éléments suivants :

Nom. Affiche tous les profils de Web App Firewall configurés dans l'appliance.

Signature liée. Affiche l'objet signatures lié au profil dans la colonne précédente, le cas échéant.

Stratégies. Affiche la stratégie de Web App Firewall qui appelle le profil dans la colonne la plus à gauche de cette ligne, le cas échéant.

Commentaires. Affiche le commentaire associé au profil dans la colonne la plus à gauche de cette ligne, le cas échéant.

Type de profil. Affiche le type de profil. Les types sont intégrés, HTML, XML et Web 2.0.

Au-dessus du tableau se trouve une rangée de boutons et une liste déroulante qui vous permettent de créer, configurer, supprimer et afficher des informations sur vos profils :

- **Add.** Ajoutez un nouveau profil à la liste.
- **Modifier.** Modifiez le profil sélectionné.
- **Supprimer.** Supprimez le profil sélectionné de la liste.
- **Statistiques.** Affichez les statistiques du profil sélectionné.
- **Action.** Liste déroulante contenant des commandes supplémentaires. Vous permet actuellement d'importer un profil qui a été exporté à partir d'une autre configuration de Web App Firewall.

Création de profils de Web App Firewall

October 5, 2021

Vous pouvez créer un profil de Web App Firewall de deux manières : à l'aide de la ligne de commande et à l'aide de l'interface graphique. Pour créer un profil à l'aide de la ligne de commande, vous devez spécifier des options sur la ligne de commande. Le processus est similaire à celui de la configuration d'un profilet, à quelques exceptions près, les deux commandes prennent les mêmes paramètres.

Pour créer un profil à l'aide de l'interface graphique, vous devez spécifier seulement deux options. Vous spécifiez *les paramètres par défaut*de base ou avancés, la configuration par défaut des différents contrôles de sécurité et paramètres qui font partie d'un profil, puis choisissez le *type* de profil correspondant au type de contenu que le profil est destiné à protéger. Vous pouvez également ajouter un commentaire. Après avoir créé le profil, vous devez le configurer en le sélectionnant dans le volet de données, puis en cliquant sur **Modifier**.

Si vous envisagez d'utiliser la fonctionnalité d'apprentissage ou d'activer et de configurer de nombreuses protections avancées, vous devez choisir les paramètres par défaut avancés. En particulier, si vous envisagez de configurer l'une ou l'autre des vérifications d'injection SQL, soit les vérifications de script intersite, toute vérification offrant une protection contre les attaques de formulaires Web ou la vérification de cohérence des cookie, vous devez prévoir d'utiliser la fonctionnalité d'apprentissage. À moins que vous n'incluiez les exceptions appropriées pour vos sites Web protégés lors de la configuration de ces vérifications, ils peuvent bloquer le trafic légitime. Il est difficile d'anticiper toutes les exceptions sans en créer de trop larges. La fonction d'apprentissage facilite grandement cette tâche.

Sinon, les valeurs par défaut de base sont rapides et doivent fournir la protection dont vos applications Web ont besoin.

Il existe trois types de profils :

- **HTML.** Protège les sites Web HTML standard.
- **XML.** Protège les services Web et les sites Web XML.
- **Web 2.0 (HTML XML).** Protège les sites Web qui contiennent des éléments HTML et XML, tels que des flux ATOM, des blogs et des flux RSS.

Il existe également quelques restrictions sur le nom que vous pouvez attribuer à un profil. Un nom de profil ne peut pas être identique au nom attribué à un autre profil ou action dans une fonctionnalité du dispositif NetScaler. Certains noms d'actions ou de profils sont attribués à des actions ou profils intégrés et ne peuvent jamais être utilisés pour des profils utilisateur. Vous trouverez une liste complète des noms non autorisés dans les informations supplémentairesdu profil du pare-feu Web App Firewall. Si vous tentez de créer un profil avec un nom qui a déjà été utilisé pour une action ou un profil, un message d'erreur s'affiche et le profil n'est pas créé.

Pour créer un profil de Web App Firewall à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw profile <name> [-defaults ( **basic** | **advanced** )]`
- `set appfw profile <name> -type ( **HTML** | **XML** | **HTML XML** )`
- `set appfw profile <name> -comment "<comment>"`
- `save ns config`

Exemple

L'exemple suivant ajoute un profil nommé pr-basic, avec des valeurs par défaut de base, et affecte un type de profil HTML. Il s'agit de la configuration initiale appropriée pour un profil afin de protéger un site Web HTML.

```
1 add appfw profile pr-basic -defaults basic -comment "Simple profile for
      websites."
2 set appfw profile pr-basic -type HTML
3 save ns config
4 <!--NeedCopy-->
```

Pour créer un profil de Web App Firewall à l'aide de l'interface graphique

Suivez la procédure suivante pour créer un profil de Web App Firewall :

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.

2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer un profil de Web App Firewall**, définissez les paramètres de base suivants :
   a) Nom
   b) Type de profil
   c) Commentaires
   d) Valeurs par défaut
   e) Description
4. Cliquez sur **OK**.
5. Dans la section **Paramètres avancés**, effectuez les configurations suivantes :
   a) Contrôles de sécurité
   b) Paramètres du profil
   c) Profilage dynamique
   d) Règles de relaxation
   e) Règles de refus
   f) Règle apprise
   g) Journalisation étendue



6. Dans la section **Vérifications de sécurité**, sélectionnez une protection de sécurité et cliquez sur Paramètres **d'action*.
7. Dans la page de vérification de sécurité, définissez les paramètres.

> **Remarque :**
>
> Le paramètre **Règle active** est disponible uniquement pour la vérification **d'injection SQL HTML** afin d'activer la règle de relaxation ou la règle de refus pour la vérification d'injection SQL. Pour plus d'informations, consultez la rubrique Règles de relaxation et de refus .

8. Cliquez sur **OK** et sur **Fermer**.
9. Dans la section **Paramètres du profil**, définissez les paramètres du profil. Pour plus d'informations, consultez la rubrique Configurer les paramètres du profil de Web App Firewall .

10. Dans la section **Profilage dynamique**, sélectionnez une vérification de sécurité pour ajouter des paramètres de profil dynamique. Pour plus d'informations, consultez la rubrique Profil dynamique .
11. Dans la section **Règles de relaxation**, cliquez sur **Modifier** pour ajouter une règle de relaxation pour un contrôle de sécurité. Pour plus d'informations, consultez la section Règle de relaxation pour plus de détails.
12. Dans la section **Règles de refus**, ajoutez une règle de refus pour la vérification HTML SQL Injection. Pour plus d'informations, consultez la rubrique Règles de refus HTML .
13. Dans la section **Règle apprise**, définissez les paramètres d'apprentissage. Pour plus d'informations, consultez la rubrique d' apprentissage sur le Web App Firewall .
14. Dans la section **Journalisation étendue**, cliquez sur **Ajouter** pour masquer les données sensibles. Pour plus d'informations, consultez la rubrique de journalisation étendue .
15. Cliquez sur **Terminé**, puis cliquez sur **Fermer**.



Appliquer la conformité HTTP RFC

September 8, 2021

Citrix Web App Firewall inspecte le trafic entrant pour vérifier la conformité HTTP RFC et supprime

toute demande qui comporte des violations RFC par défaut. Toutefois, il existe certains scénarios dans lesquels l'appliance peut devoir contourner ou bloquer une demande de conformité non RFC. Dans ce cas, vous pouvez configurer la solution matérielle-logicielle pour contourner ou bloquer ces demandes au niveau global ou au niveau du profil.

Bloquer ou contourner les demandes non conformes à la RFC au niveau mondial

Le module HTTP marque une requête comme non valide si elle est incomplète ou invalide et que ces requêtes ne peuvent pas être traitées par WAF. Par exemple, une requête HTTP entrante dont l'en-tête d'hôte est manquant. Pour bloquer ou contourner ces demandes non valides, vous devez configurer l' `malformedReqAction` option dans les paramètres globaux du pare-feu de l'application.

> **Remarque :**
>
> Si vous désactivez l'option de blocage dans le `malformedReqAction` paramètre, l'appliance contourne l'ensemble du traitement du pare-feu de l'application pour toutes les demandes de conformité non RFC et transmet les demandes au module suivant.

Pour bloquer ou contourner les demandes HTTP non RFC non valides à l'aide de l'interface de ligne de commande

Pour bloquer ou contourner les demandes non valides, entrez la commande suivante :

```
set appfw settings -malformedreqaction <action>
```

Exemple :

```
set appfw settings -malformedReqAction block
```

Pour afficher les paramètres d'action de demande mal formés

Pour afficher les paramètres d'action de demande mal formés, entrez la commande suivante :

```
show appfw settings
```

Sortie :

```
1 DefaultProfile: APPFW_BYPASS UndefAction: APPFW_BLOCK SessionTimeout:
      900    LearnRateLimit: 400    SessionLifetime: 0
    SessionCookieName: citrix_ns_id ImportSizeLimit: 134217728
    SignatureAutoUpdate: OFF SignatureUrl:"https://s3.amazonaws.com/
    NSAppFwSignatures/SignaturesMapping.xml" CookiePostEncryptPrefix:
    ENC GeoLocationLogging: OFF CEFLogging: OFF      EntityDecoding:
     OFF    UseConfigurableSecretKey: OFF SessionLimit: 100000
    MalformedReqAction: block log stats
2  Done
```



```
3 <!--NeedCopy-->
```

Pour bloquer ou contourner les demandes HTTP non RFC non valides à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité** > **Citrix Web App Firewall**.
2. Dans la page **Citrix Web App Firewall**, cliquez sur **Modifier les paramètres du moteur** sous **Paramètres**.
3. Dans la page **Configurer les paramètres du Citrix Web App Firewall**, sélectionnez l'option **Log mal formed Request** en tant que Bloc, Log ou Stats.
4. Cliquez sur **OK** et sur **Fermer**.

> **Remarque :**
>
> Si vous désélectionnez l'action de blocage ou si vous ne sélectionnez aucune action de demande mal formée, l'appliance contourne la demande sans en insinuer l'utilisateur.

Bloquer ou contourner les demandes non conformes RFC au niveau du profil

D'autres demandes non conformes RFC peuvent être configurées pour bloquer ou contourner au niveau du profil. Vous devez configurer le profil RFC en mode Block ou Bypass. Ce faisant, tout trafic non valide qui correspond au profil de Web App Firewall est ignoré ou bloqué en conséquence.

> **Remarque :**
>
> Lorsque vous définissez le profil RFC en mode « Contournement », vous devez vous assurer de désactiver l'option de transformation dans les **paramètres de script intersite HTML** et dans les sections **Paramètres d'injection HTML SQL** . Si vous activez l'option et que vous définissez le profil rfc en mode Bypass, l'appliance affiche un message d'avertissement : « Transformer les scripts intersites » et « Transformer les caractères spéciaux SQL » sont tous deux activés. Il est recommandé de l'éteindre lorsqu'il est utilisé avec `APPFW_RFC_BYPASS`.
>
> **Important :**
>
> De plus, l'appliance affiche une note d'avertissement : « Les contrôles de sécurité Appfw activés peuvent ne pas être applicables aux demandes qui enfreignent les vérifications RFC lorsque ce profil est défini. L'activation d'un paramètre de transformation n'est pas recommandée car les demandes peuvent être partiellement transformées qui contiennent des violations RFC. «

Pour configurer un profil RFC dans le profil Web App Firewall à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :


```
set appfw profile <profile_name> -rfcprofile <rfcprofile_name
```

Exemple

```
set appfw profile P1 -rfcprofile APPFW_RFC_BLOCK
```

> **Remarque :**
>
> Par défaut, le profil rfc est lié au profil Web App Firewall en mode Bloc.

Pour configurer un profil RFC dans le profil Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Dans la page **Profil du Web App Firewall**, cliquez sur **Paramètres de profil dans** la section **Paramètres avancés** .
4. Dans la section **Paramètres HTML**, définissez le profil RFC en mode APPFW_RFC_BYPASS.
   Le système affiche un message d'avertissement : « Les vérifications de sécurité Appfw activées peuvent ne pas s'appliquer aux demandes qui violent les vérifications RFC lorsque ce profil est défini. L'activation d'un paramètre de transformation n'est pas recommandée car les requêtes peuvent être partiellement transformées qui contiennent des violations RFC ».

Configuration des profils de Web App Firewall

August 20, 2021

Pour configurer un profil de Web App Firewall défini par l'utilisateur, configurez d'abord les vérifications de sécurité, appelées *protections profondes* ou *protections avancées* dans l'assistant Pare-feu Web App. Certaines vérifications nécessitent une configuration si vous voulez les utiliser du tout. D'autres ont des configurations par défaut sûres mais limitées dans leur portée ; vos sites Web peuvent avoir besoin ou bénéficier d'une configuration différente qui tire parti de plus de fonctionnalités de certains contrôles de sécurité.

Après avoir configuré les vérifications de sécurité, vous pouvez également configurer d'autres paramètres qui contrôlent le comportement, pas d'une seule vérification de sécurité, mais de la fonctionnalité Web App Firewall. La configuration par défaut est suffisante pour protéger la plupart des sites Web, mais vous devez les consulter pour vous assurer qu'ils conviennent à vos sites Web protégés.

> **Remarque :**
>
> La longueur du nom du profil et toute la longueur du nom d'objet d'importation peuvent être définies à 127 caractères.

Pour plus d'informations sur les contrôles de sécurité Web App Firewall, voir Protections avancées.

Pour configurer un profil de Web App Firewall à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw profile <name> <arg1> [<arg2> ...]`

  où :

  - `<arg1>` = un paramètre et toutes les options associées.
  - `<arg2>` = un deuxième paramètre et toutes les options associées.
  - … = paramètres et options supplémentaires.

  Pour obtenir une description des paramètres à utiliser lors de la configuration de contrôles de sécurité spécifiques, voir Protections avancées.

- `save ns config`

Exemple

L'exemple suivant montre comment activer le blocage pour les vérifications HTML SQL Injection et HTML Cross-Site Scripting dans un profil nommé pr-basic. Cette commande permet de bloquer ces actions sans apporter d'autres modifications au profil.

```
1 set appfw profile pr-basic -crossSiteScriptingAction block -
     SQLInjectionAction block
2 <!--NeedCopy-->
```

Lier la règle de relaxation à un profil Web App Firewall

Lorsque Web App Firewall détecte une violation, l'utilisateur a la possibilité de contourner l'action appliquée via des règles de relaxation. La règle de relaxation est une exception appliquée à la violation de sécurité détectée. Par exemple, les règles de relaxation d'URL de démarrage protègent contre la navigation forcée. Les vulnérabilités connues des serveurs Web exploitées par les pirates peuvent être détectées et bloquées en activant un ensemble de règles d'URL de refus par défaut. Les attaques lancées couramment, telles que Buffer Overflow, SQL ou cross-site scripting peuvent également être facilement détectées.

Pour lier des règles d'exemption de sécurité ou de relaxation à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind appfw profile <name> ((-startURL <expression> [-resourceId  <
    string>]) | -denyURL <expression> | (-fieldConsistency <string>   <
    formActionURL> [-isRegex ( REGEX | NOTREGEX )]) | (-
    cookieConsistency <string> [-isRegex ( REGEX | NOTREGEX )]) | (-
    SQLInjection <string> <formActionURL> [-isRegex ( REGEX | NOTREGEX )
    ] [-location <location>] [-valueType <valueType> <valueExpression
    >....
<!--NeedCopy-->
```

Pour lier des règles d'exemption de sécurité ou de relaxation à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez un profil et cliquez sur **Modifier**.
3. Dans la page **Profil du Citrix Web App Firewall**, cliquez sur **Règles de relaxation** dans la section **Paramètres avancés**.
4. Dans la section **Règles de relaxation**, cliquez sur **StarTurl** et cliquez sur **Modifier**.
5. Dans la page **Démarrer les règles de relaxation d'URL**, cliquez sur **Ajouter**.
6. Dans la page **Démarrer la règle de relaxation d'URL**, définissez les paramètres suivants :
   a) Activé. Cochez la case pour activer la règle de relaxation
   b) URL de démarrage. Entrez la valeur de l'expression régulière
   c) Commentaires. Fournissez une brève description de la règle de relaxation.
7. Cliquez sur **Créer** et **Fermer**.



Pour configurer un profil de Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez le profil à configurer, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Configurer le profil du Web App Firewall**, sous l'onglet **Vérifications de sécurité**, configurez les vérifications de sécurité.
   - Pour activer ou désactiver une action pour une vérification, dans la liste, activez ou désactivez la case à cocher correspondant à cette action.
   - Pour configurer d'autres paramètres pour les vérifications qui en ont, dans la liste, cliquez sur le chevron bleu à l'extrême droite de cette vérification. Dans la boîte de dialogue qui s'affiche, configurez les paramètres. Ceux-ci varient d'une vérification à l'autre.

     Vous pouvez également sélectionner une coche et, en bas de la boîte de dialogue, cliquez sur Ouvrir pour afficher la boîte de dialogue **Configurer la relaxation** ou **Configurer la règle** pour cette vérification. Ces boîtes de dialogue varient également d'une vérification à l'autre. La plupart d'entre eux comprennent un onglet **Vérifications** et un onglet **Général**. Si la vérification prend en charge les relaxations ou les règles définies par l'utilisateur,

l'onglet **Vérifications** inclut un bouton **Ajouter**, qui ouvre une nouvelle boîte de dialogue, dans laquelle vous pouvez spécifier une relaxation ou une règle pour la vérification. (Un assouplissement est une règle permettant d'exempter le trafic spécifié du contrôle.) Si les relaxations ont déjà été configurées, vous pouvez en sélectionner une et cliquer sur **Ouvrir** pour la modifier.

- Pour consulter les exceptions ou les règles apprises pour une vérification, sélectionnez la vérification, puis cliquez sur **Violations apprises**. Dans la boîte de dialogue **Gérer les règles apprises**, sélectionnez successivement chaque exception ou règle apprise.
  - Pour modifier l'exception ou la règle, puis l'ajouter à la liste, cliquez sur **Modifier et déployer**.
  - Pour accepter l'exception ou la règle sans modification, cliquez sur **Déployer**.
  - Pour supprimer l'exception ou la règle de la liste, cliquez sur **Ignorer**.
- Pour actualiser la liste des exceptions ou des règles à réviser, cliquez sur **Actualiser**.
- ouvrez le visualiseur d'apprentissage et utilisez-le pour consulter les règles apprises, cliquez sur **Visualizer**.
- examinez les entrées du journal pour les connexions correspondant à une vérification, sélectionnez la vérification, puis cliquez sur Journaux. Vous pouvez utiliser ces informations pour déterminer quelles vérifications correspondent aux attaques, de sorte que vous pouvez activer le blocage de ces vérifications. Vous pouvez également utiliser ces informations pour déterminer quelles vérifications correspondent au trafic légitime, de sorte que vous pouvez configurer une exemption appropriée pour autoriser ces connexions légitimes. Pour plus d'informations sur les journaux, consultez Journaux, statistiques et rapports.
- Pour désactiver complètement une coche, dans la liste, désactivez toutes les cases à droite de cette coche.

4. Sous l'onglet **Paramètres**, configurez les paramètres du profil.
   - Pour associer le profil à l'ensemble de signatures que vous avez précédemment créé et configuré, sous Paramètres communs, choisissez cet ensemble de signatures dans la liste déroulante **Signatures** .

     > **Remarque :**
     >
     > Vous pouvez utiliser la barre de défilement située à droite de la boîte de dialogue pour afficher la section Paramètres communs.

   - Pour configurer un objet Erreur HTML ou XML, sélectionnez l'objet dans la liste déroulante appropriée.

> **Remarque :**
>
> Vous devez d'abord charger l'objet d'erreur que vous souhaitez utiliser dans le volet Importations. Pour plus d'informations sur l'importation d'objets d'erreur, voir Importations.

- Pour configurer le type de contenu XML par défaut, tapez la chaîne de type de contenu directement dans les zones de texte Demande par défaut et réponse par défaut, ou cliquez sur Gérer les types de contenu autorisés pour gérer la liste des types de contenu autorisés. »Plus…

5. Si vous souhaitez utiliser la fonctionnalité d'apprentissage, cliquez sur Apprentissage et configurez les paramètres d'apprentissage du profil, comme décrit dans Configuration et utilisation de la fonctionnalité d'apprentissage.
6. Cliquez sur **OK** pour enregistrer vos modifications et revenir au volet **Profils** .

Paramètres du profil du pare-feu d'application Web

October 5, 2021

Voici les paramètres de profil que vous devez configurer sur la solution matérielle-logicielle.

À l'invite de commandes, tapez :

```
add appfw profile <name> [-invalidPercentHandling <invalidPercentHandling
>] [-checkRequestHeaders ( ON | OFF )] [-URLDecodeRequestCookies ( ON |
 OFF )] [-optimizePartialReqs ( ON | OFF )] [-errorURL <expression>] [-
logEveryPolicyHit ( ON | OFF )] [-stripHtmlComments <stripHtmlComments>] [-
stripXmlComments ( none | all )] [-postBodyLimitSignature <positive_integer
>][-fileUploadMaxNum <positive_integer>][-canonicalizeHTMLResponse ( ON
| OFF )][-percentDecodeRecursively ( ON | OFF )] [-multipleHeaderAction
<multipleHeaderAction> ...][-inspectContentTypes <inspectContentTypes>
...][-semicolonFieldSeparator ( ON | OFF )]
```

Exemple :

```
add appfw profile profile1 [-invalidPercentHandling secure_mode] [-checkRequestHeaders
 ON] [-URLDecodeRequestCookies OFF] [-optimizePartialReqs OFF]
```

Où,

Le pourcentage de Handling n'est pas valide. Configurez la méthode de traitement des noms et des valeurs codés en pourcentage.

Les paramètres disponibles fonctionnent comme suit :

asp_mode - Enlève et analyse le pourcentage non valide pour l'analyse. Exemple curl -v "http://<vip>/forms/login.html?field=sel%zzect -> Invalid percent encoded char(%zz) est enlevé, le reste du contenu est inspecté et une action est entreprise pour la vérification SQLInjection.
secure_mode - Nous détectons la valeur codée Invalid Percent (Pourcentage non valide) et nous l'ignorons. Exemple curl -v "http://<vip>/forms/login.html?field=sel%zzect -> Invalid percent encoded char(%zz) est détecté, les compteurs sont incrémentés et le contenu est transmis tel qu'il est au serveur.
apache_mode - Ce mode fonctionne de la même manière que le mode sécurisé.
Valeurs possibles : apache_mode, asp_mode, secure_mode Valeur
par défaut : secure_mode

Optimisez les demandes partielles. Lorsque la fonction est DÉSACTIVÉ/ACTIVÉE (sans objet sécurisé), une appliance Citrix ADC envoie la demande partielle au serveur principal. Cette réponse partielle a été renvoyée au client. OptimizePartialReqs est logique lorsque l'objet Safe est configuré. La solution matérielle-logicielle envoie des demandes de réponse complète du serveur lorsqu'elle est désactivée, et ne demande qu'une réponse partielle lorsqu'elle est activée.

Les paramètres disponibles sont les suivants :

ON - Les demandes partielles du client entraînent des demandes partielles adressées au serveur principal.
OFF - Les demandes partielles du client sont remplacées par des demandes complètes adressées au serveur principal Valeurs
possibles : ON, OFF Valeur
par défaut : ON

Cookies de demande de décodage d'URL. URL Decode demande des cookies avant de les soumettre à des vérifications SQL et de script intersite.

Valeurs possibles : ON, OFF Valeur
par défaut : OFF

Limite du corps de la publication de signature (octets). Limite la charge utile de la requête (en octets) inspectée à la recherche de signatures avec l'emplacement spécifié comme « HTTP_POST_BODY ».

Valeur par défaut : 8096 Valeur
minimale : 0 Valeur
maximale : 4294967295

Limite de corps de publication (octets). Limite la charge utile de la demande (en octets) inspectée par le pare-feu d'application Web.

Valeur par défaut : 20000000 Valeur

minimale : 0 Valeur
maximale : 10 Go

Pour plus d'informations sur le paramètre de sécurité et sa procédure GUI, consultez la rubrique Configurer le profil du Web App Firewall .

PostBodyLimitAction. PostBodyLimit respecte les paramètres d'erreur lorsque vous spécifiez la taille maximale du corps HTTP à autoriser. Pour respecter les paramètres d'erreur, vous devez configurer une ou plusieurs actions Limite du corps de publication. La configuration s'applique également aux demandes pour lesquelles l'en-tête de codage de transfert est segmenté.

```
set appfw profile <profile_name> -PostBodyLimitAction block log stats
```

Où,
Bloquer - Cette action bloque la connexion qui viole le contrôle de sécurité et elle est basée sur la taille maximale du corps HTTP configuré (limite de corps post-). Vous devez toujours activer cette option.

Journal - Consigner les violations de cette vérification de sécurité.

Stats - Générez des statistiques pour cette vérification de sécurité.

> **Remarque :**
>
> Le format du journal pour l'action de limitation du corps de publication est désormais modifié pour suivre le format de journalisation d'audit
> standard, par exemple :
> `ns.log.4.gz:Jun 25 1.1.1.1. <local0.info> 10.101.10.100 06/25/2020:10:10:28 GMT 0-PPE-0 : default APPFW APPFW_POSTBODYLIMIT 1506 0 : <Netscaler IP> 4234-PPE0 - testprof ><URL> Request post body length(<Post Body Length >)exceeds post body limit.`

InspectQueryContentTypes Inspectez les requêtes de demande et les formulaires Web pour les scripts SQL injectés et intersite pour les types de contenu suivants.

```
set appfw profile p1 -inspectQueryContentTypes HTML XML JSON OTHER
```

Valeurs possibles : HTML, XML, JSON, OTHER

Par défaut, ce paramètre est défini sur « InspectQueryContentTypes : HTML JSON OTHER » pour les profils appfw de base et avancés.

Exemple pour inspecter le type de contenu de la requête en tant que XML :

```
1 > set appfw profile p1 -type XML
2 Warning: HTML, JSON checks except "InspectQueryContentTypes" & "
     Infer Content-Type XML Payload Action" will not be applicable when
     profile type is not HTML or JSON respectively.
3 <!--NeedCopy-->
```


Exemple pour inspecter le type de contenu de la requête en HTML :

```
1 > set appfw profile p1 -type HTML
2 Warning: XML, JSON checks except "InspectQueryContentTypes" & "Infer
      Content-Type XML Payload Action" will not be applicable when
     profile type is not XML or JSON respectively
3 Done
4 <!--NeedCopy-->
```

Exemple pour inspecter le type de contenu de requête au format JSON :

```
1 > set appfw profile p1 -type JSON
2 Warning: HTML, XML checks except "InspectQueryContentTypes" & "Infer
      Content-Type XML Payload Action will not be applicable when profile
      type is not HTML or XML respectively
3 Done
4 <!--NeedCopy-->
```

Expression ErrorUrl. URL utilisée par le Citrix Web App Firewall comme URL d'erreur. Longueur maximale : 2047.

> **Remarque :**
>
> Pour bloquer les violations dans une URL demandée, si l'URL d'erreur est similaire à l'URL de signature, la solution matérielle-logicielle réinitialise la connexion.

LogeVeryPolicyHit - Consignez chaque correspondance de profil, quels que soient les résultats des contrôles de sécurité.
Valeurs possibles : ON, OFF.
Valeur par défaut : OFF.

StripXMLComments - Supprimez les commentaires XML avant de transférer une page Web envoyée par un site Web protégé en réponse à une demande d'un utilisateur.
Valeurs possibles : none, all, exclude_script_tag.
Valeur par défaut : aucune

PostBodyLimitSignature - Taille maximale autorisée du corps de publication HTTP pour l'inspection des signatures pour l'emplacement HTTP_POST_BODY dans les signatures, en octets.
Les changements de valeur peuvent avoir un impact sur le processeur et le profil de latence.
Valeur par défaut : 2048.
Valeur minimale : 0 Valeur
maximale : 4294967295

FileUploadMaxNum : nombre maximal autorisé de téléchargements de fichiers par demande de soumission de formulaire. Le paramètre maximum (65535) permet un nombre illimité de téléchargements.

Valeur par défaut : 65535 Valeur
minimale : 0 Valeur
maximale : 65535

CanonicAlizeHTMLResponse - Effectuez le codage des entités HTML pour tous les caractères spéciaux des réponses envoyées par vos sites Web protégés.
Valeurs possibles : ON, OFF Valeur
par défaut : ON

PercentDecodeRecursivement - Configurez si le pare-feu d'application doit utiliser le décodage récursif en pourcentage.
Valeurs possibles : ON, OFF Valeur
par défaut : ON

MultipleHeaderAction - Une ou plusieurs actions d'en-tête multiples. Les paramètres disponibles fonctionnent comme suit :

- Bloc. Bloquez les connexions comportant plusieurs en-têtes.
- Bûche. Consignez les connexions qui ont plusieurs en-têtes.
- KeepLast. Ne conservez que le dernier en-tête lorsque plusieurs en-têtes sont présents.

InspectContentTypes : une ou plusieurs listes InspectContentType.

- application/x-www-form-urlencoded
- données multipart/formulaire
- texte/x-gwt-rpc

Valeurs possibles : aucun, application/x-www-form-urlencoded, multipart/form-data, text/x-gwt-rpc

SemiColonFieldSeparator - Autorise « ; » comme séparateur de champ de formulaire dans les requêtes URL et les corps de formulaire POST.
Valeurs possibles : ON, OFF Valeur
par défaut : OFF

Modification d'un type de profil de Web App Firewall

August 20, 2021

Si vous avez choisi le type de profil incorrect pour un profil Web App Firewall ou si le type de contenu du site Web protégé a changé, vous pouvez modifier le type de profil.

> **Remarque** Lorsque vous modifiez le type de profil, vous perdez tous les paramètres de configuration et les relaxations ou règles apprises pour les fonctionnalités que le nouveau type de profil ne prend pas en charge. Par exemple, si vous modifiez le type de profil Web 2.0 en XML, vous perdez

> toutes les options de configuration pour l'URL de démarrage, la vérification de cohérence des champs de formulaire et les autres vérifications de sécurité spécifiques au HTML. La configuration des options prises en charge par l'ancien et le nouveau type de profil reste inchangée.

Pour modifier un type de profil de Web App Firewall à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw profile <name> -type ( **HTML** | **XML** | **HTML XML** )`
- `save ns config`

Exemple

L'exemple suivant montre comment modifier le type d'un profil nommé pr-basic, de HTML à HTML XML, ce qui équivaut au type Web 2.0 de l'interface graphique.

```
1 set appfw profile pr-basic -type HTML XML
2 save ns config
3 <!--NeedCopy-->
```

Pour modifier un type de profil de Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Web App Firewall > Stratégies**.
2. Dans le volet d'informations, cliquez sur **Action**, puis sur **Modifier le type de profil**.
3. Dans la boîte de dialogue **Modifier le type de profil de Web App Firewall**, liste déroulante **Type** de profil, sélectionnez un nouveau type de profil.
4. Cliquez sur **OK** pour enregistrer vos modifications et revenir au volet **Profils** .

Exportation et importation d'un profil de Web App Firewall

January 21, 2021

Vous pouvez répliquer toute la configuration d'un profil de Web App Firewall (y compris tous les objets liés, tels que l'objet d'erreur HTML, l'objet d'erreur XML, le schéma WSDL ou XML, les signatures, etc.) sur plusieurs appliances. Vous pouvez sélectionner un profil cible et exporter la configuration pour l'enregistrer dans le système de fichiers local de votre ordinateur, ou transférer la configuration archivée pour la stocker sur un serveur. De même, vous pouvez parcourir le système de fichiers local de votre ordinateur ou importer l'archive depuis le serveur pour sélectionner un profil précédemment exporté et l'importer dans votre appliance NetScaler.

L'option permettant d'exporter l'intégralité de la configuration du profil, puis de l'importer dans une autre appliance, peut s'avérer utile dans différents cas d'utilisation. Par exemple, vous pouvez configurer un profil de Web App Firewall dans une configuration de banc d'essai pour tester et valider qu'il fonctionne comme prévu. Une fois que vous êtes satisfait, vous pouvez exporter le profil et importer la configuration du profil vers vos appliances NetScaler de production. Cette fonctionnalité est également utile pour sauvegarder votre configuration. Vous pouvez exporter le profil avant d'apporter des modifications, de sorte que vous pouvez facilement restaurer la configuration à un état connu si nécessaire.

> **Remarque**
>
> Les profils de Web App Firewall exportés et archivés à partir d'une version ne peuvent pas être restaurés sur un système exécutant une version différente, car les modifications introduites dans les versions les plus récentes peuvent entraîner des problèmes de compatibilité. Si vous tentez de restaurer un profil archivé dans une version différente de celle à partir de laquelle il a été exporté, un message d'erreur est enregistré dans ns.log.

La fonctionnalité de profil d'exportation et d'importation est disponible dans l'interface graphique (GUI) et l'interface de ligne de commande (CLI). L'interface graphique est recommandée, car elle offre des options **d'action** faciles à utiliser. En cliquant sur un bouton, vous pouvez **exporter** ou **importer** toute la configuration d'un profil.

Exportation de profils de Web App Firewall avec l'interface de ligne de commande

Si vous utilisez l'interface de ligne de commande pour **exporter** un profil, vous devez **archiver** la configuration, puis **l'exporter**. Pour **importer** un profil, vous devez **importer** l'archive dans l'appliance NetScaler, puis exécuter la commande **restore** pour extraire la configuration. L'ensemble de commandes CLI suivant peut être utilisé pour exporter, importer et gérer les configurations de profils.

Commandes CLI pour exporter les archives :

- `archive appfw profile <name> <archivename> [-comment <string>]`
- `export appfw archive <name> <target>`

Commandes CLI pour importer des archives :

- **`import`** `appfw archive <src> <name> [-comment <string>]`
- `restore appfw profile <archivename>`

Commandes CLI pour gérer les archives :

- `show appfw archive`
- `rm appfw archive <name>`

L'exportation d'un profil à partir d'une appliance et l'importation vers une autre nécessite cinq étapes dans l'interface de ligne de commande. Les 3 premières étapes sont exécutées sur l'appliance source

sur laquelle la configuration de profil est initialement créée, et les 2 étapes suivantes sont exécutées sur l'appliance cible sur laquelle la configuration de profil doit être répliquée.

Exporter le profil à partir de l'appliance NetScaler source :

Étape 1 : Créer une archive du profil configuré.

Étape 2 : Exportez l'archive vers le système de fichiers NetScaler.

Étape 3 : Utilisez un utilitaire de transfert de fichiers tel que scp pour transférer le fichier d'archive exporté à partir de l'appliance NetScaler A vers l'appliance NetScaler cible.

Importer le profil vers l'appliance NetScaler cible :

Étape 4 : Exécutez la commande import pour importer le fichier archivé. Vous pouvez importer l'archive à partir du système de fichiers local de NetScaler ou utiliser le protocole HTTP ou HTTPS pour importer l'archive à partir d'un serveur à l'aide de l'URL.

Étape 5 : Exécutez la commande restore pour restaurer la configuration du profil à partir de l'archive importée

Pour exporter un profil de Web App Firewall à l'aide de l'interface de ligne de commande :

Tout d'abord, **archivez** la configuration du profil, puis **exportez** l'archive vers un emplacement cible. À l'invite de commandes, tapez les commandes suivantes :

```
archive appfw profile <profileName> <archiveName>
```

où :

- <profileName> est le nom du profil à archiver.
- <archiveName> est le nom du fichier d'archive à créer.

L'exécution de la commande ci-dessus crée 2 instances du fichier d'archive. Un dans le dossier /var/tmp et un autre dans le dossier /var/archive/appfw.

```
export appfw archive <archiveName> <target>
```

où :

- <archiveName> est le nom de l'archive à exporter. (Le même nom que dans la commande précédente.
- <target> est un chemin de fichier commençant par local : comme préfixe, suivi de <archiveName>.

L'exécution de la commande export enregistre le fichier d'archive exporté sur le système de fichiers de votre appliance NetScaler dans le dossier /var/tmp.

Exemples :

```
> archive appfw profile test_pr archived_test_pr
```

```
> export appfw archive archived_test_pr local:dutA_test_pr
```


Après l'exécution des deux commandes ci-dessus, le dossier /var/tmp contient le fichier archived_test_pr et la copie exportée, duta_test_pr, dont la taille est identique. À partir de l'interface de ligne de commande, vous pouvez passer dans le shell pour accéder au dossier afin de vérifier que ces fichiers sont présents.

Après avoir exporté le fichier d'archive, vous pouvez utiliser **scp** ou un autre utilitaire de transfert de fichiers de ce type pour transférer une copie du fichier d'archive de l'appliance NetScaler sur laquelle ils ont été créés vers votre appliance NetScaler cible.

Importation de profils de Web App Firewall à l'aide de l'interface de ligne de commande

Après avoir correctement scp le fichier archivé de l'appliance source vers l'appliance cible, vous êtes prêt à **importer** l'archive du profil, puis à exécuter la commande **restore** pour répliquer la configuration du profil sur l'appliance cible.

Connectez-vous à l'appliance cible. Passez dans le shell et le cd dans le dossier /var/tmp pour vérifier que la taille du fichier scp 'd de cette appliance correspond à la taille du fichier archivé d'origine sur l'appliance source. Quittez le shell pour revenir à la ligne de commande.

Pour importer un profil à l'aide de l'interface de lignede commande :

À l'invite de commandes, tapez les commandes suivantes :

```
import appfw archive <src> <name> [-comment <string>]
```

où

- <src> est l'emplacement du fichier d'archive après qu'il a été transféré à partir de l'appliance source sur laquelle il a été créé. Vous pouvez utiliser un système de fichiers local et un nom de fichier. Si vous avez placé l'archive sur un serveur, vous pouvez utiliser une URL pour importer le fichier archivé. Si le chemin d'accès ou le nom du fichier contient des espaces, placez l'URL entre guillemets droits.
- <name> est le nom du fichier d'archive à importer.
- <string> est une description facultative du but de l'archive.

```
restore appfw profile <archiveName>
```

Exemples :

A. Importer à partir d'un fichier local suivi de la restauration :

```
> import appfw archive local:dutA_test_pr dut2_test_pr
```

```
> restore appfw profile dut2_test_pr
```

B. Importer à partir de l'URL suivie de la restauration :


```
import appfw archive http://10.217.30.16/FFC/Profile_ImportExport/
dutA_test_pr.tgz my_archive
restore appfw profile my_archive
```

Cet exemple restaure le profil test_pr ainsi que tous les objets liés (tels que les signatures, la page d'erreur html, les règles de relaxation, etc.) sur l'appliance NetScaler cible.

Vous pouvez utiliser les commandes CLI suivantes pour accéder aux pages de manuel pour plus de détails.

- man archive appfw profil
- man export archive appfw
- man import archive appfw
- homme restaurer profil appfw
- man show archive appfw
- archive man rm appfw

Exportation et importation de profils de Web App Firewall à l'aide de l'interface graphique

L'interface graphique est plus facile à utiliser que l'interface de ligne de commande. L'utilitaire effectue à la fois les opérations d'archivage et d'exportation lorsque vous cliquez sur **Exporter**. De même, il exécute à la fois l'importation et la restauration lorsque vous cliquez sur **Importer**. L'interface graphique peut accéder au système de fichiers local de l'ordinateur à partir duquel vous accédez à l'utilitaire. Vous pouvez exporter une copie de l'archive et l'enregistrer sur votre ordinateur local. Vous pouvez ensuite importer cette copie directement dans l'appliance cible sans avoir à transférer manuellement le fichier d'archive d'une appliance à l'autre (s).

Pour exporter un profil de Web App Firewall à l'aide de l'interface graphique :

1. Accédez à **Configuration** > **Sécurité** > **Web App Firewall** > **Profils**.
2. Dans le volet d'informations, sélectionnez un profil à exporter. Cliquez sur **Actions** et sélectionnez **Exporter** pour télécharger et enregistrer une copie dans le système de fichiers local de votre ordinateur.

Pour importer un profil de Web App Firewall à l'aide de l'interface graphique :

1. Accédez à **Configuration** > **Sécurité** > **Web App Firewall** > **Profils**.
2. Dans le volet d'informations, cliquez sur **Actions** et sélectionnez **Importer**. Dans le volet Importer le profil du Web App Firewall, la zone de sélection Importer de* vous offre 2 options :

URL : vous pouvez choisir d'importer une archive en spécifiant une **URL**. Lorsque cette option est sélectionnée, vous devez indiquer un chemin absolu pour le fichier archivé dans la zone de saisie **URL**.

Fichier : Vous pouvez choisir d'importer une archive à partir du **fichier** local. Lorsque cette option est sélectionnée, un champ de sélection **Fichier local** s'affiche. Vous pouvez parcourir les fichiers locaux de votre ordinateur pour sélectionner le fichier d'archive cible.

Cliquez sur **Créer** pour importer l'archive spécifiée. L'exécution réussie de l'opération d'importation crée la configuration de profil sur l'appliance cible.

Résumé

- Vous pouvez répliquer l'intégralité de la configuration (y compris tous les objets d'importation ainsi que les règles de relaxation configurées pour le profil) sur plusieurs appliances, sans devoir répéter les étapes de configuration, à l'aide des fonctionnalités d'exportation et d'importation des profils.
- Les objets importés, tels que les signatures, WSDL, Schéma, page d'erreur, etc., sont inclus dans le fichier tar archivé et répliqués sur l'appliance cible.
- Les types de champs personnalisés sont inclus dans le fichier tar archivé et répliqués sur l'appliance cible.
- Les liaisons de stratégie du profil archivé ne sont pas répliquées lorsque la configuration est restaurée. Vous devez configurer la stratégie et la lier au profil après avoir importé le profil dans l'appliance.
- Le nom du fichier d'archive peut avoir jusqu'à 31 caractères. Comme pour les noms de profils, un nom d'archive doit commencer par un caractère alphanumérique ou un trait de soulignement et contenir uniquement des caractères alphanumériques et des traits de soulignement (_), nombre (#), point (.), espace (), deux-points (:), arobase (@), égal à (=) ou tiret (-).
- Les commentaires associés à l'archive doivent être suffisamment descriptifs pour indiquer le but de la configuration archivée. La longueur maximale autorisée pour un commentaire est de 255 caractères.
- La `clear config -force basic` commande ne supprime pas les profils archivés.
- La fonctionnalité de profil d'importation et d'exportation est prise en charge dans les déploiements haute disponibilité (HA).

Conseils de débogage

- Surveillez le fichier /var/log/ns.log pendant l'exécution des commandes pour voir s'il y a des messages d'ERREUR.
- Des journaux supplémentaires (_restore.log, remove.log, import.log) sont générés dans le dossier /var/tmp/. Ils peuvent aider à déboguer les problèmes pendant les opérations correspondantes. Lorsque ces journaux atteignent un Mo de taille, les messages de journal sont purgés pour réduire le fichier journal à un quart de la taille d'origine.
- Si la commande d'importation échoue lorsque vous utilisez l'option URL au lieu du système de

fichiers local, vérifiez que les paramètres du serveur de noms DNS et du routage sont correctement configurés.
- Si vous utilisez le protocole HTTPS pour importer l'archive, la commande peut échouer si le serveur HTTPS nécessite une authentification de certificat client.

Facilité de dépannage avec les journaux du pare-feu d'application Web

January 21, 2021

En cas d'attaque de sécurité, il est important de capturer l'enregistrement WAF détaillé sur l'appliance. Pour cela, vous pouvez configurer le paramètre « VerboseLogLevel » sur un profil Application Firewall.

Envisagez un trafic Web ayant une attaque de sécurité. Lorsque l'appliance reçoit le trafic, les détails de violation, tels que les détails d'en-tête HTTP, le modèle de journal et les informations de charge utile de modèle, sont consignés et envoyés au serveur ADM. Le serveur ADM surveille les journaux détaillés et les affiche sur la page Security Insight à des fins de surveillance et de suivi.

Configuration du niveau de journal verbeux à l'aide de l'interface de commande

Pour capturer des journaux WAF détaillés, configurez la commande suivante.
Dans l'interface de commande, tapez :

```
set appfw profile <profile_name> -VerboseLogLevel (pattern|patternPayload|
patternPayloadHeader)
```

Exemple

```
set appfw profile profile1 -VerboseLogLevel patternPayloadHeader
```

Les niveaux de journalisation disponibles sont les suivants :

1. Motif. Consigne uniquement le modèle de violation.
2. Charge utile de modèle. Consigne le motif de violation et 150 octets de charge utile supplémentaire de l'élément de champ.
3. En-tête de charge utile de modèle. Journalise le patter de violation, 150 octets de charge utile de l'élément de champ supplémentaire et les informations d'en-tête HTTP.

Configuration du niveau de journal verbeux à l'aide de l'interface graphique Citrix ADC

Suivez la procédure ci-dessous pour configurer le niveau de journal verbeux dans le profil WAF.

1. Dans le volet de navigation, accédez à **Sécurité** > **Profils**.

2. Dans la page **Profils**, cliquez sur **Ajouter**.
3. Dans la page **Profil du Citrix Web App Firewall**, cliquez sur **Paramètres du profil** sous **Paramètres avancés**.
4. Dans la section **Paramètres du profil**, sélectionnez le niveau de journal WAF détaillé dans le champ Niveau de journal détaillé.
5. Cliquez sur **OK** et **Terminé**.



Protection contre le chargement de fichiers

October 5, 2021

De nombreux attaquants tentent de télécharger du code malveillant, des virus ou des logiciels malveillants sous forme de pièces jointes lors de la soumission de formulaires multiples. Il est important de protéger notre réseau et de surmonter ces menaces. Pour empêcher ces téléchargements de fichiers malveillants, un administrateur Citrix ADC peut désormais configurer un ensemble de formats de

téléchargement de fichiers autorisés dans le profil WAF. Ce faisant, vous limitez les téléchargements de fichiers à des formats spécifiques et protégez la solution matérielle-logicielle contre les téléchargements de fichiers malveillants. Toutefois, la protection ne fonctionne que lorsque vous désactivez l'option « ExcludeFileUploadFormChecks » dans le profil WAF.

Fonctionnement du téléchargement de fichiers

Lorsque vous configurez des formats de téléchargement de fichiers autorisés, l'interaction entre les composants est la suivante :

- La demande du client comporte une soumission de formulaire avec un type de téléchargement de fichier, par exemple PDF.
- Dans le cadre du contrôle de sécurité, WAF inspecte la charge utile de la demande et valide le type de fichier (en fonction des numéros de signature magiques).
- Si le type de fichier est un format de fichier autorisé, l'action correspondante basée sur la liaison du type de fichier est appliquée.
- Pour valider le type de fichier, la solution matérielle-logicielle inspecte la charge utile et vérifie les nombres magiques connus aux décalages connus. Chaque type de fichier possède une séquence de nombres magiques qui valide le type de fichier.
- Seulement si la validation réussit, WAF identifie le fichier en tant que format autorisé et l'action associée est appliquée.

Configuration du chargement du type de fichier à l'aide de l'interface de ligne de commande Citrix ADC

Pour configurer les formats de fichiers autorisés, la solution matérielle-logicielle utilise un profil WAF lié aux paramètres de chargement de fichiers.

1. Configurer le profil du pare-feu d'application Web

Pour configurer un profil de pare-feu d'application Web, tapez ce qui suit :

```
set appfw profile <profile_name> [-fileUploadTypesAction <fileUploadTypesAction
>]<fileUploadTypesAction> = ( none | block | log | stats )
```

Exemple

```
set appfw profile profile1 -fileUploadTypesAction block
```

1. Liez le profil de pare-feu d'application Web avec les paramètres de téléchargement de fichiers. La commande lie l'exemption (relaxation) ou la règle spécifiée au profil de pare-feu d'application spécifié.

Pour lier un profil avec des paramètres de téléchargement de fichiers, tapez ce qui suit :

```
bind appfw profile <profile_name> - fileUploadType <form_field > <form_action_url
> -fileType <fileType> ( pdf | msdoc | text | image | any)
```

\[-isNameRegex REGEX (REGEX) | NOTREGEX)\]
> **Remarque :**
>
> Le nom du champ de formulaire est un type d'expression régulière. La valeur par défaut est 'NOTREGEX'.
Exemple
'> bind appfw profile test -fileuploadType thefile "http://10.10.10.10/fileupload_sample/upload.php" -filetype image -isNameRegex'
-->

Configurez la protection de sécurité du chargement de fichiers à l'aide de l'interface graphique Citrix ADC

Suivez la procédure ci-dessous pour définir les paramètres de chargement des fichiers.

1. Dans le volet de navigation, accédez à **Sécurité** > **Profils**.
2. Dans la page Profils, cliquez sur **Ajouter**.
3. Sur la page **Profil Citrix Web App Firewall**, cliquez sur **Contrôles de sécurité** sous **Paramètres avancés**.
4. Dans la section **Vérifications de sécurité**, accédez aux paramètres **Types de téléchargement de fichiers** .



5. Activez la case à cocher et cliquez sur **Paramètres d'action**.
6. Dans la page **Paramètres des types de téléchargement de fichiers**, définissez l'action de chargement de fichiers.
7. Cliquez sur **OK**.
8. Dans la page **Profil de Citrix Web App Firewall**, cliquez sur **OK** et **terminé**.



Configurer la règle de relaxation du chargement de fichiers à l'aide de l'interface graphique Citrix ADC

Vous pouvez assouplir la protection de sécurité du chargement de fichiers pour éviter les faux positifs. Par exemple, la solution matérielle-logicielle peut bloquer les chargements de fichiers, mais vous pouvez ajouter une règle de relaxation pour autoriser le téléchargement de fichiers à partir de sites Web spécifiques. Ce faisant, la solution matérielle-logicielle contourne l'inspection de sécurité pour le champ de formulaire spécifié et autorise les utilisateurs à télécharger des fichiers à partir du site Web mentionné dans l'URL de l'action.

Suivez la procédure ci-dessous pour créer une règle de relaxation.

1. Dans le volet de navigation, accédez à **Sécurité** > **Citrix Web App Firewall** < **Profils**.
2. Dans la page Profils, cliquez sur **Ajouter**.
3. Dans la page **Profil de Citrix Web App Firewall**, cliquez sur **Règles de relaxation** sous **Paramètres avancés**.
4. Dans la section **Règles de relaxation**, sélectionnez **Types de téléchargement de fichiers** et cliquez sur **Modifier**.



5. Dans la page **Règles de réévaluation des types de chargement de fichiers**, cliquez sur **Ajouter**.
6. Dans la page **Règle de relaxation des types de chargement de fichiers**, définissez les paramètres suivants :
   a) Activé. Activez cette case à cocher pour activer la règle de relaxation.
   b) Nom du champ de formulaire. Entrez le nom du champ qui ne nécessite pas de vérification de sécurité.
   c) URL de l'action. URL de soumission du formulaire qui doit être exemptée du contrôle de sécurité.
   d) Type de fichier. Type de fichier qui doit être autorisé pour que l'utilisateur puisse charger.
   e) Commentaires. Une brève description du chargement du fichier.
7. Cliquez sur **Create**.



8. Dans la page **Profil de Citrix Web App Firewall**, cliquez sur **OK** et **terminé**.



Configuration et utilisation de la fonction d'apprentissage

August 20, 2021

La fonction d'apprentissage est un filtre répétitif qui observe l'activité sur un site Web ou une application protégée par le Web App Firewall, afin de déterminer ce qui constitue une activité normale sur ce site Web ou application. Il génère ensuite une liste de jusqu'à 2 000 règles ou exceptions suggérées (relaxations) pour chaque vérification de sécurité qui inclut la prise en charge de la fonctionnalité d'apprentissage. Les utilisateurs trouvent généralement plus facile de configurer les relaxations en utilisant la fonction d'apprentissage qu'en saisissant manuellement les relaxations nécessaires.

Les vérifications de sécurité qui prennent en charge la fonctionnalité d'apprentissage sont les suivantes :

- Démarrer la vérification de l'URL
- Vérification de la cohérence des cookies
- Vérification de la cohérence des champs de formulaire
- Vérification des formats de champ
- Vérification du marquage des formulaires CSRF
- Vérification HTML SQL Injection
- Vérification des scripts inter-sites HTML
- Vérification par déni de service XML
- Vérification des pièces jointes XML
- Vérification de l'interopérabilité des services Web

Vous effectuez deux types d'activités différents lorsque vous utilisez la fonction d'apprentissage. Tout d'abord, vous activez et configurez la fonctionnalité pour l'utiliser. Vous pouvez utiliser l'apprentissage sur tout le trafic vers vos applications Web protégées, ou vous pouvez configurer une liste d'adresses IP (appelée liste *Ajouter des clients d'apprentissage approuvés*) à partir de laquelle la fonctionnalité d'apprentissage doit générer des recommandations. Deuxièmement, une fois que la fonctionnalité a été activée et a traité un certain nombre de trafic vers vos sites Web protégés, vous passez en revue la liste des règles et détentions suggérées (règles apprises) et marquez chacune d'entre elles l'une des désignations suivantes :

- **Modifier et déployer.** La règle est tirée dans la boîte de dialogue Modifier afin que vous puissiez la modifier et le formulaire modifié est déployé.
- **Déployer.** La règle apprise non modifiée est placée dans la liste des règles ou des assouplissements pour cette vérification de sécurité.
- **Ignorer.** La règle apprise est placée sur une liste de règles ou de relaxations qui ne sont pas déployées. La règle apprise est supprimée lorsqu'elle est ignorée. Cependant, comme ils ne sont pas ajoutés aux relaxations, ils peuvent être appris à nouveau.

L'apprentissage n'est pas effectué uniquement lorsque des relaxations sont en place, sauf pour les règles de format de champ. Lorsque les règles sont ignorées, elles sont uniquement supprimées de la base de données apprise. Comme les relaxations ne sont pas ajoutées, elles peuvent être apprises à nouveau. Lorsque les règles sont déployées, elles sont supprimées de la base de données apprise et des relaxations sont également ajoutées pour les règles. À mesure que les relaxations sont ajoutées, elles ne seraient plus apprises. Pour la protection de format de terrain, l'apprentissage est effectué indépendamment des relaxations.

Bien que vous puissiez utiliser l'interface de ligne de commande pour la configuration de base de la fonctionnalité d'apprentissage, la fonctionnalité est principalement conçue pour la configuration via l'Assistant Web App Firewall ou l'interface graphique. Vous ne pouvez effectuer que la configuration limitée de la fonctionnalité d'apprentissage à l'aide de la ligne de commande.

L'assistant intègre la configuration des fonctionnalités d'apprentissage à la configuration du Web App Firewall dans son ensemble. Il s'agit donc de la méthode la plus simple pour configurer cette fonctionnalité sur une nouvelle appliance Citrix ADC ou lors de la gestion d'une configuration simple du pare-feu Web App. Le visualiseur d'interface graphique et l'interface manuelle fournissent tous deux un accès direct à toutes les règles apprises pour toutes les vérifications de sécurité et sont donc souvent préférables lorsque vous devez passer en revue les règles apprises pour un grand nombre de vérifications de sécurité.

La taille de la base de données d'apprentissage est limitée à 20 Mo, ce qui est atteint après la génération d'environ 2 000 règles ou relaxations apprises par vérification de sécurité pour laquelle l'apprentissage est activé. Si vous n'examinez pas régulièrement et que vous approuvez ou ignorez les règles apprises et que cette limite est atteinte, une erreur est enregistrée dans le journal NetScaler et aucune autre règle apprise n'est générée tant que vous n'aurez pas examiné les règles apprises existantes et les relaxations.

Si l'apprentissage s'arrête parce que la base de données a atteint sa limite de taille, vous pouvez redémarrer l'apprentissage en examinant les règles et les relaxations existantes ou en réinitialisant les données d'apprentissage. Une fois les règles apprises ou les relaxations approuvées ou ignorées, elles sont supprimées de la base de données. Après avoir réinitialisé les données d'apprentissage, toutes les données d'apprentissage existantes sont supprimées de la base de données et réinitialisées à sa taille minimale. Lorsque la taille de la base de données est inférieure à 20 Mo, l'apprentissage redémarre automatiquement.

Pour configurer les paramètres d'apprentissage à l'aide de l'interface de ligne de commande

Spécifiez le profil de Web App Firewall à configurer et, pour chaque vérification de sécurité que vous souhaitez inclure dans ce profil, spécifiez le seuil minimum ou le seuil de pourcentage. Le seuil minimum est un nombre entier représentant le nombre minimum de sessions utilisateur que le Web App Firewall doit traiter avant d'apprendre une règle ou une relaxation (par défaut : 1). Le seuil de pourcentage est un nombre entier représentant le pourcentage de sessions utilisateur dans lesquelles le Web App Firewall doit observer un modèle particulier (URL, cookie, champ, pièce jointe ou violation de règle) avant d'apprendre une règle ou une relaxation (par défaut : 0). Utilisez les commandes suivantes :

- `set appfw learningsettings <profileName> [-startURLMinThreshold <positive_integer>] [-startURLPercentThreshold <positive_integer>] [-cookieConsistencyMinThreshold <positive_integer>] [-cookieConsistencyPercentThres <positive_integer>] [-CSRFtagMinThreshold <positive_integer>] [-CSRFtagPercentThreshold <positive_integer>] [-fieldConsistencyMinThreshold <positive_integer>] [-fieldConsistencyPercentThreshold <positive_integer>] [-crossSiteScriptingMinThreshold <positive_integer>] [-crossSiteScriptingPerce`

<positive_integer>] [-SQLInjectionMinThreshold <positive_integer>] [-SQLInjectionPercentThreshold <positive_integer>] [-fieldFormatMinThreshold <positive_integer>] [-fieldFormatPercentThreshold <positive_integer>] [-XMLWSIMinThreshold <positive_integer>] [-XMLWSIPercentThreshold <positive_integer>] [-XMLAttachmentMinThreshold <positive_integer>] [-XMLAttachmentPercentThreshold <positive_integer>]

- save ns config

Exemple

L'exemple suivant active et configure les paramètres d'apprentissage dans le profil pr-basic pour la vérification de sécurité HTML SQL Injection. Il s'agit d'une configuration d'apprentissage initiale appropriée au banc d'essai, dans laquelle vous avez un contrôle complet sur le trafic envoyé au Web App Firewall.

```
1 set appfw learningsettings pr-basic -SQLInjectionMinThreshold 10
2 set appfw learningsettings pr-basic -SQLInjectionPercentThreshold 70
3 save ns config
4 <!--NeedCopy-->
```

Pour réinitialiser les paramètres d'apprentissage à leurs valeurs par défaut à l'aide de l'interface de ligne de commande

Pour supprimer toute configuration personnalisée des paramètres d'apprentissage pour le profil et la vérification de sécurité spécifiés, et retourner les paramètres d'apprentissage à leurs valeurs par défaut, à l'invite de commandes, tapez les commandes suivantes :

- unset appfw learningsettings <profileName> [-startURLMinThreshold] [-startURLPercentThreshold] [-cookieConsistencyMinThreshold] [-cookieConsistencyPercentThreshold] [-CSRFtagMinThreshold] [-CSRFtagPercentThresh] [-fieldConsistencyMinThreshold] [-fieldConsistencyPercentThreshold] [-crossSiteScriptingMinThreshold] [-crossSiteScriptingPercentThreshold] [-SQLInjectionMinThreshold] [-SQLInjectionPercentThreshold] [-fieldFormatMinThreshold] [-fieldFormatPercentThreshold] [-XMLWSIMinThreshold] [-XMLWSIPercentThreshold] [-XMLAttachmentMinThreshold] [-XMLAttachmentPercen]
- save ns config

Pour afficher les paramètres d'apprentissage d'un profil à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
show appfw learningsettings <profileName>
```

Pour afficher les règles apprises non révisées ou les relaxations d'un profil à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
show appfw learningdata <profileName> <securityCheck>
```

Pour supprimer des règles apprises non examinées ou des relaxations spécifiques de la base de données d'apprentissage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
rm appfw learningdata <profileName> (-startURL <expression> | -cookieConsistency
 <string> | (-fieldConsistency <string> <formActionURL>)| (-crossSiteScripting
 <string> <formActionURL>)| (-SQLInjection <string> <formActionURL>)| (-
fieldFormat <string><formActionURL>)| (-CSRFTag <expression> <CSRFFormOriginURL
>)| -XMLDoSCheck <expression> | -XMLWSICheck <expression> | -XMLAttachmentCheck
 <expression>)[-TotalXMLRequests]
```

Exemple

L'exemple suivant supprime toutes les relaxations apprises non examinées pour le profil pr-basic, vérification de sécurité HTML SQL Injection, qui s'appliquent au champ de formulaire LastName.

```
1 rm appfw learningdata pr-basic -SQLInjection LastName
2 <!--NeedCopy-->
```

Pour supprimer toutes les données apprises non examinées à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
reset appfw learningdata
```


Pour exporter des données d'apprentissage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
export appfw learningdata <profileName> <securitycheck>[-target <string>]
```

Exemple

L'exemple suivant exporte les relaxations apprises pour le profil pr-basic et la vérification de sécurité HTML SQL Injection vers un fichier au format CSV (valeurs séparées par des virgules) dans le répertoire /var/learnt_data/ sous le nom de fichier spécifié dans le paramètre -target.

```
1 export appfw learningdata pr-basic SQLInjection -target sqli_ld
2 <!--NeedCopy-->
```

Pour configurer la fonctionnalité d'apprentissage à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Web App Firewall** > **Profils**.
2. Dans le volet **Profils**, sélectionnez le profil, puis cliquez sur **Modifier**.
3. Cliquez sur l'onglet Apprentissage. En haut de l'onglet Formation, vous trouverez la liste des vérifications de sécurité disponibles dans le profil actuel et qui prennent en charge la fonctionnalité d'apprentissage.
4. Pour configurer les seuils d'apprentissage, sélectionnez une vérification de sécurité, puis tapez les valeurs appropriées dans les zones de texte suivantes :

   Seuil de nombre minimum. Selon les paramètres d'apprentissage de la vérification de sécurité que vous configurez, le seuil de nombre minimum peut faire référence au nombre minimum de sessions utilisateur totales à observer, au nombre minimum de demandes à observer ou au nombre minimum de fois qu'un champ de formulaire spécifique doit être observé, avant qu'une relaxation apprise ne soit générée. Par défaut : 1

   Pourcentage du seuil de durée. Selon les paramètres d'apprentissage de la vérification de sécurité que vous configurez, le pourcentage de seuil de durée peut faire référence au pourcentage du nombre total de sessions utilisateur observées qui ont enfreint la vérification de sécurité, au pourcentage de demandes ou au pourcentage de fois qu'un champ de formulaire correspond à un type de champ particulier, avant qu'un une relaxation apprise est générée. Par défaut : 0
5. Pour supprimer toutes les données apprises et réinitialiser la fonction d'apprentissage afin qu'elle redémarre ses observations dès le début, cliquez sur **Supprimer toutes les données apprises**.

Remarque : Ce bouton supprime uniquement les recommandations apprises qui n'ont pas été examinées et approuvées ou ignorées. Il ne supprime pas les relaxations apprises qui ont été acceptées et déployées.

6. Pour limiter le moteur de formation au trafic provenant d'un ensemble spécifique d'adresses IP, cliquez sur **Clients d'apprentissage approuvés**, puis ajoutez les adresses IP que vous souhaitez utiliser à la liste.

   a) Pour ajouter une adresse IP ou une plage d'adresses IP à la liste Clients d'apprentissage approuvés, cliquez sur **Ajouter**.
   b) Dans la boîte de dialogue **Ajouter des clients d'apprentissage** approuvés, zone de liste IP des clients de confiance, tapez l'adresse IP ou une plage d'adresses IP au format CIDR.
   c) Dans la zone de texte Commentaires, tapez un commentaire qui décrit cette adresse IP ou cette plage.
   d) Cliquez sur **Créer** pour ajouter votre nouvelle adresse IP ou plage à la liste.
   e) Pour modifier une adresse IP ou une plage existante, cliquez sur l'adresse IP ou la plage, puis cliquez sur **Ouvrir**. À l'exception du nom, la boîte de dialogue qui s'affiche est identique à la boîte de dialogue **Ajouter des clients d'apprentissage approuvés**.
   f) Pour désactiver ou activer une adresse IP ou une plage, mais la laisser dans la liste, cliquez sur l'adresse IP ou la plage, puis cliquez sur **Désactiver ou Activer**, le cas échéant.
   g) Pour supprimer complètement une adresse IP ou une plage, cliquez sur l'adresse IP ou la plage, puis cliquez sur **Supprimer**.

7. Cliquez sur **Fermer** pour revenir à la boîte de dialogue Configurer le profil de Web App Firewall.
8. Cliquez sur **Fermer** pour fermer la boîte de dialogue **Configurer le profil du Web App Firewall** et revenir à l'écran **Profil du pare-feu de l'application Web**.

Pour passer en revue les règles ou les relaxations apprises à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Web App Firewall** > **Profils**.
2. Sélectionnez la vérification de sécurité pour laquelle vous souhaitez consulter les règles ou les relaxations apprises, puis cliquez sur **Gérer les règles**.
3. Dans la boîte de dialogue **Gérer les règles apprises**, choisissez la façon dont vous souhaitez passer en revue les règles apprises.

   - Pour consulter les modèles appris réels tels qu'ils sont affichés dans la fenêtre, ne faites rien et passez à l'étape suivante.
   - Pour passer en revue les données acquises de manière hiérarchique en tant qu'arbre de ramification, vous permettant de choisir des modèles généraux qui correspondent à la plupart des modèles appris, cliquez sur **Visualiseur**.

4. Si vous avez choisi de passer en revue les modèles appris, effectuez les opérations suivantes.
5. Sélectionnez la première relaxation apprise et choisissez comment la gérer.
   - Pour modifier, puis accepter la relaxation, cliquez sur **Modifier et déployer**, modifiez l'expression régulière de relaxation, puis cliquez sur **OK**.
   - Pour accepter la relaxation sans modification, cliquez sur **Déployer**.
   - Pour supprimer la relaxation de la liste sans la déployer, cliquez sur **Ignorer**.

   a) Répétez l'étape précédente pour passer en revue chaque relaxation apprise supplémentaire.
6. Si vous avez choisi d'utiliser le visualiseur d'apprentissage, effectuez les opérations suivantes.

   a) Dans l'affichage hiérarchique des branches, sélectionnez un nœud contenant un motif appris et choisissez comment le gérer.

      La zone d'écran située sous la structure arborescente, sous Regex of Selected Node, affiche une expression généralisée qui correspond à tous les motifs de ce nœud. Si vous souhaitez afficher une expression qui correspond à une seule des branches ou à une seule des feuilles, sélectionnez cette branche ou cette feuille.

      - Pour modifier, puis accepter la relaxation apprise, cliquez sur Modifier et déployer, modifiez l'expression régulière de relaxation, puis cliquez sur **OK**.
      - Pour accepter la relaxation sans modification, cliquez sur Déployer.
      - Pour supprimer la modification de la liste sans la déployer, cliquez sur **Ignorer**.

   b) Répétez l'étape précédente pour passer en revue les autres parties de l'affichage.
7. Cliquez sur **Fermer** pour revenir à la boîte de dialogue **Gérer les règles apprises**.
8. Cliquez sur **Fermer** pour revenir à la boîte de dialogue **Configurer le profil du Web App Firewall** .
9. Cliquez sur **Fermer** pour fermer la boîte de dialogue **Configurer le profil du Web App Firewall** et revenir à l'écran **Profil du pare-feu de l'application Web**.

Profilage dynamique

October 5, 2021

La fonction d'apprentissage est un filtre de modèles qui observe et apprend les activités sur le serveur principal. Sur la base de l'observation, le moteur d'apprentissage génère jusqu'à 2000 règles ou exceptions (assouplissements) pour chaque contrôle de sécurité. Pour automatiser le processus et déployer automatiquement les règles de relaxation, l'appliance Citrix ADC utilise le profilage dynamique.

Avec le profilage dynamique, l'appliance enregistre les données apprises pour un seuil prédéfini et envoie une alerte SNMP à l'utilisateur. Si l'utilisateur ne saute pas les données pendant un délai de grâce, l'appliance les déploie automatiquement en tant que règle de relaxation. Auparavant, l'utilisateur devait déployer manuellement les règles de relaxation. Actuellement, le profilage dynamique n'est disponible que pour les contrôles de sécurité suivants :

1. Injection HTML SQL
2. Script HTML Cross Site
3. Format de champ
4. URL de démarrage
5. Type de contenu
6. Formats de champs
7. Balisage de formulaire CSRF
8. Cohérence des cookies
9. Refuser URL
10. Dépassement de tampon
11. Carte de crédit
12. Protection du type de contenu
13. Protection contre les injections JSON Cmd

Par exemple, considérez la vérification de sécurité HTML SQL Injection activée avec le profilage dynamique. Vous pouvez utiliser la formation pour une liste d'adresses IP (appelée liste des clients de formation approuvés) à partir desquelles la fonctionnalité de formation doit générer des recommandations. Pour configurer une liste de clients approuvés, consultez la rubrique Apprentissage des clients de confiance. Si le trafic entrant comporte des violations, il est enregistré en tant que données apprises. Si les données apprises sont enregistrées dans le moteur d'apprentissage, la solution matérielle-logicielle envoie une alerte SNMP à l'utilisateur. Si l'utilisateur ne reconnaît pas un faux positif et n'ignore pas les données apprises dans un délai de grâce, l'appliance les déploie automatiquement en tant que règle de relaxation.

> **Remarque :**
> Après avoir configuré le profil dynamique, vous devez régulièrement revoir la configuration de l'appliance pour le déploiement automatique des règles de relaxation et l'enregistrer sur l'appliance.

Configurer le profilage dynamique à l'aide de l'interface de commande Citrix ADC

Le profilage dynamique est disponible pour les vérifications de sécurité de l'URL de démarrage, du script intersite HTML, du format des champs ou de l'injection SQL HTML. Pour configurer le profilage dynamique, vous devez suivre les étapes suivantes.

1. Configuration de l'apprentissage dynamique

2. Configuration de la période de grâce du déploiement automatique

Configuration de l'apprentissage dynamique

Dans un premier temps, vous devez configurer l'apprentissage dynamique sur votre solution matérielle-logicielle. À l'invite de commandes, tapez :

```
set appfw profile <profile_name> dynamicLearning <security_checks>
```

Exemple

```
set appfw profile test1 dynamicLearning SQLInjection CrossSiteScripting
fieldFormat startURL
```

Configuration de la période de grâce du déploiement automatique

Une fois que vous avez activé la fonctionnalité sur des vérifications de sécurité spécifiques, vous devez configurer la période de grâce pour le déploiement automatique.

```
set appfw learningsettings <profile name> -crossSiteScriptingAutoDeployGracePeriod
 <seconds>

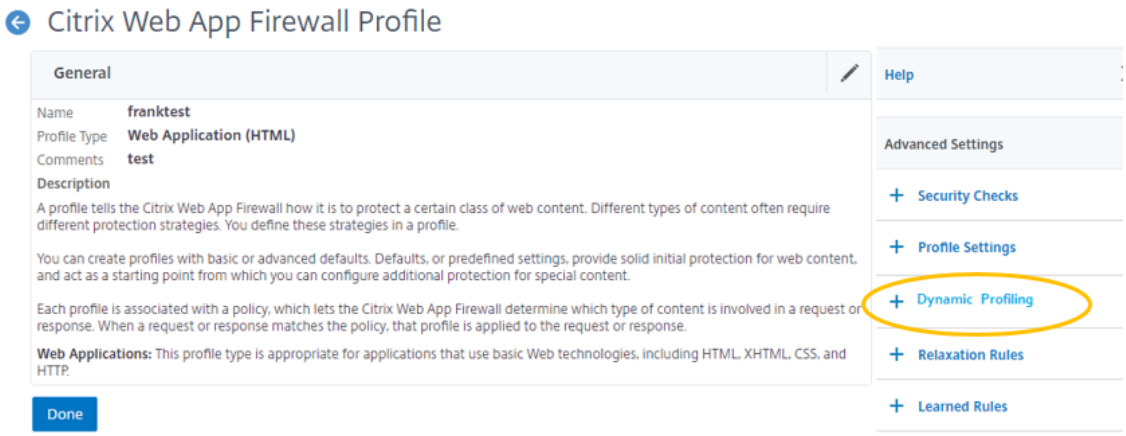
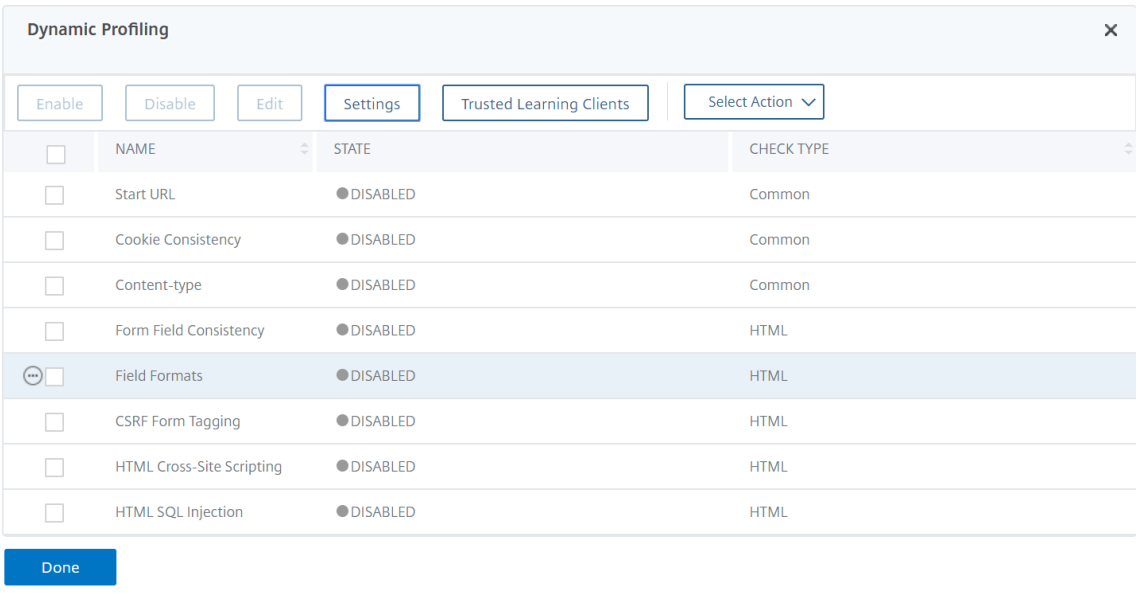
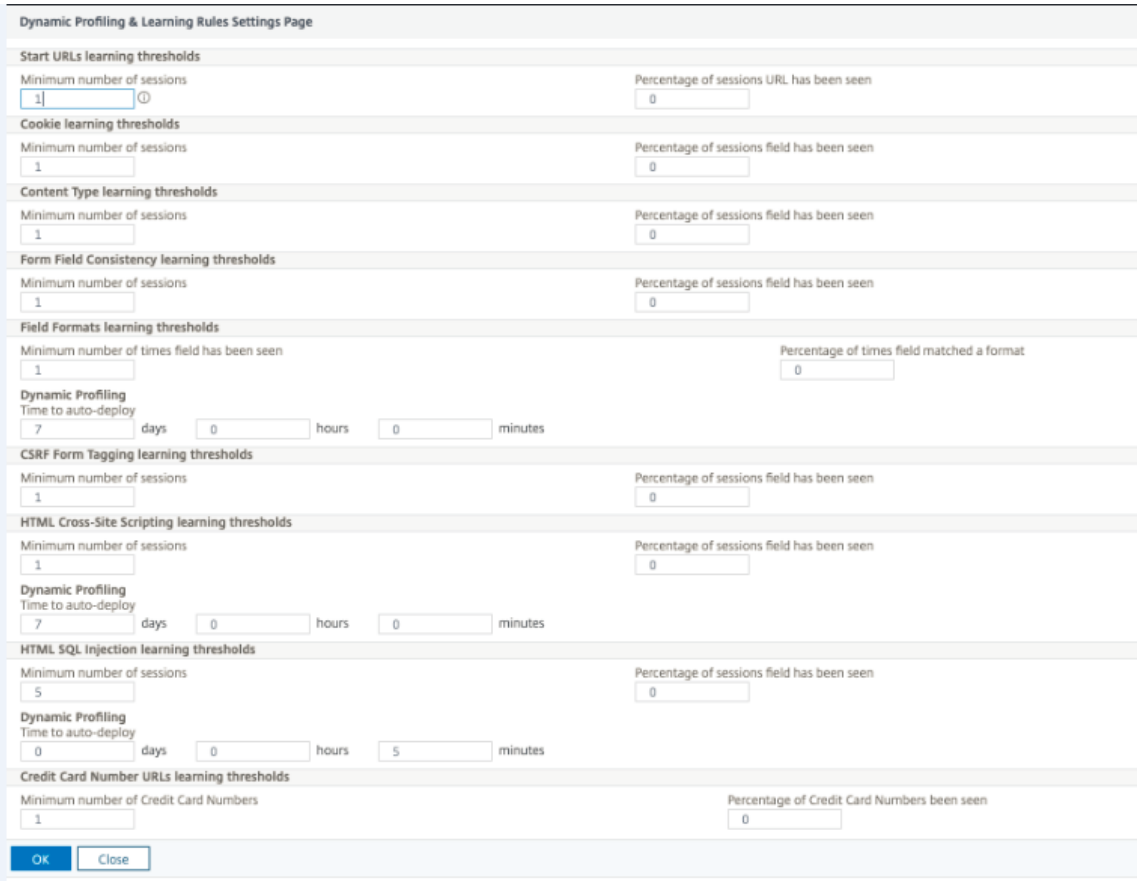
set appfw learningsettings <profile name> fieldFormatAutoDeploymentGracePeriod
 <seconds>

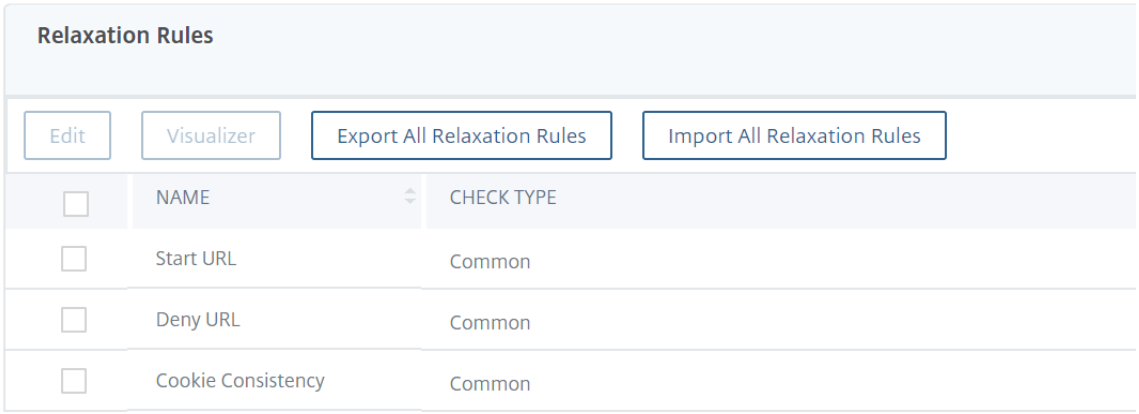
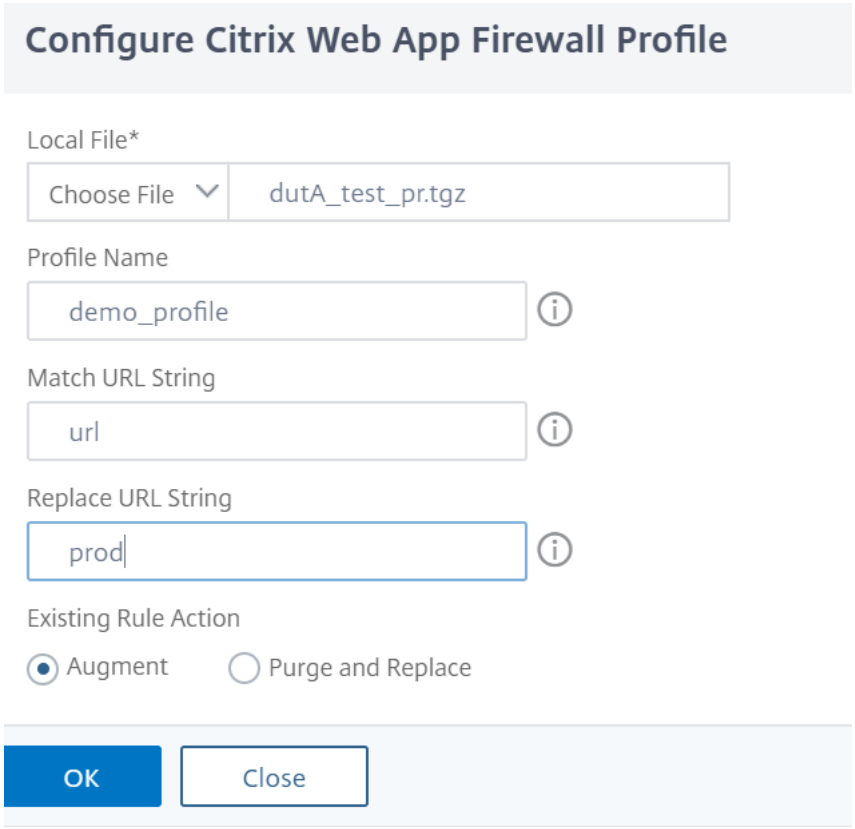
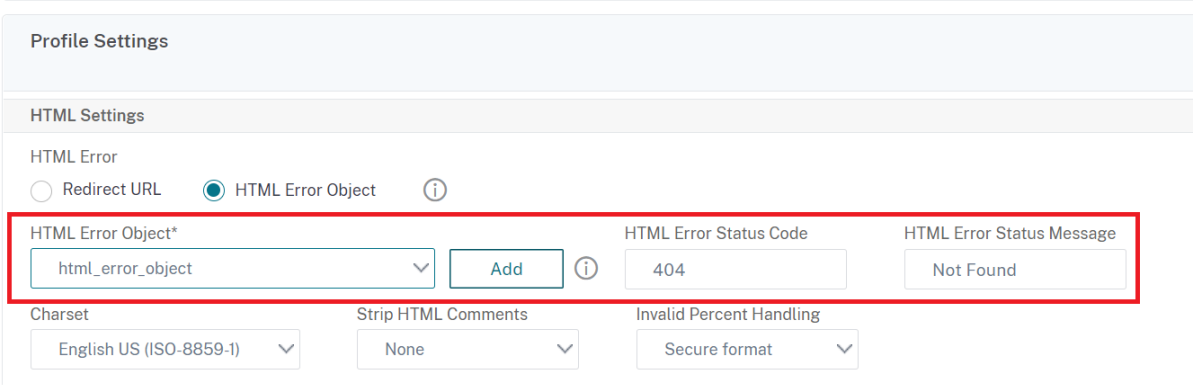
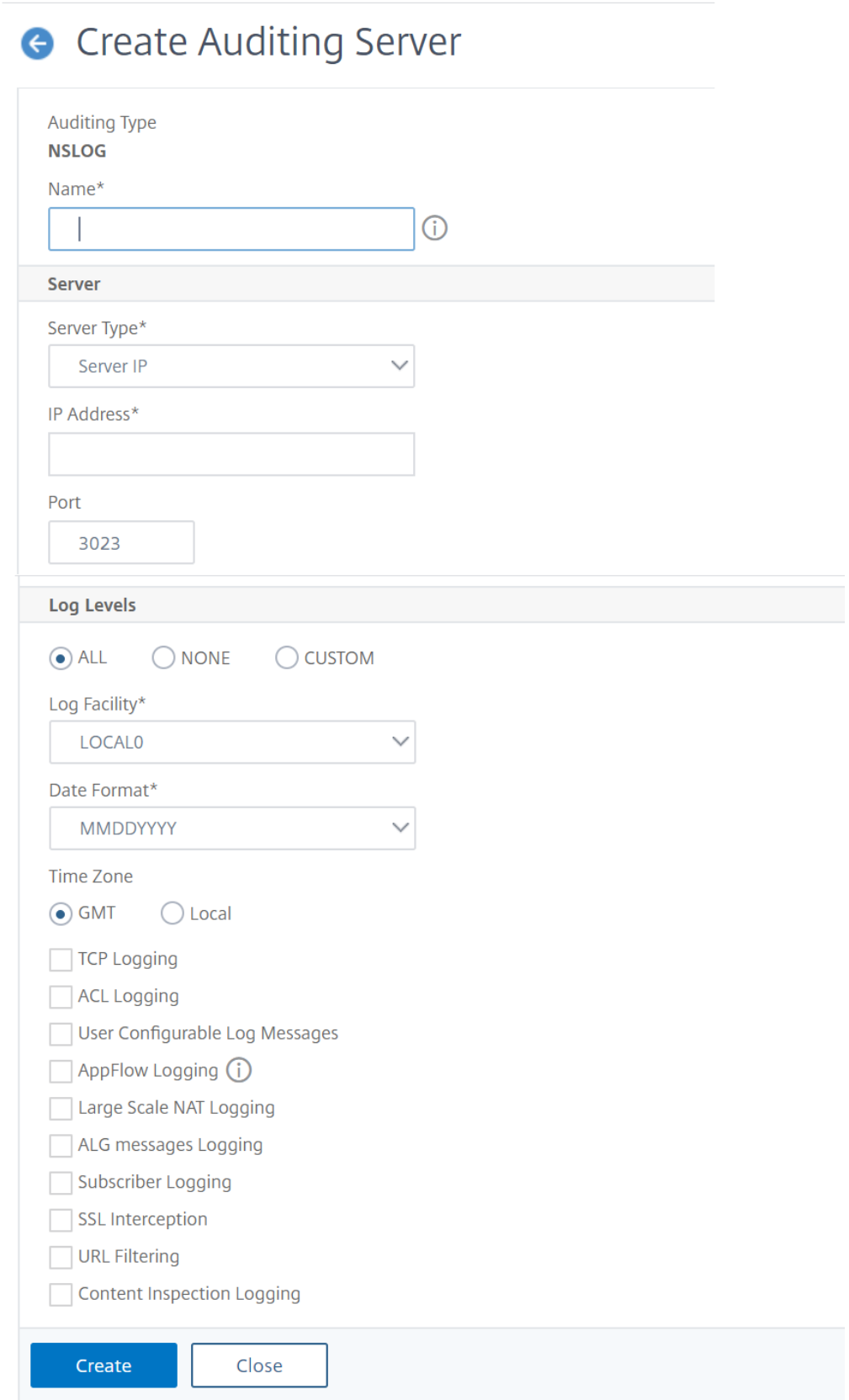
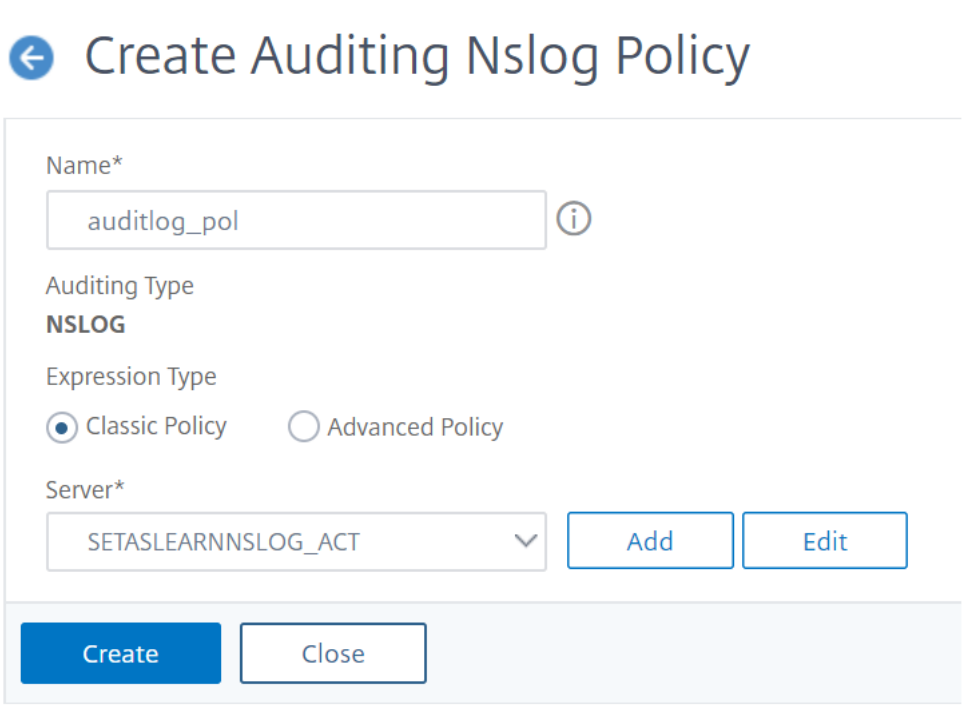
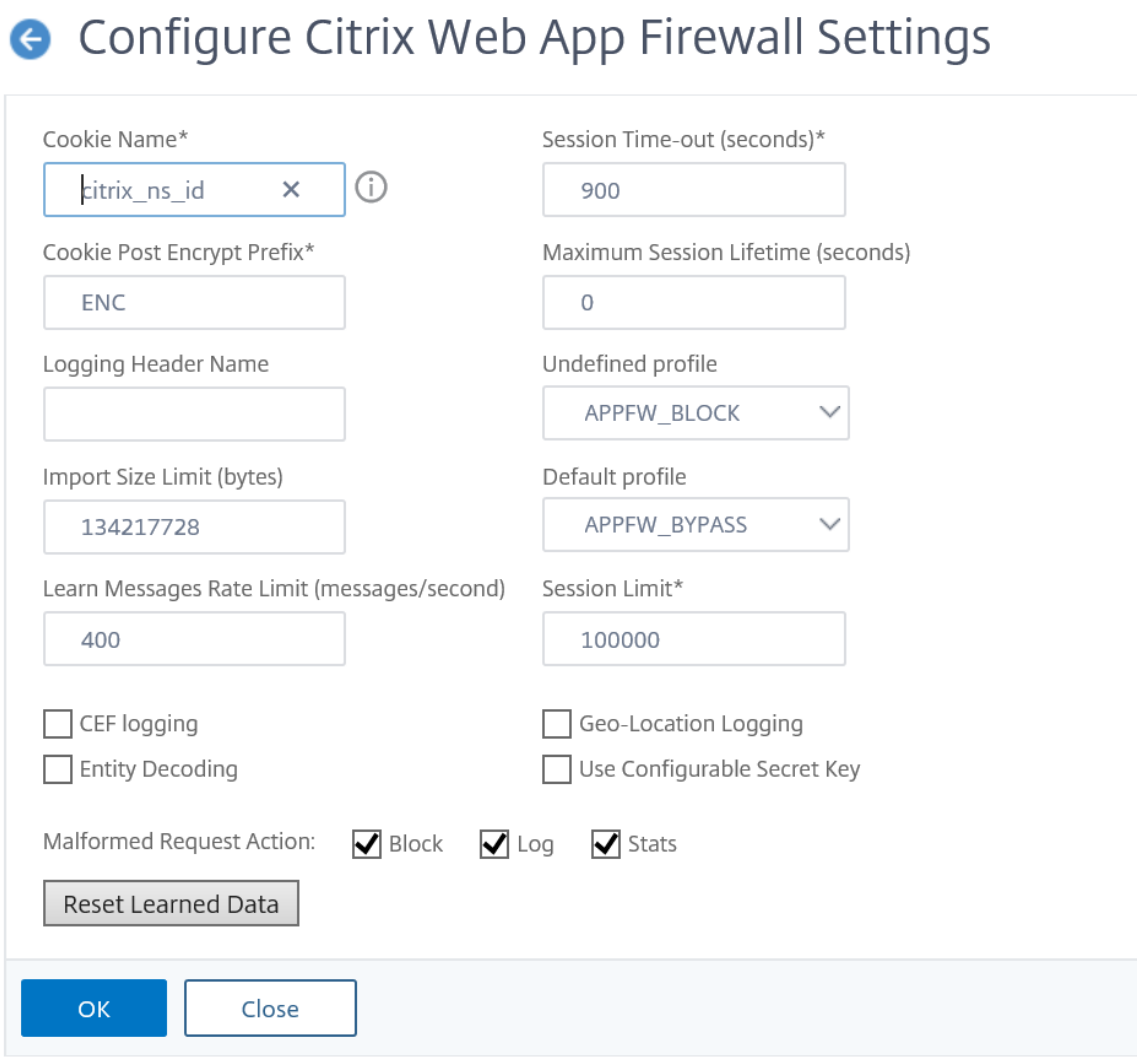
set appfw learningsettings <profile name> SQLInjectionAutoDeploymentGracePeriod
 <seconds>

set appfw learningsettings <profile name> -startURLAutoDeployGracePeriod <
seconds>
```

Exemple

```
set appfw learningsettings test1 -crossSiteScriptingAutoDeployGracePeriod 30

set appfw learningsettings test1 -startURLAutoDeployGracePeriod 7

set appfw learningsettings test1 -fieldFormatAutoDeploymentGracePeriod 10

set appfw learning settings test1 -SQLInjectionAutoDeploymentGracePeriod 12
```

> **Remarque :**
>
> Ici, la période de grâce du déploiement automatique est de quelques minutes.

Configuration du profilage dynamique à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité > Citrix Web App Firewall > Profil**.
2. Dans le volet d'informations, sélectionnez un profil et cliquez sur **Modifier**.
3. Dans la page **Profil de Citrix Web App**, cliquez sur **Profilage dynamique** sous **Paramètres avancés**.



4. Dans la section **Profilage dynamique**, sélectionnez une vérification de sécurité et cliquez sur **Modifier**.



5. Dans la page **Paramètres de profilage et d'apprentissage dynamiques**, définissez la période de grâce du contrôle de sécurité.



6. Cliquez sur **OK** et **Terminé**.

Exportation et importation de règles de relaxation

Lorsque vous activez le profilage dynamique, les données apprises sont automatiquement déployées en tant que règles de relaxation. Parallèlement, l'appliance vous permet également d'exporter les règles de relaxation basées sur le profilage dynamique et les règles de relaxation régulières. Vous pouvez exporter les règles depuis l'environnement de transit et les importer dans l'environnement de production.

> **Remarque :**
>
> Lorsque vous importez des règles dans l'environnement de production, vous devez vous assurer que le processus est additif et qu'il ne remplace pas la configuration existante.

Comment exporter et importer des règles de relaxation

Pour exporter et importer les règles de relaxation, vous devez effectuer les étapes suivantes :

1. Vous devez d'abord exporter les données de profilage dynamique. Pour cela, l'option d'exportation est disponible pour les règles de relaxation du profil WAF. Lorsque vous sélec-

tionnez cette option, vous exportez les règles de relaxation de profilage dynamique et les règles de relaxation standard. Vous pouvez utiliser l'option d'exportation pour télécharger la configuration sous forme de bundle compressé sur la solution matérielle-logicielle.

2. Une fois que vous avez exporté les données de l'environnement intermédiaire, vous devez les importer vers une autre appliance Citrix ADC. Pour cela, vous devez utiliser l'option d'importation disponible dans les règles de relaxation du profil WAF. Lorsque vous sélectionnez cette option, la solution matérielle-logicielle importe les règles de relaxation spécifiées groupées et les restaure dans le profil WAF de la solution matérielle-logicielle sélectionnée.

> **Remarque :**
>
> Si vous souhaitez importer des règles de relaxation dans un profil WAF, il existe deux types d'action :
> Augmenter — Cette action garantit que l'importation est additive et ne remplace donc aucune configuration existante.
> Remplacer — Cette action remplace la configuration existante par la configuration présente dans le bundle d'exportation compressé. »

Importer le fichier de règles de relaxation archivées à l'aide de l'interface

Pour importer les règles de relaxation, vous devez importer l'archive dans l'appliance Citrix ADC, puis exécuter la commande de restauration pour extraire la configuration. L'ensemble de commandes CLI suivant peut être utilisé pour exporter, importer et gérer les configurations.

Pour importer le fichier archivé à partir de l'emplacement spécifique et restaurer, à l'invite de commandes, tapez :

```
import appfw archive <src> <name> [-comment <string>]
```

Où,
« src » : Indique la source du fichier d'archive tar sous la forme, `<protocol>://<host>[:<port>][/<path>]`
« name » : Indique le nom de l'archive.
« commentaire » : Commentaires associés à cette archive.

```
restore appfw profile <archivename> [-relaxationRules] [-importProfileName
 <string>] [-matchUrlString <string>] [-replaceUrlString <string>] [-
overwrite] [-augment]
```

Où,
`archivename` : indique la source de l'archive tar. Il s'agit d'un argument obligatoire.
« RelaxationRules » : Possibilité d'importer toutes les règles de relaxation appfw.

`importProfileName`: indique le nom de profil créé ou mis à jour pour associer les règles de relaxation pendant l'opération de restauration.

« MatChurlString » : indique la chaîne URL d'action à correspondre dans les règles de relaxation archivées.

`replaceUrlString`: indique une chaîne à remplacer l'URL en action lors de la restauration des règles de relaxation.

`overwrite`: action de règles existantes pour purger les règles de relaxation existantes et les remplacer pendant l'importation.

`augment`: action de règles existantes pour augmenter les règles de relaxation lors de l'importation.

Exemple :

```
import appfw archive local: dutA_test_pr.tgz demo
restore appfw profile dutA_test_pr
```

Exportez le fichier archivé vers l'appliance sélectionnée à l'aide de l'interface de ligne de commande

Si vous utilisez l'interface de ligne de commande pour exporter les règles de relaxation appfw, vous devez archiver la configuration, puis l'exporter.
Pour archiver et exporter le fichier archivé, à l'invite de commandes, tapez :

```
archive appfw profile <name> <archivename> [-comment <string>]
```

Où,
`archive name` : indique la source de l'archive tar. Il s'agit d'un argument obligatoire.
`name`: indique le nom du profil appfw contenant les règles de relaxation à exporter

```
export appfw archive <name> <target>
```

Où,
nom. Nom de l'archive tar. Il s'agit d'un argument obligatoire. Longueur maximale : 31
cibles. Chemin d'accès au fichier à exporter. Il s'agit d'un argument obligatoire. Longueur maximale : 2047

Exemple :

```
> archive appfw profile test_pr archived_test_pr

> export appfw archive archived_test_pr local:dutA_test_pr
```

Pour exporter des règles de relaxation à l'aide de Citrix ADC GUI

Suivez les étapes ci-dessous pour exporter les règles de relaxation :

1. Accédez à **Sécurité** > **Citrix Web App Firewall**.
2. Dans la page de détails, cliquez sur le lien **Profils Citrix Web App Firewall** sous la section **Récapitulatif de la configuration** .

3. Dans la page **Profil de Citrix Web App Firewall**, cliquez sur le lien **Règles de relaxation** sous la section **Paramètres avancés** .
4. Dans la section **Règles de relaxation**, cliquez sur **Exporter toutes les règles de relaxation**. L'action s'applique à tous les contrôles de sécurité et à ceux pour lesquels l'apprentissage dynamique est activé sur ce profil.



Pour importer des règles de relaxation à l'aide de Citrix ADC GUI

Suivez les étapes pour importer des règles de relaxation :

1. Accédez à **Sécurité** > **Citrix Web App Firewall**.
2. Dans la page de détails, cliquez sur le lien **Citrix Web App Firewall Profiles** sous la section Configuration Summary (**Résumé de la configuration**).
3. Dans la page **Profil de Citrix Web App Firewall**, cliquez sur le lien **Règles de relaxation** sous la section **Paramètres avancés** .
4. Dans la section **Règles de relaxation**, cliquez sur **Importer toutes les règles de relaxation**.
5. Dans la page **Configurer le profil Citrix Web App Firewall**, définissez les paramètres suivants :
   a) Fichier local. Nom du fichier archivé compressé contenant les règles de relaxation.
   b) Nom du profil. Nom du profil auquel les règles de relaxation sont liées.
   c) Chaîne d'URL correspondante. Partie de l'URL qui correspond.
   d) Remplacez la chaîne d'URL. Partie de l'URL qui remplace la chaîne d'URL.
   e) Action de règle existante. Sélectionnez si la règle doit remplacer les règles existantes ou augmenter les règles existantes.
6. Cliquez sur **OK**.



Informations supplémentaires sur les profils

August 20, 2021

Voici des informations supplémentaires sur des aspects particuliers des profils de Web App Firewall. Ces informations expliquent comment inclure des caractères spéciaux dans une règle de vérification de sécurité ou de relaxation, et comment utiliser des variables lors de la configuration des profils.

Prise en charge des variables de configuration

Au lieu d'utiliser des valeurs statiques, pour configurer les contrôles de sécurité et les paramètres du pare-feu Web App, vous pouvez désormais utiliser des variables nommées Citrix ADC standard. En créant des variables, vous pouvez plus facilement exporter, puis importer des configurations vers de nouvelles appliances Citrix ADC, ou mettre à jour des appliances Citrix ADC existantes à partir d'un seul ensemble de fichiers de configuration. Cela simplifie les mises à jour lorsque vous utilisez une configuration de banc d'essai pour développer une configuration complexe de Web App Firewall qui est réglée pour votre réseau local et vos serveurs, puis transférez cette configuration vers vos appliances Citrix ADC de production.

Vous créez des variables de configuration du Web App Firewall de la même manière que les autres variables nommées Citrix ADC, conformément aux conventions Citrix ADC standard. Pour créer une variable d'expression nommée à l'aide de l'interface graphique, vous utilisez la boîte de dialogue Ajouter une expression. Pour créer une variable d'expression nommée à l'aide de la ligne de commande Citrix ADC, vous utilisez la commande add expression suivie du paramètre approprié.

Les URL et expressions suivantes peuvent être configurées avec des variables au lieu de valeurs statiques :

- **Start URL** (-starturl)
- **Deny URL** (-denyurl)
- **Form Action URL** for *Form Field Consistency Check* (-fieldconsistency)
- **Action URL** for *XML SQL Injection Check* (-xmlSQLInjection)
- **Action URL** for X*ML Cross-Site Scripting Check* (-xmlcross-site scripting)
- **Form Action URL** for *HTML SQL Injection Check* (-sqlInjection)
- **Form Action URL** for *Field Format Check* (-fieldFormat)
- **Form Origin URL** and **Form Action URL** for *Cross-Site Request Forgery (CSRF) Check* (-csrfTag)
- **Form Action URL** for *HTML Cross-Site Scripting Check* (-crossSiteScripting)
- **Safe Object** (-safeObject)
- **Action URL** for *XML Denial-of-Service (XDoS) check* (-XMLDoS)
- **URL** for *Web Services Interoperability check* (-XMLWSIURL)
- <**URL** for *XML Validation check* (-XMLValidationURL)
- **URL** for *XML Attachment check* (-XMLAttachmentURL)

Pour plus d'informations, voir Stratégies et expressions.

Pour utiliser une variable dans la configuration, vous placez le nom de la variable entre deux symboles à (@), puis l'utilisez exactement comme vous le feriez pour la valeur statique qu'elle remplace. Par exemple, si vous configurez la vérification de l'URL Refuser à l'aide de l'interface graphique et que vous souhaitez ajouter la variable d'expression nommée MyDenyURL à la configuration, tapez @myDenyURL @ dans la boîte de dialogue Ajouter une URL de refus, zone de texte Refuser l'URL. Pour effectuer la même tâche à l'aide de la ligne de commande Citrix ADC, tapez add appfw profile <name> -denyUrlAction @myDenyURL@.

Format de codage de caractères PCRE

Le système d'exploitation Citrix ADC prend en charge l'entrée directe de caractères dans le jeu de caractères ASCII imprimable uniquement : les caractères dont les codes hexadécimaux sont compris entre HEX 20 (ASCII 32) et HEX 7E (ASCII 127). Pour inclure un caractère dont le code est en dehors de cette plage dans votre configuration de Web App Firewall, vous devez entrer son code hexadécimal UTF-8 en tant qu'expression régulière PCRE.

Un certain nombre de types de caractères nécessitent un encodage à l'aide d'une expression régulière

PCRE si vous les incluez dans votre configuration de Web App Firewall en tant qu'URL, nom de champ de formulaire ou expression d'objet sécurisé. Il s'agit notamment des éléments suivants :

- **Caractères ASCII supérieurs.** Caractères avec encodages de HEX 7F (ASCII 128) à HEX FF (ASCII 255). Selon la table de caractères utilisée, ces encodages peuvent faire référence à des codes de contrôle, à des caractères ASCII avec des accents ou d'autres modifications, à des caractères alphabétiques non latins et à des symboles non inclus dans le jeu de caractères ASCII de base. Ces caractères peuvent apparaître dans les URL, les noms de champs de formulaire et les expressions d'objet sécurisé.
- **Caractères à deux octets.** Caractères avec encodages qui utilisent deux mots de 8 octets. Les caractères sur deux octets sont utilisés principalement pour représenter le texte chinois, japonais et coréen en format électronique. Ces caractères peuvent apparaître dans les URL, les noms de champs de formulaire et les expressions d'objet sécurisé.
- **Caractères de contrôle ASCII.** Caractères non imprimables utilisés pour envoyer des commandes à une imprimante. Tous les caractères ASCII dont les codes hexadécimaux sont inférieurs à HEX 20 (ASCII 32) entrent dans cette catégorie. Toutefois, ces caractères ne doivent jamais apparaître dans une URL ou un nom de champ de formulaire et apparaissent rarement, sinon jamais, dans une expression d'objet sécurisée.

L'appliance Citrix ADC ne prend pas en charge l'ensemble du jeu de caractères UTF-8, mais uniquement les caractères présents dans les huit jeux de caractères suivants :

- **Anglais US (ISO-8859-1).** Bien que l'étiquette indique « Anglais US », le Web App Firewall prend en charge tous les caractères du jeu de caractères ISO-8859-1, également appelé jeu de caractères Latin-1. Ce jeu de caractères représente entièrement la plupart des langues modernes d'Europe occidentale et représente tous les caractères rares dans le reste.
- **Chinois traditionnel (Big5).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères BIG5, qui comprend tous les caractères chinois traditionnels (idéogrammes) couramment utilisés en chinois moderne tels que parlés et écrits à Hong Kong, Macao, Taïwan, et par de nombreuses personnes d'origine ethnique chinoise qui vivent en dehors de la Chine continentale.
- **Chinois simplifié (GB2312).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères GB2312, qui inclut tous les caractères chinois simplifiés (idéogrammes) couramment utilisés en chinois moderne, tels que parlés et écrits en Chine continentale.
- **Japonais (SJIS).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères Shift-JIS (SJIS), qui comprend la plupart des caractères (idéographes) couramment utilisés dans le japonais moderne.
- **japonais (EUC-JP).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères EUC-JP, qui inclut tous les caractères (idéographes) couramment utilisés dans le japonais moderne.

- **coréen (EUC-KR).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères EUC-KR, qui inclut tous les caractères (idéographes) couramment utilisés en coréen moderne.
- **turc (ISO-8859-9).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères ISO-8859-9, qui inclut toutes les lettres utilisées en turc moderne.
- **Unicode (UTF-8).** Le Web App Firewall prend en charge certains caractères supplémentaires dans le jeu de caractères UTF-8, y compris ceux utilisés dans le russe moderne.

Lors de la configuration du Web App Firewall, vous entrez tous les caractères non-ASCII en tant qu'expressions régulières au format PCRE à l'aide du code hexadécimal attribué à ce caractère dans la spécification UTF-8. Les symboles et les caractères du jeu de caractères ASCII normal, auxquels on attribue des codes à deux chiffres dans ce jeu de caractères, sont affectés les mêmes codes dans le jeu de caractères UTF-8. Par exemple, le point d'exclamation (!), auquel est attribué le code hexadécimal 21 dans le jeu de caractères ASCII, est également hexadécimal 21 dans le jeu de caractères UTF-8. Les symboles et les caractères d'un autre jeu de caractères pris en charge ont un jeu de codes hexadécimaux appariés qui leur sont assignés dans le jeu de caractères UTF-8. Par exemple, la lettre a avec un accent aigu (á) est assignée le code UTF-8 C3 A1.

La syntaxe que vous utilisez pour représenter ces codes UTF-8 dans la configuration du Web App Firewall est "xNN" pour les caractères ASCII ; "\xNN\xNN" pour les caractères non ASCII utilisés en anglais, russe et turc ; et "\xNN\xNN\xNN" pour les caractères utilisés en chinois, japonais et coréen. Par exemple, si vous voulez représenter un ! dans une expression régulière du Web App Firewall en tant que caractère UTF-8, vous devez taper \x21. Si vous voulez inclure un á, vous devez taper \xC3\xA1.

> **Remarque :**
>
> Normalement, vous n'avez pas besoin de représenter les caractères ASCII au format UTF-8, mais lorsque ces caractères risquent de confondre un navigateur Web ou un système d'exploitation sous-jacent, vous pouvez utiliser la représentation UTF-8 du caractère pour éviter cette confusion. Par exemple, si une URL contient un espace, vous pouvez l'encoder en tant que x20 pour éviter de confondre certains navigateurs et logiciels de serveur Web.

Vous trouverez ci-dessous des exemples d'URL, de noms de champs de formulaire et d'expressions d'objet sécurisé contenant des caractères non-ASCII qui doivent être entrés en tant qu'expressions régulières au format PCRE à inclure dans la configuration du Web App Firewall. Chaque exemple montre en premier l'URL réelle, le nom du champ ou la chaîne d'expression, suivi d'une expression régulière au format PCRE.

- URL contenant des caractères ASCII étendus.

  URL réelle : `http://www.josénuñez.com`

  URL encodée : `^http://www\[.\]jos\xC3\xA9nu\xC3\xB1ez\[.\]com$`

- Une autre URL contenant des caractères ASCII étendus.

URL réelle : `http://www.example.de/trömso.html`

URL encodée : `^http://www[.]example\[.]de/tr\xC3\xB6mso[.]html$`

- Nom de champ de formulaire contenant des caractères ASCII étendus.

  `Actual Name: nome_do_usuário`

  Nom codé :`^nome_do_usu\xC3\xA1rio$`

- Expression d'objet sécurisée contenant des caractères ASCII étendus.

  Expression non encodée [A-Z]{3,6} ¥[1-9][0-9]{6,6}

  Expression codée : [A-Z]{3,6} \ xC2 \ xA5[1-9][0-9]{6,6}

Vous pouvez trouver un certain nombre de tables qui incluent l'ensemble du jeu de caractères Unicode et les encodages UTF-8 correspondants sur Internet. Un site Web utile contenant ces informations se trouve à l'URL suivante :

`http://www.utf8-chartable.de/unicode-utf8-table.pl`

Pour que les caractères du tableau de ce site Web s'affichent correctement, vous devez disposer d'une police Unicode appropriée installée sur votre ordinateur. Si vous ne le faites pas, l'affichage visuel du caractère peut être erroné. Même si vous n'avez pas de police appropriée installée pour afficher un caractère, la description et les codes UTF-8 et UTF-16 de cet ensemble de pages Web seront corrects.

Expressions PCRE inversées

En plus de faire correspondre le contenu contenant un motif, vous pouvez faire correspondre le contenu qui ne contient pas de motif à l'aide d'une expression PCRE inversée. Pour inverser une expression, il vous suffit d'inclure un point d'exclamation (!) suivi d'un espace blanc comme premier caractère de l'expression.

> **Remarque :** Si une expression est constituée uniquement d'un point d'exclamation sans aucune suite, le point d'exclamation est traité comme un caractère littéral, et non comme une syntaxe indiquant une expression inversée.

Les commandes de Web App Firewall suivantes prennent en charge les expressions PCRE inversées :

- URL de démarrage (URL)
- Refuser l'URL (URL)
- Cohérence des champs de formulaire (URL de l'action de formulaire)
- Cohérence des cookies (URL de l'action de formulaire)
- Faux de demande intersite (CSRF) (URL de l'action de formulaire)
- Scripting inter-site HTML (URL de l'action de formulaire)
- Format du champ (URL de l'action de formulaire)
- Type de champ (type)

- Champ confidentiel (URL)

Remarque : Si la vérification de sécurité contient un indicateur IsRegex ou une case à cocher, elle doit être définie sur YES ou cochée pour activer les expressions régulières dans le champ. Sinon, le contenu de ce champ est traité comme littéral et aucune expression régulière (inversée ou non) n'est analysée.

Noms non autorisés pour les profils de Web App Firewall

Les noms suivants sont attribués aux actions et profils intégrés sur l'appliance Citrix ADC et ne peuvent pas être utilisés comme noms pour un profil de Web App Firewall créé par l'utilisateur.

- AGRESSIVE
- ALLOW
- BASIC
- CLIENTAUTH
- COMPRESS
- CSSMINIFY
- DEFLATE
- DENY
- DNS-NOP
- DROP
- GZIP
- HTMLMINIFY
- IMGOPTIMIZE
- JSMINIFY
- MODERATE
- NOCLIENTAUTH
- NOCOMPRESS
- NONE
- NOOP
- NOREWRITE
- RESET
- SETASLEARNNSLOG_ACT
- SETNSLOGPARAMS_ACT
- SETSYSLOGPARAMS_ACT
- SETTMSESSPARAMS_ACT
- SETVPNPARAMS_ACT
- SET_PREAUTHPARAMS_ACT
- default_DNS64_action
- dns_default_act_Cachebypass

- dns_default_act_Drop
- nshttp_default_profile
- nshttp_default_strict_validation
- nstcp_default_Mobile_profile
- nstcp_default_XA_XD_profile
- nstcp_default_profile
- nstcp_default_tcp_interactive_stream
- nstcp_default_tcp_lan
- nstcp_default_tcp_lan_thin_stream
- nstcp_default_tcp_lfp
- nstcp_default_tcp_lfp_thin_stream
- nstcp_default_tcp_lnp
- nstcp_default_tcp_lnp_thin_stream
- nstcp_internal_apps

Statut et message d'erreur personnalisés pour l'objet d'erreur HTML, XML et JSON

August 20, 2021

Lorsque Citrix Web App Firewall détecte une violation, l'appliance gère le scénario d'erreur à l'aide d'une URL de redirection ou de l'objet erreur (importé dans le profil et activé). Si le scénario est géré à l'aide d'une configuration d'objet d'erreur, le profil WAF fournit un code et un message d'état de réponse personnalisés. Vous pouvez personnaliser les détails de l'erreur de réponse pour un objet d'erreur HTML, XML ou JSON dans le profil WAF.

> **Remarque :**
>
> Par défaut, le code d'erreur et le message d'erreur sont définis comme « 200 » et « OK » si les paramètres des objets d'erreur sont configurés.

Lors de la gestion des scénarios d'erreur, il est important que l'appliance réponde avec un code et un message d'état de réponse HTTP appropriés pour résoudre les problèmes. En fournissant un message d'état d'erreur personnalisé et un code d'état d'erreur personnalisé, l'appliance peut fournir une meilleure intervention de l'utilisateur pour résoudre un problème en cas de violation. Par exemple, si vous définissez le code d'erreur de réponse sur « 404 » et que le message d'état sur « Non trouvé », l'utilisateur peut inspecter le code d'état de la réponse et le message pour vérifier si une violation s'est produite. Cela peut aider l'utilisateur à filtrer les réponses contenant l'objet error.

Configurer un code d'état et un message personnalisés pour l'objet d'erreur HTML dans un profil WAF à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 set appfw profile <profile-name> -HTMLErrorStatusCode <value> -
     HTMLErrorStatusMessage <value> -useHTMLErrorObject ON
2 <!--NeedCopy-->
```

Exemple :

```
set appfw profile profile_1 -HTMLErrorStatusCode 404 -HTMLErrorStatusMessage
  "Not Found"  -useHTMLErrorObject ON
```

Configurer un code d'état personnalisé et un message pour un objet d'erreur XML dans un profil WAF à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 set appfw profile <profile-name> -XMLErrorStatusCode <value> -
     XMLErrorStatusMessage <value>
2 <!--NeedCopy-->
```

Exemple :

```
set appfw profile profile_1 -XMLErrorStatusCode 406 - XMLErrorStatusMessage
  "Not Acceptable"
```

Configurer un code d'état et un message personnalisés pour l'objet d'erreur JSON dans un profil WAF à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 set appfw profile <profile-name> -JSONErrorStatusCode <value> -
     JSONErrorStatusMessage <value>
2 <!--NeedCopy-->
```

Exemple :

```
set appfw profile profile_1 -JSONErrorStatusCode 500 - JSONErrorStatusMessage
  "Internal Server Error"
```


Configurer un code d'état et un message personnalisés pour un objet d'erreur HTML, JSON ou XML dans un profil WAF à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet d'informations, cliquez sur **Modifier**.
3. Dans la page **Créer un profil de Web App Firewall**, cliquez sur **Paramètres de profil dans** la section **Paramètres avancés** .
4. Dans la section **Paramètres du profil**, définissez les paramètres suivants.

   a. Objet d'erreur HTML. Sélectionnez l'option permettant de gérer des scénarios d'erreur à l'aide d'un objet d'erreur HTML. Importez l'objet erreur à partir d'une URL, d'un fichier ou d'un texte.
   b. Code d'état d'erreur HTML. Fournissez un code d'état d'erreur personnalisé.
   c. Message d'état d'erreur HTML. Fournissez un message d'erreur client.
5. Cliquez sur **OK** et **Terminé**.

> **Remarque :**
>
> La même procédure s'applique aux paramètres d'objets d'erreur personnalisés JSON et XML.



Étiquettes de stratégie

October 5, 2021

Une étiquette de stratégie se compose d'un ensemble de stratégies, d'autres étiquettes de stratégie et de banques de stratégies spécifiques au serveur virtuel. Le Web App Firewall évalue chaque stratégie liée à l'étiquette de stratégie par ordre de priorité. Si la stratégie correspond, elle filtre la connexion telle qu'elle est spécifiée dans le profil associé. Ensuite, il fait tout ce que spécifie le paramètre Goto, qui peut être de mettre fin à l'évaluation de la stratégie, d'accéder à la stratégie suivante ou d'accéder à la stratégie avec la priorité spécifiée. Si le paramètre Invoke est défini, il met fin au traitement de

l'étiquette de stratégie actuelle et commence à traiter l'étiquette de stratégie ou le serveur virtuel spécifié.

Pour créer une étiquette de stratégie de Web App Firewall à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw policylabel <labelName> http_req`
- `save ns config`

Exemple

L'exemple suivant crée une étiquette de stratégie nommée policylbl1.

```
1 add appfw policylabel policylbl1 http_req
2 save ns config
3 <!--NeedCopy-->
```

Pour lier une stratégie à une étiquette de stratégie à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `bind appfw policylabel <labelName> <policyName> <priority> [<gotoPriorityExpressi >] [-invoke (<labelType> <labelName>)]`
- `save ns config`

Exemple

L'exemple suivant lie la stratégie 1 à l'étiquette de stratégie policylbl1 avec une priorité de 1.

```
1 bind appfw policylabel policylbl1 policy1 1
2 save ns config
3 <!--NeedCopy-->
```

Pour configurer une étiquette de stratégie de Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Web App Firewall > Étiquettes de stratégie**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour ajouter une nouvelle étiquette de stratégie, cliquez sur **Ajouter**.

- Pour configurer une étiquette de stratégie existante, sélectionnez-la, puis cliquez sur **Ouvrir**.

La boîte de dialogue **Créer une étiquette de stratégie de Web App FirewallWeb App ou Configurer l'étiquette de stratégie de pare-feu** Web App s'ouvre. Les boîtes de dialogue sont presque identiques.

3. Si vous créez une nouvelle étiquette de stratégie, dans la boîte de dialogue Créer une étiquette de stratégie de Web App Firewall, tapez un nom pour votre nouvelle étiquette de stratégie.

   Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement, et peut comprendre de 1 à 127 lettres, chiffres et les symboles tiret (-), point (.) livre (#), espace (), at (@), égal (=), deux-points (:) et trait de soulignement (_).

4. Sélectionnez **Insérer une stratégie** pour insérer une nouvelle ligne et afficher une liste déroulante avec toutes les stratégies de Web App Firewall existantes.

5. Sélectionnez la stratégie que vous souhaitez lier à l'étiquette de stratégie ou sélectionnez Nouvelle stratégie pour créer une nouvelle stratégie et suivez les instructions de la section Pour créer et configurer une stratégie à l'aide de l'interface graphique. La stratégie que vous avez sélectionnée ou créée est insérée dans la liste des stratégies de Web App Firewall globalement liées.

6. Effectuez des ajustements supplémentaires.

   - Pour modifier la priorité de la stratégie, cliquez sur le champ pour l'activer, puis tapez une nouvelle priorité. Vous pouvez également sélectionner Régénérer les priorités pour renuméroter les priorités uniformément.
   - Pour modifier l'expression de stratégie, double-cliquez sur ce champ pour ouvrir la boîte de dialogue Configurer la stratégie de Web App Firewall, dans laquelle vous pouvez modifier l'expression de stratégie.
   - Pour définir l'expression Goto, double-cliquez sur le champ dans l'en-tête de colonne Goto Expression pour afficher la liste déroulante, dans laquelle vous pouvez choisir une expression.
   - Pour définir l'option Invoke, double-cliquez sur le champ dans l'en-tête de colonne Invoke pour afficher la liste déroulante, dans laquelle vous pouvez choisir une expression

7. Répétez les étapes 5 à 7 pour lier les stratégies de Web App Firewall supplémentaires souhaitées à l'étiquette de stratégie.

8. Cliquez sur **Créer** ou sur **OK**, puis cliquez sur **Fermer**. Un message apparaît dans la barre d'état indiquant que vous avez correctement créé ou modifié l'étiquette de stratégie.

Stratégies

January 21, 2021

Le pare-feu des applications Web utilise deux types de stratégies : les stratégies de pare-feu et les stratégies d'audit. Les stratégies de pare-feu contrôlent le trafic envoyé au Web App Firewall. Les stratégies d'audit contrôlent le serveur de journaux vers lequel les journaux du Web App Firewall sont envoyés.

Les stratégies de pare-feu peuvent être complexes car la règle de stratégie peut être composée de plusieurs expressions dans le langage d'expressions Citrix ADC, qui est un langage de programmation orienté objet à part entière capable de définir avec une extrême précision les connexions à filtrer. Étant donné que les stratégies de pare-feu fonctionnent dans le contexte du Web App Firewall, elles doivent répondre à certains critères liés au fonctionnement du pare-feu d'application Web et au trafic qu'il filtre de manière appropriée. Toutefois, tant que vous gardez ces critères à l'esprit, les stratégies de pare-feu sont similaires aux stratégies d'autres fonctionnalités de Citrix ADC. Les instructions ici ne visent pas à couvrir tous les aspects de l'écriture de stratégies de pare-feu, mais fournissent uniquement une introduction aux stratégies et couvrent les critères propres au Web App Firewall.

Les stratégies d'audit sont simples car la règle de stratégie est toujours ns_true. Vous devez uniquement spécifier le serveur de journaux auquel vous souhaitez envoyer les journaux, les niveaux de journalisation que vous souhaitez utiliser et quelques autres critères expliqués en détail.

Stratégies de Web App Firewall

October 5, 2021

Une stratégie de pare-feu est une règle associée à un profil. La règle est une expression ou un groupe d'expressions qui définissent les types de paires requête/réponse que le Web App Firewall doit filtrer en appliquant le profil. Les expressions de stratégie de pare-feu sont écrites dans le langage d'expressions Citrix ADC, un langage de programmation orienté objet doté de fonctionnalités spéciales pour prendre en charge des fonctions Citrix ADC spécifiques. Le profil est l'ensemble des actions que le Web App Firewall doit utiliser pour filtrer les paires requête/réponse qui correspondent à la règle.

Les stratégies de pare-feu vous permettent d'attribuer différentes règles de filtrage à différents types de contenu Web. Tous les contenus Web ne se ressemblent pas. Un site Web simple qui n'utilise aucun script complexe et qui accède et ne traite aucune donnée privée peut nécessiter uniquement le niveau de protection fourni par un profil créé avec des valeurs par défaut de base. Le contenu Web qui contient des formulaires Web améliorés par JavaScript ou qui accède à une base de données SQL

nécessite probablement une protection plus personnalisée. Vous pouvez créer un profil différent pour filtrer ce contenu et créer une stratégie de pare-feu distincte qui peut déterminer les demandes qui tentent d'accéder à ce contenu. Vous associez ensuite l'expression de stratégie à un profil que vous avez créé et vous liez globalement la stratégie pour la mettre en œuvre.

Le Web App Firewall traite uniquement les connexions HTTP et utilise donc un sous-ensemble du langage des expressions Citrix ADC global. Les informations ici sont limitées aux rubriques et exemples susceptibles d'être utiles lors de la configuration du Web App Firewall. Vous trouverez ci-dessous des liens vers des informations supplémentaires et des procédures relatives aux stratégies de pare-feu :

- Pour connaître les procédures expliquant comment créer et configurer une stratégie, reportez-vous à la section Création et configuration de stratégies de Web App Firewall.
- Pour obtenir une procédure expliquant en détail comment créer une règle de stratégie (expression), reportez-vous à la section Pour créer ou configurer une règle de Web App Firewall (expression).
- Pour obtenir une procédure expliquant comment utiliser la boîte de dialogue Ajouter une expression pour créer une règle de stratégie, reportez-vous à la section Pour ajouter une règle de pare-feu (expression) à l'aide de la boîte de dialogue Ajouter une expression.
- Pour obtenir une procédure expliquant comment afficher les liaisons actuelles d'une stratégie, reportez-vous à la section Affichage des liaisons d'une stratégie de pare-feu.
- Pour connaître les procédures expliquant comment lier une stratégie de Web App Firewall, reportez-vous à la section Liaison des stratégies de Web App Firewall.
- Pour plus d'informations sur le langage des expressions Citrix ADC, consultez Politiques et expressions.

> **Remarque**
>
> Web App Firewall évalue les stratégies en fonction de la priorité configurée et des expressions goto. À la fin de l'évaluation de la stratégie, la dernière stratégie évaluée à true est utilisée et la configuration de sécurité du profil correspondant est appelée pour traiter la demande.
>
> Par exemple, imaginez un scénario dans lequel il existe deux stratégies.
>
> - Policy_1 est une stratégie générique avec expression=NS_true et possède un profile_1 correspondant qui est un profil de base. La priorité est fixée à 100.
> - Policy_2 est plus spécifique avec expression=HTTP.REQ.URL.contains (« XYZ ») et a un profile_2 correspondant qui est un profil avancé. L'expression GoTo est définie sur NEXT et la priorité est définie sur 95, ce qui est une priorité supérieure à celle de Policy_1.
>
> Dans ce scénario, si la chaîne cible « XYZ » est détectée dans l'URL de la demande traitée, la correspondance Policy_2 est déclenchée car elle a une priorité plus élevée, même si Policy_1 est également une correspondance. Toutefois, conformément à la configuration de l'expression GoTo de Policy_2, l'évaluation de la stratégie se poursuit et la prochaine policy_1 est également

> traitée. À la fin de l'évaluation de la stratégie, Policy_1 évalue la valeur true et les vérifications de sécurité de base configurées dans Profile_1 sont appelées.
>
> Si la stratégie Policy_2 est modifiée et que l'expression GoTo passe de **NEXT** à **END**, la demande traitée qui contient la chaîne cible « XYZ » déclenche la correspondance Policy_2 en raison de la priorité et, conformément à la configuration de l'expression GoTo, l'évaluation de la stratégie se termine à ce point. Policy_2 est évalué comme vrai et les vérifications de sécurité avancées configurées dans Profile_2 sont appelées.
>
> **FIN SUIVANTE**
>
> L'évaluation des politiques se fait en un seul passage. Une fois que l'évaluation de la stratégie est terminée pour la demande et que les actions de profil correspondantes sont invoquées, la demande ne passe pas par une autre ronde d'évaluation de la stratégie.

Création et configuration de stratégies Web App Firewall

September 8, 2021

Une stratégie de pare-feu comprend deux éléments : une *règle*et un *profil*associé. La règle sélectionne le trafic HTTP correspondant aux critères que vous avez définis et envoie ce trafic au Web App Firewall pour filtrage. Le profil contient les critères de filtrage utilisés par le Web App Firewall.

La règle de stratégie consiste en une ou plusieurs expressions dans le langage d'expressions Citrix ADC. La syntaxe des expressions Citrix ADC est un langage de programmation puissant orienté objet qui vous permet de désigner précisément le trafic que vous souhaitez traiter avec un profil spécifique. Pour les utilisateurs qui ne connaissent pas la syntaxe du langage des expressions Citrix ADC ou qui préfèrent configurer leur appliance Citrix ADC à l'aide d'une interface Web, l'interface graphique fournit deux outils : le menu **Préfixe** et la boîte de dialogue **Ajouter une expression** . Les deux vous aident à écrire des expressions qui sélectionnent exactement le trafic que vous souhaitez traiter. Les utilisateurs expérimentés qui connaissent parfaitement la syntaxe peuvent préférer utiliser la ligne de commande Citrix ADC pour configurer leurs appliances Citrix ADC.

> **Remarque :**
>
> Outre la syntaxe des expressions par défaut, pour des raisons de compatibilité ascendante, le système d'exploitation Citrix ADC prend en charge la syntaxe des expressions classiques Citrix ADC sur les appliances Citrix ADC Classic et nCore et les appliances virtuelles. Les expressions classiques ne sont pas prises en charge sur les appliances Citrix ADC Cluster et les appliances virtuelles. Les utilisateurs actuels de Citrix ADC qui souhaitent migrer des configurations existantes vers le cluster Citrix ADC doivent migrer toutes les stratégies qui contiennent des expressions classiques vers la syntaxe des expressions par défaut.

Pour plus d'informations sur les langages d'expressions Citrix ADC, reportez-vous à la section Stratégies et expressions.

Vous pouvez créer une stratégie de pare-feu à l'aide de l'interface graphique ou de la ligne de commande Citrix ADC.

Pour créer et configurer une stratégie à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw policy <name><rule> <profileName>`
- `save ns config`

Exemple

L'exemple suivant montre comment ajouter une stratégie nommée pl-blog, avec une règle qui intercepte tout le trafic vers ou depuis l'hôte blog.example.com, et associe cette stratégie au profil pr-blog. Il s'agit d'une stratégie appropriée pour protéger un blog hébergé sur un nom d'hôte spécifique.

```
1 add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com
     ")" pr-blog
2 <!--NeedCopy-->
```

Pour créer et configurer une stratégie à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Web App Firewall** > **Stratégies**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une stratégie de pare-feu, cliquez sur **Ajouter**. La **stratégie Create Web App Firewall** s'affiche.
   - Pour modifier une stratégie de pare-feu existante, sélectionnez-la, puis cliquez sur **Modifier**.

   La stratégie **Créer une stratégie de Web App Firewall** ou **Configurer la stratégie de pare-feu Web App** s'affiche.
3. Si vous créez une stratégie de pare-feu, dans la boîte de dialogue **Créer une stratégie de Web App Firewall**, zone de texte Nom de la stratégie, tapez un nom pour votre nouvelle stratégie.

   Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement. Il peut être composé de 1 à 128 lettres, chiffres et le trait d'union (-), point (.) livre (#), espace (), à (@), égal à (=), deux-points (:) et soulignement (_).

   Si vous configurez une stratégie de pare-feu existante, ce champ est en lecture seule. Vous ne pouvez pas le modifier.

4. Sélectionnez le profil que vous souhaitez associer à cette stratégie dans la liste déroulante Profil. Vous pouvez créer un profil à associer à votre stratégie en cliquant sur Nouveau, et vous pouvez modifier un profil existant en cliquant sur Modifier.
5. Dans la zone de texte Expression, créez une règle pour votre stratégie.
    - Vous pouvez saisir une règle directement dans la zone de texte.
    - Vous pouvez cliquer sur Préfixe pour sélectionner le premier terme de votre règle et suivre les instructions.
    - Vous pouvez cliquer sur Ajouter pour ouvrir la boîte de dialogue Ajouter une expression et l'utiliser pour construire la règle.
6. Cliquez sur **Créer** ou sur **OK**, puis cliquez sur **Fermer**.

Pour créer ou configurer une règle de Web App Firewall (expression)

La règle de stratégie, également appelée *expression*, définit le trafic Web que le Web App Firewall filtre à l'aide du profil associé à la stratégie. Comme les autres règles de stratégie (ou *expressions*) Citrix ADC, les règles Web App Firewall utilisent la syntaxe des expressions Citrix ADC. Cette syntaxe est puissante, flexible et extensible. Il est trop complexe pour être décrit complètement dans cet ensemble d'instructions. Vous pouvez utiliser la procédure suivante pour créer une règle de stratégie de pare-feu simple, ou vous pouvez la lire comme un aperçu du processus de création de stratégie.

1. Si ce n'est pas déjà fait, accédez à l'emplacement approprié dans l'assistant **Web App Firewall** ou dans l'interface graphique Citrix ADC pour créer votre règle de stratégie :
    - Si vous configurez une stratégie dans l'assistant **Web App Firewall**, dans le volet de navigation, cliquez sur **Web App Firewall**, puis dans le volet d'informations, cliquez sur **Assistant Web App Firewall**, puis accédez à l'écran **Spécifier une règle** .
    - Si vous configurez une stratégie manuellement, dans le volet de navigation, développez **Web App Firewall**, **Stratégies**, puis **Pare-feu**. Dans le volet d'informations, pour créer une stratégie, cliquez sur **Ajouter**. Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Ouvrir**.
2. Sur l'écran **Spécifier une règle**, la boîte de dialogue **Créer un profil de Web App FirewallWeb App ou la boîte de dialogue Configurer le profil de pare-feu**Web App, cliquez sur**Préfixe**, puis choisissez le préfixe de votre expression dans la liste déroulante. Vos choix sont les suivants :
    - **HTTP.** Choisissez un protocole HTTP si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole.
    - **DIT.** Choisissez des sites Web protégés si vous souhaitez examiner certains aspects de la demande concernant le destinataire de la demande.
    - **CLIENT.** Choisissez un client qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'expéditeur de la demande.

- **SERVEUR.** Choisissez un client auquel la demande a été envoyée et si vous souhaitez examiner certains aspects du destinataire de la demande.

Une fois que vous avez choisi un préfixe, le Web App Firewall affiche une fenêtre d'invite en deux parties qui affiche les choix suivants possibles en haut, et une brève explication de la signification du choix sélectionné en bas.

3. Choisissez votre prochain trimestre.

   Si vous avez choisi le protocole HTTP comme préfixe, votre seul choix est REQ, qui spécifie la paire Request/Réponse. (Le Web App Firewall fonctionne sur la demande et la réponse en tant qu'unité plutôt que sur chacune d'elles séparément.) Si vous avez choisi un autre préfixe, vos choix sont plus variés. Pour obtenir de l'aide sur un choix spécifique, cliquez une fois sur ce choix pour afficher des informations le concernant dans la fenêtre d'invite inférieure.

   Lorsque vous avez choisi le terme souhaité, double-cliquez dessus pour l'insérer dans la fenêtre **Expression** .

4. Tapez une période après le terme que vous venez de choisir. Vous êtes ensuite invité à choisir votre prochain terme, comme décrit à l'étape précédente. Lorsqu'un terme nécessite que vous saisissez une valeur, renseignez la valeur appropriée. Par exemple, si vous choisissez HTTP.REQ.HEADER (« »), tapez le nom de l'en-tête entre les guillemets.

5. Continuez à choisir des termes à partir des invites et à renseigner toutes les valeurs nécessaires, jusqu'à ce que votre expression soit terminée.

   Voici quelques exemples d'expressions à des fins spécifiques.

   - **Hôte Web spécifique.** Pour faire correspondre le trafic d'un hôte Web particulier :

     ```
     1 HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
     2 <!--NeedCopy-->
     ```

     Pour `shopping.example.com`, remplacez le nom de l'hôte Web auquel vous souhaitez faire correspondre.

   - **Dossier ou répertoire Web spécifique.** Pour faire correspondre le trafic provenant d'un dossier ou d'un répertoire particulier sur un hôte Web :

     ```
     1 HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")
     2 <!--NeedCopy-->
     ```

     Pour www.example.com, remplacez le nom de l'hôte Web. Pour le dossier, remplacez le dossier ou le chemin d'accès au contenu que vous souhaitez faire correspondre. Par exemple, si votre panier se trouve dans un dossier appelé /solutions/orders, vous remplacez cette chaîne par un dossier.

   - **Type de contenu spécifique : images GIF.** Pour correspondre aux images au format GIF :


```
HTTP.REQ.URL.ENDSWITH(".png")
<!--NeedCopy-->
```

Pour correspondre aux images d'autres formats, remplacez une autre chaîne à la place de .png.

- **Type de contenu spécifique : scripts.** Pour correspondre à tous les scripts CGI situés dans le répertoire CGI-BIN :

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")
<!--NeedCopy-->
```

Pour faire correspondre tous les JavaScript aux extensions .js :

```
HTTP.REQ.URL.ENDSWITH(".js")
<!--NeedCopy-->
```

Pour plus d'informations sur la création d'expressions de stratégie, voir Stratégies et expressions.

> **Remarque :**
>
> Si vous utilisez la ligne de commande pour configurer une stratégie, n'oubliez pas d'échapper aux guillemets doubles dans les expressions Citrix ADC. Par exemple, l'expression suivante est correcte si elle est entrée dans l'interface graphique :

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
<!--NeedCopy-->
```

Si vous êtes entré sur la ligne de commande, vous devez toutefois taper la commande suivante :

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
<!--NeedCopy-->
```

Pour ajouter une règle de pare-feu (expression) à l'aide de la boîte de dialogue Ajouter une expression

La boîte de dialogue **Ajouter une expression** (également appelée Éditeur d'expression) aide les utilisateurs qui ne connaissent pas le langage des expressions Citrix ADC à construire une stratégie correspondant au trafic qu'ils veulent filtrer.

1. Si ce n'est pas déjà fait, accédez à l'emplacement approprié dans l'assistant **Web App Firewall** ou dans l'interface graphique Citrix ADC :

- Si vous configurez une stratégie dans l'assistant **Web App Firewall**, dans le volet de navigation, cliquez sur **Web App Firewall**, puis dans le volet d'informations, cliquez sur **Assistant Web App Firewall**, puis accédez à l'écran **Spécifier une règle** .
- Si vous configurez une stratégie manuellement, dans le volet de navigation, développez **Web App Firewall**, **Stratégies**, puis **Pare-feu**. Dans le volet d'informations, pour créer une stratégie, cliquez sur **Ajouter**. Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Ouvrir**.

2. Sur l'écran **Spécifier une règle**, dans la boîte de dialogue **Créer un profil de Web App Firewall** ou dans la boîte de dialogue **Configurer le profil de Web App Firewall**, cliquez sur **Ajouter**.
3. Dans la boîte de **dialogue Ajouter une expression**, dans la zone Construire une expression, dans la première zone de liste, choisissez l'un des préfixes suivants :
   - **HTTP.** Choisissez le protocole HTTP si vous souhaitez examiner certains aspects de la requête qui se rapportent au protocole HTTP. Le choix par défaut.
   - **DIT.** Choisissez des sites Web protégés si vous souhaitez examiner certains aspects de la demande concernant le destinataire de la demande.
   - **CLIENT.** Choisissez l'ordinateur qui a envoyé la demande si vous souhaitez examiner certains aspects de l'expéditeur de la demande.
   - **SERVEUR.** Choisissez l'ordinateur auquel la demande a été envoyée et examinez certains aspects du destinataire de la demande.
4. Dans la deuxième zone de liste, choisissez votre prochain terme. Les termes disponibles diffèrent en fonction du choix que vous avez fait à l'étape précédente, car la boîte de dialogue ajuste automatiquement la liste pour contenir uniquement les termes valides pour le contexte. Par exemple, si vous avez sélectionné HTTP dans la zone de liste précédente, le seul choix est REQ, pour les demandes. Étant donné que le Web App Firewall traite les demandes et les réponses associées comme une seule unité et filtre les deux, vous n'avez pas besoin de réponses spécifiques séparément. Une fois que vous avez choisi votre deuxième trimestre, une troisième zone de liste apparaît à droite du second. La fenêtre d'aide affiche une description du deuxième terme et la fenêtre **Aperçu de l'expression** affiche votre expression.
5. Dans la troisième zone de liste, choisissez le terme suivant. Une nouvelle zone de liste apparaît à droite, et la fenêtre d'aide change pour afficher une description du nouveau terme. La fenêtre **Aperçu de l'expression** est mise à jour pour afficher l'expression telle que vous l'avez spécifiée à ce moment-là.
6. Continuez à choisir des termes et lorsque vous y êtes invité à remplir des arguments, jusqu'à ce que votre expression soit terminée. Si vous commettez une erreur ou souhaitez modifier votre expression après avoir déjà sélectionné un terme, vous pouvez simplement choisir un autre terme. L'expression est modifiée et tous les arguments ou autres termes que vous avez ajoutés après le terme que vous avez modifié sont effacés.
7. Lorsque vous avez fini de construire votre expression, cliquez sur **OK** pour fermer la boîte de dialogue **Ajouter une expression** . Votre expression est insérée dans la zone de texte **Expression**

.

Liaison des stratégies de Web App Firewall

August 20, 2021

Après avoir configuré vos stratégies de Web App Firewall, vous les liez à Global ou à un point de liaison pour les mettre en œuvre. Après la liaison, toute demande ou réponse qui correspond à une stratégie de Web App Firewall est transformée par le profil associé à cette stratégie.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel entier positif. Dans le système d'exploitation Citrix ADC, les priorités de stratégie fonctionnent dans l'ordre inverse - plus le nombre est élevé, plus la priorité est faible.

Étant donné que la fonctionnalité de pare-feu d'application Web n'implémente que la première stratégie correspondant à une demande, et non les stratégies supplémentaires qu'elle pourrait également correspondre, la priorité de stratégie est importante pour obtenir les résultats que vous souhaitez obtenir. Si vous attribuez à votre première stratégie une priorité faible (par exemple 1000), vous configurez le Web App Firewall pour l'exécuter uniquement si d'autres stratégies avec une priorité supérieure ne correspondent pas à une demande. Si vous attribuez à votre première stratégie une priorité élevée (telle que 1), vous configurez le Web App Firewall pour qu'il l'exécute en premier et ignorez toutes les autres stratégies qui peuvent également correspondre. Vous pouvez vous laisser beaucoup de place pour ajouter d'autres stratégies dans n'importe quel ordre, sans avoir à réaffecter des priorités, en définissant des priorités avec des intervalles de 50 ou 100 entre chaque stratégie lorsque vous liez vos stratégies.

Pour plus d'informations sur les stratégies de liaison sur l'appliance Citrix ADC, reportez-vous à la section « Politiques et expressions ». «

Pour lier une stratégie de Web App Firewall à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `bind appfw global <policyName>`
- `bind appfw profile <profile_name> -crossSiteScripting data`

Exemple

L'exemple suivant lie la stratégie nommée pl-blog et lui attribue une priorité de 10.


```
bind appfw global pl-blog 10
save ns config
<!--NeedCopy-->
```

Configurer les expressions de journal

La prise en charge de l'expression de journal pour la liaison du Web App Firewall est ajoutée pour consigner les informations d'en-tête HTTP lorsqu'une violation se produit.

L'expression de journal est liée au profil Application, et la liaison contient l'expression qui doit être évaluée et envoyée aux frameworks de journalisation en cas de violation.

L'enregistrement du journal des violations du Web App Firewall avec les informations d'en-tête http est enregistré. Vous pouvez spécifier une expression de journal personnalisée et cela aide à l'analyse et au diagnostic lorsque des violations sont générées pour le flux actuel (demande/réponse).

Exemple de configuration

```
bind appfw profile <profile> -logexpression <string> <expression>
add policy expression headers "" HEADERS(100):"+HTTP.REQ.FULL_HEADER"
add policy expression body_100 ""BODY:"+HTTP.REQ.BODY(100)"
bind appfw profile test -logExpression log_body body_100
bind appfw profile test -logExpression log_headers  headers
bind appfw profile test -logExpression ""URL:"+HTTP.REQ.URL+" IP:"+
   CLIENT.IP.SRC"
<!--NeedCopy-->
```

Exemples de journaux

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
   .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
   POST request=http://10.217.222.44/test/credit.html msg= HEADERS(100)
   :POST /test/credit.html HTTP/1.1^M User-Agent: curl/7.24.0 (amd64-
   portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Host:
    10.217.222.44^M Accept: /^M Content-Length: 33^M Content-Type:
   application/x-www-form-urlencoded^M ^M  cn1=58 cn2=174 cs1=test cs2=
   PPE1 cs4=ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```



```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=BODY:ata=
    asdadasdasdasddddddddddddddd cn1=59 cn2=174 cs1=test cs2=PPE1 cs4=
    ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=URL:/test/
    credit.html IP:10.217.222.128 cn1=60 cn2=174 cs1=test cs2=PPE1 cs4=
    ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Other violation logs
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_STARTURL|6|src=10.217.222.128 spt=26409 method=POST
    request=http://10.217.222.44/test/credit.html msg=Disallow Illegal
    URL. cn1=61 cn2=174 cs1=test cs2=PPE1 cs4=ALERT cs5=2017 act=not
    blocked
<!--NeedCopy-->
```

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_SAFECOMMERCE|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=Maximum
    number of potential credit card numbers seen cn1=62 cn2=174 cs1=test
     cs2=PPE1 cs4=ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

Remarque

1. Seule la prise en charge des journaux d'audit est disponible. La prise en charge du flux de données et de la visibilité dans les informations de sécurité serait ajoutée dans les futures versions.
2. Si des journaux d'audit sont générés, seuls 1024 octets de données peuvent être générés par message de journal.
3. Si le flux de journaux est utilisé, les limites sont basées sur la taille maximale prise en charge des limitations de taille du protocole de journalisation du flux de journaux/ipfix. La taille maximale de prise en charge du flux de journaux est supérieure à 1024 octets.

Pour lier une stratégie Web App Firewall à l'aide de l'interface graphique

1. Procédez comme suit :
   - Accédez à **Sécurité** > **Web App Firewall** et, dans le volet d'informations, cliquez sur Gestionnaire de stratégies de pare-feu des applications Web.
   - Accédez à **Sécurité** > **Web App Firewall** > **Stratégies > Stratégiesde pare-feu**, puis dans le volet d'informations, cliquez sur**Gestionnaire de stratégies**.
2. Dans la boîte de dialogue **Gestionnaire de stratégies de Web App Firewall**, choisissez le point de liaison auquel vous souhaitez lier la stratégie dans la liste déroulante. Les choix sont les suivants :
   - **Remplacer Global.** Les stratégies liées à ce point de liaison traitent tout le trafic provenant de toutes les interfaces de l'appliance Citrix ADC et sont appliquées avant toute autre stratégie.
   - **Serveur virtuel LB.** Les stratégies liées à un serveur virtuel d'équilibrage de charge sont appliquées uniquement au trafic traité par ce serveur virtuel d'équilibrage de charge et sont appliquées avant toute stratégie globale par défaut. Après avoir sélectionné Serveur virtuel LB, vous devez également sélectionner le serveur virtuel d'équilibrage de charge spécifique auquel vous souhaitez lier cette stratégie.
   - **Serveur virtuel CS.** Les stratégies liées à un serveur virtuel de commutation de contenu sont appliquées uniquement au trafic traité par ce serveur virtuel de commutation de contenu et sont appliquées avant toute stratégie globale par défaut. Après avoir sélectionné CS Virtual Server, vous devez également sélectionner le serveur virtuel de commutation de contenu spécifique auquel vous souhaitez lier cette stratégie.
   - **Global par défaut.** Les stratégies liées à ce point de liaison traitent tout le trafic provenant de toutes les interfaces de l'appliance Citrix ADC.
   - **Étiquette de stratégie.** Les stratégies liées à un trafic de traitement d'étiquette de stratégie que l'étiquette de stratégie leur achemine. L'étiquette de stratégie contrôle l'ordre dans lequel les stratégies sont appliquées à ce trafic.
   - **Aucun.** Ne liez pas la stratégie à un point de liaison.
3. Cliquez sur **Continuer**. Une liste des stratégies de Web App Firewall existantes s'affiche.
4. Sélectionnez la stratégie que vous souhaitez lier en cliquant dessus.
5. Effectuez des ajustements supplémentaires à la liaison.
   - Pour modifier la priorité de stratégie, cliquez sur le champ pour l'activer, puis tapez une nouvelle priorité. Vous pouvez également sélectionner Régénérer les priorités pour renuméroter les priorités uniformément.
   - Pour modifier l'expression de stratégie, double-cliquez sur ce champ pour ouvrir la boîte de dialogue **Configurer la stratégie de Web App Firewall**, dans laquelle vous pouvez modifier l'expression de stratégie.
   - Pour définir l'expression Goto, double-cliquez sur **le champ** dans l'en-tête de colonne Optimer l'expression pour afficher la liste déroulante, dans laquelle vous pouvez choisir une

expression.
- Pour définir l'option Invoquer, double-cliquez sur le champ dans l'en-tête de colonne Invoquer pour afficher la liste déroulante, dans laquelle vous pouvez choisir une expression

6. Répétez les étapes 3 à 6 pour ajouter toutes les stratégies de Web App Firewall supplémentaires que vous souhaitez lier globalement.
7. Cliquez sur **OK**. Un message apparaît dans la barre d'état indiquant que la stratégie a été liée avec succès.

Affichage d'une liaison de stratégie

January 21, 2021

Vous pouvez vérifier rapidement quelles liaisons sont en place pour n'importe quelle stratégie de pare-feu en affichant les liaisons dans l'interface graphique.

Pour afficher les liaisons d'une stratégie de Web App Firewall

1. Accédez à **Sécurité > Citrix Web App Firewall > Stratégies > Stratégies de pare-feu**
2. Dans le volet d'informations, sélectionnez la stratégie à vérifier, puis cliquez sur Afficher les liaisons. La boîte de message Détails de liaison pour la stratégie : Stratégie s'affiche, avec une liste de liaisons pour la stratégie sélectionnée.
3. Cliquez sur **Fermer**.

Informations supplémentaires sur les stratégies de Web App Firewall

January 21, 2021

Vous trouverez ci-dessous des informations supplémentaires sur certains aspects des stratégies de Web App Firewall que les administrateurs système qui gèrent le pare-feu Web App peuvent avoir besoin de connaître.

Comportement correct mais inattendu

La sécurité des applications Web et les sites Web modernes sont complexes. Dans un certain nombre de scénarios, une stratégie Citrix ADC peut entraîner le comportement du Web App Firewall dans certaines situations différent de celui d'un utilisateur familier avec les stratégies normalement prévu. Voici un certain nombre de cas où le Web App Firewall peut se comporter de manière inattendue.

- **Demande avec un en-tête HTTP Host manquant et une URL absolue.** Lorsqu'un utilisateur envoie une demande, dans la majorité des cas, l'URL de la demande est relative. Autrement dit, il prend comme point de départ l'URL du référent, l'URL où se trouve le navigateur de l'utilisateur lorsqu'il envoie la requête. Si une requête est envoyée sans en-tête Host et avec une URL relative, la demande est normalement bloquée à la fois parce qu'elle enfreint la spécification HTTP et parce qu'une requête qui ne parvient pas à spécifier l'hôte peut, dans certaines circonstances, constituer une attaque. Toutefois, si une requête est envoyée avec une URL absolue, même si l'en-tête Host est manquant, la demande contourne le Web App Firewall et est transmise au serveur Web. Bien qu'une telle requête viole la spécification HTTP, elle ne constitue pas une menace possible car une URL absolue contient l'hôte.

Règles d'audit

January 21, 2021

Les stratégies d'audit déterminent les messages générés et consignés au cours d'une session de Web App Firewall. Les messages sont enregistrés au format SYSLOG sur le serveur NSLOG local ou sur un serveur de journalisation externe. Différents types de messages sont enregistrés en fonction du niveau de journalisation sélectionné.

Pour créer une stratégie d'audit, vous devez d'abord créer un serveur NSLOG ou un serveur SYSLOG. Et puis vous créez la stratégie et spécifiez le type de journal et le serveur vers lequel les journaux sont envoyés.

Pour créer un serveur d'audit à l'aide de l'interface de ligne de commande

Vous pouvez créer deux types différents de serveur d'audit : un serveur NSLOG ou un serveur SYSLOG. Les noms des commandes sont différents, mais les paramètres des commandes sont les mêmes.

Pour créer un serveur d'audit, à l'invite de commandes, tapez les commandes suivantes :

- `add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat (MMDDYYYY | DDMMYYYY)] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]`
- `save ns config`

Exemple

L'exemple suivant crée un serveur syslog nommé syslog1 à l'adresse IP 10.124.67.91, avec des niveaux de journalisation d'urgence, critique et avertissement, fonction de journalisation définie sur LOCAL1, qui enregistre toutes les connexions TCP :

```
1 add audit syslogAction syslog1 10.124.67.91 -logLevel emergency
     critical warning -logFacility
2 LOCAL1 -tcp ALL
3 save ns config
4 <!--NeedCopy-->
```

Pour modifier ou supprimer un serveur d'audit à l'aide de l'interface de ligne de commande

- Pour modifier un serveur d'audit, tapez la commande set audit <type>, le nom du serveur d'audit et les paramètres à modifier, avec leurs nouvelles valeurs.
- Pour supprimer un serveur d'audit, tapez la commande rm audit <type> et le nom du serveur d'audit.

Exemple

L'exemple suivant modifie le serveur syslog nommé syslog1 pour ajouter des erreurs et des alertes au niveau du journal :

```
1 set audit syslogAction syslog1 10.124.67.91 -logLevel emergency
     critical warning alert error
2 -logFacility LOCAL1 -tcp ALL
3 save ns config
4 <!--NeedCopy-->
```

Pour créer ou configurer un serveur d'audit à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Citrix Web App Firewall** > **Stratégies** > **Audit** > **Nslog**.
2. Dans la page Audit Nslog, cliquez sur l'onglet **Serveurs**.
3. Procédez comme suit :
   - Pour ajouter un nouveau serveur d'audit, cliquez sur **Ajouter**.
   - Pour modifier un serveur d'audit existant, sélectionnez le serveur, puis cliquez sur **Modifier**.
4. Dans la page **Créer un serveur d'audit**, définissez les paramètres suivants :

- Nom
- Type de serveur
- Adresse IP
- Port
- Niveaux de journalisation
- Installation de journaux
- Format de la date
- Fuseau horaire
- Journalisation TCP
- Journalisation ACL
- Messages de journal configurables par l'utilisateur
- Journalisation de AppFlow
- Journalisation NAT à grande échelle
- Journalisation des messages ALG
- Journalisation des abonnés
- Interception SSL
- filtrage d'URL
- Journalisation de l'inspection du contenu

5. Cliquez sur **Créer** et **Fermer**.



Pour créer une stratégie d'audit à l'aide de l'interface de ligne de commande

Vous pouvez créer une stratégie NSLOG ou SYSLOG. Le type de stratégie doit correspondre au type de serveur. Les noms des commandes des deux types de stratégie sont différents, mais les paramètres des commandes sont les mêmes.

À l'invite de commandes, tapez les commandes suivantes :

- `add audit syslogPolicy <name> <-rule > <action>`
- `save ns config`

Exemple

L'exemple suivant crée une stratégie nommée SysLogp1 qui enregistre le trafic du Web App Firewall sur un serveur syslog nommé syslog1.

```
add audit syslogPolicy syslogP1 rule "ns_true"action syslog1
save ns config
```

Pour configurer une stratégie d'audit à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set audit syslogPolicy <name> [-rule <expression>] [-action <string>]`
- `save ns config`

Exemple

L'exemple suivant modifie la stratégie nommée SysLogp1 pour consigner le trafic du Web App Firewall sur un serveur syslog nommé syslog2.

```
set audit syslogPolicy syslogP1 rule "ns_true"action syslog2
save ns config
```

Pour configurer une stratégie d'audit à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Citrix Web App Firewall** > **Stratégies**.
2. Dans le volet d'informations, cliquez sur **Audit Nslog Policy**.
3. Dans la page Audit Nslog, cliquez sur **l'onglet Stratégies** et effectuez l'une des opérations suivantes :
   - Pour ajouter une nouvelle stratégie, cliquez sur **Ajouter**.
   - Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Modifier**.

4. Dans la page **Créer une stratégie Nslog d'audit**, définissez les paramètres suivants :
   - Nom
   - Type d'audit
   - Type d'expression
   - Serveur
5. Cliquez sur **Créer**.



Importations

January 21, 2021

Plusieurs fonctionnalités de pare-feu d'application Web utilisent des fichiers externes que vous téléchargez sur le pare-feu d'application Web lorsque vous le configurez. À l'aide de l'interface graphique, vous gérez ces fichiers dans le volet Importations, qui comporte quatre onglets correspondant aux quatre types de fichiers que vous pouvez importer : objets d'erreur HTML, objets d'erreur XML, schémas XML et fichiers WSDL (Web Services Description Language). À l'aide de la ligne de commande Citrix ADC, vous pouvez importer ces types de fichiers, mais vous ne pouvez pas les exporter.

Objet d'erreur HTML

Lorsqu'une connexion d'un utilisateur à une page HTML ou Web 2.0 est bloquée, ou qu'un utilisateur demande une page HTML ou Web 2.0 inexistante, le Web App Firewall envoie une réponse d'erreur HTML au navigateur de l'utilisateur. Lors de la configuration de la réponse d'erreur que le Web App Firewall doit utiliser, vous avez deux choix :

- Vous pouvez configurer une URL de redirection, qui peut être hébergée sur n'importe quel serveur Web auquel les utilisateurs ont également accès. Par exemple, si vous avez une page d'erreur personnalisée sur votre serveur Web, 404.html, vous pouvez configurer le Web App Firewall pour rediriger les utilisateurs vers cette page lorsqu'une connexion est bloquée.
- Vous pouvez configurer un objet d'erreur HTML, qui est une page Web HTML hébergée sur le Web App Firewall lui-même. Si vous choisissez cette option, vous devez télécharger l'objet d'erreur HTML dans le Web App Firewall. Vous le faites dans le volet Importations, sous l'onglet Objet d'erreur HTML.

L'objet d'erreur doit être un fichier HTML standard qui ne contient aucune syntaxe autre que HTML, à l'exception des variables de personnalisation de l'objet d'erreur du Web App Firewall. Il ne peut pas contenir de scripts CGI, de code analysé par le serveur ou de code PHP. Les variables de personnalisation vous permettent d'intégrer des informations de dépannage dans l'objet d'erreur que l'utilisateur reçoit lorsqu'une demande est bloquée. Bien que la plupart des demandes bloquées par le Web App Firewall soient illégitimes, même un pare-feu Web App correctement configuré peut parfois bloquer les demandes légitimes, en particulier lorsque vous le déployez pour la première fois ou après avoir apporté des modifications importantes à vos sites Web protégés. En intégrant des informations dans la page d'erreur, vous fournissez à l'utilisateur les informations qu'il doit fournir à la personne du support technique afin que tous les problèmes puissent être résolus.

Les variables de personnalisation de la page d'erreur du Web App Firewall sont les suivantes :

- $ {NS_TRANSACTION_ID}. ID de transaction attribué par le Web App Firewall à cette transaction.
- $ {NS_APPFW_SESSION_ID}. ID de session de Web App Firewall.
- $ {NS_APPFW_VIOLATION_CATEGORY}. Vérification de sécurité ou règle spécifique de Web App Firewall qui a été violée.
- $ {NS_APPFW_VIOLATION_LOG}. Message d'erreur détaillé associé à la violation.
- ${COOKIE Le contenu du cookie spécifié. Par<CookieName>, remplacez le nom du cookie spécifique que vous souhaitez afficher sur la page d'erreur. Si vous avez plusieurs cookies dont vous souhaitez afficher le contenu pour le dépannage, vous pouvez utiliser plusieurs instances de cette variable de personnalisation, chacune avec le nom de cookie approprié.
  Remarque : si le blocage est activé pour la vérification de cohérence des cookies, les cookies bloqués ne sont pas affichés sur la page d'erreur car le pare-feu de l'application Web les bloque.

Pour utiliser ces variables, vous les incorporez au HTML ou au XML de l'objet de page d'erreur comme

s'il s'agissait d'une chaîne de texte ordinaire. Lorsque l'objet d'erreur est affiché à l'utilisateur, pour chaque variable de personnalisation, le Web App Firewall remplace les informations auxquelles la variable se réfère. Un exemple de page d'erreur HTML qui utilise des variables personnalisées est illustré ci-dessous.

```
<!doctype html public "-//w3c//dtd html 4.0//en"> <html> <head> <
   title>Page Not Accessible</title> </head> <body> <h1>Page Not
   Accessible</h1> <p>The page that you accessed is not available. You
    can:</p> <ul> <li>return to the <b><a href="[homePage]">home page
   </a></b>, re-establish your session, and try again, or,</li> <li>
   report this incident to the help desk via <b><a href="mailto:[
   helpDeskEmailAddress]">email</a></b> or by calling [
   helpDeskPhoneNumber].</li> </ul> <p>If you contact the help desk,
   please provide the following information:</p> <table cellpadding=8
   width=80%> <tr><th align="right" width=30%>Transaction ID:</th><td
   align="left" valign="top" width=70%>${
 NS_TRANSACTION_ID }
 </td></tr> <tr><th align="right" width=30%>Session ID:</th><td align=
    "left" valign="top" width=70%>${
 NS_APPFW_SESSION_ID }
 </td></tr> <tr><th align="right" width=30%>Violation Category:</th><
    td align="left" valign="top" width=70%>${
 NS_APPFW_VIOLATION_CATEGORY }
 </td></tr> <tr><th align="right" width=30%>Violation Log:</th><td
    align="left" valign="top" width=70%>${
 NS_APPFW_VIOLATION_LOG }
 </td></tr> <tr><th align="right" width=30%>Cookie Name:</th><td align
    ="left" valign="top" width=70%>${
 COOKIE("[cookieName]") }
 </td></tr> </table> <body> <html>
<!--NeedCopy-->
```

Pour utiliser cette page d'erreur, copiez-la dans un éditeur de texte ou HTML. Remplacez les informations locales appropriées par les variables suivantes, qui sont placées entre crochets pour les distinguer des variables Citrix ADC. (Laisser inchangés) :

- [homePage]. L'URL de la page d'accueil de votre site Web.
- [helpDeskEmailAddress]. Adresse e-mail que vous souhaitez que les utilisateurs utilisent pour signaler les incidents de blocage.
- [helpDeskPhoneNumber]. Numéro de téléphone que vous souhaitez que les utilisateurs appellent pour signaler les incidents de blocage.
- [cookieName]. Nom du cookie dont vous souhaitez afficher le contenu sur la page d'erreur.

Objet d'erreur XML

Lorsqu'une connexion d'un utilisateur à une page XML est bloquée ou qu'un utilisateur demande une application XML inexistante, le Web App Firewall envoie une réponse d'erreur XML au navigateur de l'utilisateur. Vous configurez la réponse d'erreur en téléchargeant une page d'erreur XML vers le Web App Firewall dans le volet Importations, sous l'onglet Objet d'erreur XML. Toutes les réponses d'erreur XML sont hébergées sur le Web App Firewall. Vous ne pouvez pas configurer une URL de redirection pour les applications XML.

> **Remarque** :
> Vous pouvez utiliser les mêmes variables de personnalisation dans un objet d'erreur XML que dans un objet d'erreur HTML.

Schéma XML

Lorsque le Web App Firewall effectue une vérification de validation sur la demande d'un utilisateur pour une application XML ou Web 2.0, il peut valider la demande par rapport au schéma XML ou au document de type de conception (DTD) pour cette application et rejeter toute demande qui ne suit pas le schéma ou la DTD. Un schéma XML et une DTD sont des fichiers de configuration XML standard qui décrivent la structure d'un type spécifique de document XML.

WSDL

Lorsque le Web App Firewall effectue une vérification de validation sur la demande d'un utilisateur pour un service Web basé sur SOAP XML, il peut valider la demande par rapport au fichier WSDL (Web Services Type Definition) pour ce service Web. Un fichier WSDL est un fichier de configuration SOAP XML standard qui définit les éléments d'un service Web XML SOAP spécifique.

Importation et exportation de fichiers

August 20, 2021

Vous pouvez importer des objets d'erreur HTML ou XML, des schémas XML, des DTD et des WSDL dans le Web App Firewall à l'aide de l'interface graphique ou de la ligne de commande. Vous pouvez modifier n'importe lequel de ces fichiers dans une zone de texte Web après les avoir importés, pour apporter de petites modifications directement sur Citrix ADC au lieu d'avoir à les faire sur votre ordinateur, puis à les réimporter. Enfin, vous pouvez exporter l'un de ces fichiers vers votre ordinateur, ou supprimer l'un de ces fichiers, à l'aide de l'interface graphique.

> **Remarque :**
>
> Vous ne pouvez pas supprimer ou exporter un fichier importé à l'aide de la ligne de commande.

Pour importer un fichier à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `import appfw htmlerrorpage <src> <name>`
- `<save> ns config`

Exemple

L'exemple suivant importe un objet d'erreur HTML à partir d'un fichier nommé error.html et lui attribue le nom HTMLError.

```
1 import htmlerrorpage error.html HTMLError
2 save ns config
3 <!--NeedCopy-->
```

Pour importer un fichier à l'aide de l'interface graphique

Avant de tenter d'importer un schéma XML, un fichier DTD ou WSDL ou un objet d'erreur HTML ou XML à partir d'un emplacement réseau, vérifiez que Citrix ADC peut se connecter à l'ordinateur Internet ou LAN où se trouve le fichier. Sinon, vous ne pouvez pas importer le fichier ou l'objet.

1. Accédez à **Sécurité > Citrix Web App Firewall > Importations**.
2. Accédez à **Application Pare-feu** > **Importations**.
3. Dans le volet **Importations du pare-feu d'application**, sélectionnez l'onglet correspondant au type de fichier à importer, puis cliquez sur **Ajouter**.

   Les onglets sont Page d'erreur HTML, Page d'erreur XML, Schéma XML ou WSDL. Le processus de téléchargement est identique sur les quatre onglets du point de vue de l'utilisateur.
4. Remplissez les champs de dialogue.
   - **Nom** : nom de l'objet importé.
   - **Importer à partir** : choisissez l'emplacement du fichier HTML, du fichier XML, du schéma XML ou du fichier WSDL que vous souhaitez importer dans la liste déroulante :
     - **URL : URL** Web d'un site Web accessible à l'appliance.
     - **Fichier :** fichier sur un disque dur local ou en réseau ou un autre périphérique de stockage.

- **Texte :** Tapez ou collez le texte de la réponse personnalisée directement dans un champ de texte de l'interface graphique.

La troisième zone de texte passe à la valeur appropriée. Les trois valeurs possibles sont indiquées ci-dessous.

- **URL**—Saisissez l'URL dans la zone de texte.
- **Fichier** : saisissez directement le chemin d'accès et le nom du fichier HTML, ou cliquez sur Parcourir et accédez au fichier HTML.
- **Texte**—Le troisième champ est supprimé, laissant un espace vide.

5. Cliquez sur **Continuer**. La boîte de dialogue Contenu du fichier s'affiche. Si vous avez choisi URL ou Fichier, la zone de texte Contenu du fichier contient le fichier HTML que vous avez spécifié. Si vous avez choisi Texte, la zone de texte Contenu du fichier est vide.
6. Si vous avez choisi Texte, tapez ou copiez et collez le code HTML de réponse personnalisé que vous souhaitez importer.
7. Cliquez sur **Terminé**.
8. Pour supprimer un objet, sélectionnez-le, puis cliquez sur **Supprimer**.

Pour exporter un fichier à l'aide de l'interface graphique

Avant de tenter d'exporter un schéma XML, un fichier DTD ou WSDL ou un objet d'erreur HTML ou XML, vérifiez que le Web App Firewall peut accéder à l'ordinateur sur lequel le fichier doit être enregistré. Sinon, vous ne pouvez pas exporter le fichier.

1. Accédez à **Sécurité** > **Web App Firewall** > **Importations**.
2. Dans le volet **Importations du Web App Firewall**, sélectionnez l'onglet correspondant au type de fichier à exporter.

   Le processus d'exportation est identique sur les quatre onglets du point de vue de l'utilisateur.
3. Sélectionnez le fichier à exporter.
4. Développez la liste déroulante Action, puis sélectionnez **Exporter**.
5. Dans la boîte de dialogue, choisissez **Enregistrer le fichier** et cliquez sur **OK**.
6. Dans la boîte de dialogue **Parcourir**, accédez au système de fichiers local et au répertoire où vous souhaitez enregistrer le fichier exporté, puis cliquez sur **Enregistrer**.

Pour modifier un objet d'erreur HTML ou XML dans l'interface graphique

Vous modifiez le texte des objets d'erreur HTML et XML dans l'interface graphique sans exporter, puis les réimporter.

1. Accédez à **Sécurité > Citrix Web App Firewall > Importations**, puis sélectionnez l'onglet correspondant au type de fichier à modifier.
2. Accédez à **Application Pare-feu** > **Importations**, puis sélectionnez l'onglet correspondant au type de fichier à modifier.
3. Sélectionnez le fichier à modifier, puis cliquez sur **Modifier**.

   Le texte de l'objet d'erreur HTML ou XML s'affiche dans une zone de texte du navigateur. Vous pouvez modifier le texte à l'aide des outils et méthodes d'édition standard basés sur le navigateur de votre navigateur.

   Remarque : La fenêtre d'édition est conçue pour vous permettre d'apporter des modifications mineures à votre objet d'erreur HTML ou XML. Pour apporter des modifications importantes, vous pouvez préférer exporter l'objet d'erreur sur votre ordinateur local et utiliser les outils standard d'édition de page Web HTML ou XML.
4. Cliquez sur **OK**, puis sur **Fermer**.

Configuration globale

January 21, 2021

La configuration globale du Web App Firewall affecte tous les profils et stratégies. Les éléments de configuration globale sont les suivants :

- **Paramètres du moteur.** Ensemble de paramètres globaux (nom de cookie de session, délai d'expiration de session, durée de vie maximale de session, nom d'en-tête de journalisation, profil non défini, profil par défaut et limite de taille d'importation) qui concernent toutes les connexions que le Web App Firewall traite, plutôt qu'un sous-ensemble spécifique de connexions.
- **Champs confidentiels.** Jeu de champs de formulaire dans les formulaires Web qui contiennent des informations sensibles qui ne doivent pas être consignées dans les journaux du Web App Firewall. Les champs de formulaire tels que les champs de mot de passe sur une page d'ouverture de session ou les informations de carte de crédit sur un formulaire de commande de panier d'achat sont normalement désignés comme des champs confidentiels.
- **Types de champs.** Liste des types de champs de formulaire Web utilisés par la vérification de sécurité Formats de champ. Chacun de ces types de champ est défini par une expression régulière conforme à la norme PCRE qui définit le type de données et la longueur minimum/-maximale des données qui doivent être autorisées dans ce type de champ de formulaire.
- **Types de contenu XML.** Liste des types de contenu reconnus comme XML et soumis à des vérifications de sécurité spécifiques au XML. Chacun de ces types de contenu est défini par une

expression régulière conforme à la norme PCRE qui définit le type MIME exact attribué à ce contenu.

- **Types de contenu JSON.** Liste des types de contenu reconnus comme JSON et soumis à des vérifications de sécurité spécifiques à JSON. Chacun de ces types de contenu est défini par une expression régulière conforme à la norme PCRE qui définit le type MIME exact attribué à ce contenu.

Paramètres du moteur

August 20, 2021

Les paramètres du moteur affectent toutes les demandes et réponses traitées par Citrix Web App Firewall. Voici les paramètres :

- **Cookie name**—nom du cookie qui stocke l'ID de session Citrix ADC.
- **Session timeout**—Période d'inactivité maximale autorisée. Si une session utilisateur n'affiche aucune activité pendant cette période, la session est interrompue et l'utilisateur doit la rétablir en visitant une page de démarrage désignée.
- **Préfixe de post-chiffrement des cookies**—Chaîne qui précède la partie chiffrée de tous les cookies chiffrés.
- **Maximum session lifetime**—durée maximale, en secondes, pendant laquelle une session est autorisée à rester active. Une fois cette période atteinte, la session est interrompue et l'utilisateur doit la rétablir en visitant une page de démarrage désignée. Ce paramètre ne peut pas être inférieur au délai d'expiration de la session. Pour désactiver ce paramètre, afin qu'il n'y ait pas de durée de vie maximale de session, définissez la valeur sur zéro (0).
- **Nom de l'en-tête de journalisation** : nom de l'en-tête HTTP contenant l'adresse IP du client, pour la journalisation.
- **Profil non défini** : profil appliqué lorsque l'action de stratégie correspondante est considérée comme non définie.
- **Profil par défaut** : profil appliqué aux connexions qui ne correspondent pas à une stratégie.
- **Limite de taille d'importation** : nombre maximal d'octets de tous les fichiers importés dans l'appliance, y compris les signatures, les fichiers WSDL, les schémas, les pages d'erreur HTML et XML. Lors d'une importation, si la taille de l'objet importé entraîne le nombre cumulé de tous les fichiers importés dépasse la limite configurée, l'opération d'importation échoue. Et l'appliance affiche le message d'erreur suivant : « *ERREUR : Échec de l'importation - dépassement de la limite de taille totale configurée sur les objets importés* ».
- **Learn message rate limit** : nombre maximal de demandes et de réponses par seconde que le moteur d'apprentissage doit traiter. Toute demande supplémentaire ou réponse supérieure à cette limite ne sera pas envoyée au moteur d'apprentissage.

- **Décodage d'entité** : décodez les entités HTML lors de l'exécution des vérifications du Web App Firewall.
- **Journaliser la requête mal formée** : permet d'activer la journalisation des requêtes HTTP mal formées.
- **Utiliser une clé secrète configurable** : utilisez une clé secrète configurable pour les opérations du Web App Firewall. Cette clé secrète est utilisée pour signer et vérifier les données. Lorsque « UseConfigurableSeecretKey » est activé, vous devez utiliser la clé activée dans le paramètre « set ns EncryptionParams ».
- **Réinitialiser les données apprises** : supprimez toutes les données apprises du Web App Firewall. Redémarre le processus d'apprentissage en recueillant de nouvelles données.

Deux paramètres, *Réinitialiser les données apprises* et la *mise à jour automatique des signatures*, se trouvent à différents endroits selon que vous utilisez l'interface de commande ou l'interface graphique Citrix ADC pour configurer votre Citrix Web App Firewall. Lorsque vous utilisez l'interface de commande, vous configurez Réinitialiser les données apprises à l'aide de la commande reset appfw learning data. Cela ne prend pas de paramètres et n'a pas d'autres fonctions. Vous pouvez configurer la signature Mise à jour automatique dans la commande set appfw settings. Le paramètre -SignatureAutoUpdate active ou désactive la mise à jour automatique des signatures, et -SignatureUrl configure l'URL qui héberge le fichier de signatures mis à jour.

Lorsque vous utilisez l'interface graphique Citrix ADC, vous configurez Réinitialiser les données apprises dans **Sécurité >**Citrix Web App Firewall**> Paramètres du moteur**. L'option **Réinitialiser les données acquises** se trouve en bas de la boîte de dialogue. Vous configurez la mise à jour automatique des signatures pour chaque jeu de signatures dans **Sécurité** > **Citrix Web App Firewall** > **Signatures**, en sélectionnant le fichier de signatures, en cliquant sur le bouton droit de la souris et en sélectionnant **Paramètres de mise à jour automatique**.

Normalement, les valeurs par défaut des paramètres du **Web App Firewall** sont correctes. Si les paramètres par défaut provoquent un conflit avec d'autres serveurs ou provoquent une déconnexion prématurée de vos utilisateurs, vous devez toutefois les modifier.

La limite de session du **Web App Firewall** est configurable à l'aide de la commande suivante :

```
1 > set appfw settings -sessionLimit 500000
2
3 Done
4
5 Default value:100000   Max value:500000 per PE
6 <!--NeedCopy-->
```

Pour configurer les paramètres du moteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- set appfw settings [-sessionCookieName <name>] [-sessionTimeout <positiveInteger>] [-sessionLifetime <positiveInteger>][-clientIPLoggingHeader <headerName>] [-undefaction <profileName>] [-defaultProfile <profileName>] [-importSizeLimit <positiveInteger>] [-logMalformedReq (ON | OFF)] [-signatureAutoUpdate (ON | OFF)] [-signatureUrl <expression>] [-cookiePostEncryptPrefix <string>] [-entityDecoding (ON | OFF)] [-useConfigurableSecretKey (ON | OFF)][-learnRateLimit <positiveInteger>]
- save ns config

Exemple

```
set appfw settings -sessionCookieName citrix-appfw-id -sessionTimeout
    3600
-sessionLifetime 14400 -clientIPLoggingHeader NS-AppFW-Client-IP -
    undefaction APPFW_RESET
-defaultProfile APPFW_RESET -importSizeLimit 4096
save ns config
<!--NeedCopy-->
```

Pour configurer les paramètres du moteur à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité** > **Citrix Web App Firewall**
2. Dans le volet d'informations, cliquez sur **Modifier les paramètres du moteur** sous **Paramètres**.
3. Dans la boîte de dialogue **Paramètres du moteur de Web App Firewall**, définissez les paramètres suivants :
   - Nom du cookie
   - Délai d'expiration de la session
   - Préfixe de chiffrement des messages de cookies
   - Durée de vie maximale de session
   - Nom de l'en-tête de journalisation
   - Profil non défini
   - Profil par défaut
   - Limite de taille d'importation
   - Apprendre les messages Limite
   - Décodage d'entité
   - Journaliser les demandes mal formées
   - Utiliser la clé secrète
   - Apprendre la limite de fréquence des messages

- Mise à jour automatique des signatures

4. Cliquez sur **OK**.



Champs confidentiels

August 20, 2021

Vous pouvez désigner des champs de formulaire Web comme confidentiels afin de protéger les informations que les utilisateurs y saisissent. Normalement, toutes les informations qu'un utilisateur saisie dans un formulaire Web sur l'un de vos serveurs Web protégés sont enregistrées dans les journaux Citrix ADC. Toutefois, les informations saisies dans un champ de formulaire Web désigné comme confidentiel ne sont pas enregistrées. Ces informations ne sont enregistrées que lorsque le site Web est configuré pour enregistrer ces données, normalement dans une base de données sécurisée.

Les types de renseignements courants que vous pourriez vouloir protéger avec une désignation de champ confidentiel sont les suivants :

- Mots de passe
- Numéros de carte de crédit, codes de validation et dates d'expiration
- Numéros de sécurité sociale
- Numéros d'identification fiscale
- Adresses de domicile
- Numéros de téléphone privés

En plus d'être une bonne pratique, l'utilisation appropriée des désignations de terrain confidentielles peut être nécessaire pour la conformité PCI-DSS sur les serveurs de commerce électronique, la conformité HIPAA sur les serveurs qui gèrent les informations médicales aux États-Unis et la conformité avec d'autres normes de protection des données.

> **Important** :
>
> Dans les deux cas suivants, la désignation de zone confidentielle ne fonctionne pas comme prévu :

- Si un formulaire Web comporte un champ confidentiel ou une URL d'action supérieure à 256 caractères, l'URL de champ ou d'action est tronquée dans les journaux Citrix ADC.
- Avec certaines transactions SSL, les journaux sont tronqués si le champ confidentiel ou l'URL de l'action est supérieur à 127 caractères.

Dans l'un ou l'autre de ces cas, le Web App Firewall masque une chaîne de 15 caractères avec la lettre « x », au lieu de la chaîne de huit caractères normale. Pour s'assurer que toute information confidentielle est supprimée, l'utilisateur doit utiliser les expressions de nom de champ de formulaire et d'URL d'action correspondant aux 256 premiers ou (dans les cas où SSL est utilisé) les 127 premiers caractères.

Pour configurer votre Web App Firewall pour traiter un champ de formulaire Web sur un site Web protégé comme confidentiel, ajoutez ce champ à la liste Champs confidentiels. Vous pouvez entrer le nom du champ sous la forme d'une chaîne, ou vous pouvez entrer une expression régulière compatible PCRE spécifiant un ou plusieurs champs. Vous pouvez activer la désignation de champ confidentiel lorsque vous ajoutez le champ ou la modifier ultérieurement.

Pour ajouter un champ confidentiel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw confidField <fieldName> <url> [-isRegex ( REGEX | NOTREGEX )] [-comment "<string>"] [-state ( ENABLED | DISABLED )]`
- `save ns config`

Exemple

L'exemple suivant montre comment ajouter tous les champs de formulaire Web dont le nom commence par Password à la liste des champs confidentiels.

```
1 add appfw confidField Password "https?://www[.]example[.]com/[^<>]\*[^a
     -z]password[0-9a-z._-]\*[.](asp|cgi|htm|html|htp|js|php)" -isRegex
     REGEX -state ENABLED
2 save ns config
3 <!--NeedCopy-->
```

Pour modifier un champ confidentiel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw confidField <fieldName> <url> [-isRegex ( REGEX | NOTREGEX ) ][-comment "<string>"] [-state ( ENABLED | DISABLED )]`
- `save ns config`

Exemple

L'exemple suivant modifie la désignation de champ confidentiel pour ajouter un commentaire.

```
1 set appfw confidField Password "https?://www[.]example[.]com/[^<>]\*[^a
     -z]password[0-9a-z._-]\*[.](asp|cgi|htm|html|htp|js|php)" -comment "
     Protect password fields." -isRegex REGEX -state ENABLED
2 save ns config
3 <!--NeedCopy-->
```

Pour supprimer un champ confidentiel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `rm appfw confidField <fieldName> <url>`
- `save ns config`

Pour configurer un champ confidentiel à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Pare-feu d'application**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Gérer les champs confidentiels**.
3. Dans la boîte de dialogue Gérer les champs confidentiels, effectuez l'une des opérations suivantes :

- Pour ajouter un nouveau champ de formulaire à la liste, cliquez sur Ajouter.
- Pour modifier une désignation de champ confidentiel existante, sélectionnez le champ, puis cliquez sur **Modifier**.
  La boîte de dialogue **Champs confidentiels de Web App Firewall** s'affiche.

  > **Remarque** :
  > Si vous sélectionnez une désignation de champ confidentiel existante, puis cliquez sur **Ajouter**, la boîte de dialogue **Créer un champ de formulaire confidentiel**affiche les informations relatives à ce champ confidentiel. Vous pouvez modifier ces informations pour créer votre nouveau champ confidentiel.

4. Dans la boîte de dialogue, remplissez les éléments. Ils sont :
   - **Activez la case à cocher.** Sélectionnez ou désactivez pour activer/désactiver cette désignation de champ confidentiel.
   - **Est un nom de champ de formulaire une case à cocher expression régulière.** Sélectionnez ou désactivez pour activer les expressions régulières au format PCRE dans le nom du champ de formulaire.
   - **Nom du champ.** Entrez une chaîne littérale ou une expression régulière au format PCRE qui représente un nom de champ spécifique ou qui correspond à plusieurs champs dont les noms suivent un modèle.
   - **URL de l'action.** Entrez une URL littérale ou une expression régulière qui définit une ou plusieurs URL de la ou des pages Web sur lesquelles se trouvent le ou les formulaires Web contenant le champ confidentiel.
   - **Commentaires.** Entrez un commentaire. Facultatif.
5. Cliquez sur **Créer** ou **sur OK**.
6. Pour supprimer une désignation de champ confidentiel de la liste des champs confidentiels, sélectionnez la liste des champs confidentiels à supprimer, puis cliquez sur Supprimer pour la supprimer, puis cliquez sur **OK** pour confirmer votre choix.
7. Lorsque vous avez terminé d'ajouter, de modifier et de supprimer des désignations de champs confidentiels, cliquez sur **Fermer**.

Exemples

Voici quelques expressions régulières qui définissent les noms de champs de formulaire que vous pourriez trouver utiles :

- `^passwd_ (Applies confidential-field status to all field names that begin with the “passwd_” string.)`
- `^((\[0-9a-zA-Z._-]*||\\x\[0-9A-Fa-f][0-9A-Fa-f])+-)?passwd_ (Applies confidential-field status to all field names that begin with the string passwd_, or that contain the string -passwd_ after another string that might contain non-ASCII special characters.)`

Voici quelques expressions régulières qui définissent des types d'URL spécifiques que vous pourriez trouver utiles. Remplacez vos propres hôtes et domaines Web par ceux figurant dans les exemples.

- Si le formulaire Web apparaît sur plusieurs pages Web de l'hôte Web www.example.com, mais que toutes ces pages Web sont nommées logon.pl ?, vous pouvez utiliser l'expression régulière suivante :

```
https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_.-]*/)*logon
   [.]pl?
<!--NeedCopy-->
```

- Si le formulaire Web apparaît sur plusieurs pages Web de l'hôte Web www.example-español.com, qui contient le caractère spécial n-tilde (ñ), vous pouvez utiliser l'expression régulière suivante, qui représente le caractère spécial n-tilde sous la forme d'une chaîne UTF-8 encodée contenant C3 B1, le code hexadécimal attribué à cette dans le jeu de caractères UTF-8 :

```
https?://www[.]example-espa\xC3\xB1ol[.]com/([0-9A-Za-z][0-9A-Za-
   z_.-]\*/)\* logon[.]pl?
<!--NeedCopy-->
```

- Si le formulaire Web contenant query.pl apparaît sur plusieurs pages Web sur différents hôtes dans le domaine example.com, vous pouvez utiliser l'expression régulière suivante :

```
https?://([0-9A-Za-z][0-9A-Za-z_-.]*[.])\*example[.]com/([0-9A-Za
   -z][0-9A-Za-z_-.]\*/)*logon[.]pl?
<!--NeedCopy-->
```

- Si le formulaire Web contenant query.pl apparaît sur plusieurs pages Web sur différents hôtes dans différents domaines, vous pouvez utiliser l'expression régulière suivante :

```
https?://([0-9A-Za-z][0-9A-Za-z_-.]\*[.])\*[0-9A-Za-z][0-9A-Za-z_
   -.]+[.][a-z]{
2,6 }
/([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon[.]pl?
<!--NeedCopy-->
```

- Si le formulaire Web apparaît sur plusieurs pages Web de l'hôte Web www.example.com, mais que toutes ces pages Web sont nommées logon.pl ?, vous pouvez utiliser l'expression régulière suivante :

```
https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon
   [.]pl?
<!--NeedCopy-->
```


Types de champs

August 20, 2021

Un type de champ est une expression régulière au format PCRE qui définit un format de données particulier et des longueurs minimum/maximales de données pour un champ de formulaire dans un formulaire Web. Les types de champs sont utilisés dans la vérification Formats des champs.

Le Web App Firewall est livré avec plusieurs types de champs par défaut, à savoir :

- entier. Chaîne de n'importe quelle longueur composée de nombres seulement, sans virgule décimale, et avec un signe moins (-) facultatif.
- Alpha. Chaîne de n'importe quelle longueur composée de lettres seulement.
- alphanum. Chaîne de n'importe quelle longueur composée de lettres et/ou de chiffres.
- nohtml. Chaîne de n'importe quelle longueur composée de caractères, y compris la ponctuation et les espaces, qui ne contient pas de symboles ou de requêtes HTML.
- tout. N'importe quoi du tout.

> **Important :**
>
> L'affectation de n'importe quel type de champ comme type de champ par défaut, ou à un champ, permet d'envoyer des scripts actifs, des commandes SQL et d'autres contenus potentiellement dangereux à vos sites Web et applications protégés dans ce champ de formulaire. Vous devez utiliser le n'importe quel type avec parcimonie, si vous l'utilisez du tout.

Vous pouvez également ajouter vos propres types de champs à la liste Types de champs. Par exemple, vous pouvez ajouter un type de champ pour un numéro de sécurité sociale, un code postal ou un numéro de téléphone dans votre pays. Vous pouvez également ajouter un type de champ pour un numéro d'identification client ou un numéro de carte de crédit de magasin.

Pour ajouter un type de champ à la liste Types de champ, saisissez le nom du champ sous la forme d'une chaîne littérale ou d'une expression régulière au format PCRE.

Pour ajouter un type de champ à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw fieldType <name> <regex> <priority> [-comment "<string>"]`
- `save ns config`

Exemple

L'exemple suivant montre comment ajouter un type de champ nommé SSN qui correspond aux numéros de sécurité sociale américains à la liste Types de champs et définir sa priorité sur 1.

```
add appfw fieldType SSN "^[1-9][0-9]{
 2,2 }
 -[0-9 }
 {
 2,2 }
 -[0-9]{
 4,4 }
 $" 1
save ns config
<!--NeedCopy-->
```

Pour modifier un type de champ à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw fieldType <name> <regex> <priority> [-comment "<string>"]`
- `save ns config`

Exemple

L'exemple suivant montre comment modifier le type de champ pour ajouter un commentaire.

```
set appfw fieldType SSN "^[1-9][0-9]{
 2,2 }
 -[0-9 }
 {
 2,2 }
 -[0-9]{
 4,4 }
 $" 1 -comment "US Social Security Number"
save ns config
<!--NeedCopy-->
```

Pour supprimer un type de champ à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `>rm appfw fieldType <name>`
- `save ns config`

Pour configurer un type de champ à l'aide de l'interface graphique

1. Accédez à Sécurité > Pare-feu d'application.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Gérer les types de champs**.
3. Dans la boîte de dialogue **Gérer les types de champs**, effectuez l'une des opérations suivantes :
   - Pour ajouter un nouveau type de champ à la liste, cliquez sur **Ajouter**.
   - Pour modifier un type de champ existant, sélectionnez-le, puis cliquez sur **Modifier**. La boîte de dialogue **Configurer le type de champ** s'affiche.

   > **Remarque :**
   >
   > Si vous sélectionnez une désignation de type de champ existante, puis cliquez sur **Ajouter**, la boîte de dialogue affiche les informations relatives à ce type de champ. Vous pouvez modifier ces informations pour créer votre nouveau type de champ.
4. Dans la boîte de dialogue, remplissez les éléments. Ils sont :
   - Nom
   - Expression régulière
   - Priority
   - Commentaire
5. Cliquez sur Créer ou sur OK.
6. Pour supprimer un type de champ de la liste Types de champ, sélectionnez le type de champ à supprimer, puis cliquez sur **Supprimer** pour le supprimer, puis cliquez sur **OK** pour confirmer votre choix.
7. Lorsque vous avez terminé d'ajouter, de modifier et de supprimer des types de champ, cliquez sur **Fermer**.

Exemples

Voici quelques expressions régulières pour les types de champs que vous pourriez trouver utiles :

Numéros de sécurité sociale aux`^[1-9][0-9]{ 2,2 } -[0-9 } { 2,2 } -[0-9]{ 4,4 } $` États-Unis

Numéro du permis de conduire en`^\[A-C\]\[0-9\]{ 7,7 } $` Californie

Numéros de téléphone`^+[0-9]{ 1,3 } [0-9()-]{ 1,40 } $` internationaux avec codes de pays

Numéros de code postal`^[0-9]{ 5,5 } -[0-9]{ 4,4 } $` américain

`^[0-9A-Za-z][0-9A-Za-z.+_-]{ 0,25 } @([0-9A-Za-z][0-9A-Za-z_-]*[.]){ 1,4 } [A-Za-z]{ 2,6 } $` Adresses e-mail

Types de contenu XML

January 21, 2021

Par défaut, le Web App Firewall traite les fichiers qui suivent certaines conventions de dénomination comme XML. Vous pouvez configurer le Web App Firewall pour examiner le contenu Web à la recherche de chaînes ou de modèles supplémentaires indiquant que ces fichiers sont des fichiers XML. Cela peut garantir que le Web App Firewall reconnaît tout le contenu XML de votre site, même si certains contenus XML ne respectent pas les conventions normales d'attribution de noms XML, ce qui garantit que le contenu XML est soumis à des vérifications de sécurité XML.

Pour configurer les types de contenu XML, ajoutez les modèles appropriés à la liste Types de contenu XML. Vous pouvez entrer un type de contenu sous forme de chaîne, ou vous pouvez entrer une expression régulière compatible PCRE spécifiant une ou plusieurs chaînes. Vous pouvez également modifier les modèles de types de contenu XML existants.

Pour ajouter un modèle de type de contenu XML à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw XMLContentType <XMLContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]`
- `save ns config`

Exemple

L'exemple suivant montre comment ajouter le motif. */xml à la liste des types de contenu XML et la désigne comme une expression régulière.

```
1 add appfw XMLContentType ".*/xml" -isRegex REGEX
2 <!--NeedCopy-->
```

Pour supprimer un modèle de type de contenu XML à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `rm appfw XMLContentType <XMLContenttypevalue>`
- `save ns config`

Pour configurer la liste des types de contenu XML à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Web App Firewall**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Gérer les types de contenu XML**.
3. Dans la boîte de dialogue **Gérer les types de contenu XML**, effectuez l'une des opérations suivantes :
   - Pour ajouter un nouveau type de contenu XML, cliquez sur Ajouter.
   - Pour modifier un type de contenu XML existant, sélectionnez-le, puis cliquez sur Modifier. La boîte de dialogue Configurer le type de contenu XML du Web App Firewall apparaît. Remarque : Si vous sélectionnez un modèle de type de contenu XML existant, puis cliquez sur Ajouter, la boîte de dialogue affiche les informations relatives à ce modèle de type de contenu XML. Vous pouvez modifier ces informations pour créer votre nouveau modèle de type de contenu XML.
4. Dans la boîte de dialogue, remplissez les éléments. Ils sont :
   - **IsRegex.** Sélectionnez ou désactivez pour activer les expressions régulières au format PCRE dans le nom du champ de formulaire.
   - **Type de contenu XML** Entrez une chaîne littérale ou une expression régulière au format PCRE correspondant au modèle de type de contenu XML que vous souhaitez ajouter.
5. Cliquez sur **Créer**.
6. Pour supprimer un modèle de type de contenu XML de la liste, sélectionnez-le, puis cliquez sur **Supprimer** pour le supprimer, puis cliquez sur **OK** pour confirmer votre choix.
7. Lorsque vous avez terminé d'ajouter et de supprimer des modèles de type de contenu XML, cliquez sur **Fermer**.

Types de contenu JSON

January 21, 2021

Par défaut, le Web App Firewall traite les fichiers avec le type de contenu "application/json" comme des fichiers JSON. Le paramètre par défaut permet au pare-feu d'application Web de reconnaître le contenu JSON dans les requêtes et les réponses, et de gérer ce contenu de manière appropriée.

Vous pouvez configurer le Web App Firewall pour examiner le contenu Web à la recherche de chaînes ou de modèles supplémentaires indiquant que ces fichiers sont des fichiers JSON. Cela peut garantir que le Web App Firewall reconnaît tout le contenu JSON de votre site, même si certains contenus JSON ne suivent pas les conventions d'attribution de noms JSON normales, garantissant que le contenu JSON est soumis à des vérifications de sécurité JSON.

Pour configurer les types de contenu JSON, ajoutez les modèles appropriés à la liste Types de contenu JSON. Vous pouvez entrer un type de contenu sous forme de chaîne, ou vous pouvez entrer une

expression régulière compatible PCRE spécifiant une ou plusieurs chaînes. Vous pouvez également modifier les modèles de types de contenu JSON existants.

Pour ajouter un modèle de type de contenu JSON à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw JSONContentType <JSONContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]`
- `save ns config`

Exemple

L'exemple suivant montre comment ajouter le motif. */json à la liste des types de contenu JSON et la désigne comme une expression régulière.

```
1 add appfw JSONContentType ".*/json" -isRegex REGEX
2 <!--NeedCopy-->
```

Pour configurer la liste des types de contenu JSON à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Pare-feu d'application**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Gérer les types de contenu JSON**.
3. Dans la boîte de dialogue Gérer les types de contenu JSON, effectuez l'une des opérations suivantes :
   - Pour ajouter un nouveau type de contenu JSON, cliquez sur Ajouter.
   - Pour modifier un type de contenu JSON existant, sélectionnez-le, puis cliquez sur Modifier. La boîte de dialogue Configurer le type de contenu JSON du Web App Firewall s'affiche. Remarque : Si vous sélectionnez un modèle de type de contenu JSON existant, puis cliquez sur Ajouter, la boîte de dialogue affiche les informations relatives à ce modèle de type de contenu JSON. Vous pouvez modifier ces informations pour créer votre nouveau modèle de type de contenu JSON.
4. Dans la boîte de dialogue, remplissez les éléments. Ils sont :
   - **IsRegex.** Sélectionnez ou désactivez pour activer les expressions régulières au format PCRE dans le nom du champ de formulaire.
   - **Type de contenu JSON** Entrez une chaîne littérale ou une expression régulière au format PCRE qui correspond au modèle de type de contenu JSON que vous souhaitez ajouter.
5. Cliquez sur **Créer** ou **sur OK**.
6. Pour supprimer un modèle de type de contenu JSON de la liste, sélectionnez-le, puis cliquez sur **Supprimer** pour le supprimer, puis cliquez sur **OK** pour confirmer votre choix.

7. Lorsque vous avez terminé d'ajouter et de supprimer des modèles de type de contenu XML, cliquez sur **Fermer**.

Statistiques et rapports

September 8, 2021

Les informations conservées dans les journaux et les statistiques, et affichées dans les rapports, fournissent des conseils importants sur la configuration et la maintenance du Web App Firewall.

Statistiques du Web App Firewall

Lorsque vous activez l'action de statistiques pour les signatures du pare-feu Web App Firewall ou les contrôles de sécurité, le Web App Firewall conserve des informations sur les connexions qui correspondent à cette signature ou à cette vérification de sécurité. Vous pouvez afficher les informations statistiques accumulées sous l'onglet
Surveillance en sélectionnant l'un des choix suivants dans la zone de liste Sélectionner un groupe :

- **Web App Firewall.** Un résumé de toutes les informations statistiques collectées par votre dispositif Web App Firewall pour tous les profils.
- **Web App Firewall (par profil).** Les mêmes informations, mais affichées par profil plutôt que résumées.

Vous pouvez utiliser ces informations pour surveiller le fonctionnement de votre Web App Firewall et déterminer s'il y a une activité anormale ou un nombre anormal d'accès lors d'une vérification de la signature ou de la sécurité. Si vous constatez un tel modèle d'activité anormale, vous pouvez vérifier les journaux de cette signature ou de cette vérification de sécurité pour diagnostiquer et prendre des mesures correctives.

Compteur statistique de relaxation

En fonction de la relaxation appliquée au trafic violé, vous pouvez également afficher des détails statistiques tels que le nombre de fois qu'une violation se produit sur l'appliance, le nombre de règles de relaxation appliquées au moment de la violation et le dernier horodatage appliqué. En effectuant cette opération, le moteur d'apprentissage centralisé peut supprimer automatiquement les liaisons de relaxation inutilisées ou redondantes. Pour plus d'informations, consultez la rubrique Moteur d'apprentissage WAF .

Le compteur statistique des coups de relaxation est disponible uniquement pour les contrôles de sécurité suivants.

• Starturl
• Refuser une URL
• Scriptage intersite
• Injection SQL

Pour afficher les statistiques des compteurs d'accès aux règles de relaxation à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat appfw profile p1
```

Exemple :

```
stat appfw profile p1 -fullvalues
```

Statistiques des règles Starturl

Règle	hits	Tarif	heure du dernier coup
87a4…51177	0	0	Jeu… 1970
5b83…dc12a	0	0	Jeu… 1970
12345	0	0	Jeu… 1970

Pour afficher les statistiques des compteurs d'accès aux règles de relaxation à l'aide de l'interface graphique

Effectuez les étapes suivantes pour afficher les statistiques de compteur d'accès de la règle de relaxation :

1. Accédez à **Sécurité > Citrix Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez un **profil Web App Firewall** et cliquez sur **Statistiques**.
3. La page **Statistiques du Citrix Web App Firewall** affiche les détails des statistiques.
4. Vous pouvez sélectionner Vue tabulaire ou passer à la vue graphique pour afficher les données sous forme de tableau ou de graphique.

Rapports du Web App Firewall

Les rapports Web App Firewall fournissent des informations sur la configuration de votre Web App Firewall et sur la façon dont il gère le trafic pour vos sites Web protégés.

Le rapport PCI DSS

La norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI), version 1.2, comprend 12 critères de sécurité auxquels la plupart des sociétés de cartes de crédit exigent que les entreprises qui acceptent les paiements en ligne par cartes de crédit et de débit respectent. Ces critères sont conçus pour prévenir le vol d'identité, le piratage et d'autres types de fraude. Si un fournisseur de services Internet ne répond pas aux critères PCI DSS, ce fournisseur de services Internet ou ce marchand risquent de perdre l'autorisation d'accepter les paiements par carte de crédit via le site Web.

Les FAI et les commerçants en ligne prouvent qu'ils sont conformes à la norme PCI DSS en faisant effectuer un audit par une société d'évaluateur de sécurité qualifié (QSA) PCI DSS. Le rapport PCI DSS est conçu pour les aider avant et pendant l'audit. Avant l'audit, il indique quels paramètres Web App Firewall sont pertinents pour PCI DSS, comment ils doivent être configurés et (plus important encore) si la configuration actuelle de votre pare-feu Web App Firewall répond à la norme. Au cours de l'audit, le rapport peut être utilisé pour démontrer la conformité aux critères PCI DSS pertinents.

Le rapport PCI DSS consiste en une liste des critères pertinents pour la configuration de votre Web App Firewall. Sous chaque critère, il répertorie vos options de configuration actuelles, indique si votre configuration actuelle est conforme au critère PCI DSS et explique comment configurer le Web App Firewall pour que vos sites Web protégés soient conformes au critère.

Le rapport PCI DSS se trouve sous **Système > Rapports**. Pour générer le rapport sous forme de fichier Adobe PDF, cliquez sur Générer un rapport PCI DSS. Selon les paramètres de votre navigateur, le rapport s'affiche dans la fenêtre contextuelle ou vous êtes invité à l'enregistrer sur votre disque dur.

> **Remarque :**
>
> Pour afficher ce rapport et d'autres rapports, le programme Adobe Reader doit être installé sur votre ordinateur.

Le rapport PCI DSS comprend les sections suivantes :

- **Description.** Description du rapport PCI DSS Compliance Summary.
- **Licence et statut des fonctionnalités du pare-feu.** Indique si le Web App Firewall est sous licence et activé sur votre appliance Citrix ADC.
- **Résumé exécutif.** Tableau qui répertorie les critères PCI DSS et qui indique quels critères sont pertinents pour le Web App Firewall.
- **Informations détaillées sur les critères PCI DSS.** Pour chaque critère PCI DSS pertinent pour la configuration de votre Web App Firewall, le rapport PCI DSS fournit une section qui contient des informations sur la conformité de votre configuration et, si ce n'est pas le cas, comment la mettre en conformité.
- **Configuration.** Données pour les profils individuels, auxquels vous accédez soit en cliquant sur Configuration du Web App Firewall en haut du rapport, soit directement depuis le volet Rap-

ports. Le rapport de configuration du Web App Firewall est le même que le rapport PCI DSS, le résumé spécifique au PCI DSS étant omis.

Le rapport de configuration du Web App Firewall

Le rapport Configuration du Web App Firewall se trouve sous **Système > Rapports**. Pour l'afficher, cliquez sur **Générer un rapport de configuration du Web App Firewall**. Selon les paramètres de votre navigateur, le rapport s'affiche dans la fenêtre contextuelle ou vous êtes invité à l'enregistrer sur votre disque dur.

Le rapport Configuration du Web App Firewall commence par une page Résumé, qui comprend les sections suivantes :

- **Stratégies de Web App Firewall.** Tableau qui répertorie vos stratégies de Web App Firewall actuelles, affichant le nom de la stratégie, le contenu de la stratégie, l'action (ou le profil) à laquelle elle est associée et les informations de liaison globales.
- **Profils de Web App Firewall.** Tableau qui répertorie vos profils Web App Firewall actuels et indique à quelle stratégie chaque profil est associé. Si un profil n'est pas associé à une stratégie, le tableau affiche INACTIF à cet emplacement.

Pour télécharger toutes les pages de rapport pour toutes les stratégies, en haut de la page Synthèse des profils, cliquez sur **Télécharger tous les profils**. Vous affichez la page de rapport pour chaque profil individuel en sélectionnant ce profil dans le tableau en bas de l'écran. La page Profil d'un profil individuel indique si chaque action de vérification est activée ou désactivée pour chaque vérification, ainsi que les autres paramètres de configuration de la vérification.

Pour télécharger un fichier PDF contenant la page de rapport PCI DSS du profil actuel, cliquez sur **Télécharger le profil actuel** en haut de la page. Pour revenir à la page Synthèse des profils, cliquez sur **Profils de Web App Firewall**. Pour revenir à la page principale, cliquez sur **Accueil**. Vous pouvez actualiser le rapport PCI DSS à tout moment en cliquant sur **Actualiser** dans le coin supérieur droit du navigateur.

Journaux du Web App Firewall

October 5, 2021

Les messages de journal générés par le Web App Firewall peuvent être très utiles pour suivre les modifications de configuration, les appels de stratégie de Web App Firewall et les violations des contrôles de sécurité.

Lorsque l'action de journal est activée pour les vérifications de sécurité ou les signatures, les messages de journal qui en résultent fournissent des informations sur les demandes et les réponses observées

par le Web App Firewall lors de la protection de vos sites Web et applications. Les informations les plus importantes sont l'action entreprise par le Web App Firewall lorsqu'une signature ou une violation du contrôle de sécurité a été observée. Pour certaines vérifications de sécurité, le message de journal peut fournir des informations utiles supplémentaires, telles que l'emplacement et le modèle détecté qui a déclenché la violation. Vous pouvez déployer des vérifications de sécurité en mode non bloqué et surveiller les journaux pour déterminer si les transactions qui déclenchent des violations de sécurité sont des transactions valides (faux positifs). Si tel est le cas, vous pouvez supprimer ou reconfigurer la signature ou les contrôles de sécurité, déployer des assouplissements ou prendre d'autres mesures appropriées pour atténuer les faux positifs avant d'activer le blocage de cette signature ou de cette vérification de sécurité. Une augmentation excessive du nombre de messages de violation dans les journaux peut indiquer une augmentation du nombre de demandes malveillantes. Cela peut vous avertir que votre application est peut-être attaquée pour exploiter une vulnérabilité spécifique détectée et contrecarrée par les protections du Web App Firewall.

> **Remarque :**
>
> La journalisation Citrix Web App Firewall doit être utilisée uniquement avec des serveurs SYSLOG externes.

Journaux au format Citrix ADC (natif)

Le Web App Firewall utilise les journaux au format Citrix ADC (également appelés journaux de format natif) par défaut. Ces journaux ont le même format que ceux générés par d'autres fonctionnalités de Citrix ADC. Chaque journal contient les champs suivants :

- Horodatage. Date et heure de la connexion.
- Gravité. Niveau de gravité du journal.
- module. Module Citrix ADC qui a généré l'entrée de journal.
- Type d'événement. Type d'événement, tel qu'une violation de signature ou une violation du contrôle de sécurité.
- ID de l'événement. ID attribué à l'événement.
- IP du client. Adresse IP de l'utilisateur dont la connexion a été enregistrée.
- ID de transaction. ID attribué à la transaction à l'origine du journal.
- ID de session. ID attribué à la session utilisateur à l'origine du journal.
- Message. Le message du journal. Contient des informations identifiant la signature ou le contrôle de sécurité qui a déclenché l'entrée du journal.

Vous pouvez rechercher n'importe lequel de ces champs ou n'importe quelle combinaison d'informations provenant de différents champs. Votre sélection est limitée uniquement par les fonctionnalités des outils que vous utilisez pour afficher les journaux. Vous pouvez observer les messages de journal du Web App Firewall dans l'interface graphique en accédant à la visionneuse Syslog Citrix ADC, ou vous pouvez vous connecter manuellement à l'appliance Citrix ADC et accéder

aux journaux à partir de l'interface de ligne de commande, ou vous pouvez passer dans le shell et suivre les journaux directement à partir du dossier /var/log/.

Exemple de message de journal de format natif

```
1 Jun 22 19:14:37 <local0.info> 10.217.31.98 06/22/2015:19:14:37 GMT ns
     0-PPE-1 :
2 default APPFW APPFW_cross-site scripting 60 0 :  10.217.253.62 616-PPE1
      y/3upt2K8ySWWId3Kavbxyni7Rw0000
3 pr_ffc http://aaron.stratum8.net/FFC/login.php?login_name=abc&passwd=
4 12345&drinking_pref=on&text_area=%3Cscript%3E%0D%0A&loginButton=
     ClickToLogin&as_sfid=
5 AAAAAAWEXcNQLlSokNmqaYF6dvfqlChNzSMsdyO9JXOJomm2v
6 BwAMOqZIChv21EcgBc3rexIUcfm0vckKlsgoOeC_BArx1Ic4NLxxkWMtrJe4H7SOfkiv9NL7AG4juPIan

7 %3D&as_fid=feeec8758b41740eedeeb6b35b85dfd3d5def30c Cross-site script
     check failed for
8 field text_area="Bad tag: script" <blocked>
9 <!--NeedCopy-->
```

Journaux du format commun des événements (CEF)

Le Web App Firewall prend également en charge les journaux CEF. CEF est une norme de gestion des journaux ouverts qui améliore l'interopérabilité des informations liées à la sécurité provenant de différents périphériques et applications de sécurité et de réseau. CEF permet aux clients d'utiliser un format de journal des événements commun afin que les données puissent être facilement collectées et agrégées pour analyse par un système de gestion d'entreprise. Le message de journal est divisé en différents champs afin que vous puissiez facilement analyser le message et écrire des scripts pour identifier les informations importantes.

Analyse du message de journal CEF

En plus de la date, de l'horodatage, de l'adresse IP du client, du format de journal, de l'appliance, de l'entreprise, de la version de build, du module et des informations de vérification de sécurité, les messages de journal CEF du Web App Firewall incluent les informations suivantes :

- src — adresse IP source
- spt — numéro de port source
- request — URL de la demande
- act — action (par exemple bloquée, transformée)
- msg — message (message concernant la violation du contrôle de sécurité observée)
- cn1 — ID d'événement
- cn2 — ID de transaction HTTP
- cs1 — nom du profil

- cs2 — ID EPI (par exemple PPE1)
- cs3 - ID de session
- cs4 — Gravité (par exemple, INFO, ALERTE)
- CS5 — année de l'événement
- cs6 - Catégorie de violation de signature
- method — Méthode (par exemple GET/POST)

Par exemple, considérez le message de journal au format CEF suivant, qui a été généré lorsqu'une violation d'URL de démarrage a été déclenchée :

```
Jun 12 23:37:17 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0
|APPFW|APPFW_STARTURL|6|src=10.217.253.62 spt=47606 method=GET
request=http://aaron.stratum8.net/FFC/login.html msg=Disallow Illegal
    URL. cn1=1340
cn2=653 cs1=pr_ffc cs2=PPE1 cs3=EsdGd3VD0OaaURLcZnj05Y6DOmE0002 cs4=
    ALERT cs5=2015
act=blocked
<!--NeedCopy-->
```

Le message ci-dessus peut être divisé en différents composants. Reportez-vous au tableau des composants du journal CEP .

Exemple de violation de vérification de demande au format journal CEF : la demande n'est pas bloquée

```
Jun 13 00:21:28 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_FIELDCONSISTENCY|6|src=10.217.253.62 spt=761 method=GET request=
http://aaron.stratum8.net/FFC/login.php?login_name=abc&passwd=
123456789234&drinking_pref=on&text_area=&loginButton=ClickToLogin&
    as_sfid
=
    AAAAAAWIahZuYoIFbjBhYMP05mJLTwEfIY0a7AKGMg3jIBaKmwtK4t7M7lNxOgj7Gmd3SZc8KUj6CP

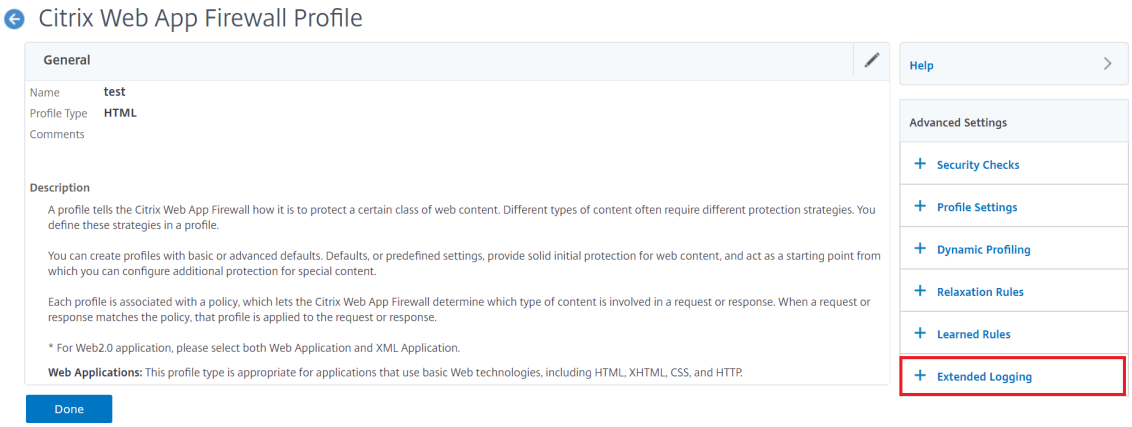
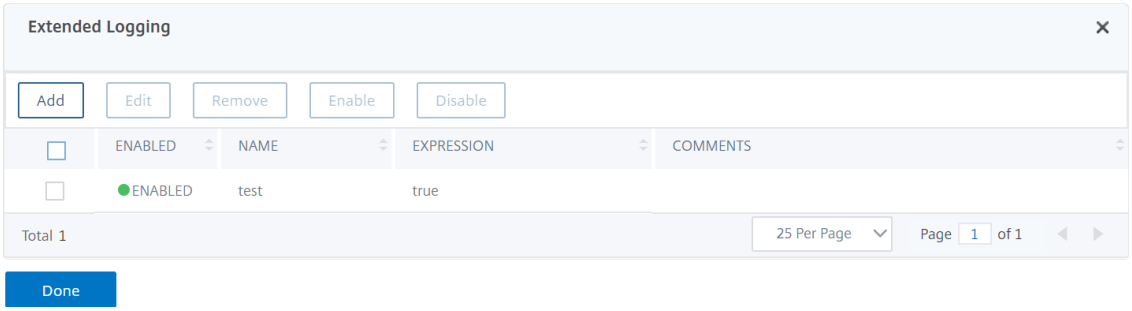
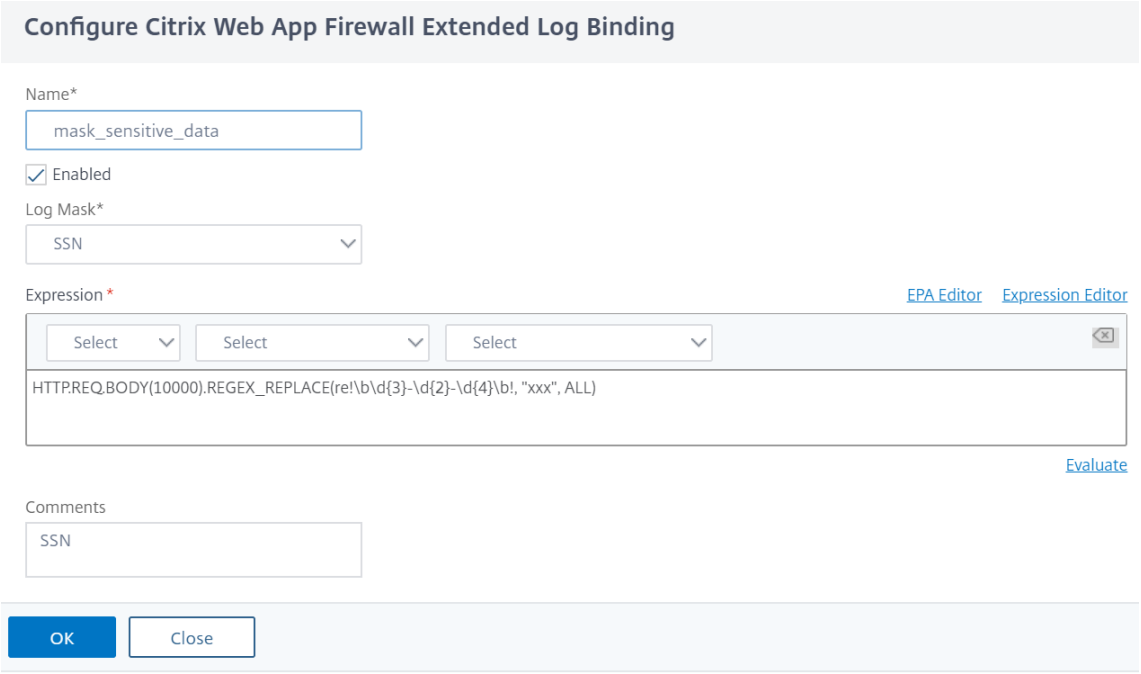
7W5kIWDRHN8PtK1Zc-txHkHNx1WknuG9DzTuM7t1THhluevXu9I4kp8%3D&as_fid=
    feeec8758b4174
0eedeeb6b35b85dfd3d5def30c msg=Field consistency check failed for field
     passwd cn1=1401
cn2=707 cs1=pr_ffc cs2=PPE1 cs3=Ycby5IvjL6FoVa6Ah94QFTIUpC80001 cs4=
    ALERT cs5=2015 act=
not blocked
<!--NeedCopy-->
```

Exemple d'une violation de vérification de réponse au format CEF : la réponse est transformée


```
1 Jun 13 00:25:31 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
     .0|APPFW|
2 APPFW_SAFECOMMERCE|6|src=10.217.253.62 spt=34041 method=GET request=
3 http://aaron.stratum8.net/FFC/CreditCardMind.html msg=Maximum number of
      potential credit
4 card numbers seen cn1=1470 cn2=708 cs1=pr_ffc cs2=PPE1
5 cs3=Ycby5IvjL6FoVa6Ah94QFTIUpC80001 cs4=ALERT cs5=2015 act=transformed
6 <!--NeedCopy-->
```

Exemple de violation de signature côté requête au format CEF : la demande est bloquée

```
1 Jun 13 01:11:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
     .0|APPFW|
2 APPFW_SIGNATURE_MATCH|6|src=10.217.253.62 spt=61141 method=GET request=
3 http://aaron.stratum8.net/FFC/wwwboard/passwd.txt msg=Signature
     violation rule ID 807:
4 web-cgi /wwwboard/passwd.txt access  cn1=140 cn2=841 cs1=pr_ffc cs2=
     PPE0
5 cs3=OyTgjbXBqcpBFeENKDlde3OkMQ00001 cs4=ALERT cs5=2015 cs6=web-cgi act=
     blocked
6 <!--NeedCopy-->
```

Enregistrement de la géolocalisation dans les messages de violation du pare-feu Web App Firewall

La géolocalisation, qui identifie l'emplacement géographique d'où proviennent les demandes, peut vous aider à configurer le Web App Firewall pour un niveau de sécurité optimal. Pour contourner les implémentations de sécurité telles que la limitation de débit, qui reposent sur les adresses IP des clients, les logiciels malveillants ou les ordinateurs malveillants peuvent continuer à modifier l'adresse IP source dans les demandes. L'identification de la région spécifique d'où proviennent les demandes peut aider à déterminer si les demandes proviennent d'un utilisateur valide ou d'un appareil tentant de lancer des cyberattaques. Par exemple, si un nombre excessif de demandes sont reçues d'une zone spécifique, il est facile de déterminer si elles sont envoyées par des utilisateurs ou par une machine non fiable. L'analyse de géolocalisation du trafic reçu peut être très utile pour dévier les attaques telles que les attaques par déni de service (DoS).

Le Web App Firewall vous offre la commodité d'utiliser la base de données Citrix ADC intégrée pour identifier les emplacements correspondant aux adresses IP d'où proviennent les requêtes malveillantes. Vous pouvez ensuite appliquer un niveau de sécurité plus élevé pour les demandes provenant de ces emplacements. Les expressions de stratégie Citrix Advanced (PI) vous permettent de configurer des stratégies basées sur l'emplacement qui peuvent être utilisées conjointement avec la base de données d'emplacement intégrée pour personnaliser la protection par pare-feu, renforçant ainsi

votre défense contre les attaques coordonnées lancées par des clients malveillants dans une région spécifique.

Vous pouvez utiliser la base de données intégrée Citrix ADC ou n'importe quelle autre base de données. Si la base de données ne contient aucune information d'emplacement pour l'adresse IP du client particulier, le journal CEF affiche la géolocalisation en tant que géolocalisation inconnue.

Remarque : La journalisation de la géolocalisation utilise le format CEF (Common Event Format). Par défaut, la journalisation CEF et GeolocationLogging sont désactivées. Vous devez explicitement activer les deux paramètres.

Exemple de message de journal CEF affichant des informations de géolocalisation

```
June 8 00:21:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_STARTURL|6|src=10.217.253.62 geolocation=NorthAmerica.US.Arizona.
    Tucson.\*.\*
spt=18655 method=GET request=http://aaron.stratum8.net/FFC/login.html
msg=Disallow Illegal URL. cn1=77 cn2=1547 cs1=test_pr_adv cs2=PPE1
cs3=KDynjg1pbFtfhC/nt0rBU1o/Tyg0001 cs4=ALERT cs5=2015 act=not blocked
<!--NeedCopy-->
```

Exemple de message de journal indiquant geolocation= Unknown

```
June 9 23:50:53 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|
APPFW|APPFW_STARTURL|6|src=10.217.30.251 geolocation=Unknown spt=5086
method=GET request=http://aaron.stratum8.net/FFC/login.html msg=
    Disallow Illegal URL.
cn1=74 cn2=1576 cs1=test_pr_adv cs2=PPE2 cs3=
    PyR0eOEM4gf6GJiTyauiHByL88E0002
cs4=ALERT cs5=2015 act=not blocked
<!--NeedCopy-->
```

Utilisation de la ligne de commande pour configurer l'action du journal et d'autres paramètres de journal

Pour configurer l'action de journal pour les contrôles de sécurité d'un profil à l'aide de la ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `set appfw profile <name> SecurityCheckAction ([log] | [none])`
- `unset appfw profile <name> SecurityCheckAction`

Exemples


```
set appfw profile pr_ffc StartURLAction log

unset appfw profile pr_ffc StartURLAction
```

Pour configurer la journalisation CEF à l'aide de la ligne de commande

La journalisation CEF est désactivée par défaut. À l'invite de commandes, tapez l'une des commandes suivantes pour modifier ou afficher le paramètre actuel :

- `set appfw settings CEFLogging on`
- `unset appfw settings CEFLogging`
- `sh appfw settings | grep CEFLogging`

Pour configurer la consignation des numéros de carte de crédit à l'aide de la ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `set appfw profile <name> -doSecureCreditCardLogging ([ON] | [OFF])`
- `unset appfw profile <name> -doSecureCreditCardLogging`

Pour configurer la journalisation de la géolocalisation à l'aide de la ligne de commande

1. Utilisez la commande set pour activer GeolocationLogging. Vous pouvez activer la journalisation CEF en même temps. Utilisez la commande unset pour désactiver la journalisation de géolocalisation. La commande show affiche les paramètres actuels de tous les paramètres de Web App Firewall, sauf si vous incluez la commande grep pour afficher le paramètre d'un paramètre spécifique.
   - `set appfw settings GeoLocationLogging ON [CEFLogging ON]`
   - `unset appfw settings GeoLocationLogging`
   - `sh appfw settings | grep GeoLocationLogging`
2. Spécifiez la base de données

   ```
   add locationfile /var/netscaler/inbuilt_db/Citrix_netscaler_InBuilt_GeoIP_DB
   .csv
   ```

   ou

   ```
   add locationfile <path to database file>
   ```

Personnalisation des journaux du Web App Firewall

Les expressions de format par défaut (PI) vous permettent de personnaliser les informations incluses dans les journaux. Vous avez la possibilité d'inclure les données spécifiques que vous souhaitez capturer dans les messages de journal générés par le Web App Firewall. Par exemple, si vous utilisez l'authentification AAA-TM en même temps que les vérifications de sécurité du Web App Firewall et que vous souhaitez connaître l'URL consultée qui a déclenché la violation du contrôle de sécurité, le nom de l'utilisateur qui a demandé l'URL, l'adresse IP source et le port source à partir duquel l'utilisateur

a envoyé la demande, vous peut utiliser les commandes suivantes pour spécifier des messages de journal personnalisés qui incluent toutes les données :

```
1 > sh version
2 NetScaler NS12.1: Build 50.0013.nc, Date: Aug 28 2018, 10:51:08   (64-
     bit)
3  Done
4 <!--NeedCopy-->
```

```
1 > add audit messageaction custom1 ALERT 'HTTP.REQ.URL + " " + HTTP.REQ.
     USER.NAME + " " + CLIENT.IP.SRC + ":" + CLIENT.TCP.SRCPORT'
2 Warning: HTTP.REQ.USER has been deprecated. Use AAA.USER instead.
3  Done
4 <!--NeedCopy-->
```

```
1 > add appfw profile test_profile
2  Done
3 <!--NeedCopy-->
```

```
1 > add appfw policy appfw_pol true test_profile -logAction custom1
2  Done
3 <!--NeedCopy-->
```

Configuration de la stratégie Syslog pour séparer les journaux du Web App Firewall

Le pare-feu Web App vous offre la possibilité d'isoler et de rediriger les messages du journal de sécurité du Web App Firewall vers un autre fichier journal. Cela peut être souhaitable si le Web App Firewall génère un grand nombre de journaux, ce qui rend difficile l'affichage des autres messages de journal Citrix ADC. Vous pouvez également utiliser cette option lorsque vous souhaitez uniquement afficher les messages du journal du Web App Firewall et que vous ne souhaitez pas voir les autres messages de journal.

Pour rediriger les journaux du Web App Firewall vers un autre fichier journal, configurez une action Syslog pour envoyer les journaux du Web App Firewall à une autre fonction de journalisation. Vous pouvez utiliser cette action lors de la configuration de la stratégie Syslog et la lier globalement pour une utilisation par Web App Firewall.

Exemple :

1. Passez au shell et utilisez un éditeur tel que vi pour éditer le fichier /etc/syslog.conf. Ajoutez une nouvelle entrée pour utiliser local2.* pour envoyer les journaux vers un fichier distinct, comme illustré dans l'exemple suivant :

   ```
   local2.\* /var/log/ns.log.appfw
   ```


2. Redémarrez le processus Syslog. Vous pouvez utiliser la commande grep pour identifier l'ID de processus Syslog (PID), comme illustré dans l'exemple suivant :

   ```
   root@ns\## **ps -A | grep syslog**

   1063 ?? Ss 0:03.00 /usr/sbin/syslogd -b 127.0.0.1 -n -v -v -8 -C

   root@ns## **kill -HUP** 1063
   ```

3. À partir de l'interface de ligne de commande, configurez l'action et la stratégie Syslog. Liez-le en tant que stratégie globale de Web App Firewall.

```
> add audit syslogAction sysact 1.1.1.1 -logLevel ALL -logFacility LOCAL2

> add audit syslogPolicy syspol1 ns_true sysact1

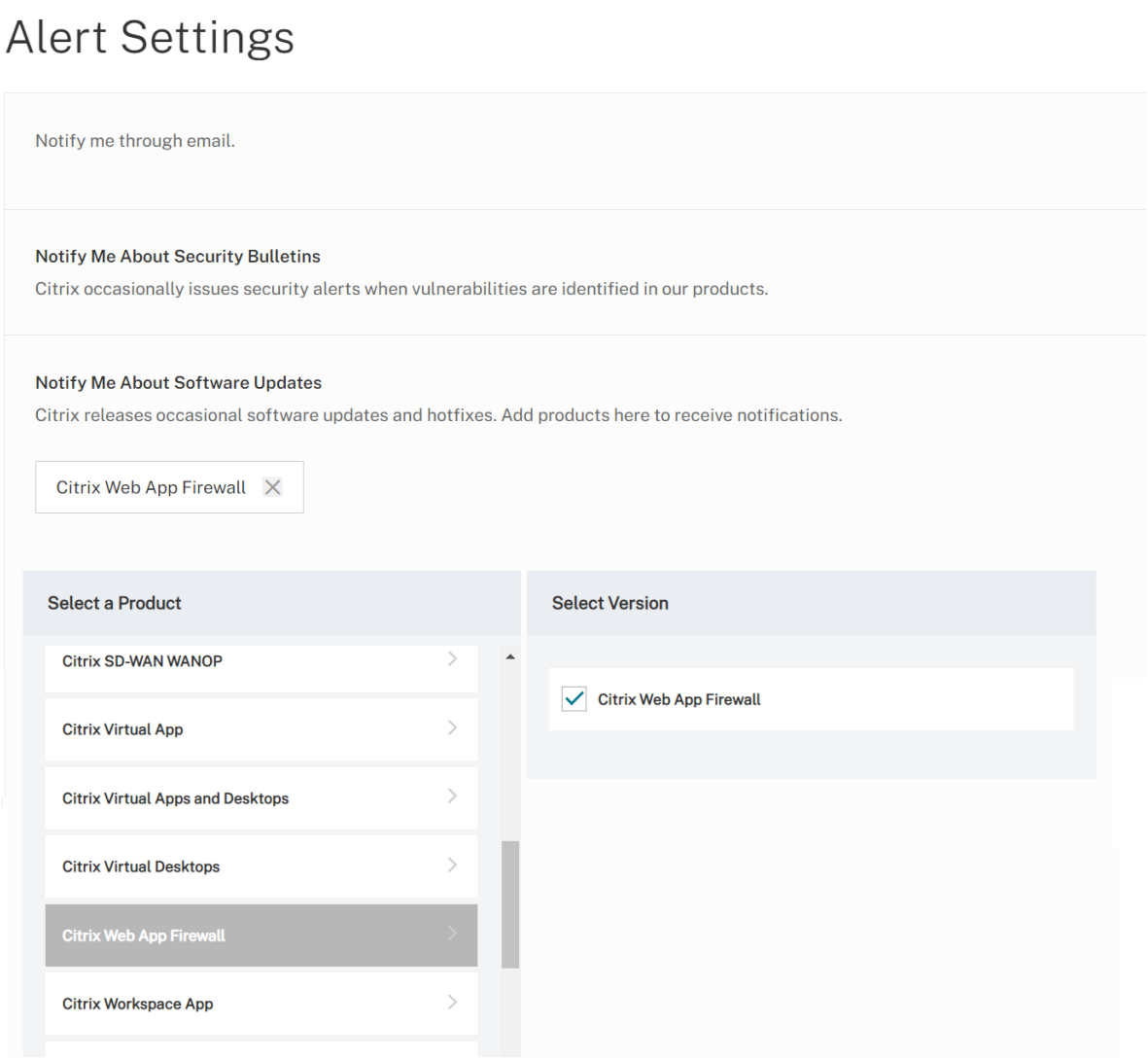
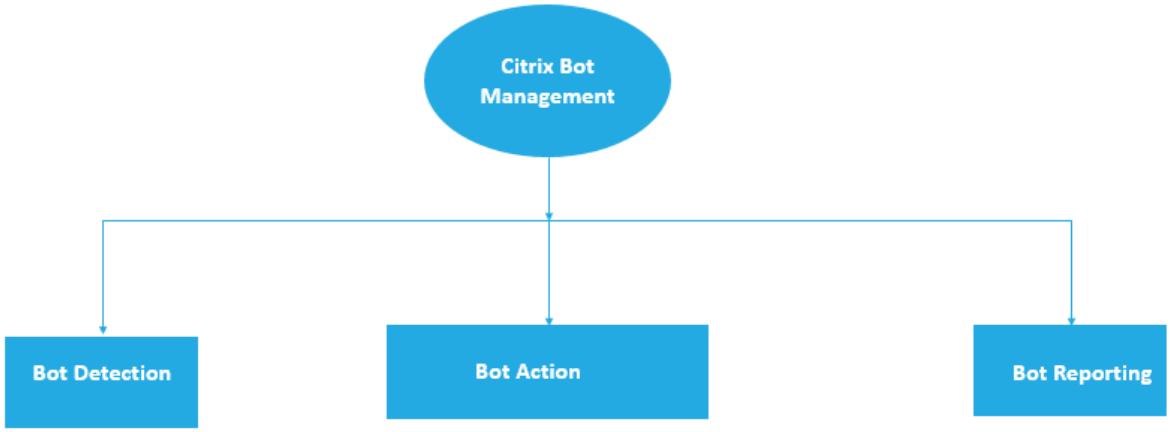
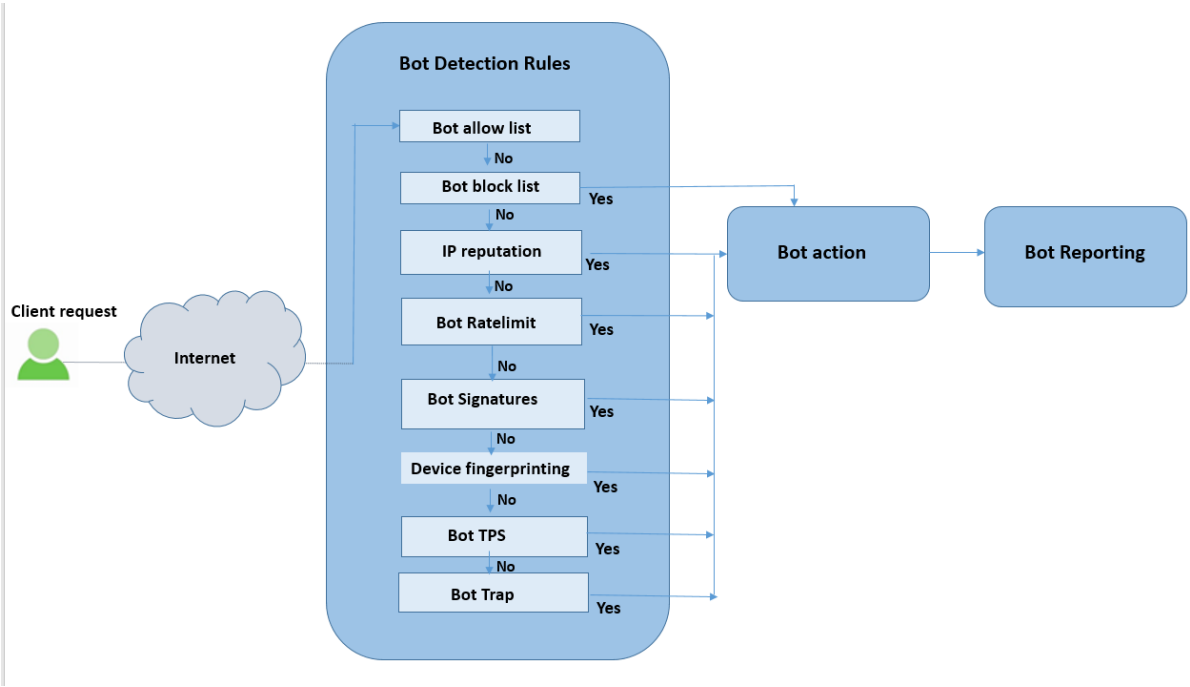
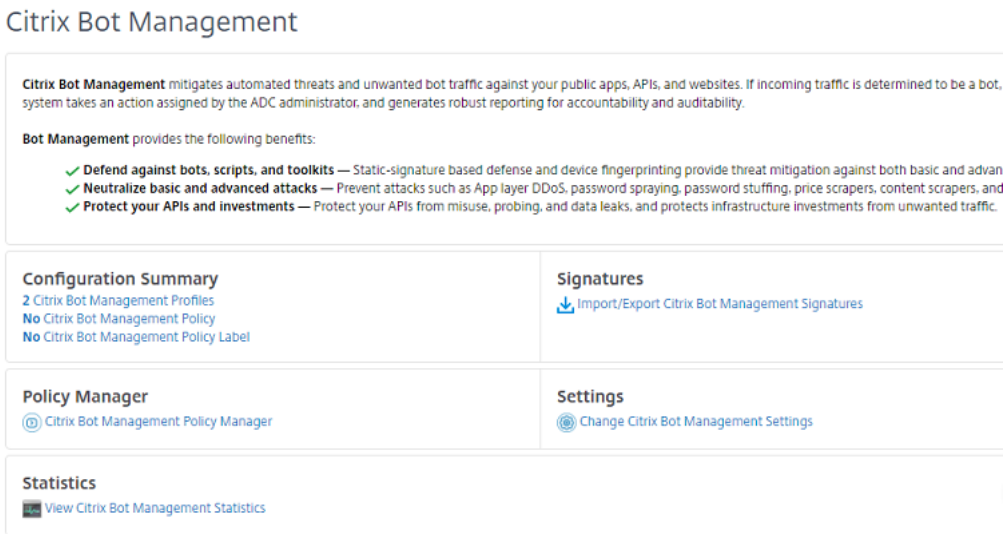
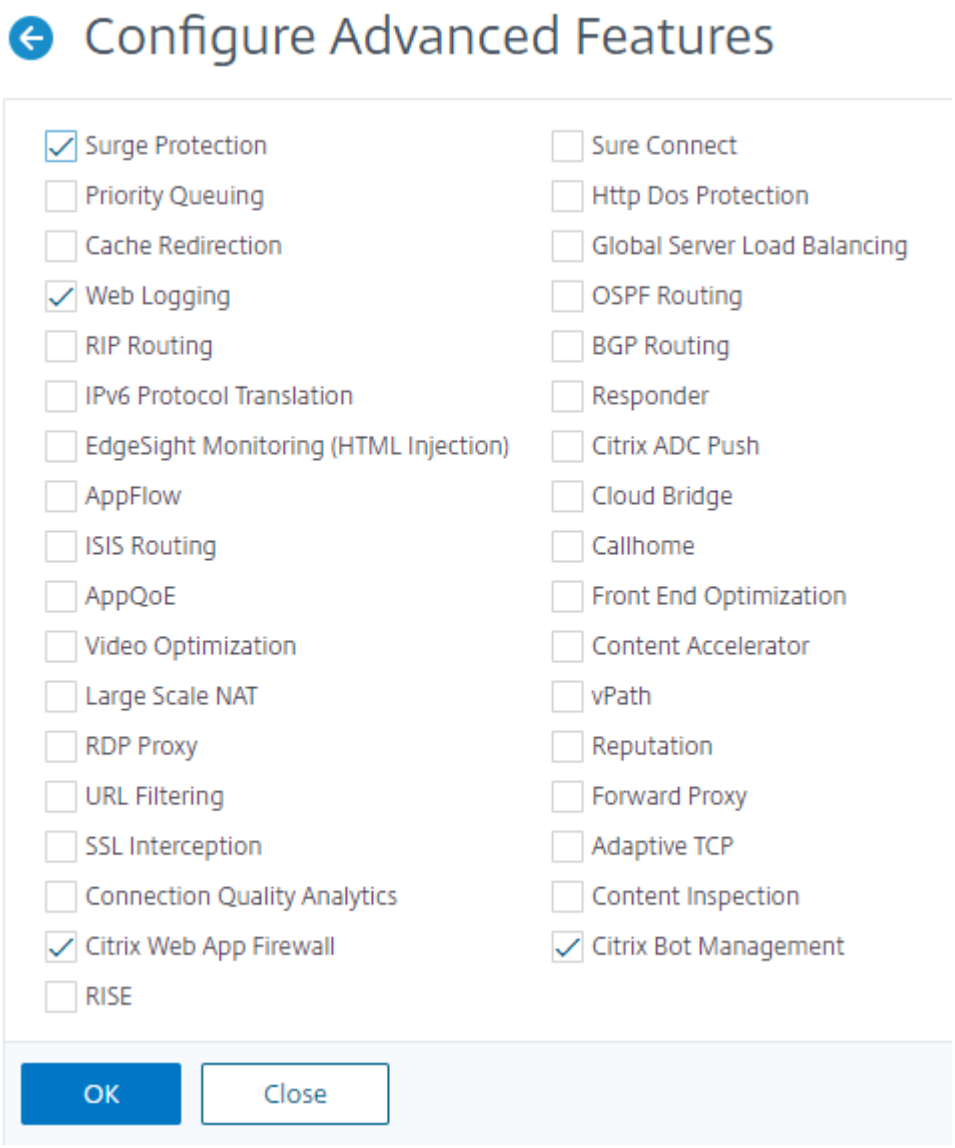
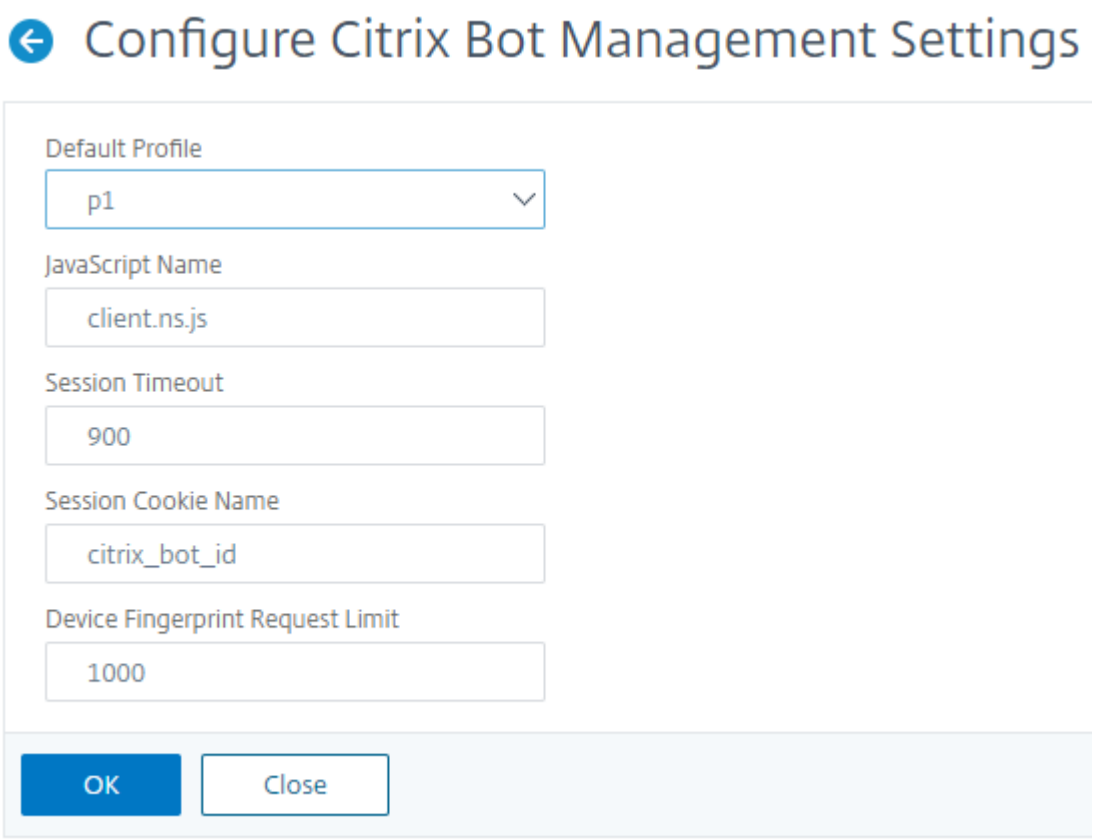
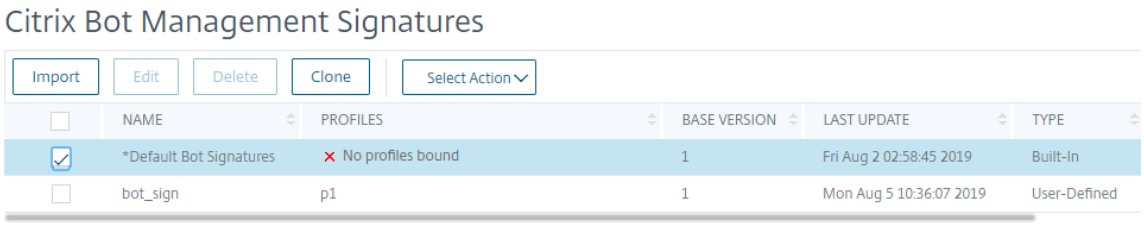
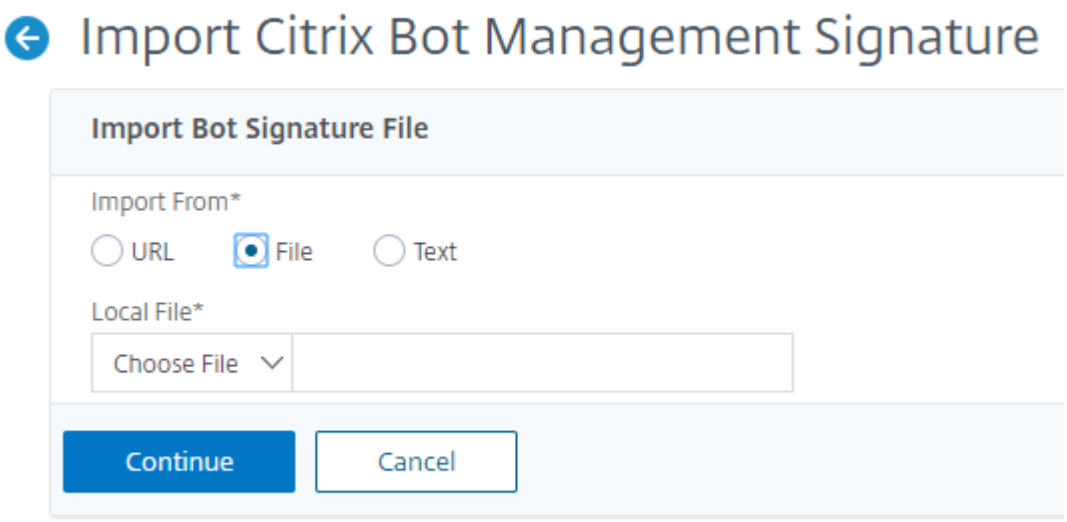
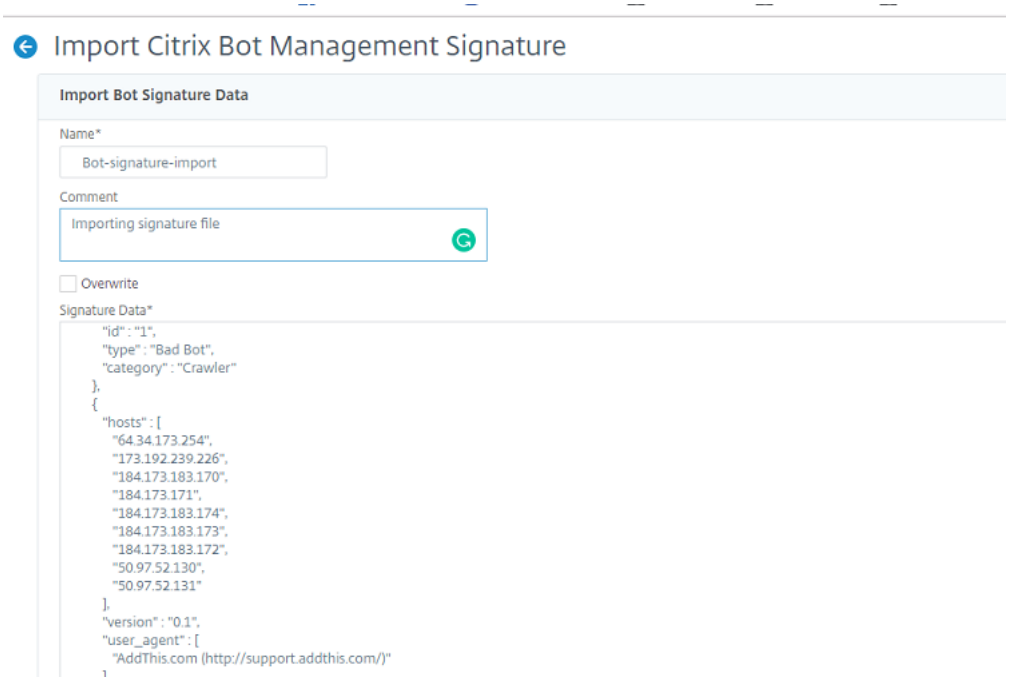
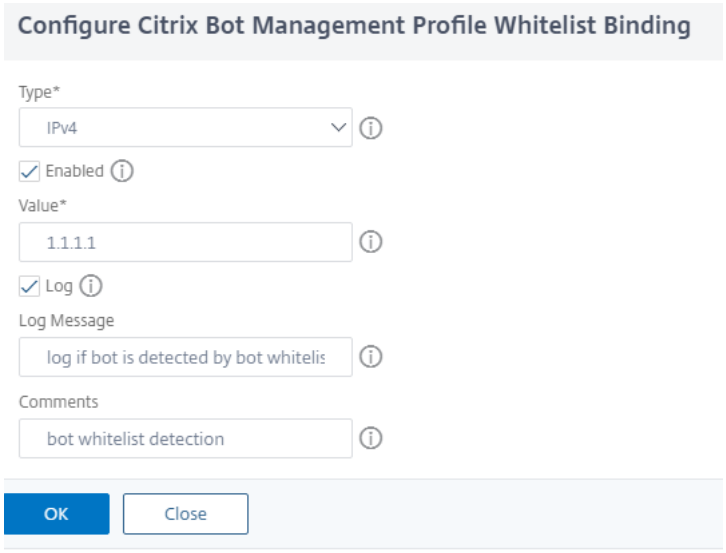
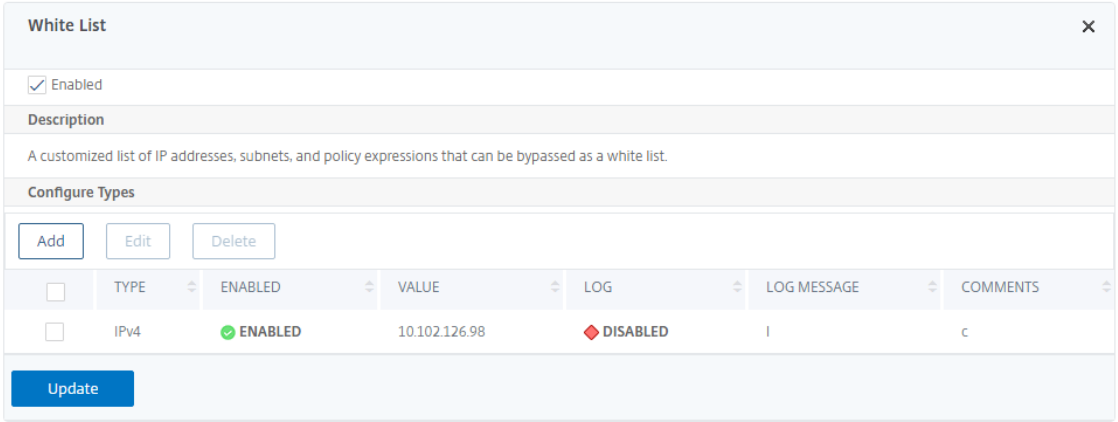
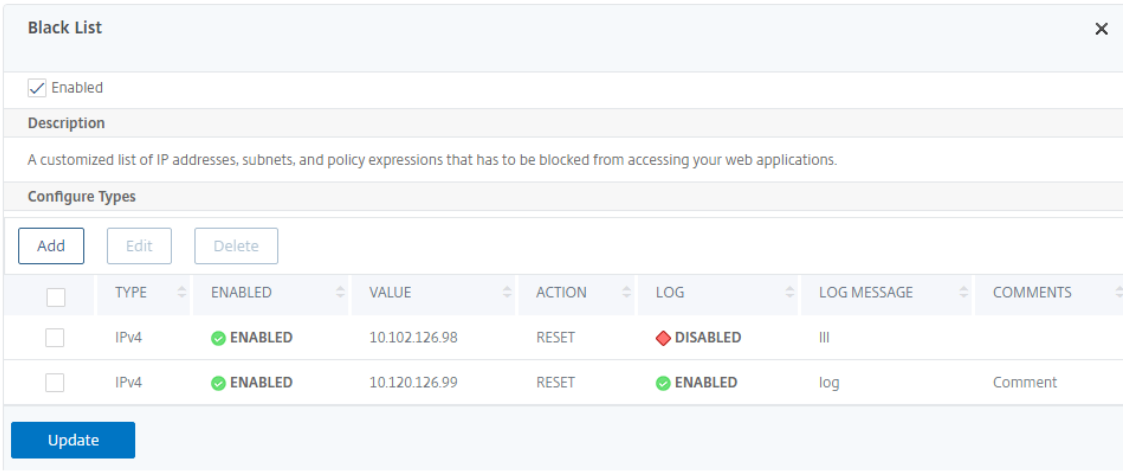
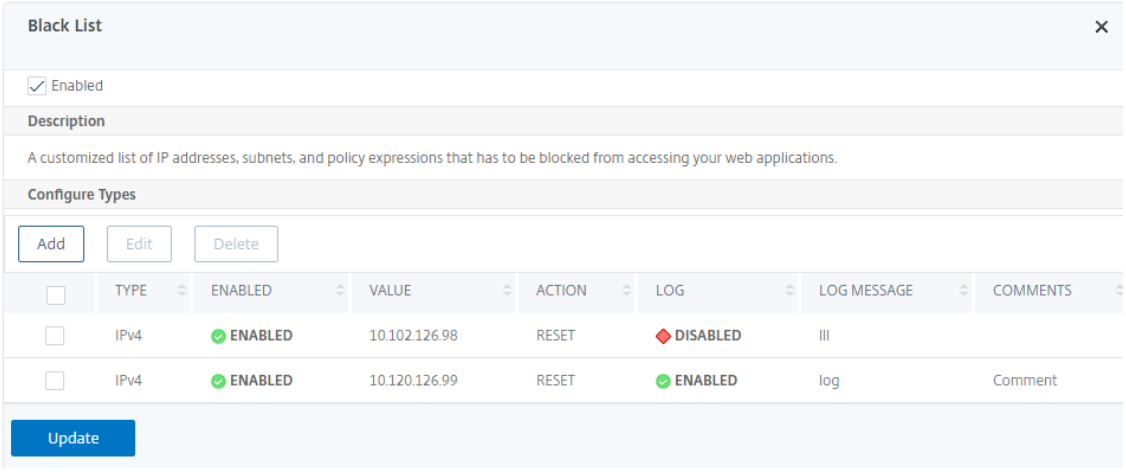
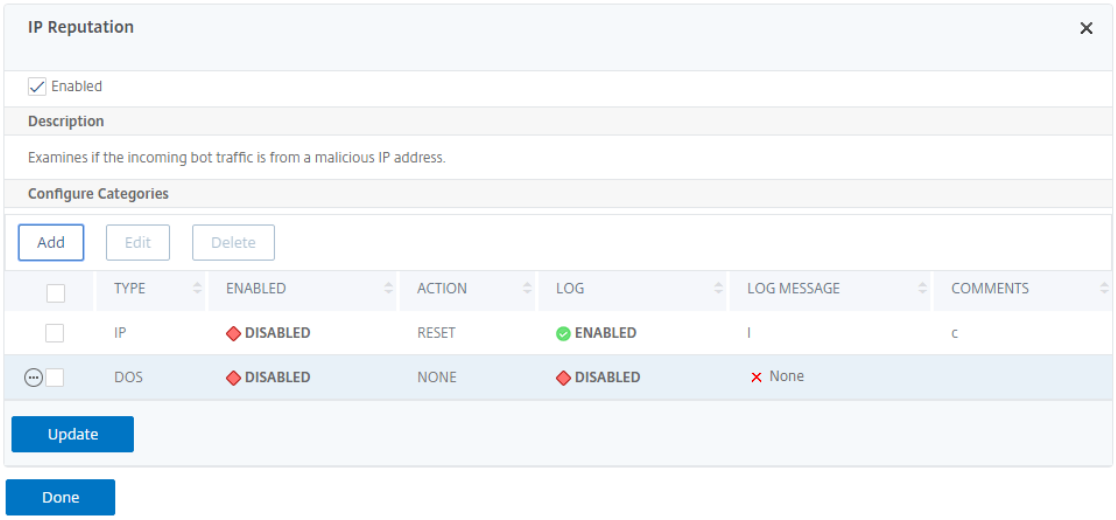
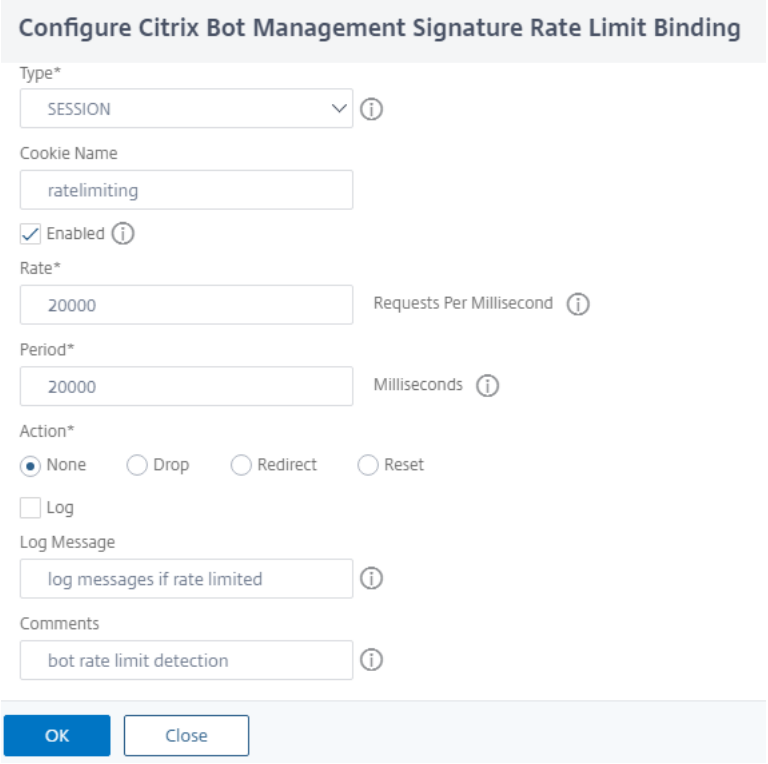
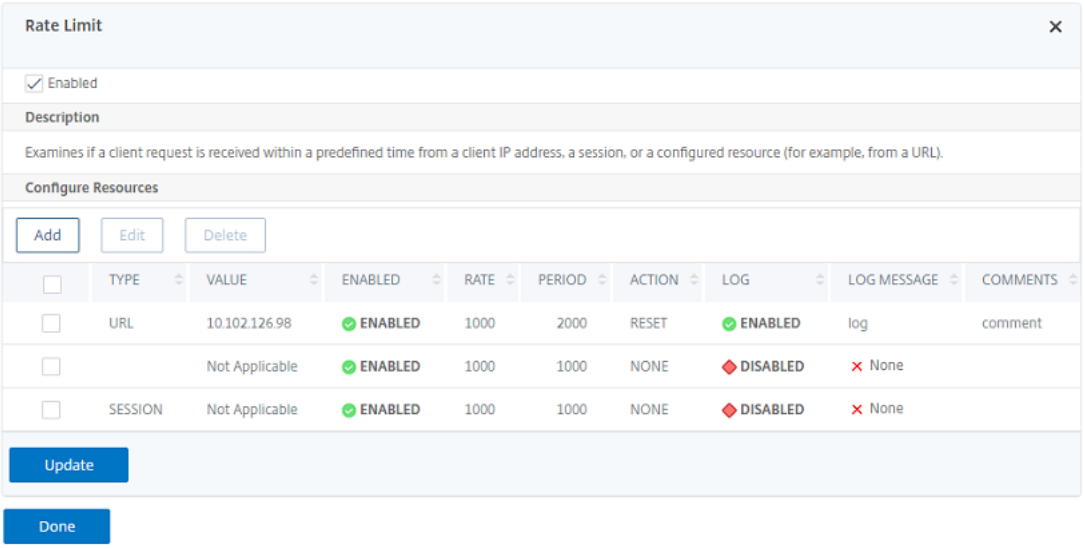
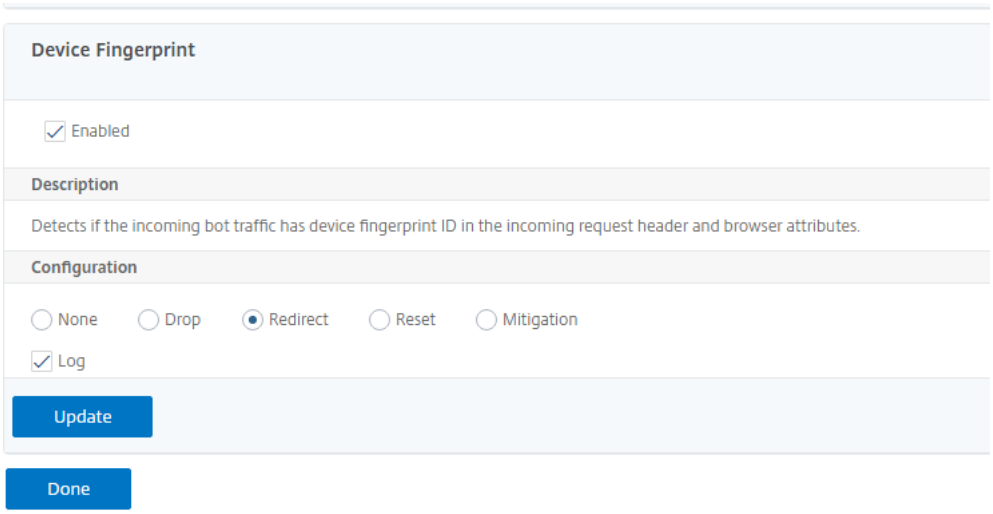
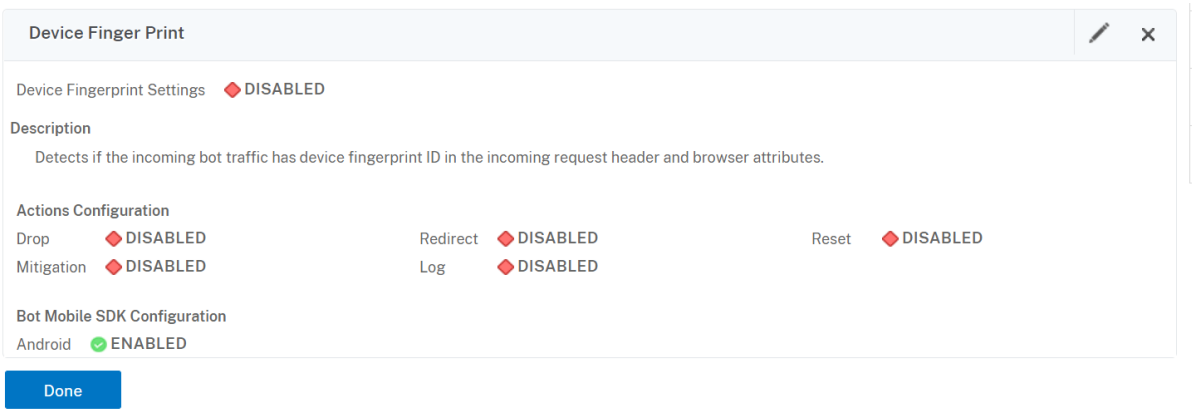
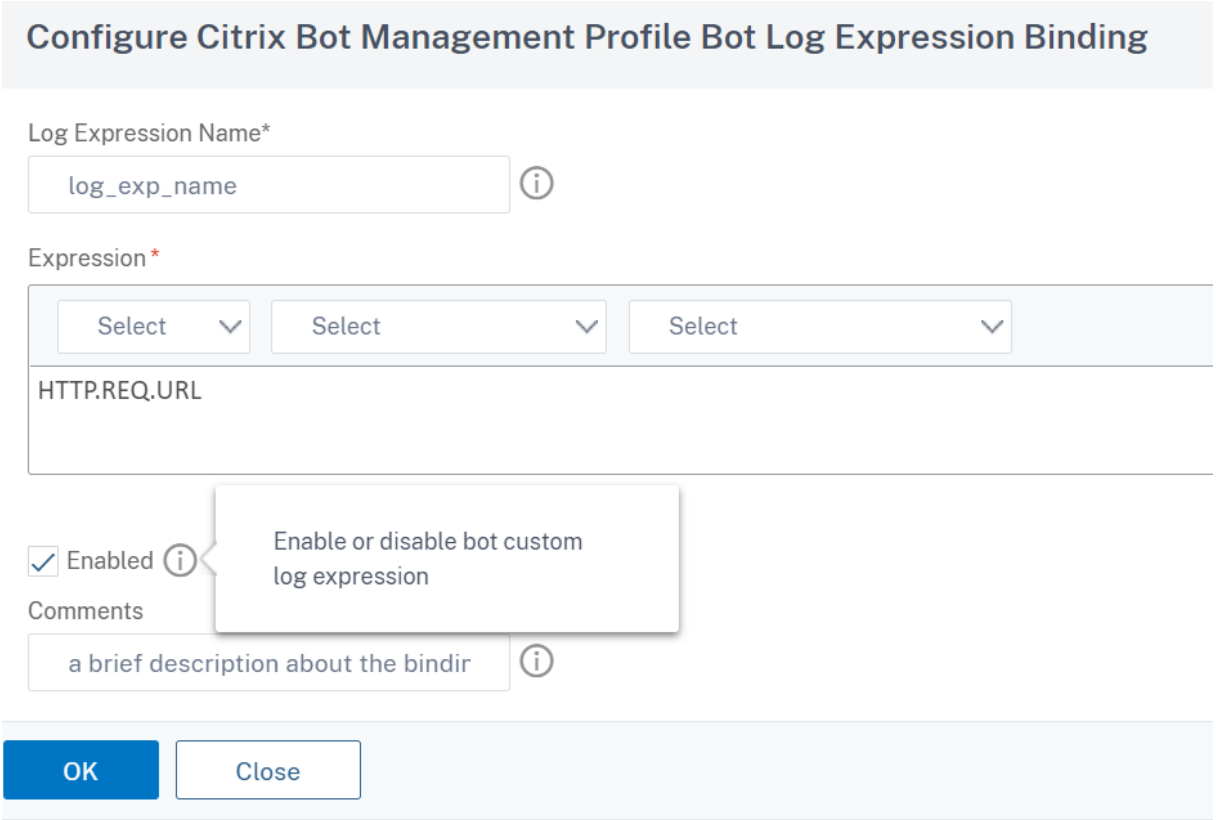
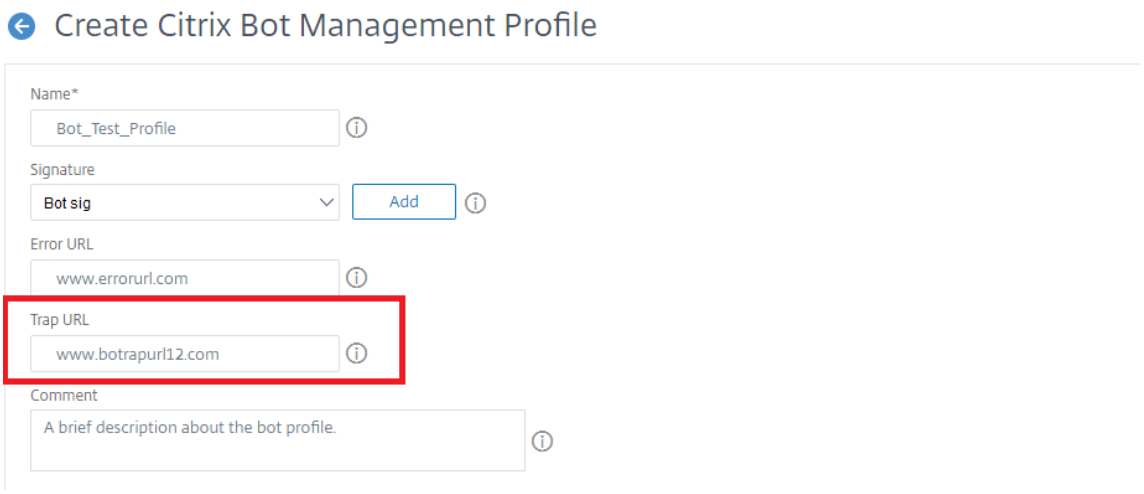
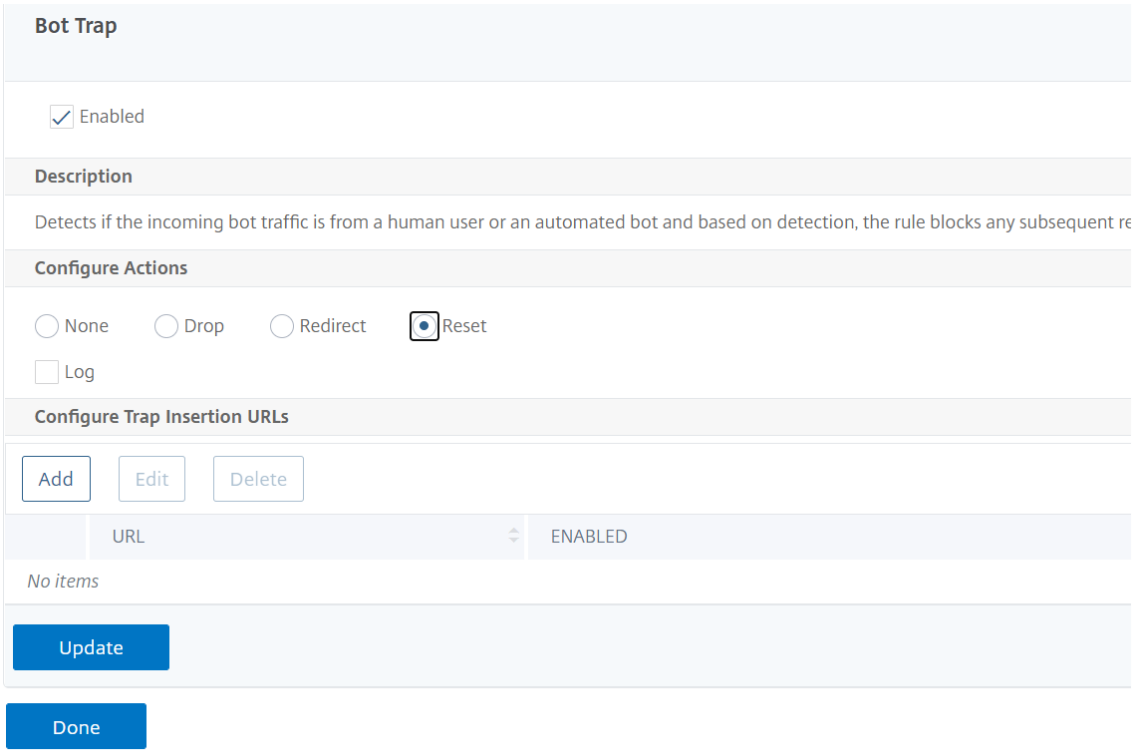
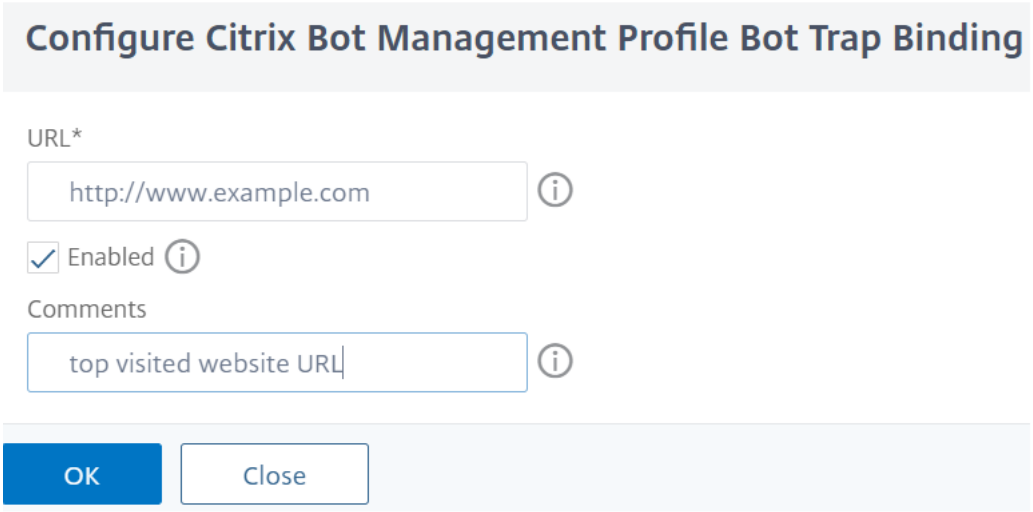
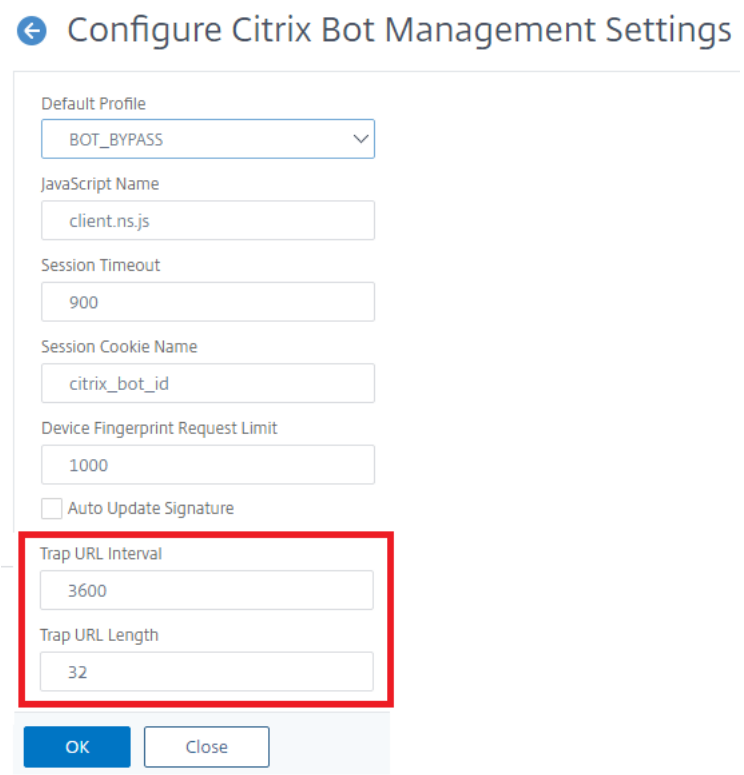
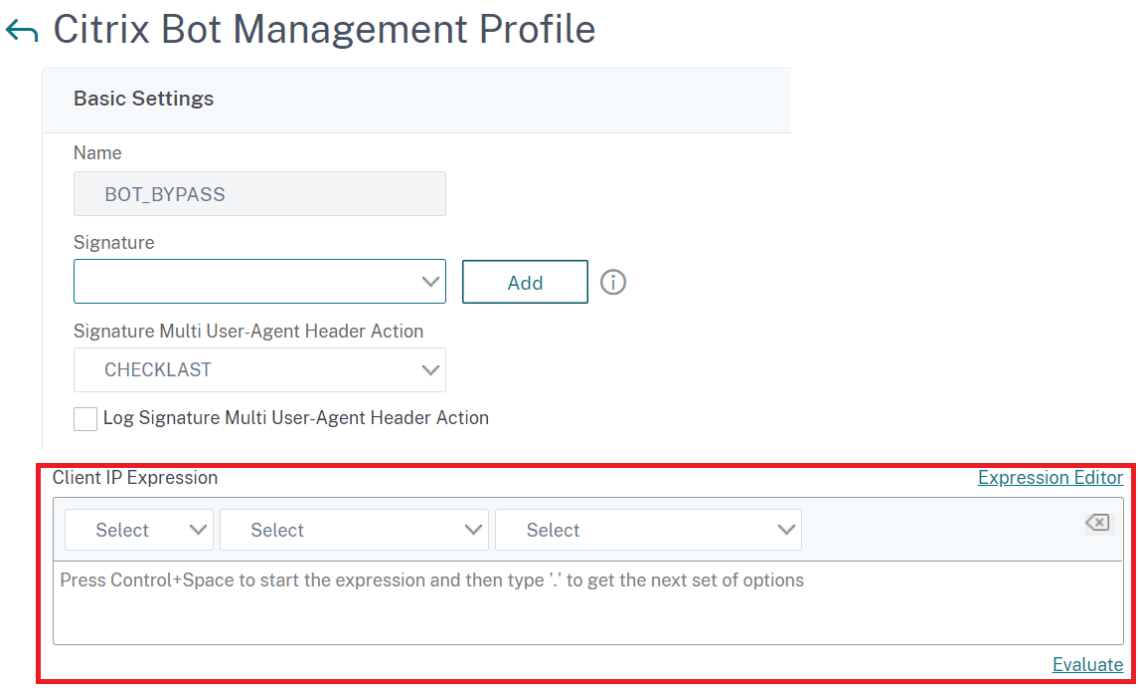
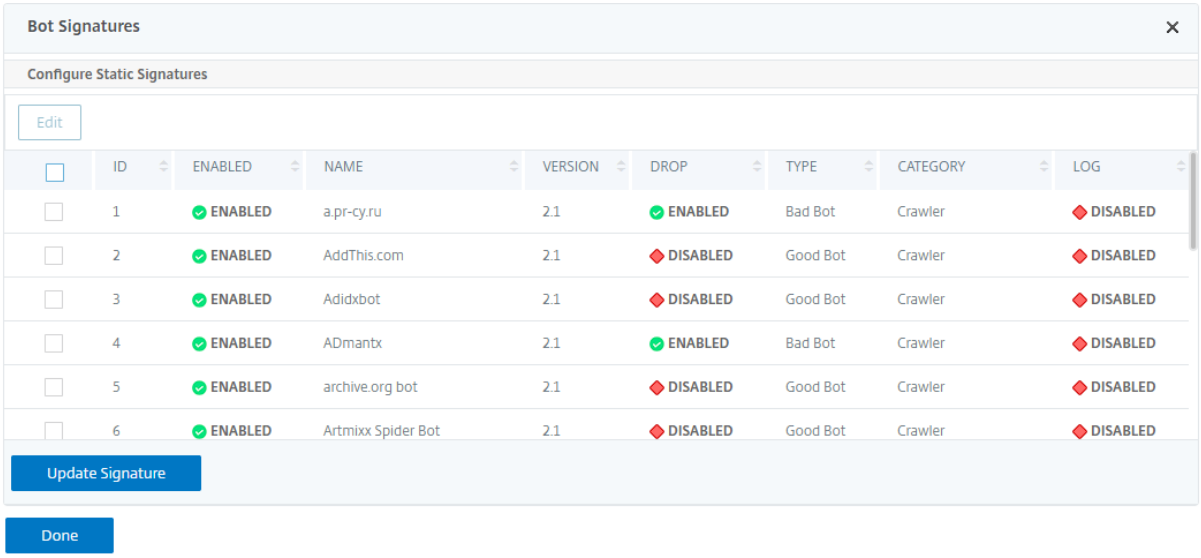
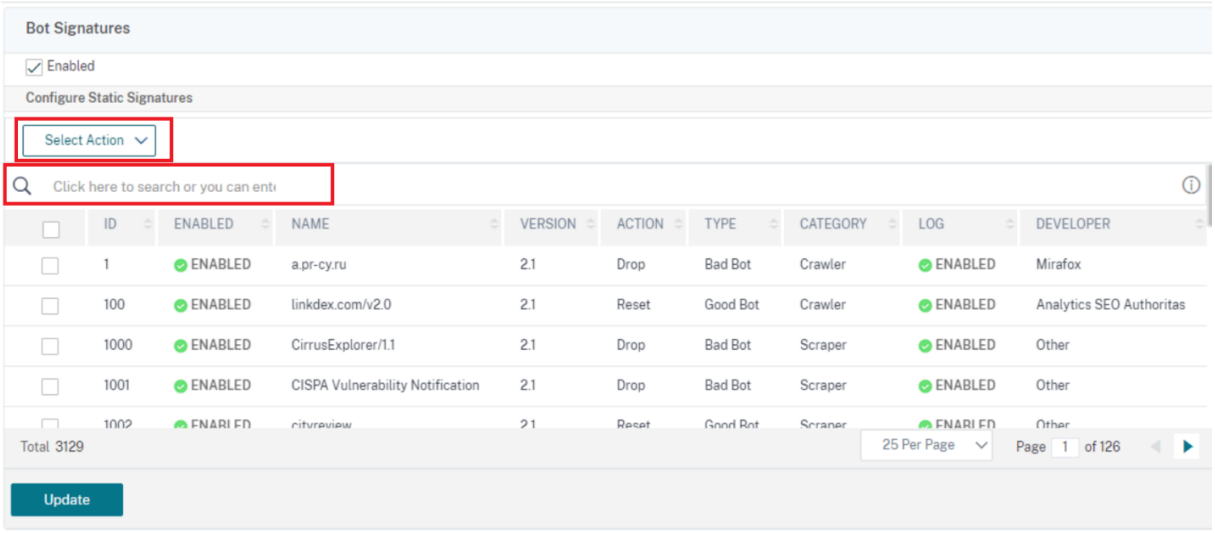
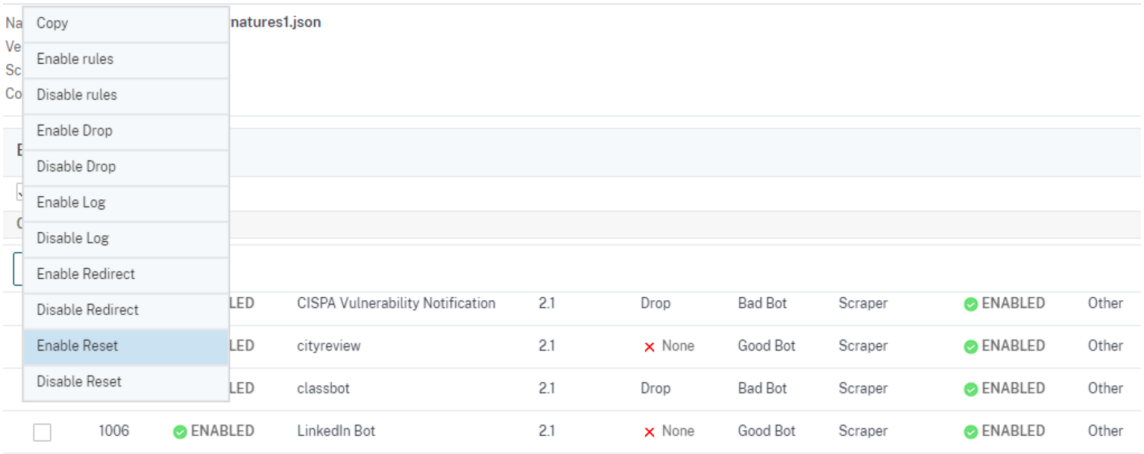
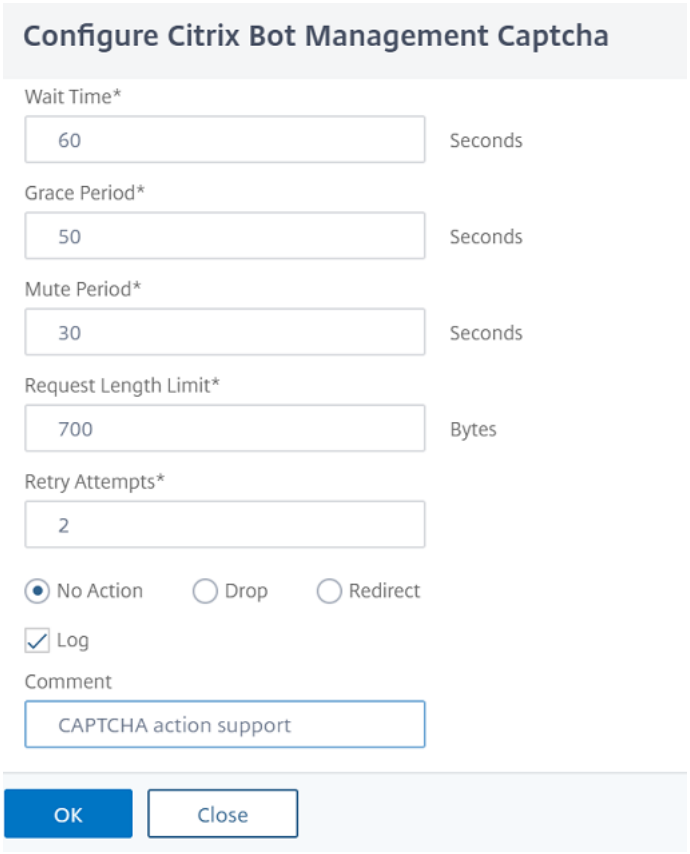
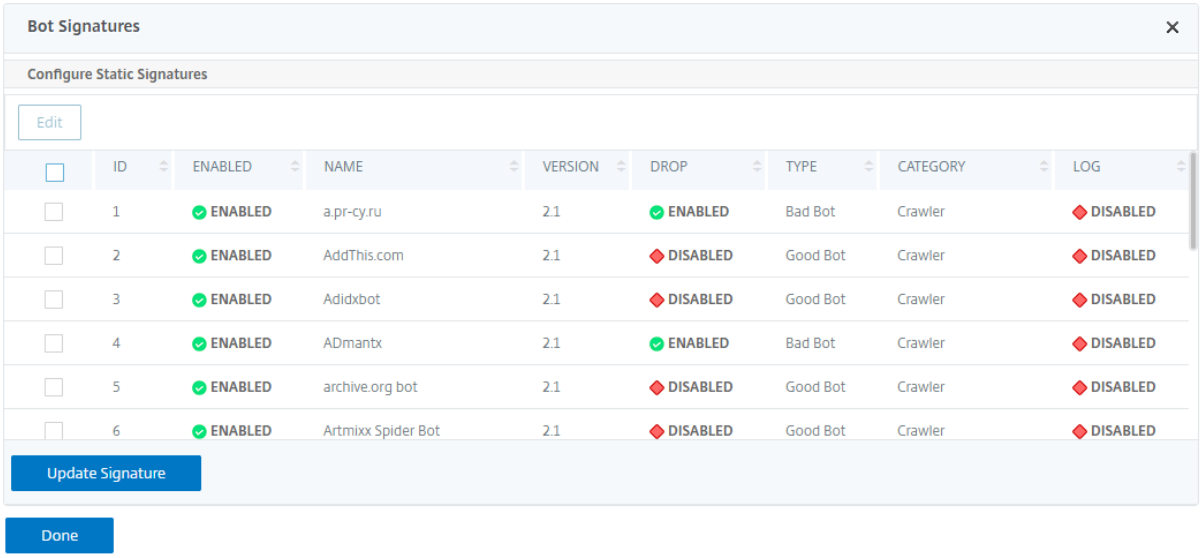
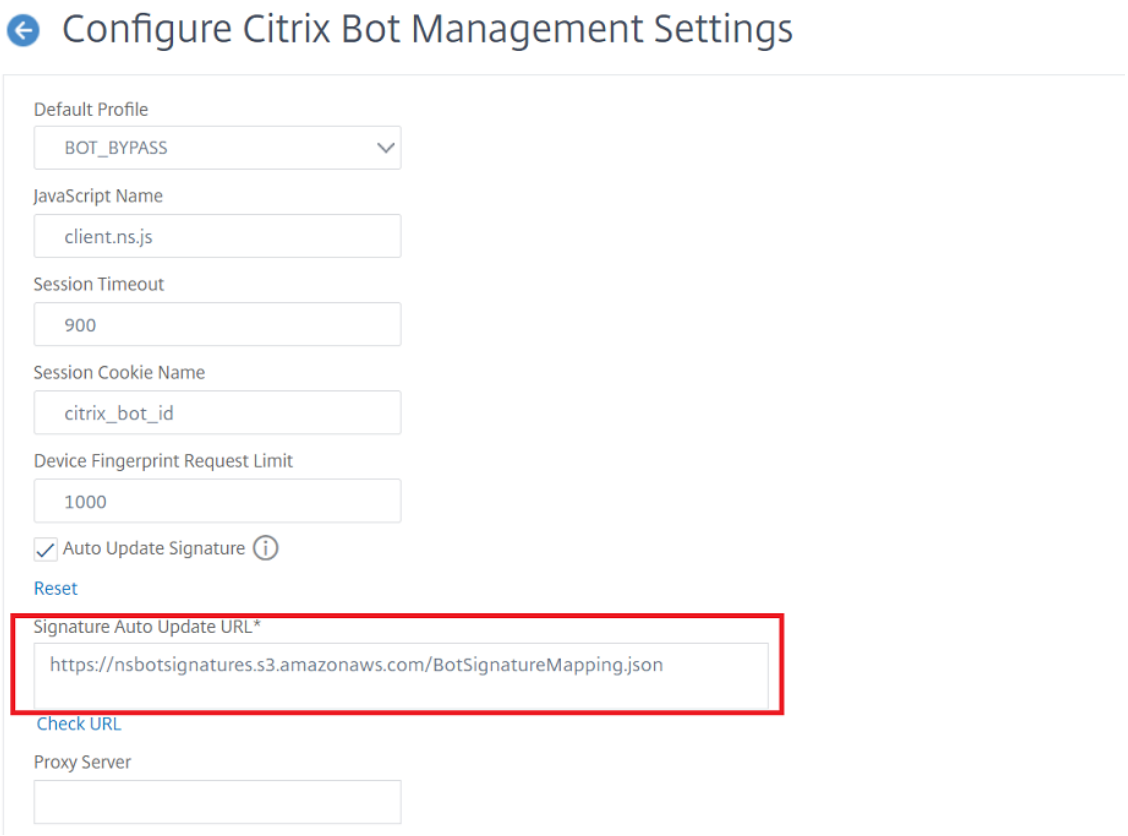
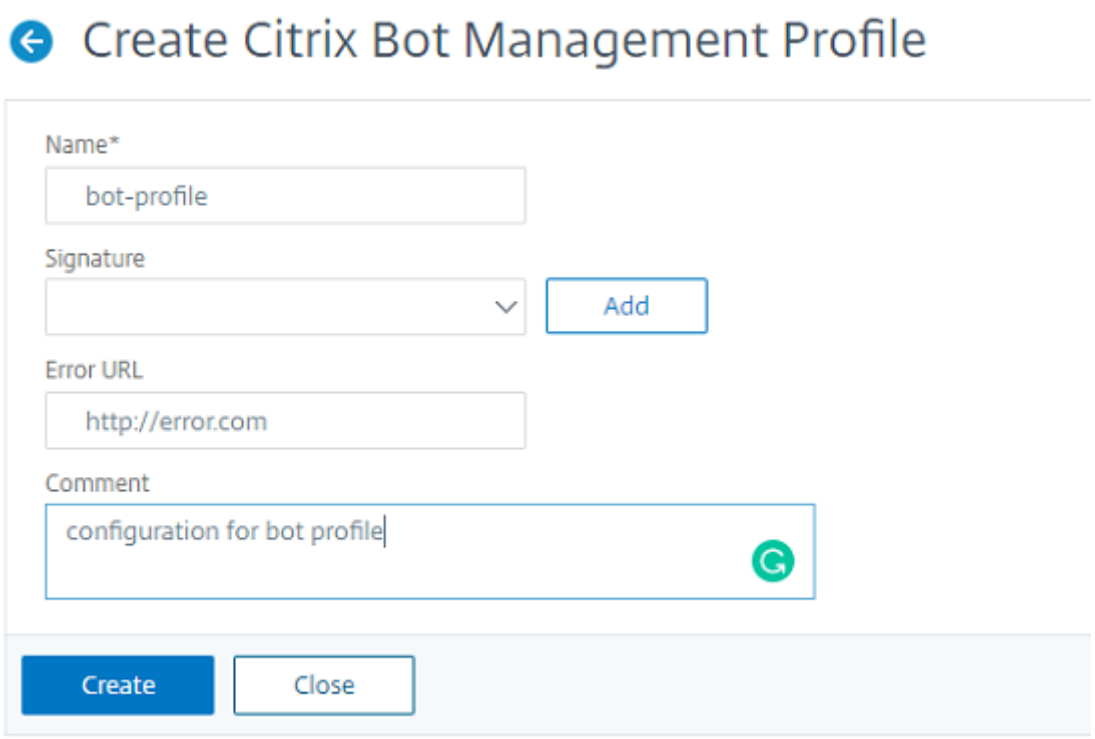
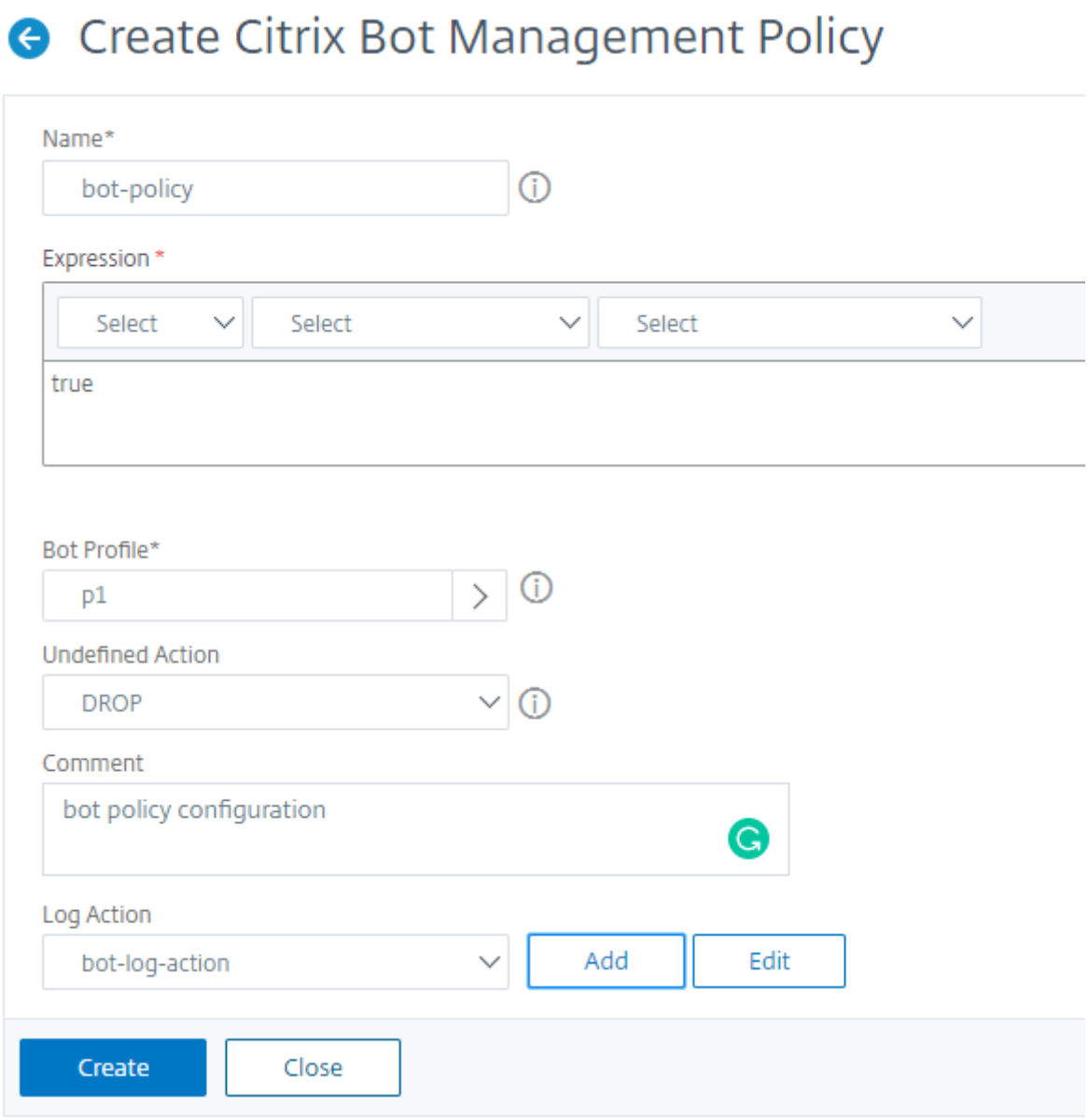
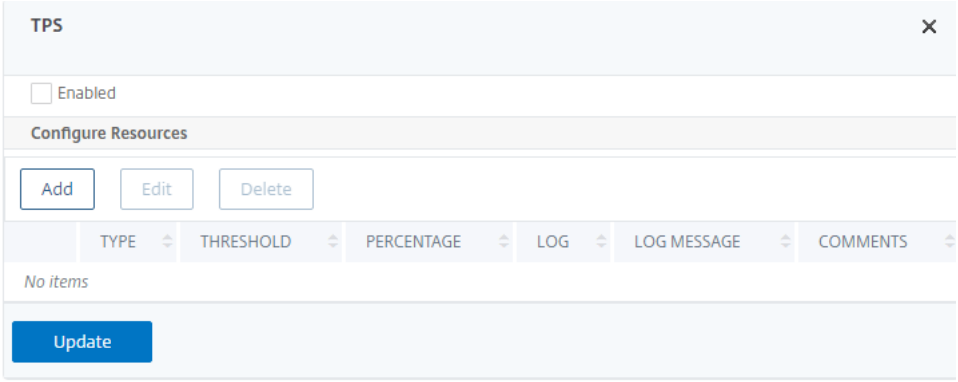
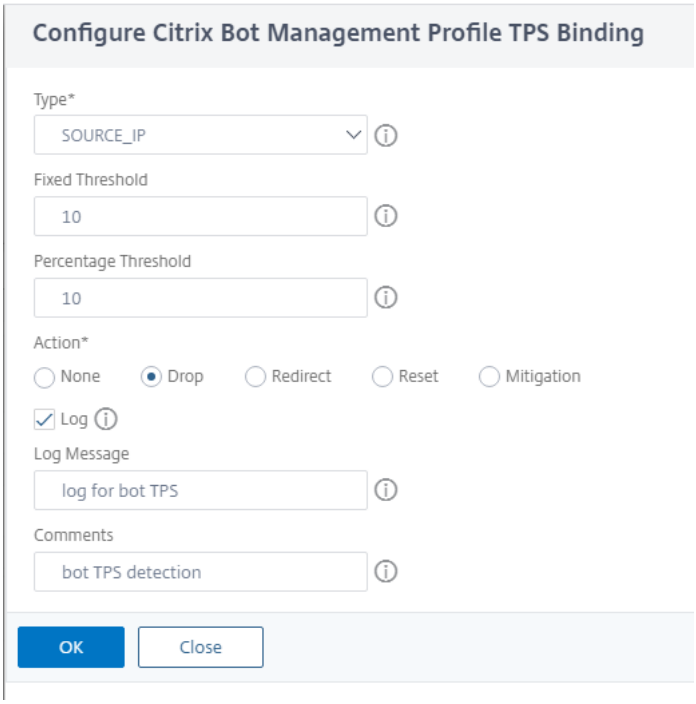
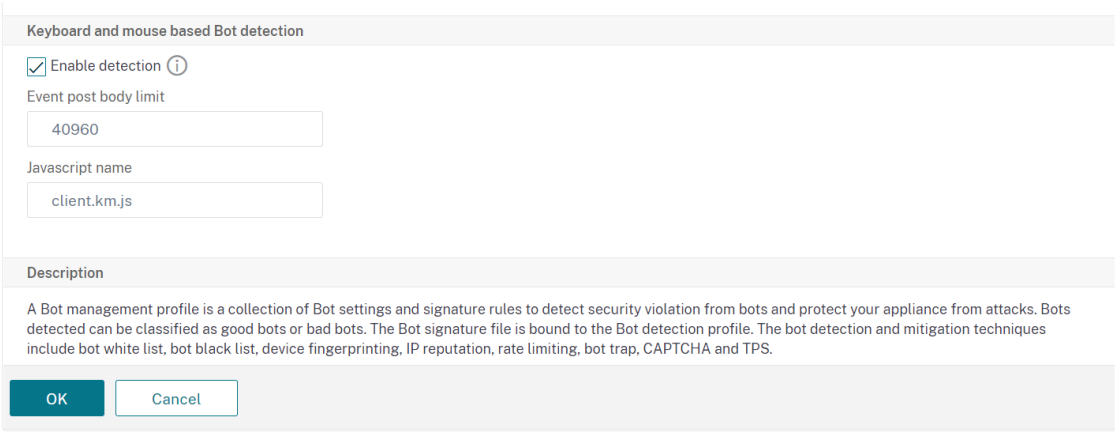
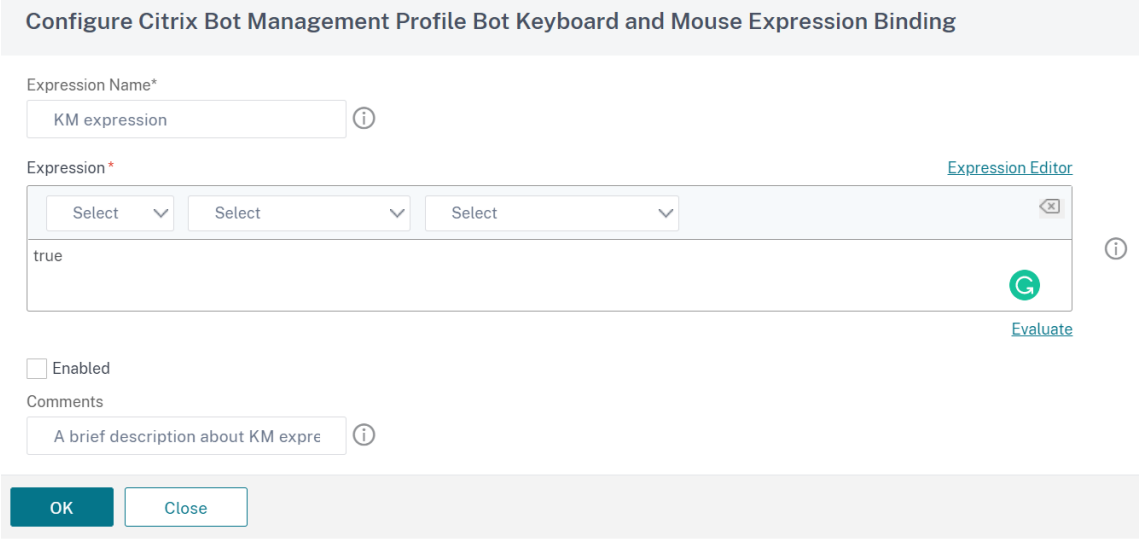
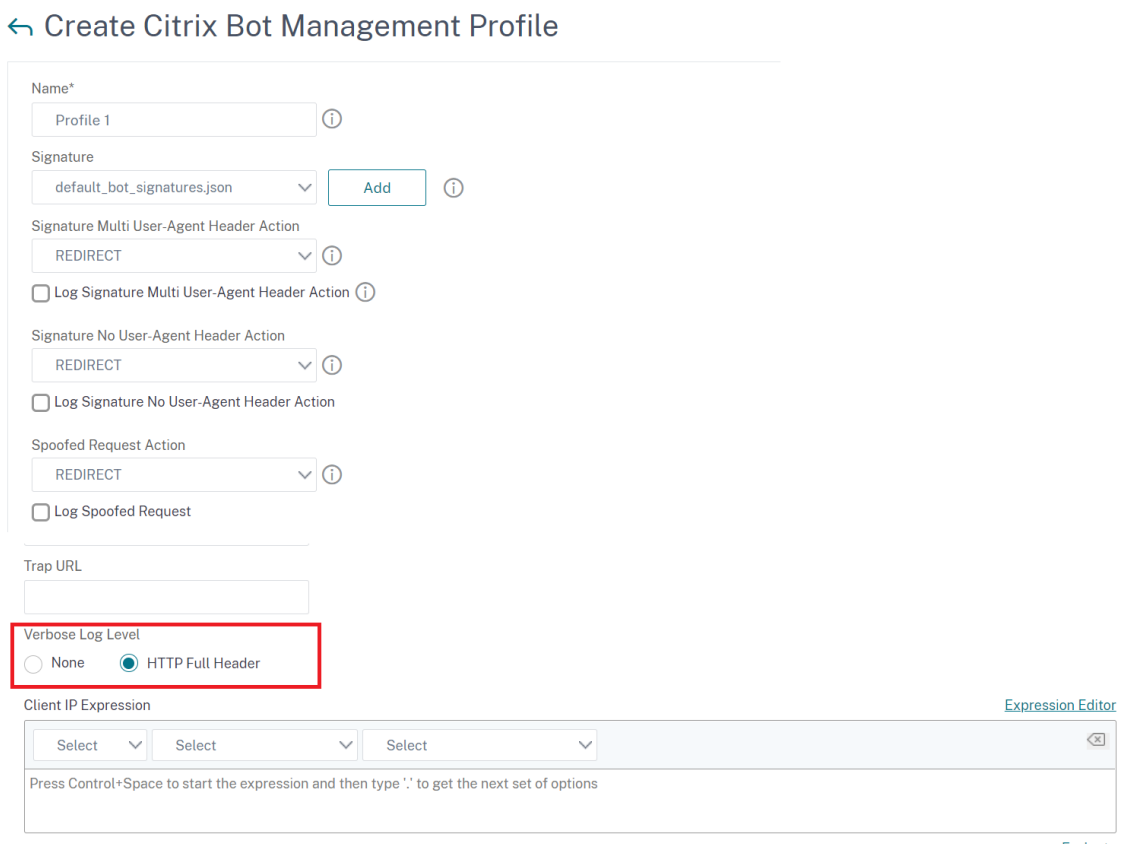
> bind appfw global syspol1 100
```

1. Toutes les violations de vérification de sécurité du Web App Firewall seront désormais redirigées vers le fichier /var/log/ns.log.appfw. Vous pouvez suivre ce fichier pour afficher les violations du Web App Firewall qui sont déclenchées pendant le traitement du trafic en cours.

   ```
   root@ns## tail -f ns.log.appfw
   ```

Avertissement : Si vous avez configuré la stratégie Syslog pour rediriger les journaux vers une autre fonction de journalisation, les messages du journal du Web App Firewall n'apparaissent plus dans le fichier /var/log/ns.log.

Affichage des journaux du Web App Firewall

Vous pouvez afficher les journaux à l'aide de la visionneuse Syslog ou en vous connectant à l'appliance Citrix ADC, en ouvrant un shell UNIX et en utilisant l'éditeur de texte UNIX de votre choix.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Basculez vers le shell et reculez les journaux ns.logs dans le dossier /var/log/ pour accéder aux messages de journal relatifs aux violations du contrôle de sécurité du Web App Firewall :

- `Shell`
- `tail -f /var/log/ns.log`

Vous pouvez utiliser l'éditeur vi, ou n'importe quel éditeur de texte Unix ou outil de recherche de texte, pour afficher et filtrer les journaux pour des entrées spécifiques. Par exemple, vous pouvez utiliser la commande grep pour accéder aux messages de journal relatifs aux violations de la carte de crédit :

- `tail -f /var/log/ns.log | grep SAFECOMMERCE`

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique Citrix inclut un outil très utile (Syslog Viewer) pour analyser les messages de journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Pour afficher les messages de journal d'une vérification de sécurité spécifique d'un profil, accédez à **Web App Firewall** > **Profils**, sélectionnez le profil cible, puis cliquez sur Vérifications de sécurité. Mettez en surbrillance la ligne correspondant au contrôle de sécurité cible, puis cliquez sur Journaux. Lorsque vous accédez aux journaux directement à partir de la vérification de sécurité sélectionnée du profil, il filtre les messages de journal et affiche uniquement les journaux relatifs aux violations du contrôle de sécurité sélectionné. La visionneuse Syslog peut afficher les journaux du Web App Firewall au format natif ainsi qu'au format CEF. Toutefois, pour que la visionneuse Syslog puisse filtrer les messages de journal spécifiques au profil cible, les journaux doivent être au format de journal CEF lorsqu'ils sont accessibles à partir du profil.
- Vous pouvez également accéder à la visionneuse Syslog en accédant à **Citrix ADC** > **Système** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien Messages Syslog pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris tous les journaux de violation des contrôles de sécurité du Web App Firewall pour tous les profils. Ceci est utile pour le débogage lorsque plusieurs violations de contrôle de sécurité peuvent être déclenchées pendant le traitement des demandes.
- Accédez à **Web App Firewall** > **stratégies** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien Messages Syslog pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris tous les journaux de violation des contrôles de sécurité pour tous les profils.

La visionneuse Syslog basée sur HTML fournit les options de filtre suivantes pour sélectionner uniquement les messages de journal qui vous intéressent :

- **Fichier** : le fichier /var/log/ns.log actuel est sélectionné par défaut et les messages correspondants apparaissent dans la visionneuse Syslog. Une liste des autres fichiers journaux du répertoire /var/log est disponible au format .gz compressé. Pour télécharger et décompresser un fichier journal archivé, il suffit de sélectionner le fichier journal dans la liste déroulante. Les messages de journal relatifs au fichier sélectionné sont ensuite affichés dans la visionneuse Syslog. Pour actualiser l'affichage, cliquez sur l'icône Actualiser (un cercle de deux flèches).
- **Zone de liste Module** : vous pouvez sélectionner le module Citrix ADC dont vous souhaitez afficher les journaux. Vous pouvez le définir sur APPFW pour les journaux de Web App Firewall.
- **Zone de liste Type d'événement** : cette zone contient un ensemble de cases à cocher permettant de sélectionner le type d'événement qui vous intéresse. Par exemple, pour afficher les messages de journal relatifs aux violations de signature, vous pouvez activer la case à cocher **APPFW_SIGNATURE_MATCH** . De même, vous pouvez cocher une case pour activer le contrôle de sécurité spécifique qui vous intéresse. Vous pouvez sélectionner plusieurs options.
- **Gravité** : vous pouvez sélectionner un niveau de gravité spécifique pour afficher uniquement les journaux correspondant à ce niveau de gravité. Laissez toutes les cases à cocher vides si vous souhaitez afficher tous les journaux.

  Pour accéder aux messages du journal des violations de vérification de sécurité du Web App Firewall pour un contrôle de sécurité spécifique, filtrez en sélectionnant **APPFW** dans les op-

tions déroulantes du module. Le type d'événement affiche un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous activez la case à cocher **APPFW_FIELDFORMAT** et que vous cliquez sur le bouton Appliquer, seuls les messages de journalisation relatifs aux violations des contrôles de sécurité des formats de champ apparaissent dans la visionneuse Syslog. De même, si vous activez les cases à cocher **APPFW_SQL** et **APPFW_STARTURL** et que vous cliquez sur le bouton **Appliquer**, seuls les messages de journal relatifs à ces deux violations de vérification de sécurité apparaîtront dans la visionneuse Syslog.

Si vous placez le curseur sur la ligne d'un message de journal spécifique, plusieurs options, telles que **Module**, **EventType**, **EventID**, **ClientIP**, **TransactionID**, etc., apparaissent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans les journaux.

Cliquez pour déployer : cette fonctionnalité n'est disponible que dans l'interface graphique. Vous pouvez utiliser la visionneuse Syslog pour non seulement afficher les journaux, mais également pour déployer des règles de relaxation basées sur les messages de journal pour les violations de vérification de sécurité du Web App Firewall. Les messages de journal doivent être au format de journal CEF pour cette opération. Si la règle de relaxation peut être déployée pour un message de journal, une case à cocher apparaît sur le bord droit de la zone Syslog Viewer sur la ligne. Activez la case à cocher, puis sélectionnez une option dans la liste Action pour déployer la règle de relaxation.
Edit & Deploy,
Deployet
Deploy All sont disponibles en tant qu'options d'action. Par exemple, vous pouvez sélectionner un message de journal individuel à modifier et à déployer. Vous pouvez également sélectionner les cases à cocher de plusieurs messages de journal provenant d'un ou de plusieurs contrôles de sécurité et utiliser l'option Déployer ou Déployer tout. La fonctionnalité Click to Deploy est actuellement prise en charge pour les contrôles de sécurité suivants :

- URL de démarrage
- Dépassement de tampon d'URL
- Injection SQL
- script intersite
- cohérence sur le terrain
- Cohérence des cookies

Pour utiliser la fonctionnalité Click to Deploy dans l'interface graphique

1. Dans la **visionneuse Syslog**, sélectionnez **APPFW** dans les options du **module** .
2. Sélectionnez le contrôle de sécurité pour lequel filtrer les messages de journal correspondants.
3. Cochez la case pour sélectionner la règle.
4. Utilisez la liste déroulante d'options **Action** pour déployer la règle de relaxation.
5. Vérifiez que la règle apparaît dans la section de règle de relaxation correspondante.

> **Remarque :**
>
> Les règles d'injection SQL et de script intersite qui sont déployées à l'aide de l'option Click **Deploy** n'incluent pas les recommandations de relaxation fine.

Résumé

- **Prise en charge du format de journal CEF** : l'option de format de journal CEF fournit une option pratique pour surveiller, analyser et analyser les messages de journal du Web App Firewall afin d'identifier les attaques, d'affiner les paramètres configurés pour réduire les faux positifs et de collecter des statistiques.
- **Click to Deploy** : la visionneuse Syslog offre une option permettant de filtrer, d'évaluer et de déployer des règles de relaxation pour des violations de contrôle de sécurité uniques ou multiples à partir d'un emplacement pratique.
- **Option de personnalisation des messages de journal** : vous pouvez utiliser des expressions PI avancées pour personnaliser les messages de journal et inclure les données que vous souhaitez voir dans les journaux.
- **Séparer les journaux spécifiques au Web App Firewall** : vous avez la possibilité de filtrer et de rediriger les journaux spécifiques au pare-feu d'application vers un fichier journal distinct.
- **Journalisation à distance** : vous pouvez rediriger les messages de journal vers un serveur Syslog distant.
- **Journalisation de la géolocalisation** : vous pouvez configurer le Web App Firewall pour inclure la géolocalisation de la zone à partir de laquelle la demande est reçue. Une base de données de géolocalisation intégrée est disponible, mais vous avez la possibilité d'utiliser une base de données de géolocalisation externe. L'appliance Citrix ADC prend en charge les bases de données de géolocalisation statiques IPv4 et IPv6.
- **Message de journal riche en informations** : voici quelques exemples du type d'informations pouvant être incluses dans les journaux, en fonction de la configuration :
  - Une stratégie de Web App Firewall a été déclenchée.
  - Une violation du contrôle de sécurité a été déclenchée.
  - Une demande a été considérée comme mal formée.
  - Une demande ou une réponse a été bloquée ou non bloquée.
  - Les données de demande (telles que les caractères spéciaux de script SQL ou intersite) ou les données de réponse (telles que les numéros de carte de crédit ou les chaînes d'objets sûrs) ont été transformées.
  - Le nombre de cartes de crédit dans la réponse a dépassé la limite configurée.
  - Le numéro et le type de la carte de crédit.
  - Les chaînes de journaux configurées dans les règles de signature et l'ID de signature.
  - Informations de géolocalisation sur la source de la demande.
  - Entrée utilisateur masquée (X'd out) pour les champs confidentiels protégés.

Masquer les données sensibles à l'aide d'un modèle regex

La fonction de stratégie avancée (PI) REGEX_REPLACE dans une expression de journal (liée à un profil de pare-feu d'application Web (WAF)) vous permet de masquer les données sensibles dans les journaux WAF. Vous pouvez utiliser cette option pour masquer les données à l'aide d'un modèle d'expression régulière et fournir un modèle de caractère ou de chaîne pour masquer les données. Vous pouvez également configurer la fonction PI pour remplacer la première occurrence ou toutes les occurrences du modèle d'expression régulière.

Par défaut, l'interface graphique Citrix fournit le masque suivant :

- SSN
- Carte de crédit
- Mot de passe
- Nom d'utilisateur

Masquer les données sensibles dans les journaux du pare-feu d'application Web

Vous pouvez masquer des données sensibles dans les journaux WAF en configurant l'expression de stratégie avancée REGEX_REPLACE dans l'expression de journal liée à un profil WAF.
Pour masquer les données sensibles, vous devez effectuer les étapes suivantes :

1. Ajouter un profil de pare-feu d'application Web
2. Liaison d'une expression de journal au profil WAF

Ajouter un profil de pare-feu d'application Web

À l'invite de commandes, tapez :

```
add appfw profile <name>
```

Exemple :

```
Add appfw profile testprofile1
```

Liaison d'une expression de journal avec le profil de pare-feu d'application Web

À l'invite de commandes, tapez :

```
bind appfw profile <name> -logExpression <string> <expression> -comment <
string>
```

Exemple :

```
bind appfw profile testProfile -logExpression "MaskSSN""HTTP.REQ.BODY
(10000).REGEX_REPLACE(re!\b\d{ 3 } -\d{ 2 } -\d{ 4 } \b!, “xxx” , ALL)"-
comment "SSN Masked"
```


Masquer les données sensibles dans les journaux du pare-feu d'application Web à l'aide de l'interface graphique Citrix ADC

1. Dans le volet de navigation, développez **Sécurité** > **Citrix Web App Firewall** > **Profils**.
2. Sur la page **Profils**, cliquez sur **Modifier**.
3. Sur la page **Profil de Citrix Web App Firewall**, accédez à la section **Paramètres avancés** et cliquez sur **Enregistrement étendu**.



4. Dans la section **Enregistrement étendu**, cliquez sur **Ajouter**.



5. Sur la page **Créer une liaison de journal étendue Citrix Web App Firewall**, définissez les paramètres suivants :
   a) Name. Nom de l'expression du journal.
   b) Activé. Sélectionnez cette option pour masquer les données sensibles.
   c) Masque de journal. Sélectionnez les données à masquer.
   d) Expression. Entrez l'expression de stratégie avancée qui vous permet de masquer les données sensibles dans les journaux WAF
   e) Commentaires. Brève description du masquage des données sensibles.
6. Cliquez sur **Créer** et **Fermer**.



Annexes

January 21, 2021

Le matériel supplémentaire suivant fournit des détails supplémentaires sur les tâches de Web App Firewall complexes ou périphériques.

Format de codage de caractères PCRE

August 20, 2021

Le **système d'exploitation Citrix ADC prend en charge l'entrée directe** de caractères dans le jeu de caractères ASCII imprimable uniquement : les caractères dont les codes hexadécimaux sont compris entre HEX 20 (ASCII 32) et HEX 7E (ASCII 127). Pour inclure un caractère dont le code est en dehors de cette plage dans votre configuration de Web App Firewall, vous devez entrer son code hexadécimal UTF-8 en tant qu'expression régulière PCRE.

De nombreux types de caractères nécessitent un encodage à l'aide d'une expression régulière PCRE si vous les incluez dans votre configuration de Web App Firewall en tant qu'URL, nom de champ de formulaire ou expression d'objet sécurisé. Il s'agit notamment des éléments suivants :

- **Caractères ASCII supérieurs.** Caractères avec encodages de HEX 7F (ASCII 128) à HEX FF (ASCII

255). Selon la table de caractères utilisée, ces encodages peuvent faire référence à des codes de contrôle, à des caractères ASCII avec des accents ou d'autres modifications, à des caractères alphabétiques non latins et à des symboles non inclus dans le jeu de caractères ASCII de base. Ces caractères peuvent apparaître dans les URL, les noms de champs de formulaire et les expressions d'objet sécurisé.

- **Caractères à deux octets.** Caractères avec encodages qui utilisent deux mots de 8 octets. Les caractères sur deux octets sont utilisés principalement pour représenter le texte chinois, japonais et coréen en format électronique. Ces caractères peuvent apparaître dans les URL, les noms de champs de formulaire et les expressions d'objet sécurisé.

  Caractères de contrôle ASCII. Caractères non imprimables utilisés pour envoyer des commandes à une imprimante. Tous les caractères ASCII dont les codes hexadécimaux sont inférieurs à HEX 20 (ASCII 32) entrent dans cette catégorie. Toutefois, ces caractères ne doivent jamais apparaître dans une URL ou un nom de champ de formulaire et apparaissent rarement, sinon jamais, dans une expression d'objet sécurisée.

L'appliance Citrix ADC ne prend pas en charge l'ensemble du jeu de caractères UTF-8, mais uniquement les caractères présents dans les huit jeux de caractères suivants :

- **Anglais US (ISO-8859-1).** Bien que l'étiquette indique « Anglais US », le Web App Firewall prend en charge tous les caractères du jeu de caractères ISO-8859-1, également appelé jeu de caractères Latin-1. Ce jeu de caractères représente entièrement la plupart des langues modernes d'Europe occidentale et représente tous les caractères rares dans le reste.
- **Chinois traditionnel (Big5).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères BIG5, qui comprend tous les caractères chinois traditionnels (idéogrammes) couramment utilisés en chinois moderne tels que parlés et écrits à Hong Kong, Macao, Taïwan, et par de nombreuses personnes d'origine ethnique chinoise qui vivent en dehors de la Chine continentale.
- **Chinois simplifié (GB2312).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères GB2312, qui inclut tous les caractères chinois simplifiés (idéogrammes) couramment utilisés en chinois moderne, tels que parlés et écrits en Chine continentale.
- **Japonais (SJIS).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères Shift-JIS (SJIS), qui comprend la plupart des caractères (idéographes) couramment utilisés dans le japonais moderne.
- **japonais (EUC-JP).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères EUC-JP, qui inclut tous les caractères (idéographes) couramment utilisés dans le japonais moderne.
- **coréen (EUC-KR).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères EUC-KR, qui inclut tous les caractères (idéographes) couramment utilisés en coréen moderne.

- **turc (ISO-8859-9).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères ISO-8859-9, qui inclut toutes les lettres utilisées en turc moderne.
- **Unicode (UTF-8).** Le Web App Firewall prend en charge certains autres caractères du jeu de caractères UTF-8, y compris ceux utilisés dans le russe moderne.

Lors de la configuration du Web App Firewall, vous entrez tous les caractères non-ASCII en tant qu'expressions régulières au format PCRE à l'aide du code hexadécimal attribué à ce caractère dans la spécification UTF-8. Les symboles et les caractères du jeu de caractères ASCII normal, auquel on attribue des codes à deux chiffres dans ce jeu de caractères, sont affectés les mêmes codes dans le jeu de caractères UTF-8. Par exemple, le point d'exclamation (!), auquel est attribué le code hexadécimal 21 dans le jeu de caractères ASCII, est également hexadécimal 21 dans le jeu de caractères UTF-8. Les symboles et les caractères d'un autre jeu de caractères pris en charge ont un jeu de codes hexadécimaux appariés qui leur sont assignés dans le jeu de caractères UTF-8. Par exemple, la lettre a avec un accent aigu (á) est assignée le code UTF-8 C3 A1.

La syntaxe que vous utilisez pour représenter ces codes UTF-8 dans la configuration du Web App Firewall est "\xNN" pour les caractères ASCII ; "\xNN\xNN" pour les caractères non ASCII utilisés en anglais, russe et turc ; et "\xNN\xNN\xNN" pour les caractères utilisés en chinois, japonais et coréen. Par exemple, si vous voulez représenter un ! dans une expression régulière du Web App Firewall en tant que caractère UTF-8, vous devez taper \x21. Si vous voulez inclure un á, vous devez taper \xC3\xA1.

> **Remarque :**
>
> Normalement, vous n'avez pas besoin de représenter les caractères ASCII au format UTF-8, mais lorsque ces caractères risquent de confondre un navigateur Web ou un système d'exploitation sous-jacent, vous pouvez utiliser la représentation UTF-8 du caractère pour éviter cette confusion. Par exemple, si une URL contient un espace, vous pouvez l'encoder en tant que x20 pour éviter de confondre certains navigateurs et logiciels de serveur Web.

Vous trouverez ci-dessous des exemples d'URL, de noms de champs de formulaire et d'expressions d'objet sécurisé contenant des caractères non-ASCII qui doivent être entrés en tant qu'expressions régulières au format PCRE à inclure dans la configuration du Web App Firewall. Chaque exemple montre en premier l'URL réelle, le nom du champ ou la chaîne d'expression, suivi d'une expression régulière au format PCRE.

- URL contenant des caractères ASCII étendus.

  URL réelle : `http://www.josénuñez.com`
  URL encodée : `^http://www\[.\]jos\\xC3\\xA9nu\\xC3\\xB1ez\[.\]com$`

- Une autre URL contenant des caractères ASCII étendus.

  URL réelle : `http://www.example.de/trömso.html`
  URL encodée : `^http://www[.]example[.\]de/tr\xC3\xB6mso[.]html$`

  Nom de champ de formulaire contenant des caractères ASCII étendus.

Nom réel : nome_do_usuário Nom
encodé : ^nome_do_usu \ xC3 \ xA1rio$

- Expression d'objet sécurisée contenant des caractères ASCII étendus.

  Expression non encodée [A-Z]{3,6} ¥[1-9 \][0-9]{6,6} Expression
  codée : [A-Z]{3,6} \ xC2 \ xA5 [1-9] [0-9] {6,6}

Vous pouvez trouver plusieurs tables qui incluent l'ensemble du jeu de caractères Unicode et les encodages UTF-8 correspondants sur Internet. Un site Web utile contenant ces informations est disponible dans le tableau suivant.

http://www.utf8-chartable.de/unicode-utf8-table.pl

Pour que les caractères du tableau de ce site Web s'affichent correctement, vous devez disposer d'une police Unicode appropriée installée sur votre ordinateur. Si vous ne le faites pas, l'affichage visuel du caractère peut être erroné. Même si vous n'avez pas de police appropriée installée pour afficher un caractère, la description et les codes UTF-8 et UTF-16 de cet ensemble de pages Web sont corrects.

Types de signature WASC Whitehat pour utilisation WAF

August 20, 2021

Le Citrix Web App Firewall accepte et génère des règles de blocage pour tous les types de vulnérabilité générés par les analyseurs Whitehat. Cependant, certaines vulnérabilités sont les plus applicables à un pare-feu d'application Web. Vous trouverez ci-dessous des listes de ces vulnérabilités, classées selon qu'elles sont traitées par les types de signature WASC 1.0, WASC 2.0 ou les meilleures pratiques.

Types de signature WASC 1.0

- Contrebande de requêtes HTTP
- Fractionnement de la réponse HTTP
- Contrebande de réponse HTTP
- Injection d'octets nuls
- Inclusion de fichiers distants
- Abus de redirecteur d'URL

Types de signature WASC 2.0

- Abus de fonctionnalité
- Force Brute
- Usurpation de contenu

- Déni de service
- Indexation d'annuaires
- Fuites d'informations
- Anti-automatisation insuffisante
- Authentification insuffisante
- Autorisation insuffisante
- Expiration de session insuffisante
- Injection LDAP
- Fixation de session

Recommandations

- Attribut de saisie semi-automatique
- Contrôle d'accès aux cookies insuffisant
- Insuffisance du mot de passe
- Utilisation de la méthode HTTP non valide
- Cookie de session non Non-HttpOnly
- Cookie de session persistante
- Informations personnelles identifiables
- Messages HTTP pouvant être mis en cache sécurisés
- Cookie de session non sécurisé

Prise en charge en continu pour le traitement des demandes

August 20, 2021

Citrix Web App Firewall prend en charge le streaming côté demande pour fournir une augmentation significative des performances. Au lieu de mettre en mémoire tampon une demande, l'appliance examine le trafic entrant à la recherche de violations de sécurité telles que SQL, les scripts intersites, la cohérence des champs et les formats de champ. Lorsque l'appliance a terminé le traitement des données d'un champ, la demande est transférée au serveur principal pendant que l'appliance continue d'évaluer d'autres champs. Ce traitement des données améliore considérablement le temps de traitement dans la gestion des formulaires ont de nombreux champs.

> **Remarque :**
>
> Citrix Web App Firewall prend en charge une taille de publication maximale de 20 Mo sans diffusion en continu. Pour une meilleure utilisation des ressources, Citrix vous recommande d'activer la diffusion en continu uniquement pour les charges utiles supérieures à 20 Mo. En outre, le

> serveur principal doit accepter les requêtes tronquées si la diffusion en continu est activée.

Bien que le processus de diffusion en continu soit transparent pour les utilisateurs, des ajustements mineurs de configuration sont nécessaires en raison des modifications suivantes :

RegEx Pattern Match : La correspondance de motif RegEx est maintenant limitée à 4K pour la correspondance de chaîne de caractères contigus.

Correspondance des noms de champ : le moteur d'apprentissage Web App Firewall ne peut distinguer que les 128 premiers octets du nom. Si un formulaire comporte plusieurs champs dont les noms ont une correspondance de chaîne identique pour les 128 premiers octets, le moteur d'apprentissage ne les distingue pas. De même, la règle de relaxation déployée pourrait, par inadvertance, modérer tous ces champs.

La suppression des espaces blancs, le décodage en pourcentage, le décodage Unicode et la conversion des charset sont effectués pendant la canonicalisation pour fournir une inspection de contrôle de sécurité. La limite de 128 octets est applicable à la représentation canonicalisée du nom de champ au format UTF-8. Les caractères ASCII mesurent 1 octet, mais la représentation UTF-8 des caractères dans certaines langues internationales peut varier de 1 octet à 4 octets. Si chaque caractère d'un nom prend 4 octets pour la conversion au format UTF-8, seuls les 32 premiers caractères du nom peuvent être distingués par la règle apprise.

Vérification de cohérence des champs : lorsque vous activez la cohérence des champs, tous les formulaires de la session sont stockés en fonction de la balise « as_fid » insérée par le Web App Firewall sans tenir compte de la mention « action_url ».

- **Balisage de formulaire obligatoire pour la cohérence des champs de formulaire :** lorsque le contrôle de cohérence des champs est activé, la balise de formulaire doit également être activée. La protection de cohérence des champs peut ne pas fonctionner si le balisage des formulaires est désactivé.
- **Cohérence des champs de formulaire sans session :** le Web App Firewall n'effectue plus la conversion « GET » en « POST » des formulaires lorsque le paramètre de cohérence de champ sans session est activé. La balise de formulaire est également requise pour la cohérence des champs sans session.
- **Falsification de as_fid :** Si un formulaire est soumis après la falsification d'as_fid, il déclenche une violation de cohérence de champ même si aucun champ n'a été falsifié. Dans les requêtes non-streaming, cela était autorisé car les formulaires peuvent être validés en utilisant le « action_url » stocké dans la session.

Signatures : Les signatures ont maintenant les spécifications suivantes :

- **Emplacement :** Il est désormais obligatoire que l'emplacement doit être spécifié pour chaque modèle. Tous les modèles de la règle **DOIVENT** avoir une balise `<Location>`.
- **Correspondance rapide :** Toutes les règles de signature doivent avoir un modèle de correspondance rapide. S'il n'y a pas de modèle de correspondance rapide, une tentative est faite pour en

sélectionner un si possible. La correspondance rapide est une chaîne littérale mais PCRE peut être utilisée pour la correspondance rapide s'ils contiennent une chaîne littérale utilisable.

- Emplacements**obsolètes : les emplacements** suivants ne sont plus pris en charge dans les règles de signature.
  - HTTP_ANY
  - HTTP_RAW_COOKIE
  - HTTP_RAW_HEADER
  - HTTP_RAW_RESP_HEADER
  - HTTP_RAW_SET_COOKIE

Scripting inter-site/SQL Transform : Les données brutes sont utilisées pour la transformation car les caractères spéciaux SQL tels que guillemet simple (‘), barre oblique inverse () et point-virgule (;)) et les balises de script inter-site sont identiques et ne nécessitent pas de canonicalisation des données. La représentation de caractères spéciaux tels que le codage d'entité HTML, l'encodage en pourcentage ou l'ASCII sont évaluées pour l'opération de transformation.

Le Web App Firewall n'inspecte plus le nom et la valeur de l'attribut pour l'opération de transformation de script inter-site. Désormais, seuls les noms d'attributs de script intersite sont transformés lorsque le streaming est activé.

Traitement des balises de script inter-sites : dans le cadre des modifications de streaming dans NetScaler 10.5.e build et versions ultérieures, le traitement des balises de script inter-site a changé. Dans les versions antérieures, la présence de crochets ouverts (<), or close bracket (>) ou de crochets ouverts et fermément (<>) était marquée comme violation de script inter-site. Le comportement a changé dans la version 10.5.e à partir. La présence de seulement le caractère entre crochets ouverts (<) ou seulement le caractère entre crochets (>) n'est plus considérée comme une attaque. C'est lorsqu'un caractère de parenthèse ouvert (<) est suivi par un caractère de parenthèse fermé (>), l'attaque de script inter-site est signalée. Les deux caractères doivent être présents dans le bon ordre (< followed by >) pour déclencher la violation de script inter-site.

> **Remarque :**
>
> **Message de modification du journal des violations SQL : Dans** le cadre des modifications de streaming dans la version 10.5.e ultérieure, nous traitons maintenant les données d'entrée en blocs. La correspondance de motifs RegEx est désormais limitée à 4K pour la correspondance de chaînes de caractères contiguës. Avec cette modification, les messages du journal des violations SQL peuvent inclure des informations différentes par rapport aux versions précédentes. Le mot clé et le caractère spécial dans l'entrée sont séparés par plusieurs octets. L'appliance dispose d'une trace des mots-clés SQL et des chaînes spéciales lors du traitement des données, au lieu de mettre en mémoire tampon toute la valeur d'entrée. Outre le nom du champ, le message de journal inclut le mot-clé SQL, le caractère spécial SQL ou les deux mots clés SQL et le caractère

> spécial SQL. Le reste de l'entrée n'est plus inclus dans le message de journal, comme illustré dans l'exemple suivant :
>
> **Exemple :**
>
> Dans la version 10.5, lorsque le Web App Firewall détecte la violation SQL, la chaîne d'entrée entière peut être incluse dans le message de journal suivant :
>
> La vérification du mot-clé SQL a échoué pour le champ **text="sélectionnez un nom dans testbed1 ; (;) ».**<blocked>*
>
> Dans la version 11.0, nous enregistrons uniquement le nom du champ, le mot clé et le caractère spécial (le cas échéant) dans le message de journal suivant.
>
> Échec de la vérification des mots-clés SQL pour le champ `text="select(;)"<blocked>`
>
> Cette modification s'applique aux demandes qui contiennent des types de contenu **application/x-www-form-urlencoded**, **multipart/form-data**ou **text/x-gwt-rpc** . Les messages de journal générés lors du traitement des charges utiles **JSON** ou **XML** ne sont pas affectés par cette modification.

Corps RAW POST : Les contrôles de sécurité sont toujours effectués sur le corps RAW POST.

ID de formulaire : Le pare-feu Web App Firewall inséré « as_fid », qui est un hachage calculé du formulaire est plus unique pour la session utilisateur. Il s'agit d'une valeur identique pour un formulaire spécifique indépendamment de l'utilisateur ou de la session.

Jeu de caractères : si une demande n'a pas de jeu de caractères, le jeu de caractères par défaut spécifié dans le profil d'application est utilisé lors du traitement de la demande.

Compteurs :

Les compteurs avec le préfixe « se » et « appfwreq » sont ajoutés pour suivre le moteur de streaming et les compteurs de requêtes du moteur de streaming.

```
nsconsmg -d statswt0 -g se_err_

nsconsmg -d statswt0 -g se_tot_

nsconsmg -d statswt0 -g se_cur_

nsconsmg -d statswt0 -g appfwreq_err_

nsconsmg -d statswt0 -g appfwreq_tot_

nsconsmg -d statswt0 -g appfwreq_cur_
```

`_err counters` : indique l'événement rare qui doit avoir réussi mais a échoué en raison d'un problème d'allocation de mémoire ou d'une autre crise de ressources.

`_tot counters` : compteurs toujours plus nombreux.

`_cur counters` : compteurs indiquant les valeurs actuelles qui changent en fonction de l'utilisation des transactions en cours.

Conseils :

- Les vérifications de sécurité du Web App Firewall doivent fonctionner de la même manière qu'auparavant.
- Il n'y a pas de commande définie pour le traitement des contrôles de sécurité.
- Le traitement côté réponse n'est pas affecté et reste inchangé.
- La diffusion en continu n'est pas engagée si un VPN sans client est utilisé.

> **Important :**
>
> **Calcul de la longueur du cookie :** dans la version 10.5.e en plus de la version 11.0 (dans les versions antérieures à 65.x), la façon de traiter l'en-tête du cookie Web App Firewall a été modifiée. L'appliance a évalué le cookie individuellement, et si la longueur d'un cookie dans l'en-tête du cookie dépassait la longueur configurée, la violation de dépassement de tampon a été déclenchée. Par conséquent, les demandes bloquées dans la version 10.5 de NetScaler ou les versions antérieures peuvent être autorisées. La longueur de l'en-tête entier du cookie n'est pas calculée pour déterminer la longueur du cookie. Dans certains cas, la taille totale des cookies peut être supérieure à la valeur acceptée, et le serveur peut répondre par « 400 Bad Request ».
>
> **Remarque :**
> La modification a été rétablie. Le comportement de NetScaler version 10.5.e vers la version 59.13xx.e et ses versions ultérieures est similaire aux versions non améliorées de la version 10.5. L'en-tête de Cookie brut entier est maintenant pris en compte lors du calcul de la longueur du cookie. Les espaces environnants et les point-virgule (;) séparant les paires nom-valeur sont également inclus dans la détermination de la longueur du cookie.

Tracer les requêtes HTML avec les journaux de sécurité

August 20, 2021

> **Remarque :**
>
> Cette fonctionnalité est disponible dans Citrix ADC version 10.5.e.

Le dépannage nécessite l'analyse des données reçues dans la demande du client et peut s'avérer difficile. Surtout s'il y a un trafic important qui circule à travers l'appareil. Les problèmes de diagnostic peuvent affecter la fonctionnalité ou la sécurité de l'application peut nécessiter une réponse rapide.

Citrix ADC isole le trafic pour un profil de Web App Firewall et recueille `nstrace` pour les demandes HTML. Le `nstrace` collecté en mode appfw inclut les détails de la demande avec les messages de

journal. Vous pouvez utiliser « Suivre le flux TCP » dans la trace pour afficher les détails de la transaction individuelle, y compris les en-têtes, la charge utile et le message de journal correspondant dans le même écran.

Cela vous donne un aperçu complet de votre trafic. Avoir une vue détaillée de la demande, de la charge utile et des enregistrements de journaux associés peut être utile pour analyser la violation des contrôles de sécurité. Vous pouvez facilement identifier le motif qui déclenche la violation. Si le modèle doit être autorisé, vous pouvez prendre la décision de modifier la configuration ou d'ajouter une règle de relaxation.

Avantages

1. **Isoler le trafic pour un profil spécifique** : cette amélioration est utile lorsque vous isolez le trafic pour un seul profil ou des transactions spécifiques d'un profil pour le dépannage. Vous n'avez plus à parcourir l'ensemble des données collectées dans la trace ou besoin de filtres spéciaux pour isoler les demandes qui vous intéressent qui peuvent être fastidieux avec un trafic lourd. Vous pouvez afficher les données que vous préférez.
2. **Collecter des données pour des demandes spécifiques** : Le suivi peut être collecté pour une durée spécifiée. Vous ne pouvez collecter le suivi que pour quelques demandes pour isoler, analyser et déboguer des transactions spécifiques si nécessaire.
3. **Identifier les réinitialisations ou les abandons** : La fermeture inattendue des connexions n'est pas facilement visible. La trace collectée en mode —appfw capture une réinitialisation ou un abandon, déclenchée par le Web App Firewall. Cela permet d'isoler plus rapidement un problème lorsque vous ne voyez pas de message de violation de vérification de sécurité. Les demandes mal formées ou d'autres demandes non conformes RFC arrêtées par le Web App Firewall seront désormais plus faciles à identifier.
4. **Afficher le trafic SSL déchiffré** : le trafic HTTPS est capturé en texte brut pour faciliter le dépannage.
5. **Fournit une vue complète** : Permet de regarder l'ensemble de la requête au niveau du paquet, de vérifier la charge utile, d'examiner les journaux pour vérifier quelle violation de vérification de sécurité est déclenchée et d'identifier le modèle de correspondance dans la charge utile. Si la charge utile est constituée de données inattendues, de chaînes indésirables ou de caractères non imprimables (caractère nul, \ r ou \ n et ainsi de suite), ils sont faciles à découvrir dans la trace.
6. **Modifier la configuration** : le débogage peut fournir des informations utiles pour décider si le comportement observé est le comportement correct ou si la configuration doit être modifiée.
7. **Accélérer le temps de réponse** : un débogage plus rapide du trafic cible peut améliorer le temps de réponse pour fournir des explications ou une analyse des causes premières par l'équipe d'ingénierie et de support Citrix.

Pour plus d'informations, voir Configuration manuelle à l'aide de la rubrique Interface de ligne de

commande .

Pour configurer le suivi de débogage d'un profil à l'aide de l'interface de ligne de commande

Étape 1. Activer la trace ns.

Vous pouvez utiliser la commande show pour vérifier le paramètre configuré.

- `set appfw profile <profile> -trace ON`

Étape 2. Recueillir des traces. Vous pouvez continuer à utiliser toutes les options applicables à la `nstrace` commande.

- `start nstrace -mode APPFW`

Étape 3. Arrêtez la trace.

- `stop nstrace`

Emplacement de la trace : Le `nstrace` est stocké dans un dossier horodaté qui est créé dans le répertoire /var/nstrace et peut être consulté à l'aide de `wireshark`. Vous pouvez suivre le `/var/log/ns.log` pour voir les messages de journal fournissant des détails sur l'emplacement de la nouvelle trace.

Conseils :

- Lorsque l'option de mode appfw est utilisée, le `nstrace` collectera uniquement les données pour un ou plusieurs profils pour lesquels le « nstrace » a été activé.
- L'activation de la trace sur le profil ne démarre pas automatiquement la collecte des traces tant que vous n'exécutez explicitement la commande « start ns trace » pour collecter la trace.
- Bien que l'activation du suivi sur un profil n'ait pas d'effet négatif sur les performances du Web App Firewall, vous pouvez activer cette fonctionnalité uniquement pour la durée pendant laquelle vous souhaitez collecter les données. Il est recommandé de désactiver l'indicateur —trace après avoir recueilli la trace. Cette option empêche le risque d'obtenir par inadvertance des données à partir de profils pour lesquels vous aviez activé cet indicateur dans le passé.
- L'action de bloc ou de journal doit être activée pour que la vérification de sécurité de l'enregistrement de transaction soit incluse dans le `nstrace`.
- Les réinitialisations et les annulations sont enregistrées indépendamment des actions de vérification de sécurité lorsque le suivi est « On » pour les profils.
- Cette fonctionnalité est uniquement applicable pour le dépannage des demandes reçues du client. Les traces en mode —appfw n'incluent pas les réponses reçues du serveur.
- Vous pouvez continuer à utiliser toutes les options applicables à la `nstrace` commande. Par exemple,

  ```
  start nstrace -tcpdump enabled -size 0 -mode appFW
  ```


- Si une demande déclenche plusieurs violations, l'enregistrement `nstrace` pour cet enregistrement inclut tous les messages de journal correspondants.
- Le format de message de journal CEF est pris en charge pour cette fonctionnalité.
- Les violations de signature déclenchant une action de blocage ou de journal pour les vérifications côté requête seront également incluses dans la trace.
- Seules les requêtes HTML (non-XML) sont collectées dans la trace.

Prise en charge de Web App Firewall pour les configurations de cluster

August 20, 2021

> **Remarque :**
>
> Citrix Web App Firewall pour les configurations par répartition et partiellement répartie a été introduit dans la version 11.0 de Citrix ADC.

Un cluster est un groupe d'appliances Citrix ADC configurées et gérées en tant que système unique. Chaque appliance du cluster est appelée nœud. Selon le nombre de nœuds sur lesquels les configurations sont actives, les configurations de cluster sont appelées configurations striped, striped partielles et spotted. Le Web App Firewall est entièrement pris en charge dans toutes les configurations.

Les deux principaux avantages de la prise en charge des serveurs virtuels striped et striped partiels dans les configurations de cluster sont les suivants :

1. Prise en charge du basculement de session : les configurations de serveurs virtuels répartis et partiellement répartis prennent en charge le basculement de session. Les fonctionnalités avancées de sécurité du Web App Firewall, telles que Démarrer la fermeture de l'URL et la cohérence des champs de formulaire vérifient, conservent et utilisent des sessions pendant le traitement des transactions. Dans une configuration haute disponibilité ou dans une configuration de cluster repéré, lorsque le nœud qui traite le trafic du Web App Firewall échoue, toutes les informations de session sont perdues et l'utilisateur doit rétablir la session. Dans les configurations de serveur virtuel par bandes, les sessions utilisateur sont répliquées sur plusieurs nœuds. Si un nœud tombe en panne, un nœud exécutant le réplica devient le propriétaire. Les informations de session sont conservées sans impact visible sur l'utilisateur.
2. Évolutivité : n'importe quel nœud du cluster peut traiter le trafic. Plusieurs nœuds du cluster peuvent traiter les demandes entrantes servies par le serveur virtuel par répartition. Cela améliore la capacité du pare-feu Web App à traiter plusieurs demandes simultanées, améliorant ainsi les performances globales.

Les contrôles de sécurité et les protections de signature peuvent être déployés sans nécessiter de configuration supplémentaire de Web App Firewall spécifique au cluster. Vous pouvez effectuer la

configuration habituelle du Web App Firewall sur le nœud CCO (Configuration Coordinator) pour la propagation vers tous les nœuds.

> **Remarque :**
>
> Les informations de session sont répliquées sur plusieurs nœuds, mais pas sur tous les nœuds de la configuration par répartition. Par conséquent, la prise en charge du basculement prend en charge un nombre limité de défaillances simultanées. Si plusieurs nœuds échouent simultanément, le Web App Firewall peut perdre les informations de session en cas d'échec avant que la session ne soit répliquée sur un autre nœud.

Résumé

- Le Web App Firewall offre une évolutivité, un débit élevé et une prise en charge du basculement de session dans les déploiements de cluster.
- Toutes les vérifications de sécurité du Web App Firewall et toutes les protections de signature sont prises en charge dans toutes les configurations de cluster.
- Les cartes de caractères ne sont pas encore prises en charge pour un cluster. Le moteur d'apprentissage recommande les Types de champ dans les règles apprises pour la vérification de sécurité Format de champ.
- Les statistiques et les règles apprises sont agrégées à partir de tous les nœuds d'un cluster.
- La table de hachage distribuée (DHT) fournit la mise en cache de la session et offre la possibilité de répliquer les informations de session sur plusieurs nœuds. Lorsqu'une demande est adressée au serveur virtuel, l'appliance Citrix ADC crée des sessions de Web App Firewall dans le DHT et peut également récupérer les informations de session à partir du DHT.
- Le clustering est sous licence avec les licences Advanced et Premium. Cette fonctionnalité n'est pas disponible avec la licence Standard.

Débogage et dépannage

August 20, 2021

Reportez-vous aux informations de dépannage et de débogage suivantes liées à chacune des fonctionnalités de Web App Firewall :

- Pare-feu d'application - CPU élevé
- Mémoire
- Échec du chargement de fichiers volumineux
- Apprentissage
- Signatures
- Journal de suivi

- Divers

Utilisation élevée du processeur

January 21, 2021

Voici quelques-unes des fonctionnalités et des problèmes de débogage liés à l'UC élevés rencontrés et les meilleures pratiques à suivre lorsque vous travaillez avec le Web App Firewall :

Vérifiez les accès aux stratégies, les liaisons, la configuration réseau, la configuration du Web App Firewall :

- Identifier les erreurs de configuration
- Identifier *vserver* qui dessert le trafic affecté

Inspectez les journaux des fichiers journaux suivants à la recherche de violations de sécurité et de modifications récentes de configuration :

- `/var/log/ns.log`
- `/var/nslog/import.log`
- `/var/nslog/aslearn.log`
- `tail -f /var/log/ns.log | grep APPFW_SIGNATURE_MATCH`

Exemple :

```
1 Jun 13 01:11:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
     .0|APPFW| APPFW_SIGNATURE_MATCH|6|src=10.217.253.62 spt=61141 method
     =GET request= http://aaron.stratum8.net/FFC/wwwboard/passwd.txt msg=
     Signature violation rule ID 807: web-cgi /wwwboard/passwd.txt access
      cn1=140 cn2=841 cs1=pr_ffc cs2=PPE0 cs3=
     OyTgjbXBqcpBFeENKDlde3OkMQ00001 cs4=ALERT cs5=2015 cs6=web-cgi act=
     not blocked
2 <!--NeedCopy-->
```

Isolez le trafic effectué :

- Isoler le profil
- Isoler le contrôle de sécurité
- Isoler l'URL, le serveur virtuel et les paramètres de trafic

Le suivi conditionnel au niveau du profil permet d'identifier les enregistrements de trafic et de violation :

- `set appfw profile <profile> -trace ON`
- `start nstrace -mode APPFW -size 0`

- `stop nstrace`

Remarque : Assurez-vous que la trace est collectée avec l'option -size 0.

Vérifiez les compteurs d'activité appfw, dht, IP réputation :

- `nsconmsg -g as_ -g appfwreq_ -g iprep -d current`

Surveiller la taille de la fenêtre pour les réinitialisations en connexion :

Appfw définit la taille de la fenêtre sur 9845 lorsque Citrix ADC réinitialise la connexion en raison d'un message http non valide.

Exemples :

- Demande mal formée reçue - réinitialisation de la connexion
- Problèmes liés au processeur élevé
- Vérifier les limites du système dans les fiches techniques
- Inspectez l'utilisation du processeur, appfw, DHT et l'activité liée à la mémoire. Surveiller les sessions appfw
- nsconmsg -g cc_cpu_use -g appfwreq -g as -g dht -g mem_AS_OBJ -g mem_AS_COMPONENT -d current

Surveillez la mémoire allouée et libérée des composants et objets du Web App Firewall pendant la période cible. Il aide à isoler la protection conduisant à une utilisation élevée du processeur.

- Sortie du profileur
- Observer les journaux

Isoler la vérification appfw conduisant à un processeur élevé :

- startURLClosure
- Cohérence des fichiers formels
- CSRF
- Protection contre les cookies
- Vérification de l'en-tête du référent

Vérifiez que la mise à jour automatique des signatures ne conduit pas à une CPU élevée (Désactiver pour confirmer).

Mémoire

August 20, 2021

Voici quelques-unes des meilleures pratiques à suivre en cas de problèmes liés à la mémoire d'utilisation du Web App Firewall :

nsconmsg, commande utilisation :

- Recherchez des statistiques de mémoire globales pour vérifier qu'il y a suffisamment de mémoire dans le système et qu'il n'y a pas d'échecs d'allocation de mémoire en exécutant la commande suivante :

  ```
  * *- nsconmsg -d memstats
  ```

- Observez les limites de mémoire allouées et maximales actuelles pour appsecure, la réputation IP, le cache et la compression en exécutant la commande suivante :

  ```
  nsconmsg -d memstats | egrep -i APPSECURE|IPREP|CACHE|CMP
  ```

- Vérifiez les compteurs d'activité appfw, DHT, IP réputation en exécutant la commande suivante :

  ```
  nsconmsg -g as -g appfwreq_ -g iprep -d current
  ```

- Vérifiez tous les compteurs d'erreur du Web App Firewall en exécutant la commande suivante :

  ```
  nsconmsg -g as_ -g appfwreq_ -g iprep_ -d stats | grep err
  ```

- Vérifiez tous les compteurs d'erreurs système en exécutant la commande suivante :

  ```
  nsconmsg -g err -d current
  ```

- Inspectez les compteurs CPU, APPFWREQ, AS et DHT en exécutant la commande suivante :

  ```
  nsconmsg -g cc_cpu_use -g appfwreq -g as -g dht -d current
  ```

- Vérifiez la mémoire cache configurée en exécutant la commande suivante :
- `show cacheparameter`
- Vérifiez la mémoire configurée en exécutant la commande suivante :

  ```
  nsconmsg -d memstats | egrep -i CACHE
  ```

- Identifier la distribution de la mémoire dans les composants et objets du Web App Firewall :

Afficher la mémoire AS_OBJ_ :

```
nsconmsg -K newnslog -d stats | grep AS_OBJ | egrep -v AppFW_cpu0|total |
sort -k3
```

Afficher la mémoire AS_COMPONENT_ :

```
nsconmsg -K newnslog -d stats | grep AS_COMPONENT | egrep -v AppFW_cpu0|
total | sort -k3
```

Vérifiez le nombre de sessions actives en exécutant la commande suivante :

Nombre de**sessions actives de moniteur/tracé** :

```
nsconmsg -g as_alive_sessions -d current
```

Moniteur/tracé total alloué, gratuit, sessions mises à jour :

- `nsconmsg -g as_tot_alloc_sessions -g as_tot_free_sessions -d current`
- `nsconmsg -g as_tot_update_sessions -d current`

Si nécessaire, réduisez le délai d'expiration de session pour vous assurer que les limites de session ne sont pas utilisées en exécutant la commande suivante :

```
set appfwsettings -sessionTimeout <300>
```

Si nécessaire, définissez la durée de vie maximale de la session en exécutant la commande suivante :

```
set appfwsettings -sessionLifetime <7200>
```

Vérification de la mémoire allouée et utilisée

Pour vérifier la mémoire totale allouée et la mémoire utilisée :

- Utilisez la commande **nsconmsg —d memstats**. Observez le champ **MEM_APPSECURE**.
- Utilisez la commande **stat appfw** pour obtenir des informations sur la consommation de mémoire.

Le Web App Firewall ne supprime pas automatiquement les journaux après une certaine période de temps ou de taille.

- `All AppFw logs are archived in the */var/log/ns.log*` fichier. Le fichier *ns.log* effectue la tâche de survol.

Pour plus d'informations, consultez le lien suivant :<http://support.citrix.com/article/CTX121898>

Augmentation de la mémoire de Web App Firewall :

- Il n'y a pas d'option CLI pour augmenter la mémoire du Web App Firewall. La mémoire de Web App Firewall est spécifique à la plate-forme.
- Vous pouvez utiliser l'option *nsapimgr* pour augmenter la mémoire, mais ce n'est pas recommandé.

La mémoire maximale autorisée pour le Web App Firewall est déterminée par la plate-forme et la désactivation de l'IC n'affecte pas l'allocation de mémoire.

Échec du téléchargement de fichiers volumineux

January 21, 2021

Lorsque vous rencontrez des échecs de téléchargement de fichiers volumineux, vérifiez les éléments suivants :

— Limite postbody du pare-feu d'application mal configurée
— Activation de l'analyse de téléchargement de fichiers entraînant une augmentation du temps de traitement.
— Atteler les limites du système ;

Pour les charges utiles supérieures à 20 Mo, Citrix vous recommande d'activer la diffusion en continu sur le profil de pare-feu de l'application. En outre, vous devez vous assurer que le serveur principal prend en charge les requêtes tronquées avant d'activer la diffusion en continu.

Depuis la version 11.0, l'indicateur de diffusion peut être activé par profil pour éviter la mise en mémoire tampon en exécutant la commande suivante :

```
set appfw profile <profile name> -streaming on
```

Apprentissage

August 20, 2021

Voici quelques-unes des meilleures pratiques recommandées en cas de problèmes de fonctionnalité d'apprentissage :

Processus d'apprentissage :

- Vérifiez que le processus *aslearn est en* cours d'exécution.
- Vérifier la sortie de la commande supérieure
- Vérifiez la sortie de la commande ps en exécutant la commande suivante :

  ```
  ps -ax | grep aslearn | grep -v "grep"
  ```

  Exemple :

  ```
  1  root@ns# ps -ax | grep aslearn | grep -v "grep"
  2  1439  ??  Ss     0:03.86 /netscaler/aslearn -start -f /netscaler/
        aslearn.conf
  3  <!--NeedCopy-->
  ```

- Identifiez les commandes de configuration récentes exécutées avant le problème observé en vérifiant le fichier *ns.log* :

  ```
  /var/log/ns.log
  ```

- Inspectez les journaux d'apprentissage pour rechercher les messages d'apprentissage :

  ```
  /var/log/aslearn.log
  ```

- Isoler le profil et le contrôle de sécurité effectué

- Identifiez l'interface graphique et la commande CLI qui échoue en exécutant la commande suivante :

  ```
  show appfw learningdata <profileName> <securityCheck>
  ```

  Exemples :

  - `show learningdata test_profile starturl`
  - `show learningdata test_profile crosssiteScripting`
  - `show learningdata test_profile sqLInjection`
  - `show learningdata test_profile csRFtag`
  - `show learningdata test_profile fieldformat`
  - `show learningdata test_profile fieldconsistency`

- Effectuer la vérification de l'intégrité de sqlite à partir de l'invite de shell bsd :

  ```
  nsshell ## sqlite3 /var/nslog/asl/<profile_name_in_lowercase>.db '
  pragma integrity_check;
  ```

  Exemples :

  ```
  1  root@ns# sqlite3 /var/nslog/asl/tsk0247284.db 'pragma
        integrity_check;'
  2  ok
  3  <!--NeedCopy-->
  ```

- Déployez ou supprimez des règles pour recommencer à apprendre :
  - Si 2000 éléments d'apprentissage (par protection) sont atteints, vous ne pouvez plus commencer à apprendre pour cette protection.
  - Si une taille de 20 Mo est atteinte pour la base de données, arrêtez l'apprentissage pour toutes les protections
  - Redémarrer comme processus d'apprentissage

  ```
  */netscaler/aslearn -start -f/netscaler/aslearn.conf*
  ```

- Vérifiez l'espace dans le dossier /var en exécutant ce qui suit :

  ```
  du -h /var
  ```

- Vérifiez les limites de seuil d'apprentissage en exécutant la commande suivante :

  ```
  show appfwlearningsettings <profile_name> <securityCheck>
  ```

- Collectez les données apprises en exécutant la commande suivante :

  ```
  export appfwlearningdata <profile_name> <securityCheck>
  ```

- vérifier que les données apprises sont téléchargées dans le collecteur.

Signatures

January 21, 2021

Prise en main des signatures

Pour ajouter une signature :

1. Sélectionnez la signature **par défaut**et cliquez sur **ajouter**pour en faire une copie.
2. Donnez un nom significatif. Le nouvel objet sig est ajouté en tant qu'objet défini par l'utilisateur.
3. Activez les règles cibles qui correspondent à vos besoins spécifiques.
    - Les règles sont désactivées par défaut.
    - plus de règles nécessitent plus de traitement
4. Configurez les actions :

    Les actions Bloquer et Log sont activées par défaut. Stats est une autre option
5. Définissez la signature à utiliser par votre profil.

Conseils pour l'utilisation des signatures

- Optimisez les frais de traitement en activant uniquement les signatures applicables à la protection de votre application.
- Chaque motif de la règle doit correspondre pour déclencher une correspondance de signature.
- Vous pouvez ajouter vos propres règles personnalisées pour inspecter les requêtes entrantes afin de détecter différents types d'attaques, telles que les attaques par injection SQL ou par script intersite.
- Vous pouvez également ajouter des règles pour inspecter les réponses afin de détecter et de bloquer les fuites d'informations sensibles telles que les numéros de carte de crédit.
- Ajoutez plusieurs conditions de vérification de sécurité pour créer votre propre vérification personnalisée.

Meilleures pratiques d'utilisation des signatures

Voici quelques-unes des meilleures pratiques que vous pouvez suivre lorsque vous rencontrez des problèmes liés à Signatures :

- Vérifiez que la commande import a réussi sur primaire et secondaire.

- Vérifiez que les sorties CLI et GUI sont cohérentes.
- Vérifiez ns.log pour identifier les erreurs lors de l'importation de signature et de la mise à jour automatique.
- Vérifiez si le serveur de noms DNS est configuré correctement.
- Vérifiez l'incompatibilité de la version du schéma.
- Vérifiez si le périphérique n'est pas en mesure d'accéder à l'URL Signature Update hébergée sur AWS pour la mise à jour automatique.
- Vérifiez l'incompatibilité de version entre les signatures par défaut et celles ajoutées par l'utilisateur.
- Vérifiez l'incompatibilité de version entre les objets de signature sur les nœuds principal et secondaire.
- Surveiller l'utilisation élevée du processeur (désactivez la mise à jour automatique pour exclure le problème avec la mise à jour de signature).

Journal de suivi

January 21, 2021

Pour enregistrer les journaux de suivi :

1. Activez le suivi du profil. Vous pouvez utiliser la commande show pour vérifier le paramètre configuré.

```
set appfw profile <profile> -trace ON
```

1. Commencez à collecter la trace. Vous pouvez continuer à utiliser toutes les options applicables à la commande nstrace.

```
start nstrace -mode APPFW
```

1. Arrêter la collecte de la trace

```
stop nstrace
```

Emplacement de la trace : Le nstrace est stocké dans un dossier horodaté qui est créé dans le répertoire */var/nstrace* et peut être consulté à l'aide de wireshark. Vous pouvez suivre le fichier */var/log/ns.log* pour voir les messages de journal fournissant des détails sur l'emplacement de la nouvelle trace.

Avantages des journaux de suivi :

- Isoler le trafic pour un profil spécifique

- Collecter des données pour des demandes spécifiques
- Identifier les réinitialisations ou les abandons
- Afficher le trafic SSL déchiffré : le trafic HTTPS est capturé en texte brut pour faciliter le dépannage.
- Offre une vue complète : permet d'examiner la demande entière au niveau des paquets, de vérifier la charge utile, d'afficher les journaux pour vérifier quelle violation de vérification de sécurité est déclenchée et d'identifier le modèle de correspondance dans la charge utile. Si la charge utile est constituée de données inattendues, de chaînes de courrier indésirable ou de caractères non imprimables (caractère nul, \r ou \n etc), ils sont faciles à découvrir dans la trace.
- Accélérer le temps de réponse : débogage plus rapide sur le trafic cible pour effectuer une analyse des causes premières.

Divers

August 20, 2021

Voici les résolutions de certains des problèmes que vous pouvez rencontrer lors de l'utilisation du Web App Firewall.

- Le Web App Firewall définit la taille de la fenêtre sur 9845 lors de la réinitialisation de la connexion pour les messages http non valides.

  — Demande mal formée reçue - réinitialisation de la connexion [Client/Serveur envoyant un en-tête de longueur de contenu non valide]
  — Type de contenu inconnu dans les en-têtes de demande

- Limite système : l'application semble gelée

  — Se produit lorsque la limite maximale de session est atteinte. (100 Ko)
  — Moins de mémoire système pour le fonctionnement.

  - La fonctionnalité de réputation IP ne fonctionne pas
    : le processus iprep prend environ cinq minutes après l'activation de la fonction de réputation. La fonctionnalité de réputation IP peut ne pas fonctionner pendant cette durée.

- Violations inattendues Web App Firewall en cours de déclenchement

  — Le délai d'expiration de la session a une valeur par défaut de 900 secondes. Si le délai d'expiration de session est défini sur une valeur faible, le navigateur peut déclencher des faux positifs pour les vérifications qui reposent sur la sessionisation (par exemple CSRF, FFC). Vérifiez le délai d'expiration de session et regardez l'ID de session (cs3 dans les journaux CEF). Si l'ID de session est différent, le délai d'expiration de session peut en être la raison.
  — Si le formulaire est généré dynamiquement par javascript, il peut déclencher de fausses violations FFC.

- Nom de champ vide dans les journaux des violations FFC (avant la version 11.0)

  Cela peut être vu dans des scénarios où nous rencontrons un champ de formulaire qui n'est pas dans les formulaires de notre session.

  Scénarios où cela peut se produire :

  — La session a expiré à partir du moment où le formulaire a été envoyé au client et de sa réception.
  — Le formulaire a été généré côté client à l'aide d'un script java.

Références

August 20, 2021

Reportez-vous aux ressources supplémentaires suivantes pour plus d'informations et des conseils utiles lors de l'utilisation du Web App Firewall :

- CommentCitrix Web App Firewall modifie le[trafic](http://support.citrix.com/article/CTX131488)de données des applications

  – En-têtes conditionnels modifiés par le Web App Firewall ;
  – Mise en cache intégrée et interopérabilité avec Web App Firewall ;

- Suividesrequêtes HTML avec les journaux de violation de sécurité du Web App Firewall sur NetScalerAppliance
  - Isolation de la demande et débogage de la transaction de bout en bout.
- Protection de haut niveau
  - relaxations de sécurité
- Informations sur la configuration et le déploiement.
  - Application
  - Pare-feu
  - Journaux
- Détails concernant l'anatomie des messages de journal du Web App Firewall.

  <https://regex101.com/>
- Configuration des expressions régulières.
- Fiches techniques

  — Utilisation de la mémoire recommandée et du processeur pour le système ;

— Garantir suffisamment de mémoire pour le Web App Firewall et configurer la limite de cache de manière appropriée.

Signature Alerte Articles

January 21, 2021

Citrix Web Application Firewall (WAF) annonce les mises à jour de signature que vous pouvez télécharger et appliquer sur votre appliance. Lorsque vous détectez une attaque de sécurité, vous recevrez une notification par e-mail concernant la mise à jour de la nouvelle signature. Vous pouvez télécharger la signature et l'appliquer sur votre appliance.

Comment recevoir une notification d'alerte de signature

January 21, 2021

Cet article explique comment configurer les paramètres d'alerte de signature pour recevoir des notifications par e-mail pour les nouvelles mises à jour de signature.

Synthèse

Les administrateurs réseau souhaitent recevoir une notification par e-mail pour les nouvelles mises à jour et notifications de signature du pare-feu d'application Web.

Problème

Un administrateur réseau qui souhaite être averti lorsqu'une nouvelle signature est disponible pour le pare-feu d'application Web peut choisir d'être notifié par e-mail. L'administrateur recevra une notification par courriel lorsque de nouvelles signatures seront disponibles pour être téléchargées.
Administrateurs réseau pour recevoir une notification par e-mail pour les nouvelles mises à jour de signature.

Solution

Pour recevoir une notification par e-mail concernant les nouvelles mises à jour de signature, suivez les étapes ci-dessous :

1. Connectez-vous au site Web de support Citrix `https://support.citrix.com/user/alerts`.

2. Dans la section **Paramètres d'alerte**, activez l'option M'avertir par e-mail.
3. Sélectionnez **Ajouter des produits** pour afficher le catalogue de produits.
4. Cliquez sur **Citrix Web App Firewall**, puis activez la case à cocher **Citrix Web App Firewall**.
5. Cliquez sur **Enregistrer les paramètres**.



1. Dans la section **Paramètres d'alerte**, activez l'option M'avertir par e-mail.
2. Sélectionnez **Ajouter des produits** pour afficher le catalogue de produits.
3. Cliquez sur **Pare-feu d'application**, puis activez la case à cocher **Signatures**.
4. Cliquez sur **Enregistrer les paramètres**.

Mise à jour de signature version 27

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées dans la version 27. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques. La mise à jour de signature inclut l'ID de signature, la version de signature et la liste des CVE adressés.

Version de signature

Signature version 27 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0 et Citrix ADC 12.1.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999921	cve-2018-1002000	WEB-MISCWordpress Arigato Autoresponder et Newsletter SQL Injection vulnérabilité.
999920		Web-MisscWordPress plug-in Corner Ad 1.0.7 - Scripting inter-site stocké
999919	cve-2018-1002009	Vulnérabilité de script intersite Web-miscWordPress Arigato Autoresponder et Newsletter bft_unsubscribe.
999918	cve-2018-1002002	Web-miscWordPress Arigato Autoresponder et Newsletter vulnérabilité de script multi-site.
999918	cve-2018-1002003	Web-miscWordPress Arigato Autoresponder et Newsletter vulnérabilité de script multi-site.
999918	cve-2018-1002004	Web-miscWordPress Arigato Autoresponder et Newsletter vulnérabilité de script multi-site.

Règle de signature	ID CVE	Description
999918	cve-2018-1002005	Web-miscWordPress Arigato Autoresponder et Newsletter vulnérabilité de script multi-site.
999918	cve-2018-1002006	Web-miscWordPress Arigato Autoresponder et Newsletter vulnérabilité de script multi-site.
999918	cve-2018-1002007	Web-miscWordPress Arigato Autoresponder et Newsletter vulnérabilité de script multi-site.
999917	cve-2018-1002001	Web-miscWordPress Arigato Autoresponder et Newsletter vulnérabilité de script multi-site.
999917	cve-2018-1002008	Web-miscWordPress Arigato Autoresponder et Newsletter vulnérabilité de script multi-site.
999916	cve-2018-8719	Web-miscWordPress Plug-in WP Security Audit Journal - wp-content/uploads/wp-security-audit-log/* accès illimité
999915	cve-2019-7743	WEB-MISC- Joomla phar : // exécution de vulnérabilité d'injection d'objet wrapper de flux de fichiers non phar téléchargés
999914		Web-MisscWordPress Plug-in E-mail Abonnés et Newsletter 3.4.7 Vulnérabilité de divulgation d'informations

Règle de signature	ID CVE	Description
999913		Web-miscWordPress plug-in AD Manager WD v1.0.11 - wd_ads_admin_class.php Téléchargement de fichier arbitraire
999912		WEB-IIS Microsoft IIS - Divulgation de nom de fichier abrégé ou de dossier

Mise à jour de signature version 28

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées dans la version 28. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques. La mise à jour de signature inclut l'ID de signature, la version de signature et la liste des CVE adressés.

Version de signature

Signature version 28 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0 et Citrix ADC 12.1 et Citrix ADM 13.0.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999898	CVE-2018-12895	WEB-MISC WordPress avant 4.9.7-Vulnérabilité de traversée du répertoire.
999899	CVE-2019-9618	WEB-Misc-Gracemedia Media Player Plug-in WordPress 1.0 Vulnérabilité d'inclusion de fichiers locaux arbitraire

Règle de signature	ID CVE	Description
999900	CVE-2018-20714	WEB-MISC plug-in WordPress WooCommerce avant 3.4.6 - Vulnérabilité de suppression de fichier.
999901	CVE-2018-11868	WEB-MISC FlowPaper FlexPaper avant 2.3.7 peut permettre l'exécution de code à distance réinitialisation des fichiers de configuration.
999902	CVE-2018-11868	WEB-MISC FlowPaper FlexPaper avant 2.3.7 peut permettre l'exécution de code à distance.
999903	CVE-2019-9184	Web-Misc-Joomla ! J2Store plug-in 3.x Avant 3.3.7 Autorise l'injection SQL.
999904	CVE-2019-9168	WEB-MISC plug-in WordPress WooCommerce avant 3.5.5-cross-site scripting via la légende Photoswipe.
999905		WEB-MISC plug-in WordPress Abandoned Panier avant 5.1.3 pour WooCommerce stocké Cross-Site Scripting.
999906	CVE-2019-8942	WEB-MISC WordPress avant 4.9.9 et 5.x avant 5.0.1-exécution de code à distance.
999907	CVE-2019-8942	WEB-MISC WordPress avant 4.9.9 et 5.x avant 5.0.1-exécution de code à distance.
999908	CVE-2019-8942	WEB-MISC WordPress avant 4.9.9 et 5.x avant 5.0.1-exécution de code à distance

Règle de signature	ID CVE	Description
999909	CVE-2017-16562	Web-misc-Deluxe Thème UserPro WordPress Plug-in Vulnérabilité de contournement de sécurité via up_auto_log=true Paramètre
999910	CVE-2018-20782	WEB-MISC plug-in WordPress Globee avant 1.1.2 pour Woocommerce-IPN Messages Usurpation
999911	CVE-2019-6340	Exécution de code à distance Drupal-arbitraire dans Drupal Core 8 RESTful WebServices

Mise à jour de signature version 29

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées dans la version 29. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 29 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque** :
>
> L'activation des règles de signature du corps de publication et du corps de la réponse peut affecter le CPU Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999896	CVE-2019-2725	Weblogic 10.3.6 Exécution de code à distance
999897	CVE-2019-2725	Weblogic 10.3.6 Exécution de code à distance

Mise à jour de signature version 30

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées dans la version 30. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 30 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque**
>
> L'activation des règles de signature du corps de publication et du corps de la réponse peut affecter le CPU Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999879	<>	WEB-MISC Plug-in WordPress WooCommerce Checkout Manager - Vulnérabilité de téléchargement de fichier arbitraire
999880	<>	Web-MISC WordPress Plug-in Advance Contact Form 7 DB avant 1.6.1 - Vulnérabilité dans l'injection SQL

Règle de signature	ID CVE	Description
999881	<>	WEB-MISC WordPress Plug-in Contact Form Builder avant 1.0.67 - Vulnérabilité d'inclusion de fichier local
999882	<>	Tentative d'injection aveugle d'URI HTTP SQL
999883	<>	WEB-MISC Loco Translate Plug-in WordPress 2.1.1 et versions antérieures - Vulnérabilité d'inclusion de fichiers locaux
999884	<>	WEB-MISC Plug-in WordPress Duplique-page antérieure à 3.4 - Vulnérabilité dans l'injection SQL
999885	CVE-2019-0232	WEB-MISC Apache Tomcat RCE via des scripts CGI .CMD lorsque EnableCMDlineargu-ments=true dans MS Windows
999886	CVE-2019-0232	WEB-MISC Apache Tomcat RCE via des scripts CGI .BAT lorsque EnableCMDlineargu-ments=true dans MS Windows
999887	CVE-2019-10692	WWEB-MISC WordPress plug-in wp-google-maps antérieures à 7.11.18 - Vulnérabilité dans l'injection de SQL.
999888	CVE-2019-10946	WEB-MISC Joomla! Avant la version 3.9.5 - Vulnérabilité de contournement de la sécurité
999889	CVE-2019-10945	WEB-MISC Joomla! Avant 3.9.5 - Vulnérabilité de traversée d'annuaire

Règle de signature	ID CVE	Description
999890	CVE-2019-9912	WEB-MISC WPGoogleMaps plug-in WordPress antérieur à 7.10.41 Vulnérabilité de script inter-site réfléchie
999890	CVE-2019-9912	WEB-MISC WPGoogleMaps plug-in WordPress antérieur à 7.10.41 Vulnérabilité de script inter-site réfléchie
999891	CVE-2019-9911	WEB-MISC Plug-in WordPress Réseaux Sociaux Auto-Poster Avant 4.2.8 - Vulnérabilité de script inter-site réfléchie
999892	CVE-2019-9908	WEB-MISC Plug-in WordPress Font_Organizer 2.1.1 - Script inter-site réfléchi
999893	CVE-2019-9787	WEB-MISC WordPress avant 4.9.7 - Vulnérabilité d'exécution de code à distance
999894	CVE-2019-9568	WEB-MISC Forminator Forminator Contact Form, sondage et quiz Builder plug-in WordPress avant la vulnérabilité 1.6 Blind SQLi
999895	CVE-2019-9567	Formulaire de contact WEB-MISC Forminator, Sondage & Quiz Builder plug-in WP avant 1.6 Vulnérabilité persistante de script intersite
999877	CVE-2018-20062	WEB-MISC NONECMS V1.3 - Vulnérabilité d'exécution de code PHP arbitraire dans le filtre ThinkPHP

Règle de signature	ID CVE	Description
999878	CVE-2019-9082	Vulnérabilité d'exécution de code à distance WEB-MISC dans ThinkPHP 5.x avant 5.1.32

Mise à jour de signature version 32

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées dans la version 32. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 32 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque**
>
> L'activation des règles de signature du corps de publication et du corps de la réponse peut affecter le CPU Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999875	CVE-2016-4438, CVE-2016-3087	WEB-STRUTS Apache Struts 2.3.20 à 2.3.28.1 Vulnérabilité d'exécution à distance via URL
999876	CVE-2019-10867	WEB-MISC Pimcore antérieur à 5.7.1 - Vulnérabilité de désérialisation (CVE-2019-10867)

Mise à jour de signature version 33

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées dans la version 33. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 33 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque**
>
> L'activation des règles de signature du corps de publication et du corps de la réponse peut affecter le CPU Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle	CVE	Description	Référence sur les vulnérabilités
999860		Vulnérabilité liée au script inter-site du plug-in WordPress Yuzo	https://www.wordfence.com/blog/2019/04/yuzo-related-posts-zero-day-vulnerability-exploited-in-the-wild
999861	CVE-2019-12099		cve,2019-12099

Règle	CVE	Description	Référence sur les vulnérabilités
999862		Backup de base de données WordPress plug-in <= 5.2 - Exécution de code à distance	https://www.wordfence.com/blog/2019/05/os-command-injection-vulnerability-patched-in-wp-database-backup-plug-in
999863		WordPress plug-in Slick Popup - Escalation des privilèges	https://www.wordfence.com/blog/2019/05/privilege-escalation-flaw-present-in-slick-popup-plug-in
999864	CVE-2019-10866	Plug-in WordPress Form Maker 1.13.3 - Injection SQL	cve,2019-10866
999865		Plug-in WordPress Give — Scripting inter-site stocké pour les donateurs	https://blog.sucuri.net/2019/05/wordpress-plug-in-give-stored-xss-for-donors.html
999866		Plug-in WordPress My Calendar <= 3.1.9 - Vulnérabilité de script intersite non authentifié	https://wpvulndb.com/vulnerabilities/9267

Règle	CVE	Description	Référence sur les vulnérabilités
999867		Plug-in WordPress Slimstat <= 4.8 - Script inter-site stocké non authentifié	https://blog.sucuri.net/2019/05/slimstat-stored-xss-from-visitors.html
999868	CVE-2019-2618	Vulnérabilité de téléchargement arbitraire de WebLogic	cve,2019-2618
999869	CVE-2019-11871	WEB-WORDPRESS Plug-in WordPress Custom Field Suite antérieure à 2.5.15 - Vulnérabilité de script inter-site	cve,2019-11871
999870		WEB-WORDPRESS WordPress Live Chat Support plug-in Vulnérabilité de script inter-site persistant antérieure 8.0.27 via le paramètre wplc_custom_js	https://blog.sucuri.net/2019/05/persistent-cross-site-scripting-in-wp-live-chat-support-plug-in.html
999871		WEB-WORDPRESS plug-in WordPress W3 Total Cache antérieur à 0.9.7.4 - Vulnérabilité d'exécution de code à distance PHAR	https://wpvulndb.com/vulnerabilities/9270

Règle	CVE	Description	Référence sur les vulnérabilités
999872		WEB-WORDPRESS plug-in WordPress W3 Total Cache antérieur à 0.9.7.4 - Vulnérabilité d'exécution de code à distance PHAR	https://wpvulndb.com/vulnerabilities/9269
999873	CVE-2019-0604	WEB-MISC Microsoft Windows SharePoint Server - Vulnérabilité d'exécution de code à distance	cve,2019-0604
999874		WEB-WORDPRESS Yuzo Publications associées à Yuzo Vulnérabilité de script inter-site stockée non authentifiée dans 5.12.91	https://www.wordfence.com/blog/2019/04/yuzo-related-posts-zero-day-vulnerability-exploited-in-the-wild

Mise à jour de signature version 34

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées dans la version 34. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 34 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque**
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999843		WEB-WORDPRESS plug-in WordPress Membre Ultimate avant la version 2.0.46 - Définition d'un fichier arbitraire pour la lecture
999844		WEB-WORDPRESS plug-in WordPress Membre Ultimate avant la version 2.0.46 - Fichier arbitraire Lu
999845		WEB-WORDPRESS plug-in WordPress Ultimate Member avant la version 2.0.46 - Suppression de fichier via le remplacement de fichier
999846		WEB-WORDPRESS plug-in WordPress Ultimate Member avant la version 2.0.46 - Suppression de fichiers
999847		WEB-WORDPRESS Plug-in WordPress Shortlinks avant 2.1.10 - Vulnérabilité d'injection CSV
999848		WEB-WORDPRESS Plug-in WordPress Shortlinks antérieures à 2.1.10 - Vulnérabilité de script intersite stockée non authentifiée

Règle de signature	ID CVE	Description
999849		WEB-WORDPRESS Plug-in WordPress FV Flowplayer Video Player avant 7.3.13.727 - Vulnérabilité de script inter-site stockée non authentifiée
999850		WEB-WORDPRESS plug-in WordPress Téléchargements numériques faciles avant 2.9.16 - Vulnérabilité de script inter-sites stockés non authentifiés
999851		WEB-WORDPRESS plug-in WordPress Crelly Slider antérieur à la version 1.3.5 - Vulnérabilité de téléchargement de fichier arbitraire
999853	CVE-2019-2615	Vulnérabilité de divulgation d'informations dans Oracle WebLogic Server WEB-MISC
999854	CVE-2019-11872	Plug-in WordPress Hustle avant 6.0.8.1 - Vulnérabilité d'injection CSV
999855	CVE-2019-11231	WEB-MISC GetSimple CMS version 3.3.15 et antérieure - Vulnérabilité de téléchargement de fichiers arbitraire
999856	CVE-2019-11231	WEB-MISC GetSimple CMS Version 3.3.15 et antérieure - Divulgation d'informations sur les clés API

Règle de signature	ID CVE	Description
999857		WEB-WORDPRESS WordPress plug-in WP Backup de base de données antérieures à 5.2 - Vulnérabilité d'injection de commande
999858		WEB-WORDPRESS plug-in WordPress Slick Popup to 1.7.1 - Vulnérabilité d'escalade de privilèges
999859	CVE-2019-12099	Vulnérabilité d'exécution de code à distance WEB-MISC PHP Fusion CMS dans la version 9.03.00 et antérieure

Mise à jour de signature version 35

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées dans la version 35. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 35 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque**
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999834	CVE-2019-13024	WEB-MISC Centreon Version 19.04 et Prior - Vulnérabilité d'injection de commandes
999835	CVE-2019-5420	Mode de développement WEB-MISC Rails - Vulnérabilité de divulgation de jeton secret
999836	CVE-2019-5418	WEB-MISC Rails Action View - Vulnérabilité de divulgation de contenu de fichiers
999837	CVE-2018-12426, CVE-2019-11185	WEB-WORDPRESS WP Live Chat Support Pro Plug-in avant 8.0.26 - Téléchargement de fichier arbitraire
999838	CVE-2019-10270	WEB-WORDPRESS plug-in WordPress Ultimate Member avant la version 2.0.40 - Réinitialisation arbitraire du mot de passe
999839	CVE-2019-12826	WEB-WORDPRESS Plug-in WordPress Widget Logic Avant 5.10.2 - Vulnérabilité CSRF
999840		WEB-WORDPRESS plug-in WordPress Calendrier d'événements tout-en-un antérieur à 2.5.39 - Vulnérabilité de script inter-site
999841	CVE-2019-11565	WEB-WORDPRESS plug-in WordPress Imprimer mon blog avant 1.6.7 - Vulnérabilité SSRF non authentifiée

Règle de signature	ID CVE	Description
999842		WEB-WORDPRESS plug-in WordPress Membre Ultimate Avant la version 2.0.46 - Multiple `cross-site scripting</LogString`

Mise à jour de signature version 36

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées dans la version 36. Vous pouvez télécharger et configurer les règles de signature pour protéger votre appliance contre les attaques fragiles de sécurité.

Version de signature

Signature version 36 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque** :
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999817		WEB-WORDPRESS Plug-in d'insertion publicitaire WordPress avant la version 2.4.22 - Exécution de code à distance

Règle de signature	ID CVE	Description
999818	CVE-2019-7839	WEB-MISC Adobe ColdFusion Multiple Versions - Vulnérabilité d'exécution de code à distance via HTTP/SOAP DotNet à Java (CVE-2019-7839)
999819	CVE-2019-7839	WEB-MISC Adobe ColdFusion Multiple Versions - Vulnérabilité d'exécution de code à distance via HTTP/SOAP Java-to-DotNet (CVE-2019-7839)
999820	CVE-2019-11469	WEB-MISC Zoho ManageEngine Applications Manager antérieures à 14 build 14150 autorise SQLi via le paramètre resourceid (CVE-2019-11469)
999821	CVE-2019-11448	WEB-MISC Zoho ManageEngine Application Manager 11.0 à 14.0 - Injection SQL non authentifiée (CVE-2019-11448)
999822	CVE-2019-1003000	Plug-in de sécurité de script WEB-MISC Jenkins jusqu'à 1.49 - Vulnérabilité de contournement du sandbox (CVE-2019-1003000)
999823		WEB-WORDPRESS WordPress Cforms2 plug-in jusqu'à 15.0.1 - Vulnérabilité d'injection HTML non authentifiée

Règle de signature	ID CVE	Description
999824	CVE-2019-0193	WEB-MISC Apache Solr avant 8.2 - Vulnérabilité d'exécution de code à distance DIH via le paramètre DataConfig (CVE-2019-0193)
999825	CVE-2019-11580	WEB-MISC Atlassian Crowd Pdkinstall Development Plug-in activé - RCE non authentifié (CVE-2019-11580)
999826	CVE-2019-0192	WEB-MISC Apache Solr jusqu'à 5.5.5/6.6.5 - Vulnérabilité d'exécution de code à distance dans l'API de configuration (CVE-2019-0192)
999827		WEB-WORDPRESS WooCommerce Variation Swatch plug-in Jusqu'à 1.0.61 - Vulnérabilité de script inter-site réfléchie
999828	CVE-2019-1003001	WEB-MISC Jenkins Pipeline Groovy plug-in jusqu'à 2.61 - Vulnérabilité de contournement de sandbox via la création de travaux (CVE-2019-1003001)
999829	CVE-2019-1003001	WEB-MISC Jenkins Pipeline Groovy plug-in jusqu'à 2.61 - Vulnérabilité de contournement du sandbox (CVE-2019-1003001)
999830		WEB-WORDPRESS WordPress Bold Page Builder Plug-in antérieur à 2.3.2 - Vulnérabilité de contournement de sécurité

Règle de signature	ID CVE	Description
999831	CVE-2019-15107	WEB-MISC Webmin antérieur à 1.930 - Vulnérabilité d'exécution de code à distance non authentifiée (CVE-2019-15107)
999832	CVE-2019-2767	WEB-MISC Oracle BI Publisher 11.1.1.9.0 et 12.2.1.4 - Vulnérabilité XXE (CVE-2019-2767)
999833	CVE-2019-15106	WEB-MISC Zoho ManageEngine OpManager via 12.4x - Vulnérabilité de contournement de l'authentification (CVE-2019-15106)
999948	CVE-2014-0114	Apache Struts 1 à 1.3.10 permet la manipulation ClassLoader permettant l'exécution arbitraire de code via HTTP_FORM_FIELD
999949	CVE-2013-4316	Apache Struts 2 avant 2.3.15.2 permet l'invocation dynamique de méthode en affectant la confidentialité, l'intégrité ou la disponibilité
999950	CVE-2013-4316	Apache Struts 2 avant 2.3.15.2 permet l'invocation dynamique de méthode en affectant la confidentialité, l'intégrité ou la disponibilité

Remarque :

La règle de signature 999947 est supprimée en raison d'un problème de performances.

Mise à jour de signature version 37

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées dans la version 37. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 37 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque**
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999806	CVE-2019-3394	WEB-MISC Atlassian Confluence ou datacenter - Vulnérabilité de divulgation de fichiers locaux (CVE-2019-3394)
999807	CVE-2019-13569	WEB-WORDPRESS Icegram Email Abonnés & Newsletter Plug-in Avant 4.1.8 - SQLi Via ESFPX_Lists Param (CVE-2019-13569)
999808	CVE-2019-13569	WEB-WORDPRESS Icegram Email Abonnés & Newsletter plug-in Avant 4.1.8 - SQLi Via Order Param (CVE-2019-13569)

Règle de signature	ID CVE	Description
999809	CVE-2019-2768	WEB-MISC Oracle BI Publisher - Vulnérabilité de jeton de session prévisible (CVE-2019-2768)
999810	CVE-2019-1003001	WEB-MISC Jenkins Pipeline Groovy plug-in jusqu'à 2.61 - Vulnérabilité de contournement de sandbox via la mise à jour des travaux (CVE-2019-1003001)
999811	CVE-2019-13575	WEB-WORDPRESS WPEverest Everest Forms plug-in Avant 1.5.0 - Injection SQL (CVE-2019-13575)
999812	CVE-2019-15896	Plug-in WEB-WORDPRESS LifterLMS jusqu'à 3.34.5 - Vulnérabilité de contournement de sécurité (CVE-2019-15896)
999813	CVE-2019-3396	WEB-MISC Atlassian Confluence ou datacenter - Vulnérabilité d'exécution de code à distance (CVE-2019-3396)
999814	CVE-2019-5475	WEB-MISC Sonatype Nexus Repository Manager avant 2.14.14 - Exécution de code à distance via Createrepo Path (CVE-2019-5475)
999815	CVE-2019-5475	WEB-MISC Sonatype Nexus Repository Manager avant 2.14.14 - Exécution de code à distance via Mergerepo Path (CVE-2019-5475)

Règle de signature	ID CVE	Description
999816	CVE-2019-15104	WEB-MISC Zoho ManageEngine OpManager Version antérieure à 12.4 - Vulnérabilité d'injection SQL (CVE-2019-15104)

Mise à jour de signature version 38

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées dans la version 38. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 38 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque**
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999800	CVE-2019-12517	WEB-WORDPRESS plug-in SlickQuiz version 1.3.7.1 et antérieure - Vulnérabilité de script intersite (CVE-2019-12517)

Règle de signature	ID CVE	Description
999801	CVE-2019-10392	WEB-MISC Jenkins Git Client Plug-in 2.8.4 et antérieur - Vulnérabilité dans l'injection de commandes du système d'exploitation (CVE-2019-10392)
999802	CVE-2019-8371	WEB-MISC OpenEMR antérieur à 5.0.2 - Vulnérabilité d'exécution de code à distance via le champ Form_Filedata (CVE-2019-8371)
999803	CVE-2019-8371	WEB-MISC OpenEMR antérieur à 5.0.2 - Vulnérabilité d'exécution de code à distance via le champ Form_Image (CVE-2019-8371)
999804	CVE-2019-12516	WEB-WORDPRESS plug-in SlickQuiz version 1.3.7.1 et antérieures - Vulnérabilité dans l'injection SQL (CVE-2019-12516)
999805	CVE-2019-1262	WEB-MISC Microsoft SharePoint Server - Vulnérabilité de script intersite (CVE-2019-1262)

Mise à jour des signatures pour décembre 2019

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2019-12-19. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 39 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque**
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999760		Versions WEB-MISC FusionPBX antérieures à 4.4.7 et 4.5.5 - Vulnérabilité d'exécution de code à distance via /app/exec/exec.php
999761	CVE-2019-12747	Typo3 WEB-MISC avant 8.7.27 et 9.5.8 - Désérialisation des données non fiables (CVE-2019-12747)
999762	CVE-2019-13608	WEB-MISC Citrix StoreFront Server - Vulnérabilité d'injection d'entités externes XML (CVE-2019-13608)
999763		WEB-WORDPRESS WordPress Avant 5.2.4 - Vulnérabilité de la vue non authentifiée de messages privés ou de projets de posts/pages via FORM
999764		WEB-WORDPRESS WordPress Avant 5.2.4 - Vulnérabilité de la vue non authentifiée de messages privés ou de projets de posts/pages via URL

Règle de signature	ID CVE	Description
999765	CVE-2019-15954	WEB-MISC Total.js CMS 12.0.0 - Vulnérabilité d'injection de code JavaScript via JSON (CVE-2019-15954)
999766	CVE-2019-15954	WEB-MISC Total.js CMS 12.0.0 - Vulnérabilité d'injection de code JavaScript via FORM (CVE-2019-15954)
999767		WEB-WORDPRESS SyntaxHighlighter Plug-in évolué antérieur à 5.3.1 - Vulnérabilité de script inter-site stockée via un commentaire
999768		WEB-WORDPRESS SyntaxHighlighter Plug-in évolué antérieur à 5.3.1 - Vulnérabilité de script inter-site stockée via POST
999769		WEB-WORDPRESS SyntaxHighlighter Plug-in évolué antérieur à 5.3.1 - Vulnérabilité de script inter-site stockée via JSON
999770	CVE-2019-16120	Plug-in de tickets d'événement WEB-WORDPRESS avant 4.10.7.2 - Vulnérabilité d'injection CSV (CVE-2019-16120)
999771	CVE-2019-15029	WEB-MISC FusionPBX antérieure à 4.4.8 - Vulnérabilité d'exécution de code à distance (CVE-2019-15029)

Règle de signature	ID CVE	Description
999772		WEB-WORDPRESS Sassy Social Share Plug-in antérieur à 3.3.4 - Vulnérabilité de script intersite non authentifiée
999773		WEB-WORDPRESS E-mail Abonnés & Newsletter Plug-in version 4.3.1 et antérieures - Vulnérabilité SQLi aveugle non authentifiée
999774	CVE-2019-3398	WEB-MISC Atlassian Confluence ou centre de données - Vulnérabilité de traversée de chemin de téléchargement (CVE-2019-3398)
999775	CVE-2019-15952	WEB-MISC Total.js CMS 12.0.0 - Vulnérabilité de traversée du chemin de modèle de page (CVE-2019-15952)
999776	CVE-2019-17236	WEB-WORDPRESS IgniteUp Bientôt et plug-in Mode Maintenance Jusqu'à 3.4.0 - Script inter-site stocké (CVE-2019-17236)
999777	CVE-2019-10475	WEB-MISC Jenkins Build-Metrics plug-in 1.3 - Vulnérabilité de script intersite réfléchie (CVE-2019-10475)
999778	CVE-2019-17132	WEB-MISC vBulletin antérieur à 5.5.4 Patch Level 2 - Vulnérabilité d'exécution de code à distance de point de terminaison de l'API Avatar (CVE-2019-17132)

Règle de signature	ID CVE	Description
999779	CVE-2019-14994	WEB-MISC Atlassian Jira Service Desk - Vulnérabilité de traversée de chemin (CVE-2019-14994)
999780	CVE-2019-19367	WEB-MISC FusionPBX 4.4.1 et Prior - Vulnérabilité de script intersite (CVE-2019-19367)
999781	CVE-2019-18668	Plug-in WEB-WORDPRESS Currency Switcher avant 2.11.2 - Vulnérabilité de contournement dans le paramètre de devise via POST (CVE-2019-18668)
999782	CVE-2019-18668	Plug-in WEB-WORDPRESS Currency Switcher avant 2.11.2 - Vulnérabilité de contournement dans le paramètre de devise via GET (CVE-2019-18668)
999783	CVE-2019-16663	WEB-MISC RConfig 3.9.2 et Prior - Vulnérabilité d'exécution de code à distance via Search.crud.php (CVE-2019-16663)
999784		WEB-MISC Apache Solr jusqu'à 8.3.0 - Exécution de code à distance non authentifiée via le modèle personnalisé VelocityResponseWriter
999785	CVE-2019-17235	WEB-WORDPRESS IgniteUp bientôt et plug-in Mode Maintenance Jusqu'à 3.4.0 - Divulgation d'informations via Csv (CVE-2019-17235)

Règle de signature	ID CVE	Description
999786	CVE-2019-17235	WEB-WORDPRESS IgniteUp bientôt et plug-in Mode Maintenance jusqu'à 3.4.0 - Divulgation d'informations via Bcc (CVE-2019-17235)
999787	CVE-2019-12276	WEB-MISC GrandNode 4.40 - Vulnérabilité de traversée de chemin LetsenCryptController (CVE-2019-12276)
999788		WEB-WORDPRESS E-mail Abonnés & Newsletter Plug-in Avant la version 4.2.3 - Divulgation d'informations non authentifiées
999789	CVE-2019-4013	WEB-MISC IBM BigFix Platform 9.5 - Téléchargement de fichiers arbitraires authentifiés avec privilèges root (CVE-2019-4013)
999790	CVE-2019-11409	WEB-MISC FusionPBX Version 4.4.3 et antérieure - Exécution de code à distance via /app/basic_operator_panel/exec.php (CVE-2019-11409)
999791	CVE-2019-11409	WEB-MISC FusionPBX Version 4.4.3 et antérieure - Exécution de code à distance via /app/operator_panel/exec.php (CVE-2019-11409)

Règle de signature	ID CVE	Description
999792	CVE-2019-16662	WEB-MISC RConfig 3.9.2 et Prior - Exécution de code à distance non authentifiée via AjaxServerSettingSchk.php (CVE-2019-16662)
999793	CVE-2019-7609	WEB-MISC Elastic Kibana avant 5.6.15 et 6.6.1 - Une vulnérabilité de pollution par un prototype permet un RCE non authentifié (CVE-2019-7609)
999794	CVE-2019-10092	WEB-MISC Serveur HTTP Apache jusqu'à 2.4.39 - mod_proxy Scripting inter-site limité (CVE-2019-10092)
999795	CVE-2019-16520	PLUG-IN WEB-WORDPRESS All In One SEO Pack avant 3.2.7 - Vulnérabilité de script intersite stockée (CVE-2019-16520)
999796	CVE-2019-17234	WEB-WORDPRESS IgniteUp Bientôt et Plug-in Mode Maintenance jusqu'à 3.4.0 - Suppression de fichier arbitraire (CVE-2019-17234)
999797	CVE-2019-16525	Plug-in WEB-WORDPRESS Checklist avant la version 1.1.9 - Vulnérabilité de script intersite (CVE-2019-16525)
999798		Plug-in SVG sécurisé WEB-WORDPRESS antérieur à 1.9.6 - Vulnérabilité de script intersite

Règle de signature	ID CVE	Description
999799		WEB-WORDPRESS E-mail Abonnés & Newsletter Plug-in avant la version 4.2.3 - Création d'options arbitraires non authentifiées

Mise à jour de signature version 40

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées pour la semaine 2020-01-14. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques. La mise à jour de signature inclut l'ID de signature, la version de signature et la liste des CVE adressés.

Version de signature

Signature version 40 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> La version 40 de mise à jour de signature inclut un correctif pour la règle de signature incorrecte 1861.
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999732	CVE-2019-1620	WEB-MISC Cisco Data Center Network Manager avant 11.2 (1) - Vulnérabilité de téléchargement de fichiers arbitraire (CVE-2019-1620)
999733	CVE-2019-16702	WEB-MISC Integard Pro 2.2.0.9026 - Vulnérabilité de dépassement de tampon NoJS (CVE-2019-16702)
999734	CVE-2019-1621	WEB-MISC Cisco Data Center Network Manager avant 11.2 (1) - Vulnérabilité de téléchargement de fichiers arbitraire (CVE-2019-1621)
999735	CVE-2019-8451	WEB-MISC Atlassian Jira Server avant 8.4.0 - Vulnérabilité de falsification de requêtes côté serveur (CVE-2019-8451)
999736		WEB-WORDPRESS Plug-in de conformité aux cookies GDPR antérieur à 4.0.3 - Vulnérabilité de suppression de paramètres arbitraires authentifiés
999737	CVE-2019-11287	WEB-MISC Pivotal RabbitMQ 3.7.x avant 3.7.21 et 3.8.x avant 3.8.1 - Vulnérabilité de déni de service (CVE-2019-11287)
999738		WEB-WORDPRESS Ultimate Addons pour Elementor avant 1.20.1 - Vulnérabilité de contournement de l'authentification via Facebook

Règle de signature	ID CVE	Description
999739		WEB-WORDPRESS Ultimate Addons pour Elementor avant 1.20.1 - Vulnérabilité de contournement de l'authentification via Google Login
999740	CVE-2019-19366	WEB-MISC FusionPBX antérieur à 4.4.10 - Vulnérabilité de script inter-site dans xml_cdr_search.php via le paramètre de redirection (CVE-2019-19366)
999741	CVE-2019-16931	Plug-in WEB-WORDPRESS Visualizer antérieur à la version 3.3.1 - Vulnérabilité de script intersite non authentifiée (CVE-2019-16931)
999742	CVE-2019-16932	WEB-WORDPRESS Plug-in Visualizer antérieur à la version 3.3.1 - SSRF non authentifié (CVE-2019-16932)
999743	CVE-2019-1619	WEB-MISC Cisco Data Center Network Manager avant 11.1 (1) - Vulnérabilité de contournement de l'authentification (CVE-2019-1619)
999744	CVE-2019-12562	WEB-MISC DotNetNuke Before 9.4.0 - Vulnérabilité de script inter-site stocké (CVE-2019-12562)

Règle de signature	ID CVE	Description
999745	CVE-2019-8371	WEB-MISC OpenEMR antérieur à 5.0.2 - Vulnérabilité d'exécution de code à distance via le champ Form_Filedata (CVE-2019-8371)
999746	CVE-2019-8371	WEB-MISC OpenEMR antérieur à 5.0.2 - Vulnérabilité d'exécution de code à distance via le champ Form_Image (CVE-2019-8371)
999747		WEB-WORDPRESS Beaver Builder Ultimate Addons antérieurs à 1.24.1 - Vulnérabilité de contournement de l'authentification via Facebook
999748		WEB-WORDPRESS Beaver Builder Ultimate Addons antérieurs à 1.24.1 - Vulnérabilité de contournement de l'authentification via Google Login
999749	CVE-2019-19650	WEB-MISC Zoho ManageEngine AM avant la construction 13640 - SQLi via l'agent Servlet (CVE-2019-19650)
999750		WEB-MISC Zoho ManageEngine AM avant la construction 13620 - Divulgation de clé API via le servlet OpmRequestHandlerServlet

Règle de signature	ID CVE	Description
999751	CVE-2019-1622	WEB-MISC Cisco Data Center Network Manager 11.0 (1) - Vulnérabilité de divulgation d'informations (CVE-2019-1622)
999752	CVE-2019-16759	WEB-MISC vBulletin antérieur à la version 5.5.4 Patch Level 1 - Vulnérabilité d'exécution de code à distance (CVE-2019-16759)
999753		Image en vedette WEB-WORDPRESS à partir du plug-in d'URL antérieure à 2.7.8 - Vulnérabilité liée aux contrôles d'accès manquants sur l'API REST
999754	CVE-2019-10098	WEB-MISC Serveur HTTP Apache jusqu'à 2.4.39 - Vulnérabilité de redirection auto-référentielle mod_rewrite (CVE-2019-10098)
999755	CVE-2019-1936	WEB-MISC Cisco UCS Director 6.0 à 6.6.1.0 et 6.7.0.0 à 6.7.1.0 - Vulnérabilité d'injection de commandes (CVE-2019-1936)
999756	CVE-2019-19649	WEB-MISC Zoho ManageEngine AM avant la construction 13620 - Paramètre SQLi via EventID non authentifié (CVE-2019-19649)

Règle de signature	ID CVE	Description
999757	CVE-2019-19649	WEB-MISC Zoho ManageEngine AM avant la construction 13620 - Paramètre SQLi via entité non authentifié (CVE-2019-19649)
999758	CVE-2019-15036	WEB-MISC JetBrains TeamCity Before 2019.1 - Vulnérabilité d'injection de commandes du système d'exploitation (CVE-2019-15036)
999759	CVE-2019-17239	WEB-WORDPRESS Télécharger des plug-ins et des thèmes depuis le plug-in de tableau de bord jusqu'à 1.5 - Vulnérabilité de script intersite stockée (CVE-2019-17239)

Mise à jour de signature version 41

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées pour la semaine 2020-02-04. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques. La mise à jour de signature inclut l'ID de signature, la version de signature et la liste des CVE adressés.

Version de signature

Signature version 41 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> La version 41 de mise à jour de signature inclut un correctif pour la règle de signature incorrecte 1861.

> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999717		WEB-WORDPRESS WordPress Version 5.3.x et Prior - Vulnérabilité de déni de service via xmlrpc.php pingback.ping méthode
999718		WEB-WORDPRESS Backup and Staging by WP Time Capsule plug-in avant 1.21.16 - Vulnérabilité de contournement de l'authentification
999719	CVE-2019-19731	WEB-MISC Roxy Fileman pour .NET 1.4.5 - Vulnérabilité de traversée de chemin via RENAMEFILE (CVE-2019-19731)
999720	CVE-2019-19915	WEB-WORDPRESS 301 Redirections — Plug-in Easy Redirect Manager jusqu'à 2.4.0 - Vulnérabilités multiples (CVE-2019-19915)
999721	CVE-2019-17662	WEB-MISC Cybele Software ThInVNC antérieure à la version 1.0b1 - Vulnérabilité de traversée d'annuaire (CVE-2019-17662)

Règle de signature	ID CVE	Description
999722	CVE-2020-6168	WEB-WORDPRESS Plug-in minimal à venir bientôt et en mode maintenance avant 2.17 - Vulnérabilité liée au paramètre de maintenance (CVE-2020-6168)
999723	CVE-2020-6166	WEB-WORDPRESS Plug-in Minimal Bientôt Bientôt et Maintenance Mode avant 2.17 - Vulnérabilité liée à la modification de thème (CVE-2020-6166)
999724	CVE-2020-6166	WEB-WORDPRESS Plug-in Minimale Bientôt et Mode Maintenance avant 2.17 - Vulnérabilité liée aux paramètres d'exportation (CVE-2020-6166)
999725		Plug-in du client WEB-WORDPRESS IniFiniteWP antérieur à 1.9.4.5 - Vulnérabilité de contournement de l'authentification
999726	CVE-2019-16773	WEB-WORDPRESS Versions WordPress antérieures à 5.3.1 - Vulnérabilité de script inter-site via l'API REST avec l'objet JSON (CVE-2019-16773)
999727	CVE-2019-16773	WEB-WORDPRESS Versions WordPress antérieures à 5.3.1 - Vulnérabilité de script inter-site via l'API REST avec FORM FIELD (CVE-2019-16773)

Règle de signature	ID CVE	Description
999728	CVE-2019-16773	WEB-WORDPRESS Versions WordPress antérieures à 5.3.1 - Vulnérabilité de script inter-site via user-edit.php (CVE-2019-16773)
999729	CVE-2019-16773	WEB-WORDPRESS Versions WordPress antérieures à 5.3.1 - Vulnérabilité de script inter-site via profile.php (CVE-2019-16773)
999730	CVE-2019-16113	WEB-MISC Bludit 3.9.2 - Vulnérabilité d'exécution de code à distance par téléchargement d'images via uuid (CVE-2019-16113)
999731	CVE-2019-16113	WEB-MISC Bludit 3.9.2 - Vulnérabilité d'exécution de code à distance par téléchargement d'images via filename (CVE-2019-16113)

Mise à jour des signatures pour février 2020

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-02-11. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 42 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque**
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999707		Plug-in WEB-WORDPRESS WPCentral antérieur à la version 1.4.8 - Vulnérabilité d'escalade de privilèges
999708	CVE-2019-15979	WEB-MISC Cisco Data Center Network Manager antérieur à 11.3 (1) - Vulnérabilité d'injection de commandes (CVE-2019-15979)
999709	CVE-2019-15978	WEB-MISC Cisco Data Center Network Manager antérieur à 11.3 (1) - Vulnérabilité d'injection de commande (CVE-2019-15978)
999710	CVE-2019-15975	WEB-MISC Cisco Data Center Network Manager antérieur à 11.3 (1) - Vulnérabilité de contournement d'authentification (CVE-2019-15975)
999711	CVE-2019-15976	WEB-MISC Cisco Data Center Network Manager antérieur à 11.3 (1) - Vulnérabilité de contournement d'authentification (CVE-2019-15976)

Règle de signature	ID CVE	Description
999712	CVE-2019-16405	WEB-MISC Centreon antérieure à la version 19.10.2 - Vulnérabilité d'exécution de code à distance (CVE-2019-16405)
999713	CVE-2020-7048	Plug-in de réinitialisation de base de données WEB-WORDPRESS WP jusqu'à 3.1 - Vulnérabilité de réinitialisation de table de base de données non authentifiée (CVE-2020-7048)
999714	CVE-2020-7108	Plug-in WEB-WORDPRESS LearnDash antérieur à la version 3.1.2 - Vulnérabilité de script intersite réfléchie (CVE-2020-7108)
999715	CVE-2019-15977	WEB-MISC Cisco Data Center Network Manager antérieur à 11.3 (1) - Vulnérabilité de contournement d'authentification (CVE-2019-15977)
999716	CVE-2020-2096	WEB-MISC Jenkins Gitlab Hook Plug-in Version 1.4.2 et antérieure - Vulnérabilité de script intersite (CVE-2020-2096)

Mise à jour des signatures pour février 2020

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-02-27. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre

appliance contre les attaques.

Version de signature

Signature version 43 applicable pour NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999696	CVE-2019-15983	WEB-MISC Cisco Data Center Network Manager antérieur à 11.3 (1) - Vulnérabilité d'entité externe XML (CVE-2019-15983) via CablePlans
999697	CVE-2019-20197	WEB-MISC Nagios XI 5.6.9 - Vulnérabilité d'exécution de commande arbitraire authentifiée (CVE-2019-20197)
999698	CVE-2020-8417	Plug-in d'extraits de code WEB-WORDPRESS antérieur à 2.14.0 - Vulnérabilité CSRF (CVE-2020-8417)
999699		Plug-in WEB-WORDPRESS WPCentral antérieur à la version 1.4.8 - Vulnérabilité d'escalade de privilèges

Règle de signature	ID CVE	Description
999700	CVE-2020-8596	Plug-in de base de données des participants WEB-WORDPRESS antérieur à 1.9.5.6 - Vulnérabilité d'injection SQL authentifiée (CVE-2020-8596)
999701	CVE-2020-8426	Plug-in WEB-WORDPRESS Elementor Page Builder antérieur à 2.8.5 - Vulnérabilité de script inter-site reflétée authentifiée (CVE-2020-8426)
999702	CVE-2019-19509	WEB-MISC RConfig 3.9.3 - Vulnérabilité d'exécution de code à distance via ajaxArchiveFiles.php (CVE-2019-19509)
999703	CVE-2019-8449	WEB-MISC Atlassian Jira Server avant 8.4.0 - Vulnérabilité de divulgation d'informations (CVE-2019-8449)
999704	CVE-2019-9194	WEB-MISC ELFinder antérieur à 2.1.48 - Vulnérabilité d'injection de commande de connecteur PHP (CVE-2019-9194)
999705	CVE-2019-15985	WEB-MISC Cisco Data Center Network Manager antérieur à 11.3 (1) - Vulnérabilité d'injection SQL (CVE-2019-15985) via GetVMHostData

Règle de signature	ID CVE	Description
999706	CVE-2020-8549	WEB-WORDPRESS Strong Témoignages Plug-in antérieur à 2.40.1 - Vulnérabilité de script intersite stockée (CVE-2020-8549)

Mise à jour des signatures pour avril 2020

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-04-27. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 44 est applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999683	CVE-2020-9043	Plug-in WEB-WORDPRESS WPCentral antérieur à 1.5.1 - Vulnérabilité de divulgation de clé de connexion (CVE-2020-9043)

Règle de signature	ID CVE	Description
999684		WEB-WORDPRESS Plug-in Duplicate-post version 3.2.3 et antérieure - Scripting inter-site persistant
999685		WEB-WORDPRESS Plug-in Duplicate-post version 3.2.3 et antérieure - Scripting inter-site persistant
999686	CVE-2020-0618	WEB-MISC Microsoft SQL Server Reporting Services - Vulnérabilité d'exécution de code à distance (CVE-2020-0618)
999687	CVE-2019-16278	WEB-MISC Nostromo Nhttpd antérieur à 1.3.7 - La fonction Strcutl permet l'exécution de code à distance non authentifié (CVE-2019-16278)
999688	CVE-2019-1937	WEB-MISC Cisco UCS Director 6.6.0.0 à 6.6.1.0 et 6.7.0.0 à 6.7.1.0 - Vulnérabilité de contournement d'authentification (CVE-2019-1937)
999689		WEB-WORDPRESS Plug-in Duplicate-post version 3.2.3 et antérieure - Scripting inter-site persistant
999690	CVE-2020-9006	Plug-in WEB-WORDPRESS Popup Builder antérieur à 3.0 - Vulnérabilité dans l'injection SQL via la désérialisation PHP (CVE-2020-9006)

Règle de signature	ID CVE	Description
999691		WEB-WORDPRESS Plug-in Duplicate-post version 3.2.3 et antérieure - Scripting inter-site persistant
999692		WEB-MISC empêche la contrebande de requêtes via l'en-tête de longueur de contenu et de transfert
999693		Plug-in WEB-WORDPRESS ThemeGrill Demo Importer avant 1.6.3 - Vulnérabilité de contournement d'authentification et d'effacement de base de données
999694	CVE-2019-17237	WEB-WORDPRESS IgniteUp Bientôt disponible et plug-in Mode de maintenance avant 3.4.1 - Vulnérabilité CSRF via message (CVE-2019-17237)
999695	CVE-2019-17237	WEB-WORDPRESS IgniteUp Bientôt disponible et plug-in Mode de maintenance avant 3.4.1 - Vulnérabilité CSRF via Subject (CVE-2019-17237)

Mise à jour de la signature pour mai 2020

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-05-26. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 45 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC. Selon la dernière version de Snort, les règles de signature avec ID 1258, 1306, 2520, 2661, 5695, 10996, 11817, 12056, 15471, 17049 et 21634 ont été supprimées.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999666		Plug-in WEB-WORDPRESS Duplicator antérieur à 1.3.28 - Vulnérabilité de téléchargement de fichier arbitraire non authentifié
999667	CVE-2020-10220	WEB-MISC RConfig à 3.94 - Vulnérabilité dans l'injection SQL (CVE-2020-10220)
999668	CVE-2020-5844	WEB-MISC Artica Pandora FMS 7.0 - Exécution de fichiers arbitraires de type dangereux Via /attachment/files_repo/ (CVE-2020-5844)
999669	CVE-2020-8813	WEB-MISC Cacti antérieure à 1.2.10 - Vulnérabilité d'exécution de code à distance via graph_realtime.php (CVE-2020-8813)
999670	CVE-2020-8654	WEB-MISC EyeSofNetwork 5.3 - Vulnérabilité d'exécution de code à distance (CVE-2020-8654)

Règle de signature	ID CVE	Description
999671	CVE-2020-10196	WEB-WORDPRESS Sygnoos Popup Builder Plug-in antérieur à 3.64.1 - Vulnérabilité de script intersite non authentifiée (CVE-2020-10196)
999672	CVE-2019-15949	WEB-MISC Nagios XI avant 5.6.6 - Vulnérabilité d'exécution de code à distance en tant que racine (CVE-2019-15949)
999673	CVE-2020-10879	WEB-MISC RConfig 3.9.5 et antérieures - Vulnérabilité d'exécution de code à distance via search.crud.php (CVE-2020-10879)
999674	CVE-2020-8656	WEB-MISC EyeSofNetwork 5.3 - Vulnérabilité d'injection SQL dans l'API EyeSofNetwork 2.4.2 (CVE-2020-8656)
999675	CVE-2020-10195	WEB-WORDPRESS Sygnoos Popup Builder Plug-in Avant 3.64.1 - Divulgation d'informations système authentifiées (CVE-2020-10195)
999676	CVE-2020-10195	WEB-WORDPRESS Sygnoos Popup Builder Plug-in Avant 3.64.1 - Divulgation d'informations sur les abonnés authentifiés (CVE-2020-10195)

Règle de signature	ID CVE	Description
999677	CVE-2020-10195	WEB-WORDPRESS Sygnoos Popup Builder plug-in antérieur à 3.64.1 - Modification des paramètres authentifiés (CVE-2020-10195)
999678	CVE-2020-0646	Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance dans le workflow .NET Framework via SOAP 1.2 (CVE-2020-0646)
999679	CVE-2020-0646	Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance dans le workflow .NET Framework via SOAP 1.1 (CVE-2020-0646)
999680	CVE-2020-10221	WEB-MISC RConfig à 3.94 - Vulnérabilité d'exécution de code à distance (CVE-2020-10221)
999681	CVE-2019-19134	WEB-WORDPRESS Hero Maps Premium avant 2.2.3 - Vulnérabilité liée aux scripts intersites réfléchis non authentifiés (CVE-2019-19134)
999682	CVE-2020-10385	Plug-in WEB-WORDPRESS WPForms antérieur à 1.5.9 - Vulnérabilité de script intersite stockée (CVE-2020-10385)

Mise à jour de la signature pour juin 2020

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-06-03. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 46 applicable pour NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999643		WEB-WORDPRESS 10Web Map Builder for Google Maps plug-in antérieur à 10.0.64 - Vulnérabilité de script intersite non authentifiée via la page gmwd_setup
999644		WEB-WORDPRESS 10Web Map Builder for Google Maps plug-in 10.0.64 et versions antérieures - Vulnérabilité de script intersite via la page options_gmwd
999645	CVE-2020-5187	WEB-MISC DNN jusqu'à 9.4.4 - Vulnérabilité de traversée de chemin via une URL (CVE-2020-5187)

Règle de signature	ID CVE	Description
999646	CVE-2020-5187	WEB-MISC DNN jusqu'à 9.4.4 - Vulnérabilité de traversée de chemin via local (CVE-2020-5187)
999647	CVE-2020-9335	Plug-in de la galerie de photos WEB-WORDPRESS avant 1.5.46 - Vulnérabilité de script inter-site via le champ image_alt_text_ (CVE-2020-9335)
999648	CVE-2020-9335	Plug-in WEB-WORDPRESS Photo Gallery antérieur à 1.5.46 - Vulnérabilité de script intersite via le champ de nom (CVE-2020-9335)
999649	CVE-2020-9335	Plug-in WEB-WORDPRESS Photo Gallery avant 1.5.46 - Vulnérabilité de script intersite via les champs de description (CVE-2020-9335)
999650	CVE-2020-10189	WEB-MISC Zoho ManageEngine Desktop Central avant 10.0.479 - Exécution de code à distance non authentifié Vuln (CVE-2020-10189)
999651	CVE-2020-10189	WEB-MISC Zoho ManageEngine Desktop Central antérieur à 10.0.479 - Téléchargement de fichier arbitraire non authentifié Vuln (CVE-2020-10189)

Règle de signature	ID CVE	Description
999652		WEB-WORDPRESS Champs de retrait flexibles pour le plug-in WooCommerce antérieur à 2.3.2 - Modification des paramètres non authentifiés Vuln
999653	CVE-2020-0688	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance de clé de validation (CVE-2020-0688)
999654	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Vulnérabilité d'exécution de code à distance via le paramètre ip_src (CVE-2020-8947, CVE-2019-20224)
999655	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Vulnérabilité d'exécution de code à distance via le paramètre dst_port (CVE-2020-8947, CVE-2019-20224)
999656	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Vulnérabilité d'exécution de code à distance via le paramètre src_port (CVE-2020-8947, CVE-2019-20224)
999657	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Vulnérabilité d'exécution de code à distance via le paramètre ip_dst (CVE-2020-8947, CVE-2019-20224)

Règle de signature	ID CVE	Description
999658	CVE-2020-5186	WEB-MISC DNN jusqu'à 9.5.0 - Vulnérabilité de script intersite via le téléchargement XML du journal (CVE-2020-5186)
999659		WEB-WORDPRESS WP Sitemap Page plug-in 1.6.2 et antérieur - Vulnérabilité de script inter-site via wsp_exclude_pages
999660	CVE-2020-5188	WEB-MISC DNN jusqu'à 9.5.0 - Vulnérabilité des autorisations non sécurisées via UploadFromURL (CVE-2020-5188)
999661	CVE-2020-5188	WEB-MISC DNN jusqu'à 9.5.0 - Vulnérabilité des autorisations non sécurisées via UploadFromLocal (CVE-2020-5188)
999662	CVE-2020-7799	WEB-MISC FusionAuth avant 1.11.0 - Vulnérabilité d'exécution de code à distance via le thème API (CVE-2020-7799)
999663	CVE-2020-7799	WEB-MISC FusionAuth antérieure à 1.11.0 - Vulnérabilité d'exécution de code à distance via un modèle d'e-mail API (CVE-2020-7799)
999664	CVE-2020-7799	WEB-MISC FusionAuth avant 1.11.0 - Vulnérabilité d'exécution de code à distance via le thème GUI (CVE-2020-7799)

Règle de signature	ID CVE	Description
999665	CVE-2020-7799	WEB-MISC FusionAuth antérieure à 1.11.0 - Vulnérabilité d'exécution de code à distance via un modèle d'e-mail d'interface graphique (CVE-2020-7799)

Mise à jour de la signature pour juin 2020

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-06-12. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 47 applicable pour NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque :**
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999580	CVE-2020-6010	Plug-in WEB-WORDPRESS LearnPress LMS antérieur à 3.2.6.9 - Vulnérabilité dans l'injection SQL (CVE-2020-6010)

Règle de signature	ID CVE	Description
999581		WEB-MISC Nagios XI jusqu'à 5.6.13 - Vulnérabilité d'exécution de commande arbitraire de service Commande_Test
999582	CVE-2020-0932	Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance dans le balisage de source WebPart via SOAP 1.2 (CVE-2020-0932)
999583	CVE-2020-0932	Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance dans le balisage de source WebPart via SOAP 1.1 (CVE-2020-0932)
999584	CVE-2020-12642	WEB-WORDPRESS Plug-in Ninja Forms antérieur à 3.4.24.2 - Vulnérabilité de falsification de requête inter-site via des champs d'importation (CVE-2020-12642)
999585	CVE-2020-12642	WEB-WORDPRESS Plug-in Ninja Forms antérieur à 3.4.24.2 - Vulnérabilité de falsification de requête intersite via un formulaire d'importation (CVE-2020-12642)
999586	CVE-2020-11450	WEB-MISC Microstrategy Web 10.4 - Vulnérabilité de divulgation d'informations (CVE-2020-11450)

Règle de signature	ID CVE	Description
999587	CVE-2020-7935	WEB-MISC Artica Pandora FMS 7.0 - Le téléchargement sans restriction de fichier présentant une vulnérabilité de type dangereux permet RCE (CVE-2020-7935)
999588	CVE-2020-12116	WEB-MISC Zoho ManageEngine OpManager avant la construction 125125 - Vulnérabilité de divulgation d'informations (CVE-2020-12116)
999589		WEB-WORDPRESS Elementor Page Builder antérieur à la version 2.9.6 - Vulnérabilité d'escalade de privilèges
999590	CVE-2020-11738	WEB-WORDPRESS - Plug-in Duplicator Snap Creek antérieur à 1.3.28 - Vulnérabilité de traversée de chemin (CVE-2020-11738)
999591	CVE-2020-10389	WEB-MISC Chadha PHPKB Standard Multi-Language 9 - Vulnérabilité d'exécution de code à distance (CVE-2020-10389)
999592	CVE-2020-11516	Plug-in Datepicker Formulaire de contact WEB-WORDPRESS 7 jusqu'à 2.6.0 - Vulnérabilité de script intersite stockée (CVE-2020-11516)
999593		WEB-MISC Nagios XI jusqu'à 5.6.13 - Vulnérabilité d'exécution de commande arbitraire Export-RRD via étape

Règle de signature	ID CVE	Description
999594		WEB-MISC Nagios XI jusqu'à 5.6.13 - Vulnérabilité d'exécution de commande arbitraire Export-RRD via End
999595		WEB-MISC Nagios XI jusqu'à 5.6.13 - Vulnérabilité d'exécution de commande arbitraire dans Export-RRD via le démarrage
999596	CVE-2019-19799	Zoho ManageEngine Applications Manager précédent à 14600 - Vulnérabilité de divulgation d'informations (CVE-2019-19799)
999597	CVE-2020-10458	WEB-MISC Chadha PHPKB Standard Multi-Language 9 - Vulnérabilité de suppression arbitraire de dossiers (CVE-2020-10458)
999598	CVE-2017-9822	WEB-MISC DNN avant 9.1.1 - Vulnérabilité d'exécution de code à distance via le cookie de personnalisation DNNN (CVE-2017-9822)
999599	CVE-2020-7953	WEB-MISC OpServices OPMon 9.3.2 - Vulnérabilité de divulgation d'informations non authentifiées via nmap_options Param (CVE-2020-7953)
999600	CVE-2020-7953	WEB-MISC OpServices OpMon 9.3.2 - Vulnérabilité de divulgation d'informations non authentifiées via l'hôte Param (CVE-2020-7953)

Règle de signature	ID CVE	Description
999601		WEB-MISC Bolt CMS 3.7.0 - Renommer le fichier en une vulnérabilité de type dangereux via le paramètre newname
999602		WEB-MISC Bolt CMS 3.7.0 - Vulnérabilité de traversée de chemin via le paramètre newname
999603		WEB-MISC Bolt CMS 3.7.0 - Vulnérabilité de traversée de chemin via un paramètre oldname
999604		WEB-MISC Bolt CMS 3.7.0 - Vulnérabilité de traversée de chemin via le paramètre parent
999605		WEB-MISC Bolt CMS 3.7.0 - Vulnérabilité de validation de champ incorrecte dans le paramètre displayname
999606	CVE-2020-9004	WEB-MISC - Wowza Streaming Engine 4.7.8 - Vulnérabilité d'autorisation incorrecte dans les journaux de vue (CVE-2020-9004)
999607	CVE-2020-9004	WEB-MISC - Wowza Streaming Engine 4.7.8 - Vulnérabilité d'autorisation incorrecte dans les paramètres du cache des médias (CVE-2020-9004)
999608	CVE-2020-9004	WEB-MISC - Wowza Streaming Engine 4.7.8 - Vulnérabilité d'autorisation incorrecte dans les paramètres des applications (CVE-2020-9004)

Règle de signature	ID CVE	Description
999609	CVE-2020-9004	WEB-MISC - Wowza Streaming Engine 4.7.8 - Vulnérabilité d'autorisation incorrecte dans les paramètres du serveur (CVE-2020-9004)
999610		WEB-MISC PrestaShop 1.7.6.5 - Vulnérabilité CSRF via Filemanager
999611	CVE-2020-10238	WEB-MISC Joomla! Précédent à 3.9.16 - Vulnérabilité de contournement de sécurité via com_templates (CVE-2020-10238)
999612	CVE-2020-11510	WEB-WORDPRESS LearnPress Plug-in LMS antérieur à 3.2.6.9 - Escalade des privilèges via learnpress_create_page (CVE-2020-11510)
999613	CVE-2020-11510	WEB-WORDPRESS LearnPress Plug-in LMS antérieur à 3.2.6.9 - Escalade des privilèges via learn-press_update_order_status (CVE-2020-11510)
999614	CVE-2020-8636	WEB-MISC OpServices OPMon 9.3.2 - Vulnérabilité d'exécution de code à distance non authentifiée via le paramètre nmap_options (CVE-2020-8636)

Règle de signature	ID CVE	Description
999615	CVE-2020-8636	WEB-MISC OpServices OPMon 9.3.2 - Vulnérabilité d'exécution de code à distance non authentifiée via un paramètre hôte (CVE-2020-8636)
999616	CVE-2020-11511	WEB-WORDPRESS LearnPress Plug-in LMS Avant 3.2.6.9 - Escalade des privilèges via accept-to-be teacher (CVE-2020-11511)
999617	CVE-2020-11451	WEB-MISC Microstrategy Web - Vulnérabilité de chargement de type de fichier non sécurisé via JSP (CVE-2020-11451)
999618	CVE-2020-11451	WEB-MISC Microstrategy Web - Vulnérabilité de chargement de type de fichier non sécurisé via ASP (CVE-2020-11451)
999619	CVE-2020-11515	WEB-WORDPRESS WP SEO Plug-in Rank Math avant 1.0.41 - Vulnérabilité de redirection via l'API REST via l'URL (CVE-2020-11515)
999620	CVE-2020-11515	WEB-WORDPRESS WP SEO Plug-in Rank Math avant 1.0.41 - Vulnérabilité de redirection via l'API REST rest_route Param (CVE-2020-11515)

Règle de signature	ID CVE	Description
999621	CVE-2020-10457	WEB-MISC Chadha PHPKB Standard Multi-Language 9 - Vulnérabilité de changement de nom de fichier arbitraire via IMGName (CVE-2020-10457)
999622	CVE-2020-10457	WEB-MISC Chadha PHPKB Standard Multi-Language 9 - Vulnérabilité de changement de nom de fichier arbitraire via ImGurl (CVE-2020-10457)
999623	CVE-2019-1821	WEB-MISC Cisco Prime Infrastructure - Vulnérabilité d'exécution de code à distance (CVE-2019-1821)
999624		Plug-in WEB-WORDPRESS Page Builder antérieur à 2.10.16 - Vulnérabilité CSRF via Ajax action_builder_content
999625		Plug-in WEB-WORDPRESS Page Builder antérieur à 2.10.16 - Vulnérabilité CSRF via Live Editor
999626	CVE-2020-11514	WEB-WORDPRESS WP SEO Plug-in Rank Math avant 1.0.41 - Escalade de privilèges via l'API REST via URL (CVE-2020-11514)
999627	CVE-2020-11514	WEB-WORDPRESS WP SEO Plug-in Rang Math avant 1.0.41 - Escalade de privilèges via l'API REST rest_route Param (CVE-2020-11514)

Règle de signature	ID CVE	Description
999628	CVE-2019-6713	WEB-MISC ThinkCMF antérieur à 5.0.190312 - Vulnérabilité d'injection de code via /route/editpost.html (CVE-2019-6713)
999629	CVE-2019-6713	WEB-MISC ThinkCMF antérieur à 5.0.190312 - Vulnérabilité d'injection de code via /route/addpost.html (CVE-2019-6713)
999630		WEB-WORDPRESS plug-in Google Site Kit avant la version 1.8.0 - Vulnérabilité de vérification non protégée
999631	CVE-2020-9315	WEB-MISC Oracle iPlanet Web Server 7.0.x - Vulnérabilité de contrôle d'accès incorrecte (CVE-2020-9315)
999632	CVE-2020-1947	WEB-MISC Apache ShardingSphere 4.0.0-RC3 et 4.0.0 - Vulnérabilité d'exécution de code à distance dans SnakeYaml (CVE-2020-1947)
999633	CVE-2020-7961	Liferay Portal antérieur à 7.2.1 CE GA2 - Vulnérabilité RCE de désérialisation dans JSONWS via JSON-RPC (CVE-2020-7961)
999634	CVE-2020-7961	Liferay Portal antérieur à 7.2.1 CE GA2 - Vulnérabilité RCE de désérialisation dans JSONWS via le chemin d'URL (CVE-2020-7961)

Règle de signature	ID CVE	Description
999635	CVE-2020-7961	Liferay Portal antérieur à 7.2.1 CE GA2 - Vulnérabilité RCE de désérialisation dans JSONWS via une requête de formulaire et d'URI (CVE-2020-7961)
999636	CVE-2020-8518	WEB-MISC Horde Groupware Webmail Edition 5.2.22 - Vulnérabilité d'exécution de code à distance (CVE-2020-8518)
999637	CVE-2020-7351	WEB-MISC Fonality Trixbox CE 2.8.0.4 et antérieures - Vulnérabilité d'exécution de code à distance (CVE-2020-7351)
999638	CVE-2020-12720	WEB-MISC vBulletin antérieur à 5.6.1 Patch Level 1 - Vulnérabilité d'injection SQL non authentifiée (CVE-2020-12720)
999639	CVE-2019-19800	Zoho ManageEngine Applications Manager précédent à 14520 - Vulnérabilité de traversée de chemin (CVE-2019-19800)
999640	CVE-2020-10386	WEB-MISC Chadha PHPKB Standard Multi-Langue 9 - Exécution de code à distance (CVE-2020-10386)
999641	CVE-2020-8497	WEB-MISC Artica Pandora FMS 7.0 - Vulnérabilité de divulgation d'informations non authentifiées (CVE-2020-8497)

Règle de signature	ID CVE	Description
999642	CVE-2020-6009	WEB-WORDPRESS LearnDash LMS Plug-in antérieur à 3.1.6 - Vulnérabilité d'injection SQL non authentifiée (CVE-2020-6009)

Mise à jour de la signature pour juillet 2020

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-07-01. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 48 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999563		WEB-WORDPRESS Page Builder Plug-in PageLayer antérieur à 1.1.2 - Vulnérabilité de script intersite via pagelayer_cf_to_email

Règle de signature	ID CVE	Description
999564		WEB-WORDPRESS Page Builder Plug-in PageLayer antérieur à 1.1.2 - Vulnérabilité de script inter-site via pagelayer-phone
999565		WEB-WORDPRESS Page Builder Plug-in PageLayer antérieur à 1.1.2 - Vulnérabilité de script intersite via pagelayer-address
999566	CVE-2020-1961	WEB-MISC Apache Syncope - Vulnérabilité d'injection de modèle côté serveur (CVE-2020-1961)
999567	CVE-2019-18935	WEB-MISC Progress Telerik UI pour ASP.NET AJAX - Vulnérabilité de désérialisation dans .NET RadaSyncupload (CVE-2019-18935)
999568	CVE-2020-9463	WEB-MISC Centreon 19.10 - Vulnérabilité liée à l'injection de commandes du système d'exploitation (CVE-2020-9463)
999569		Plug-in de révision du support WEB-WORDPRESS antérieur à 3.7.6 - Vulnérabilité de script intersite stockée non authentifiée
999570		WEB-WORDPRESS Page Builder Plug-in PageLayer avant 1.1.2 - Contrôle d'accès incorrect Vuln Via pagelayer_save_template

Règle de signature	ID CVE	Description
999571		WEB-WORDPRESS Page Builder Plug-in PageLayer antérieur à 1.1.2 - Contrôle d'accès incorrect Vuln Via pagelayer_update_site_title
999572		WEB-WORDPRESS Page Builder Plug-in PageLayer avant 1.1.2 - Contrôle d'accès incorrect Vuln Via pagelayer_save_content
999573		WEB-WORDPRESS par glisser-déposer pour le formulaire de contact 7 antérieur à 1.3.3.3 - Vulnérabilité de téléchargement d'extension de fichier arbitraire
999574	CVE-2020-9314	WEB-MISC Oracle iPlanet Web Server 7.0.x - Vulnérabilité d'injection d'image (CVE-2020-9314)
999575	CVE-2020-9484	WEB-MISC Apache Tomcat Plusieurs versions - Désérialisation des données non fiables (CVE-2020-9484)
999576	CVE-2020-13252	WEB-MISC Centreon antérieure à 19.04.15 - Vulnérabilité d'exécution de code à distance (CVE-2020-13252)
999577	CVE-2020-11453	WEB-MISC Microstrategy Web - Vulnérabilité CSRF via SOAP (CVE-2020-11453)
999578	CVE-2020-11453	WEB-MISC Microstrategy Web - Vulnérabilité CSRF (CVE-2020-11453)

Règle de signature	ID CVE	Description
999579	CVE-2020-7237	WEB-MISC Cacti antérieure à 1.2.8 - Vulnérabilité d'exécution de code à distance (CVE-2020-7237)

Mise à jour des signatures pour août 2020

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-08-26. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 49 applicable pour NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999556	CVE-2020-13241	WEB-MISC Microweber 1.1.18 - Téléchargement sans restriction de fichier présentant une vulnérabilité de type dangereux (CVE-2020-13241)

Règle de signature	ID CVE	Description
999557	CVE-2020-3250	WEB-MISC Cisco UCS Director - Vulnérabilité de traversée de chemin d'API REST via UserAPIDownloadFile (CVE-2020-3250)
999558		WEB-WORDPRESS PageBuilder KingComposer plug-in antérieur à 2.9.4 - Suppression arbitraire des répertoires Via action=bulk-delete
999559		WEB-WORDPRESS PageBuilder KingComposer Plug-in antérieur à 2.9.4 - Vulnérabilité d'exécution de code à distance via action=upload
999560	CVE-2018-1999024	WEB-MISC Moodle - Vulnérabilité de script multisite dans MathJax dans Unicode (CVE-2018-1999024)
999561	CVE-2020-13693	Plug-in WEB-WORDPRESS BBPress antérieur à 2.6.5 - Vulnérabilité d'escalade de privilèges non authentifiée (CVE-2020-13693)
999562	CVE-2020-12847	Cellules Pydio WEB-MISC antérieures à 2.0.7 - Vulnérabilité d'exécution de code à distance (CVE-2020-12847)

Mise à jour des signatures pour septembre 2020

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-09-26. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 50 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999532	CVE-2020-1956	WEB-MISC Apache Kylin - Cube Migrer l'exécution de code à distance via dest-config (CVE-2020-1956)
999533	CVE-2020-1956	WEB-MISC Apache Kylin - Cube Migrer l'exécution de code à distance via src-config (CVE-2020-1956)
999534	CVE-2020-1956	WEB-MISC Apache Kylin - Cube Migrer l'exécution de code à distance via ProjectName (CVE-2020-1956)
999535	CVE-2020-3247	WEB-MISC Cisco UCS Director - Vulnérabilité de création de liens symboliques arbitraires dans CopyFileRunnable (CVE-2020-3247)

Règle de signature	ID CVE	Description
999536	CVE-2019-16872	WEB-MISC Portainer avant 1.22.1 - Vulnérabilité de contrôle d'accès incorrecte via des piles de mise à jour (CVE-2019-16872)
999537	CVE-2019-16872	WEB-MISC Portainer avant 1.22.1 - Vulnérabilité de contrôle d'accès incorrecte via Create Stacks (CVE-2019-16872)
999538	CVE-2020-13855	WEB-MISC Artica Pandora FMS 7.44 - Vulnérabilité de téléchargement de fichiers arbitraire via le gestionnaire de référentiel de fichiers (CVE-2020-13855)
999539	CVE-2020-5902	WEB-MISC F5 BIG-IP - Vulnérabilité RCE dans l'interface utilisateur de gestion du trafic via /hsqldb (CVE-2020-5902)
999540	CVE-2020-5902	WEB-MISC F5 BIG-IP - Vulnérabilité RCE dans l'interface utilisateur de gestion du trafic via /tmui (CVE-2020-5902)
999541		WEB-MISC WebERP 4.15.1 et antérieures - Vulnérabilité de divulgation d'informations non authentifiées
999542	CVE-2020-7209	WEB-MISC HP Linuxki antérieur à 6.0-2 - Vulnérabilité RCE non authentifiée via timeline.php et horodatage Param (CVE-2020-7209)

Règle de signature	ID CVE	Description
999543	CVE-2020-7209	WEB-MISC HP Linuxki antérieur à 6.0-2 - Vulnérabilité RCE non authentifiée via kivis.php et ts Param (CVE-2020-7209)
999544	CVE-2020-7209	WEB-MISC HP Linuxki antérieur à 6.0-2 - Vulnérabilité RCE non authentifiée via kivis.php et end Param (CVE-2020-7209)
999545	CVE-2020-7209	WEB-MISC HP LinuXki antérieur à 6.0-2 - Vulnérabilité RCE non authentifiée via kivis.php et démarrage de Param (CVE-2020-7209)
999546	CVE-2020-7209	WEB-MISC HP LinuXki antérieur à 6.0-2 - Vulnérabilité RCE non authentifiée via kivis.php et pid Param (CVE-2020-7209)
999547	CVE-2020-7209	WEB-MISC HP Linuxki antérieur à 6.0-2 - Vulnérabilité RCE non authentifiée via kidsk_trace_view.php et end Param (CVE-2020-7209)
999548	CVE-2020-7209	WEB-MISC HP LinuXki antérieur à 6.0-2 - Vulnérabilité RCE non authentifiée via kidsk_trace_view.php et démarrage de Param (CVE-2020-7209)

Règle de signature	ID CVE	Description
999549		WEB-MISC PHP-Fusion antérieure à 9.03.70 - Vulnérabilité dans l'injection d'objet PHP
999550	CVE-2020-1181	WEB-MISC Microsoft SharePoint Server - Exécution de code à distance via des composants WebPart (CVE-2020-1181)
999551	CVE-2020-10547	WEB-MISC RConfig antérieur à 3.9.5 - Vulnérabilité SQLi non authentifiée dans les éléments de stratégie via SearchColumn (CVE-2020-10547)
999552	CVE-2020-10547	WEB-MISC RConfig antérieures à 3.9.5 - Vulnérabilité SQLi non authentifiée dans les éléments de stratégie via SearchField (CVE-2020-10547)
999553	CVE-2020-8605	WEB-MISC Trend Micro InterScan Web Security Virtual Appliance virtuelle antérieure au correctif 4 SP2 6.5 - Vulnérabilité RCE (CVE-2020-8605)
999554	CVE-2019-10068	WEB-MISC Kentico CMS plusieurs versions - Vulnérabilité d'exécution de code à distance non authentifiée (CVE-2019-10068)

Règle de signature	ID CVE	Description
999555	CVE-2020-11108	WEB-MISC PI-hole jusqu'à 4.4 - Vulnérabilité RCE authentifiée (CVE-2020-11108)

Mise à jour des signatures pour octobre 2020

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-10-13. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 51 applicable pour NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999505		WEB-WORDPRESS plug-in WordPress wpDiscuz 7.0.0 Jusqu'à 7.0.4 - Vulnérabilité de téléchargement de fichier arbitraire non authentifié
999506		WEB-WORDPRESS Quiz & Survey Master - Vulnérabilité de script inter-site dans la fonction Questions

Règle de signature	ID CVE	Description
999507	CVE-2020-8604	WEB-MISC Trend Micro IWS VA avant 6.5 SP2 Patch 4 - Path Traversal Vuln Via /log_search and cf Param (CVE-2020-8604)
999508	CVE-2020-8604	WEB-MISC Trend Micro IWS VA avant 6.5 SP2 Patch 4 - Path Traversal Vuln Via /collection and cf Param (CVE-2020-8604)
999509	CVE-2020-8604	WEB-MISC Trend Micro IWS VA avant 6.5 SP2 Patch 4 - Path Traversal Vuln Via /log_search and File Param (CVE-2020-8604)
999510	CVE-2020-8604	WEB-MISC Trend Micro IWS VA avant 6.5 SP2 Patch 4 - Path Traversal Vuln Via /collection and File Param (CVE-2020-8604)
999511	CVE-2020-7361	WEB-MISC Zentao Enterprise 8.8.3 et antérieures - Vulnérabilité d’exécution de code à distance via Repo-Edit (CVE-2020-7361)
999512	CVE-2020-7361	WEB-MISC Zentao Pro 8.8.3 et antérieures - Vulnérabilité d’exécution de code à distance via Repo-Edit (CVE-2020-7361)
999513	CVE-2020-7361	WEB-MISC Zentao Enterprise 8.8.3 et antérieures - Vulnérabilité d’exécution de code à distance via Repo-Create (CVE-2020-7361)

Règle de signature	ID CVE	Description
999514	CVE-2020-7361	WEB-MISC Zentao Pro 8.8.3 et antérieures - Vulnérabilité d'exécution de code à distance via Repo-Create (CVE-2020-7361)
999515	CVE-2020-5768	WEB-WORDPRESS Icegram Email Abonnés & Newsletter Plug-in antérieur à 4.5.1 - Vulnérabilité d'injection SQL (CVE-2020-5768)
999516	CVE-2020-5767	WEB-WORDPRESS Icegram Email Abonnés & Newsletter Plug-in avant 4.5.1 - Vulnérabilité CSRF (CVE-2020-5767)
999517	CVE-2020-15299	Plug-in WEB-WORDPRESS KingComposer antérieur à 2.9.5 - Vulnérabilité de script intersite (CVE-2020-15299)
999518	CVE-2020-13854	WEB-MISC Artica Pandora FMS - Vulnérabilité d'escalade de privilèges (CVE-2020-13854)
999519	CVE-2020-13852	WEB-MISC Artica Pandora FMS - Vulnérabilité de téléchargement de fichiers arbitraire via le gestionnaire de fichiers (CVE-2020-13852)
999520	CVE-2020-13700	WEB-WORDPRESS plug-in WordPress acf-to-rest-api Before 3.3.0 - Vulnérabilité de divulgation d'informations via URI (CVE-2020-13700)

Règle de signature	ID CVE	Description
999521	CVE-2020-13700	WEB-WORDPRESS plug-in WordPress acf-to-rest-api avant 3.3.0 - Vulnérabilité de divulgation d'informations via URL (CVE-2020-13700)
999522	CVE-2020-13379	WEB-MISC Grafana 3.0.1 à 7.0.1 - Contournement CSRF menant à une vulnérabilité DOS (CVE-2020-13379)
999523	CVE-2020-12851	Cellules Pydio WEB-MISC antérieures à 2.0.7 - Vulnérabilité d'écriture de fichier arbitraire (CVE-2020-12851)
999524	CVE-2020-12848	Cellules Pydio WEB-MISC antérieures à 2.0.7 - Vulnérabilité de connexion en tant qu'utilisateur partagé temporaire (CVE-2020-12848)
999525	CVE-2020-11749	WEB-MISC Artica Pandora FMS antérieur à 7.47 - Vulnérabilité de script intersite via le navigateur SNMP (CVE-2020-11749)
999526	CVE-2020-11579	WEB-MISC PHPKBV9 - Vulnérabilité d'exfiltration de fichiers (CVE-2020-11579)
999527	CVE-2020-10546	WEB-MISC RConfig antérieures à 3.9.5 - Vulnérabilité SQLi non authentifiée dans les stratégies de conformité via SearchColumn (CVE-2020-10546)

Règle de signature	ID CVE	Description
999528	CVE-2020-10546	WEB-MISC RConfig antérieures à 3.9.5 - Vulnérabilité SQLi non authentifiée dans les stratégies de conformité via SearchField (CVE-2020-10546)
999529	CVE-2019-16876	WEB-MISC Portainer avant 1.22.1 - Vulnérabilité de traversée d'annuaire (CVE-2019-16876)
999530		WEB-WORDPRESS - Plug-in AdNing antérieur à 1.5.6 - Vulnérabilité de suppression de fichier arbitraire non authentifiée
999531		WEB-WORDPRESS - Plug-in AdNing antérieur à 1.5.6 - Vulnérabilité de téléchargement de fichier arbitraire non authentifié

Mise à jour de la signature pour octobre 2020

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-10-29. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 52 applicable pour NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC. En outre, les versions vulnérables sont mentionnées dans certaines chaînes de journal des règles de signature. Vous devez l'activer en conséquence.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999500	CVE-2018-14667	WEB-MISC RichFaces Framework 3.X à 3.3.4 - Injection EL via UserResource (CVE-2018-14667)
999501	CVE-2018-12533	WEB-MISC RichFaces Framework 3.1.0 à 3.3.4 - Injection EL via Paint2DResource (CVE-2018-12533)
999502	CVE-2015-0279, CVE-2018-12532	WEB-MISC RichFaces Framework 4.X à 4.5.17 - Injection EL via MediaOutputResource (CVE-2015-0279, CVE-2018-12532)
999503	CVE-2013-2165	WEB-MISC RichFaces v4 antérieure à 4.3.3 - Vulnérabilité de désérialisation d'objet Java (CVE-2013-2165)
999504	CVE-2013-2165	WEB-MISC RichFaces v3 antérieure à 3.3.4 - Vulnérabilité de désérialisation d'objet Java (CVE-2013-2165)

Mise à jour des signatures pour novembre 2020

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-11-10. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 53 applicable pour NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque**
>
> L'activation des règles de signature du corps de poste et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999411		WEB-WORDPRESS plug-in WordPress wpDiscuz 7.0.0 Jusqu'à 7.0.4 - Vulnérabilité de téléchargement de fichier arbitraire non authentifié
999412		WEB-WORDPRESS Quiz & Survey Master - Vulnérabilité de script inter-site dans la fonction Questions
999413		WEB-WORDPRESS Plug-in WordPress Gestionnaire de fichiers antérieur à 6.9 - Vulnérabilité d'exécution de commandes ELFinder non authentifiées

Règle de signature	ID CVE	Description
999414	CVE-2020-11700	WEB-MISC Titan SpamTitan antérieur à 7.08 - Vulnérabilité de divulgation d'informations (CVE-2020-11700)
999415	CVE-2020-9446	WEB-MISC Apache OfBiz 17.12.03 - Vulnérabilité de désérialisation non sécurisée dans XML-RPC (CVE-2020-9446)
999416	CVE-2020-9446	WEB-MISC Apache OfBiz 17.12.03 - Vulnérabilité de script intersite XML-RPC (CVE-2020-9446)
999417	CVE-2020-9047	WEB-MISC ExacqVision Web Service jusqu'à 20.06.3.0 - Vulnérabilité dans l'injection de commandes du système d'exploitation (CVE-2020-9047)
999418	CVE-2020-8866	WEB-MISC Horde Groupware Webmail Edition 5.2.22 - Vulnérabilité liée au chargement sans restriction de fichier via edit.php (CVE-2020-8866)
999419	CVE-2020-8866	WEB-MISC Horde Groupware Webmail Edition 5.2.22 - Vulnérabilité liée au chargement sans restriction de fichier via add.php (CVE-2020-8866)
999420	CVE-2020-8865	WEB-MISC Horde Groupware Webmail Edition 5.2.22 - Vulnérabilité d'inclusion de fichier arbitraire via edit.php (CVE-2020-8865)

Règle de signature	ID CVE	Description
999421	CVE-2020-8816	WEB-MISC PI-hole avant 4.3.2 - Vulnérabilité d'exécution de code à distance via removestatic (CVE-2020-8816)
999422	CVE-2020-8816	WEB-MISC PI-hole antérieure à 4.3.2 - Vulnérabilité d'exécution de code à distance via AddMac (CVE-2020-8816)
999423	CVE-2020-8243	WEB-MISC Pulse Connect sécurisé avant 9.1R8.2 - Vulnérabilité d'exécution de code à distance (CVE-2020-8243)
999424	CVE-2020-8218	WEB-MISC Pulse Connect sécurisé avant 9.1R8 - Vulnérabilité d'exécution de code à distance (CVE-2020-8218)
999425	CVE-2020-6143, CVE-2020-6144	WEB-MISC OS4ED OpenSIS - Vulnérabilité d'injection de code via /install/Ins1.php (CVE-2020-6143, CVE-2020-6144)
999426	CVE-2020-6142	WEB-MISC OS4ed OpenSIS - Vulnérabilité de traversée de chemin via modname (CVE-2020-6142)
999427	CVE-2020-6141	WEB-MISC OS4ed OpenSIS antérieur à 7.4 - Vulnérabilité SQLi non authentifiée via USERNAME (CVE-2020-6141)

Règle de signature	ID CVE	Description
999428	CVE-2020-6140	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi non authentifiée via username_stn_id (CVE-2020-6140)
999429	CVE-2020-6139	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi non authentifiée via username_stf_email (CVE-2020-6139)
999430	CVE-2020-6138	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi non authentifiée via uname (CVE-2020-6138)
999431	CVE-2020-6137	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi non authentifiée via password_stf_email (CVE-2020-6137)
999432	CVE-2020-6125	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via GetSchool.php et paramètre u (CVE-2020-6125)
999433	CVE-2020-6124	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via EmailCheckOthers.php (CVE-2020-6124)
999434	CVE-2020-6123	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via EmailCheck.php et paramètre p_id (CVE-2020-6123)

Règle de signature	ID CVE	Description
999435	CVE-2020-6123	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via EmailCheck.php et paramètre e-mail (CVE-2020-6123)
999436	CVE-2020-6122	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via les paramètres CheckDuplicateStudent.php et mn (CVE-2020-6122)
999437	CVE-2020-6121	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via CheckDuplicateStudent.php et paramètre ln (CVE-2020-6121)
999438	CVE-2020-6120	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via les paramètres CheckDuplicateStudent.php et fn (CVE-2020-6120)
999439	CVE-2020-6119	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via CheckDuplicateStudent.php et paramètre byear (CVE-2020-6119)
999440	CVE-2020-6118	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via CheckDuplicateStudent.php et paramètre bmonth (CVE-2020-6118)

Règle de signature	ID CVE	Description
999441	CVE-2020-6117	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via CheckDuplicateStudent.php et paramètre bday (CVE-2020-6117)
999442	CVE-2020-5780	WEB-WORDPRESS plug-in WordPress E-mail Abonnés et Newsletter avant 4.5.6 - Vulnérabilité de falsification de courrier électronique (CVE-2020-5780)
999443	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation Java non sécurisée via JSON-RPC (CVE-2020-4280)
999444	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation Java non sécurisée via RemoteMethod (CVE-2020-4280)
999445	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation Java non sécurisée via RemoteJavaScript (CVE-2020-4280)
999446	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation Java non sécurisée via JSON-RPC (CVE-2020-4280)

Règle de signature	ID CVE	Description
999447	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation Java non sécurisée via RemoteMethod (CVE-2020-4280)
999448	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation Java non sécurisée via RemoteJavaScript (CVE-2020-4280)
999449	CVE-2020-24786	WEB-MISC Zoho ManageEngine AdManager Plus 7.0 avant la construction 55 - Vulnérabilité d'authentification incorrecte (CVE-2020-24786)
999450	CVE-2020-24389	WEB-WORDPRESS Plug-in de téléchargement de fichiers multiples par glisser-déposer avant 1.3.5.5 - Vulnérabilité de contournement de sécurité (CVE-2020-24389)
999451	CVE-2020-24046	WEB-MISC TitanHQ SpamTitan Gateway 7.08 - Vulnérabilité d'escalade de privilèges (CVE-2020-24046)
999452	CVE-2020-17506	WEB-MISC Artica Web Proxy 4.30.000000 - Vulnérabilité d'injection SQL dans PreAuth via le paramètre Apikey (CVE-2020-17506)

Règle de signature	ID CVE	Description
999453	CVE-2020-17505	WEB-MISC Artica Web Proxy 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via le paramètre Service-CMDS-Peform (CVE-2020-17505)
999454	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /fuel/users/items (CVE-2020-17463)
999455	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /fuel/sitevariables/items (CVE-2020-17463)
999456	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /carburant/permission-s/items (CVE-2020-17463)
999457	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /fuel/pages/items (CVE-2020-17463)
999458	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /carburant/navigation/items (CVE-2020-17463)
999459	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /fuel/logs/items (CVE-2020-17463)
999460	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /carburant/blocs/items (CVE-2020-17463)

Règle de signature	ID CVE	Description
999461	CVE-2020-16875	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance dans la stratégie DLP (CVE-2020-16875)
999462	CVE-2020-16171	WEB-MISC Acronis Cyber Backup antérieure à 12.5 Build 16342 - Vulnérabilité d'en-tête SSRF via Shard (CVE-2020-16171)
999463	CVE-2020-14947	Inventaire OCS WEB-MISC antérieur à 2.8 - Vulnérabilité d'injection de commande du système d'exploitation via SNMP_MIB_DIRECTORY (CVE-2020-14947)
999464	CVE-2020-14947	Inventaire OCS WEB-MISC antérieur à 2.8 - Vulnérabilité dans l'injection de commandes du système d'exploitation via mib_file (CVE-2020-14947)
999465	CVE-2020-14008	WEB-MISC Zoho ManageEngine Applications Manager jusqu'à 14710 - Vulnérabilité d'exécution de code à distance (CVE-2020-14008)
999466	CVE-2020-13925	WEB-MISC Apache Kylin avant 3.1.0 - Vulnérabilité d'exécution de code à distance via le travail (CVE-2020-13925)

Règle de signature	ID CVE	Description
999467	CVE-2020-13925	WEB-MISC Apache Kylin avant 3.1.0 - Vulnérabilité d'exécution de code à distance via un projet (CVE-2020-13925)
999468	CVE-2020-13854	WEB-MISC Artica Pandora FMS - Vulnérabilité d'escalade de privilèges (CVE-2020-13854)
999469	CVE-2020-13405	WEB-MISC Microweber avant 1.1.20 - Vulnérabilité de divulgation d'informations non authentifiées (CVE-2020-13405)
999470	CVE-2020-13376	WEB-MISC SecurEnvoy SecurMail 9.3.503 - Vulnérabilité de traversée du chemin de cookie dans SecurEnvoyReply (CVE-2020-13376)
999471	CVE-2020-13159	WEB-MISC Artica Web Proxy antérieur à 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via le domaine (CVE-2020-13159)
999472	CVE-2020-13159	WEB-MISC Artica Web Proxy antérieur à 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via netbiosname (CVE-2020-13159)

Règle de signature	ID CVE	Description
999473	CVE-2020-13159	WEB-MISC Artica Web Proxy antérieur à 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via un alias (CVE-2020-13159)
999474	CVE-2020-13159	WEB-MISC Artica Web Proxy antérieur à 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via le nom d'hôte (CVE-2020-13159)
999475	CVE-2020-13159	WEB-MISC Artica Web Proxy antérieur à 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via dhclient_server (CVE-2020-13159)
999476	CVE-2020-13159	WEB-MISC Artica Web Proxy antérieur à 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via dhclient_interface (CVE-2020-13159)
999477	CVE-2020-13159	WEB-MISC Artica Web Proxy antérieur à 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via dhclient_mac (CVE-2020-13159)

Règle de signature	ID CVE	Description
999478	CVE-2020-13158	WEB-MISC Artica Web Proxy antérieur à 4.30.000000 - Vulnérabilité de traversée de chemin via une fenêtre contextuelle (CVE-2020-13158)
999479	CVE-2020-12851	Cellules Pydio WEB-MISC antérieures à 2.0.7 - Vulnérabilité d'écriture de fichier arbitraire (CVE-2020-12851)
999480	CVE-2020-12848	Cellules Pydio WEB-MISC antérieures à 2.0.7 - Vulnérabilité de connexion en tant qu'utilisateur partagé temporaire (CVE-2020-12848)
999481	CVE-2020-11699	WEB-MISC Titan SpamTitan antérieur à 7.08 - Vulnérabilité d'exécution de code à distance (CVE-2020-11699)
999482	CVE-2020-11579	WEB-MISC PHPKBV9 - Vulnérabilité d'exfiltration de fichiers (CVE-2020-11579)
999483	CVE-2020-10818	WEB-MISC Artica Web Proxy 4.26 - Vulnérabilité d'injection de commande du système d'exploitation via fw.system.info.php (CVE-2020-10818)
999484	CVE-2020-10228	WEB-MISC Vtenext CE antérieure à la version 20 - Téléchargement sans restriction de fichier présentant une vulnérabilité de type dangereux (CVE-2020-10228)

Règle de signature	ID CVE	Description
999485	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager antérieur à 3.21.2 - Vulnérabilité RCE via les rôles CoreUI_User (CVE-2020-10204)
999486	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager antérieur à 3.21.2 - Vulnérabilité RCE via les privilèges CoreUI_Role (CVE-2020-10204)
999487	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager antérieur à 3.21.2 - Vulnérabilité RCE via les rôles CoreUI_Role (CVE-2020-10204)
999488	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager antérieur à 3.21.2 - Vulnérabilité RCE via REST Endpoint /bower/group (CVE-2020-10199)
999489	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager antérieur à 3.21.2 - Vulnérabilité RCE via REST Endpoint /go/group (CVE-2020-10199)
999490	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager antérieur à 3.21.2 - Vulnérabilité RCE via REST Endpoint /docker/group (CVE-2020-10199)
999491	CVE-2019-19699	WEB-MISC Centreon jusqu'à 19.10 - Vulnérabilité d'exécution de code à distance (CVE-2019-19699)

Règle de signature	ID CVE	Description
999492	CVE-2019-19499	WEB-MISC Apache Grafana jusqu'à 6.4.3 - Vulnérabilité de lecture de fichier arbitraire (CVE-2019-19499)
999493	CVE-2019-18394	WEB-MISC Ignite Realtime Openfire jusqu'à 4.4.2 - Vulnérabilité de falsification de requête côté serveur FaviConservlet (CVE-2019-18394)
999494	CVE-2019-18393	WEB-MISC Ignite Realtime Openfire jusqu'à 4.4.2 - Vulnérabilité de traversée d'annuaire Plug-Inservlet (CVE-2019-18393)
999495	CVE-2019-16759	WEB-MISC vBulletin antérieur à 5.6.2 - Vulnérabilité d'exécution de code à distance via un modèle imbriqué (CVE-2019-16759)
999496	CVE-2019-15715	WEB-MISC MantiSBT antérieures à 1.3.20 et 2.22.1 - Vulnérabilité d'exécution de code à distance via neato_tool (CVE-2019-15715)
999497	CVE-2019-15715	WEB-MISC MantiSBT antérieures à 1.3.20 et 2.22.1 - Vulnérabilité d'exécution de code à distance via dot_tool (CVE-2019-15715)
999498	CVE-2019-11043	WEB-MISC PHP-FPM Plusieurs versions - Une vulnérabilité d'écriture hors limites permet l'exécution de code arbitraire (CVE-2019-11043)

Règle de signature	ID CVE	Description
999499		WEB-WORDPRESS plug-in WordPress Autoptimize jusqu'à 2.7.6 - Vulnérabilité de téléchargement de fichier arbitraire authentifié

Mise à jour de la signature pour décembre 2020

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-12-02. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 54 applicable pour NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC. Dans le cadre de la mise à jour de signature version 54, la chaîne de journal pour la signature 999720 est modifiée pour s'assurer qu'elle inclut uniquement des caractères ASCI.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999394	CVE-2020-8255	WEB-MISC Pulse Connect Secure antérieure à 9.1R9 - Vulnérabilité de divulgation d'informations (CVE-2020-8255)

Règle de signature	ID CVE	Description
999395	CVE-2020-6128	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via CoursePeriodModal.php (CVE-2020-6128)
999396	CVE-2020-6126, CVE-2020-6127	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via CoursePeriodModal.php (CVE-2020-6126, CVE-2020-6127)
999397	CVE-2020-28328	WEB-MISC SuiteCRM antérieur à 7.11.16 - Vulnérabilité d'exécution de code à distance (CVE-2020-28328)
999398	CVE-2020-27995	WEB-MISC Zoho ManageEngine Applications Manager 14 avant la construction 14560 - Vulnérabilité dans l'injection SQL (CVE-2020-27995)
999399	CVE-2020-26879	WEB-MISC Ruckus VRioT Server antérieur à 1.6.0 - Vulnérabilité de contournement d'autorisation via /service/ (CVE-2020-26879)
999400	CVE-2020-26879	WEB-MISC Ruckus VRioT Server antérieur à 1.6.0 - Vulnérabilité de contournement d'autorisation via /reboot (CVE-2020-26879)

Règle de signature	ID CVE	Description
999401	CVE-2020-26879	WEB-MISC Ruckus VRioT Server antérieur à 1.6.0 - Vulnérabilité de contournement d'autorisation via /patch/ (CVE-2020-26879)
999402	CVE-2020-26879	WEB-MISC Ruckus VRioT Server antérieur à 1.6.0 - Vulnérabilité de contournement d'autorisation via /upgrade/ (CVE-2020-26879)
999403	CVE-2020-26879	WEB-MISC Ruckus VRioT Server antérieur à 1.6.0 - Vulnérabilité de contournement d'autorisation via /module/ (CVE-2020-26879)
999404	CVE-2020-26878	WEB-MISC Ruckus VRioT Server antérieur à 1.6.0 - Vulnérabilité dans l'injection de commandes du système d'exploitation arbitraire (CVE-2020-26878)
999405	CVE-2020-25790	WEB-MISC Typesetter CMS 5.x à 5.1 - Vulnérabilité de chargement de fichiers non sécurisés (CVE-2020-25790)
999406	CVE-2020-25540	WEB-MISC ThinkAdmin v6 - Vulnérabilité de traversée d'annuaire (CVE-2020-25540)
999407	CVE-2020-14883	WEB-MISC Oracle WebLogic Server - Vulnérabilité d'exécution de code à distance authentifiée (CVE-2020-14883)

Règle de signature	ID CVE	Description
999408	CVE-2020-14882, CVE-2020-14750	WEB-MISC Oracle WebLogic Server - Vulnérabilité de contournement d'authentification (CVE-2020-14882, CVE-2020-14750)
999409	CVE-2020-11975, CVE-2020-13942	WEB-MISC Apache Unomi avant 1.5.2 - Vulnérabilité d'exécution de code à distance (CVE-2020-11975, CVE-2020-13942)
999410	CVE-2020-11803	WEB-MISC Titan SpamTitan antérieures à 7.08 - Vulnérabilité d'exécution de code à distance (CVE-2020-11803)

Mise à jour de la signature pour décembre 2020

January 21, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-12-17. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 55 applicable pour NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999377		WEB-WORDPRESS TI WooCommerce Wishlist Plugin antérieur à 1.21.11 - Vulnérabilité de divulgation d'informations via tinvwl_export_settings
999378		WEB-WORDPRESS TI WooCommerce Wishlist Plugin avant 1.21.11 - Options WP Change Vulnérabilité via tinvwl_import_settings
999379	CVE-2020-6134	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via MassDropModal.php (CVE-2020-6134)
999380	CVE-2020-6133	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via CourseMoreInfo.php (CVE-2020-6133)
999381	CVE-2020-6132	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via ChooseCP.php (CVE-2020-6132)
999382	CVE-2020-6131	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via MassScheduleSessionSet.php (CVE-2020-6131)
999383	CVE-2020-6130	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via MassDropSessionSet.php (CVE-2020-6130)

Règle de signature	ID CVE	Description
999384	CVE-2020-6129	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via CpSessionSet.php (CVE-2020-6129)
999385	CVE-2020-35234	WEB-WORDPRES Easy WP SMTP Plugin antérieur à 1.4.4 - Vulnérabilité de divulgation d'informations (CVE-2020-35234)
999386	CVE-2020-25042	WEB-MISC Mara CMS 7.5 - Vulnérabilité de téléchargement de fichier arbitraire (CVE-2020-25042)
999387	CVE-2020-13526	WEB-MISC ProcessMaker - Vulnérabilité d'injection SQL via ClientSetupajax (CVE-2020-13526)
999388	CVE-2020-13525	WEB-MISC ProcessMaker - Vulnérabilité dans l'injection SQL via ReportTables_Ajax (CVE-2020-13525)
999389	CVE-2020-12147	WEB-MISC Silver Peak Unity Orchestrator - Vulnérabilité des requêtes MySQL arbitraires via l'API REST SQLExecution (CVE-2020-12147)
999390	CVE-2020-12146	WEB-MISC Silver Peak Unity Orchestrator - Vulnérabilité de traversée de chemin via l'API REST DebugFiles (CVE-2020-12146)

Règle de signature	ID CVE	Description
999391	CVE-2020-12145	WEB-MISC Silver Peak Unity Orchestrator - Vulnérabilité de contournement d'authentification (CVE-2020-12145)
999392	CVE-2019-8394	WEB-MISC Zoho ManageEngine ServiceDesk Plus antérieur à 10.0 Build 10012 - Vulnérabilité de téléchargement de fichiers arbitraire (CVE-2019-8394)
999393	CVE-2019-11447	WEB-MISC CutePHP CuteNews 2.1.2 - Vulnérabilité d'exécution de code à distance (CVE-2019-11447)

Mise à jour des signatures pour janvier 2021

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-01-18. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 56 applicable pour NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999366	CVE-2020-8466	WEB-MISC Trend Micro IWSSVA 6.5 SP2 avant la construction 1919 - Vulnérabilité d'injection de commandes du système d'exploitation non authentifiée (CVE-2020-8466)
999367	CVE-2020-6135	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via Validator.php (CVE-2020-6135)
999368	CVE-2020-4001	WEB-MISC VMware SD-WAN Orchestrator - Vulnérabilité de pass-the-hachage (CVE-2020-4001)
999369	CVE-2020-4000	WEB-MISC VMware SD-WAN Orchestrator - Vulnérabilité de traversée de chemin (CVE-2020-4000)
999370	CVE-2020-3984	WEB-MISC VMware SD-WAN Orchestrator - Vulnérabilité d'injection SQL via un module (CVE-2020-3984)
999371	CVE-2020-35606	WEB-MISC Webmin jusqu'à 1.962 - Vulnérabilité d'exécution de code à distance (CVE-2020-35606)
999372	CVE-2020-17143	WEB-MISC Microsoft Exchange Server - Vulnérabilité de divulgation d'informations (CVE-2020-17143)
999373	CVE-2020-17141	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance via RouteComplaint (CVE-2020-17141)

Règle de signature	ID CVE	Description
999374	CVE-2020-10816	WEB-MISC Zoho ManageEngine Applications Manager 14 avant la construction 14790 - Vulnérabilité d'authentification incorrecte (CVE-2020-10816)
999375	CVE-2019-5533	WEB-MISC VMware SD-WAN Orchestrator - Vulnérabilité de divulgation d'informations (CVE-2019-5533)
999376	CVE-2018-15961	WEB-MISC Adobe ColdFusion 12 avant la mise à jour 6 ou 14 - Vulnérabilité de téléchargement de fichier arbitraire (CVE-2018-15961)

Mise à jour des signatures pour février 2021

February 12, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-02-03. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 57 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999339		Connecteur de réunion ZOOM WEB-MISC 4.6.348.20201217 - Vulnérabilité d'exécution de code à distance via proxyPasswd
999340		Connecteur de réunion de zoom WEB-MISC 4.6.348.20201217 - Vulnérabilité d'exécution de code à distance via proxyName
999341	CVE-2021-3129	Ignition WEB-MISC antérieure à 2.5.2 - Vulnérabilité d'exécution de code à distance non authentifiée (CVE-2021-3129)
999342	CVE-2021-3025	WEB-MISC Invision Community IPS Community Suite antérieure à 4.5.4.2 - Vulnérabilité d'injection SQL via SortDir (CVE-2021-3025)
999343	CVE-2021-2109	WEB-MISC Oracle WebLogic Server - Vulnérabilité d'exécution de code à distance via injection JNDI (CVE-2021-2109)
999344	CVE-2020-7200	WEB-MISC HPE Systems Insight Manager 7.6.x - Vulnérabilité de désérialisation non sécurisée dans AMF (CVE-2020-7200)

Règle de signature	ID CVE	Description
999345	CVE-2020-7199	WEB-MISC HPE EIM antérieur à 1.21 - Vulnérabilité d'authentification incorrecte dans /Private/EIMApplianceIP (CVE-2020-7199)
999346	CVE-2020-7199	WEB-MISC HPE EIM antérieur à 1.21 - Vulnérabilité d'authentification incorrecte dans /Private/adminPassreset (CVE-2020-7199)
999347	CVE-2020-7199	WEB-MISC HPE EIM avant 1.21 - Vulnérabilité d'authentification incorrecte dans /Private/ResetAppliance (CVE-2020-7199)
999348	CVE-2020-6136	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité SQLi via DownloadWindow.php (CVE-2020-6136)
999349	CVE-2020-35729	WEB-MISC KLog Server 2.4.1 et antérieur - Vulnérabilité d'injection de commande du système d'exploitation (CVE-2020-35729)
999350	CVE-2020-35701	WEB-MISC Cacti 1.2.16 et antérieures - Vulnérabilité dans l'injection SQL via site_id (CVE-2020-35701)
999351	CVE-2020-35489	Formulaire de contact WEB-WORDPRESS 7 antérieur à 5.3.2 - Vulnérabilité de téléchargement de fichiers sans restriction (CVE-2020-35489)

Règle de signature	ID CVE	Description
999352	CVE-2020-27615	Plugin de connexion WEB-WORDPRESS antérieur à 1.6.4 - Vulnérabilité dans l'injection SQL (CVE-2020-27615)
999353	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et antérieures - Vulnérabilité XSS via /fuel/sitevariables/create (CVE-2020-26046)
999354	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et antérieures - Vulnérabilité XSS via /fuel/sitevariables/edit (CVE-2020-26046)
999355	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et antérieures - Vulnérabilité XSS via /carburant/navigation/create (CVE-2020-26046)
999356	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et antérieures - Vulnérabilité XSS via /fuel/navigation/edit (CVE-2020-26046)
999357	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et antérieures - Vulnérabilité XSS via /fuel/blocks/create (CVE-2020-26046)
999358	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et antérieures - Vulnérabilité XSS via /fuel/blocks/edit (CVE-2020-26046)
999359	CVE-2020-26045	WEB-MISC Fuel CMS 1.4.11 - Vulnérabilité dans SQLi via /fuel/permissions/create (CVE-2020-26045)

Règle de signature	ID CVE	Description
999360	CVE-2020-17519	WEB-MISC Apache Flink avant 1.11.3 - Vulnérabilité de divulgation de fichiers arbitraire (CVE-2020-17519)
999361	CVE-2020-17518	WEB-MISC Apache Flink 1.5.1 à 1.11.2 - Vulnérabilité de téléchargement de fichier d'emplacement arbitraire (CVE-2020-17518)
999362	CVE-2019-16010	WEB-MISC Cisco SD-WAN vManage antérieur à 19.2.2 - Vulnérabilité XSS stockée (CVE-2019-16010)
999363	CVE-2019-15000	WEB-MISC VMware Bitbucket Server et centre de données - Vulnérabilité d'injection de commandes Git via at (CVE-2019-15000)
999364	CVE-2019-15000	WEB-MISC VMware Bitbucket Server et centre de données - Vulnérabilité d'injection de commande Git via UNTIL/Untilid (CVE-2019-15000)
999365	CVE-2019-15000	WEB-MISC VMware Bitbucket Server et centre de données - Vulnérabilité d'injection de commande Git via Since/SinceID (CVE-2019-15000)

Mise à jour des signatures pour février 2021

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-02-17. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 58 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999328	CVE-2021-3317	WEB-MISC KLog Server 2.4.1 et antérieur - Vulnérabilité d'injection de commandes OS (CVE-2021-3317)
999329	CVE-2021-3110	WEB-MISC PrestaShop antérieur à 1.7.7.1 - Vulnérabilité par injection SQL via id_products (CVE-2021-3110)
999330	CVE-2021-3110	WEB-MISC PrestaShop antérieur à 1.7.7.1 - Vulnérabilité par injection SQL via /module/Product-Comments/CommentGrade (CVE-2021-3110)
999331	CVE-2021-25646	WEB-MISC Apache Druid antérieur à 0.20.1 - Vulnérabilité d'exécution de code à distance (CVE-2021-25646)

Règle de signature	ID CVE	Description
999332	CVE-2020-36171	Plugin WEB-WORDPRESS Elementor Page Builder antérieur à 3.0.14 - Vulnérabilité XSS (CVE-2020-36171)
999333	CVE-2020-35765	WEB-MISC Zoho ManageEngine Applications Manager avant la version 15000 - Vulnérabilité par injection SQL (CVE-2020-35765)
999334	CVE-2020-35589	Tentatives de connexion de limite WEB-WORDPRESS rechargées avant 2.15.2 - Vulnérabilité de script intersite reflétée (CVE-2020-35589)
999335	CVE-2020-26282	Proxy BrowserUp WEB-MISC antérieur à 2.1.2 - Injection de modèle entraînant une vulnérabilité RCE via MostRecentEntry (CVE-2020-26282)
999336	CVE-2020-26282	Proxy BrowserUp WEB-MISC antérieur à 2.1.2 - Injection de modèle entraînant une vulnérabilité RCE via des entrées (CVE-2020-26282)
999337	CVE-2020-14815	WEB-MISC Oracle Business Intelligence Enterprise Edition - Vulnérabilité de script intersite reflétée (CVE-2020-14815)

Règle de signature	ID CVE	Description
999338		Addon de base de données WEB-WORDPRESS Contact Form 7 avant 1.2.5.4 - Vulnérabilité SQLi via l'action Supprimer en masse

Mise à jour de signatures pour mars 2021

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-03-08. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 59 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999313	CVE-2021-25299	WEB-MISC NagioSXi Jusqu'à 5.7.5 - Vulnérabilité XSS via URL (CVE-2021-25299)

Règle de signature	ID CVE	Description
999314	CVE-2021-25298	WEB-MISC NagioSXi Jusqu'à 5.7.5 - Vulnérabilité d'exécution de code à distance via l'assistant DigitalOcean (CVE-2021-25298)
999315	CVE-2021-25297	WEB-MISC NagioSXi Jusqu'à 5.7.5 - Vulnérabilité d'exécution de code à distance via l'assistant Switch (CVE-2021-25297)
999316	CVE-2021-25296	WEB-MISC NagioSXi Jusqu'à 5.7.5 - Vulnérabilité d'exécution de code à distance via l'assistant WindowsWMI (CVE-2021-25296)
999317	CVE-2021-24164	Plugin WEB-WORDPRESS Ninja Forms antérieur à 3.4.34.1 - Vulnérabilité de divulgation d'informations (CVE-2021-24164)
999318	CVE-2021-24163	Plugin WEB-WORDPRESS Ninja Forms antérieur à 3.4.34 - Vulnérabilité de contournement d'autorisation (CVE-2021-24163)
999319	CVE-2021-21972	Plugin WEB-MISC VMware vCenter Server - Vulnérabilité d'exécution de code à distance (CVE-2021-21972)

Règle de signature	ID CVE	Description
999320	CVE-2020-35129	WEB-MISC Mautic avant 3.2.4 - Vulnérabilité XSS via un nouveau formulaire de surveillance sociale (CVE-2020-35129)
999321	CVE-2020-35129	WEB-MISC Mautic avant 3.2.4 - Vulnérabilité XSS via Edit Social Monitoring Form (CVE-2020-35129)
999322	CVE-2020-35128	WEB-MISC Mautic avant 3.2.4 - Formulaire Vulnérabilité XSS via les nouvelles entreprises (CVE-2020-35128)
999323	CVE-2020-35128	WEB-MISC Mautic avant 3.2.4 - Vulnérabilité XSS via le formulaire Edit Companies (CVE-2020-35128)
999324	CVE-2020-35125	WEB-MISC Mautic antérieur à 3.2.4 - Vulnérabilité XSS via l'en-tête de référence (CVE-2020-35125)
999325	CVE-2020-35125	WEB-MISC Mautic Avant 3.2.4 - Vulnérabilité XSS via le[retour] mauticform (CVE-2020-35125)
999326	CVE-2020-13933	WEB-MISC Apache Shiro antérieur à la version 1.6.0 - Vulnérabilité de contournement d'authentification via un point-virgule (CVE-2020-13933)

Règle de signature	ID CVE	Description
999327	CVE-2020-13921, CVE-2020-9483	WEB-MISC Apache SkyWalking antérieur à la version 8.4.0 - Vulnérabilité par injection SQL via la fonctionnalité QueryLogs (CVE-2020-13921, CVE-2020-9483)

Mise à jour de signatures pour mars 2021

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-03-09. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 60 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999311	CVE-2021-26855	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance via X-AnonResource-Backend (CVE-2021-26855)
999312	CVE-2021-26855	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance via X-BEResource (CVE-2021-26855)

Mise à jour de signatures pour mars 2021

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-03-11. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 61 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999308	CVE-2021-21302	WEB-MISC PrestaShop antérieur à 1.7.7.2 - Vulnérabilité d'injection CSV (CVE-2021-21302)
999309	CVE-2020-35749	Web-WORDPRESS Simple Job Board avant 2.9.4 - Vulnérabilité de divulgation arbitraire de fichiers (CVE-2020-35749)
999310	CVE-2019-16012	WEB-MISC Cisco SD-WAN vManage antérieur à la version 19.2.2 - Vulnérabilité par injection SQL (CVE-2019-16012)

Mise à jour de signatures pour mars 2021

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-03-11. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 62 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999307	CVE-2021-27065	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance (CVE-2021-27065)

Mise à jour des signatures pour avril 2021

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-04-08. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 63 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999294	CVE-2021-3273	WEB-MISC NagioSXi antérieur à la version 5.7 - Vulnérabilité par injection de code (CVE-2021-3273)
999295	CVE-2021-3197	WEB-MISC SaltStack antérieur à 3002.3 - Vulnérabilité d'exécution de code à distance via ssh_priv (CVE-2021-3197)

Règle de signature	ID CVE	Description
999296	CVE-2021-3197	WEB-MISC SaltStack antérieur à 3002.3 - Vulnérabilité d'exécution de code à distance via ssh_port (CVE-2021-3197)
999297	CVE-2021-3197	WEB-MISC SaltStack antérieur à 3002.3 - Vulnérabilité d'exécution de code à distance via ssh_options (CVE-2021-3197)
999298	CVE-2021-3197	WEB-MISC SaltStack antérieur à 3002.3 - Vulnérabilité d'exécution de code à distance via ProxyCommand dans un objet JSON (CVE-2021-3197)
999299	CVE-2021-25282	WEB-MISC SaltStack antérieur à 3002.3 - Vulnérabilité de traversée de chemin via pillar_roots.write (CVE-2021-25282)
999300	CVE-2021-24166	Plugin WEB-WORDPRESS Ninja Forms antérieur à 3.4.34 - Vulnérabilité CSRF (CVE-2021-24166)
999301	CVE-2021-24085	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'usurpation (CVE-2021-24085)
999302	CVE-2021-22986	API REST WEB-MISC F5 iControl - Vulnérabilité d'exécution de code à distance (CVE-2021-22986)

Règle de signature	ID CVE	Description
999303	CVE-2021-21978	WEB-MISC VMware View Planner Harness 4.x antérieur à 4.6 Security Patch 1 - Vulnérabilité d'exécution de code à distance (CVE-2021-21978)
999304	CVE-2020-23132	WEB-MISC Joomla! Avant 3.9.25 - Vulnérabilité du chemin de téléchargement com_media non sécurisé via file_path (CVE-2020-23132)
999305	CVE-2020-23132	WEB-MISC Joomla! Avant 3.9.25 - Vulnérabilité du chemin de téléchargement com_media non sécurisé via image_path (CVE-2020-23132)
999306	CVE-2020-22425	WEB-MISC Centreon antérieur à 20.10.4 - Vulnérabilité par injection SQL (CVE-2020-22425)

Mise à jour des signatures pour avril 2021

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-04-22. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 64 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999275	CVE-2021-3378	WEB-MISC FortiLogger 4.4.2.2 - Vulnérabilité de téléchargement de fichiers arbitraires non authentifiés (CVE-2021-3378)
999276	CVE-2021-28925	Analyseur de réseau WEB-MISC Nagios antérieur à 2.4.3 - Vulnérabilité par injection SQL (CVE-2021-28925)
999277	CVE-2021-28924	Analyseur de réseau WEB-MISC Nagios antérieur à 2.4.3 - Vulnérabilité XSS (CVE-2021-28924)
999278	CVE-2021-27927	WEB-MISC Zabbix - Vulnérabilité CSRF via action=authentication.update (CVE-2021-27927)
999279	CVE-2021-26295	WEB-MISC Apache of Biz 17.12.06 - Vulnérabilité de désérialisation arbitraire non authentifiée (CVE-2021-26295)
999280	CVE-2021-25770	WEB-MISC JetBrains YouTrack avant 2020.5.3123 - Vulnérabilité d'injection de modèles côté serveur (CVE-2021-25770)

Règle de signature	ID CVE	Description
999281	CVE-2021-25283	WEB-MISC SaltStack antérieur à 3002.5 - Vulnérabilité d'exécution de code à distance (CVE-2021-25283)
999282	CVE-2021-25283	WEB-MISC SaltStack antérieur à 3002.5 - Vulnérabilité d'exécution de code à distance via un objet JSON (CVE-2021-25283)
999283	CVE-2021-24218	Plugin WEB-WORDPRESS Facebook pour WordPress antérieur à la version 3.0.4 - Vulnérabilité de script intersite stockée (CVE-2021-24218)
999284	CVE-2021-24217	Plugin WEB-WORDPRESS Facebook pour WordPress antérieur à la version 3.0.2 - Vulnérabilité d'injection d'objets PHP (CVE-2021-24217)
999285	CVE-2021-24209	Plugin Web-WORDPRESS WP Super Cache antérieur à 1.7.2 - Vulnérabilité d'exécution de code à distance dans wp-cache-config.php (CVE-2021-24209)
999286	CVE-2021-24209	Plugin Web-WORDPRESS WP Super Cache antérieur à 1.7.2 - Vulnérabilité d'injection de code arbitraire (CVE-2021-24209)
999287	CVE-2021-24165	Plugin WEB-WORDPRESS Ninja Forms antérieur à 3.4.34 - Vulnérabilité de redirection ouverte (CVE-2021-24165)

Règle de signature	ID CVE	Description
999288	CVE-2021-21975	WEB-MISC vRealize Operations Manager - Vulnérabilité de falsification de requête côté serveur non authentifiée (CVE-2021-21975)
999289	CVE-2020-35578	WEB-MISC Nagios XI antérieur à 5.8.0 - Vulnérabilité d'exécution de code à distance (CVE-2020-35578)
999290	CVE-2020-2766	WEB-MISC Oracle WebLogic Server - Vulnérabilité SSRF non authentifiée (CVE-2020-2766)
999291	CVE-2020-17523	WEB-MISC Apache Shiro antérieur à la version 1.7.1 - Vulnérabilité de contournement d'authentification via l'espace (CVE-2020-17523)
999292	CVE-2020-17523	WEB-MISC Apache Shiro antérieur à la version 1.7.1 - Vulnérabilité de contournement d'authentification via Dot (CVE-2020-17523)
999293	CVE-2020-15160	WEB-MISC PrestaShop antérieur à 1.7.6.8 - Vulnérabilité par injection SQL (CVE-2020-15160)

Mise à jour de la signature pour juin 2021

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-06-02. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 65 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 et Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999243	CVE-2021-31761	WEB-MISC Webmin antérieur à 1.974 - Vulnérabilité XSS via /servers/link.cgi/ (CVE-2021-31761)
999244	CVE-2021-31761	WEB-MISC Webmin avant 1.974 - Vulnérabilité XSS via /tunnel/link.cgi/ (CVE-2021-31761)
999245	CVE-2021-31166	Pile de protocole HTTP Microsoft WEB-IIS - Vulnérabilité d'exécution de code à distance (CVE-2021-31166)
999246	CVE-2021-29447	WEB-WORDPRESS WordPress antérieur à 5.7.1 - Vulnérabilité XXE des médiathèques (CVE-2021-29447)

Règle de signature	ID CVE	Description
999247	CVE-2021-28157	Serveur WEB-MISC Devolutions avant 2021.1 et 2020.3.18 - Vulnérabilité d'injection SQL via la suppression de l'utilisateur (CVE-2021-28157)
999248	CVE-2021-27905	WEB-MISC Apache Solr antérieur à 8.2.2 - Vulnérabilité SSRF ReplicationHandler via LeaderURL (CVE-2021-27905)
999249	CVE-2021-27905	WEB-MISC Apache Solr antérieur à 8.2.2 - Vulnérabilité SSRF ReplicationHandler via MasterURL (CVE-2021-27905)
999250	CVE-2021-27890	WEB-MISC MyBB antérieur à 1.8.26 - Vulnérabilité par injection SQL Propriétés du thème (CVE-2021-27890)
999251	CVE-2021-27850, CVE-2019-0195	WEB-MISC Apache Tapestry - Vulnérabilité de divulgation d'informations non authentifiées (CVE-2021-27850 et CVE-2019-0195)
999252	CVE-2021-27183	WEB-MISC MDaemon antérieur à 20.0.4 - Vulnérabilité d'écriture arbitraire de fichiers (CVE-2021-27183)
999253	CVE-2021-27181	WEB-MISC MDaemon antérieur à la version 20.0.4 - Vulnérabilité de fixation de jetons anti-CSRF (CVE-2021-27181)

Règle de signature	ID CVE	Description
999254	CVE-2021-27180	WEB-MISC MDaemon avant 20.0.4 - Vulnérabilité XSS réfléchie (CVE-2021-27180)
999255	CVE-2021-24340	Statistiques WP WEB-WORDPRESS antérieures à 13.0.8 - Vulnérabilité d'injection SQL non authentifiée (CVE-2021-24340)
999256	CVE-2021-24171	Web-WORDPRESS WooCommerce Upload Files Plugin avant 59.4 - Vulnérabilité de traversée de chemin (CVE-2021-24171)
999257	CVE-2021-24171	Web-WORDPRESS WooCommerce Upload Files Plugin avant 59.4 - Vulnérabilité de téléchargement arbitraire de fichiers (CVE-2021-24171)
999258	CVE-2021-22658	WEB-MISC Advantech iView Antérieur à 5.7.03.6112 - Vulnérabilité SQLi via Uservlet et user_password (CVE-2021-22658)
999259	CVE-2021-22658	WEB-MISC Advantech iView Antérieur à 5.7.03.6112 - Vulnérabilité SQLi via Uservlet et nom_utilisateur (CVE-2021-22658)
999260	CVE-2021-22658	WEB-MISC Advantech iView Antérieur à 5.7.03.6112 - Vulnérabilité SQLi via CommandServlet et user_password (CVE-2021-22658)

Règle de signature	ID CVE	Description
999261	CVE-2021-22658	WEB-MISC Advantech iView Antérieur à 5.7.03.6112 - Vulnérabilité SQLi via CommandServlet et nom_utilisateur (CVE-2021-22658)
999262	CVE-2021-21983	WEB-MISC VMware vRealize Operations Manager antérieur à la version 8.4 - Vulnérabilité d'écriture de fichiers arbitraire (CVE-2021-21983)
999263	CVE-2020-6754	DotCMS WEB-MISC antérieur à la version 5.2.4 - Vulnérabilité de traversée d'annuaire via les ressources (CVE-2020-6754)
999264	CVE-2020-27128	WEB-MISC Cisco SD-WAN vManage antérieur à la version 20.3.1 - Vulnérabilité d'écriture de fichiers arbitraire via le traitement à distance (CVE-2020-27128)
999265	CVE-2020-27128	WEB-MISC Cisco SD-WAN vManage antérieur à 20.3.1 - Vulnérabilité d'écriture de fichiers arbitraire via dr (CVE-2020-27128)
999266	CVE-2020-15714	WEB-MISC RConfig 3.9.5 et antérieur - Vulnérabilité par injection SQL (CVE-2020-15714)
999267	CVE-2020-15713	WEB-MISC RConfig antérieur à 3.9.6 - Vulnérabilité par injection SQL (CVE-2020-15713)

Règle de signature	ID CVE	Description
999268	CVE-2020-14295	Cactus WEB-MISC antérieurs à 1.2.13 - Vulnérabilité par injection SQL (CVE-2020-14295)
999269	CVE-2020-13778	WEB-MISC RConfig antérieur à 3.9.5 - Vulnérabilité d'exécution de code à distance via ajaxEditTemplate.php (CVE-2020-13778)
999270	CVE-2020-13778	WEB-MISC RConfig antérieur à 3.9.5 - Vulnérabilité d'exécution de code à distance via ajaxAddTemplate.php (CVE-2020-13778)
999271	CVE-2020-13592	Application de gestion de projets WEB-MISC Rukovoditel - Vulnérabilité par injection SQL via selected_fields (CVE-2020-13592)
999272	CVE-2020-13592	Application de gestion de projets WEB-MISC Rukovoditel - Vulnérabilité par injection SQL via lists_id (CVE-2020-13592)
999273	CVE-2020-13591	Application de gestion de projets WEB-MISC Rukovoditel - Vulnérabilité par injection SQL (CVE-2020-13591)

Règle de signature	ID CVE	Description
999274	CVE-2020-13550	WEB-MISC Advantech WebAccess/SCADA - Vulnérabilité de traversée de chemin via FileName (CVE-2020-13550)

Mise à jour de la signature pour juillet 2021

August 20, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-07-08. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 66 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Voici une liste des règles de signature, des ID CVE et leur description.

Règle de signature	ID CVE	Description
999231	CVE-2021-34074	WEB-MISC Artica Pandora FMS jusqu'à 7.54 - Vulnérabilité de chargement arbitraire de fichiers via un chemin relatif (CVE-2021-34074)

Règle de signature	ID CVE	Description
999232	CVE-2021-32633	WEB-MISC Plone CMS - Vulnérabilité d'exécution de code à distance des modèles de pages Zope via le téléchargement (CVE-2021-32633)
999233	CVE-2021-32633	WEB-MISC Plone CMS - Vulnérabilité d'exécution de code à distance des modèles de pages Zope via un nouveau (CVE-2021-32633)
999234	CVE-2021-31181	WEB-MISC Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance (CVE-2021-31181)
999235	CVE-2021-24370	Web-WORDPRESS Fancy Product Designer Plugin avant 5.6.9 - Vulnérabilité RCE via fpd_custom_uplod_file (CVE-2021-24370)
999236	CVE-2021-24370	Web-WORDPRESS Fancy Product Designer Plugin avant 5.6.9 - Vulnérabilité RCE via custom-image-handler.php (CVE-2021-24370)
999237	CVE-2021-24354	WEB-WORDPRESS Simple 301 Redirige le plugin avant 2.0.4 - Vulnérabilité d'installation arbitraire du plugin (CVE-2021-24354)

Règle de signature	ID CVE	Description
999238	CVE-2021-24352	Plugin de redirection WEB-WORDPRESS Simple 301 avant 2.0.4 - Vulnérabilité d'exportation de redirection (CVE-2021-24352)
999239	CVE-2021-1497, CVE-2021-1498	WEB-MISC Cisco HyperFlex HX antérieur à 4.0 (2e) - Vulnérabilité d'exécution de code à distance (CVE-2021-1497, CVE-2021-1498)
999240	CVE-2020-21057	WEB-MISC FusionPBX 4.5.7 - Vulnérabilité de traversée de chemin via la fonction de suppression de dossier (CVE-2020-21057)
999241	CVE-2020-16245	WEB-MISC Advantech iView antérieur à la version 5.7.03.6112 - Vulnérabilité de traversée de chemin via BackupDatabase (CVE-2020-16245)
999242	CVE-2020-10148	WEB-MISC SolarWinds Orion Multiple Versions - Vulnérabilité de contournement de l'authentification (CVE-2020-10148)

Mise à jour Signature pour août 2021

September 8, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-08-29. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre

appliance contre les attaques.

Version de signature

Signature version 67 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste de règles de signature, d'ID CVE et de sa description.

Règle de signature	ID DE LA CVE	Description
999183	CVE-2021-37557	Versions multiples de WEB-MISC Centreon - Vulnérabilité par injection SQL (CVE-2021-37557)
999184	CVE-2021-35501	WEB-MISC Artica Pandora FMS jusqu'à 7.54 - Vulnérabilité XSS stockée par Visual Console (CVE-2021-35501)
999185	CVE-2021-35464	WEB-MISC ForgeRock Access Management et OpenAM - Vulnérabilité d'exécution de code à distance (CVE-2021-35464)
999186	CVE-2021-34523	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'élévation de privilèges (CVE-2021-34523)

Règle de signature	ID DE LA CVE	Description
999187	CVE-2021-34473	WEB-MISC Microsoft Exchange Server - Vulnérabilité de contournement de l'authentification par requête côté serveur via requête (CVE-2021-34473)
999188	CVE-2021-34473	WEB-MISC Microsoft Exchange Server - Vulnérabilité de contournement de l'authentification par falsification de requête côté serveur via un cookie (CVE-2021-34473)
999189	CVE-2021-33203	WEB-MISC Django - Vulnérabilité de divulgation de l'existence de fichiers TemplateDetailView via Absolute Path (CVE-2021-33203)
999190	CVE-2021-33203	WEB-MISC Django - Vulnérabilité de divulgation de l'existence de fichiers TemplateDetailView via la traversée de chemin (CVE-2021-33203)
999191	CVE-2021-33203	WEB-MISC Django - Vulnérabilité de divulgation de l'existence de fichiers TemplateDetailView via une barre oblique inverse (CVE-2021-33203)
999192	CVE-2021-33203	WEB-MISC Django - Vulnérabilité de divulgation de l'existence de fichiers TemplateDetailView via Slash (CVE-2021-33203)

Règle de signature	ID DE LA CVE	Description
999193	CVE-2021-3287, CVE-2020-28653	WEB-MISC Zoho ManageEngine OPManager antérieur à 12.5.329 - Vulnérabilité RCE non authentifiée (CVE-2021-3287, CVE-2020-28653)
999194	CVE-2021-32789	Plugin WooCommerce WEB-WORDPRESS Jusqu'à 5.5.0 - Vulnérabilité par injection SQL via taxonomie et rest_route (CVE-2021-32789)
999195	CVE-2021-32789	Plugin WooCommerce WEB-WORDPRESS Jusqu'à 5.5.0 - Vulnérabilité par injection SQL via taxonomie (CVE-2021-32789)
999196	CVE-2021-32604	WEB-MISC SolarWinds Serv-U antérieur à 15.2.3 - Vulnérabilité de script intersite via le paramètre SindereMail (CVE-2021-32604)
999197	CVE-2021-32093	WEB-MISC National Security Agency Emissary 5.9.0 - Vulnérabilité de lecture arbitraire de fichiers (CVE-2021-32093)
999198	CVE-2021-31760	WEB-MISC Webmin avant 1.974 - Une vulnérabilité CSRF conduit à RCE via run.cgi (CVE-2021-31760)
999199	CVE-2021-31207	WEB-MISC Microsoft Exchange Server - Vulnérabilité de contournement des fonctionnalités de sécurité (CVE-2021-31207)

Règle de signature	ID DE LA CVE	Description
999200	CVE-2021-31195	WEB-MISC Microsoft Exchange Server - vulnérabilité d'exécution de code à distance (CVE-2021-31195)
999201	CVE-2021-28474	WEB-MISC Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance (CVE-2021-28474)
999202	CVE-2021-24385	Plugin WEB-WORDPRESS FileBird 4.7.3 - Vulnérabilité par injection SQL via le paramètre SelectedFolder et rest_route (CVE-2021-24385)
999203	CVE-2021-24385	Plugin WEB-WORDPRESS FileBird 4.7.3 - Vulnérabilité par injection SQL via le paramètre SelectedFolder (CVE-2021-24385)
999204	CVE-2021-24385	Web-WORDPRESS FileBird Plugin 4.7.3 - Vulnérabilité par injection SQL via un corps codé en JSON (CVE-2021-24385)
999205	CVE-2021-24356	WEB-WORDPRESS Simple 301 Redirige le plugin avant 2.0.4 - Vulnérabilité d'activation arbitraire du plugin (CVE-2021-24356)
999206	CVE-2021-23024	Versions multiples WEB-MISC F5 BIG-IQ - Vulnérabilité d'exécution de code à distance (CVE-2021-23024)

Règle de signature	ID DE LA CVE	Description
999207	CVE-2021-22911	WEB-MISC Rocket.Chat Server 3.11, 3.12 et 3.13 - Vulnérabilité d'injection NOSQL aveugle (CVE-2021-22911)
999208	CVE-2021-22900	WEB-MISC Pulse Connect Secure avant 9.1R11.4 - Vulnérabilité d'exécution de code à distance via smimeCert.cgi (CVE-2021-22900)
999209	CVE-2021-22900	WEB-MISC Pulse Connect Secure avant 9.1R11.4 - Vulnérabilité d'exécution de code à distance via admincert.cgi (CVE-2021-22900)
999210	CVE-2021-22900	WEB-MISC Pulse Connect Secure avant 9.1R11.4 - Vulnérabilité d'exécution de code à distance via clientauthcert.cgi (CVE-2021-22900)
999211	CVE-2021-22160	WEB-MISC Apache Pulsar - Vulnérabilité de contournement de l'authentification des jetons Web JSON (CVE-2021-22160)
999212	CVE-2021-21809	WEB-MISC Moodle - Vulnérabilité d'exécution de code à distance via le plugin Spellchecker et la méthode GetSuggestions (CVE-2021-21809)

Règle de signature	ID DE LA CVE	Description
999213	CVE-2021-21809	WEB-MISC Moodle - Vulnérabilité d'exécution de code à distance via le plugin orthographe et la méthode CheckWords (CVE-2021-21809)
999214	CVE-2021-21809	WEB-MISC Moodle - Vulnérabilité d'exécution de code à distance via s__aspellpath (CVE-2021-21809)
999215	CVE-2021-21805	WEB-MISC Advantech R-SeeNet - Vulnérabilité d'exécution de code à distance non authentifiée (CVE-2021-21805)
999216	CVE-2021-21804	WEB-MISC Advantech R-SeeNet - Vulnérabilité d'inclusion de fichiers locaux via sub_opt (CVE-2021-21804)
999217	CVE-2021-21587	WEB-MISC Dell Wyse Management Suite antérieure à la version 3.3 - Vulnérabilité de traversée de chemin via /image/os/listfiles (CVE-2021-21587)
999218	CVE-2021-21587	WEB-MISC Dell Wyse Management Suite antérieure à la version 3.3 - Vulnérabilité de traversée de chemin via /image/app/rsp/listfiles (CVE-2021-21587)

Règle de signature	ID DE LA CVE	Description
999219	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite antérieure à 3.3 - Vulnérabilité de traversée de chemin via /image/app et FileName (CVE-2021-21586)
999220	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite antérieure à la version 3.3 - Vulnérabilité de traversée de chemin via /image/os et nom de fichier (CVE-2021-21586)
999221	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite antérieure à 3.3 - Vulnérabilité de traversée de chemin via /image/os et FilePath (CVE-2021-21586)
999222	CVE-2020-25223	WEB-MISC Sophos SG UTM - Exécution de code à distance via SID et /var (CVE-2020-25223)
999223	CVE-2020-25223	WEB-MISC Sophos SG UTM - Exécution de code à distance via SID et /webadmin.plx (CVE-2020-25223)
999224	CVE-2020-21056	WEB-MISC FusionPBX 4.5.7 - Vulnérabilité de traversée de chemin via foldernew (CVE-2020-21056)
999225	CVE-2020-21055	WEB-MISC FusionPBX 4.5.7 - Vulnérabilité de traversée de chemin via la fonction de renommage de fichier (CVE-2020-21055)

Règle de signature	ID DE LA CVE	Description
999226	CVE-2020-16245	WEB-MISC Advantech iView antérieur à 5.7.03.6112 - Vulnérabilité de traversée de chemin dans FindSummaryUpdateDeviceListExpo (CVE-2020-16245)
999227	CVE-2020-16245	WEB-MISC Advantech iView antérieur à la version 5.7.03.6112 - Vulnérabilité de traversée de chemin via FindCFGDeviceListExport (CVE-2020-16245)
999228	CVE-2020-14181	WEB-MISC Atlassian Jira Server - Vulnérabilité de divulgation d'informations via ViewUserHover.jspa (CVE-2020-14181)
999229	CVE-2020-14005	WEB-MISC SolarWinds Orion avant 2020.2.1 HF 2 - Exécution de code à distance via ExecuteVBScript Type d'action (CVE-2020-14005)
999230	CVE-2020-14005	WEB-MISC SolarWinds Orion avant 2020.2.1 HF 2 - Exécution de code à distance via ExecuteExternalProgram Type d'action (CVE-2020-14005)

Mise à jour des signatures pour septembre 2021

October 5, 2021

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-09-11. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre

appliance contre les attaques.

Version de signature

Signature version 68 applicable aux plates-formes NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 et Citrix ADC 13.1.

> **Remarque :**
>
> l'activation des règles de signature du corps Post et du corps de réponse peut affecter le processeur Citrix ADC.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	COUVERCLE DE LA CVE	Description
999163	CVE-2021-37556	WEB-MISC Centreon Multiple Versions - Vulnérabilité d'injection SQL via un paramètre de fin (CVE-2021-37556)
999164	CVE-2021-37556	WEB-MISC Centreon Multiple Versions - Vulnérabilité d'injection SQL via le paramètre de démarrage (CVE-2021-37556)
999165	CVE-2021-37353	Assistant Docker WEB-MISC Nagios XI antérieur à 1.1.3 - Vulnérabilité SSRF via un paramètre hôte sans schéma d'URI (CVE-2021-37353)
999166	CVE-2021-37353	Assistant Docker WEB-MISC Nagios XI antérieur à 1.1.3 - Vulnérabilité SSRF via un paramètre hôte avec schéma d'URI (CVE-2021-37353)

Règle de signature	COUVERCLE DE LA CVE	Description
999167	CVE-2021-34638	Plugin de gestionnaire de téléchargement WEB-WORDPRESS antérieur à 3.1.25 - Vulnérabilité de traversée de répertoires (CVE-2021-34638)
999168	CVE-2021-33766	WEB-MISC Microsoft Exchange Server - Vulnérabilité de divulgation d'informations (CVE-2021-33766)
999169	CVE-2021-32682	WEB-MISC ElFinder antérieur à 2.1.59 - Vulnérabilité d'injection de commande via l'archivage (CVE-2021-32682)
999170	CVE-2021-26084	WEB-MISC Confluence Server and Data Center - Vulnérabilité d'injection OGNL via doenterpagevariables (CVE-2021-26084)
999171	CVE-2021-26084	WEB-MISC Confluence Server and Data Center - Vulnérabilité d'injection OGNL via createpage-entervariables (CVE-2021-26084)
999172	CVE-2021-23394	WEB-MISC ElFinder antérieur à 2.1.59 - Vulnérabilité d'exécution de code à distance via Phar Makefile (CVE-2021-23394)
999173	CVE-2021-23394	WEB-MISC ElFinder antérieur à 2.1.59 - Vulnérabilité d'exécution de code à distance via Phar Rename (CVE-2021-23394)

Règle de signature	COUVERCLE DE LA CVE	Description
999174	CVE-2021-23394	WEB-MISC ElFinder antérieur à 2.1.59 - Vulnérabilité d'exécution de code à distance via Phar Upload (CVE-2021-23394)
999175	CVE-2020-36289	WEB-MISC Atlassian Jira Server - Vulnérabilité de divulgation d'informations via QueryComponentRenderer-Value (CVE-2020-36289)
999176	CVE-2020-16245	WEB-MISC Advantech IView antérieur à 5.7.03.6112 - Vulnérabilité de traversée de chemin via FindSummaryCfgDeviceListExport (CVE-2020-16245)
999177	CVE-2020-16245	WEB-MISC Advantech IView antérieur à 5.7.03.6112 - Vulnérabilité de traversée de chemin via FindUpdateDeviceListExport (CVE-2020-16245)
999178	CVE-2020-13774	WEB-MISC Ivanti Endpoint Manager Versions multiples - Vulnérabilité RCE via EditLaunchPadDialog.aspx (CVE-2020-13774)
999179	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance via une page personnalisée (CVE-2020-1147)

Règle de signature	COUVERCLE DE LA CVE	Description
999180	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance via quicklinksdialogform.aspx (CVE-2020-1147)
999181	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance via quicklinks.aspx (CVE-2020-1147)
999182	CVE-2020-11110	WEB-MISC Apache Grafana jusqu'à la version 6.7.1 - Vulnérabilité XSS (CVE-2020-11110)
999522	CVE-2020-13379	WEB-MISC Grafana 3.0.1 à 7.0.1 - Contournement de CSRF menant à une vulnérabilité DOS (CVE-2020-13379)

Gestion des bots

August 20, 2021

Parfois, le trafic Web entrant est composé de bots et la plupart des organisations souffrent d'attaques de bot. Les applications Web et mobiles sont des moteurs de revenus importants pour les entreprises et la plupart des entreprises sont menacées par des cyberattaques avancées, telles que les robots. Un bot est un logiciel qui effectue automatiquement certaines actions à plusieurs reprises à un rythme beaucoup plus rapide qu'un humain. Les robots peuvent interagir avec des pages Web, envoyer des formulaires, exécuter des actions, numériser des textes ou télécharger du contenu. Ils peuvent accéder à des vidéos, poster des commentaires et tweeter sur les plateformes de médias sociaux. Certains bots, connus sous le nom de chatbots, peuvent tenir des conversations de base avec des utilisateurs humains.

Un bot qui effectue un service utile, tel que le service à la clientèle, le chat automatisé et les bots de recherche sont de bons bots. Dans le même temps, un bot qui peut capturer ou télécharger du contenu à partir d'un site Web, voler des informations d'identification d'utilisateur, du contenu de spam et effectuer d'autres types de cyberattaques est un bot malveillant.
Avec un bon nombre de robots défectueux exécutant des tâches malveillantes, il est essentiel de gérer le trafic des robots et de protéger vos applications web contre les attaques de robots. En utilisant la gestion de bot Citrix, vous pouvez détecter le trafic de bot entrant et atténuer les attaques de bot pour protéger vos applications Web.
La gestion des bots Citrix permet d'identifier les bots malveillants et de protéger votre appliance contre les attaques de sécurité avancées. Il détecte les bots bons et les bots malveillants et identifie si le trafic entrant est une attaque de bot. En utilisant la gestion des bots, vous pouvez atténuer les attaques et protéger vos applications Web.

La gestion de bot Citrix ADC offre les avantages suivants :

- **Défendre contre les bots, les scripts et les boîtes à outils**. Permet d'atténuer les menaces en temps réel à l'aide de la défense statique basée sur la signature et des empreintes digitales de l'appareil.
- **Neutraliser les attaques de base et avancées automatisées**. Empêche les attaques, telles que les DDoS de couche d'application, la pulvérisation de mot de passe, le remplissage de mot de passe, les racleurs de prix et les racleurs de contenu.
- **Protégez vos API et vos investissements**. Protège vos API contre une utilisation abusive injustifiée et protège les investissements d'infrastructure contre le trafic automatisé.

Certains cas d'utilisation dans lesquels vous pouvez bénéficier de l'utilisation du système de gestion de bot Citrix sont :

- Connexion forcée brute. Un portail Web gouvernemental est constamment attaqué par des bots qui tentent de forcer les connexions utilisateur. L'organisation a découvert l'attaque en regardant les journaux Web et en voyant des utilisateurs spécifiques sélectionnés encore et encore avec des tentatives de connexion rapides et des mots de passe incrémentés à l'aide d'une approche d'attaque par dictionnaire. En vertu de la loi, ils doivent se protéger eux-mêmes et protéger leurs utilisateurs. En déployant la gestion de bot Citrix, ils peuvent arrêter la connexion par force brute à l'aide de techniques d'empreintes digitales de l'appareil et de limitation de débit.
- Bloquer les bots malveillant et les bots d'empreintes digitales des périphériques inconnus. Une entité Web reçoit 100 000 visiteurs par jour. Ils doivent améliorer l'empreinte sous-jacente et ils dépensent une fortune. Lors d'un audit récent, l'équipe a découvert que 40 % du trafic provenait de bots, de capture de contenu, de collecte de nouvelles, de vérification des profils d'utilisateurs, etc. Ils veulent bloquer ce trafic pour protéger leurs utilisateurs et réduire leurs coûts d'hébergement. Grâce à la gestion des bots, ils peuvent bloquer les bots malveillants connus et les bots inconnus d'empreintes digitales qui martèlent leur site. En bloquant ces

bots, ils peuvent réduire le trafic de bots de 90 %.

Que fait Citrix bot management ?

La gestion des bots de Citrix aide les organisations à protéger leurs applications Web et leurs ressources publiques contre les attaques de sécurité avancées. Lorsqu'un trafic entrant est un bot, le système de gestion du bot détecte le type de bot, attribue une action et génère des informations sur les robots, comme indiqué dans le diagramme suivant.



Comment fonctionne la gestion de bot Citrix ADC

Le diagramme suivant montre comment fonctionne la gestion de bot Citrix ADC. Le processus implique huit techniques de détection qui permettent de détecter le trafic entrant comme un bon ou un mauvais robot. Par défaut, les bons robots détectés par les signatures sont autorisés et les robots défectueux détectés par les signatures sont supprimés.



1. Le processus commence par activer la fonctionnalité de gestion des robots sur l'appliance.
2. Lorsqu'un client envoie une demande, l'appliance évalue le trafic à l'aide des règles de stratégie de bot. Si la demande entrante est identifiée comme un bot, l'appliance applique un profil de détection de bot.
3. Vous devez lier le fichier de signature de bot par défaut ou personnalisé au profil de détection de bot. Le fichier de signature de bot contient une liste de règles de signature de bot permettant d'identifier le type de bot entrant.
4. Les règles de détection des robots sont disponibles dans huit catégories de détection dans le fichier de signature. Les catégories sont la liste d'autorisation, la liste de blocage, la signature statique, la réputation IP, l'empreinte digitale de l'appareil et la limitation de débit. En fonction du trafic bot, le système applique une règle de détection au trafic.
5. Si le trafic bot entrant correspond à une entrée de la liste des robots autorisés, le système contourne les autres techniques de détection et l'action associée consigne les données.
6. Pour les techniques de détection autres que la liste d'autorisation des robots, si une demande entrante correspond à une règle configurée, l'action correspondante est appliquée. Les actions possibles sont le dépôt, la redirection, la réinitialisation, l'atténuation et le journal. CAPTCHA est une action d'atténuation prise en charge pour la réputation IP, les empreintes digitales des appareils et les techniques de détection TPS.

Détection des robots

October 5, 2021

Le système de gestion des bots Citrix ADC utilise six techniques différentes pour détecter le trafic de robots entrant. Les techniques sont utilisées comme règles de détection pour détecter le type de bot. Les techniques sont la liste d'autorisation des robots, la liste des bots bloqués, la réputation IP, l'empreinte digitale de l'appareil, la limitation du débit, le piège de bot, le TPS et le CAPTCHA.

> **Remarque :**
>
> La gestion des bots prend en charge un maximum de 32 entités de configuration pour les techniques de liste de blocage, de liste d'autorisation et de limitation de débit.

Liste blanche des bots. Liste personnalisée d'adresses IP, de sous-réseaux et d'expressions de stratégie pouvant être ignorées en tant que liste autorisée.

Liste noire des robots. Une liste personnalisée d'adresses IP, de sous-réseaux et d'expressions de stratégie dont l'accès à vos applications Web doit être bloqué.

Réputation IP. Cette règle détecte si le trafic de bot entrant provient d'une adresse IP malveillante.

empreinte digitale de l'appareil. Cette règle détecte si le trafic de bot entrant comporte l'ID d'empreinte digitale de l'appareil dans l'en-tête de la demande entrante et les attributs de navigateur d'un trafic de bot client entrant.

> **Limitation :**
>
> 1. JavaScript doit être activé dans le navigateur client.
> 2. Ne fonctionne pas pour les réponses XML.

Expression de journal de bot. La technique de détection vous permet de capturer des informations supplémentaires sous forme de messages de journal. Les données peuvent être le nom de l'utilisateur qui a demandé l'URL, l'adresse IP source et le port source à partir duquel l'utilisateur a envoyé la demande ou les données générées à partir d'une expression.

Limite de taux. Ce taux de règle limite les demandes multiples provenant du même client.

Piège à robots. Détecte et bloque les robots automatisés en annonçant une URL d'interruption dans la réponse du client. L'URL apparaît invisible et n'est pas accessible si le client est un utilisateur humain. La technique de détection est efficace pour bloquer les attaques de robots automatisés.

TPS. Détecte le trafic entrant en tant que bots si le nombre maximal de demandes et le pourcentage d'augmentation des demandes dépassent l'intervalle de temps configuré.

CAPTCHA. Cette règle utilise un CAPTCHA pour atténuer les attaques de bots. Un CAPTCHA est une validation de question-réponse pour déterminer si le trafic entrant provient d'un utilisateur humain ou d'un robot automatisé. La validation permet de bloquer les bots automatisés qui causent des violations de sécurité aux applications Web. Vous pouvez configurer CAPTCHA en tant qu'action de bot dans les techniques de réputation IP et de détection des empreintes digitales de l'appareil.

Voyons maintenant comment configurer chaque technique pour détecter et gérer le trafic de votre bot.

Comment mettre à niveau votre appliance vers la configuration de gestion des bots basée sur l'interface de ligne de commande Citrix ADC

Si vous mettez à niveau votre appliance à partir d'une version antérieure (Citrix ADC version 13.0 build 58.32 ou antérieure), vous devez d'abord convertir manuellement la configuration de gestion des bots existante en configuration de gestion des bots basée sur l'interface de ligne de commande Citrix ADC une seule fois. Suivez les étapes suivantes pour convertir manuellement votre configuration de gestion des bots.

1. Après la mise à niveau vers la dernière version, connectez-vous à l'outil de mise à niveau "upgrade_bot_config.py" à l'aide de la commande suivante

   À l'invite de commandes, tapez :

   ```
   shell "/var/python/bin/python /netscaler/upgrade_bot_config.py > /var/bot_upgrade_commands.txt"
   ```

2. Exécutez la configuration à l'aide de la commande suivante.

   À l'invite de commandes, tapez :

   ```
   batch -f /var/bot_upgrade_commands.txt
   ```

3. Enregistrez la configuration mise à niveau.

```
save ns config
```

Configuration de la gestion des robots Citrix ADC basée sur l'interface de ligne

La configuration de la gestion des bots vous permet de lier une ou plusieurs techniques de détection de bots à un profil de bot spécifique. Vous commencez le processus en activant la fonctionnalité de gestion des bots sur votre appliance. Une fois cette option activée, vous importez le fichier de signature du bot dans la solution matérielle-logicielle. Après l'importation, vous devez créer un profil de bot. Vous créez ensuite une stratégie de bot à laquelle le profil de bot est lié pour évaluer le trafic entrant en tant que bot et liez la stratégie globalement ou à un serveur virtuel.

> **Remarque :**
>
> Si vous mettez à niveau votre appliance à partir d'une version antérieure, vous devez d'abord convertir manuellement la configuration existante de gestion des robots. Pour plus d'informations, consultez la section Comment mettre à niveau vers la configuration de gestion des robots basée sur Citrix ADC CLI .

Vous devez effectuer les étapes suivantes pour configurer la gestion des robots basée sur Citrix ADC :

1. Enable bot management
2. Import bot signature
3. Add bot profile

4. Bind bot profile
5. Add bot policy
6. Bind bot policy
7. Configure bot settings

Enable bot management

Avant de commencer, assurez-vous que la fonctionnalité de gestion des bots est activée sur la solution matérielle-logicielle. Si vous disposez d'un nouveau Citrix ADC ou VPX, vous devez activer la fonctionnalité avant de la configurer. Si vous mettez à niveau un dispositif Citrix ADC ou VPX depuis une version antérieure de la version du logiciel Citrix ADC vers la version actuelle, vous devez activer la fonctionnalité avant de la configurer. À l'invite de commandes, tapez :

```
enable ns feature Bot
```

Import bot signature

Vous pouvez importer le fichier bot de signature par défaut et le lier au profil de robot. À l'invite de commandes, tapez :

```
import bot signature [<src>] <name> [-comment <string>] [-overwrite]
```

Où,
src. Chemin d'accès local et nom du fichier, ou URL (protocole, hôte, chemin d'accès et nom de fichier) du fichier dans lequel stocker le fichier de signature importé. Remarque : L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS qui nécessite une authentification par certificat client pour y accéder. Longueur maximale :
nom 2047. Nom à attribuer à l'objet de fichier de signature de bot sur Citrix ADC. Il s'agit d'un argument obligatoire. Longueur maximale : 31
commentaires. Tout commentaire permettant de conserver les informations relatives à l'objet de fichier de signature. Longueur maximale : 255.
Overwrite. Écrase le fichier existant.
Remarque : utilisez l'option `overwrite` pour mettre à jour le contenu du fichier de signature. Vous pouvez également utiliser la commande `update bot signature <name>` pour mettre à jour le fichier de signature sur l'appliance Citrix ADC

Exemple

```
import bot signature http://www.example.com/signature.json signaturefile -
comment commentsforbot -overwrite
```


> **Remarque :**
>
> Vous pouvez utiliser l'option de remplacement pour mettre à jour le contenu du fichier de signature. Vous pouvez également utiliser la commande `update bot signature <name>` pour mettre à jour le fichier de signature dans l'appliance Citrix ADC.

Add bot profile

Un profil de bot est un ensemble de paramètres de profil permettant de configurer la gestion des bots sur l'appliance. Vous pouvez configurer les paramètres pour effectuer la détection des bots.

À l'invite de commandes, tapez :

```
add bot profile <name> [-signature <string>] [-errorURL <string>] [-trapURL
 <string>] [-comment <string>] [-whiteList ( ON | OFF )] [-blackList ( ON
 | OFF )] [-rateLimit ( ON | OFF )] [-deviceFingerprint ( ON | OFF )] [-
deviceFingerprintAction ( none | log | drop | redirect | reset | mitigation
 )] [-ipReputation ( ON | OFF )] [-trap ( ON | OFF )] [-trapAction ( none |
 log | drop | redirect | reset )] [-tps ( ON | OFF )]
```

Exemple :

```
add bot profile profile1 -signature signature -errorURL http://www.example
.com/error.html -trapURL /trap.html -whitelist ON -blacklist ON -ratelimit
 ON -deviceFingerprint ON -deviceFingerprintAction drop -ipReputation ON -
trap ON
```

Bind bot profile

Après avoir créé un profil de bot, vous devez lier le mécanisme de détection des bots au profil.

À l'invite de commandes, tapez :

```
bind bot profile <name> ((-blackList [-type ( IPv4 | Subnet | Expression
 )] [-enabled ( ON | OFF )] [-value <string>] [-action ( log | drop |
reset )] [-logMessage <string>] [-comment <string>])| (-whiteList [-type
 ( IPv4 | Subnet | Expression )] [-enabled ( ON | OFF )] [-value <string
>] [-log ( ON | OFF )] [-logMessage <string>] [-comment <string>]))|
(-rateLimit [-type ( session |SOURCE_IP | url )] [-enabled ( ON | OFF
)] [-url <string>] [-cookieName <string>] [-rate <positive_integer>] [-
timeslice <positive_integer>] [-action ( none | log | drop | redirect |
reset )] [-logMessage <string>] [-comment <string>])| (-ipReputation [-
category <ipReputationCategory>] [-enabled ( ON | OFF )] [-action ( none
 | log | drop | redirect | reset | mitigation )] [-logMessage <string>]
```



```
[-comment <string>])| (-captchaResource [-url <string>] [-enabled ( ON |
 OFF )] [-waitTime <positive_integer>] [-gracePeriod <positive_integer>]
 [-mutePeriod <positive_integer>] [-requestLengthLimit <positive_integer
>] [-retryAttempts <positive_integer>] [-action ( none | log | drop |
redirect | reset )] [-logMessage <string>] [-comment <string>])| (-tps
 [-type ( SOURCE_IP | GeoLocation | REQUEST_URL | Host )] [-threshold <
positive_integer>] [-percentage <positive_integer>] [-action ( none | log |
 drop | redirect | reset | mitigation )] [-logMessage <string>] [-comment <
string>])
```

Exemple :

L'exemple suivant concerne la liaison de la technique de détection de réputation IP à un profil de bot spécifique.

```
bind bot profile profile5 -ipReputation -category BOTNET -enabled ON -
action drop -logMessage message
```

Add bot policy

Vous devez ajouter la stratégie de bot pour évaluer le trafic des robots.

À l'invite de commandes, tapez :

```
add bot policy <name> -rule <expression> -profileName <string> [-undefAction
 <string>] [-comment <string>] [-logAction <string>]
```

Où,

Name. Nom de la stratégie de bot. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), la livre (#), l'espace (), à (@), égal à (=), deux-points (:) et les caractères de soulignement. Peut être modifié après l'ajout de la stratégie de bot.

Rule. Expression utilisée par la stratégie pour déterminer si le profil de bot doit être appliqué à la demande spécifiée. Il s'agit d'un argument obligatoire. Longueur maximale : 1499

profileName. Nom du profil de bot à appliquer si la demande correspond à cette stratégie de bot. Il s'agit d'un argument obligatoire. Longueur maximale : 127

undefAction. Action à effectuer si le résultat de l'évaluation des politiques n'est pas défini (UNDEF). Un événement UNDEF indique une condition d'erreur interne. Longueur maximale : 127

Comment. Tout type d'informations concernant cette stratégie de bot. Longueur maximale : 255

logAction. Nom de l'action de journal à utiliser pour les demandes qui correspondent à cette stratégie. Longueur maximale : 127

Exemple :

```
add bot policy pol1 -rule "HTTP.REQ.HEADER(\"header\").CONTAINS(\"custom
\")"- profileName profile1 -undefAction drop -comment commentforbotpolicy -
logAction log1
```

Bind bot policy global

À l'invite de commandes, tapez :

```
bind bot global -policyName <string> -priority <positive_integer> [-gotoPriorityExpres
 <expression>][-type ( REQ_OVERRIDE | REQ_DEFAULT )] [-invoke (-labelType (
 vserver | policylabel )-labelName <string>)]
```

Exemple :

```
bind bot global -policyName pol1 -priority 100 -gotoPriorityExpression NEXT
-type REQ_OVERRIDE
```

Bind bot policy to a virtual server

À l'invite de commandes, tapez :

```
bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>] )| <
serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>]
 [-gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )] [-
invoke (<labelType> <labelName>)] )| -analyticsProfile <string>@)
```

Exemple :

```
bind lb vserver lb-server1 -policyName pol1 -priority 100 -gotoPriorityExpression
 NEXT -type REQ_OVERRIDE
```

Configure bot settings

Vous pouvez personnaliser les paramètres par défaut si nécessaire.
À l'invite de commandes, tapez :

```
set bot settings [-defaultProfile <string>] [-javaScriptName <string>]
 [-sessionTimeout <positive_integer>] [-sessionCookieName <string>] [-
dfpRequestLimit <positive_integer>] [-signatureAutoUpdate ( ON | OFF )]
[-signatureUrl <URL>] [-proxyServer <ip_addr|ipv6_addr|*>] [-proxyPort <
port|*>]
```

Où,

defaultProfile. Profil à utiliser lorsqu'une connexion ne correspond à aucune stratégie. Le paramètre par défaut est «, qui renvoie les connexions inégalées vers Citrix ADC sans essayer de les filtrer davantage. Longueur maximale : 31

javaScriptName. Nom du code JavaScript utilisé par la fonctionnalité BotNet en réponse. Doit commencer par une lettre ou un chiffre et peut être composé de 1 à 31 lettres, chiffres et symboles de trait d'union (-) et de trait de soulignement (_). La condition suivante s'applique uniquement à l'interface de ligne de commande Citrix ADC : Si le nom inclut un ou plusieurs espaces, insérez le nom entre guillemets doubles ou simples (par exemple, « nom de mon cookie » ou « nom de mon cookie »). Longueur maximale : 31

SessionTimeout. La session expite, en secondes, après quoi une session utilisateur est interrompue.

Valeur minimale : 1, Valeur maximale : 65535

sessionCookieName. Nom du cookie SessionCookie que la fonctionnalité BotNet utilise pour le suivi. Doit commencer par une lettre ou un chiffre et peut être composé de 1 à 31 lettres, chiffres et symboles de trait d'union (-) et de trait de soulignement (_). La condition suivante s'applique uniquement à l'interface de ligne de commande Citrix ADC : Si le nom inclut un ou plusieurs espaces, insérez le nom entre guillemets doubles ou simples (par exemple, « nom de mon cookie » ou « nom de mon cookie »). Longueur maximale : 31

dfpRequestLimit. Nombre de demandes à autoriser sans cookie de session de bot si l'empreinte digitale de l'appareil est activée.

Valeur minimale : 1, Valeur maximale : 4294967295

SignatureAutoUpdate. Indicateur utilisé pour activer/désactiver les signatures de mise à jour automatique des bots.

Valeurs possibles : ON, OFF

Valeur par défaut : OFF

signatureUrl. URL pour télécharger le fichier de mappage des signatures de bots à partir du serveur.

Valeur par défaut : `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`.

Longueur maximale : 2047

ProxyServer. IP du serveur proxy pour obtenir les signatures mises à jour d'AWS.

ProxyPort. Port du serveur proxy pour obtenir les signatures mises à jour d'AWS. Valeur par défaut : 8080

Exemple :

```
set bot settings -defaultProfile profile1 -javaScriptName json.js -sessionTimeout
 1000 -sessionCookieName session
```


Configuration de la gestion des robots à l'aide de l'interface graphique Citrix ADC

Vous pouvez configurer la gestion des robots Citrix ADC en activant d'abord la fonctionnalité sur l'appliance. Une fois que vous l'avez activée, vous pouvez créer une stratégie de bot pour évaluer le trafic entrant en tant que bot et envoyer le trafic vers le profil de bot. Ensuite, vous créez un profil de bot, puis vous liez le profil à une signature de bot. Vous pouvez également cloner le fichier de signature du bot par défaut et utiliser le fichier de signature pour configurer les techniques de détection. Après avoir créé le fichier de signature, vous pouvez l'importer dans le profil du bot.



1. Activer la fonctionnalité de gestion des robots
2. Configuration des paramètres de gestion des bots
3. Signature par défaut du robot Cloner Citrix
4. Importer la signature du bot Citrix
5. Configuration des paramètres de signature du bot
6. Créer un profil de bot
7. Créer une stratégie de bot

Activer la fonctionnalité de gestion des robots

Pour activer la gestion des bots, procédez comme suit :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Sur la page **Configurer les fonctionnalités avancées**, cochez la case **Gestion des bots** .
3. Cliquez sur **OK**, puis sur **Fermer**.



Configuration des paramètres de gestion des bots pour la technique d'empreinte digitale

Pour configurer la technique d'empreinte digitale de l'appareil, procédez comme suit :

1. Accédez à **Sécurité** > **Citrix Bot Management**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres de gestion des robots Citrix**.
3. Dans la **section Configurer les paramètres de gestion des bots Citrix**, définissez les paramètres suivants.
   a) Profil par défaut. Sélectionnez un profil de bot.

b) Nom JavaScript. Nom du fichier JavaScript utilisé par la gestion des robots dans sa réponse au client.
c) Délai d'expiration de session. Délai d'expiration en secondes après lequel la session utilisateur est interrompue.
d) Cookie de session. Nom du cookie de session utilisé par le système de gestion des robots pour le suivi.
e) Limite de demande d'empreinte digitale du périphérique Nombre de demandes à autoriser sans cookie de session de bot, si l'empreinte digitale de l'appareil est activée



4. Cliquez sur **OK**.

Fichier de signature de robot clone

Pour cloner le fichier de signature du bot, procédez comme suit :

1. Accédez à **Sécurité** > **Citrix Bot Management** and **Signatures**.
2. Dans la page **Signatures de Citrix Bot Management**, sélectionnez l'enregistrement de signatures de robots par défaut et cliquez sur **Cloner**.
3. Dans la page **Signature du robot clone**, saisissez un nom et modifiez les données de signature.

4. Cliquez sur **Create**.



Importer le fichier de signature de bot

Si vous possédez votre propre fichier de signature, vous pouvez l'importer sous forme de fichier, de texte ou d'URL. Pour importer le fichier de signature du bot, procédez comme suit :

1. Accédez à **Sécurité** > **Citrix Bot Management** and **Signatures**.
2. Sur la page **Citrix Bot Management Signatures**, importez le fichier sous forme d'URL, de fichier ou de texte.
3. Cliquez sur **Continuer**.



4. Sur la page Importer la signature Citrix Bot Management, définissez les paramètres suivants.
   a) Name. Nom du fichier de signature du bot.
   b) Comment. Brève description du fichier importé.
   c) Overwrite. Activez cette case à cocher pour autoriser l'écrasement des données pendant la mise à jour du fichier.
   d) Données de signature. Modifier les paramètres de signature

5. Cliquez sur **Terminé**.



Configurer la liste des robots autorisés à l'aide de l'interface graphique Citrix ADC

Cette technique de détection vous permet de contourner les URL que vous configurez une URL répertoriée autorisée. Pour configurer une URL de liste d'autorisation, procédez comme suit :

1. Accédez à **Sécurité** > **Citrix Bot Management** and **Profiles**.
2. Sur la page **Profils de gestion des bots Citrix**, sélectionnez un fichier et cliquez sur **Modifier**.
3. Sur la page **Profil de gestion des bots Citrix**, accédez à la section **Paramètres de signature** et cliquez sur **Liste blanche**.
4. Dans la section **Liste blanche**, définissez les paramètres suivants :
   a) Activé. Cochez la case pour valider les URL de la liste d'autorisation dans le cadre du processus de détection.
   b) Configurez les types. Configurez une URL de liste d'autorisation. L'URL est ignorée lors de la détection du bot. Cliquez sur Ajouter pour ajouter une URL à la liste des robots autorisés.
   c) Dans la page **Configurer la liaison de la liste blanche du profil Citrix Bot Management**, définissez les paramètres suivants :
      i. Tapez. Le type d'URL peut être une adresse IPv4, une adresse IP de sous-réseau ou une adresse IP correspondant à une expression de stratégie.
      ii. Activé. Cochez la case pour valider l'URL.
      iii. Valeur. adresse URL.
      iv. Bûche. Activez la case à cocher pour stocker les entrées du journal.

v. Message du journal. Brève description du journal.
vi. Commentaires. Brève description de l'URL de la liste d'autorisation.
vii. Cliquez sur **OK**.



5. Cliquez sur **Update**.
6. Cliquez sur **Terminé**.



Configurer la liste des bots bloqués à l'aide de l'interface graphique Citrix ADC

Cette technique de détection vous permet de supprimer les URL que vous configurez comme URL répertoriées dans la liste des blocs. Pour configurer une URL de liste de blocage, procédez comme suit.

1. Accédez à **Sécurité** > **Citrix Bot Management** and **Profiles**.
2. Sur la page **Profils de gestion des bots Citrix**, sélectionnez un fichier de signature et cliquez sur **Modifier**.

3. Sur la page **Profil de gestion des robots Citrix**, accédez à la section **Paramètres de signature** et cliquez sur **Liste noire**.
4. Dans la section **Liste noire**, définissez les paramètres suivants :
   a) Activé. Activez la case à cocher pour valider les URL des listes bloquées dans le cadre du processus de détection.
   b) Configurez les types. Configurez une URL pour qu'elle fasse partie du processus de détection de la liste des bots bloqués. Ces URL sont supprimées lors de la détection du bot. Cliquez sur Ajouter pour ajouter une URL à la liste des bots bloqués
   c) Dans la page **Configurer la liaison de la liste noire des profils Citrix Bot Management**, définissez les paramètres suivants.
      i. Tapez. Le type d'URL peut être une adresse IPv4, une adresse IP de sous-réseau ou une adresse IP.
      ii. Activé. Cochez la case pour valider l'URL.
      iii. Valeur. adresse URL.
      iv. Bûche. Activez la case à cocher pour stocker les entrées du journal.
      v. Message du journal. Brève description de la connexion.
      vi. Commentaires. Brève description de l'URL de la liste de blocage.
      vii. Cliquez sur **OK**.



5. Cliquez sur **Update**.
6. Cliquez sur **Terminé**.



Configuration de la réputation IP à l'aide de l'interface graphique Citrix ADC

Cette configuration est une condition préalable à la fonctionnalité de réputation IP des bots. La technique de détection vous permet d'identifier toute activité malveillante provenant d'une adresse IP entrante. Dans le cadre de la configuration, nous définissons différentes catégories de bots malveillants et associons une action de bot à chacune d'entre elles. Effectuez la procédure suivante pour configurer la technique de réputation IP.

1. Accédez à **Sécurité** > **Citrix Bot Management** and **Profiles**.
2. Sur la page **Profils de gestion des bots Citrix**, sélectionnez un fichier de signature et cliquez sur **Modifier**.
3. Sur la page **Profil Citrix Bot Management**, accédez à la section **Signature Settings (Paramètres de signature**) et cliquez sur **IP Reputation**.
4. Dans la section **Réputation IP**, définissez les paramètres suivants :
   a) Activé. Activez cette case à cocher pour valider le trafic de bots entrant dans le cadre du processus de détection.
   b) Configurez les catégories. Vous pouvez utiliser la technique de réputation IP pour le trafic entrant des robots dans différentes catégories. En fonction de la catégorie configurée, vous pouvez supprimer ou rediriger le trafic du bot. Cliquez sur **Ajouter** pour configurer une catégorie de robots malveillants.
   c) Dans la page **Configurer la liaison de réputation IP du profil Citrix Bot Management**, définissez les paramètres suivants :
      i. Catégorie. Sélectionnez une catégorie de bots malveillants dans la liste. Associez une action de robot en fonction de la catégorie.
      ii. Activé. Cochez la case pour valider la détection de signature de réputation IP.

iii. Action de robot. En fonction de la catégorie configurée, vous ne pouvez attribuer aucune action, suppression, redirection, atténuation ou action CAPTCHA.
iv. Bûche. Activez la case à cocher pour stocker les entrées du journal.
v. Message du journal. Brève description du journal.
vi. Commentaires. Brève description de la catégorie de robots.

5. Cliquez sur **OK**.
6. Cliquez sur **Update**.
7. Cliquez sur **Terminé**.



Configurez la limite de débit des robots à l'aide de l'interface graphique Citrix ADC

Cette technique de détection vous permet de bloquer les robots en fonction du nombre de demandes reçues dans un délai prédéfini à partir d'une adresse IP client, d'une session ou d'une ressource configurée (par exemple, à partir d'une URL). Pour configurer la technique de limite de débit, procédez comme suit.

1. Accédez à **Sécurité** > **Citrix Bot Management** and **Profiles**.
2. Sur la page **Profils de gestion des bots Citrix**, sélectionnez un fichier de signature et cliquez sur **Modifier**.
3. Sur la page **Profil de gestion des robots Citrix**, accédez à la section **Paramètres de signature** et cliquez sur **Limite de taux**.
4. Dans la section **Limite de taux**, définissez les paramètres suivants :

   a) Activé. Cochez la case pour valider le trafic de bots entrant dans le cadre du processus de détection.

b) Séance. Demandes de limite de débit en fonction d'une session. Cliquez sur Ajouter pour configurer les demandes de limite de débit en fonction d'une session.

c) Dans la page **Configurer la limite de débit de signature Citrix Bot Management**, définissez les paramètres suivants.

i. Catégorie. Sélectionnez une catégorie de bots malveillants dans la liste. Associez une action en fonction de la catégorie.

ii. Activé. Cochez la case pour valider le trafic de bots entrant.

iii. Action de robot. Choisissez une action de robot pour la catégorie sélectionnée.

iv. Bûche. Activez la case à cocher pour stocker les entrées du journal.

v. Message du journal. Brève description du journal.

vi. Commentaires. Brève description de la catégorie de robots.

vii. Cliquez sur **OK**.



5. Cliquez sur **Update**.
6. Cliquez sur **Terminé**.



Configuration de la technique d'empreinte digitale de l'appareil à l'aide de l'interface graphique Citrix ADC

Cette technique de détection envoie un défi de script Java au client et extrait les informations du périphérique. En fonction des informations de l'appareil, la technique supprime ou contourne le trafic du bot. Suivez les étapes pour configurer la technique de détection.

1. Accédez à **Sécurité** > **Citrix Bot Management** and **Profiles**.
2. Sur la page **Profils de gestion des bots Citrix**, sélectionnez un fichier de signature et cliquez sur **Modifier**.
3. Sur la page **Profil de gestion des robots Citrix**, accédez à la section **Paramètres de signature** et cliquez sur **Empreinte digitale du périphérique**.
4. Dans la section **Device Fingerprint**, définissez les paramètres suivants :
   a) Activé. Définissez cette option pour activer la règle.
   b) Configuration. Pour l'empreinte digitale de périphérique donnée, n'attribuez aucune action, suppression ou redirection, atténuation ou action CAPTCHA.
   c) Bûche. Activez la case à cocher pour stocker les entrées du journal.
5. Cliquez sur **Update**.
6. Cliquez sur **Terminé**.



Configuration de la technique d'empreinte digitale de l'appareil pour les applications mobiles (Android)

La technique d'empreinte digitale du périphérique détecte un trafic entrant en tant que bot en insérant un script JavaScript dans la réponse HTML au client. Le script JavaScript, lorsqu'il est appelé par le navigateur, collecte les attributs du navigateur et du client et envoie une demande à la solution matérielle-logicielle. Les attributs sont examinés pour déterminer si le trafic est un bot ou un humain.

La technique de détection est encore étendue pour détecter les bots sur une plateforme mobile (Android). Contrairement aux applications Web, dans le trafic mobile (Android), la détection des bots basée sur un script JavaScript ne s'applique pas. Pour détecter les bots dans un réseau mobile, la technique utilise un SDK mobile de bot intégré aux applications mobiles côté client. Le SDK intercepte le trafic mobile, collecte les détails de l'appareil et envoie les données à l'appliance. Du côté de l'appliance, la technique de détection examine les données et détermine si la connexion provient d'un bot ou d'un humain.

Fonctionnement de la technique d'empreinte digitale de l'appareil pour une application mobile

Les étapes suivantes expliquent le flux de travail de détection des bots permettant de détecter si une demande émanant d'un appareil mobile provient d'un humain ou d'un robot.

1. Lorsqu'un utilisateur interagit avec une application mobile, le comportement de l'appareil est enregistré par le SDK mobile de robot.
2. Le client envoie une demande à l'appliance Citrix ADC.
3. Lors de l'envoi de la réponse, la solution matérielle-logicielle insère un cookie de session de bot avec les détails de la session et les paramètres pour collecter les paramètres du client.

4. Lorsque l'application mobile reçoit la réponse, le kit SDK de robot Citrix qui est intégré à l'application mobile valide la réponse, récupère les paramètres d'empreinte digitale de l'appareil enregistrés et l'envoie à l'appliance.
5. La technique de détection des empreintes digitales de l'appareil côté appliance valide les détails de l'appareil et met à jour le cookie de session de bot s'il s'agit d'un robot suspecté ou non.
6. Lorsque le cookie a expiré ou que la protection par empreinte digitale de l'appareil préfère valider et collecter périodiquement les paramètres de l'appareil, toute la procédure ou le défi est répété.

Prérequis

Pour commencer à utiliser la technique de détection des empreintes digitales des appareils Citrix ADC pour les applications mobiles, vous devez télécharger et installer le SDK mobile bot dans votre application mobile.

Configuration de la technique de détection des empreintes digitales pour les applications mobiles (Android) à l'aide de la CLI

À l'invite de commandes, tapez :

```
set bot profile <profile name> -deviceFingerprintMobile ( NONE | Android )
```

Exemple :

```
set bot profile profile 1 -deviceFingerprintMobile Android
```

Configurer la technique de détection des empreintes digitales de l'appareil pour les applications mobiles (Android) à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Citrix Bot Management** and **Profiles**.
2. Sur la page **Profils de gestion des bots Citrix**, sélectionnez un fichier et cliquez sur **Modifier**.
3. Sur la page **Citrix Bot Management Profile**, cliquez sur **Device Fingerprint** sous **Paramètres du profil**.
4. Dans la section **Configure Bot Mobile SDK**, sélectionnez le type de client mobile.
5. Cliquez sur **Mettre à jour** et **terminé**.



Configurer l'expression du journal des robots

Si le client est identifié comme un robot, la gestion des robots Citrix vous permet de capturer des informations supplémentaires sous forme de messages de journal. Les données peuvent être le nom de l'utilisateur qui a demandé l'URL, l'adresse IP source et le port source à partir duquel l'utilisateur a envoyé la demande ou les données générées à partir d'une expression. Pour effectuer une journalisation personnalisée, vous devez configurer une expression de journal dans le profil de gestion des robots.

Liez l'expression de journal dans le profil de robot à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind bot profile <name> (-logExpression -name <string> -expression <
    expression> [-enabled ( ON | OFF )]) -comment <string>
<!--NeedCopy-->
```

Exemple :

```
bind bot profile profile1 -logExpression exp1 -expression HTTP.REQ.URL -
enabled ON -comment "testing log expression"
```

Lier l'expression de journal au profil de bot à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Bot Management > Profils**.
2. Sur la page **Profils de gestion Citrix Bot**, sélectionnez **Expressions de journal de bots** dans la section **Paramètres du profil** .
3. Dans la section Paramètres d'expression du journal de **bots*, cliquez sur **Ajouter**.
4. Dans la page **Configure Citrix Bot Management Profile Bot Log Expression Binding**, définissez les paramètres suivants.

a) Nom de l'expression du journal. Nom de l'expression du journal.
b) Expression. Saisissez l'expression de journal.
c) Activé. Activez ou désactivez la liaison de l'expression de journal.
d) Commentaires. Une brève description de la liaison d'expression du journal de bot.

5. Cliquez sur**OK** et sur **Terminé**.



Configurer la technique de piège bot

La technique d'interruption de robot Citrix insère de manière aléatoire ou périodique une URL d'interruption dans la réponse du client. Vous pouvez également créer une liste d'URL de déroutement et ajouter des URL pour cela. L'URL apparaît invisible et inaccessible si le client est un utilisateur humain. Toutefois, si le client est un robot automatisé, l'URL est accessible et lorsqu'on y accède, l'attaquant est classé comme robot et toute demande ultérieure du bot est bloquée. La technique du piège est efficace pour bloquer les attaques des robots.

L'URL de déroutement est une URL alphanumérique de longueur configurable et elle est générée automatiquement à un intervalle configurable. La technique vous permet également de configurer une URL d'injection d'interruption pour les sites Web les plus visités ou les sites Web fréquemment visités.

Ce faisant, vous pouvez spécifier l'objectif d'injection de l'URL d'interruption de bot pour les requêtes correspondant à l'URL d'injection de déroutement.

> **Remarque :**
>
> Bien que l'URL d'interruption de bot soit générée automatiquement, la gestion des bots Citrix ADC vous permet toujours de configurer une URL d'interruption personnalisée dans le profil de bot. Ceci est fait pour renforcer
> la technique de détection des bots et rendre plus difficile l'accès des attaquants à l'URL de trap.

Pour terminer la configuration du bot trap, vous devez suivre les étapes suivantes.

1. Activer l'URL de bot-trap
2. Configurer l'URL d'interruption de bot dans le profil de bot
3. Liaison de l'URL d'injection de bot-trap au profil de bot
4. Configurer la longueur et l'intervalle de l'URL d'interruption de bots dans les paramètres

Activer la protection des URL de bot-trap

Avant de commencer, vous devez vous assurer que la protection de l'URL de déroutement de bots est activée sur l'appliance. À l'invite de commandes, tapez :

```
enable ns feature Bot
```

Configurer l'URL d'interruption de bot dans le profil de bot

Vous pouvez configurer l'URL de l'interruption de bot et spécifier une action d'interruption dans le profil du bot.
À l'invite de commandes, tapez :

```
add bot profile <name> -trapURL <string> -trap ( ON | OFF )-trapAction <
trapAction>
```

Où,

`trapURL`. URL utilisée par la protection contre les bots comme URL de déroutement. Longueur maximale : 127

`trap`. Activez la détection des bots trap. Valeurs possibles : ON, OFF, Valeur par défaut : OFF

`trapAction`. Action à prendre en fonction de la détection des bots. Valeurs possibles : NONE, LOG, DROP, REDIRECT, RESET, MITIGATION. Valeur par défaut : AUCUN

Exemple :

```
add bot profile profile1 -trapURL www.bottrap1.com trap ON -trapAction
RESET
```


Liaison de l'URL d'injection de bot-trap au profil de bot

Vous pouvez configurer l'URL d'injection de bot trap et la lier au profil de bot.
À l'invite de commandes, tapez :

```
bind bot profile <profile_name> trapInjectionURL -url <url> -enabled ON|OFF
-comment <comment>
```

Où,

URL. Request URL regex pattern pour lequel l'URL d'interruption de bot est insérée. Longueur maximale : 127

Exemple :

```
bind bot profile profile1 trapInjectionURL -url www.example.com -enabled ON
-comment insert a trap URL randomly
```

Configurer la longueur et l'intervalle de l'URL d'interruption de bots dans les paramètres

Vous pouvez configurer la longueur de l'URL de l'interruption de bot et également définir l'intervalle de génération automatique de l'URL d'interruption de bot.
À l'invite de commandes, tapez :

```
set bot settings -trapURLAutoGenerate ( ON | OFF )-trapURLInterval <positive_integer
> -trapURLLength <positive_integer>
```

Où,

trapURLInterval. Durée en secondes après laquelle l'URL de l'interruption de bot est mise à jour. Valeur par défaut : 3600, Valeur minimale : 300, Valeur maximale : 86400

trapURLLength. Longueur de l'URL d'interruption de bots générée automatiquement. Valeur par défaut : 32, Valeur minimale : 10, Valeur maximale : 255

Exemple :

```
set bot settings -trapURLAutoGenerate ON -trapURLInterval 300 -trapURLLength
 60
```

Configurer l'URL de bot-trap à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Bot Management > Profils**.
2. Dans la page **Profils de gestion des bots Citrix**, cliquez sur **Modifier** pour configurer la technique d'URL de déroutement de robot.
3. Dans la page **Créer un profil de gestion des bots Citrix**, saisissez l'URL de l'interruption de bot dans la section générale.



4. Dans la page **Créer un profil Citrix Bot Management**, cliquez sur **Bot Trapdans les paramètres du profil**.
5. Dans la section **Bot Trap**, définissez les paramètres suivants.

   a. Activé. Activez la case à cocher pour activer la détection des déroutement de robots
   b. Description. Brève description de l'URL.
   c. Configurez les actions. Action à entreprendre pour le bot détecté par l'accès au bot-trap.



6. Dans la section **Configurer les URL d'insertion de déroutement**, cliquez sur **Ajouter**.
7. Dans la page **Configurer la liaison d'interruption de bot Trap de profil Citrix Bot Manage-**

ment, définissez les paramètres suivants.

a) URL de déroutement. Tapez l'URL que vous souhaitez confirmer en tant qu'URL d'injection de bots trap.
b) Activé. Activez ou désactivez l'URL d'injection de bots trap.
c) Comment. Une brève description de l'URL d'injection de déroutement.



8. Dans la section **Paramètres de signature**, cliquez sur **Bot Trap**.
9. Dans la section **Bot Trap**, définissez les paramètres suivants :
   a) Activé. Cochez la case pour activer la détection des bots trap.
   b) Dans la section Configurer, définissez les paramètres suivants.
      i. Action : Action à entreprendre pour le bot détecté par l'accès au bot-trap.
      ii. Bûche. Activez ou désactivez la journalisation pour la liaison de bots trap.
10. Cliquez sur **Mettre à jour** et **terminé**.

Configurer les paramètres de l'URL de l'interruption

Effectuez les étapes suivantes pour configurer les paramètres de l'URL d'interruption de bot :

1. Accédez à **Sécurité > Citrix Bot Management**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres de gestion des robots Citrix**.
3. Dans la **section Configurer les paramètres de gestion des bots Citrix**, définissez les paramètres suivants.
   a) Intervalle d'URL d'interruption. Durée en secondes après laquelle l'URL de l'interruption de bot est mise à jour.

b) Longueur de l'URL de déroutement. Longueur de l'URL d'interruption de bots générée automatiquement.

4. Cliquez sur **OK** et **Terminé**.



Expression de stratégie IP client pour la détection de robots

La gestion des robots Citrix vous permet désormais de configurer une expression de stratégie avancée pour extraire l'adresse IP du client à partir d'un en-tête de requête HTTP, d'un corps de requête HTTP, d'une URL de requête HTTP ou d'une expression de stratégie avancée. La valeur extraite peut être utilisée par un mécanisme de détection de bot (tel que TPS, piège de bot ou limite de débit) pour détecter si la demande entrante est un bot.

> **Remarque :**
>
> Si vous n'avez pas configuré d'expression IP client, l'adresse IP du client source par défaut ou existante est utilisée pour la détection des robots. Si une expression est configurée, le résultat de l'évaluation fournit l'adresse IP du client pouvant être utilisée pour la détection des robots.

Vous pouvez configurer et utiliser l'expression IP du client pour extraire l'adresse IP du client réelle si la demande entrante passe par un serveur proxy et si l'adresse IP du client est présente dans l'en-tête. En ajoutant cette configuration, l'appliance peut utiliser le mécanisme de détection des robots pour assurer une sécurité accrue aux clients et serveurs logiciels.

Configurer l'expression de stratégie IP du client dans le profil de robot à l'aide de l'interface de ligne

À l'invite de commandes, tapez :

```
add bot profile <name> [-clientIPExpression <expression>]
<!--NeedCopy-->
```

Exemple :

```
add bot profile profile1 -clientIPExpression 'HTTP.REQ.HEADER("X-Forwarded-For")ALT CLIENT.IP.SRC.TYPECAST_TEXT_T'
```

Configurer l'expression de stratégie IP du client dans le profil de robot à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Bot Management > Profils**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer un profil de gestion Citrix Bot**, définissez l'expression IP du client.
4. Cliquez sur **Créer** et **Fermer**.



Configurer CAPTCHA pour la réputation IP et la détection des empreintes digitales des périphériques

CAPTCHA est un acronyme qui signifie « Completely Automated Public Turing test to tell Computers and Humans Apart ». CAPTCHA est conçu pour tester si un trafic entrant provient d'un utilisateur humain ou d'un robot automatisé. CAPTCHA permet de bloquer les bots automatisés qui causent des violations de sécurité aux applications Web. Dans l'appliance ADC, CAPTCHA utilise le module challenge-réponse pour identifier si le trafic entrant provient d'un utilisateur humain et non d'un robot automatisé.

Configurer les signatures statiques des robots

Cette technique de détection vous permet d'identifier les informations de l'agent utilisateur à partir des détails du navigateur. Sur la base des informations de l'agent utilisateur, le bot est identifié comme un bot mauvais ou bon, puis vous lui attribuez une action de bot. Suivez les étapes ci-dessous pour configurer la technique de signature statique :

1. Dans le volet de navigation, développez **Sécurité > Citrix Bot Management > Signatures**.
2. Dans la page **Citrix Bot Management Signatures**, sélectionnez un fichier de signatures et cliquez sur **Edit**.
3. Sur la page **Signature de Citrix Bot Management**, accédez à la section **Signature Settings (Paramètres de signature**), puis cliquez sur **Bot Signatures**.
4. Dans la section **Bot Signatures**, définissez les paramètres suivants :
    a) Configurer les signatures statiques. Cette section contient une liste d'enregistrements de signatures statiques de robots. Vous pouvez sélectionner un enregistrement et cliquer sur **Modifier** pour lui attribuer une action de robot.
    b) Cliquez sur **OK**.
5. Cliquez sur **Mettre à jour la signature**.
6. Cliquez sur **Terminé**.



Délimitation des signatures statiques

La gestion des robots Citrix ADC protège votre application Web contre les robots. Les signatures statiques des bots aident à identifier les robots bons et défectueux en fonction de paramètres de requête tels que l'agent utilisateur dans la demande entrante.
La liste des signatures dans le fichier est énorme et de nouvelles règles sont ajoutées et les règles périmées sont supprimées périodiquement. En tant qu'administrateur, il se peut que vous souhaitiez rechercher une signature spécifique ou une liste de signatures sous une catégorie. Pour filtrer facilement les signatures, la page de signature du bot offre une fonctionnalité de recherche améliorée. La fonction de recherche vous permet de trouver des règles de signature et de configurer sa propriété en fonction d'un ou de plusieurs paramètres de signature tels que l'action, l'ID de signature, le développeur et le nom de la signature.

Action : Sélectionnez une action de bot que vous préférez configurer pour une catégorie spécifique de règles de signature. Les types d'action disponibles sont les suivants :

- Activez Selected. Activez toutes les règles de signature sélectionnées.
- Désactivez la sélection. Désactivez toutes les règles de signatures sélectionnées.
- Déposer la sélection. Sélectionnez l'action comme « Déposer » vers toutes les règles de signature sélectionnées.
- Redirection sélectionnée. Appliquez l'action en tant que « Redirection » à toutes les règles de signature sélectionnées.
- Réinitialiser la sélection. Appliquez l'action « Réinitialiser » à toutes les règles de signature sélectionnées.
- Journal sélectionné. Appliquez l'action en tant que « journal » à toutes les règles de signature sélectionnées.

- Supprimer Drop Selected. Définissez l'action de dépôt sur toutes les règles de signature sélectionnées.
- Supprimer la redirection sélectionnée. Définissez l'action de redirection sur toutes les règles de signature sélectionnées.
- Supprimer Réinitialiser la sélection. Définissez l'action de réinitialisation sur toutes les règles de signature sélectionnées.
- Supprimer le journal sélectionné. Définissez l'action de journal sur toutes les règles de signature sélectionnées.

Catégorie. Sélectionnez une catégorie pour filtrer les règles de signature en conséquence. Vous trouverez ci-dessous la liste des catégories disponibles pour le tri des règles de signature.

- Action : Triez en fonction de l'action du bot.
- Catégorie. Triez en fonction de la catégorie de robots.
- Développeur. Triez en fonction de l'éditeur de la société hôte.
- Activé. Triez en fonction des règles de signature activées.
- ID. Triez en fonction de l'ID de règle de signature.
- Bûche. Triez en fonction des règles de signature pour lesquelles la journalisation est activée.
- Name. Triez en fonction du nom de la règle de signature.
- Tapez. Triez en fonction du type de signature.
- Version. Trier en fonction de la version de la règle de signature.

Rechercher les règles de signature statique des robots en fonction des types d'actions et de catégories à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité > Citrix Bot Management > Signature**.
2. Dans la page de détails, cliquez sur **Ajouter**.
3. Dans la page **Signatures Citrix Bot Management**, cliquez sur Modifier dans la section **Signature statique** .
4. Dans la section **Configurer la signature statique**, sélectionnez une action de signature dans la liste déroulante.
5. Utilisez la fonction de recherche pour sélectionner une catégorie et filtrer les règles en conséquence.
6. Cliquez sur **Update**.



Modifiez la propriété de règle de signature statique du bot à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité > Citrix Bot Management > Signature**.
2. Dans la page de détails, cliquez sur **Ajouter**.
3. Dans la page **Signatures Citrix Bot Management**, cliquez sur Modifier dans la section **Signature statique** .
4. Dans la section **Configurer la signature statique**, sélectionnez une action dans la liste déroulante.
5. Utilisez la fonction de recherche pour sélectionner une catégorie et filtrer les règles en conséquence.
6. Dans la liste de signatures statiques, sélectionnez une signature pour modifier sa propriété.



7. Cliquez sur **OK** pour confirmer.

Fonctionnement de CAPTCHA dans la gestion des robots Citrix ADC

Dans la gestion des bots Citrix ADC, la validation CAPTCHA est configurée en tant qu'action de stratégie à exécuter après l'évaluation de la stratégie de bot. L'action CAPTCHA n'est disponible que pour les techniques de réputation IP et de détection des empreintes digitales de l'appareil. Voici les étapes à suivre pour comprendre le fonctionnement du CAPTCHA :

1. Si une violation de sécurité est observée pendant la détection de la réputation IP ou de l'empreinte digitale de l'appareil, l'appliance ADC envoie un défi CAPTCHA.
2. Le client envoie la réponse CAPTCHA.
3. La solution matérielle-logicielle valide la réponse CAPTCHA et, si le CAPTCHA est valide, la demande est autorisée et transmise au serveur principal.
4. Si la réponse CATCHA n'est pas valide, la solution matérielle-logicielle envoie un nouveau défi CAPTCHA jusqu'à ce que le nombre maximal de tentatives soit atteint.
5. Si la réponse CAPTCHA n'est pas valide, même après le nombre maximal de tentatives, la solution matérielle-logicielle abandonne ou redirige la demande vers l'URL d'erreur configurée.
6. Si vous avez configuré l'action de journalisation, la solution matérielle-logicielle stocke les détails de la demande dans le fichier ns.log.

Configurez les paramètres CAPTCHA à l'aide de l'interface graphique Citrix ADC

L'action CAPTCHA de gestion des bots n'est prise en charge que pour les techniques de réputation IP et de détection des empreintes digitales de l'appareil. Suivez les étapes suivantes pour configurer les paramètres **CAPTCHA** .

1. Accédez à **Sécurité > Citrix Bot Management and Profiles**.
2. Sur la page **Profils de gestion des bots Citrix**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page **Citrix Bot Management Profile**, accédez à la section **Signature Settings (Paramètres de signature**) et cliquez sur **CAPTCHA**.
4. Dans la section **Paramètres CAPTCHA**, cliquez sur **Ajouter pour configurer les paramètres CAPTCHA** sur le profil :
5. Dans la page **Configurer le CAPTCHA de Citrix Bot Management**, définissez les paramètres suivants.
    a) URL. URL de bot pour laquelle l'action CAPTCHA est appliquée pendant les techniques de réputation IP et de détection des empreintes digitales de l'appareil.
    b) Activé. Définissez cette option pour activer la prise en charge du CAPTCHA.
    c) L'heure de la grâce. Durée jusqu'à ce qu'aucun nouveau défi CAPTCHA n'est envoyé après la réception de la réponse CAPTCHA valide actuelle.

d) Le temps d'attente. Durée d'attente de l'appliance ADC jusqu'à ce que le client envoie la réponse CAPTCHA.

e) Période de mise en sourdine. Durée pendant laquelle le client qui a envoyé une réponse CAPTCHA incorrecte doit attendre jusqu'à ce qu'il soit autorisé à essayer ensuite. Pendant cette période de mise en sourdine, l'appliance ADC n'autorise aucune demande. Portée : 60 à 900 secondes, Recommandé : 300 secondes

f) Limite de durée de la demande. Longueur de la demande pour laquelle le challenge CAPTCHA est envoyé au client. Si la longueur est supérieure à la valeur de seuil, la demande est abandonnée. La valeur par défaut est de 10 à 3 000 octets.

g) Tentatives de nouvelle tentative. Nombre de tentatives que le client est autorisé à réessayer de résoudre le défi CAPTCHA. Plage : 1-10, Recommandé : 5.

h) Aucune action d'action/supérieur/redirection à effectuer si le client échoue à la validation CAPTCHA.

i) Bûche. Définissez cette option pour stocker les informations de demande du client en cas d'échec du CAPTCHA de réponse. Les données sont stockées dans `ns.log` un fichier.

j) Comment. Une brève description de la configuration CAPTCHA.

6. Cliquez sur **OK** et **Terminé**.



7. Accédez à **Sécurité > Citrix Bot Management > Signatures**.
8. Dans la page **Citrix Bot Management Signatures**, sélectionnez un fichier de signatures et cliquez sur **Edit**.
9. Sur la page **Signature Citrix Bot Management**, accédez à la section **Signature Settings (Paramètres de signature**) et cliquez sur **Bot Signatures**.
10. Dans la section **Bot Signatures**, définissez les paramètres suivants :
11. Configurez les **signatures statiques**. Sélectionnez un enregistrement de signature statique de robot et cliquez sur Modifier pour lui attribuer une action de robot.
12. Cliquez sur **OK**.
13. Cliquez sur **Mettre à jour la signature**.
14. Cliquez sur **Terminé**.



Mise à jour automatique des signatures de bots

La technique de signature statique des bots utilise une table de recherche de signature avec une liste de bons bots et de mauvais robots. Les robots sont classés en fonction de la chaîne de l'agent utilisateur et des noms de domaine. Si la chaîne de l'agent utilisateur et le nom de domaine dans le trafic de bot entrant correspondent à une valeur de la table de recherche, une action de bot configurée est appliquée.

Les mises à jour des signatures de bots sont hébergées sur le cloud AWS et la table de recherche de signature communique avec la base de données AWS pour les mises à jour des signatures. Le planificateur de mise à jour automatique des signatures s'exécute toutes les heures pour vérifier la **base de données AWS** et mettre à jour la table des signatures dans l'appliance Citrix ADC.

L'URL de mise à jour automatique de signature à configurer est la suivante : `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`

> **Remarque :**
>
> Vous pouvez également configurer un serveur proxy et mettre à jour périodiquement les signatures depuis le cloud AWS vers l'appliance via le proxy. Pour la configuration du proxy, vous devez définir l'adresse IP et l'adresse du port du proxy dans les paramètres du bot.

Fonctionnement de la mise à jour automatique de signature

Le diagramme suivant montre comment les signatures de robots sont récupérées à partir du cloud AWS, mises à jour sur Citrix ADC et affichées sur Citrix ADM pour obtenir un résumé de la mise à jour des signatures.

Le planificateur de mise à jour automatique des signatures de bot effectue les opérations suivantes :

1. Récupère le fichier de mappage à partir de l'URI AWS.
2. Vérifie les dernières signatures du fichier de mappage avec les signatures existantes dans l'appliance ADC.
3. Télécharge les nouvelles signatures depuis AWS et vérifie l'intégrité de la signature.
4. Met à jour les signatures de bots existantes avec les nouvelles signatures dans le fichier de signature du bot.
5. Génère une alerte SNMP et envoie le résumé de la mise à jour des signatures à Citrix ADM.

Configurer la mise à jour automatique de

Pour configurer la mise à jour automatique de la signature du bot, procédez comme suit :

Activer la mise à jour automatique de signature

Vous devez activer l'option de mise à jour automatique dans les paramètres du bot sur l'appliance ADC.
À l'invite de commandes, tapez :

```
set bot settings -signatureAutoUpdate ON
```

Configurer les paramètres du serveur proxy (facultatif)

Si vous accédez à la base de données de signatures AWS via un serveur proxy, vous devez configurer le serveur proxy et le port.

```
set bot settings -proxyserver -proxyport
```

Exemple :

```
set bot settings -proxy server 1.1.1.1 -proxyport 1356
```

Configuration de la mise à jour automatique de la signature du bot à l'aide de l'interface graphique Citrix ADC

Suivez les étapes suivantes pour configurer la mise à jour automatique de la signature du bot :

1. Accédez à **Sécurité > Citrix Bot Management**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres de gestion des robots Citrix**.
3. Dans les **paramètres Configurer Citrix Bot Management**, cochez la case **Signature de mise à jour automatique** .



4. Cliquez sur **OK** et sur **Fermer**.

Créer un profil de gestion des bots

Un profil de bot est un ensemble de paramètres de gestion des bots utilisés pour détecter le type de bot. Dans un profil, vous déterminez comment le Web App Firewall applique chacun de ses filtres (ou vérifications) au trafic des robots vers vos sites Web, ainsi que les réponses de ceux-ci.

Pour configurer le profil de bot, procédez comme suit :

1. Accédez à **Sécurité** > **Citrix Bot Management** > **Profils**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer un profil de gestion des bots Citrix**, définissez les paramètres suivants.
   a) Name. Nom du profil du bot.
   b) Signature. Nom du fichier de signature du bot.
   c) URL d'erreur. URL pour les redirections.
   d) Comment. Brève description du profil.
4. Cliquez sur **Créer** et **Fermer**.



Créer une stratégie de bot

La stratégie de bot contrôle le trafic acheminé vers le système de gestion des bots et contrôle également les journaux de bots envoyés au serveur de journaux d'audit. Suivez la procédure pour configurer la stratégie de bot.

1. Accédez à **Sécurité** > **Citrix Bot Management** > **Stratégies de bot**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer une stratégie de gestion des bots Citrix**, définissez les paramètres suivants.
   a) Name. Nom de la stratégie Bot.
   b) Expression. Tapez l'expression ou la règle de stratégie directement dans la zone de texte.
   c) Profil de bot. Profil de bot pour appliquer la stratégie de bot.
   d) Action non définie. Sélectionnez une action que vous préférez attribuer.
   e) Comment. Brève description de la stratégie.
   f) Action de journalisation. Action de message du journal d'audit pour la journalisation du trafic des robots. Pour plus d'informations sur l'action du journal d'audit, consultez la rubrique Journalisation d'audit.
4. Cliquez sur **Créer** et **Fermer**.



Transactions de bots par seconde (TPS)

La technique de robot Transactions Per Second (TPS) détecte le trafic entrant en tant que bot si le nombre de requêtes par seconde (RPS) et le pourcentage d'augmentation du RPS dépassent la valeur de seuil configurée. La technique de détection protège vos applications Web contre les bots automatisés qui peuvent provoquer des activités de grattage Web, une connexion par forçage brute et d'autres attaques malveillantes.

> **Remarque :**
>
> La technique de bot détecte un trafic entrant en tant que bot uniquement si les deux paramètres

> sont configurés et si les deux valeurs dépassent la limite de seuil.
> Considérons un scénario dans lequel l'appliance reçoit de nombreuses requêtes provenant d'une URL spécifique et vous souhaitez que la gestion des bots Citrix ADC détecte s'il y a une attaque de bot. La technique de détection TPS examine le nombre de demandes (valeur configurée) provenant de l'URL en moins d'une seconde et l'augmentation en pourcentage (valeur configurée) du nombre de demandes reçues en 30 minutes. Si les valeurs dépassent la limite de seuil, le trafic est considéré comme un robot et la solution matérielle-logicielle exécute l'action configurée.

Configurer la technique des transactions de bot par seconde (TPS)

Pour configurer TPS, vous devez effectuer les étapes suivantes :

1. Activer le bot TPS
2. Liaison des paramètres TPS au profil de gestion des bots

Liaison des paramètres TPS au profil de gestion des bots

Une fois que vous avez activé la fonctionnalité TPS de robot, vous devez lier les paramètres TPS au profil de gestion des robots.

À l'invite de commandes, tapez :

```
bind bot profile <name>… (-tps [-type ( SourceIP | GeoLocation | RequestURL
 | Host )] [-threshold <positive_integer>] [-percentage <positive_integer
>] [-action ( none | log | drop | redirect | reset | mitigation )] [-
logMessage <string>])
```

Exemple :

```
bind bot profile profile1 -tps -type RequestURL -threshold 1 -percentage
100000 -action drop -logMessage log
```

Activer la transaction de robot par seconde (TPS)

Avant de commencer, vous devez vous assurer que la fonctionnalité Bot TPS est activée sur la solution matérielle-logicielle. À l'invite de commandes, tapez :

```
set bot profile profile1 -enableTPS ON
```

Configurez les transactions de robot par seconde (TPS) à l'aide de l'interface graphique Citrix ADC

Suivez les étapes suivantes pour configurer les transactions de bot par seconde :

1. Accédez à **Sécurité > Citrix Bot Management > Profils**.
2. Dans la page **Profils de gestion des bots Citrix**, sélectionnez un profil et cliquez sur **Modifier**.
3. Dans la page **Créer un profil de gestion des bots Citrix**, cliquez sur **TPS** sous la section **Paramètres de signature** .
4. Dans la section **TPS**, activez la fonctionnalité et cliquez sur **Ajouter**.



5. Dans la page **Configurer la liaison TPS du profil Citrix Bot Management**, définissez les paramètres suivants.
   a) Tapez. Types d'entrée autorisés par la technique de détection. Valeurs possibles : IP SOURCE, GÉOLOCALISATION, HÔTE, URL.

      SOURCE_IP — TPS basé sur l'adresse IP du client.

      GÉOLOCALISATION — TPS en fonction de l'emplacement géographique du client.

      HOST - TPS basé sur les demandes des clients transférées vers une adresse IP de serveur principal spécifique.

      URL : TPS basé sur les demandes des clients provenant d'une URL spécifique.

   b) Seuil fixe. Nombre maximal de requêtes autorisées à partir d'un type d'entrée TPS dans un intervalle de temps d'une seconde.

   c) Seuil de pourcentage. Augmentation maximale en pourcentage des demandes provenant d'un type d'entrée TPS dans un intervalle de 30 minutes.

   d) Action : Action à entreprendre pour le bot détecté par la liaison TPS.

   e) Bûche. Activez ou désactivez la journalisation pour la liaison TPS.

   f) Message du journal. Message à consigner pour le bot détecté par la liaison TPS. Longueur maximale : 255.

   g) Commentaires. Une brève description de la configuration du TPS. Longueur maximale : 255

6. Cliquez sur **OK**, puis sur **Fermer**.



Détection de robots basée sur la dynamique de la souris et du clavier

Pour détecter les robots et atténuer les anomalies de grattage Web, la gestion des robots Citrix ADC utilise une technique améliorée de détection des robots basée sur le comportement de la souris et du clavier. Contrairement aux techniques de robots classiques qui nécessitent une interaction humaine directe (par exemple, la validation CAPTCHA), la technique améliorée surveille passivement la dynamique de la souris et du clavier. L'appliance Citrix ADC collecte ensuite les données utilisateur en temps réel et analyse le comportement entre un humain et un bot.

La détection passive des robots utilisant la dynamique de la souris et du clavier présente les avantages suivants par rapport aux mécanismes de détection de robots existants :

- Assure une surveillance continue tout au long de la session utilisateur et élimine un point de contrôle unique.
- Ne nécessite aucune interaction humaine et il est totalement transparent pour les utilisateurs.

Fonctionnement de la détection des robots à l'aide de la dynamique de la souris

La technique de détection des robots utilisant la dynamique du clavier et de la souris se compose de deux composants, un enregistreur de pages Web et un détecteur de robots. L'enregistreur de pages Web est un code JavaScript qui enregistre les mouvements du clavier et de la souris lorsqu'un utilisateur effectue une tâche sur la page Web (par exemple, en remplissant un formulaire d'inscription). L'enregistreur envoie ensuite les données par lots à l'appliance Citrix ADC. L'appliance stocke ensuite

les données sous forme d'enregistrement KM et les envoie au détecteur de robots sur le serveur Citrix ADM, qui analyse si l'utilisateur est un humain ou un robot.

Les étapes suivantes expliquent comment les composants interagissent entre eux :

1. L'administrateur Citrix ADC configure l'expression de stratégie via ADM StyleBook, CLI ou NITRO ou toute autre méthode.
2. L'URL est définie dans le profil du bot lorsque l'administrateur active la fonctionnalité sur l'appliance.
3. Lorsqu'un client envoie une demande, l'appliance Citrix ADC suit la session et toutes les demandes de la session.
4. L'appliance insère un code JavaScript (enregistreur de page Web) dans la réponse si la demande correspond à l'expression configurée sur le profil du bot.
5. Le JavaScript collecte ensuite toute l'activité du clavier et de la souris et envoie les données KM dans une URL POST (transitoire).
6. L'appliance Citrix ADC stocke les données et les envoie au serveur Citrix ADM à la fin de la session. Une fois que l'appliance reçoit les données complètes d'une demande POST, les données sont envoyées au serveur ADM.
7. La plateforme CAS analyse les données et, sur la base de l'analyse, le résultat est disponible sur l'interface graphique Citrix ADM.

L'enregistreur JavaScript enregistre les mouvements suivants de la souris et du clavier :

- Événements clavier — tous les événements
- Événements de souris - déplacement de la souris, souris vers le haut, souris vers le bas
- Événements Presse-papiers - coller
- Événements personnalisés - remplissage automatique, annulation automatique
- horodatage de chaque événement

Configurer la détection de bots à l'aide de la dynamique de

La configuration de gestion des robots Citrix ADC inclut l'activation ou la désactivation de la fonction de détection basée sur le clavier et la souris, et configure l'URL JavaScript dans le profil de robot. Procédez comme suit pour configurer la détection des robots à l'aide de la dynamique de la souris et du clavier :

1. Activer la détection basée sur le clavier et la souris
2. Configurer l'expression pour décider quand le JavaScript peut être injecté dans la réponse HTTP

Activer la détection des robots basée sur la souris clavier

Avant de commencer la configuration, assurez-vous d'avoir activé la fonctionnalité de détection de robots basée sur le clavier et la souris sur l'appliance.

À l'invite de commandes, tapez :

```
1 add bot profile <name> -KMDetection ( ON | OFF )
2 <!--NeedCopy-->
```

Exemple :

```
add bot profile profile1 -KMDetection ON
```

Configurer l'expression de bot pour l'insertion JavaScript

Configurez l'expression du bot pour évaluer le trafic et insérer JavaScript. Le JavaScript est inséré uniquement si l'expression est évaluée comme true.

À l'invite de commandes, tapez :

```
1 bind bot profile <name> -KMDetectionExpr -name <string> -expression <
     expression> -enabled ( ON | OFF ) - comment <string>
2 <!--NeedCopy-->
```

Exemple :

```
bind bot profile profile1 -KMDetectionExpr -name test -expression http.req.
url.startswith("/testsite")-enabled ON
```

Configurer le nom de fichier JavaScript inséré dans la réponse HTTP pour la détection de bots basée sur le clavier et la souris

Pour collecter les détails de l'action de l'utilisateur, l'appliance envoie un nom de fichier JavaScript dans la réponse HTTP. Le fichier JavaScript collecte toutes les données d'un enregistrement KM et les envoie à l'appliance.

À l'invite de commandes, tapez :

```
1 set bot profile profile1 - KMJavaScriptName <string>
2 <!--NeedCopy-->
```

Exemple :

```
set bot profile profile1 -KMJavaScriptName script1
```

Configurer la taille de la biométrie comportementale

Vous pouvez configurer la taille maximale des données de comportement de la souris et du clavier qui peuvent être envoyées sous forme d'enregistrement KM à l'appliance et traitées par le serveur ADM.

À l'invite de commandes, tapez :


```
set bot profile profile1 -KMEventsPostBodyLimit <positive_integer>
<!--NeedCopy-->
```

Exemple :

```
set bot profile profile1 - KMEventsPostBodyLimit 25
```

Une fois que vous avez configuré l'appliance Citrix ADC pour configurer le JavaScript et collecter la biométrie du comportement du clavier et de la souris, l'appliance envoie les données au serveur Citrix ADM. Pour plus d'informations sur la façon dont le serveur Citrix ADM détecte les bots de la biométrie comportementale, consultez la rubrique Violations de bots .

Configurer les paramètres d'expression des robots clavier et souris à l'aide de l'interface graphique

1. Accédez à **Sécurité > Citrix Bot Management and Profiles**.
2. Sur la page **Profils de gestion des bots Citrix**, sélectionnez un profil et cliquez sur **Modifier**.
3. Dans la section **Détection de robots basée sur le clavier et la souris**, définissez les paramètres suivants :
   a) Activez la détection. Activez la case à cocher pour détecter le comportement dynamique du clavier et de la souris basé sur un robot.
   b) Limite de corps post-événement. Taille des données dynamiques du clavier et de la souris envoyées par le navigateur pour être traitées par l'appliance Citrix ADC.
4. Cliquez sur **OK**.



5. Sur la page **Profil Citrix Bot Management**, accédez à la section **Paramètres du profil** et cliquez sur **Paramètres d'expression de bots basés sur le clavier et la souris**.
6. Dans la section **Paramètres d'expression de bots basés sur le clavier et la souris**, cliquez sur **Ajouter**.

7. Dans la page **Configure Citrix Bot Management Profile Keyboard and Mouse Expression Binding**, définissez les paramètres suivants :

   a) Nom de l'expression. Nom de l'expression de stratégie de robot pour la dynamique de détection du clavier et de la souris.
   b) Expression. Expression de stratégie de bot.
   c) Activé. Activez la case à cocher pour activer la liaison de l'expression clavier et du bot et de la souris.
   d) Commentaires. Une brève description de l'expression de stratégie du bot et de sa liaison au profil du bot.
   e) Cliquez sur **OK** et sur **Fermer**.

8. Dans la section **Paramètres d'expression de bots basés sur le clavier et la souris**, cliquez sur **Mettre à jour**.



Journalisation verbale pour le trafic des robots

Lorsqu'une demande entrante est identifiée comme un robot, l'appliance Citrix ADC consigne plus de détails d'en-tête HTTP à des fins de surveillance et de dépannage. La fonctionnalité de journalisation verbeuse des robots est similaire à la journalisation verbeuse du module Web App Firewall.

Considérez un trafic entrant provenant d'un client. Si le client est identifié comme un robot, l'appliance Citrix ADC utilise la fonctionnalité de journalisation détaillée pour consigner les informations d'en-tête HTTP complètes (adresse de domaine, URL, en-tête d'agent utilisateur, en-tête de cookie). Les détails du journal sont ensuite envoyés au serveur ADM à des fins de surveillance et de dépannage. Le message de consignation verbeux n'est pas stocké dans le fichier "ns.log".

Configurer la journalisation verbale des robots à l'aide de l'interface de ligne de commande

Pour capturer des informations d'en-tête HTTP détaillées sous forme de journaux, vous pouvez configurer le paramètre de journalisation détaillée dans le profil de bot. À l'invite de commandes, tapez :

```
1 set bot profile <name> [-verboseLogLevel ( NONE | HTTP_FULL_HEADER ) ]
2 <!--NeedCopy-->
```

Exemple :

```
set bot profile p1 -verboseLogLevel HTTP_FULL_HEADER
```

Configurez la journalisation verbale des robots à l'aide de l'interface graphique Citrix ADC

Suivez la procédure ci-dessous pour configurer le niveau de journalisation détaillé dans le profil de bot.

1. Dans le volet de navigation, accédez à **Sécurité > Citrix Bot Management**.
2. Dans la page **Profils de gestion des bots Citrix**, cliquez sur **Ajouter**.
3. Dans la page **Créer un profil de gestion des bots Citrix**, sélectionnez le niveau de journalisation verbeux en tant qu' **en-tête complet HTTP**.
4. Cliquez sur **OK** et **Terminé**.



Gestion des bots

January 21, 2021

Voici quelques-uns des scénarios de dépannage couverts dans la gestion des bot Citrix ADC.

1. Comment gérer les cas faux positifs ?

   Vous pouvez utiliser la fonctionnalité de liste d'autorisation bot pour gérer les cas de faux positifs et ces transactions peuvent être contournées.

2. Comment trouver plus de détails sur le mauvais trafic de bot ?

   Vous pouvez utiliser la fonctionnalité de journalisation d'audit pour obtenir des détails sur le trafic classé comme bots défectueux.

3. Pourquoi devriez-vous changer le nom de signature par défaut ?

   Vous pouvez modifier le nom de signature par défaut si des conflits sont détectés au niveau des ressources de point de terminaison desservies par l'appliance Citrix ADC.

Gestion des bots

October 5, 2021

1. Qu'est-ce que la gestion des bots Citrix ADC ?

   La gestion des bots Citrix ADC détecte et distingue le trafic des bons robots, des mauvais robots et des clients humains. La fonctionnalité de gestion des bots protège vos applications Web contre les mauvais robots en appliquant une action configurée sur les demandes entrantes.

2. Pourquoi Citrix ADC doit-il gérer les bots de votre application Web ?

   Les robots malveillants représentent 30% de votre trafic Internet. Les bots malveillants ont un impact sur les applications Web de diverses manières, telles que le lancement d'une attaque DoS, le spam d'adresses e-mail, le ralentissement de l'application à l'aide de programmes de téléchargement, le téléchargement de contenu à partir de sites Web, etc. En outre, les robots peuvent facilement contourner certains des mécanismes de détection bien connus entraînant une perte de données, de revenus et de réputation pour votre organisation.

3. Quelles sont les techniques utilisées pour détecter un bot entrant ?

   L'appliance utilise des techniques de détection telles que la réputation IP, la limitation du débit, l'empreinte digitale de l'appareil, le TPS et les techniques de détection des bots. En outre, vous pouvez configurer une liste de blocage personnalisée sur l'interface graphique Citrix ADC pour catégoriser les bots défectueux spécifiques à l'organisation.

4. Qu'est-ce qu'un fichier de signature de bot et son objectif ?

   Le fichier de signature du bot contient l'empreinte des bons et des mauvais robots connus. Le fichier de signatures est mis à jour périodiquement pour inclure les dernières signatures de bots pour une meilleure protection contre les bots.

5. Quel type de licence Citrix ADC dois-je acheter ?

   La gestion des robots est disponible avec la licence ADC Premium.

6. Où puis-je trouver des journaux de bot pour le dépannage ?

   Les journaux d'audit Citrix ADC fournissent des détails sur les robots détectés. Pour plus d'informations, consultez la rubrique Audit Logging .

7. Existe-t-il une fonctionnalité de mise à jour automatique pour les fichiers de signature de bot ?

   Oui, la gestion des robots Citrix ADC prend en charge la fonctionnalité de mise à jour automatique.

8. Existe-t-il une condition préalable à l'utilisation de la technique de réputation IP des robots ?

   Activez la fonctionnalité de réputation IP avant d'activer et de configurer la réputation IP dans le profil de bot.

Articles d'alerte de signature de bot

February 12, 2021

La gestion des bots Citrix annonce les mises à jour de signature que vous pouvez télécharger et appliquer sur votre appliance. Lorsque vous détectez une attaque de bot, vous recevrez une notification par e-mail concernant la mise à jour de la nouvelle signature. Vous pouvez télécharger la signature et l'appliquer sur votre appliance.

Mise à jour de la signature du bot pour novembre 2020

October 5, 2021

De nouvelles règles de signatures sont générées pour les bots identifiés dans la semaine 2020-11-11. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre solution matérielle-logicielle contre les attaques de bots.

Version de signature du bot

Signature version 5 applicable à la plate-forme Citrix ADC 13.0.

Signatures de nouveaux robots

Vous trouverez ci-dessous une liste des règles de signature de bot, de la catégorie et de son type.

Catégorie	Type de robot	Nombre de signatures
Scraper	Bon Bot	3
Marketing	Bon Bot	23
Feed Fetcher	Bon Bot	2
Outil	Bad Bot	3
Moteur de recherche	Bon Bot	34
Crawler	Bon Bot	6
Sans catégorie	Bad Bot	6
Analyseur de virus	Bon Bot	1
Créateur de capture d'écran	Bon Bot	7
Scraper	Bad Bot	1
Outil	Bon Bot	7

Mise à jour de la signature du bot pour janvier 2021

October 5, 2021

Certaines signatures de bots existantes sont mises à jour. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre solution matérielle-logicielle contre les attaques de bots.

Version de signature du bot

Signature version 6 est applicable aux plates-formes Citrix ADC avec des versions 13.0 61.x ou ultérieures.

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

Règle de signature de bot	ID	Description
143	Crawler	Bon Bot
561	Scraper	Bon Bot
857	Moniteur de site	Bon Bot
892	Moniteur de site	Bad Bot
894	Moniteur de site	Bad Bot
980	Scraper	Bad Bot
1025	Moniteur de site	Bad Bot
1029	Feed Fetcher	Bad Bot
1030	Créateur de capture d'écran	Bad Bot
1034	Outil	Bad Bot
1039	Marketing	Bad Bot
1042	Moniteur de site	Bad Bot
1047	Moniteur de site	Bad Bot
1053	Moniteur de site	Bad Bot
1072	Moteur de recherche	Bad Bot
1073	Feed Fetcher	Bad Bot
1074	Sans catégorie	Bad Bot
1078	Créateur de capture d'écran	Bad Bot
1109	Marketing	Bad Bot
1132	Feed Fetcher	Bad Bot
1138	Marketing	Bad Bot
1150	Moteur de recherche	Bad Bot
1164	Moteur de recherche	Bad Bot
1167	Marketing	Bad Bot
1173	Outil	Bad Bot
1174	Marketing	Bad Bot
1176	Moteur de recherche	Bad Bot

Règle de signature de bot	ID	Description
1 178	Tester de vitesse	Bad Bot
1185	Créateur de capture d'écran	Bad Bot
1209	Sans catégorie	Bad Bot
1244	Moniteur de site	Bad Bot
1251	Moteur de recherche	Bad Bot
1254	Moniteur de site	Bad Bot
1256	Sans catégorie	Bad Bot
1259	Outil	Bad Bot
1287	Moteur de recherche	Bad Bot
1296	Moteur de recherche	Bad Bot
1312	Sans catégorie	Bad Bot
1316	Marketing	Bad Bot
1322	Moniteur de site	Bad Bot
1325	Créateur de capture d'écran	Bad Bot
1328	Moteur de recherche	Bad Bot
1330	Marketing	Bad Bot
1337	Outil	Bad Bot
1360	Moteur de recherche	Bad Bot
1367	Moteur de recherche	Bad Bot
1374	Outil	Bad Bot
1380	Sans catégorie	Bad Bot
1388	Moteur de recherche	Bad Bot
1400	Feed Fetcher	Bad Bot
1413	Sans catégorie	Bad Bot
1420	Feed Fetcher	Bad Bot
1422	Moniteur de site	Bad Bot
1442	Sans catégorie	Bad Bot
1447	Moteur de recherche	Bad Bot
1460	Marketing	Bad Bot

Règle de signature de bot	ID	Description
1467	Outil	Bad Bot
1469	Outil	Bad Bot
1471	Moteur de recherche	Bad Bot
1484	Sans catégorie	Bad Bot
1493	Marketing	Bad Bot
1502	Moniteur de site	Bad Bot
1504	Sans catégorie	Bad Bot
1506	Sans catégorie	Bad Bot
1518	Sans catégorie	Bad Bot
1520	Moteur de recherche	Bad Bot
1531	Feed Fetcher	Bad Bot
1533	Sans catégorie	Bad Bot
1540	Moteur de recherche	Bad Bot
1556	Marketing	Bad Bot
1560	Sans catégorie	Bad Bot
1564	Outil	Bad Bot
1570	Moniteur de site	Bad Bot
1575	Moteur de recherche	Bad Bot
1586	Analyseur de virus	Bad Bot
1588	Sans catégorie	Bad Bot
1594	Outil	Bad Bot
1619	Marketing	Bad Bot
1623	Outil	Bad Bot
1626	Moteur de recherche	Bad Bot
1632	Feed Fetcher	Bad Bot
1648	Moteur de recherche	Bad Bot
1652	Marketing	Bad Bot
1660	Marketing	Bad Bot
1713	Outil	Bad Bot

Règle de signature de bot	ID	Description
1719	Moteur de recherche	Bad Bot
1722	Sans catégorie	Bad Bot
1744	Sans catégorie	Bad Bot
1754	Sans catégorie	Bad Bot
1757	Sans catégorie	Bad Bot
1762	Sans catégorie	Bad Bot
1769	Sans catégorie	Bad Bot
1771	Marketing	Bad Bot
1779	Outil	Bad Bot
1782	Outil	Bad Bot
1785	Tester de vitesse	Bad Bot
1786	Outil	Bad Bot
1792	Moniteur de site	Bad Bot
1869	Outil	Bad Bot
1928	Marketing	Bad Bot
1942	Moniteur de site	Bad Bot
1949	Marketing	Bad Bot
1954	Marketing	Bad Bot
1964	Sans catégorie	Bad Bot
1969	Moteur de recherche	Bad Bot
2294	Moteur de recherche	Bad Bot
2303	Sans catégorie	Bad Bot
2308	Scraper	Bad Bot
2335	Marketing	Bad Bot
2374	Sans catégorie	Bad Bot
2377	Sans catégorie	Bad Bot
2385	Outil	Bad Bot
2389	Sans catégorie	Bad Bot
2414	Sans catégorie	Bad Bot

Règle de signature de bot	ID	Description
2421	Sans catégorie	Bad Bot
2424	Sans catégorie	Bad Bot
2427	Sans catégorie	Bad Bot
2429	Moteur de recherche	Bad Bot
2437	Sans catégorie	Bad Bot
2440	Moteur de recherche	Bad Bot
2443	Sans catégorie	Bad Bot
2453	Marketing	Bad Bot
2472	Marketing	Bad Bot
2474	Feed Fetcher	Bad Bot
2482	Sans catégorie	Bad Bot
2500	Créateur de capture d’écran	Bad Bot
2503	Sans catégorie	Bad Bot
2507	Sans catégorie	Bad Bot
2516	Outil	Bad Bot
2536	Marketing	Bad Bot
2543	Outil	Bad Bot
2548	Outil	Bad Bot
2557	Marketing	Bad Bot
2561	Sans catégorie	Bad Bot
2572	Sans catégorie	Bad Bot
2578	Sans catégorie	Bad Bot
2584	Sans catégorie	Bad Bot
2588	Sans catégorie	Bad Bot
2592	Moteur de recherche	Bad Bot
2600	Outil	Bad Bot
2606	Sans catégorie	Bad Bot
2611	Sans catégorie	Bad Bot
2622	Outil	Bad Bot

Règle de signature de bot	ID	Description
2625	Outil	Bad Bot
2631	Outil	Bad Bot
2635	Outil	Bad Bot
2637	Créateur de capture d'écran	Bad Bot
2641	Moteur de recherche	Bad Bot
2655	Sans catégorie	Bad Bot
2657	Marketing	Bad Bot
2663	Sans catégorie	Bad Bot
2666	Outil	Bad Bot
2672	Feed Fetcher	Bad Bot
2674	Outil	Bad Bot
2681	Moteur de recherche	Bad Bot
2684	Marketing	Bad Bot
2690	Sans catégorie	Bad Bot
2704	Sans catégorie	Bad Bot
2707	Sans catégorie	Bad Bot
2714	Feed Fetcher	Bad Bot
2722	Sans catégorie	Bad Bot
2726	Feed Fetcher	Bad Bot
2730	Créateur de capture d'écran	Bad Bot
2736	Sans catégorie	Bad Bot
2749	Sans catégorie	Bad Bot
2753	Outil	Bad Bot
2756	Outil	Bad Bot
2760	Tester de vitesse	Bad Bot
2780	Outil	Bad Bot
2785	Moniteur de site	Bad Bot
2789	Sans catégorie	Bad Bot
2797	Outil	Bad Bot

Règle de signature de bot	ID	Description
2801	Outil	Bad Bot
2808	Outil	Bad Bot
2810	Sans catégorie	Bad Bot
2813	Sans catégorie	Bad Bot
2816	Sans catégorie	Bad Bot
2820	Vérificateur de liens	Bad Bot
2824	Vérificateur de liens	Bad Bot
2831	Créateur de capture d'écran	Bad Bot
2843	Outil	Bad Bot
2846	Outil	Bad Bot
2849	Marketing	Bad Bot
2851	Sans catégorie	Bad Bot
2855	Sans catégorie	Bad Bot
2859	Outil	Bad Bot
2873	Sans catégorie	Bad Bot
2875	Créateur de capture d'écran	Bad Bot
2879	Sans catégorie	Bad Bot
2881	Sans catégorie	Bad Bot
2886	Moniteur de site	Bad Bot
2899	Sans catégorie	Bad Bot
2916	Sans catégorie	Bad Bot
2924	Outil	Bad Bot
2932	Marketing	Bad Bot
2935	Vérificateur de liens	Bad Bot
2939	Marketing	Bad Bot
2942	Sans catégorie	Bad Bot
2955	Moteur de recherche	Bad Bot
2960	Outil	Bad Bot
2964	Sans catégorie	Bad Bot

Règle de signature de bot	ID	Description
2972	Marketing	Bad Bot
2978	Analyseur de vulnérabilité	Bad Bot
2980	Outil	Bad Bot
2985	Marketing	Bad Bot
2993	Sans catégorie	Bad Bot
2999	Créateur de capture d'écran	Bad Bot
3003	Feed Fetcher	Bad Bot
3005	Sans catégorie	Bad Bot
3013	Sans catégorie	Bad Bot
3016	Sans catégorie	Bad Bot
3021	Moteur de recherche	Bad Bot
3026	Sans catégorie	Bad Bot
3030	Marketing	Bad Bot
3065	Marketing	Bad Bot
3068	Sans catégorie	Bad Bot
3072	Marketing	Bad Bot
3077	Marketing	Bad Bot
3080	Sans catégorie	Bad Bot
3086	Scraper	Bad Bot
3092	Moteur de recherche	Bad Bot
3100	Sans catégorie	Bad Bot
3104	Outil	Bad Bot
3111	Sans catégorie	Bad Bot
3116	Moniteur de site	Bad Bot
3118	Outil	Bad Bot
3120	Marketing	Bad Bot
3122	Moteur de recherche	Bad Bot
3126	Marketing	Bad Bot
3141	Outil	Bad Bot

Règle de signature de bot	ID	Description
3143	Sans catégorie	Bad Bot
3145	Scraper	Bad Bot
3150	Sans catégorie	Bad Bot
3173	Vérificateur de liens	Bad Bot
3176	Sans catégorie	Bad Bot
3186	Tester de vitesse	Bad Bot
3190	Scraper	Bad Bot
3203	Moteur de recherche	Bad Bot
3216	Sans catégorie	Bad Bot
3220	Outil	Bad Bot
3223	Vérificateur de liens	Bad Bot
3241	Sans catégorie	Bad Bot
3245	Moniteur de site	Bad Bot
3285	Sans catégorie	Bad Bot
3304	Marketing	Bad Bot
3307	Vérificateur de liens	Bad Bot
3316	Outil	Bad Bot
3326	Marketing	Bad Bot
3333	Moteur de recherche	Bad Bot
3340	Moteur de recherche	Bad Bot
3344	Marketing	Bad Bot
3350	Sans catégorie	Bad Bot
3355	Marketing	Bad Bot
3365	Sans catégorie	Bad Bot
3378	Sans catégorie	Bad Bot
3388	Outil	Bad Bot
3396	Sans catégorie	Bad Bot
3400	Sans catégorie	Bad Bot
3421	Sans catégorie	Bad Bot

Règle de signature de bot	ID	Description
3439	Sans catégorie	Bad Bot
3447	Feed Fetcher	Bad Bot
3451	Outil	Bad Bot
3459	Créateur de capture d'écran	Bad Bot
3469	Analyseur de vulnérabilité	Bad Bot
3475	Sans catégorie	Bad Bot
3485	Moteur de recherche	Bad Bot
3493	Outil	Bad Bot
3502	Marketing	Bad Bot
3507	Moteur de recherche	Bad Bot
3523	Sans catégorie	Bad Bot
3535	Tester de vitesse	Bad Bot
3549	Sans catégorie	Bad Bot
3556	Sans catégorie	Bad Bot
3561	Sans catégorie	Bad Bot
3565	Sans catégorie	Bad Bot
3572	Moteur de recherche	Bad Bot
3578	Sans catégorie	Bad Bot
3610	Moteur de recherche	Bad Bot
3617	Sans catégorie	Bad Bot
3621	Marketing	Bad Bot
3632	Outil	Bad Bot
3635	Marketing	Bad Bot
3653	Sans catégorie	Bad Bot
3661	Moteur de recherche	Bad Bot
3704	Sans catégorie	Bad Bot
3707	Sans catégorie	Bad Bot
3711	Sans catégorie	Bad Bot
3730	Moteur de recherche	Bad Bot

Règle de signature de bot	ID	Description
3740	Moniteur de site	Bad Bot
3759	Moteur de recherche	Bad Bot
3764	Sans catégorie	Bad Bot
3770	Sans catégorie	Bad Bot

Mise à jour de la signature du bot pour mars 2021

October 5, 2021

Certaines signatures de bots existantes sont mises à jour. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre solution matérielle-logicielle contre les attaques de bots.

Version de signature du bot

Signature version 7 est applicable aux plates-formes Citrix ADC avec des versions 13.0 61.x ou ultérieures.

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

Règle de signature de bot	ID	Description
278	Scraper	Bon Bot
378	Scraper	Bon Bot
379	Scraper	Bon Bot
380	Scraper	Bon Bot
381	Scraper	Bon Bot
382	Scraper	Bon Bot
383	Scraper	Bon Bot
384	Scraper	Bon Bot
385	Scraper	Bon Bot
386	Scraper	Bon Bot

Règle de signature de bot	ID	Description
387	Scraper	Bon Bot
389	Scraper	Bon Bot
390	Scraper	Bon Bot
391	Scraper	Bon Bot
494	Scraper	Bon Bot
627	Moteur de recherche	Bon Bot
660	Moteur de recherche	Bon Bot
3840	Crawler	Bon Bot

Mise à jour de la signature du bot pour août 2021

October 5, 2021

De nouvelles signatures sont ajoutées et certaines signatures de bots existantes sont mises à jour. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre solution matérielle-logicielle contre les attaques de bots.

Version de signature du bot

Signature version 8 est applicable aux plates-formes Citrix ADC avec des versions 13.0 61.x ou ultérieures.

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

Règle de signature de bot	ID	Description
236	Scraper	Bon Bot
378	Scraper	Bon Bot
381	Scraper	Bon Bot
382	Scraper	Bon Bot
390	Scraper	Bon Bot

Règle de signature de bot	ID	Description
544	Scraper	Bon Bot
702	Moteur de recherche	Bon Bot
979	Scraper	Bad Bot
3791	Tester de vitesse	Bon Bot
3797	Marketing	Bon Bot
3800	Marketing	Bon Bot
3824	Crawler	Bad Bot
3833	Moteur de recherche	Bon Bot
3849	Crawler	Bon Bot
3871	Marketing	Bon Bot
3963	Marketing	Bon Bot
4027	Moteur de recherche	Bon Bot

Nouvelle signature de bot

Règle de signature de bot	ID	Description
4028	Marketing	Bon Bot
4029	Outil	Bon Bot
4030	Scraper	Bon Bot
4031	Scraper	Bon Bot
4032	Sans catégorie	Bad Bot
4033	Crawler	Bon Bot
4034	Crawler	Bon Bot
4035	Marketing	Bon Bot
4036	Analyseur de vulnérabilité	Bon Bot
4037	Analyseur de vulnérabilité	Bon Bot
4038	Sans catégorie	Bad Bot
4039	Outil	Bon Bot
4040	Crawler	Bon Bot

Règle de signature de bot	ID	Description
4041	Outil	Bon Bot
4042	Crawler	Bon Bot
4043	Créateur de capture d'écran	Bon Bot
4044	Scraper	Bad Bot
4045	Scraper	Bad Bot
4046	Scraper	Bad Bot
4047	Sans catégorie	Bad Bot
4048	Feed Fetcher	Bon Bot
4049	Sans catégorie	Bad Bot
4050	Crawler	Bon Bot
4051	Crawler	Bon Bot
4052	Outil	Bon Bot
4053	Outil	Bon Bot
4054	Scraper	Bad Bot
4055	Sans catégorie	Bon Bot
4056	Marketing	Bon Bot
4057	Créateur de capture d'écran	Bon Bot
4058	Crawler	Bon Bot
4059	Sans catégorie	Bad Bot
4060	Moteur de recherche	Bon Bot
4061	Moteur de recherche	Bon Bot
4062	Moteur de recherche	Bon Bot
4063	Moteur de recherche	Bon Bot
4064	Outil	Bon Bot
4065	Scraper	Bon Bot
4066	Marketing	Bon Bot
4067	Marketing	Bon Bot
4068	Sans catégorie	Bad Bot
4069	Sans catégorie	Bad Bot

Règle de signature de bot	ID	Description
4070	Sans catégorie	Bad Bot
4071	Outil	Bon Bot
4072	Outil	Bad Bot
4073	Sans catégorie	Bad Bot
4074	Sans catégorie	Bad Bot
4075	Outil	Bad Bot
4076	Marketing	Bon Bot
4077	Scraper	Bon Bot
4078	Crawler	Bon Bot
4079	Crawler	Bon Bot
4080	Outil	Bad Bot
4081	Moteur de recherche	Bon Bot
4082	Outil	Bon Bot
4083	Sans catégorie	Bad Bot
4084	Sans catégorie	Bad Bot
4085	Outil	Bon Bot
4086	Outil	Bon Bot
4087	Outil	Bad Bot
4088	Moteur de recherche	Bon Bot
4089	Marketing	Bon Bot
4090	Outil	Bon Bot
4091	Outil	Bon Bot
4092	Outil	Bon Bot
4093	Outil	Bon Bot
4094	Sans catégorie	Bon Bot
4095	Moniteur de site	Bon Bot
4096	Moniteur de site	Bon Bot
4097	Moniteur de site	Bon Bot
4098	Crawler	Bon Bot

Règle de signature de bot	ID	Description
4099	Moteur de recherche	Bon Bot
4100	Moteur de recherche	Bon Bot
4101	Moteur de recherche	Bon Bot
4102	Moteur de recherche	Bon Bot
4103	Marketing	Bon Bot
4104	Marketing	Bon Bot
4105	Marketing	Bon Bot
4106	Marketing	Bon Bot
4107	Marketing	Bon Bot
4108	Marketing	Bon Bot
4109	Moteur de recherche	Bon Bot
4110	Crawler	Bon Bot
4111	Crawler	Bon Bot
4112	Crawler	Bon Bot
4113	Analyseur de vulnérabilité	Bon Bot
4114	Crawler	Bon Bot
4115	Outil	Bon Bot
4116	Sans catégorie	Bad Bot
4117	Sans catégorie	Bad Bot
4118	Sans catégorie	Bad Bot
4119	Sans catégorie	Bad Bot
4120	Marketing	Bon Bot
4121	Marketing	Bon Bot
4122	Marketing	Bon Bot
4123	Marketing	Bon Bot
4124	Marketing	Bon Bot
4125	Marketing	Bon Bot
4126	Marketing	Bon Bot
4127	Marketing	Bon Bot

Règle de signature de bot	ID	Description
4128	Marketing	Bon Bot
4129	Marketing	Bon Bot
4130	Marketing	Bon Bot
4131	Outil	Bon Bot
4132	Marketing	Bon Bot
4133	Marketing	Bon Bot
4134	Outil	Bon Bot
4135	Marketing	Bon Bot
4136	Marketing	Bon Bot
4137	Marketing	Bon Bot
4138	Marketing	Bon Bot
4139	Marketing	Bon Bot
4140	Marketing	Bon Bot
4141	Marketing	Bon Bot
4142	Marketing	Bon Bot
4143	Marketing	Bon Bot
4144	Marketing	Bon Bot
4145	Moteur de recherche	Bon Bot
4146	Moteur de recherche	Bon Bot
4147	Moteur de recherche	Bon Bot
4148	Moteur de recherche	Bon Bot
4149	Moteur de recherche	Bon Bot
4150	Moteur de recherche	Bon Bot
4151	Moteur de recherche	Bon Bot
4152	Moteur de recherche	Bon Bot
4153	Moteur de recherche	Bon Bot
4154	Moteur de recherche	Bon Bot
4155	Moteur de recherche	Bon Bot
4156	Créateur de capture d’écran	Bon Bot

Règle de signature de bot	ID	Description
4157	Moteur de recherche	Bon Bot
4158	Moteur de recherche	Bon Bot
4159	Moteur de recherche	Bon Bot
4160	Créateur de capture d'écran	Bon Bot
4161	Moteur de recherche	Bon Bot
4162	Moteur de recherche	Bon Bot
4163	Outil	Bon Bot
4164	Moteur de recherche	Bon Bot
4165	Marketing	Bon Bot
4166	Sans catégorie	Bad Bot
4167	Outil	Bad Bot
4168	Tester de vitesse	Bon Bot
4169	Scraper	Bad Bot
4170	Outil	Bon Bot
4171	Scraper	Bad Bot
4172	Web Crawler	Bon Bot
4173	Outil	Bon Bot
4174	Crawler	Bon Bot
4175	Crawler	Bon Bot
4176	Outil	Bon Bot
4177	Moteur de recherche	Bon Bot
4178	Outil	Bon Bot
4179	Web Crawler	Bon Bot
4180	Outil	Bon Bot
4181	Moniteur de site	Bon Bot
4182	Moniteur de site	Bon Bot
4183	Moniteur de site	Bon Bot
4184	Moniteur de site	Bon Bot
4185	Moteur de recherche	Bon Bot

Règle de signature de bot	ID	Description
4186	Outil	Bon Bot
4187	Outil	Bon Bot
4188	Créateur de capture d'écran	Bon Bot
4189	Marketing	Bon Bot
4190	Moteur de recherche	Bon Bot
4191	Moteur de recherche	Bon Bot
4192	Moteur de recherche	Bon Bot
4193	Moteur de recherche	Bon Bot
4194	Outil	Bon Bot
4195	Moteur de recherche	Bad Bot
4196	Outil	Bon Bot
4197	Outil	Bon Bot
4198	Marketing	Bon Bot
4199	Marketing	Bon Bot
4200	Analyseur de vulnérabilité	Bon Bot
4201	Outil	Bon Bot
4202	Outil	Bon Bot
4203	Sans catégorie	Bad Bot
4204	Sans catégorie	Bad Bot
4205	Moteur de recherche	Bon Bot
4206	Marketing	Bon Bot
4207	Marketing	Bon Bot
4208	Moteur de recherche	Bon Bot
4209	Moteur de recherche	Bon Bot
4210	Tester de vitesse	Bon Bot
4211	Outil	Bon Bot
4212	Feed Fetcher	Bon Bot
4213	Feed Fetcher	Bon Bot
4214	Scraper	Bad Bot

Règle de signature de bot	ID	Description
4215	Outil	Bon Bot
4216	Outil	Bon Bot
4217	Outil	Bad Bot
4218	Scraper	Bad Bot
4219	Marketing	Bon Bot
4220	Outil	Bon Bot
4221	Outil	Bad Bot
4222	Moniteur de site	Bon Bot
4223	Marketing	Bon Bot
4224	Moteur de recherche	Bon Bot
4225	Moteur de recherche	Bon Bot
4226	Moteur de recherche	Bon Bot
4227	Marketing	Bon Bot
4228	Marketing	Bon Bot
4229	Outil	Bon Bot
4230	Sans catégorie	Bad Bot
4231	Créateur de capture d’écran	Bon Bot
4232	Outil	Bon Bot
4233	Moniteur de site	Bon Bot
4234	Moniteur de site	Bon Bot
4235	Moniteur de site	Bon Bot
4236	Moniteur de site	Bon Bot
4237	Moniteur de site	Bon Bot
4238	Moniteur de site	Bon Bot
4239	Sans catégorie	Bad Bot
4240	Marketing	Bon Bot
4241	Marketing	Bon Bot
4242	Marketing	Bon Bot
4243	Marketing	Bon Bot

Règle de signature de bot	ID	Description
4244	Marketing	Bon Bot
4245	Marketing	Bon Bot
4246	Marketing	Bon Bot
4247	Moteur de recherche	Bon Bot
4248	Moteur de recherche	Bon Bot
4249	Créateur de capture d'écran	Bon Bot
4250	Moteur de recherche	Bon Bot
4251	Moteur de recherche	Bon Bot
4252	Crawler	Bon Bot
4253	Crawler	Bon Bot
4254	Crawler	Bon Bot
4255	Outil	Bon Bot
4256	Sans catégorie	Bon Bot
4257	Outil	Bon Bot
4258	Crawler	Bon Bot
4259	Crawler	Bon Bot
4260	Outil	Bon Bot
4261	Outil	Bon Bot
4262	Outil	Bon Bot
4263	Marketing	Bon Bot
4264	Crawler	Bad Bot
4265	Moteur de recherche	Bon Bot
4266	Sans catégorie	Bon Bot
4267	Outil	Bon Bot
4268	Outil	Bon Bot
4269	Moteur de recherche	Bon Bot
4270	Moteur de recherche	Bon Bot
4271	Moteur de recherche	Bon Bot
4272	Moteur de recherche	Bon Bot

Règle de signature de bot	ID	Description
4273	Moteur de recherche	Bon Bot
4274	Moteur de recherche	Bon Bot
4275	Moteur de recherche	Bon Bot
4276	Sans catégorie	Bad Bot
4277	Sans catégorie	Bad Bot
4278	Sans catégorie	Bad Bot
4279	Marketing	Bon Bot
4280	Crawler	Bon Bot
4281	Sans catégorie	Bad Bot
4282	Marketing	Bon Bot
4283	Marketing	Bon Bot
4284	Marketing	Bon Bot
4285	Marketing	Bon Bot
4286	Marketing	Bon Bot
4287	Marketing	Bon Bot
4288	Marketing	Bon Bot
4289	Marketing	Bon Bot
4290	Marketing	Bon Bot
4291	Marketing	Bon Bot
4292	Marketing	Bon Bot
4293	Marketing	Bon Bot
4294	Marketing	Bon Bot
4295	Moteur de recherche	Bon Bot
4296	Moteur de recherche	Bon Bot
4297	Moteur de recherche	Bon Bot
4298	Moteur de recherche	Bon Bot
4299	Moteur de recherche	Bon Bot
4300	Moteur de recherche	Bon Bot
4301	Moteur de recherche	Bon Bot

Règle de signature de bot	ID	Description
4302	Moteur de recherche	Bon Bot
4303	Moteur de recherche	Bon Bot
4304	Moteur de recherche	Bon Bot
4305	Moteur de recherche	Bon Bot
4306	Créateur de capture d'écran	Bon Bot
4307	Moteur de recherche	Bon Bot
4308	Moteur de recherche	Bon Bot
4309	Moteur de recherche	Bon Bot
4310	Moteur de recherche	Bon Bot
4311	Créateur de capture d'écran	Bon Bot
4312	Moteur de recherche	Bon Bot
4313	Moteur de recherche	Bon Bot
4314	Moteur de recherche	Bon Bot
4315	Moteur de recherche	Bon Bot
4316	Moteur de recherche	Bon Bot
4317	Moteur de recherche	Bon Bot
4318	Créateur de capture d'écran	Bon Bot
4319	Créateur de capture d'écran	Bon Bot
4320	Sans catégorie	Bad Bot
4321	Sans catégorie	Bon Bot
4322	Crawler	Bon Bot
4323	Outil	Bon Bot
4324	Outil	Bon Bot
4325	Outil	Bon Bot
4326	Scraper	Bad Bot
4327	Moteur de recherche	Bon Bot
4328	Marketing	Bon Bot
4329	Sans catégorie	Bad Bot
4330	Moniteur de site	Bon Bot

Règle de signature de bot	ID	Description
4331	Moteur de recherche	Bon Bot
4332	Moteur de recherche	Bon Bot
4333	Sans catégorie	Bad Bot
4334	Scraper	Bon Bot
4335	Marketing	Bon Bot
4336	Marketing	Bon Bot
4337	Outil	Bon Bot
4338	Outil	Bon Bot
4339	Outil	Bon Bot
4340	Crawler	Bon Bot
4341	Crawler	Bon Bot
4342	Analyseur de vulnérabilité	Bon Bot
4343	Analyseur de vulnérabilité	Bon Bot
4344	Scraper	Bon Bot
4345	Marketing	Bon Bot
4346	Marketing	Bon Bot
4347	Marketing	Bon Bot
4348	Marketing	Bon Bot
4349	Marketing	Bon Bot
4350	Marketing	Bon Bot
4351	Marketing	Bon Bot
4352	Marketing	Bon Bot
4353	Marketing	Bon Bot
4354	Marketing	Bon Bot
4355	Moteur de recherche	Bon Bot
4356	Moteur de recherche	Bon Bot
4357	Moteur de recherche	Bon Bot
4358	Moteur de recherche	Bon Bot
4359	Moteur de recherche	Bon Bot

Règle de signature de bot	ID	Description
4360	Moteur de recherche	Bon Bot
4361	Moteur de recherche	Bon Bot
4362	Moteur de recherche	Bon Bot
4363	Moteur de recherche	Bon Bot
4364	Moteur de recherche	Bon Bot
4365	Créateur de capture d'écran	Bon Bot
4366	Moteur de recherche	Bon Bot
4367	Moteur de recherche	Bon Bot
4368	Moteur de recherche	Bon Bot
4369	Moteur de recherche	Bon Bot
4370	Créateur de capture d'écran	Bon Bot
4371	Moteur de recherche	Bon Bot
4372	Moteur de recherche	Bon Bot
4373	Moteur de recherche	Bon Bot
4374	Moteur de recherche	Bon Bot
4375	Moteur de recherche	Bon Bot
4376	Créateur de capture d'écran	Bon Bot
4377	Crawler	Bon Bot
4378	Crawler	Bon Bot
4379	Moteur de recherche	Bon Bot
4380	Moteur de recherche	Bon Bot
4381	Moteur de recherche	Bon Bot
4382	Moteur de recherche	Bon Bot
4383	Crawler	Bon Bot
4384	Moteur de recherche	Bon Bot
4385	Outil	Bon Bot
4386	Sans catégorie	Bon Bot
4387	Crawler	Bon Bot
4388	Crawler	Bon Bot

Règle de signature de bot	ID	Description
4389	Outil	Bon Bot
4390	Outil	Bon Bot
4391	Outil	Bon Bot
4392	Outil	Bon Bot
4393	Outil	Bon Bot
4394	Sans catégorie	Bon Bot
4395	Outil	Bon Bot
4396	Moniteur de site	Bon Bot
4397	Moniteur de site	Bon Bot
4398	Outil	Bad Bot
4399	Outil	Bad Bot
4400	Outil	Bad Bot
4401	Outil	Bad Bot
4402	Outil	Bad Bot
4403	Outil	Bad Bot
4404	Moteur de recherche	Bon Bot
4405	Moteur de recherche	Bon Bot
4406	Moteur de recherche	Bon Bot
4407	Sans catégorie	Bon Bot

Redirection de cache

January 21, 2021

Dans un déploiement standard, différents clients demandent à plusieurs reprises aux serveurs Web le même contenu. Pour supprimer le serveur Web d'origine du traitement de chaque requête, une appliance Citrix ADC avec la redirection du cache activée peut servir ce contenu à partir d'un serveur de cache plutôt que du serveur d'origine.

L'appliance Citrix ADC analyse les demandes entrantes, envoie des demandes de données mises en cache aux serveurs de cache et envoie des demandes non mises en cache et des requêtes HTTP dynamiques aux serveurs d'origine.

La redirection du cache est une fonctionnalité basée sur des stratégies. Par défaut, les demandes qui correspondent à une stratégie sont envoyées au serveur d'origine et toutes les autres demandes sont envoyées à un serveur de cache. Pour le test ou la maintenance, vous pouvez ignorer l'évaluation des stratégies et diriger toutes les demandes vers le cache ou le serveur d'origine.

Vous pouvez combiner la commutation de contenu avec la redirection de cache pour mettre en cache du contenu sélectif et diffuser du contenu à partir de serveurs de cache spécifiques pour des types spécifiques de contenu demandé.

Une appliance Citrix ADC configurée pour la redirection du cache peut être déployée à la périphérie d'un réseau, devant le serveur d'origine ou n'importe où le long de l'épine dorsale du réseau. Dans un déploiement périphérique, couramment utilisé par les fournisseurs de services Internet (FAI), les câblodistributeurs, les réseaux de distribution de contenu et les réseaux d'entreprise, l'appliance Citrix ADC réside directement devant les clients. Dans un déploiement côté serveur, l'appliance Citrix ADC est plus proche des serveurs d'origine.

La redirection du cache est utilisée le plus souvent avec le type de service HTTP, mais elle prend également en charge le protocole HTTPS sécurisé.

Stratégies de redirection de cache

January 21, 2021

Un serveur virtuel de redirection de cache applique des stratégies de redirection de cache à chaque requête entrante. Par défaut, si une demande correspond à l'une des stratégies configurées, elle est considérée comme non mise en cache et l'appliance Citrix ADC l'envoie au serveur d'origine. D'autres demandes sont envoyées à un serveur de cache. Ce comportement peut être inversé, de sorte que les demandes qui correspondent aux stratégies de redirection de cache configurées sont envoyées aux serveurs de cache.

L'appliance fournit un ensemble de stratégies pour la redirection du cache. Si ces stratégies intégrées ne conviennent pas à votre déploiement, vous pouvez configurer des stratégies de redirection de cache définies par l'utilisateur.

Remarque : une fois que vous avez déterminé les stratégies de redirection du cache intégrées à utiliser ou que vous avez créé des stratégies définies par l'utilisateur, procédez à la configuration de la redirection du cache. Pour utiliser cette fonctionnalité, vous devez configurer au moins un serveur virtuel de redirection de cache et, pour un fonctionnement normal, vous devez lier au moins une stratégie de redirection de cache à ce serveur virtuel.

Stratégies de redirection de cache intégrées

October 5, 2021

L'appliance Citrix ADC fournit des stratégies de redirection de cache intégrées qui traitent les demandes de cache classiques. Ces stratégies sont basées sur les méthodes HTTP, les jetons URL ou URL de la demande entrante, la version HTTP ou les en-têtes HTTP et leurs valeurs dans la demande.

Les stratégies de redirection de cache intégrées peuvent être directement liées à un serveur virtuel et ne nécessitent aucune configuration supplémentaire.

Les stratégies de redirection du cache utilisent deux types de langages d'expressions d'appliance, la stratégie classique et la stratégie avancée. Pour plus d'informations sur ces langues, voir Stratégies et expressions.

Stratégies de redirection de cache classiques intégrées

Les stratégies de redirection de cache intégrées basées sur des expressions classiques sont appelées *stratégies de redirection de cache classiques*. Pour obtenir une description complète des expressions classiques et la façon de les configurer, voir Stratégies et expressions.

Les stratégies de redirection de cache classiques évaluent les caractéristiques de base du trafic et d'autres données. Par exemple, les stratégies de redirection de cache classiques peuvent déterminer si une requête ou une réponse HTTP contient un type particulier d'en-tête ou d'URL.

L'appliance Citrix ADC fournit les stratégies de redirection de cache classiques intégrées suivantes :

Nom de la stratégie intégrée	Description
bypass-non-get	Isolez le cache si la demande utilise une méthode HTTP autre que GET.
bypass-cache-control	Ignorez le cache si l'en-tête de la demande contient un en-tête Cache-Control : no-cache ou Cache-Control : no-store, ou si la requête HTTP contient un en-tête Pragma.
bypass-dynamic-url	Contournez le cache si l'URL suggère que le contenu est dynamique, comme l'indique la présence de l'une des extensions suivantes : cgi, asp, exe, cfm, ex, shtml ou htx. Contournez également le cache si l'URL commence par l'un des éléments suivants : /cgi-bin/, /bin/ ou /exec/.

Nom de la stratégie intégrée	Description
jetons d'URL de contournement	Contournez le cache car la demande est dynamique, comme indiqué par l'un des jetons suivants dans l'URL : ? , ! , ou =.
cookie de contournement	Contournez le cache pour toute URL contenant un en-tête de cookie et une extension autre que .png ou .jpg.

Stratégies de redirection de cache de stratégie avancées intégrées

Les stratégies de redirection de cache intégrées basées sur des expressions de stratégie avancées sont appelées *stratégies de redirection de cache de stratégie avancée*. Pour obtenir une description complète des expressions de stratégie avancées et savoir comment les configurer, consultez Stratégies et expressions.

Outre les mêmes types d'évaluations effectuées par les stratégies de redirection de cache classiques, les stratégies de redirection de cache de stratégie avancée vous permettent d'analyser davantage de données (par exemple, le corps d'une requête HTTP) et de configurer davantage d'opérations dans la règle de stratégie (par exemple, diriger la demande vers le cache ou serveur d'origine).

Les appliances Citrix ADC fournissent les deux actions intégrées suivantes pour les stratégies de redirection du cache de stratégie avancée :

- CACHE
- ORIGIN

Comme leur nom l'indique, ils dirigent la demande vers le serveur de cache ou le serveur d'origine, respectivement.

Remarque : Si vous utilisez la stratégie de redirection du cache de stratégie avancée intégrée, vous ne pouvez pas modifier l'action.

L'appliance Citrix ADC fournit les stratégies de redirection de cache de stratégie avancées intégrées suivantes :

Nom de la stratégie intégrée	Description
bypass-non-get_adv	Isolez le cache si la demande utilise une méthode HTTP autre que GET.

Nom de la stratégie intégrée	Description
bypass-cache-control_adv	Ignorez le cache si l'en-tête de la demande contient un en-tête Cache-Control : no-cache ou Cache-Control : no-store, ou si la requête HTTP contient un en-tête Pragma.
bypass-dynamic-url_adv	Contournez le cache si l'URL suggère que le contenu est dynamique, comme l'indique la présence de l'une des extensions suivantes : cgi, asp, exe, cfm, ex, shtml ou htx. Contournez également le cache si l'URL commence par l'un des éléments suivants : /cgi-bin/, /bin/ ou /exec/.
bypass-urltokens_adv	Contournez le cache car la demande est dynamique, comme indiqué par l'un des jetons suivants dans l'URL : ? , ! , ou =.
bypass-cookie_adv	Contournez le cache pour toute URL contenant un en-tête de cookie et une extension autre que .png ou .jpg.

Afficher les stratégies de redirection de cache intégrées

Vous pouvez afficher les stratégies de redirection de cache disponibles à l'aide de l'interface de ligne de commande ou de l'utilitaire de configuration.

Afficher les stratégies de redirection de cache intégrées à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show cr policy [<policyName>]
```

Exemple :

```
1 > show cr policy
2 1)       Cache-By-Pass RULE: NS_NON_GET          Policy:bypass-non-get
3 2)       Cache-By-Pass RULE: (NS_CACHECONTROL_NOSTORE ||
     NS_CACHECONTROL_NOCACHE || NS_HEADER_PRAGMA)    Policy:bypass-cache-
     control
4 3)       Cache-By-Pass RULE: (NS_EXT_CGI || NS_EXT_ASP || NS_EXT_EXE ||
      NS_EXT_CFM || NS_EXT_EX || NS_EXT_SHTML || NS_EXT_HTX) || (
```



```
      NS_URL_PATH_CGIBIN || NS_URL_PATH_EXEC || NS_URL_PATH_BIN)
      Policy:bypass-dynamic-url
4)       Cache-By-Pass RULE: NS_URL_TOKENS       Policy:bypass-
   urltokens
5)       Cache-By-Pass RULE: (NS_HEADER_COOKIE && NS_EXT_NOT_GIF &&
   NS_EXT_NOT_JPEG)     Policy:bypass-cookie
 Done
<!--NeedCopy-->
```

Afficher les stratégies de redirection de cache intégrées à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Stratégies. Les stratégies de redirection de cache configurées apparaissent dans le volet de détails.
2. Sélectionnez l'une des stratégies configurées pour afficher les détails.

Configurer une stratégie de redirection du cache

October 5, 2021

Une stratégie de redirection de cache inclut une ou plusieurs expressions (également appelées *règles*). Chaque expression représente une condition qui est évaluée lorsque la demande du client est comparée à la stratégie.

Vous ne configurez pas explicitement les actions des stratégies de redirection du cache. Par défaut, l'appliance Citrix ADC considère que toute demande correspondant à une stratégie ne peut pas être mise en cache et dirige la demande vers le serveur d'origine au lieu du cache.

Les stratégies de redirection de cache basées sur le format de stratégie classique sont appelées *stratégies de redirection de cache classiques*. Chacune de ces stratégies a un nom et inclut une expression classique ou un ensemble d'expressions classiques qui sont combinées à l'aide d'opérateurs logiques.

Pour les stratégies de redirection de cache classiques, vous ne configurez pas explicitement les actions pour les stratégies. Par défaut, l'appliance Citrix ADC considère que toute demande correspondant à une stratégie ne peut pas être mise en cache et dirige la demande vers le serveur d'origine au lieu du cache.

Les stratégies de redirection du cache basées sur le format de stratégie le plus récent sont appelées *stratégies de redirection avancées*. Cette stratégie porte un nom et inclut une expression de stratégie avancée ou un ensemble d'expressions de stratégie avancées qui sont combinées à l'aide d'opérateurs logiques, et les actions intégrées suivantes :

- CACHE

- ORIGIN

Pour plus d'informations sur les expressions classiques et les expressions de stratégie avancées, consultez la section Stratégies et expressions.

Ajouter une stratégie de redirection de cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter une stratégie de redirection du cache et vérifier la configuration :

```
1 -  add cr policy <policyName> \*\*-rule\*\* <expression>
2 -  show cr policy [<policyName>]
3 <!--NeedCopy-->
```

Exemples :

Stratégie avec une expression simple :

```
1 > add cr policy-CRD-1 -rule "REQ.HTTP.URL != /\*.jpeg"
2  Done
3 > show cr policy-CRD-1
4          Cache-By-Pass RULE: REQ.HTTP.URL != '/\*.jpeg'   Policy:Policy
               -CRD-1
5  Done
6 <!--NeedCopy-->
```

Stratégie avec une expression composée :

```
1 > add cr policy-CRD-2 -rule "REQ.HTTP.METHOD == POST && (REQ.HTTP.URL
     == /\*.cgi || REQ.HTTP.URL != /\*.png)"
2  Done
3 > show cr policy-CRD-2
4          Cache-By-Pass RULE: REQ.HTTP.METHOD == POST && (REQ.HTTP.URL
               == '/\*.cgi' || REQ.HTTP.URL != '/\*.png')   Policy:Policy-
               CRD-2
5  Done
6 <!--NeedCopy-->
```

Stratégie qui évalue un en-tête :

```
1 > add cr policy-CRD-3 -rule "REQ.HTTP.HEADER If-Modified-Since EXISTS"
2  Done
3 > show cr policy-CRD-3
4          Cache-By-Pass RULE: REQ.HTTP.HEADER If-Modified-Since EXISTS
                 Policy:Policy-CRD-3
```



```
5  Done
6 <!--NeedCopy-->
```

Ajouter une stratégie de redirection de cache de stratégie avancée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter une stratégie de redirection du cache et vérifier la configuration :

```
1 -  add cr policy <policyName> \*\*-rule\*\* <expression> [-action<
     string>] [-logAction<string>]
2 -  show cr policy [<policyName>]
3 <!--NeedCopy-->
```

Exemples :

Stratégie avec une expression simple :

```
1 > add cr policy crpol1 -rule !(HTTP.REQ.URL.ENDSWITH(".jpeg" )) -action
      origin
2  Done
3 > show cr policy crpoll
4          Policy: crpol1 Rule: !(HTTP.REQ.URL.ENDSWITH(".jpeg")) Action:
               ORIGIN
5  Done
6 <!--NeedCopy-->
```

Stratégie avec une expression composée :

```
1 > add cr policy crpol11 -rule "http.req.method.eq(post) && (HTTP.REQ.
     URL.ENDSWITH(".png") || HTTP.REQ.URL.ENDSWITH(".cgi"))"  -action
     cache
2  Done
3 > show cr policy crpol11
4          Policy: crpol11    Rule: http.req.method.eq(post) && (HTTP.REQ
              .URL.ENDSWITH(".png") || HTTP.REQ.URL.ENDSWITH(".cgi"))
             Action: CACHE
5  Done
6 <!--NeedCopy-->
```

Stratégie qui évalue un en-tête :

```
1 > add cr policy crpol12 -rule http.req.header("If-Modified-Since").
     exists -action origin
```



```
 Done
> show cr policy crpol12
         Policy: crpol12    Rule: http.req.header("If-Modified-Since").
            exists   Action: ORIGIN
 Done
<!--NeedCopy-->
```

Modifier ou supprimer une stratégie de redirection de cache à l'aide de l'interface de ligne de commande

- Pour modifier une stratégie de redirection de cache, utilisez la commande set cr policy, qui est similaire à la commande add cr policy, sauf que vous entrez le nom d'une stratégie existante.
- Pour supprimer une stratégie, utilisez la `rm cr policy` commande, qui n'accepte que l'<name>argument. Si la stratégie est liée à un serveur virtuel, vous devez la dissocier avant de pouvoir la supprimer.

Pour plus d'informations sur la suppression de la liaison d'une stratégie de redirection de cache, voir Délier une stratégie d'un serveur virtuel de redirection de cache.

Configurer une stratégie de redirection de cache avec une expression simple à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Stratégies.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer une stratégie de redirection de cache, dans la zone de texte Nom*, tapez le nom de la stratégie, puis dans la zone Expression, cliquez sur Ajouter.
4. Pour configurer une expression simple, saisissez-la. Voici un exemple d'expression qui vérifie la présence d'une `.jpeg` extension dans une URL :

   - Type d'expression - Général
   - Type de flux -REQ
   - Protocole -HTTP
   - Qualificatif -URL
   - Opérateur - ! =
   - Valeur - /.jpeg

   L'expression simple de l'exemple suivant vérifie la présence d'un en-tête If-Modified-Since dans une demande :

   - Type d'expression - Général
   - Type de flux -REQ

- Protocole -HTTP
- Qualificatif -HEADER
- Opérateur -EXISTS
- Nom de l'en-tête -If-Modified-Since

5. Lorsque vous avez fini de saisir l'expression, cliquez sur OK ou sur Créer, puis cliquez sur Fermer.

Configurer une stratégie de redirection de cache avec une expression composée à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Stratégies.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la zone de texte Nom, saisissez un nom pour la stratégie.

   Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement, et peut comprendre de 1 à 127 lettres, chiffres et les symboles tiret (-), point (.), livre (#), espace (), at (@), égal (=) et trait de soulignement (_). Vous devez choisir un nom qui permettra aux autres utilisateurs de savoir facilement quel type de contenu cette stratégie a été créée pour détecter.
4. Choisissez le type d'expression composée que vous souhaitez créer. Vos choix sont les suivants :

   - **Faites correspondre n'importe quelle expression**. La stratégie correspond au trafic si une ou plusieurs expressions individuelles correspondent au trafic.
   - **Faites correspondre toutes les expressions**. La stratégie ne correspond au trafic que si chaque expression individuelle correspond au trafic.
   - **Expressions tabulaires**. Permet de basculer la liste Expressions au format tabulaire avec trois colonnes. Dans la colonne la plus à droite, vous placez l'un des opérateurs suivants :
     - L'opérateur AND [&&], pour exiger que, pour correspondre à la stratégie, une demande doit correspondre à la fois à l'expression actuelle et à l'expression suivante.

L'opérateur OR [	], pour exiger que, pour correspondre à la stratégie, une demande doit correspondre soit à l'expression actuelle, soit à l'expression suivante, soit aux deux. Ce n'est que si la demande ne correspond pas à l'une ou l'autre des expressions qu'elle ne correspond pas à la stratégie.

–

Vous pouvez également regrouper des expressions dans des sous-groupes imbriqués en sélectionnant une expression existante et en cliquant sur l'un des opérateurs suivants :

- L'opérateur BEGIN SUBGROUP [+ (opérateur)], qui indique à l'appliance Citrix ADC de commencer un sous-groupe imbriqué avec l'expression sélectionnée. (Pour supprimer cet opérateur de l'expression, cliquez sur - (.)
- L'opérateur END SUBGROUP [+)], qui indique à l'appliance Citrix ADC de mettre fin au sous-groupe imbriqué actuel avec l'expression sélectionnée. (Pour supprimer cet opérateur de l'expression, cliquez sur -).)

- **Forme libre avancée**. Désactive complètement l'éditeur d'expressions et transforme la liste Expressions en une zone de texte dans laquelle vous pouvez taper une expression composée. Il s'agit à la fois de la méthode la plus puissante et la plus difficile pour créer une expression de stratégie, et n'est recommandée que pour ceux qui connaissent parfaitement le langage des expressions classiques Citrix ADC.

  Pour plus d'informations sur la création d'expressions classiques dans la zone de texte de forme libre avancée, reportez-vous à la section Configuration des politiques et expressions classiques.

  Attention : Si vous passez en mode avancé d'édition d'expression de forme libre, vous ne pouvez pas revenir à aucun des autres modes. Ne choisissez pas ce mode d'édition d'expression, sauf si vous êtes sûr de vouloir l'utiliser.

5. Si vous avez choisi Correspondance à n'importe quelle expression, Correspondance à toutes les expressions ou Expressions tabulaires, cliquez sur **Ajouter** pour afficher la boîte de dialogue Ajouter une expression.

Vous devez laisser le type d'expression défini sur Général pour les stratégies de redirection du cache.

6. Dans la liste déroulante Type de flux, choisissez un type de flux pour votre expression.

   Le type de flux détermine si la stratégie examine les connexions entrantes ou sortantes. Deux choix s'offrent à vous :

   - **REQ**. Configure l'appliance Citrix ADC pour examiner les connexions entrantes ou les demandes.
   - **RES**. Configure la solution matérielle-logicielle pour qu'elle examine les connexions sortantes ou les réponses.

7. Dans la liste déroulante Protocole, choisissez un protocole pour votre expression.

   Le protocole détermine le type d'informations que la stratégie examine dans la demande ou la réponse. Selon que vous avez choisi REQ ou RES dans la liste déroulante précédente, les quatre ou seulement trois des options suivantes sont disponibles :

   - **HTTP**. Configure la solution matérielle-logicielle pour qu'elle examine l'en-tête HTTP.
   - **SSL**. Configure le dispositif pour qu'il examine le certificat client SSL. Disponible uniquement si vous avez choisi REQ (requêtes) dans la liste déroulante précédente.
   - **TCP**. Configure la solution matérielle-logicielle pour qu'elle examine l'en-tête TCP.
   - **IP**. Configure la solution matérielle-logicielle pour qu'elle examine l'adresse IP source ou de destination.

8. Sélectionnez un qualificatif pour votre expression dans la liste déroulante Qualificatif.

   Le contenu de la liste déroulante Qualificatif dépend du protocole que vous avez choisi. Le tableau suivant décrit les choix disponibles pour chaque protocole.

   Tableau 1. Qualificateurs de stratégie de redirection de cache disponibles pour chaque protocole

Protocole	Qualificatif	Définition
HTTP	METHOD	Méthode HTTP utilisée dans la demande.
-	URL	Contenu de l'en-tête de l'URL.
-	URLTOKENS	Jetons d'URL dans l'en-tête HTTP.
-	VERSION	Version HTTP de la connexion.
-	HEADER	Partie d'en-tête de la requête HTTP.

Protocole	Qualificatif	Définition
-	URLLEN	Longueur du contenu de l'en-tête de l'URL.
-	URLQUERY	Partie de requête du contenu de l'en-tête de l'URL.
-	URLQUERYLEN	Longueur de la partie de requête de l'en-tête de l'URL.
SSL	CLIENT.CERT	Certificat client SSL dans son ensemble.
-	CLIENT.CERT.SUBJECT	Contenu du champ Objet du certificat client.
-	CLIENT.CERT.ISSUER	Émetteur de certificat client.
-	CLIENT.CERT.SIGALGO	Algorithme de signature utilisé dans le certificat client.
-	CLIENT.CERT.VERSION	Version du certificat client.
-	CLIENT.CERT.VALIDFROM	Date à partir de laquelle le certificat client est valide. (La date de début.)
-	CLIENT.CERT.VALIDTO	Date après laquelle le certificat client n'est plus valide. (La date de fin.)
-	CLIENT.CERT.SERIALNUMBER	Numéro de série du certificat client.
-	CLIENT.CIPHER.TYPE	Méthode de chiffrement utilisée dans le certificat client.
-	CLIENT.CIPHER.BITS	Nombre de bits significatifs dans la clé de chiffrement.
-	CLIENT.SSL.VERSION	Version SSL du certificat client.
TCP	SOURCEPORT	Port source de la connexion TCP.
-	DESTPORT	Port de destination de la connexion TCP.

Protocole	Qualificatif	Définition
-	MSS	Taille de segment maximale (MSS) de la connexion TCP.
Adresse IP	SOURCEIP	Adresse IP source de la connexion.
-	DESTIP	Adresse IP de destination de la connexion.

9. Sélectionnez l'opérateur de votre expression dans la liste déroulante Opérateur.

   Vos choix dépendent du qualificatif choisi à l'étape précédente. La liste complète des opérateurs pouvant apparaître dans cette liste déroulante est la suivante :

   - == . Correspond exactement à la chaîne de texte suivante.
   - != . Ne correspond pas à la chaîne de texte suivante.
     - . Est supérieur au nombre entier suivant.
   - CONTAINS . Contient la chaîne de texte suivante.
   - CONTENTS . Le contenu de l'en-tête, de l'URL ou de la requête URL désignés.
   - EXISTS . L'en-tête ou la requête spécifiés existe.
   - NOTCONTAINS . Ne contient pas la chaîne de texte suivante.
   - NOTEXISTS . L'en-tête ou la requête spécifiés n'existe pas.

   Si vous souhaitez que cette stratégie s'applique aux demandes envoyées à un hôte spécifique, vous pouvez laisser le signe par défaut, le signe égal (==).

10. Si la zone de texte Valeur est visible, tapez la chaîne ou le nombre approprié dans la zone de texte.

    Par exemple, si vous souhaitez que cette stratégie sélectionne les demandes envoyées à l'hôte shopping.example.com, vous devez taper cette chaîne dans la zone de texte Valeur.

11. Si vous avez choisi HEADER comme qualificatif, tapez l'en-tête souhaité dans la zone de texte Header Name (Nom de l'en-tête).
12. Cliquez sur OK pour ajouter votre expression à la liste Expression.
13. Répétez les étapes 4 à 11 pour créer des expressions supplémentaires.
14. Cliquez sur Fermer pour fermer la boîte de dialogue Ajouter une expression et revenir à la boîte de dialogue Créer une stratégie de redirection de cache.

Configurations de redirection de cache

January 21, 2021

En fonction de votre déploiement et de la topologie réseau, vous pouvez configurer l'un des types de redirection de cache suivants :

- **Transparent**. Un cache transparent peut résider sur une variété de points le long d'une épine dorsale du réseau afin d'alléger le trafic le long de l'itinéraire de livraison. En mode transparent, le serveur virtuel de redirection de cache intercepte tout le trafic acheminé vers l'appliance Citrix ADC et applique des stratégies de redirection de cache pour déterminer si le contenu doit être diffusé à partir du cache ou du serveur d'origine.
- **Transférer le proxy**. Un serveur de cache proxy de transfert réside à la périphérie d'un réseau local d'entreprise et fait face au réseau étendu. En mode proxy de transfert, le serveur virtuel de redirection de cache résout le nom d'hôte de la requête entrante à l'aide d'un serveur DNS et transmet les demandes de contenu ne pouvant pas être mises en cache aux serveurs d'origine résolus. Les requêtes pouvant être mises en cache sont envoyées aux serveurs de cache configurés.
- **Proxy inverse**. Les caches de proxy inversé sont configurés pour des serveurs d'origine spécifiques. Le trafic entrant dirigé vers le proxy inverse peut être servi à partir d'un serveur de cache ou envoyé au serveur d'origine avec ou sans modification de l'URL.

Configurer la redirection transparente

August 20, 2021

Lorsque vous configurez la redirection transparente du cache, l'appliance Citrix ADC évalue tout le trafic qu'il reçoit, afin de déterminer s'il peut être mis en cache. Ce mode réduit le trafic le long de l'itinéraire de livraison et est souvent utilisé lorsque le serveur de cache réside sur l'épine dorsale d'un fournisseur de services Internet ou d'un transporteur.

Par défaut, les demandes pouvant être mises en cache sont envoyées à un serveur de cache et les demandes non mises en cache au serveur d'origine. Par exemple, lorsque l'appliance Citrix ADC reçoit une demande dirigée vers un serveur Web, elle compare les en-têtes HTTP de la requête avec un ensemble d'expressions de stratégie. Si la demande ne correspond pas à la stratégie, l'appliance transmet la demande à un serveur de cache. Si la demande correspond à une stratégie, l'appliance transmet la demande, inchangée, au serveur Web.

Pour plus d'informations sur la façon de modifier ce comportement par défaut, voir Accès direct à la stratégie vers le cache plutôt que vers l'origine.

Pour configurer la redirection transparente, activez d'abord la redirection du cache et l'équilibrage de charge, puis configurez le mode Edge. Ensuite, créez un serveur virtuel de redirection de cache avec une adresse IP générique (*), afin que ce serveur virtuel puisse recevoir le trafic provenant de l'appliance sur n'importe quelle adresse IP de l'appliance. À ce serveur virtuel, lier des stratégies de redirection de cache qui décrivent les types de requêtes qui ne doivent pas être mises en cache. Ensuite, créez un serveur virtuel d'équilibrage de charge qui recevra le trafic du serveur virtuel de redirection de cache pour les demandes pouvant être mises en cache. Enfin, créez un service qui représente un serveur de cache physique et le lier au serveur virtuel d'équilibrage de charge.

Activer la redirection du cache et l'équilibrage de charge

October 5, 2021

Les fonctionnalités de redirection du cache et d'équilibrage de charge de l'appliance ne sont pas activées par défaut. Ils doivent être activés avant que toute configuration de redirection de cache puisse prendre effet.

Activer la redirection du cache et l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour activer la redirection du cache et l'équilibrage de charge, puis vérifiez les paramètres :

```
-  enable ns feature cr lb
-  show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable ns feature cr lb
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 4)     Content Switching               CS                  ON
 5)     Cache Redirection               CR                  ON
            ...
```



```
13              ...
14              ...
15
16  23)     appliance Push                  push                    OFF
17  Done
18 <!--NeedCopy-->
```

Activer la redirection du cache et l'équilibrage de charge à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Pour activer la redirection du cache, dans le volet d'informations, sous **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.
   a) Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, cochez la case en regard de la **redirection du cache**, puis cliquez sur **OK**.
   b) Dans Activer/Désactiver les fonctionnalités ? , cliquez sur Oui.
3. Pour activer l'équilibrage de charge, dans le volet d'informations, sous **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités de base**.
   a) Dans la boîte de dialogue **Configurer les fonctionnalités de base**, cochez la case en regard de l'équilibrage de charge, puis cliquez sur **OK**.
   b) Dans Activer/Désactiver les fonctionnalités ? , cliquez sur Oui.

Configurer le mode Edge

August 20, 2021

Lorsqu'il est déployé à la périphérie d'un réseau, l'appliance Citrix ADC prend connaissance dynamiquement des serveurs sur ce réseau. Le mode Edge permet à l'appliance de connaître dynamiquement jusqu'à 40 000 serveurs HTTP et connexions TCP proxy pour ces serveurs.

Ce mode active la collecte de statistiques pour les services appris dynamiquement et est généralement utilisé dans les déploiements transparents pour la redirection du cache.

Activer le mode Edge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer le mode Edge et vérifiez le paramètre :

```
1 - enable ns mode Edge
2 - show ns mode
```



```
<!--NeedCopy-->
```

Exemple :

```
> enable ns mode edge
 Done

> show ns mode

        Mode                          Acronym             Status
        -------                       -------             ------
          ...
          ...
          ...
 6)     MAC-based forwarding          MBF                 ON
 7)     Edge configuration            Edge                ON
 8)     Use Subnet IP                 USNIP               OFF
          ...
          ...
          ...
 16)    Bridge BPDUs                  BridgeBPDUs         OFF
 Done
<!--NeedCopy-->
```

Activer le mode Edge à l'aide de l'interface graphique

1. Dans le volet de navigation, développez Système, puis cliquez sur Paramètres.
2. Dans le volet d'informations, sous Modes et fonctionnalités, cliquez sur Configurer les modes.
3. Dans la boîte de dialogue Configurer les modes, activez la case à cocher en regard de la Configuration de la périphérie, puis cliquez sur OK.
4. Dans Activer/Désactiver la ou les fonctions ?, cliquez sur Oui.

Configurer un serveur virtuel de redirection de cache

August 20, 2021

Par défaut, un serveur virtuel de redirection de cache transfère les demandes pouvant être mises en cache au serveur virtuel d'équilibrage de charge pour le cache, et transfère les demandes non mises en cache au serveur d'origine (sauf dans une configuration de proxy inverse, dans laquelle les demandes non mises en cache sont envoyées à un serveur virtuel d'équilibrage de charge). Il existe trois types de serveurs virtuels de redirection de cache : transparents, proxy de transfert et proxy inverse.

Un serveur virtuel de redirection de cache transparent utilise une adresse IP de * et un numéro de port, généralement 80, qui peuvent accepter le trafic HTTP envoyé à n'importe quelle adresse IP que représente l'appliance. Par conséquent, vous ne pouvez configurer qu'un seul serveur virtuel de redirection de cache transparent. Tous les serveurs virtuels de redirection de cache supplémentaires que vous configurez doivent être des serveurs proxy de transfert ou de redirection de proxy inverse.

ajouter un serveur virtuel de redirection de cache en mode transparent à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un serveur virtuel de redirection de cache et vérifier la configuration :

```
1 -  add cr vserver <name> <serviceType> [<IPAddress> <port> ] [-
     cacheType <cacheType>] [-redirect <redirect>]
2 -  show cr vserver [<name>]
3 <!--NeedCopy-->
```

Exemple :

```
1 add cr vserver Vserver-CRD-1 HTTP * 80 -cacheType TRANSPARENT -redirect
      POLICY
2 > show cr vserver Vserver-CRD-1
3         Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
4         State: UP  ARP:DISABLED
5         Client Idle Timeout: 180 sec
6         Down state flush: ENABLED
7         Disable Primary Vserver On Down : DISABLED
8         Default:        Content Precedence: RULE        Cache:
             TRANSPARENT
9         On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
10        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
11  Done
12 <!--NeedCopy-->
```

Modifier ou supprimer un serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

- Pour modifier un serveur virtuel, utilisez la commande set cr vserver, qui ressemble à la commande add cr vserver, sauf que vous entrez le nom d'un serveur virtuel existant.
- Pour supprimer un serveur virtuel, utilisez la commande `rm cr vserver`, qui accepte uniquement l'argument <name>.

Ajouter un serveur virtuel de redirection de cache en mode transparent à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (redirection de cache), spécifiez les valeurs des paramètres suivants comme indiqué :
   - Nom* : nom
   - Port* : port

   *Paramètre obligatoire
4. Dans la liste déroulante Protocole, sélectionnez un protocole pris en charge (par exemple, **HTTP**). Si le serveur virtuel doit recevoir du trafic sur un port autre que le port standard pour le protocole sélectionné, entrez une nouvelle valeur dans le champ Port.
5. Cliquez sur l'onglet Avancé.
6. Vérifiez que Type de cache est défini sur TRANSPARENT et Redirection est défini sur POLICY.
7. Cliquez sur Créer, puis sur Fermer. Le volet Serveurs virtuels de redirection de cache affiche le nouveau serveur virtuel.
8. Sélectionnez le nouveau serveur virtuel de redirection de cache pour afficher les détails de sa configuration.

Lier les stratégies au serveur virtuel de redirection de cache

August 20, 2021

Les stratégies de redirection de cache ne sont pas automatiquement liées au serveur virtuel de redirection de cache. Un serveur virtuel de redirection de cache basé sur une stratégie ne peut pas fonctionner sauf si vous lui liez au moins une stratégie.

Liez des stratégies à un serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 -  bind cr vserver <name> -policyName <string>
2 -  show cr vserver [<name>]
3 <!--NeedCopy-->
```


Exemple :

```
> bind cr vserver Vserver-CRD-1 -policyName bypass-cache-control
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-dynamic-url
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-urltokens
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-cookie
 Done

> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: RULE        Cache:
           TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: bypass-dynamic-url
3)      Cache bypass  Policy: bypass-urltokens
4)      Cache bypass  Policy: bypass-cookie
 Done
<!--NeedCopy-->
```

Liez une stratégie définie par l'utilisateur à un serveur virtuel de redirection de cache à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Cliquez sur le serveur virtuel que vous souhaitez configurer, puis cliquez sur Ouvrir.
3. Sous l'onglet Stratégies, sélectionnez le type de la stratégie, puis cliquez sur Insérer une stratégie.
4. Sous colonne Nom de la stratégie, sélectionnez la stratégie que vous souhaitez lier.
5. Cliquez sur OK.

Supprimer la liaison d'une stratégie d'un serveur virtuel de redirection de cache

August 20, 2021

Lorsque vous dissociez une stratégie du serveur virtuel de redirection de cache, l'appliance Citrix ADC n'applique plus la stratégie lors de l'évaluation des demandes client.

Dissocier une stratégie d'un serveur virtuel de redirection de cache à l'aide de la commande CLI

À l'invite de commandes, tapez :

```
-  unbind cr vserver <name> -policyName <string>
-  show cr vserver [<name>]
<!--NeedCopy-->
```

Exemple :

```
unbind cr vserver Vserver-CR-1 -policyName bypass-non-get
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: RULE        Cache:
           TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
 Done
<!--NeedCopy-->
```

Dissocier une stratégie définie par l'utilisateur d'un serveur virtuel de redirection de cache à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Cliquez sur le serveur virtuel que vous souhaitez configurer, puis cliquez sur Ouvrir.
3. Sous l'onglet Stratégies, sous Nom de la stratégie, sélectionnez la stratégie à dissocier.
4. Cliquez sur Dissocier la stratégie, puis cliquez sur OK.

Créer un serveur virtuel d'équilibrage de charge

August 20, 2021

Le serveur virtuel de redirection de cache sur l'appliance Citrix ADC peut envoyer des demandes à une batterie de serveurs de cache, si la demande est mise en cache, ou à la batterie de serveurs d'origine si la demande n'est pas mise en cache.

Chaque serveur de cache est représenté sur l'appliance par un service, qui est lié à un serveur virtuel d'équilibrage de charge qui reçoit les demandes du serveur virtuel de redirection de cache et transfère ces demandes aux serveurs.

Pour plus d'informations sur la configuration des serveurs virtuels d'équilibrage de charge et d'autres options de configuration, voir Équilibrage de charge.

Créer un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel d'équilibrage de charge et vérifier la configuration :

```
-  add lb vserver <name> <serviceType> [<IPAddress>] [<port>]
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Exemple :

```
> add lb vserver Vserver-LB-CR HTTP 10.102.20.30 80
 Done
> show lb vserver Vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 00:00:08.470
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
```



```
18          Push: DISABLED  Push VServer:
19          Push Multi Clients: NO
20          Push Label Rule: none
21   Done
22  <!--NeedCopy-->
```

Créer un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), spécifiez les valeurs des paramètres suivants comme indiqué :
   - Nom*-nom
   - Adresse IP* - Adresse IP
   - Port *-Port

   *Paramètre obligatoire
4. Dans la liste Protocole, sélectionnez un protocole pris en charge (par exemple, **HTTP**). Si le serveur virtuel doit recevoir du trafic sur un port autre que le port connu pour le protocole sélectionné, entrez une nouvelle valeur dans le champ Port.
5. Cliquez sur Créer, puis sur Fermer. Le volet Serveurs virtuels d'équilibrage de charge affiche le nouveau serveur virtuel.

Configurer un service HTTP

August 20, 2021

Sur l'appliance Citrix ADC, un service représente un serveur physique sur le réseau. Dans la configuration de redirection de cache transparente, le service représente le serveur de cache. Les requêtes pouvant être mises en cache sont envoyées par le serveur virtuel de redirection de cache au serveur virtuel d'équilibrage de charge qui, à son tour, transfère chaque requête au service approprié, qui la transmet au serveur de cache.

Configurer un service HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service HTTP et vérifier la configuration :


```
-  add service <name> <IP> <serviceType> <port> -cacheType <cacheType>
-  show service [<name>]
<!--NeedCopy-->
```

Exemple :

```
> add service Service-HTTP-1 10.102.29.40 HTTP 80 -cacheType
   TRANSPARENT
 Done
> show service Service-HTTP-1
        Service-HTTP-1 (10.102.29.40:80) - HTTP
        State: DOWN
        Last state change was at Fri Jul  2 09:14:17 2010
        Time since last state change: 0 days, 00:00:13.820
        Server Name: 10.102.29.40
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): YES
        Idle timeout: Client: 180 sec   Server: 360 sec
        Client IP: DISABLED
        Cache Type: TRANSPARENT Redirect Mode:
        Cacheable: NO
        SC: OFF
        SP: ON
        Down state flush: ENABLED

1)      Monitor Name: tcp-default
                State: DOWN     Weight: 1
                Probes: 3       Failed [Total: 3 Current: 3]
                Last response: Failure - Time out during TCP connection
                    establishment stage
                Response Time: N/A
 Done
<!--NeedCopy-->
```

Modifier ou supprimer un service à l'aide de l'interface de ligne de commande

- Pour modifier un service, utilisez la commande set service, qui ressemble à la commande add service, sauf que vous entrez le nom d'un service existant.

- Pour supprimer un service, utilisez la commande `rm service`, qui accepte uniquement l'argument <name>.

Ajouter un service HTTP à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Services
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un service, spécifiez les valeurs des paramètres suivants comme indiqué :
   - Nom du service* : nom
   - Serveur*—IP
   - Port* : port

   *Paramètre obligatoire
4. Dans la liste déroulante Protocol*, sélectionnez un protocole pris en charge (par exemple, **HTTP**).
5. Cliquez sur Créer, puis sur Fermer.

Lier/supprimer la liaison d'un service de/vers un serveur virtuel d'équilibrage de charge

August 20, 2021

Vous devez lier un service au serveur virtuel d'équilibrage de charge. Cela permet à l'équilibreur de charge de transférer la demande au serveur représenté par le service. Si votre configuration change, vous pouvez dissocier un service du serveur virtuel d'équilibrage de charge.

Liez un service à un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 -  bind lb vserver <name> <serviceName>
2 -  show lb vserver [<name>]
3 <!--NeedCopy-->
```

Exemple :


```
> bind lb vserver vserver-LB-CR service-HTTP-1
 Done
> show lb vserver Vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 00:42:25.610
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
 Done
<!--NeedCopy-->
```

Dissocier un service d'un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

Pour dissocier un service, utilisez la commande `unbind lb vserver` au lieu de `bind lb vserver`.

Lier/dissocier un service à partir d'un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels
2. Dans le volet d'informations, sélectionnez le serveur virtuel à partir duquel vous souhaitez lier/dissocier le service, puis cliquez sur Ouvrir.
3. Sous l'onglet Services, dans la colonne Actif, coche/désactivez la case à cocher en regard du nom du service.
4. Cliquez sur OK.

Désactiver le paramètre d'utilisation du port proxy pour la mise en cache transparente

August 20, 2021

Si l'option Utiliser l'adresse IP source (USIP) est désactivée sur un service de cache configuré sur l'appliance Citrix ADC, l'appliance transmet les demandes client au service de cache à l'aide d'une adresse IP de sous-réseau (SNIP) appartenant à l'appliance ou d'une adresse IP mappée (MIP) en tant qu'adresse IP source et d'un port aléatoire en tant que port source. Le port sélectionné au hasard est appelé port proxy.

Toutefois, si vous souhaitez configurer un cache entièrement transparent (une configuration de cache dans laquelle le service de cache reçoit l'adresse IP et le numéro de port du client), vous devez non seulement activer l'option USIP, globalement ou sur le service de cache, mais aussi désactiver le paramètre Utiliser le port proxy, globalement ou sur l'onglet service de cache. La désactivation du paramètre Utiliser le port proxy permet à l'appliance d'utiliser le port source du client comme port source lorsqu'elle se connecte au service de cache et garantit une configuration entièrement transparente du cache.

Pour plus d'informations sur la configuration de l'option Utiliser le port proxy globalement ou sur un service, consultez Configuration du port source pour les connexions côté serveur.

Attribuer une plage de ports à l'appliance Citrix ADC

January 21, 2021

Le partage de l'adresse IP du client peut créer un conflit qui empêche les périphériques réseau, tels que les routeurs, les serveurs de cache, les serveurs d'origine et d'autres appliances Citrix ADC, de déterminer l'appliance, et donc le client, auquel la réponse doit être envoyée.

Une méthode pour résoudre ce problème consiste à attribuer une plage de ports source à l'appliance Citrix ADC. Cette allocation permet aux périphériques réseau d'identifier sans ambiguïté l'appliance Citrix ADC qui a envoyé la demande.

Attribuer une plage de ports source à une appliance Citrix ADC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ns param -crPortRange <startPortNumber-endPortNumber>
```


Attribuer une plage de ports source à une appliance Citrix ADC à l'aide de l'interface graphique de l'appliance

1. Dans le volet de navigation, cliquez sur Système, puis sur Paramètres.
2. Dans le groupe Paramètres, cliquez sur le lien Modifier les paramètres système globaux.
3. Dans le groupe Plage de ports de redirection de cache, spécifiez la plage de ports de l'appliance en saisissant un numéro de port pour le port de départ et un numéro de port pour le port de fin.
4. Cliquez sur OK.

Activer l'équilibrage de charge des serveurs virtuels pour rediriger les demandes vers le cache

August 20, 2021

Si un serveur virtuel d'équilibrage de charge est configuré pour écouter sur une combinaison d'adresse IP et de port particulière, il a priorité sur le serveur virtuel de redirection de cache pour toutes les requêtes destinées à cette combinaison adresse-port. Par conséquent, le serveur virtuel de redirection de cache ne traite pas ces demandes.

Si vous souhaitez remplacer cette fonctionnalité et laisser le serveur virtuel de redirection de cache décider si la requête doit être servie à partir du cache ou non, configurez le serveur virtuel d'équilibrage de charge particulier pour être mis en cache.

Une telle configuration est généralement utilisée lorsqu'un fournisseur de services Internet utilise une appliance Citrix ADC à la périphérie de son réseau et que tout le trafic circule à travers l'appliance.

Activer l'équilibrage de charge des serveurs virtuels pour rediriger les demandes vers le cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
-  set lb vserver <name> [-cacheable ( YES | NO)]
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-CR  - cacheable YES
> show lb vserver vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
```



```
6          Time since last state change: 0 days, 01:05:51.510
7          Effective State: DOWN
8          Client Idle Timeout: 180 sec
9          Down state flush: ENABLED
10         Disable Primary Vserver On Down : DISABLED
11         Port Rewrite : DISABLED
12         No. of Bound Services :  1 (Total)       0 (Active)
13         Configured Method: LEASTCONNECTION
14         Mode: IP
15         Persistence: NONE
16         Cacheable: YES  PQ: OFF SC: OFF
17         Vserver IP and Port insertion: OFF
18         Push: DISABLED  Push VServer:
19         Push Multi Clients: NO
20         Push Label Rule: none
21
22 1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
23  Done
24 <!--NeedCopy-->
```

Pour une redirection transparente du cache, l'appliance intercepte tout le trafic et évalue chaque requête afin de déterminer s'il est possible de le mettre en cache. Les demandes non mises en cache sont envoyées inchangées au serveur d'origine.

Lorsque vous utilisez la redirection de cache transparente, vous pouvez désactiver la redirection de cache pour l'équilibrage de charge des serveurs virtuels qui dirigent toujours le trafic vers les serveurs d'origine.

Désactiver la mise en cache d'un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

Pour désactiver la mise en cache d'un serveur virtuel d'équilibrage de charge, utilisez la commande unset lb vserver au lieu de définir lb vserver. Spécifiez la valeur NO pour le paramètre de mise **en cache** .

Activer ou désactiver les serveurs virtuels d'équilibrage de charge pour rediriger les requêtes vers le cache à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel à partir duquel vous souhaitez activer/désactiver la mise en cache, puis cliquez sur Ouvrir.
3. Sous l'onglet Avancé, coche/désactivez la case à cocher Redirection du cache.
4. Cliquez sur OK.

Configurer la redirection de proxy de transfert

August 20, 2021

Un proxy de transfert est un point de contact unique pour un client ou un groupe de clients. Dans cette configuration, l'appliance Citrix ADC redirige les demandes non mises en cache vers un serveur d'origine et redirige les demandes pouvant être mises en cache vers un cache proxy de transfert ou un cache transparent.

Lorsque l'appliance est configurée en tant que proxy de transfert, les utilisateurs doivent modifier leurs navigateurs afin que le navigateur envoie des demandes au proxy de transfert au lieu des serveurs de destination.

Un serveur virtuel de redirection de cache proxy de transfert sur l'appliance compare la demande avec une stratégie de mise en cache. Si la demande n'est pas mise en cache, l'appliance interroge un serveur virtuel d'équilibrage de charge DNS pour la résolution de la destination, puis envoie la demande au serveur d'origine. Si la demande peut être mise en cache, l'appliance transmet la demande à un serveur virtuel d'équilibrage de charge pour le cache.

L'appliance s'appuie sur un nom de domaine hôte ou une adresse IP dans l'en-tête HOST de la demande pour déterminer la destination demandée. S'il n'y a pas d'en-tête HOST dans la demande, l'appliance insère un en-tête HOST basé sur l'adresse IP de destination dans la demande.

Généralement, l'appliance Citrix ADC agit comme un proxy de transfert dans un réseau local d'entreprise. Dans une telle configuration, l'appliance réside à la périphérie d'un réseau local d'entreprise et intercepte les demandes des clients avant qu'elles ne soient acheminés vers le réseau étendu. La configuration de l'appliance en mode proxy de transfert réduit le trafic sur le WAN.

Pour configurer la redirection du cache proxy de transfert, activez tout d'abord l'équilibrage de charge et la redirection du cache sur l'appliance. Ensuite, configurez un serveur virtuel d'équilibrage de charge DNS et les services associés. Configurez également un serveur virtuel d'équilibrage de charge et liez-lui les services appropriés pour le cache. Configurez un serveur virtuel de redirection de cache proxy de transfert et liez le DNS et les serveurs virtuels d'équilibrage de charge à celui-ci. Vous devez également configurer les stratégies de mise en cache et les lier au serveur virtuel de redirection de cache. Pour terminer la configuration, configurez les navigateurs clients pour qu'ils utilisent le proxy de transfert.

Pour plus d'informations sur la façon d'activer la redirection du cache et l'équilibrage de charge sur l'appliance, voir Activer la redirection du cache et l'équilibrage de charge.

Pour plus d'informations sur la création d'un serveur virtuel d'équilibrage de charge, voir Créer un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la configuration des services représentant le serveur de cache, voir Configurer un service HTTP.

Pour plus d'informations sur la façon de lier le service à un serveur virtuel, voir Lier/dissocier un service vers/depuis un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la création d'un serveur de redirection de cache proxy de transfert, consultez Configurer un serveur virtuel de redirection de cacheet créer un serveur virtuel de type TRANSPARENT ou FORWARD.

Pour plus d'informations sur la liaison des stratégies de redirection du cache au serveur virtuel de redirection du cache, voir Configurer une stratégie de redirection de cache.

Créer un service DNS

August 20, 2021

Un service DNS est une représentation, sur l'appliance Citrix ADC, d'un serveur DNS physique dans le réseau. Un serveur virtuel d'équilibrage de charge DNS envoie des demandes DNS au serveur DNS du réseau via un tel service.

Créer un service DNS à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour créer un service DNS et vérifier la configuration :

```
-  add service <name> <IP> <serviceType> <port>
-  show service [<name>]
<!--NeedCopy-->
```

Exemple :

```
add service Service-DNS-1 10.102.29.41 DNS 53
show service Service-DNS-1
        Service-DNS-1 (10.102.29.41:53) - DNS
        State: DOWN
        Last state change was at Fri Jul  2 10:14:32 2010
        Time since last state change: 0 days, 00:00:13.550
        Server Name: 10.102.29.41
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
```



```
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: ping-default
                State: DOWN     Weight: 1
                Probes: 3       Failed [Total: 3 Current: 3]
                Last response: Failure - Probe timed out.
                Response Time: 2000.0 millisec
 Done
<!--NeedCopy-->
```

Ajouter un service DNS à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un service, spécifiez les valeurs des paramètres suivants comme indiqué :
   - Nom du service* : nom
   - Serveur*—IP
   - Port* : port

*Paramètre obligatoire

1. Dans la liste déroulante Protocol*, sélectionnez un protocole pris en charge (par exemple, **DNS**).
2. Cliquez sur Créer, puis sur Fermer.

Créer un serveur virtuel d'équilibrage de charge DNS

August 20, 2021

Le serveur virtuel DNS permet au proxy de transfert d'effectuer la résolution DNS avant de transférer une demande client à un serveur d'origine. Le serveur virtuel d'équilibrage de charge DNS est associé au service DNS qui représente le serveur DNS physique sur le réseau.

Créer un serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour créer un serveur virtuel d'équilibrage de charge DNS et vérifier la configuration :

```
-  add lb vserver <name> <serviceType>
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Exemple :

```
> add lb vserver Vserver-DNS-1 DNS
 Done
> show lb vserver Vserver-DNS-1
        Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 10:32:28 2010
        Time since last state change: 0 days, 00:00:08.10
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
 Done
<!--NeedCopy-->
```

Créer un serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), dans la zone Nom, tapez un nom pour le serveur virtuel.
4. Dans la liste déroulante Protocol*, sélectionnez un protocole pris en charge (par exemple, **DNS**).
5. Cliquez sur Créer, puis sur Fermer. Le volet Serveurs virtuels DNS affiche le nouveau serveur virtuel.

Lier le service DNS au serveur virtuel

August 20, 2021

Pour que le serveur DNS réponde aux demandes DNS, le service représentant le serveur DNS doit être lié au serveur virtuel DNS.

Liez le service DNS au serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier le service DNS au serveur virtuel d'équilibrage de charge et vérifiez la configuration :

```
-  bind lb vserver <name> <serviceName>
-  show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> bind lb vserver Vserver-DNS-1 Service-DNS-1
 Done
> show lb vserver Vserver-DNS-1
        Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 10:32:28 2010
        Time since last state change: 0 days, 00:12:16.80
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE

1) Service-DNS-1 (10.102.29.41: 53) - DNS State: DOWN   Weight: 1
 Done
>
<!--NeedCopy-->
```


Dissocier un service DNS du serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

Utilisez la commande `unbind lb vserver` au lieu de `bind lb vserver`.

Lier/supprimer la liaison d'un service DNS de/vers un serveur virtuel d'équilibrage de charge à partir de l'interface

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels
2. Dans le volet d'informations, sélectionnez le serveur virtuel vers/à partir duquel vous souhaitez lier/dissocier le service DNS, puis cliquez sur Ouvrir.
3. Sous l'onglet Services, dans la colonne Actif, coche/désactivez la case à cocher en regard du nom du service.
4. Cliquez sur OK.

Configurer un navigateur Web client pour utiliser un proxy de transfert

January 21, 2021

Lorsque vous configurez l'appliance Citrix ADC en tant que serveur virtuel de redirection de cache proxy de transfert dans le réseau, vous devez configurer le navigateur Web client pour envoyer des demandes au proxy de transfert. Généralement, lorsque vous utilisez un proxy de transfert, la seule route vers les serveurs du réseau est via le proxy de transfert.

Reportez-vous à la documentation de votre navigateur pour configurer le navigateur afin qu'il utilise un proxy de transfert. Spécifiez l'adresse IP et le numéro de port du serveur virtuel de redirection du cache proxy de transfert pour cette configuration.

Configurer la redirection de proxy inverse

August 20, 2021

Un proxy inverse réside devant un ou plusieurs serveurs Web et protège le serveur d'origine contre les demandes des clients. Souvent, un cache proxy inverse est un frontal pour toutes les requêtes client à un serveur. Un administrateur affecte un cache proxy inverse à un serveur d'origine spécifique. Le cache proxy inverse est différent des caches proxy transparents et transparents, qui mettent en cache le contenu fréquemment demandé pour toutes les demandes adressées à n'importe quel serveur d'origine, et le choix d'un serveur est basé sur la demande.

Contrairement à un cache de proxy transparent, le cache de proxy inverse a sa propre adresse IP et peut remplacer les domaines et URL de destination dans une requête non mise en cache par de nouveaux domaines et URL de destination.

Vous pouvez déployer la redirection du cache proxy inverse du côté serveur d'origine ou au bord d'un réseau. Lorsqu'il est déployé sur le serveur d'origine, le serveur virtuel de redirection de cache proxy inverse est un frontal pour toutes les demandes adressées au serveur d'origine.

En mode proxy inverse, lorsque l'appliance reçoit une demande, un serveur virtuel de redirection de cache évalue la demande et la transmet à un serveur virtuel d'équilibrage de charge pour le cache ou à un serveur virtuel d'équilibrage de charge pour l'origine. La demande entrante peut être transformée en modifiant l'en-tête de l'hôte ou l'URL de l'hôte avant qu'elle ne soit envoyée au serveur principal.

Pour configurer la redirection du cache proxy inverse, activez d'abord la redirection du cache et l'équilibrage de charge. Ensuite, configurez un serveur virtuel d'équilibrage de charge et des services pour envoyer des demandes de mise en cache aux serveurs de cache. Configurez également un serveur virtuel d'équilibrage de charge et les services associés pour les serveurs d'origine. Ensuite, configurez un serveur virtuel de redirection de cache proxy inverse et liez les stratégies de redirection de cache pertinentes à celui-ci. Enfin, configurez les stratégies de mappage et liez-les au serveur virtuel de redirection de cache proxy inverse.

Les stratégies de mappage ont une action associée qui permet au serveur virtuel de redirection de cache de transférer toute demande non mise en cache vers le serveur virtuel d'équilibrage de charge pour l'origine.

Assurez-vous de créer la destination du serveur de cache par défaut.

Pour plus d'informations sur la façon d'activer la redirection du cache et l'équilibrage de charge sur l'appliance, voir Activer la redirection du cache et l'équilibrage de charge.

Pour plus d'informations sur la création d'un serveur virtuel d'équilibrage de charge, voir Créer un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la configuration des services représentant le serveur de cache, voir Configurer un service HTTP.

Pour plus d'informations sur la façon de lier le service à un serveur virtuel, voir Lier/dissocier un service vers/depuis un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la création d'un serveur de redirection de cache proxy inverse, voir Configurer un serveur virtuel de redirection de cacheet créer un serveur virtuel de type REVERSE.

Pour plus d'informations sur la liaison des stratégies de redirection de cache intégrées au serveur virtuel de redirection du cache, voir Lier les stratégies au serveur virtuel de redirection du cache.

Configurer les stratégies de mappage

Si une requête entrante n'est pas mise en cache, le serveur virtuel de redirection de cache de proxy inverse remplace le domaine et l'URL de la requête par le domaine et l'URL d'un serveur d'origine cible et transmet la demande au serveur virtuel d'équilibrage de charge pour l'origine.

Une stratégie de mappage permet au serveur virtuel de redirection de cache proxy inverse de remplacer le domaine de destination et l'URL et de transférer la demande au serveur virtuel d'équilibrage de charge pour l'origine.

Une stratégie de mappage doit d'abord traduire le domaine et l'URL, puis transmettre la demande au serveur virtuel d'équilibrage de charge d'origine.

Une stratégie de mappage peut mapper un domaine, un préfixe d'URL et un suffixe d'URL, comme suit :

- Mappage de domaine : vous pouvez mapper un domaine sans préfixe ni suffixe. Le mappage de domaine est le mappage par défaut du serveur virtuel (par exemple, mappage de www.mycompany.com vers www.myrealcompany.com).
- Mappage de préfixe : Vous pouvez remplacer un modèle spécifié préfixé dans le cadre de l'URL (par exemple, mappage de www.mycompany.com/sports/index.html à www.mycompany.com/news/index.
- Correspondance de suffixe : Vous pouvez remplacer le suffixe de fichier dans l'URL (par exemple, mappage de www.mycompany.com/sports/index.html à www.mycompany.com/sports/index.asp).

Les chaînes source et destination en cours de mappage doivent être similaires. Si vous spécifiez un domaine source, vous devez spécifier un domaine de destination, et si vous spécifiez un suffixe source, vous devez spécifier un suffixe de destination. De même, si vous spécifiez une URL exacte à partir de la source, l'URL cible doit également être une URL exacte.

Une fois que vous avez configuré des stratégies de mappage pour le mode proxy inverse, vous devez les lier au serveur virtuel de redirection de cache.

Vous pouvez utiliser des combinaisons d'URL source, d'URL cible et de domaines source et cible pour configurer les trois types de mappage de domaine.

Configurer une stratégie de mappage pour le mode proxy inverse à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour ajouter un mappage de stratégies et vérifier la configuration :

```
1 - add policy map <mapPolicyName> -sd <string> [-su <string>] [-td <
    string>] [-tu <string>]
2 - show policy map [<mapPolicyName>]
3 <!--NeedCopy-->
```


Exemple :

La commande suivante mappe un domaine dans une demande client à un domaine cible :

```
> add policy map myMappingPolicy -sd www.mycompany.com -td www.
   myrealcompany.com
 Done
> show policy map myMappingPolicy
1)      Name: myMappingPolicy
        Source Domain: www.mycompany.com        Source Url:
        Target Domain: www.myrealcompany.com    Target Url:
 Done
<!--NeedCopy-->
```

Voici un exemple de mappage d'un suffixe d'URL à un autre suffixe d'URL :

```
> add policy map myOtherMappingPolicy -sd www.mycompany.com -td www.
   myrealcompany.com -su /news.html -tu /realnews.html
 Done
> show policy map myOtherMappingPolicy
1)      Name: myOtherMappingPolicy
        Source Domain: www.mycompany.com        Source Url: /news.html
        Target Domain: www.myrealcompany.com    Target Url: /realnews.
           html
 Done
<!--NeedCopy-->
```

Configurer une stratégie de mappage pour le mode proxy inverse à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Stratégies de carte**.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer une stratégie de carte, spécifiez les valeurs des paramètres suivants comme indiqué :
   - Nom*- mapPolicyName
   - Domaine source*-sd
   - Domaine cible*-td
   - URL source-su
   - URL cible-tu

   *Paramètre obligatoire
4. Cliquez sur Créer, puis sur Fermer. Le volet Carte affiche la nouvelle stratégie de mappage.

Liez la stratégie de mappage au serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier la stratégie de mappage au serveur virtuel de redirection de cache et vérifier la configuration :

```
-  bind cr vserver <name> -policyName <string> [<targetVserver>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> bind cr vserver Vserver-CRD-3 -policyName myMappingPolicy Vserver-LB-
    CR
 Done
> show cr vserver Vserver-CRD-3
        Vserver-CRD-3 (10.102.29.50:88) - HTTP  Type: CONTENT
        State: UP
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default: Vserver-LB-CR  Content Precedence: RULE        Cache:
           REVERSE
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Policy:         Target: Vserver-LB-CR   Priority: 0     Hits: 0
1)      Map: myMappingPolicy Target: Vserver-LB-CR
 Done
<!--NeedCopy-->
```

Liez la stratégie de mappage au serveur virtuel de redirection de cache à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel à partir duquel vous souhaitez lier la stratégie de mappage, puis cliquez sur **Ouvrir**.
3. Dans **Configurer le serveur virtuel**(redirection du cache), sous **l'onglet Stratégies**, sélectionnez **Carte**, puis cliquez sur **Insérer une stratégie**.
4. Dans la colonne **Nom de la stratégie**, sélectionnez la stratégie dans la liste déroulante.
5. Dans la colonne **Target**, cliquez sur la flèche vers le bas, puis sélectionnez le serveur virtuel dans la liste déroulante.
6. Cliquez sur **OK**.

Redirection sélective du cache

August 20, 2021

La redirection sélective du cache envoie des demandes pour des types particuliers de contenu, par exemple des images, à un serveur de cache ou à un groupe de serveurs de cache et envoie d'autres types de contenu à un serveur de cache ou à un groupe de serveurs de cache différent. Vous pouvez configurer la redirection avancée du cache en modes Transparent, Inverse Proxy ou Transparent.

Dans la redirection sélective du cache, l'appliance Citrix ADC intercepte une demande client et transfère les demandes non mises en cache vers la destination d'origine dans la demande client. Pour les demandes pouvant être mises en cache, l'appliance envoie les demandes au serveur de cache de destination qui peut servir du contenu d'un type de contenu spécifique.

La redirection sélective du cache implique la configuration de stratégies de commutation de contenu en plus des stratégies de redirection du cache. L'appliance évalue d'abord les stratégies de redirection de cache liées au serveur virtuel de redirection de cache. Si une demande correspond à une stratégie de redirection de cache, le serveur virtuel de redirection de cache envoie la demande au serveur d'origine ou à un serveur virtuel d'équilibrage de charge pour l'origine. Si aucune stratégie de redirection de cache ne correspond à la demande, l'appliance évalue les stratégies de commutation de contenu liées au serveur virtuel de redirection de cache. Si une stratégie de commutation de contenu correspond à la demande, le serveur virtuel de redirection de cache redirige la demande vers un serveur virtuel d'équilibrage de charge pour le cache.

Pour configurer la redirection sélective du cache, activez tout d'abord la redirection du cache, l'équilibrage de charge et la commutation de contenu sur l'appliance Citrix ADC. Ensuite, configurez un serveur virtuel d'équilibrage de charge pour le cache et un service HTTP associé. Après cela, configurez un serveur virtuel de redirection de cache et liez à la fois les stratégies de redirection de cache et de commutation de contenu. Une fois que vous avez lié les stratégies, vous pouvez configurer le serveur virtuel pour donner la priorité aux stratégies de commutation de contenu basées sur une règle ou une URL.

Lorsqu'elle est configurée pour la redirection du cache en mode transparent dans une topologie de déploiement périphérique, l'appliance envoie tout le trafic HTTP pouvant être mis en cache à une batterie de cache transparente. Les clients accèdent à Internet via l'appliance, configurée en tant que commutateur de couche 4 recevant du trafic sur le port 80.

L'appliance peut diriger les demandes d'images (par exemple, des fichiers .png et .jpg) vers un serveur de la batterie de cache transparente, et toutes les autres demandes de contenu statique vers d'autres serveurs de la batterie. Pour cette configuration, vous configurez les stratégies de commutation de contenu pour envoyer des images au cache d'image et envoyer tous les autres contenus pouvant être mis en cache dans un cache par défaut.

Remarque : La configuration décrite ici concerne la redirection du cache sélectif transparent. Par conséquent, il ne nécessite pas un serveur virtuel d'équilibrage de charge pour l'origine, de même qu'une configuration de proxy inverse.

Pour configurer ce type de redirection sélective du cache, activez d'abord la redirection du cache, l'équilibrage de charge et la commutation de contenu. Ensuite, configurez un serveur virtuel d'équilibrage de charge pour le cache et configurez un service HTTP associé. Ensuite, configurez un serveur virtuel de redirection de cache et créez et liez les stratégies de redirection de cache et de commutation de contenu à ce serveur virtuel.

Pour plus d'informations sur la façon d'activer la redirection du cache et l'équilibrage de charge sur l'appliance, voir Activer la redirection du cache et l'équilibrage de charge.

Activer la commutation de contenu

October 5, 2021

Pour configurer la redirection sélective du cache, après avoir activé les fonctionnalités d'équilibrage de charge et de redirection du cache sur l'appliance, vous devez activer la commutation de contenu.

Activer la commutation de contenu à l'aide de la CLI

À l'invite de commandes, tapez :

```
-  enable ns feature CS

-  show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable ns feature cs
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 4)     Content Switching               CS                  ON
 5)     Cache Redirection               CR                  ON
          ...
```



```
13            ...
14            ...
15  23)     appliance Push                  push                  OFF
16  Done
17 <!--NeedCopy-->
```

Activer la redirection du cache et l'équilibrage de charge à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Dans le volet d'informations, sous Modes et fonctionnalités, cliquez sur **Configurer les fonctionnalités de base**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités de base**, cochez la case en regard du **changement de contenu**, puis cliquez sur **OK**.
4. Dans Activer/Désactiver les fonctionnalités ? , cliquez sur Oui.

Configurer un serveur virtuel d'équilibrage de charge pour le cache

August 20, 2021

Créez un serveur virtuel d'équilibrage de charge et un service HTTP pour chaque type de serveur de cache qui sera utilisé. Par exemple, si vous souhaitez servir des fichiers JPEG d'un serveur de cache et des fichiers GIF d'un autre serveur de cache et utiliser un troisième serveur de cache pour le reste du contenu, créez un service HTTP et un serveur virtuel pour chacun des trois types de serveurs de cache. Ensuite, liez chaque service à son serveur virtuel respectif.

Pour plus d'informations sur la création d'un serveur virtuel d'équilibrage de charge, voir Créer un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la configuration des services représentant le serveur de cache, voir Configurer un service HTTP.

Pour plus d'informations sur la façon de lier le service à un serveur virtuel, voir Lier/dissocier un service vers/depuis un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la création d'un serveur de redirection de cache proxy transparent, voir Configurer un serveur virtuel de redirection de cacheet créer un serveur virtuel de type TRANSPARENT.

Pour plus d'informations sur la liaison des stratégies de redirection de cache intégrées au serveur virtuel de redirection du cache, voir Lier les stratégies au serveur virtuel de redirection du cache.

Configurer une stratégie de redirection de cache pour un type de contenu spécifique

Pour identifier les demandes qui contiennent une extension .png ou .jpeg en tant que mise en cache, vous configurez une stratégie de redirection de cache et la liez au serveur virtuel de redirection de cache.

Remarque : si une demande correspond à une stratégie, l'appliance Citrix ADC la transmet au serveur d'origine. Par conséquent, dans la procédure suivante, vous configurez les stratégies pour qu'elles correspondent aux demandes qui n'ont
pas d'extensions « .png » ou « .jpeg ».

Pour configurer la redirection du cache pour un type de contenu spécifique, configurez une stratégie qui utilise une expression simple, comme décrit dans Configurer une stratégie de redirection de cache.

Configurer les stratégies de commutation de contenu

October 5, 2021

Vous devez créer une stratégie de commutation de contenu pour identifier les types spécifiques de contenu à mettre en cache dans un serveur de cache ou une batterie de serveurs et identifier d'autres types de contenu à diffuser à partir d'un autre serveur de cache ou batterie de serveurs. Par exemple, vous pouvez configurer une stratégie pour déterminer l'emplacement des fichiers image portant les extensions .png et .jpeg.

Après avoir défini la stratégie de commutation de contenu, vous la liez à un serveur virtuel de redirection de cache et spécifiez un serveur virtuel d'équilibrage de charge. Les demandes qui correspondent à la stratégie sont transférées vers le serveur virtuel d'équilibrage de charge nommé. Les demandes qui ne correspondent pas à la stratégie de commutation de contenu sont transférées au serveur virtuel d'équilibrage de charge par défaut pour le cache.

Pour plus d'informations sur la fonction de commutation de contenu et la configuration des stratégies de commutation de contenu, voir Commutation de contenu.

Vous devez d'abord créer la stratégie de commutation de contenu, puis la lier au serveur virtuel de redirection de cache.

Créer une stratégie de commutation de contenu à l'aide de la commande CLI

Sur la ligne de commande, tapez :

```
1 -  add cs policy <policyName> [-url <string> | -rule <expression>]
2 -  show cs policy [<policyName>]
3 <!--NeedCopy-->
```


Exemples :

```
> add cs policy-CS-JPEG -rule "REQ.HTTP.URL == '/\*.jpeg'"
 Done
> show cs policy-CS-JPEG
         Rule: REQ.HTTP.URL == '/\*.jpeg'         Policy: Policy-CS-
            JPEG
         Hits: 0
 Done
>

> add cs policy-CS-GIF -rule "REQ.HTTP.URL == '/ *.png'"
 Done
> show cs policy-CS-GIF
         Rule: REQ.HTTP.URL == '/ *.png'         Policy: Policy-CS-GIF
         Hits: 0
 Done
>

> add cs policy-CS-JPEG-URL -url /\*.jpg
 Done
> show cs policy-CS-JPEG-URL
         URL: /\*.jpg     Policy: Policy-CS-JPEG-URL
         Hits: 0
 Done
>

> add cs policy-CS-GIF-URL -url /\*.png
 Done
> show cs policy-CS-GIF-URL
         URL: /\*.png     Policy: Policy-CS-GIF-URL
         Hits: 0
 Done
<!--NeedCopy-->
```

Créer une stratégie de changement de contenu basée sur une URL à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Changement de contenu > Stratégies.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer une stratégie de commutation de contenu, dans la zone de texte Nom, tapez un nom pour la stratégie.
4. Sélectionnez le bouton radio URL.

5. Dans la zone de texte Valeur, tapez la valeur de la chaîne (par exemple, **/sports**).
6. Cliquez sur Créer, puis sur Fermer. La stratégie que vous avez créée apparaît dans la page Content Switching Policies.

Créer une stratégie de changement de contenu basée sur des règles à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Changement de contenu > Stratégies.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer une stratégie de commutation de contenu, dans la zone de texte Nom, tapez un nom pour la stratégie.
4. Sélectionnez le bouton radio Expression, puis cliquez sur Configurer.
5. Dans la boîte de dialogue Créer une expression, choisissez la syntaxe d'expression que vous souhaitez utiliser.
   - Si vous souhaitez utiliser la stratégie avancée, acceptez la valeur par défaut et passez à l'étape suivante.
   - Si vous souhaitez utiliser la syntaxe classique, cliquez sur Basculer vers la syntaxe classique.

   La partie Expression de la boîte de dialogue change en fonction de votre choix. La vue Expression de stratégie avancée comporte moins d'éléments que la vue Expression de syntaxe classique. Dans la vue Expression de stratégie avancée, au lieu d'une fenêtre d'aperçu, un bouton permet d'accéder à un évaluateur d'expression. L'évaluateur évalue l'expression que vous avez entrée pour vérifier qu'elle est valide, puis affiche une analyse de l'effet de l'expression.
6. Entrez vos expressions de stratégie.

   Pour plus d'informations sur l'utilisation de la syntaxe avancée, voir Configurer l'expression de stratégie avancée : Commencer.
7. Cliquez sur **Créer**, puis sur **Fermer**. La stratégie que vous avez créée apparaît dans le volet **Stratégies de changement de contenu** .

Liez la stratégie de commutation de contenu à un serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier la stratégie de commutation de contenu à un serveur virtuel de redirection de cache et vérifiez la configuration :

```
1 - bind cs vserver <name> <targetVserver> [-policyName <string>]
2 - show cs vserver [<name>]
```



```
<!--NeedCopy-->
```

Exemple :

```
> bind cs vserver Vserver-CR-1 lbcachejpeg -policyName Policy-CS-JPEG
 Done
> bind cs vserver Vserver-CR-1 lbcachegif -policyName Policy-CS-GIF
 Done
> show cs vserver Vserver-CR-1
        Vserver-CR-1 (10.102.29.60:80) - HTTP   Type: CONTENT
        State: UP
        Last state change was at Fri Jul  2 12:53:45 2010
        Time since last state change: 0 days, 00:00:58.920
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        State Update: DISABLED
        Default:        Content Precedence: RULE
        Cacheable: YES
        Vserver IP and Port insertion: OFF
        Case Sensitivity: ON
        Push: DISABLED  Push VServer:
        Push Label Rule: none

1)      Policy: Policy-CS-JPEG  Target: lbcachejpeg     Priority: 0
       Hits: 0
2)      Policy: Policy-CS-GIF   Target: lbcachegif      Priority: 0
       Hits: 0
 Done
>
<!--NeedCopy-->
```

Liez la stratégie de commutation de contenu à un serveur virtuel de redirection de cache à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez lier la stratégie (par exemple, **vServer-CS-1**), puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue Configurer le serveur virtuel (commutation de contenu), sous **l'onglet Stratégies**, cliquez sur CSW, puis sur **Insérer une stratégie**.

4. Dans la colonne **Nom de la stratégie**, sélectionnez la stratégie que vous souhaitez configurer pour le serveur virtuel de commutation de contenu.
5. Dans la colonne **Target**, cliquez sur la flèche verte et sélectionnez le serveur virtuel d'équilibrage de charge cible dans la liste.
6. Cliquez sur **OK**.

Configurer la priorité pour l'évaluation des stratégies

August 20, 2021

Vous pouvez configurer une stratégie de commutation de contenu en fonction soit d'une règle, qui est une configuration générique pour prendre en charge différents types de contenu, soit d'une URL, plus spécifique et définissant exactement le type de contenu à envoyer à un serveur de cache particulier. Essentiellement, le même contenu peut être défini par une stratégie basée sur des règles ou une stratégie basée sur des URL.

Une fois que vous avez lié des stratégies de commutation de contenu de l'un ou l'autre type à un serveur virtuel de redirection de cache, vous pouvez configurer le serveur virtuel pour donner la priorité aux stratégies basées sur une règle ou une URL. Cela déterminera à son tour les serveurs vers lesquels les requêtes particulières sont dirigées.

Pour configurer la priorité pour l'évaluation de stratégie, utilisez le paramètre de priorité, qui spécifie le type de stratégie (URL ou RULE) qui a priorité sur le serveur virtuel de redirection de contenu.

Valeurs possibles : RULE, URL

Valeur par défaut : RULE

Configurer la priorité pour l'évaluation des stratégies à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la priorité pour l'évaluation des stratégies et vérifier la configuration :

```
1 -  set cr vserver <name> [-precedence (RULE | URL)]
2 -  show cr vserver <name>
3 <!--NeedCopy-->
```

Exemple :

```
1 > set cr vserver Vserver-CRD-1 -precedence URL
2  Done
```



```
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>
<!--NeedCopy-->
```

Configurer la priorité pour l'évaluation des stratégies à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Changement de contenu > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer la priorité (par exemple, **vServer-CS-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (Commutation de contenu), sous l'onglet Avancé, en regard de Priorité, cliquez sur Règle ou URL, puis cliquez sur OK.

Administrer un serveur virtuel de redirection de cache

January 21, 2021

Pour administrer un serveur virtuel de redirection de cache, vous devez afficher les statistiques de redirection de cache. Vous devrez peut-être activer ou désactiver les serveurs de redirection de cache ou diriger les appels de stratégie vers le cache au lieu de l'origine. Les tâches administratives incluent également la sauvegarde d'un serveur virtuel de redirection de cache et la gestion des connexions client.

Afficher les statistiques de redirection du cache du serveur virtuel

August 20, 2021

Vous pouvez afficher les propriétés d'un serveur virtuel de redirection de cache et les statistiques sur le trafic passé par un serveur virtuel de redirection de cache. Vous pouvez également afficher les serveurs virtuels de redirection de cache et les stratégies que vous avez liés à l'équilibrage de charge des serveurs virtuels.

Pour afficher les statistiques d'un serveur virtuel de redirection de cache spécifique, utilisez le paramètre name pour spécifier le nom du serveur virtuel pour lequel les statistiques seront affichées. Sinon, les statistiques de tous les serveurs virtuels de redirection de cache sont affichées. Longueur maximale : 127

Afficher les statistiques d'un serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat cr vserver [<name>]
```

Exemple :

```
1  > stat cr vserver Vserver-CRD-1
2
3  Vserver Summary
4                            IP  port     Protocol        State
5  Vser...CRD-1         0.0.0.0    80         HTTP           UP
6
7  VServer Stats:
8                                          Rate (/s)
                                              Total
9  Requests                                       0
                         0
10 Responses                                      0
                         0
11 Request bytes                                  0
                         0
12 Response bytes                                 0
                         0
13
14  Done
15 >
16 <!--NeedCopy-->
```


Afficher les statistiques d'un serveur virtuel de redirection de cache à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez afficher les statistiques (par exemple, **vServer-CRD-1**), puis cliquez sur Statistiques.

omettez le nom du serveur pour afficher les statistiques de base pour tous les serveurs virtuels de redirection de cache. Inclure le nom du serveur pour afficher des statistiques détaillées pour ce serveur virtuel, y compris le nombre et la taille des demandes et des réponses qui passent par le serveur virtuel

Afficher les statistiques d'un serveur virtuel de redirection de cache à l'aide des utilitaires de surveillance et de tableau de bord

1. Pour afficher les statistiques à l'aide des utilitaires de surveillance, cliquez sur l'onglet Surveillance.
2. Dans le menu déroulant Sélectionner un groupe, choisissez Serveurs virtuels CR. Une liste des serveurs virtuels de redirection de cache apparaît.
3. Pour afficher les statistiques à l'aide des utilitaires de tableau de bord, cliquez sur l'onglet Tableau de bord.
4. Cliquez sur Client d'applet ou Client de démarrage Web en regard de l'utilitaire statistique.
5. Dans le menu déroulant Sélectionner un groupe, choisissez Serveurs virtuels CR. Le tableau de bord affiche des statistiques récapitulatives pour les serveurs virtuels de redirection de cache.
6. Pour afficher un graphique de l'activité du serveur virtuel, cliquez sur Graphique. Une représentation graphique des statistiques du serveur virtuel apparaît.

Activer ou désactiver un serveur virtuel de redirection de cache

January 21, 2021

Lorsque vous créez un serveur virtuel de redirection de cache, il est activé par défaut. Si vous désactivez un serveur virtuel de redirection de cache, son état passe à OUT OF SERVICE et il arrête de rediriger les requêtes client mises en cache. Toutefois, l'appliance Citrix ADC continue de répondre aux demandes ARP et ping pour l'adresse IP de ce serveur virtuel.

Activer ou désactiver un serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez l'une des commandes suivantes :


```
-  enable cr vserver <name>
-  show cr vserver <name>
-  disable cr vserver <name>
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemples :

```
> enable cr vserver Vserver-CRD-1
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>

> disable cr vserver Vserver-CRD-1
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: OUT OF SERVICE  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>
<!--NeedCopy-->
```


Activer ou désactiver un serveur virtuel de redirection de cache à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet de navigation, développez Redirection du cache, puis cliquez sur Serveurs virtuels.
3. Dans le volet d'informations, sélectionnez le serveur virtuel que vous souhaitez activer ou désactiver (par exemple, **vServer-CRD-1**), puis cliquez sur Statistiques.
4. Dans la boîte de dialogue Poursuivre, cliquez sur Oui.

Demandes de stratégie directes de mise en cache au lieu du serveur Web d'origine

August 20, 2021

Par défaut, lorsqu'une demande correspond à une stratégie, l'appliance Citrix ADC transfère la demande directement au serveur d'origine ou à un serveur virtuel d'équilibrage de charge pour l'origine, selon la façon dont vous avez configuré la redirection du cache.

Vous pouvez modifier le comportement par défaut de sorte que lorsqu'une demande correspond à une stratégie, la demande soit transférée vers un serveur virtuel d'équilibrage de charge pour le cache.

Pour modifier la destination d'une demande de stratégie par l'origine ou le cache, utilisez le `onPolicyMatch` paramètre, qui spécifie où envoyer les demandes correspondant à la stratégie de redirection du cache.

Les options valides sont les suivantes :

1. `CACHE` - Dirige toutes les requêtes correspondantes vers le cache.
2. `ORIGIN` - Dirige toutes les requêtes correspondantes vers le serveur d'origine.

> **Remarque :**
>
> Pour que cette option fonctionne, vous devez sélectionner le type de redirection du cache comme `POLICY`.

Valeurs possibles : `CACHE`, `ORIGIN`

Valeur par défaut : `ORIGIN`

Modifier la destination d'une demande de stratégie par l'origine ou le cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour modifier la destination d'un appel de stratégie et vérifier la configuration :


```
set cr vserver <name> [-onPolicyMatch (ORIGIN | CACHE)]
<!--NeedCopy-->
```

```
show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> set cr vserver Vserver-CRD-1 -onPolicyMatch CACHE
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Modifier la destination d'un accès de stratégie vers l'origine ou le cache à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez modifier la destination d'une demande de stratégie (par exemple, **vServer-CRD-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue **Configurer le serveur virtuel (redirection du cache)**, cliquez sur **Avancé**.
4. Sélectionnez **CACHE** ou **ORIGIN** dans la liste déroulante **Rediriger vers** .
5. Cliquez sur **OK**.

Sauvegarder un serveur virtuel de redirection de cache

August 20, 2021

La redirection du cache peut échouer si le serveur virtuel principal échoue ou s'il est incapable de gérer un trafic excessif. Vous pouvez spécifier un serveur virtuel de sauvegarde pour prendre en charge le traitement du trafic lorsque le serveur virtuel principal échoue.

Pour spécifier un serveur virtuel de redirection de cache de sauvegarde, utilisez le paramètre BackupvServer, qui spécifie Sauvegarde Virtual Server. Longueur maximale : 127

Spécifier un serveur virtuel de redirection de cache de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour spécifier un serveur virtuel de redirection de cache de sauvegarde et vérifier la configuration :

```
-  set cr vserver <name> [-backupVServer <string>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> set cr vserver Vserver-CRD-1 -backupVServer Vserver-CRD-2
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

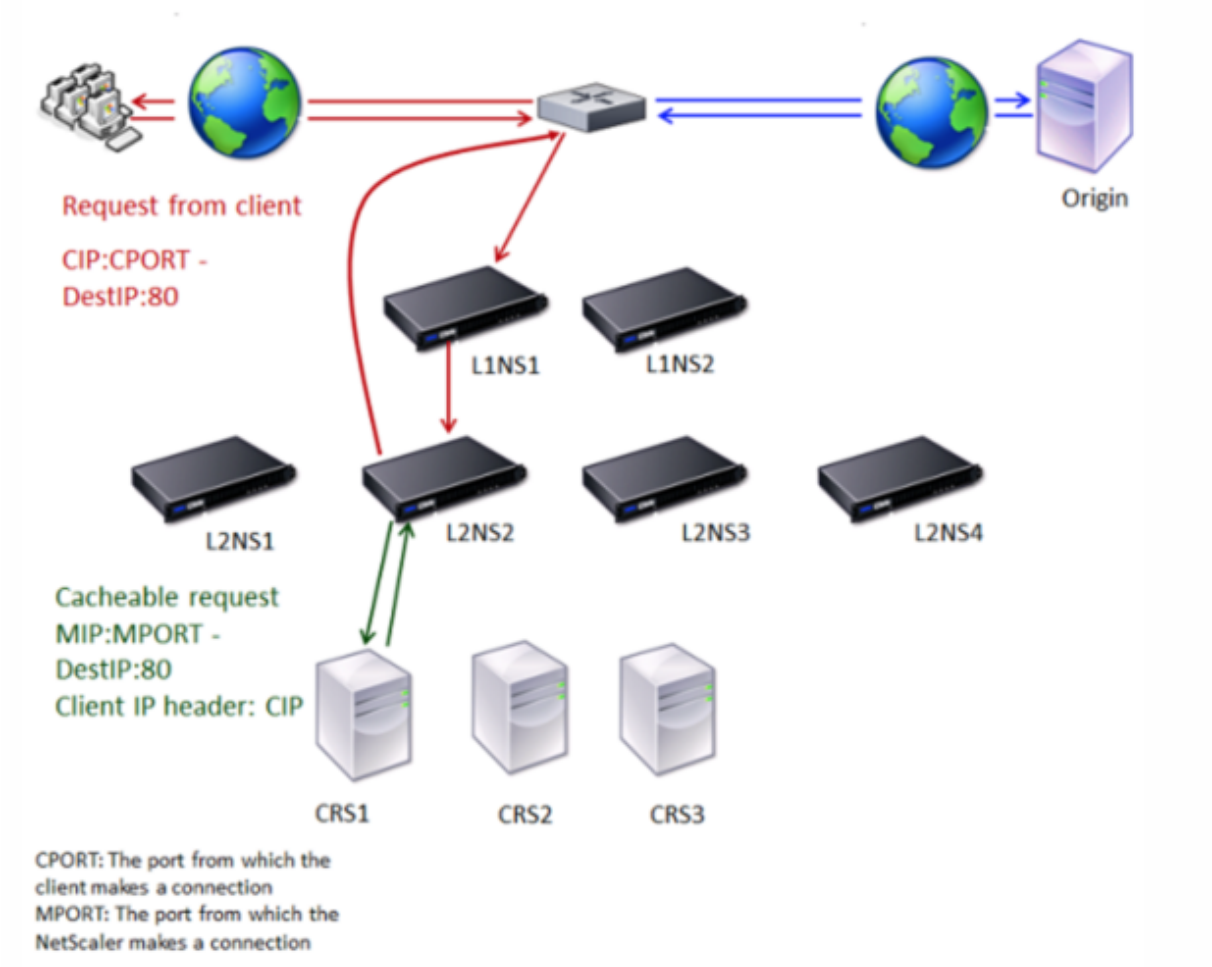
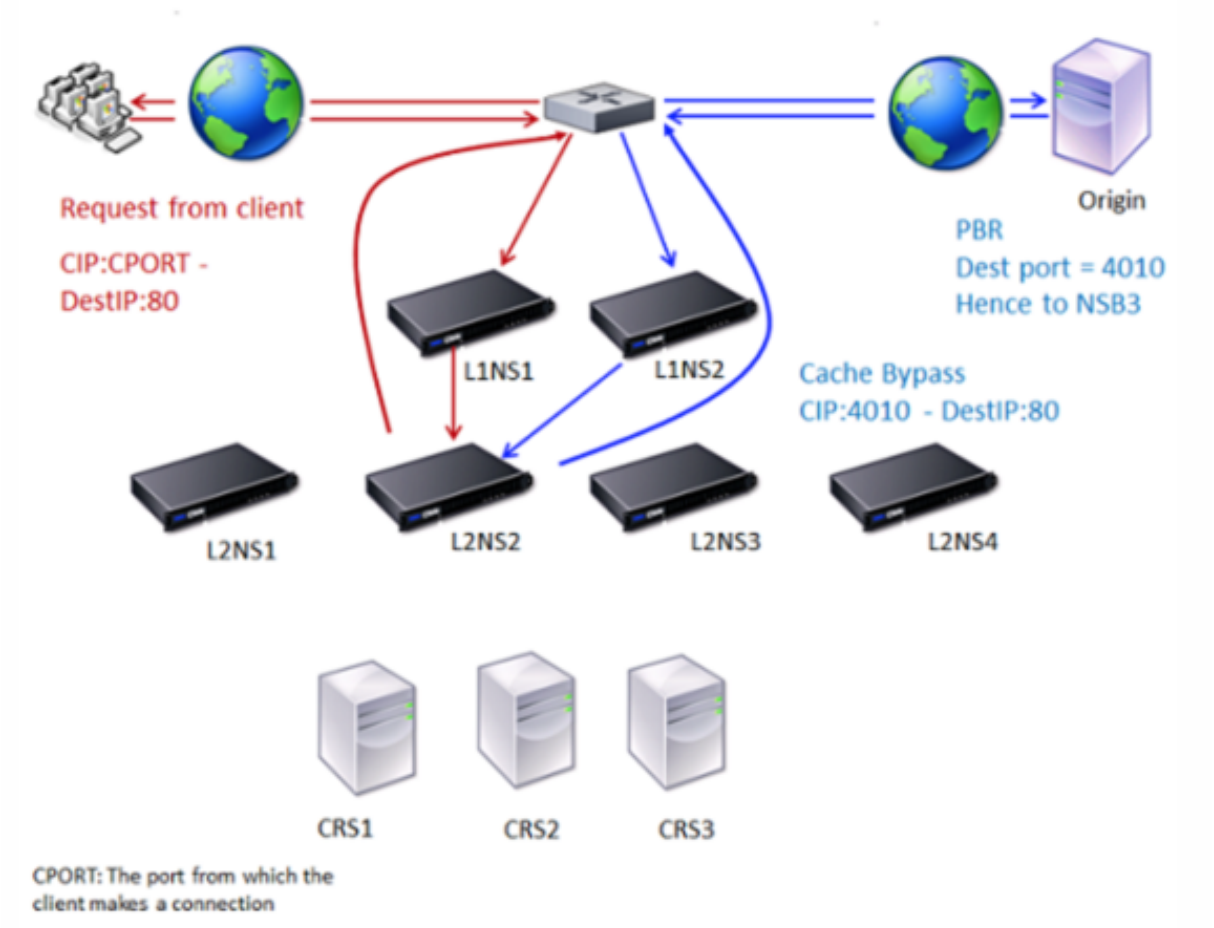
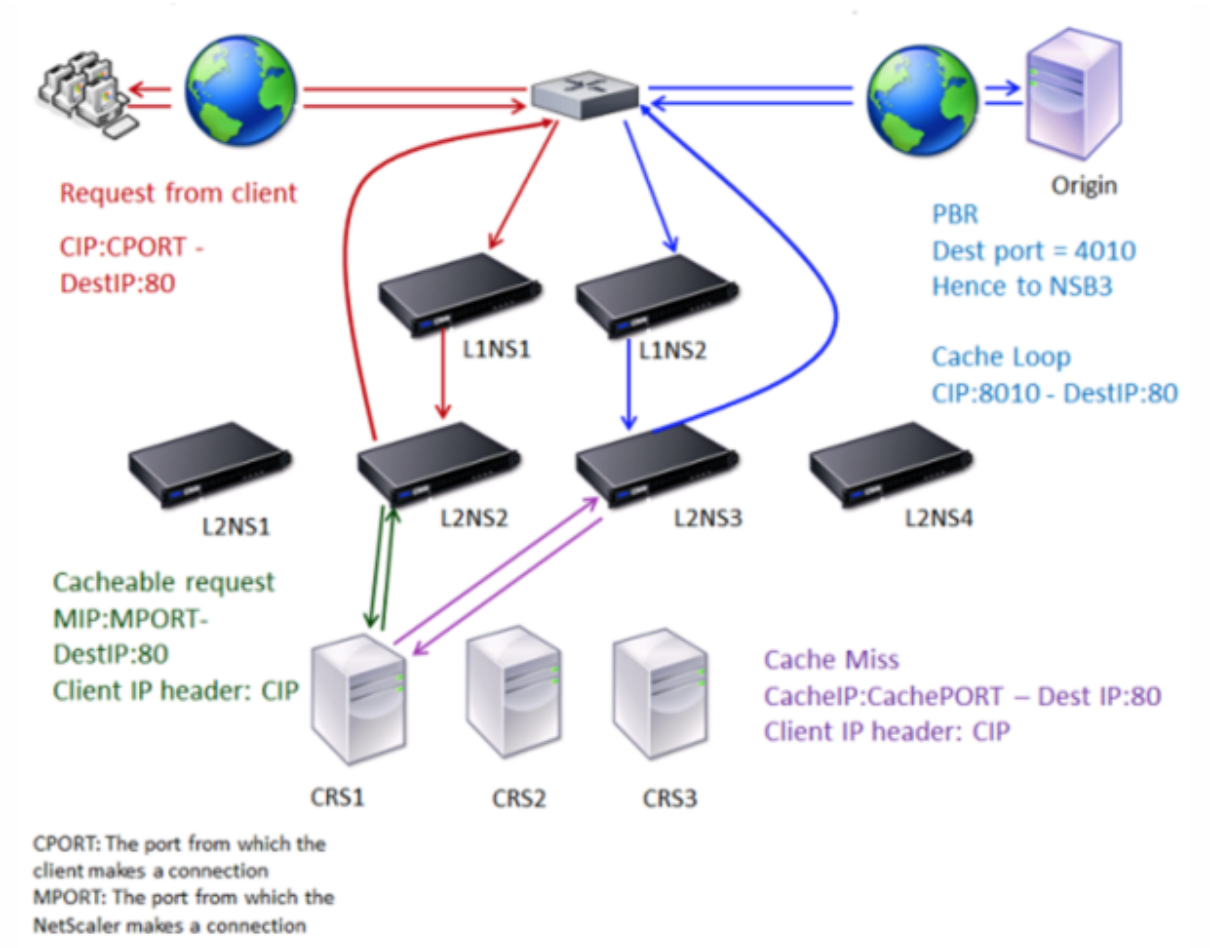
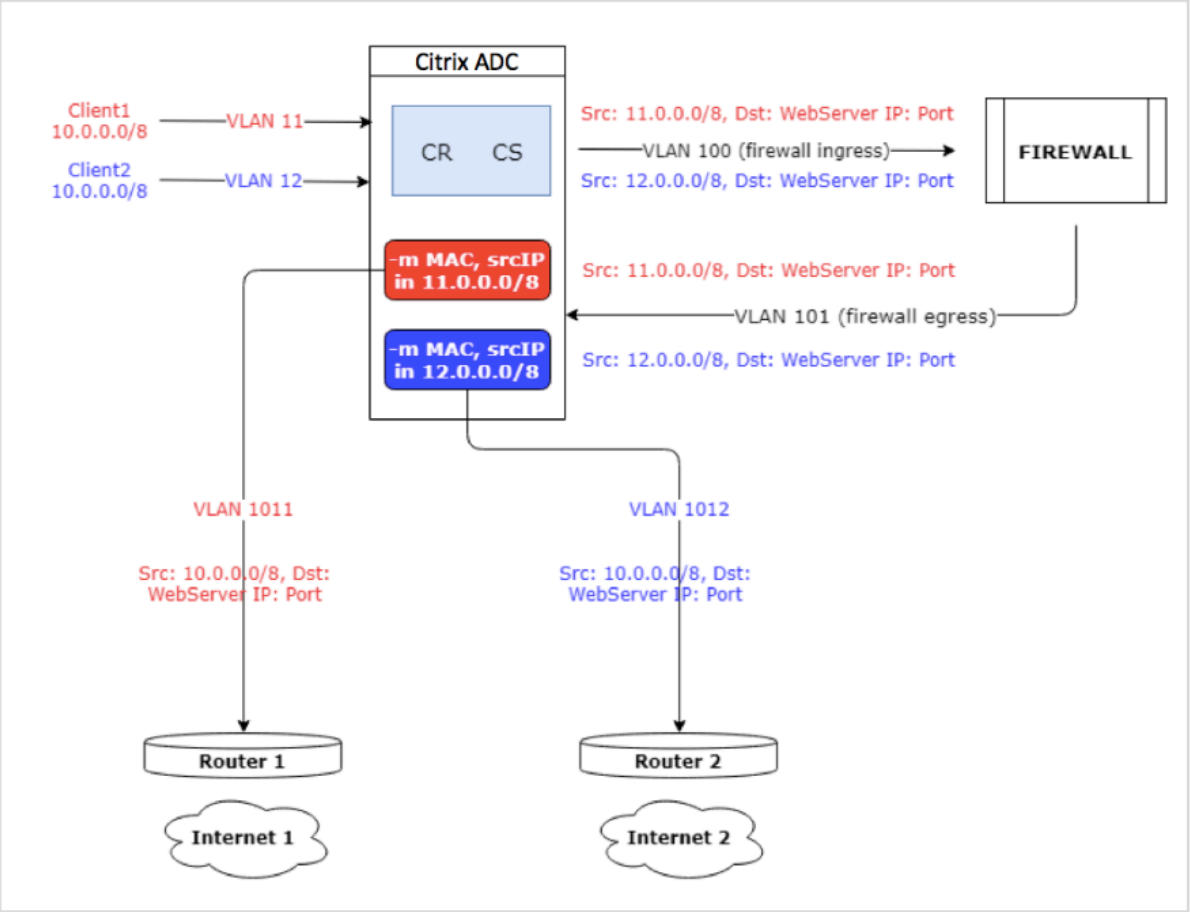
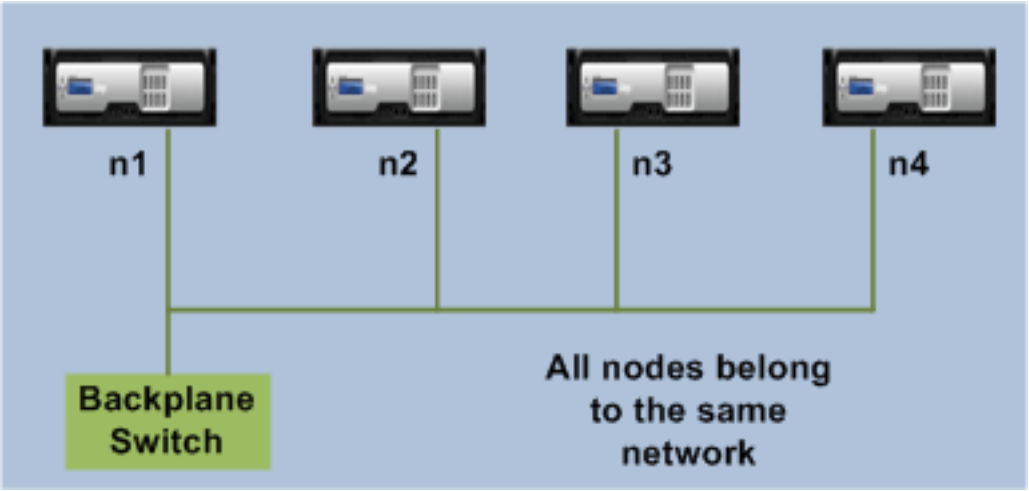
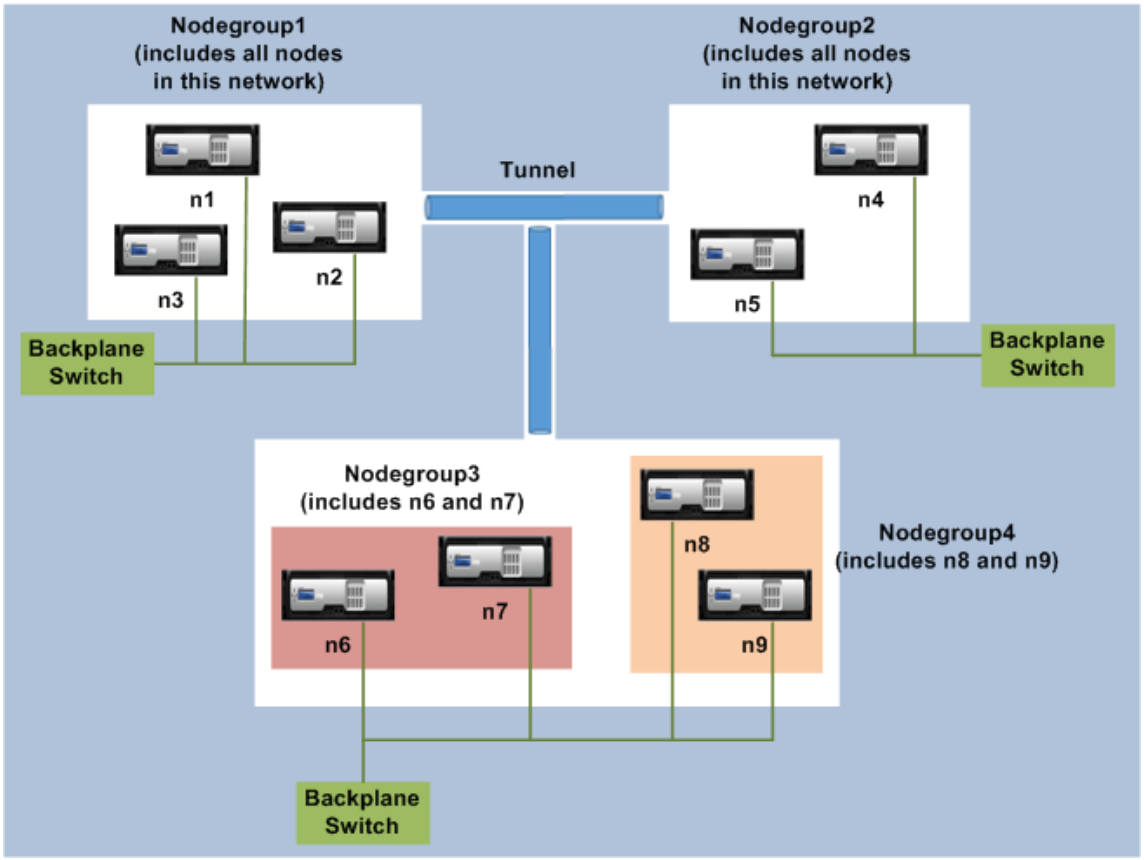
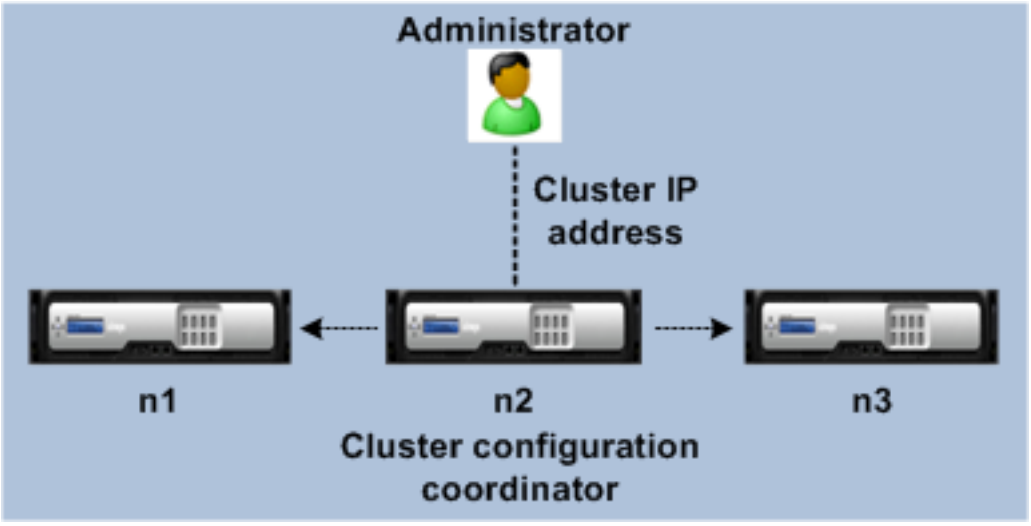
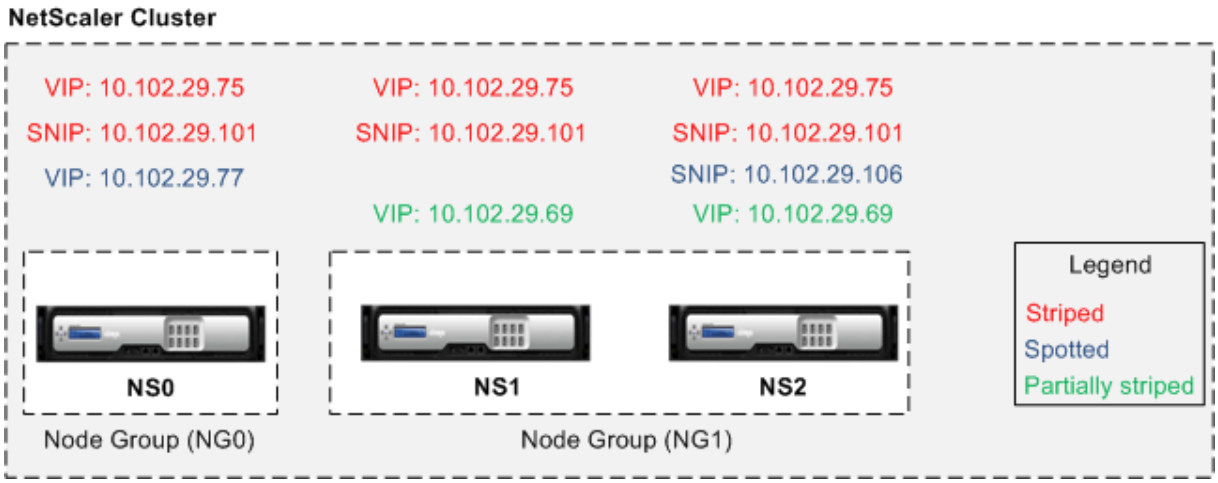
1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Spécifier un serveur virtuel de redirection de cache de sauvegarde à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez modifier la destination d'une demande de stratégie (par exemple, **vServer-CRD-1**), puis cliquez sur

Ouvrir.

3. Dans la boîte de dialogue Configurer le serveur virtuel (redirection du cache), sélectionnez l'onglet Avancé.
4. Dans la liste déroulante Sauvegarde Virtual Server, sélectionnez le serveur virtuel.
5. Cliquez sur OK.

Gérer les connexions client pour un serveur virtuel

August 20, 2021

Vous pouvez configurer des délais d'expiration sur un serveur virtuel de redirection de cache afin que les connexions clientes ne soient pas maintenues ouvertes indéfiniment. Vous pouvez également insérer des en-têtes Via dans les requêtes. Pour réduire éventuellement la congestion du réseau, vous pouvez réutiliser les connexions TCP ouvertes. Vous pouvez activer ou désactiver le nettoyage retardé des connexions de serveur virtuel de redirection de cache.

Vous pouvez configurer l'appliance pour qu'elle envoie des réponses ICMP aux demandes PING en fonction de vos paramètres. Sur l'adresse IP correspondant au serveur virtuel, définissez ICMP RESPONSE sur VSVR_CNTRLD et sur le serveur virtuel, définissez ICMP VSERVER RESPONSE.

Les paramètres suivants peuvent être définis sur un serveur virtuel :

- Lorsque vous définissez ICMP VSERVER RESPONSE sur PASSIVE sur tous les serveurs virtuels, l'appliance répond toujours.
- Lorsque vous définissez ICMP VSERVER RESPONSE sur ACTIVE sur tous les serveurs virtuels, l'appliance répond même si un serveur virtuel est UP.
- Lorsque vous définissez ICMP VSERVER RESPONSE sur ACTIVE sur certains et PASSIVE sur d'autres, l'appliance répond même si un serveur virtuel défini sur ACTIVE est UP.

Ce document contient les renseignements suivants :

- Configurer le délai d'expiration du client
- Insérer des en-têtes Via dans les requêtes
- Réutiliser les connexions TCP
- Configurer le nettoyage de la connexion retardée

Configurer le délai d'expiration du client

Vous pouvez spécifier l'expiration des demandes client en définissant une valeur de délai d'attente pour le serveur virtuel de redirection de cache. La valeur de délai d'attente est le nombre de secondes

pendant lesquelles le serveur virtuel de redirection de cache attend de recevoir une réponse pour la demande du client.

Pour configurer une valeur de délai d'expiration, utilisez le paramètre CLTTimeout, qui spécifie le temps, en secondes, après lequel l'appliance Citrix ADC ferme toutes les connexions client inactives. La valeur par défaut est 180sec pour les services HTTP/SSL et 9000sec pour les services TCP.

Configurer le délai d'expiration du client à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour configurer le délai d'expiration du client et vérifier la configuration :

```
-  set cr vserver <name> [-cltTimeout <secs>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> set cr vserver Vserver-CRD-1 -cltTimeout 6000
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Configurer le délai d'expiration du client à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le délai d'expiration du client (par exemple, **vServer-CRD-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (redirection de cache), sélectionnez l'onglet Avancé.

4. Dans la zone de texte Délai d'expiration du client (secondes), entrez la valeur de délai d'expiration en secondes.
5. Cliquez sur OK.

Insérer des en-têtes Via dans les requêtes

Un en-tête Via répertorie les protocoles et les destinataires entre les points de départ et de fin d'une requête ou d'une réponse et informe le serveur des proxys via lesquels la demande a été envoyée. Vous pouvez configurer le serveur virtuel de redirection de cache pour insérer un en-tête Via dans chaque requête HTTP. Le paramètre via est activé par défaut lorsque vous créez un serveur virtuel de redirection de cache.

Pour activer ou désactiver l'insertion d'en-tête VIA dans les requêtes client, utilisez le paramètre via, qui spécifie l'état du système lors de l'insertion d'un en-tête Via dans les requêtes HTTP.

Valeurs possibles : ON, OFF

Valeur par défaut : ON

Activer ou désactiver l'insertion d'en-tête VIA dans les requêtes client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
-  set cr vserver <name> [-via (ON|OFF)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> set cr vserver Vserver-CRD-1 -via ON
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

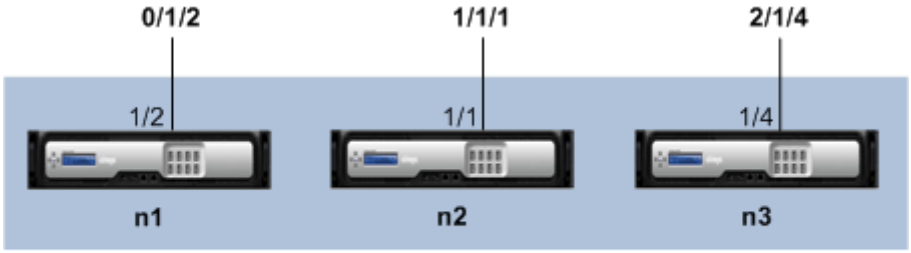
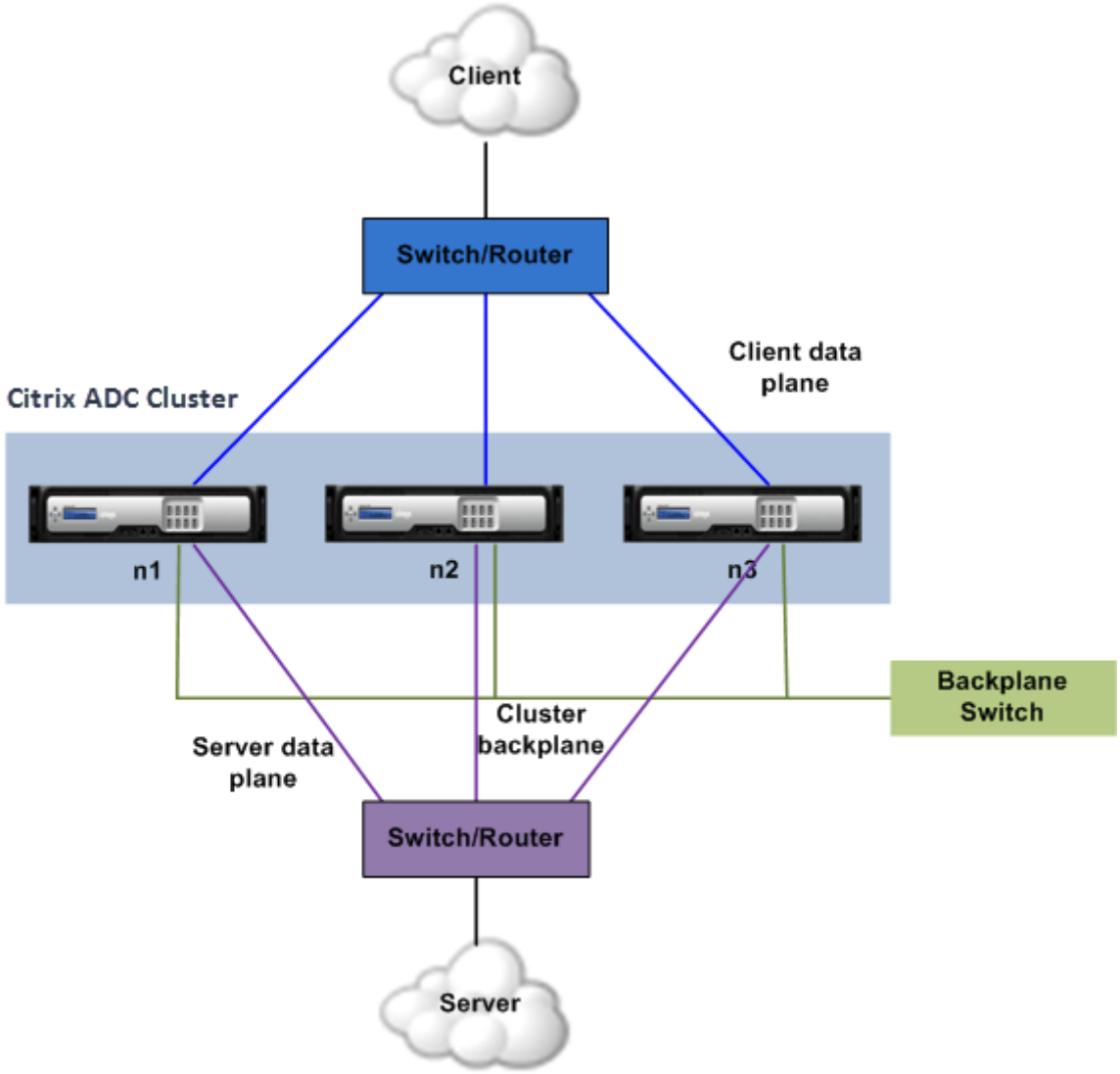
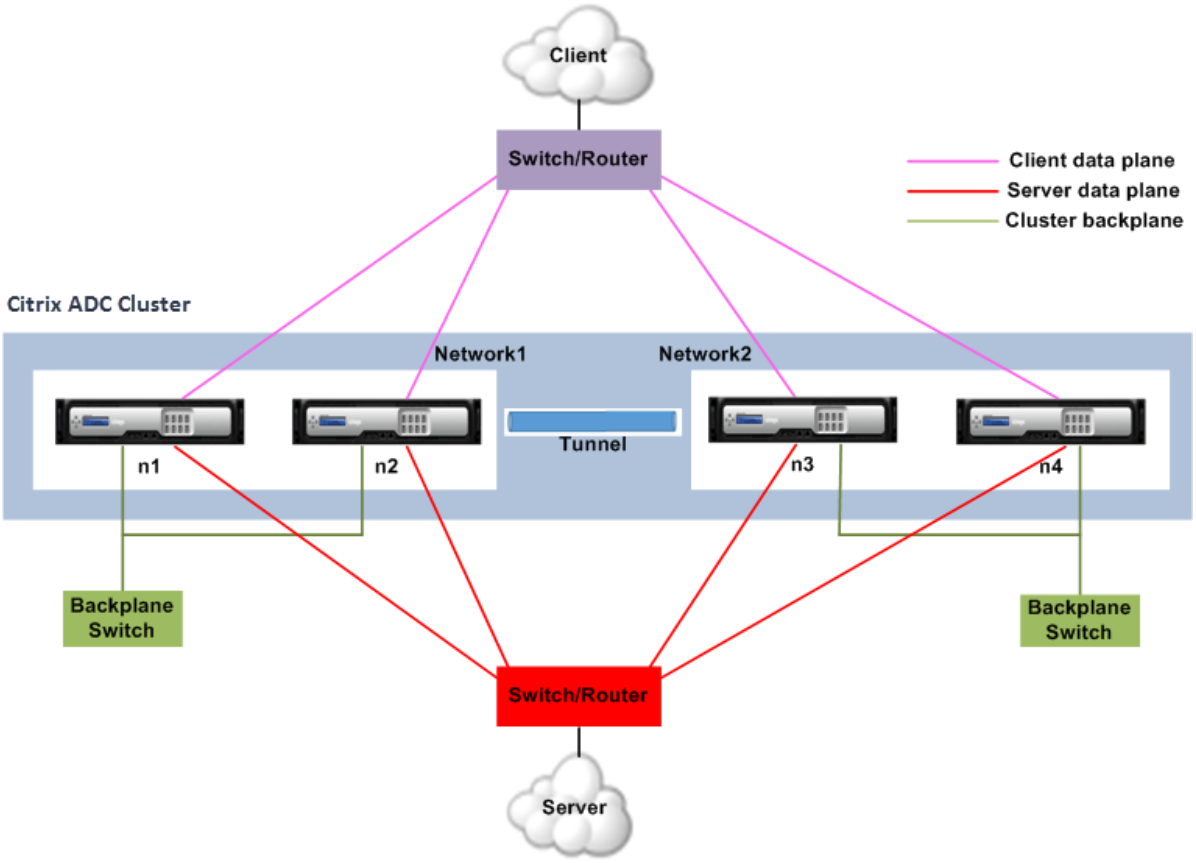
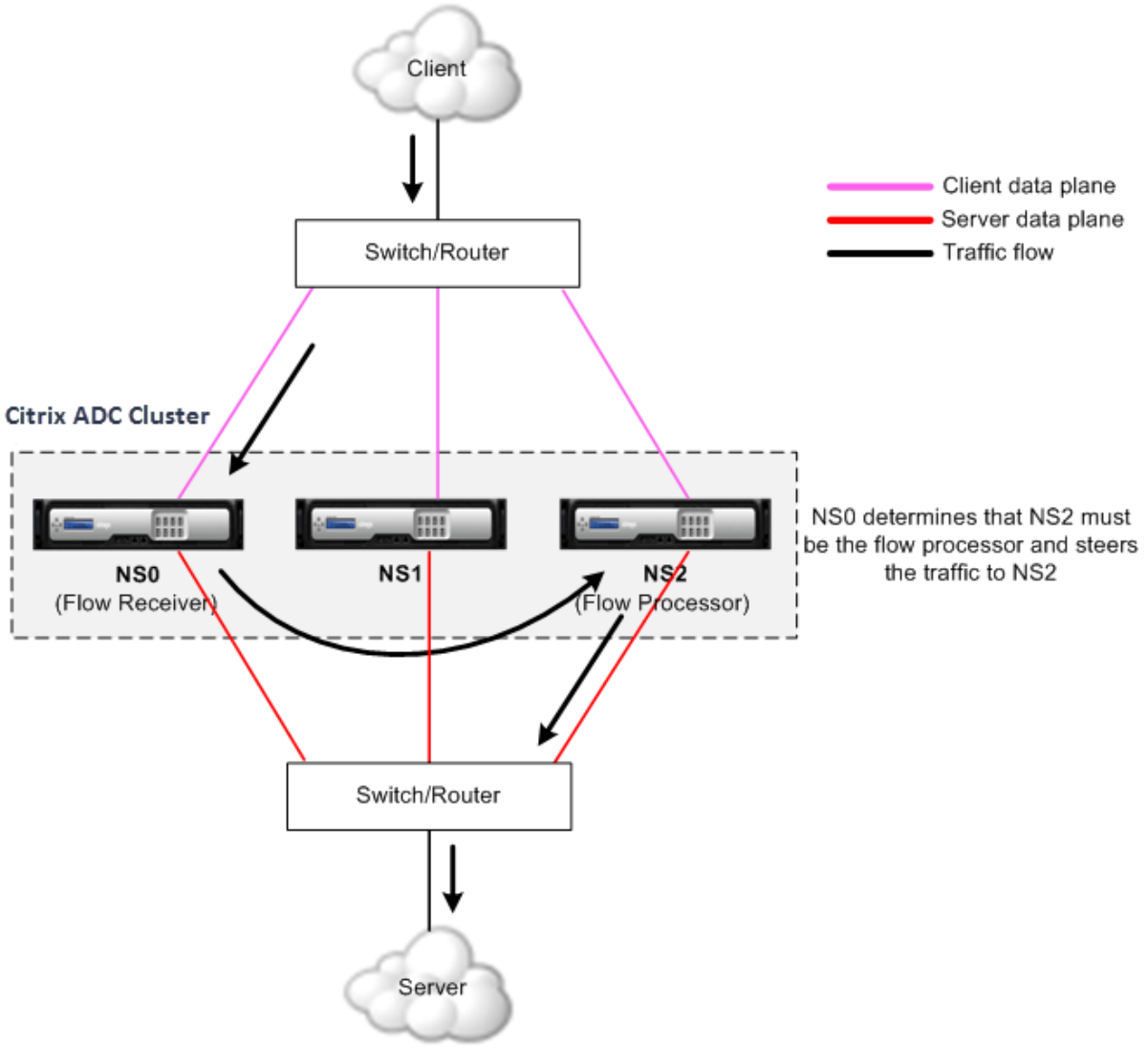
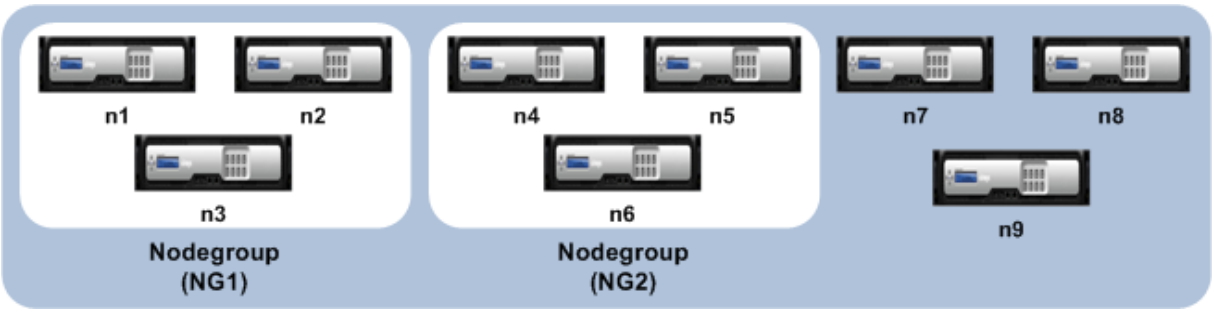
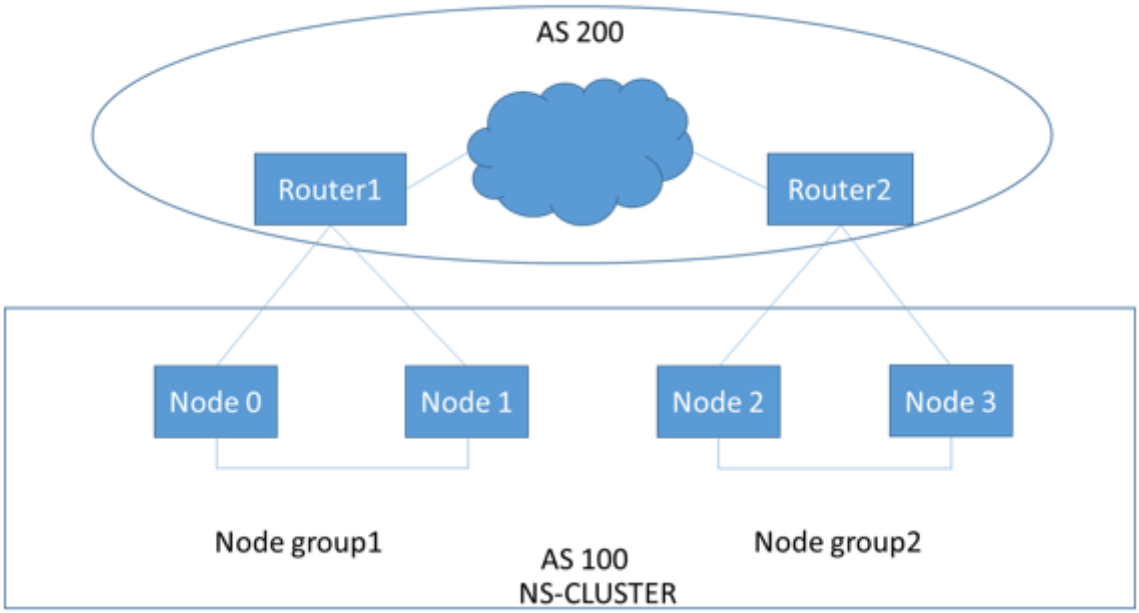
1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
```



```
16   Done
17  >
18  <!--NeedCopy-->
```

Activer ou désactiver l'insertion d'en-tête VIA dans les requêtes client à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le délai d'expiration du client (par exemple, **vServer-CRD-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (redirection de cache), sélectionnez l'onglet Avancé.
4. Activez la case à cocher Via.
5. Cliquez sur OK.

Réutiliser les connexions TCP

Vous pouvez configurer l'appliance Citrix ADC pour réutiliser les connexions TCP au cache et aux serveurs d'origine sur les connexions client. Cela peut améliorer les performances en économisant le temps nécessaire à l'établissement d'une session entre le serveur et l'appliance. L'option de réutilisation est activée par défaut lorsque vous créez un serveur virtuel de redirection de cache.

Pour activer ou désactiver la réutilisation des connexions TCP, utilisez le paramètre de réutilisation, qui spécifie l'état de réutilisation des connexions TCP au cache ou aux serveurs d'origine sur les connexions client.

Valeurs possibles : ON, OFF

Valeur par défaut : ON

Activer ou désactiver la réutilisation des connexions TCP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1  -  set cr vserver <name> [-reuse (ON|OFF)]
2  -  show cr vserver <name>
3  <!--NeedCopy-->
```

Exemple :

```
1  > set cr vserver Vserver-CRD-1 -reuse ON
2   Done
```



```
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Activer ou désactiver la réutilisation des connexions TCP à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le délai d'expiration du client (par exemple, **vServer-CRD-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (redirection de cache), sélectionnez l'onglet Avancé.
4. Activez la case à cocher Réutiliser.
5. Cliquez sur OK.

Configurer le nettoyage de la connexion retardée

L'option de vidage d'état en panne effectue un nettoyage retardé des connexions sur un serveur virtuel de redirection de cache. L'option de vidage d'état bas est activée par défaut lorsque vous créez un serveur virtuel de redirection de cache.

Pour activer ou désactiver l'option de vidage de l'état vers le bas, définissez le paramètre DownState-Flush.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

Activer la désactivation de l'option de vidage de l'état en bas à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le nettoyage de la connexion retardée et vérifier la configuration :

```
-  set cr vserver <name> [-downStateFlush (ENABLED | DISABLED)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> set cr vserver Vserver-CRD-1 -downStateFlush ENABLED
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Activer ou désactiver la réutilisation des connexions TCP à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le délai d'expiration du client (par exemple, **vServer-CRD-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (redirection de cache), cliquez sur onglet Avancé.
4. Activez la case à cocher Défoncement de l'état.
5. Cliquez sur OK.

Activer la vérification de l'état TCP externe pour les serveurs virtuels UDP

August 20, 2021

Dans les clouds publics, vous pouvez utiliser l'appliance Citrix ADC comme équilibreur de charge de deuxième niveau lorsque l'équilibreur de charge natif est utilisé comme premier niveau. L'équilibreur de charge natif peut être un équilibrage de charge d'application (ALB) ou un équilibreur de charge réseau (NLB). La plupart des clouds publics ne prennent pas en charge les sondes de santé UDP dans leurs équilibreurs de charge natifs. Pour surveiller l'intégrité de l'application UDP, les clouds publics recommandent d'ajouter un point de terminaison basé sur TCP à votre service. Le point de terminaison reflète l'intégrité de l'application UDP.

L'appliance Citrix ADC prend en charge le contrôle d'intégrité basé sur TCP externe pour un serveur virtuel UDP. Cette fonctionnalité introduit un écouteur TCP sur le VIP du serveur virtuel de redirection de cache et le port configuré. L'écouteur TCP reflète l'état du serveur virtuel.

Pour activer la vérification de l'état TCP externe pour les serveurs virtuels UDP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour activer une vérification d'intégrité TCP externe avec l'option tcpProbePort :

```
add cr vserver <name> <serviceType> -tcpProbePort <tcpProbePort>

<!--NeedCopy-->
```

Exemple :

```
add cr vserver Vserver-CR-1 HTTP -tcpProbePort 80
<!--NeedCopy-->
```

Pour activer la vérification de l'état TCP externe pour les serveurs virtuels UDP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Serveurs virtuels**, puis créez un serveur virtuel.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel.
3. Dans le volet **Paramètres de base**, ajoutez le numéro de port dans le champ **Port de sonde TCP**.
4. Cliquez sur **OK**.

Redirection du cache de niveau N

January 21, 2021

Pour gérer efficacement de grandes quantités de données mises en cache, généralement plusieurs gigaoctets par seconde, un fournisseur d'accès Internet (ISP) déploie plusieurs serveurs de cache dédiés. La fonction de redirection du cache de l'appliance Citrix ADC peut aider à équilibrer la charge des serveurs de cache, mais un seul ou plusieurs appliances peuvent ne pas gérer efficacement le volume important de trafic.

Vous pouvez résoudre le problème en déployant les appliances Citrix ADC en deux niveaux (couches), où les appliances du niveau supérieur équilibrent la charge de celles du niveau inférieur et celles du niveau inférieur équilibrent les serveurs de cache. Cet arrangement est appelé *redirection du cache à n niveaux*.

À des fins telles que l'audit et la sécurité, un fournisseur de services Internet doit suivre les détails du client, tels que l'adresse IP, les informations fournies et l'heure de l'interaction. Par conséquent, les connexions client via une appliance Citrix ADC doivent être entièrement transparentes. Toutefois, si vous configurez la redirection transparente du cache, avec les appliances Citrix ADC déployées en parallèle, l'adresse IP du client doit être partagée entre toutes les appliances. Le partage de l'adresse IP du client crée un conflit qui empêche les périphériques réseau, tels que les routeurs, les serveurs de cache, les serveurs d'origine et les autres appliances Citrix ADC, de déterminer l'appliance, et donc le client, auquel la réponse doit être envoyée.

Mise en œuvre de la redirection du cache à n niveau

Pour résoudre le problème, la redirection du cache n tier de l'appliance fractionne la plage de ports source entre les appliances du niveau inférieur et inclut l'adresse IP du client dans la requête envoyée aux serveurs de cache. Les appliances Citrix ADC de niveau supérieur sont configurées pour effectuer un équilibrage de charge sans session afin d'éviter une charge inutile sur les appliances.

Lorsque l'appliance Citrix ADC de niveau inférieur communique avec un serveur de cache, elle utilise une adresse IP mappée (MIP) pour représenter l'adresse IP source. Par conséquent, le serveur de cache peut identifier l'appliance à partir de laquelle il a reçu la demande et envoyer la réponse à la même appliance.

L'appliance Citrix ADC de niveau inférieur insère l'adresse IP du client dans l'en-tête de la requête envoyée au serveur de cache. L'adresse IP du client dans l'en-tête permet à l'appliance de déterminer le client vers lequel le paquet doit être transféré lorsqu'il reçoit la réponse d'un serveur de cache ou du serveur d'origine en cas d'échec du cache. Le serveur d'origine détermine la réponse à envoyer en fonction de l'adresse IP du client insérée dans l'en-tête de la requête.

Le serveur d'origine envoie la réponse à une appliance de niveau supérieur, y compris le numéro de

port source à partir duquel le serveur d'origine a reçu la demande. Toute la plage de ports source, 1024 à 65535, est distribuée entre les appliances Citrix ADC de niveau inférieur. Chaque appliance de niveau inférieur se voit attribuer exclusivement un groupe d'adresses dans la plage. Cette allocation permet à l'appliance de niveau supérieur d'identifier sans ambiguïté l'appliance Citrix ADC de niveau inférieur qui a envoyé la demande au serveur d'origine. L'appliance de niveau supérieur peut donc transmettre la réponse à l'appliance de niveau inférieur appropriée.

Les appliances Citrix ADC de niveau supérieur sont configurées pour effectuer le routage basé sur des stratégies, et les stratégies de routage sont définies pour déterminer l'adresse IP de l'appliance de destination à partir de la plage de ports source.

Configuration nécessaire pour configurer le CRD N-Tier

La configuration suivante est nécessaire pour le fonctionnement de la redirection du cache à n niveaux :

Pour chaque appliance Citrix ADC de niveau supérieur :

- Activez le mode Couche 3.
- Définissez des stratégies pour les itinéraires basés sur des règles (PBR) afin que le trafic soit transféré en fonction de la plage du port de destination.
- Configurez un serveur virtuel d'équilibrage de charge.
- Configurez le serveur virtuel pour écouter tout le trafic provenant du client. Définissez le type de service/protocole sur ANY et l'adresse IP sous forme d'astérisque (*).
- Activez l'équilibrage de charge sans session avec le mode de redirection basé sur Mac pour éviter toute charge inutile sur les appliances Citrix ADC de niveau supérieur.
- Assurez-vous que l'option Utiliser le port proxy est activée.
- Créez un service pour chaque appliance de niveau inférieur et liez tous les services au serveur virtuel.

Pour chaque appareil Citrix ADC de niveau inférieur :

- Configurez la plage de ports de redirection du cache sur l'appliance. Attribuez une plage exclusive à chaque appliance de niveau inférieur.
- Configurez un serveur virtuel d'équilibrage de charge et activez la redirection basée sur Mac.
- Créez un service pour chaque serveur de cache devant être équilibré par cette appliance. Lors de la création du service, activez l'insertion de l'adresse IP du client dans l'en-tête. Ensuite, liez tous les services au serveur virtuel d'équilibrage de charge.
- Configurez un serveur virtuel de redirection de cache en mode transparent avec les paramètres suivants :
  - Activez l'option Origin USIP.
  - Ajoutez une expression IP source pour inclure l'adresse IP du client dans l'en-tête.
  - Activez l'option Utiliser la plage de ports.

Fonctionnement de la redirection du cache à n niveau lors d'un accès au cache

La figure suivante montre comment la redirection du cache fonctionne lorsqu'une requête client est mise en cache et que la réponse est envoyée à partir d'un serveur de cache.

Figure 1. Redirection du cache en cas d'accès au cache



Deux appliances Citrix ADC, L1NS1 et L1NS2, sont déployées dans le niveau supérieur, et quatre appliances Citrix ADC, L2NS1, L2NS2, L2NS3 et L2NS4, sont déployées dans le niveau inférieur. Le client A envoie une requête, qui est transmise par le routeur. Les serveurs de cache CRS1, CRS2 et CRS3 desservent les demandes de cache. Origin Server O traite les demandes non mises en cache.

Flux de trafic

1. Le client envoie une demande, et le routeur la transmet à L1NS1.
2. La charge L1NS1 équilibre la demande sur L2NS2.
3. La charge L2NS2 équilibre la requête vers le serveur de cache CRS1, et la demande peut être mise en cache. L2NS2 inclut l'adresse IP du client dans l'en-tête de la requête.

4. CRS1 envoie la réponse à L2NS2 car L2NS2 a utilisé son MIP comme adresse IP source lors de la connexion à CRS1.
5. Avec l'aide de l'adresse IP du client dans l'en-tête de la requête, L2NS2 identifie le client d'où provient la requête. L2NS2 envoie directement la réponse au routeur, évitant ainsi toute charge inutile sur l'appliance dans le niveau supérieur.
6. Le routeur transmet la réponse au client A.

Fonctionnement de la redirection du cache à n niveau lors d'un contournement du cache

La figure suivante montre comment fonctionne la redirection du cache lorsqu'une demande client est envoyée à un serveur d'origine pour une réponse.

Figure 2. Redirection du cache en cas de contournement du cache



Deux appliances Citrix ADC, L1NS1 et L1NS2, sont déployées dans le niveau supérieur, et quatre appliances Citrix ADC, L2NS1, L2NS2, L2NS3 et L2NS4, sont déployées dans le niveau inférieur. Le client A envoie une requête, qui est transmise par le routeur. Les serveurs de cache CRS1, CRS2 et CRS3 desservent les demandes de cache. Origin Server O traite les demandes non mises en cache.

Flux de trafic

1. Le client envoie une demande, et le routeur la transmet à L1NS1.
2. La charge L1NS1 équilibre la demande sur L2NS2.
3. La requête ne peut pas être mise en cache (contournement du cache). Par conséquent, L2NS2 envoie la demande au serveur d'origine via le routeur.
4. Le serveur d'origine envoie la réponse à une appliance de niveau supérieur, L1NS2.
5. Conformément aux stratégies PBR, L1NS2 transfère le trafic à l'appliance appropriée du niveau inférieur, L2NS2.
6. L2NS2 utilise l'adresse IP du client dans l'en-tête de requête pour identifier le client d'où provient la requête et envoie la réponse directement au routeur, évitant ainsi toute charge inutile sur l'appliance dans le niveau supérieur.
7. Le routeur transmet la réponse au client A.

Fonctionnement de la redirection du cache à n niveau lors d'une absence de cache

La figure suivante montre comment la redirection du cache fonctionne lorsqu'une requête client n'est pas mise en cache.

Figure 3. Redirection du cache en cas d'échec du cache



Deux appliances Citrix ADC, L1NS1 et L1NS2, sont déployées dans le niveau supérieur, et quatre appliances Citrix ADC, L2NS1, L2NS2, L2NS3 et L2NS4, sont déployées dans le niveau inférieur. Le client A envoie une requête, qui est transmise par le routeur. Les serveurs de cache CRS1, CRS2 et CRS3 desservent les demandes de cache. Origin Server O traite les demandes non mises en cache.

Flux de trafic

1. Le client envoie une demande, et le routeur la transmet à L1NS1.
2. La charge L1NS1 équilibre la demande sur L2NS2.
3. La charge L2NS2 équilibre la requête vers le serveur de cache CRS1 car la requête est mise en cache.
4. CRS1 n'a pas la réponse (cache miss). CRS1 transmet la demande au serveur d'origine par l'intermédiaire de l'appliance du niveau inférieur. L2NS3 intercepte le trafic.
5. L2NS3 prend l'adresse IP du client à partir de l'en-tête et transmet la requête au serveur d'origine. Le port source inclus dans le paquet est le port L2NS3 à partir duquel la demande est envoyée au serveur d'origine.
6. Le serveur d'origine envoie la réponse à une appliance de niveau supérieur, L1NS2.

7. Conformément aux stratégies PBR, L1NS2 transfère le trafic à l'appliance appropriée du niveau inférieur, L2NS3.
8. L2NS3 transmet la réponse au routeur.
9. Le routeur transmet la réponse au client A.

Configurer les appliances Citrix ADC de niveau supérieur

January 21, 2021

Configurez chacune des appliances Citrix ADC de niveau supérieur comme suit.

Configurez une appliance de niveau supérieur pour la redirection du cache à n niveau à l'aide de la commande CLI

À l'invite de commandes, tapez les commandes suivantes :

- `add service \<name\>@ \<serviceIP\> \<serviceType\> \<port\>`

  Exécutez cette commande pour chaque service à ajouter.

- `add lb vserver \<name\>@ ANY \* \<port\> -persistenceType \<persistenceMethod \> -lbMethod \<lbMethod\> -m MAC -sessionless ENABLED -cltTimeout \< client\\_Timeout\\_Value\>`

- `bind lb vserver \<name\>@ \<serviceName\>`

  Exécutez cette commande pour chaque service à lier.

- `enable ns mode l3`

- `add ns pbr \<name\> \<action\> -srcPort \<sourcePortNumber\> -destPort \<startPortNumber-endPortNumber\> -nexthop \<serviceIpAddress\> -protocol TCP`

- `apply ns pbrs`

  Exécutez cette commande après avoir ajouté tous les PBR nécessaires.

Configurez une appliance de niveau supérieur pour la redirection du cache à n niveau à l'aide de l'interface graphique

1. Activer le mode L3 :
   a) Dans le volet de navigation, cliquez sur Système, puis sur Paramètres.
   b) Dans le groupe Paramètres, cliquez sur le lien Configurer les modes.
   c) Activez la case à cocher Mode couche 3 (transfert IP).

d) Cliquez sur OK.

2. Configurer le routage basé sur des règles (PBR) :
   a) Accédez à Système > Réseau > PBR.
   b) Dans le volet Routage basé sur des règles (PBR), cliquez sur Ajouter.
   c) Tapez un nom pour le PBR.
   d) Sélectionnez l'action comme Autoriser.
   e) Dans la zone Prochain saut, tapez l'adresse IP du service, qui représente une appliance de niveau inférieur.
   f) Sélectionnez TCP dans la liste déroulante Protocole.
   g) Tapez le port source et la plage du port de destination correspondant à l'appliance de niveau inférieur en cours d'ajout.
   h) Cliquez sur Créer.
   i) Dans le volet d'informations, sélectionnez le PBR et cliquez sur Appliquer.
   j) Répétez l'étape (i) à l'étape (vii) pour chaque appareil de niveau inférieur.
3. Créez un service pour chaque appliance de niveau inférieur :
   a) Accédez à Gestion du trafic > Équilibrage de charge > Services.
   b) Dans le volet d'informations, cliquez sur Ajouter.
   c) Spécifiez le nom, le protocole, l'adresse IP et le port. Le protocole doit être ANY.
   d) Cliquez sur Créer.
4. Configurez un serveur virtuel d'équilibrage de charge :
   a) Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
   b) Dans le volet d'informations, cliquez sur Ajouter.
   c) Spécifiez le nom, le protocole, l'adresse IP et le port. Le protocole doit être ANY et l'adresse IP doit être *.
   d) Dans l'onglet Services, sélectionnez les services qui représentent les appliances Citrix ADC de niveau inférieur.
   e) Dans l'onglet Avancé, activez le mode de redirection en tant que mode MAC et activez la case à cocher Sans session.
   f) Cliquez sur Créer.

Configurer les appliances Citrix ADC de niveau inférieur

January 21, 2021

Configurez chacun des appliances Citrix ADC de niveau inférieur comme suit.

Configurer une appliance de niveau inférieur pour la redirection du cache à n niveau à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add service <name>@ <cacheServiceIP> <serviceType> <port> -cip ENABLED "ClientIP"-cachetype transparent`

  Répétez l'opération pour chaque serveur de cache.

- `add lb vserver <name>@ <serviceType> -m MAC`
- `bind lb vserver <name>@ <cacheServiceName>`

  Répétez l'opération pour chaque serveur de cache.

- `add cr vserver <name> <serviceType> * <port> -srcIPExpr "HTTP.REQ. HEADER("ClientIP")"-originusip ON -usePortRange ON`
- `set ns param-crPortRange <startPortNumber-endPortNumber>`

Configurer une appliance de niveau inférieur pour la redirection du cache à n niveau à l'aide de l'interface graphique

1. Créez un service pour chaque serveur de cache. Pour créer un service :
   a) Accédez à Gestion du trafic > Équilibrage de charge > Services.
   b) Dans le volet d'informations, cliquez sur Ajouter, puis spécifiez le nom et le protocole. Désactivez la case à cocher Directement adressable.
   c) Dans l'onglet Avancé, activez la case à cocher Remplacer global et la case à cocher IP du client, puis dans la zone En-tête, tapez ClientIp.
   d) Dans la zone Type de cache, sélectionnez Cache transparent.
   e) Cliquez sur Créer.
2. Configurez un serveur virtuel d'équilibrage de charge :
   a) Accédez à Gestion du trafic > Équilibrage de charge > Services virtuels.
   b) Dans le volet d'informations, cliquez sur Ajouter et spécifiez le nom, le protocole, l'adresse IP et le port. L'adresse IP doit être un astérisque (*).
   c) Dans l'onglet Services, sélectionnez les services qui représentent les serveurs de cache.
   d) Dans l'onglet Avancé, pour Mode de redirection, sélectionnez Basé sur MAC.
   e) Cliquez sur Créer.
3. Configurer un serveur virtuel de redirection de cache :
   a) Accédez à Gestion du trafic > Équilibrage de charge > Services virtuels.
   b) Dans le volet d'informations, cliquez sur Ajouter et spécifiez le nom, le protocole, l'adresse IP et le port. L'adresse IP doit être *.
   c) Pour Type de cache, sélectionnez Transparent.

d) Sous l'onglet Avancé, dans la zone Serveur de cache, sélectionnez le nouveau serveur virtuel d'équilibrage de charge et cochez les cases Origin USIP et Use Port Range. Dans la zone Expression IP source, tapez HTTP.REQ.HEADER (« CLIENTIP »).
e) Cliquez sur Créer.

4. Affectez une plage de ports source à l'appliance :
   a) Dans le volet de navigation, cliquez sur Système, puis sur Paramètres.
   b) Dans le groupe Paramètres, cliquez sur le lien Modifier les paramètres système globaux.
   c) Dans le groupe Plage de ports de redirection de cache, spécifiez la plage de ports de l'appliance en saisissant un numéro de port pour le port de départ et un numéro de port pour le port de fin.
   d) Cliquez sur OK.

Traduire l'adresse IP de destination d'une requête vers l'adresse IP d'origine

August 20, 2021

Vous pouvez configurer le serveur virtuel de redirection de cache proxy de transfert sur l'appliance Citrix ADC pour traduire l'adresse IP de destination de l'atterrissage de la requête sur le serveur virtuel de redirection de cache vers l'adresse IP du serveur d'origine. Cette traduction se produit indépendamment du fait que la demande soit envoyée aux serveurs mis en cache ou au serveur d'origine.
Auparavant, le serveur virtuel de redirection de cache proxy de transfert dans l'environnement de fournisseur de services ne pouvait pas être utilisé efficacement pour envoyer du trafic à travers le pare-feu en raison des limitations de la redirection de cache à l'aide de stratégies de commutation de contenu. Le serveur virtuel de redirection de cache n'a pas traduit l'adresse IP d'origine dans l'adresse IP de destination lorsque le paquet a été envoyé au cache. L'adresse IP de destination était celle du serveur d'origine uniquement lorsque les requêtes ont été traitées à partir du serveur mis en cache.

Remarque : La traduction de l'adresse IP de destination d'une requête vers l'adresse IP d'origine n'est pas prise en charge pour un serveur virtuel de redirection de cache transparent. Pour un serveur virtuel de redirection de cache transparent, cette option doit être définie sur OFF.

Cas d'utilisation

Dans un déploiement sur lequel l'appliance Citrix ADC est configurée pour la redirection du cache proxy, le pare-feu et les adresses IP client réutilisées, le pare-feu ne peut pas distinguer/utiliser les adresses IP réutilisées. Par conséquent, ces adresses IP réutilisées doivent être traduites en différentes adresses IP. Pour traduire les adresses IP réutilisées, l'appliance Citrix ADC doit effectuer les opérations suivantes :

1. Interrogez un serveur virtuel d'équilibrage de charge DNS pour la résolution de la destination.
2. Mettez à jour l'adresse IP d'origine et le numéro de port dans la destination.
3. Renvoyez la demande au pare-feu.

Considérez le déploiement suivant qui dispose d'une appliance Citrix ADC configurée pour la redirection du cache proxy, le pare-feu et deux routeurs (routeur 1 et routeur 2). Le trafic réseau circule vers Internet 1 via le routeur 1 et vers Internet 2 via le routeur 2 respectivement.



Dans cet exemple, les demandes d'entrée des clients proviennent de deux VLAN différents, VLAN11 ou VLAN12. L'adresse IP du client (10.0.0.0) est réutilisée.
En fonction des stratégies de redirection du cache et de commutation de contenu, la demande peut aller directement au serveur d'origine ou au pare-feu.

- Si la demande doit contourner le pare-feu et aller sur Internet, alors en fonction de la demande d'entrée VLAN, Routeur 1 ou Routeur 2 est sélectionné et la demande est envoyée à Internet 1 ou Internet 2.
- Si la requête doit passer par le pare-feu, l'adresse IP source de la requête doit être traduite en adresse IP spécifique. L'adresse IP traduite peut être utilisée pour identifier le VLAN par lequel la demande est venue. Par exemple, si la demande d'entrée provient de VLAN11, l'adresse IP

source est traduite en 11.x.x.x. Si la requête provient de VLAN12, l'adresse IP source est traduite en 12.x.x.x.

Une fois la demande traitée par le pare-feu, la demande est renvoyée à l'appliance. À l'aide de la combinaison de stratégies d'écoute et de profils réseau, l'appliance convertit l'adresse IP source en adresse IP d'origine et envoie la demande au routeur 1 ou 2 en fonction de l'ID VLAN d'entrée.

Remarque : Le mode du serveur virtuel d'équilibrage de charge lié au cache doit toujours être défini sur le mode MAC. Bien que le mode IP de cette fonctionnalité ne soit pas bloqué, le réglage en mode IP entraîne un comportement inattendu.

Pour traduire l'adresse IP de destination et le numéro de port de la requête vers l'adresse IP d'origine à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
set cr vserver <vsname> -useoriginIpPortForCache <YES|NO>
<!--NeedCopy-->
```

Exemple :

```
set cr vserver cvsrv1 -useoriginIpPortForCache YES
<!--NeedCopy-->
```

Lorsque UseOriginIPportForCache est défini sur Oui et si la demande doit être traitée à partir des serveurs mis en cache, l'adresse IP de destination de la requête est convertie en adresse IP du serveur d'origine.

Remarque : si UseOriginIPportForCache est activé, définissez toujours le serveur virtuel d'équilibrage de charge lié au cache en mode MAC.

Pour traduire l'adresse IP de destination et le port de la requête à l'adresse IP d'origine à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Redirection du cache** > **Serveurs virtuels**, puis cliquez sur **Ajouter**.
2. Spécifiez les détails du serveur virtuel de redirection de cache.
3. Sélectionnez **Utiliser le port IP d'origine** pour le cache pour activer la traduction de l'adresse IP de destination de la requête vers l'adresse IP d'origine.
4. Cliquez sur **OK**.

Mise en cluster

January 21, 2021

> **Remarque**
>
> Cette fonctionnalité est disponible avec une licence Citrix ADC Advanced ou Premium Edition.

Un cluster Citrix ADC est un groupe d'appliances nCore qui travaillent ensemble en tant qu'image système unique. Chaque appliance du cluster est appelée nœud. Le cluster peut comporter une appliance ou jusqu'à 32 appliances matérielles Citrix ADC nCore ou virtuelles en tant que nœuds.

Le trafic client est distribué entre les nœuds pour fournir une haute disponibilité, un débit élevé et une évolutivité.

Pour créer un cluster, vous devez effectuer les opérations suivantes :

- Ajoutez les appliances en tant que nœuds de cluster.
- Configurez la communication entre les nœuds.
- Configurez des liens vers les réseaux client et serveur.
- Configurez les appliances et configurez la distribution du trafic client et serveur.

Matrice de prise en charge du cluster Citrix ADC

October 5, 2021

Le clustering dans l'appliance Citrix ADC prend en charge une large gamme de fonctionnalités dans les configurations Citrix ADC.

Le tableau suivant répertorie les fonctionnalités de Citrix ADC et fournit l'état de prise en charge dans différentes versions Citrix ADC des configurations de cluster. L'état de prise en charge de certaines fonctionnalités Citrix ADC dans un cluster Citrix ADC BLX 13.0 est différent de celui d'un cluster Citrix ADC non BLX (MPX ou VPX, SDX ADC) 13.0.

> **Important**
>
> L'entrée « Niveau de nœud » dans le tableau indique que la fonctionnalité est prise en charge uniquement sur les nœuds de cluster individuels.

Fonctionnalités Citrix ADC	11.1	12.1	13.0	13.0 Cluster Citrix ADC BLX	Citrix ADC 13.1
FIPS SSL	Non	Non	Non	Non	Non
Offre groupée de certificats SSL	Non	Non	Non	Non	Non
Interception SSL	SO	Non	Non	Non	Non
Actions de changement de contenu	Oui	Oui	Oui	Oui	Oui
Journalisation basée sur des règles pour les stratégies de changement de contenu	Oui	Oui	Oui	Oui	Oui
Limitation de débit	Oui	Oui	Oui	Oui	Oui
Analyse des actions	Oui	Oui	Oui	Non	Oui
GSLB	Oui	Oui	Oui	Oui	Oui
RTSP	Oui	Oui	Oui	Oui	Oui
DNSSEC	Non	Non	Non	Non	Non
DNS64	Non	Non	Non	Non	Non
FTP	Oui	Oui	Oui	Non	Oui
TFTP	Non	Oui	Oui	Oui	Oui
Mise en miroir des connexions	Non	Non	Non	Non	Non
Mise en cache intégrée	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds

Fonctionnalités Citrix ADC	11.1	12.1	13.0	13.0 Cluster Citrix ADC BLX	Citrix ADC 13.1
Cache partagé volumineux	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds
Optimisation frontale	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds
Pare-feu d'application	Oui	Oui	Oui	Non	Oui
Protection par déni de service HTTP (HDOSP)	Niveau de noeuds	Obsolète	Obsolète	Obsolète	Supprimé
Queuing prioritaire (PQ)	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Obsolète	Supprimé
Connexion sûre (SC)	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Obsolète	Supprimé
AppQoE	Oui	Oui	Oui	Non	Oui
Protection contre les surtensions	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Oui	Niveau de noeuds
MPTCP	Oui	Oui	Oui	Non	Oui
SNIP striped	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.

Fonctionnalités Citrix ADC	11.1	12.1	13.0	13.0 Cluster Citrix ADC BLX	Citrix ADC 13.1
MSR	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.
IS-IS (IPv4 et IPv6)	Oui	Oui	Oui	Non	Oui
Trames Jumbo	Oui	Oui	Oui	Non	Oui
Tunnelage IP-IP	Oui	Oui	Oui	Non	Oui
Équilibrage de charge de liaison	Oui	Oui	Oui	Oui	Oui
FIS (ensemble d’interfaces de basculement)	Oui	Oui	Oui	Non	Oui
Redondance des liens (LR)	Oui	Oui	Oui	Non	Oui
NAT46	Non	Non	Oui	Oui	Oui
NAT64	Non	Non	Oui	Oui	Oui
RNAT6	Oui	Oui	Oui	Oui	Oui
LSN/CGNAT	Non	Oui	Oui	Non	Oui
ReadyLogo IPv6	Non	Oui	Oui	Non	Oui

Fonctionnalités Citrix ADC	11.1	12.1	13.0	13.0 Cluster Citrix ADC BLX	Citrix ADC 13.1
Domaines de trafic	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Non	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.
Moniteur de routage	Oui ; Seulement avec DR.	Oui ; **Remarque :** pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui **Remarque :** prise en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Non	Oui **Remarque :** prise en charge dans les clusters L2. Non pris en charge dans les clusters L3.
Tunnelage GRE (CB)	Non	Non	Non	Non	Non
Mode couche 2	Oui	Oui	Oui	Non	Oui
Profils de réseau	Oui	Oui	Oui	Non	Oui
Légende HTTPS	Oui	Oui	Oui	Oui	Oui
AAA-TM	Niveau de noeuds	Oui	Oui	Non	Oui
AppFlow	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds
Web Insight	Oui	Oui	Oui	Non	Oui
HDX Insight	Oui	Oui	Oui	Non	Oui
VMAC/VRRP	Oui	Oui	Oui	Non	Oui

Fonctionnalités Citrix ADC	11.1	12.1	13.0	13.0 Cluster Citrix ADC BLX	Citrix ADC 13.1
NetScaler Push	Non	Non	Non	Non	Non
Basculement de connexion avec état	Non	Non	Non	Non	Non
Arrêt gracieux	Non	Oui	Oui	Oui	Oui
Mise à l'Autoscale DBS	Non	Non	Oui	Oui	Oui
DSR utilisant TOS	Non	Non	Non	Oui	Non
Finer Startup-RR Control	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds
XML XSM	Non	Non	Non	Non	Non
DHCP RA	Non	Non	Non	Non	Non
Groupe de ponts	Oui	Oui	Oui	Non	Oui
Pont réseau	Non	Non	Non	Non	Non
Interface Web sur Citrix ADC (WiONs)	Oui	Oui	Oui	Non	Oui
Surveillance EdgeSight	Obsolète	Obsolète	Obsolète	Non	Obsolète
Tables de mesures - Local	Non	Non	Non	Non	Non
Mise en cache DNS	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds
Call Home	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds

Fonctionnalités Citrix ADC	11.1	12.1	13.0	13.0 Cluster Citrix ADC BLX	Citrix ADC 13.1
Mode proxy ICA Citrix Gateway	Oui	Oui	Oui	Non	Oui
Citrix Gateway (VPN SSL /VPN complet et VPN sans client)	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds
Connecteur Citrix CloudBridge	Non	Oui	Oui	Non	Oui
Routage basé sur des stratégies (PBR/PBR6)	Oui	Oui	Oui	Non	Oui
Routage basé sur une stratégie IPv4 (PBR) avec serveur virtuel LLB comme prochain saut	Non	Non	Oui	Non	Oui
Routage basé sur une stratégie IPv6 (PBR6) avec serveur virtuel LLB comme saut suivant	Non	Non	Non	Non	Non
Sensibilisation des abonnés	Non	Non	Non	Non	Non

Fonctionnalités Citrix ADC	11.1	12.1	13.0	13.0 Cluster Citrix ADC BLX	Citrix ADC 13.1
Routage dynamique	Oui avec la prise en charge des protocoles v6 (ospfv3, RIPng, ISIS6, BGP6)	Oui avec la prise en charge des protocoles v6 (ospfv3, RIPng, ISIS6, BGP6)	Oui avec la prise en charge des protocoles v6 (ospfv3, RIPng, ISIS6, BGP6)	Oui	Oui avec la prise en charge des protocoles v6 (ospfv3, RIPng, ISIS6, BGP6)
SYSLOG-TCP, équilibrage de charge des serveurs syslog, prise en charge SNIP et prise en charge de FQDN pour syslog	Oui ; **Remarque :** pris en charge à partir de NetScaler 11.1 Build 54.16.	Oui	Oui	Oui	Oui
Gestion des robots	Non	Non	Oui	Non	Oui
VXLAN	Non	Non	Non	Non	Non

De plus, les configurations Citrix ADC suivantes sont prises en charge :

Équilibrage de charge, persistance de l'équilibrage de charge, équilibrage de charge DNS, SIP, Max-Client, Spillover (connexion et dynamique). Spillover basé sur la bande passante, DataStream, le contrôle de la compression, le filtrage du contenu, la mise en mémoire tampon TCP, la redirection du cache, le déni de service distribué (DDoS). Keep-alive du client, mise en réseau de base (IPv4 et IPv6), OSPF (IPv4 et IPv6), RIP (IPv4 et IPv6), RIP (IPv4 et IPv6). VLAN, ICMP, fragmentation, MBF, ACL, ACL simple, MSR, découverte MTU de chemin, IP IP, SNMP, stratégies (classiques et avancées). Réécriture, répondeur, légende HTTP, journalisation du serveur Web, journalisation d'audit (NSLOG et Syslog). USIP, commandes de localisation, API NITRO, AppExpert, KRPC.

Conditions préalables

October 5, 2021

Les appliances Citrix ADC (MPX, VPX, SDX ADC, BLX) devant être ajoutées à un cluster doivent répondre aux conditions préalables suivantes :

- Toutes les appliances doivent avoir la même version et la même version logicielles.
- Toutes les appliances doivent être du même type de plate-forme. Cela signifie qu'un cluster doit posséder soit toutes les appliances matérielles (Citrix ADC MPX), soit toutes les appliances Citrix ADC VPX, soit toutes les appliances Citrix BLX, soit toutes les instances Citrix SDX ADC.

  Remarque :

  - Pour un cluster d'appliances matérielles (MPX), les appliances doivent être du même type de modèle.
  - Pour la formation du cluster hétérogène, toutes les appliances doivent être de type plate-forme MPX.
  - Pour un cluster de appliances virtuelles (VPX), les appliances doivent être déployées sur les hyperviseurs suivants : XenServer, Hyper-V, VMware ESX et KVM.
  - Pour configurer un cluster d'instances SDX Citrix ADC, reportez-vous à la section Configuration d'un cluster d'instances Citrix ADC.
  - Les trames Jumbo sont prises en charge sur un cluster Citrix ADC composé d'instances Citrix ADC SDX.
  - Vous pouvez créer des clusters L3 d'instances SDX.
  - Pour plus d'informations sur la configuration d'un cluster Citrix ADC BLX, reportez-vous à la section Cluster Citrix ADC BLX.
- Les appareils peuvent appartenir à différents réseaux.
- Être initialement configuré et connecté à un réseau côté client et côté serveur commun.
- Pour un cluster d'appliances virtuelles (Citrix ADC VPX, Citrix ADC BLX, ou instance Citrix SDX ADC) qui possède de grandes configurations, il est recommandé d'utiliser 6 Go de RAM pour chaque nœud du cluster.

Vue d'ensemble du cluster

January 21, 2021

Un cluster Citrix ADC est formé en regroupant les appliances Citrix ADC. En fonction de l'emplacement

réseau des appliances Citrix ADC que vous avez l'intention d'ajouter le cluster, vous devez être conscient des configurations de cluster suivantes :

> **Remarque**
>
> Sauf indication contraire, les fonctions et configurations de cluster sont identiques pour les clusters L2 et L3.

- **Cluster L2 :** Dans ce déploiement de cluster, tous les nœuds de cluster appartiennent au même réseau.



- **Cluster L3 (également appelé « cluster en mode INC ») :** Dans ce déploiement de cluster, les nœuds de cluster peuvent appartenir à différents réseaux. Les nœuds de cluster d'un réseau spécifique doivent être regroupés en groupes de nœuds qui incluent uniquement les nœuds de ce réseau. Sur la figure suivante, nous voyons que les nœuds n1, n2, n3 sont dans le même réseau et sont regroupés dans Nodegroup1.

  De même, le cas pour les nœuds n4 et n5, qui sont regroupés dans Nodegroup2. Dans le troisième réseau, il y a deux groupes de nœuds. Nodegroup3 inclut n6 et n7 et Nodegroup4 inclut n8 et n9.

  > **Remarque**
  >
  > Prise en charge à partir de NetScaler 11.0.



Synchronisation entre les nœuds de cluster

August 20, 2021

Toutes les configurations d'un cluster Citrix ADC sont effectuées sur l'adresse IP du cluster, qui est l'adresse de gestion du cluster. Le nœud de cluster possède l'adresse IP du cluster appelée coordinateur de configuration de cluster (CCO), comme illustré dans la figure suivante :



Les configurations disponibles sur le CCO sont automatiquement propagées aux autres nœuds de cluster et, par conséquent, tous les nœuds de cluster ont les mêmes configurations.

- Citrix ADC permet seulement quelques configurations à effectuer sur des nœuds de cluster individuels via leur adresse NSIP. Dans ce cas, vous devez assurer manuellement la cohérence de la configuration sur tous les nœuds du cluster. Ces configurations ne sont pas propagées sur les autres nœuds de cluster. Pour plus d'informations sur les opérations prises en charge sur chaque nœud de cluster, voir Opérations prises en charge sur des nœuds de cluster individuels.
- Les commandes suivantes lorsqu'elles sont exécutées sur l'adresse IP du cluster ne sont pas propagées vers d'autres nœuds de cluster :
  - **shutdown.** Arrête uniquement le coordinateur de configuration.
  - **reboot.** Redémarre uniquement le coordinateur de configuration.
  - **rm cluster instance.** Supprime l'instance de cluster du nœud sur lequel vous exécutez la commande.
- Pour qu'une commande se propage vers d'autres nœuds de cluster :
  - Le quorum doit être configuré sur l'instance de cluster.
  - La plupart du quorum du cluster avec (n/2 + 1) des nœuds de cluster doit être actif pour que le cluster soit opérationnel.
  - Un cluster peut s'exécuter avec un nombre minimum de nœuds lorsque la règle de majorité (n/2 + 1) est relâchée.

Lorsqu'un nœud est ajouté à un cluster, les configurations et les fichiers (certificats SSL, licences, DNS, etc.) disponibles sur le CCO sont synchronisés avec le nœud de cluster nouvellement ajouté. Lorsqu'un nœud de cluster existant, qui a été délibérément désactivé ou qui a échoué, est à nouveau ajouté, le cluster compare les configurations disponibles sur le nœud avec les configurations disponibles sur le CCO. En cas de non-concordance dans les configurations, le nœud est synchronisé à l'aide de l'une des méthodes suivantes :

- **Full synchronization.** Si la différence entre les configurations dépasse 255 commandes, toutes

les configurations du CCO sont appliquées au nœud qui rejoint le cluster. Le nœud reste opérationnel indisponible pendant la synchronisation.

- **Incremental Synchronization.** Si la différence entre les configurations est inférieure ou égale à 255 commandes, seules les configurations qui ne sont pas disponibles sont appliquées au nœud qui rejoint le cluster. L'état opérationnel du nœud reste inchangé.

> **Remarque**
>
> Vous pouvez également synchroniser manuellement les configurations et les fichiers. Pour plus d'informations, consultezSynchronisation des configurations de cluster et Synchronisation des fichiers de cluster.

Configurations striped, striped partielles et spotted

August 20, 2021

En vertu de la propagation des commandes, tous les nœuds d'un cluster ont les mêmes configurations. Toutefois, vous pouvez souhaiter que certaines configurations soient disponibles uniquement sur certains nœuds de cluster. Bien que vous ne puissiez pas restreindre les nœuds sur lesquels les configurations sont disponibles, vous pouvez spécifier les nœuds sur lesquels les configurations sont actives.

Par exemple, vous pouvez :

- définir une adresse SNIP pour être active sur un seul noeud, ou
- définir une adresse SNIP pour être active sur tous les nœuds, ou
- définir une adresse VIP pour être active sur un seul noeud, ou
- définir une adresse VIP pour être active sur tous les nœuds, ou
- définir une adresse VIP pour être active uniquement sur deux nœuds d'un cluster à 3 nœuds

Selon le nombre de nœuds sur lesquels les configurations sont actives, les configurations de cluster sont appelées configurations striped, striped partielles et spotted.

Figure 1. Cluster à trois nœuds avec configurations striped, striped partielles et spotted



Le tableau suivant fournit plus de détails sur les types de configurations :

Type de configuration	Actif sur	Applicable à	Configurations
Configuration par bandes	Tous les nœuds de cluster	Toutes les entrées	Aucune configuration spécifique n'est requise pour créer une entité striped. Par défaut, toutes les entités définies sur une adresse IP de cluster sont agrégées sur tous les nœuds de cluster.
Configuration striped partielle	Sous-ensemble de nœuds de cluster	Reportez-vous à Groupes de nœuds de cluster.	Liez les entités que vous souhaitez partiellement striped à un groupe de nœuds. La configuration est active uniquement sur les nœuds de cluster appartenant au groupe de nœuds.

Type de configuration	Actif sur	Applicable à	Configurations
Configuration spotted	Nœud de cluster unique	Adresse SNIP, ID de moteur SNMP, nom d'hôte des nœuds de cluster, entités pouvant être liées à un groupe de nœuds	Une configuration spotted peut être définie à l'aide de l'une des deux approches. **Adresse SNIP** Lors de la création de l'adresse SNIP, spécifiez le nœud sur lequel vous souhaitez que l'adresse SNIP soit active, en tant que nœud propriétaire. **Exemple**, `add ns ip 10.102.29.106 255.255.255.0 -type SNIP -ownerNode 2` (en supposant que l'ID NS2 du nœud est 2). **Remarque** : vous ne pouvez pas modifier la propriété d'une adresse SNIP spotted au moment de l'exécution. Pour modifier la propriété, vous devez d'abord supprimer l'adresse SNIP et l'ajouter à nouveau en spécifiant le nouveau propriétaire. **Entités pouvant être liées à un groupe de nœuds.** En liant l'entité à un groupe de nœuds à un seul membre.

Type de configuration	Actif sur	Applicable à	Configurations

> **Remarque**
>
> - Lorsque vous désactivez USIP, Citrix vous recommande d'utiliser des adresses SNIP repérées. Vous pouvez utiliser des adresses SNIP striped uniquement en cas de pénurie d'adresses IP. L'utilisation d'adresses IP striped peut entraîner des problèmes de flux ARP si aucune adresse IP spotted n'est présente dans le même sous-réseau pour la résolution ARP.
> - Lorsque vous activez USIP, Citrix vous recommande d'utiliser des adresses SNIP striped en tant que Gateway pour le trafic initié par le serveur.

Prise en charge des propriétaires ARP pour IP par bandes

Dans une configuration de cluster, vous pouvez configurer un nœud spécifique pour répondre à la demande ARP pour une adresse IP répartie. Le nœud configuré répond au trafic ARP.

Un nouveau paramètre « ARPowner » est introduit dans les commandes « add, set et unset IP ».

Pour activer le propriétaire ARP sur un nœud à l'aide de l'interface de ligne de commande.

À l'invite de commandes, tapez :

```
add ns ip <ip_address> -arpOwner <node_id>
```

> **Remarque**
>
> Le paramètre propriétaire ARP est pris en charge uniquement dans le cluster L2.

Prise en charge du propriétaire de découverte de voisins pour l'adresse IPv6 par répartition

Dans une configuration de cluster, vous pouvez configurer un nœud spécifique en tant que propriétaire de découverte de voisin (ND) pour l'adresse IPv6 par répartition afin de déterminer l'adresse de la couche de liaison. Un client envoie un message de sollicitation de voisin (NS) à tous les nœuds de la configuration du cluster. Le propriétaire ND répond à l'aide d'un message Neighbor Advertisement (NA) avec l'adresse de couche de liaison pour l'adresse IPv6 par répartition et sert le trafic.

Pour activer le propriétaire ND sur un nœud à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
add ns ip6 <IPv6Address> -ndOwner <node id>

set  ns ip6 <IPv6Address> -ndOwner <node id>
<!--NeedCopy-->
```

Exemple :

```
add ns ip6 2001::21/64 -ndOwner 1

set ns ip6 2001::21/64 -ndOwner 1
<!--NeedCopy-->
```

Pour activer le propriétaire ND sur un nœud à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > IP**.
2. Dans la page **IPs**, accédez à l'onglet **IPv6s** et cliquez sur **Ajouter**.
3. Dans la page **Créer IPv6**, sélectionnez l'un des ID de noeud répertoriés dans **NDOwner dans le menu déroulant Cluster**.

> **Remarque**
>
> Le paramètre de propriétaire ND est pris en charge uniquement dans le cluster L2.

Communication dans une configuration de cluster

January 21, 2021

Les interfaces des appliances Citrix ADC ajoutées à un cluster sont préfixées d'un ID de nœud. Il aide à identifier le nœud de cluster auquel appartient l'interface. Par conséquent, l'identifiant de l'interface c/u, où c est le numéro du Controller et u le numéro de l'unité, devient maintenant n/c/u, où n est l'ID du nœud. Par exemple, dans la figure suivante, l'interface 1/2 du noeud n1 est représentée par 0/1/2, l'interface 1/1 du noeud n2 est représentée par 1/1/1 et l'interface 1/4 du noeud n3 est représentée par 2/1/4.

Figure 1. Convention d'attribution de noms d'interface dans un cluster



- **Communication du serveur**-
  Le cluster communique avec le serveur via les connexions physiques entre le nœud du cluster et le périphérique de connexion côté serveur. Le regroupement logique de ces connexions physiques est appelé plan de données du serveur.
- **Communication client**- Le cluster communique avec le client via les connexions physiques entre le nœud de cluster et le périphérique de connexion côté client. Le regroupement logique de ces connexions physiques est appelé plan de données client.
- **Communication inter-nœuds**- Les nœuds de cluster peuvent également communiquer entre eux. La manière dont ils communiquent dépend de l'existence du nœud sur le même réseau ou sur plusieurs réseaux.
  - Les nœuds de cluster du même réseau communiquent entre eux à l'aide du backplane du cluster. Le backplane est un ensemble d'interfaces dans lesquelles une interface de chaque nœud est connectée à un commutateur commun, appelé commutateur de backplane de cluster. Les différents types de trafic qui traversent le fond de panier, qui est utilisé par la communication entre nœuds sont :
    * Messagerie de noeud à noeud (NNM)
    * Circulation orientée
    * Propagation et synchronisation de la configuration
  - Chaque nœud du cluster utilise une adresse spéciale de commutateur de backplane de cluster MAC pour communiquer avec d'autres nœuds via le backplane. Le MAC spécial du cluster est de la forme : `0x02 0x00 0x6F <cluster_id> <node_id> <reserved >)`, où `cluster_id` est l'ID d'instance de cluster, `node_id` est le numéro de nœud de l'appliance Citrix ADC ajouté à un cluster.

Les figures suivantes montrent les interfaces de communication dans les clusters L2 et L3.

Figure 2. Interfaces de communication de cluster - cluster L2



Figure 3. Interfaces de communication de cluster - cluster L3



Distribution du trafic dans une configuration de cluster

August 20, 2021

Dans une configuration de cluster, les réseaux externes visualisent la collection d'appliances Citrix ADC en tant qu'entité unique. Ainsi, le cluster doit sélectionner un nœud unique qui doit recevoir le trafic. Le cluster effectue cette sélection à l'aide du mécanisme de distribution du trafic d'agrégation de liens de cluster (ECMP) ou du mécanisme de distribution du trafic d'agrégation de liens de cluster. Le nœud sélectionné est appelé récepteur de flux.

> **Remarque**
>
> Pour un cluster L3 (nœuds sur différents réseaux), seule la distribution du trafic ECMP peut être utilisée.

Le récepteur de flux obtient le trafic, puis, à l'aide de la logique de cluster interne détermine le nœud qui doit traiter le trafic. Ce nœud est appelé le processeur de flux. Le récepteur de flux permet de diriger le trafic vers le processeur de flux sur le fond de panier si le récepteur de flux et le processeur

de flux sont sur le même réseau. Le trafic est dirigé à travers le tunnel si le récepteur de flux et le processeur de flux se trouvent sur des réseaux différents.

> **Remarque**
>
> - Le récepteur de débit et le processeur de débit doivent être des nœuds capables de servir le trafic.
> - À partir de NetScaler 11, vous pouvez désactiver la direction sur le backplane du cluster. Pour plus d'informations, voir Désactivation du pilotage sur le fond de panier de cluster.

Figure 1. Distribution du trafic dans un cluster



La figure précédente montre une demande client qui traverse le cluster. Le client envoie une demande à une adresse IP virtuelle (VIP). Un mécanisme de distribution du trafic configuré sur le plan de données client sélectionne l'un des nœuds de cluster comme récepteur de flux. Le récepteur de flux reçoit

le trafic, détermine le nœud qui doit traiter le trafic et dirige la demande vers ce nœud (à moins que le récepteur de flux ne se sélectionne lui-même comme processeur de flux).

Le processeur de flux établit une connexion avec le serveur. Le serveur traite la demande et envoie la réponse à l'adresse IP du sous-réseau (SNIP) qui a envoyé la demande au serveur.

- Si l'adresse SNIP est une adresse IP striped et striped partielle, le mécanisme de distribution du trafic configuré sur le plan de données du serveur sélectionne l'un des nœuds de cluster comme récepteur de flux. Le récepteur de flux reçoit le trafic, détermine le processeur de flux et dirige la demande vers le processeur de flux à travers le backplane du cluster.
- Si l'adresse SNIP est une adresse IP spotted, le nœud qui possède l'adresse SNIP reçoit la réponse du serveur.

Dans une topologie de cluster asymétrique (tous les nœuds de cluster ne sont pas connectés au commutateur externe), vous devez utiliser des jeux de liens exclusivement ou combinés avec ECMP ou agrégation de liens de cluster. Pour plus d'informations, voir Utilisation de jeux de liens.

Groupes de nœud de cluster

August 20, 2021

> **Remarque**
>
> Les groupes de nœuds sont pris en charge à partir de NetScaler 10.1.

Comme son nom l'indique, un groupe de nœuds de cluster est un groupe de nœuds de cluster.

Figure 1. Cluster Citrix ADC avec groupes de nœuds



La figure précédente montre un cluster qui a des groupes de nœuds NG1 et NG2 qui incluent chacun 3 nœuds de cluster. Le cluster possède également 3 nœuds qui ne font partie d'aucun groupe de nœuds.

Un groupe de nœuds peut être configuré pour les éléments suivants :

- Pour définir des configurations spotted et striped partielles. Pour plus d'informations, voir Groupes de nœuds pour configurations ponctuées et partiellement réparties.

- Pour configurer la redondance des groupes de nœuds. Pour plus d'informations, voir Configuration de la redondance pour les groupes de nœuds.
  Remarque : pris en charge à partir de NetScaler 10.5 Build 52.1115.e.
- Pour définir un cluster L3 (également appelé cluster en mode INC). Dans un cluster L3, les nœuds de cluster peuvent être issus de différents réseaux. Vous devez regrouper les nœuds appartenant à un réseau dans un seul groupe de nœuds. Par exemple, si n1, n2, n3 sont dans network1 et n4, n5, n6 sont dans network2, alors NG1 doit inclure des nœuds de network1 et NG2 doit inclure des nœuds de network2. Pour configurer un cluster L3, reportez-vous à la section Création d'un cluster Citrix ADC.

> **Remarque**
>
> - Prise en charge à partir de NetScaler 11.
> - Les fonctions précédentes d'un groupe de nœuds s'excluent mutuellement. Cela signifie qu'un groupe de nœuds ne peut fournir qu'une des fonctionnalités mentionnées ci-dessus.

État du cluster et du nœud

January 21, 2021

Pour qu'un cluster soit fonctionnel, la plupart des nœuds (n/2 + 1) doivent être opérationnels (l'état opérationnel est ACTIF).

> **Important**
>
> À partir de NetScaler version 10.5, vous pouvez configurer le cluster pour qu'il soit fonctionnel même lorsque le critère majoritaire n'est pas satisfait. Cette configuration doit être effectuée lors de la création d'un cluster.

Pour plus d'informations sur les états d'un nœud de cluster, reportez-vous à la section États d'un nœud de cluster.

Routage dans un cluster

January 21, 2021

Le routage dans un cluster fonctionne de la même manière que le routage dans un système autonome. Quelques points à noter :

- Toutes les configurations de routage doivent être effectuées à partir de l'adresse IP du cluster et les configurations sont propagées aux autres nœuds du cluster.

- Les routes sont limitées au nombre maximal de routes ECMP prises en charge par le routeur amont.
- Les configurations de routage spécifiques au nœud doivent être effectuées à l'aide de l'argument du nœud propriétaire comme suit :

```
  router ospf
    owner-node 0
      ospf router-id 97.131.0.1
    exit-owner-node
  !
<!--NeedCopy-->
```

La commande suivante affiche la configuration du cluster consolidé pour tous les nœuds de VTYSH.

```
show cluster-config
```

La commande suivante affiche l'état du cluster sur chaque nœud.

```
show cluser node
```

Routage IPv4 dans le cluster L2

La section suivante contient des exemples de configurations qui vous aident à configurer le routage IPv4 OSPF et BGP dans le cluster L2.

Ajout d'une adresse SNIP spotted et activation du routage dynamique

Dans la configuration suivante, le routage OSPF et BGP sont activés. En outre, les adresses SNIP spotted sont ajoutées et le routage dynamique est activé sur ces adresses SNIP.

```
en ns fea ospf bgp
add vlan 10
add ns ip 10.10.10.1 255.255.255.0 -dynamicrouting enabled -ownernode 1
add ns ip 10.10.10.2 255.255.255.0 -dynamicrouting enabled -ownernode 2
add ns ip 10.10.10.3 255.255.255.0 -dynamicrouting enabled -ownernode 3
bind vlan 10 -ipaddress 10.10.10.1 255.255.255.0
<!--NeedCopy-->
```

Configuration VTYSH IPv4 OSPF

Pour configurer IPv4 OSPF dans le cluster L2, vous devez :

- Définir la priorité sur zéro.
- Configurez l'ID du routeur en tant que configuration spotted.

> **Remarque**
>
> Les instructions de configuration OSPF pour le cluster L2 s'appliquent également à OSPFv3.

Dans l'exemple de configuration suivant, IPv4 OSPF est configuré.

```
       interface vlan10
        IP OSPF PRIORITY 0
        !
       router ospf
           owner-node 1
             ospf router-id 97.131.0.1
           exit-owner-node
           owner-node 2
             ospf router-id 97.131.0.2
           exit-owner-node
           owner-node 3
             ospf router-id 97.131.0.3
           exit-owner-node
       network 10.10.10.0/24 area 0
       redistribute kernel
        !
<!--NeedCopy-->
```

Configuration de VTYSH IPv4 BGP

Dans l'exemple de configuration VTYSH suivant, IPv4 BGP est configuré.

```
     router bgp 100
       neighbor 10.10.10.10 remote-as 200
      owner-node 1
       neighbor 10.10.10.10 update-source 10.10.10.1
      exit-owner-node
      owner-node 2
       neighbor 10.10.10.10 update-source 10.10.10.2
      exit-owner-node
      owner-node 3
       neighbor 10.10.10.10 update-source 10.10.10.3
      exit-owner-node
     redistribute kernel
     !
<!--NeedCopy-->
```


> **Remarque**
>
> La commande update-source est utilisée pour chaque voisin avec l'argument owner-node dans la configuration suivante pour se connecter à l'adresse IP source appropriée.

Routage IPv6 dans le cluster L2

La section suivante contient des exemples de configurations qui vous aident à configurer le routage IPv6 OSPF et BGP dans le cluster L2.

Activer le routage IPv6

Avant de configurer le routage IPv6 dans un cluster L2, vous devez activer la fonction IPv6.

Pour activer le routage IPv6 à l'aide de la CLI,

À l'invite de commandes, tapez :

- `enable ns fea ipv6pt`

Ajout d'une adresse SNIP6 spotted et activation du routage dynamique

Dans la configuration suivante, le routage OSPF et BGP sont activés. En outre, les adresses SNIP6 spotted sont ajoutées et le routage dynamique est activé sur ces adresses SNIP6.

```
add ns ip6 3ffa::1/64 -dynamicrouting enabled -ownernode 1
add ns ip6 3ffa::2/64 -dynamicrouting enabled -ownernode 2
add ns ip6 3ffa::3/64 -dynamicrouting enabled -ownernode 3
add vlan 10
bind vlan 10 -ipaddress 3ffa::1/64
<!--NeedCopy-->
```

Configuration de VTYSH IPv6 BGP

Dans l'exemple de configuration VTYSH suivant, IPv6 BGP est configuré.

```
  router bgp 100
   neighbor 3ffa::10 remote-as 200
     owner-node 1
      neighbor 3ffa::10 update-source 3ffa::1
     exit-owner-node
     owner-node-2
      neighbor 3ffa::10 update-source 3ffa::2
     exit-owner-node
```



```
9       owner-node-3
10       neighbor 3ffa::10 update-source 3ffa::3
11      exit-owner-node
12    no neighbor 3ffa::10 activate
13    address-family ipv6
14     redistribute kernel
15     neighbor 3ffa::10 activate
16    exit-address-family
17   !
18 <!--NeedCopy-->
```

Installer les itinéraires appris IPv6

Le cluster Citrix ADC peut utiliser des routes apprises par divers protocoles de routage après avoir installé les routes dans la table de routage de cluster Citrix ADC.

Pour installer des routes apprises IPv6 vers la table de routage interne à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- `ns route-install ipv6 bgp`
- `ns route-install ipv6 ospf`
- `ns route-install default`

> **Remarque**
>
> - Si vous devez échanger des routes IPv4 sur un voisin IPv6, vous devez supprimer la commande VTYSH `no neighbor 3ffa::10 active` de la configuration antérieure.
> - La commande `update-source` VTYSH doit être utilisée pour chaque nœud propriétaire afin de spécifier l'adresse IP source IPv6 droite lors de la connexion à l'homologue BGP comme indiqué dans la configuration IPv4 de BGP.

Routage dans un cluster L3

Le routage dans un cluster L3 fonctionne uniquement lorsque les configurations suivantes sont effectuées sur l'appliance Citrix ADC.

- Activez le routage dynamique pour un VLAN.

```
1  set vlan <id> -dynamicrouting enabled
2  <!--NeedCopy-->
```


- Pour atteindre tous les nœuds de cluster, les adresses IP VIP, CLIP et Citrix ADC (NSIP) doivent être annoncées par des protocoles de routage avec la `set vlan` commande.

Scénario de déploiement pour BGP dans le cluster L3

Prenons un exemple où tous les nœuds de cluster sont regroupés dans le réseau AS 100, et les routeurs en amont se trouvent dans un AS 200 différent.

La figure suivante illustre le déploiement AS 100 et AS 200 dans une configuration de cluster.



Dans ce déploiement, CLIP annonce CCO aux routeurs en amont. Certains nœuds de cluster abandonnent le trafic annoncé, car une boucle AS est détectée.

Pour résoudre le problème, configurez la commande suivante en mode routeur BGP VTYSH pour chaque voisin.

À l'invite de commandes VTYSH, tapez :

```
neighbor <peer_ip> allowas-in 1
```

Citrix vous recommande de configurer l'un des éléments suivants :

- Configurez des mapping d'itinéraire pour ne connaître que les réseaux souhaités, tels que l'itinéraire par défaut, l'IP Citrix ADC (NSIP) et les sous-réseaux NSIP sur les nœuds de cluster.
- Configurez les routes en amont pour ne faire connaître que les réseaux souhaités tels que CLIP et Citrix ADC IP (NSIP) dans le cluster.

Adressage IP d'un cluster

August 20, 2021

Outre les types standard d'adresses IP appartenant à Citrix ADC (Citrix ADC NSIP, Virtual IP (VIP) et Subnet IP (SNIP)), une appliance Citrix ADC en cluster peut avoir une adresse IP de gestion de cluster (CLIP). Il peut également avoir des adresses IP striped et spotted.

- **Adresse CLIP.** Adresse IP appartenant au nœud de coordinateur de cluster (CCO). L'adresse CLIP peut flotter entre différents nœuds dans une configuration de cluster. Si le CLIP est déplacé vers un autre nœud du cluster, ce nœud devient le CCO. Le CCO est l'appliance Citrix ADC responsable des tâches de gestion dans le cluster. Un administrateur réseau utilise l'adresse CLIP pour se connecter au cluster pour effectuer des tâches de configuration et de gestion, telles que l'accès à l'interface graphique unifiée, la création de rapports, le suivi du flux de paquets et la collecte des journaux. Vous pouvez ajouter plusieurs adresses CLIP dans un cluster sur des réseaux identiques ou différents. Seules les configurations effectuées sur le CCO via l'adresse IP du cluster sont propagées vers d'autres nœuds du cluster.
- **Adresse IP par bandes**. Une adresse IP logique disponible sur tous les nœuds du cluster, il peut s'agir d'une adresse VIP ou SNIP.
- **Adresse IP spotted**. Une adresse IP logique (de préférence SNIP) n'est disponible que sur un nœud. Une adresse IP spotted n'a de visibilité que sur ce nœud. Pour réduire la surcharge de gestion du trafic, Citrix vous recommande d'utiliser une adresse SNIP repéré pour la communication back-end avec le serveur.

Le tableau suivant fournit les détails des configurations.

Adresse IP	NSIP	VIP	SNIP
Spotted	Oui	Oui	Oui
Striped	Non	Oui	Oui

Par exemple, dans un groupe de clusters à quatre nœuds, vous devez configurer chaque nœud avec une adresse SNIP spotted. Pour plus d'informations sur la configuration d'une configuration IP ponctuée, consultez Configurations rayées, partiellement rayées et ponctuées.

Vous pouvez définir une adresse SNIP pour être active sur un seul nœud, ou active sur tous les nœuds. Si l'adresse IP virtuelle et l'adresse IP de sous-réseau sont disponibles uniquement sur un nœud spécifique, elles sont de configuration ponctuelle. La configuration est définie comme répartie si l'adresse IP du sous-réseau et l'adresse IP du serveur virtuel sont disponibles sur tous les nœuds. Les adresses SNIP repéré aident à réduire le trafic de direction et de fond de panier.

Meilleures pratiques pour les liaisons VLAN et la configuration de l'itinéraire lors de la jonction d'un nœud au cluster

Liaisons IP VLAN

Lorsque vous liez un VLAN avec l'adresse IP repéré, le cluster Citrix ADC doit être configuré avec les adresses IP repéré dans le même sous-réseau sur tous les nœuds. Par exemple, dans un cluster à deux nœuds avec le nœud 0 et le nœud 1, vous pouvez avoir la configuration suivante :

```
1 add ns ip 192.254.101.101 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 1
2 add ns ip 192.254.101.102 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 0
3 add vlan 100
4 bind vlan 100 -IPAddress 192.254.101.101 255.255.255.0
5 <!--NeedCopy-->
```

Configuration du routage

Lorsque la configuration de routage est requise avec l'adresse IP repéré comme passerelle par défaut, le cluster ADC doit être configuré avec les adresses IP repéré dans le même sous-réseau sur tous les nœuds. Par exemple, dans un cluster à deux nœuds avec le nœud 0 et le nœud 1, vous pouvez avoir la configuration suivante :

```
1 add ns ip 192.254.101.101 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 1
2 add ns ip 192.254.101.102 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 0
3
4 add route 192.254.102.0 255.255.255.0 192.254.101.103
5 <!--NeedCopy-->
```

> **Remarque**
>
> Dans une configuration de cluster L3, seule la configuration SNIP repéré est prise en charge.

Configuration de la mise en cluster de couche 3

August 20, 2021

Comprendre le cluster L3

La demande d'étendre le déploiement à haute disponibilité et d'augmenter l'évolutivité du trafic client sur différents réseaux guidés pour établir le cluster L3. Le cluster L3 vous permet de regrouper les appliances Citrix ADC sur des sous-réseaux individuels (cluster L2).

Le cluster L3 est également appelé « cluster en mode INC (Independent Network Configuration) ». Dans le déploiement de cluster L3, les nœuds de cluster du même réseau sont regroupés pour former un groupe de nœuds. Le cluster L3 utilise le tunneling GRE pour diriger les paquets sur les réseaux. Les messages de pulsation dans les clusters L3 sont routés.

Ce document comprend les détails suivants :

- Architecture
- Exemple

Architecture

L'architecture de cluster L3 comprend les composants suivants :

- **Groupe de nœuds**. Les nœuds de cluster de chaque réseau (n1, n2) et (n3, n4), comme illustré dans la figure suivante, sont regroupés pour former un groupe de nœuds. Ces groupes de nœuds sont terminés au commutateur de couche 3 de chaque côté du réseau.
  - Le cluster communique avec le client via les connexions physiques entre le nœud de cluster et le périphérique de connexion côté client. Le regroupement logique de ces connexions physiques est appelé plan de données client.
  - Le cluster communique avec le serveur via les connexions physiques entre le nœud de cluster et le périphérique de connexion côté serveur. Le regroupement logique de ces connexions physiques est appelé plan de données du serveur.
- **Commutateur de backplane.** Les nœuds de cluster du même réseau communiquent entre eux à l'aide du backplane du cluster. Le backplane est un ensemble d'interfaces dans lesquelles une interface de chaque nœud est connectée à un commutateur commun, appelé commutateur de backplane de cluster.
- **Tunnel GRE.** Les paquets entre les nœuds d'un cluster L3 sont échangés sur un tunnel GRE non chiffré qui utilise les adresses NSIP des nœuds source et destination pour le routage. Le mécanisme de direction change pour les nœuds appartenant aux différents réseaux. Les paquets sont dirigés par un tunnel GRE vers le nœud sur l'autre sous-réseau, au lieu de réécrire le MAC.

Exemple

Prenons un exemple de déploiement de cluster L3 composé des éléments suivants :

- Trois appliances Citrix ADC (n1, n2 et n3) nœuds sont regroupés dans Nodegroup1.

- De même, les nœuds n4 et n5 sont regroupés dans Nodegroup2. Dans le troisième réseau, il y a deux groupes de nœuds. Nodegroup3 inclut n6 et n7 et Nodegroup4 inclut n8 et n9.
- Les appliances Citrix ADC qui appartiennent au même réseau sont combinées pour former un groupe de nœuds.

Points à prendre en compte avant de configurer le cluster L3

Tenez compte des points suivants avant de configurer le cluster L3 sur une appliance Citrix ADC :

- Le backplane n'est pas obligatoire lors de la configuration des sous-réseaux L3. Si le fond de panier n'est pas spécifié, le nœud ne passe pas à l'état d'échec du fond de panier.

  > **Remarque**
  >
  > Si vous avez plusieurs nœuds dans le même réseau L2, il est obligatoire de définir l'interface du fond de panier. Si l'interface du fond de panier n'est pas mentionnée, les nœuds passent à l'état d'échec du fond de panier.

- Les fonctionnalités L2 et les SNIP par répartition ne sont pas pris en charge dans le cluster L3.
- La distribution du trafic externe dans le cluster L3 prend uniquement en charge le chemin ECMP (Equal Cost Multiple Path).
- Les erreurs ICMP et la fragmentation ne sont pas traitées lorsque la direction est désactivée dans un déploiement de cluster L3 :
- Les entités réseau (`route`, `route6`, `pbr` et `pbr6`) doivent être liées au groupe de nœuds de configuration.
- VLAN, RNAT et le tunnel IP ne peuvent pas être liés à un groupe de nœuds de configuration.
- Le groupe de nœuds de configuration doit toujours avoir la propriété STRICT "YES.
- Les nœuds de cluster ne doivent pas être ajoutés à un groupe de nœuds de configuration via la commande « add cluster node ».
- La commande `add cluster instance -INC enabled` efface les entités réseau (route, route6, PBR, pb6, RNAT, tunnel IP, ip6tunnel).
- La commande `clear config extended`+ ne prend pas en charge les entités (route, route6, PBR, pb6, RNAT, tunnel IP, ip6tunnel) dans un cluster L3.

Configuration du cluster L3

Dans une configuration de cluster L3, la commande cluster a différents attributs à configurer qui sont basés sur les nœuds et les groupes de nœuds. La configuration du cluster L3 inclut également un profil IPv6 en dehors des profils IPv4.

La configuration d'un cluster L3 sur une appliance Citrix ADC comprend les tâches suivantes :

- Créer une instance de cluster
- Créer un groupe de nœuds dans un cluster L3
- Ajouter une appliance Citrix ADC au cluster et au groupe avec groupe de nœuds
- Ajouter une adresse IP de cluster au nœud
- Activer l'instance de cluster
- Enregistrer la configuration
- Ajouter un nœud à un groupe de nœuds existant
- Créer un groupe de nœuds dans un cluster L3
- Regrouper les nouveaux nœuds au groupe de nœuds nouvellement créé
- Joindre le nœud au cluster

Configuration des éléments suivants à l'aide de l'interface de ligne de commande

- **Pour créer une instance de cluster**

  ```
  add cluster instance <clid> -inc (<ENABLED|DISABLED>)[-processLocal <
  ENABLED | DISABLED]
  ```

- **Pour créer un groupe de nœuds dans un cluster L3**

  ```
  add cluster nodegroup <name>
  ```

- **Pour ajouter une appliance Citrix ADC au cluster et associer à un groupe de nœuds**

  ```
  add cluster node <nodeid> <nodeip> -backplane <interface_name> node
  group <ng>
  ```

- **Pour ajouter l'adresse IP du cluster sur ce nœud**

  ```
  add ns ip <IPAddress> <netmask> -type clip
  ```

- **Activer l'instance de cluster**

  ```
  enable cluster instance <clId>
  ```

- **Enregistrer la configuration**

  ```
  save ns config
  ```

- **Redémarrage à chaud de l'appliance**

  ```
  reboot -warm
  ```

- **Pour ajouter un nouveau nœud à un groupe de nœuds existant**

  ```
  add cluster node <nodeid> <nodeip> -nodegroup <ng>
  ```

- **Pour créer un groupe de nœuds dans un cluster L3**

  ```
  add cluster nodegroup <ng>
  ```


- **Pour regrouper de nouveaux nœuds vers le groupe de nœuds nouvellement créé**

  ```
  add cluster node <nodeid> <nodeip> -nodegroup <ng>
  ```

- **Pour joindre le nœud au cluster**

```
    join cluster  - clip <ip_addr> -password <password>

    add cluster instance 1  - inc ENABLED  - processLocal  ENABLED

       Done
<!--NeedCopy-->
```

> **Remarque**
>
> Le paramètre « inc » doit être ENABLED pour un cluster L3.

```
    add cluster nodegroup ng1

       Done

    > add cluster node 0 1.1.1.1  - state ACTIVE -backplane 0/1/1  -
       nodegroup ng1

       Done

    > add ns ip 1.1.1.100 255.255.255.255  - type clip

       Done

    > enable cluster instance 1

       Done

    > save ns config

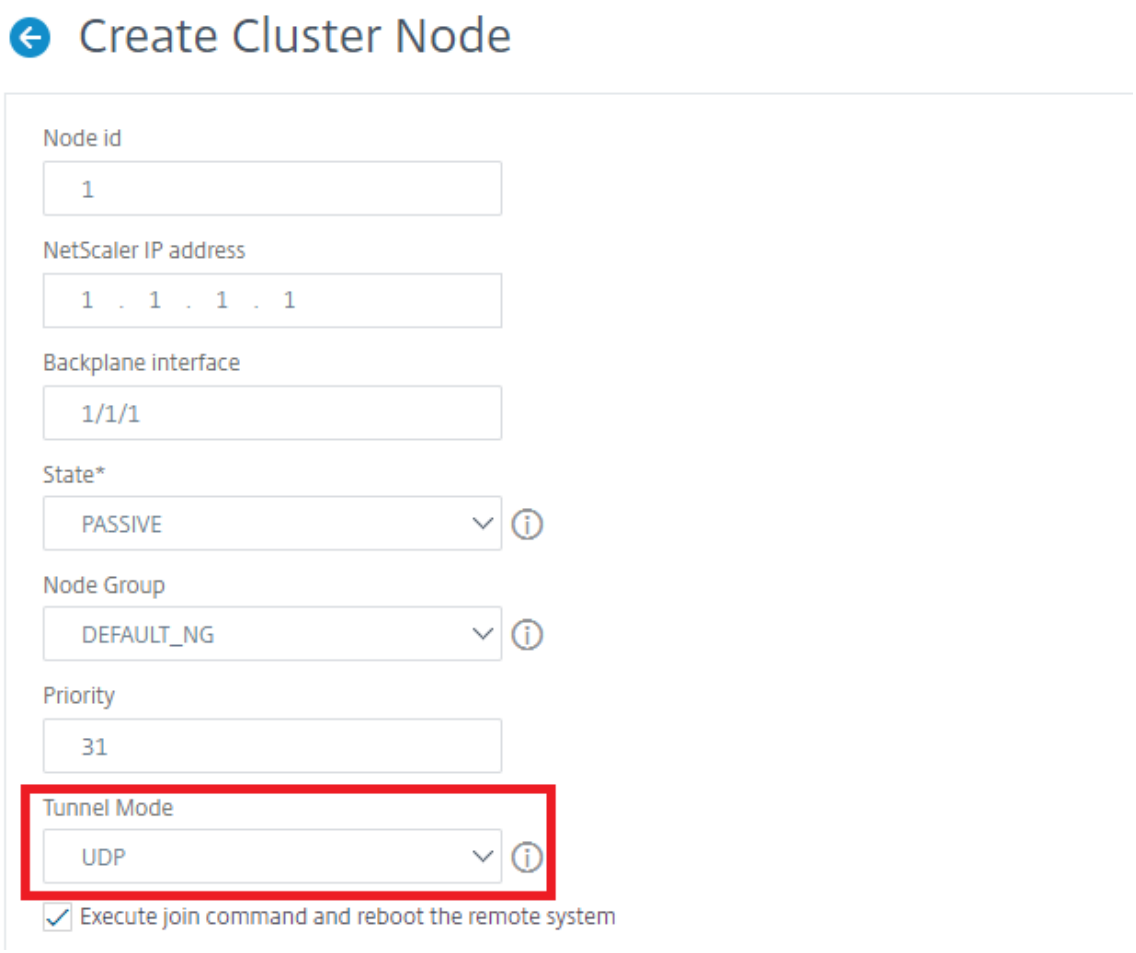
       Done

    > add cluster node 1 1.1.1.2  - state ACTIVE  - nodegroup ng1

       Done

    > add cluster nodegroup ng2

       Done

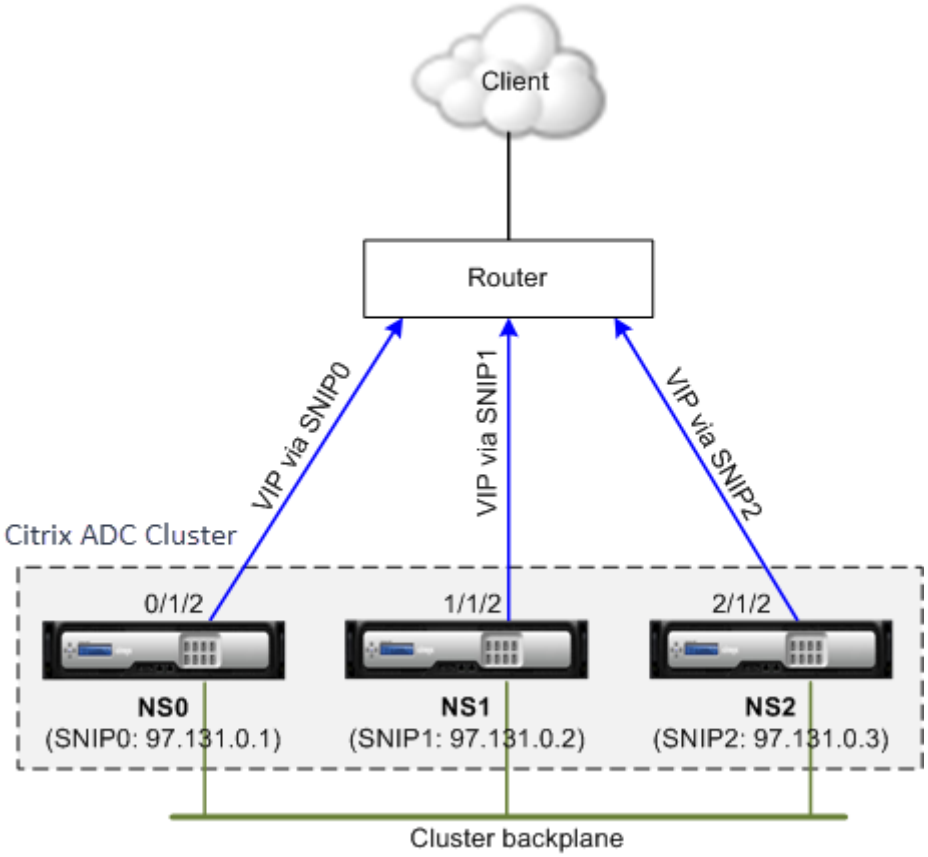
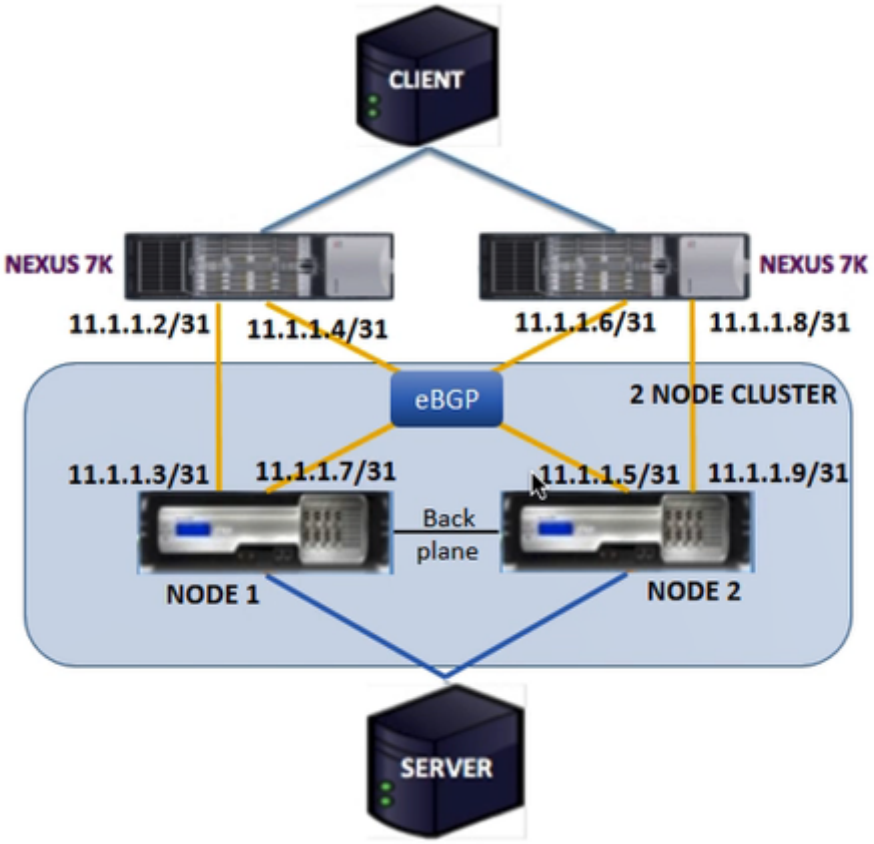
    > add cluster node 4 2.2.2.1  - state ACTIVE  - nodegroup ng2
```



```
30
31        Done
32
33     > add cluster node 5 2.2.2.2  -state ACTIVE  -nodegroup ng2
34
35        Done
36
37     > join cluster -clip 1.1.1.100 -password nsroot
38 <!--NeedCopy-->
```

Adresse IP du cluster publicitaire d'un cluster L3

Configurez l'adresse IP du cluster à publier sur le routeur amont pour rendre la configuration du cluster accessible à partir de n'importe quel sous-réseau.L'adresse IP du cluster est annoncée en tant que route du noyau par les protocoles de routage dynamique configurés sur un nœud.

La publicité de l'adresse IP du cluster comprend les tâches suivantes :

- **Activez l'option de routage de l'hôte de l'adresse IP du cluster**.L'option de route de l'hôte transmet l'adresse IP du cluster vers une table de routage ZeBOS pour la redistribution des routes du noyau via des protocoles de routage dynamiques.
- **Configuration d'un protocole de routage dynamique sur un nœud**.Un protocole de routage dynamique annonce l'adresse IP du cluster au routeur amont. Pour plus d'informations sur la configuration d'un protocole de routage dynamique, voirConfiguration des routes dynamiques.

Pour activer l'option de routage hôte de l'adresse IP du cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 -  add nsip <IPAddress> <netmask> -hostRoute ENABLED
2
3 -  show nsip <IPAddress>
4
5     > add ns ip 10.102.29.60 255.255.255.255 -hostRoute ENABLED
6
7        Done
8 <!--NeedCopy-->
```

Configurations spotted et striped partielles sur un cluster L3

Les configurations ponctuées et partiellement entrelacées sur le cluster L3 diffèrent légèrement de celles du cluster L2. La configuration peut différer d'un nœud à l'autre car les nœuds résident sur des

sous-réseaux différents. Les configurations réseau peuvent être spécifiques à un nœud dans le cluster L3. Par conséquent, vous devez configurer les configurations ponctuelles ou partiellement rayées en fonction des paramètres mentionnés ci-dessous.

Pour configurer des configurations ponctuées et partiellement répartie sur une appliance Citrix ADC sur le cluster L3, effectuez les tâches suivantes :

- Ajouter un groupe de propriétaires de cluster à une table de routage statique IPv4
- Ajouter un groupe de propriétaires de cluster à une table de routage statique IPv6
- Ajouter un groupe de propriétaires de cluster à un routage basé sur une stratégie IPv4
- Ajouter un groupe de propriétaires de cluster à un PBR IPv6
- Ajouter un VLAN
- Lier un VLAN à un groupe de propriétaires spécifique du groupe de nœuds de cluster

Configuration des éléments suivants à l'aide de l'interface de ligne de commande

- **Pour ajouter un groupe de propriétaires de cluster à une table de routage statique IPv4 de l'appliance Citrix ADC**

  ```
  add route <network> <netmask> <gateway> -owner group <ng>
  ```

- **Pour ajouter un groupe propriétaire de cluster à une table de routage statique IPv6 de l'appliance Citrix ADC**

  ```
  add route6 <network> -owner group <ng>
  ```

- **Pour ajouter un groupe de propriétaires de cluster à un PBR IPv4**

  ```
  add pbr <name> <action> -owner group <ng>
  ```

- **Pour ajouter un groupe propriétaire de cluster à un PBR IPv6**

  ```
  add pbr6 <name> <action> -owner group <ng>
  ```

- **Pour ajouter un VLAN**

  ```
  add vlan <id>
  ```

- **Pour lier un VLAN à un groupe propriétaire spécifique de groupe de nœuds de cluster**

  ```
  bind vlan <id> -ifnum - [IPAddress <ip_addr | ipv6_addr> [-owner group <ng>]
  ```

  Les commandes suivantes sont des exemples de configurations ponctuelles et partiellement rayées qui peuvent être configurées à l'aide de l'interface de ligne de commande.

```
1     > add route 10.102.29.0 255.255.255.0 10.102.29.2  - ownergroup ng2
2
3         Done
4
```



```
5      > add route6 fe80::9404:60ff:fedd:a464/64  - ownergroup ng1
6
7          Done
8
9      > add pbr pbr1 allow  - ownergroup ng1
10
11         Done
12
13     > add pbr6 pbr2 allow  - ownergroup ng2
14
15         Done
16
17     > add vlan 2
18
19         Done
20
21     > bind vlan 2  - ifnum 1/2  - [IPAddress 10.102.29.80 | fe80::9404:60
          ff:fedd:a464/64-ownergroup ng1
22
23         Done
24 <!--NeedCopy-->
```

Configuration du groupe de nœuds

Dans un cluster L3, pour répliquer le même ensemble de configurations sur plusieurs groupes de nœuds, les commandes suivantes sont utilisées :

Configuration des éléments suivants à l'aide de l'interface de commande

- **Pour ajouter une route statique IPv4 à la table de routage de l'appliance Citrix ADC**

  ```
  add route <network> <netmask> <gateway> -ownerGroup <ng>
  ```

Exemple de configuration :

```
1 add route 0 0 10.102.53.1  - ownerGroup ng1
2
3 add route 0 0 10.102.53.1  - ownerGroup ng2
4 <!--NeedCopy-->
```

Vous définissez un nouveau groupe de nœuds 'all' pour prendre en charge la configuration précédente, et vous devez configurer les commandes suivantes :

Configuration des éléments suivants à l'aide de l'interface de ligne de commande

- **Pour ajouter un nouveau groupe de nœuds à un cluster avec un paramètre strict**

  ```
  add cluster node group <name> -strict <YES | NO>
  ```

- **Pour lier un nœud de cluster ou une entité au groupe de nœuds donné**

  ```
  bind cluster nodegroup <name> -node <nodeid>
  ```

- **Pour ajouter une route statique IPv4 à tous les ownergroup**

  ```
  add route <network> <netmask> <gateway> -ownerGroup <ng>
  ```

Exemple de configuration :

```
1 add cluster nodegroup all -strict YES
2
3 bind cluster nodegroup all -node 1
4
5 bind cluster nodegroup all -node 2
6
7 add route 0 0 10.102.53.1 -ownerGroup all
8 <!--NeedCopy-->
```

Distribution du trafic dans un cluster L3

Dans une configuration de cluster, les réseaux externes visualisent la collection d'appliances Citrix ADC en tant qu'entité unique. Ainsi, le cluster doit sélectionner un nœud unique qui doit recevoir le trafic. Dans le cluster L3, cette sélection est effectuée à l'aide de l'ECMP. Le nœud sélectionné est appelé récepteur de flux.

> **Remarque**
>
> Pour un cluster L3 (nœuds sur différents réseaux), seule la distribution du trafic ECMP peut être utilisée.

Le récepteur de flux obtient le trafic, puis, à l'aide de la logique de cluster interne détermine le nœud qui doit traiter le trafic. Ce nœud est appelé le processeur de flux. Le récepteur de flux permet de diriger le trafic vers le processeur de flux sur le fond de panier si le récepteur de flux et le processeur de flux sont sur le même réseau. Le trafic est dirigé à travers le tunnel si le récepteur de flux et le processeur de flux se trouvent sur des réseaux différents.

> **Remarque**
>
> - Le récepteur de débit et le processeur de débit doivent être des nœuds capables de servir le trafic.

> - À partir de NetScaler 11, vous pouvez désactiver la direction sur le backplane du cluster. Pour plus d'informations, voir Désactivation du pilotage sur le fond de panier du cluster.

La figure précédente montre une demande client qui traverse le cluster. Le client envoie une demande à une adresse IP virtuelle (VIP). Un mécanisme de distribution du trafic configuré sur le plan de données client sélectionne l'un des nœuds de cluster comme récepteur de flux. Le récepteur de flux reçoit le trafic, détermine le nœud qui doit traiter le trafic et dirige la demande vers ce nœud (à moins que le récepteur de flux ne se sélectionne lui-même comme processeur de flux). Si le processeur de flux et le récepteur de flux se trouvent dans le même groupe de nœuds, le paquet est dirigé sur le fond de panier. Et si le processeur de flux et le récepteur de flux se trouvent dans des groupes de nœuds différents, le paquet est dirigé à travers le tunnel sur le chemin routé.

Le processeur de flux établit une connexion avec le serveur. Le serveur traite la demande et envoie la réponse à l'adresse IP du sous-réseau (SNIP) qui a envoyé la demande au serveur. Étant donné que dans le cluster L3, le SNIP est toujours un SNIP repéré, le nœud propriétaire de l'adresse SNIP reçoit la réponse du serveur.

Configuration d'un cluster Citrix ADC

August 20, 2021

Les appliances Citrix ADC que vous souhaitez ajouter au cluster doivent satisfaire aux critères spécifiés dans Prérequis pour les nœuds de cluster. Avant de configurer un cluster, vous devez connaître les bases du cluster. Pour plus d'informations, voir Présentation du cluster.

Pour former un cluster, vous devez configurer la communication inter-nœuds, créer le cluster (en ajoutant le premier dispositif Citrix ADC), puis ajouter les autres nœuds de cluster. Chacune de ces étapes est expliquée avec des détails pertinents dans les sujets suivants.

> **Remarque**
>
> Bien qu'il existe quelques différences dans la configuration d'un cluster L2 et L3, il existe également de nombreuses similitudes. Les rubriques suivantes expliquent la configuration des deux types de cluster tout en mettant en évidence les configurations spécifiques aux clusters L3.

Configuration de la communication entre les nœuds

August 20, 2021

Les nœuds d'une configuration de cluster communiquent entre eux à l'aide des mécanismes de communication inter-nœuds suivants :

- Les nœuds qui se trouvent dans le réseau (même sous-réseau) communiquent entre eux via le backplane du cluster. Le backplane doit être explicitement configuré. Voici les étapes détaillées.
- À travers les réseaux, la direction des paquets se fait via un tunnel GRE et d'autres communications de noeud à noeud sont acheminées entre les noeuds selon les besoins.

> **Important**
>
> - À partir de la version 11.0, toutes les versions, un cluster peut inclure des nœuds de différents réseaux.
> - À partir de la version 13.0 build 58.3, la direction GRE est prise en charge sur les cartes réseau Fortville dans un cluster L3.

Pour configurer le backplane du cluster, procédez comme suit pour chaque nœud

1. Identifiez l'interface réseau que vous souhaitez utiliser pour le backplane.
2. Connectez un câble Ethernet ou optique à partir de l'interface réseau sélectionnée au commutateur de backplane de cluster.

Par exemple, pour utiliser l'interface 1/2 comme interface de backplane pour le nœud 4, connectez un câble de l'interface 1/2 du nœud 4 au commutateur de backplane.

Points importants à noter lors de la configuration du backplane du cluster

- N'utilisez pas l'interface de gestion de l'appliance (0/x) comme interface de backplane. Dans un cluster, l'interface 0/1/x est lue comme suit :

  0 -> ID de nœud 0
  1/x -> Interface de Citrix ADC

- N'utilisez pas les interfaces de fond de panier pour les plans de données client ou serveur.
- Citrix recommande d'utiliser le canal Link Aggregate (LA) pour le fond de panier du cluster.
- Dans un cluster à deux nœuds, où le fond de panier est connecté dos à dos, le cluster est opérationnel hors service dans l'une des conditions suivantes :
  - L'un des nœuds est redémarré.
  - L'interface du fond de panier de l'un des nœuds est désactivée.

  Par conséquent, Citrix vous recommande de consacrer un commutateur distinct pour le fond de panier, de sorte que l'autre nœud de cluster et le trafic ne soient pas affectés. Vous ne pouvez pas mettre à l'échelle le cluster avec un lien dos à dos. Vous pouvez rencontrer un temps d'arrêt dans l'environnement de production lorsque vous mettez à l'échelle les nœuds de cluster.
- Les interfaces de backplane de tous les nœuds d'un cluster doivent être connectées au même commutateur et liées au même VLAN L2.

- Si vous avez plusieurs clusters avec le même ID d'instance de cluster, assurez-vous que les interfaces de backplane de chaque cluster sont liées à un VLAN différent.
- L'interface du backplane est toujours surveillée, quels que soient les paramètres de surveillance HA de cette interface.
- L'état de l'usurpation MAC sur les différentes plates-formes de virtualisation peut affecter le mécanisme de direction sur le backplane du cluster. Par conséquent, assurez-vous que l'état approprié est configuré :
  - XenServer - Désactiver l'usurpation MAC
  - Hyper-V - Activer l'usurpation MAC
  - VMware ESX - Activer l'usurpation MAC (assurez-vous également que « Transmissions forgées » est activé)
- Le MTU du backplane du cluster est automatiquement mis à jour. Toutefois, si des trames jumbo sont configurées sur le cluster, le MTU du backplane du cluster doit être explicitement configuré. La valeur doit être définie sur 78 + X, X étant la MTU maximale des plans de données client et serveur. Par exemple, si la MTU d'un plan de données serveur est 7500 et du plan de données client 8922. La MTU d'un fond de panier de cluster doit être définie sur 78 + 8922 = 9000. Pour définir ce MTU, utilisez la commande suivante :

  ```
  > set interface <backplane_interface> -mtu <value>
  ```

- La MTU pour les interfaces du commutateur de fond de panier doit être supérieure ou égale à 1 578 octets. Elle est applicable si le cluster possède des fonctionnalités telles que MBF, stratégies L2, ACL, routage dans les déploiements CLAG et vPath.

Prise en charge des tunnels basée sur UDP pour les grappes L2 et L3

À partir de Citrix ADC version 13.0 build 36.x, le cluster Citrix ADC L2 et L3 peut diriger le trafic en utilisant le tunneling basé sur UDP. Il est défini pour les communications inter-nœuds de deux nœuds dans un cluster. En utilisant le paramètre « mode tunnel », vous pouvez définir le mode tunnel GRE ou UDP à partir de la commande add and set cluster node.

Dans un déploiement de cluster L3, les paquets entre les nœuds Citrix ADC sont échangés sur un tunnel GRE non chiffré qui utilise les adresses NSIP des nœuds source et destination pour le routage. Lorsque cet échange se produit sur Internet, en l'absence d'un tunnel IPSec, les NSIP sont exposés sur Internet et peuvent entraîner des problèmes de sécurité.

> **Important**
>
> Citrix recommande aux clients d'établir leur propre solution IPSec lors de l'utilisation d'un cluster L3.

Le tableau suivant vous aide à classer la prise en charge des tunnels en fonction de différents déploiements.

Types de direction	AWS	Microsoft Azure	Local
MAC	Non pris en charge	Non pris en charge	Pris en charge
tunnel GRE	Pris en charge	Non pris en charge	Pris en charge
Tunnel UDP	Pris en charge	Pris en charge	Pris en charge

> **Important**
>
> Dans un cluster L3, le mode tunnel est défini sur GRE par défaut.

Configuration d'un tunnel basé sur UDP

Vous pouvez ajouter un nœud de cluster en définissant les paramètres de l'ID de nœud et en mentionnant l'état. Configurez le fond de panier en fournissant le nom de l'interface et sélectionnez le mode tunnel de votre choix (GRE ou UDP).

Procédures CLI

Pour activer le mode tunnel UDP à l'aide de l'interface de ligne de commande.

À l'invite de commandes, tapez :

- `add cluster node <nodeId>@ [-state <state>] [-backplane <interface_name>] [-tunnelmode <tunnelmode>]`
- `set cluster node <nodeId>@ [-state <state>] [-tunnelmode <tunnelmode>]`

> **Remarque**
>
> Les valeurs possibles pour le mode tunnel sont NONE, GRE, UDP.

Exemple

- `add cluster node 1 -state ACTIVE -backplane 1/1/1 -tunnelmode UDP`
- `set cluster node 1 -state ACTIVE -tunnelmode UDP`

Procédures GUI

Pour activer le mode tunnel UDP à l'aide de l'interface graphique.

1. Accédez à **Système > Cluster > Nœuds**.
2. Dans la page **Nœuds de cluster**, cliquez sur **Ajouter**.

3. Dans le champ **Créer un nœud de cluster**, définissez le paramètre **Mode tunnel** sur UDP et cliquez sur **Créer**.



4. Cliquez sur **Fermer**.

Création d'un cluster Citrix ADC

August 20, 2021

Pour créer un cluster, commencez par prendre l'un des appliances Citrix ADC que vous souhaitez ajouter au cluster. Sur ce nœud, vous devez créer l'instance de cluster et définir l'adresse IP de cluster. Ce nœud est le premier nœud de cluster et est appelé coordinateur de configuration de cluster (CCO). Toutes les configurations effectuées sur l'adresse IP du cluster sont stockées sur ce nœud, puis propagées aux autres nœuds du cluster.

La responsabilité de CCO dans une grappe n'est pas fixée à un nœud spécifique. Il peut changer au fil du temps en fonction des facteurs suivants :

- La priorité du nœud. Le nœud ayant la priorité la plus élevée (numéro de priorité le plus bas) devient CCO. Par conséquent, si un nœud dont le numéro de priorité est inférieur à l'ACO existant est ajouté, le nouveau nœud prend le relais en tant que CCO.

  > **Remarque**
  >
  > La priorité de nœud peut être configurée à partir de NetScaler 10.1.

- Si le CCO actuel tombe en panne, le nœud avec le numéro de priorité le plus bas prend le relais en tant que CCO. Si la priorité n'est pas définie ou s'il existe plusieurs nœuds avec le numéro de priorité le plus bas, le CCO est sélectionné parmi l'un des nœuds disponibles.

> **Remarque**
>
> Les configurations de l'appliance (y compris les adresses SNIP et les VLAN) sont effacées en exécutant implicitement la `clear ns config extended` commande. Toutefois, le VLAN par défaut et le NSVLAN ne sont pas effacés de l'appliance. Par conséquent, si vous souhaitez que le NSVLAN soit sur le cluster, assurez-vous qu'il est créé avant l'ajout de l'appliance au cluster. Pour un cluster L3 (nœuds de cluster sur différents réseaux), les configurations réseau ne sont pas effacées de l'appliance.
>
> **Important**
>
> HA Monitor (HAMON) sur une configuration de cluster est utilisé pour surveiller l'intégrité d'une interface sur chaque nœud. Le paramètre HAMON doit être activé sur chaque nœud pour surveiller l'état de l'interface. Si l'état opérationnel de l'interface HAMON activée s'éteint pour une raison quelconque, le nœud de cluster respectif est marqué comme étant malsain (NOT UP) et ce nœud ne peut pas servir le trafic.

Pour créer un cluster à l'aide de l'interface de ligne de commande

1. Ouvrez une session sur une appliance (par exemple, une appliance dotée d'une adresse NSIP 10.102.29.60) que vous souhaitez ajouter au cluster.
2. Ajoutez une instance de cluster.

   ```
   add cluster instance <clId> -quorumType <NONE | MAJORITY> -inc <ENABLED
    | DISABLED> -backplanebasedview <ENABLED | DISABLED><!--NeedCopy-->
   ```

   > **Remarque**
   >
   > ```
   > 1     -  L'ID d'instance de cluster doit être unique au sein d'un
   >           réseau local.
   > ```
   >
   > - Le paramètre `-quorumType` doit être défini sur MAJORITY et non sur NONE dans les scénarios suivants :

  - Topologies qui n'ont pas de liens redondants entre les nœuds de cluster. Ces topologies peuvent être sujettes à la partition réseau en raison d'un point de défaillance unique.
  - Lors d'opérations de cluster telles que l'ajout ou la suppression de nœuds.
- Pour un cluster L3, assurez-vous que le paramètre `-inc` est défini sur ENABLED. Le paramètre `-inc` doit être désactivé pour un cluster L2.
- Lorsque le paramètre `-backplanebasedview` est activé, la vue opérationnelle (ensemble de nœuds servant le trafic) est décidée en fonction des pulsations reçues uniquement sur l'interface du fond de panier. Par défaut, ce paramètre est désactivé. Lorsque ce paramètre est désactivé, un nœud ne dépend pas de la réception des pulsations de cœur uniquement sur le fond de panier.

3. [Uniquement pour un cluster de niveau 3] Créez un groupe de nœuds. À l'étape suivante, le nœud de cluster nouvellement ajouté doit être associé à ce groupe de nœuds.

   > **Remarque**
   >
   > Ce groupe de nœuds comprend tout ou un sous-ensemble des appliances Citrix ADC qui appartiennent au même réseau.

   ```
   add cluster nodegroup <name><!--NeedCopy-->
   ```

4. Ajoutez le dispositif Citrix ADC au cluster.

   "'add cluster node -state -backplane -nodegroup

   ```
   > **Remarque** Pour un cluster L3 :
   >
   >-  Le paramétre de groupe de nœuds doit être défini sur le nom du groupe de nœuds créé.
   >-  Le paramétre fond de panier est obligatoire pour les nœuds associés à un groupe de nœuds comportant plusieurs nœuds, afin que les nœuds du réseau puissent communiquer entre eux.</span>

   Exemple :

   Ajout d'un nœud pour un cluster L2 (tous les nœuds de cluster se trouvent dans le même réseau).
   ```

   add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1

   ```
   Ajout d'un nœud pour un cluster L3 qui inclut un nœud unique de chaque réseau. Ici, vous n'avez pas à définir le backplane.
   ```

   add cluster node 0 10.102.29.60 -state PASSIVE -nodegroup ng1


```
Ajout d'un nœud pour un cluster L3 qui inclut plusieurs nœuds de
    chaque réseau. Ici, vous devez définir le fond de panier
   afin que les nœuds d'un réseau puissent communiquer entre eux
   .
```

add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1 -nodegroup ng1
“‘

5. Ajoutez l’adresse IP du cluster (par exemple, 10.102.29.61) sur ce nœud.

```
add ns ip <IPAddress> <netmask> -type clip
<!--NeedCopy-->
```

Exemple

```
> add ns ip 10.102.29.61 255.255.255.255 -type clip
<!--NeedCopy-->
```

6. Activez l’instance de cluster.

```
enable cluster instance <clId><!--NeedCopy-->
```

7. Enregistrez la configuration.

```
save ns config<!--NeedCopy-->
```

8. Redémarrez l’appliance à chaud.

```
reboot -warm<!--NeedCopy-->
```

Vérifiez les configurations de cluster à l’aide de la commande show cluster instance. Vérifiez que la sortie de la commande affiche l’adresse NSIP de l’appliance en tant que nœud du cluster.

9. Une fois que le nœud est UP, connectez-vous au CLIP et modifiez les informations d’identification RPC pour l’adresse IP du cluster et l’adresse IP du nœud. Pour plus d’informations sur la modification du mot de passe d’un nœud RPC, voir Modifier le mot de passe d’un nœud RPC.

Pour créer un cluster à l’aide de l’interface graphique

1. Ouvrez une session sur une appliance (par exemple, une appliance dotée d’une adresse NSIP 10.102.29.60) que vous avez l’intention d’ajouter au cluster.
2. Accédez à **Système > Cluster.**
3. Dans le volet d’informations, cliquez sur le lien **Gérer le cluster** .
4. Dans la boîte de dialogue Configuration du cluster, définissez les paramètres requis pour créer un cluster. Pour une description d’un paramètre, placez le curseur de la souris sur la zone de texte correspondante.

5. Cliquez sur **Créer**.
6. Dans la boîte de dialogue Configurer l'instance de cluster, activez la case à cocher Activer l'instance de cluster.
7. Dans le volet Nœuds de cluster, sélectionnez le nœud et cliquez sur **Ouvrir.**
8. Dans la boîte de dialogue Configurer le nœud de cluster, définissez l'état.
9. Cliquez sur **OK**, puis cliquez sur **Enregistrer.**
10. Redémarrez l'appliance à chaud.
11. Une fois que le nœud est UP, connectez-vous au CLIP et modifiez les informations d'identification RPC pour l'adresse IP du cluster et l'adresse IP du nœud. Pour plus d'informations sur la modification du mot de passe d'un nœud RPC, voir Modifier le mot de passe d'un nœud RPC.

Prise en charge du mode strict pour l'état de synchronisation du cluster

Vous pouvez désormais configurer un nœud de cluster pour afficher les erreurs lors de l'application de la configuration. Un nouveau paramètre, « SyncStatusStrictMode » est introduit dans la commande add and set cluster instance afin de suivre l'état de chaque nœud d'un cluster. Par défaut, le paramètre « SyncStatusStrictMode » est désactivé.

Pour activer le mode strict à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cluster instance <clID> [-syncStatusStrictMode (ENABLED | DISABLED)]
```

Exemple :

```
set cluster instance 1 -syncStatusStrictMode ENABLED
```

Pour afficher l'état du mode strict à l'aide de l'interface de ligne de commande

```
1     >show cluster instance
2     1) Cluster ID: 1
3         Dead Interval: 3 secs
4         Hello Interval: 200 msecs
5         Preemption: DISABLED
6         Propagation: ENABLED
7         Quorum Type: MAJORITY
8         INC State: DISABLED
9         Process Local: DISABLED
10        Retain Connections: NO
11        Heterogeneous: NO
12        Backplane based view: DISABLED
```



```
13          Cluster sync strict mode: ENABLED
14          Cluster Status: ENABLED(admin), ENABLED(operational), UP
15
16        WARNING(s):
17          (1) - There are no spotted SNIPs configured on the cluster.
                Spotted SNIPs can help improve cluster performance
18
19          Member Nodes:
20          Node ID     Node IP      Health     Admin State  Operational
                State
21          -------     -------      ------     -----------
                -----------------
22      1)      1           192.0.2.20      UP         ACTIVE       ACTIVE(
            Configuration Coordinator)
23      2)      2           192.0.2.21      UP         ACTIVE       ACTIVE
24      3)      3           192.0.2.19*     UP         ACTIVE       ACTIVE
25  <!--NeedCopy-->
```

Pour afficher la raison d'échec de synchronisation d'un nœud de cluster à l'aide de l'interface graphique

1. Accédez à **Système > Cluster > Nœuds de cluster**.
2. Dans la page **Nœuds de cluster**, faites défiler l'écran vers l'extrême droite pour afficher les détails de la raison d'échec de synchronisation des nœuds de cluster.

Ajout d'un nœud au cluster

August 20, 2021

Vous pouvez facilement redimensionner la taille d'un cluster pour inclure un maximum de 32 nœuds. Lorsqu'une appliance Citrix ADC est ajoutée au cluster, les configurations de cette appliance sont effacées (en exécutant en interne la commande clear ns config -extended). Les adresses SNIP, les paramètres **MTU** de l'interface du fond de panier et toutes les configurations de VLAN (à l'exception du VLAN et du NSVLAN par défaut) sont également effacés de l'appliance.

Les configurations de cluster sont ensuite synchronisées sur ce nœud. Il peut y avoir une baisse intermittente du trafic pendant que la synchronisation est en cours.

> **Important**
>
> Avant d'ajouter une appliance Citrix ADC à un cluster :

- Configurez l'interface de backplane pour le nœud. Vérifiez la rubrique précédente.
- Vérifiez si les licences disponibles sur l'appliance correspondent à celles disponibles sur le coordinateur de configuration. L'appliance n'est ajoutée que si les licences correspondent.
- Si vous souhaitez que le NSVLAN soit sur le cluster, assurez-vous que le NSVLAN est créé sur l'appliance avant d'être ajouté au cluster.
- Citrix vous recommande d'ajouter le nœud en tant que nœud passif. Ensuite, après avoir joint le nœud au cluster, complétez la configuration spécifique du nœud à partir de l'adresse IP du cluster. Exécutez la commande forcer cluster sync si le cluster a uniquement des adresses IP repéré. Et qui a une liaison VLAN L3, ou a des routes statiques.
- Lorsqu'une appliance dotée d'un canal d'agrégat de liens préconfiguré est ajoutée à un cluster, le canal LA continue d'exister dans l'environnement de cluster. Le canal LA est renommé de LA/x en NodeId/LA/x, où LA/x est l'identificateur de canal LA.

Pour ajouter un nœud au cluster à l'aide de l'interface de ligne de commande

Remarque

Lorsque vous ajoutez un nœud à une configuration de cluster, si le nœud a une route statique par défaut, il est ajouté au nœud de coordinateur de cluster (CCO). Si cette route statique par défaut pointe vers une Gateway incorrecte, elle peut entraîner des temps d'arrêt des services. Par conséquent, vérifiez la route statique par défaut du nouveau nœud, avant de l'ajouter à la configuration du cluster.

1. Ouvrez une session sur l'adresse IP du cluster, à l'invite de commandes, procédez comme suit :
   - Ajoutez l'appliance (par exemple, 10.102.29.70) au cluster.

   Remarque

   Pour un cluster L3 :

   ```
   1 -  Le paramétre de groupe de nœuds doit être défini sur un
        groupe de nœuds qui posséde des nœuds du même réseau.
   ```

   - Si ce nœud appartient au même réseau que le premier nœud ajouté, configurez le groupe de nœuds utilisé pour ce nœud.
   - Si ce nœud appartient à un réseau différent, créez un groupe de nœuds et liez ce nœud au groupe de nœuds.
   - Le paramètre fond de panier est obligatoire pour les nœuds associés à un groupe de nœuds comportant plusieurs nœuds, afin que les nœuds du réseau puissent communiquer entre eux.

   ```
   1 add cluster node <nodeId> <IPAddress> -state <state> -backplane <
       interface_name> -nodegroup <name>
   ```



```
2
3 Example:
4
5 add cluster node 1 10.102.29.70 -state PASSIVE -backplane 1/1/1
6 <!--NeedCopy-->
```

- Enregistrez la configuration.

```
1 save ns config
2 <!--NeedCopy-->
```

2. Ouvrez une session sur le nœud nouvellement ajouté (par exemple, 10.102.29.70) et rejoignez le nœud au cluster.

```
1 join cluster -clip <ip_addr> -password <password>
2
3 Example:
4
5 join cluster -clip 10.102.29.61 -password nsroot
6 <!--NeedCopy-->
```

3. Configurez les commandes suivantes sur le CLIP.
   - Lier un VLAN à une interface

     ```
     1 bind vlan <id> -ifnum <interface_name>
     2 <!--NeedCopy-->
     ```

     Exemple :

     ```
     1 bind vlan 1 -ifnum 2/1/2
     2 <!--NeedCopy-->
     ```

   - Ajouter une adresse IP ponctuée au nœud nouvellement ajouté

     ```
     1 add ns ip <IpAddress> <netmask> -ownerNode <positive_interger
         >
     2 <!--NeedCopy-->
     ```

     Exemple :

     ```
     1 add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2
     2 <!--NeedCopy-->
     ```

   - Vérifier le VLAN sur NSIP


```
show vlan <id>
<!--NeedCopy-->
```

Exemple :

```
show vlan 1
<!--NeedCopy-->
```

4. Effectuez les configurations suivantes :
   - Si le nœud est ajouté à un cluster qui a uniquement des adresses IP spotted, les configurations sont synchronisées avant que les adresses IP spotted ne soient affectées à ce nœud. Dans de tels cas, les liaisons VLAN L3 peuvent être perdues. Pour éviter cette perte, ajoutez une IP par répartition ou ajoutez les liaisons VLAN L3.
   - Définissez les configurations spotted requises.
   - Définissez le MTU pour l'interface de backplane.
5. Enregistrez la configuration.

```
save ns config
<!--NeedCopy-->
```

6. Redémarrez l'appliance à chaud.

```
reboot -warm
<!--NeedCopy-->
```

7. Une fois que le nœud est UP et que la synchronisation a réussi, modifiez les informations d'identification RPC pour le nœud à partir de l'adresse IP du cluster. Pour plus d'informations sur la modification du mot de passe d'un nœud RPC, voir Modifier le mot de passe d'un nœud RPC.

```
set rpcNode <node-NSIP> -password <passwd>

Example:

set rpcNode 192.0.2.4 -password mypassword
<!--NeedCopy-->
```

8. Définissez le nœud du cluster sur Actif.

```
set cluster node <nodeID> -state active.

Example:
```



```
4
5 set cluster node 1 -state active
6 <!--NeedCopy-->
```

Pour ajouter un nœud au cluster à l'aide de l'interface graphique

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster > Nœuds**.
3. Dans le volet d'informations, cliquez sur **Ajouter** pour ajouter le nouveau nœud (par exemple, 10.102.29.70).
4. Dans la boîte de dialogue **Créer un nœud de cluster**, configurez le nouveau nœud. Pour une description d'un paramètre, placez le curseur de la souris sur la zone de texte correspondante.
5. Cliquez sur **Créer**. Lorsque vous êtes invité à effectuer un redémarrage à chaud, cliquez sur **Oui.**
6. Une fois que le nœud est UP et que la synchronisation a réussi, modifiez les informations d'identification RPC pour le nœud à partir de l'adresse IP du cluster. Pour plus d'informations sur la modification du mot de passe d'un nœud RPC, voir Modifier le mot de passe d'un nœud RPC.
7. Accédez à **Système > Cluster > Noeuds > Modifier**.
8. Modifiez l'état en **ACTIVE** et confirmez.

Pour joindre un nœud précédemment ajouté au cluster à l'aide de l'interface graphique

Si vous avez utilisé l'interface de ligne de commande pour ajouter un nœud au cluster, mais que vous n'avez pas joint le nœud au cluster, vous pouvez utiliser la procédure suivante.

> **Remarque**
>
> Lorsqu'un nœud rejoint le cluster, il prend en charge sa part de trafic à partir du cluster et, par conséquent, une connexion existante peut être interrompue.

1. Connectez-vous au nœud que vous souhaitez joindre au cluster (par exemple, 10.102.29.70).
2. Accédez à **Système > Cluster.**
3. Dans le volet d'informations, sous Mise en route, cliquez sur le lien Joindre un cluster.
4. Dans la boîte de dialogue Joindre au cluster existant, définissez l'adresse IP du cluster et le `nsroot` mot de passe du coordinateur de configuration. Pour une description d'un paramètre, placez le curseur de la souris sur la zone de texte correspondante.
5. Cliquez sur **OK.**

Affichage des détails d'un cluster

January 21, 2021

Vous pouvez afficher les détails de l'instance de cluster et des nœuds de cluster en vous connectant à l'adresse IP du cluster.

Pour afficher les détails d'une instance de cluster à l'aide de l'interface de ligne de commande

Ouvrez une session sur l'adresse IP du cluster et, à l'invite de commandes, tapez :

```
show cluster instance <clId>
```

> **Remarque**
>
> Lorsque la commande précédente est exécutée à partir de l'adresse NSIP du nœud non-CCO, la commande affiche l'état du cluster sur ce nœud.

Pour afficher les détails d'un nœud de cluster à l'aide de l'interface de ligne de commande

Ouvrez une session sur l'adresse IP du cluster et, à l'invite de commandes, tapez :

```
show cluster node <nodeId>
```

Pour afficher les détails d'une instance de cluster à l'aide de l'interface graphique

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster.**
3. Dans le volet d'informations, sous **Mise en route**, cliquez sur le lien **Gérer le cluster**pour afficher les détails du cluster.

Pour afficher les détails d'un nœud de cluster à l'aide de l'interface graphique

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster > Nœuds.**
3. Dans le volet d'informations, cliquez sur le nœud pour lequel vous souhaitez afficher les détails.

Répartition du trafic entre les nœuds de cluster

January 21, 2021

Après avoir créé le cluster Citrix ADC et effectué les configurations requises, vous devez déployer ECMP (Equal Cost Multiple Path) ou l'agrégation de liens de cluster (LA) sur le plan de données client (pour le trafic client) ou le plan de données du serveur (pour le trafic serveur). Ces mécanismes répartissent le trafic externe sur les nœuds de cluster.

Direction du backplane basée sur des règles

La direction du backplane basée sur des stratégies (PBS) est un mécanisme dans le déploiement du cluster, qui dirige le trafic entre les nœuds du cluster en fonction de la méthode de hachage définie pour le flux. Le flux est défini par une combinaison de paramètres L2 et L3 similaires à la liste de contrôle d'accès (ACL).

Le PBS prend en charge à la fois le trafic IPv4 et IPv6. Dans le cas des déploiements IPv6, la direction prend en charge une option supplémentaire `[dfdprefix <positive_integer>]`. Il offre la flexibilité de choisir le même processeur de flux pour le même préfixe IP. L'option de préfixe est prise en charge uniquement pour les méthodes de hachage IP source ou IP de destination.

> **Remarque**
>
> Si le mécanisme PBS n'est pas utilisé pour diriger le trafic, le trafic est dirigé par la méthode par défaut.

Pour configurer les nouveaux attributs ACL, à l'interface de ligne de commande, tapez les commandes suivantes :

Commandes CLI pour IPv4

- `add ns acl <aclname> <aclaction> [-type (classic | dfd)] [-dfdhash <dfdhash>]`
- `set ns acl <aclname> <aclaction> [-dfdhash <dfdhash>`
- `show ns acl [<aclname>][-type (classic | DFD)]`
- `apply ns acls [-type (classic | DFD)]`
- `clear ns acls [-type (classic | DFD)]`
- `renumber ns acls [-type (classic | DFD)]`

Commandes CLI pour IPv6

- `add ns acl6 <acl6name> <acl6action> [-type (classic | dfd)][-dfdhash <dfdhash>][-dfdprefix <positive_interger>]`

- `set ns acl6 <acl6name> <acl6action> [-dfdhash <dfdhash>][-dfdprefix <positive_interger>]`
- `show ns acl6 [<acl6name>][-type (classic | DFD)]`
- `apply ns acls6 [-type (classic | DFD)]`
- `clear ns acls6 [-type (classic | DFD)]`
- `renumber ns acls6 [-type (classic | DFD)]`

Voici les différents types de méthodes de hachage que vous pouvez spécifier pour diriger le paquet vers le processeur de flux :

- SIP-SPORT-DIP-DPORT
- SIP
- DIP
- SIP-DIP
- SIP-SPORT

Limitations

1. La distribution du flux de trafic entre les nœuds de cluster n'est pas assurée, car le processeur de flux est déterminé par les règles configurées par l'administrateur.
2. Le mode L2 n'est pas pris en charge.
3. Les groupes de nœuds et les SNIP par répartition ne sont pas pris en charge, car il n'existe aucun scénario de déploiement.
4. MPTCP n'est pas pris en charge.
5. Prise en charge uniquement du trafic TCP, UDP et ICMP.
6. Le cluster sur le mode L3 n'est pas pris en charge.
7. Processus local au niveau du service n'est pas pris en charge.

Utilisation du chemin d'accès multiple à coût égal (ECMP)

August 20, 2021

En utilisant le mécanisme ECMP (Equal Cost Multiple Path) sur un déploiement de cluster, les nœuds de cluster actifs annoncent les adresses IP du serveur virtuel. Le nœud de cluster qui reçoit le trafic annoncé dirige le trafic vers le nœud qui doit traiter le trafic. Il peut y avoir une direction redondante dans les serveurs virtuels repérés et partiellement entrelacés. Par conséquent, à partir de NetScaler 11, les adresses IP de serveurs virtuels spotted et striped partiels annoncent les nœuds propriétaires, ce qui réduit la direction redondante.

Vous devez avoir une connaissance détaillée des protocoles de routage pour utiliser ECMP. Pour plus d'informations, reportez-vous à la section Configuration des routes dynamiques. Pour plus

d'informations sur le routage dans un cluster, voir Routage dans un cluster.

Pour utiliser ECMP, vous devez d'abord effectuer les opérations suivantes :

- Activez le protocole de routage requis (OSPF, RIP, BGP ou ISIS) sur l'adresse IP du cluster.
- Liez les interfaces et l'adresse IP spotted (avec le routage dynamique activé) à un VLAN.
- Configurez le protocole de routage sélectionné et redistribuez les routes du noyau sur les ZEBO à l'aide du shell VTYSH.

Effectuez des configurations similaires sur l'adresse IP du cluster et sur le périphérique de connexion externe.

> **Remarque**
>
> - Assurez-vous que les licences du cluster prennent en charge le routage dynamique, sinon ECMP ne fonctionne pas.
> - ECMP n'est pas pris en charge pour les serveurs virtuels génériques car RHI a besoin d'une adresse VIP pour faire de la publicité sur un routeur et des serveurs virtuels génériques. Comme ils n'ont pas d'adresses VIP associées.

Figure 1. Topologie ECMP



Lorsque vous utilisez le mécanisme ECMP pour la distribution du trafic sur un déploiement de clus-

ter, les nœuds de cluster actifs annoncent les adresses IP du serveur virtuel sur le routeur amont. Le routeur ECMP peut atteindre l'adresse VIP via SNIP0, SNIP1 ou SNIP2. Le flux de trafic dans la figure 1 est décrit comme suit :

1. Le client envoie une requête au VIP hébergé sur le cluster.
2. Le routeur amont, basé sur les routes apprises du VIP, transmet le paquet à l'un des nœuds. Disons NS1. Le nœud NS1 est le récepteur de flux.
3. Le récepteur de flux (NS1) détermine le nœud qui doit traiter le trafic, appelé processeur de flux. Par exemple, Node NS2 est le processeur de flux.
4. Le récepteur de flux (NS1) avec SNIP1 (97.131.0.2) achemine la demande vers le processeur de flux (NS2) avec SNIP2 (97.131.0.3).
5. Le processeur de flux (NS2) établit une connexion avec le serveur.
6. Le serveur traite la demande et envoie la réponse à l'adresse SNIP qui a envoyé la demande au serveur.

Remarques :

- Seuls les nœuds ACTIVE annoncent les routes VIP.
- Les nœuds INACTIFS n'annoncent pas les routes VIP.
- Tous les nœuds ACTIVE annoncent les VIP rayés.
- Seuls les nœuds de propriétaire ACTIVE annoncent des VIP ponctués ou partiellement rayés.

Pour configurer ECMP sur le cluster à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'adresse IP du cluster.
2. Activez le protocole de routage.

```
enable ns feature <feature>
```

Exemple : pour activer le protocole de routage OSPF.

```
enable ns feature ospf
```

3. Ajoutez un VLAN.

```
add vlan <id>
```

Exemple

```
add vlan 97
```

4. Liez les interfaces des nœuds de cluster au VLAN.

```
bind vlan <id> -ifnum <interface_name>
```


Exemple

```
bind vlan 97 -ifnum 0/1/2 1/1/2 2/1/2
```

5. Ajoutez une adresse SNIP spotted pour chaque nœud et activez le routage dynamique sur celui-ci.

```
add ns ip <SNIP> <netmask> -ownerNode <positive_integer> -
    dynamicRouting ENABLED
```

Exemple

```
add ns ip 97.131.0.1 255.0.0.0 -ownerNode 0 -dynamicRouting
    ENABLED -type SNIP
add ns ip 97.131.0.2 255.0.0.0 -ownerNode 1 -dynamicRouting
    ENABLED -type SNIP
add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2 -dynamicRouting
    ENABLED -type SNIP
```

6. Liez l'une des adresses SNIP spotted au VLAN. Lorsque vous liez une adresse SNIP spotted à un VLAN, toutes les autres adresses SNIP spotted définies sur le cluster dans ce sous-réseau sont automatiquement liées au VLAN.

```
bind vlan <id> -IPAddress <SNIP> <netmask>
```

Exemple

```
bind vlan 97 -ipAddress 97.131.0.1 255.0.0.0
```

> **Remarque**
>
> Vous pouvez utiliser les adresses NSIP des nœuds de cluster au lieu d'ajouter des adresses SNIP. Si c'est le cas, vous n'avez pas à effectuer les étapes 3 à 6.

7. Configurez le protocole de routage sur les ZEBOs à l'aide du shell VTYSH.

Exemple :

Pour configurer un protocole de routage OSPF sur les ID de nœud 0, 1 et 2.

```
vtysh
! interface vlan97 !
 router ospf   owner-node 0
ospf router-id 97.131.0.1   exit-owner-node
owner-node 1    ospf router-id 97.131.0.2
exit-owner-node
owner-node 2
```



```
8 ospf router-id 97.131.0.3   exit-owner-node   redistribute kernel
    network 97.0.0.0/8 area 0  !
```

> **Remarque**
>
> Pour que les adresses VIP soient annoncées, le paramètre RHI est fait en utilisant le paramètre vServerRhilevel comme suit :

```
1 add ns ip <IPAddress> <netmask> -type VIP -vserverRHILevel <
    vserverRHILevel>
```

Pour les paramètres RHI spécifiques à OSPF, il existe d'autres paramètres qui peuvent être effectués comme suit :

```
1 add ns ip <IPAddress> <netmask> -type VIP -ospfLSAType ( TYPE1 |
    TYPE5 ) -ospfArea <positive_integer>
```

Utilisez la commande add ns ip6 pour exécuter les commandes précédentes sur les adresses IPv6.

8. Configurez ECMP sur le commutateur externe. Les exemples de configuration suivants sont fournis pour le commutateur Cisco® Nexus 7000 C7010 version 5.2(1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

```
1 //For OSPF (IPv4 addresses) Global config: Configure terminal
    feature ospf    Interface config:  Configure terminal
    interface Vlan10      no shutdown      ip address 97.131.0.5/8
       Configure terminal  router ospf 1  network 97.0.0.0/8 area
    0.0.0.0  --------------------------------
2
3 //For OSPFv3 (IPv6 addresses) Global config:  Configure terminal
    feature ospfv3    Configure terminal  interface Vlan10      no
    shutdown      ipv6 address use-link-local-only      ipv6 router
     ospfv3 1 area 0.0.0.0    Configure terminal  router ospfv3 1
```

Noeuds de cluster de surveillance de routeur dans le déploiement ECMP

Dans une configuration de cluster, sur un nœud propriétaire qui possède une configuration d'adresse SNIP spotted, vous pouvez maintenant désactiver l'option OwnerDownResponse. Par défaut, l'option est activée, permettant au nœud de répondre à une requête ICMP/ARP/ICMP6/ND6 provenant du routeur en amont. Vous pouvez maintenant désactiver cette option pour permettre au routeur de surveiller si un nœud de cluster est actif ou inactif. Lorsque le routeur envoie une demande, si l'option est désactivée, il identifie le nœud propriétaire comme étant inactif et indisponible pour la distribution du trafic.

Pour configurer ECMP pour la distribution du trafic des routes statiques à l'aide de l'interface de ligne de commande

```
add ns ip <ipddress> <netmask> -ownernode <node-id>  - ownerDownResponse
    disable
```

Cas d'utilisation : ECMP avec routage BGP

January 21, 2021

Pour configurer ECMP avec le protocole de routage BGP, effectuez les opérations suivantes :

1. Connectez-vous à l'adresse IP du cluster.
2. Activer le protocole de routage BGP.

```
> enable ns feature bgp
```

3. Ajoutez un VLAN et liez les interfaces requises.

```
> add vlan 985
> bind vlan 985 -ifnum 0/0/1 1/0/1
```

4. Ajoutez les adresses IP spotted et liez-les au VLAN.

```
> add ns ip 10.100.26.14 255.255.255.0 -ownerNode 1 -
    dynamicRouting ENABLED
> add ns ip 10.100.26.15 255.255.255.0 -ownerNode 2 -
    dynamicRouting ENABLED
> bind vlan 985 -ipAddress 10.100.26.10 255.255.255.0
```

5. Configurez le protocole de routage BGP sur les ZEBOs à l'aide du shell VTYSH.

```
> vtysh conf t router bgp 65535 neighbor 10.100.26.1 remote-as
    65535
```

6. Configurez BGP sur le commutateur externe. Les exemples de configuration suivants sont fournis pour le commutateur Cisco® Nexus 7000 C7010 version 5.2(1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

```
> router bgp 65535 no synchronization
  bgp log-neighbor-changes neighbor 10.100.26.14 remote-as 65535
     neighbor 10.100.26.15 remote-as 65535 no auto-summary
  dont-capability-negotiate
```



```
4   dont-capability-negotiate
5   no dynamic-capability
```

Configuration du cluster ECMP à l'aide du commutateur Cisco Nexus 7000 avec protocole de routage

August 20, 2021

Avec ECMP sur une configuration de cluster, une appliance Citrix ADC est capable de gérer le trafic via un protocole de routage. Le mécanisme ECMP aide à faire la publicité des adresses IP du serveur virtuel via tous les nœuds de cluster actifs.

Pour utiliser ECMP, vous devez d'abord activer le protocole BGP sur l'adresse IP du cluster. Liez les interfaces et l'adresse IP spotted (avec le routage dynamique activé) à un VLAN. Configurez le protocole de routage sélectionné et redistribuez les routes du noyau sur les ZEBO à l'aide du shell VTYSH.

Cas d'utilisation : Cluster ECMP à l'aide du commutateur Cisco Nexus 7000 avec protocole de routage

Prenons un exemple de déploiement de cluster avec un commutateur Cisco Nexus 7000 :

- Deux appliances Citrix ADC (nœud 1 et nœud 2), connectées au commutateur Nexus (en amont).
- Deux commutateurs Cisco Nexus 7000.
- Client et serveur (tracer le trafic HTTP via le commutateur Nexus). Avec HSRP (Hot Standby Router Protocol) activé côté client.



Conditions préalables

Tenez compte des points suivants avant de configurer les nœuds de cluster sur une appliance Citrix ADC.

1. Toutes les appliances doivent être du même type de plate-forme.
2. Le protocole BGP (BGP) doit être activé sur les nœuds du cluster.

Configuration à l'aide de l'interface de ligne de commande sur une appliance Citrix ADC

1. Ouvrir une session sur une appliance (par exemple, avec l'adresse NSIP 1.1.1.1)
2. Pour ajouter un nœud de cluster.

```
add cluster node 0 1.1.1.2 -state ACTIVE -backplane 0/10/8
```

3. Pour ajouter l'adresse IP du cluster

```
add ns ip 1.1.1.10 255.255.255.254 -type clip
```


4. Enregistrer la configuration

```
save ns config
```

5. Redémarrage à chaud de l'appliance

```
reboot -warm
```

6. Pour ajouter le nœud 1 à l'aide de CLIP

```
add cluster node 1 2.2.2.2 -state ACTIVE -backplane 1/10/8
```

7. Pour joindre un nœud au cluster

```
join cluster -clip 1.1.1.10 -password nsroot
```

8. Effectuez la configuration suivante sur CLIP

   - `enable ns feature bgp ospf DYNAMICROUTING`
   - `add ns ip 11.1.1.3 255.255.255.254 -dynamicRouting ENABLED -ownerNode 0`
   - `add ns ip 11.1.1.7 255.255.255.254 -dynamicRouting ENABLED -ownerNode 0`
   - `add ns ip 11.1.1.5 255.255.255.254 -dynamicRouting ENABLED -ownerNode 1`
   - `add ns ip 11.1.1.9 255.255.255.254 -dynamicRouting ENABLED -ownerNode 1`

Sur le routeur Cisco Nexus (11.1.1.2/31 et 11.1.1.4/31), vous devez effectuer les configurations suivantes à l'aide de la ligne de commande :

- `feature ospf`
- `feature bgp`
- `feature interface-vlan`
- `feature hsrp`

```
> interface vlan100
   no shutdown
   ip address 50.1.1.1/8
    hsrp 50
     ip 50.50.50.50

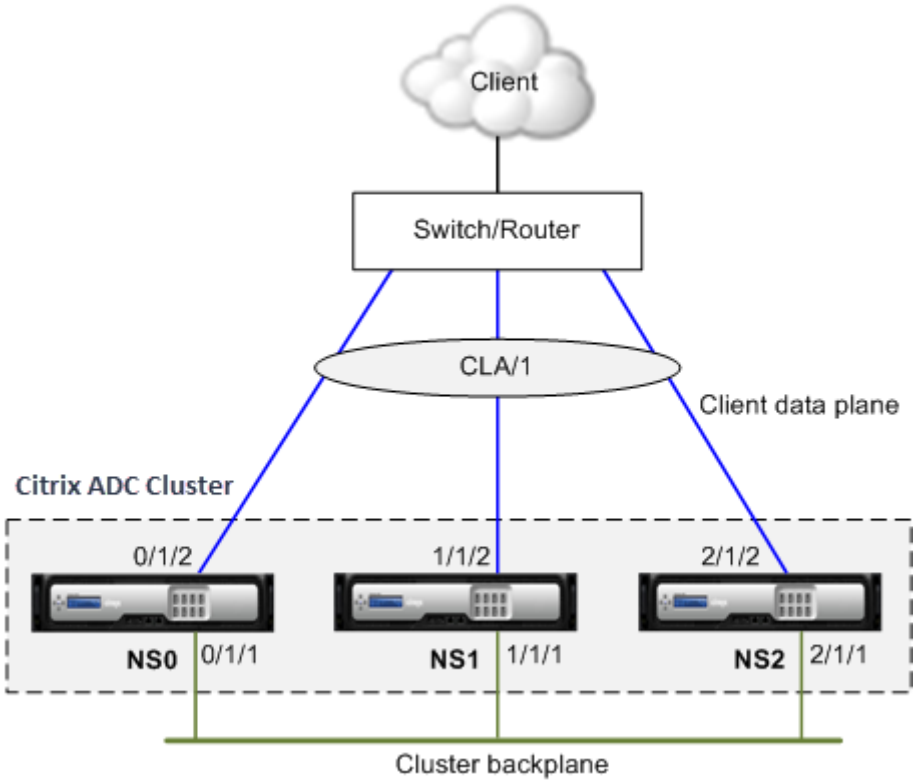
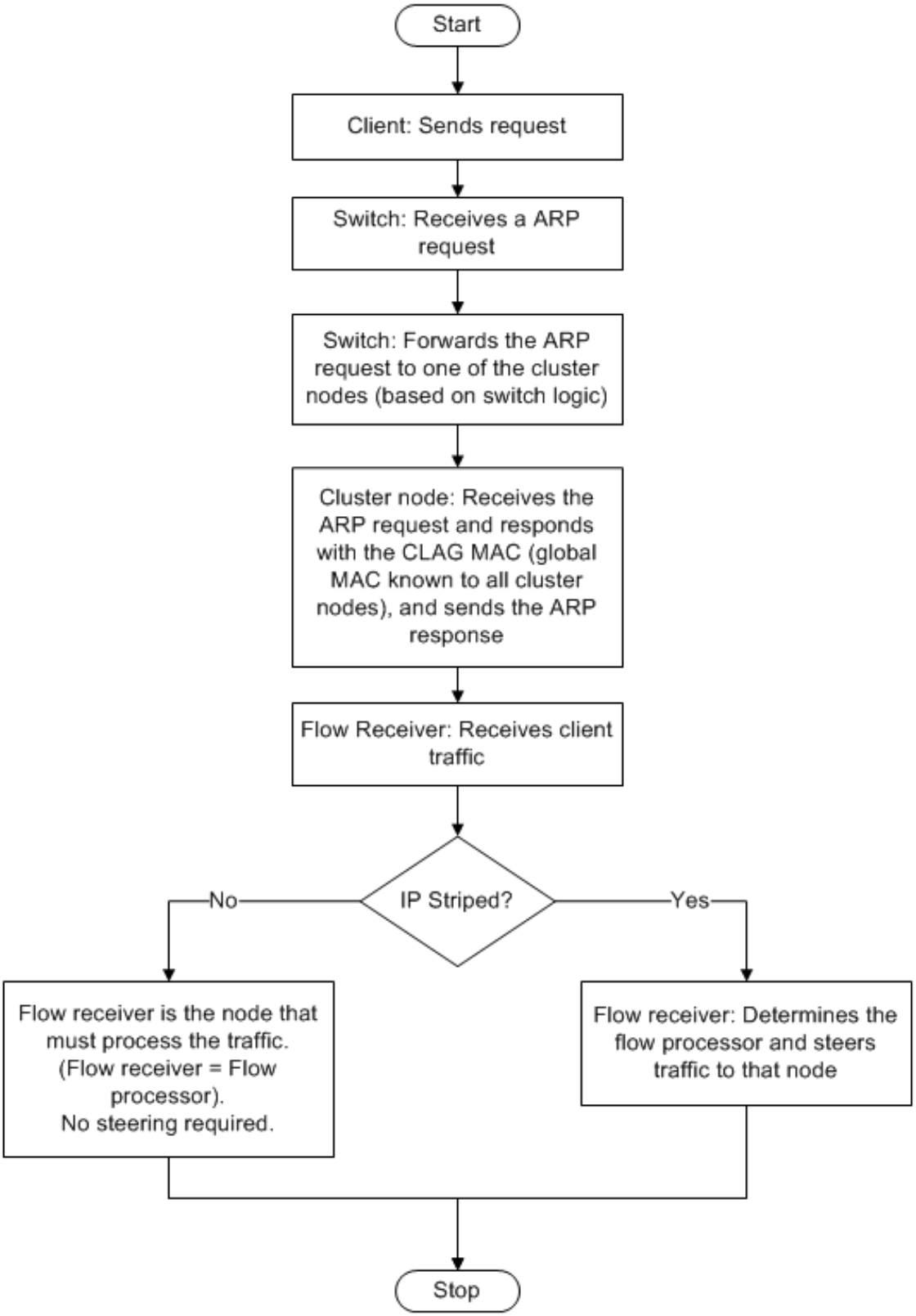
```



```
> interface Ethernet 4/15
  ip address 11.1.1.2/31
  no shutdown

> interface Ethernet 4/19
  ip address 11.1.1.4/31
  no shutdown

> interface Ethernet 4/22
  switchport
   switchport access vlan 100
```

Sur le routeur Cisco Nexus (11.1.1.6/31 et 11.1.1.8/31), vous devez effectuer les configurations suivantes à l'aide de la ligne de commande :

- `feature ospf`
- `feature bgp`
- `feature interface-vlan`
- `feature hsrp`

```
> interface vlan100
  no shutdown
  no ip redirects
  ip address 50.1.1.2/8
   hsrp 50
   ip 50.50.50.50

> interface Ethernet 4/13
  ip address 11.1.1.6/31
  no shutdown

> interface Ethernet 4/15
  ip address 11.1.1.8/31
  no shutdown

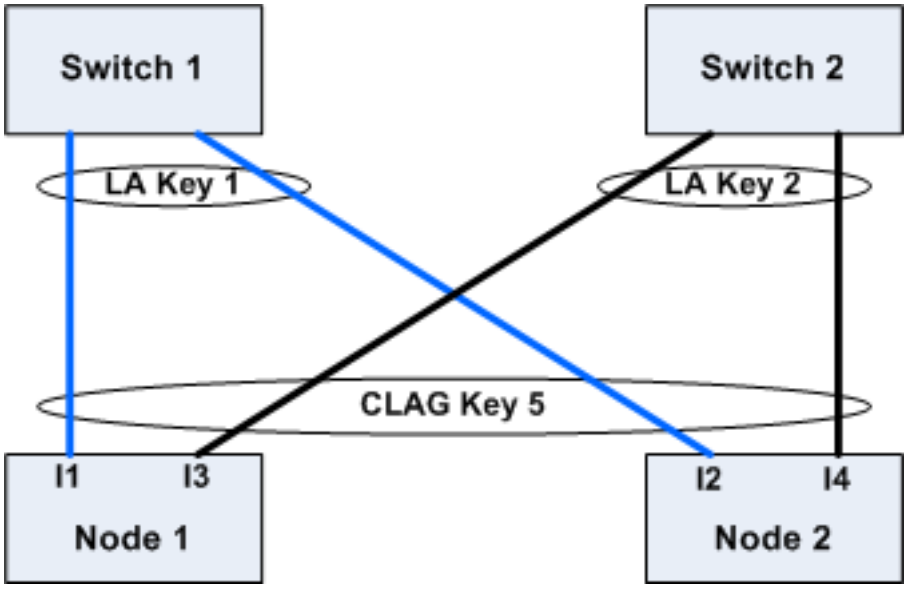
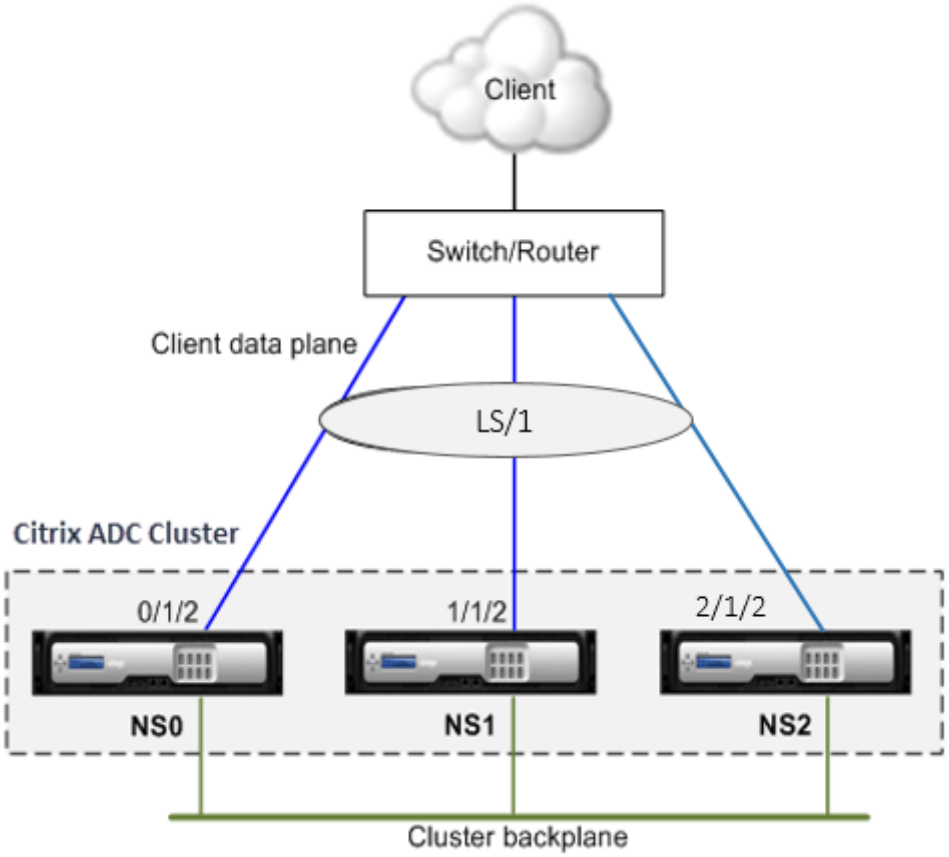
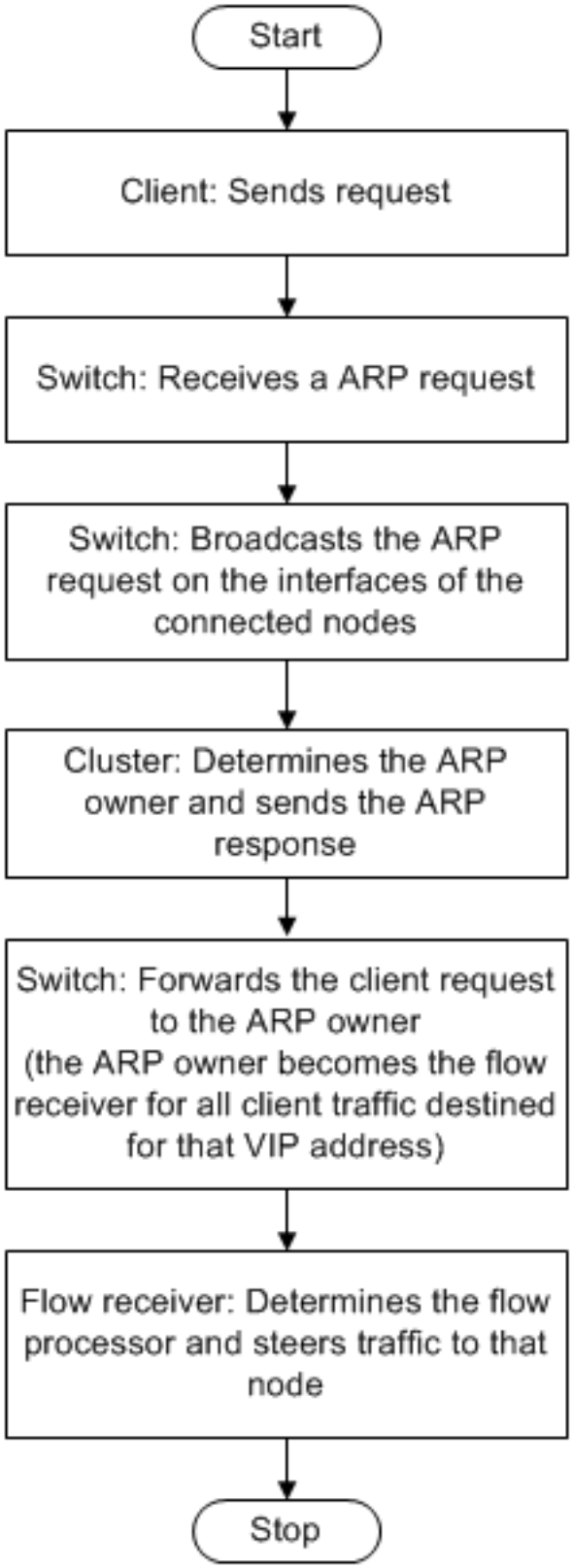
> interface Ethernet 4/22
  switchport
  switchport access vlan 100
```

Pour le protocole BGP, vous devez effectuer les configurations suivantes sur CLIP de l'appliance Citrix ADC :

```
> vtysh
ns# router bgp 1
```



```
 redistribute kernel
 owner-node 0
 neighbor 11.1.1.2 remote-as 2
 neighbor 11.1.1.2 as-origination-interval 1
 neighbor 11.1.1.2 advertisement-interval 0
 neighbor 11.1.1.6 remote-as 2
 neighbor 11.1.1.6 as-origination-interval 1
 neighbor 11.1.1.6 advertisement-interval 0
owner-node 1
 neighbor 11.1.1.4 remote-as 2
 neighbor 11.1.1.4 as-origination-interval 1
 neighbor 11.1.1.4 advertisement-interval 0
 neighbor 11.1.1.8 remote-as 2
 neighbor 11.1.1.8 as-origination-interval 1
 neighbor 11.1.1.8 advertisement-interval 0
exit-owner-node
```

Effectuez les configurations suivantes sur le routeur Cisco Nexus (11.1.1.3 et 11.1.1.5)

```
> ip access-list acl1
  10 permit ip 50.0.0.0/8 any
  route-map test permit
  match ip address acl1
 router bgp 2
  address-family ipv4 unicast
   redistribute direct route-map test
   maximum-paths 2
 neighbor 11.1.1.3 remote-as 1
  address-family ipv4 unicast
  neighbor 11.1.1.5 remote-as 1
 address-family ipv4 unicast
```

Effectuez les configurations suivantes sur le routeur Cisco Nexus (11.1.1.7 et 11.1.1.9)

```
> ip access-list acl1
   10 permit ip 50.0.0.0/8 any
  route-map test permit 1
   match ip address acl1
  router bgp 2
   address-family ipv4 unicast
   redistribute direct route-map test
   maximum-paths 2
  neighbor 11.1.1.7 remote-as 1
   address-family ipv4 unicast
  neighbor 11.1.1.9 remote-as 1
```



```
12    address-family ipv4 unicast
```

Pour le protocole OSPF, vous devez effectuer les configurations suivantes sur CLIP de l'appliance Citrix ADC :

```
1  > vtysh
2  ns# router osfp 1
3  redistribute kernel
4  owner-node 0
5   network 15.1.1.2/31 area 0
6   network 15.1.1.6/31 area 0
7  exit-owner-node
8
9  owner-node 1
10  network 15.1.1.4/31 area 0
11  network 15.1.1.8/31 area 0
12 exit-owner-node
13
14 route-map map2 permit 1
15 set metric 10
```

Sur le routeur Cisco Nexus (11.1.1.2/31 et 11.1.1.4/31), vous devez effectuer les configurations suivantes à l'aide de la ligne de commande :

```
1  > route-map- map2 permit 1
2     set metric 10
3
4     interface Ethernet4/15
5       ip address 15.1.1.2/31
6       ip router ospf 1 area 0.0.0.0
7       no shutdown
8
9     interface Ethernet4/19
10      ip address 15.1.1.4/31
11      ip router ospf 1 area 0.0.0.0
12      no shutdown
13
14    router ospf 1
15     router-id 1.1.1.1
16     redistribute direct route-map map2
```

Sur le routeur Cisco Nexus (11.1.1.7/31 et 11.1.1.9/31), vous devez effectuer les configurations suivantes à l'aide de la ligne de commande :

```
1  > route-map- map2 permit 1
```



```
2      set metric 10
3
4     interface Ethernet4/13
5       ip address 15.1.1.6/31
6       ip router ospf 1 area 0.0.0.0
7       no shutdown
8
9      interface Ethernet4/15
10      ip address 15.1.1.8/31
11      ip router ospf 1 area 0.0.0.0
12      no shutdown
13
14     router ospf 1
15       router-id 1.1.1.2
16       redistribute direct route-map map2
```

Utilisation de l'agrégation de liens de cluster

August 20, 2021

L'agrégation de liens de cluster est un groupe d'interfaces de nœuds de cluster. Il s'agit d'une extension de l'agrégation de liens Citrix ADC. La seule différence est que, alors que l'agrégation de liens nécessite que les interfaces proviennent du même périphérique, dans l'agrégation de liens de cluster, les interfaces proviennent de différents nœuds du cluster. Pour plus d'informations sur l'agrégation de liens, voir Configuration de l'agrégation de liens.

> **Important**
>
> - L'agrégation des liens de cluster est prise en charge pour un cluster d'appliances matérielles (MPX).
> - L'agrégation des liens de cluster est prise en charge pour un cluster d'appliances virtuelles (VPX) déployées sur des hyperviseurs ESX et KVM, avec les restrictions suivantes :
> - Des interfaces dédiées doivent être utilisées. Cela signifie que les interfaces ne doivent pas être partagées avec d'autres machines virtuelles.
> - Lorsqu'un nœud devient INACTIF, l'interface LA de cluster correspondante est marquée comme mise hors tension, de sorte que le trafic de données n'est pas envoyé à un nœud INACTIF.
> - Lorsqu'un nœud devient ACTIF, l'interface LA de cluster correspondante est marquée comme mise sous tension.

- Si les interfaces membres d'agrégation de liens de cluster sont désactivées manuellement ou si l'agrégation de liens de cluster elle-même est désactivée manuellement, la capacité de mise hors tension de l'interface n'est obtenue que par le mécanisme de délai d'expiration LACP.
- Le MTU Jumbo n'est pas pris en charge sur l'agrégation de liens de cluster LACP.

Remarque : l'agrégation des liens de cluster n'est pas prise en charge sur les appliances VPX déployées sur XenServer, AWS et Hyper-V.

- À partir de la version 12. 0, l'agrégation des liens de cluster est prise en charge sur les appliances Citrix ADC SDX.
- Le nombre d'interfaces pouvant être liées au cluster LA est de 16 (à partir de chaque nœud). Le nombre maximal d'interfaces dans le cluster LA peut être (16 * n), où n est le nombre de nœuds dans un cluster. Le nombre total d'interfaces dans la cluster LA dépend du nombre d'interfaces pour chaque canal de port sur le commutateur amont.
- Si une appliance Citrix ADC utilise des interfaces Intel Fortville, le passage d'un nœud de cluster en mode passif peut entraîner une panne de quelques secondes avec CLAG. Le problème se produit car LACP est activé pour CLAG pour fonctionner correctement, et le temps d'arrêt dépend des minuteries LACP de la carte réseau.

Par exemple, considérez un cluster à trois nœuds où les trois nœuds sont connectés au commutateur en amont. Un canal LA de cluster (CLA/1) est formé par des interfaces de liaison 0/1/2, 1/1/2 et 2/1/2.

Figure 1. Topologie d'agrégation de liens de cluster



Un canal LA de cluster possède les attributs suivants :

- Chaque canal a un MAC unique convenu par les nœuds de cluster.
- Le canal peut lier les interfaces des nœuds locaux et distants.
- Un maximum de quatre canaux LA de cluster sont pris en charge dans un cluster.
- Les interfaces de backplane ne peuvent pas faire partie d'un canal LA de cluster.
- Lorsqu'une interface est liée à un canal LA de cluster, les paramètres de canal ont priorité sur les paramètres d'interface réseau. Une interface réseau peut être liée à un seul canal.
- L'accès de gestion à un nœud de cluster ne doit pas être configuré sur un canal LA de cluster (par exemple, CLA/1) ou ses interfaces membres. Cela est dû au fait que lorsque le nœud est INACTIF, l'interface LA du cluster correspondante est marquée comme étant hors tension et perd donc l'accès à la gestion.

Figure 2. Flux de distribution du trafic à l'aide du cluster LA



Prise en charge de la sauvegarde et de la restauration du cluster LA sur Citrix ADC MPX

Vous pouvez sauvegarder et restaurer la configuration du cluster de LA sur Citrix ADC MPX. L'adresse MAC LA du cluster est indépendante de l'adresse MAC de l'interface physique des nœuds du cluster et peut changer après le processus de sauvegarde et de restauration. La CLUSTER LA peut servir le trafic une fois le processus de restauration de cluster terminé. Pour plus d'informations sur la sauvegarde et la restauration, reportez-vous à la section Sauvegarde et restauration de la configuration du cluster

Agrégation de liens de cluster statique

August 20, 2021

Vous devez configurer un canal LA de cluster statique sur l'adresse IP du cluster et sur le périphérique de connexion externe. Si possible, configurez le commutateur amont pour distribuer le trafic en fonction de l'adresse IP ou du port au lieu de l'adresse MAC.

Pour configurer un canal LA de cluster statique à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'adresse IP du cluster.

   > **Remarque**
   >
   > Assurez-vous de configurer le canal LA du cluster sur l'adresse IP du cluster avant de configurer l'agrégation des liens sur le commutateur externe. Sinon, le commutateur transfère le trafic au cluster même si le canal LA du cluster n'est pas configuré. Cela peut entraîner une perte de trafic.

2. Créez un canal LA de cluster.

   ```
   add channel <id> -speed <speed>
   ```

   Exemple

   ```
   add channel CLA/1 -speed 1000
   ```

   > **Remarque**
   >
   > Vous ne devez pas spécifier la vitesse comme AUTO. Vous devez plutôt spécifier explicitement la vitesse comme 10, 100, 1000 ou 10000. Seules les interfaces dont la vitesse correspond à l' <speed> attribut dans le canal LA du cluster sont ajoutées à la liste de distribution active.

3. Liez les interfaces requises au canal LA du cluster. Assurez-vous que les interfaces ne sont pas utilisées pour le backplane du cluster.

```
bind channel <id> <ifnum>
```

Exemple

```
bind channel CLA/1 0/1/2 1/1/2 2/1/2
```

4. Vérifiez les configurations.

```
show channel <id>
```

Exemple

```
show channel CLA/1
```

> **Remarque**
>
> Vous pouvez lier le canal LA du cluster à un VLAN à l'aide de la `bind vlan` commande. Les interfaces du canal sont automatiquement liées au VLAN.

5. Configurez LA statique sur le commutateur externe. Les exemples de configuration suivants sont fournis pour le Cisco® Nexus 7000 C7010 version 5.2 (1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

```
Global config:
Configure terminal

Interface level config:

interface Ethernet2/47
switchport
switchport access vlan 10
channel-group 7 mode on
no shutdown

interface Ethernet2/48
switchport
switchport access vlan 10
channel-group 7 mode on
no shutdown
```


Agrégation de liens de cluster dynamique

August 20, 2021

Le canal LA de cluster dynamique utilise le protocole LACP (Link Aggregation Control Protocol).

Vous devez effectuer des configurations similaires sur l'adresse IP du cluster et sur le périphérique de connexion externe. Si possible, configurez le commutateur amont pour distribuer le trafic en fonction de l'adresse IP ou du port au lieu de l'adresse MAC.

> **Points à retenir**
>
> - Activez LACP (en spécifiant le mode LACP comme ACTIVE ou PASSIVE).

```
>**Note**
>
> Make sure the LACP mode is not set as PASSIVE on both the Citrix ADC
    cluster and the external connecting device.
```

> - Spécifiez la même clé LACP sur chaque interface que vous souhaitez faire partie du canal. Pour créer un canal LA de cluster, la clé LACP peut avoir une valeur comprise entre 5 et 8. Par exemple, si vous définissez la clé LACP sur les interfaces 0/1/2, 1/1/2 et 2/1/2 à 5, CLA/1 est créé. Les interfaces 0/1/2, 1/1/2 et 2/1/2 sont automatiquement liées à CLA/1. De même, si vous définissez la clé LACP sur 6, le canal CLA/2 est créé.
> - Spécifiez le type de LAG en tant que Cluster.

Pour configurer un canal LA de cluster dynamique à l'aide de l'interface de ligne de commande

Sur l'adresse IP du cluster, pour chaque interface que vous souhaitez ajouter au canal LA du cluster, tapez :

```
set interface <id> -lacpMode <lacpMode> -lacpKey <positive_integer> -
lagType CLUSTER<!--NeedCopy-->
```

Exemple :

Pour configurer un cluster CLA/1 canal LA sur 3 interfaces.

```
> set interface 0/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 1/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 2/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
```


> **Remarque**
>
> Vous pouvez également activer la redondance des liens dans un cluster avec LACP.

De même, configurez LA dynamique sur le commutateur externe. Les exemples de configuration suivants sont fournis pour le Cisco® Nexus 7000 C7010 version 5.2 (1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

```
Global config:
Configure terminal
feature lacp
Interface level config:

interface Ethernet2/47
switchport
switchport access vlan 10
channel-group 7 mode active
no shutdown

interface Ethernet2/48
switchport
switchport access vlan 10
channel-group 7 mode active
no shutdown
```

Liaison de la redondance dans un cluster avec LACP

January 21, 2021

Un cluster Citrix ADC fournit la redondance des liens pour LACP afin de garantir que tous les nœuds possèdent la même clé de partenaire.

Pour comprendre la nécessité de la redondance de lien, considérons l'exemple de la configuration de cluster suivante avec les cas d'accompagnement (avec une attention au cas 3) :



Dans cette configuration, les interfaces I1, I2, I3 et I4 sont liées au canal LACP avec KEY 5. Côté partenaire, I1 et I2 sont connectés au commutateur 1 pour former un seul canal LA avec KEY 1. De même, I3 et I4 sont connectés au commutateur 2 pour former un seul canal LA avec KEY 2.

Considérons maintenant les cas suivants pour comprendre la nécessité de la redondance des liens :

- **Cas 1 : le commutateur 1 est en haut et le commutateur 2 est en panne**

  Dans ce cas, le cluster LA sur les deux nœuds cesserait de recevoir des LACPDU de la Key2 et commencerait à recevoir des LACPDU de la Key1. Sur les deux nœuds, la cluster LA est connecté à KEY 1 et I1 et I2 est UP et le canal sur les deux nœuds serait UP.

- **Cas 2 : Switch1 tombe en panne et Switch2 devient UP**

  Dans ce cas, le cluster LA sur les deux nœuds cesserait de recevoir des LACPDU de la Key1 et commencerait à recevoir des LACPDU de la Key2. Sur les deux nœuds, la cluster LA est connecté à Key2 et I3 et I4 est UP et le canal sur les deux nœuds serait UP.

- **Cas 3 : Switch1 et Switch2 sont UP**

  Dans ce cas, il est possible que la LA de cluster sur node1 choisisse Key1 comme partenaire et que LA de cluster sur node2 choisisse Key2 comme partenaire. Cela signifie que I1 sur node1 et I4 sur node2 reçoivent du trafic qui n'est pas souhaitable. Cela peut arriver parce que la machine d'état LACP est au niveau du noeud et choisit ses partenaires sur la base du premier arrivé, premier servi.

  Pour résoudre ces problèmes, la redondance des liens du cluster dynamique LA est prise en charge. Pour configurer la redondance de liaison sur un canal ou une interface, vous devez l'activer et éventuellement spécifier le débit de seuil comme suit :

  ```
  set channel CLA/1 -linkRedundancy ON -lrMinThroughput <positive_integer
  >
  ```


Le débit des canaux partenaires est vérifié par rapport au débit seuil configuré. Le canal partenaire qui satisfait le débit seuil est sélectionné de manière FIFO (premier entré, premier sorti). Si aucun des canaux partenaires n'atteint le seuil ou si le débit de seuil n'est pas configuré, le canal partenaire avec le nombre maximal de liaisons est sélectionné.

> **Remarque**
>
> Le débit de seuil peut être configuré à partir de NetScaler 11.

Utilisation du mode USIP dans le cluster

August 20, 2021

En mode USIP source (USIP), le cluster ou l'appliance Citrix ADC transfère chaque paquet vers le serveur principal approprié avec l'adresse IP du client.

Distribution du trafic en mode USIP

Le comportement du mode USIP diffère de la distribution du trafic entre le plan de données client et le plan de données du serveur dans le déploiement ECMP et CLAG. La section suivante fournit plus d'informations sur le comportement du mode USIP. Pour plus d'informations sur CLAG en mode USIP, voir Utilisation de l'agrégation de liens de cluster.

Mode USIP

Le cluster utilise l'adresse IP du client pour ouvrir la connexion côté serveur. Le port source peut ou non être préservé en fonction du `useproxyport` paramètre.

`useproxyport` Scénarios USIP

L'USIP `useproxyport` est activé pour le flux de trafic, le port source est sélectionné de manière à ce que le trafic inverse se hache vers le processeur de flux. Il assure une direction unique côté serveur.

L'USIP `useproxyport` est désactivé pour le flux de trafic, le port source est préservé et il y a donc une double direction côté serveur.

> **Important**
>
> - Lorsque USIP est allumé, l'adresse IP du client est utilisée dans la connexion au serveur principal, et la distribution du trafic pour la réponse est nécessaire entre les nœuds de cluster. Vous pouvez utiliser le déploiement ECMP ou CLAG pour la distribution du trafic côté serveur. En l'absence de distribution du trafic côté serveur, l'ensemble du trafic de retour

> peut atterrir sur un nœud de cluster unique, ce qui entraîne une congestion.
> - La `set rsskeytype -rsskey symmetric` commande est utilisée pour réduire la double direction à la direction unique du trafic dans les déploiements `useproxyport` hors tension. Où le 4 tuple de la connexion reste le même pour le serveur et le client. Par exemple, serveur virtuel en mode MAC générique.

Limitations

L'USIP ne fonctionne pas lorsque le processus local est désactivé.

Déploiement en mode USIP

La figure suivante illustre un déploiement en mode USIP dans une configuration de cluster.

Configurer les éléments suivants à l'aide de l'interface

1. Activez le protocole de routage.

```
enable ns feature <feature>
```

Exemple :

```
enable ns feature ospf
```

2. Ajoutez une adresse SNIP spotted pour chaque nœud et activez le routage dynamique sur celui-ci.

```
add ns ip <SNIP> <netmask> -dynamicRouting ( ENABLED | DISABLED )
    - ownerNode <positive_interger>  - ownerdownResponse ( YES | NO
   )
```

Exemple

```
-  add ns ip 192.0.2.1 255.255.255.0 -dynamicRouting ENABLED -
   ownerNode 0  - ownerDownResponse NO
-  add ns ip 192.0.2.2 255.255.255.0 -dynamicRouting ENABLED -
   ownerNode 1  - ownerDownResponse NO
-  add ns ip 192.0.2.3 255.255.255.0 -dynamicRouting ENABLED -
   ownerNode 2  - ownerDownResponse NO
```

3. Ajoutez un VLAN.

```
add vlan <id>
```


Exemple

```
add vlan 300
```

4. Liez les interfaces des nœuds de cluster au VLAN.

```
bind vlan <id> -ifnum <interface_name>
```

Exemple

```
bind vlan 300 -ifnum 0/1/2 1/1/2 2/1/2
```

5. Liez l'une des adresses SNIP spotted au VLAN. Lorsque vous liez une adresse SNIP spotted à un VLAN, toutes les autres adresses SNIP spotted définies sur le cluster dans ce sous-réseau sont automatiquement liées au VLAN.

```
bind vlan <id> -IPAddress <ip_addr | ipv6_addr> -netmask
```

Exemple

```
bind vlan 300  - IPAddress 192.0.2.1 255.255.255.0
```

6. Configurez le protocole de routage sur les ZEBOs à l'aide du shell VTYSH. Configurez le protocole de routage OSPF sur les ID de nœud 0, 1 et 2.

```
vtysh
configure terminal
ns block-sec-rtadv
router ospf
owner -node 0
router-id 192.0.2.1
exit-owner-node
owner-node 1
router-id 192.0.2.2
exit-owner-node
owner-node 2
router-id 192.0.2.3
exit-owner-node
network 192.0.2.0/24 area 0
default-information originate always
```

7. Effectuez les configurations suivantes sur le routeur Cisco 3750 à l'aide de l'interface de ligne de commande.

```
Configure terminal
```



```
feature ospf
interface vlan300
no shutdown
ip address 192.0.2.100/24
Configure terminal
router ospf 1
router-id 192.0.2.100
network 192.0.2.0 0.0.0.255 area 0
```

Remarques

- La distribution du trafic sur le client et le serveur n'est pas nécessairement identique. Par exemple, vous pouvez configurer ECMP côté client et CLAG côté serveur ou opposé.
- Prévoyez une capacité supplémentaire du fond de panier car il y a plus de surcharge de direction dans le déploiement USIP.
- La configuration associée à CLAG et à Monitor Static Route (MSR) doit rester la même côté serveur.
- La direction du trafic est plus présente dans les déploiements en mode USIP.

Gestion du cluster Citrix ADC

January 21, 2021

Après avoir créé un cluster et configuré le mécanisme de distribution du trafic requis, le cluster est capable de servir le trafic. Pendant la durée de vie du cluster, vous pouvez effectuer les tâches de cluster suivantes :

- Configuration des groupes de nœuds
- Désactivation des nœuds d'un cluster
- Découvrir les appliances Citrix ADC
- Affichage des statistiques
- Synchronisation des configurations de cluster et des fichiers de cluster
- Synchronisation de l'heure entre les nœuds
- Mise à niveau ou rétrogradation du logiciel des nœuds de cluster

Configuration des jeux de liens

January 21, 2021

Linkset est un groupe d'interfaces de nœuds de cluster qui appartiennent au même domaine de diffusion. Dans les ensembles de liens, chaque nœud possède les informations sur les interfaces des autres nœuds qui sont connectées au même domaine de diffusion.

> **Remarque**
>
> Les jeux de liens sont une configuration obligatoire dans les scénarios suivants :
>
> - Pour les déploiements nécessitant le transfert basé sur Mac (MBF).
> - Pour le mode « -m MAC » activé sur le serveur virtuel avec le mode MBF activé globalement.
> - Améliorer la gérabilité des stratégies ACL et L2 impliquant des interfaces. Vous définissez un jeu de liens des interfaces et ajoutez des stratégies ACL et L2 basées sur des ensembles de liens.

Dans une configuration de cluster, les fonctionnalités suivantes utilisent MBF en interne.

- Transmission de la session
- L2Conn
- Serveur virtuel en mode MAC
- Moniteur transparent
- LLB

Les jeux de liens doivent être configurés uniquement via l'adresse IP du cluster.

Prenons un exemple avec un cluster à trois nœuds. Dans la figure suivante, les interfaces 0/1/2, 1/1/2 et 2/1/2 sont dans le même domaine de diffusion et peuvent donc être configurées en tant que linkset (LS/1).

Figure 1. Topologie des jeux de liens



Figure 2. Flux de distribution du trafic à l'aide de jeux de liens



Pour configurer un jeu de liens à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'adresse IP du cluster.
2. Créez un jeu de liens.

   "'add linkset

   ```
   **Exemple**

   ```add linkset LS/1<!--NeedCopy-->
   ```

3. Liez les interfaces requises au jeu de liens. Assurez-vous que les interfaces ne sont pas utilisées pour le backplane du cluster.

   "'bind linkset -ifnum ...

   ```
   **Exemple**

   ```bind linkset LS/1 -ifnum 0/1/2 1/1/2 2/1/2<!--NeedCopy-->
   ```

4. Vérifiez les configurations du jeu de liens.

   "'show linkset

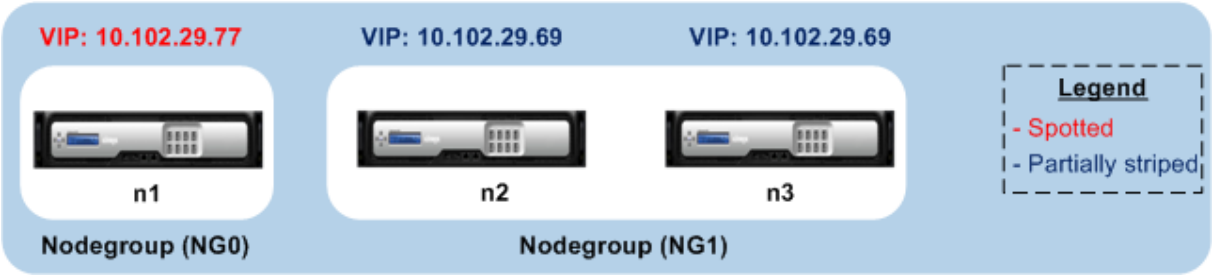
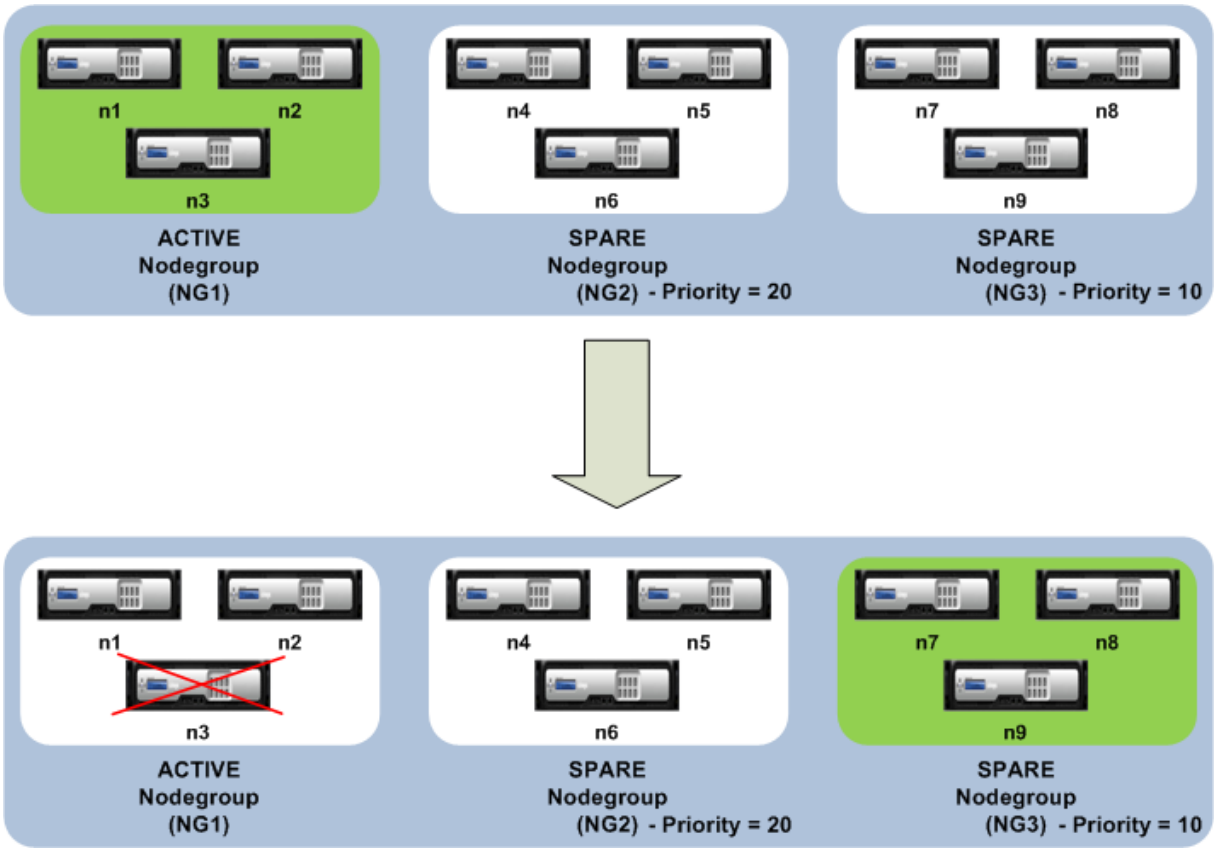
   ```
   **Exemple**

   ```show linkset LS/1<!--NeedCopy-->
   ```

> **Remarque**
>
> Vous pouvez lier le jeu de liens à un VLAN à l'aide de la `bind vlan` commande. Les interfaces du jeu de liens sont automatiquement liées au VLAN.

Pour configurer un jeu de liens à l'aide de l'interface graphique

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Réseau > Linksets**.
3. Dans le volet d'informations, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Créer un jeu de liens** :
   - Spécifiez le nom du jeu de liens en définissant le paramètre Linkset.
   - Spécifiez les interfaces à ajouter au jeu de liens et cliquez sur Ajouter . Répétez cette étape pour chaque interface que vous souhaitez ajouter au jeu de liens.
5. Cliquez sur **Créer**, puis sur **Fermer**.


   ```

# Groupes de nœuds pour les configurations ponctuelles et partiellement répartites

August 20, 2021

En vertu du comportement de cluster par défaut, toutes les configurations effectuées sur l'adresse IP du cluster sont disponibles sur tous les nœuds du cluster. Toutefois, il peut arriver que certaines configurations soient disponibles uniquement sur des nœuds de cluster spécifiques.

Vous pouvez atteindre cette exigence en définissant un groupe de nœuds qui inclut les nœuds de cluster spécifiques, puis en liant la configuration à ce groupe de nœuds. Il garantit que la configuration est active uniquement sur ces nœuds de cluster. Ces configurations sont appelées partiellement rayées ou ponctuées (si elles sont actives un seul nœud). Pour plus d'informations, voir Configurations rayées, partiellement rayées et ponctuées.

Par exemple, considérez un cluster avec trois nœuds. Vous créez un groupe de nœuds NG0 qui inclut le nœud n1 et un autre groupe de nœuds NG1 qui inclut n2 et n3. Liez les serveurs virtuels d'équilibrage de charge 0,77 à NG0 et l'équilibrage de charge du serveur virtuel 0.69 à NG1.

Cela signifie que le serveur virtuel 0.77 n'est actif que sur n1 et donc seul n1 reçoit le trafic qui est dirigé vers 0.77. De même, le serveur virtuel 0.69 n'est actif que sur les nœuds n2 et n3 et, par conséquent, seuls n2 et n3 reçoivent du trafic qui est dirigé vers 0.69.

Figure 1. Cluster Citrix ADC avec groupes de nœuds configurés pour les configurations ponctuées et partielles




Les entités ou configurations que vous pouvez lier à un groupe de nœuds sont les suivantes :

- Équilibrage de charge, changement de contenu, redirection du cache, authentification, autorisation et audit des serveurs virtuels

  > **Remarque**
  >
  > Les serveurs virtuels d'équilibrage de charge FTP ne peuvent pas être liés à des groupes de nœuds.

- Serveur virtuel VPN (pris en charge à partir de NetScaler 10.5 Build 50.10)

 

- Sites Global Server Load Balancing (GSLB) et autres entités GSLB (pris en charge à partir de NetScaler 10.5 Build 52.11)
- Identificateurs de limite et identificateurs de flux

## Comportement des groupes de nœuds

January 21, 2021

En raison de l'interopérabilité des groupes de nœuds avec différentes fonctionnalités et entités Citrix ADC, certains aspects comportementaux doivent être notés. Les nœuds d'un groupe de nœuds peuvent également être sauvegardés. Lisez la suite pour plus d'informations.

### Comportement général d'un groupe de nœuds de cluster

- Un groupe de nœuds qui a des entités liées ne peut pas être supprimé.
- Impossible de supprimer un nœud de cluster appartenant à un groupe de nœuds avec des entités qui lui sont liées.
- Impossible de supprimer une instance de cluster qui comporte des groupes de nœuds avec des entités qui lui sont liées.
- Vous ne pouvez pas ajouter une entité qui a une dépendance à une autre entité. Il ne doit pas faire partie du groupe de nœuds. Si vous devez le faire, supprimez d'abord la dépendance. Ajoutez ensuite les deux entités au groupe de nœuds et réassociez les entités.

  **Exemples :**

  - Supposons que vous disposez d'un serveur virtuel, VS1, dont la sauvegarde est le serveur virtuel VS2. Pour ajouter VS1 à un groupe de nœuds, assurez-vous d'abord que VS2 est supprimé en tant que serveur de sauvegarde de VS1. Ensuite, liez chaque serveur individuellement au groupe de nœuds, puis configurez VS2 comme sauvegarde pour VS1.
  - Supposons que vous disposez d'un serveur virtuel de commutation de contenu, CSVS1, dont le serveur virtuel d'équilibrage de charge cible est LBVS1. Pour ajouter CSVS1 à un groupe de nœuds, supprimez d'abord LBVS1 comme cible. Ensuite, liez chaque serveur individuellement au groupe de nœuds, puis configurez LBVS1 comme cible.
  - Supposons que vous disposez d'un serveur virtuel d'équilibrage de charge, LBVS1, qui a une stratégie qui appelle un autre serveur virtuel d'équilibrage de charge, LBVS2. Pour ajouter l'un des serveurs virtuels, supprimez d'abord l'association. Ensuite, liez chaque serveur individuellement au groupe de nœuds, puis réassociez les serveurs virtuels.

 

- Vous ne pouvez pas lier une entité à un groupe de nœuds. Il n'a pas de nœuds et l'option stricte est activée. Par conséquent, vous ne pouvez pas délier le dernier nœud d'un groupe de nœuds qui a des entités liées à celui-ci et dont l'option stricte est activée.
- L'option stricte ne peut pas être modifiée pour un groupe de nœuds qui n'a pas de nœuds mais qui a des entités liées.

### Sauvegarde de nœuds dans un groupe de nœuds

Par défaut, un groupe de nœuds est conçu pour fournir des nœuds de sauvegarde pour les membres d'un groupe de nœuds. Si un membre de groupe de nœuds tombe en panne, un nœud de cluster qui n'est pas membre du groupe de nœuds remplace dynamiquement le nœud défaillant. Ce nœud est appelé le nœud de remplacement.

> **Remarque**
>
> Pour un groupe de nœuds à un seul membre, un nœud de sauvegarde est automatiquement présélectionné lorsqu'une entité est liée au groupe de nœuds.

Lorsque le membre d'origine du groupe de nœuds apparaît, le nœud de remplacement, par défaut, est remplacé par le nœud membre d'origine.

Toutefois, à partir de NetScaler 10.5 Build 50.10, Citrix ADC vous permet de modifier ce comportement de remplacement. Lorsque vous activez l'option Sticky, le nœud de remplacement est conservé même après que le nœud membre d'origine apparaît. Le nœud d'origine ne prend le relais que lorsque le nœud de remplacement tombe en panne.

Vous pouvez également désactiver la fonctionnalité de sauvegarde. Pour ce faire, vous devez activer l'option stricte. Dans ce scénario, lorsqu'un membre de groupe de nœuds tombe en panne, aucun autre nœud de cluster n'est récupéré en tant que nœud de sauvegarde. Le nœud d'origine continue de faire partie du groupe de nœuds lorsqu'il apparaît. Cette option garantit que les entités liées à un groupe de nœuds sont actives uniquement sur les membres du groupe de nœuds.

> **Remarque**
>
> L'option stricte et collante ne peut être définie que lors de la création d'un groupe de nœuds.

## Configuration des groupes de nœuds pour les configurations ponctuelles et partiellement répartie

August 20, 2021

Pour configurer un groupe de nœuds pour des configurations ponctuelles et partiellement répartie, vous devez d'abord créer un groupe de nœuds, puis lier les nœuds requis au groupe de nœuds. Vous

 

associez ensuite les entités requises à ce groupe de nœuds. Les entités qui sont liées au groupe de nœuds sont les suivantes :

- **Repéré** - S'il est lié à un groupe de nœuds qui a un seul nœud.
- **Partiellement rayé** - S'il est lié à un groupe de nœuds qui comporte plusieurs nœuds.

**Quelques points à retenir :**

- GSLB est pris en charge sur un cluster uniquement lorsque les sites GSLB sont liés à des groupes de nœuds qui ont un seul nœud de cluster. Pour plus d'informations, voir Configuration de GSLB dans un cluster.
- Citrix Gateway est pris en charge sur un cluster uniquement lorsque les serveurs virtuels VPN sont liés à des groupes de nœuds qui ont un seul nœud de cluster. L'option collante doit être activée sur le groupe de nœuds.
- Pour les versions antérieures à NetScaler 11, le pare-feu d'application n'est pris en charge que sur des nœuds de cluster individuels (configuration ponctuée). Les profils de pare-feu d'application ne peuvent être associés qu'à des serveurs virtuels liés à des groupes de nœuds dotés d'un seul nœud de cluster. Cela signifie que l'application vous n'êtes pas autorisé à faire ce qui suit :
  - Liez les profils de pare-feu d'application à des serveurs virtuels striped ou striped partiels.
  - Liez la stratégie à un point de liaison global ou à des étiquettes de stratégie définies par l'utilisateur.
  - Délier, à partir d'un groupe de nœuds, un serveur virtuel qui possède des profils de pare-feu d'application.
- NetScaler 11 a introduit la prise en charge du pare-feu des applications pour les configurations par bandes et partiellement répartites. Pour plus d'informations, voir Prise en charge du pare-feu d'application pour les configurations de cluster.

Vérifiez les fonctionnalités Citrix ADC prises en charge dans un cluster pour voir les versions NetScaler à partir desquelles GSLB, Citrix Gateway et le pare-feu d'application sont pris en charge dans un cluster.

### Pour configurer un groupe de nœuds à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'adresse IP du cluster.
2. Créez un groupe de nœuds. Type :

   ```
   add cluster nodegroup <name> -strict (YES | NO)<!--NeedCopy-->
   ```

   Exemple

   ```
   1 add cluster nodegroup NG0 -strict YES
   ```


3. Liez les nœuds requis au groupe de nœuds. Tapez la commande suivante pour chaque membre du groupe de nœuds :

   ```
   bind cluster nodegroup <name> -node <nodeId><!--NeedCopy-->
   ```

   Exemple

   Pour lier des nœuds avec les ID 1, 5 et 6.

   ```
   1 > bind cluster nodegroup NG0 -node 1
   2 > bind cluster nodegroup NG0 -node 5
   3 > bind cluster nodegroup NG0 -node 6
   ```

4. Liez l'entité au groupe de nœuds. Tapez la commande suivante une fois pour chaque entité que vous souhaitez lier :

   ```
   bind cluster nodegroup <name> (-vServer <string> | -identifierName <
   string> | -gslbSite <string> -service <string>)<!--NeedCopy-->
   ```

   > **Remarque**
   >
   > Les paramètres GSLBSite et de service sont disponibles à partir de NetScaler 10.5.

   Exemple

   Pour lier des serveurs virtuels VS1 et VS2 et l'identificateur de limite de débit nommé identifier1.

   ```
   1 > bind cluster nodegroup NG0 -vServer VS1
   2 > bind cluster nodegroup NG0 -vServer VS2
   3 > bind cluster nodegroup NG0 -identifierName identifier1
   ```

5. Vérifiez les configurations en affichant les détails du groupe de nœuds. Type :

   ```
   show cluster nodegroup <name><!--NeedCopy-->
   ```

   Exemple

   ```
   1 > show cluster nodegroup NG0
   ```

Pour configurer un groupe de nœuds à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster > Groupes de nœuds.**
3. Dans le volet d'informations, cliquez sur **Ajouter.**
4. Dans la boîte de dialogue **Créer un groupe de nœuds**, configurez le groupe de nœuds :
   a) Sous **Noeuds de cluster**, cliquez sur le bouton **Ajouter**.
      - La liste Disponible affiche les nœuds que vous pouvez lier au groupe de nœuds et la liste Configuré affiche les nœuds qui sont liés au groupe de nœuds.

- Cliquez sur le **signe+** dans la liste Disponible pour lier le nœud. De même, cliquez sur le signe **-** dans la liste Configuré pour dissocier le nœud.

b) Sous **Serveurs virtuels**, sélectionnez l'onglet correspondant au type de serveur virtuel que vous souhaitez lier au groupe de nœuds. Cliquez sur le bouton **Add**.
   - La liste Disponible affiche les serveurs virtuels que vous pouvez lier au groupe de nœuds et la liste Configuré affiche les serveurs virtuels liés au groupe de nœuds.
   - Cliquez sur le **signe+** dans la liste Disponible pour lier le serveur virtuel. De même, cliquez sur le signe - dans la liste Configuré pour dissocier le serveur virtuel.

Configuration de la redondance pour les groupes de nœuds

January 21, 2021

> **Remarque**
>
> Prise en charge à partir de NetScaler 10.5 Build 52.1115.e.

Les groupes de nœuds peuvent être configurés de telle sorte que lorsqu'un groupe de nœuds tombe en panne, un autre groupe de nœuds peut prendre en charge et traiter le trafic. Par exemple, lorsqu'un groupe de nœuds NG1 tombe en panne, NG2 prend le relais.

> **Remarque**
>
> Cette fonctionnalité peut être utilisée pour configurer la redondance du centre de données où chaque groupe de nœuds est configuré en tant que centre de données.

Pour atteindre ce cas d'utilisation, les nœuds de cluster doivent être regroupés logiquement en groupes de nœuds, où certains groupes de nœuds doivent être configurés comme ACTIVE et d'autres comme SPARE. Le groupe de nœuds actif ayant la priorité la plus élevée (c'est-à-dire le numéro de priorité le plus bas) est rendu opérationnel actif et sert donc le trafic. Lorsqu'un nœud de ce groupe de nœuds actif sur le plan opérationnel baisse, le nombre de nœuds de ce groupe de nœuds est comparé au nombre de nœuds des autres groupes de nœuds actifs par ordre de priorité. Si un groupe de nœuds a un nombre de nœuds supérieur ou égal, ce groupe de nœuds est rendu opérationnel actif. Sinon, les groupes de nœuds de rechange sont vérifiés.

> **Remarque**
>
> - Un seul groupe de nœuds spécifiques à l'état peut être actif à un moment donné dans le temps.
> - Un nœud de cluster hérite de l'état du groupe de nœuds. Ainsi, si un nœud avec l'état « SPARE » est ajouté au groupe de nœuds avec l'état « ACTIF », le nœud se comporte automatiquement comme un nœud actif.

- Le paramètre de préemption défini pour l'instance de cluster détermine si le groupe de nœuds actif initial prend le contrôle lorsqu'il se reproduit.
- Un groupe de nœuds de rechange peut prendre en charge un groupe de nœuds et héberger le trafic actif lorsqu'un groupe de nœuds actif tombe en panne.

La figure suivante montre une configuration de groupe de nœuds pour laquelle la redondance des groupes de nœuds est définie. NG1 est initialement le groupe de nœuds actif. Lorsqu'il perd l'un des nœuds, le groupe de nœuds de rechange (NG3) avec la priorité la plus élevée commence à servir le trafic.

Figure 1. Cluster Citrix ADC avec redondance de groupe de nœuds configurée.



Configuration de la redondance pour les groupes de nœuds

1. Connectez-vous à l'adresse IP du cluster.
2. Créez le groupe de nœuds actif et liez les nœuds de cluster requis.

```
1 > add cluster nodegroup NG1 -state ACTIVE
2 > bind cluster nodegroup NG1 -node n1
3 > bind cluster nodegroup NG1 -node n2
4 > bind cluster nodegroup NG1 -node n3
```


3. Créez le groupe de nœuds de rechange et liez les nœuds requis.

```
1 > add cluster nodegroup NG2 -state SPARE -priority 20
2 > bind cluster nodegroup NG2 -node n4
3 > bind cluster nodegroup NG2 -node n5
4 > bind cluster nodegroup NG2 -node n6
```

4. Créez un autre groupe de nœuds de rechange et liez les nœuds requis.

```
1 > add cluster nodegroup NG3 -state SPARE -priority 10
2 > bind cluster nodegroup NG3 -node n7
3 > bind cluster nodegroup NG3 -node n8
4 > bind cluster nodegroup NG3 -node n9
```

Désactivation de l'orientation sur le backplane du cluster

January 21, 2021

> **Remarque**
>
> Prise en charge à partir de NetScaler 11.

Le comportement par défaut d'un cluster Citrix ADC consiste à diriger le trafic qu'il reçoit (récepteur de flux) vers un autre nœud (processeur de flux). Le processeur de flux doit alors traiter le trafic. Ce processus de direction du trafic du récepteur de flux vers le processeur de flux se produit sur le backplane du cluster et est appelé direction.

Si nécessaire, vous pouvez désactiver la direction afin que le processus devienne local pour le récepteur de débit et que le récepteur de débit devienne donc le processeur de débit. Une telle configuration de configuration peut s'avérer utile lorsque vous avez un lien de latence élevée.

> **Remarque**
>
> Cette configuration s'applique uniquement aux serveurs virtuels répartis par bandes.

- Pour les serveurs virtuels partiellement répartis par répartition, si le récepteur de flux est un nœud non propriétaire, le trafic est dirigé vers un nœud propriétaire. Si toutefois, le récepteur de flux est un nœud propriétaire, la direction est désactivée.
- Pour les serveurs virtuels repéré, le récepteur de flux est le processeur de flux, et il n'y a donc pas besoin de direction.

Quelques points à retenir lors de la désactivation du mécanisme de direction :

- Les SNIP striped ne sont pas pris en charge car la direction est désactivée.
- MPTCP et FTP ne fonctionnent pas.

- Le mode L2 doit être désactivé.
- Si USIP est activé, le trafic peut ne pas revenir au même nœud que la direction est désactivée.
- Le trafic dirigé vers l'adresse IP du cluster est dirigé vers le coordinateur de configuration.
- Lorsqu'un nœud rejoint ou quitte un cluster, il est possible que plus de connexions 1/N soient affectées. C'est parce qu'un changement dans les nœuds disponibles, peut entraîner le rehachage des routes. En conséquence, le trafic est acheminé vers un autre nœud et en raison de la non-disponibilité de la direction, le trafic n'est pas traité.

La direction peut être désactivée au niveau du serveur virtuel individuel ou au niveau global. La configuration globale a priorité sur le paramètre du serveur virtuel.

- Désactivation de la direction du backplane pour tous les serveurs virtuels répartis par bandes

  Configurez au niveau de l'instance de cluster. Le trafic destiné à n'importe quel serveur virtuel par répartition n'est pas dirigé sur le fond de panier du cluster.

  ```
  add cluster instance \<clId\> -processLocal ENABLED<!--NeedCopy-->
  ```

- Désactivation de la direction du backplane pour un serveur virtuel par bandes spécifique

  Configurez sur un serveur virtuel par bandes. Le trafic destiné au serveur virtuel n'est pas dirigé sur le fond de panier du cluster.

  ```
  add lb vserver <name> <serviceType> -processLocal ENABLED<!--NeedCopy
  -->
  ```

Synchronisation des configurations de cluster

January 21, 2021

Les configurations Citrix ADC disponibles sur le coordinateur de configuration sont synchronisées avec les autres nœuds du cluster lorsque :

- Un nœud rejoint le cluster
- Un nœud rejoint le cluster
- Une nouvelle commande est exécutée via l'adresse IP du cluster

En outre, vous pouvez synchroniser avec force les configurations disponibles sur le coordinateur de configuration (synchronisation complète) avec un nœud de cluster spécifique. Assurez-vous de synchroniser un nœud de cluster à la fois, sinon le cluster peut être affecté.

Pour synchroniser les configurations de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes de l'appliance sur laquelle vous souhaitez synchroniser les configurations, tapez :

```
force cluster sync
```

Pour synchroniser les configurations de cluster à l'aide de l'interface graphique

1. Ouvrez une session sur l'appliance sur laquelle vous souhaitez synchroniser les configurations.
2. Accédez à **Système > Cluster.**
3. Dans le volet d'informations, sous **Utilitaires**, cliquez sur Forcer la synchronisation du cluster.
4. Cliquez sur **OK.**

Synchronisation du temps entre les nœuds de cluster

January 21, 2021

Le cluster utilise un protocole PTP (Precision Time Protocol) pour synchroniser l'heure entre les nœuds de cluster. PTP utilise des paquets de multidiffusion pour synchroniser l'heure. S'il y a des problèmes dans la synchronisation de l'heure, vous devez désactiver PTP et configurer NTP (Network Time Protocol) sur le cluster.

Pour activer/désactiver PTP à l'aide de l'interface de ligne de commande

À l'invite de commandes de l'adresse IP du cluster, tapez :

```
set ptp -state disable
```

Pour activer/désactiver PTP à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster.**
3. Dans le volet d'informations, sous **Utilitaires**, cliquez sur **Configurer les paramètres PTP.**
4. Dans la boîte de dialogue **Activer/Désactiver PTP**, indiquez si vous souhaitez activer ou désactiver PTP.
5. Cliquez sur **OK.**

Synchronisation des fichiers de cluster

October 5, 2021

Les fichiers disponibles sur le coordinateur de configuration sont appelés fichiers de cluster. Ces fichiers sont automatiquement synchronisés sur les autres nœuds de cluster lorsque le nœud est ajouté au cluster et périodiquement, pendant la durée de vie du cluster. Vous pouvez également synchroniser manuellement les fichiers de cluster.

Important : La suppression de tout certificat ou fichier clé dans un environnement de cluster limite la configuration de l'appliance ADC. Rajoutez les fichiers au même emplacement pour apporter des modifications de configuration.

Les répertoires et fichiers du coordinateur de configuration qui sont synchronisés sont les suivants :

- /nsconfig/ssl/
- /var/netscaler/ssl/
- /var/vpn/signet/
- /nsconfig/dns/
- /nsconfig/monitors/
- /nsconfig/nstemplates/
- /nsconfig/ssh/
- /nsconfig/rc.netscaler
- /nsconfig/resolv.conf
- /nsconfig/inetd.conf
- /nsconfig/syslog.conf
- /nsconfig/snmpd.conf
- /nsconfig/ntp.conf
- /nsconfig/httpd.conf
- /nsconfig/sshd_config
- /nsconfig/hosts
- /nsconfig/enckey
- /var/nslw.bin/etc/krb5.conf
- /var/nslw.bin/etc/krb5.keytab
- /var/lib/likewise/db/
- /var/download/
- /var/wi/tomcat/webapps/
- /var/wi/Tomcat/conf/Catalina/LocalHost/
- /var/wi/java_home/lib/security/cacerts
- /var/wi/java_home/jre/lib/security/cacerts
- /nsconfig/license/

- /nsconfig/rc.conf

> **Conseil**
>
> Les fichiers (certificats et fichiers clés) copiés manuellement sur le coordinateur de configuration du cluster (ou via le shell) ne sont pas automatiquement disponibles sur les autres nœuds de cluster. Exécutez la commande « synchroniser les fichiers de cluster » à partir de l'adresse IP du cluster avant d'exécuter une commande qui dépend de ces fichiers.

Pour synchroniser les fichiers de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes de l'adresse IP du cluster, tapez :

```
1 sync cluster files <mode>
```

Pour synchroniser des fichiers de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster.**
3. Dans le volet d'informations, sous **Utilitaires**, cliquez sur Synchroniser les fichiers de cluster.
4. Dans la boîte de dialogue **Synchroniser** les fichiers de cluster, sélectionnez les fichiers à synchroniser dans la liste déroulante Mode.
5. Cliquez sur **OK.**

Affichage des statistiques d'un cluster

January 21, 2021

Vous pouvez afficher les statistiques d'une instance de cluster et des nœuds de cluster pour évaluer les performances ou résoudre les problèmes de fonctionnement du cluster.

Pour afficher les statistiques d'une instance de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes de l'adresse IP du cluster, tapez :

```
1 stat cluster instance <clId>
```


Pour afficher les statistiques d'un nœud de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes de l'adresse IP du cluster, tapez :

```
stat cluster node <nodeid>
```

> **Remarque**
>
> La `stat cluster node <nodeid>` commande affiche les statistiques de niveau cluster lorsque vous exécutez la commande à partir de l'adresse IP du cluster. Toutefois, lorsque vous exécutez à partir de l'adresse NSIP d'un nœud de cluster, la commande affiche des statistiques au niveau du nœud.

Pour afficher les statistiques d'une instance de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster.**
3. Dans le volet d'informations, au centre de la page, cliquez sur **Statistiques.**

Pour afficher les statistiques d'un nœud de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster > Nœuds.**
3. Dans le volet d'informations, sélectionnez un nœud et cliquez sur **Statistiques** pour afficher les statistiques du nœud. Pour afficher les statistiques de tous les nœuds, cliquez sur **Statistiques** sans sélectionner un nœud spécifique.

Découvrir les appliances Citrix ADC

January 21, 2021

Vous pouvez découvrir les appliances présentes dans le même sous-réseau que le nœud actuel. Les appliances découvertes requises peuvent ensuite être ajoutées sélectivement au cluster. Cette opération peut être effectuée pour créer un cluster ou ajouter des nœuds à un cluster existant.

> **Remarque**
>
> - L'opération de découverte ne peut être effectuée que par l'intermédiaire de l'utilitaire de

> configuration.
> - Cette opération ne peut pas détecter les appliances Citrix ADC à partir de différents réseaux.
> - Lors de l'exécution de cette opération pour ajouter des nœuds à un cluster existant, les configurations de VLAN L3 sont effacées du nœud. Veillez à définir ces configurations une fois que l'appliance est ajoutée au cluster.

Pour découvrir les appliances à l'aide de l'interface graphique

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster > Nœuds.**
3. Dans le volet d'informations, en bas de la page, cliquez sur **Découvrir NetScalers.**
4. Dans la boîte de dialogue **Discover NetScalers**, définissez les paramètres suivants :
   - **Plage d'adresses IP** : spécifiez la plage d'adresses IP dans laquelle vous souhaitez découvrir les appliances. Par exemple, vous pouvez rechercher toutes les adresses NSIP comprises entre 10.102.29.4 et 10.102.29.15 en spécifiant cette option comme 10.102.29.4 - 15.
   - **Interface de backplane** : spécifiez les interfaces à utiliser comme interface de backplane. Il s'agit d'un paramètre facultatif. Si vous ne spécifiez pas ce paramètre, vous devez le actualiser après l'ajout du nœud au cluster.
5. Cliquez sur **OK.**
6. Sélectionnez les appliances que vous souhaitez ajouter au cluster.
7. Cliquez sur **OK.**

Désactivation d'un nœud de cluster

August 20, 2021

Vous pouvez supprimer temporairement un nœud d'un cluster en désactivant l'instance de cluster sur ce nœud. Un nœud désactivé n'est pas synchronisé avec les configurations de cluster. Lorsque le nœud est à nouveau activé, les configurations de cluster sont automatiquement synchronisées dessus. Pour plus d'informations, voir Synchronisation entre les nœuds de cluster.

Un nœud désactivé ne peut pas servir le trafic et toutes les connexions existantes sur ce nœud sont terminées.

> **Remarque**
>
> Si les configurations d'un nœud coordinateur non configuré désactivé sont modifiées (via l'adresse NSIP du nœud), les configurations ne sont pas automatiquement synchronisées sur ce nœud. Vous pouvez synchroniser manuellement les configurations comme décrit dans Synchronisation des configurations de cluster.

Pour désactiver un nœud de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes du nœud que vous souhaitez désactiver, tapez :

```
disable cluster instance <clId>
```

> **Remarque**
>
> Pour désactiver le cluster, exécutez la commande disable cluster instance sur l'adresse IP du cluster.

Pour désactiver un nœud de cluster à l'aide de l'utilitaire de configuration

1. Sur le nœud que vous souhaitez désactiver, accédez à **Système > Cluster**, puis cliquez sur **Gérer le cluster.**
2. Dans la boîte de dialogue **Configurer** l'instance de cluster, **désactivez** la case à cocher Activer l'instance de cluster.

   > **Remarque**
   >
   > Pour désactiver l'instance de cluster sur tous les nœuds, exécutez la procédure précédente sur l'adresse IP du cluster.

Suppression d'un nœud de cluster

August 20, 2021

Lorsqu'un nœud est supprimé du cluster, les configurations de cluster sont effacées du nœud (en exécutant en interne la commande clear ns config -extended). Les adresses SNIP, les paramètres **MTU** de l'interface du fond de panier et toutes les configurations de VLAN (à l'exception du VLAN et du NSVLAN par défaut) sont également effacés de l'appliance.

> **Remarque**
>
> - Si le nœud supprimé était le coordinateur de configuration de cluster (CCO), un autre nœud est automatiquement sélectionné en tant que CCO et l'adresse IP du cluster est affectée à ce nœud. Toutes les sessions d'adresse IP de cluster actuelles ne sont pas valides et vous devez démarrer une nouvelle session.
> - Pour supprimer l'ensemble du cluster, vous devez supprimer chaque nœud individuellement. Lorsque vous supprimez le dernier nœud, les adresses IP du cluster sont supprimées.
> - Lorsqu'un nœud actif est supprimé, la capacité de service de trafic du cluster est réduite d'un nœud. Les connexions existantes sur ce nœud sont terminées.

Pour supprimer un nœud de cluster à l'aide de l'interface de ligne de commande

Pour NetScaler 10.1 et versions ultérieures

1. Connectez-vous à l'adresse IP du cluster et à l'invite de commandes, tapez :

```
rm cluster node <nodeId>

save ns config
```

2. Ouvrez une session sur le nœud supprimé, l'adresse NSIP et, à l'invite de commandes, tapez :

```
save ns config
```

> **Remarque**
>
> Si l'adresse IP du cluster est inaccessible depuis le nœud, exécutez la commande d'instance de cluster rm sur l'adresse NSIP de ce nœud lui-même.

Pour NetScaler 10

1. Ouvrez une session sur le nœud que vous souhaitez supprimer du cluster et supprimez la référence à l'instance de cluster.

```
rm cluster instance <clId>

save ns config
```

2. Ouvrez une session sur l'adresse IP du cluster et supprimez le nœud à partir duquel vous avez supprimé l'instance de cluster.

```
rm cluster node <nodeId>

save ns config
```

   Assurez-vous de ne pas exécuter la `rm cluster node` commande à partir du nœud local. Il en résulte des configurations incohérentes entre le CCO et le nœud.

Pour supprimer un nœud de cluster à l'aide de l'interface graphique

Sur l'adresse IP du cluster, accédez à **Système > Cluster > Nœuds**, sélectionnez le nœud à supprimer et cliquez sur **Supprimer.**

Suppression du nœud d'un cluster déployé à l'aide de l'agrégation de liens de cluster

August 20, 2021

Pour supprimer un nœud d'un cluster qui utilise l'agrégation de liens de cluster comme mécanisme de distribution du trafic, vous devez vous assurer que le nœud est rendu passif afin qu'il ne reçoive aucun trafic, puis, sur le commutateur en amont, supprimez l'interface correspondante du canal.

Pour plus d'informations sur l'agrégation de liens de cluster, voir Utilisation de l'agrégation de liens de cluster.

Pour supprimer un nœud d'un cluster qui utilise l'agrégation des liens de cluster comme mécanisme de distribution du trafic

1. Connectez-vous à l'adresse IP du cluster.
2. Définissez l'état du nœud de cluster que vous souhaitez supprimer sur PASSIVE.

```
set cluster node <nodeId> -state PASSIVE
```

3. Sur le commutateur en amont, supprimez l'interface correspondante du canal à l'aide de commandes spécifiques au commutateur.

> **Remarque**
>
> Vous n'avez pas besoin de supprimer manuellement l'interface des nœuds sur le canal d'agrégation des liens de cluster. Il est automatiquement supprimé lorsque le nœud est supprimé à l'étape suivante.

4. Supprimez le nœud du cluster.

```
rm cluster node <nodeId>
```

Détection d'une sonde jumbo sur un cluster

August 20, 2021

Si une trame Jumbo est activée sur une interface de cluster, l'interface du fond de panier doit être suffisamment grande pour prendre en charge tous les paquets dans le cadre Jumbo. Il est atteint en réglant l'unité de transmission maximale (MTU) du fond de panier comme suit :

Backplane_MTU = maximum (tous les MTU de l'interface de cluster) + 78

Pour vérifier la configuration précédente, vous devez envoyer une sonde jumbo (de la taille de calcul précédente) à tous les nœuds homologues d'une configuration de cluster. Si la sonde échoue, l'appliance affiche un message d'avertissement dans la sortie de la commande « show cluster instance ».

En mode interface de commande, tapez la commande suivante :

```
> show cluster instance
  Cluster ID: 1
  Dead Interval: 3 secs
  Hello Interval: 200 msecs
  Preemption: DISABLED
  Propagation: ENABLED
  Quorum Type: MAJORITY
  INC State: DISABLED
  Process Local: DISABLED
  Cluster Status: ENABLED(admin),    ENABLED(operational), UP
```

> **Avertissement**
>
> Le MTU d'une interface de backplane doit être suffisamment grand pour gérer tous les paquets du cadre. Il doit être égal à <MTU_VAL>. Si la valeur recommandée n'est pas configurable par l'utilisateur, vous devez vérifier la valeur MTU des interfaces jumbo.

Sl. non	Nœuds membres	Intégrité	État d'administration	État de l'opération
1	ID du nœud : 1 ; IP du nœud : 10.102.53.167	UP	Active	ACTIVE (Coordonnateur de configuration)
2	ID du nœud : 2 ; IP du nœud : 10.102.53.168	UP	Active	Actif

Surveillance des itinéraires pour les itinéraires dynamiques dans le cluster

January 21, 2021

Vous pouvez utiliser un moniteur d'itinéraires pour rendre un nœud de cluster dépendant de la ta-

ble de routage interne, qu'il contienne ou non un itinéraire appris dynamiquement. Un moniteur de routage sur chaque nœud vérifie la table de routage interne pour s'assurer qu'une entrée d'itinéraire permettant d'atteindre un réseau particulier est toujours présente. Si l'entrée d'itinéraire n'est pas présente, l'état du moniteur d'itinéraire passe à DOWN.

Dans un déploiement de cluster, si la liaison latérale côté client ou serveur d'un nœud diminue, le trafic est dirigé vers ce nœud via les nœuds homologues pour traitement. La direction du trafic est implémentée en configurant le routage dynamique et en ajoutant des entrées ARP statiques, pointant vers l'adresse MAC spéciale de chaque nœud, sur tous les nœuds. S'il y a beaucoup de nœuds dans un déploiement de cluster, ajouter et gérer des entrées ARP statiques avec des adresses MAC spéciales sur tous les nœuds est une tâche lourde. Maintenant, les nœuds utilisent implicitement des adresses MAC spéciales pour diriger les paquets. Par conséquent, les entrées ARP statiques pointant vers des adresses MAC spéciales ne doivent plus être ajoutées aux nœuds de cluster.

Pour lier un nœud de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*> [<
    netmask>])
unbind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*> [<
    netmask>])
```

Considérons un scénario où le nœud 1 est lié au moniteur de routage 1.1.1.0 255.255.255.0. Lorsqu'un itinéraire dynamique échoue, le nœud 1 devient INACTIVE. L'état de santé est disponible dans la `show cluster node` commande par ID de nœud comme suit.

```
Node ID: 1
IP:  10.102.169.96
Backplane:  1/1/2
Health: NOT UP
Reason(s): Route Monitor(s) of the node have failed
Route Monitor -  Network: 1.1.1.0   Netmask: 255.255.255.0   State:
    DOWN
```

Surveillance de la configuration du cluster à l'aide de MIB SNMP avec liaison SNMP

August 20, 2021

SNMP MIB est des informations spécifiques au périphérique configurées sur l'agent SNMP pour identifier une appliance Citrix ADC. Il peut identifier des informations telles que le nom de l'appliance, l'administrateur et l'emplacement. Dans une configuration de cluster, vous pouvez maintenant configurer le MIB SNMP dans n'importe quel nœud en incluant le paramètre « OwnerNode » dans la commande set SNMP MIB. Sans ce paramètre, la commande set SNMP MIB s'applique uniquement au nœud CCO (Cluster Coordinator).

Pour afficher la configuration MIB d'un nœud de cluster autre que CCO, incluez le paramètre « OwnerNode » dans la commande show SNMP MIB.

Configuration de la MIB SNMP sur CLIP

Pour configurer et afficher la configuration MIB sur CLIP à l'aide de l'interface de ligne de commande.

```
set snmp mib [-contact <string>] [-name <string>] [-location <string>]
      [-customID <string>] [-ownerNode <positive_integer>]
Done
show snmp mib [-ownerNode <positive_integer>]

 > set mib -contact John -name NS59 -location San Jose -customID 123 -
    ownerNode 3
Done
> sh mib -ownerNode 3
        --------------------
         Cluster Node ID: 3
        --------------------
        NetScaler system MIB:
        sysDescr:    NetScaler NS11.1: Build 46.4.a.nc, Date: Jun  7
           2016, 10:27:29
        sysUpTime:   124300
        sysObjectID: .1.3.6.1.4.1.5951.1.1
        sysContact:  John
        sysName:     NS59
        sysLocation: San Jose
        sysServices: 72
        Custom ID: 123
 Done

> unset mib -contact -name -location -customID -ownerNode 3
 Done
> sh mib -ownerNode 3
        --------------------
         Cluster Node ID: 3
        --------------------
```



```
29          NetScaler system MIB:
30          sysDescr:    NetScaler NS11.1: Build 46.4.a.nc, Date: Jun 7
               2016, 10:27:29
31          sysUpTime:   146023
32          sysObjectID: .1.3.6.1.4.1.5951.1.1
33          sysContact:  WebMaster (default)
34          sysName:     NetScaler
35          sysLocation: POP (default)
36          sysServices: 72
37          Custom ID: Default
38    Done
```

Messages d'interruption SNMP de cluster

Dans la configuration du cluster, les configurations d'alarme d'interruptions SNMP doivent être effectuées à partir du CLIP. Les commandes sont propagées à chacun des nœuds.

Pour plus d'informations sur la configuration de SNMP, consultez Configuration de Citrix ADC pour générer des interruptions SNMP.

Voici les interruptions spécifiques au cluster qui sont disponibles :

```
1    >sh snmp alarm | grep cluster
2        CLUSTER-BACKPLANE-HB-MISSING N/A N/A 86400   ENABLED - ENABLED
3        CLUSTER-CCO-CHANGE N/A N/A N/A ENABLED - ENABLED
4        CLUSTER-NODE-HEALTH N/A N/A 86400 ENABLED - ENABLED
5        CLUSTER-NODE-QUORUM N/A N/A 86400 ENABLED - ENABLED
6        CLUSTER-OVS-CHANGE N/A N/A N/A ENABLED - ENABLED
7        CLUSTER-PROP-FAILURE N/A N/A N/A ENABLED - ENABLED
8        CLUSTER-SYNC-FAILURE N/A N/A N/A ENABLED - ENABLED
9        CLUSTER-SYNC-PARTIAL-SUCCESS N/A N/A N/A ENABLED - ENABLED
10       CLUSTER-VERSION-MISMATCH N/A N/A 86400 ENABLED - ENABLED
```

Surveillance des échecs de propagation des commandes dans un déploiement de cluster

January 21, 2021

Dans un déploiement de cluster, vous pouvez utiliser la nouvelle commande « show prop status » pour accélérer la surveillance et le dépannage des problèmes. Problèmes liés à l'échec de propagation de commande sur les nœuds non-CCO. Cette commande affiche jusqu'à 20 des échecs de propagation

des commandes les plus récents sur tous les nœuds non-CCO. Vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique de l'appliance Citrix ADC pour effectuer cette opération. Vous pouvez y accéder via l'adresse CLIP ou via l'adresse NSIP de n'importe quel nœud du déploiement du cluster.

Arrêt gracieux des nœuds

August 20, 2021

Dans une configuration de cluster, certaines connexions existantes (1/Nième connexions, où N est la taille du cluster) au niveau du cluster ou au niveau du serveur virtuel spécifique sont perdues. Ce comportement est observé si un nœud quitte ou rejoint le système. Pour remédier à la perte, vous devez gérer avec élégance les connexions existantes. Une gestion gracieuse se fait en configurant l'option « conserver les connexions sur le cluster » dans l'adresse CLIP et en spécifiant un intervalle de délai dans le NSIP du nœud.

La gestion gracieuse des connexions est applicable dans deux scénarios :

1. Mise à niveau du cluster
2. Ajout d'un nouveau nœud

Gestion gracieuse des nœuds dans la mise à niveau du cluster

Pour mettre à niveau un cluster, vous devez mettre à niveau un nœud à la fois. Avant de mettre à niveau un nœud, vous devez le définir à l'état passif, puis le définir à l'état actif après la mise à niveau. Pour éviter de mettre fin à des connexions existantes lors de la mise à niveau du nœud, arrêtez-le avec un intervalle de temporisation configuré. Sinon, 1/Nth (où N est la taille du cluster) des connexions du cluster sont terminées.

> **Remarque**
>
> Si les sessions existantes ne sont pas terminées dans l'intervalle de temporisation configuré, elles se terminent après le délai de grâce.

Voici les étapes pour gérer avec élégance les nœuds dans un scénario de mise à niveau de cluster :

1. Envisagez une configuration de cluster de cinq nœuds (n0, n1, n2, n3, n4).
2. Avant d'arrêter un nœud, vous devez configurer l'option « RetainConnectionSonCluster ». Il permet de conserver toutes les connexions existantes de ce nœud au niveau du cluster ou du serveur virtuel pendant un intervalle de temps spécifique.

   Exemple

Sur CLIP

“‘set cluster instance –retainConnectionsOnCluster YES

```
OU

```set lb vserver <vserver name>  - retainConnectionsOnCluster Yes
   <!--NeedCopy-->
```

3. Maintenant, connectez-vous à l’adresse NSIP du noeud n3 et définissez le noeud n3 sur PASSIVE avec un délai d’attente interne.

   Exemple

   “‘set cluster node n3 –state PASSIVE –delay 60

```
```saveconfig<!--NeedCopy-->
```

4. Une fois le délai de grâce expiré, fermez toutes les connexions, arrêtez n3 et redémarrez l’appliance Citrix ADC.
5. Mettez à niveau l’appliance. Ensuite, lorsque l’interface de ligne de commande est connectée à l’adresse NSIP de l’appliance, définissez le nœud sur ACTIVE.

   Exemple

   “‘set cluster node n3 –state ACTIVE

```
```saveconfig<!--NeedCopy-->
```

6. Répétez les étapes 4 à 6 pour tous les nœuds du cluster.
7. Une fois que tous les nœuds ont été mis à niveau et définis sur ACTIVE, réinitialisez l’option RetainConnectionSonCluster à partir de l’adresse CLIP.

   Exemple

   “‘set cluster instance -retainConnectionsOnCluster NO

```
OU

```set lb vserver <vserver name>  - retainConnectionsOnCluster NO
   <!--NeedCopy-->
```

> **Remarque**

> En cas de non-correspondance de version lors de la mise à niveau d'un cluster, la propagation du cluster est automatiquement désactivée et aucune commande n'est autorisée sur le CLIP.

Gestion gracieuse des nœuds lors d'un ajout de nouveaux nœuds

La gestion gracieuse des nœuds décrit comment ajouter un nouveau nœud au cluster Citrix ADC existant. Considérez que vous disposez d'un cluster Citrix ADC qui dessert déjà le trafic. Et vous souhaitez ajouter une appliance supplémentaire en tant que nœud au cluster sans mettre fin à ses connexions existantes. Pour réaliser le scénario précédent, définissez l'option permettant de conserver les connexions existantes soit au niveau global, soit à un niveau de serveur virtuel spécifique. Une fois terminé, enregistrez la configuration. Définissez maintenant l'option pour conserver les connexions à NO, pour permettre la réaffectation des connexions existantes d'autres nœuds vers le nouveau nœud.

Voici les étapes pour gérer avec élégance les nœuds si un nœud vient d'être ajouté :

1. Vous enregistrez la configuration existante sur laquelle l'option « RetainConnectionsonCluster » est activée. Ce faisant, vous pouvez conserver toutes les connexions existantes de ce nœud au niveau du cluster ou du serveur virtuel pendant un intervalle de temps spécifique.

   Sur CLIP

   ```
   set cluster instance x - retainConnectionsOnCluster YES
   ```

   OU

   ```
   set lb vserver xxxx -retainConnectionsOnCluster Yes
   ```

2. Ajoutez un nœud 'n5' à la configuration du cluster.
3. Désactivez l'option « RetainConnectionCluster » sur « NO » pour distribuer les connexions existantes d'autres nœuds vers le nouveau nœud n5.

   Sur CLIP

   ```
   set cluster instance x - retainConnectionsOnCluster NO
   ```

   OU

   ```
   set lb vserver xxxx -retainConnectionsOnCluster NO
   ```

> **Remarque**
>
> La direction du fond de panier dépend du type de mécanisme de distribution du trafic (ECMP, CLAG et USIP) sur la configuration d'un cluster. L'augmentation de la direction du backplane est basée sur le type de trafic.

Configuration de l'arrêt progressif des nœuds dans un cluster

Pour configurer l'arrêt progressif des nœuds dans un cluster, procédez comme suit :

1. Configurez l'option « RetainConnectionsonCluster » au niveau global (cluster).
2. Configurez l'option « RetainConnectionsonCluster » au niveau du serveur virtuel.
3. Définissez le nœud (quittant le système) à l'état passif avec un délai d'attente gracieux spécifié dans l'adresse NSIP du nœud.
4. Surveillez les connexions existantes pour vous assurer que toutes les transactions sont terminées dans le délai de grâce.

Pour conserver les connexions existantes au niveau global (cluster) à l'aide de l'interface de ligne de commande

Vous pouvez conserver les connexions existantes au niveau global ou à un niveau de serveur virtuel spécifique. Cette option est configurée pour conserver toutes les connexions existantes au niveau global. Par défaut, cette option est désactivée.

À l'invite de commandes, tapez :

```
1 - set cluster instance <clusterID> - retainConnectionsOnCluster YES
2
3 - set cluster instance 60 - retainConnectionsOnCluster YES
```

Pour conserver les connexions existantes d'un serveur virtuel spécifique dans le cluster à l'aide de l'interface de ligne de commande

Cette option est configurée pour conserver les connexions existantes spécifiques à un serveur virtuel d'équilibrage de charge. Pour conserver ces connexions, nous activons cette option au niveau du serveur virtuel. Par défaut, cette option est désactivée.

À l'invite de commandes, tapez :

```
1 - set lb vserver <clusterID> - retainConnectionsOnCluster Yes
2
3 - set lb vserver v1 - retainConnectionsOnCluster Yes
```

Pour définir un nœud de cluster à l'état passif à l'aide de l'interface de ligne de commande

Pour définir un nœud de cluster à l'état passif avec un intervalle de délai d'attente gracieux. Ce paramètre est effectué dans le NSIP du nœud lorsque la propagation est désactivée lors de la mise à niveau du cluster.

À l'invite de commandes, tapez :


```
1  -  set cluster node <clusterID> -state passive
2 -backplane <interface_name>@
3 -priority <positive_integer>
4 -delay <mins>
5
6  -  set cluster node 4  - state PASSIVE -delay 60
7
8  -  set cluster instance 60  -  retainConnectionsOnCluster YES
9  -  set lb vserver v1  - retainConnectionsOnCluster Yes
10 -  set cluster node 4  - state PASSIVE -delay 60
```

> **Remarque**
>
> Vous pouvez observer le comportement suivant sur un nœud de cluster lorsqu'il est défini sur passif avec une option de délai configurée à partir d'un CLIP :
>
> - Après le délai d'expiration, le nœud apparaît comme passif à partir du NSIP du nœud.
> - La commande **show cluster instance** de CLIP affiche le nœud comme actif à partir du CLIP. Attendu que la commande **show cluster node** sur le CLIP affiche le nœud comme passif.

Pour configurer l'arrêt gracieux des nœuds à l'aide de l'interface graphique

1. Accédez à **Configuration > Système > Cluster** et cliquez sur **Gérer le cluster.**
2. Dans la page **Gérer le cluster**, sélectionnez l'option **Conserver les connexions sur le cluster** .
3. Cliquez sur **OK**, puis sur **Terminé**.

Arrêt gracieux des services

August 20, 2021

À partir de NetScaler 12.1 build 49.xx, les clusters Citrix ADC prennent en charge l'arrêt gracieux des services. Pour arrêter les services de manière gracieuse, vous pouvez effectuer l'une des tâches suivantes.

- Désactivez explicitement le service et
  - Définissez un délai (en secondes).
  - Activez l'arrêt progressif.
- Ajoutez un code ou une chaîne TROFS au moniteur.

Pour plus de détails, voir Arrêt gracieux des services.

Pour configurer l'arrêt progressif d'un service à l'aide de l'interface de ligne de commande

Désactiver avec l'option gracieuse uniquement :

À l'invite de commandes, tapez :

```
disable service <name> [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Exemple

```
disable service svc1 -graceFul YES
Done
sh service svc1
                svc1 (10.102.225.11:80) - HTTP
                State: GOING OUT OF SERVICE   Graceful (number of
                   active clients: 1)
                Last state change was at Wed Jul 25 10:46:29 2018
                Time since last state change: 0 days, 00:00:02.680
                ... ... ... .
                ... ... ... .
                Traffic Domain: 0

1)            Monitor Name: tcp-default
                                State: UP              Weight: 1
                                                Passive: 0
                                Probes: 26           Failed [Total: 0
                                   Current: 0]
                                Last response: Success - TCP syn+ack
                                   received.
                                Response Time: 0.0 millisec
<!--NeedCopy-->
```

Désactiver avec timeout et option gracieuse :

À l'invite de commandes, tapez :

```
disable service <name> [<delay>] [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Exemple


```
disable service svc1 2000 -graceFul YES

Done
> sh service svc1
                svc1 (10.102.225.11:80) - HTTP
                State: GOING OUT OF SERVICE (Graceful (number of active
                    clients: 1), Out Of Service in 1998 seconds)
                Last state change was at Wed Jul 25 10:49:08 2018
                Time since last state change: 0 days, 00:00:01.710
                ……..
                ……..
                Traffic Domain: 0

1)            Monitor Name: tcp-default
                                State: UP              Weight: 1
                                                Passive: 0
                                Probes: 57           Failed [Total: 0
                                    Current: 0]
                                Last response: Success - TCP syn+ack
                                    received.
                                Response Time: 0.0 millisec
Done
<!--NeedCopy-->
```

Désactiver le groupe de services avec timeout et option gracieuse :

À l'invite de commandes, tapez :

```
disable serviceGroup <serviceGroupName>@ [<serverName>@ <port>] [-delay
<secs>] [-graceFul ( YES | NO )]
Show service group <serviceGroupName>
<!--NeedCopy-->
```

Exemple :

```
disable servicegroup sg -delay 2000 -graceFul yes
sh servicegroup sg
                sg - HTTP
                State: DISABLED                Effective State: OUT OF
                    SERVICE Monitor Threshold : 0
                Max Conn: 0       Max Req: 0          Max Bandwidth: 0
                    kbits
                Use Source IP: NO
                Client Keepalive(CKA): NO
                ……..
```



```
9                    … … …
10
11
12                  1)   200.200.10.21:80       Server Name: server3
                       Server ID: None Weight: 1
13                                  State:    GOING OUT OF SERVICE (learnt
                                       from node:2 )     Graceful (number
                                       of active clients: 6), Out Of
                                       Service in 1993 seconds
14                                  Last state change was at Mon Aug 13
                                       15:15:11 2018
15                                   … … …
16
17                  2)   200.200.10.22:80       Server Name: server4
                       Server ID: None Weight: 1
18                                  State:    GOING OUT OF SERVICE (learnt
                                       from node:2 )     Graceful (number
                                       of active clients: 7), Out Of
                                       Service in 1993 seconds
19                                  Last state change was at Mon Aug 13
                                       15:15:11 2018
20  <!--NeedCopy-->
```

> **Remarque**
> CLIP affiche la valeur agrégée de toutes les connexions clients actives à partir de tous les nœuds de cluster.

Pour configurer l'arrêt progressif d'un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Ouvrez le service et, dans la liste Action, cliquez sur **Désactiver**. Entrez un temps d'attente, puis sélectionnez Graceful.

Pour configurer un code ou une chaîne TROFS dans un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
1  add lb monitor <monitor-name> HTTP -trofsCode <respcode>
2  add lb monitor <monitor-name> HTTP-ECV  -trofsString <resp string>
3  add lb monitor <monitor-name> TCP-ECV  -trofsString <resp string>
4  <!--NeedCopy-->
```


Pour configurer un code ou une chaîne TROFS dans un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Dans le volet Moniteurs, cliquez sur Ajouter, puis effectuez l'une des opérations suivantes :
    - Sélectionnez Type as HTTP, puis spécifiez un code TROFS.
    - Sélectionnez Type en tant que HTTP-ECV ou TCP-ECV, puis spécifiez une chaîne TROFS.

Prise en charge du logo IPv6 Ready pour les clusters

August 20, 2021

Vous pouvez tester les appliances en cluster pour la certification IPv6 Ready Logo. Les commandes modifiées pour tester les protocoles de base IPv6, comme pour les cas de test ND, le traitement de la sollicitation de routeur et l'envoi de messages de publicité d'itinéraire et de redirection de routeur, sont disponibles dans une configuration en cluster. Voici les fonctionnalités IPv6 disponibles pour tester les protocoles de base IPv6.

Voici les fonctionnalités modifiées disponibles pour passer les protocoles de base IPv6, tels que les cas de test ND, le traitement de la sollicitation de routeur et l'envoi de la publicité d'itinéraire et la messagerie de redirection de routeur dans la suite de tests IPv6ReadyLogo phase2.

- Lier des SNIP locaux
- Résolution des adresses et inaccessibilité des voisins
- Découverte du routeur et du préfixe
- Redirection du routeur
- DoDAD

Avec ces commandes modifiées, les configurations suivantes sont prises en charge dans une appliance en cluster.

Configurations supportables pour tester les protocoles de base IPv6

Pour qu'une configuration en cluster réussissent les cas de test du logo IPv6 Ready, vous pouvez exécuter les configurations suivantes sur l'adresse IP de gestion de cluster (CLIP).

- configuration IP6 globale
- configuration IPv6 de base
- plus de configurations IPv6

Configuration globale

Une configuration IPv6 globale vous permet de définir les paramètres IPv6 globaux (tels que relearning, routereDirection, ndBaseReachTime, nRetransmissionTime, natprefix, td et doodad) pour exécuter la configuration IPv6 de base.

À l'invite de commandes, tapez ce qui suit :

```
set ipv6 [-ralearning ( ENABLED | DISABLED )] [-routerRedirection (
    ENABLED | DISABLED )] [-ndBasereachTime<positive_integer>][-
    ndRetransmissionTime <positive_integer>] [-natprefix <ipv6_addr|*>[-
    td<positive_integer>]] [-doDAD ( ENABLED | DISABLED )]
```

Configuration IPv6 de base

La configuration IPv6 de base vous permet de créer une adresse IPv6 et de se lier à une interface VLAN. Vous pouvez effectuer les configurations suivantes pour tester les protocoles de base IPv6.

Pour ajouter un VLAN à la configuration en cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add vlan <id>
```

Pour ajouter un autre VLAN à la configuration en cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add vlan <id>
```

Pour lier une interface à un VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind vlan <id> -ifnum <interface_name>
```

Pour lier une interface à un VLAN à l'aide de l'interface de ligne de commande

Cette commande ajoute le préfixe global en tant que préfixe sur lien dans les informations RA pour les publicités de routeur suivantes. À l'invite de commandes, tapez :

```
bind vlan <id> -ifnum <interface_name>
```

Pour ajouter l'adresse SNIP IPv6 sur un VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
add ns ip6 <IPv6Address>@ [-scope ( global | link-local )][-type <type>
```


Pour ajouter l'adresse IPv6 sur VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
add ns ip6 <IPv6Address>@ [-scope ( global | link-local )][-type <type>
```

Pour lier une adresse IPv6 au VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> [-ifnum <interface_name> [-tagged]][-IPAddress <ip_addr|
    ipv6_addr|
```

Pour lier l'adresse IPv6 au VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> [-ifnum <interface_name> [-tagged]][-IPAddress <ip_addr|
    ipv6_addr|
```

Pour afficher l'adresse IPv6 locale de liaison attachée au VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
sh VLAN
```

Exemple 1

```
add vlan 2
add vlan 3
bind vlan 2 -ifnum 1/2
bind vlan 3 -ifnum 1/3
add ip6 fe80::9404:60ff:fedd:a464/64 -vlan 2 -scope link-local -type
    SNIP
add ip6 fe80::c0ee:7bff:fede:263f/64 -vlan 3 -scope link-local -type
    SNIP
add ip6 3ffe:501:ffff:100:9404:60ff:fedd:a464/64 -vlan 2
add ip6 3ffe:501:ffff:101:c0ee:7bff:fede:263f/64 -vlan 3
bind vlan 2 -ipAddress 3ffe:501:ffff:100:9404:60ff:fedd:a464/64
bind vlan 3 -ipAddress 3ffe:501:ffff:101:c0ee:7bff:fede:263f/64
```

Exemple 2


```
sh vlan
1)      VLAN ID: 2      VLAN Alias Name:
        Interfaces : 1/6
        IPs :
             3ffe:501:ffff:100:2e0:edff:fe15:ea2a/64
3)      VLAN ID: 3      VLAN Alias Name:
        Link-local IPv6 addr: fe80::9404:60ff:fedd:a464/64
        Interfaces : 1/5
        IPs :
             3ffe:501:ffff:101:2e0:edff:fe15:ea2b/64
 Done
```

Plus de configuration de cluster IPv6

Pour tester les protocoles de base IPv6, vous pouvez utiliser les configurations IPv6 nouvelles ou modifiées suivantes.

Pour définir les paramètres d'annonce de routeur spécifiques au VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set nd6RAvariables -vlan <positive_integer> [-ceaseRouterAdv ( YES | NO
    )] [-sendRouterAdv ( YES | NO )] [-srcLinkLayerAddrOption ( YES | NO
     )][-onlyUnicastRtAdvResponse ( YES | NO )] [-managedAddrConfig (
    YES | NO)] [-otherAddrConfig ( YES | NO )] [-currHopLimit <
    positive_integer>][-maxRtAdvInterval <positive_integer>] [-
    minRtAdvInterval<positive_integer>] [-linkMTU <positive_integer>] [-
    reachableTime<positive_integer>] [-retransTime <positive_integer>]
    [-defaultLifeTime<integer>]
```

Pour définir les paramètres configurables d'un préfixe global sur lien à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )][-
    autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )][-
    decrementPrefixLifeTimes ( YES | NO )] [-prefixValideLifeTime   <
    positive_integer>] [-prefixPreferredLifeTime <positive_integer>]
```

Pour ajouter des paramètres configurables à un préfixe global sur lien à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
add onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )][-
    autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )][-
    decrementPrefixLifeTimes ( YES | NO )]-prefixValideLifeTime <
    positive_integer>][-prefixPreferredLifeTime <positive_integer>]
```

Pour définir une liaison sur lien vers les paramètres configurables du préfixe IPv6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
help set onLinkIPv6Prefix
```

Pour lier un lien on-link aux paramètres configurables du préfixe IPv6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
help bind nd6RAvariables
```

Pour afficher ND6RAVariables à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
help sh nd6RAvariables
```

Exemple

```
> sh nd6RAvariables
  1) Vlan : 1
     SendAdvert     : NO   CeaseAdv       : NO        SourceLLAddress:
        YES
     UnicastOnly    : NO   ManagedFlag    : NO        OtherConfigFlag:
        NO
     CurHopLimit    : 64   MaxRtrAdvInterv: 600       MinRtrAdvInterv:
        198
     LinkMTU        : 0    ReachableTime  : 0          RetransTimer   :
         0
     DefaultLifetime: 1800 LastRAsentTime : 0          NextRAdelay    :
         0

  2) Vlan : 2
     SendAdvert     : NO   CeaseAdv       : NO         SourceLLAddress:
         YES
     UnicastOnly    : NO   ManagedFlag    : NO         OtherConfigFlag:
         NO
```



```
12       CurHopLimit     : 64    MaxRtrAdvInterv: 600         MinRtrAdvInterv:
             198
13       LinkMTU         : 0     ReachableTime  : 0           RetransTimer    :
             0
14       DefaultLifetime: 1800 LastRAsentTime : 0           NextRAdelay     :
             0
15  Done
16  >
17  > sh nd6Ravariables  -vlan 2
18    1) Vlan : 2
19       SendAdvert      : NO    CeaseAdv       : NO          SourceLLAddress:
             YES
20       UnicastOnly     : NO    ManagedFlag    : NO          OtherConfigFlag:
             NO
21       CurHopLimit     : 64    MaxRtrAdvInterv: 600         MinRtrAdvInterv:
             198
22       LinkMTU         : 0     ReachableTime  : 0           RetransTimer    :
             0
23       DefaultLifetime: 1800 LastRAsentTime : 0           NextRAdelay     :
             0
24       Prefix :
25  3ffe:501:ffff:100::/64
26  Done
```

Gestion des messages de pulsation de cluster

August 20, 2021

La gestion des messages de pulsation dans un cluster est similaire à leur gestion dans une configuration haute disponibilité (HA). Les nœuds peuvent envoyer et recevoir des messages de pulsation entre eux sur toutes les interfaces activées. Pour éviter une augmentation du trafic résultant des messages de pulsation, vous pouvez désormais désactiver l'option de pulsation sur les interfaces des nœuds. Toutefois, l'option pulsation sur l'interface de backplane ne peut pas être désactivée, car elle est nécessaire pour maintenir la connectivité entre les nœuds de cluster.

Pour plus d'informations sur la gestion des messages cardiaques, voir Gestion des messages Heartbeat haute disponibilité sur un dispositif NetScaler Appliance.

Pour gérer les messages de pulsation sur une interface de nœud à l'aide de l'interface de ligne de commande Citrix ADC

À l'invite de commandes, tapez :


```
set interface <ID> [-HAHeartBeat (ON | OFF)]
Show interface <ID>
```

Configuration de l'état de réponse du nœud propriétaire

August 20, 2021

Vous pouvez configurer l'option OwnerDownResponse sur un nœud qui a une adresse SNIP repéré. Par défaut, l'option est activée. Il permet à l'adresse IP repéré de répondre aux requêtes PING ou ARP (provenant du routeur amont) lorsque le nœud est inactif. Si vous désactivez l'option, l'adresse IP ne peut pas répondre aux demandes du routeur lorsque le nœud propriétaire est inactif.

Pour savoir comment cette fonctionnalité est utilisée pour surveiller les routes statiques dans le déploiement ECMP, reportez-vous à la rubrique Using Equal Cost Multiple Path (ECMP) .

Pour définir l'état de réponse du nœud propriétaire à l'aide de l'interface de ligne de commande Citrix ADC

À l'invite de commandes, tapez :

```
add ns ip <IPAddress> [-ownerNode <positive_integer>] [-
    ownerDownResponse (YES | NO )] [-td <positive_integer>]
```

Exemple

```
add ns ip 2.2.2.2 255.255.255.0 -ownernode 6  - ownerdownResponse YES
```

Pour définir l'état de réponse du nœud propriétaire à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Système > Réseau > IP**, puis cliquez sur **Ajouter** pour créer une adresse SNIP spotted.
2. Dans la page **Créer une adresse IP**, activez ou désactivez la case à cocher **OwnerDownResponse**.

Pour modifier l'état de réponse du nœud propriétaire à l'aide de l'interface graphique Citrix ADC

Accédez à **Système > Réseau > IP**, sélectionnez une adresse IP et cliquez sur **Modifier**pour sélectionner ou désactivez la case à cocher **OwnerDownResponse**.

Surveillance de la prise en charge de la route statique (MSR) pour les nœuds inactifs dans une configuration de cluster spotted

January 21, 2021

Dans un cluster configuré avec l'option MSR activée sur la route, seuls les nœuds actifs peuvent sonder un itinéraire statique. Il peut atteindre un réseau alors que les nœuds inactifs et de secours n'ont aucun lien avec l'itinéraire et ne peuvent pas y sonder. Vous pouvez maintenant configurer un nœud inactif ou de rechange pour envoyer une sonde PING et ARP à la route IPv4 et envoyer une sonde ping6 et nd6 à la route IPv6. Vous ne pouvez effectuer cette opération que dans une configuration de cluster repéré dans laquelle l'adresse SNIP est active et détenue exclusivement par un seul nœud.

Liaison d'interface VRRP dans un cluster actif à nœud unique

August 20, 2021

Lorsque vous migrez une configuration haute disponibilité (HA) vers une configuration de cluster, toutes les configurations doivent être compatibles et être prises en charge dans le cluster. Pour ce faire, vous pouvez maintenant configurer les ID de routeur virtuel (VRID et VRID6s) sur une interface de nœud.

> **Important**
>
> Actuellement, seul un système de cluster actif à nœud unique prend en charge les VRID et les VRID6.

Pour obtenir des instructions sur la configuration des VRID et des VRID6, reportez-vous à la section Configuration des adresses MAC virtuelles.

Pour configurer un ID de routeur virtuel sur un cluster actif à nœud unique, ajoutez le VRID ou le VRID6 et liez-le à l'interface de nœud de cluster.

Pour ajouter un VRID à l'aide de l'interface de ligne de commande Citrix ADC

À l'invite de commandes, tapez :


```
add vrID <ID>
```

Pour lier un VRID à l'interface de nœud de cluster à l'aide de l'interface CLI de Citrix ADC

À l'invite de commandes, tapez :

```
Bind vrid <ID> -ifnum <interface_name> | -trackifNum <interface_name

Add vrID 100
Bind vrid 100  - ifnum 1/1  1/2
done
```

Pour ajouter un VRID6 à l'aide de l'interface de ligne de commande Citrix ADC

À l'invite de commandes, tapez :

```
add vrID6 <ID>
```

Pour lier un VRID6 à une interface de nœud de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind vrid6 <ID> -ifnum <interface_name> | -trackifNum <interface_name>

Add vrID6 100
Bind vrid6 100  - ifnum 1/1  1/2
Done
```

Scénarios de configuration et d'utilisation du cluster

January 21, 2021

Cette section explique certains scénarios dans lesquels le cluster Citrix ADC peut être configuré et configuré pour différentes fonctionnalités et topologies réseau. Donnez des commentaires si vous souhaitez que d'autres scénarios soient documentés.

Création d'un cluster à deux nœuds

January 21, 2021

Un cluster à deux nœuds est une exception à la règle selon laquelle un cluster n'est fonctionnel que lorsqu'un minimum de nœuds (n/2 + 1), où n est le nombre de nœuds de cluster, sont capables de servir le trafic. Si la même formule est appliquée à un cluster à deux nœuds, le cluster échouerait si un nœud tombe en panne (n/2 +1=2).

Un cluster à deux nœuds est fonctionnel même si un seul nœud est capable de servir le trafic.

La création d'un cluster à deux nœuds est la même chose que la création d'un autre cluster. Vous ajoutez un nœud en tant que coordinateur de configuration et l'autre nœud comme autre nœud de cluster.

> **Remarque**
>
> La synchronisation incrémentielle de configuration n'est pas prise en charge dans un cluster à deux nœuds. Seule la synchronisation complète est prise en charge.

Migration d'une configuration HA vers une configuration de cluster

August 20, 2021

Pour migrer une installation de haute disponibilité (HA) existante vers une installation de cluster, vous devez d'abord supprimer les appliances Citrix ADC de la configuration de haute disponibilité et créer une sauvegarde du fichier de configuration de haute disponibilité. Vous pouvez ensuite utiliser les deux appliances pour créer un cluster et charger le fichier de configuration sauvegardé dans le cluster.

> **Remarque**
>
> - Avant de charger le fichier de configuration HA sauvegardé sur le cluster, vous devez le modifier pour le rendre compatible avec le cluster. Reportez-vous à l'étape pertinente de la procédure.
> - Utilisez la **batch -f <backup_filename>** pour télécharger le fichier de configuration sauvegardé.

L'approche précédente est une solution de migration de base qui entraîne des temps d'arrêt pour l'application déployée. En tant que tel, il ne doit être utilisé que dans les déploiements où la disponibilité des applications n'est pas prise en compte.

Cependant, dans la plupart des déploiements, la disponibilité de l'application est d'une importance primordiale. Dans de tels cas, vous devez utiliser l'approche qui permet de migrer une configuration HA vers une configuration de cluster sans aucun temps d'arrêt. Dans cette approche, une configuration HA existante est migrée vers une configuration de cluster en supprimant d'abord l'appliance secondaire et en utilisant cette solution pour créer un cluster à nœud unique. Une fois que le cluster devient opérationnel et sert le trafic, l'appliance principale de la configuration HA est ajoutée au cluster.

Pour convertir une configuration HA en configuration de cluster (sans temps d'arrêt) à l'aide de l'interface de ligne de commande

Considérons l'exemple d'une installation HA avec l'appliance primaire (NS1) - 10.102.97.131 et l'appliance secondaire (NS2) - 10.102.97.132.

1. Assurez-vous que les configurations de la paire HA sont stables.
2. Connectez-vous à l'une des appliances HA, accédez au shell et créez une copie du fichier ns.conf (par exemple, ns_backup.conf).
3. Ouvrez une session sur l'appliance secondaire, NS2, et effacez les configurations. Cette opération supprime NS2 de la configuration HA et en fait une appliance autonome.

```
1 > clear ns config full
```

> **Remarque**
>
> - Cette étape est requise pour vous assurer que NS2 ne commence pas à posséder des adresses VIP, maintenant qu'il s'agit d'une appliance autonome.
> - À ce stade, l'appliance principale, NS1, est toujours active et continue de servir le trafic.

4. Créez un cluster sur NS2 (désormais un dispositif secondaire) et configurez-le en tant que nœud PASSIF.

```
1  > add cluster instance 1
2
3  > add cluster node 0 10.102.97.132 -state PASSIVE -backplane
     0/1/1
4
5  > add ns ip 10.102.97.133 255.255.255.255 -type CLIP
6
7  > enable cluster instance 1
8
9  > save ns config
10
11 > reboot -warm
```

5. Modifiez le fichier de configuration sauvegardé comme suit :
   - Supprimez les entités qui ne sont pas prises en charge sur un cluster. Pour obtenir la liste des fonctionnalités non prises en charge, consultez Fonctions Citrix ADC prises en charge par un cluster. Il s'agit d'une étape facultative. Si vous n'effectuez pas cette étape, l'exécution des commandes non prises en charge échoue.

- Supprimez les configurations qui ont des interfaces ou mettez à jour les noms d'interface de la convention c/u vers la convention n/c/u .

  Exemple

  ```
  > add vlan 10 -ifnum 0/1
  ```

  doit être changé en

  ```
  > add vlan 10 -ifnum 0/0/1 1/0/1
  ```

- Le fichier de configuration de sauvegarde peut avoir des adresses SNIP. Ces adresses sont striped sur tous les nœuds de cluster. Il est recommandé d'ajouter des adresses IP spotted pour chaque nœud.

  Exemple

  ```
  > add ns ip 1.1.1.1 255.255.255.0 -ownerNode 0

  > add ns ip 1.1.1.2 255.255.255.0 -ownerNode 1
  ```

- Mettez à jour le nom d'hôte pour spécifier le nœud propriétaire.

  Exemple

  ```
  > set ns hostname ns0 -ownerNode 0

  > set ns hostname ns1 -ownerNode 1
  ```

- Modifiez toutes les autres configurations réseau pertinentes qui dépendent des adresses IP repéré. Par exemple, L3 VLAN, configuration RNAT qui utilise SNIP comme NATIP, règles INAT qui fait référence aux SNIP/MIPS).

6. Sur le cluster, procédez comme suit :

   - Apportez les modifications topologiques au cluster en connectant le backplane du cluster, le canal d'agrégation des liens du cluster, etc.
   - Appliquez les configurations du fichier de configuration sauvegardé et modifié au coordinateur de configuration via l'adresse IP du cluster.

     ```
     > batch -f ns_backup.conf
     ```

   - Configurez des mécanismes de distribution du trafic externe tels que ECMP ou l'agrégation de liens de cluster.

7. Basculez le trafic de la configuration HA vers le cluster.

- Ouvrez une session sur l'appliance principale, NS1, et désactivez toutes les interfaces qui s'y trouve.

```
> disable interface <interface_id>
```

- Ouvrez une session sur l'adresse IP du cluster et configurez NS2 en tant que nœud ACTIVE.

```
> set cluster node 0 -state ACTIVE
```

> **Remarque**
>
> Il peut y avoir une petite quantité (de l'ordre de secondes) de temps d'arrêt entre la désactivation des interfaces et l'activation du nœud de cluster.

8. Ouvrez une session sur l'appliance principale, NS1, et supprimez-la de la configuration HA.
   - Effacez toutes les configurations. Cette opération supprime NS1 de la configuration HA et en fait une appliance autonome.

```
> clear ns config full
```

   - Activez toutes les interfaces.

```
> enable interface <interface_id>
```

9. Ajoutez NS1 au cluster.
   - Ouvrez une session sur l'adresse IP du cluster et ajoutez NS1 au cluster.

```
> add cluster node 1 10.102.97.131 -state PASSIVE -backplane
   1/1/1
```

   - Connectez-vous à NS1 et joignez-le au cluster en exécutant séquentiellement les commandes suivantes :

```
> join cluster -clip 10.102.97.133 -password nsroot

> save ns config

> reboot -warm
```

10. Ouvrez une session sur NS1 et effectuez les modifications de topologie et de configuration requises.
11. Connectez-vous à l'adresse IP du cluster et définissez NS1 comme nœud ACTIVE.

```
> set cluster node 1 -state ACTIVE
```


Transition entre un cluster L2 et L3

August 20, 2021

> **Remarque**
>
> Prise en charge à partir de NetScaler 11.

Un cluster L2 est un cluster où tous les nœuds proviennent du même réseau et un cluster L3 peut inclure des nœuds provenant de différents réseaux. Vous pouvez passer d'un type de cluster à l'autre sans interruption pour les applications déployées sur Citrix ADC.

Transition d'un cluster de L2 à L3

Vous pouvez effectuer la transition vers un cluster L3 lorsque vous souhaitez que le cluster inclue des nœuds provenant d'autres réseaux.

Sur l'adresse IP du cluster, procédez comme suit :

1. Créez un groupe de nœuds.

   Exemple

   ```
   1 > add cluster nodegroup NG0
   ```

   Ce groupe de nœuds est utilisé à l'étape suivante pour regrouper tous les nœuds du cluster L2 existant.

2. Transition du cluster L2 vers un cluster L3.

   Exemple

   ```
   1 > set cluster instance 1 -inc ENABLED -nodegroup NG0
   ```

   Cette commande atteint le double objectif de la transition vers le cluster L3 et également d'ajouter tous les nœuds du cluster L2 au groupe de nœuds.

3. Vous pouvez désormais ajouter d'autres nœuds au cluster, comme expliqué dans Ajout d'un nœud au cluster.

Transition d'un cluster de L3 à L2

Vous pouvez effectuer une transition vers un cluster L2 lorsque vous souhaitez conserver des nœuds appartenant à un seul réseau.

Sur l'adresse IP du cluster, procédez comme suit :

1. Supprimez les nœuds de cluster des réseaux que vous ne souhaitez pas conserver.

   Exemple

   ```
   1 > rm cluster node <nodeId>
   ```

2. Transition du cluster L3 vers un cluster L2.

   Exemple

   ```
   1 > set cluster instance 1 -inc DISABLED
   ```

   Le cluster inclut désormais les nœuds d'un seul réseau.

Configuration de GSLB dans un cluster

August 20, 2021

> **Remarque**
>
> Prise en charge à partir de NetScaler 10.5 Build 52.11.

Pour configurer GSLB dans un cluster, vous devez lier les différentes entités GSLB à un groupe de nœuds. Le groupe de nœuds doit avoir un seul nœud membre.

> **Remarques**
>
> - Si vous avez configuré la méthode GSLB de proximité statique, assurez-vous que la base de données de proximité statique est présente sur tous les nœuds de cluster. Cela se produit par défaut si le fichier de base de données est disponible à l'emplacement par défaut. Toutefois, si le fichier de base de données est conservé dans un répertoire autre que /var/netscaler/locdb/, vous devez synchroniser manuellement le fichier sur tous les nœuds du cluster.
> - La `show gslb domain` commande n'est pas prise en charge dans une configuration de cluster.

Pour configurer GSLB dans un cluster à l'aide de l'interface de ligne de commande :

Ouvrez une session sur l'adresse IP du cluster et effectuez les opérations suivantes à l'invite de commandes :

1. Configurez les différentes entités GSLB. Pour plus d'informations, voir Entités de configuration GSLB.

> **Remarque**
>
> Lors de la création du site GSLB, assurez-vous de spécifier l'adresse IP du cluster et l'adresse IP du cluster publique. L'adresse IP du cluster public n'est nécessaire que lorsque le cluster est déployé derrière un périphérique NAT. Lors de la configuration d'un site GSLB, vous devez utiliser l'adresse IP du cluster du même site. Ces paramètres sont nécessaires pour assurer la disponibilité de la fonctionnalité de synchronisation automatique GSLB.

```
add gslb site <siteName> <siteType> <siteIPAddress> -publicIP <ip_addr>
 -clip <ip_addr> <publicCLIP><!--NeedCopy-->
```

2. Créez un groupe de nœuds de cluster.

```
add cluster nodegroup <name> <name>@ [-strict ( YES | NO )] [-sticky (
YES | NO )] [-state <state>] [-priority <positive_integer>]<!--NeedCopy
-->
```

> **Remarque**
>
> Activez l'option collante si vous souhaitez configurer GSLB basé pour les utilisateurs VPN.

3. Liez un nœud de cluster unique au groupe de nœuds.

```
bind cluster nodegroup <name> -node <nodeId><!--NeedCopy-->
```

4. Liez le site GSLB local au groupe de nœuds.

```
bind cluster nodegroup <name> -gslbSite <string><!--NeedCopy-->
```

> **Remarque**
>
> Assurez-vous que l'adresse IP de l'adresse IP du site GSLB local est striped (disponible sur tous les nœuds de cluster).

5. Liez le service ADNS (ou ADNS-TCP) ou le serveur virtuel d'équilibrage de charge DNS (ou DNS-TCP) au groupe de nœuds.

   Pour lier le service ADNS :

   "'bind cluster nodegroup -service

```
1 **Pour lier le serveur virtuel d'équilibrage de charge DNS :**
2
3 ```bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
```

6. Liez le serveur virtuel GSLB au groupe de nœuds.

```
bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
```


7. [Facultatif] Pour configurer GSLB en fonction des utilisateurs VPN, liez le serveur virtuel VPN au groupe de nœuds GSLB.

   ```
   bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

8. Vérifiez les configurations.

   ```
   show gslb runningConfig<!--NeedCopy-->
   ```

Pour configurer GSLB dans un cluster à l'aide de l'interface graphique :

Ouvrez une session sur l'adresse IP du cluster et effectuez les opérations suivantes dans l'onglet Configuration :

1. Configurez les entités GSLB.

   Accédez à **Gestion du trafic > GSLB** pour effectuer les configurations requises.

2. Créez un groupe de nœuds et effectuez d'autres configurations liées au groupe de nœuds.

   Accédez à **Système > Cluster > Groupes de nœuds** pour effectuer les configurations requises.

Pour les configurations détaillées à effectuer, reportez-vous à la description fournie dans la procédure CLI précédente.

Prise en charge de la topologie parent-enfant GSLB dans un cluster

À partir de NetScaler 12.1 build 49.xx, la topologie parent-enfant GSLB est prise en charge dans le cluster.

Pour plus d'informations sur la topologie parent-enfant, voir Déploiement de la topologie parent-enfant à l'aide du protocole MEP.

Pour configurer la topologie parent-enfant GSLB dans un cluster à l'aide de l'interface de ligne de commande

Site parent

Effectuez la configuration suivante :

1. Créez un groupe de nœuds de cluster.

   ```
   add cluster nodegroup <name>
   ```

   Exemple :

   ```
   add cluster nodegroup parentng
   ```

2. Liez un nœud de cluster unique au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -node <nodeId>
   ```


Exemple :

```
bind cluster nodegroup parentng -node n2
```

3. Liez le site GSLB local au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -gslbSite <string>
   ```

   Exemple :

   ```
   bind cluster nodegroup parentng -gslbSite site1
   ```

4. Liez le service ADNS (ou ADNS-TCP) ou le serveur virtuel d'équilibrage de charge DNS (ou DNS-TCP) au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -service <string>
   ```

   Exemple :

   ```
   bind cluster nodegroup parentng - service ADNS
   ```

5. Liez le serveur virtuel GSLB au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -vServer <string>
   ```

   Exemple :

   ```
   bind cluster nodegroup parentng -vServce gslbvs1
   ```

Site enfant

Effectuez la configuration suivante :

1. Créez un groupe de nœuds de cluster.

   ```
   add cluster nodegroup <name>
   ```

   Exemple :

   ```
   add cluster nodegroup childng
   ```

2. Liez un nœud de cluster unique au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -node <nodeId>
   ```

   Exemple :

   ```
   bind cluster nodegroup childng -node -n3
   ```

3. Liez le site GSLB local au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -gslbSite <string>
   ```

   Exemple :

   ```
   bind cluster nodegroup childng -gslbSite site1
   ```


> **Remarque**
>
> Pour que les sites parents et enfants échangent des statistiques agrégées dans des méthodes d'équilibrage de charge basées sur des mesures, vous devez ajouter des services GSLB locaux sur le site enfant. Les méthodes d'équilibrage de charge basées sur des métriques sont le moins de connexion, la moins de bande passante et le moins de paquets.

Pour configurer la topologie parent-enfant GSLB dans un cluster à l'aide de l'interface graphique

1. Configurez les entités GSLB.

   Accédez à **Gestion du trafic** > **GSLB** pour effectuer les configurations requises.

2. Créez un groupe de nœuds.

   Accédez à **Système** > **Cluster** > **Groupes de nœuds** pour effectuer les configurations requises.

3. Dans la page Groupe de nœuds, sélectionnez le groupe de nœuds auquel vous souhaitez lier un nœud, cliquez sur **Modifier**, puis effectuez les tâches suivantes. Vous pouvez également effectuer ces tâches lors de l'ajout d'un groupe de nœuds.

   - Liez un nœud au groupe de nœuds.

     Dans **Paramètres avancés**, cliquez sur **Nœuds de cluster** et effectuez les tâches suivantes :

     - Dans la section **Nœuds de cluster**, cliquez sur **Aucun nœud de cluster**.
     - Dans **Sélectionner le nœud de cluster**, cliquez sur > et sélectionnez le nœud que vous souhaitez lier au groupe de nœuds. Vous pouvez également ajouter un nœud de cluster.

   - Liez le site GSLB local au groupe de nœuds.

     Dans Paramètres avancés, cliquez sur Sites GSLB et effectuez les tâches suivantes :

     - Dans la section **Sites GSLB**, cliquez sur Aucun site GSLB.
     - Dans le **menu Sélectionner un site GSLB**, cliquez sur > et sélectionnez le site GSLB que vous souhaitez lier au groupe de nœuds. Vous pouvez également ajouter un site GSLB.

   - Liez le serveur virtuel GSLB au groupe de nœuds.

     Dans **Paramètres avancés**, cliquez sur **Serveurs virtuels** et effectuez la tâche suivante :

     - Dans le volet **Serveurs virtuels**, cliquez sur +.
     - Dans **Choisir un serveur virtuel**, sélectionnez le serveur que vous souhaitez lier au groupe de nœuds.

- Liez le service ADNS (ou ADNS-TCP) ou le serveur virtuel d'équilibrage de charge DNS (ou DNS-TCP) au groupe de nœuds.

  Dans **Paramètres avancés**, cliquez sur **Services** et effectuez les tâches suivantes :

  - Dans la section **Services**, cliquez sur **Aucun service**.
  - Dans **Sélectionner un service**, sélectionnez le service que vous souhaitez lier au groupe de nœuds. Vous pouvez également ajouter un service.

> **Remarque**
>
> Pour les sites enfants, il suffit de lier le nœud de cluster et le site GSLB local au groupe de nœuds.

Utilisation de la redirection du cache dans un cluster

August 20, 2021

La redirection du cache dans un cluster fonctionne de la même manière que sur une appliance Citrix ADC autonome. La seule différence est que les configurations sont effectuées sur l'adresse IP du cluster. Pour plus d'informations sur la redirection du cache, voir Redirection du cache.

Points à retenir lors de l'utilisation de la redirection de cache en mode transparent sur un cluster :

- Avant de configurer la redirection du cache, assurez-vous que vous avez connecté tous les nœuds au commutateur externe et que vous avez configuré des jeux de liens. Sinon, les demandes client sont supprimées.
- Lorsque le mode MAC est activé sur un serveur virtuel d'équilibrage de charge, assurez-vous que le mode MBF est activé sur le cluster à l'aide de la commande enable ns mode MBF. Sinon, les requêtes sont envoyées directement au serveur d'origine au lieu d'être envoyées au serveur de cache.

Utilisation du mode L2 dans une configuration de cluster

January 21, 2021

> **Remarque**
>
> Prise en charge de NetScaler 10.5 et versions ultérieures.

Pour utiliser le mode L2 dans une configuration de cluster, vous devez vous assurer des éléments suivants :

- Les adresses IP spotted doivent être disponibles sur tous les nœuds, selon les besoins.
- Les jeux de liens doivent être utilisés pour communiquer avec le réseau externe.
- Les topologies asymétriques ou les groupes LA de cluster asymétrique ne sont pas pris en charge.
- Le groupe LA de cluster est recommandé.
- Le trafic est distribué entre les nœuds de cluster uniquement pour les déploiements où des services existent.

Utilisation du canal LA de cluster avec des jeux de liens

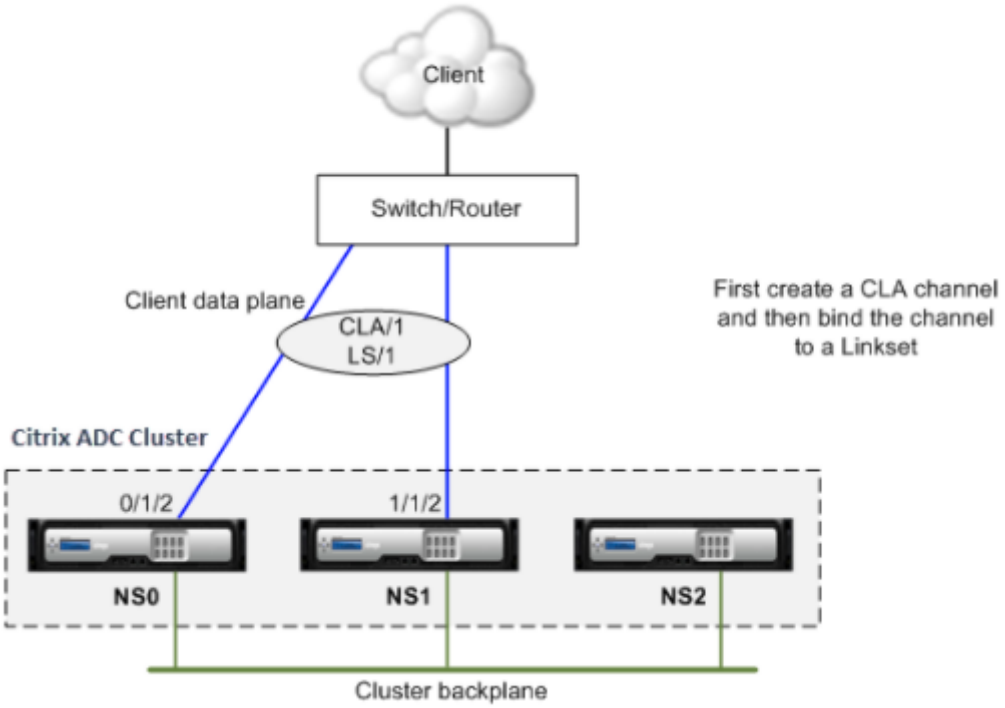
January 21, 2021

Dans une topologie de cluster asymétrique, certains nœuds de cluster ne sont pas connectés au réseau en amont. Dans ce cas, vous devez utiliser des jeux de liens. Pour optimiser les performances, vous pouvez lier les interfaces connectées au commutateur en tant que canal LA de cluster, puis lier le canal à un jeu de liens.

Pour comprendre comment une combinaison de canaux LA de cluster et de jeux de liens peut être utilisée, envisagez un cluster à trois nœuds pour lequel le commutateur en amont ne dispose que de deux ports. Vous pouvez connecter deux des nœuds de cluster au commutateur et laisser l'autre nœud non connecté.

> **Remarque**
>
> De même, vous pouvez également utiliser une combinaison d'ECMP et de jeux de liens dans une topologie asymétrique.

Figure 1. Linksets et topologie des canaux LA de cluster



Pour configurer le canal LA de cluster et les ensembles de liens à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'adresse IP du cluster.
2. Liez les interfaces connectées à un canal LA de cluster.

```
add channel CLA/1 -ifnum 0/1/2 1/1/2
```

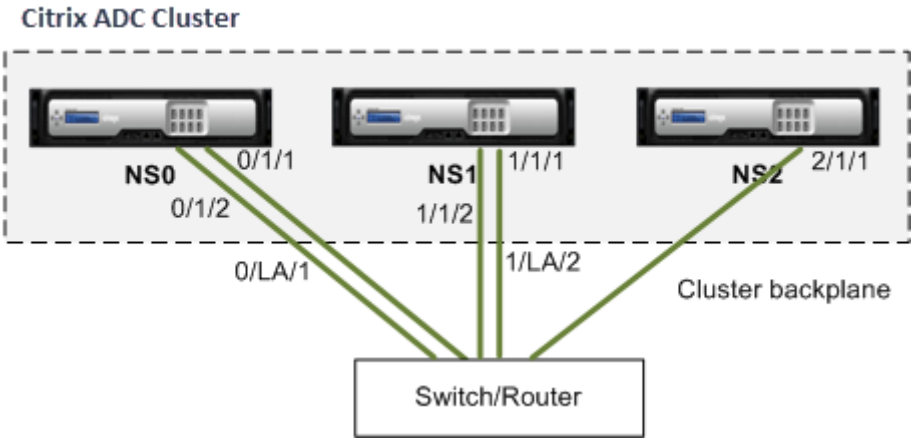
3. Liez le canal LA du cluster au jeu de liens.

```
add linkset LS/1 -ifnum CLA/1
```

backplane sur le canal LA

January 21, 2021

Dans ce déploiement, les canaux LA sont utilisés pour le backplane du cluster.



- NS0 - nodeId: 0, NSIP: 10.102.29.60
- NS1 - nodeId: 1, NSIP: 10.102.29.70
- NS2 - nodeId: 2, NSIP: 10.102.29.80

Pour déployer un cluster avec les interfaces de backplane en tant que canaux LA

1. Créez un cluster de nœuds NS0, NS1 et NS2.

   a) Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :

   ```
   > create cluster instance 1
   > add cluster node 0 10.102.29.60 -state ACTIVE
   > enable cluster instance 1
   > add ns ip 10.102.29.61 255.255.255.255 -type CLIP
   > save ns config
   > reboot -warm
   ```

   b) Connectez-vous à l'adresse IP du cluster et procédez comme suit :

   ```
   > add cluster node 1 10.102.29.70 -state ACTIVE
   > add cluster node 2 10.102.29.80 -state ACTIVE
   ```

   c) Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

   ```
   > join cluster -clip 10.102.29.61 -password nsroot
   > save ns config
   > reboot -warm
   ```

   Comme on le voit dans les commandes précédentes, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de fond de panier des trois nœuds de cluster.

2. Connectez-vous à l'adresse IP du cluster et procédez comme suit :

   a) Créez les canaux LA pour les nœuds NS0 et NS1.

```
> add channel 0/LA/1 -ifnum 0/1/1 0/1/2
> add channel 1/LA/2 -ifnum 1/1/1 1/1/2
```

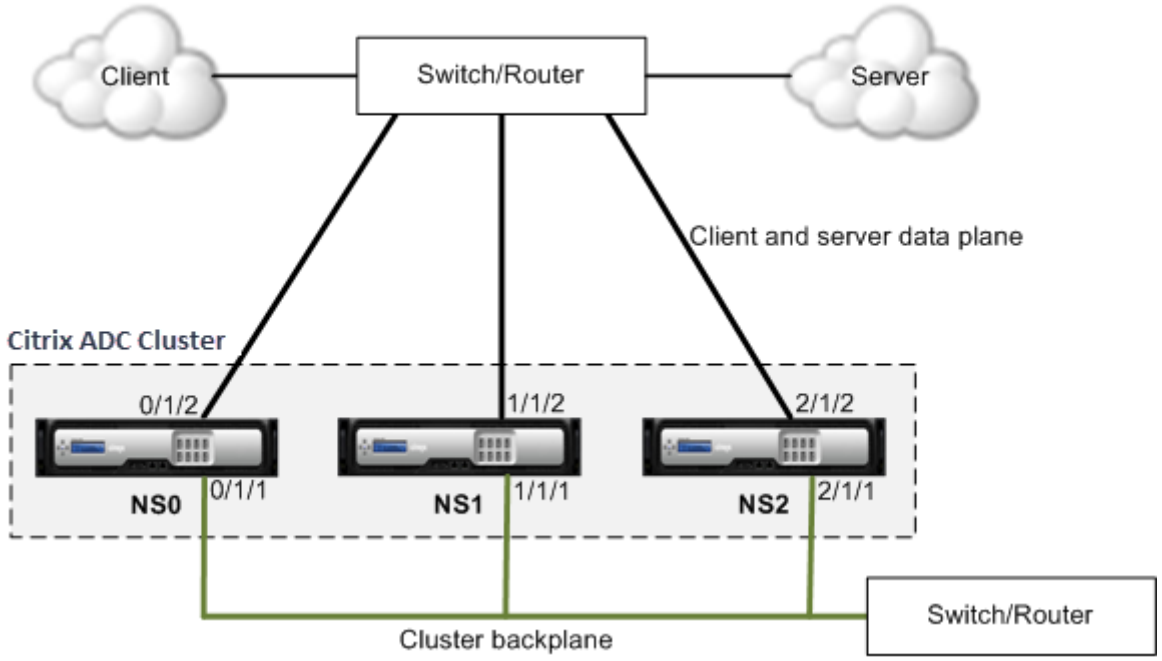
   b) Configurez le backplane pour les nœuds de cluster.

```
> set cluster node 0 -backplane 0/LA/1
> set cluster node 1 -backplane 1/LA/2
> set cluster node 2 -backplane 2/1/1
```

Interfaces communes pour le client et le serveur et interfaces dédiées pour le backplane

August 20, 2021

Il s'agit d'un déploiement à un bras du cluster Citrix ADC. Dans ce déploiement, les réseaux client et serveur utilisent les mêmes interfaces pour communiquer avec le cluster. Le backplane du cluster utilise des interfaces dédiées pour la communication entre nœuds.



- NS0 - nodeId: 0, NSIP: 10.102.29.60
- NS1 - nodeId: 1, NSIP: 10.102.29.70

- NS2 - nodeId: 2, NSIP: 10.102.29.80

Pour déployer un cluster avec une interface commune pour le client et le serveur et une interface différente pour le backplane du cluster

1. Créez un cluster de nœuds NS0, NS1 et NS2.
2. Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :

```
1 > create cluster instance 1
2 > add cluster node 0 10.102.29.60 -state ACTIVE -backplane
    0/1/1
3 > enable cluster instance 1
4 > add ns ip 10.102.29.61 255.255.255.255 -type CLIP
5 > save ns config
6 > reboot -warm
```

3. Connectez-vous à l'adresse IP du cluster et procédez comme suit :

```
1 > add cluster node 1 10.102.29.70 -state ACTIVE -backplane
    1/1/1
2 > add cluster node 2 10.102.29.80 -state ACTIVE -backplane
    2/1/1
```

4. Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
1 > join cluster -clip 10.102.29.61 -password nsroot
2 > save ns config
3 > reboot -warm
```

Comme on le voit dans les commandes précédentes, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de fond de panier des trois nœuds de cluster.

1. Sur l'adresse IP du cluster, créez des VLAN pour les interfaces de backplane et pour les interfaces client et serveur.

   //Pour les interfaces de backplane

```
1 > add vlan 10
2 > bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //Pour les interfaces connectées aux réseaux client et serveur.

```
1 > add vlan 20
2 > bind vlan 20 0/1/2 1/1/2 2/1/2
```


2. Sur le commutateur, créez des VLAN pour les interfaces correspondant aux interfaces de backplane et aux interfaces client et serveur. Les exemples de configuration suivants sont fournis pour le commutateur Cisco® Nexus 7000 C7010 version 5.2(1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

   //Pour les interfaces de backplane. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/47
  switchport access vlan 100
  switchport mode access
  end
```

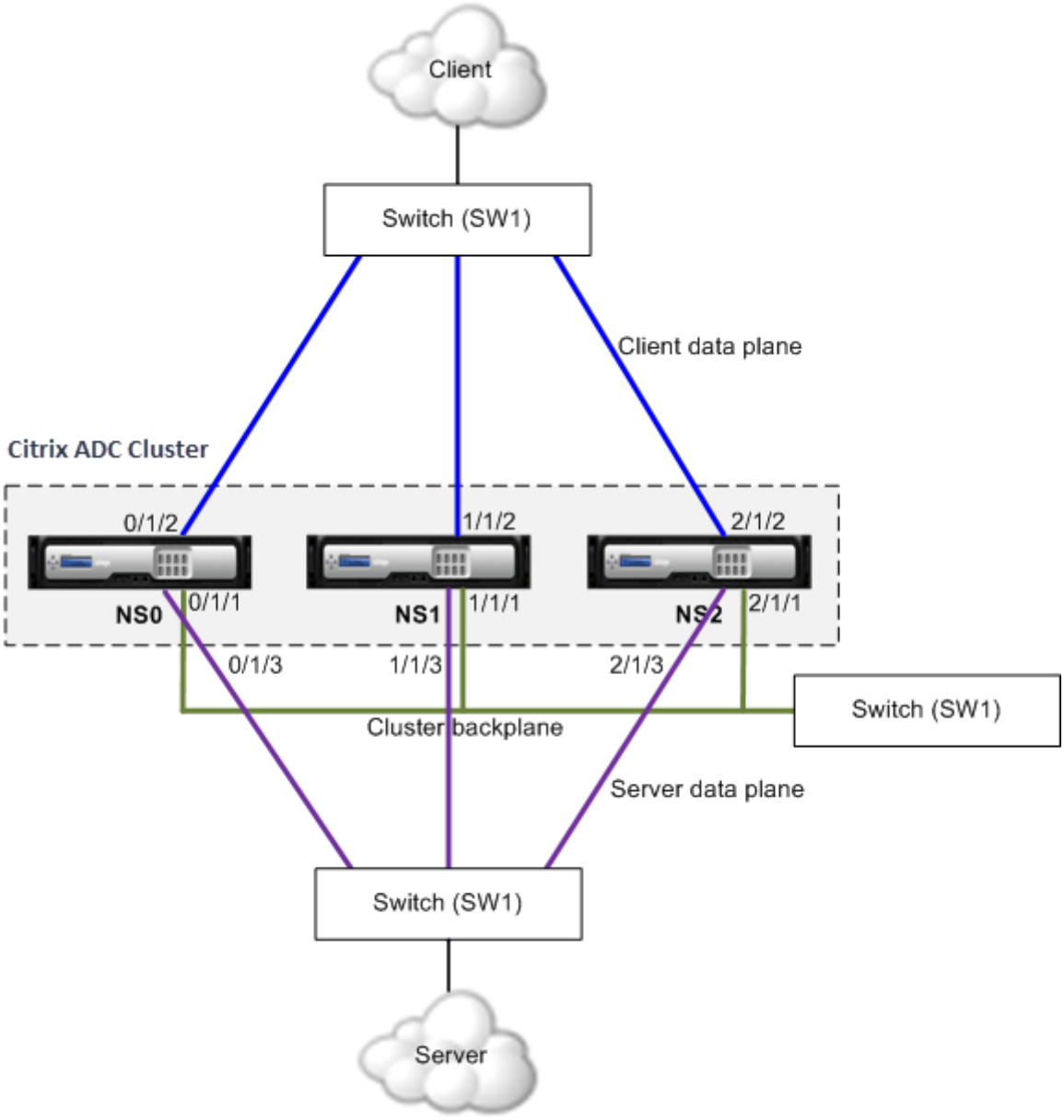
   //Pour les interfaces connectées aux réseaux client et serveur. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/47
  switchport access vlan 200
  switchport mode access
  end
```

Commutateur commun pour le client, le serveur et le backplane

August 20, 2021

Dans ce déploiement, le client, le serveur et le backplane utilisent des interfaces dédiées sur le même commutateur pour communiquer avec le cluster Citrix ADC.



- NS0 - nodeId: 0, NSIP: 10.102.29.60
- NS1 - nodeId: 1, NSIP: 10.102.29.70
- NS2 - nodeId: 2, NSIP: 10.102.29.80

Pour déployer un cluster avec un commutateur commun pour le client, le serveur et le backplane

1. Créez un cluster de nœuds NS0, NS1 et NS2.
2. Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :


```
1 > create cluster instance 1
2 > add cluster node 0 10.102.29.60 -state ACTIVE -backplane
     0/1/1
3 > enable cluster instance 1
4 > add ns ip 10.102.29.61 255.255.255.255 -type CLIP
5 > save ns config
6 > reboot -warm
```

3. Connectez-vous à l'adresse IP du cluster et procédez comme suit :

```
1 > add cluster node 1 10.102.29.70 -state ACTIVE -backplane
     1/1/1
2 > add cluster node 2 10.102.29.80 -state ACTIVE -backplane
     2/1/1
```

4. Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
1 > join cluster -clip 10.102.29.61 -password nsroot
2 > save ns config
3 > reboot -warm
```

Comme on le voit dans les commandes précédentes, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de fond de panier des trois nœuds de cluster.

1. Sur l'adresse IP du cluster, créez des VLAN pour les interfaces backplane, client et serveur.

   //Pour les interfaces de backplane

```
1 > add vlan 10
2 > bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //Pour les interfaces côté client

```
1 > add vlan 20
2 > bind vlan 20 0/1/2 1/1/2 2/1/2
```

   //Pour les interfaces côté serveur

```
1 > add vlan 30
2 > bind vlan 30 0/1/3 1/1/3 2/1/3
```

2. Sur le commutateur, créez des VLAN pour les interfaces correspondant aux interfaces de backplane et aux interfaces client et serveur. Les exemples de configuration suivants sont fournis

pour le commutateur Cisco® Nexus 7000 C7010 version 5.2(1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

//Pour les interfaces de backplane. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/47
  switchport access vlan 100
  switchport mode access
  end
```

//Pour les interfaces client. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/48
  switchport access vlan 200
  switchport mode access
  end
```

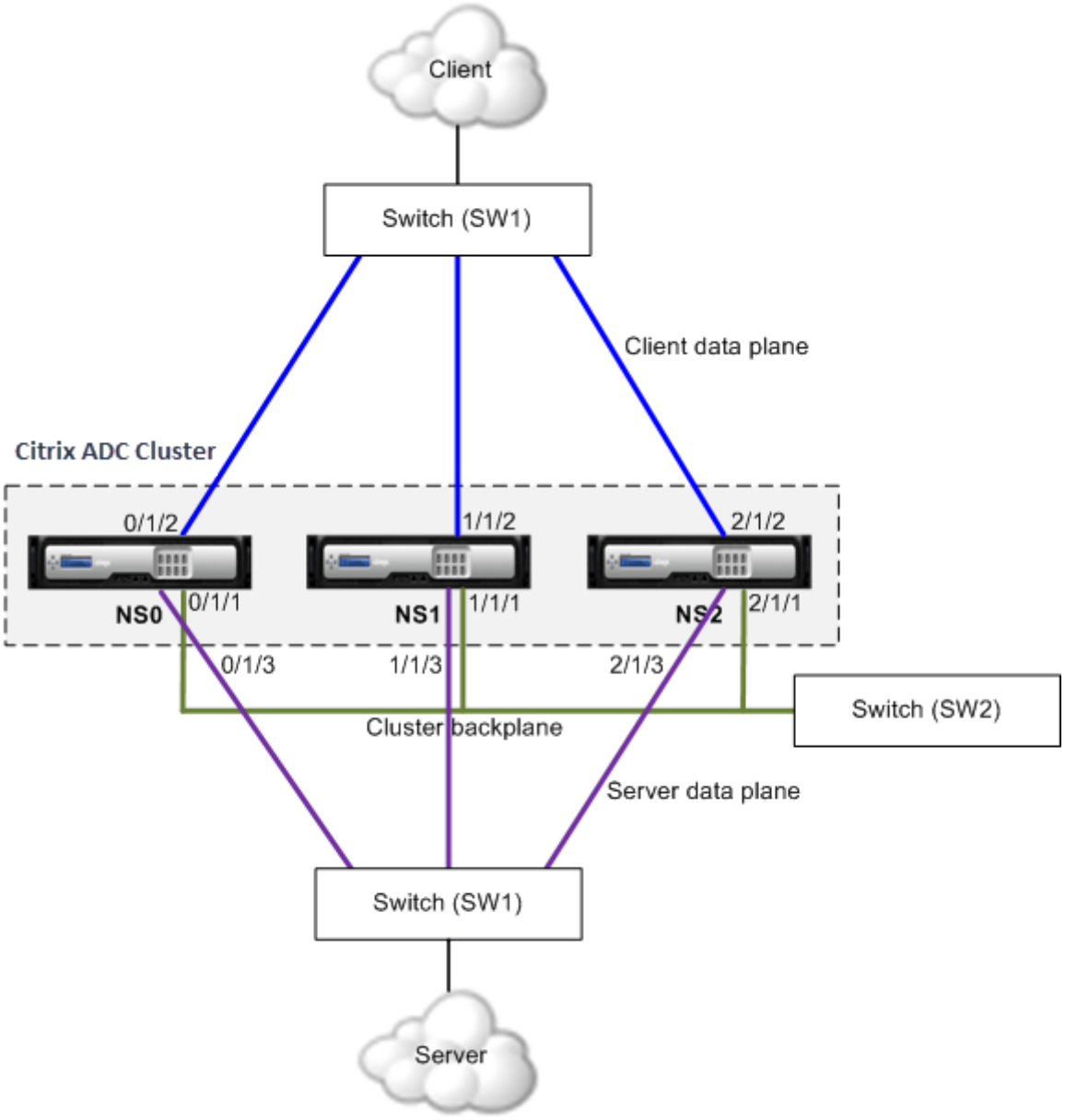
//Pour les interfaces serveur. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/49
  switchport access vlan 300
  switchport mode access
  end
```

Commutateur commun pour le client et le serveur et commutateur dédié pour le backplane

January 21, 2021

Dans ce déploiement, les clients et les serveurs utilisent différentes interfaces sur le même commutateur pour communiquer avec le cluster Citrix ADC. Le backplane du cluster utilise un commutateur dédié pour la communication entre nœuds.



- NS0 - nodeId: 0, NSIP: 10.102.29.60
- NS1 - nodeId: 1, NSIP: 10.102.29.70
- NS2 - nodeId: 2, NSIP: 10.102.29.80

Pour déployer un cluster avec le même commutateur pour les clients et les serveurs et un autre commutateur pour le backplane du cluster

1. Créez un cluster de nœuds NS0, NS1 et NS2.
    - Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :


```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE -backplane
   0/1/1
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

- Connectez-vous à l'adresse IP du cluster et procédez comme suit :

```
> add cluster node 1 10.102.29.70 -state ACTIVE -backplane
   1/1/1
> add cluster node 2 10.102.29.80 -state ACTIVE -backplane
   2/1/1
```

- Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot -warm
```

Comme on le voit dans les commandes précédentes, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de fond de panier des trois nœuds de cluster.

2. Sur l'adresse IP du cluster, créez des VLAN pour les interfaces backplane, client et serveur.

   //Pour les interfaces de backplane

```
> add vlan 10
> bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //Pour les interfaces côté client

```
> add vlan 20
> bind vlan 20 0/1/2 1/1/2 2/1/2
```

   //Pour les interfaces côté serveur

```
> add vlan 30
> bind vlan 30 0/1/3 1/1/3 2/1/3
```

3. Sur le commutateur, créez des VLAN pour les interfaces correspondant aux interfaces de backplane et aux interfaces client et serveur. Les exemples de configuration suivants sont fournis

pour le commutateur Cisco® Nexus 7000 C7010 version 5.2(1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

//Pour les interfaces de backplane. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/47
> switchport access vlan 100
> switchport mode access
> end
```

//Pour les interfaces client. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/48
> switchport access vlan 200
> switchport mode access
> end
```

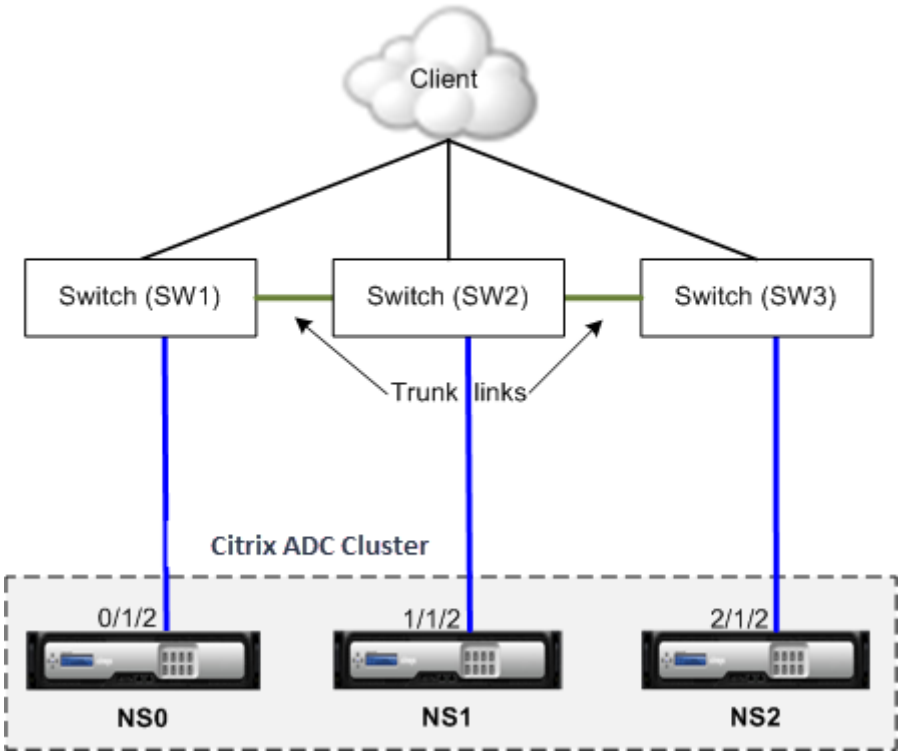
//Pour les interfaces serveur. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/49
> switchport access vlan 300
> switchport mode access
> end
```

Commutateur différent pour chaque nœud

January 21, 2021

Dans ce déploiement, chaque nœud de cluster est connecté à un commutateur différent et les liaisons de jonction sont configurées entre les commutateurs.



Les configurations de cluster sont les mêmes que les autres scénarios de déploiement. La plupart des configurations côté client sont effectuées sur les commutateurs côté client.

Exemples de configurations de cluster

January 21, 2021

L'exemple suivant peut être utilisé pour configurer un cluster à quatre nœuds avec ECMP, LA de cluster ou Linksets.

1. Créez le cluster.
    - Ouvrez une session sur le premier nœud.
    - Ajoutez l'instance de cluster.

```
1   > add cluster instance 1
```

    - Ajoutez le premier nœud au cluster.

```
1   > add cluster node 0 10.102.33.184 -backplane 0/1/1
```

    - Activez l'instance de cluster.


```
1   > enable cluster instance 1
```

- Ajoutez l'adresse IP du cluster.

```
1   > add ns ip 10.102.33.185 255.255.255.255 -type CLIP
```

- Enregistrez les configurations.

```
1   > save ns config
```

- Redémarrez l'appliance à chaud.

```
1   > reboot -warm
```

2. Ajoutez les trois autres nœuds au cluster.
   - Connectez-vous à l'adresse IP du cluster.
   - Ajoutez le deuxième nœud au cluster.

```
1   > add cluster node 1 10.102.33.187 -backplane 1/1/1
```

   - Ajoutez le troisième nœud au cluster.

```
1   > add cluster node 2 10.102.33.188 -backplane 2/1/1
```

   - Ajoutez le quatrième nœud au cluster.

```
1   > add cluster node 3 10.102.33.189 -backplane 3/1/1
```

3. Joignez les nœuds ajoutés au cluster. Cette étape n'est pas applicable au premier nœud.
   - Connectez-vous à chaque nœud nouvellement ajouté.
   - Joignez le nœud au cluster.

```
1   > join cluster -clip 10.102.33.185 -password nsroot
```

   - Enregistrez la configuration.

```
1   > save ns config
```

   - Redémarrez l'appliance à chaud.

```
1   > reboot -warm
```


4. Configurez le cluster Citrix ADC via l'adresse IP du cluster.

   // Activer la fonction d'équilibrage de charge

   ```
   1      > enable ns feature lb
   ```

   // Ajout d'un serveur virtuel d'équilibrage de charge

   ```
   1      > add lb vserver first_lbvserver http
   2      ....
   3      ....
   ```

5. Configurez l'un des mécanismes de distribution de trafic suivants (ECMP, LA de cluster ou Linkset) pour le cluster.

   ECMP

   - Connectez-vous à l'adresse IP du cluster.
   - Activez le protocole de routage OSPF.

     ```
     1   > enable ns feature ospf
     ```

   - Ajoutez un VLAN.

     ```
     1   > add vlan 97
     ```

   - Liez les interfaces des nœuds de cluster au VLAN.

     ```
     1   > bind vlan 97 -ifnum 0/1/4 1/1/4 2/1/4 3/1/4
     ```

   - Ajoutez un SNIP spotted sur chaque nœud et activez le routage dynamique sur celui-ci.

     ```
     1   > add ns ip 1.1.1.10 255.255.255.0 -ownerNode 0 -
           dynamicRouting ENABLED
     2   > add ns ip 1.1.1.11 255.255.255.0 -ownerNode 1 -
           dynamicRouting ENABLED
     3   > add ns ip 1.1.1.12 255.255.255.0 -ownerNode 2 -
           dynamicRouting ENABLED
     4   > add ns ip 1.1.1.13 255.255.255.0 -ownerNode 3 -
           dynamicRouting ENABLED
     ```

   - Liez l'une des adresses SNIP au VLAN.

     ```
     1   > bind vlan 97 -ipAddress 1.1.1.10 255.255.255.0
     ```


- Configurez le protocole de routage sur les ZEBOs à l'aide du shell VTYSH.

  Cluster statique LA

  - Connectez-vous à l'adresse IP du cluster.
  - Ajouter un canal LA de cluster.

    ```
    1   > add channel CLA/1 -speed 1000
    ```

  - Liez les interfaces au canal LA du cluster.

    ```
    1   > bind channel CLA/1 0/1/5 1/1/5 2/1/5 3/1/5
    ```

  - Effectuez une configuration équivalente sur le commutateur.

    Cluster dynamique LA

    * Connectez-vous à l'adresse IP du cluster.
    * Ajoutez les interfaces au canal LA du cluster.

      ```
      1   > set interface 0/1/5 -lacpmode active -lacpkey 5 -
          lagtype cluster
      2   > set interface 1/1/5 -lacpmode active -lacpkey 5 -
          lagtype cluster
      3   > set interface 2/1/5 -lacpmode active -lacpkey 5 -
          lagtype cluster
      4   > set interface 3/1/5 -lacpmode active -lacpkey 5 -
          lagtype  cluster
      ```

    * Effectuez une configuration équivalente sur le commutateur.

    Ensembles de liens. Supposons que le nœud avec NodeID 3 n'est pas connecté au commutateur. Vous devez configurer un jeu de liens afin que le nœud non connecté puisse utiliser les autres interfaces de nœud pour communiquer avec le commutateur.

  a) Connectez-vous à l'adresse IP du cluster.

  b) Ajouter un jeu de liens.

     ```
     1  > add linkset LS/1
     ```

  c) Liez les interfaces connectées au jeu de liens.

     ```
     1  > bind linkset LS/1 -ifnum 0/1/6 1/1/6 2/1/6
     ```

6. Mettez à jour l'état des nœuds de cluster en ACTIVE.


```
> set cluster node 0 -state ACTIVE
> set cluster node 1 -state ACTIVE
> set cluster node 2 -state ACTIVE
> set cluster node 3 -state ACTIVE
```

Utilisation de VRRP dans une configuration de cluster

August 20, 2021

Virtual Router Redundancy Protocol (VRRP) est pris en charge dans une configuration de cluster pour IPv4 et IPv6. Les deux fonctionnalités VRRP prises en charge dans une configuration de cluster sont VRRP basé sur l'interface et VRRP basé sur IP.

VRRP basé sur IP

Dans VRRP basé sur IP, les adresses VIP par bandes liées au même VRID sont configurées sur tous les nœuds d'une configuration de cluster. Ces adresses VIP sont actives sur tous les nœuds

L'un des nœuds de cluster agit en tant que propriétaire VRID et envoie la publicité VRRP à d'autres nœuds. En cas d'échec du nœud propriétaire VRID, un autre nœud du cluster assume la propriété du VRID et commence à envoyer des publicités VRRP. Vous pouvez également affecter un nœud de cluster spécifique en tant que propriétaire du VRID.

> **Remarque**
>
> Citrix vous recommande d'utiliser la méthode basée sur IP pour le déploiement VRRP dans le cluster.

Configuration du VRRP basé sur IP pour IPv4

Effectuez les tâches suivantes sur une configuration de cluster pour configurer le VRRP basé sur IP pour IPv4 :

- **Ajoutez un VRID**. Un VRID est un entier utilisé par la configuration de cluster pour former une adresse MAC virtuelle. L'adresse VMAC générique est sous la forme de 00:00:5e:00:02:<VRID>.
- **(Facultatif) Affectez un nœud en tant que propriétaire de l'adresse MAC virtuelle**. Vous pouvez définir le paramètre de nœud propriétaire (lors de l'ajout ou de la modification de VRID6) sur l'ID du nœud de cluster pour l'affecter en tant que propriétaire de l'adresse MAC virtuelle. Si le nœud propriétaire attribué échoue, l'un des nœuds de cluster UP est dynamiquement choisi comme propriétaire de l'adresse MAC virtuelle. Vous pouvez définir le nœud propriétaire à l'aide de la `set vrID <id> -ownerNode <positive_interger>` commande.

- **Liez le VRID à l'adresse VIP des nœuds**. Liez le VRID créé à l'adresse VIP entrelacée.

Pour ajouter un VRID à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 - add vrid <ID> [-ownerNode <positive_integer>]
2 - show vrid <ID>
```

Pour lier le VRID à l'adresse VIP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set ns ip <IPv4Address> -vrid <ID><!--NeedCopy-->`
- `show vrid <ID><!--NeedCopy-->`

Pour ajouter un VRID à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > VMAC** et, sous l'onglet **VMAC**, cliquez sur **Ajouter** .
2. Dans la page Créer un **VMAC**, spécifiez une valeur dans le champ **ID du routeur virtuel**, puis cliquez sur **Créer** .

Pour lier le VRID à une adresse VIP à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > IP**, sous l'onglet **IPv4s**, sélectionnez une adresse VIP et cliquez sur **Modifier**.
2. Définissez le paramètre **Virtual Router ID** lors de la modification de la configuration VIP.

```
1 > add vrid 90
2  Done
3 > set ns ip 192.0.2.90 - vrid 90
4  Done
```

Configuration du VRRP basé sur IP pour IPv6

Effectuez les tâches suivantes sur une configuration de cluster pour configurer le VRRP basé sur IP pour IPv6 :

- **Ajoutez un VRID6**. Un VRID6 est un entier utilisé par la configuration de cluster pour former une adresse MAC6 virtuelle. L'adresse générique VMAC6 est sous la forme de 00:00:5e:00:02:<VRID6>.

- **(Facultatif) Affectez un nœud en tant que propriétaire de l'adresse MAC6 virtuelle**. Vous pouvez définir le paramètre de nœud propriétaire (lors de l'ajout ou de la modification de VRID6) sur l'ID du nœud de cluster pour l'affecter en tant que propriétaire de l'adresse MAC6 virtuelle. Si le nœud propriétaire attribué échoue, l'un des nœuds de cluster UP est dynamiquement choisi comme propriétaire de l'adresse MAC6 virtuelle.
- **Liez le VRID6 à l'adresse VIP6 des nœuds**. Liez le VRID6 créé à l'adresse VIP6 entrelacée.

Pour ajouter un VRID6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add vrid6 <ID> [-ownerNode <positive_integer>]<!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

Pour lier l'adresse VRID6 à VIP6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set ns ip6 <IPv6Address> -vrid6 <ID><!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

Pour ajouter un VRID6 à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > VMAC** et, sous l'onglet **VMAC6**, cliquez sur **Ajouter** .
2. Sur la page **Créer MAC6 virtuel**, spécifiez une valeur dans le champ **ID du routeur virtuel**, puis cliquez sur **Créer** .

Pour lier le VRID6 à une adresse VIP6 à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > IP**, sous l'onglet **IPv6s**, sélectionnez une adresse VIP et cliquez sur **Modifier**.
2. Définissez le paramètre **Virtual Router ID** lors de la modification de la configuration VIP6.

```
1 > add vrid6 90
2  Done
3 > set ns ip6 2001:db8::5001  - vrid6 90
4  Done
```

VRRP basé sur l'interface

Dans la fonction VRRP basée sur l'interface, la même adresse MAC virtuelle est configurée sur les deux nœuds du cluster. Cette adresse MAC virtuelle est utilisée dans les annonces GARP et les réponses

ARP pour les adresses IP configurées sur un nœud. Cette fonctionnalité est utile dans une configuration de cluster à deux nœuds active de secours qui dispose de périphériques/routeurs externes qui n'acceptent pas les publicités GARP.

> **Remarque**
>
> La fonction VRRP basée sur l'interface ne s'applique qu'à un cluster à deux nœuds dont un nœud est en état actif et l'autre noeud servant de rechange.

Avec la même adresse MAC virtuelle sur les deux nœuds de cluster, lorsque le nœud actif tombe en panne et que le nœud de secours prend le relais comme actif, l'adresse MAC des adresses IP du nouveau nœud actif reste inchangée et les tables ARP des périphériques/routeurs externes n'ont pas besoin d'être mises à jour.

Configuration de VRRP basé sur l'interface pour IPv4

Effectuez les tâches suivantes sur une configuration de cluster pour configurer VRRP basé sur l'interface pour IPv4 :

- **Ajoutez un VRID**. Un VRID est un entier utilisé par la configuration de cluster pour former une adresse MAC virtuelle.
- **Liez le VRID aux interfaces de nœud**. Liez les interfaces au VRID créé. Les interfaces liées (dans le nœud actif actuel) utilisent l'adresse MAC virtuelle dans les publicités GARP et les réponses ARP pour ses adresses IPv4. Vous devez associer le VRID aux interfaces des deux nœuds de la configuration du cluster de secours actif. En effet, contrairement à une configuration de haute disponibilité, les ID d'interface diffèrent dans une configuration de cluster.

Pour ajouter un VRID à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 - add vrid <ID>
2 - show vrid <ID>
```

Pour lier le VRID à une interface à l'aide de la CLI

À l'invite de commandes, tapez :

```
1 - bind vrid <ID> -ifnum <interface_name>
2 - show vrid <ID>
```


Pour ajouter un VRID et le lier à des interfaces à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > VMAC** et, sous l'onglet **VMAC**, cliquez sur **Ajouter** .
2. Sur la page **Créer un MAC virtuel**, spécifiez une valeur dans le champ Identifiant du routeur ****virtuel*, liez les interfaces dans la section**Associer les interfaces**, puis cliquez sur**Créer**.

```
> add vrid 300
 Done
> bind vrid 300 -ifnum 1/1/2 2/1/3
 Done
```

Configuration du VRRP basé sur l'interface pour IPv6

Effectuez les tâches suivantes sur une configuration de cluster pour configurer le VRRP basé sur l'interface pour IPv6 :

- **Ajoutez un VRID6**. Un VRID6 est un entier utilisé par la configuration de cluster pour former une adresse MAC6 virtuelle. L'adresse générique VMAC6 est sous la forme de 00:00:5 e : 00:01 : <VRID6>.
- **Liez le VRID6 aux interfaces de nœud**. Liez les interfaces au VRID6 créé. Les interfaces liées (dans le nœud actif actuel) utilisent l'adresse MAC6 virtuelle dans les publicités GARP et les réponses ARP pour ses adresses IPv6. Vous devez associer le VRID6 aux interfaces des deux nœuds de la configuration du cluster de secours actif. En effet, contrairement à une configuration de haute disponibilité, les ID d'interface diffèrent dans une configuration de cluster.

Pour ajouter un VRID6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
-  add vrid6 <ID>
-  show vrid6 <ID>
```

Pour lier le VRID6 à une interface à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `bind vrid6 <ID> -ifnum <interface_name><!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

Pour ajouter un VRID6 et le lier à des interfaces à l'aide de l'interface graphique

1. Naviguez **Système > Réseau > VMAC** et, sous l'onglet **VMAC6**, cliquez sur **Ajouter** .

2. Sur la page **Créer MAC6 virtuel**, spécifiez une valeur dans le champ **ID du routeur virtuel**, liez les interfaces dans la section **Associer les interfaces**, puis cliquez sur **Créer** .

```
> add vrid6 100
 Done
> bind vrid6 100 -ifnum 0/1/1 1/1/2 2/1/3
 Done
```

Services de surveillance dans un cluster à l'aide de la surveillance des chemins

August 20, 2021

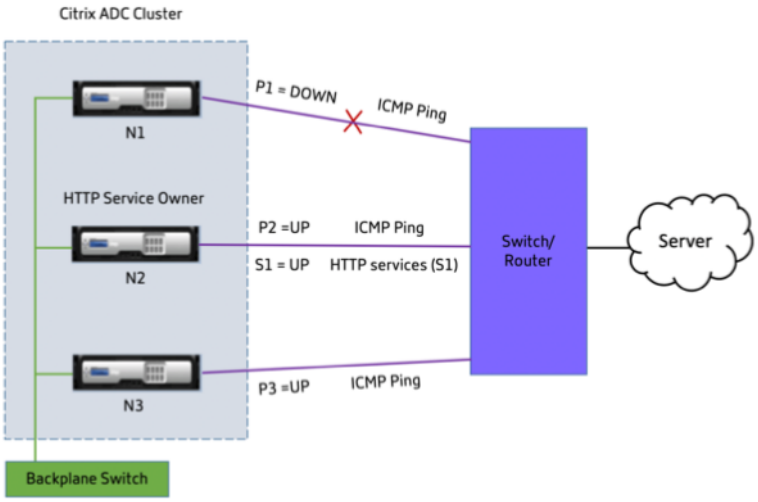
Dans une configuration de cluster, la propriété des services de surveillance est répartie entre les nœuds. Par conséquent, différents nœuds surveillent différents services. Le nœud qui surveille un service est appelé propriétaire du service. Seul le propriétaire du service sonde le serveur pour surveiller l'état des services qui lui sont affectés. Il communique en outre l'état des services à tous les autres nœuds du cluster. L'inconvénient de la surveillance distribuée est que la connectivité réseau et l'état de liaison entre tous les nœuds et le serveur n'est pas déterminé. Pour surmonter cet inconvénient, vous pouvez utiliser la surveillance du chemin.

> **Remarque**
>
> Vous ne pouvez pas sélectionner un nœud pour surveiller un service. La sélection des nœuds pour surveiller un service se fait via un mécanisme interne. Vous pouvez voir le nœud propriétaire pour surveiller les services à l'aide de la commande `show service <service name>` et `show serviceGroup <service group name>`.

La surveillance des chemins vérifie la connectivité réseau et l'état de la liaison entre un nœud et le service fourni par le serveur. Un nœud envoie des pings ICMP pour vérifier si le serveur est accessible ou non.

Fonctionnement de la surveillance des chemins

Prenons un exemple de cluster Citrix ADC composé de trois nœuds N1, N2 et N3. N2 est le propriétaire du service qui surveille l'état des services HTTP (S1). Il annonce l'état du service à d'autres nœuds du cluster. La surveillance des chemins est activée sur tous les nœuds du cluster, pour tous les services. Chaque nœud envoie uniquement un ping ICMP au serveur. Le propriétaire du service envoie à la fois la demande de service HTTP et un ping ICMP. Chaque nœud signale son état de surveillance de chemin au propriétaire du service.



Les deux paramètres suivants déterminent l'état de service d'un nœud :

- S = état de service annoncé par le propriétaire du service
- P = état de suivi du chemin de chaque nœud

Si un nœud peut atteindre un serveur ou non, détermine l'état de surveillance du chemin pour ce nœud.

Le tableau suivant présente l'état du service défini en fonction de l'état de surveillance du chemin, lorsque le paramètre PathMonitorInDV est activé ou désactivé.

Paramètre	État de surveillance des chemins	État du service
PathMonitorInDV = NO ; Est la configuration par défaut.	P1 = DOWN	S1 = DOWN
	P2 = UP	S1 = DOWN
	P3 = UP	S1 = DOWN
PathMonitorInv = OUI	P1 = DOWN	S1 = DOWN
	P2 = UP	S1 = UP
	P3 = UP	S1 = UP

Dans cet exemple, le propriétaire du service décide de l'état du service pour tous les nœuds en fonction du nœud dont l'état de surveillance du chemin est défini sur DOWN. Si l'état de surveillance du chemin d'accès pour l'un des nœuds est DOWN, le propriétaire du service définit l'état du service pour tous les nœuds comme étant DOWN. L'état du service pour tous les nœuds est défini sur UP uniquement si l'état de surveillance du chemin pour chacun des nœuds est UP.

Vous pouvez utiliser la surveillance des chemins d'accès pour les nœuds individuels en activant le paramètre PathMonitorIndv. Ce paramètre permet au propriétaire du service de définir l'état du service pour chaque nœud en fonction de l'état de surveillance du chemin d'accès de ce nœud respectif.

> **Remarque**
>
> Si le paramètre PathMonitorInDV est défini, certaines fonctionnalités telles que la persistance peuvent se briser.

Configuration de la surveillance des chemins

La surveillance des chemins est applicable à tous les services et groupes de services. Le paramètre de surveillance du chemin est désactivé par défaut.

Pour activer la surveillance des chemins d'accès pour les services/groupes de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <service name> <IP address> <service type> <port> [-
    pathMonitor <YES | NO>] [-pathMonitorIndv <YES | NO>]

add servicegroup <servicegroup name> <service type> [-pathMonitor <YES
    | NO>] [-pathMonitorIndv <YES | NO>]
<!--NeedCopy-->
```

Exemple :

```
add service s1 1.1.1.1 HTTP 80 -pathMonitor YES
add servicegroup sg_1 HTTP -pathMonitor YES

add service s1 1.1.1.1 HTTP 80 -pathMonitor YES -pathMonitorIndv YES
add servicegroup sg_1 HTTP -pathMonitor YES -pathMonitorIndv YES
<!--NeedCopy-->
```

Vous pouvez également définir le paramètre de surveillance du chemin à partir de la commande set, comme suit :

```
set service <service name> [-pathMonitor <YES | NO>] [-pathMonitorIndv
    <YES | NO>]
set servicegroup <servicegroup name> [-pathMonitor <YES | NO>] [-
    pathMonitorIndv <YES | NO>]
<!--NeedCopy-->
```


Exemple :

```
set service s1 -pathMonitor YES
set servicegroup sg_1 -pathMonitor YES


set service s1 -pathMonitorIndv YES
set servicegroup sg_1 -pathMonitorIndv NO
<!--NeedCopy-->
```

Pour activer la surveillance des chemins d'accès pour les services/groupes de services à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.

   Pour les groupes de services, accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services** .

2. Dans le volet **Services/Groupes** de services, sélectionnez un groupe de services/services dans la liste, puis double-cliquez pour l'ouvrir.
3. Sous l'onglet **Paramètres du service**, cliquez sur **Modifier** .
4. Sélectionnez **Suivi des chemins**.
5. Sélectionnez **Surveillance des chemins individuels**, si vous souhaitez l'appliquer, puis cliquez sur **OK**.

> **Remarque**
>
> Vous ne pouvez activer la surveillance des chemins individuels que si vous activez la surveillance des chemins.

Sauvegarde et restauration de la configuration du cluster

August 20, 2021

Vous pouvez sauvegarder l'état actuel d'un nœud de cluster Citrix ADC. Plus tard, vous pouvez utiliser les fichiers sauvegardés pour restaurer le nœud au même état de cluster. Par mesure de précaution, vous devez utiliser cette fonctionnalité avant d'effectuer une mise à niveau sur les nœuds du cluster.

Sauvegardez la configuration d'un cluster

Vous pouvez effectuer une sauvegarde de base ou complète en fonction des éléments suivants :

- Type de données à sauvegarder.
- Fréquence à laquelle vous créez une sauvegarde.
- **Sauvegarde basique.** Sauvegarde uniquement les fichiers de configuration. Vous pouvez effectuer ce type de sauvegarde fréquemment, car les fichiers qu'il sauvegarde changent constamment. Les fichiers sauvegardés sont répertoriés dans le tableau.

Répertoire

Sous-répertoire ou fichiers

/nsconfig/

- ns.conf
- Zebos.conf
- rc.netscaler
- snmpd.conf
- nsbefore.sh
- nsafter.sh
- inetd.conf
- ntp.conf
- syslog.conf
- newsyslog.conf
- crontab
- host.conf
- hôtes
- Ttys
- sshd_config
- httpd.conf
- surveillance
- rc.conf
- ssh_config
- heure locale
- question
- issue.net

/var/

- download/*
- log/wicmd.log
- wi/tomcat/webapps/*
- wi/tomcat/logs/*
- wi/tomcat/conf/catalina/localhost/*
- nslw.bin/etc/krb.conf

- nslw.bin/etc/krb.keytab
- netscaler/locdb/*
- lib/likewise/db/*
- vpn/bookmark/*
- netscaler/crl
- nstemplates/*
- learnt_data/*

/netscaler/

- custom.html
- vsr.html
- **Sauvegarde complète.** Outre les fichiers sauvegardés par une sauvegarde de base, une sauvegarde complète sauvegarde certains fichiers moins fréquemment mis à jour. Les fichiers sauvegardés lors de l'utilisation de l'option de sauvegarde complète sont répertoriés dans le tableau.

Répertoire

Sous-répertoire ou fichiers

/nsconfig/

- ssl/*
- licence/*
- fips/*

/var/

- netscaler/ssl/*
- wi/java_home/jre/lib/security/cacerts/*
- wi/java_home/lib/security/cacerts/*

> **Important**
>
> La sauvegarde et la restauration ne fonctionnent pas si CLAG est configuré sur une configuration de cluster SDX.

La sauvegarde est stockée sous la forme d'un fichier TAR compressé dans le répertoire /var/ns_sys_backup/. Pour éviter les problèmes dus à la non-disponibilité de l'espace disque, vous pouvez stocker un maximum de 50 fichiers de sauvegarde dans ce répertoire. Vous pouvez utiliser la commande rm system backup pour supprimer les fichiers de sauvegarde existants afin de créer davantage de sauvegardes.

Lorsque vous effectuez l'opération de sauvegarde sur un CLIP d'une configuration de cluster, des fichiers de sauvegarde sont créés sur chacun des nœuds de cluster.

Comment sauvegarder une configuration de cluster

Pour sauvegarder la configuration du cluster sur CLIP à l'aide de l'interface de ligne de commande Citrix ADC.

À l'invite de commandes, procédez comme suit :

- Enregistrez la configuration.

  ```
  save ns config<!--NeedCopy-->
  ```

- Créez le fichier de sauvegarde (de base ou complet).

  "'create system backup [][–level (basic | full)][-comment]

  ```
  1  **Exemple**
  2
  3  ```create system backup cluster-backup-1  -level basic<!--
       NeedCopy-->
  ```

La commande précédente crée un fichier TAR de sauvegarde sur chacun des nœuds de cluster avec le nom de fichier spécifié. Par exemple, le fichier Cluster-Backup-1.tgz est créé sur chacun des nœuds de cluster.

> **Remarque**
>
> Si le nom de fichier n'est pas spécifié, les fichiers TAR de sauvegarde sont créés sur chacun des nœuds de cluster avec la convention de dénomination suivante :
>
> - backup_<level>_<nsip_address of the cluster node 0>_<date-timestamp >.tgz<!--NeedCopy-->
> - backup_<level>_<nsip_address of the cluster node 1>_<date-timestamp >.tgz<!--NeedCopy-->
>
> Par exemple, sur une configuration de cluster à trois nœuds,
>
> - backup_<level>_<nsip_address of the cluster node 0>_<date-timestamp >.tgz<!--NeedCopy--> est créé sur le noeud 0
> - backup _<level>_<nsip_address of the cluster node 1>_<date-timestamp >.tgz<!--NeedCopy--> est créé sur le noeud 1
> - backup_<level>_<nsip_address of the cluster node 2>_<date-timestamp >.tgz<!--NeedCopy--> est créé sur le noeud 2

- Vérifiez les fichiers de sauvegarde créés sur CLIP.

  ```
  show system backup<!--NeedCopy-->
  ```


Restaurer une configuration de cluster

Lorsqu'un nœud de cluster devient défectueux, vous pouvez le remplacer par un nouveau nœud. Vous pouvez définir le nouveau nœud d'un cluster à l'aide d'un fichier de sauvegarde du nœud défectueux.

Par exemple, dans une configuration de cluster à trois nœuds, si node1 devient défectueux, vous pouvez remplacer ce nœud défectueux par un nouveau nœud en tant que node1. En utilisant l'opération de restauration, vous pouvez restaurer l'un des fichiers de sauvegarde du nœud défectueux sur le nouveau nœud.

> **Remarque**
>
> L'opération de restauration échoue si le fichier de sauvegarde est renommé ou si le contenu du fichier est modifié.

Comment faire pour restaurer un nœud de cluster

Pour restaurer un nœud de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

- Obtenez la liste des fichiers de sauvegarde disponibles sur CLIP.

  ```
  show system backup<!--NeedCopy-->
  ```

- Copiez le fichier tar de sauvegarde dans le répertoire /var/ns_sys_backup du nœud de cluster, qui doit être restauré.
- Ajoutez le fichier tar de sauvegarde à la mémoire du nœud du cluster en exécutant la commande suivante sur le nœud du cluster.

  "'add system backup

  ```
  **Exemple**

  ```add system backup CLUSTER-BACKUP-1.tgz<!--NeedCopy-->
  ```

  > **Remarque**
  >
  > La commande doit être exécutée sur le nœud de cluster pour être restaurée.

- Restaurez le nœud du cluster en spécifiant le fichier de sauvegarde.

  "'restore system backup

  ```
  **Exemple**

  ```restore system backup CLUSTER-BACKUP-1.tgz<!--NeedCopy-->
  ```


> **Remarque**
>
> La commande doit être exécutée sur le nœud de cluster pour être restaurée.

- Redémarrez le nœud du cluster.

  reboot

> **Remarque**
>
> La commande doit être exécutée sur le nœud de cluster pour être restaurée.

Mise à niveau ou rétrogradation du cluster Citrix ADC

August 20, 2021

Tous les nœuds d'un cluster Citrix ADC doivent exécuter la même version logicielle. Par conséquent, pour mettre à niveau ou rétrograder le cluster, vous devez mettre à niveau ou rétrograder chaque appliance Citrix ADC du cluster, un nœud à la fois.

Un nœud en cours de mise à niveau ou de rétrogradation n'est pas supprimé du cluster. Le nœud reste une partie du cluster et sert le trafic ininterrompu, sauf pour les temps d'arrêt lorsque le nœud redémarre après sa mise à niveau ou sa rétrogradation.

Toutefois, en raison de l'incompatibilité des versions logicielles entre les nœuds du cluster, la propagation de la configuration est désactivée sur le cluster. La propagation de la configuration n'est activée qu'après que tous les nœuds de cluster sont de la même version. Étant donné que la propagation de la configuration est désactivée lors de la mise à niveau lors de la rétrogradation d'un cluster, vous ne pouvez pas effectuer de configurations via l'adresse IP du cluster pendant cette période.

> **Important**
>
> - Dans une configuration de cluster dont le paramètre global de connexion maximale (MaxConn) est défini sur une valeur différente de zéro, les connexions CLIP peuvent échouer si l'une des conditions suivantes est remplie :
>
> ```
> 1 - Upgrading the setup from Citrix ADC 13.0 76.x build to
>     Citrix ADC 13.0 79.x build.
> 2 - Restarting the CCO node in a cluster setup running Citrix
>     ADC 13.0 76.x build.
> ```
>
> Solutions :
>
> ```
> 1 \- Avant de mettre à niveau une configuration de cluster de
>     Citrix ADC 13.0 76.x vers la version Citrix ADC 13.0 79.x,
> ```



```
    le paramétre global de connexion maximale (MaxConn) doit ê
    tre défini sur zéro. Aprés la mise à niveau de la
    configuration, vous pouvez définir le paramétre MaxConn sur
    la valeur souhaitée, puis enregistrer la configuration.
2 \-  La version Citrix ADC 13.0 76.x n'est pas adaptée aux
    configurations de cluster. Citrix recommande de ne pas
    utiliser la version Citrix ADC 13.0 76.x pour une
    configuration de cluster.
```

- Dans une configuration de cluster, une appliance Citrix ADC peut se bloquer lorsque :

```
1 -  upgrading the setup from Citrix ADC 13.0 47.x or 13.0 52.x
    build to a later build, or
2 -  upgrading the setup to Citrix ADC 13.0 47.x or 13.0 52.x
    build
```

Solution : Pendant le processus de mise à niveau, effectuez les opérations suivantes :

```
1 \-  Désactivez tous les nœuds de cluster, puis mettez à niveau
    chaque nœud de cluster.
2 \-  Activez tous les nœuds de cluster aprés la mise à niveau de
     tous les nœuds.
```

Points à noter avant de mettre à niveau ou de rétrograder le cluster

- Vous ne pouvez pas ajouter de nœuds de cluster lors de la mise à niveau ou de la rétrogradation de la version du logiciel de cluster.
- Vous pouvez effectuer des configurations au niveau des nœuds via l'adresse NSIP de nœuds individuels. Assurez-vous d'effectuer les mêmes configurations sur tous les nœuds pour les maintenir synchronisés.
- Vous ne pouvez pas exécuter la `start nstrace` commande à partir de l'adresse IP du cluster lorsque le cluster est mis à niveau. Toutefois, vous pouvez obtenir la trace de nœuds individuels en effectuant cette opération sur des nœuds de cluster individuels à l'aide de leur adresse NSIP.
- La version Citrix ADC 13.0 76.x n'est pas adaptée aux configurations de cluster. Citrix recommande de ne pas utiliser la version Citrix ADC 13.0 76.x pour une configuration de cluster.
- Les versions Citrix ADC 13.0 47.x et 13.0 52.x ne conviennent pas à une configuration de cluster. C'est parce que les communications inter-nœuds ne sont pas compatibles dans ces versions.
- Lors de la mise à niveau d'un cluster, il est possible que les nœuds mis à niveau aient des fonctionnalités supplémentaires activées qui ne sont pas disponibles sur les nœuds qui ne sont pas encore mis à niveau. Cela entraîne un avertissement d'incompatibilité de licence pendant

la mise à niveau du cluster. Cet avertissement est automatiquement résolu lorsque tous les nœuds de cluster sont mis à niveau.

> **Important**
>
> - Citrix vous recommande d'attendre que le nœud précédent devienne actif avant de mettre à niveau ou de rétrograder le nœud suivant.
> - Citrix recommande que le nœud de configuration du cluster soit mis à niveau/rétrogradé en dernier afin d'éviter plusieurs déconnexions des sessions IP de cluster.

Pour effectuer une mise à niveau ou une rétrogradation du logiciel des nœuds de cluster

1. Assurez-vous que le cluster est stable et que les configurations sont synchronisées sur tous les nœuds.
2. Accédez à chaque nœud via son adresse NSIP et effectuez les opérations suivantes :
   - Mettez à niveau ou rétrogradez le nœud du cluster. Pour obtenir des informations détaillées sur la mise à niveau et la rétrogradation du logiciel d'une appliance, consultez Mettre à niveau et rétrograder une appliance NetScaler.
   - Enregistrez les configurations.
   - Redémarrez l'appliance.
3. Répétez l'étape 2 pour chacun des autres nœuds de cluster.

Opérations prises en charge sur des nœuds de cluster individuels

January 21, 2021

En règle générale, les appliances Citrix ADC qui font partie d'un cluster ne peuvent pas être configurées individuellement à partir de leur adresse NSIP. Cependant, certaines opérations constituent une exception à cette règle. Ces opérations, lorsqu'elles sont exécutées à partir de l'adresse NSIP, ne sont pas propagées vers d'autres nœuds de cluster.

Les opérations sont les suivantes :

- cluster instance (set | rm | enable | disable)
- cluster node (set | rm)
- ns trace (début | show | stop)
- interface (set | enable | disable)
- route (add | rm | set | unset)

- ARP (ajouter | rm | envoyer -all)
- force cluster sync
- sync cluster files
- désactiver la synchronisation NTP
- save ns config
- reboot
- shutdown

Par exemple, lorsque vous exécutez la commande `disable interface 1/1/1` à partir de l'adresse NSIP d'un nœud de cluster, l'interface est désactivée uniquement sur ce nœud. Comme la commande n'est pas propagée, l'interface 1/1/1 reste activée sur tous les autres nœuds de cluster.

Prise en charge de cluster hétérogène

August 20, 2021

L'appliance Citrix ADC prend en charge un cluster hétérogène dans un déploiement de cluster. Un cluster hétérogène couvre des nœuds de différents matériels Citrix ADC et vous pouvez avoir une combinaison de différentes plates-formes dans le même cluster.

> **Important**
>
> La formation ou la prise en charge d'un cluster hétérogène est possible et limitée uniquement aux plates-formes matérielles MPX.

La prise en charge et la formation du cluster hétérogène dépendent de certains modèles Citrix ADC. Le tableau suivant répertorie les plates-formes prises en charge dans la formation d'un cluster hétérogène, avec un nombre égal de moteurs de paquets.

Nombre de moteurs de paquets	Plates-formes matérielles MPX	Plates-formes matérielles MPX prises en charge pour former un cluster hétérogène
5	MPX 11500	MPX 14020
7	MPX 11515	MPX 14040
9	MPX 11530	MPX 14060

Le tableau suivant répertorie les plates-formes prises en charge dans la formation d'un cluster hétérogène, avec un nombre inégal de moteurs de paquets.

Plates-formes matérielles	Plates-formes matérielles prises en charge pour former un cluster hétérogène
MPX 150XX	MPX 140XX

Pour plus d'informations sur la façon de former un déploiement de cluster hétérogène des appliances Citrix ADC MPX avec le nombre différent de moteurs de paquets sur différents chipsets SSL, consultez la section **Déploiements de clusters hétérogènes** de la configuration de déchargement SSL.

> **Remarque**
>
> Avant la version 13.0 build 47.x, si vous exécutez la commande « jointure cluster » à partir du nœud qui a un nombre inégal de moteurs de paquets, le message d'erreur suivant s'affiche : « Incompatibilité dans le nombre de PPE actifs entre CCO et nœud local ».

Points à noter

1. Le paramètre UC de gestion supplémentaire doit être le même sur tous les nœuds du cluster.
2. Le nœud nouvellement ajouté doit avoir la même capacité sur les plans de données et le fond de panier, que celle des nœuds de cluster existants.
3. S'il existe des périphériques de plates-formes mixtes prenant en charge différents chiffrements, alors le cluster se mettrait d'accord sur une liste de chiffrement commune.

FAQ

August 20, 2021

Liste de la FAQ sur la mise en cluster.

Combien d'appliances Citrix ADC peuvent être incluses dans un seul cluster Citrix ADC ?

Un cluster Citrix ADC peut inclure une appliance ou jusqu'à 32 appliances matérielles ou virtuelles Citrix ADC nCore. Chacun de ces nœuds doit satisfaire aux critères spécifiés dans Prérequis pour les nœuds de cluster.

Un dispositif Citrix ADC peut-il faire partie de plusieurs clusters ?

Non. Une appliance Citrix ADC ne peut appartenir qu'à un cluster.

Qu'est-ce qu'une adresse IP de cluster ? Quel est son masque de sous-réseau ?

L'adresse IP du cluster est l'adresse de gestion d'un cluster Citrix ADC. Toutes les configurations de cluster doivent être effectuées en accédant au cluster via cette adresse. Le masque de sous-réseau de l'adresse IP du cluster est fixé à 255.255.255.255.

Comment puis-je faire un nœud de cluster spécifique en tant que coordinateur de configuration de cluster ?

Pour définir manuellement un nœud spécifique comme coordinateur de configuration de cluster, vous devez définir la priorité de ce nœud sur la valeur numérique la plus basse (priorité la plus élevée). Pour comprendre, considérons un cluster avec trois nœuds qui ont les priorités suivantes :

n1 - 29, n2 - 30, n3 - 31

Ici, n1 est le coordinateur de configuration. Si vous voulez faire de n2 le coordinateur de configuration, vous devez définir sa priorité sur une valeur inférieure à n1, par exemple 28. Lors de l'enregistrement de la configuration, n2 devient le coordinateur de configuration.

> **Remarque**
>
> n2 avec sa valeur de priorité d'origine 30 devient le coordinateur de configuration lorsque n1 tombe en panne. Le nœud avec la valeur de priorité la plus basse suivante est sélectionné au cas où le coordinateur de configuration tombe en panne.

Pourquoi les interfaces réseau d'un cluster sont-elles représentées en notation 3-tuple (n/u/c) au lieu de la notation 2-tuple régulière (u/c) ?

Lorsqu'une appliance Citrix ADC fait partie d'un cluster, vous devez être en mesure d'identifier le nœud auquel appartient l'interface. Par conséquent, la convention de dénomination de l'interface réseau pour les nœuds de cluster est modifiée de u/c à n/u/c, où n indique l'ID du nœud.

Comment puis-je définir le nom d'hôte pour un nœud de cluster ?

Le nom d'hôte d'un nœud de cluster doit être spécifié en exécutant la commande **set ns hostname** via l'adresse IP du cluster. Par exemple, pour définir le nom d'hôte du nœud de cluster avec l'ID 2, la commande est la suivante :

set ns hostname hostName1 -**ownerNode** 2

Puis-je détecter automatiquement les appliances Citrix ADC afin de pouvoir les ajouter à un cluster ?

Oui. L'utilitaire de configuration vous permet de découvrir les appliances présentes dans le même sous-réseau que l'adresse NSIP du coordinateur de configuration. Pour plus d'informations, voir Découvrir les appliances NetScaler.

La capacité de service de trafic d'un cluster est-elle affectée si un nœud est supprimé ou désactivé, redémarré ou arrêté ou rendu inactif ?

Oui. Lorsque l'une de ces opérations est effectuée sur un nœud actif du cluster, le cluster dispose d'un nœud de moins pour servir le trafic. En outre, les connexions existantes sur ce nœud sont terminées.

J'ai plusieurs appareils autonomes, dont chacun a des configurations différentes. Puis-je les ajouter à un seul cluster ?

Oui. Vous pouvez ajouter des appliances ayant des configurations différentes à un seul cluster. Toutefois, lorsque l'appliance est ajoutée au cluster, les configurations existantes sont effacées. Pour utiliser les configurations disponibles sur chacune des appliances individuelles, vous devez :

1. Créez un fichier*.conf unique pour toutes les configurations.
2. Modifiez le fichier de configuration pour supprimer les entités qui ne sont pas prises en charge dans un environnement de cluster.
3. Mettez à jour la convention de dénomination des interfaces du format 2-tuple (u/c) au format 3-tuple (n/u/c).
4. Appliquez les configurations au nœud coordinateur de configuration du cluster à l'aide de la commande batch.

Puis-je migrer les configurations d'une appliance Citrix ADC autonome ou d'une installation HA vers la configuration en cluster ?

Non. Lorsqu'un nœud est ajouté à une configuration en cluster, ses configurations sont implicitement effacées à l'aide de la commande **clear ns config** (avec l'option **étendue**). En outre, les adresses SNIP et toutes les configurations de VLAN (à l'exception du VLAN par défaut et du NSVLAN) sont effacées. Par conséquent, il est recommandé de sauvegarder les configurations avant d'ajouter l'appliance à un cluster. Avant d'utiliser le fichier de configuration sauvegardé pour le cluster, vous devez :

1. Modifiez le fichier de configuration pour supprimer les entités qui ne sont pas prises en charge dans un environnement de cluster.
2. Mettez à jour la convention de dénomination des interfaces du format à deux tuples (x/y) au format à trois tuples (x/y/z).

3. Appliquez les configurations au nœud coordinateur de configuration du cluster à l'aide de la commande **batch**.

Les interfaces de fond de panier fait-elles partie des VLAN L3 ?

Oui, par défaut, les interfaces de backplane sont présentes sur tous les VLAN L3 configurés sur le cluster.

Comment puis-je configurer un cluster qui inclut des nœuds provenant de différents réseaux ?

> **Remarque**
>
> Prise en charge à partir de NetScaler 11.0.

Un cluster qui inclut des nœuds provenant de différents réseaux est appelé cluster L3 (parfois appelé cluster en mode INC). Dans un cluster L3, tous les nœuds appartenant à un réseau unique doivent être regroupés dans un seul groupe de nœuds. Par conséquent, si un cluster comprend deux nœuds provenant chacun de trois réseaux différents, vous devez créer 3 groupes de nœuds (un pour chaque réseau) et associer chacun de ces groupes de nœuds aux nœuds qui appartiennent à ce réseau. Pour plus d'informations sur la configuration, reportez-vous aux étapes de configuration d'un cluster.

Comment puis-je configurer/désinstaller le NSVLAN sur un cluster ?

Faites l'une des opérations suivantes :

- Pour rendre le NSVLAN disponible dans un cluster, assurez-vous que chaque appliance a le même NSVLAN configuré avant d'être ajouté à un cluster.
- Pour supprimer le NSVLAN d'un nœud de cluster, supprimez d'abord le nœud du cluster, puis supprimez le NSVLAN de l'appliance.

J'ai un cluster configuré où certains nœuds Citrix ADC ne sont pas connectés au réseau externe. Le cluster peut-il encore fonctionner normalement ?

Oui. Le cluster prend en charge un mécanisme appelé linksets, qui permet aux nœuds non connectés de servir le trafic en utilisant les interfaces des nœuds connectés. Les nœuds non connectés communiquent avec les nœuds connectés via le backplane du cluster. Pour plus d'informations, voir Utilisation de jeux de liens.

Comment les déploiements nécessitant le transfert basé sur Mac (MBF) peuvent-ils être pris en charge dans une configuration en cluster ?

Les déploiements qui utilisent MBF doivent utiliser des jeux de liens. Pour plus d'informations, voir Utilisation de jeux de liens.

Puis-je exécuter des commandes à partir de l'adresse NSIP d'un nœud de cluster ?

Non. L'accès aux nœuds de cluster individuels via les adresses NSIP est en lecture seule. Par conséquent, lorsque vous vous connectez à l'adresse NSIP d'un nœud de cluster, vous ne pouvez afficher que les configurations et les statistiques. Vous ne pouvez rien configurer. Toutefois, il existe certaines opérations que vous pouvez exécuter à partir de l'adresse NSIP d'un nœud de cluster. Pour plus d'informations, voir Opérations prises en charge sur des nœuds individuels.

Puis-je désactiver la propagation de la configuration entre les nœuds de cluster ?

Non, vous ne pouvez pas désactiver explicitement la propagation des configurations de cluster entre les nœuds de cluster. Toutefois, lors d'une mise à niveau ou d'une mise à niveau logicielle, une erreur d'incompatibilité de version peut automatiquement désactiver la propagation de la configuration.

Puis-je modifier l'adresse NSIP ou le NSVLAN d'une appliance Citrix ADC lorsqu'elle fait partie du cluster ?

Non. Pour effectuer de telles modifications, vous devez d'abord supprimer l'appliance du cluster, effectuer les modifications, puis ajouter l'appliance au cluster.

Le cluster Citrix ADC prend-il en charge les VLAN L2 et L3 ?

Oui. Un cluster prend en charge les VLAN entre les nœuds de cluster. Les VLAN doivent être configurés sur l'adresse IP du cluster.

- **VLAN L2.** Vous pouvez créer un VLAN de couche 2 en liant des interfaces appartenant à différents nœuds du cluster.
- **VLAN L3.** Vous pouvez créer un VLAN de couche 3 en liant des adresses IP appartenant à différents nœuds du cluster. Les adresses IP doivent appartenir au même sous-réseau. Assurez-vous que l'un des critères suivants est satisfait. Sinon, les liaisons VLAN L3 peuvent échouer.
  - Tous les nœuds ont une adresse IP sur le même sous-réseau que celui lié au VLAN.
  - Le cluster a une adresse IP répartie et le sous-réseau de cette adresse IP est lié au VLAN.

Lorsque vous ajoutez un nœud à un cluster qui n'a repéré que des adresses IP repéré, la synchronisation se produit avant que les adresses IP ponctuées ne soient affectées à ce nœud. Dans de tels cas,

les liaisons VLAN L3 peuvent être perdues. Pour éviter cette perte, ajoutez une IP par répartition ou ajoutez les liaisons VLAN L3 sur le NSIP du nœud nouvellement ajouté.

Comment puis-je configurer SNMP sur un cluster Citrix ADC ?

SNMP surveille le cluster et tous les nœuds du cluster de la même manière qu'une appliance autonome. La seule différence est que SNMP sur un cluster doit être configuré via l'adresse IP du cluster. Lors de la génération d'interruptions spécifiques au matériel, deux autres varbinds sont inclus pour identifier le nœud du cluster : l'ID du nœud et l'adresse NSIP du nœud.

Quels détails dois-je disposer lorsque je contacte le support technique pour des problèmes liés au cluster ?

L'appliance Citrix ADC fournit une commande **show techsupport -scope cluster** qui extrait les données de configuration, les informations statistiques et les journaux de tous les nœuds de cluster. Exécutez cette commande sur l'adresse IP du cluster.

La sortie de cette commande est enregistrée dans un fichier nommé *collector_cluster_<nsip_CCO>_P_<date-timestamp>.tar.gz* qui est disponible dans le répertoire */var/tmp/support/cluster/* du coordinateur de configuration.

Envoyez cette archive à l'équipe de support technique pour déboguer le problème.

Puis-je utiliser des adresses IP par bandes comme Gateway par défaut des serveurs ?

Dans les déploiements de cluster, assurez-vous que la passerelle par défaut du serveur pointe vers une adresse IP répartie (si vous utilisez une adresse IP appartenant à Citrix ADC). Par exemple, dans le cas de déploiements LB avec USIP activé, la passerelle par défaut doit être une adresse SNIP par répartition.

Puis-je afficher les configurations de routage d'un nœud de cluster spécifique à partir de l'adresse IP du cluster ?

Oui. Vous pouvez afficher et effacer les configurations spécifiques à un nœud en spécifiant le nœud propriétaire lorsque vous entrez dans l'interpréteur de commandes VTYSH.

Par exemple, pour afficher la sortie d'une commande sur les nœuds 0 et 1, la commande est la suivante :

```
\> vtysh
ns# owner-node 0 1
ns(node-0 1)\# show cluster state
ns(node-0 1)\# exit-cluster-node
```



```
5  ns\#
```

Comment puis-je spécifier le nœud pour lequel je veux définir la priorité système LACP ?

> **Remarque**
>
> Prise en charge à partir de NetScaler 10.1.

Dans un cluster, vous devez définir ce nœud comme nœud propriétaire à l'aide de la commande **set lacp** .

Par exemple : Pour définir la priorité système LACP pour un nœud avec ID 2 :

```
set lacp -sysPriority 5 -ownerNode 2<!--NeedCopy-->
```

Comment les tunnels IP sont-ils configurés dans une configuration de cluster ?

> **Remarque**
>
> Prise en charge à partir de NetScaler 10.1.

La configuration des tunnels IP dans un cluster est identique à celle d'une appliance autonome. La seule différence est que dans une configuration de cluster, l'adresse IP locale doit être une adresse SNIP par répartition.

Comment puis-je ajouter un jeu d'interface de basculement (FIS) sur les nœuds d'un cluster Citrix ADC ?

> **Remarque**
>
> Prise en charge à partir de NetScaler 10.5.

Sur l'adresse IP du cluster, spécifiez l'ID du nœud du cluster sur lequel le FIS doit être ajouté, à l'aide de la commande suivante :

```
add fis <name> -ownerNode <nodeId>
```

> **Remarques**
>
> - Le nom FIS de chaque nœud de cluster doit être unique.
> - Un canal LA de cluster peut être ajouté à un FIS. Assurez-vous que le canal LA du cluster dispose d'une interface locale en tant qu'interface membre.

Pour plus d'informations sur FIS, voir Configuration du jeu d'interfaces de basculement.

Comment les profils réseau sont-ils configurés dans une configuration de cluster ?

> **Remarque**
>
> Prise en charge à partir de NetScaler 10.5.

Vous pouvez lier des adresses IP spotted à un profil net. Ce profil réseau peut alors être lié à un serveur ou service virtuel d'équilibrage de charge repéré (défini à l'aide d'un groupe de nœuds). Les recommandations suivantes doivent être suivies, faute de quoi, les configurations de profil réseau ne sont pas respectées et les paramètres USIP/USNIP sont utilisés :

> **Remarque**
>
> - Si le paramètre **strict** du groupe de nœuds est défini sur **Oui**, le profil réseau doit contenir au moins une adresse IP de chaque membre du groupe de nœuds.
> - Si le paramètre **strict** du groupe de nœuds est défini sur **Non**, le profil réseau doit inclure au moins une adresse IP de chacun des nœuds de cluster.

Comment puis-je configurer des WIonNS dans une configuration de cluster ?

> **Remarque**
>
> Prise en charge à partir de NetScaler 11.0 Build 62.x.

Pour utiliser des WIONsWIonNS sur un cluster, vous devez effectuer les opérations suivantes :

1. Assurez-vous que le package Java et le package WI sont présents dans le même répertoire sur tous les nœuds de cluster.
2. Créez un serveur virtuel d'équilibrage de charge dont la persistance est configurée.
3. Créez des services avec des adresses IP comme adresse NSIP de chacun des nœuds de cluster que vous souhaitez servir le trafic WI. Cette étape ne peut être configurée qu'à l'aide de l'interface de ligne de commande Citrix ADC.
4. Liez les services au serveur virtuel d'équilibrage de charge.

> **Remarque**
>
> Si vous utilisez WIonNS via une connexion VPN, assurez-vous que le serveur virtuel d'équilibrage de charge est défini comme WIHOME.

Le canal LA de cluster peut-il être utilisé pour l'accès à la gestion ?

Non. L'accès de gestion à un nœud de cluster ne doit pas être configuré sur un canal LA de cluster (par exemple, CLA/1) ou ses interfaces membres. C'est parce que lorsque le nœud est INACTIF, l'interface LA du cluster correspondante est marquée comme hors tension, et perd donc l'accès à la gestion.

Comment les nœuds de cluster communiquent entre eux et quels sont les différents types de trafic qui traversent le fond de panier ?

Un backplane est un ensemble d'interfaces dans lequel une interface de chaque nœud est connectée à un commutateur commun, appelé commutateur de backplane de cluster. Les différents types de trafic qui traversent un fond de panier, qui est utilisé par la communication entre nœuds sont :

- Messagerie de noeud à noeud (NNM)
- Circulation orientée
- Propagation et synchronisation de la configuration

Chaque nœud du cluster utilise une adresse spéciale de commutateur de backplane de cluster MAC pour communiquer avec d'autres nœuds via le backplane. Le MAC spécial du cluster est de la forme : **0x02 0x00 0x6F**<cluster_id> <node_id> <reserved>, où <cluster_id> est l'ID d'instance de cluster. Le <node_id> est le numéro de nœud de l'appliance Citrix ADC qui est ajouté à un cluster.

> **Remarque**
>
> La quantité de trafic qui est gérée par un fond de panier a une surcharge CPU négligeable.

Qu'est-ce qui est routé sur le tunnel GRE pour le cluster de couche 3 ?

Seul le trafic de données dirigé passe par le tunnel GRE. Les paquets sont dirigés par le tunnel GRE vers le nœud de l'autre sous-réseau.

Comment les messages NNM (messagerie nœud à nœud) et les pulsations de cœur sont échangés, et comment sont-ils routés ?

Le NNM, les messages de pulsation et le protocole de cluster sont du trafic non dirigé. Ces messages ne sont pas envoyés par le tunnel, mais ils sont acheminés directement.

Quelles sont les recommandations MTU lorsque les trames Jumbo sont activées pour le trafic en tunnel de cluster de couche 3 ?

Voici les recommandations de cluster de couche 3 de Jumbo MTU sur tunnel GRE :

- Le MTU Jumbo peut être configuré entre les nœuds de cluster sur le chemin L3 pour prendre en charge la surcharge du tunnel GRE.
- La fragmentation ne se produit pas pour les paquets pleine taille qui doivent être piloté.
- La direction du trafic continue de fonctionner même si les cadres Jumbo ne sont pas autorisés, mais avec plus de frais généraux en raison de la fragmentation.

Comment la clé de hachage globale est générée et partagée sur tous les nœuds ?

Le `rsskey` pour une appliance autonome est généré au moment du démarrage. Dans une configuration de cluster, le premier nœud contient le `rsskey` du cluster. Chaque nouveau nœud se joignant au cluster synchronise le `rsskey`.

Quel est le besoin de `set rsskeytype -rsskey symmetric` commande pour `*:*`, USIP on, `useproxyport` off, topologies ?

Il n'est pas spécifique à un cluster, s'applique également à une appliance autonome. Avec USIP ON et l'utilisation du port proxy désactivé, symétrique `rsskey` réduit à la fois la direction Core to Core (C2C) et la direction nœud à nœud.

Quels sont les facteurs qui contribuent au changement du nœud CCO ?

Le premier nœud ajouté pour former une configuration de cluster devient le nœud du coordinateur de configuration (CCO). Les facteurs suivants contribuent à modifier le nœud CCO dans la configuration du cluster :

- Lorsque le nœud CCO actuel est supprimé de la configuration du cluster
- Lorsque le nœud CCO actuel se bloque
- Lorsque la priorité du nœud non-CCO est modifiée (priorité inférieure a priorité plus élevée)
- Dans des conditions dynamiques comme, accessibilité du réseau entre les nœuds
- Lorsqu'il y a des changements dans les états de noeud (actifs, de secours et passifs). Les nœuds actifs sont préférés en tant que CCO.
- Lorsqu'il y a un changement de configuration et que le nœud ayant la configuration la plus récente est préféré en tant que CCO.

Dépannage du cluster Citrix ADC

January 21, 2021

Si une défaillance se produit dans un cluster Citrix ADC, la première étape du dépannage consiste à obtenir des informations sur l'instance de cluster. Vous pouvez obtenir les informations en exécutant les `show cluster node nodeId` commandes `show cluster instance clId` et sur les nœuds de cluster respectivement.

Si vous ne parvenez pas à trouver le problème en utilisant les deux approches ci-dessus, vous pouvez utiliser l'une des méthodes suivantes :

- **Isolez la source de l'échec.** Essayez de contourner le cluster pour atteindre le serveur. Si la tentative réussit, le problème est probablement lié à la configuration du cluster.

- **Vérifiez les commandes récemment exécutées.** Exécutez la commande history pour vérifier les configurations récentes effectuées sur le cluster. Vous pouvez également consulter le fichier ns.conf pour vérifier les configurations qui ont été implémentées.
- **Vérifiez les fichiers ns.log.** Utilisez les fichiers journaux, disponibles dans le répertoire /var/log/ de chaque nœud, pour identifier les commandes exécutées, l'état des commandes et les changements d'état.
- **Vérifiez les fichiers newnslog.** Utilisez les `newnslog` fichiers, disponibles dans le répertoire /var/nslog/ de chaque nœud, pour identifier les événements qui se sont produits sur les nœuds de cluster. Vous pouvez afficher plusieurs `newnslog` fichiers sous la forme d'un seul fichier, en copiant les fichiers dans un seul répertoire, puis en exécutant la commande suivante :

```
nsconmsg -K newnslog-node<id> -K     newnslog.node<id> -d current
```

Si vous ne parvenez toujours pas à résoudre le problème, vous pouvez essayer de suivre les paquets sur le cluster ou utiliser la `techsupport -scope cluster` commande show. Vous pouvez utiliser la commande pour envoyer le rapport à l'équipe de support technique.

Suivi des paquets d'un cluster Citrix ADC

August 20, 2021

Le système d'exploitation Citrix ADC fournit un utilitaire appelé *ns trace* pour obtenir un vidage des paquets reçus et envoyés par une appliance. L'utilitaire stocke les paquets dans des fichiers de suivi. Vous pouvez utiliser ces fichiers pour déboguer des problèmes dans le flux de paquets vers les nœuds de cluster. Les fichiers de suivi doivent être affichés avec l'application Wireshark.

Certains aspects saillants de l'utilitaire ns trace sont les suivants :

- Peut être configuré pour tracer les paquets de manière sélective à l'aide d'expressions classiques et d'expressions par défaut.
- Peut capturer la trace dans plusieurs formats : ns trace format (.cap) et format de vidage TCP (.pcap).
- Peut agréger les fichiers de trace de tous les nœuds de cluster sur le coordinateur de configuration.
- Peut fusionner plusieurs fichiers de trace en un seul fichier de trace (uniquement pour les fichiers .cap).

Vous pouvez utiliser l'utilitaire de trace ns à partir de la ligne de commande Citrix ADC ou du shell Citrix ADC.

Pour suivre les paquets d'une appliance autonome

Exécutez la commande start ns trace sur l'appliance. La commande crée des fichiers de trace dans le répertoire /var/nstrace/<date-timestamp>. Les noms des fichiers de trace sont de la forme nstrace<id\ >.cap.

Vous pouvez afficher l'état en exécutant la commande show ns trace. Vous pouvez arrêter le suivi des paquets en exécutant la commande stop ns trace.

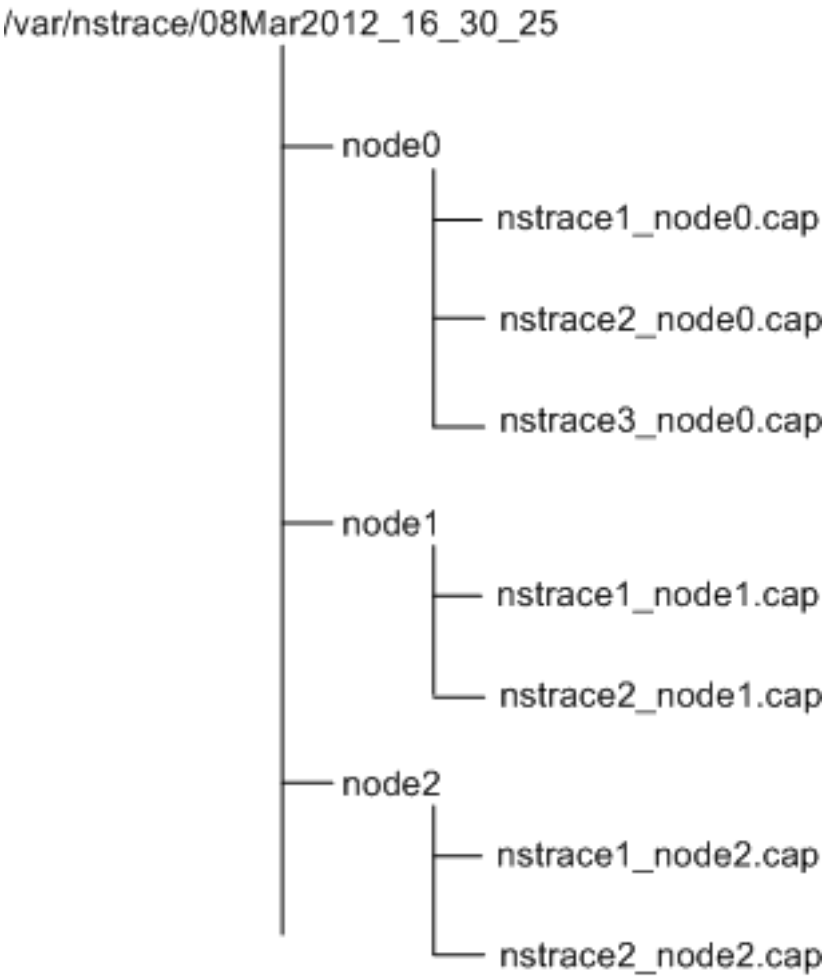
> **Remarque**
>
> Vous pouvez également exécuter l'utilitaire de trace ns à partir du shell Citrix ADC en exécutant le fichier
> nstrace.sh. Toutefois, il est recommandé d'utiliser l'utilitaire de trace ns via l'interface de ligne de commande Citrix ADC.

Pour suivre les paquets d'un cluster

Vous pouvez suivre les paquets sur tous les nœuds de cluster et obtenir tous les fichiers de trace sur le coordinateur de configuration.

Exécutez la commande start ns trace sur l'adresse IP du cluster. La commande est propagée et exécutée sur tous les nœuds du cluster. Les fichiers de trace sont stockés dans des nœuds de cluster individuels dans le répertoire /var/nstrace/<date-timestamp>. Les noms des fichiers de trace sont de la forme nstrace<id>_node<id\ >.cap.

Vous pouvez utiliser les fichiers de trace de chaque nœud pour déboguer les opérations des nœuds. Mais si vous voulez que les fichiers de trace de tous les nœuds de cluster se trouvent dans un seul emplacement, vous devez exécuter la commande stop ns trace sur l'adresse IP du cluster. Les fichiers de trace de tous les nœuds sont téléchargés sur le coordinateur de configuration du cluster dans le répertoire /var/nstrace/<date-timestamp> comme suit :



Fusionner plusieurs fichiers de trace

Vous pouvez préparer un fichier unique à partir des fichiers de trace (pris en charge uniquement pour. Fichiers Cap) obtenus à partir des nœuds de cluster. Les fichiers de trace uniques vous donnent une vue cumulative de la trace des paquets de cluster. Les entrées de suivi dans le fichier de suivi unique sont triées en fonction de l'heure à laquelle les paquets ont été reçus sur le cluster.

Pour fusionner les fichiers de trace, dans le shell Citrix ADC, tapez :

```
1 > nstracemerge.sh -srcdir \<DIR\> -dstdir \<DIR\> -filename \<name\> -
    filesize \<num\>
```

Où,

- `srcdir` est le répertoire à partir duquel les fichiers de trace sont fusionnés. Tous les fichiers de suivi de ce répertoire sont fusionnés en un seul fichier.
- `dstdir` est le répertoire où le fichier de trace fusionné est créé.
- `Filename` est le nom du fichier de trace qui est créé.

- `Filesize` est la taille du fichier de trace.

Exemples

Voici quelques exemples d'utilisation de l'utilitaire de trace ns pour filtrer les paquets.

- Pour suivre les paquets sur les interfaces de backplane de trois nœuds :

  Utilisation d'expressions classiques :

```
1   > start nstrace -filter "INTF == 0/1/1 && INTF == 1/1/1 && INTF
      == 2/1/1"
```

  Utilisation des expressions par défaut :

```
1   > start nstrace -filter "CONNECTION.INTF.EQ("0/1/1") &&
      CONNECTION.INTF.EQ("1/1/1") && CONNECTION.INTF.EQ("2/1/1")"
```

- Pour suivre les paquets à partir d'une adresse IP source 10.102.34.201 ou d'un système dont le port source est supérieur à 80 et le nom de service n'est pas "s1" :

  Utilisation d'expressions classiques

```
1   > start nstrace -filter "SOURCEIP == 10.102.34.201 || (SVCNAME !=
      s1 && SOURCEPORT > 80)"
```

  Utilisation d'expressions par défaut

```
1   > start nstrace -filter "CONNECTION.SRCIP.EQ(10.102.34.201) || (
      CONNECTION.SVCNAME.NE("s1") && CONNECTION.SRCPORT.GT(80))"
```

> **Remarque**
>
> Pour plus d'informations sur les filtres utilisés dans ns trace, voir ns trace.

Capture des clés de session SSL lors d'une trace

Lorsque vous exécutez la commande « start ns trace », vous pouvez définir le nouveau `capsslkeys` paramètre pour capturer les clés principales SSL pour toutes les sessions SSL. Si vous incluez ce paramètre, un fichier nommé nstrace.sslkeys est généré avec la trace des paquets. Ce fichier peut être importé dans Wireshark pour déchiffrer le trafic SSL dans le fichier de trace correspondant.

Cette fonctionnalité est similaire aux navigateurs Web qui exportent des clés de session qui peuvent ultérieurement être importées dans Wireshark pour décrypter le trafic SSL.

Avantages de l'utilisation des clés de session SSL

Voici les avantages de l'utilisation des clés de session SSL :

1. Génère des fichiers de trace plus petits qui n'incluent pas les paquets supplémentaires créés par le mode SSLPLAIN de capture.
2. Permet d'afficher le texte brut [SP (1] à partir de la trace et de choisir de partager le fichier des clés principales ou de protéger les données sensibles en ne le partageant pas.

Limitations de l'utilisation des clés de session SSL

Voici les limites de l'utilisation des clés de session SSL :

1. Les sessions SSL ne peuvent pas être déchiffrées si les paquets initiaux de la session ne sont pas capturés.
2. Les sessions SSL ne peuvent pas être capturées si le mode FIPS (Federal Information Processing Standard) est activé.

Pour capturer les clés de session SSL à l'aide de l'interface de ligne de commande (CLI)

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver les clés de session SSL dans un fichier de suivi et vérifier l'opération de suivi.

```
1  > start nstrace -capsslkeys ENABLED
2  > show nstrace
3  Example
4  > start nstrace -capsslkeys ENABLED
5  > show nstrace
6        State:  RUNNING          Scope:  LOCAL            TraceLocation:
             "/var/nstrace/04May2016_17_51_54/..."
7        Nf:  24                  Time:  3600              Size:  164
                        Mode:  TXB NEW_RX
8        Traceformat:  NSCAP      PerNIC:  DISABLED        FileName:  04
            May2016_17_51_54 Link:  DISABLED
9        Merge:  ONSTOP           Doruntimecleanup:  ENABLED TraceBuffers:
              5000      SkipRPC:  DISABLED
10       SkipLocalSSH:  DISABLED  Capsslkeys:  ENABLED     InMemoryTrace:
             DISABLED
11   Done
```

Pour configurer les clés de session SSL à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Configuration > Système > Diagnostics > Outils de support technique** et cliquez sur **Démarrer une nouvelle trace** pour démarrer le suivi des paquets chiffrés sur une appliance.

2. Dans la page **Démarrer le suivi**, activez la case à cocher **Capturer les clés principales SSL** .
3. Cliquez sur **OK** et **Terminé**.

Pour importer les clés principales SSL dans Wireshark

Dans l'interface graphique Wireshark, accédez à **Edition > Préférences > Protocoles > SSL > (Pre) -Master-Secret nom du fichier journal** et spécifiez les fichiers de clé principale obtenus à partir de l'appliance.

Résolution des problèmes courants

August 20, 2021

Lors de la jonction d'un nœud au cluster, je reçois le message suivant, "ERREUR : nom/numéro d'interface non valide." Que dois-je faire pour résoudre cette erreur ?

Cette erreur se produit si vous avez fourni une interface de fond de panier non valide ou incorrecte lors de l'utilisation de la commande add cluster node pour ajouter le nœud. Pour résoudre cette erreur, vérifiez l'interface que vous avez fournie lors de l'ajout du nœud. Assurez-vous que vous n'avez pas spécifié l'interface de gestion de l'appliance comme interface de backplane et que le <nodeId> bit de l'interface est identique à l'ID du nœud. Par exemple, si le NodeID est 3, l'interface du fond de panier doit être 3/<c>/<u>.

Lors de la jonction d'un nœud au cluster, je reçois le message suivant : "ERREUR : Le clustering ne peut pas être activé, car le nœud local n'est pas membre du cluster." Que dois-je faire pour résoudre cette erreur ?

Cette erreur se produit lorsque vous essayez de joindre un nœud sans ajouter le NSIP du nœud au cluster. Pour résoudre cette erreur, vous devez d'abord ajouter l'adresse NSIP du nœud au cluster à l'aide de la commande **add cluster node**, puis exécuter la commande **jointure cluster**.

Lors de la jonction d'un nœud au cluster, je reçois le message suivant, "ERREUR : Connexion refusée." Que dois-je faire pour résoudre cette erreur ?

Cette erreur peut se produire pour les raisons suivantes :

- **Problèmes de connectivité.** Le nœud ne peut pas se connecter à l'adresse IP du cluster. Essayez d'effectuer un ping sur l'adresse IP du cluster à partir du nœud que vous essayez de joindre.

- **Dupliquer l'adresse IP du cluster.** Vérifiez si l'adresse IP du cluster existe sur un nœud non cluster. Si c'est le cas, créez une adresse IP de cluster et essayez de rejoindre le cluster.

En joignant un nœud au cluster, j'obtiens le message suivant, "ERROR: License mismatch between the configuration coordinator and the local node." Que dois-je faire pour résoudre cette erreur ?

L'appliance que vous joignez au cluster doit posséder les mêmes licences que le coordinateur de configuration. Cette erreur se produit lorsque les licences sur le nœud que vous rejoignez ne correspondent pas aux licences sur le coordinateur de configuration. Pour résoudre cette erreur, exécutez les commandes suivantes sur les deux nœuds et comparez les sorties.

À partir de la ligne de commande :

- `show ns hardware`
- `show ns license`

À partir de la coque :

- `nsconmsg -g feature -d stats`
- `ls /nsconfig/license`
- Afficher le contenu du fichier /var/log/license.log

Que dois-je faire lorsque les configurations d'un nœud de cluster ne sont pas synchronisées avec les configurations de cluster ?

Habituellement, les configurations sont automatiquement synchronisées entre tous les nœuds de cluster. Toutefois, si vous pensez que les configurations ne sont pas synchronisées sur un nœud spécifique, vous devez forcer la synchronisation en exécutant la commande forcer cluster sync à partir du nœud que vous souhaitez synchroniser. Pour plus d'informations, consultez Synchronisation des configurations de cluster.

Lors de la configuration d'un nœud de cluster, je reçois le message suivant : "ERREUR : La session est en lecture seule ; connectez-vous à l'adresse IP du cluster pour modifier la configuration."

Toutes les configurations d'un cluster doivent être effectuées via l'adresse IP du cluster et les configurations sont propagées aux autres nœuds de cluster. Toutes les sessions établies via l'adresse NSIP des nœuds individuels sont en lecture seule.

Pourquoi l'état du nœud affiche-t-il « INACTIVE » lorsque l'état du nœud affiche « UP » ?

Un nœud sain peut être dans l'état INACTIF pour diverses raisons. Une analyse du ns.log ou des compteurs d'erreurs peut vous aider à déterminer la raison exacte.

Comment puis-je résoudre la santé d'un nœud lorsque son état affiche « NOT UP » ?

La santé du**nœud "Not UP**" indique qu'il y a des problèmes avec le nœud. Pour connaître la cause première, vous devez exécuter la commande **show cluster node** . Cette commande affiche les propriétés du nœud et la raison de l'échec du nœud.

Que dois-je faire lorsque l'état d'un nœud apparaît comme « NOT UP » et que la raison indique que les commandes de configuration ont échoué sur un nœud ?

Ce problème se produit lorsque certaines commandes ne sont pas exécutées sur les nœuds de cluster. Dans de tels cas, vous devez vous assurer que les configurations sont synchronisées à l'aide de l'une des options suivantes :

- Si certains des nœuds de cluster sont dans cet état, vous devez effectuer l'opération de synchronisation forcée du cluster sur ces nœuds. Pour plus d'informations, consultez Synchronisation des configurations de cluster.
- Si tous les nœuds de cluster sont dans cet état, vous devez désactiver, puis activer l'instance de cluster sur tous les nœuds de cluster.

Lorsque j'exécute la commande set virtual server, j'obtiens le message suivant, « Aucune ressource de ce type.« Que dois-je faire pour résoudre ce problème ?

La commande **set vserver** n'est pas prise en charge dans le clustering. Les commandes **unset vserver, enable vserver, disable vserver** et **rm vserver** ne sont pas non plus prises en charge. Toutefois, la commande **show vserver** est prise en charge.

Je ne peux pas configurer le cluster sur une session Telnet. Que dois-je faire ?

Sur une session telnet, l'adresse IP du cluster est accessible uniquement en mode lecture seule. Par conséquent, vous ne pouvez pas configurer un cluster sur une session telnet.

Je remarque une différence d'heure significative entre les nœuds de cluster. Que dois-je faire pour résoudre ce problème ?

Lorsque des paquets PTP sont supprimés en raison du commutateur de fond de panier ou si les ressources physiques sont surexploitées dans un environnement virtuel, l'heure ne sera pas synchronisée.

Pour synchroniser les heures, vous devez effectuer les opérations suivantes sur l'adresse IP du cluster :

1. Désactivez PTP.

   set ptp -state disable

2. Configurer le protocole NTP (Network Time Protocol) pour le cluster. Pour plus d'informations, voir Configuration de la synchronisation de l'horloge.

Que dois-je faire, s'il n'y a pas de connectivité à l'adresse IP du cluster et à l'adresse NSIP d'un nœud de cluster ?

Si vous ne pouvez pas accéder à l'adresse IP du cluster ou au NSIP d'un nœud de cluster, vous devez accéder à l'appliance via la console série. Si l'adresse NSIP est accessible, vous pouvez SSH vers l'adresse IP du cluster à partir du shell en exécutant la commande suivante à l'invite shell :

"'# ssh nsroot@

```
## Que dois-je faire pour récupérer un nœud de cluster qui a des problémes de connectivité ?

Pour restaurer un nœud qui présente des problémes de connectivité :

1.  Désactivez l'instance de cluster sur ce nœud (car vous ne pouvez pas exécuter de commandes à partir du NSIP d'un nœud de cluster).

1.  Exécutez les commandes requises pour restaurer le nœud.

1.  Activez l'instance de cluster sur ce nœud.

## Certains nœuds du cluster ont deux itinéraires par défaut. Comment puis-je supprimer la deuxiéme route par défaut du nœud de cluster ?

Pour supprimer l'itinéraire par défaut supplémentaire, procédez comme suit sur chaque nœud qui a l'itinéraire supplémentaire :

1.  Désactivez l'instance de cluster.

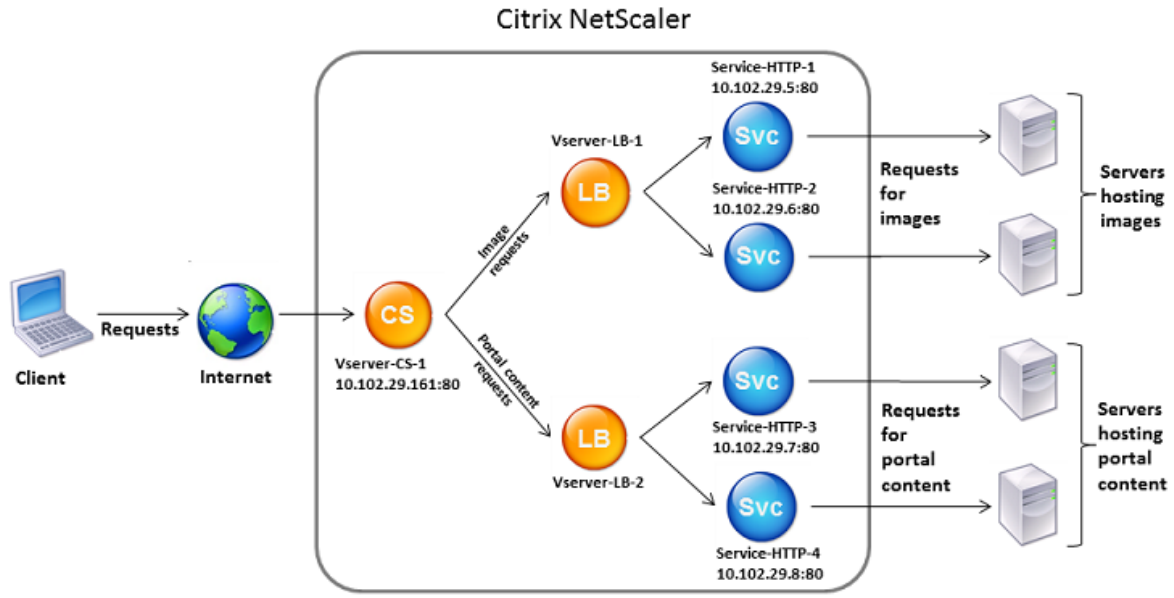
    ```disable cluster instance <clId><!--NeedCopy-->
```

1. Retirez l'itinéraire.

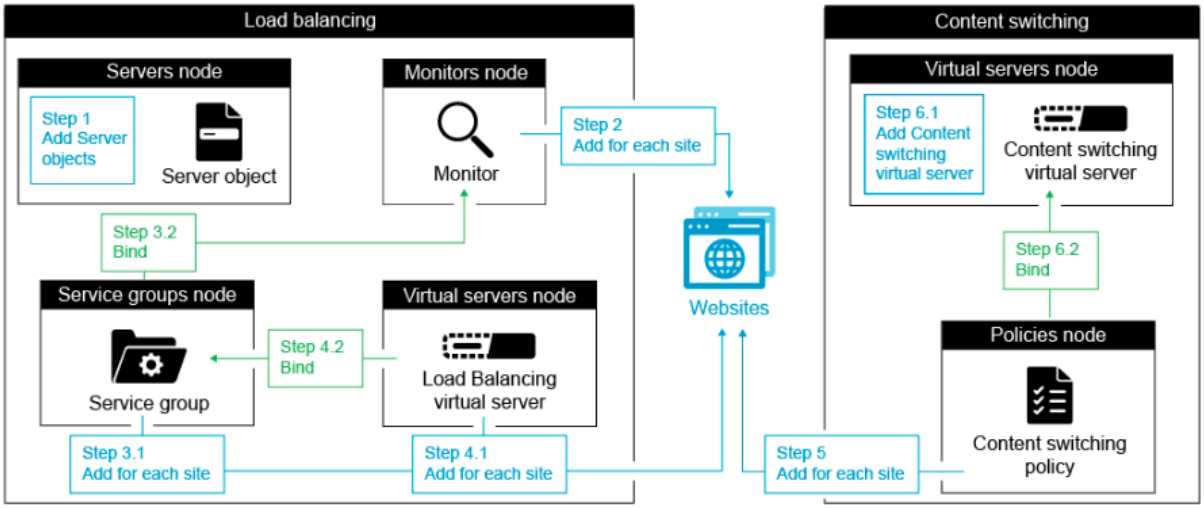
   ```
   rm route <network> <netmask> <gateway><!--NeedCopy-->
   ```

2. Activez l'instance de cluster.

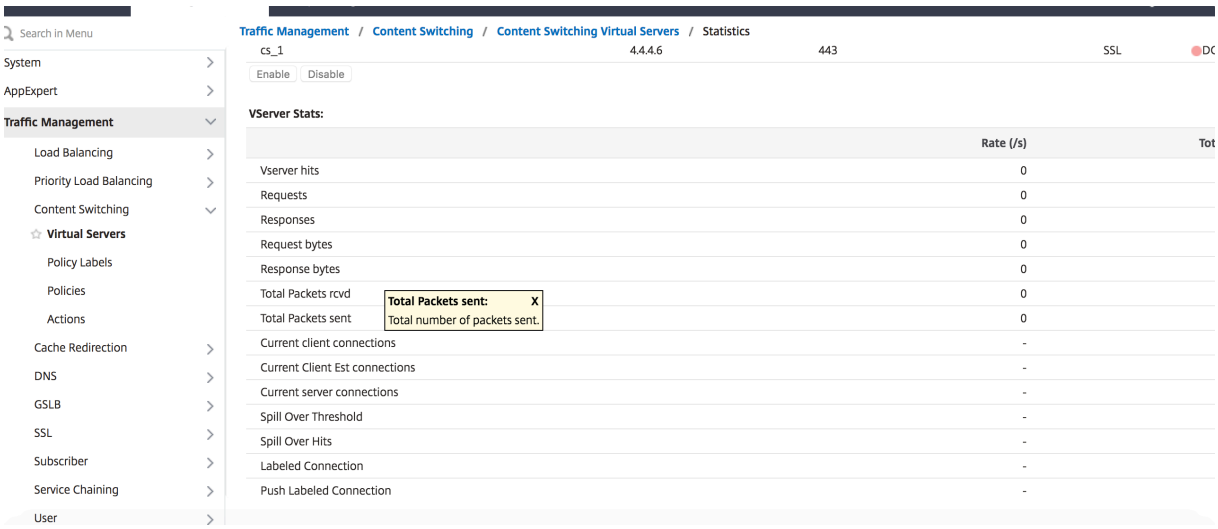
   ```
   enable cluster instance <clId><!--NeedCopy-->
   ```


   ```

### La fonctionnalité de cluster est affectée lorsqu'un nœud de cluster existant est mis en ligne. Que dois-je faire pour résoudre ce problème ?

Si le mot de passe RPC d'un nœud est modifié par rapport à l'adresse IP du cluster lorsque ce nœud est hors du cluster, alors, lorsque le nœud est en ligne, il y a une incompatibilité dans les informations d'identification RPC et peut affecter la fonctionnalité du cluster. Pour résoudre ce problème, utilisez la commande set ns RPCNode pour mettre à jour le mot de passe sur le NSIP du nœud qui est entré en ligne.

## Commutation de contenu

October 5, 2021

Dans les sites Web complexes d'aujourd'hui, vous souhaiterez peut-être présenter différents contenus à différents utilisateurs. Par exemple, vous pouvez souhaiter autoriser les utilisateurs de la plage d'adresses IP d'un client ou d'un partenaire à accéder à un portail Web spécial. Vous souhaiterez peut-être présenter du contenu pertinent à une zone géographique spécifique aux utilisateurs de cette zone. Vous souhaiterez peut-être présenter du contenu dans différentes langues aux locuteurs de ces langues. Vous souhaiterez peut-être présenter du contenu adapté à des appareils spécifiques, tels que des smartphones, aux utilisateurs de ces appareils. La fonctionnalité de commutation de contenu Citrix ADC permet à l'appliance de distribuer les demandes des clients sur plusieurs serveurs en fonction du contenu spécifique que vous souhaitez présenter à ces utilisateurs.

Pour configurer la commutation de contenu, créez d'abord une configuration de commutation de contenu de base, puis personnalisez-la en fonction de vos besoins. Cela implique l'activation de la fonctionnalité de commutation de contenu, la configuration de l'équilibrage de charge pour le ou les serveurs qui hébergent chaque version du contenu en cours de commutation, la création d'un serveur virtuel de commutation de contenu, la création de stratégies pour choisir les demandes qui sont dirigées vers quel serveur virtuel d'équilibrage de charge, et liaison des stratégies au serveur virtuel de commutation de contenu. Vous pouvez ensuite personnaliser la configuration en fonction de vos besoins en définissant la priorité de vos stratégies, en protégeant votre configuration en configurant un serveur virtuel de sauvegarde et en améliorant les performances de votre configuration en redirigeant les demandes vers un cache.

### Fonctionnement de la commutation de contenu

La commutation de contenu permet à l'appliance Citrix ADC de diriger les demandes envoyées au même hôte Web vers différents serveurs avec un contenu différent. Par exemple, vous pouvez configurer la solution matérielle-logicielle pour diriger les demandes de contenu dynamique (telles que les URL avec un suffixe .asp, .dll ou .exe) vers un serveur et les demandes de contenu statique vers

 

un autre serveur. Vous pouvez configurer la solution matérielle-logicielle pour qu'elle effectue une commutation de contenu en fonction des en-têtes TCP/IP et de la charge utile.

Vous pouvez également utiliser la commutation de contenu pour configurer la solution matérielle-logicielle afin de rediriger les demandes vers différents serveurs avec un contenu différent en fonction de divers attributs du client. Voici quelques-uns de ces attributs clients :

- **Type d'appareil.** La solution matérielle-logicielle examine l'agent utilisateur ou l'en-tête HTTP personnalisé dans la demande du client pour le type de périphérique à partir duquel la demande est originaire. En fonction du type d'appareil, il dirige la demande vers un serveur Web spécifique. Par exemple, si la demande provient d'un téléphone cellulaire, la demande est dirigée vers un serveur, capable de fournir un contenu que l'utilisateur peut consulter sur le téléphone cellulaire. Une demande émanant d'un ordinateur est dirigée vers un serveur différent, capable de diffuser un contenu conçu pour un écran d'ordinateur.
- **Langage.** La solution matérielle-logicielle examine l'en-tête HTTP Accept-Language dans la demande du client et détermine la langue utilisée par le navigateur du client. La solution matérielle-logicielle envoie ensuite la demande à un serveur qui diffuse du contenu dans cette langue. Par exemple, en utilisant la commutation de contenu en fonction de la langue, l'appliance peut envoyer une personne dont le navigateur est configuré pour demander du contenu en français à un serveur avec la version française d'un journal. Il peut envoyer une autre personne dont le navigateur est configuré pour demander du contenu en anglais à un serveur avec la version anglaise.
- **Cookie.** La solution matérielle-logicielle examine les en-têtes de requête HTTP pour un cookie précédemment défini par le serveur. S'il trouve le cookie, il dirige les requêtes vers le serveur approprié, qui héberge du contenu personnalisé. Par exemple, si un cookie indique que le client est membre d'un programme de fidélisation de la clientèle, la demande est dirigée vers un serveur plus rapide ou un serveur doté d'un contenu spécial. S'il ne trouve pas de cookie, ou si le cookie indique que l'utilisateur n'est pas membre, la demande est dirigée vers un serveur destiné au grand public.
- **Méthode HTTP.** La solution matérielle-logicielle examine l'en-tête HTTP de la méthode utilisée et envoie la demande du client au bon serveur. Par exemple, les demandes GET d'images peuvent être dirigées vers un serveur d'images, tandis que les demandes POST peuvent être dirigées vers un serveur plus rapide qui gère le contenu dynamique.
- **Données de la couche 3/4.** L'appliance examine les demandes relatives à l'adresse IP source ou de destination, au port source ou de destination, ou à toute autre information présente dans les en-têtes TCP ou UDP, et dirige la demande du client vers le bon serveur. Par exemple, les demandes provenant d'adresses IP sources appartenant à des clients peuvent être dirigées vers un portail Web personnalisé sur un serveur plus rapide, ou vers un portail doté d'un contenu spécial.

Un déploiement de commutation de contenu typique comprend les entités décrites dans le diagramme suivant.

 

Figure 1. Architecture de commutation de contenu




Une configuration de commutation de contenu se compose d'un serveur virtuel de commutation de contenu, d'une configuration d'équilibrage de charge consistant en serveurs et services virtuels d'équilibrage de charge, et de stratégies de commutation de contenu. Pour configurer la commutation de contenu, vous devez configurer un serveur virtuel de commutation de contenu et l'associer à des stratégies et à des serveurs virtuels d'équilibrage de charge. Ce processus crée un *groupe de contenus*, un groupe de tous les serveurs virtuels et stratégies impliqués dans une configuration de commutation de contenu particulière.

La commutation de contenu peut être utilisée avec les connexions HTTP, HTTPS, TCP et UDP. Pour HTTPS, vous devez activer le déchargement SSL.

Lorsqu'une demande atteint le serveur virtuel de commutation de contenu, le serveur virtuel applique les stratégies de commutation de contenu associées à cette demande. La priorité de la stratégie définit l'ordre dans lequel les stratégies liées au serveur virtuel de commutation de contenu sont évaluées. Si vous utilisez des stratégies de stratégie avancées, lorsque vous liez une stratégie au serveur virtuel de commutation de contenu, vous devez attribuer une priorité à cette stratégie. Si vous utilisez des stratégies Citrix ADC Classic, vous pouvez attribuer une priorité à vos stratégies, mais vous n'êtes pas obligé de le faire. Si vous attribuez des priorités, les stratégies sont évaluées dans l'ordre que vous avez défini. Si ce n'est pas le cas, l'appliance Citrix ADC évalue vos stratégies dans l'ordre dans lequel elles ont été créées.

Outre la configuration des priorités de stratégie, vous pouvez manipuler l'ordre d'évaluation de stratégie à l'aide d'expressions Goto et d'invocations de banque de stratégies. Pour plus d'informations sur la configuration avancée des stratégies, consultez Configuration des stratégies

 

avancées.

Après avoir évalué les stratégies, le serveur virtuel de commutation de contenu achemine la demande vers le serveur virtuel d'équilibrage de charge approprié, qui l'envoie au service approprié.

Les serveurs virtuels de commutation de contenu peuvent uniquement envoyer des demandes à d'autres serveurs virtuels. Si vous utilisez un équilibreur de charge externe, vous devez créer un serveur virtuel d'équilibrage de charge pour celui-ci et lier son serveur virtuel en tant que service au serveur virtuel de commutation de contenu.

## Configuration de la commutation de contenu de base

October 5, 2021

Avant de configurer la commutation de contenu, vous devez comprendre comment la commutation de contenu est configurée et comment les services et les serveurs virtuels sont connectés.

Pour configurer une configuration de commutation de contenu de base et fonctionnelle, commencez par activer la fonction de commutation de contenu. Créez ensuite au moins un groupe de contenus. Pour chaque groupe de contenus, créez un serveur virtuel de commutation de contenu pour accepter les demandes adressées à un groupe de sites Web qui utilisent la commutation de contenu. Créez également une configuration d'équilibrage de charge, qui inclut un groupe de serveurs virtuels d'équilibrage de charge vers lesquels le serveur virtuel de commutation de contenu dirige les demandes. Pour spécifier les demandes à diriger vers quel serveur virtuel d'équilibrage de charge, créez au moins deux stratégies de commutation de contenu, une pour chaque type de demande à rediriger. Lorsque vous avez créé les serveurs virtuels et les stratégies, liez les stratégies au serveur virtuel de commutation de contenu. Vous pouvez également lier une stratégie à plusieurs serveurs virtuels de commutation de contenu. Lorsque vous liez une stratégie, vous spécifiez le serveur virtuel d'équilibrage de charge vers lequel les demandes correspondant à la stratégie doivent être dirigées.

En plus de lier des stratégies individuelles à un serveur virtuel de commutation de contenu, vous pouvez lier des étiquettes de stratégie. Si vous créez plusieurs groupes de contenu, vous pouvez lier une stratégie ou une étiquette de stratégie à plusieurs des serveurs virtuels de commutation de contenu.

> **Remarque**
>
> Après avoir créé un groupe de contenus, vous pouvez modifier son serveur virtuel de commutation de contenu pour personnaliser la configuration.

### Activation du changement de contenu

Pour utiliser la fonctionnalité de changement de contenu, vous devez activer la commutation de contenu. Vous pouvez configurer des entités de changement de contenu même si la fonctionnalité de

 

changement de contenu est désactivée. Toutefois, les entités ne fonctionneront pas.

### Pour activer la commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer la commutation de contenu et vérifier la configuration :

```
enable ns feature CS

show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable  feature ContentSwitch
    Done
> show feature

    Feature                       Acronym             Status
    -------                       -------             ------
1)     Web Logging                   WL                  OFF
2)     Surge Protection              SP                  ON
3)     Load Balancing                LB                  ON
4)     Content Switching             CS                  ON
.
.
.
22)    Responder                     RESPONDER           ON
23)    NetScaler Push                push                OFF
Done
<!--NeedCopy-->
```

Pour activer la commutation de contenu à l'aide de l'interface graphique

Accédez à **Système > Paramètres** et, dans le groupe **Modes et fonctionnalités**, sélectionnez **Configurer les fonctionnalités de base**, puis sélectionnez **Changement de contenu**.

La figure suivante illustre la configuration pas à pas de Content Switching.



Création de serveurs virtuels de commutation de contenu

Vous pouvez ajouter, modifier et supprimer des serveurs virtuels de commutation de contenu. L'état d'un serveur virtuel est en panne lorsque vous le créez, car le serveur virtuel d'équilibrage de charge n'y est pas encore lié.

Pour créer un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Exemple :

```
add cs vserver Vserver-CS-1 HTTP 10.102.29.161 80
<!--NeedCopy-->
```

Pour ajouter un serveur virtuel de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis ajoutez un serveur virtuel.
2. Spécifiez un nom pour le serveur virtuel de commutation de contenu.

> **Remarque**
>
> Il existe différents serveurs virtuels de commutation de contenu pour chaque protocole.

> (Par exemple, HTTP et SSL).

3. Renseignez les champs pertinents, puis cliquez sur **OK**.

Statistiques du serveur virtuel de commutation de contenu

Les statistiques du serveur virtuel de commutation de contenu affichent des informations telles que la sélection du serveur virtuel, les octets de demande, les octets de réponse, le nombre total de paquets reçus, le nombre total de paquets envoyés, le seuil de débordement, la sélection de débordement, les connexions actuelles établies par le client et la sélection de sauvegarde du serveur virtuel en panne.

Les statistiques du serveur virtuel de commutation de contenu affichent également les détails récapitulatifs du serveur virtuel d'équilibrage de charge par défaut lié.

Pour afficher les statistiques du serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat cs vserver <name>
<!--NeedCopy-->
```

Exemple :

```
stat cs vserver CS_stats
<!--NeedCopy-->
```



```
Vserver Summary
                          IP  port     Protocol        State
CS_stats             1.1.1.1    80         HTTP           UP

VServer Stats:
                                          Rate (/s)                Total
Vserver hits                                      0                    0
Requests                                          0                    0
Responses                                         0                    0
Request bytes                                     0                    0
Response bytes                                    0                    0
Total Packets rcvd                                0                    0
Total Packets sent                                0                    0
Current client connections                       --                    0
Current Client Est connections                   --                    0
Current server connections                       --                    0
Spill Over Threshold                             --                    0
Spill Over Hits                                  --                    0
Labeled Connection                               --                    0
Push Labeled Connection                          --                    0
Deferred Request                                  0                    0
Invalid Request/Response                         --                    0
Invalid Request/Response Dropped                 --                    0
Vserver Down Backup Hits                         --                    0
Current Multipath TCP sessions                   --                    0
Current Multipath TCP subflows                   --                    0
Apdex for client response times.                 --                 1.00
Average client TTLB                              --                    0

 Done
```

Pour afficher les statistiques du serveur virtuel de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels**.
2. Sélectionnez le serveur virtuel et cliquez sur **Statistiques**.



Configuration d'une configuration d'équilibrage de charge pour la commutation de contenu

Le serveur virtuel de commutation de contenu redirige toutes les demandes vers un serveur virtuel d'équilibrage de charge. Vous devez créer un serveur virtuel d'équilibrage de charge pour chaque version du contenu qui est commuté. Cela est vrai même si votre configuration ne comporte qu'un seul serveur pour chaque version du contenu et que vous n'effectuez donc aucun équilibrage de charge avec ces serveurs. Vous pouvez également configurer l'équilibrage de charge réel avec plusieurs serveurs à équilibrage de charge qui reflètent chaque version du contenu. Dans les deux scénarios, le serveur virtuel de commutation de contenu doit disposer d'un serveur virtuel d'équilibrage de charge spécifique affecté à chaque version du contenu en cours de commutation.

Le serveur virtuel d'équilibrage de charge transfère ensuite la demande à un service. Si un seul service lui est lié, il le sélectionne. Si plusieurs services lui sont liés, il utilise sa méthode d'équilibrage de charge configurée pour sélectionner un service pour la demande, et transfère cette demande au service qu'il a sélectionné.

Pour configurer une configuration d'équilibrage de charge de base, vous devez effectuer les tâches suivantes :

- Créer des serveurs virtuels d'équilibrage de charge
- Créer des services
- Liez les services au serveur virtuel d'équilibrage de charge

Pour plus d'informations sur l'équilibrage de charge, voir Fonctionnement de l'équilibrage de charge. Pour obtenir des instructions détaillées sur la configuration d'une configuration d'équilibrage de charge de base, voir Configurer l'équilibrage de charge de base.

Configuration d'une action de commutation de contenu

Vous spécifiez le serveur virtuel d'équilibrage de charge cible pour une stratégie de commutation de contenu lorsque vous liez la stratégie au serveur virtuel de commutation de contenu. Par conséquent, vous devez configurer une stratégie pour chaque serveur virtuel d'équilibrage de charge vers lequel diriger le trafic.

Toutefois, si votre stratégie de changement de contenu utilise une règle de stratégie avancée, vous pouvez configurer une action pour cette stratégie. Dans l'action, vous pouvez spécifier le nom du serveur virtuel d'équilibrage de charge cible ou configurer une expression basée sur la demande qui, au moment de l'exécution, calcule le nom du serveur virtuel d'équilibrage de charge auquel envoyer la demande. L'expression d'action doit être spécifiée dans la stratégie avancée.

L'option d'expression peut réduire considérablement la taille de votre configuration de commutation de contenu, car vous n'avez besoin que d'une seule stratégie par serveur virtuel de commutation de contenu. Les stratégies de commutation de contenu qui utilisent une action peuvent également être liées à plusieurs serveurs virtuels de commutation de contenu, car le serveur virtuel d'équilibrage de charge cible n'est plus spécifié dans la stratégie de commutation de contenu. La possibilité de lier une stratégie unique à plusieurs serveurs virtuels de commutation de contenu contribue à réduire davantage la taille de votre configuration de commutation de contenu.

Après avoir créé une action, vous créez une stratégie de changement de contenu et spécifiez l'action dans la stratégie, de sorte que l'action soit exécutée lorsque cette stratégie correspond à une demande.

> **Remarque**
>
> Vous pouvez également, pour une stratégie de commutation de contenu qui utilise une règle de stratégie avancée, spécifier le serveur virtuel d'équilibrage de charge cible lors de la liaison de la stratégie à un serveur virtuel de commutation de contenu, au lieu d'utiliser une action distincte. Pour les stratégies basées sur le domaine, les stratégies basées sur des URL et les stratégies basées sur des règles qui utilisent des expressions classiques, aucune action n'est disponible. Par conséquent, pour ces types de stratégies, vous spécifiez le nom du serveur virtuel d'équilibrage de charge cible lorsque vous liez la stratégie à un serveur virtuel de commutation de contenu.

Configuration d'une action qui spécifie le nom du serveur virtuel d'équilibrage de charge cible

Si vous choisissez de spécifier le nom du serveur virtuel d'équilibrage de charge cible dans une action de commutation de contenu, vous avez besoin d'autant de stratégies de commutation de contenu que de serveurs virtuels d'équilibrage de charge cible. Dans ce cas, les décisions de changement de contenu sont basées sur la règle de la stratégie de changement de contenu, et l'action spécifie simplement le serveur virtuel d'équilibrage de charge cible. Lorsqu'une demande correspond à la stratégie, elle est transférée au serveur virtuel d'équilibrage de charge spécifié.

Pour créer et vérifier une action de commutation de contenu qui spécifie le nom du serveur virtuel d'équilibrage de charge cible, à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add cs action <name> -targetLBVserver <string> [-comment <string>]

show cs action <name>
<!--NeedCopy-->
```

Exemple :

```
> add cs action mycsaction -targetLBVserver mylbvserver -comment "
    Forwards requests to mylbvserver."
 Done
> show cs action mycsaction
    Name: mycsaction
    Target LB Vserver: mylbvserver
    Hits: 0
    Undef Hits: 0
    Action Reference Count: 0
    Comment: "Forwards requests to mylbvserver."

 Done
>
<!--NeedCopy-->
```

Pour configurer une action de commutation de contenu qui spécifie le nom du serveur virtuel d'équilibrage de charge cible, à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Changement de contenu > Actions**.
2. Configurez une action de commutation de contenu et spécifiez le nom du serveur virtuel d'équilibrage de charge cible.

Configuration d'une action qui spécifie une expression pour sélectionner la cible au moment de l'exécution

Si vous choisissez de configurer une expression basée sur une demande qui peut calculer dynamiquement le nom du serveur virtuel d'équilibrage de charge cible, vous devez configurer une seule stratégie de commutation de contenu pour sélectionner le serveur virtuel approprié. La règle de la stratégie peut être un simple VRAI (la stratégie correspond à toutes les demandes) car, dans ce cas, les décisions de changement de contenu sont basées sur l'expression de l'action. En configurant une ex-

pression dans une action, vous pouvez réduire considérablement la taille de votre configuration de changement de contenu.

Si vous choisissez de configurer une expression basée sur la demande pour calculer le nom du serveur virtuel d'équilibrage de charge cible au moment de l'exécution, vous devez examiner attentivement comment nommer les serveurs virtuels d'équilibrage de charge dans la configuration. Vous devez être en mesure de dériver leurs noms à l'aide de l'expression de stratégie basée sur la demande dans l'action.

Par exemple, si vous changez de demande en fonction du suffixe d'URL (extension de la ressource demandée), lorsque vous nommez les serveurs virtuels d'équilibrage de charge, vous pouvez suivre la convention d'ajout du suffixe d'URL à une chaîne prédéterminée, par exemple `mylb_`. Par exemple, les serveurs virtuels d'équilibrage de charge pour les pages HTML et les fichiers PDF peuvent être nommés `mylb_html` et `mylb_pdf`, respectivement. Dans ce cas, la règle que vous pouvez utiliser dans l'action de changement de contenu pour sélectionner le serveur virtuel d'équilibrage de charge approprié est `"mylb_"+HTTP.REQ.URL.SUFFIX`. Si le serveur virtuel de commutation de contenu reçoit une demande de page HTML, l'expression est `mylb_html`renvoyée et la demande est basculée vers le serveur virtuel `mylb_html`.

Pour créer une action de changement de contenu qui spécifie une expression, à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour créer une action de changement de contenu qui spécifie une expression et vérifiez la configuration :

```
add cs action <name> -targetVserverExpr <expression>) [-comment <string
    >]

show cs action <name>
<!--NeedCopy-->
```

Exemple :

```
> add cs action mycsaction1 -targetvserverExpr '"mylb_" + HTTP.REQ.URL.
    SUFFIX'
 Done
> show cs action mycsaction1
    Name: mycsaction1
    Target Vserver Expression: "mylb_" + HTTP.REQ.URL.SUFFIX
    Target LB Vserver: No_Target
                ...
 Done
>
<!--NeedCopy-->
```


Pour configurer une action de changement de contenu qui spécifie une expression à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Changement de contenu > Actions**.
2. Configurez une action de commutation de contenu et spécifiez une expression qui calculera dynamiquement le nom du serveur virtuel d'équilibrage de charge cible.

Configuration des stratégies de changement de contenu

Une stratégie de commutation de contenu définit un type de demande qui doit être dirigée vers un serveur virtuel d'équilibrage de charge. Ces stratégies sont appliquées dans l'ordre des priorités qui leur sont attribuées ou (si vous utilisez des stratégies Citrix ADC Classic et que vous n'attribuez pas de priorités lors de la liaison) dans l'ordre dans lequel les stratégies ont été créées.

Les politiques peuvent être les suivantes :

- **Stratégies basées sur le domaine.** L'appliance Citrix ADC compare le domaine d'une URL entrante aux domaines spécifiés dans les stratégies. La solution matérielle-logicielle renvoie ensuite le contenu le plus approprié. Les stratégies basées sur le domaine doivent être des stratégies classiques. Les stratégies de stratégie avancées ne sont pas prises en charge pour ce type de stratégie de changement de contenu.
- **Stratégies basées sur les URL.** La solution matérielle-logicielle compare une URL entrante aux URL spécifiées dans les stratégies. La solution matérielle-logicielle renvoie ensuite le contenu basé sur l'URL le plus approprié, qui correspond généralement à l'URL configurée la plus longue. Les stratégies basées sur une URL doivent être des stratégies classiques. Les stratégies de stratégie avancées ne sont pas prises en charge pour ce type de stratégie de changement de contenu.
- **Stratégies basées sur des règles.** La solution matérielle-logicielle compare les données entrantes aux expressions spécifiées dans les stratégies. Vous créez des stratégies basées sur des règles à l'aide d'une expression classique ou d'une expression de stratégie avancée. Les stratégies de stratégie classique et avancée sont prises en charge pour les stratégies de changement de contenu basées sur des règles.

  > **Remarque**
  >
  > Une stratégie basée sur des règles peut être configurée avec une action facultative. Une stratégie comportant une action peut être liée à plusieurs serveurs virtuels ou étiquettes de stratégie.

  Si vous définissez une priorité lorsque vous liez vos stratégies au serveur virtuel de commutation de contenu, les stratégies sont évaluées par ordre de priorité. Si vous ne définissez pas de priorités spécifiques lors de la liaison de vos stratégies, les stratégies sont évaluées dans l'ordre dans lequel elles ont été créées.

Pour plus d'informations sur les stratégies et expressions classiques Citrix ADC, reportez-vous à la section Configuration des stratégies et expressions classiques. Pour plus d'informations sur les stratégies de stratégie avancées, consultez Configuration des expressions de stratégie avancées.

Pour créer une stratégie de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
add cs policy <policyName> -domain <domain>

add cs policy <policyName> -url <URLValue>

add cs policy <policyName> -rule <RULEValue>

add cs policy <policyName> -rule <RULEValue> -action <actionName>
<!--NeedCopy-->
```

Exemple :

```
add cs policy-CS-1 -url "http://example.com"

add cs policy-CS-1 -domain "example.com"

add cs policy-CS-1 -rule "CLIENT.IP.SRC.SUBNET(24).EQ(10.217.84.0)"

add cs policy-CS-2 -rule "SYS.TIME.BETWEEN(GMT 2009 Nov,GMT 2009 Dec)"

add cs policy-CS-3 -rule "http.req.method.eq(GET)" -action act1
<!--NeedCopy-->
```

Pour renommer une stratégie de changement de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rename cs policy <policyName> <newName>
<!--NeedCopy-->
```

Exemple :

```
rename cs policy myCSPolicy myCSPolicy1
<!--NeedCopy-->
```


Pour renommer une stratégie de changement de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Changement de contenu > Stratégies**, sélectionnez une stratégie et, dans la liste Action, sélectionnez Renommer.

Pour créer une stratégie de changement de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Stratégies**, puis cliquez sur **Ajouter**.
2. Renseignez les champs pertinents, puis cliquez sur **Créer**.

Configuration des étiquettes de stratégie de commutation de contenu

Une étiquette de stratégie est un point de liaison défini par l'utilisateur auquel les stratégies sont liées. Lorsqu'une étiquette de stratégie est appelée, toutes les stratégies qui lui sont liées sont évaluées dans l'ordre de priorité que vous leur avez attribué. Un libellé de stratégie peut inclure une ou plusieurs stratégies, chacune pouvant se voir attribuer son propre résultat. Une correspondance sur une stratégie dans l'étiquette de stratégie peut entraîner la poursuite de la stratégie suivante, l'appel d'un autre libellé de stratégie ou d'une ressource appropriée, ou la fin immédiate de l'évaluation de la stratégie et le retour du contrôle de la stratégie qui a appelé l'étiquette de stratégie. Vous pouvez créer des étiquettes de stratégie pour les stratégies avancées uniquement.

Une étiquette de stratégie de changement de contenu se compose d'un nom, d'un type d'étiquette et d'une liste de stratégies liées à l'étiquette de stratégie. Le type d'étiquette de stratégie spécifie le protocole qui a été affecté aux stratégies liées à l'étiquette. Il doit correspondre au type de service du serveur virtuel de commutation de contenu auquel la stratégie qui appelle l'étiquette de stratégie est liée. Par exemple, vous pouvez lier des stratégies de charge utile TCP à une étiquette de stratégie de type TCP uniquement. La liaison des stratégies de charge utile TCP à une étiquette de stratégie de type HTTP n'est pas prise en charge.

Chaque stratégie d'une étiquette de stratégie de changement de contenu est associée soit à une cible (qui est équivalente à l'action associée à d'autres types de stratégies, telles que les stratégies de réécriture et de répondeur), soit à une option GoToPriorityExpression et à une option d'appel. En d'autres termes, pour une stratégie donnée dans un libellé de stratégie de changement de contenu, vous pouvez spécifier une cible ou définir l'option GoToPriorityExpression et l'option invoke. De plus, si plusieurs stratégies sont évaluées sur true, seule la cible de la dernière stratégie évaluée sur true est prise en compte.

Vous pouvez utiliser l'interface de ligne de commande Citrix ADC ou l'interface graphique pour configurer les étiquettes de stratégie de commutation de contenu. Dans l'interface de ligne de commande Citrix ADC, vous commencez par créer une étiquette de stratégie à l'aide de la commande add cs policy label. Ensuite, vous liez les stratégies à l'étiquette de stratégie, une stratégie à la fois, à l'aide de la

commande bind cs policy label. Dans l'interface graphique Citrix ADC, vous effectuez les deux tâches dans une seule boîte de dialogue.

Pour créer une étiquette de stratégie de changement de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add cs policylabel <labelName> <cspolicylabelTypetype>`
<!--NeedCopy-->
```

Exemple :

```
add cs policylabel testpollab http
<!--NeedCopy-->
```

Pour renommer une étiquette de stratégie de changement de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rename cs policylabel <labelName> <newName>`
<!--NeedCopy-->
```

Exemple :

```
rename cs policylabel oldPolicyLabelName newPolicyLabelName
<!--NeedCopy-->
```

Pour renommer une étiquette de stratégie de changement de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Changement de contenu > Étiquettes**de stratégie, sélectionnez une étiquette de stratégie et, dans la liste Action, sélectionnez Renommer.

Pour lier une stratégie à une étiquette de stratégie de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une stratégie à une étiquette de stratégie et vérifier la configuration :


```
bind cs policylabel <labelName> <policyName> <priority>[-targetVserver
    <string>] | [-gotoPriorityExpression <expression>] | [-invoke <
    labeltype> <labelName>] ]

show cs policylabel <labelName>
<!--NeedCopy-->
```

Exemple :

```
bind cs policylabel testpollab test_Pol 100 -targetVserver LBVIP
show cs policylabel testpollab
        Label Name: testpollab
        Label Type: HTTP
        Number of bound policies: 1
        Number of times invoked: 0
        Policy Name: test_Pol
        Priority: 100
        Target Virtual Server: LBVIP
<!--NeedCopy-->
```

> **Remarque**
>
> Si une stratégie est configurée avec une action, le serveur virtuel cible (TargetvServer), accédez à l'expression de priorité (GoToPriorityExpression) et les paramètres invoke (invoke) ne sont pas requis. Si une stratégie n'est pas configurée avec une action, vous devez configurer au moins l'un des paramètres suivants : TargetvServer, GoToPriorityExpression et invoke.

Pour délier une stratégie d'une étiquette de stratégie à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour délier une stratégie d'une étiquette de stratégie et vérifier la configuration :

```
unbind cs policylabel <labelName> <policyName>

show cs policylabel <labelName>
<!--NeedCopy-->
```

Exemple :

```
unbind cs policylabel testpollab test_Pol
show cs policylabel testpollab
        Label Name: testpollab
        Label Type: HTTP
```



```
5         Number of bound policies: 0
6         Number of times invoked: 0
7 <!--NeedCopy-->
```

Pour supprimer une étiquette de stratégie à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 rm cs policylabel <labelName>
2 <!--NeedCopy-->
```

Pour gérer une étiquette de stratégie de changement de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Étiquettes**de stratégie, configurez une étiquette de stratégie, liez des stratégies à l'étiquette et, le cas échéant, spécifiez une priorité, une expression GoToPriority et une option d'appel.

Stratégies de liaison à un serveur virtuel de commutation de contenu

Après avoir créé votre serveur virtuel de commutation de contenu et vos stratégies, vous liez chaque stratégie au serveur virtuel de commutation de contenu. Lorsque vous liez la stratégie au serveur virtuel de commutation de contenu, vous spécifiez le serveur virtuel d'équilibrage de charge cible.

> **Remarque**
>
> Si votre stratégie de changement de contenu utilise une règle de stratégie avancée, vous pouvez configurer une action de changement de contenu pour la stratégie. Si vous configurez une action, vous devez spécifier le serveur virtuel d'équilibrage de charge cible lorsque vous configurez l'action, et non lorsque vous liez la stratégie au serveur virtuel de commutation de contenu. Pour plus d'informations sur la configuration d'une action de changement de contenu, consultez la section
> Configuration d'une action de changement de contenu.

Pour lier une stratégie à un serveur virtuel de commutation de contenu et sélectionner un serveur virtuel d'équilibrage de charge cible à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
bind cs vserver <name>[-lbvserver<string> -targetLBVServer<string> -
    policyname <string> -priority <positive_integer>] [-
    gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )]
    [-invoke (<labelType> <labelName>)]
<!--NeedCopy-->
```

Exemple :

```
bind cs vserver csw-vip2 -policyname csw-ape-policy2 -priority 14 -
    gotoPriorityExpression NEXT

bind cs vserver csw-vip3 -policyname rewrite-policy1 -priority 17 -
    gotoPriorityExpression
'q.header("a").count' -flowtype REQUEST -invoke policylabel label1

bind cs vserver Vserver-CS-1 Vserver-LB-1 -policyname Policy-CS-1 -
    priority 20
<!--NeedCopy-->
```

> **Remarque**
>
> Les paramètres, serveur virtuel d'équilibrage de charge cible (TargetvServer), aller à l'expression de priorité (GoToPriorityExpression) et méthode invoke (invoke) ne peuvent pas être utilisés si une stratégie comporte une action.

Pour lier une stratégie à un serveur virtuel de commutation de contenu et sélectionner un serveur virtuel d'équilibrage de charge cible à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, ouvrez un serveur virtuel et, dans la section Liaison de stratégie de commutation de
contenu, liez une stratégie au serveur virtuel et spécifiez un serveur virtuel d'équilibrage de charge cible.

Configuration de la journalisation basée sur des stratégies pour la commutation de contenu

Vous pouvez configurer la journalisation basée sur une stratégie pour une stratégie de changement de contenu. La journalisation basée sur des stratégies vous permet de spécifier un format pour les messages de journal. Le contenu du message de journal est défini à l'aide d'une expression de stratégie avancée dans la stratégie de changement de contenu. Lorsque l'action de commutation de contenu spécifiée dans la stratégie est exécutée, l'appliance Citrix ADC construit le message de journal à partir de l'expression et écrit le message dans le fichier journal. La journalisation basée sur des stratégies est

particulièrement utile si vous souhaitez tester et dépanner une configuration dans laquelle les actions de changement de contenu identifient le serveur virtuel d'équilibrage de charge cible au moment de l'exécution.

> **Remarque**
>
> Si plusieurs stratégies liées à un serveur virtuel donné ont la valeur TRUE et sont configurées avec une action de message d'audit, l'appliance Citrix ADC n'effectue pas toutes les actions de message d'audit. Il exécute uniquement l'action de message d'audit configurée pour la stratégie dont l'action de changement de contenu est effectuée.

Pour configurer la journalisation basée sur une stratégie pour une stratégie de changement de contenu, vous devez d'abord configurer une action de message d'audit. Pour plus d'informations sur la configuration d'une action de message d'audit, consultez Configuration de l'appliance Citrix ADC pour la journalisation des audits. Après avoir configuré l'action du message d'audit, vous spécifiez l'action dans une stratégie de changement de contenu.

Pour configurer la journalisation basée sur une stratégie pour une stratégie de commutation de contenu à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour configurer la journalisation basée sur une stratégie pour une stratégie de commutation de contenu et vérifier la configuration :

```
set cs policy <policyName> -logAction <string>

show cs policy <policyName>
<!--NeedCopy-->
```

Exemple :

```
> set cs policy cspol1 -logAction csLogAction
 Done
> show cs policy cspol1

    Policy: cspol1  Rule: TRUE  Action: csact1
    LogAction: csLogAction
    Hits: 0

1)  CS Vserver: csvs1
    Priority: 10
 Done
>
<!--NeedCopy-->
```


Pour configurer la journalisation basée sur une stratégie pour une stratégie de commutation de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Stratégies**, ouvrez une stratégie et, dans la liste Action du journal, sélectionnez une action de journal pour la stratégie.

Vérification de la configuration

Pour vérifier que la configuration de la commutation de contenu est correcte, vous devez afficher les entités de changement de contenu. Pour vérifier le bon fonctionnement après le déploiement de votre configuration de commutation de contenu, vous pouvez afficher les statistiques générées lors de l'accès aux serveurs.

Affichage des propriétés des serveurs virtuels de commutation de contenu

Vous pouvez afficher les propriétés des serveurs virtuels de commutation de contenu que vous avez configurés sur l'appliance Citrix ADC. Vous pouvez utiliser ces informations pour vérifier si le serveur virtuel est correctement configuré et, si nécessaire, pour résoudre les problèmes. Outre les détails tels que le nom, l'adresse IP et le port, vous pouvez afficher les différentes stratégies liées à un serveur virtuel et ses paramètres de gestion du trafic.

Les stratégies de changement de contenu sont affichées dans l'ordre de priorité. Si plusieurs stratégies ont la même priorité, elles sont affichées dans l'ordre dans lequel elles sont liées au serveur virtuel.

> **Remarque**
>
> Si vous avez configuré le serveur virtuel de commutation de contenu pour transférer le trafic vers un serveur virtuel d'équilibrage de charge, vous pouvez également afficher les stratégies de commutation de contenu en affichant les propriétés du serveur virtuel d'équilibrage de charge.

Pour afficher les propriétés des serveurs virtuels de commutation de contenu à l'aide de l'interface de ligne de commande

Pour répertorier les propriétés de base de tous les serveurs virtuels de commutation de contenu de votre configuration, ou les propriétés détaillées d'un serveur virtuel de commutation de contenu spécifique, à l'invite de commandes, tapez l'une des commandes suivantes :

```
show cs vserver

show cs vserver <name>
<!--NeedCopy-->
```


Exemple

```
1.
show cs vserver Vserver-CS-1
Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
Last state change was at Thu Jun 30 10:48:59 2011
Time since last state change: 6 days, 20:03:00.760
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
Default: Content Precedence: RULE
Vserver IP and Port insertion: OFF
Case Sensitivity: ON
Push: DISABLED Push VServer:
Push Label Rule: none

...
1) Policy : __ESNS_PREBODY_POLICY Priority:0
2) Policy : __ESNS_POSTBODY_POLICY Priority:0

1) Compression Policy Name: __ESNS_CMP_POLICY Priority: 2147483647
GotoPriority Expression: END
Flowtype: REQUEST

2) Rewrite Policy Name: __ESNS_REWRITE_POLICY Priority: 2147483647
GotoPriority Expression: END
Flowtype: REQUEST

3) Cache Policy Name: dfbx Priority: 10
GotoPriority Expression: END
Flowtype: REQUEST

4) Responder Policy Name: __ESNS_RESPONDER_POLICY Priority: 2147483647
GotoPriority Expression: END

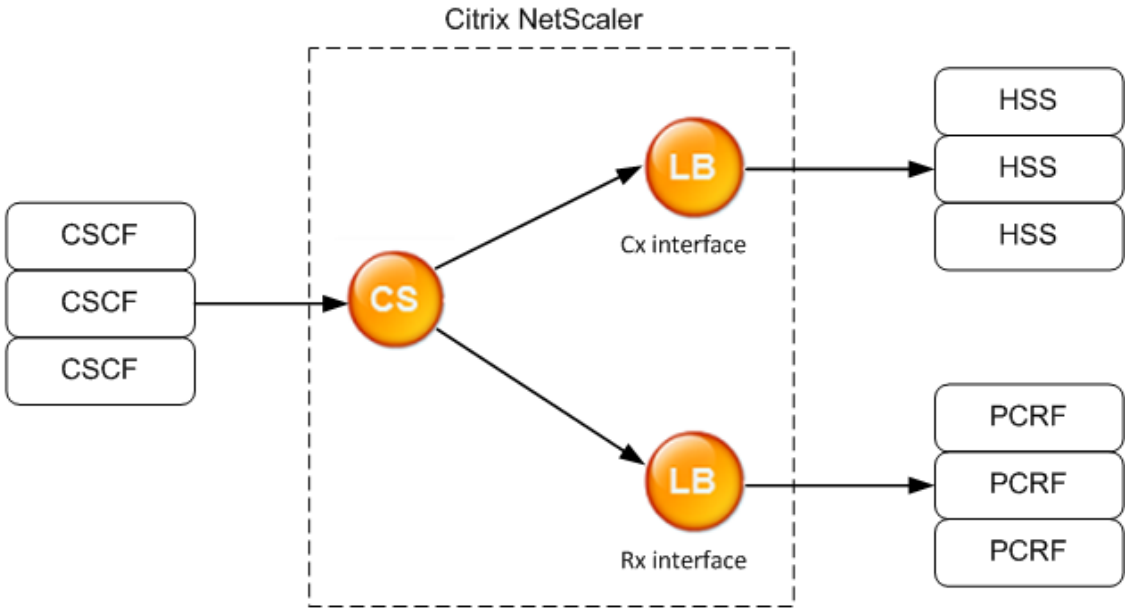
1) Policy: wiki Target: LBVIP2 Priority: 25 Hits: 0
2) Policy: plain Target: LBVIP1 Priority: 90 Hits: 0
3) Policy: DispOrderTest2 Target: KerbAuthLBVS Priority: 91 Hits: 0
4) Policy: test_Pol Target: LBVIP1 Priority: 92 Hits: 0
5) Policy: PolicyNameTesting Target: LBVIP1 Priority: 100 Hits: 0
 Done
```



```
>

show cs vserver
1) Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
…
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED

2) apubendpt (10.111.111.1:80) - HTTP Type: CONTENT
State: UP
…
Client Idle Timeout: 180 sec
Down state flush: DISABLED
…

3) apubendpt1 (10.111.111.2:80) - HTTP Type: CONTENT
State: UP
…
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
…
<!--NeedCopy-->
```

Affichage des stratégies de changement de contenu

Vous pouvez afficher les propriétés des stratégies de changement de contenu que vous avez définies, telles que le nom, le domaine, l'URL ou l'expression, et utiliser ces informations pour détecter toute erreur dans la configuration ou pour dépanner si quelque chose ne fonctionne pas correctement.

Pour afficher les propriétés des stratégies de changement de contenu à l'aide de l'interface de ligne de commande

Pour répertorier les propriétés de base de toutes les stratégies de commutation de contenu de votre configuration ou les propriétés détaillées d'une stratégie de commutation de contenu spécifique, à l'invite de commandes, tapez l'une des commandes suivantes :

```
show cs policy

show cs policy <PolicyName>
```



```
<!--NeedCopy-->
```

Exemple :

```
show cs policy

show cs policy-CS-1
<!--NeedCopy-->
```

Pour afficher les propriétés des stratégies de changement de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Changement de contenu** > **Stratégies**, sélectionnez une stratégie et, dans la liste Action, sélectionnez **Afficher les liaisons**.

Affichage d'une configuration de serveur virtuel de commutation de contenu à l'aide du visualiseur

Le visualiseur de commutation de contenu est un outil que vous pouvez utiliser pour afficher une configuration de changement de contenu au format graphique. Vous pouvez utiliser le visualiseur pour afficher les éléments de configuration suivants :

- Un résumé des serveurs virtuels d'équilibrage de charge auxquels le serveur virtuel de commutation de contenu est lié.
- Tous les services et groupes de services liés au serveur virtuel d'équilibrage de charge et tous les moniteurs liés aux services.
- Les détails de configuration de tout élément affiché.
- Toutes les stratégies liées au serveur virtuel de commutation de contenu. Il n'est pas nécessaire que ces stratégies soient des stratégies de changement de contenu. De nombreux types de stratégies, tels que les stratégies de réécriture, peuvent être liés à un serveur virtuel de commutation de contenu.

Après avoir configuré les différents éléments d'une configuration de commutation de contenu et d'équilibrage de charge, vous pouvez exporter l'intégralité de la configuration vers un fichier de modèle d'application.

> **Remarque**
>
> Le visualiseur nécessite une interface graphique, il n'est donc disponible que via l'interface graphique.

Pour afficher une configuration de commutation de contenu à l'aide du visualiseur dans l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel que vous souhaitez afficher, puis cliquez sur **Visualiseur**.
3. Dans la fenêtre **Visualiseur de changement de contenu**, vous pouvez ajuster la zone d'affichage comme suit :
    - Cliquez sur les icônes **Zoom avant** et **Zoom arrière** pour augmenter ou réduire la zone d'affichage.
    - Cliquez sur l'icône **Enregistrer l'image** pour enregistrer le graphique en tant que fichier image.
    - Dans le champ de texte Rechercher, commencez à taper le nom de l'élément que vous recherchez. Lorsque vous avez saisi suffisamment de caractères pour identifier l'élément, son emplacement est mis en surbrillance. Pour restreindre la recherche, cliquez sur le menu déroulant et sélectionnez le type d'élément que vous souhaitez rechercher.
4. Pour afficher les détails de configuration des entités liées à ce serveur virtuel, vous pouvez effectuer les opérations suivantes :
    - Pour afficher les stratégies liées au serveur virtuel, dans la barre d'outils située en haut de la boîte de dialogue, sélectionnez une ou plusieurs icônes de stratégie spécifiques aux fonctionnalités. Si les étiquettes de stratégie sont configurées, elles apparaissent dans la zone d'affichage principale.
    - Pour afficher les détails de configuration d'un service ou d'un groupe de services lié, cliquez sur l'icône du service, sur l'onglet Tâches associées, puis sur Afficher les services aux membres.
    - Pour afficher les détails de configuration d'un moniteur, cliquez sur l'icône du moniteur, cliquez sur l'onglet **Tâches associées**, puis cliquez sur **Afficher le moniteur**.
5. Pour afficher des statistiques détaillées pour n'importe quel serveur virtuel dans la configuration de commutation de contenu, cliquez sur le serveur virtuel pour lequel vous souhaitez afficher les statistiques, puis sur l'onglet Tâches associées, puis sur **Statistiques**.
6. Pour afficher une liste comparative des paramètres dont les valeurs diffèrent ou ne sont pas définies entre les conteneurs de services d'un serveur virtuel d'équilibrage de charge, cliquez sur l'icône d'un conteneur, cliquez sur l'onglet **Tâches associées**, puis sur **Différence des attributs de service**.
7. Pour afficher les détails de liaison de moniteur pour les services d'un conteneur, dans la boîte de dialogue Diff des attributs de service, dans la colonne Groupe du conteneur, cliquez sur **Détails**. Cette liste comparative vous aide à déterminer quel conteneur de services possède la

configuration que vous souhaitez appliquer à tous les conteneurs de services.

8. Pour afficher le nombre de demandes reçues par seconde à un moment donné par les serveurs virtuels de la configuration, et le nombre de demandes sélectionnées par seconde à un moment donné pour les stratégies de réécriture, de répondeur et de cache, cliquez sur Afficher les statistiques. Les informations statistiques sont affichées sur les nœuds respectifs du visualiseur. Ces informations ne sont pas mises à jour en temps réel. Il est actualisé manuellement. Pour actualiser les informations, cliquez sur Actualiser les statistiques.

   > **Remarque**
   >
   > Cette option n'est disponible que sur les versions Citrix ADC nCore.

9. Pour copier les détails de configuration d'un élément dans un document ou une feuille de calcul, cliquez sur l'icône de cet élément, sur Tâches associées, sur Copier les propriétés, puis collez les informations dans un document.
10. Pour exporter l'intégralité de la configuration affichée dans le visualiseur vers un fichier de modèle d'application, cliquez sur l'icône du serveur virtuel de commutation de contenu, cliquez sur Tâches associées, puis sur Créer un modèle. Lors de la création du modèle d'application, vous pouvez configurer des variables dans certaines expressions de stratégie et actions. Pour plus d'informations sur la création du fichier de modèle d'application et la configuration des variables pour un modèle, consultez AppExpert.

Personnalisation de la configuration de base de la commutation de contenu

October 5, 2021

Après avoir configuré une configuration de commutation de contenu de base, il se peut que vous deviez la personnaliser en fonction de vos besoins. Si vos serveurs Web sont basés sur UNIX et s'appuient sur des chemins d'accès sensibles à la casse, vous pouvez configurer la sensibilité à la casse pour l'évaluation des stratégies. Vous pouvez également définir une priorité pour l'évaluation des stratégies de changement de contenu que vous avez configurées. Vous pouvez configurer des serveurs virtuels de commutation de contenu HTTP et SSL pour qu'ils écoutent sur plusieurs ports au lieu de créer des serveurs virtuels distincts. Si vous souhaitez configurer la commutation de contenu pour un réseau local virtuel spécifique, vous pouvez configurer un serveur virtuel de commutation de contenu avec une stratégie d'écoute.

Configuration de la sensibilité à la casse pour l'évaluation des stratégies

Vous pouvez configurer le serveur virtuel de commutation de contenu pour traiter les URL comme sensibles à la casse dans les stratégies basées sur les URL. Lorsque la sensibilité à la casse est configurée, l'appliance Citrix ADC prend en compte le cas lors de l'évaluation des stratégies. Par exemple, si la sensibilité à la casse est désactivée, les URL /a/1.htm et /A/1.HTM sont traitées comme identiques. Si la sensibilité à la casse est activée, ces URL sont traitées séparément et peuvent être basculées vers des cibles différentes.

Pour configurer la sensibilité à la casse à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cs vserver \<name\> -caseSensitive (ON|OFF)
```

Exemple :

```
1 set cs vserver Vserver-CS-1 -caseSensitive ON
2 <!--NeedCopy-->
```

Pour configurer la sensibilité à la casse en utilisant l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez Paramètres de **trafic, puis Sensibles**à la casse.

Définition de la priorité pour l'évaluation des politiques

La priorité fait référence à l'ordre dans lequel les stratégies liées à un serveur virtuel sont évaluées. Il n'est pas nécessaire de configurer la priorité, la priorité par défaut fonctionne souvent correctement.

Vous pouvez configurer une priorité basée sur une URL ou une priorité basée sur des règles dans les scénarios suivants :

- Une stratégie ou un ensemble de stratégies doit être appliqué en premier lieu.
- Une autre stratégie ou ensemble de stratégies est appliqué uniquement si le premier ensemble ne correspond pas à une demande.

Priorité avec les stratégies basées sur une URL

S'il existe plusieurs URL correspondantes pour la demande entrante, la priorité (priorité) des stratégies basées sur les URL est la suivante :

1. Domaine et URL exacte

2. Domaine, préfixe et suffixe
3. Domaine et suffixe
4. Domaine et préfixe
5. Domaine uniquement
6. URL exacte
7. Préfixe et suffixe
8. Suffixe uniquement
9. Préfixe uniquement
10. Valeur par défaut

Si vous configurez la priorité en fonction de l'URL, l'URL de la demande est comparée aux URL configurées. Si aucune des URL configurées ne correspond à l'URL de la demande, les stratégies basées sur des règles sont vérifiées. Si l'URL de la demande ne correspond à aucune stratégie basée sur des règles ou si le groupe de contenu sélectionné pour la demande est en panne, la demande est traitée comme suit :

- Si vous configurez un groupe par défaut pour le serveur virtuel de commutation de contenu, la demande est transférée au groupe par défaut.
- Si le groupe par défaut configuré est arrêté ou si aucun groupe par défaut n'est configuré, un message d'erreur « HTTP 404 introuvable » est envoyé au client.

> **Remarque**
>
> Vous devez configurer la priorité basée sur l'URL si le type de contenu (par exemple, les images) est le même pour tous les clients. Toutefois, si différents types de contenu doivent être diffusés en fonction des attributs du client (tels que Accept-Language), vous devez utiliser une priorité basée sur des règles.

Priorité avec les stratégies basées sur des règles

Si vous configurez la priorité en fonction des règles, qui est le paramètre par défaut, la demande est testée en fonction des stratégies basées sur des règles que vous avez configurées. Si la demande ne correspond à aucune stratégie basée sur des règles ou si le groupe de contenu sélectionné pour la demande entrante est en panne, la demande est traitée de la manière suivante :

- Si un groupe par défaut est configuré pour le serveur virtuel de commutation de contenu, la demande est transférée au groupe par défaut.
- Si le groupe par défaut configuré est arrêté ou si aucun groupe par défaut n'est configuré, un message d'erreur « HTTP 404 introuvable » est envoyé au client.

Pour configurer la priorité à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set cs vserver \<name\> -precedence ( RULE | URL )
```

Exemple :

```
set cs vserver Vserver-CS-1 -precedence RULE
```

Pour configurer la priorité à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**, puis spécifiez Priorité.

Prise en charge de plusieurs ports pour les serveurs virtuels de commutation de contenu de type HTTP et SSL

Vous pouvez configurer Citrix ADC de sorte que les serveurs virtuels de commutation de contenu HTTP et SSL écoutent sur plusieurs ports, sans avoir à configurer des serveurs virtuels distincts. Cette fonctionnalité est particulièrement utile si vous souhaitez baser une décision de changement de contenu sur une partie de l'URL et d'autres paramètres L7. Au lieu de configurer plusieurs serveurs virtuels avec la même adresse IP et différents ports, vous pouvez configurer une adresse IP et spécifier le port sous la forme *. Par conséquent, la taille de la configuration est également réduite.

Pour configurer un serveur virtuel de commutation de contenu HTTP ou SSL afin qu'il écoute sur plusieurs ports à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
add cs vserver \<name\> \<serviceType\> \<IPAddress\> Port \*
```

Exemple

```
1  > add cs vserver cs1 HTTP 10.102.92.215 *
2   Done
3  > sh cs vserver cs1
4          cs1 (10.102.92.215:*) - HTTP    Type: CONTENT
5          State: UP
6          Last state change was at Tue May 20 01:15:49 2014
7          Time since last state change: 0 days, 00:00:03.270
8          Client Idle Timeout: 180 sec
9          Down state flush: ENABLED
10         Disable Primary Vserver On Down : DISABLED
11         Appflow logging: ENABLED
12         Port Rewrite : DISABLED
```



```
13          State Update: DISABLED
14          Default:        Content Precedence: RULE
15          Vserver IP and Port insertion: OFF
16          L2Conn: OFF     Case Sensitivity: ON
17          Authentication: OFF
18          401 Based Authentication: OFF
19          Push: DISABLED  Push VServer:
20          Push Label Rule: none
21          IcmpResponse: PASSIVE
22          RHIstate:  PASSIVE
23          TD: 0
24   Done
25  <!--NeedCopy-->
```

Pour configurer un serveur virtuel de commutation de contenu HTTP ou SSL afin qu'il écoute sur plusieurs ports à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis créez un serveur virtuel de type HTTP ou SSL.
2. Utilisez un astérisque (*) pour spécifier le port.

Configuration des serveurs virtuels génériques par VLAN

Si vous souhaitez configurer la commutation de contenu pour le trafic sur un VLAN spécifique, vous pouvez créer un serveur virtuel générique avec une stratégie d'écoute qui le limite au traitement du trafic uniquement sur le VLAN spécifié.

Pour configurer un serveur virtuel générique qui écoute un VLAN spécifique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1  add cs vserver <name> <serviceType> IPAddress `* Port *` -listenpolicy
       <expression> [-listenpriority <positive_integer>]
2  <!--NeedCopy-->
```

Exemple :

```
1  add cs vserver Vserver-CS-vlan1 ANY * *
2  -listenpolicy "CLIENT.VLAN.ID.EQ(2)"  -listenpriority 10
3  <!--NeedCopy-->
```


Pour configurer un serveur virtuel générique qui écoute un VLAN spécifique à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis configurez un serveur virtuel. Spécifiez une stratégie d'écoute qui la limite au traitement du trafic uniquement sur le VLAN spécifié.

Une fois que vous avez créé ce serveur virtuel, vous le liez à un ou plusieurs services, comme décrit dans Configuration de l'équilibrage de charge de base.

Configuration du paramètre de version de Microsoft SQL Server

Vous pouvez spécifier la version de Microsoft® SQL Server® pour un serveur virtuel de commutation de contenu de type MSSQL. Le paramètre de version est recommandé si vous pensez que certains clients n'exécutent pas la même version que votre produit Microsoft SQL Server. Le paramètre de version assure la compatibilité entre les connexions côté client et côté serveur en veillant à ce que toutes les communications soient conformes à la version du serveur.

Pour définir le paramètre de version de Microsoft SQL Server à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir le paramètre de version Microsoft SQL Server pour un serveur virtuel de commutation de contenu et vérifier la configuration :

- `set cs vserver \<name\> -mssqlServerVersion \<mssqlServerVersion\>`
- `show cs vserver \<name\>`

Exemple

```
1 > set cs vserver myMSSQLcsvip -mssqlServerVersion 2008R2 Done > show cs
      vserver myMSSQLcsvip myMSSQLcsvip (192.0.2.13:1433) - MSSQL Type:
     CONTENT State: UP . . . . . MSsql Server Version: 2008R2 . . . . .
      . Done >
2 <!--NeedCopy-->
```

Pour définir le paramètre de version de Microsoft SQL Server à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme MSSQL.
2. Dans **les paramètres avancés**, spécifiez la **version du serveur**.

Activer la vérification de l'état TCP externe pour les serveurs virtuels UDP

Dans les clouds publics, vous pouvez utiliser l'appliance Citrix ADC en tant qu'équilibreur de charge de deuxième niveau lorsque l'équilibreur de charge natif est utilisé en tant que premier niveau. L'équilibreur de charge natif peut être un équilibreur de charge d'application (ALB) ou un équilibreur de charge réseau (NLB). La plupart des clouds publics ne prennent pas en charge les sondes de santé UDP dans leurs équilibreurs de charge natifs. Pour surveiller l'état de l'application UDP, les clouds publics recommandent d'ajouter un point de terminaison TCP à votre service. Le point de terminaison reflète l'intégrité de l'application UDP.

L'appliance Citrix ADC prend en charge le contrôle d'intégrité basé sur TCP externe pour un serveur virtuel UDP. Cette fonctionnalité introduit un écouteur TCP sur la VIP du serveur virtuel de commutation de contenu et du port configuré. L'écouteur TCP reflète l'état du serveur virtuel.

Pour activer la vérification de l'état TCP externe pour les serveurs virtuels UDP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour activer une vérification d'intégrité TCP externe avec l'option tcpProbePort :

```
1 add cs vserver <name> <protocol> <IPAddress> <port> -tcpProbePort <
     tcpProbePort>
2 <!--NeedCopy-->
```

Exemple :

```
1 add cs vserver Vserver-CS-1 UDP 10.102.29.161 5002 -tcpProbePort 5000
2 <!--NeedCopy-->
```

Pour activer la vérification de l'état TCP externe pour les serveurs virtuels UDP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis créez un serveur virtuel.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel.
3. Dans le volet **Paramètres de base**, ajoutez le numéro de port dans le champ **Port de la sonde TCP** .
4. Cliquez sur **OK**.

Commutation de contenu pour le protocole de Diameter

January 21, 2021

Pour le trafic de protocole de Diameter, vous pouvez configurer l'appliance Citrix ADC (ou l'appliance virtuelle) pour qu'elle agisse en tant qu'agent relais qui équilibre la charge et transfère un paquet à la destination appropriée sur la base du contenu du message (valeur AVP dans le message). Étant donné que l'appliance n'effectue aucun traitement au niveau de l'application, elle fournit des services de relais pour toutes les applications de Diameter, comme spécifié par les stratégies de commutation de contenu configurées. Par conséquent, l'appliance annonce l'ID d'application relais dans le message CEA (Capability Exchange answer) lorsque le client établit une connexion de Diameter. Vous devez configurer un serveur virtuel de commutation de contenu, des serveurs virtuels d'équilibrage de charge et des services pour représenter les nœuds de Diameter. Lorsqu'une demande atteint le serveur virtuel de commutation de contenu, le serveur virtuel applique les stratégies de commutation de contenu associées à ce type de demande. Après avoir évalué les stratégies, le serveur virtuel de commutation de contenu achemine la demande vers le serveur virtuel d'équilibrage de charge approprié, qui l'envoie au service approprié.

Une interface de Diameter fournit une connexion entre les différents nœuds de Diameter. L'exemple de déploiement suivant utilise les interfaces Cx et Rx. Une interface Cx fournit une connexion entre un CSCF et un HSS. Une interface Rx fournit une connexion entre un CSCF et un PCRF. Tous les messages atteignent l'appliance Citrix ADC. Selon que le message concerne une interface Cx ou Rx et selon les stratégies de commutation de contenu définies, Citrix ADC sélectionne un pool de serveurs d'équilibrage de charge approprié.



CSCF=Call Session Control Function
HSS=Home Subscriber Server
PCRF=Policy and Charging Rules Function

Exemple de configuration

1. Pour chaque entité, créez un service, un serveur d'équilibrage de charge et liez le service au serveur virtuel.

```
1 add service svc_pcrf[1-3] 1.1.1.1[1-3] DIAMETER 3868
2 add service svc_hss[1-3] 1.1.1.2[1-3] DIAMETER 3868
3 add lb vserver vs_rx DIAMETER -persistenceType DIAMETER -
     persistavpno 263
4 add lb vserver vs_cx DIAMETER -persistenceType DIAMETER -
     persistavpno 263
5 bind lb vserver vs_rx svc_pcrf[1-3]
6 bind lb vserver vs_cx svc_hss[1-3]
7 <!--NeedCopy-->
```

2. Créez un serveur virtuel de commutation de contenu et deux actions (une pour chaque serveur virtuel d'équilibrage de charge). Créez deux stratégies de commutation de contenu et liez ces stratégies au serveur virtuel de commutation de contenu, en spécifiant une priorité pour chaque stratégie.

```
1 add cs vserver cs_diameter DIAMETER 10.1.1.10 3868
2 add cs action cx_action -targetLBVserver vs_cx
3 add cs action rx_action - targetLBvserver vs_rx
```



```
add cs policy cx_policy -rule "DIAMETER.REQ.AUTH_APPLICATION_ID.EQ
    (16777216)" -action cx_action
add cs policy rx_policy -rule "DIAMETER.REQ.AUTH_APPLICATION_ID.EQ
    (16777236)" -action rx_action
bind cs vserver cs_diameter -policyName rx_policy -priority 100
bind cs vserver cs_diameter -policyName cx_policy -priority 110
<!--NeedCopy-->
```

Protection de la configuration de commutation de contenu contre les défaillances

January 21, 2021

Le changement de contenu peut échouer lorsque le serveur virtuel de commutation de contenu tombe en panne ou ne parvient pas à gérer le trafic excessif, ou pour d'autres raisons. Pour réduire les risques de défaillance, vous pouvez prendre les mesures suivantes pour protéger la configuration du changement de contenu contre les défaillances :

Configuration d'un serveur virtuel de sauvegarde

Si le serveur virtuel de commutation de contenu principal est marqué « DOWN » ou « DISABLED », l'appliance Citrix ADC peut diriger les demandes vers un serveur virtuel de commutation de contenu de sauvegarde. Il peut également envoyer un message de notification au client concernant la panne ou la maintenance du site. Le serveur virtuel de commutation de contenu de sauvegarde est un proxy et est transparent pour le client.

Lors de la configuration du serveur virtuel de sauvegarde, vous pouvez spécifier le paramètre de configuration Disable Primary When Down pour vous assurer que, lorsque le serveur virtuel principal revient, il reste le secondaire jusqu'à ce que vous le forcez manuellement à prendre le relais en tant que serveur principal. Il est utile si vous souhaitez vous assurer que toutes les mises à jour de la base de données sur le serveur pour la sauvegarde sont préservées, ce qui vous permet de synchroniser les bases de données avant de restaurer le serveur virtuel principal.

Vous pouvez configurer un serveur virtuel de commutation de contenu de sauvegarde lorsque vous créez un serveur virtuel de commutation de contenu ou lorsque vous modifiez les paramètres facultatifs d'un serveur virtuel de commutation de contenu existant. Vous pouvez également configurer un serveur virtuel de commutation de contenu de sauvegarde pour un serveur virtuel de commutation de contenu de sauvegarde existant, créant ainsi des serveurs virtuels de commutation de contenu de sauvegarde en cascade. La profondeur maximale des serveurs virtuels de commutation de contenu de sauvegarde en cascade est de 10. L'appliance recherche un serveur virtuel de commutation de

contenu de sauvegarde qui est en service et accède à ce serveur virtuel de commutation de contenu pour diffuser le contenu.

> **Remarque**
>
> Si un serveur virtuel de commutation de contenu est configuré avec un serveur virtuel de commutation de contenu de sauvegarde et une URL de redirection, le serveur virtuel de commutation de contenu de sauvegarde a priorité sur l'URL de redirection. La redirection est utilisée lorsque les serveurs virtuels principaux et de sauvegarde sont en panne.

Pour configurer un serveur virtuel de commutation de contenu de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cs vserver <name> -backupVserver <string> -disablePrimaryOnDown (ON
   |OFF)
<!--NeedCopy-->
```

Exemple

```
set cs vserver Vserver-CS-1 -backupVserver Vserver-CS-2 -
   disablePrimaryOnDown ON
<!--NeedCopy-->
```

Pour configurer un serveur virtuel de commutation de contenu de sauvegarde à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme MYSQL.
2. Dans **Paramètres avancés**, sélectionnez **Protection**et spécifiez un **serveur virtuel de sauvegarde**.

Détourner le trafic excédentaire vers un serveur virtuel de sauvegarde

L'option de débordement détourne les nouvelles connexions arrivant à un serveur virtuel de commutation de contenu vers un serveur virtuel de commutation de contenu de sauvegarde lorsque le nombre de connexions au serveur virtuel de commutation de contenu dépasse la valeur de seuil configurée. La valeur de seuil est calculée dynamiquement, ou vous pouvez définir la valeur. Le nombre

de connexions établies (dans TCP) sur le serveur virtuel est comparé à la valeur seuil. Lorsque le nombre de connexions atteint le seuil, les nouvelles connexions sont détournées vers le serveur virtuel de commutation de contenu de sauvegarde.

Si les serveurs virtuels de commutation de contenu de sauvegarde atteignent le seuil configuré et ne parviennent pas à prendre la charge, le serveur virtuel de commutation de contenu principal détourne toutes les demandes vers l'URL de redirection. Si une URL de redirection n'est pas configurée sur le serveur virtuel de commutation de contenu principal, les requêtes suivantes sont supprimées.

Pour configurer un serveur virtuel de commutation de contenu pour détourner de nouvelles connexions vers un serveur virtuel de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cs vserver <name> -soMethod <methodType> -soThreshold <
    thresholdValue> -soPersistence <persistenceValue> -
    soPersistenceTimeout <timeoutValue>
<!--NeedCopy-->
```

Exemple

```
set cs vserver Vserver-CS-1 -soMethod Connection -soThreshold 1000 -
    soPersistence enabled -soPersistenceTimeout 2
<!--NeedCopy-->
```

Pour définir un serveur virtuel de commutation de contenu pour détourner de nouvelles connexions vers un serveur virtuel de sauvegarde à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme MYSQL.
2. Dans **Paramètres avancés**, sélectionnez **Protection**et configurez le débordement.

Configuration d'une URL de redirection

Vous pouvez configurer une URL de redirection pour communiquer l'état de l'appliance Citrix ADC si un serveur virtuel de commutation de contenu de type HTTP ou HTTPS est DOWN ou DISABLED. Cette URL peut être locale ou distante.

Les URL de redirection peuvent être des URL absolues ou des URL relatives. Si l'URL de redirection configurée contient une URL absolue, la redirection HTTP est envoyée à l'emplacement configuré, quelle que soit l'URL spécifiée dans la requête HTTP entrante. Si l'URL de redirection configurée contient

uniquement le nom de domaine (URL relative), la redirection HTTP est envoyée à un emplacement après avoir ajouté l'URL entrante au domaine configuré dans l'URL de redirection.

Citrix recommande d'utiliser une URL absolue. Autrement dit, une URL se terminant par/, par exemple www.example.com/ au lieu d'une URL relative. Une redirection d'URL relative peut faire en sorte que l'analyseur de vulnérabilité signale un faux positif.

> **Remarque**
>
> Si un serveur virtuel de commutation de contenu est configuré avec un serveur virtuel de sauvegarde et une URL de redirection, le serveur virtuel de sauvegarde a priorité sur l'URL de redirection. Une URL de redirection est utilisée lorsque les serveurs virtuels principaux et de sauvegarde sont en panne.

Lorsque la redirection est configurée et que le serveur virtuel de commutation de contenu n'est pas disponible, l'appliance émet une redirection HTTP 302 vers le navigateur de l'utilisateur.

Pour configurer une URL de redirection lorsque le serveur virtuel de commutation de contenu n'est pas disponible à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cs vserver <name> -redirectURL <URLValue>
<!--NeedCopy-->
```

Exemple

```
set cs vserver Vserver-CS-1 -redirectURL http://www.newdomain.com/
   mysite/maintenance
<!--NeedCopy-->
```

Pour configurer une URL de redirection lorsque le serveur virtuel de commutation de contenu n'est pas disponible à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme MYSQL.
2. Dans **Paramètres avancés**, sélectionnez **Protection**et spécifiez une URL de redirection.

Configuration de l'option de mise à jour de l'état

La fonction de commutation de contenu permet la distribution des demandes client sur plusieurs serveurs en fonction du contenu spécifique présenté aux utilisateurs. Pour une commutation de

contenu efficace, le serveur virtuel de commutation de contenu distribue le trafic aux serveurs virtuels d'équilibrage de charge en fonction du type de contenu, et les serveurs virtuels d'équilibrage de charge distribuent le trafic aux serveurs physiques selon la méthode d'équilibrage de charge spécifiée.

Pour une gestion fluide du trafic, il est important que le serveur virtuel de commutation de contenu connaisse l'état des serveurs virtuels d'équilibrage de charge. L'option de mise à jour de l'état permet de marquer le serveur virtuel de commutation de contenu comme DOWN si le serveur virtuel d'équilibrage de charge qui lui est lié est DOWN. Un serveur virtuel d'équilibrage de charge est DOWN si tous les serveurs physiques qui y sont liés sont DOWN.

Lorsque la mise à jour d'état est désactivée :

L'état du serveur virtuel de commutation de contenu est marqué comme UP. Il reste UP même s'il n'y a pas de serveur virtuel d'équilibrage de charge lié qui est UP.

Lorsque la mise à jour de l'état est activée :

Lorsque vous ajoutez un serveur virtuel de commutation de contenu, initialement, son état est affiché comme DOWN. Lorsque vous liez un serveur virtuel d'équilibrage de charge dont l'état est UP, l'état du serveur virtuel de commutation de contenu devient UP.

Si plusieurs serveurs virtuels d'équilibrage de charge sont liés et si l'un d'eux est spécifié par défaut, l'état du serveur virtuel de commutation de contenu reflète l'état du serveur virtuel d'équilibrage de charge par défaut.

Si plusieurs serveurs virtuels d'équilibrage de charge sont liés sans que l'un d'eux soit spécifié par défaut, l'état du serveur virtuel de commutation de contenu est marqué UP uniquement si tous les serveurs virtuels d'équilibrage de charge liés sont UP.

Pour configurer l'option de mise à jour d'état à l'aide de la CLI

À l'invite de commandes, tapez :

```
1 add cs vserver <name> <protocol> <ipAddress> <port> -stateUpdate
     ENABLED
2 <!--NeedCopy-->
```

Exemple

```
1  add cs vserver csw_vserver HTTP 10.18.250.154 80 -stateupdate ENABLED
      -cltTimeout 180
2 <!--NeedCopy-->
```


Pour configurer l'option de mise à jour de l'état à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme MYSQL.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres de trafic**, puis sélectionnez **Mise à jour de l'état**.

Rincer la file d'attente des surtensions

Lorsqu'un serveur physique reçoit un sursaut de demandes, il devient lent à répondre aux clients qui lui sont actuellement connectés, ce qui laisse les utilisateurs insatisfaits et mécontents. Souvent, la surcharge provoque également les clients à recevoir des pages d'erreur. Pour éviter de telles surcharges, l'appliance Citrix ADC fournit des fonctionnalités telles que la protection contre les surtensions, qui contrôle la vitesse d'établissement de nouvelles connexions à un service.

L'appliance effectue le multiplexage des connexions entre les clients et les serveurs physiques. Lorsqu'elle reçoit une demande client pour accéder à un service sur un serveur, l'appliance recherche une connexion déjà établie au serveur qui est libre. S'il trouve une connexion libre, il utilise cette connexion pour établir un lien virtuel entre le client et le serveur. S'il ne trouve pas de connexion libre existante, l'appliance établit une nouvelle connexion avec le serveur et établit un lien virtuel entre le client et le serveur. Toutefois, si l'appliance ne peut pas établir de nouvelle connexion avec le serveur, elle envoie la demande client à une file d'attente de surtension. Si tous les serveurs physiques liés au serveur virtuel d'équilibrage de charge ou de commutation de contenu atteignent la limite supérieure des connexions client (valeur maximale du client, seuil de protection contre les surtensions ou capacité maximale du service), l'appliance ne peut pas établir de connexion avec un serveur. La fonction de protection contre les surtensions utilise la file d'attente pour réguler la vitesse d'ouverture des connexions avec les serveurs physiques. L'appliance gère une file d'attente de surtension différente pour chaque service lié au serveur virtuel.

La longueur d'une file d'attente de surtension augmente lorsqu'une requête pour laquelle l'appliance ne peut pas établir de connexion, et la longueur diminue chaque fois qu'une demande de la file d'attente est envoyée au serveur ou qu'une demande est dépassée et supprimée de la file d'attente.

Si la file d'attente de surtension d'un service ou d'un groupe de services devient trop longue, vous pouvez la vider. Vous pouvez vider la file d'attente de surtension d'un service ou d'un groupe de services spécifique, ou de tous les services et groupes de services liés à un serveur virtuel d'équilibrage de charge. Le vidange d'une file d'attente de surtension n'affecte pas les connexions existantes. Seules les requêtes présentes dans la file d'attente de surtension sont supprimées. Pour ces demandes, le client doit faire une nouvelle demande.

Vous pouvez également vider la file d'attente de surtension d'un serveur virtuel de commutation de contenu. Si un serveur virtuel de commutation de contenu transfère certaines requêtes à un serveur virtuel d'équilibrage de charge particulier, et que le serveur virtuel d'équilibrage de charge reçoit

également d'autres demandes, lorsque vous videz la file d'attente de surtension du serveur virtuel de commutation de contenu, seules les demandes reçues de ce changement de contenu serveur virtuel sont vidé. Les autres requêtes de la file d'attente de surtension du serveur virtuel d'équilibrage de charge ne sont pas vidées.

> **Remarque**
>
> Vous ne pouvez pas vider les files d'attente de surtension des serveurs virtuels de redirection de cache, d'authentification, de VPN ou de serveurs virtuels GSLB ou des services GSLB.
> N'utilisez pas la fonctionnalité Protection contre les surtensions si USIP (USIP) est activée.

Pour vider une file d'attente de surtension à l'aide de l'interface de ligne de commande

La commande flush ns surgeQ fonctionne de la manière suivante :

- Vous pouvez spécifier le nom d'un service, d'un groupe de services ou d'un serveur virtuel dont la file d'attente de surtension doit être vidé.
- Si vous spécifiez un nom lors de l'exécution de la commande, la file d'attente de surtension de l'entité spécifiée est vidé. Si plusieurs entités portent le même nom, l'appliance vide les files d'attente de surtension de toutes ces entités.
- Si vous spécifiez le nom d'un groupe de services, ainsi qu'un nom de serveur et un port lors de l'exécution de la commande, l'appliance vide la file d'attente de surtension du membre du groupe de services spécifié uniquement.
- Vous ne pouvez pas spécifier directement un membre de groupe de services (<serverName> et <port>) sans spécifier le nom du groupe de services (<name>) et vous ne pouvez pas spécifier <port> sans un <serverName>. Spécifiez le <serverName> et <port> si vous souhaitez vider la file d'attente de surtension pour un membre du groupe de services spécifique.
- Si vous exécutez la commande sans spécifier de nom, l'appliance vide les files d'attente de surtension de toutes les entités présentes sur l'appliance.
- Si un membre du groupe de services est identifié par un nom de serveur, vous devez spécifier le nom du serveur dans cette commande ; vous ne pouvez pas spécifier son adresse IP.

À l'invite de commandes, tapez :

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>].
<!--NeedCopy-->
```

Exemples

```
1. flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80
The above command flushes the surge queue of the service or virtual
   server that is named SVC1ANZGB and has IP address as 10.10.10

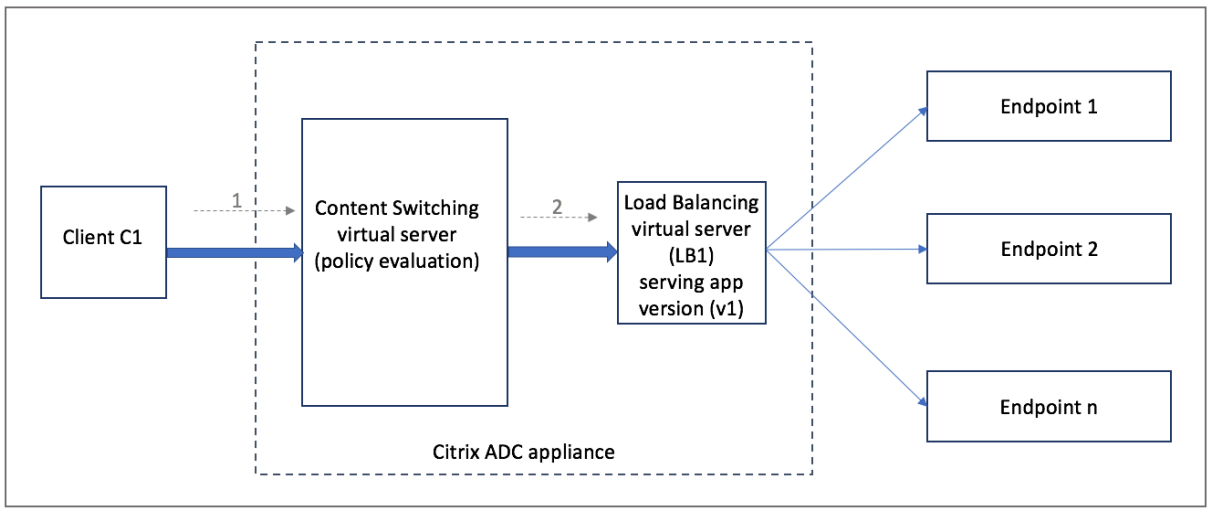
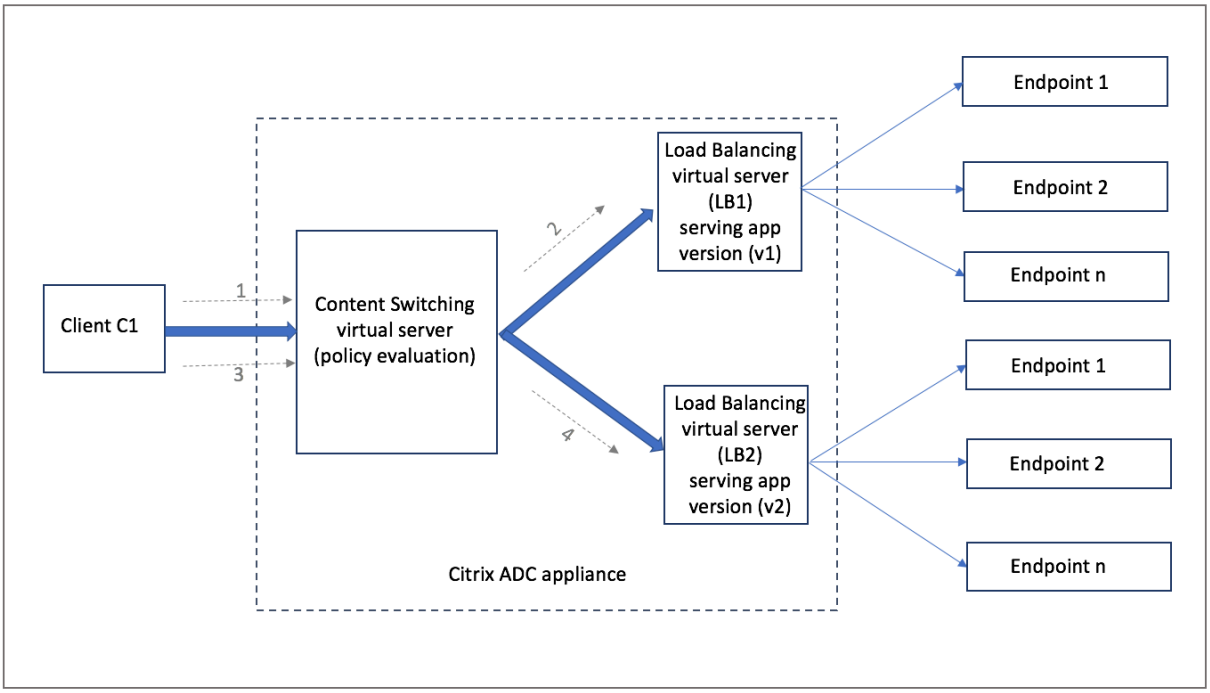
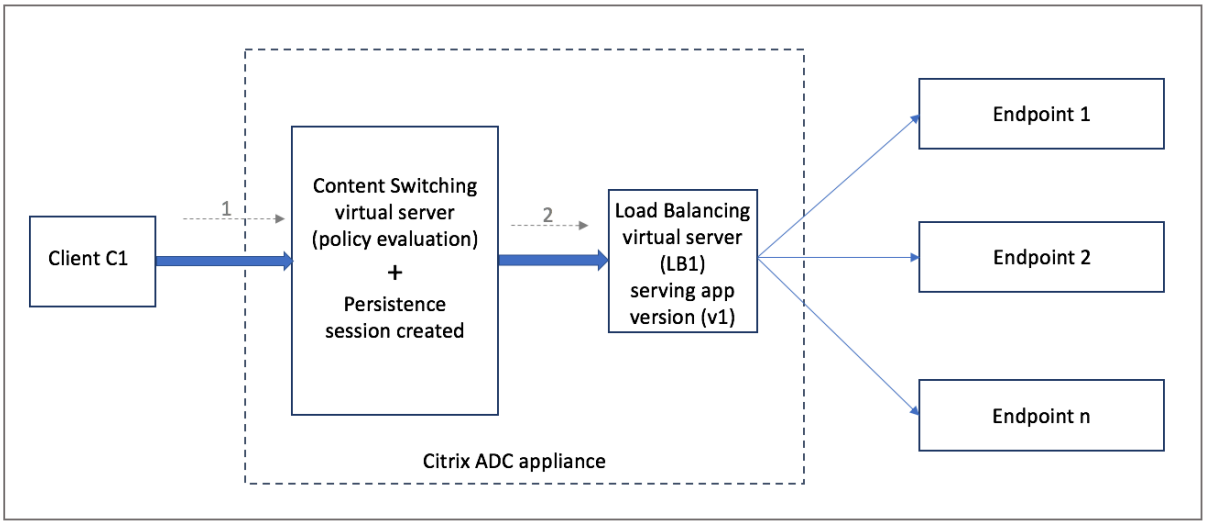
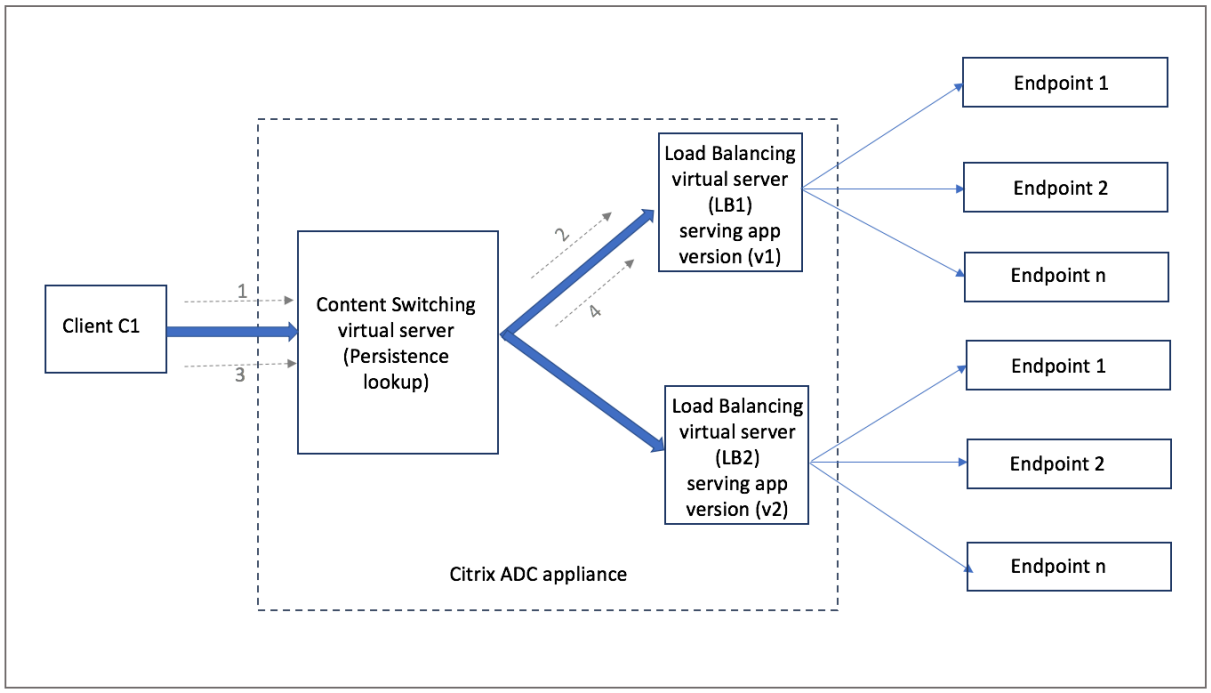
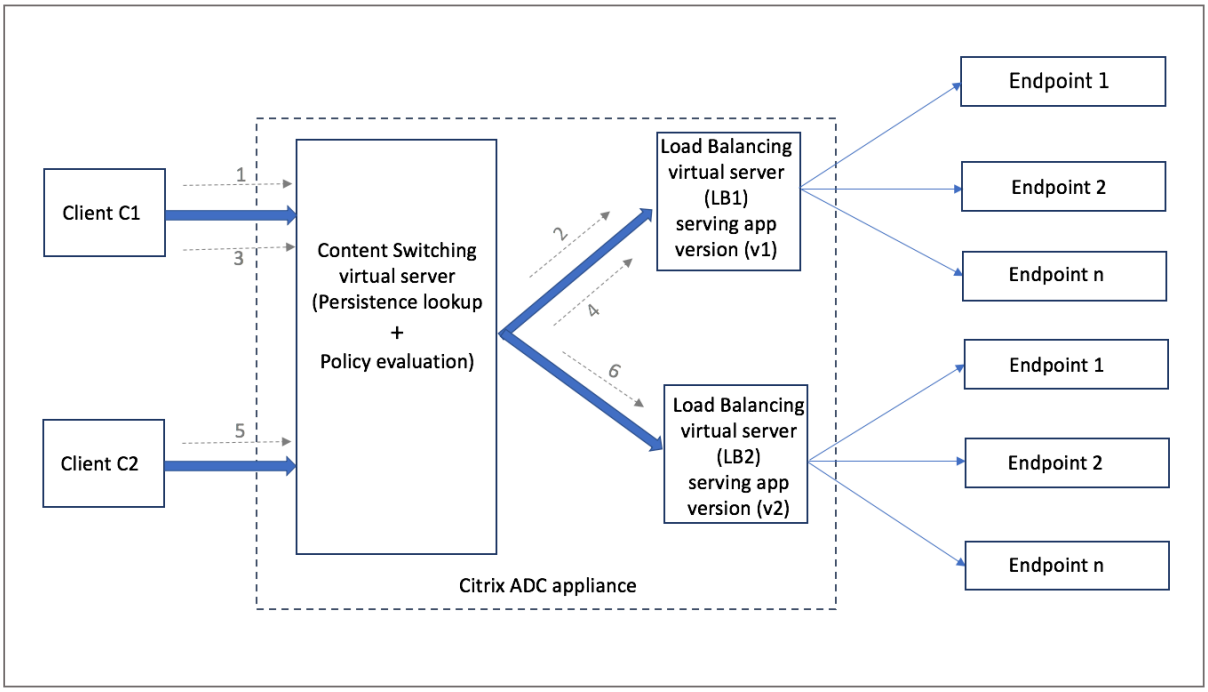
```



```
2. flush ns surgeQ
The above command flushes all the surge queues on the appliance.
<!--NeedCopy-->
```

Pour vider une file d'attente de surtension à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Changement de contenu > Serveurs virtuels**, sélectionnez un serveur virtuel et, dans la liste Action, sélectionnez **Queue d'attente de surtension**.

Gestion d'une configuration de commutation de contenu

October 5, 2021

Une fois qu'une configuration de commutation de contenu est configurée, elle peut nécessiter des modifications périodiques. Lorsque des systèmes d'exploitation ou des logiciels sont mis à jour, ou que le matériel est épuisé et remplacé, il se peut que vous deviez arrêter votre configuration. La charge de votre configuration peut augmenter et nécessiter davantage de ressources. Vous pouvez également modifier la configuration pour améliorer les performances.

Ces tâches peuvent nécessiter des stratégies de dissociation du serveur virtuel de commutation de contenu, ou la désactivation ou la suppression des serveurs virtuels de commutation de contenu. Après avoir modifié votre configuration, vous devrez peut-être réactiver les serveurs et réassocier les stratégies. Vous pouvez également renommer vos serveurs virtuels.

Stratégies de déliement du serveur virtuel de commutation de contenu

Lorsque vous disposez d'une stratégie de changement de contenu de son serveur virtuel, le serveur virtuel n'inclut plus cette stratégie lorsqu'il détermine où diriger les demandes.

Pour délier une stratégie d'un serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind cs vserver <name> -policyname <string>
```

Exemple :

```
unbind cs vserver Vserver-CS-1 -policyname Policy-CS-1
```


Pour délier une stratégie d'un serveur virtuel de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Cliquez sur la section **Stratégies**, sélectionnez la stratégie, puis cliquez sur **Unbind**.

Supprimer les serveurs virtuels de commutation de contenu

Normalement, vous supprimez un serveur virtuel de commutation de contenu uniquement lorsque vous n'avez plus besoin du serveur virtuel. Lorsque vous supprimez un serveur virtuel de commutation de contenu, l'appliance Citrix ADC délie d'abord toutes les stratégies du serveur virtuel de commutation de contenu, puis la supprime.

Pour supprimer un serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm cs vserver <name>
```

Exemple :

```
rm cs vserver Vserver-CS-1
```

Pour supprimer un serveur virtuel de commutation de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez un serveur virtuel, puis cliquez sur **Supprimer**.

Désactivation et réactivation des serveurs virtuels de commutation de contenu

Les serveurs virtuels de commutation de contenu sont activés par défaut lorsque vous les créez. Vous pouvez désactiver un serveur virtuel de commutation de contenu à des fins de maintenance. Si vous désactivez le serveur virtuel de commutation de contenu, l'état du serveur virtuel de commutation de contenu passe à Out of Service. Lorsqu'il est hors service, le serveur virtuel de commutation de contenu ne répond pas aux demandes.

Pour désactiver ou réactiver un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `disable cs vserver <name>`

- `enable cs vserver <name>`

Exemple :

```
disable cs vserver Vserver-CS-1
enable cs vserver Vserver-CS-1
```

Pour désactiver ou réactiver un serveur virtuel à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez un serveur virtuel et, dans la liste **Action**, sélectionnez **Activer** ou **désactiver**.

Changement de nom des serveurs virtuels de commutation de contenu

Vous pouvez renommer un serveur virtuel de commutation de contenu sans le délier. Le nouveau nom est automatiquement propagé à toutes les parties concernées de la configuration Citrix ADC.

Pour renommer un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rename cs vserver <name> <newName>
```

Exemple :

```
1 `rename cs vserver Vserver-CS-1 Vserver-CS-2`
```

Pour renommer un serveur virtuel à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez un serveur virtuel et, dans la liste **Action**, sélectionnez **Renommer**.

Gestion des stratégies de changement de contenu

Vous pouvez modifier une stratégie existante en configurant les règles ou en modifiant l'URL de la stratégie, ou vous pouvez supprimer une stratégie. Vous pouvez également renommer une stratégie de commutation de contenu avancée existante. Vous pouvez créer différentes stratégies en fonction de l'URL. Les stratégies basées sur l'URL peuvent être de différents types, comme décrit dans le tableau suivant.

Pour plus d'informations, voir Exemples de stratégies basées sur des URL.

> **Remarque**
>
> Vous pouvez configurer la commutation de contenu basée sur des règles à l'aide d'expressions de stratégie classiques ou d'expressions de stratégie avancées.

Pour modifier, supprimer ou renommer une stratégie à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `set cs policy <policyName> [-domain <domainValue>] [-rule <ruleValue>] [-url <URLValue>]`
- `rm cs policy <policyName>`
- `rename cs policy <policyName> <newPolicyName>`

Exemple :

```
set cs policy-CS-1 -domain "www.domainxyz.com"

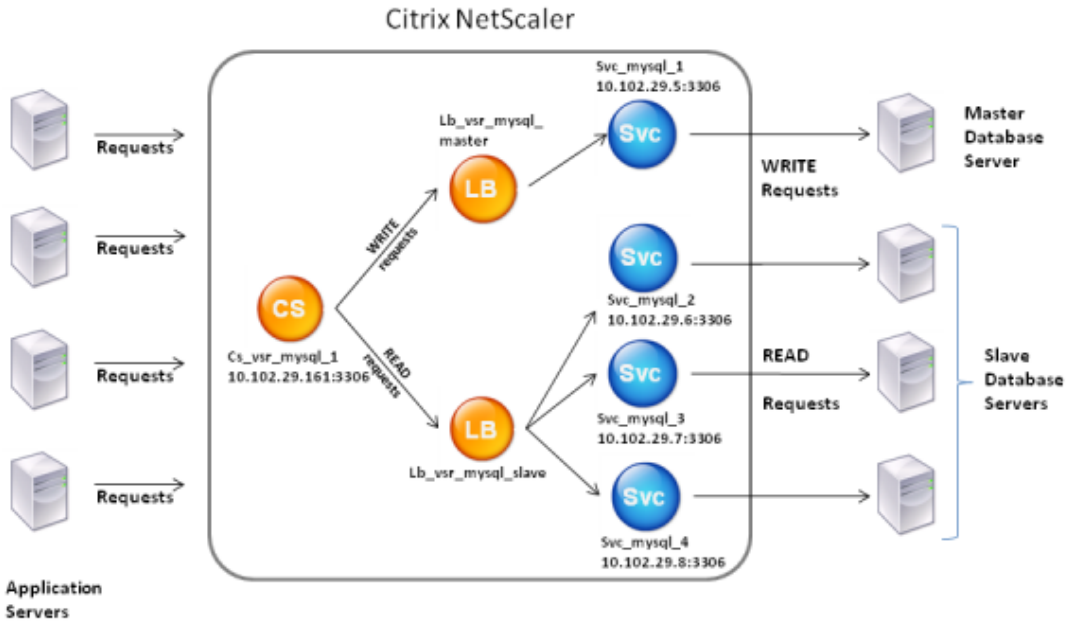
set cs policy-CS-1 -rule "CLIENT.IP.SRC.SUBNET(22).EQ(10.100.148.0)"

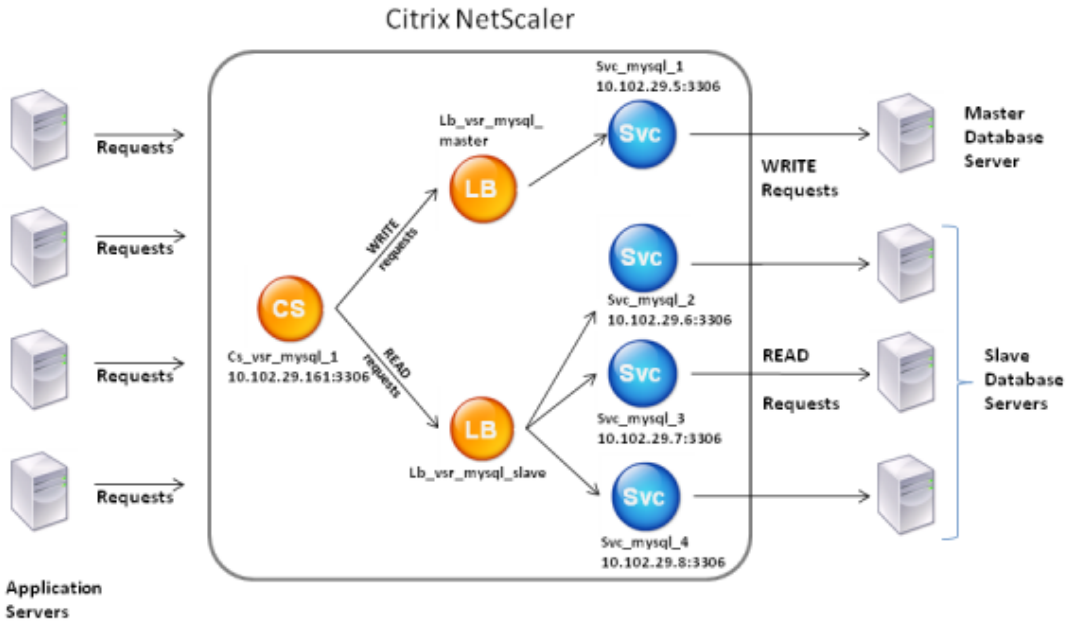
set cs policy-CS-2 -rule "SYS.TIME.BETWEEN(GMT 2010 Jun,GMT 2010 Jul)"

set cs policy-CS-1 -url /sports/*

rename cs policy-CS-1 Policy-CS-11

rm cs policy-CS-1
```

Pour modifier, supprimer ou renommer une stratégie à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Changement de contenu > Stratégies**.
2. Sélectionnez la stratégie, puis supprimez-la, modifiez-la ou, dans la liste **Action**, cliquez sur **Renommer**.

Gestion des connexions client

August 20, 2021

Pour garantir une gestion efficace des connexions client, vous pouvez configurer les serveurs virtuels de commutation de contenu sur l'appliance Citrix ADC afin d'utiliser les fonctionnalités suivantes :

- **Configuration de la réponse ICMP.** Vous pouvez configurer l'appliance Citrix ADC pour qu'elle envoie des réponses ICMP aux demandes PING en fonction de vos paramètres. Sur l'adresse IP correspondant au serveur virtuel, définissez la réponse ICMP sur VSVR_CNTRLD et, sur le serveur virtuel, définissez le serveur virtuel ICMP RESPONSE.
  Les paramètres suivants peuvent être définis sur un serveur virtuel :
  - Lorsque vous définissez le serveur virtuel ICMP RESPONSE sur PASSIF sur tous les serveurs virtuels, l'appliance Citrix ADC répond toujours.
  - Lorsque vous définissez le serveur virtuel ICMP RESPONSE sur ACTIVE sur tous les serveurs virtuels, l'appliance ADC répond même si un serveur virtuel est activé.
  - Lorsque vous définissez le serveur virtuel ICMP RESPONSE sur ACTIVE sur certains et PASSIF sur d'autres, l'appliance ADC répond même si un serveur virtuel défini sur ACTIVE est UP.

Redirection des requêtes client vers un cache

La fonctionnalité de redirection de cache Citrix ADC redirige les requêtes HTTP vers un cache. Vous pouvez réduire considérablement la charge de réponse aux requêtes HTTP et améliorer les performances de votre site Web en implémentant correctement la fonction de redirection du cache.

Un cache stocke le contenu HTTP fréquemment demandé. Lorsque vous configurez la redirection du cache sur un serveur virtuel, l'appliance Citrix ADC envoie des requêtes HTTP pouvant être mises en cache au cache et des requêtes HTTP non mises en cache au serveur Web d'origine. Pour plus d'informations sur la redirection du cache, voir « Redirection du cache ».

Pour configurer la redirection du cache sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cs vserver \<name\> -cacheable \<Value\>
```

Exemple

```
set cs vserver Vserver-CS-1 -cacheable yes
```

Pour configurer la redirection du cache sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres de trafic**, puis **Cacheable**.

Activation du nettoyage retardé des connexions de serveur virtuel

Dans certaines conditions, vous pouvez configurer le paramètre de vidage d'état en panne pour mettre fin aux connexions existantes lorsqu'un service ou un serveur virtuel est DOWN. La fin des connexions existantes libère des ressources et, dans certains cas, accélère la récupération des configurations d'équilibrage de charge surchargées.

Pour configurer le paramètre de vidage d'état en panne sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cs vserver \<name\> -downStateFlush \<Value\>
```

Exemple

```
1 set cs vserver Vserver-CS-1 -downStateFlush enabled
2 <!--NeedCopy-->
```

Pour configurer le paramètre de vidage d'état en panne sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres de trafic**, puis sélectionnez **Défoncement de l'état**.

Réécriture des ports et des protocoles pour la redirection

Les serveurs virtuels et les services qui y sont liés peuvent utiliser différents ports. Lorsqu'un service répond à une connexion HTTP avec une redirection, vous devrez peut-être configurer l'appliance Citrix ADC pour modifier le port et le protocole pour vous assurer que la redirection passe correctement. Vous le faites en activant et en configurant le paramètre redirectPortRewrite.

Pour configurer la redirection HTTP sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cs vserver \<name\> -redirectPortRewrite \<Value\>
```


Exemple

```
set cs vserver Vserver-CS-1 -redirectPortRewrite enabled
<!--NeedCopy-->
```

Pour configurer la redirection HTTP sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres de trafic**, puis **Réécrire**.

Insertion de l'adresse IP et du port d'un serveur virtuel dans l'en-tête de requête

Si plusieurs serveurs virtuels communiquent avec différentes applications sur le même service, vous devez configurer l'appliance Citrix ADC pour ajouter l'adresse IP et le numéro de port du serveur virtuel approprié aux requêtes HTTP envoyées à ce service. Ce paramètre permet aux applications exécutées sur le service d'identifier le serveur virtuel qui a envoyé la demande.

Si le serveur virtuel principal est en panne et que le serveur virtuel de sauvegarde est en service, les paramètres de configuration du serveur virtuel de sauvegarde sont ajoutés aux demandes du client. Si vous souhaitez ajouter la même balise d'en-tête, que les demandes proviennent du serveur virtuel principal ou du serveur virtuel de sauvegarde, vous devez configurer la balise d'en-tête requise sur les deux serveurs virtuels.

> **Remarque**
>
> Cette option n'est pas prise en charge pour les serveurs virtuels génériques ou les serveurs virtuels factice.

Pour insérer l'adresse IP et le port du serveur virtuel dans les demandes du client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cs vserver \<name\> -insertVserverIPPort \<vServerIPPORT\>
```

Exemple

```
set cs vserver Vserver-CS-1 -insertVserverIPPort 10.201.25.136:80
<!--NeedCopy-->
```


Pour insérer l'adresse IP et le port du serveur virtuel dans les demandes du client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres de trafic** et, dans la liste Insertion de port IP du serveur virtuel, sélectionnez VIPADR ou V6TOV4MAPPING, puis spécifiez un en-tête de port dans la valeur d'insertion du port IP du serveur virtuel.

Définition d'une valeur de délai d'attente pour les connexions client inactives

Vous pouvez configurer un serveur virtuel pour qu'il mette fin aux connexions client inactives après l'expiration d'un délai d'attente configuré. Lorsque vous configurez ce paramètre, l'appliance Citrix ADC attend le temps que vous spécifiez et, si le client est inactif après cette période, il ferme la connexion client.

Pour définir une valeur de délai d'expiration pour les connexions client inactives à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cs vserver \<name\> -cltTimeout \<Value\>
```

Exemple

```
1 set cs vserver Vserver-CS-1 -cltTimeout 100
2 <!--NeedCopy-->
```

Pour définir une valeur de délai d'expiration pour les connexions client inactives à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres de trafic**et spécifiez une valeur de **délai d'inactivité du client**.

Identification des connexions avec les paramètres de connexion 4-tuple et couche 2

Vous pouvez désormais définir l'option L2Conn pour un serveur virtuel de commutation de contenu. Lorsque l'option L2Conn est définie, les connexions au serveur virtuel de commutation de contenu sont identifiées par la combinaison des paramètres de connexion 4-tuple (<source IP>:<source

port>::<destination IP>:<destination port>) et de couche 2. Les paramètres de connexion de couche 2 sont l'adresse MAC, l'ID VLAN et l'ID de canal.

Pour définir l'option L2Conn pour un serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour configurer le paramètre L2Conn pour un serveur virtuel de commutation de contenu et vérifier la configuration :

```
1 -  set cs vserver \<name\> -l2Conn (**ON** | **OFF**)
2 -  show cs vserver \<name\>
```

Exemple

```
1  > set cs vserver mycsvserver -l2Conn ON
2  Done
3  > show cs vserver mycsvserver
4       mycsvserver (192.0.2.56:80) - HTTP   Type: CONTENT
5       State: UP
6           . . .
7           . . .
8       L2Conn: ON Case Sensitivity: ON
9           . . .
10          . . .
11 Done
12 >
13 <!--NeedCopy-->
```

Pour définir l'option L2Conn pour un serveur virtuel de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres de trafic**, puis **Paramètres de couche 2**.

Prise en charge de la persistance du serveur virtuel de commutation de contenu

August 20, 2021

Les applications passent des architectures monolithiques à l'architecture microservices. Différentes versions d'une même application peuvent coexister dans l'architecture des microservices. L'appliance Citrix ADC doit prendre en charge le déploiement continu des applications. Il est réalisé par des plates-formes qui effectuent des déploiements Canaries (tels que Spinnaker). Dans une configuration de déploiement continu, une version plus récente d'une application est déployée automatiquement et exposée au trafic client par étapes jusqu'à ce que l'application soit stable pour prendre le trafic complet. De plus, il doit y avoir des services ininterrompus au client.

La fonctionnalité de commutation de contenu Citrix ADC permet à l'appliance Citrix ADC de distribuer les demandes client sur plusieurs serveurs virtuels d'équilibrage de charge en fonction des stratégies liées au serveur virtuel de commutation de contenu.

Pour les déploiements continus, la commutation de contenu permet de sélectionner le serveur virtuel d'équilibrage de charge desservant différentes versions d'une application.

Dans la commutation de contenu, la sélection d'un serveur virtuel d'équilibrage de charge pour une version d'application spécifique change au moment de l'exécution en raison de la modification des stratégies de commutation de contenu. Au cours de cette transition, si certaines sessions sont présentes avec des versions plus anciennes de l'application, ce trafic doit continuer à être servi uniquement par des versions plus anciennes. Pour prendre en charge cette exigence, l'appliance Citrix ADC maintient la persistance sur plusieurs groupes d'équilibrage de charge derrière un serveur virtuel de commutation de contenu. La persistance du serveur virtuel de commutation de contenu permet une transition transparente des clients d'une version à l'autre.

Types de persistance pris en charge sur le serveur virtuel de commutation de contenu

Les types de persistance suivants sont pris en charge sur les serveurs virtuels de commutation de contenu.

Type de persistance	Description
IP source	**SOURCEIP**. Les connexions à partir de la même adresse IP du client font partie de la même session de persistance. Pour plus de détails, voir Persistance de l'adresse IP source.

Type de persistance	Description
Cookie HTTP	**COOKIEINSERT**. Les connexions qui ont le même en-tête de cookie HTTP font partie de la même session de persistance. Le format du cookie que l'appliance Citrix ADC insère est le suivant : **NSC_ <vid_str of CSvserver> = <vid_str of Lbvserver> où NSC_XXXX est l'ID du serveur virtuel dérivé du nom du serveur virtuel. Pour plus de détails, voir persistance des cookies HTTP.
ID de session SSL	**SSLSESSION**. Les connexions qui ont le même ID de session SSL font partie de la même session de persistance. Pour plus de détails, voir persistance des ID de session SSL.

Vous pouvez configurer une valeur de délai d'attente pour la persistance basée sur les cookies HTTP. Si vous définissez la valeur du délai d'expiration sur 0, l'appliance ADC ne spécifie pas le délai d'expiration, quelle que soit la version du cookie HTTP utilisée. Le délai d'expiration dépend alors du logiciel client, et ces cookies ne sont valides que si le logiciel est en cours d'exécution.

Selon le type de persistance que vous avez configuré, le serveur virtuel peut prendre en charge 250 000 connexions persistantes simultanées ou n'importe quel nombre de connexions persistantes jusqu'à concurrence des limites imposées par la quantité de mémoire de votre appliance Citrix ADC. Le tableau suivant montre quels types de persistance appartiennent à chaque catégorie.

Type de persistance	Nombre de connexions persistantes simultanées prises en charge
IP source, ID de session SSL	250,000
Cookie HTTP	Limite de mémoire. Dans CookieInsert, si le délai d'expiration n'est pas 0, le nombre de connexions est limité par la mémoire.

Certains types de persistance sont spécifiques à des types particuliers de serveur virtuel. Le tableau suivant répertorie chaque type de persistance et indique quels types de persistance sont pris en charge sur quels types de serveur virtuel.

Type de persis-tance	HTTP	HTTPS	TCP	UDP/IP	SSL_Pont	SSL_TCP	RTSP	SIP_UDP
SOURCEI	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
COOKIEINSERT	Oui	Oui	Non	Non	Non	Non	Non	Non
SSLSESSI	Non	Oui	Non	Non	Oui	Oui	Non	Non

Prise en charge de la persistance des sauvegardes

Vous pouvez configurer le serveur virtuel de commutation de contenu pour qu'il utilise le type de persistance IP source comme type de persistance de sauvegarde lorsque le type de persistance du cookie échoue. Il est utile pour les déploiements canaries dans l'architecture des microservices.
Lorsque le type de persistance des cookies échoue, l'appliance revient à la persistance basée sur l'IP source uniquement lorsque le navigateur client ne renvoie aucun cookie dans la requête. Cependant, si le navigateur renvoie un cookie (pas nécessairement le cookie de persistance), il est supposé que le navigateur supporte les cookies et donc la persistance de sauvegarde n'est pas déclenchée.
Vous pouvez également définir une valeur de délai d'attente pour la persistance des sauvegardes. Le délai d'expiration est la période pendant laquelle une session de persistance est en vigueur.

Fonctionnement de la persistance sur le serveur virtuel de commutation de contenu

Scénario 1 : Un serveur virtuel de commutation de contenu sans persistance

L'exemple suivant illustre le déploiement de plusieurs versions d'une application avec un serveur virtuel de commutation de contenu sans persistance.



Lorsque le client C1 envoie une demande à l'application, la demande est envoyée au serveur virtuel de commutation de contenu dans l'appliance Citrix ADC. Le serveur virtuel de commutation de contenu évalue la stratégie et transmet la demande au serveur virtuel d'équilibrage de charge (LB1) qui dessert la version v1 de l'application.



Considérons qu'une nouvelle version v2 de l'application est déployée et doit être exposée à un sous-ensemble d'utilisateurs. Le nouveau serveur virtuel d'équilibrage de charge (LB2) desservant la version v2 est lié au serveur virtuel de commutation de contenu par la stratégie de commutation de contenu appropriée.

Lorsque le client C1 envoie une nouvelle demande, la stratégie est à nouveau évaluée et la demande est transmise au serveur virtuel d'équilibrage de charge LB2. Ainsi, les transactions pour les applications avec état échouent si plusieurs versions de l'application sont déployées.

Scénario 2 : Changement de contenu serveur virtuel avec persistance

L'exemple suivant illustre le déploiement de plusieurs versions de l'application avec un serveur virtuel de commutation de contenu avec persistance.



Lorsque le client C1 envoie une demande à l'application, la demande est envoyée au serveur virtuel de commutation de contenu dans l'appliance Citrix ADC. Le serveur virtuel de commutation de contenu évalue la stratégie, crée une entrée de session de persistance et transmet la demande au serveur virtuel d'équilibrage de charge LB1 qui fournit la version v1 de l'application.



Le même client C1 demande à nouveau l'application, et la demande est envoyée au serveur virtuel de commutation de contenu dans l'appliance Citrix ADC. Une recherche de la session de persistance est effectuée et le serveur virtuel d'équilibrage de charge LB1 est extrait de la session de persistance existante et la demande est transférée à LB1. Aucune rupture de la transaction existante ne se produit avec cette solution ; par conséquent, le maintien du caractère étatique de l'application.



Considérons un nouveau client C2. La nouvelle demande C2 est envoyée à la version la plus récente de l'application par le biais d'une évaluation de stratégie, car il n'y a pas de session de persistance existante pour ce client. Il se traduit par un déploiement réussi de la version la plus récente de l'application sans rompre son état d'apatridie.

En raison de la prise en charge de la persistance, les clients peuvent déployer plusieurs contenus ou différentes versions de l'application de manière transparente sans affecter les transactions existantes, en particulier pour les applications avec état. Ce n'est pas possible sans persistance dans l'image.

Configurer le type de persistance sur le serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cs vserver <name> -PersistenceType <type> [-timeout <integer>]
<!--NeedCopy-->
```

Exemple :

```
set cs vserver Vserver-CS-1 -persistenceType SOURCEIP -timeout 60
<!--NeedCopy-->
```


Configurer le type de persistance sur le serveur virtuel de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels**, puis cliquez sur **Ajouter** .
2. Dans **Paramètres de base**, configurez les détails de persistance.

Résolution des problèmes

January 21, 2021

Si la fonctionnalité de commutation de contenu ne fonctionne pas comme prévu après l'avoir configurée, vous pouvez utiliser certains outils courants pour accéder aux ressources Citrix ADC et diagnostiquer le problème.

Ressources pour le dépannage du changement de contenu

Pour obtenir de meilleurs résultats, utilisez les ressources suivantes pour résoudre un problème de commutation de contenu sur une appliance Citrix ADC :

- Fichier de configuration
- `newnslog` Dossier pertinent
- Fichiers de suivi
- Diagramme de topologie de réseau pour la configuration réseau du client
- Documentation Citrix, telles que les notes de mise à jour, les articles du Centre de connaissances et la documentation produit.

Outre les ressources précédentes, les outils suivants accélèrent le dépannage :

- Le `iehttpheaders` ou un utilitaire similaire
- L'application Wireshark personnalisée pour les fichiers de trace Citrix ADC
- Un utilitaire SSH pour l'accès en ligne de commande
- Un utilitaire HyperTerminal pour accéder à la console

Résolution des problèmes de commutation de contenu

Les problèmes les plus courants de commutation de contenu impliquent la fonctionnalité de commutation de contenu ne fonctionne pas du tout, ou ne fonctionne que de façon intermittente, et les réponses Service non disponible.

- **Problème**

La fonction de commutation de contenu ne fonctionne pas.

Résolution

Vérifiez la configuration comme suit :

- Vérifiez que l'appliance est sous licence pour la commutation de contenu.
- Vérifiez que la fonctionnalité est activée.
- Dans le fichier de configuration, vérifiez que les stratégies de commutation de contenu valides sont correctement liées aux serveurs virtuels d'équilibrage de charge.

- **Problème**

Le client reçoit une réponse 503 - Service non disponible.

Résolution

- Vérifiez l'URL et les liaisons de stratégie. Le client reçoit la réponse 503 lorsqu'aucune des stratégies que vous avez configurées n'est évaluée et qu'aucun serveur virtuel d'équilibrage de charge par défaut n'est défini et lié au serveur virtuel de commutation de contenu.
- À partir de la configuration, vérifiez les stratégies et l'URL est accessible par le client.
- Vérifiez que, pour chaque type de demande, la stratégie correspondante est évaluée. Si la stratégie n'est pas évaluée, vérifiez l'expression de la stratégie et mettez-la à jour si nécessaire.
- Vérifiez l'URL et les en-têtes de requête et de réponse HTTP. Pour ce faire, enregistrez une `HTTPHeader` trace et, si nécessaire, enregistrez les traces de paquets sur l'appliance et le client.

- **Problème**

Par intermittence, la fonction de changement de contenu ne fonctionne pas comme prévu.

Résolution

- Étudiez le diagramme de topologie de réseau, le cas échéant, de la configuration pour comprendre les différents périphériques installés entre le client et les serveurs.
- Vérifiez la configuration et les liaisons de stratégie. Assurez-vous que l'URL de l'expression de stratégie correspond à celle de la demande client.
- Vérifiez que les priorités appropriées sont affectées aux stratégies. Une priorité ou une priorité incorrecte attribuée à une stratégie peut causer un problème.
- Exécutez les commandes suivantes pour vérifier les liaisons et les valeurs des compteurs de sélection de stratégie dans la sortie des commandes :

```
show cs vserver \<CS VServer\>

show cs policy \<CS Policy\>
```



```
stat cs vserver \<CS VServer\>
```

- À l'aide `iehttpheaders` d'un utilitaire similaire, déterminez si les en-têtes HTTP pour les requêtes ou les réponses fournissent des pointeurs vers le problème.
- Consultez les notes de mise à jour et les articles du Centre de connaissances.
- Si le problème n'est toujours pas résolu, contactez le support technique Citrix avec les données appropriées pour plus d'informations.

DataStream

August 20, 2021

La fonctionnalité Citrix ADC DataStream fournit un mécanisme intelligent de commutation de requête au niveau de la couche de base de données en distribuant les requêtes basées sur la requête SQL envoyée.

Lorsqu'il est déployé devant des serveurs de base de données, une appliance Citrix ADC assure une distribution optimale du trafic à partir des serveurs d'applications et des serveurs Web. Les administrateurs peuvent segmenter le trafic en fonction des informations contenues dans la requête SQL et en fonction des noms de base de données, des noms d'utilisateur, des jeux de caractères et de la taille des paquets.

Vous pouvez configurer l'équilibrage de charge pour basculer les demandes en fonction d'algorithmes d'équilibrage de charge. Vous pouvez également élaborer les critères de commutation en configurant la commutation de contenu pour prendre une décision basée sur un paramètre de requête SQL. Vous pouvez configurer davantage les moniteurs pour suivre l'état des serveurs de base de données.

> **Remarque**
>
> Citrix ADC DataStream est pris en charge uniquement pour les bases de données MySQL et MS SQL. Pour plus d'informations sur la version de protocole, les jeux de caractères, les requêtes spéciales et les transactions prises en charge, consultez DataStream Reference.

Fonctionnement de DataStream

Dans DataStream, l'appliance ADC est placée en ligne entre l'application ou les serveurs Web et les serveurs de base de données. Sur l'appliance, les serveurs de base de données sont représentés par des services.

Un déploiement DataStream typique se compose des entités décrites dans le diagramme suivant.

Figure 1. Modèle d'entité DataStream



Comme le montre cette figure, une configuration DataStream peut consister en :

- Serveur virtuel de commutation de contenu (CS) facultatif.
- Configuration d'équilibrage de charge consistant en des serveurs virtuels d'équilibrage de charge (LB1 et LB2).
- Services (Svc1, Svc2, Svc3 et Svc4).
- Stratégies de changement de contenu (facultatif).

Les clients (serveurs d'applications ou Web) envoient des demandes à l'adresse IP d'un serveur virtuel (CS) de commutation de contenu configuré sur l'appliance Citrix ADC. L'appliance authentifie les clients à l'aide des informations d'identification utilisateur de base de données configurées sur l'appliance. Le serveur virtuel (CS) de commutation de contenu applique les stratégies de commutation de contenu associées aux demandes. Après avoir évalué les stratégies, le serveur virtuel de commutation de contenu (CS) achemine les requêtes vers le serveur virtuel d'équilibrage de charge approprié (LB1 ou LB2). Ensuite, le serveur virtuel d'équilibrage de charge distribue les requêtes aux serveurs de base de données appropriés (représentés par les services de l'appliance) en fonction de l'algorithme d'équilibrage de charge. L'appliance Citrix ADC utilise les mêmes informations d'identification utilisateur de base de données pour authentifier la connexion avec le serveur de base de données.

Si un serveur virtuel de commutation de contenu n'est pas configuré sur l'appliance, les clients (applications ou serveurs Web) envoient leurs demandes à un serveur virtuel d'équilibrage de charge configuré sur l'appliance. L'appliance Citrix ADC authentifie le client à l'aide des informations d'identification de l'utilisateur de base de données configurées sur l'appliance, puis utilise les mêmes informations d'identification pour authentifier la connexion avec le serveur de base de données. Le serveur virtuel d'équilibrage de charge distribue les requêtes aux serveurs de base de données selon l'algorithme d'équilibrage de charge. L'algorithme d'équilibrage de charge le plus efficace pour la commutation de base de données est la méthode de connexion la plus faible.

DataStream utilise le multiplexage de connexion pour permettre à plusieurs requêtes côté client d'être effectuées sur la même connexion côté serveur. Les propriétés de connexion suivantes sont prises en compte :

- Nom d'utilisateur
- Database name
- Taille du paquet
- Jeu de caractères

Configurer les utilisateurs de base

August 20, 2021

Dans les bases de données, une connexion est toujours avec état, ce qui signifie que lorsqu'une connexion est établie, elle doit être authentifiée.

Configurez votre nom d'utilisateur et votre mot de passe de base de données sur l'appliance NetScaler. Par exemple, si vous avez un utilisateur John configuré sur la base de données, vous devez également configurer l'utilisateur John sur ADC. L'ajout de noms d'utilisateur et de mots de passe de base de données sur ADC les ajoute au fichier `nsconfig`.

> **Remarque**
>
> Les noms sont sensibles à la casse.

ADC utilise ces informations d'identification utilisateur pour authentifier les clients, puis authentifier les connexions serveur avec les serveurs de base de données.

Ajouter un utilisateur de base de données à l'aide de la CLI

À l'invite de commandes, tapez

```
add db user <username> - password <password>
```

Exemple :


```
add db user nsdbuser -password dd260427edf
<!--NeedCopy-->
```

Ajouter un utilisateur de base de données à l'aide de l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de base de données** et configurez un utilisateur de base de données.

Si vous avez modifié le mot de passe de l'utilisateur de base de données sur le serveur de base de données, vous devez réinitialiser le mot de passe de l'utilisateur correspondant configuré sur l'appliance ADC.

Réinitialiser le mot de passe d'un utilisateur de base de données à l'aide de la CLI

À l'invite de commandes, tapez

```
set db user <username> -password <password>
<!--NeedCopy-->
```

Exemple :

```
set db user nsdbuser -password dd260538abs
<!--NeedCopy-->
```

Réinitialiser le mot de passe des utilisateurs de base de données en utilisant l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de base de données**, sélectionnez un utilisateur et entrez de nouvelles valeurs pour le mot de passe.

Si un utilisateur de base de données n'existe plus sur le serveur de base de données, vous pouvez le supprimer de l'appliance ADC. Toutefois, si l'utilisateur continue d'exister sur le serveur de base de données et que vous supprimez l'utilisateur de l'appliance ADC, toute demande du client portant ce nom d'utilisateur n'est pas authentifiée. Par conséquent, la demande n'est pas acheminée vers le serveur de base de données.

Supprimer un utilisateur de base de données à l'aide de la CLI

À l'invite de commandes, tapez

```
rm db user <username>
<!--NeedCopy-->
```


Exemple :

```
rm db user nsdbuser
<!--NeedCopy-->
```

Supprimer un utilisateur de base de données à l'aide de l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de base de données**, sélectionnez un utilisateur et cliquez sur **Supprimer**.

Configurer un profil de base de données

August 20, 2021

Un profil de base de données est un ensemble nommé de paramètres configurés une fois mais appliqués à plusieurs serveurs virtuels qui nécessitent ces paramètres particuliers. Après avoir créé un profil de base de données, vous le liez à des serveurs virtuels d'équilibrage de charge ou de commutation de contenu. Vous pouvez créer autant de profils que vous le souhaitez.

Créer un profil de base de données à l'aide de la CLI

Sur la ligne de commande, tapez les commandes suivantes pour créer un profil de base de données et vérifier la configuration :

```
add db dbProfile <name> [-interpretQuery ( YES | NO )] [-stickiness (
    YES | NO )] [-kcdAccount <string>]

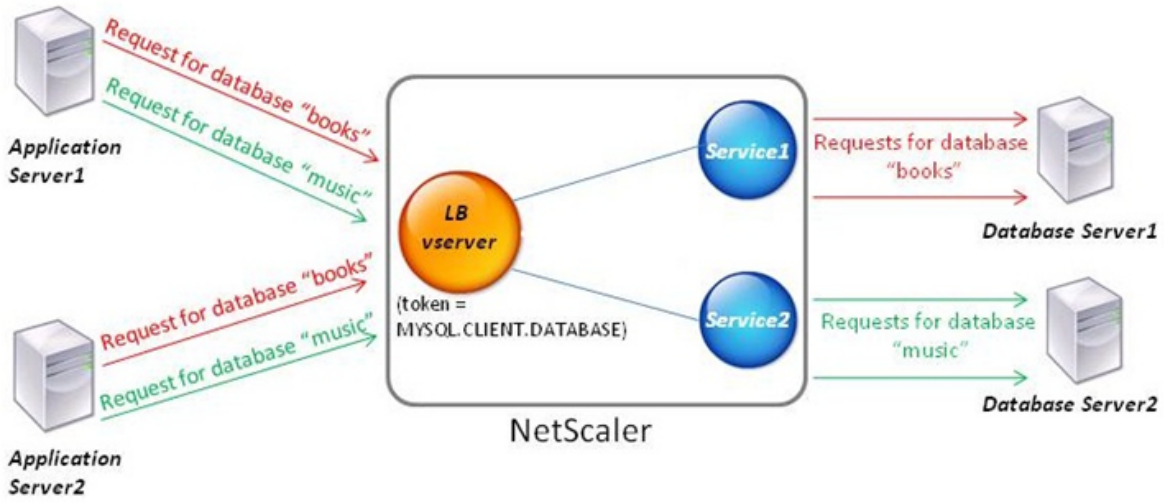
show db dbProfile
<!--NeedCopy-->
```

Exemple :

```
> add dbProfile myDBProfile -interpretQuery YES -stickiness YES -
    kcdAccount mykcdaccnt
 Done
> show dbProfile myDBProfile
    Name: myDBProfile
    Interpret Query: YES
    Stickyness: YES
    KCD Account: mykcdaccnt
    Reference count: 0
```



```
9
10   Done
11  >
12  <!--NeedCopy-->
```

Créer un profil de base de données à l'aide de l'interface graphique

Accédez à **Système > Profils** et, sous l'onglet **Profils de base** de données, configurez un profil de base de données.

Liez un profil de base de données à un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez :

```
1  set (lb | cs) vserver <name> -dbProfileName <string>
2  <!--NeedCopy-->
```

Liez un profil de base de données à un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels ou Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Profils**et, dans la liste **Profil DB**, sélectionnez un profil à lier au serveur virtuel. Pour créer un profil, cliquez sur plus (+).

Configurer l'équilibrage de charge pour DataStream

August 20, 2021

Avant de configurer une configuration d'équilibrage de charge, vous devez activer la fonction d'équilibrage de charge. Ensuite, commencez par créer au moins un service pour chaque serveur de base de données dans le groupe d'équilibrage de charge. Une fois les services configurés, vous êtes prêt à créer un serveur virtuel d'équilibrage de charge et à lier les services au serveur virtuel.

> **Remarque** :
>
> Pour les bases de données, l'équilibrage de charge ne peut se produire que sur des serveurs de base de données homogènes (serveurs de base de données qui contiennent exactement les mêmes bases de données). Pour une configuration qui contient des bases de données

> uniques sur différents serveurs, vous devez utiliser la commutation de contenu. Si certains de vos serveurs de base de données hébergent un contenu identique, vous pouvez utiliser l'équilibrage de charge sur ces serveurs uniquement. Vous pouvez ensuite utiliser des stratégies de commutation de contenu pour envoyer des demandes au serveur virtuel d'équilibrage de charge qui gère l'équilibrage de charge pour ces bases de données.
>
> L'appliance Citrix ADC stocke le nom de la base de données et les informations de connexion au cours de la session de base de données. Lorsqu'une requête est effectuée sur la base de données, elle utilise ces informations pour se connecter au serveur de base de données spécifique.

Valeurs de paramètres spécifiques à DataStream

- Protocole

  Utilisez le type de protocole MYSQL pour les bases de données MySQL et le type de protocole MSSQL pour les bases de données MS SQL lors de la configuration des serveurs et services virtuels. Les protocoles MySQL et TDS sont utilisés par les clients pour communiquer avec les serveurs de base de données respectifs à l'aide de requêtes SQL. Pour plus d'informations sur le protocole MySQL, reportez-vous à la section http://dev.mysql.com/doc/internals/en/client-server-protocol.html. Pour plus d'informations sur le protocole TDS, reportez-vous à la section http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

- Port

  Port sur lequel le serveur virtuel écoute les connexions client. Utilisez le port 3306 pour les serveurs de base de données MySQL.

- Méthode

  Il est recommandé d'utiliser la méthode de connexion minimale pour un meilleur équilibrage de charge et une charge serveur réduite. Toutefois, d'autres méthodes, telles que Round Robin, Least Response Time, Source IP Hash, Source IP Destination IP Hash, Least Bandwidth, Least Packets, et Source IP Source Port Hash, sont également prises en charge.

  Remarque : La méthode de hachage d'URL n'est pas prise en charge pour DataStream.

- Version MS SQL Server

  Si vous utilisez Microsoft SQL Server et que vous attendez que certains clients exécutent une version différente de votre produit Microsoft SQL Server, définissez le paramètre Version du serveur pour le serveur virtuel d'équilibrage de charge. Le paramètre de version assure la compatibilité entre les connexions côté client et côté serveur en veillant à ce que toutes les communications soient conformes à la version du serveur. Pour plus d'informations sur la définition du paramètre Server Version, consultez Configuration du paramètre de version MySQL et Microsoft SQL Server.

- Version du serveur MySQL

  Si vous utilisez MySQL Server et que vous attendez que certains clients exécutent une version différente de votre produit MySQL Server, définissez le paramètre Version du serveur pour le serveur virtuel d'équilibrage de charge. Le paramètre de version assure la compatibilité entre les connexions côté client et côté serveur en veillant à ce que toutes les communications soient conformes à la version du serveur. Pour plus d'informations sur la définition du paramètre Server Version, consultez Configuration du paramètre de version MySQL et Microsoft SQL Server.

Configurer la commutation de contenu pour DataStream

October 5, 2021

Vous pouvez segmenter le trafic en fonction des informations contenues dans la requête SQL, en fonction des noms de base de données, des noms d'utilisateur, des jeux de caractères et de la taille des paquets.

Vous pouvez configurer des stratégies de commutation de contenu avec des expressions de stratégie avancées pour basculer le contenu en fonction des propriétés de connexion. Par exemple, le nom d'utilisateur et le nom de la base de données, les paramètres de commande et la requête SQL pour sélectionner le serveur.

Les expressions de stratégie avancées évaluent le trafic associé aux serveurs de bases de données MYSQL et MS SQL. Utilisez des expressions basées sur les demandes dans les stratégies de stratégie avancées pour prendre des décisions de changement de demande au point de liaison du serveur virtuel de commutation de contenu. Utilisez des expressions basées sur les réponses (expressions commençant par MYSQL.RES) pour évaluer les réponses du serveur aux moniteurs d'intégrité configurés par l'utilisateur.

Pour plus d'informations sur les expressions de stratégie avancées, consultez Expressions de stratégie avancées : DataStream.

> **Remarque :**
>
> Pour les bases de données, l'équilibrage de charge ne peut avoir lieu que sur des serveurs de base de données homogènes (serveurs de base de données qui contiennent exactement les mêmes bases de données). Pour une configuration qui contient des bases de données uniques sur différents serveurs, vous devez utiliser la commutation de contenu. Si certains de vos serveurs de base de données hébergent un contenu identique, vous pouvez utiliser l'équilibrage de charge sur ces serveurs uniquement. Vous pouvez ensuite utiliser des stratégies de commutation de contenu pour envoyer des demandes au serveur virtuel d'équilibrage de charge qui gère l'équilibrage

> de charge pour ces bases de données.
>
> L'appliance Citrix ADC stocke actuellement le nom de la base de données et les informations de connexion au cours de la session de base de données. Lorsqu'une requête est effectuée dans la base de données, elle utilise ces informations pour se connecter au serveur de base de données spécifique.

Valeurs de paramètres spécifiques à DataStream

- Protocole

  Utilisez le type de protocole MYSQL pour les bases de données MySQL et le type de protocole MSSQL pour les bases de données MS SQL lors de la configuration des serveurs et services virtuels. Les protocoles MySQL et TDS sont utilisés par les clients pour communiquer avec les serveurs de base de données respectifs à l'aide de requêtes SQL. Pour plus d'informations sur le protocole MySQL, reportez-vous à la section http://dev.mysql.com/doc/internals/en/client-server-protocol.html. Pour plus d'informations sur le protocole TDS, reportez-vous à la section http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

- Port

  Port sur lequel le serveur virtuel écoute les connexions client. Utilisez le port 3306 pour les serveurs de bases de données MySQL.

- Version de MS SQL Server

  Si vous utilisez Microsoft SQL Server et que vous attendez que certains clients exécutent une version différente de celle de votre produit Microsoft SQL Server, définissez le paramètre Version du serveur pour le serveur virtuel de commutation de contenu. Le paramètre de version assure la compatibilité entre les connexions côté client et côté serveur en veillant à ce que toutes les communications soient conformes à la version du serveur. Pour plus d'informations sur la définition du paramètre Server Version, consultez Configuration du paramètre de version Microsoft SQL Server.

Configurer des moniteurs pour DataStream

August 20, 2021

Pour suivre l'état de chaque serveur de base de données à charge équilibrée en temps réel, vous devez lier un moniteur à chaque service. Le moniteur est configuré pour tester le service en envoyant des sondes périodiques au service, parfois appelées exécution d'une vérification de l'état. Si le moniteur reçoit une réponse rapide à ses sondes, il marque le service comme UP. S'il ne reçoit pas de réponse en temps opportun au nombre désigné de sondes, il marque le service comme DOWN.

Pour DataStream, vous devez utiliser les moniteurs intégrés : MYSQL-ECV et MSSQL-ECV. À l'aide de ce moniteur, vous pouvez envoyer une requête SQL et analyser la réponse pour une chaîne.

Avant de configurer des moniteurs pour DataStream, vous devez ajouter des informations d'identification utilisateur de base de données à votre appliance NetScaler. Pour plus d'informations sur la configuration des moniteurs, voir Configurer les moniteurs dans une configuration d'équilibrage de charge.

Lorsque vous créez un moniteur, une connexion TCP est établie avec le serveur de base de données et la connexion est authentifiée à l'aide du nom d'utilisateur fourni lors de la création du moniteur. Vous pouvez ensuite exécuter une requête SQL sur le serveur de base de données et évaluer la réponse du serveur pour vérifier si elle correspond à la règle configurée.

Les exemples suivants concernent les serveurs MYSQL.

Exemples :

Dans l'exemple suivant, la valeur du message d'erreur est évaluée pour déterminer l'état du serveur.

```
add lb monitor lb_mon1 MYSQL-ECV -sqlQuery "select * from
table2;" -evalrule "mysql.res.error.message.contains("Invalid
User")"-database "NS" -userName "user1"
<!--NeedCopy-->
```

Dans l'exemple suivant, le nombre de lignes dans la réponse est évalué pour déterminer l'état du serveur.

```
add lb monitor lb_mon4 MYSQL-ECV -sqlQuery "select * from
table4;" -evalrule "mysql.res.atleast_rows_count(7)" -database "NS" -
   userName "user2"
<!--NeedCopy-->
```

Dans l'exemple suivant, la valeur d'une colonne particulière est évaluée pour déterminer l'état du serveur.

```
add lb monitor lb_mon3 MYSQL-ECV
-sqlQuery "select * from ABC;" -evalrule "mysql.res.row(1).double_elem
   (2) == 345.12"
-database "NS" -userName "user3"
<!--NeedCopy-->
```

Les exemples suivants concernent les serveurs MSSQL.

Exemples :

Dans l'exemple suivant, la valeur du message d'erreur est évaluée pour déterminer l'état du serveur.


```
add lb monitor lb_mon1 MSSQL-ECV -sqlQuery "select * from
table2;" -evalrule "mssql.res.error.message.contains("Invalid
User")"-database "NS" -userName "user1"
<!--NeedCopy-->
```

Dans l'exemple suivant, le nombre de lignes dans la réponse est évalué pour déterminer l'état du serveur.

```
add lb monitor lb_mon4 MSSQL-ECV -sqlQuery "select * from
table4;" -evalrule "mssql.res.atleast_rows_count(7)" -database "NS" -
   userName "user2"
<!--NeedCopy-->
```

Dans l'exemple suivant, la valeur d'une colonne particulière est évaluée pour déterminer l'état du serveur.

```
add lb monitor lb_mon3 MSSQL-ECV
-sqlQuery "select * from ABC;" -evalrule "mssql.res.row(1).double_elem
   (2) == 345.12"
-database "NS" -userName "user3"
<!--NeedCopy-->
```

Cas d'utilisation 1 : Configurer DataStream pour une architecture de base de données primaire/secondaire

August 20, 2021

Un scénario de déploiement couramment utilisé est l'architecture de base de données principale/secondaire dans laquelle la base de données primaire réplique toutes les informations vers les bases de données secondaires.

Pour l'architecture de base de données primaire/secondaire, vous pouvez souhaiter que toutes les requêtes WRITE soient envoyées à la base de données principale et toutes les requêtes READ aux bases de données secondaires.

La figure suivante illustre les entités et les valeurs des paramètres que vous devez configurer sur l'appliance.

Figure 1. Modèle d'entité DataStream pour la configuration de base de données primaire/secondaire



Dans cet exemple de scénario, un service (SVC_MySQL_1) est créé pour représenter la base de données principale et est lié à un serveur virtuel d'équilibrage de charge (LB_VSR_MySQL_Primary). Trois autres services (SVC_MySQL_2, SVC_MySQL_3 et SVC_MySQL_4) sont créés pour représenter les trois bases de données secondaires, et ils sont liés à un autre serveur virtuel d'équilibrage de charge (LB_VSR_MySQL_Secondary).

Un serveur virtuel de commutation de contenu (CS_VSR_MySQL_1) est configuré avec les stratégies associées pour envoyer toutes les requêtes WRITE au serveur virtuel d'équilibrage de charge LB_VSR_MySQL_Primary. Toutes les requêtes READ sont envoyées au serveur virtuel d'équilibrage de charge LB_VSR_MySQL_Secondary.

Lorsqu'une demande atteint le serveur virtuel de commutation de contenu, le serveur virtuel applique les stratégies de commutation de contenu associées à cette demande. Après avoir évalué les stratégies, le serveur virtuel de commutation de contenu achemine la demande vers le serveur virtuel d'équilibrage de charge approprié, qui l'envoie au service approprié.

Le tableau suivant répertorie les noms et valeurs des entités ainsi que la stratégie configurée sur l'appliance Citrix ADC.

Type d'entité	Nom	Adresse IP	Protocole	Port	Expression.
Services	Svc_mysql_1	198.51.100.5	MYSQL	3306	SO
	Svc_mysql_2	198,51.100.6	MYSQL	3306	SO
	Svc_mysql_3	198,51.100.7	MYSQL	3306	SO
	Svc_mysql_4	198,51.100.8	MYSQL	3306	SO
Équilibrage de charge des serveurs virtuels	Lb_vsr_mysql_	198.51.100.201	MYSQL	3306	SO
	Lb_vsr_mysql_secondary	198.51.100.202	MYSQL	3306	SO
Serveur virtuel de commutation de contenu	Cs_vsr_mysql_	198.51.100.161	MYSQL	3306	SO
Stratégie de commutation de contenu	Cs_select	SO	SO	SO	`MYSQL.REQ.QUERY.COMMAND.contains("select")`

Tableau 1. Noms et valeurs des entités et des stratégies

Pour configurer DataStream pour une configuration de base de données principale/secondaire à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez

```
add service Svc_mysql_1 198.51.100.5 mysql 3306

add service Svc_mysql_2 198.51.100.6 mysql 3306

add service Svc_mysql_3 198.51.100.7 mysql 3306

add service Svc_mysql_4 198.51.100.8 mysql 3306

add lb vserver Lb_vsr_mysql_primary mysql 198.51.100.201 3306

add lb vserver Lb_vsr_mysql_secondary mysql 198.51.100.202 3306
```



```
12
13 bind lb vserver Lb_vsr_mysql_primary svc_mysql_1
14
15 bind lb vserver Lb_vsr_mysql_secondary svc_mysql_2
16
17 bind lb vserver Lb_vsr_mysql_secondary svc_mysql_3
18
19 bind lb vserver Lb_vsr_mysql_secondary svc_mysql_4
20
21 add cs vserver Cs_vsr_mysql_1 mysql 198.51.100.161 3306
22
23 add cs policy Cs_select -rule "MYSQL.REQ.QUERY.COMMAND.contains("
      select")"
24
25 bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_primary
26
27 bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_secondary -policy
      Cs_select -priority 10
28 <!--NeedCopy-->
```

Cas d'utilisation 2 : Configurer la méthode de jeton d'équilibrage de charge pour DataStream

February 12, 2021

Vous pouvez configurer la méthode jeton d'équilibrage de charge pour DataStream afin de baser la sélection des serveurs de base de données sur la valeur du jeton extrait des requêtes client (serveur d'application ou serveur Web). Ces jetons sont définis à l'aide d'expressions SQL. Pour les demandes suivantes avec le même jeton, l'appliance Citrix ADC envoie les demandes au même serveur de base de données qui a traité la demande initiale. Les demandes avec le même jeton sont envoyées au même serveur de base de données jusqu'à ce que la limite maximale de connexion soit atteinte ou que l'entrée de session ait dépassé.

Vous pouvez utiliser les exemples d'expressions SQL suivants pour définir des jetons :

MySQL	MS SQL
MYSQL.REQ.QUERY.TEXT	MSSQL.REQ.QUERY.TEXT
MYSQL.REQ.QUERY.TEXT (n)	MSSQL. REQ.QUERY.TEXT (n)
MYSQL.REQ.QUERY.COMMAND	MSSQL.REQ.QUERY.COMMAND

MySQL	MS SQL
MYSQL.CLIENT.USER	MSSQL.CLIENT.USER
MYSQL.CLIENT.DATABASE	MSSQL.CLIENT.DATABASE
MYSQL.CLIENT.CAPABILITIES	

L'exemple suivant montre comment fonctionne la fonctionnalité Citrix ADC DataStream lorsque vous configurez la méthode jeton d'équilibrage de charge.

Figure 1. DataStream et méthode jeton d'équilibrage de charge



Dans cet exemple, le jeton est le nom de la base de données. Une demande contenant des livres de jetons est envoyée au serveur de bases de données1 et une demande contenant de la musique de jetons est envoyée au serveur de bases de données2. Toutes les demandes suivantes avec des livres de jetons sont envoyées au serveur de bases de données1 et les demandes avec de la musique de jetons sont envoyées au serveur de bases de données2. Cette configuration fournit une pseudo-persistance avec les serveurs de base de données.

Configurer cet exemple à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add service Service1 192.0.2.9 MYSQL 3306
2
3 add service Service2 192.0.2.11 MYSQL 3306
4
```



```
add lb vserver token_lb_vserver MYSQL 192.0.2.15 3306 -lbmethod token -
    rule MYSQL.CLIENT.DATABASE

bind lb vserver token_lb_vserver Service1

bind lb vserver token_lb_vserver Service2
<!--NeedCopy-->
```

Configurer cet exemple à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme **MYSQL**.
2. Cliquez dans la section **Service** et configurez deux services spécifiant le protocole comme MYSQL. Liez ces services au serveur virtuel.
3. Dans **Paramètres avancés**, cliquez sur **Méthode** et, dans la liste **Méthode d'équilibrage de charge**, sélectionnez **TOKEN** et spécifiez l'expression **MYSQL.CLIENT.DATABASE**.

Cas d'utilisation 3 : Consigner les transactions MSSQL en mode transparent

August 20, 2021

Vous pouvez configurer l'appliance Citrix ADC pour qu'elle fonctionne de manière transparente entre les clients et les serveurs MSSQL, et uniquement consigner ou analyser les détails de toutes les transactions client-serveur. Le mode transparent est conçu pour que l'appliance Citrix ADC transfère uniquement les requêtes MSSQL au serveur, puis relaie les réponses du serveur aux clients. Au fur et à mesure que les demandes et les réponses passent par l'appliance, l'appliance consigne les informations qu'elle a recueillies, comme spécifié par la journalisation d'audit ou la configuration AppFlow, ou recueille des statistiques, comme spécifié par la configuration Action Analytics. Il n'est pas nécessaire d'ajouter des utilisateurs de base de données à l'appliance.

En mode transparent, l'appliance Citrix ADC n'effectue pas d'équilibrage de charge, de commutation de contenu ou de multiplexage de connexion pour les demandes. Cependant, il répond au paquet de pré-connexion d'un client au nom du serveur afin qu'il puisse empêcher le chiffrement d'être convenu lors de la négociation de pré-connexion. Le paquet de connexion et les paquets suivants sont transférés au serveur.

Récapitulatif des tâches de configuration

Pour la journalisation ou l'analyse des requêtes MSSQL en mode transparent, vous devez effectuer les opérations suivantes :

- Configurez l'appliance Citrix ADC comme Gateway par défaut pour les clients et les serveurs.
- Sur l'appliance Citrix ADC, effectuez l'une des opérations suivantes :
  - **Configurer globalement l'option USIP (USIP) d'utiliser l'adresse IP source :** créez un serveur virtuel d'équilibrage de charge avec une adresse IP générique et le numéro de port sur lequel les serveurs MSSQL écoutent les demandes (un serveur virtuel générique spécifique au port). Ensuite, activez l'option USIP globalement. Si vous configurez un serveur virtuel générique spécifique au port, vous n'avez pas besoin de créer des services MSSQL sur l'appliance. L'appliance détecte les services en fonction de l'adresse IP de destination dans les demandes du client.
  - **Si vous ne souhaitez pas configurer l'option USIP globalement :** créez des services MSSQL avec l'option USIP activée sur chacun d'eux. Si vous configurez des services, vous n'avez pas besoin de créer un serveur virtuel générique spécifique au port.
- Configurez la journalisation d'audit, AppFlow ou Action Analytics pour consigner ou collecter des statistiques sur les demandes. Si vous configurez un serveur virtuel, vous pouvez lier vos stratégies au serveur virtuel ou au point de liaison global. Si vous ne configurez pas de serveur virtuel, vous pouvez lier vos stratégies uniquement au point de liaison global.

Configurer le mode transparent à l'aide d'un serveur virtuel générique

Vous pouvez configurer le mode transparent en configurant un serveur virtuel générique spécifique au port et en activant le mode Use Source IP (USIP) globalement. Lorsqu'un client envoie à sa Gateway par défaut (l'appliance Citrix ADC) une requête avec l'adresse IP d'un serveur MSSQL dans l'en-tête de l'adresse IP de destination, l'appliance vérifie si l'adresse IP de destination est disponible. Si l'adresse IP est disponible, le serveur virtuel transmet la demande au serveur. Sinon, il supprime la demande.

Créer un serveur virtuel générique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel générique et vérifier la configuration :

```
1 add lb vserver <name> <serviceType> <IPAddress> <port>
2
3 show lb vserver <name>
4 <!--NeedCopy-->
```

Exemple :


```
> add lb vserver wildcardLbVs MSSQL * 1433
 Done
> show lb vserver wildcardLbVs
    wildcardLbVs (*:1433) - MSSQL   Type: ADDRESS
    State: UP
    . . .

 Done
>
<!--NeedCopy-->
```

Créer un serveur virtuel générique à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et créez un serveur virtuel. Spécifiez MSSQL comme protocole et * comme adresse IP.

Activer le mode USIP (USIP) à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer le mode USIP globalement et vérifier la configuration :

```
enable ns mode USIP

show ns mode
<!--NeedCopy-->
```

Exemple :

```
> enable ns mode USIP
 Done
> show ns mode

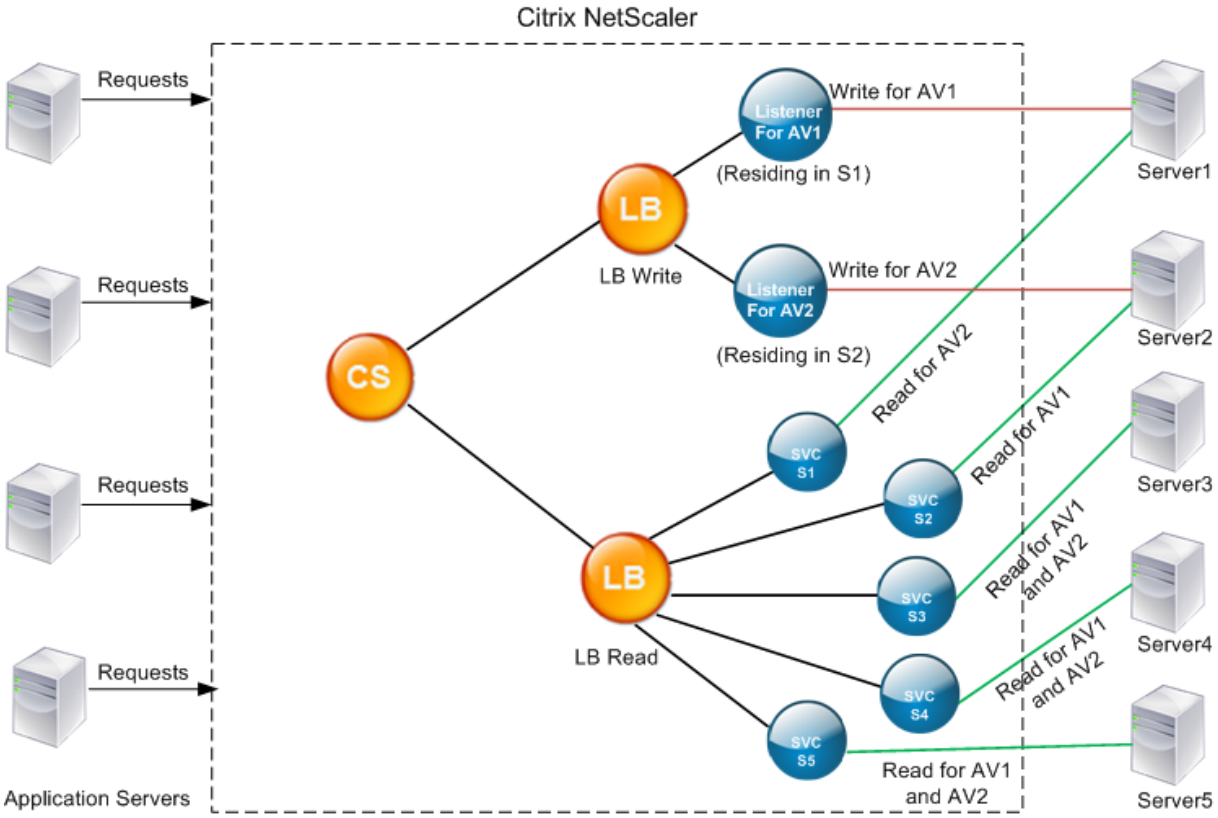
    Mode                              Acronym
       Status
    -------                           -------
       ------
                . . .
 3) Use Source IP                 USIP                           ON
                . . .
 Done
>
<!--NeedCopy-->
```


Activer le mode USIP globalement à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres** et, dans Modes et fonctionnalités, sélectionnez **Configurer les modes** .
2. Sélectionnez **Utiliser l'adresse IP source**.

Configurer le mode transparent à l'aide des services MSSQL

Vous pouvez configurer le mode transparent en configurant les services MSSQL et en activant USIP sur chaque service. Lorsqu'un client envoie sa Gateway par défaut (l'appliance Citrix ADC) une requête avec l'adresse IP d'un serveur MSSQL dans l'en-tête de l'adresse IP de destination, l'appliance transmet la demande au serveur de destination.

Créer un service MSSQL et activer le mode USIP sur le service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service MSSQL, avec USIP activé, et vérifiez la configuration :

```
add service <name> (<IP> | <serverName>) <serviceType> <port> -usip YES
    `

show service <name>
<!--NeedCopy-->
```

Exemple

```
> add service myDBservice 192.0.2.0 MSSQL 1433 -usip YES
 Done
> show service myDBservice
    myDBservice (192.0.2.0:1433) - MSSQL
    State: UP
                . . .
    Use Source IP: YES      Use Proxy Port: YES
                . . .
 Done
>
<!--NeedCopy-->
```

Créer un service MSSQL, avec USIP activé, à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et configurez un service.

2. Spécifiez le protocole comme **MSSQL** et, dans **Paramètres**, sélectionnez **Utiliser l'adresse IP source**.

Cas d'utilisation 4 : équilibrage de charge spécifique à la base de données

August 20, 2021

Une batterie de serveurs de base de données doit être équilibrée non seulement en fonction des états des serveurs, mais également de la disponibilité de la base de données sur chaque serveur. Un service peut être en service et un périphérique d'équilibrage de charge peut l'afficher comme étant à l'état UP, mais la base de données demandée peut être indisponible sur ce service. La demande n'est pas servie si une requête est transférée à un service sur lequel la base de données n'est pas disponible. Par conséquent, un périphérique d'équilibrage de charge doit être conscient de la disponibilité d'une base de données sur chaque service. Et lorsqu'il prend une décision d'équilibrage de charge, il ne doit tenir compte que des services sur lesquels la base de données est disponible.

À titre d'exemple, considérez que les serveurs de base de données server1, server2 et server3 hébergent les bases de données mydatabase1 et mydatabase2. Si mydatabase1 devient indisponible sur server2, le périphérique d'équilibrage de charge doit être conscient de ce changement d'état. Il doit équilibrer la charge des requêtes pour mydatabase1 sur uniquement server1 et server3. Une fois que mydatabase1 est disponible sur server2, le périphérique d'équilibrage de charge doit inclure server2 dans les décisions d'équilibrage de charge. De même, si mydatabase2 devient indisponible sur server3, le périphérique doit effectuer des demandes d'équilibrage de charge pour mydatabase2 uniquement sur server1 et server2. Il ne doit inclure server3 dans ses décisions d'équilibrage de charge que lorsque mydatabase2 devient disponible. Ce comportement d'équilibrage de charge doit être cohérent dans toutes les bases de données hébergées sur la batterie de serveurs.

L'appliance Citrix ADC implémente ce comportement en récupérant une liste de toutes les bases de données actives sur un service. Pour récupérer la liste des bases de données actives, l'appliance utilise un moniteur configuré avec une requête SQL appropriée. Si la base de données demandée n'est pas disponible sur un service, l'appliance exclut le service des décisions d'équilibrage de charge jusqu'à ce qu'il devienne disponible. Ce comportement assure un service ininterrompu aux clients.

> **Remarque**
>
> L'équilibrage de charge spécifique à la base de données est pris en charge uniquement pour les types de service MSSQL et MySQL. Cette prise en charge est également disponible pour le déploiement haute disponibilité de Microsoft SQL Server 2012.

Pour configurer l'équilibrage de charge spécifique à la base de données, vous devez configurer les éléments suivants :

- Activez la fonction d'équilibrage de charge et configurez un serveur virtuel d'équilibrage de charge de type MSSQL ou MySQL.
- Configurez les services qui hébergent la base de données et liez les services au serveur virtuel. Le moniteur a besoin d'informations d'identification d'utilisateur valides pour ouvrir une session sur le serveur de base de données. Vous devez donc configurer un compte d'utilisateur de base de données sur chacun des serveurs, puis ajouter le compte d'utilisateur à l'appliance Citrix ADC.
- Ensuite, vous configurez un moniteur MSSQL-ECV ou MYSQL-ECV et liez le moniteur à chaque service.
- Enfin, vous devez tester la configuration pour vous assurer qu'elle fonctionne comme prévu. Avant d'effectuer ces tâches de configuration, assurez-vous de bien comprendre le fonctionnement de l'équilibrage de charge spécifique à la base de données.

Fonctionnement de l'équilibrage de charge spécifique de base de données

Pour l'équilibrage de charge spécifique à la base de données, vous configurez un moniteur qui interroge périodiquement chaque serveur de base de données pour les noms de toutes les bases de données actives sur celui-ci. L'appliance Citrix ADC stocke les résultats et met à jour régulièrement les enregistrements en fonction des informations récupérées grâce à la surveillance. Lorsqu'un client interroge une base de données particulière, l'appliance utilise la méthode d'équilibrage de charge configurée pour sélectionner un service, puis vérifie ses enregistrements pour déterminer si la base de données est disponible sur ce service. Si les enregistrements indiquent que la base de données n'est pas disponible, elle utilise la méthode d'équilibrage de charge configurée pour sélectionner le service disponible suivant, puis répète la vérification. L'appliance transmet la requête au premier service disponible sur lequel la base de données est active.

Activer l'équilibrage de charge

Vous pouvez configurer des entités d'équilibrage de charge telles que les services et les serveurs virtuels lorsque la fonctionnalité d'équilibrage de charge est désactivée. Les entités ne fonctionnent pas tant que vous n'avez pas activé la fonction.

Activer l'équilibrage de charge à l'aide de la CLI

À l'invite de commandes, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

```
enable ns feature LB

show ns feature
<!--NeedCopy-->
```


Exemple :

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```

Activer l'équilibrage de charge à l'aide de l'interface graphique

Accédez à **Système > Paramètres** et, dans **Configurer les fonctionnalités de base**, sélectionnez **Équilibrage de charge**.

Configurer un serveur virtuel d'équilibrage de charge pour l'équilibrage de charge spécifique à la base de données

Pour configurer un serveur virtuel pour équilibrer la charge des bases de données en fonction de la disponibilité, vous activez le paramètre d'équilibrage de charge spécifique à la base de données sur le serveur virtuel. L'activation du paramètre modifie la logique d'équilibrage de charge de sorte que l'appliance Citrix ADC renvoie les résultats de la sonde de surveillance envoyée au service sélectionné, avant de transférer la requête à ce service.

Configurer un serveur virtuel d'équilibrage de charge pour l'équilibrage de charge spécifique à la base de données à l'aide de la CLI

À l'invite de commandes, tapez la commande suivante pour configurer un serveur virtuel d'équilibrage de charge pour l'équilibrage de charge spécifique à la base de données et vérifiez la configuration :

```
add lb vserver <name> <serviceType> <ipAddress> <port> -dbsLb ENABLED

show lb vserver <name>
<!--NeedCopy-->
```


Configurer les services

Après avoir activé la fonctionnalité d'équilibrage de charge, vous devez créer au moins un service pour chaque serveur d'applications qui doit être inclus dans votre configuration d'équilibrage de charge. Les services que vous configurez fournissent les connexions entre l'appliance Citrix ADC et les serveurs équilibrés de charge. Chaque service a un nom et spécifie une adresse IP, un port et le type de données qui est servi.

Si vous créez un service sans créer d'objet serveur au préalable, l'adresse IP du service est également le nom du serveur qui héberge le service. Si vous préférez identifier les serveurs par nom plutôt que par adresse IP, vous pouvez créer des objets serveur, puis spécifier le nom d'un serveur au lieu de son adresse IP lorsque vous créez un service.

Configurer les utilisateurs de base

Dans les bases de données, une connexion est toujours avec état, ce qui signifie que lorsqu'une connexion est établie, elle doit être authentifiée.

Configurez le nom d'utilisateur et le mot de passe de votre base de données sur Citrix ADC. Par exemple, si vous avez un utilisateur John configuré sur la base de données, vous devez également configurer l'utilisateur John sur ADC. Les noms d'utilisateur et mots de passe de base de données ajoutés à ADC sont ajoutés au fichier `nsconfig`.

> **Remarque**
>
> Les noms sont sensibles à la casse.

ADC utilise ces informations d'identification utilisateur pour authentifier les clients, puis authentifier les connexions serveur avec les serveurs de base de données.

Ajouter un utilisateur de base de données à l'aide de la CLI

À l'invite de commandes, tapez

```
1 add db user <username> - password <password>
2 <!--NeedCopy-->
```

Exemple :

```
1 add db user nsdbuser -password dd260427edf
2 <!--NeedCopy-->
```


Ajouter un utilisateur de base de données à l'aide de l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de base de données** et configurez un utilisateur de base de données.

Si vous avez modifié le mot de passe de l'utilisateur de base de données sur le serveur de base de données, vous devez réinitialiser le mot de passe de l'utilisateur correspondant configuré sur l'appliance Citrix ADC.

Réinitialiser le mot de passe d'un utilisateur de base de données à l'aide de la CLI

À l'invite de commandes, tapez

```
set db user <username> -password <password>
<!--NeedCopy-->
```

Exemple :

```
set db user nsdbuser -password dd260538abs
<!--NeedCopy-->
```

Réinitialiser le mot de passe des utilisateurs de base de données en utilisant l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de base de données**, sélectionnez un utilisateur et entrez de nouvelles valeurs pour le mot de passe.

Si un utilisateur de base de données n'existe plus sur le serveur de base de données, vous pouvez le supprimer de l'appliance Citrix ADC. Toutefois, si l'utilisateur continue d'exister sur le serveur de base de données et que vous supprimez l'utilisateur de l'appliance ADC, toute demande du client portant ce nom d'utilisateur n'est pas authentifiée. Par conséquent, le nom d'utilisateur n'est pas routé vers le serveur de base de données.

Supprimer un utilisateur de base de données à l'aide de la CLI

À l'invite de commandes, tapez

```
rm db user <username>
<!--NeedCopy-->
```

Exemple :

```
rm db user nsdbuser
<!--NeedCopy-->
```


Supprimer un utilisateur de base de données à l'aide de l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de base de données**, sélectionnez un utilisateur et cliquez sur **Supprimer**.

Configurer un moniteur pour récupérer les noms des bases de données actives

Vous pouvez créer un moniteur pour récupérer la liste de toutes les bases de données actives sur une instance de base de données. Le moniteur ouvre une session sur le serveur de base de données à l'aide d'informations d'identification utilisateur valides et exécute une requête SQL appropriée. La requête SQL que vous devez utiliser dépend du déploiement de votre serveur SQL. Par exemple, dans une configuration de mise en miroir de base de données MSSQL, vous pouvez utiliser la requête suivante pour récupérer une liste de bases de données actives disponibles sur une instance de serveur.

```
select name from sys.databases where state=0
<!--NeedCopy-->
```

Dans une configuration de base de données MySQL, vous pouvez utiliser les requêtes suivantes pour récupérer une liste de bases de données actives disponibles sur une instance de serveur.

Afficher les bases de données :

Vous configurez également le moniteur pour évaluer la réponse à une condition d'erreur et pour stocker les résultats s'il n'y a pas d'erreur. Si la réponse contient une erreur, le moniteur marque le service comme DOWN. L'appliance exclut le service des décisions d'équilibrage de charge jusqu'à ce qu'une erreur ne soit plus renvoyée.

> **Remarque**
>
> La fonction d'équilibrage de charge spécifique à la base de données est prise en charge uniquement pour les types de service MSSQL et MySQL. Par conséquent, le type de moniteur doit être MSSQL-ECV ou MYSQL-ECV.

Configurer un moniteur pour récupérer les noms de toutes les bases de données actives hébergées sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour récupérer les noms de toutes les bases de données actives hébergées sur un service et vérifier la configuration :

```
add lb monitor <monitorName> <type> -userName <string> -sqlQuery <text>
    -evalRule <expression> -storedb ENABLED

show lb monitor <monitorName>
<!--NeedCopy-->
```


Configurer un moniteur pour récupérer les noms de toutes les bases de données actives hébergées sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Surveille** et configurez un moniteur de type MSSQL-ECV ou MYSQL-ECV.
2. Dans **Paramètres spéciaux**, spécifiez un nom d'utilisateur, une requête et une règle. Par exemple, pour MSSQL-ECV, la requête doit être « select name from sys.databases where state=0 ») et une règle doit être MSSQL.RES.TYPE.NE (ERROR). Pour MYSQL-ECV, la requête doit être « show databases » et une règle doit être MYSQL.RES.TYPE.NE (ERROR).

Prise en charge du déploiement des groupes de disponibilité pour MSSQL

Considérons le scénario suivant dans lequel l'équilibrage de charge spécifique à la base de données est configuré dans un déploiement de groupe haute disponibilité. S1 à S5 sont les services de l'appliance ADC. DB1 à DB4 est les bases de données sur les serveurs représentés par les services S1 à S5. AV1 et AV2 sont les groupes de disponibilité. Chaque groupe de disponibilité contient jusqu'à une instance de serveur de base de données principale et jusqu'à quatre instances de serveur de base de données secondaires. Un service, représentant les serveurs du groupe de disponibilité, peut être principal pour un groupe de disponibilité et secondaire pour un autre groupe de disponibilité. Chaque groupe de disponibilité contient différentes bases de données et un écouteur, qui est un service. Toutes les demandes arrivent sur le service d'écoute qui réside dans la base de données principale. AVI contient des bases de données DB1 et DB2. AV2 contient des bases de données DB3 et DB4. L1 et L2 sont les écouteurs sur AV1 et AV2 respectivement. S1 est le service principal pour AV1 et S2 est le service principal pour AV2.



Service	Liste des bases de données actives sur le service
S1	DB1, DB2, DB3, DB4
S2	DB3, DB4
S3	DB3, DB4
S4	DB1, DB2
S5	DB1, DB2

Groupe de disponibilité	Bases de données	Services représentant les serveurs du groupe de disponibilité
AV1	DB1, DB2	S1, S4, S5
AV2	DB3, DB4	S1, S2, S3

Les requêtes s’écoulent comme suit :

1. Une requête READ pour AV1 est équilibrée de charge entre S4 et S5. S1 est le principal pour AV1.
2. Une requête WRITE pour AV1 est dirigée vers L1.
3. Une requête READ pour AV2 est équilibrée de charge entre S1 et S3. S2 est le principal pour AV2.
4. Une requête WRITE pour AV1 est dirigée vers L2.

Exemple de configuration

1. Configurez les serveurs virtuels d'équilibrage de charge et de commutation de contenu
   - `add lb vserver lbwrite -dbslb enabled`
   - `add lbvserver lbread MSSQL -dbslb enabled`
   - `add csvserver csv MSSQL 1.1.1.10 1433`
2. Configurez deux services de processus d'écoute, un pour chaque groupe de disponibilité, et cinq services S1 à S5 représentant les bases de données DB1 à DB4.
   - `add service L1 1.1.1.11 MSSQL 1433`
   - `add service L2 1.1.1.12 MSSQL 1433`
   - `add service s1 1.1.1.13 MSSQL 1433`
   - `add service s2 1.1.1.14 MSSQL 1433`
   - `add service s3 1.1.1.15 MSSQL 1433`
   - `add service s4 1.1.1.16 MSSQL 1433`
   - `add service s5 1.1.1.17 MSSQL 1433`
3. Liez les services aux serveurs virtuels d'équilibrage de charge.
   - `bind lbvserver lbwrite L1`
   - `bind lbvserver lbwrite L2`
   - `bind lbvserver lbread s1`
   - `bind lbvserver lbread s2`
   - `bind lbvserver lbread s3`
   - `bind lbvserver lbread s4`
   - `bind lbvserver lbread s5`
4. Configurer les utilisateurs de base de données.
   - `add db user nsdbuser1 -password dd260427edf`
   - `add db user nsdbuser2 -password ccd1234xyzw`
5. Configurez deux moniteurs, Monitor_L1 et Monitor_L2 pour chaque service de processus d'écoute, pour récupérer la liste des bases de données actives dans ce groupe de disponibilité. Ajoutez un moniteur, monitor1 pour récupérer la liste des bases de données de l'instance de serveur de base de données secondaire.
   - ```
     add lb monitor monitor_L1 MSSQL-ECV -userName user1 -sqlQuery "
     SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replica_
      b ON a.replica_id=b.replica_id INNER JOIN sys.availability_group_listeners
      c on b.group_id = c.group_id INNER JOIN sys.availability_group_listener_ip_a
      d on c.listener_id = d.listener_id WHERE b.role = 1 and d.ip_address
     ```


     ```

```
 like '1.1.1.11'"-evalRule "MSSQL.RES.TYPE.NE(ERROR)" -storedb
ENABLED
```

- `add lb monitor monitor_L2 MSSQL-ECV -userNameuser1 -sqlQuery "
SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replicca
 b ON a.replica_id=b.replica_id INNER JOIN sys.availability_group_listeners
 c on b.group_id = c.group_id INNER JOIN sys.availability_group_listener_ip_a
 d on c.listener_id = d.listener_id WHERE b.role = 1 and d.ip_address
 like '1.1.1.12'"-evalRule "MSSQL.RES.TYPE.NE(ERROR)"-storedb
ENABLED`
- `add lb monitor monitor1 MSSQL-ECV -userNameuser1 -sqlQuery "SELECT
name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replica_states
 b ON a.replica_id=b.replica_id WHERE b.role = 2"-evalRule "MSSQL.
RES.TYPE.NE(ERROR)"-storedb ENABLED`

6. Configurez les stratégies de lecture et d'écriture.
   - `add cs policy pol_write -rule "MSSQL.REQ.QUERY.TEXT.CONTAINS("
insert")"`
   - `add cs policy pol_read -rule "MSSQL.REQ.QUERY.TEXT.CONTAINS("select
")"`
7. Liez les stratégies au serveur virtuel de commutation de contenu.
   - `bind csvserver csv -targetLBVserver lbwrite -policyName pol_write -
priority 11`
   - `bind csvserver csv -targetLBVserver lbread -policyName pol_read -
priority 12`
8. Liez les moniteurs aux services. Liez les moniteurs aux services L1 et L2 pour obtenir la liste des bases de données actives pour le groupe de disponibilité pour lequel il est l'écouteur. Liez les moniteurs à tous les services liés au serveur virtuel en lecture seule.
   - `bind service L1 -monitorName monitor_L1`
   - `bind service L2 -monitorName monitor_L2`
   - `bind service s1 -monitorName monitor1`
   - `bind service s2 -monitorName monitor1`
   - `bind service s3 -monitorName monitor1`
   - `bind service s4 -monitorName monitor1`
   - `bind service s5 -monitorName monitor1`

Exemples de configuration pour le serveur virtuel MSSQL

Pour configurer un serveur virtuel d'équilibrage de charge pour l'équilibrage de charge spécifique à la base de données :

```
1 add lb vserver DBSpecificLB1 MSSQL 192.0.2.10 1433 -dbsLb ENABLED
```



```
2
3 Done
4
5 show lb vserver DBSpecificLB1
6
7 DBSpecificLB1 (192.0.2.10:1433) - MSSQL Type: ADDRESS
8 . . .
9 DBS_LB: ENABLED
10
11 Done
12 <!--NeedCopy-->
```

Pour configurer les services :

ajouter le service msservice1 5.5.5.5 MSSQL 1433

Pour configurer un moniteur pour récupérer les noms de toutes les bases de données actives hébergées sur un service à l'aide de la ligne de commande :

```
1 add lb monitor mssql-monitor1 MSSQL-ECV -userName user1 -sqlQuery "
     select name from sys.databases where state=0" -evalRule "MSSQL.RES.
     TYPE.NE(ERROR)" -storedb EN
2
3 Done
4
5 show lb monitor mssql-monitor1
6
7 1)   Name.......: mssql-monitor1    Type......: MSSQL-ECV
8
9 ...
10
11 Special parameters: Database.....:""
12
13 User name.....:"user1"
14
15 Query..:select name from sys.databases where state=0 EvalRule...:MSSQL.
     RES.TYPE.NE(ERROR)
16
17 Version...:70 STORE_DB...:ENABLED
18
19 Done
20 <!--NeedCopy-->
```


Exemples de configuration pour le serveur virtuel MySQL

Pour configurer un serveur virtuel d'équilibrage de charge pour l'équilibrage de charge spécifique à la base de données :

```
add lb vserver DBSpecificLB1 MYSQL 192.0.2.10 3306 -dbsLb ENABLED

Done

show lb vserver DBSpecificLB1

DBSpecificLB1 (192.0.2.10:3306) - MYSQL Type: ADDRESS

. . .

DBS_LB: ENABLED

Done
<!--NeedCopy-->
```

Pour configurer les services :

```
add service msservice1 5.5.5.5 MYSQL 3306
<!--NeedCopy-->
```

Pour configurer un moniteur pour récupérer les noms de toutes les bases de données actives hébergées sur un service à l'aide de la ligne de commande :

```
add lb monitor mysql-monitor1 MYSQL-ECV -userName user1 -sqlQuery "show
    databases" -evalRule "MYSQL.RES.TYPE.NE(ERROR)" -storedb ENABLED

Done

show lb monitor mysql-monitor1

1)     Name.......: mysql-monitor1  Type......: MYSQL-ECV  State....:
   ENABLED

...

Special parameters: Database.....:""

User name.....:"user1" Query..:show databases

EvalRule...:MYSQL.RES.TYPE.NE(ERROR) STORE_DB...:ENABLED
```



```
16
17 Done
18 <!--NeedCopy-->
```

Référence DataStream

August 20, 2021

Cette référence décrit les protocoles MySQL et TDS, les versions de la base de données, les méthodes d'authentification et les jeux de caractères pris en charge par la fonctionnalité DataStream. Il décrit également comment Citrix ADC traite les demandes de transaction et les requêtes spéciales qui modifient l'état d'une connexion.

Vous pouvez également configurer l'appliance Citrix ADC pour générer des messages de journal d'audit pour la fonctionnalité DataStream.

Versions de base de données, protocoles et méthodes d'authentification pris en charge

	Base de données MySQL	Base de données MS SQL
Versions de base de données	Base de données MySQL versions 4.1, 5.0, 5.1, 5.4, 5.5, 5.6	Base de données MS SQL versions 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014 (prise en charge de l'authentification Kerberos)
Protocoles	Protocole MySQL version 10. Pour plus d'informations sur le protocole MySQL, consultez MySQL Client/Server Protocol	Protocole TDS (Tabular Data Stream) version 7.1 et supérieure. Pour plus d'informations sur le protocole TDS, voir Tabular Data Stream Protocol.
Méthodes d'authentification	L'authentification native MySQL est prise en charge.	L'authentification SQL Server et l'authentification Windows (Kerberos/NTLM) sont prises en charge.

Jeux de caractères

La fonctionnalité DataStream prend en charge uniquement le jeu de caractères UTF-8.

Le jeu de caractères utilisé par le client lors de l'envoi d'une demande peut être différent du jeu de caractères utilisé dans les réponses du serveur de base de données. Bien que le paramètre charset soit défini lors de l'établissement de la connexion, il peut être modifié à tout moment en envoyant une requête SQL. Le jeu de caractères est associé à une connexion et, par conséquent, les requêtes sur les connexions avec un jeu de caractères ne peuvent pas être multiplexées sur une connexion avec un jeu de caractères différent.

L'appliance Citrix ADC analyse les requêtes envoyées par le client et les réponses envoyées par le serveur de base de données.

Le jeu de caractères associé à une connexion peut être modifié après la poignée de main initiale en utilisant les deux requêtes suivantes :

```
SET NAMES <charset> COLLATION <collation>

SET CHARACTER SET <charset>
<!--NeedCopy-->
```

Transactions

Dans MySQL, les transactions sont identifiées à l'aide du paramètre de connexion AUTOCOMMIT ou des requêtes BEGIN:COMMIT. Le paramètre AUTOCOMMIT peut être défini pendant la poignée de main initiale ou après l'établissement de la connexion à l'aide de la requête SET AUTOCOMMIT.

L'appliance Citrix ADC analyse explicitement chaque requête pour déterminer le début et la fin d'une transaction.

Dans le protocole MySQL, la réponse contient deux indicateurs pour indiquer si la connexion est une transaction : les indicateurs TRANSACTION et AUTOCOMMIT.

Si la connexion est une transaction, l'indicateur TRANSACTION est défini. Ou, si le mode AutoCommit est OFF, l'indicateur AUTOCOMMIT n'est pas défini. L'appliance ADC analyse la réponse et si l'indicateur TRANSACTION est défini ou si l'indicateur AUTOCOMMIT n'est pas défini, il ne procède pas au multiplexage de connexion. Lorsque ces conditions ne sont plus remplies, l'appliance ADC commence le multiplexage de connexion.

> **Remarque**
>
> Les transactions sont également prises en charge pour MS SQL.

Requêtes spéciales

Il existe des requêtes spéciales, telles que SET et PREPARE, qui modifient l'état de la connexion et peuvent interrompre la commutation de demande. Par conséquent, ces requêtes doivent être traitées différemment.

Lors de la réception d'une demande contenant des requêtes spéciales, l'appliance Citrix ADC envoie une réponse OK au client et stocke également la demande dans la connexion.

Lorsqu'une requête non spéciale, telle que INSERT et SELECT, est reçue avec une requête stockée, l'appliance ADC recherche la connexion côté serveur sur laquelle la requête stockée a déjà été envoyée au serveur de base de données. Si aucune connexion de ce type n'existe, l'appliance ADC crée une connexion et envoie d'abord la requête stockée, puis envoie la requête avec la requête non spéciale.

Dans les requêtes spéciales SET, USE db et INIT_DB, l'appliance modifie un champ de la connexion côté serveur correspondant à la requête spéciale. Cette modification permet une meilleure réutilisation de la connexion côté serveur.

Seules 16 requêtes sont stockées dans chaque connexion.

Voici une liste des requêtes spéciales pour lesquelles le dispositif ADC a un comportement modifié.

- Requête SET

  Les requêtes SQL SET définissent les variables associées à la connexion. Ces requêtes sont également utilisées pour définir des variables globales, mais à l'heure actuelle, l'appliance ADC n'est pas en mesure de faire la différence entre les variables locales et globales. Pour cette requête, l'appliance ADC utilise le mécanisme 'store and forward'.

- Requête USE <db>

  À l'aide de cette requête, l'utilisateur peut modifier la base de données associée à une connexion. Dans ce cas, l'appliance ADC analyse la valeur <db> envoyée et modifie un champ dans la connexion côté serveur pour refléter la nouvelle base de données à utiliser.

- INIT_DB, commande

  À l'aide de cette requête, l'utilisateur peut modifier la base de données associée à une connexion. Dans ce cas, l'appliance ADC analyse la valeur <init_db> envoyée et modifie un champ dans la connexion côté serveur pour refléter la nouvelle base de données à utiliser.

- COM_PREPARE

  L'appliance ADC arrête l'activation de la demande lors de la réception de cette commande.

- Requête PREPARE

  Cette requête est utilisée pour créer des instructions préparées qui sont associées à une connexion. Pour cette requête, l'appliance ADC utilise le mécanisme 'store and forward'.

Support des messages du journal d'audit

Vous pouvez maintenant configurer l'appliance Citrix ADC pour générer des messages de journal d'audit pour la fonctionnalité DataStream. Les messages du journal d'audit sont générés lorsque des connexions côté client et côté serveur sont établies, fermées ou supprimées. Les catégories de messages que vous pouvez enregistrer et afficher sont ERREUR et INFO. Les messages d'erreur pour les connexions côté client commencent par « CS » et les messages d'erreur pour les connexions côté serveur commencent par « SS ». Des informations supplémentaires sont fournies si nécessaire. Par exemple, les messages de journalisation pour les connexions fermées (CS_CONN_CLOSED) incluent uniquement l'ID de connexion. Toutefois, les messages de journal pour les connexions établies (CS_CONN_ESTD) incluent des informations telles que le nom d'utilisateur, le nom de la base de données et l'adresse IP du client en plus de l'ID de connexion.

Système de noms de domaine

January 21, 2021

Remarque : à partir de la version 13.0 build 41.x, l'appliance Citrix ADC en mode ADNS et proxy est entièrement conforme au jour de l'indicateur DNS 2019.

Vous pouvez configurer l'appliance Citrix ADC pour qu'elle fonctionne en tant que serveur de noms de domaine faisant autorité (serveur ADNS) pour un domaine. Ajoutez les enregistrements de ressources DNS appartenant au domaine pour lequel l'appliance fait autorité et configurez les paramètres d'enregistrement de ressources. Vous pouvez également configurer l'appliance en tant que serveur DNS proxy qui équilibre la charge d'une batterie de serveurs de noms DNS qui se trouvent à l'intérieur ou à l'extérieur de votre réseau. Configurez l'appliance en tant que résolveur final et redirecteur. Vous pouvez configurer des suffixes DNS qui permettent la résolution de noms lorsque les noms de domaine complets ne sont pas configurés. L'appliance prend également en charge la requête DNS ANY qui récupère tous les enregistrements appartenant à un domaine.

Vous pouvez configurer l'appliance pour qu'elle fonctionne simultanément en tant que serveur DNS faisant autorité pour un domaine et serveur proxy DNS pour un autre domaine. Lorsque vous configurez l'appliance en tant que serveur DNS ou serveur proxy DNS faisant autorité pour une zone, vous pouvez autoriser l'appliance à utiliser le protocole TCP pour les tailles de réponse qui dépassent la limite de taille spécifiée pour le protocole UDP (User Datagram Protocol).

Fonctionnement du DNS sur Citrix ADC

Vous pouvez configurer l'appliance Citrix ADC pour qu'elle fonctionne en tant que serveur ADNS, serveur proxy DNS, résolveur final et redirecteur. Vous pouvez ajouter des enregistrements de ressources DNS sur l'appliance Citrix ADC, y compris les enregistrements suivants :

- Enregistrements de service (SRV)
- Enregistrements IPv6 (AAAA)
- Enregistrements d'adresse (A)
- Enregistrements d'échange de courrier (MX)
- Enregistrements de nom canonique (CNAME)
- Enregistrements de pointeur (PTR)
- Enregistrements de début d'autorisation (SOA)
- Enregistrements texte (TXT)

En outre, vous pouvez configurer Citrix ADC pour équilibrer la charge des serveurs de noms DNS externes.

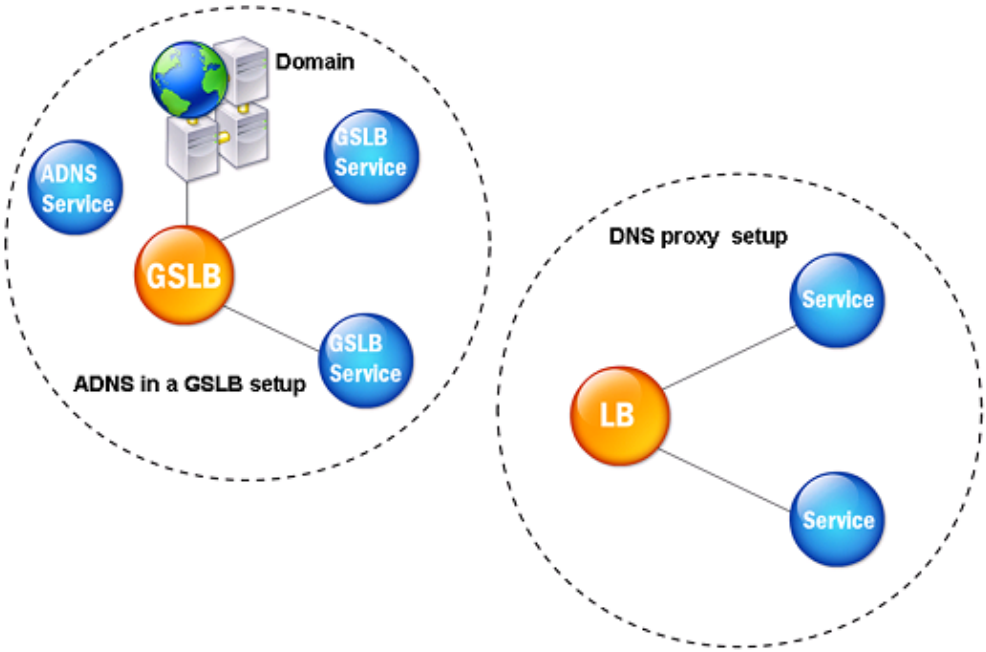
L'appliance Citrix ADC peut être configurée en tant qu'autorité pour un domaine. Ajoutez des enregistrements SOA et NS valides pour le domaine.

Un serveur ADNS est un serveur DNS qui contient des informations complètes sur une zone.

Pour configurer l'appliance Citrix ADC en tant que serveur ADNS pour une zone, vous devez ajouter un service ADNS, puis configurer la zone. Pour ce faire, vous ajoutez des enregistrements SOA et NS valides pour le domaine. Lorsqu'un client envoie une demande DNS, l'appliance Citrix ADC recherche le nom de domaine dans les enregistrements de ressources configurés. Vous pouvez configurer le service ADNS à utiliser avec la fonctionnalité GSLB (Global Server Load Balancing) Citrix ADC.

Vous pouvez déléguer un sous-domaine en ajoutant des enregistrements NS pour le sous-domaine à la zone du domaine parent. Vous pouvez ensuite rendre Citrix ADC faisant autorité pour le sous-domaine, en ajoutant un « enregistrement de colle » pour chacun des serveurs de noms de sous-domaine. Si GSLB est configuré, Citrix ADC prend une décision d'équilibrage de charge GSLB en fonction de sa configuration et répond avec l'adresse IP du serveur virtuel sélectionné. La figure suivante montre les entités d'une configuration GSLB ADNS et d'une configuration de proxy DNS.

Figure 1. Modèle d'entité proxy DNS



L'appliance Citrix ADC peut fonctionner en tant que proxy DNS. La mise en cache des enregistrements DNS, qui est une fonction importante d'un proxy DNS, est activée par défaut sur l'appliance Citrix ADC. La mise en cache permet à l'appliance Citrix ADC de fournir des réponses rapides pour les traductions répétées. Créez un serveur virtuel DNS d'équilibrage de charge et des services DNS, puis liez ces services au serveur virtuel.

Citrix ADC offre deux options, la durée de vie minimale (TTL) et la durée de vie maximale pour configurer la durée de vie des données mises en cache. Les données mises en cache durent comme spécifié par vos paramètres pour ces deux options. Citrix ADC vérifie la TTL de l'enregistrement DNS provenant du serveur. Si la TTL est inférieure à la TTL minimale configurée, elle est remplacée par la TTL minimale configurée. Si la TTL est supérieure à la TTL maximale configurée, elle est remplacée par la TTL maximale configurée.

Citrix ADC permet également la mise en cache des réponses négatives pour un domaine. Une réponse négative indique que les informations sur un domaine demandé n'existent pas ou que le serveur ne peut pas fournir de réponse à la requête. Le stockage de ces informations est appelé *mise en cache négative*. La mise en cache négative permet d'accélérer les réponses aux requêtes sur un domaine et peut éventuellement fournir le type d'enregistrement.

Une réponse négative peut être l'une des réponses suivantes :

- Message d'erreur NXDOMAIN - Si une réponse négative est présente dans le cache local, Citrix ADC renvoie un message d'erreur (NXDOMAIN). Si la réponse n'est pas dans le cache local, la requête est transférée au serveur et le serveur renvoie une erreur NXDOMAIN au contrôleur de domaine Citrix ADC. Citrix ADC met en cache la réponse localement, puis renvoie le message d'erreur au client.
- Message d'erreur NODATA - Le Citrix ADC envoie un message d'erreur NODATA, si le nom de domaine dans la requête est valide mais que les enregistrements du type donné ne sont pas disponibles.

Le Citrix ADC prend en charge la résolution récursive des requêtes DNS. En résolution récursive, le résolveur (client DNS) envoie une requête récursive à un serveur de noms pour un nom de domaine. Si le serveur de noms interrogé fait autorité pour le domaine, il répond avec le nom de domaine demandé. Sinon, Citrix ADC interroge les serveurs de noms de manière récursive jusqu'à ce que le nom de domaine demandé soit trouvé.

Avant de pouvoir appliquer l'option de requête récursive, vous devez d'abord l'activer. Vous pouvez également définir le nombre de fois que le résolveur DNS doit envoyer une demande de résolution (nouvelles tentatives DNS) si une recherche DNS échoue.

Vous pouvez configurer Citrix ADC en tant que redirecteur DNS. Un redirecteur transmet les demandes DNS aux serveurs de noms externes. Le Citrix ADC vous permet d'ajouter des serveurs de noms externes et fournit une résolution de noms pour les domaines en dehors du réseau. Citrix ADC vous permet également de définir la priorité de recherche de nom sur DNS ou WINS (Windows Internet Name Service).

Autoriser l'appliance ADC à utiliser DNS pour résoudre le nom d'hôte à son adresse IP respective

Remarque : vous avez besoin d'un utilitaire SSH pour accéder à l'interface de ligne de commande (CLI) de l'appliance.

Par défaut, l'appliance ADC ne peut pas résoudre le nom d'hôte à son adresse IP respective. Effectuez les tâches suivantes pour activer la résolution de noms sur l'appliance :

1. Définissez les serveurs de noms.
2. Définissez un suffixe DNS.

Points à noter

Effectuez la recherche DNS à partir de l'interface de ligne de commande. Les recherches DNS de l'invite shell du système d'exploitation FreeBSD échouent car l'entrée dans le fichier /etc/resolv.conf pointe vers l'adresse IP 127.0.0.2.

Les commandes suivantes ne sont pas disponibles dans l'interface de ligne de commande de l'appliance :

```
- host
- dig
- getent/MIP
- nslookup
<!--NeedCopy-->
```

Si l'appliance ne parvient pas à effectuer un ping sur le serveur DNS sur son adresse SNIP, l'état du serveur s'affiche comme étant inactif. La réussite du ping est importante lorsque l'appliance se trouve derrière un pare-feu.

Configuration de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add dns nameServer <Name_Server_IP_Address>
add dns suffix <DNS_Suffix>
<!--NeedCopy-->
```

Pour vérifier la configuration, tapez :

```
show dns nameServer
show dns suffix
<!--NeedCopy-->
```

Pour tester la résolution DNS, tapez :

```
show dns addrec <Host_Name>
<!--NeedCopy-->
```

Configuration de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Noms Serveurs > Ajouter**.
2. Dans la boîte de dialogue **Créer un serveur** de noms, entrez l'adresse IP du serveur de noms et cliquez sur **Créer** .
3. Accédez à **Gestion du trafic > DNS > Suffixe DNS > Ajouter**.
4. Dans la boîte de dialogue **Créer un suffixe DNS**, entrez le suffixe DNS, tel que example.com, à utiliser pour toutes les requêtes d'hôte, puis cliquez sur **Créer**.

Round Robin DNS

Lorsqu'un client envoie une requête DNS pour rechercher l'enregistrement de ressource DNS, il reçoit une liste d'adresses IP se résolvant au nom de la requête DNS. Le client utilise ensuite l'une des adresses IP de la liste, généralement le premier enregistrement ou l'adresse IP. Par conséquent, un serveur unique est utilisé pour la TTL totale du cache et est surchargé lorsque de nombreuses requêtes arrivent.

Lorsque Citrix ADC reçoit une demande DNS, il répond en modifiant l'ordre de la liste des enregistrements de ressources DNS dans une méthode round robin. Cette fonctionnalité est appelée *Round Robin DNS*. Round robin répartit également le trafic entre les centres de données. Citrix ADC exécute cette fonction automatiquement. Vous n'avez pas à configurer ce comportement.

Vue d'ensemble fonctionnelle

Si Citrix ADC est configuré en tant que serveur ADNS, il renvoie les enregistrements DNS dans l'ordre dans lequel les enregistrements sont configurés. Lorsque Citrix ADC est configuré en tant que proxy DNS, il renvoie les enregistrements DNS dans l'ordre dans lequel il reçoit les enregistrements du serveur. L'ordre des enregistrements présents dans le cache correspond à l'ordre dans lequel les enregistrements sont reçus du serveur.

Citrix ADC modifie ensuite l'ordre dans lequel les enregistrements sont envoyés dans la réponse DNS dans une méthode round robin. La première réponse contient le premier enregistrement dans l'ordre, la deuxième réponse contient le deuxième enregistrement dans l'ordre et l'ordre se poursuit dans la même séquence. Ainsi, les clients demandant le même nom peuvent se connecter à différentes adresses IP.

Exemple de DNS Round Robin

À titre d'exemple de Round Robin DNS, considérez les enregistrements DNS qui ont été ajoutés comme suit :

```
1   add dns addRec ns1 1.1.1.1  add dns addRec ns1 1.1.1.2  add dns
       addRec ns1 1.1.1.3  add dns addRec ns1 1.1.1.4
2 <!--NeedCopy-->
```

Le domaine, abc.com est lié à un enregistrement NS comme suit :

```
1   add dns nsrec abc.com. ns1
2 <!--NeedCopy-->
```

Lorsque Citrix ADC reçoit une requête pour l'enregistrement A de ns1, les enregistrements Address sont servis dans une méthode round robin comme suit. Dans la première réponse DNS, 1.1.1.1 est servi comme premier enregistrement :


```
1   ns1.                    1H IN A         1.1.1.1  ns1.
                           1H IN A         1.1.1.2  ns1.
                           1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4
2 <!--NeedCopy-->
```

Dans la deuxième réponse DNS, la deuxième adresse IP, 1.1.1.2 est servi comme premier enregistrement :

```
1   ns1.                    1H IN A         1.1.1.2  ns1.
                           1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4  ns1.
                           1H IN A         1.1.1.1
2 <!--NeedCopy-->
```

Dans la troisième réponse DNS, la troisième adresse IP, 1.1.1.2 est servi comme premier enregistrement :

```
1   ns1.                    1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4  ns1.
                           1H IN A         1.1.1.1  ns1.
                           1H IN A         1.1.1.2
2 <!--NeedCopy-->
```

Configurer les enregistrements de ressources DNS

August 20, 2021

Vous configurez les enregistrements de ressources sur l'appliance Citrix® ADC lorsque vous configurez l'appliance en tant que serveur ADNS pour une zone. Vous pouvez également configurer les enregistrements de ressources sur l'appliance si les enregistrements de ressources appartiennent à une zone pour laquelle l'appliance est un serveur proxy DNS. Sur l'appliance, vous pouvez configurer les types d'enregistrements suivants :

- Dossiers de service
- Enregistrements AAAA
- Enregistrements d'adresse
- Enregistrements Mail Exchange
- Enregistrements du serveur de noms
- Dossiers canoniques
- Enregistrements de pointeur

- Enregistrements NAPTR
- Début des enregistrements de l'autorité
- Enregistrements de texte

Le tableau suivant répertorie les types d'enregistrement que vous pouvez configurer pour un enregistrement de nom de domaine sur l'appliance Citrix ADC. Par exemple, vous pouvez configurer un maximum de 25 adresses IP pour un enregistrement.

Tableau 1. Type et numéro d'enregistrement configurables

Type d'enregistrement	Nombre de dossiers
Adresse (A)	25
IPv6 (AAAA)	5
Échange de courrier (MX)	12
Serveur de noms (NS)	16
Service (SRV)	8
Pointeur (PTR)	20
Nom canonique (CNAME)	1
Début de l'autorisation (SOA)	1
Texte (TXT)	20
Pointeur d'autorité de nommage (NAPTR)	20

> **Remarque :**
>
> Le nombre maximal d'adresses IP pour un nom d'hôte spécifique est 25. Cependant, le nombre d'enregistrements d'adresses différents peut être supérieur à 25.

Créer des enregistrements SRV pour un service

August 20, 2021

L'enregistrement SRV fournit des informations sur les services disponibles sur l'appliance Citrix ADC. Un enregistrement SRV contient les informations suivantes :

- Nom du service et du protocole
- Nom de domaine
- TTL

- Classe DNS
- Priorité de la cible
- Poids des enregistrements ayant la même priorité
- Port du service
- Nom d'hôte du service.

Citrix ADC choisit en premier l'enregistrement SRV qui a le paramètre de priorité le plus bas. Si un service possède plusieurs enregistrements SRV avec la même priorité, les clients utilisent le champ de pondération pour déterminer l'hôte à utiliser.

Ajouter un enregistrement SRV à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement SRV et vérifier la configuration :

```
1 -  add dns srvRec <domain> <target> -priority <positive_integer> -
     weight <positive_integer> -port <positive_integer> [-TTL <secs>]
2 -  sh dns srvRec <domain>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns srvRec _http._tcp.example.com nameserver1.com -priority 1 -
     weight 1 -port 80
2  Done
3 > show dns srvRec _http._tcp.example.com
4 1)      Domain Name : _http._tcp.example.com
5         Target Host : nameserver1.com
6         Priority : 1    Weight : 1
7         Port : 80       TTL : 3600 secs
8  Done
9 <!--NeedCopy-->
```

Modifier ou supprimer un enregistrement SRV à l'aide de l'interface de ligne de commande

- Pour modifier un enregistrement SRV, tapez :
  - La `set dns srvRec` commande
  - Nom du domaine pour lequel l'enregistrement SRV est configuré
  - Nom de l'hôte cible qui héberge le service associé
  - Les paramètres à modifier, avec leurs nouvelles valeurs
- Pour supprimer un enregistrement SRV, tapez :

- La `rm dns srvRec` commande
- Nom du domaine pour lequel l'enregistrement SRV est configuré
- Nom de l'hôte cible qui héberge le service associé

Configurer un enregistrement SRV à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements SRV** et créez un enregistrement SRV.

Créer des enregistrements AAAA pour un nom de domaine

August 20, 2021

Un enregistrement de ressource AAAA stocke une adresse IPv6 unique.

Ajouter un enregistrement AAAA à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement AAAA et vérifier la configuration :

```
1 -  add dns aaaaRec <hostName> <IPv6Address> ... [-TTL <secs>]
2 -  show dns aaaaRec <hostName>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns aaaaRec www.example.com 2001:0db8:0000:0000:0000:0000:1428:57
     ab
2  Done
3 > show dns aaaaRec www.example.com
4 1)      Host Name : www.example.com
5         Record Type : ADNS              TTL : 5 secs
6         IPV6 Address : 2001:db8::1428:57ab
7  Done
8 <!--NeedCopy-->
```

Pour supprimer un enregistrement AAAA et toutes les adresses IPv6 associées au nom de domaine, tapez la `rm dns aaaaRec` commande et le nom de domaine pour lesquels l'enregistrement AAAA est configuré. Pour supprimer uniquement un sous-ensemble des adresses IPv6 associées au nom de domaine dans un enregistrement AAAA, tapez ce qui suit :

- `rm dns aaaaRec` commande

- Nom de domaine pour lequel l'enregistrement AAAA est configuré
- Les adresses IPv6 que vous souhaitez supprimer

Ajouter un enregistrement AAAA à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements AAAA** et créez un enregistrement AAAA.

Créer des enregistrements d'adresse pour un nom de domaine

August 20, 2021

Les enregistrements d'adresse (A) sont des enregistrements DNS qui mappent un nom de domaine à une adresse IPv4.

Vous ne pouvez pas supprimer les enregistrements d'adresse d'un hôte participant à l'équilibrage de charge du serveur global (GSLB). Toutefois, Citrix ADC supprime les enregistrements d'adresse ajoutés pour les domaines GSLB lorsque vous déliez le domaine d'un serveur virtuel GSLB. Seuls les enregistrements configurés par l'utilisateur peuvent être supprimés manuellement. Vous ne pouvez pas supprimer un enregistrement pour un hôte référencé par des enregistrements tels que NS, MX ou CNAME.

Ajouter un enregistrement d'adresse à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement Address et vérifier la configuration :

```
1 -  add dns addRec <hostName> <IPAddress> [-TTL <secs>]
2 -  show dns addRec <hostName>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns addRec ns.example.com 192.0.2.0
2  Done
3 > show dns addRec ns.example.com
4 1)      Host Name : ns.example.com
5         Record Type : ADNS                    TTL : 5 secs
6         IP Address : 192.0.2.0
7  Done
8 <!--NeedCopy-->
```


Pour supprimer un enregistrement Address et toutes les adresses IP associées au nom de domaine, tapez la `rm dns addRec` commande et le nom de domaine pour lesquels l'enregistrement Address est configuré. Pour supprimer uniquement un sous-ensemble des adresses IP associées au nom de domaine dans un enregistrement Address, tapez ce qui suit :

- `rm dns addRec` commande
- Nom de domaine pour lequel l'enregistrement Address est configuré
- Les adresses IP que vous souhaitez supprimer

Ajouter un enregistrement d'adresse à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements d'adresse** et créez un enregistrement d'adresse.

Créer des enregistrements MX pour un serveur d'échange de messagerie

August 20, 2021

Les enregistrements Mail Exchange (MX) sont utilisés pour diriger les messages électroniques sur Internet. Un enregistrement MX contient une préférence MX qui spécifie le serveur MX à utiliser. Les valeurs de préférence MX varient de 0 à 65536. Un enregistrement MX contient un numéro de préférence MX unique. Vous pouvez définir la préférence MX et les valeurs TTL pour un enregistrement MX.

Lorsqu'un message électronique est envoyé via Internet, un agent de transfert de courrier envoie une requête DNS demandant l'enregistrement MX pour le nom de domaine. Cette requête renvoie une liste des noms d'hôte des serveurs d'échange de messagerie pour le domaine, ainsi qu'un numéro de préférence. S'il n'y a pas d'enregistrements MX, la demande est faite pour l'enregistrement Adresse de ce domaine. Un seul domaine peut avoir plusieurs serveurs d'échange de messagerie.

Ajouter un enregistrement MX à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement MX et vérifier la configuration :

```
1 - add dns mxRec <domain> -mx <string> -pref <positive_integer> [-TTL <
    secs>]
2 - show dns mxRec <domain>
3 <!--NeedCopy-->
```

Exemple :


```
> add dns mxRec example.com -mx mail.example.com -pref 1
 Done
> show dns mxRec example.com
1)      Domain : example.com    MX Name : mail.example.com
        Preference :   1        TTL : 5 secs
 Done
<!--NeedCopy-->
```

Modifier ou supprimer un enregistrement MX à l'aide de l'interface de ligne de commande

- Pour modifier un enregistrement MX, tapez la `set dns mxRec` commande, le nom du domaine pour lequel l'enregistrement MX est configuré, le nom de l'enregistrement MX et les paramètres à modifier, avec leurs nouvelles valeurs.
- Pour définir la valeur par défaut du paramètre TTL, tapez la `unset dns mxRec` commande, le nom du domaine pour lequel l'enregistrement MX est configuré, le nom de l'enregistrement MX et -TTL sans valeur TTL. Vous pouvez utiliser la commande `unset dns mxRec` pour désactiver uniquement le paramètre TTL.
- Pour supprimer un enregistrement MX, tapez la `rm dns mxRec` commande, le nom du domaine pour lequel l'enregistrement MX est configuré et le nom de l'enregistrement MX.

Ajouter un enregistrement MX à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements d'échange de messagerie** et créez un enregistrement MX.

Créer des enregistrements NS pour un serveur faisant autorité

August 20, 2021

Les enregistrements NS (Name Server) spécifient le serveur faisant autorité pour un domaine. Vous pouvez configurer un maximum de 16 enregistrements NS. Vous pouvez utiliser un enregistrement NS pour déléguer le contrôle d'un sous-domaine à un serveur DNS.

Créer un enregistrement NS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un enregistrement NS et vérifier la configuration :


```
-  add dns nsRec <domain> <nameServer> [-TTL <secs>]
-  show dns nsRec <domain>
<!--NeedCopy-->
```

Exemple :

```
> add dns nsRec example.com nameserver1.example.com
 Done
> show dns nsRec example.com
1)      Domain : example.com    NameServer : nameserver1.example.com
        TTL : 5 sec
 Done
<!--NeedCopy-->
```

Pour supprimer un enregistrement NS, tapez la commande `rm dns nsRec`, le nom du domaine auquel appartient l'enregistrement NS et le nom du serveur de noms.

Créer un enregistrement NS à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements du serveur de noms** et créez un enregistrement NS.

Créer des enregistrements CNAME pour un sous-domaine

August 20, 2021

Un enregistrement de nom canonique (enregistrement CNAME) est un alias pour un nom DNS. Ces enregistrements sont utiles lorsque plusieurs services interrogent le serveur DNS. L'hôte qui a un enregistrement d'adresse (A) ne peut pas avoir d'enregistrement CNAME.

Parfois, une appliance Citrix ADC en mode proxy demande un enregistrement d'adresse à partir du cache plutôt que du serveur.

Ajouter un enregistrement CNAME à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un enregistrement CNAME et vérifier la configuration :

```
-  add dns cnameRec <aliasName> <canonicalName> [-TTL <secs>]
-  show dns cnameRec <aliasName>
<!--NeedCopy-->
```


Exemple :

```
> add dns cnameRec www.example.com www.examplenw.com
 Done
> show dns cnameRec www.example.com
        Alias Name      Canonical Name  TTL
1)      www.example.com        www.examplenw.com       5 secs
 Done
<!--NeedCopy-->
```

Pour supprimer un enregistrement CNAME pour un domaine donné, tapez la commande `rm dns cnameRec` et l'alias du nom de domaine.

Ajouter un enregistrement CNAME à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements canoniques** et créez un enregistrement CNAME.

Enregistrements CNAME de cache

Lorsqu'il est déployé en mode proxy, l'appliance ADC n'envoie pas toujours la requête pour un enregistrement d'adresse au serveur principal. Ce problème se produit lorsque pour une réponse à une requête pour un enregistrement d'adresse, une chaîne CNAME partielle est présente dans le cache. Il y a peu de conditions dans lesquelles ADC met en cache l'enregistrement CNAME partiel et sert la requête à partir du cache. Voici les conditions :

- Citrix ADC doit être déployé en mode proxy.
- La réponse du serveur principal doit avoir une chaîne CNAME, pour laquelle le type d'enregistrement de la dernière entrée de la section réponse doit être CNAME et le type de question non CNAME.
- La réponse du serveur principal ne peut pas être un domaine sans données ou NX.
- La réponse du serveur principal doit être une réponse faisant autorité.

Créer des enregistrements NAPTR pour le domaine des télécommunications

January 21, 2021

NAPTR (Naming Address Pointer) est l'un des enregistrements DNS les plus couramment utilisés dans le domaine des télécommunications. Les enregistrements NAPTR mappent l'espace d'adressage

de téléphonie Internet à l'espace d'adressage Internet. Ils permettent donc à un appareil mobile d'envoyer une demande au serveur approprié. La combinaison des enregistrements NAPTR avec des enregistrements de service (SRV) permet le chaînage de plusieurs enregistrements afin de former des règles de réécriture complexes qui produisent de nouvelles étiquettes de domaine ou des identifiants de ressource uniformes (URI). Le code DNS pour NAPTR est 35.

Les Citrix ADC prennent en charge NAPTR dans deux modes : le mode ADNS et le mode proxy. En mode proxy, ADC met en cache la réponse des serveurs et utilise les enregistrements mis en cache pour les futures requêtes du serveur. Un maximum de 20 enregistrements NAPTR peuvent être ajoutés pour un domaine particulier dans Citrix ADC. Citrix ADC met en cache la réponse à une requête d'enregistrement NAPTR DNS. Toutes les demandes ultérieures pour l'enregistrement NAPTR sont servies à partir du cache.

Créer un enregistrement NAPTR à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement NAPTR et vérifier la configuration :

```
add dns naptrRec <order> <preference>[flags<string>][services<string>](
regexp<expressions>|-replacement<string>)[-TTL<secs>]
```

Supprimer un enregistrement NAPTR à l'aide de CLU

```
rm dns naptrRec<domain> (<order> <preference> [-flags <string>] [-services
 <string>] (-regexp <expression> | -replacement <string>))| -recordId <
positive_integer>@)
```

Configurer un enregistrement NAPTR à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements NAPTR** et créez un enregistrement NAPTR.

Créer des enregistrements PTR pour les adresses IPv4 et IPv6

August 20, 2021

Un enregistrement de pointeur (PTR) traduit une adresse IP en son nom de domaine. Les enregistrements IPv4 PTR sont représentés par les octets d'une adresse IP dans l'ordre inverse avec la chaîne "in-addr.arpa." joint à la fin. Par exemple, l'enregistrement PTR pour l'adresse IP 1.2.3.4 est 4.3.2.1.in-addr.arpa.

Les adresses IPv6 sont mappées inversement sous le domaine IP6.ARPA. Les cartes inverses IPv6 utilisent une séquence de quartets séparés par des points avec le suffixe “.IP6.ARPA” tel que défini dans la norme RFC 3596. Par exemple, le nom de domaine de recherche inverse correspondant à l’adresse 4321:0:1:2:3:4:567:89 ab serait b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA.

Ajouter un enregistrement PTR à l’aide de l’interface de ligne de commande

À l’invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement PTR et vérifier la configuration :

```
1 -  add dns ptrRec <reverseDomain> <domain> [-TTL <secs>]
2 -  show dns ptrRec <reverseDomain>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns ptrRec 0.2.0.192.in-addr.arpa example.com
2  Done
3 > show dns ptrRec 0.2.0.192.in-addr.arpa
4 1)      Reverse Domain Name : 0.2.0.192.in-addr.arpa
5         Domain Name : example.com              TTL : 3600 secs
6  Done
7 <!--NeedCopy-->
```

Pour supprimer un enregistrement PTR, tapez la commande `rm dns ptrRec` et le nom de domaine inverse associé à l’enregistrement PTR

Ajouter un enregistrement PTR à l’aide de l’interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements PTR** et créez un enregistrement PTR.

Créer des enregistrements SOA pour les informations faisant autorité

August 20, 2021

Un enregistrement Start of Authority (SOA) est créé uniquement au sommet de la zone et contient des informations sur la zone. L’enregistrement inclut, entre autres paramètres, le serveur de noms principal, les informations de contact (e-mail) et les valeurs par défaut (minimum) de durée de vie (TTL) pour les enregistrements.

Créer un enregistrement SOA à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement SOA et vérifier la configuration :

```
1 - add dns soaRec <domain> -originServer <originServerName> -contact <
    contactName>
2 - sh dns soaRec <do main>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns soaRec example.com -originServer nameserver1.example.com -
    contact admin.example.com
2  Done
3 > show dns soaRec example.com
4 1)      Domain Name : example.com
5         Origin Server : nameserver1.example.com
6         Contact : admin.example.com
7         Serial No. : 100        Refresh : 3600 secs     Retry : 3 secs
8         Expire : 3600 secs      Minimum : 5 secs        TTL : 3600 secs
9  Done
10 <!--NeedCopy-->
```

Modifier ou supprimer un enregistrement SOA à l'aide de l'interface de ligne de commande

- Pour modifier un enregistrement SOA, tapez la commande `set dns soaRec`, le nom du domaine pour lequel l'enregistrement est configuré et les paramètres à modifier, avec leurs nouvelles valeurs.
- Pour supprimer un enregistrement SOA, tapez la commande `rm dns soaRec` et le nom du domaine pour lequel l'enregistrement est configuré.

Configurer un enregistrement SOA à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements SOA** et créez un enregistrement SOA.

Créer des enregistrements TXT pour contenir du texte descriptif

August 20, 2021

Les hôtes de domaine stockent les enregistrements TXT à des fins informatives. Le composant RDATA d'un enregistrement TXT, qui consiste en une ou plusieurs chaînes de caractères de longueur variable, peut stocker pratiquement toutes les informations qu'un destinataire pourrait avoir besoin de connaître sur le domaine. Il peut également inclure des informations sur le fournisseur de services, la personne à contacter, les adresses e-mail et les détails associés. La protection SPF (Sender Policy Framework) a été le cas d'utilisation le plus important pour l'enregistrement TXT.

Tous les types de configuration (configurations DNS, proxy DNS, résolveur final et redirecteur faisant autorité) sur l'appliance Citrix ADC prennent en charge les enregistrements TXT. Vous pouvez ajouter un maximum de 20 enregistrements de ressources TXT à un domaine. Chaque enregistrement de ressource est stocké avec un ID d'enregistrement unique généré en interne. Vous pouvez afficher l'ID d'un enregistrement et l'utiliser pour le supprimer. Toutefois, vous ne pouvez pas modifier un enregistrement de ressource TXT.

Créer un enregistrement de ressource TXT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un enregistrement de ressource TXT et vérifier la configuration :

```
1 -  add dns txtRec <domain> <string> ... [-TTL <secs>]
2 -  show dns txtRec [<domain> | -type <type>]
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns txtRec www.example.com "Contact: Mark" "Email: mark@example.
     com" -TTL 36000
2  Done
3 > show dns txtRec www.example.com
4 1)  Domain : www.example.com    Record id: 13783       TTL : 36000 secs
      Record Type : ADNS
5         "Contact: Mark"
6         "Email: mark@example.com"
7  Done
8 <!--NeedCopy-->
```

Supprimer un enregistrement de ressource TXT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour supprimer un enregistrement de ressource TXT et vérifier la configuration :

```
1 -  rm dns txtRec <domain> (<string> ... | -recordId <positive_integer>)
```



```
-  show dns txtRec [<domain> | -type <type>]
<!--NeedCopy-->
```

Exemple :

Vous pouvez d'abord utiliser la `show dns txtRec` commande pour afficher l'ID d'enregistrement de l'enregistrement de ressource TXT que vous souhaitez supprimer, comme indiqué :

```
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 36865       TTL : 36000 secs
    Record Type : ADNS
        "Contact: Evan"
        "Email: evan@example.com"
2)  Domain : www.example.com    Record id: 14373       TTL : 36000 secs
    Record Type : ADNS
        "Contact: Mark"
        "Email: mark1@example.com"
 Done
<!--NeedCopy-->
```

La méthode la plus simple de suppression d'un enregistrement TXT consiste à utiliser l'ID d'enregistrement. Si vous souhaitez fournir les chaînes, saisissez-les dans l'ordre dans lequel elles sont stockées dans l'enregistrement. Dans l'exemple suivant, l'enregistrement TXT est supprimé à l'aide de son ID d'enregistrement.

```
>rm dns txtRec www.example.com -recordID 36865
 Done
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 14373       TTL : 36000 secs
    Record Type : ADNS
        "Contact: Mark"
        "Email: mark1@example.com"
 Done
<!--NeedCopy-->
```

Configurer un enregistrement TXT à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements TXT** et créez un enregistrement TXT.

Afficher les statistiques DNS

August 20, 2021

Vous pouvez afficher les statistiques DNS générées par l'appliance Citrix ADC. Les statistiques DNS incluent les statistiques d'exécution, de configuration et d'erreur.

Afficher les statistiques des enregistrements DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat dns
```

Exemple :

```
1  > stat dns
2  DNS Statistics
3
4  Runtime Statistics
5  Dns queries                          21
6  NS queries                            8
7  SOA queries                          18
8  .
9  .
10 .
11 Configuration Statistics
12 AAAA records                         17
13 A records                            36
14 MX records                            9
15 .
16 .
17 .
18 Error Statistics
19 Nonexistent domain                   17
20 No AAAA records                       0
21 No A records                         13
22 .
23 .
24 .
25 Done
26 <!--NeedCopy-->
```


Afficher les statistiques des enregistrements DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, cliquez sur **Statistiques**.

Configurer une zone DNS

August 20, 2021

Une entité de zone DNS sur l'appliance Citrix ADC facilite la propriété d'un domaine sur l'appliance. Une zone de l'appliance vous permet également d'implémenter les extensions de sécurité DNS (DNSSEC) pour la zone ou de décharger les opérations DNSSEC de la zone des serveurs DNS vers l'appliance. Les opérations de signe DNSSEC sont effectuées sur tous les enregistrements de ressources dans une zone DNS. Par conséquent, si vous souhaitez signer une zone ou décharger des opérations DNSSEC pour une zone, vous devez d'abord créer la zone sur l'appliance Citrix ADC.

Créez une zone DNS sur l'appliance dans les scénarios suivants :

- L'appliance Citrix ADC possède tous les enregistrements d'une zone, c'est-à-dire qu'elle fonctionne en tant que serveur DNS faisant autorité pour la zone. La zone doit être créée avec le paramètre ProxyMode défini sur NO.
- L'appliance Citrix ADC ne possède qu'un sous-ensemble des enregistrements d'une zone. Tous les autres enregistrements de ressources de la zone sont hébergés sur un ensemble de serveurs de noms principaux. L'appliance est configurée en tant que serveur proxy DNS pour ces serveurs principaux. Une configuration typique dans laquelle l'appliance Citrix ADC ne possède qu'un sous-ensemble des enregistrements de ressources dans la zone est une configuration GSLB (Global Server Load Balancing). L'appliance Citrix ADC possède uniquement les noms de domaine GSLB, tandis que les serveurs de noms principaux possèdent tous les autres enregistrements. La zone doit être créée avec le paramètre proxyMode défini sur YES.
- Vous souhaitez décharger les opérations DNSSEC d'une zone de vos serveurs DNS faisant autorité vers l'appliance. La zone doit être créée avec le paramètre proxyMode défini sur YES. Vous devrez peut-être configurer d'autres paramètres pour la zone.

La rubrique actuelle décrit comment créer une zone pour les deux premiers scénarios. Pour plus d'informations sur la configuration d'une zone de déchargement des opérations DNSSEC vers l'appliance, consultez Décharger les opérations DNSSEC vers l'appliance Citrix ADC.

> **Remarque**
>
> Si l'appliance ADC fonctionne en tant que serveur DNS faisant autorité pour une zone, vous devez créer les enregistrements de début d'autorité (SOA) et de serveur de noms (NS) pour la zone avant de créer la zone. Si ADC Citrix fonctionne en tant que serveur proxy DNS pour une zone,

> les enregistrements SOA et NS ne doivent pas être créés sur l'appliance Citrix ADC. Pour plus d'informations sur la création d'enregistrements SOA et NS, voir Configurer les enregistrements de ressources DNS.

Lorsque vous créez une zone, tous les noms de domaine et enregistrements de ressources existants se terminant par le nom de la zone sont automatiquement traités comme faisant partie de la zone. En outre, tous les nouveaux enregistrements de ressource créés avec un suffixe correspondant au nom de la zone sont implicitement inclus dans la zone.

Créez une zone DNS sur l'appliance Citrix ADC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour ajouter une zone DNS à l'appliance Citrix ADC et vérifier la configuration :

```
1 -  add dns zone <zoneName> -proxyMode ( YES | NO )
2 -  show dns zone [<zoneName> | -type <type>]
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns zone example.com -proxyMode Yes
2  Done
3 > show dns zone example.com
4          Zone Name : example.com
5          Proxy Mode : YES
6 Done
7 <!--NeedCopy-->
```

Modifier ou supprimer une zone DNS à l'aide de l'interface de ligne de commande

- Pour modifier une zone DNS, tapez la commande `set dns zone`, le nom de la zone DNS et les paramètres à modifier, avec leurs nouvelles valeurs.
- Pour supprimer une zone DNS, tapez la `rm dns zone` commande et le nom de la zone DNS.

Configurer une zone DNS à l'aide de l'interface graphique

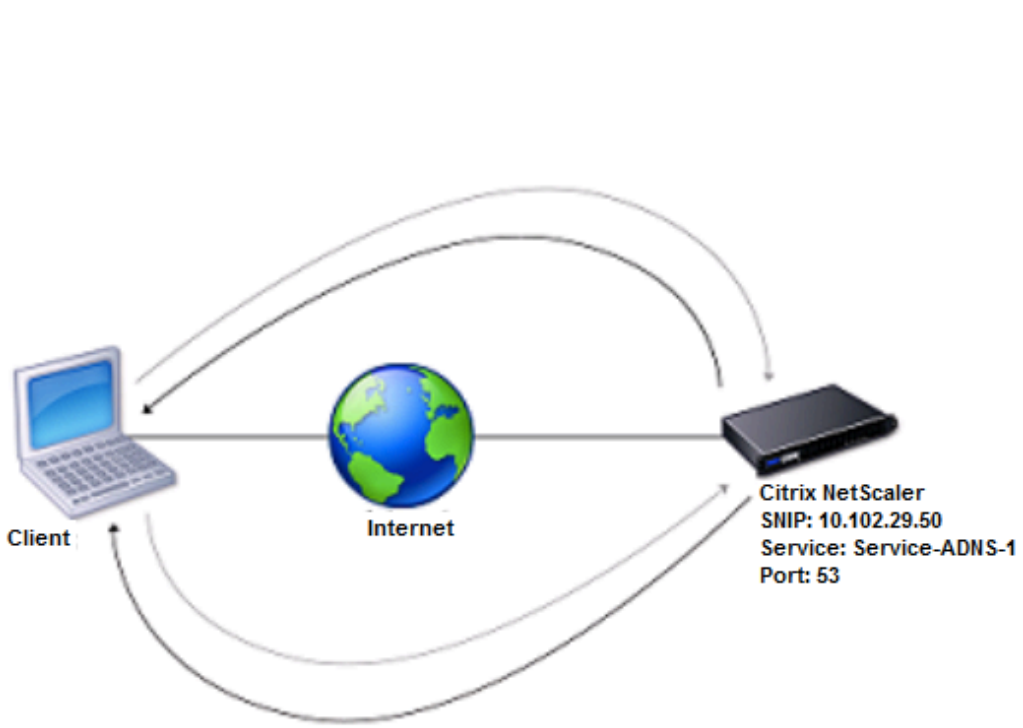
Accédez à **Gestion du trafic > DNS > Zones** et créez une zone DNS.

Configurer le Citrix ADC en tant que serveur ADNS

August 20, 2021

Vous pouvez configurer l'appliance ADC pour qu'elle fonctionne en tant que serveur de noms de domaine (ADNS) faisant autorité pour un domaine. En tant que serveur ADNS pour un domaine, Citrix ADC résout les demandes DNS pour tous les types d'enregistrements DNS appartenant au domaine. Pour configurer Citrix ADC pour qu'il fonctionne en tant que serveur ADNS pour un domaine, vous devez créer un service ADN et configurer les enregistrements NS et Adresse pour le domaine sur Citrix ADC. Le service ADNS peut être configuré à l'aide de l'adresse IP du sous-réseau (SNIP) ou d'une adresse IP distincte. Le diagramme topologique suivant présente un exemple de configuration et le flux de demandes et de réponses.

Figure 1. Citrix ADC en tant qu'ADNS



Le tableau suivant présente les paramètres configurés pour le service ADNS illustrés dans le diagramme topologique précédent.

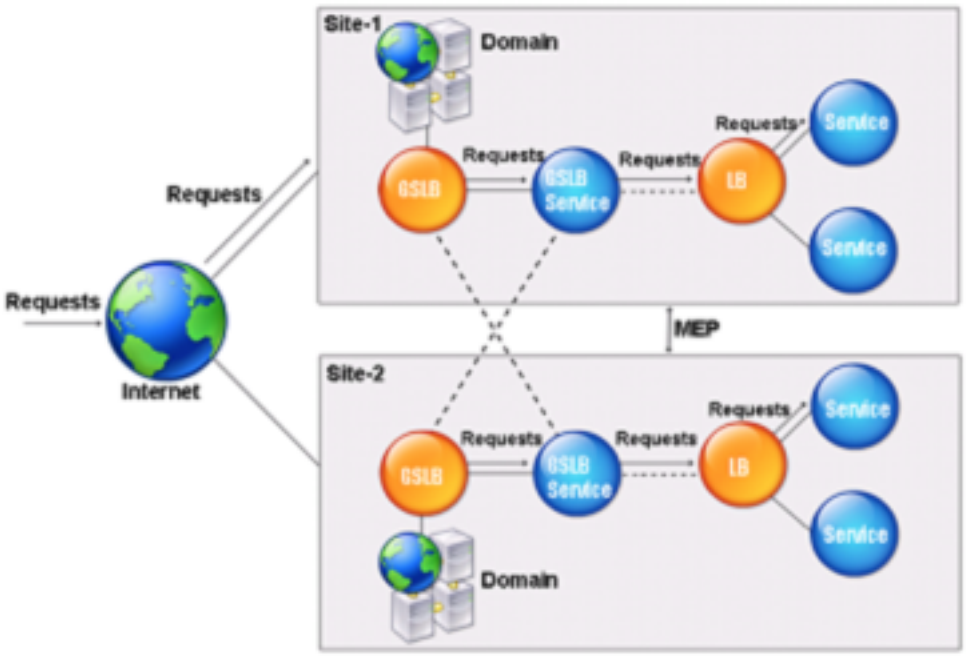
Type d'entité	Nom	Adresse IP	Type	Port
Service ADNS	Service-ADNS-1	10.102.29.51	ADNS	53

Tableau 1. Exemple de configuration du service ADNS

Pour configurer une configuration ADNS, vous devez configurer le service ADNS. Pour obtenir des instructions sur la configuration du service ADNS, voir Équilibrage de charge.

Pendant la résolution DNS, le serveur ADNS demande au proxy DNS ou au serveur DNS local d'interroger Citrix ADC pour l'adresse IP du domaine. Étant donné que Citrix ADC fait autorité pour le domaine, il envoie l'adresse IP au proxy DNS ou au serveur DNS local. Le diagramme suivant décrit l'emplacement et le rôle du serveur ADNS dans une configuration GSLB.

Figure 2. Modèle d'entité GSLB



Remarque : En mode ADNS, si vous supprimez des enregistrements SOA et ADNS, les éléments suivants ne fonctionnent pas pour le domaine hébergé par Citrix ADC : N'IMPORTE QUELLE requête (pour plus d'informations sur la requête ANY, voir requête DNS ANY) et réponses négatives, telles que NODATA et NXDOMAIN.

Créer un service ADNS

Un service ADNS est utilisé pour l'équilibrage global de la charge de service. Pour plus d'informations sur la création d'une configuration GSLB, reportez-vous à la section Équilibrage global de la charge des serveurs. Vous pouvez ajouter, modifier, activer, désactiver et supprimer un service ADNS. Pour obtenir des instructions sur la création d'un service ADNS, voir Configurer les services.

Remarque : Vous pouvez configurer le service ADNS pour utiliser SNIP ou toute nouvelle adresse IP.

Lorsque vous créez un service ADNS, Citrix ADC répond aux requêtes DNS sur l'IP et le port du service ADNS configurés.

Vous pouvez vérifier la configuration en affichant les propriétés du service ADNS. Vous pouvez afficher des propriétés telles que le nom, l'état, l'adresse IP, le port, le protocole et le nombre maximal de connexions client.

Configurer la configuration de l'ADNS pour utiliser TCP

Par défaut, certains clients utilisent le protocole UDP (User Datagram Protocol) pour DNS, qui spécifie une limite de 512 octets pour la longueur de charge utile des paquets UDP. Pour gérer des charges utiles dont la taille dépasse 512 octets, le client doit utiliser TCP. Pour activer les communications DNS via TCP, vous devez configurer l'appliance Citrix ADC pour qu'elle utilise le protocole TCP pour DNS. Citrix ADC définit ensuite le bit de troncation dans les paquets de réponse DNS. Le bit de troncature spécifie que la réponse est trop grande pour UDP et que le client doit envoyer la requête via une connexion TCP. Le client utilise ensuite le protocole TCP sur le port 53 et ouvre une nouvelle connexion au Citrix ADC. Citrix ADC écoute sur le port 53 avec l'adresse IP du service ADNS pour accepter les nouvelles connexions TCP du client.

Pour configurer Citrix ADC pour qu'il utilise le protocole TCP, vous devez configurer un service ADNS_TCP. Pour obtenir des instructions sur la création d'un service ADNS_TCP, reportez-vous à la section Équilibrage de charge.

> **Important**
>
> Pour configurer Citrix ADC pour qu'il utilise UDP pour DNS et utilise TCP uniquement lorsque la longueur de charge utile d'UDP dépasse 512 octets, vous devez configurer les services ADNS et ADNS_TCP. L'adresse IP du service ADNS_TCP doit être la même que l'adresse IP du service ADNS.

Ajouter des enregistrements de ressources DNS

Après avoir créé un service ADNS, vous pouvez ajouter des enregistrements DNS. Pour obtenir des instructions sur l'ajout d'enregistrements DNS, voir Configurer les enregistrements de ressources DNS.

Supprimer les services ADNS

Pour obtenir des instructions sur la suppression des services, voir Équilibrage de charge.

Configurer la délégation de domaine

La délégation de domaine est le processus d'attribution de la responsabilité d'une partie de l'espace de domaine à un autre serveur de noms. Par conséquent, lors de la délégation de domaine, la responsabilité de répondre à la requête est déléguée à un autre serveur DNS. La délégation utilise des enregistrements NS.

Dans l'exemple suivant, sub1.abc.com est le sous-domaine de abc.com. La procédure décrit les étapes pour déléguer le sous-domaine au serveur de noms ns2.sub1.abc.com et ajouter un enregistrement Address pour ns2.sub1.abc.com.

Pour configurer la délégation de domaine, vous devez effectuer les tâches suivantes, décrites dans les sections suivantes :

1. Créez un enregistrement SOA pour un domaine.
2. Créez un enregistrement NS pour ajouter un serveur de noms pour le domaine.
3. Créez un enregistrement d'adresse pour le serveur de noms.
4. Créez un enregistrement NS pour déléguer le sous-domaine.
5. Créez un enregistrement de collage pour le serveur de noms.

Créer un enregistrement SOA

Pour obtenir des instructions sur la configuration des enregistrements SOA, reportez-vous à la section Créer des enregistrements SOA pour obtenir des informations faisant autorité.

Créer un enregistrement NS pour un serveur de noms

Pour obtenir des instructions sur la configuration d'un enregistrement NS, voir Créer des enregistrements NS pour un serveur faisant autorité. Dans la liste **Serveur de noms**, sélectionnez le serveur principal de noms faisant autorité, par exemple ns1.abc.com.

Créer un enregistrement d'adresse

Pour obtenir des instructions sur la configuration des enregistrements d'adresses, voir Créer des enregistrements d'adresses pour un nom de domaine. Dans les zones de texte Nom d'hôte et Adresse IP, tapez respectivement le nom de domaine de l'enregistrement Adresse DNS et l'adresse IP, par exemple ns1.abc.com et 10.102.11.135.

Créer un enregistrement NS pour la délégation de domaine

Pour obtenir des instructions sur la configuration des enregistrements NS, voir Créer des enregistrements NS pour un serveur faisant autorité. Dans la liste **Serveur de noms**, sélectionnez le serveur de noms principal faisant autorité, par exemple ns2.sub1.abc.com.

Créer un enregistrement de colle

Les enregistrements NS sont généralement définis immédiatement après l'enregistrement SOA (pas une restriction). Un domaine doit avoir au moins deux enregistrements NS. Si un enregistrement NS est défini dans un domaine, il doit avoir un enregistrement Address correspondant. Cet enregistrement d'adresse est appelé enregistrement collé. Les enregistrements de colle accélèrent les requêtes DNS.

Pour obtenir des instructions sur l'ajout d'enregistrements de colle pour un sous-domaine, reportez-vous à la procédure d'ajout d'un enregistrement Address (A), Configurer les enregistrements de ressources DNS.

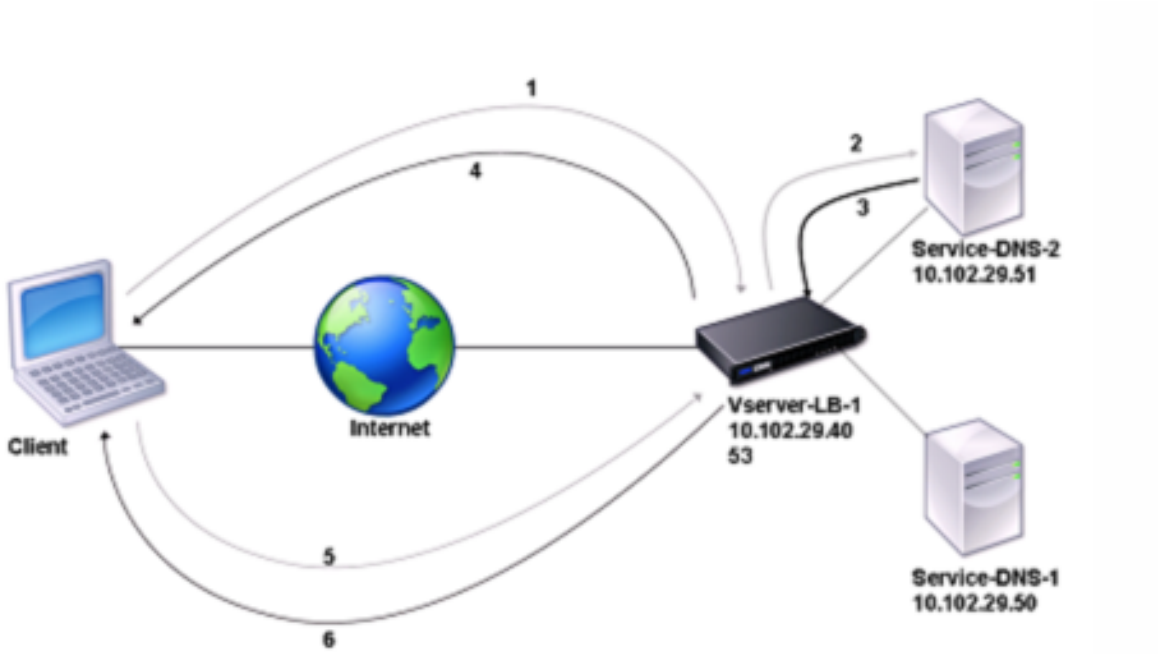
Pour obtenir des instructions sur la configuration des enregistrements d'adresses, voir Créer des enregistrements d'adresses pour un nom de domaine. Dans les zones de texte Nom d'hôte et Adresse IP, tapez le nom de domaine pour l'enregistrement Adresse DNS et l'adresse IP, par exemple ns2.sub1.abc.com et 10.102.12.135, respectivement.

Configurer l'appliance Citrix ADC en tant que serveur proxy DNS

August 20, 2021

En tant que serveur proxy DNS, l'appliance ADC peut fonctionner comme proxy pour un serveur DNS unique ou un groupe de serveurs DNS. Le flux des demandes et des réponses est illustré dans l'exemple de diagramme topologique suivant.

Figure 1. Citrix ADC en tant que proxy DNS



Par défaut, l'appliance Citrix ADC met en cache les réponses des serveurs de noms DNS. Lorsque l'appliance reçoit une requête DNS, elle vérifie le domaine interrogé dans son cache. Si l'adresse du domaine interrogé est présente dans son cache, Citrix ADC renvoie l'adresse correspondante au client. Sinon, il transfère la requête à un serveur de noms DNS qui vérifie la disponibilité de l'adresse et la renvoie au Citrix ADC. Citrix ADC renvoie ensuite l'adresse au client.

Pour les demandes d'un domaine qui a été mis en cache précédemment, Citrix ADC sert l'enregistrement Adresse du domaine à partir du cache sans interroger le serveur DNS configuré.

L'appliance rejette un enregistrement stocké dans son cache lorsque la valeur de durée de vie (TTL) de l'enregistrement atteint la valeur configurée. Un client qui demande un enregistrement expiré doit attendre que Citrix ADC récupère l'enregistrement du serveur et mette à jour son cache. Pour éviter ce retard, Citrix ADC met à jour de manière proactive le cache en récupérant l'enregistrement du serveur avant l'expiration de l'enregistrement.

Le tableau suivant répertorie les noms d'exemples et les valeurs des entités qui doivent être configurées sur Citrix ADC.

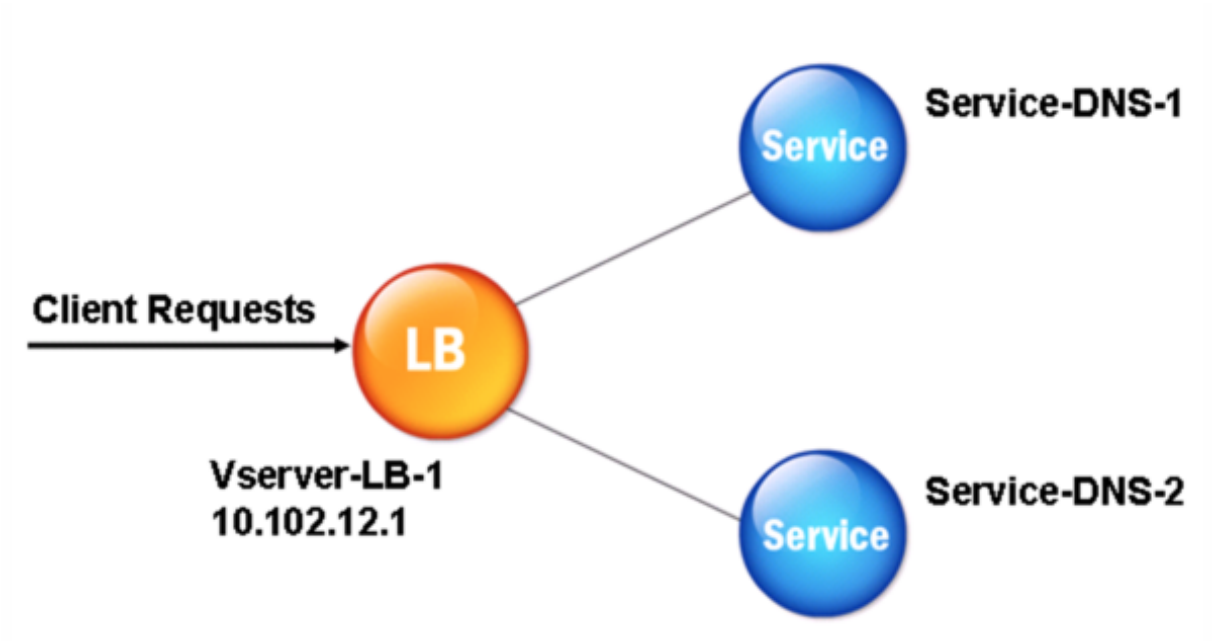
Tableau 1. Exemple de configuration d'entité proxy DNS

Type d'entité	Nom	Adresse IP	Type	Port
Serveur virtuel LB	Vserver-DNS-1	10.102.29.40	DNS	53
Services	Service-DNS-1	10.102.29.50	DNS	53

Type d'entité	Nom	Adresse IP	Type	Port
Services	Service-DNS-2	10.102.29.51	DNS	53

Le diagramme suivant montre les entités d'un proxy DNS et les valeurs des paramètres à configurer sur Citrix ADC.

Figure 2. Modèle d'entité proxy DNS



> **Remarque**
>
> Pour configurer la fonctionnalité proxy DNS, vous devez savoir comment configurer les services d'équilibrage de charge et les serveurs virtuels.

Créer un serveur virtuel d'équilibrage de charge

Pour configurer un proxy DNS sur Citrix ADC, configurez un serveur virtuel d'équilibrage de charge de type DNS. Pour configurer un serveur virtuel DNS pour équilibrer la charge d'un ensemble de serveurs DNS prenant en charge les requêtes récursives, vous devez définir l'option Récursion disponible. Avec cette option, le bit RA est défini sur ON dans les réponses DNS du serveur virtuel DNS.

Pour obtenir des instructions sur la création d'un serveur virtuel d'équilibrage de charge, voir Équilibrage decharge.

Créer des services DNS

Après avoir créé un serveur virtuel d'équilibrage de charge de type DNS, vous devez créer des services DNS. Vous pouvez ajouter, modifier, activer, désactiver et supprimer un service DNS. Pour obtenir des instructions sur la création d'un service DNS, voir Équilibrage de charge.

Lier un serveur virtuel d'équilibrage de charge aux services DNS

Pour terminer la configuration du proxy DNS, vous devez lier les services DNS au serveur virtuel d'équilibrage de charge. Pour obtenir des instructions sur la liaison d'un service à un serveur virtuel d'équilibrage de charge, reportez-vous à la section Équilibrage de charge.

Configurer la configuration du proxy DNS pour utiliser TCP

Certains clients utilisent le protocole UDP (User Datagram Protocol) pour les communications DNS. Toutefois, UDP spécifie une taille maximale de paquet de 512 octets. Lorsque la longueur de charge utile dépasse 512 octets, le client doit utiliser TCP. Lorsqu'un client envoie à l'appliance Citrix ADC une requête DNS, l'appliance transfère la requête à l'un des serveurs de noms. Si la réponse est trop volumineuse pour un paquet UDP, le serveur de noms définit le bit de troncation dans sa réponse au Citrix ADC. Le bit de troncation indique que la réponse est trop grande pour UDP et que le client doit envoyer la requête via une connexion TCP. L'appliance ADC transmet la réponse au client avec le bit de troncature intact. Il attend que le client initie une connexion TCP avec l'adresse IP du serveur virtuel d'équilibrage de charge DNS, sur le port 53. Le client envoie la requête via une connexion TCP. L'appliance Citrix ADC transfère ensuite la demande au serveur de noms et relaie la réponse au client.

Pour configurer Citrix ADC pour qu'il utilise le protocole TCP pour DNS, vous devez configurer un serveur virtuel d'équilibrage de charge et des services, tous deux de type DNS_TCP. Vous pouvez configurer des moniteurs de type DNS_TCP pour vérifier l'état des services. Pour obtenir des instructions sur la création de serveurs virtuels, de services et de moniteurs DNS_TCP, reportez-vous à la section Équilibrage de charge.

Pour mettre à jour les enregistrements de manière proactive, Citrix ADC utilise une connexion TCP au serveur pour récupérer les enregistrements.

> **Important**
>
> Pour configurer Citrix ADC pour utiliser UDP pour DNS et utiliser TCP uniquement lorsque la longueur de charge utile d'UDP dépasse 512 octets, vous devez configurer les services DNS et DNS_TCP. L'adresse IP du service DNS_TCP doit être identique à l'adresse IP du service DNS.

Configurer les valeurs de durée de vie pour les entrées DNS

La TTL est la même pour tous les enregistrements DNS avec le même nom de domaine et le même type d'enregistrement. Si la valeur TTL est modifiée pour l'un des enregistrements, la nouvelle valeur est reflétée dans tous les enregistrements du même nom de domaine et type. La valeur de TTL par défaut est 3600 secondes. Le minimum est 0 et le maximum est 604800. Si une entrée DNS a une valeur de TTL inférieure au minimum ou supérieure au maximum, elle est enregistrée en tant que valeur de TTL minimale ou maximale, respectivement.

Spécifiez le TTL minimum et maximal à l'aide de l'interface de ligne de commande

À l'invite de commandes Citrix ADC, tapez les commandes suivantes pour spécifier la TTL minimale et maximale et vérifier la configuration :

```
1 -  set dns parameter [-minTTL <secs>] [-maxTTL <secs>]
2 -  show dns parameter
3 <!--NeedCopy-->
```

Exemple :

```
1  > set dns parameter -minTTL 1200 -maxTTL 1800
2   Done
3  > show dns parameter
4          DNS parameters:
5          DNS retries: 5
6          Minimum TTL: 1200               Maximum TTL: 1800
7              .
8              .
9              .
10  Done
11 >
12 <!--NeedCopy-->
```

Spécifiez le TTL minimum et maximal à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres DNS.
3. Dans la boîte de dialogue Configurer les paramètres DNS, dans TTL, dans les zones de texte Minimum et Maximum, tapez respectivement la durée minimale et la durée maximale de vie (en secondes), puis cliquez sur OK.

Remarque : Lorsque la TTL expire, l'enregistrement est supprimé du cache. Citrix ADC contacte de manière proactive les serveurs et obtient l'enregistrement DNS juste avant l'expiration de

l'enregistrement DNS.

Vidage des enregistrements DNS

Vous pouvez supprimer tous les enregistrements DNS présents dans le cache. Par exemple, vous pouvez vider les enregistrements DNS lorsqu'un serveur est redémarré après que des modifications ont été apportées.

Supprimer tous les enregistrements proxy à l'aide de l'interface de ligne de commande

À l'invite de commandes Citrix ADC, tapez :

```
flush dns proxyRecords
```

Supprimer tous les enregistrements proxy à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Enregistrements**.
2. Dans le volet d'informations, cliquez sur Vider les enregistrements proxy.

Ajouter des enregistrements de ressources DNS

Vous pouvez ajouter des enregistrements DNS à un domaine pour lequel l'appliance Citrix ADC est configurée en tant que serveur proxy DNS. Pour plus d'informations sur l'ajout d'enregistrements DNS, reportez-vous à la section Configuration des enregistrements de ressources DNS.

Suppression d'un serveur virtuel DNS équilibrage de charge

Pour plus d'informations sur la suppression d'un serveur virtuel d'équilibrage de charge, voir Équilibrage decharge.

Limiter le nombre de demandes DNS simultanées sur une connexion client

Vous pouvez limiter le nombre de demandes DNS simultanées sur une connexion client unique, identifiée par le `<clientip:port>-<vserver ip:port>` tuple. Les demandes DNS simultanées sont les demandes que l'appliance Citrix ADC a transférées aux serveurs de noms et pour lesquelles l'appliance attend des réponses. La limitation du nombre de demandes simultanées sur une connexion client vous permet de protéger les serveurs de noms lorsqu'un client hostile tente une attaque DDoS (Distributed Denial of Service) en envoyant un flot de demandes DNS. Lorsque la limite pour une connexion client est atteinte, les demandes DNS suivantes sur la connexion sont supprimées jusqu'à ce que le nombre de demandes en attente passe en dessous de la limite. Cette limite ne s'applique pas aux demandes que l'appliance Citrix ADC traite hors de son cache.

La valeur par défaut de ce paramètre est 255. Cette valeur par défaut est suffisante dans la plupart des scénarios. Si les serveurs de noms servent de nombreuses requêtes DNS simultanées dans des conditions d'exploitation normales, vous pouvez spécifier une valeur élevée ou une valeur égale à zéro (0). La valeur 0 désactive cette fonctionnalité et spécifie qu'il n'y a pas de limite au nombre de requêtes DNS autorisées sur une seule connexion client. Ce paramètre est un paramètre global qui s'applique à tous les serveurs virtuels DNS configurés sur l'appliance Citrix ADC.
La valeur par défaut de ce paramètre est 255. Cette valeur par défaut est suffisante dans la plupart des scénarios. Si les serveurs de noms servent de nombreuses requêtes DNS simultanées dans des conditions d'exploitation normales, vous pouvez spécifier une valeur élevée ou une valeur égale à zéro (0). La valeur 0 désactive cette fonctionnalité et spécifie qu'il n'y a pas de limite au nombre de requêtes DNS autorisées sur une seule connexion client. Ce paramètre est un paramètre global qui s'applique à tous les serveurs virtuels DNS configurés sur l'appliance Citrix ADC.
La valeur par défaut de ce paramètre est 255. Cette valeur par défaut est suffisante dans la plupart des scénarios. Si les serveurs de noms servent de nombreuses requêtes DNS simultanées dans des conditions d'exploitation normales, vous pouvez spécifier une valeur élevée ou une valeur égale à zéro (0). La valeur 0 désactive cette fonctionnalité et spécifie qu'il n'y a pas de limite au nombre de requêtes DNS autorisées sur une seule connexion client. Ce paramètre est un paramètre global qui s'applique à tous les serveurs virtuels DNS configurés sur l'appliance Citrix ADC.

Spécifiez le nombre maximal de demandes DNS simultanées autorisées sur une seule connexion client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour spécifier le nombre maximal de demandes DNS simultanées autorisées sur une seule connexion client et vérifiez la configuration :

```
-  set dns parameter -maxPipeline <positive_integer>
-  show dns parameter
<!--NeedCopy-->
```

Exemple :

```
> set dns parameter -maxPipeline 1000
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
        .
        .
        .
        Max DNS Pipeline Requests: 1000
 Done
<!--NeedCopy-->
```


Spécifiez le nombre maximal de demandes DNS simultanées autorisées sur une seule connexion client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, cliquez sur Modifier les paramètres DNS.
3. Dans la boîte de dialogue Configurer les paramètres DNS, spécifiez une valeur pour les demandes de pipeline DNS Max.
4. Cliquez sur OK.

Configurer le Citrix ADC en tant que résolveur final

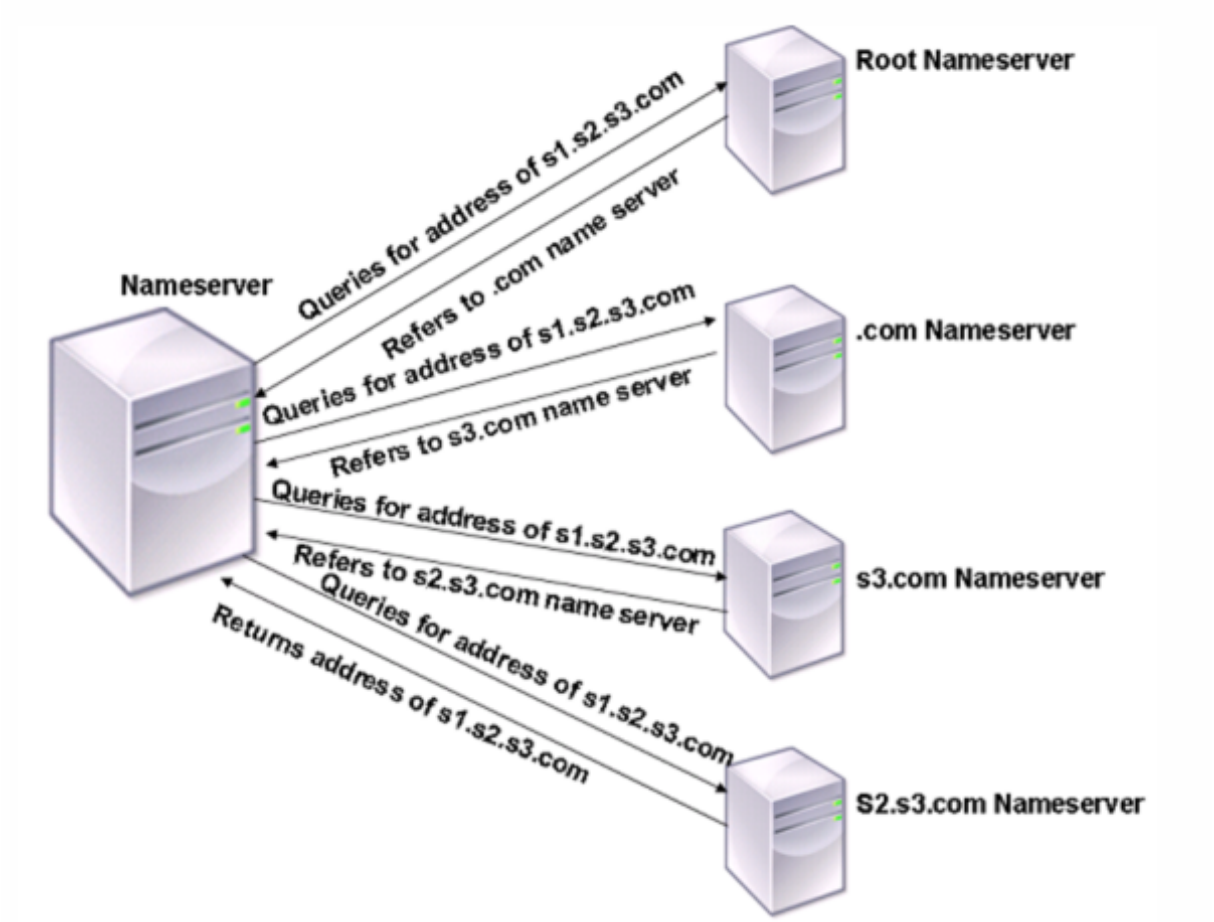
August 20, 2021

Un résolveur est une procédure appelée par un programme d'application qui traduit un nom de domaine/hôte en son enregistrement de ressource. Le résolveur interagit avec le LDNS, qui recherche le nom de domaine pour obtenir son adresse IP. Citrix ADC peut fournir une résolution de bout en bout pour les requêtes DNS.

En résolution récursive, l'appliance Citrix ADC interroge de manière récursive différents serveurs de noms pour accéder à l'adresse IP d'un domaine. Lorsque Citrix ADC reçoit une demande DNS, il vérifie son cache pour l'enregistrement DNS. Si l'enregistrement n'est pas présent dans le cache, il interroge les serveurs racine configurés dans le fichier ns.conf. Le serveur de noms racine renvoie avec l'adresse d'un serveur DNS qui contient des informations détaillées sur le domaine de deuxième niveau. Le processus est répété jusqu'à ce que l'enregistrement requis soit trouvé.

Lorsque vous démarrez l'appliance Citrix ADC pour la première fois, 13 serveurs de noms racine sont ajoutés au fichier ns.conf. Les enregistrements NS et Address pour les 13 serveurs racine sont également ajoutés. Vous pouvez modifier le fichier ns.conf, mais Citrix ADC ne vous permet pas de supprimer les 13 enregistrements. Au moins une entrée de serveur de noms est requise pour que l'appliance puisse effectuer la résolution de noms. Le diagramme suivant illustre le processus de résolution des noms.

Figure 1. Résolution récursive



Dans le processus illustré dans le diagramme, lorsque le serveur de noms reçoit une requête pour l'adresse de s1.s2.s3.com, il vérifie d'abord les serveurs de noms racine pour s1.s2.s3.com. Un serveur de noms racine renvoie avec l'adresse du serveur de noms .com. Si l'adresse de s1.s2.s3.com se trouve dans le serveur de noms, il répond avec une adresse IP appropriée. Sinon, il interroge d'autres serveurs de noms pour s3.com, puis s2.s3.com pour récupérer l'adresse de s1.s2.s3.com. De cette façon, la résolution commence toujours à partir des serveurs de noms racine et se termine par le serveur de noms faisant autorité du domaine.

Remarque : Pour la fonctionnalité de résolution récursive, la mise en cache doit être activée.

Activer la résolution récursive

Pour configurer l'appliance Citrix ADC pour qu'elle fonctionne en tant que résolveur final, vous devez activer la résolution récursive sur l'appliance.

Activer la résolution récursive à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer la résolution récursive et vérifier la configuration :

```
-  set dns parameter -recursion ENABLED
-  show dns parameter
<!--NeedCopy-->
```

Exemple :

```
> set dns parameter -recursion ENABLED
 Done
> show dns parameter
        DNS parameters:
            .
            .
            .
        Recursive Resolution : ENABLED
            .
            .
            .
 Done
<!--NeedCopy-->
```

Activer la résolution récursive à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres DNS.
3. Dans la boîte de dialogue Configurer les paramètres DNS, activez la case à cocher Activer la récursion, puis cliquez sur OK.

Définir le nombre de tentatives

Configurez l'appliance ADC pour effectuer un nombre préconfiguré de tentatives (appelées nouvelles tentatives DNS) lorsqu'elle ne reçoit pas de réponse du serveur auquel elle envoie une requête. Par défaut, le nombre de tentatives DNS est défini sur 5.

Définir le nombre de tentatives DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir le nombre de tentatives et vérifier la configuration :


```
-  set dns parameter -retries <positive_integer>
-  show dns parameter
<!--NeedCopy-->
```

Exemple :

```
> set DNS parameter -retries 3
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 3
            .
            .
            .
 Done
<!--NeedCopy-->
```

Définir le nombre de tentatives à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres DNS.
3. Dans la boîte de dialogue Configurer les paramètres DNS, dans la zone de texte Retentatives DNS, tapez le nombre de tentatives de résolution DNS, puis cliquez sur OK.

Configurer l'appliance Citrix ADC en tant que redirecteur

August 20, 2021

Un redirecteur est un serveur qui transfère les requêtes DNS aux serveurs DNS situés en dehors du réseau du serveur de redirection. Les requêtes qui ne peuvent pas être résolues localement sont transmises à d'autres serveurs DNS. Un redirecteur accumule des informations DNS externes dans son cache lorsqu'il résout des requêtes DNS. Pour configurer l'appliance Citrix ADC en tant que redirecteur, vous devez ajouter un serveur de noms externe.

L'appliance Citrix ADC vous permet d'ajouter des serveurs de noms externes vers lesquels il peut transférer les requêtes de résolution de noms qui ne peuvent pas être résolues localement. Pour configurer l'appliance Citrix ADC en tant que redirecteur, vous devez ajouter les serveurs de noms auxquels il doit transférer les requêtes de résolution de noms. Vous pouvez spécifier la priorité de recherche pour spécifier le service de noms que l'appliance Citrix ADC doit utiliser pour la résolution de noms.

> **Remarque :**
>
> L'appliance Citrix ADC en mode redirecteur prend en charge les serveurs de noms TCP, UDP et UDP-TCP.
>
> - Si vous avez configuré un serveur de noms TCP, l'appliance Citrix ADC envoie la requête DNS via TCP.
> - Si vous avez configuré un serveur de noms UDP, l'appliance Citrix ADC envoie la demande DNS via UDP.
> - Si vous avez configuré un serveur de noms UDP-TCP, l'appliance Citrix ADC envoie la demande DNS via UDP. Toutefois, si le bit tronqué est défini dans la réponse DNS, l'appliance envoie ces demandes DNS via TCP.

Ajouter un serveur de noms

August 20, 2021

Vous pouvez créer un serveur de noms en spécifiant son adresse IP ou en configurant un serveur virtuel existant comme serveur de noms.

- Serveur de**noms basé sur l'adresse IP - Serveur** de noms externe à contacter pour la résolution de noms de domaine. Si plusieurs serveurs de noms basés sur l'adresse IP sont configurés sur l'appliance et que le paramètre local n'est défini sur aucun d'entre eux, les requêtes DNS entrantes sont équilibrées de la charge sur tous les serveurs de noms, de manière ronde.
- **Serveur de noms basé sur un serveur virtuel** - Serveur virtuel DNS configuré dans le Citrix ADC. Pour un contrôle plus précis sur la façon dont les serveurs de noms DNS externes sont équilibrés (par exemple, vous voulez une méthode d'équilibrage de charge autre que la ronde préliminaire), procédez comme suit :
- Configurer un serveur virtuel DNS sur l'appliance
- Liez les serveurs de noms externes en tant que services
- Spécifiez le nom du serveur virtuel dans cette commande.

Pour vérifier la configuration, vous pouvez utiliser la`show dns nameServer` commande.

Pour supprimer un serveur de noms, dans l'interface de ligne de commande Citrix ADC, tapez la commande `rm dns nameServer` suivie de l'adresse IP du serveur de noms.

Pour afficher les détails du serveur de noms DNS, à l'interface de ligne de commande Citrix ADC, tapez la `show dns nameServer` commande suivie de l'adresse IP du serveur de noms.

Ajouter un serveur de noms (lorsque l'appliance Citrix ADC agit en tant que redirecteur) à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
add dns nameServer ((<IP>) | <dnsVserverName>)
<!--NeedCopy-->
```

Ou

```
add dns nameServer ((<IP> | <dnsVserverName>) [-type <type>]
<!--NeedCopy-->
```

Exemples :

```
add dns nameServer dnsVirtualNS

add dns nameServer 192.0.2.11 -type TCP

add dns nameServer 192.0.2.12 -type UDP_TCP


add dns nameServer 192.0.2.10
show dns nameServer 192.0.2.10

1) 192.0.2.10  -  State: UP  Protocol: UDP
Done
<!--NeedCopy-->
```

> **Remarque :**
>
> Si le type de serveur de noms n'est pas spécifié, un serveur de noms UDP est créé par défaut. Pour créer un serveur de noms de type TCP ou UDP_TCP, vous devez spécifier le type.
>
> Lorsque vous spécifiez le type UDP_TCP, deux serveurs de noms (un serveur de noms UDP et un serveur de noms TCP) sont créés pour l'adresse IP donnée.

Ajouter un serveur de noms (lorsque l'appliance Citrix ADC agit en tant que résolveur) à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>)
<!--NeedCopy-->
```

Exemple :


```
add dns nameServer 10.102.9.19 -local
show dns nameServer
1)  10.102.9.19 LOCAL -  State: UP  Protocol: UDP
Done
<!--NeedCopy-->
```

Local : Marquez l'adresse IP comme une adresse appartenant à un serveur DNS récursif local sur l'appliance Citrix ADC. L'appliance résout de manière récursive les requêtes reçues sur une adresse IP marquée comme étant locale.
Pour que la résolution récursive fonctionne, le paramètre DNS global`recursion`„ doit également être défini.
Si aucun serveur de noms n'est marqué comme étant local, l'appliance fonctionne comme un résolveur de stub et équilibre la charge des serveurs de noms.

Ajouter un serveur de noms à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **DNS** > **Serveurs de noms** et créez un serveur de noms.

Définir la priorité de recherche DNS

August 20, 2021

Vous pouvez définir la priorité de recherche sur DNS ou WINS. Cette option est utilisée dans le mode VPN SSL.

Définissez la priorité de recherche sur DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir la priorité de recherche sur DNS et vérifier la configuration :

```
-  set dns parameter -nameLookupPriority (DNS | WINS)
-  show dns parameter
<!--NeedCopy-->
```

Exemple :

```
> set dns parameter -nameLookupPriority DNS
 Done
> show dns parameter
```



```
4                .
5                .
6                .
7           Name lookup priority : DNS
8                .
9                .
10               .
11   Done
12  <!--NeedCopy-->
```

Définir la priorité de recherche sur DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur Modifier les paramètres DNS.
3. Dans la boîte de dialogue **Configurer les paramètres DNS**, sous **Priorité de recherche de nom**, sélectionnez DNS ou WINS, puis cliquez sur OK.

> **Remarque**
>
> Si le serveur virtuel DNS que vous avez configuré est DOWN et si vous définissez le –nameLookupPriority sur DNS, Citrix ADC ne tente pas de recherche WINS. Par conséquent, si un serveur virtuel DNS n'est pas configuré ou est désactivé, définissez–nameLookupPriority la sur WINS.

Désactiver et activer les serveurs de noms

August 20, 2021

La procédure suivante décrit les étapes à suivre pour activer ou désactiver un serveur de noms existant.

Activer ou désactiver un serveur de noms à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver un serveur de noms et vérifier la configuration :

```
1  -  (enable | disable) dns nameServer <IPAddress>
2  -  show dns nameServer <IPAddress>
3  <!--NeedCopy-->
```

Exemple :


```
> disable dns nameServer 10.102.9.19
 Done
> show dns nameServer 10.102.9.19
1)       10.102.9.19: LOCAL  -  State: OUT OF SERVICE
 Done
<!--NeedCopy-->
```

Activer ou désactiver un serveur de noms à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Serveurs de noms**.
2. Dans le volet d'informations, sélectionnez le serveur de noms que vous souhaitez activer ou désactiver.
3. Cliquez sur Activer ou Désactiver. Si un serveur de noms est activé, l'option Désactiver est disponible. Si un serveur de noms est désactivé, l'option Activer est disponible.

Configurer Citrix ADC en tant que résolveur de stub adapté à la sécurité sans validation

August 20, 2021

À partir de Citrix ADC 12.1 build 49.xx, Citrix ADC agit comme un stub-résolveur non validateur prenant en charge la sécurité. Pour activer cette prise en charge, le bit AD est défini dans l'en-tête DNS et le bit DO n'est pas défini dans l'en-tête OPT. Lorsque le bit AD est défini et que le bit DO n'est pas défini, le résolveur récursif en amont valide la réponse DNSSEC. Si la validation réussit, le résolveur récursif répond sans RR DNSSEC. Si la validation DNSSEC échoue, le résolveur récursif retourne avec une réponse SERVFAIL.

> **Important :**
>
> Le bit AD est défini par défaut dans le redirecteur ADC. Le bit AD n'est pas défini pour les requêtes lancées par DBS.

Prise en charge des trames Jumbo pour DNS pour gérer les réponses de grandes tailles

August 20, 2021

À partir de Citrix ADC 12.1 build 49.xx, DNS prend en charge les trames jumbo pour gérer les réponses UDP supérieures à 1 280 octets. Auparavant, l'appliance Citrix ADC ne supporte que la taille des paquets UDP jusqu'à 1 280 octets.

Vous pouvez définir la taille maximale des paquets UDP que l'appliance peut gérer en modes proxy, ADNS et redirecteur en configurant la valeur du paramètre Maximum UDP Packet Size. Par exemple, si la valeur du paramètre Maximum UDP Packet Size est définie sur 4096, l'appliance peut gérer la réponse DNS d'une taille de 4 096 octets.

> **Important**
>
> - En mode proxy, la taille minimale entre la taille de la charge utile OPT de la demande client et la valeur Maximum UDP Packet Size est prise en compte pour l'envoi de requêtes DNS au back-end. Par exemple, si la taille de charge utile OPT demande du client est de 3000 et que la valeur Maximum UDP Packet Size est 4096, 3 000 octets requêtes DNS sont envoyées au back-end.
>
> De plus, à partir du back-end, l'appliance peut recevoir des réponses de grandes tailles et traiter des réponses de grandes tailles.
> - En mode redirecteur, l'appliance définit la taille de la charge utile OPT égale à la valeur du paramètre de taille de paquet UDP.
> - Si les enregistrements DNS sont locaux de l'appliance, celle-ci peut composer des tailles de réponse aussi grandes que la valeur du paramètre Maximum UDP Packet Size. Ce paramètre s'applique aux résolveurs ADNS, proxy et récursifs.

Pour configurer la taille maximale des paquets UDP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set dns parameter [-maxUDPPacketSize <positive_integer>]
<!--NeedCopy-->
```

Exemple :

```
set dns parameter -maxUDPPacketSize 10000
<!--NeedCopy-->
```

> **Remarque** : Les valeurs minimales et maximales que vous pouvez définir pour le paramètre Maximum UDP Packet Size sont respectivement 512 et 16384. La valeur par défaut est 1280.

Pour configurer la taille maximale des paquets UDP à l'aide de l'interface de ligne de commande

1. Accédez à **Gestion du trafic** > **DNS**.
2. Dans le volet d'informations, cliquez sur **Modifier les paramètres DNS**.
3. Dans Taille maximale du paquet UDP, spécifiez la taille maximale du paquet UDP.
4. Cliquez sur **OK**.

Configurer la journalisation DNS

October 5, 2021

Vous pouvez configurer l'appliance Citrix ADC pour consigner les demandes DNS et les réponses qu'il gère. La solution matérielle-logicielle consigne les demandes et réponses DNS au format SYSLOG. Vous pouvez choisir de consigner les demandes DNS ou les réponses DNS, ou les deux, et d'envoyer les messages Syslog à un serveur de journaux distant. Les messages de journal peuvent être utilisés pour :

- Audit des réponses DNS au client
- Audit des clients DNS
- Détecter et prévenir les attaques DNS
- Dépannage

Une appliance Citrix ADC peut consigner les sections suivantes dans la demande ou la réponse DNS, en fonction de votre configuration :

- Section d'en-tête
- Section des questions
- Section Réponses
- Section de l'autorité
- Section **supplémentaire**

Profils DNS

Vous pouvez utiliser un profil DNS pour configurer les différents paramètres DNS que vous souhaitez que le point de terminaison DNS applique au trafic DNS. Dans le profil, vous pouvez activer la journalisation, la mise en cache et la mise en cache négative.

Important : Depuis la version NetScaler 11.0, l'activation de la mise en cache DNS à l'aide des paramètres DNS globaux est obsolète. Vous pouvez activer ou désactiver la mise en cache DNS à l'aide de profils DNS. Vous pouvez désormais activer la mise en cache DNS pour un serveur virtuel

individuel en activant la mise en cache DNS dans un profil DNS et en définissant le profil DNS sur le serveur virtuel individuel.

Les profils DNS prennent en charge les types de journalisation DNS suivants :

- Journalisation des requêtes DNS
- Journalisation de la section de réponses DNS
- Journalisation étendue DNS
- Journalisation des erreurs DNS

Journalisation des requêtes DNS

Vous pouvez configurer un dispositif Citrix ADC pour qu'il consigne uniquement les requêtes DNS reçues par les points de terminaison DNS sur l'appliance.

Remarque : Si des erreurs se produisent pendant le traitement d'une requête, elles sont consignées si cette option est définie dans le profil DNS.

Voici un exemple de message de journal des requêtes :

```
1 DNS DNS_QUERY 143 0 :  U:10.102.27.70#61297:10.102.27.73#53/22142/Q/
2 (RD)/NO/1/0/0/0#test.com./1#
3 <!--NeedCopy-->
```

Journalisation de la section de réponses DNS

Vous pouvez configurer une appliance Citrix ADC pour consigner toutes les sections **Réponses** des réponses DNS que l'appliance envoie au client. La journalisation de la section Réponses DNS est utile lorsque Citrix ADC est configuré en tant que résolveur DNS ou dans les cas d'utilisation GLSB.

Voici un exemple de journal de section de réponses DNS :

```
1 DNS DNS_RESPONSE 6678 0 :  U:100.100.100.210#32776:100.100.100.10#
2 53/61373/Q/(RD,AA,RA,R)/NO/1/1/2/4#n1.citrix.com1./
3 28#ANS#AAAA/120/1111:2345:6789:ffab:abcd:effa:1234:3212##
4 <!--NeedCopy-->
```

Journalisation étendue DNS

Pour configurer une appliance Citrix ADC afin de consigner les sections Authority et **Additional** dans les réponses DNS, activez la journalisation étendue avec la journalisation de la section Réponses.

Remarque : Si des erreurs se produisent pendant le traitement des requêtes ou des réponses, elles sont consignées si cette option est définie dans le profil DNS.

Voici un exemple de message consigné lorsque la recherche du cache est terminée et que la réponse est incorporée dans le paquet :

```
DNS DNS_RESPONSE 2252 0 :  T:100.100.100.118#21411:100.100.100.10
#53/48537/Q/(RD,AA,CD,RA,R)/NO/1/1/2/6#a1.citrix.com1./1#ANS#A/
120/1.1.1.1##AUTH#citrix.com1/NS/120/n2.citrix.com1#n1.citrix.com1##ADD
   #n1.citrix.com1
/A/120/1.1.1.1#1.1.1.2##n1.citrix.com1/AAAA/120/
1111:2345:6789:ffab:abcd:effa:1234:3212##n2.citrix.com1/A/120/2.1.1.2
##n2.citrix.com1/AAAA/120/2222:faff:3212:8976:123:1241:64:ff9b##OPT
   /0/1280/DO##
<!--NeedCopy-->
```

Journalisation des erreurs DNS

Vous pouvez configurer une appliance Citrix ADC pour consigner les erreurs ou les échecs qui se produisent lors du traitement d'une requête ou d'une réponse DNS. Pour ces erreurs, la solution matérielle-logicielle consigne l'en-tête DNS, les sections **Question** et les enregistrements OPT.

Voici un exemple de message consigné lorsqu'une erreur se produit pendant le traitement d'une demande ou d'une réponse DNS :

```
DNS DNS_ERROR 149 0 :  U:10.102.27.70#27832:10.102.27.73#53/61153/Q/
(RD)/NO/1/0/0/0#test.com./1140#Packet Dropped
<!--NeedCopy-->
```

Journalisation basée sur des stratégies

Vous pouvez configurer la journalisation personnalisée basée sur des expressions DNS en configurant les stratégies LogAction on DNS, Rewrite ou Responder. Vous pouvez spécifier que la journalisation se produit uniquement lorsqu'une stratégie DNS particulière est évaluée à true. Pour plus d'informations, voir Configurer la journalisation basée sur des stratégies pour DNS.

Comprendre le format de message syslog du journal Citrix ADC

L'appliance Citrix ADC consigne les demandes et réponses DNS au format Syslog suivant :

```
<transport> :<client IP>#<client ephemeral port>:<DNS endpoint IP>#<
   port>
 : <query id> /opcode/header flags/rcode/question section count/answer
    section count
/ auth section count / additional section count #<queried domain name>
/<queried type>#...
```



```
<!--NeedCopy-->
```

- **<transport>:**
  - T = TCP
  - U = UDP
- **# :** <client IP>< client ephemeral port > adresse IP et numéro de port du client DNS
- **# :** <DNS endpoint IP><port>adresse IP et numéro de port du point de terminaison DNS Citrix ADC
- **:**
  <query id>ID de requête
- **:** <opcode>code de fonctionnement. Valeurs prises en charge :
  - Q : requête
  - I : requête inverse
  - S : état
  - X0 : non affecté
  - N : notifier
  - U : mise à jour
  - X1-10 : valeurs non attribuées
- **:** <header flags>drapeaux. Valeurs prises en charge :
  - RD : récursion souhaitée
  - TC : tronqué
  - AA : réponse faisant autorité
  - CD : vérification désactivée
  - AD : données authentifiées
  - Z : non affecté
  - RA : récursion disponible
  - R : réponse
- **:** <rcode>Code de réponse. Valeurs prises en charge :
  - NON : aucune erreur
  - Erreur de format F
  - S : défaillance du serveur
  - NX : domaine inexistant
  - NI : non implémenté
  - R : requête refusée
  - YX : le nom existe alors qu'il ne doit pas
  - YXR : RR Set existe alors qu'il ne doit pas

  - NXR : Le jeu de RR qui doit exister n'existe pas
  - NAS : le serveur ne fait pas autorité pour la zone
  - NA : Non autorisé
  - NZ : nom non contenu dans la zone
  - X1-5 : non affecté

- **/nombre de sections de questions/nombre de sections de réponse/nombre de sections auth/nombre de sections supplémentaires :** section de question, nombre de sections d'autorité et nombre de sections **supplémentaires** dans la requête DNS
- **/:** <queried domain name><queried type>domaine interrogé et type interrogé dans la requête DNS
- **#ANS #<record type>/<ttl>/.. #AUTH #<domain name>/<record type>/<ttl>.. #ADD #<domain name>/<record type>/<ttl>... :**

  Dans les réponses DNS :

  La section Réponses est consignée si la journalisation de la section de réponses est activée dans le profil DNS. Les sections Authority et **Additional** sont consignées si la journalisation étendue est activée dans le profil DNS. Le format du journal diffère en fonction du type d'enregistrement. Pour plus d'informations, consultez la rubrique Présentation du format de journalisation des enregistrements.

  - ANS : section réponse
  - AUTH : autorité
  - ADD : section **supplémentaire**
- **Taille maximale de la charge utile OPT/ /UDP :** <edns version>format d'enregistrement OPT dans le journal DNS
- **<EDNS version><ECS Address>OPT/<UDP payload size>//<"DO"ou vide selon que le bit OK DNSSEC est défini ou non>/<value of RDLEN>/ECS/<Q/R>/<option length>/<Family>/<Source Prefix-Length>/<Scope Prefix-Length>/<ECS Address>:**

  Si la requête ou la réponse DNS inclut l'option EDNS Client Subnet (ECS), elle est également consignée dans le format d'enregistrement OPT dans le fichier journal DNS.

  Lorsqu'une requête DNS avec une option ECS incluant une adresse IPv4 ou IPv6 est envoyée, l'option ECS est consignée avec l'une des options suivantes :

  - « ECS/Q » indiquant que les valeurs du journal proviennent de la requête
  - « ECS/R » indiquant que les valeurs du journal proviennent de la réponse.

  La valeur de Scope Prefix-Length est également définie de manière appropriée. Dans la requête DNS, elle est définie sur zéro, et pour la réponse, elle est définie sur la valeur calculée.

  Le tableau suivant décrit les détails consignés dans différents scénarios :

Scénario	Option ECS définie dans la requête DNS	Option ECS définie dans la réponse DNS	Détails consignés
La journalisation des requêtes et la journalisation étendue sont toutes deux activées	Oui	Oui	L'option ECS est consignée avec la chaîne « ECS/R/ » et la longueur du préfixe de portée est définie sur la valeur calculée.
La journalisation des requêtes et la journalisation étendue sont toutes deux activées	Oui	Non	L'option ECS est consignée avec la chaîne « ECS/Q » et la longueur du préfixe de portée est définie sur zéro.
La journalisation des requêtes est activée, mais la journalisation étendue n'est pas activée	Oui	Oui	L'option ECS est consignée avec la chaîne « ECS/Q/ » et la longueur du préfixe de portée est définie sur zéro.
La journalisation des requêtes et la journalisation étendue ne sont pas activées	Oui	Oui	L'option ECS n'est pas consignée.
La journalisation des requêtes est activée, mais la journalisation étendue n'est pas activée	Oui	Non	L'option ECS est consignée avec la chaîne « ECS/Q/ » et la longueur du préfixe de portée est définie sur zéro.
La journalisation des requêtes n'est pas activée, mais la journalisation étendue est activée	Oui	Oui	L'option ECS est consignée avec la chaîne « ECS/R/ » et la longueur du préfixe de portée est définie sur la valeur calculée.

Scénario	Option ECS définie dans la requête DNS	Option ECS définie dans la réponse DNS	Détails consignés
La journalisation des requêtes n'est pas activée, mais la journalisation étendue est activée	Oui	Non	L'option ECS n'est pas consignée.

Comprendre le format de journalisation des enregistrements

Voici un exemple du format de journalisation des enregistrements dans un message Syslog :

```
<domainname>/<record type>/ <record ttl> / <resource record data>#<
   resource record data>#......##
<!--NeedCopy-->
```

Où :

Type d'enregistrement	Exemple de format	Données et format des enregistrements de ressources
Enregistrement de l'adresse (A)	A/5/1.1.1.1#1.1.1.2#1.1.1.3##	Adresse IPv4
Record AAAA	AAAA/5/1::1#1::2#1::3##	adresse IPv6
Record SOA	SOA/3600/ns1.dnslogging.test./	Serveur Origin, contact et autres détails. Le format d'enregistrement des ressources est : <originServer><contact>/<serial number>/<refresh rate>/<retry>/<expire>//<minimum>##
Enregistrement NS	NS/5/ns1.dnslogging.test	Nom d'hôte du serveur de noms.
Record MX	#MX/5/10/host1.dnslogging.test	Préférence suivie du nom d'hôte du serveur d'échange de messagerie
Enregistrement CNAME	CNAME/5/host1.dnslogging.test.##	Nom canonique

Type d'enregistrement	Exemple de format	Données et format des enregistrements de ressources
Enregistrement SRV	SRV/5/1/2/3/host1.dnslogging.t	Format d'enregistrement de ressource : <priority><weight>//<port>/<target># .##
Enregistrement TXT	TXT/5/dns+logging##	Les données comprennent tous les textes.
Enregistrement NAPTR	NAPTR/5/10/11////dnslogging#.	Format d'enregistrement de ressource : <order>/<preference>/<flags>/<services>/<re expression>/<replacement string># ##
Enregistrement DNSKEY	DNSKEY/5/1/3/5/AwEAAanP0K+i	Format d'enregistrement de ressource : <flags>/<protocol>/<algorithm>/<public key in base64 encoding># x6JZgiDBZhSON
Enregistrement PTR	PTR/3600/test.com.#test4.com.	Nom de domaine

Limitations de la journalisation DNS

La journalisation DNS présente les limitations suivantes :

- Si la journalisation des réponses est activée, seuls les types d'enregistrement suivants sont consignés :
  - Enregistrement de l'adresse (A)
  - Record AAAA
  - Record SOA
  - Enregistrement NS
  - Record MX
  - Enregistrement CNAME
  - Enregistrement SRV
  - Enregistrement TXT
  - Enregistrement NAPTR
  - Enregistrement DNSKEY
  - Enregistrement PTR

  Pour tous les autres types d'enregistrement, seuls les paramètres L3/L4, l'en-tête DNS et la sec-

tion Question sont consignés.

- Les enregistrements RRSIG ne sont pas consignés même si la journalisation des réponses est activée.
- Le DNS64 n'est pas pris en charge.
- Les demandes ou réponses de mise à jour proactive DNS sont consignées en fonction des paramètres du profil par défaut.
- Sur le serveur virtuel, si l'option sans session et la journalisation des réponses sont activées, les paramètres L3/L4, l'en-tête DNS et la section Question DNS sont consignés à la place de la réponse.
- La taille maximale du message Syslog est de 1 024 octets.
- Si vous avez défini un profil DNS pour une stratégie DNS avec le type d'action Réponse de réécriture, l'appliance Citrix ADC ne consigne pas la requête ou les réponses manipulées. Pour consigner les informations requises, vous devez utiliser une action de message d'audit dans la stratégie DNS.
- Les transactions DNS dues au trafic de surveillance DNS ne sont pas consignées.

Configuration de la journalisation DNS

Voici un aperçu de la configuration de la journalisation DNS :

1. Créez une action Syslog et activez le DNS dans l'action.
2. Créez une stratégie Syslog et spécifiez l'action Syslog dans la stratégie.
3. Liez globalement la stratégie Syslog pour activer la journalisation de tous les événements système Citrix ADC. Vous pouvez également lier la stratégie Syslog à un serveur virtuel d'équilibrage de charge spécifique.
4. Créez un profil DNS et définissez l'un des types de journalisation suivants que vous souhaitez activer :
    - Journalisation des requêtes DNS
    - Journalisation de la section de réponses DNS
    - Journalisation étendue DNS
    - Journalisation des erreurs DNS
5. Configurez l'un des éléments suivants, en fonction de vos besoins :
    - Service DNS et serveur virtuel pour DNS
    - Service ADNS
    - Citrix ADC en tant que redirecteur
    - Citrix ADC en tant que résolveur
6. Définissez le profil DNS créé sur l'une des entités DNS.

Configurer la journalisation DNS pour Citrix ADC configuré en tant que proxy DNS à l'aide de l'interface de ligne de commande

1. Ajoutez une action Syslog et activez le DNS dans l'action. À l'invite de commandes, tapez :

```
add audit syslogAction <name> (<serverIP> | -lbVserverName <string
    >) [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat <
    dateFormat>] [-logFacility <logFacility>] [-tcp ( NONE | ALL )]
     [-acl ( ENABLED | DISABLED )] [-timeZone ( GMT_TIME |
    LOCAL_TIME )] [-userDefinedAuditlog ( YES | NO )] [-
    appflowExport ( ENABLED |DISABLED )] [-lsn ( ENABLED | DISABLED
     )] [-alg ( ENABLED | DISABLED )] [-transport ( TCP | UDP )] [-
    tcpProfileName <string>] [-maxLogDataSizeToHold <
    positive_integer>] [-dns ( ENABLED | DISABLED)]
<!--NeedCopy-->
```

   Exemple :

   ```
   add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
   ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
   LOCAL_TIME -dns ENABLED
   ```

2. Créez une stratégie Syslog et spécifiez l'action Syslog créée dans la stratégie. À l'invite de commandes, tapez :

   ```
   add audit syslogPolicy <name> <rule> <action>
   ```

   Exemple :

   ```
   add audit syslogPolicy syslogpol1 ns_true nssyslogact1
   ```

3. Liez la stratégie Syslog globalement. À l'invite de commandes, tapez :

   ```
   bind system global [<policyName> [-priority <positive_integer>]]
   ```

   Exemple :

   ```
   bind system global syslogpol1
   ```

4. Créez un profil DNS et activez l'un des types de journaux suivants que vous souhaitez configurer :

   - Journalisation des requêtes DNS
   - Journalisation de la section de réponses DNS
   - Journalisation étendue DNS
   - Journalisation des erreurs DNS

   À l'invite de commandes, tapez :

   ```
   add dns profile <dnsProfileName> [-dnsQueryLogging ( ENABLED | DISABLED
    )] [-dnsAnswerSecLogging ( ENABLED | DISABLED )] [-dnsExtendedLogging
   ```



```
 (ENABLED | DISABLED )] [-dnsErrorLogging ( ENABLED | DISABLED )] [-
cacheRecords ( ENABLED | DISABLED )] [-cacheNegativeResponses ( ENABLED
 | DISABLED )]
```

Exemple :

```
add dns profile dnsprofile1 -dnsQueryLogging ENABLED
```

5. Configurez le service de type DNS. À l'invite de commandes, tapez :

   ```
   add service <name> <serverName> <serviceType> <port>
   ```

   Exemple :

   ```
   add service svc1 10.102.84.140 dns 53
   ```

6. Configurez un serveur virtuel d'équilibrage de charge de type DNS de type de service.

   ```
   add lb vserver <name> <serviceType> <ip> <port>
   ```

   Exemple :

   ```
   add lb vserver lb1 dns 100.100.100.10 53
   ```

7. Liez le service au serveur virtuel. À l'invite de commandes, tapez :

   ```
   bind lb vserver <name> <serviceName>
   ```

   Exemple :

   ```
   bind lb vserver lb1 svc1
   ```

8. Définissez le profil DNS créé sur le serveur virtuel. À l'invite de commandes, tapez :

   ```
   set lb vserver <name> [ - dnsProfileName <string>]
   ```

   Exemple :

   ```
   set lb vserver lb1 -dnsProfileName dnsprofile1
   ```

Exemple de configuration de journalisation DNS pour l'appliance Citrix ADC configurée en tant que proxy DNS

```
1 > add audit syslogAction nssyslogact1 10.102.151.136 -logLevel
2 CRITICAL ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -
     timeZone
3 LOCAL_TIME -dns ENABLED
4 Done
5 > add audit syslogPolicy syslogpol1 ns_true nssyslogact1
6 Done
7 > bind system global syslogpol1
8 Done
```



```
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add lb vserver lb1 dns 100.100.100.10 53  - dnsProfileName dnsprofile1
Done
> add service svc1 10.102.84.140 dns 53
Done
> bind lb vserver lb1 svc1
Done
<!--NeedCopy-->
```

Exemple de configuration de journalisation DNS pour l'appliance Citrix ADC configurée en tant qu'ADNS

```
> add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
    LOCAL_TIME
-dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add lb vserver lb1 dns 100.100.100.10 53  - dnsProfileName dnsprofile1
Done
> add service svc1 10.102.84.140 dns 53
Done
> bind lb vserver lb1 svc1
Done
<!--NeedCopy-->
```

Exemple de configuration de journalisation DNS pour l'appliance Citrix ADC configurée en tant que redirecteur

```
> add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
    LOCAL_TIME
-dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
```



```
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add dns nameserver 8.8.8.8  - dnsProfileName dnsprofile1
Done
<!--NeedCopy-->
```

Exemple de configuration de journalisation DNS pour l'appliance Citrix ADC configurée en tant que résolveur

```
> add audit syslogAction nssyslogact1 10.102.151.136
-logLevel CRITICAL ERROR WARNING NOTICE INFORMATIONAL DEBUG -
    logFacility LOCAL4
-timeZone LOCAL_TIME -dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> set dns parameter -recursion enABLED
Done
> add nameserver 1.1.1.100 -local dnsProfileName dnsprofile1
Done
<!--NeedCopy-->
```

Configurer la journalisation basée sur des stratégies pour DNS

La journalisation basée sur des stratégies vous permet de spécifier un format pour les messages de journal. Le contenu d'un message de journal est défini à l'aide d'une expression de stratégie avancée. Lorsque l'action de message spécifiée dans la stratégie est exécutée, l'appliance Citrix ADC construit le message de journal à partir de l'expression et écrit le message dans le fichier journal. Vous pouvez configurer la solution matérielle-logicielle pour qu'elle se connecte uniquement lorsqu'une stratégie DNS particulière est évaluée à True.

> **Remarque**
>
> Si vous avez défini une stratégie DNS avec un profil DNS pour le côté demande, l'appliance Citrix ADC consigne uniquement la requête.

Pour configurer la journalisation basée sur une stratégie pour une stratégie DNS, vous devez d'abord configurer une action de message d'audit. Pour plus d'informations sur la configuration d'une action de message d'audit, voir Configurer l'appliance NetScaler pour la journalisation des audits. Après avoir configuré l'action du message d'audit, spécifiez l'action du message dans une stratégie DNS.

Configurer la journalisation basée sur une stratégie pour une stratégie DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la journalisation basée sur une stratégie pour une stratégie DNS et vérifier la configuration :

```
1 - add dns action <actionName> <actionType> [-IPAddress <ip_addr|
    ipv6_addr> ... | -viewName <string> | -preferredLocList <string>
    ...] [-TTL <secs>] [-dnsProfileName <string>]
2 - set dns policy <name> [<rule>] [-actionName <string>] [-logAction <
    string>]
3 - show dns policy [<name>]
4 <!--NeedCopy-->
```

Exemple 1 :

Dans un déploiement GSLB, si vous souhaitez répondre avec des adresses IP différentes aux demandes des clients provenant d'un sous-réseau particulier, au lieu de répondre avec des adresses IP utilisées à des fins générales (telles que les adresses IP des utilisateurs internes), vous pouvez configurer une stratégie DNS avec le type d'action comme vue DNS. Dans ce cas, vous pouvez configurer la journalisation DNS sur l'action DNS spécifiée afin de pouvoir consigner les réponses spécifiques.

```
1 > add dns profile dns_prof1 -dnsqueryLogging enABLED -
    dnsanswerSecLogging enABLED
2  Done
3 > add dns view dns_view1
4  Done
5 > add dns action dns_act1 viewName -view dns_view1  - dnsprofilename
    dns_prof1
6  Done
7 > add dns policy dns_pol1 "CLIENT.IP.SRC.APPLY_MASK(255.255.255.0).EQ
    (100.100.100.0)"
8 dns_act1
9  Done
10 > bind dns global dns_pol1 100 -gotoPriorityExpression END -type
    REQ_DEFAULT
11  Done
12 > bind gslb service site_1_svc -viewName dns_view1 123.1.1.1
13  Done
```



```
> bind gslb service site_5_svc -view dns_view1 132.1.1.1
 Done
<!--NeedCopy-->
```

Remarque : Dans la configuration précédente, si vous recherchez le domaine configuré sur un serveur virtuel GSLB, par exemple, *sampletest.com*, tous les utilisateurs internes du sous-réseau 100.100.100.0/24 sont servis avec les adresses IP de la vue DNS et les réponses sont consignées. Les demandes des clients pour d'autres sous-réseaux ne sont pas consignées.

Exemple 2 :

Si vous souhaitez consigner uniquement les requêtes pour le domaine *exemple.com*, vous pouvez créer un profil DNS avec la journalisation des requêtes activée et définir le profil DNS sur une action DNS avec le type d'action
NOOP, puis créer une stratégie DNS et définir l'action DNS. Par exemple :

```
>add dns profile query_logging -dnsqueryLogging ENABLED
Done
>add dns action dns_act1 NOOP -dnsprofileName query_logging
Done
>add dns policy dns_pol1 DNS.REQ.QUESTION.DOMAIN.EQ("example.com")
   dns_act1
Done
<!--NeedCopy-->
```

Configuration des suffixes DNS

August 20, 2021

Vous pouvez configurer des suffixes DNS qui permettent à l'appliance Citrix ADC de terminer des noms de domaine non qualifiés au cours de la résolution des noms. Par exemple, lors de la résolution d'un nom de domaine non qualifié abc, si un suffixe DNS example.com est configuré, l'appliance ajoute le suffixe au nom de domaine. Ensuite, il résout le nom de domaine. Dans ce cas, il résoudrait abc.example.com. Si les suffixes DNS ne sont pas configurés, l'appliance ajoute une période aux noms de domaine non qualifiés et résout le nom de domaine.

Créer des suffixes DNS

Les suffixes DNS ont une signification et ne sont valides que lorsque Citrix ADC est configuré en tant que résolveur final ou redirecteur. Vous pouvez spécifier un suffixe pouvant contenir jusqu'à 127 caractères.

Remarque : L'ordre des suffixes DNS est important. L'appliance ADC tente les suffixes configurés dans un ordre série et s'arrête lorsqu'elle obtient une réponse réussie pour un suffixe.

Créer des suffixes DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un suffixe DNS et vérifier la configuration :

```
1 -  add dns suffix <dnsSuffix>
2 -  show dns suffix <dnsSuffix>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns suffix example.com
2  Done
3 > show dns suffix example.com
4 1)      Suffix: example.com
5 Done
6
7 <!--NeedCopy-->
```

Pour supprimer un suffixe DNS à l'aide de la ligne de commande Citrix ADC, à l'invite de commandes, tapez la `rm dns suffix` commande et le nom du suffixe DNS.

Créer des suffixes DNS à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Suffixe** DNS et créez des suffixes DNS.

Requête DNS ANY

August 20, 2021

Une requête ANY est un type de requête DNS qui récupère tous les enregistrements disponibles pour un nom de domaine. La requête AUY doit être envoyée à un serveur de noms faisant autorité pour un domaine.

Comportement en mode ADNS

En mode ADNS, l'appliance Citrix ADC renvoie les enregistrements conservés dans son cache local. S'il n'y a aucun enregistrement dans le cache, l'appliance renvoie la réponse NXDOMAIN (négative).

Si le contrôleur de domaine Citrix ADC peut correspondre aux enregistrements de délégation de domaine, il renvoie les enregistrements NS. Sinon, il renvoie les enregistrements NS du domaine racine.

Comportement en mode proxy DNS

En mode proxy, l'appliance Citrix ADC vérifie son cache local. S'il n'y a aucun enregistrement dans le cache, l'appliance transmet la requête au serveur.

Comportement pour les domaines Global Server Load Balancing (GSLB)

Si un domaine GSLB est configuré sur l'appliance ADC et qu'une requête ANY est envoyée pour le domaine GSLB (site), l'appliance renvoie l'adresse IP du service GSLB. Il sélectionne ce service via une décision d'équilibrage de charge. Si l'option de réponse IP multiple (MIR) est activée, les adresses IP de tous les services GSLB sont envoyées.

Pour que Citrix ADC renvoie ces enregistrements lorsqu'il répond à la requête ANY, tous les enregistrements correspondant à un domaine GSLB doivent être configurés sur Citrix ADC.

> **Remarque**
>
> Si les enregistrements d'un domaine sont distribués entre Citrix ADC et un serveur, seuls les enregistrements configurés sur ADC Citrix sont renvoyés.

Le Citrix ADC offre la possibilité de configurer les vues DNS et les stratégies DNS. Ces vues et stratégies sont utilisées pour effectuer l'équilibrage global de la charge du serveur. Pour plus d'informations, voir Global Server Load Balancing.

Configurer la mise en cache négative des enregistrements DNS

August 20, 2021

L'appliance Citrix ADC prend en charge la mise en cache des réponses négatives pour un domaine. Une réponse négative indique que les informations sur un domaine demandé n'existent pas ou que le serveur ne peut pas fournir de réponse à la requête. Le stockage de ces informations est appelé mise en cache négative. La mise en cache négative permet d'accélérer les réponses aux requêtes concernant un domaine.

> **Remarque :**
>
> La mise en cache négative n'est prise en charge que lorsque le serveur principal est configuré en tant que serveur DNS (ADNS) faisant autorité pour le domaine interrogé.

Une réponse négative peut être l'une des réponses suivantes :

- Message d'erreur NXDOMAIN : les serveurs DNS faisant autorité répondent avec le message d'erreur NXDOMAIN lorsque le nom de domaine demandé n'a pas d'enregistrements configurés sur le serveur. Ce message implique que le domaine interrogé est un nom de domaine non valide ou inexistant.
- Message d'erreur NODATA : si le nom de domaine dans la requête est valide mais que les enregistrements du type donné ne sont pas disponibles, l'appliance envoie un message d'erreur NODATA.

Lorsque la mise en cache négative est activée, l'appliance met en cache la réponse négative du serveur DNS et ne sert que les futures requêtes du cache. Cette action permet d'accélérer les réponses aux requêtes et de réduire le trafic DNS back-end. La mise en cache négative peut être utilisée dans tous les déploiements, c'est-à-dire lorsqu'une appliance Citrix ADC sert de proxy, de résolution finale ou de redirecteur.

Vous pouvez activer ou désactiver la mise en cache négative à l'aide d'un profil DNS. Pour plus d'informations, voir Profils DNS. Par défaut, la mise en cache négative est activée dans le profil DNS par défaut (**default**-dns-profile) qui sont liés par défaut à un serveur virtuel DNS ou dans le profil DNS nouvellement créé.

Activer ou désactiver la mise en cache négative à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver la mise en cache négative et vérifier la configuration :

```
1 -  add dns profile <dnsProfileName> [-cacheRecords ( ENABLED | DISABLED
     )] [-cacheNegativeResponses (ENABLED | DISABLED )]
2 -  show dns profile [<dnsProfileName>]
3 <!--NeedCopy-->
```

Exemple de profil DNS par défaut :

```
1 > sh dns profile default-dns-profile
2     1)   default-dns-profile
3         Query logging : DISABLED        Answer section logging :
             DISABLED
4         Extended logging : DISABLED     Error logging : DISABLED
5         Cache Records : ENABLED     Cache Negative Responses: ENABLED
6 Done
7 <!--NeedCopy-->
```

Exemple de profil DNS nouvellement créé :


```
> add dnsprofile dns_profile1 -cacheRecords ENABLED -
    cacheNegativeResponses ENABLED
Done
> show dns profile dns_profile1
    1)   dns_profile1
        Query logging : DISABLED        Answer section logging :
           DISABLED
        Extended logging : DISABLED     Error logging : DISABLED
        Cache Records : ENABLED     Cache Negative Responses: ENABLED
Done
<!--NeedCopy-->
```

Spécifier les paramètres DNS au niveau du service ou du serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, effectuez les opérations suivantes :

1. Configurez le profil DNS.

   ```
   add dns profile <dnsProfileName> [-cacheRecords ( ENABLED | DISABLED )]
    [-cacheNegativeResponses (ENABLED | DISABLED )]
   ```

2. Liez le profil DNS au service ou au serveur virtuel.

   Pour lier le profil DNS au service :

   ```
   set service <name> [-dnsProfileName <string>]
   ```

Exemple :

```
>set service service1 -dnsProfileName dns_profile1
Done
<!--NeedCopy-->
```

Pour lier le profil DNS au serveur virtuel :

```
set lb vserver <name> [-dnsProfileName <string>]
```

Exemple :

```
>set lb vserver lbvserver1 -dnsProfileName dns_profile1
Done
<!--NeedCopy-->
```


Spécifier les paramètres DNS au niveau du service ou du serveur virtuel à l'aide de l'interface graphique

1. Configurez le profil HTTP.

   Accédez à **Système** > **Profils** > **Profil DNS** et créez le profil DNS.

2. Liez le profil HTTP au service ou au serveur virtuel.

   Accédez à **Gestion du trafic** > **Équilibrage de charge**> **Services/Serveurs virtuels**et créez le profil DNS, qui doit être lié au service ou au serveur virtuel.

Réponse négative limitant le débit servie par l'appliance

Vous pouvez définir un seuil pour les réponses négatives fournies par l'appliance Citrix ADC à partir du cache. Lorsque le seuil est défini, l'appliance sert la réponse depuis le cache jusqu'à ce que le seuil soit atteint. Une fois le seuil atteint, l'appliance supprime les demandes au lieu de répondre avec une réponse NXDOMAIN.

La définition d'une limite de taux pour les réponses négatives présente les avantages suivants.

- Enregistrez les ressources sur l'appliance Citrix ADC.
- Empêchez toute requête malveillante pour les noms de domaine inexistants.

> **Remarque :** Vous pouvez définir un seuil pour les réponses négatives uniquement pour les domaines pour lesquels l'appliance ADC est configurée en tant que serveur de noms de domaine faisant autorité. Vous ne pouvez pas définir de seuil pour les enregistrements mis en cache reçus des serveurs de noms principaux faisant autorité.

Limitation de vitesse réponse négative servie par le cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez

```
set dns parameter -NXDOMainRateLimitThreshold <positive-integer>
<!--NeedCopy-->
```

Exemple :

```
set dns parameter -NXDOMainRateLimitThreshold 1000
<!--NeedCopy-->
```

nxDomainRateLimitThreshold : Lorsque ce paramètre est défini sur une valeur entière positive, les réponses sont fournies à partir du cache jusqu'à ce que ce seuil (en secondes) soit atteint. Une fois le seuil dépassé, les demandes sont supprimées. Le seuil configuré est par moteur de paquets.

Limitation de vitesse réponse négative servie par le cache à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS** et cliquez sur **Modifier les paramètres DNS**.
2. Dans la page **Configurer les paramètres DNS**, dans le champ **Seuil de limite de taux NXDOMAIN**, entrez la valeur de seuil jusqu'à ce que les réponses doivent être fournies à partir du cache.

Remarque : La valeur du **seuil de NXDOMAIN Croisé** affiche le nombre de fois où les demandes sont supprimées une fois le seuil atteint.

Cache les données de sous-réseau client EDNS0 lorsque l'appliance Citrix ADC est en mode proxy

August 20, 2021

En mode Proxy ADC Citrix, si un serveur principal prenant en charge un sous-réseau client EDNS0 (ECS) envoie une réponse contenant l'option ECS, l'appliance Citrix ADC effectue les opérations suivantes :

- Il transmet la réponse telle quelle au client et
- Stocke la réponse dans le cache, ainsi que les informations sur le sous-réseau client.

Les requêtes DNS provenant du même sous-réseau du même domaine, et pour lesquelles le serveur enverrait la même réponse, sont ensuite servies à partir du cache.

Remarque :

- La mise en cache ECS est désactivée par défaut. Activez la mise en cache des données client-sous-réseau EDNS0 dans le profil DNS associé.
- Le nombre de sous-réseaux que vous pouvez mettre en cache pour un domaine est limité aux ID de sous-réseau disponibles, c'est-à-dire 1270 dans l'appliance Citrix ADC. Vous pouvez éventuellement définir la limite à un nombre inférieur (valeur minimale : 1 ipv4/ipv6).

Activer la mise en cache des réponses ECS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

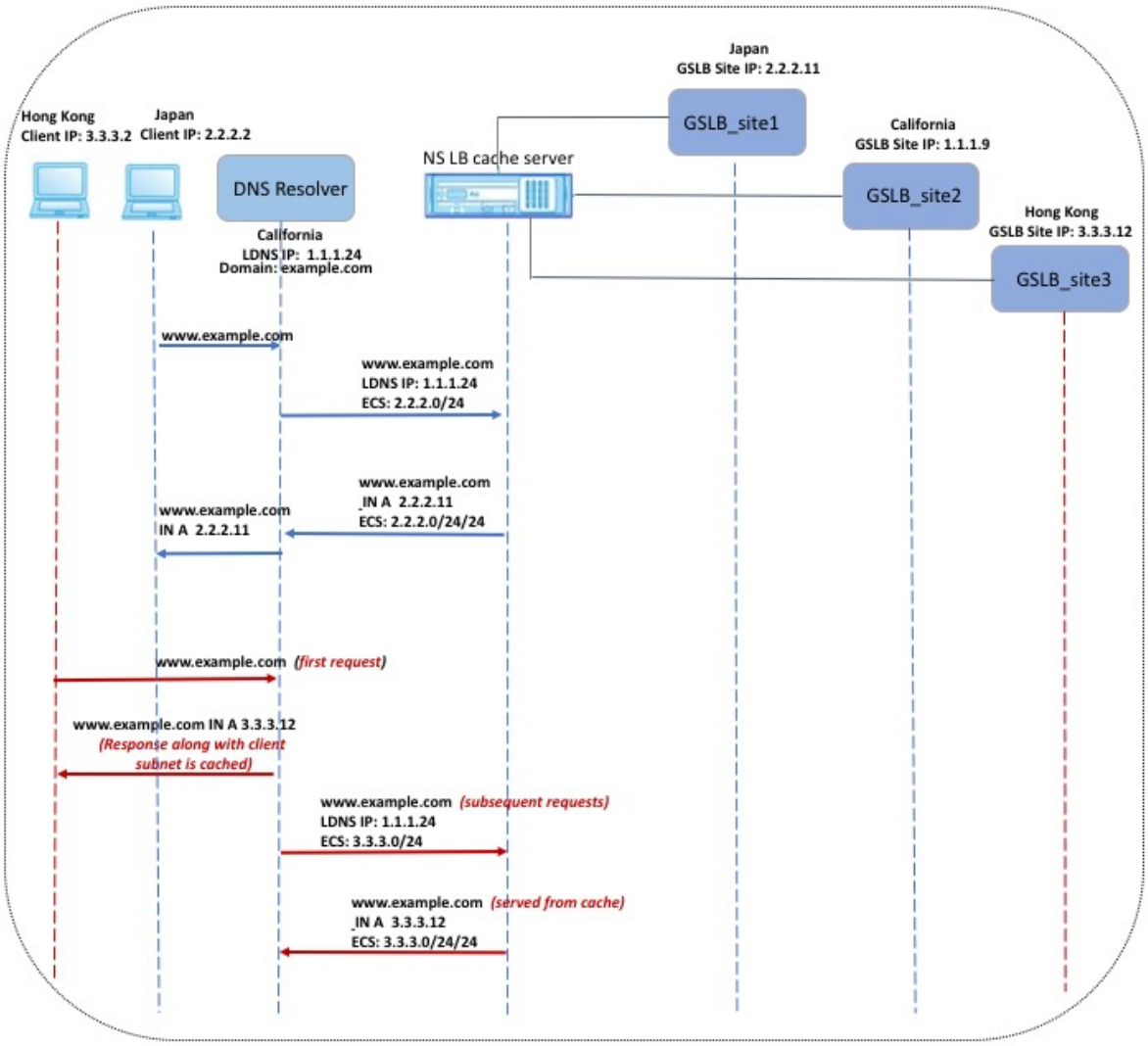
```
set dns profile <dnsProfileName> -cacheECSSubnet ( ENABLED | DISABLED )
```

Limiter le nombre de sous-réseaux pouvant être mis en cache par domaine à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set dns profile <dnsProfileName> -maxSubnetsPerDomain <positive_integer>
```


Exemple :



Dans l'exemple illustré dans la figure précédente, le client à l'adresse IP 2.2.2.2 envoie une requête pour www.example.com au résolveur DNS. Le résolveur DNS envoie la réponse suivante :

www.example.com IN A, IP est 2.2.2.11, et ECS 2.2.2.0/24/24

À ce stade, la réponse et l'identificateur de sous-réseau client-client (2.2.2.0/24) sont mis en cache. D'autres requêtes provenant du même sous-réseau et du même domaine sont servies à partir du cache.

Par exemple, si l'adresse IP du client est 2.2.2.100 et que la requête concerne www.example.com, la requête est servie à partir du cache au lieu d'être envoyée au serveur principal.

Extensions de sécurité du système de noms de domaine

February 12, 2021

DNS Security Extensions (DNSSEC) est une norme IETF (Internet Engineering Task Force). Il vise à fournir l'intégrité des données et l'authentification de l'origine des données dans les communications entre les serveurs de noms et les clients tout en transmettant des réponses UDP en texte clair. DNSSEC spécifie un mécanisme qui utilise la cryptographie à clé asymétrique et un ensemble de nouveaux enregistrements de ressources spécifiques à son implémentation.

La spécification DNSSEC est décrite dans :

- RFC 4033, « Présentation et exigences de sécurité DNS »
- RFC 4034, « Enregistrements de ressources pour les extensions de sécurité DNS »
- RFC 4035, « Modifications du protocole pour les extensions de sécurité DNS »

Les aspects opérationnels de la mise en œuvre du DNSSEC au sein du DNS sont abordés dans la RFC 4641, « DNSSEC Operational Practices ».

Vous pouvez configurer DNSSEC sur Citrix ADC. Vous pouvez générer et importer des clés pour la signature de zones DNS. Vous pouvez configurer DNSSEC pour les zones pour lesquelles Citrix ADC fait autorité. Vous pouvez configurer ADC en tant que serveur proxy DNS pour les zones signées hébergées sur une batterie de serveurs de noms principaux. Si ADC fait autorité pour un sous-ensemble d'enregistrements appartenant à une zone pour laquelle ADC est configuré en tant que serveur proxy DNS, vous pouvez inclure le sous-ensemble d'enregistrements dans l'implémentation DNSSEC.

Configurer DNSSEC

August 20, 2021

Procédez comme suit pour configurer DNSSEC :

1. Activez DNSSEC sur l'appliance Citrix ADC.
2. Créez une clé de signature de zone et une clé de signature de clé pour la zone.
3. Ajoutez les deux clés à la zone.
4. Signez la zone avec les clés.

L'appliance Citrix ADC n'agit pas en tant que résolveur DNSSEC. Le DNSSEC sur ADC est pris en charge uniquement dans les scénarios de déploiement suivants :

1. ADNS : Citrix ADC est l'ADNS et génère les signatures elle-même.

2. Proxy : Citrix ADC agit comme un proxy DNSSEC. Il est supposé que Citrix ADC est placé devant les serveurs ADNS/LDNS en mode approuvé. ADC agit uniquement comme une entité de mise en cache proxy et ne valide aucune signature.

Activer et désactiver DNSSEC

Activez DNSSEC sur Citrix ADC pour que ADC réponde aux clients prenant en charge DNSSEC. Par défaut, DNSSEC est activé.

Vous pouvez désactiver la fonctionnalité DNSSEC si vous ne souhaitez pas que Citrix ADC réponde aux clients avec des informations spécifiques à DNSSEC.

Activer ou désactiver DNSSEC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver DNSSEC et vérifier la configuration :

```
-  set dns parameter -dnssec ( ENABLED | DISABLED )
-  show dns parameter
<!--NeedCopy-->
```

Exemple :

```
> set dns parameter -dnssec ENABLED
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
         .
         .
         .
         DNSEC Extension: ENABLED
        Max DNS Pipeline Requests: 255
 Done

<!--NeedCopy-->
```

Activer ou désactiver DNSSEC à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, cliquez sur Modifier les paramètres DNS.
3. Dans la boîte de dialogue **Configurer les paramètres DNS**, activez ou **désactivez la case à cocher Activer l'extension DNSSEC**.

Créer des clés DNS pour une zone

Pour chaque zone DNS que vous souhaitez signer, vous devez créer deux paires de clés asymétriques. Une paire, appelée la clé de signature de zone (ZSK), est utilisée pour signer tous les jeux d'enregistrements de ressources dans la zone. La deuxième paire est appelée clé de signature de clé (KSK) et est utilisée pour signer uniquement les enregistrements de ressource DNSKEY dans la zone.

Lorsque le ZSK et le KSK sont créés, `suffix.key` est ajouté aux noms des composants publics des clés. Le `suffix.private` est ajouté aux noms de leurs composants privés. L'ajout se produit automatiquement.

Citrix ADC crée également un enregistrement DS (Délégation Signer) et ajoute le suffixe .ds au nom de l'enregistrement. Si la zone parent est une zone signée, vous devez publier l'enregistrement DS dans la zone parent pour établir la chaîne d'approbation.

Lorsque vous créez une clé, la clé est stockée dans le `/nsconfig/dns/` répertoire, mais elle n'est pas publiée automatiquement dans la zone. Après avoir créé une clé à l'aide de la `create dns key` commande, vous devez publier explicitement la clé dans la zone à l'aide de la `add dns key` commande. Le processus de génération d'une clé est distinct du processus de publication de la clé dans une zone pour vous permettre d'utiliser d'autres moyens pour générer des clés. Par exemple, vous pouvez importer des clés générées par d'autres programmes de génération de clés (tels que `bind -keygen`) à l'aide de Secure FTP (SFTP), puis publier les clés dans la zone. Pour plus d'informations sur la publication d'une clé dans une zone, voir Publier une clé DNS dans une zone.

Effectuez les étapes décrites dans cette rubrique pour créer une clé de signature de zone, puis répétez les étapes pour créer une clé de signature de clé. L'exemple suivant la syntaxe de commande crée d'abord une paire de clés de signature de zone pour la zone exemple.com. L'exemple utilise ensuite la commande pour créer une paire de clés de signature de clé pour la zone.

À partir de la version 13.0 build 61.x, l'appliance Citrix ADC prend désormais en charge des algorithmes de chiffrement plus puissants, tels que RSASHA256 et RSASHA512, pour authentifier une zone DNS. Auparavant, seul l'algorithme RSASHA1 était pris en charge.

Créer une clé DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
create dns key -zoneName <string> -keyType <keyType> -algorithm <algorithm>
 -keySize <positive_integer> -fileNamePrefix <string>
```

Exemple :

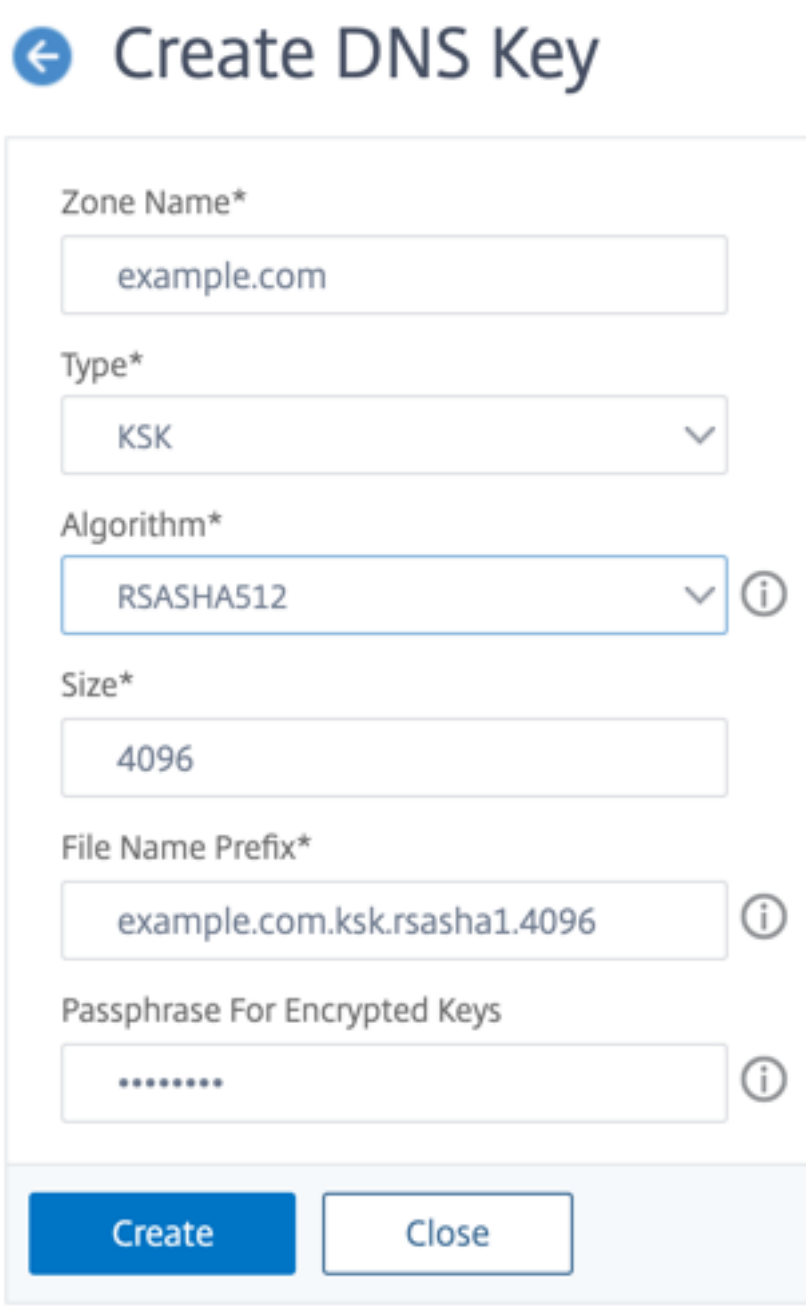
```
1 > create dns key -zoneName example.com -keyType zsk -algorithm
      RSASHA256 -keySize 1024 -fileNamePrefix example.com.zsk.rsasha1.1024
```



```
2 File Name: /nsconfig/dns/example.com.zsk.rsasha1.1024.key (public); /
     nsconfig/dns/example.com.zsk.rsasha1.1024.private (private); /
     nsconfig/dns/example.com.zsk.rsasha1.1024.ds (ds)
3 This operation may take some time, Please wait...
4  Done
5 > create dns key -zoneName example.com -keyType ksk -algorithm
     RSASHA512 -keySize 4096 -fileNamePrefix example.com.ksk.rsasha1.4096
6 File Name: /nsconfig/dns/example.com.ksk.rsasha1.4096.key (public); /
     nsconfig/dns/example.com.ksk.rsasha1.4096.private (private); /
     nsconfig/dns/example.com.ksk.rsasha1.4096.ds (ds)
7 This operation may take some time, Please wait...
8  Done
9 <!--NeedCopy-->
```

Créer une clé DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans la zone Détails, cliquez sur **Créer une clé DNS**.
3. Entrez des valeurs pour les différents paramètres et cliquez sur **Créer**.



Remarque : Pour modifier le préfixe de nom de fichier d'une clé existante :

- Cliquez sur la flèche en regard du bouton **Parcourir**.
- Cliquez sur **Local** ou **Appliance** (selon que la clé existante est stockée sur votre ordinateur local ou dans le `/nsconfig/dns/` répertoire de l'appliance)
- Accédez à l'emplacement de la clé, puis double-cliquez sur la clé.
  La zone **Préfixe du nom de fichier** est renseignée uniquement avec le préfixe de la clé existante. Modifiez le préfixe en conséquence.

Publier une clé DNS dans une zone

Une clé (clé de signature de zone ou clé de signature de clé) est publiée dans une zone en ajoutant la clé à l'appliance ADC. Une clé doit être publiée dans une zone avant de signer la zone.

Avant de publier une clé dans une zone, la clé doit être disponible dans le répertoire **/nsconfig/dns/**. Si vous avez créé la clé DNS sur un autre ordinateur (par exemple, à l'aide `bind-keygen` du programme), assurez-vous que la clé est ajoutée au `/nsconfig/dns/` répertoire. Ensuite, publiez la clé dans la zone. Utilisez l'interface graphique ADC pour ajouter la clé au `/nsconfig/dns/` répertoire. Ou bien, utilisez un autre programme pour importer la clé dans le répertoire, tel que Secure FTP (SFTP).

Utilisez la `add dns key` commande pour chaque paire de clés public-privé que vous souhaitez publier dans une zone donnée. Si vous avez créé une paire ZSK et une paire KSK pour une zone, utilisez la `add dns key` commande pour publier d'abord l'une des paires de clés dans la zone. Répétez la commande pour publier l'autre paire de clés. Pour chaque clé que vous publiez dans une zone, un enregistrement de ressource DNSKEY est créé dans la zone.

L'exemple suivant la syntaxe de commande publie d'abord la paire de clés de signature de zone (créée pour la zone example.com) dans la zone. L'exemple utilise ensuite la commande pour publier la paire de clés de signature de clé dans la zone.

Publier une clé dans une zone à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour publier une clé dans une zone et vérifier la configuration :

```
1 -  add dns key <keyName> <publickey> <privatekey> [-expires <
    positive_integer> [<units>]] [-notificationPeriod <positive_integer>
     [<units>]] [-TTL <secs>]
2 -  show dns zone [<zoneName> | -type <type>]
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns key example.com.zsk example.com.zsk.rsasha1.1024.key example.
    com.zsk.rsasha1.1024.private
2  Done
3 > add dns key example.com.ksk example.com.ksk.rsasha1.4096.key example.
    com.ksk.rsasha1.4096.private
4  Done
5 > show dns zone example.com
6          Zone Name : example.com
7          Proxy Mode : NO
8          Domain Name : example.com
9                  Record Types : NS SOA DNSKEY
```



```
10          Domain Name : ns1.example.com
11                  Record Types : A
12          Domain Name : ns2.example.com
13                  Record Types : A
14  Done
15 <!--NeedCopy-->
```

Publier une clé dans une zone DNS à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Clés**.

Remarque : Pour Clé publique et Private Key, pour ajouter une clé stockée sur votre ordinateur local, cliquez sur la flèche en regard du bouton **Parcourir**, cliquez sur **Local**, accédez à l'emplacement de la clé, puis double-cliquez sur la clé.

Configurer une clé DNS

Vous pouvez configurer les paramètres d'une clé publiée dans une zone. Vous pouvez modifier la période d'expiration, la période de notification et les paramètres de durée de vie (TTL) de la clé. Si vous modifiez la période d'expiration d'une clé, l'appliance resigne automatiquement tous les enregistrements de ressource de la zone à l'aide de la clé. La resignature se produit si la zone est signée avec la clé particulière.

Configurer une clé à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour configurer une clé et vérifier la configuration :

```
1 -  set dns key <keyName> [-expires <positive_integer> [<units>]] [-
     notificationPeriod <positive_integer> [<units>]] [-TTL <secs>]
2 -  show dns key [<keyName>]
3 <!--NeedCopy-->
```

Exemple :

```
1 > set dns key example.com.ksk -expires 30 DAYS -notificationPeriod 3
     DAYS -TTL 3600
2  Done
3 > show dns key example.com.ksk
4 1)      Key Name: example.com.ksk
5         Expires: 30 DAYS        Notification: 3 DAYS    TTL: 3600
6         Public Key File: example.com.ksk.rsasha1.4096.key
7         Private Key File: example.com.ksk.rsasha1.4096.private
```



```
8   Done
9 <!--NeedCopy-->
```

Configurer une clé à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Clés**.
2. Dans le volet d'informations, cliquez sur la clé à configurer, puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer la clé DNS, modifiez les valeurs des paramètres suivants comme indiqué :
   - Expiration : Expire
   - Période de notification — notificationPeriod
   - TTL—TTL
4. Cliquez sur OK.

Signer et supprimer la signature d'une zone DNS

Pour sécuriser une zone DNS, vous devez signer la zone avec les clés qui ont été publiées dans la zone. Lorsque vous signez une zone, Citrix ADC crée un enregistrement de ressource NSEC (Next Secure) pour chaque nom de propriétaire. Ensuite, il utilise la clé de signature de clé pour signer le jeu d'enregistrements de ressources DNSKEY. Enfin, il utilise le ZSK pour signer tous les jeux d'enregistrements de ressources de la zone, y compris les jeux d'enregistrements de ressources DNSKEY et les jeux d'enregistrements de ressources NSEC. Chaque opération de signe génère une signature pour les jeux d'enregistrements de ressources dans la zone. La signature est capturée dans un nouvel enregistrement de ressource appelé enregistrement de ressource RRSIG.

Après avoir signé une zone, enregistrez la configuration.

Signer une zone à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour signer une zone et vérifier la configuration :

```
1 -  sign dns zone <zoneName> [-keyName <string> ...]
2 -  show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]
3 -  save config
4 <!--NeedCopy-->
```

Exemple :


```
> sign dns zone example.com -keyName example.com.zsk example.com.ksk
 Done
> show dns zone example.com
         Zone Name : example.com
         Proxy Mode : NO
         Domain Name : example.com
                 Record Types : NS SOA DNSKEY RRSIG NSEC
         Domain Name : ns1.example.com
                 Record Types : A RRSIG NSEC
         Domain Name : ns2.example.com
                 Record Types : A RRSIG
         Domain Name : ns2.example.com
                 Record Types : RRSIG NSEC
Done
> save config
 Done
<!--NeedCopy-->
```

Désigner une zone à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour désigner une zone et vérifier la configuration :

```
-  unsign dns zone <zoneName> [-keyName <string> ...]
-  show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]
<!--NeedCopy-->
```

Exemple :

```
> unsign dns zone example.com -keyName example.com.zsk example.com.ksk
 Done
> show dns zone example.com
         Zone Name : example.com
         Proxy Mode : NO
         Domain Name : example.com
                 Record Types : NS SOA DNSKEY
         Domain Name : ns1.example.com
                 Record Types : A
         Domain Name : ns2.example.com
                 Record Types : A
 Done
<!--NeedCopy-->
```


Signer ou désigner une zone à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Zones**.
2. Dans le volet d'informations, cliquez sur la zone à signer, puis cliquez sur Signer/Désigner.
3. Dans la boîte de dialogue Sign/Désigner la zone DNS, effectuez l'une des opérations suivantes :
   - Pour signer la zone, activez les cases à cocher des clés (clé de signature de zone et clé de signature de clé) avec lesquelles vous souhaitez signer la zone.
     Vous pouvez signer la zone avec plus d'une clé de signature de zone ou une paire de clés de signature de clé.
   - Pour déconnecter la zone, désactivez les cases à cocher des clés (clé de signature de zone et clé de signature de clé) avec lesquelles vous souhaitez déconnecter la zone.
     Vous pouvez déconnecter la zone avec plus d'une clé de signature de zone ou une paire de clés de signature de clé.
4. Cliquez sur OK.

Afficher les enregistrements NSEC d'un enregistrement donné dans une zone

Vous pouvez afficher les enregistrements NSEC créés automatiquement par Citrix ADC pour chaque nom de propriétaire dans la zone.

Afficher l'enregistrement NSEC d'un enregistrement donné dans une zone à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour afficher l'enregistrement NSEC d'un enregistrement donné dans une zone :

```
show dns nsecRec [<hostName> | -type (ADNS | PROXY | ALL)]
```

Exemple :

```
1 > show dns nsecRec example.com
2 1)      Domain Name : example.com
3         Next Nsec Name: ns1.example.com
4         Record Types : NS SOA DNSKEY RRSIG NSEC
5  Done
6 <!--NeedCopy-->
```

Afficher l'enregistrement NSEC pour un enregistrement donné dans une zone à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements sécurisés suivants**.

2. Dans le volet d'informations, cliquez sur le nom de l'enregistrement pour lequel vous souhaitez afficher l'enregistrement NSEC. L'enregistrement NSEC de l'enregistrement sélectionné s'affiche dans la zone Détails.

Supprimer une clé DNS

Supprimez une clé de la zone dans laquelle elle est publiée lorsque la clé a expiré ou si la clé a été compromise. Lorsque vous supprimez une clé de la zone, celle-ci est automatiquement désignée avec la clé. La suppression de la clé avec cette commande ne supprime pas les fichiers clés présents dans le répertoire /nsconfig/dns/. Si les fichiers clés ne sont plus nécessaires, ils doivent être explicitement supprimés du répertoire.

Supprimer une clé de Citrix ADC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour supprimer une clé et vérifier la configuration :

```
1 -  rm dns key <keyName>
2 -  show dns key <keyName>
3 <!--NeedCopy-->
```

Exemple :

```
1 > rm dns key example.com.zsk
2  Done
3 > show dns key example.com.zsk
4 ERROR: No such resource [keyName, example.com.zsk]
5
6 <!--NeedCopy-->
```

Supprimer une clé de Citrix ADC à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Clés**.
2. Dans le volet d'informations, cliquez sur le nom de la clé que vous souhaitez supprimer de ADC, puis cliquez sur Supprimer.

Configurer DNSSEC lorsque Citrix ADC fait autorité pour une zone

August 20, 2021

Lorsque le Citrix ADC fait autorité pour une zone donnée, tous les enregistrements de ressources de la zone sont configurés sur ADC. Pour signer la zone faisant autorité, vous devez créer la signature de zone et les clés de signature de la zone, ajouter les clés à ADC, puis signer la zone. Pour plus d'informations, consultez :

- Créer des clés DNS pour une zone
- Publier une clé DNS dans une zone
- Signez et désignez une zone DNS.

Si des domaines GSLB configurés sur ADC appartiennent à la zone en cours de signature, les noms de domaine GSLB sont signés avec les autres enregistrements qui appartiennent à la zone.

Après avoir signé une zone, les réponses aux demandes des clients prenant en charge DNSSEC incluent les enregistrements de ressources RRSIG ainsi que les enregistrements de ressources demandés. Le DNSSEC doit être activé sur ADC. Pour plus d'informations sur l'activation de DNSSEC, voir Activer et désactiver DNSSEC.

Enfin, après avoir configuré DNSSEC pour la zone faisant autorité, vous devez enregistrer la configuration de Citrix ADC.

Configurer DNSSEC pour une zone pour laquelle Citrix ADC est un serveur proxy DNS

August 20, 2021

La procédure de signature d'une zone pour laquelle Citrix ADC est configuré en tant que serveur proxy DNS dépend du propriétaire d'un sous-ensemble des informations de zone appartenant aux serveurs de noms principaux. Si c'est le cas, la configuration est considérée comme une configuration de propriété partielle de zone. Si ADC ne possède pas de sous-ensemble des informations de zone, la configuration Citrix ADC pour la gestion des serveurs principaux est considérée comme une configuration de serveur proxy DNS sans zone. Les tâches de configuration DNSSEC de base pour les deux configurations Citrix ADC sont les mêmes. Toutefois, la signature de la zone partielle sur Citrix ADC nécessite quelques étapes de configuration supplémentaires.

Remarque : Les termes Configuration du serveur proxy sans zone et zone partielle sont utilisés uniquement dans le contexte de l'appliance Citrix ADC.

Important : lorsqu'il est configuré en mode proxy, ADC n'effectue pas de vérification de signature sur les réponses DNSSEC avant de mettre à jour le cache.

Si vous configurez ADC en tant que proxy DNS pour équilibrer la charge des résolveurs (serveurs) compatibles DNSSEC, vous devez définir l'option Récursion disponible lors de la configuration du serveur

virtuel DNS. Si une requête DNSSEC arrive avec le bit Checking Disabled (CD) défini, la requête est transmise au serveur avec le bit CD conservé. La réponse du serveur n'est pas mise en cache.

Configurer DNSSEC pour une configuration de serveur proxy DNS sans zone

Pour une configuration de serveur proxy DNS sans zone, la signature de zone doit être effectuée sur les serveurs de noms principaux. Sur Citrix ADC, vous configurez ADC en tant que serveur proxy DNS pour la zone. Créez un serveur virtuel d'équilibrage de charge de type de protocole DNS. Configurez les services sur ADC pour représenter les serveurs de noms. Ensuite, liez les services au serveur virtuel d'équilibrage de charge. Pour plus d'informations sur ces tâches de configuration, voir Configurer NetScaler en tant que serveur proxy DNS.

Lorsqu'un client envoie à ADC une demande DNS avec le bit OK (DO) DNSSEC défini, ADC vérifie son cache pour les informations demandées. Si les enregistrements de ressource ne sont pas disponibles dans son cache, ADC transmet la requête à l'un des serveurs de noms DNS. Ensuite, il relaie la réponse du serveur de noms au client. En outre, ADC met en cache les enregistrements de ressources RRSIG ainsi que la réponse du serveur de noms. Les demandes ultérieures des clients prenant en charge DNSSEC sont traitées à partir du cache (y compris les enregistrements de ressources RRSIG), sous réserve du paramètre Time-to-Live (TTL). Si un client envoie une requête DNS sans définir le bit DO, ADC répond uniquement avec les enregistrements de ressources demandés. Il n'inclut pas les enregistrements de ressources RRSIG spécifiques à DNSSEC.

Configurer DNSSEC pour une configuration de propriété de zone partielle

Dans certaines configurations ADC, même si l'autorité d'une zone appartient aux serveurs de noms principaux, un sous-ensemble des enregistrements de ressources appartenant à la zone peut être configuré sur ADC. ADC ne possède (ou fait autorité pour) que ce sous-ensemble d'enregistrements. Un tel sous-ensemble d'enregistrements peut être considéré comme une *zone partielle* sur ADC. ADC possède la zone partielle. Tous les autres enregistrements appartiennent aux serveurs de noms principaux.

Une configuration de zone partielle typique sur Citrix ADC est visible lorsque :

- Les domaines Global Server Load Balancing (GSLB) sont configurés sur ADC
- Les domaines GSLB font partie d'une zone pour laquelle les serveurs de noms principaux font autorité.

La signature d'une zone qui ne comprend qu'une zone partielle sur ADC implique :

- Inclusion des informations de zone partielles dans les fichiers de zone du serveur de noms backend
- Signature de la zone sur les serveurs de noms principaux
- Signature de la zone partielle sur ADC.

Le même jeu de clés doit être utilisé pour signer la zone sur les serveurs de noms et la zone partielle sur ADC.

Signer la zone sur les serveurs de noms principaux

1. Incluez les enregistrements de ressources contenus dans la zone partielle, dans les fichiers de zone des serveurs de noms.
2. Créez des clés et utilisez les clés pour signer la zone sur les serveurs de noms back-end.

Signer la zone partielle sur le Citrix ADC

1. Créez une zone avec le nom de la zone détenue par les serveurs de noms principaux. Lors de la configuration de la zone partielle, définissez le paramètre ProxyMode sur YES. Cette zone est la zone partielle qui contient les enregistrements de ressources appartenant à ADC.

   Par exemple, si le nom de la zone configurée sur les serveurs de noms principaux est example.com, vous devez créer une zone nommée example.com sur ADC. Définissez le paramètre ProxyMode sur YES. Pour plus d'informations sur l'ajout d'une zone, voir Configurer une zone DNS.

   > **Remarque**
   >
   > N'ajoutez pas d'enregistrements SOA et NS pour la zone. Ces enregistrements doivent exister sur ADC pour une zone pour laquelle ADC fait autorité.

2. Importez les clés (depuis l'un des serveurs de noms dorsaux) vers ADC, puis ajoutez-les au répertoire /nsconfig/dns/. Pour plus d'informations sur la façon dont vous pouvez importer une clé et l'ajouter à ADC, consultez Publier une clé DNS dans une zone.
3. Signez la zone partielle avec les clés importées. Lorsque vous signez la zone partielle avec les clés, ADC génère des enregistrements RRSIG et NSEC pour les jeux d'enregistrements de ressources et les enregistrements de ressources individuels dans la zone partielle, respectivement. Pour plus d'informations sur la signature d'une zone, voir Signer et désigner une zone DNS.

Configurer DNSSEC pour les noms de domaine GSLB (Global Server Load Balancing)

August 20, 2021

Si GSLB est configuré sur Citrix ADC et que ADC fait autorité pour la zone à laquelle appartiennent les noms de domaine GSLB, tous les noms de domaine GLSB sont signés lorsque la zone est signée.

Pour plus d'informations sur la signature d'une zone pour laquelle ADC fait autorité, voir Configurer DNSSEC lorsque l'appliance Citrix ADC fait autorité pour une zone.

Si les domaines GSLB appartiennent à une zone pour laquelle les serveurs de noms principaux font autorité, vous devez :

- Signez d'abord la zone sur les serveurs de noms.
- Signez ensuite la zone partielle sur ADC pour terminer la configuration DNSSEC de la zone.

Pour plus d'informations, voir Configurer DNSSEC pour une configuration de propriété de zone partielle.

Entretien de la zone

August 20, 2021

Du point de vue DNSSEC, la maintenance de zone implique le roulement des clés de signature de zone et des clés de signature de clé lorsque l'expiration de la clé est imminente. Ces tâches de maintenance de zone doivent être effectuées manuellement. La zone est résignée automatiquement et ne nécessite aucune intervention manuelle.

Signer à nouveau une zone mise à jour

Lorsqu'une zone est mise à jour (ajouter un enregistrement ou modifier un enregistrement existant), l'appliance signe automatiquement le nouvel enregistrement (ou modifié). Si une zone contient plusieurs clés de signature de zone, l'appliance signe de nouveau le nouvel enregistrement (ou modifié) avec la clé utilisée pour signer la zone.

Repasser les clés DNSSEC

Remarque : Revalez manuellement les clés DNSSEC (KSK, ZSK) avant leur expiration.

Sur Citrix ADC, vous pouvez utiliser les méthodes de pré-publication et de double signature pour effectuer un survol de la clé de signature de zone et de la clé de signature de clé. Plus d'informations sur ces deux méthodes de survol sont disponibles dans la RFC 4641, « DNSSEC Operational Practices ».

Les rubriques suivantes mappent les commandes de ADC aux étapes des procédures de survol décrites dans la RFC 4641.

La notification d'expiration de la clé est envoyée via une interruption SNMP appelée DNSKeyExpiration. Trois variables MIB, DNSKeyName, DNSKeyTimeToExpiration et DNSKeyUnitsofExpiration sont envoyées avec l'interruption SNMP DNSKeyExpiration. Pour plus d'informations, consultez *Citrix NetScaler SNMP OID Reference* at NetScaler 12.0 SNMP OID Reference.

Prépublication du survol des clés

La RFC 4641, « DNSSEC Operational Practices » définit quatre étapes pour la méthode de basculement de clé de publication : initiale, nouvelle DNSKEY, nouvelle méthode RRSIG et suppression de DNSKEY. Chaque étape est associée à un ensemble de tâches que vous devez effectuer sur ADC. Voici les descriptions de chaque étape et les tâches que vous devez effectuer. La procédure de substitution décrite ici peut être utilisée à la fois pour les clés de signature de clé et les clés de signature de zone.

- **Étape 1 : Initiale.** La zone contient uniquement les jeux de clés avec lesquels la zone a été actuellement signée. L'état de la zone dans la phase initiale correspond à l'état de la zone juste avant de commencer le processus de retournement des clés.

  Exemple :

  Considérez la clé, example.com.zsk1, avec laquelle la zone example.com est signée. La zone contient uniquement les RRSIG générés par la clé example.com.zsk1, qui doit être expirée. La clé de signature de clé est example.com.ksk1.

- **Étape 2 : Nouveau DNSKEY.** Une nouvelle clé est créée et publiée dans la zone. C'est-à-dire que la clé est ajoutée à ADC, mais la zone n'est pas signée avec la nouvelle clé tant que la phase de pré-roulement n'est pas terminée. Dans ce stade, la zone contient l'ancienne clé, la nouvelle clé et les RRSIG générés par l'ancienne clé. La publication de la nouvelle clé pour la durée complète de la phase pré-roll donne l'enregistrement de ressource DNSKEY correspondant à la nouvelle heure de la clé à propager vers les serveurs de noms secondaires.

  Exemple :

  Une nouvelle clé example.com.zsk2 est ajoutée à la zone example.com. La zone n'est pas signée avec example.com.zsk2 tant que la phase de pré-roll n'est pas terminée. La zone example.com contient des enregistrements de ressources DNSKEY pour example.com.zsk1 et example.com.zsk2.

  Commandes Citrix ADC :

  Effectuez les tâches suivantes sur ADC :

  - Créez une clé DNS à l'aide de la commande `create dns key`.

    Pour plus d'informations sur la création d'une clé DNS, y compris un exemple, voir Créer des clés DNS pour une zone.

  - Publiez la nouvelle clé DNS dans la zone à l'aide de la commande `add dns key`.

    Pour plus d'informations sur la publication de la clé dans la zone, y compris un exemple, voir Publier une clé DNS dans une zone.

- **Étape 3 : Nouveaux RRSIG.** La zone est signée avec la nouvelle clé DNS, puis non signée avec l'ancienne clé DNS. L'ancienne clé DNS n'est pas supprimée de la zone et reste publiée jusqu'à ce que les RRSIG générés par l'ancienne clé expirent.

Exemple :

La zone est signée avec example.com.zsk2, puis non signée avec example.com.zsk1. La zone continue de publier example.com.zsk1 jusqu'à ce que les RRSIG générés par example.com.zsk1 expirent.

Commandes Citrix ADC :

Effectuez les tâches suivantes sur ADC :

- Signez la zone avec la nouvelle clé DNS à l'aide de la commande `sign dns zone`.
- Déconnectez la zone avec l'ancienne clé DNS à l'aide de la commande `unsign dns zone`.

Pour plus d'informations sur la signature et la désignature d'une zone, y compris des exemples, voir Signer et désigner une zone DNS.

- **Étape 4 : Suppression de DNSKEY.** Lorsque les RRSIG générés par l'ancienne clé DNS expirent, l'ancienne clé DNS est supprimée de la zone.

  Exemple :

  L'ancienne clé DNS example.com.zsk1 est supprimée de la zone example.com.

  Commandes Citrix ADC

  Sur ADC, vous supprimez l'ancienne clé DNS à l'aide de la commande `rm dns key`. Pour plus d'informations sur la suppression d'une clé d'une zone, y compris un exemple, voir Supprimer une clé DNS.

Clé-clé à double signature

La RFC 4641, « DNSSEC Operational Practices » définit trois étapes pour le renversement de clés à double signature : initiale, nouvelle DNSKEY et suppression de DNSKEY. Chaque étape est associée à un ensemble de tâches que vous devez effectuer sur ADC. Voici les descriptions de chaque étape et les tâches que vous devez effectuer. La procédure de substitution décrite ici peut être utilisée à la fois pour les clés de signature de clé et les clés de signature de zone.

- **Étape 1 : Initiale.** La zone contient uniquement les jeux de clés avec lesquels la zone a été actuellement signée. L'état de la zone dans la phase initiale correspond à l'état de la zone juste avant de commencer le processus de retournement des clés.

  Exemple :

  Considérez la clé, example.com.zsk1, avec laquelle la zone example.com est signée. La zone contient uniquement les RRSIG générés par la clé example.com.zsk1, qui doit être expirée. La clé de signature de clé est example.com.ksk1.

- **Étape 2 : Nouveau DNSKEY.** La nouvelle clé est publiée dans la zone et la zone est signée avec la nouvelle clé. La zone contient les RRSIG générés par l'ancienne et la nouvelle clé. La durée

minimale pour laquelle la zone doit contenir les deux ensembles de RRSIG est la durée requise pour que tous les RRSIG expirent.

Exemple :

Une nouvelle clé example.com.zsk2 est ajoutée à la zone example.com. La zone est signée avec example.com.zsk2. La zone example.com contient désormais les RRSIG générés à partir des deux clés.

Commandes Citrix ADC

Effectuez les tâches suivantes sur ADC :

- Créez une clé DNS à l'aide de la commande `create dns key`.

  Pour plus d'informations sur la création d'une clé DNS, y compris un exemple, voir Créer des clés DNS pour une zone.

- Publiez la nouvelle clé dans la zone à l'aide de la commande `add dns key`.

  Pour plus d'informations sur la publication de la clé dans la zone, y compris un exemple, voir Publier une clé DNS dans une zone.

- Signez la zone avec la nouvelle clé à l'aide de la commande `sign dns zone`.

  Pour plus d'informations sur la signature d'une zone, y compris des exemples, voir Signer et désigner une zone DNS.

- **Étape 3 : Suppression de DNSKEY.** Lorsque les RRSIG générés par l'ancienne clé DNS expirent, l'ancienne clé DNS est supprimée de la zone.

  Exemple :

  L'ancienne clé DNS example.com.zsk1 est supprimée de la zone example.com.

  Commandes Citrix ADC :

  Sur ADC, vous supprimez l'ancienne clé DNS à l'aide de la commande `rm dns key`.

  Pour plus d'informations sur la suppression d'une clé d'une zone, y compris un exemple, voir Supprimer une clé DNS.

Décharger les opérations DNSSEC sur Citrix ADC

August 20, 2021

Pour les zones DNS pour lesquelles vos serveurs DNS font autorité, les opérations DNSSEC peuvent être déchargées vers l'appliance ADC. Dans un déploiement de déchargement DNSSEC, un serveur DNS envoie des réponses non signées. ADC signe la réponse dynamiquement avant de la relayer au

client. ADC met également en cache la réponse signée. Outre la réduction de la charge sur les serveurs DNS, le déchargement des opérations DNSSEC vers ADC offre les avantages suivants :

- Vous pouvez signer des enregistrements générés par les serveurs DNS par programme. Ces enregistrements ne peuvent pas être signés par des opérations de signature de zone de routine effectuées sur les serveurs DNS.
- Vous pouvez fournir des réponses signées aux clients même si vous n'avez pas implémenté DNSSEC sur vos serveurs.

Pour configurer le déchargement DNSSEC, vous devez configurer un serveur virtuel d'équilibrage de charge DNS, configurer les services qui représentent les serveurs DNS, puis lier les services au serveur virtuel. Pour plus d'informations sur la configuration d'un serveur virtuel d'équilibrage de charge DNS, la configuration des services et la liaison des services au serveur virtuel, voir Configurer une zone DNS.

Créez une entité de zone sur ADC pour chaque zone DNS dont vous souhaitez décharger les opérations DNSSEC. Pour chaque zone DNS, vous devez activer les paramètres Mode proxy et Déchargement DNSSEC. Vous pouvez éventuellement configurer la génération d'enregistrements NSEC pour une zone déchargée. Pour créer une entité de zone DNS pour le déchargement DNSSEC, suivez les instructions de cette rubrique.

Pour terminer la configuration, vous devez générer des clés DNS pour la zone, ajouter les clés à la zone, puis signer la zone avec les clés. Ce processus est le même que pour le DNSSEC normal. Pour plus d'informations sur la création de clés, l'ajout de clés à une zone et la signature de la zone, voir Extensions de sécurité du système de noms de domaine.

Après avoir configuré le déchargement DNS, vous devez vider le cache DNS sur Citrix ADC. Le vidage du cache DNS garantit que tous les enregistrements non signés dans le cache sont supprimés puis remplacés par des enregistrements signés. Pour plus d'informations sur le vidage du cache DNS, voir Vider les enregistrements DNS.

Activer le déchargement DNSSEC pour une zone à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour activer le déchargement DNSSEC pour une zone et vérifier la configuration :

```
1 -  add dns zone <zoneName> -proxyMode YES -dnssecOffload ENABLED [-nsec
       ( ENABLED | DISABLED )
2 -  show dns zone
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns zone example.com -proxyMode YES -dnssecOffload ENABLED nsec
     ENABLED
```



```
 Done
> show dns zone example.com
      Zone Name : example.com
      Proxy Mode : YES
      DNSSEC Offload: ENABLED    NSEC: ENABLED
 Done
<!--NeedCopy-->
```

Activer le déchargement DNSSEC pour une zone à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Zones**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une zone sur Citrix ADC, cliquez sur Ajouter.
   - Pour configurer le déchargement DNSSEC d'une zone existante, double-cliquez sur la zone.
3. Dans la boîte de dialogue Créer une zone DNS ou Configurer une zone DNS, activez les cases à cocher Mode proxy et Déchargement DNSSEC.
4. Si vous souhaitez que Citrix ADC génère des enregistrements NSEC pour la zone, activez la case à cocher NSEC.

Prise en charge des partitions d'administration pour DNSSEC

August 20, 2021

Dans une appliance Citrix ADC partitionnée, les clés DNS générées sont stockées aux emplacements suivants :

- Partition par défaut : /nsconfig/dns/
- Partition non par défaut : /nsconfig/partitions/ <partitionname> /dns/

Vous pouvez maintenant ajouter un mot de passe à la clé DNS. Pour ajouter un mot de passe à la clé DNS, vous devez d'abord ajouter le mot de passe dans la `create dns key` commande. Indiquez ensuite le même mot de passe dans la `add dns key` commande lors de l'ajout de la clé DNS à l'appliance ADC. Par exemple :

```
create dns key -zoneName com -keytype ksK -algorithm rsASHA1 -keysize 4096
- fileNamePrefix com.ksk.rsasha1.4096 -password 1jsfd3Wa
```

```
add dns key com.zsk.4096 /nsconfig/dns/com.zsk.rsasha1.4096.private -
password 1jsfd3Wa
```

Remarque :

- Pour un environnement partitionné par défaut, les clés sont lues à partir de l'emplacement par défaut/nsconfig/dns/. Toutefois, si les clés sont stockées dans un emplacement différent, le nom du chemin d'accès doit être fourni dans la `add dns key -private` commande. Par exemple, `add dns key -private <path name>`.
- Pour un environnement partitionné autre que par défaut, les clés sont lues à partir de l'emplacement par défaut `/nsconfig/partitions/<partitionname>/dns/`.

Prise en charge des domaines DNS génériques

January 21, 2021

Les domaines DNS génériques sont utilisés pour traiter les demandes de domaines et sous-domaines inexistants. Dans une zone, utilisez des domaines génériques pour rediriger les requêtes de tous les domaines ou sous-domaines inexistants vers un serveur particulier, au lieu de créer un enregistrement de ressources (RR) distinct pour chaque domaine. L'utilisation la plus courante d'un domaine DNS générique est de créer une zone qui peut être utilisée pour transférer le courrier d'Internet vers un autre système de messagerie.

Dans la résolution DNS, les RR génériques prennent en charge le domaine générique. Les RR génériques sont utilisés pour synthétiser les réponses aux requêtes pour un nom de domaine inexistant. Par exemple, si vous avez interrogé `http://image.example.com`et que le sous-domaine « image » n'existait pas, vous pouvez être redirigé vers exemple.com.

Un enregistrement générique comporte un astérisque (*) comme étiquette la plus à gauche d'un nom de domaine. Par exemple, `*.example.com`. Un astérisque à n'importe quel autre endroit du nom de domaine signifie un enregistrement DNS générique. Par exemple, n' `new.*.example.com` est pas un enregistrement DNS générique valide.

> **Remarque**
>
> - Le domaine générique n'est pris en charge que lorsque l'appliance Citrix ADC fait autorité pour la zone et est configurée en tant que serveur proxy ADNS ou DNS.
> - Le domaine générique n'est pas pris en charge pour les enregistrements NS et SOA.
> - Le domaine générique ne peut pas être appliqué lorsque la requête se trouve dans une autre zone.
> - Le domaine générique ne peut pas être appliqué lorsque le QNAME ou un nom entre le domaine générique et le QNAME est connu pour exister.

Exemple de configuration


```
add dns soaRec example.com -originServer n1.example.com -contact admin.
    example.com

add dns nsRec example.com n1.example.com

add dns nsRec example.com n2.example.com

add dns zone example.com  -proxyMode no

add dns addrec www.example.com 2.2.2.2

add dns addrec *.example.com 10.10.10.10

add dns addrec *.example.com 10.10.10.11

add dns aaaarec *.example.com 2001::1
<!--NeedCopy-->
```

Dans l'exemple, un nom de domaine générique est ajouté pour un enregistrement A et AAAA.

Lorsqu'une requête est reçue pour un nom de domaine existant dans la zone, l'appliance Citrix ADC répond avec la réponse correspondante. Par exemple, pour `www.example.com`, l'appliance répond avec 2.2.2.2 dans l'exemple.

Pour un nom de domaine inexistant qui correspond à un type générique, une réponse synthétisée est fournie.

Dans l'exemple, l'appliance Citrix ADC répond avec 10.10.10.10 et 10.10.10.11 pour un nom de domaine nonexist.example.com ou xyz.example.com.

La synthèse générique n'est pas applicable pour un nom de domaine existant dans la zone.

Par exemple, pour la requête `www.example.com` et le type AAAA, l'appliance Citrix ADC ne synthétise pas avec le caractère générique, car `www.example.com` existe avec le type A. Dans l'exemple, l'appliance Citrix ADC répond par une réponse NODATA.

Pour une requête par exemple abc.exemple.com et type AAAA, l'appliance Citrix ADC répond par une réponse synthétisée. Par exemple, pour `www.example.com`, l'appliance répond avec 2001 1 dans l'exemple.

Atténuer les attaques DNS DDoS

August 20, 2021

Les serveurs DNS sont l'un des composants les plus critiques d'un réseau et doivent être défendus contre les attaques. L'un des types les plus basiques d'attaques DNS est l'attaque DDoS. Les attaques de ce type sont en hausse et peuvent être destructrices. Vous pouvez effectuer les opérations suivantes pour atténuer les attaques DDoS :

- Rincer les enregistrements négatifs.
- Restreindre le temps de vie (TTL) des enregistrements négatifs.
- Préservez la mémoire Citrix ADC en limitant la mémoire consommée par le cache DNS.
- Conservez les enregistrements DNS dans le cache.
- Activer le contournement du cache DNS.

Purger les enregistrements négatifs

Une attaque DNS remplit le cache avec des enregistrements négatifs (NXDOMAIN et NODATA). Par conséquent, les réponses aux demandes légitimes ne sont pas mises en cache, de sorte que les nouvelles demandes sont envoyées à un serveur principal pour une résolution DNS. Les réponses sont donc retardées.

Vous pouvez désormais vider les enregistrements DNS négatifs du cache DNS de l'appliance Citrix ADC.

Vider les enregistrements de cache négatifs à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
flush dns proxyrecords -type (dnsRecordType | negRecType)NXDOMAIN | NODATA
```

Exemple :

```
flush dns proxyrecords -negRecType NODATA
```

Vider les enregistrements de cache négatifs à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **DNS** > **Enregistrements** .
2. Dans le volet d'informations, cliquez sur **Vider les enregistrements proxy**.
3. Dans la zone **Type de vidage**, sélectionnez **Enregistrements négatifs** .
4. Dans la zone **Type d'enregistrements négatifs**, sélectionnez **NXDOMAIN** ou **NODATA** .

Protection contre les attaques aléatoires de sous-domaine et NXDOMAIN

Pour éviter les attaques aléatoires de sous-domaine et de NXDOMAIN, vous pouvez restreindre la mémoire cache DNS et ajuster les valeurs TTL pour les enregistrements négatifs.

Pour limiter la quantité de mémoire consommée par le cache DNS, spécifiez la taille maximale du cache (en Mo), ainsi que la taille du cache (en Mo) pour stocker les réponses négatives. Lorsque l'une

ou l'autre des limites est atteinte, aucune autre entrée n'est ajoutée au cache. En outre, les messages syslog sont consignés et, si vous avez configuré les interruptions SNMP, les interruptions SNMP sont générées. Si ces limites ne sont pas définies, la mise en cache continue jusqu'à épuisement de la mémoire système.

Une valeur TTL plus élevée pour les enregistrements négatifs peut entraîner le stockage d'enregistrements qui ne sont pas précieux depuis longtemps. Une valeur de TTL inférieure entraîne l'envoi d'un plus grand nombre de demandes au serveur principal.

Le TTL de l'enregistrement négatif est défini sur une valeur qui peut être la moins élevée entre la valeur TTL ou la valeur « Expire » de l'enregistrement SOA.

Remarque :

- Cette limitation est ajoutée par moteur de paquets. Par exemple, si MaxCacheSize est défini sur 5 Mo et que l'appliance dispose de 3 moteurs de paquets, la taille totale du cache est de 15 Mo.
- La taille du cache pour les enregistrements négatifs doit être inférieure ou égale à la taille maximale du cache.
- Si vous réduisez la limite de mémoire cache DNS à une valeur inférieure à la quantité de données déjà mises en cache, la taille du cache reste supérieure à la limite jusqu'à ce que les données soient épuisées. Autant dire, dépasse son TTL0 ou est vidé (`flush dns proxyrecords` commande ou Flush Proxy Records dans l'interface graphique Citrix ADC).
- Pour configurer les interruptions SNMP, reportez-vous à la section Configuration de NetScaler pour générer des interruptions SNMP.

Limiter la mémoire consommée par le cache DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set dns parameter -maxCacheSize <MBytes> -maxNegativeCacheSize <MBytes>
```

Exemple :

```
set dns parameter - maxCacheSize 100 -maxNegativeCacheSize 25
```

Limiter la mémoire consommée par le cache DNS à l'aide de l'interface graphique

Accédez à **Configuration** > **Gestion du trafic** > **DNS**, cliquez sur **Modifier les paramètres DNS** et définissez les paramètres suivants :

- Taille maximale du cache en Mo
- Taille maximale du cache négatif en Mo

Restreindre la TTL des enregistrements négatifs à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set dns parameter -maxnegcacheTTL <secs>
```

Exemple :

```
set dns parameter -maxnegcacheTTL 360
```

Restreindre la TTL des enregistrements négatifs à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **DNS** .
2. Cliquez sur **Modifier les paramètres DNS** et définissez le paramètre **Max Negative Cache TTL in sec.**

Conserver les enregistrements DNS dans le cache

Une attaque peut inonder le cache DNS avec des entrées non importantes, mais peut provoquer le vidage des enregistrements légitimes déjà mis en cache pour faire de la place aux nouvelles entrées. Pour empêcher les attaques de remplir le cache avec des données non valides, vous pouvez conserver les enregistrements légitimes même après qu'ils dépassent leurs valeurs TTL.

Si vous activez le paramètre CacheNoExpire, les enregistrements actuellement dans le cache sont conservés jusqu'à ce que vous désactiviez le paramètre.

Remarque :

- Cette option ne peut être utilisée que lorsque la taille maximale du cache est spécifiée (paramètre MaxCacheSize).
- Si MaxNegCacheTL est configuré et CacheNoExpire est activé, CacheNoExpire prend la priorité.

Conserver les enregistrements DNS dans le cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set dns parameter -cacheNoExpire ( ENABLED | DISABLED)
```

Exemple :

```
set dns parameter -cacheNoExpire ENABLED
```

Conserver les enregistrements DNS dans le cache à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **DNS** et cliquez sur **Modifier les paramètres DNS**.
2. Sélectionnez **Cache No Expiration**.

Activer le contournement du cache DNS

Pour une meilleure visibilité et un meilleur contrôle des requêtes DNS, définissez le paramètre CacheHitByPass pour transférer toutes les requêtes vers les serveurs back-end et autoriser la génération du cache mais non utilisée. Une fois le cache créé, vous pouvez désactiver le paramètre afin que les requêtes soient traitées à partir du cache.

Activer le contournement du cache DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set dns parameter -cacheHitBypass ( ENABLED | DISABLED )
```

Exemple :

```
set dns parameter -cacheHitBypass ENABLED
```

Activer le contournement du cache DNS à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **DNS** et cliquez sur **Modifier les paramètres DNS**.
2. Sélectionnez **Cache Hit Bypass**.

Prévenir l'attaque `Slowloris`

Une requête DNS couvrant plusieurs paquets présente la menace potentielle d'une attaque `Slowloris`. L'appliance Citrix ADC peut supprimer silencieusement les requêtes DNS qui sont divisées en plusieurs paquets.

Vous pouvez définir le paramètre `splitPktQueryProcessing` sur ALLOW ou DROP une requête DNS si la requête est divisée en plusieurs paquets.

Remarque : Ce paramètre est applicable uniquement pour le TCP DNS.

Limiter les requêtes DNS à un seul paquet à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set dns parameter -splitPktQueryProcessing ( ALLOW | DROP )
```

Exemple :

```
set dns parameter -splitPktQueryProcessing DROP
```


Limiter les requêtes DNS à un seul paquet à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **DNS** et cliquez sur **Modifier les paramètres DNS**.
2. Dans la zone **Traitement des requêtes de paquets fractionnés**, choisissez **ALLOW** ou **DROP**.

Collecter des statistiques sur les réponses DNS fournies à partir du cache

Vous pouvez collecter des statistiques sur les réponses DNS fournies à partir du cache. Utilisez ensuite ces statistiques pour créer un seuil au-delà duquel plus de trafic DNS est supprimé, et appliquer ce seuil à l'aide d'une stratégie basée sur la bande passante. Auparavant, le calcul de la bande passante pour un serveur virtuel d'équilibrage de charge DNS n'était pas exact, car le nombre de requêtes envoyées à partir du cache n'était pas signalé.

En mode proxy, les statistiques relatives aux octets de requête, aux octets de réponse, au total des paquets reçus et aux statistiques Total des paquets envoyés sont continuellement mises à jour. Auparavant, ces statistiques n'étaient pas toujours mises à jour, en particulier pour un serveur virtuel d'équilibrage de charge DNS.

Le mode proxy vous permet également de déterminer le nombre de réponses DNS servies à partir du cache. Pour collecter ces statistiques, les options suivantes ont été ajoutées à la `stat lb vserver <DNSvirtualServerName>` commande :

- **Demandes** : nombre total de demandes reçues par le serveur virtuel DNS ou DNS_TCP. Inclut les demandes transférées vers le back-end et les demandes traitées depuis le cache.
- **Vserver hits** : nombre total de demandes transférées vers le back-end. Le nombre de demandes servies à partir du cache correspond à la différence entre le nombre total de demandes et le nombre de demandes servies à partir du serveur virtuel.
- **Réponses** — Nombre total de réponses envoyées par ce serveur virtuel. Par exemple, si un serveur virtuel DNS LB recevait 5 demandes DNS, en remettait 3 au back-end et en servait 2 à partir du cache, la valeur correspondante de chacune de ces statistiques serait la suivante :
  - **Vserver accès** : 3
  - **Demandes** : 5
  - **Réponses** : 5

Équilibrage de charge du pare-feu

January 21, 2021

L'équilibrage de charge du pare-feu répartit le trafic entre plusieurs pare-feu, offrant une tolérance aux pannes et un débit accru. L'équilibrage de charge du pare-feu protège votre réseau en :

- Diviser la charge entre les pare-feu, ce qui élimine un seul point de défaillance et permet au réseau d'évoluer.
- Augmentation de la haute disponibilité.

La configuration d'une appliance Citrix ADC pour l'équilibrage de charge du pare-feu est similaire à la configuration de l'équilibrage de charge, à l'exception que le type de service recommandé est ANY, que le type de moniteur recommandé est PING et que le mode serveur virtuel d'équilibrage de charge est défini sur MAC.

Vous pouvez configurer l'équilibrage de charge du pare-feu dans une configuration d'environnement sandwich, d'entreprise ou de pare-feu multiple. L'environnement sandwich est utilisé pour équilibrer la charge du trafic entrant dans le réseau depuis l'extérieur et du trafic sortant du réseau vers Internet et implique la configuration de deux appliances Citrix ADC, une de chaque côté d'un ensemble de pare-feu. Vous configurez un environnement d'entreprise pour le trafic d'équilibrage de charge quittant le réseau vers Internet. L'environnement d'entreprise implique la configuration d'une seule appliance Citrix ADC entre le réseau interne et les pare-feu qui fournissent un accès à Internet. L'environnement de pare-feu multiple est utilisé pour le trafic d'équilibrage de charge provenant d'un autre pare-feu. L'équilibrage de charge du pare-feu activé des deux côtés de l'appliance Citrix ADC améliore le flux de trafic dans le sens de sortie et d'entrée et assure un traitement plus rapide du trafic. L'environnement multipare-feu implique la configuration d'une appliance Citrix ADC en sandwich entre deux pare-feu.

Important : si vous configurez des itinéraires statiques sur l'appliance Citrix ADC pour l'adresse IP de destination et activez le mode L3, l'appliance Citrix ADC utilise sa table de routage pour acheminer le trafic au lieu d'envoyer le trafic vers le serveur d'équilibrage de charge.

Remarque : Pour que FTP fonctionne, un serveur virtuel ou un service supplémentaire doit être configuré sur l'appliance Citrix ADC avec l'adresse IP et le port comme * et 21 respectivement, et le type de service spécifié comme FTP. Dans ce cas, l'appliance Citrix ADC gère le protocole FTP en acceptant la connexion de contrôle FTP, en modifiant la charge utile et en gérant la connexion de données, le tout via le même pare-feu.

L'équilibrage de charge du pare-feu ne prend en charge que certaines des méthodes d'équilibrage de charge prises en charge par l'appliance Citrix ADC. En outre, vous pouvez configurer seulement quelques types de persistance et de moniteurs.

Méthodes d'équilibrage de charge du pare-feu

Les méthodes d'équilibrage de charge suivantes sont prises en charge pour l'équilibrage de charge du pare-feu.

- Connexions moindres
- Round Robin
- Moins de paquets
- Moins de bande passante

- Hash IP source
- Hash IP de destination
- Hash IP de destination IP source
- Hachage du port source IP source
- Méthode du temps de réponse le plus faible (LRTM)
- Chargement personnalisé

Persistance du pare-feu

Seules la persistance SOURCEIP, DESTIP et SOURCEIPDESTIP sont prises en charge pour l'équilibrage de charge du pare-feu.

Surveillance du serveur de pare-feu

Seuls les moniteurs PING et transparents sont pris en charge dans l'équilibrage de charge du pare-feu. Vous pouvez lier un moniteur PING (par défaut) au service principal qui représente le pare-feu. Si un pare-feu est configuré pour ne pas répondre aux paquets ping, vous pouvez configurer des moniteurs transparents pour surveiller les hôtes du côté approuvé via des pare-feu individuels.

Environnement Sandwich

August 20, 2021

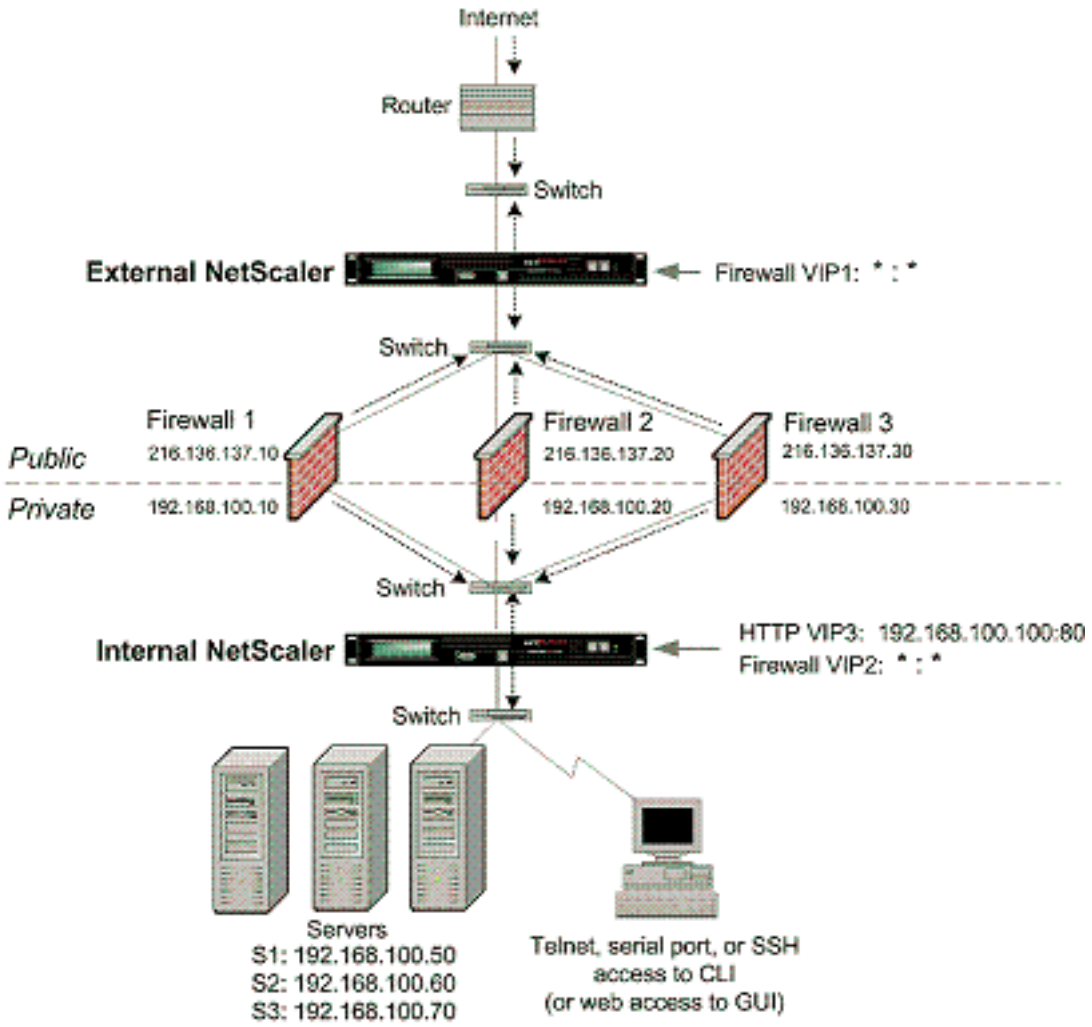
Un déploiement Citrix ADC en mode sandwich peut équilibrer la charge du trafic réseau via des pare-feu dans les deux sens : entrée (trafic entrant dans le réseau depuis l'extérieur, comme Internet) et sortie (trafic quittant le réseau vers Internet).

Dans cette configuration, un Citrix ADC se trouve de chaque côté d'un ensemble de pare-feu. Citrix ADC placé entre les pare-feu et Internet, appelé Citrix ADC externe qui gère le trafic entrant sélectionne le meilleur pare-feu, en fonction de la méthode configurée. Le Citrix ADC entre les pare-feu et le réseau privé, appelé Citrix ADC interne, suit le pare-feu à partir duquel le paquet initial d'une session est reçu. Il s'assure ensuite que tous les paquets suivants pour cette session sont envoyés au même pare-feu.

Citrix ADC interne peut être configuré en tant que gestionnaire de trafic régulier pour équilibrer la charge du trafic sur les serveurs du réseau privé. Cette configuration permet également d'équilibrer la charge du trafic provenant du réseau privé (sortie) sur les pare-feu.

Le diagramme suivant illustre l'environnement d'équilibrage de charge du pare-feu sandwich.

Figure 1. Équilibrage de charge du pare-feu (sandwich)



Le type de service ANY configure Citrix ADC pour accepter tout le trafic.

Pour bénéficier des avantages liés à HTTP et TCP, configurez le service et le serveur virtuel avec le type HTTP ou TCP. Pour que FTP fonctionne, configurez le service avec le type FTP.

Configuration de ADC Citrix ADC externe dans un environnement sandwich

Effectuez les tâches suivantes pour configurer Citrix ADC externe dans un environnement sandwich

- Activez la fonction d'équilibrage de charge.
- Configurez un service générique pour chaque pare-feu.
- Configurez un moniteur pour chaque service générique.
- Configurez un serveur virtuel générique pour le trafic provenant d'Internet.
- Configurez le serveur virtuel en mode réécriture MAC.
- Liez les services au serveur virtuel générique.
- Enregistrez et vérifiez la configuration.

Activer la fonction d'équilibrage de charge

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

```
enable ns feature LB
show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```

Pour activer l'équilibrage de charge à l'aide de l'utilitaire de configuration

Accédez à **Système > Paramètres** et, dans **Configurer les fonctionnalités de base**, sélectionnez **Équilibrage de charge**.

Configurer un service générique pour chaque pare-feu

Pour configurer un service générique pour chaque pare-feu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Exemple :


```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```

Pour configurer un service générique pour chaque pare-feu à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services** et ajoutez un service. Spécifiez **ANY** dans le champ **Protocole** et * dans le champ Port.

Configurer un moniteur pour chaque service générique

Un moniteur PING est lié par défaut au service. Vous devez configurer un moniteur transparent pour surveiller les hôtes du côté approuvé via des pare-feu individuels. Vous pouvez ensuite lier le moniteur transparent aux services. Le moniteur PING par défaut surveille la connectivité uniquement entre l'appliance Citrix ADC et le périphérique en amont. Le moniteur transparent surveille tous les périphériques existants dans le chemin d'accès entre l'appliance et le périphérique qui possède l'adresse IP de destination spécifiée dans le moniteur. Si un moniteur transparent n'est pas configuré et que l'état du pare-feu est UP mais que l'un des périphériques de saut suivants de ce pare-feu est en panne, l'appliance inclut le pare-feu lors de l'équilibrage de charge et transmet le paquet au pare-feu. Cependant, le paquet n'est pas livré à la destination finale car l'un des périphériques de saut suivants est en panne. En liant un moniteur transparent, si l'un des périphériques (y compris le pare-feu) est en panne, le service est marqué comme étant DOWN et le pare-feu n'est pas inclus lorsque l'appliance effectue l'équilibrage de charge du pare-feu.

La liaison d'un moniteur transparent remplace le moniteur PING. Pour configurer un moniteur PING en plus d'un moniteur transparent, après avoir créé et lié un moniteur transparent, vous devez lier un moniteur PING au service.

Pour configurer un moniteur transparent à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
```



```
2 bind monitor monitor-HTTP-1 fw-svc1
3 To bind a PING monitor, type the following command:
4 bind monitor PING fw-svc1
5 <!--NeedCopy-->
```

Pour créer et lier un moniteur transparent à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**, puis créez et liez un moniteur transparent.

Configurer un serveur virtuel générique pour le trafic provenant d'Internet

Pour configurer un serveur virtuel générique pour le trafic provenant d'Internet à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lb vserver <name> ANY * *
2 <!--NeedCopy-->
```

Exemple :

```
1 add lb vserver Vserver-LB-1 ANY * *
2 <!--NeedCopy-->
```

Pour configurer un serveur virtuel générique pour le trafic provenant d'Internet à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et créez un serveur virtuel générique. Spécifiez **ANY** dans le champ **Protocole** et * dans le champ Port.

Configurer le serveur virtuel en mode réécriture MAC

Pour configurer le serveur virtuel en mode réécriture MAC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 set lb vserver <name>@ -m <RedirectionMode>
2 <!--NeedCopy-->
```

Exemple :


```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

Pour configurer le serveur virtuel en mode réécriture MAC à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, vServer-LB-1).
2. Modifiez la section **Paramètres de base**, puis cliquez sur **plus**.
3. Dans la liste déroulante **Mode de redirection**, sélectionnez **Base MAC**.

Liez les services au serveur virtuel générique

Pour lier un service au serveur virtuel générique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier un service au serveur virtuel générique à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et sélectionnez le serveur virtuel pour lequel vous souhaitez lier le service.
2. Cliquez dans la section **Services** et sélectionnez un service à lier.

Enregistrer et vérifier la configuration

Lorsque vous avez terminé les tâches de configuration, veillez à enregistrer la configuration. Assurez-vous que les paramètres sont corrects.

Pour enregistrer et vérifier la configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :


```
save ns config
show vserver
<!--NeedCopy-->
```

Exemple :

```
save config
sh lb vserver FWLBVIP1
FWLBVIP1 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 06:40:14 2010
        Time since last state change: 0 days, 00:00:11.240
        Effective State: UP  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: SRCIPDESTIPHASH
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw_svc_1 (10.102.29.251: *) - ANY State: UP  Weight: 1
2) fw_svc_2 (10.102.29.18: \*) - ANY State: UP   Weight: 1
 Done
show service fw-svc1
        fw-svc1 (10.102.29.251:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 10:04:50 2010
        Time since last state change: 0 days, 00:00:38.120
        Server Name: 10.102.29.251
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED
```



```
39
40 1)      Monitor Name: monitor-HTTP-1
41                 State: DOWN     Weight: 1
42                 Probes: 5       Failed [Total: 5 Current: 5]
43                 Last response: Failure - Time out during TCP connection
                       establishment stage
44                 Response Time: 2000.0 millisec
45 2)      Monitor Name: ping
46                 State: UP       Weight: 1
47                 Probes: 3       Failed [Total: 0 Current: 0]
48                 Last response: Success - ICMP echo reply received.
49                 Response Time: 1.415 millisec
50  Done
51 <!--NeedCopy-->
```

Configuration de ADC Citrix ADC interne dans un environnement sandwich

Effectuez les tâches suivantes pour configurer le Citrix ADC interne dans un environnement sandwich

Pour le trafic à partir du serveur (sortie)

- Activez la fonction d'équilibrage de charge.
- Configurez un service générique pour chaque pare-feu.
- Configurez un moniteur pour chaque service générique.
- Configurez un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu.
- Configurez le serveur virtuel en mode réécriture MAC.
- Liez les services de pare-feu au serveur virtuel générique.

Pour le trafic sur les serveurs de réseau privé

- Configurez un service pour chaque serveur virtuel.
- Configurez un moniteur pour chaque service.
- Configurez un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs.
- Liez les services HTTP au serveur virtuel HTTP.
- Enregistrez et vérifiez la configuration.

Activer la fonction d'équilibrage de charge

Vous pouvez configurer des entités d'équilibrage de charge telles que les services et les serveurs virtuels lorsque la fonctionnalité d'équilibrage de charge est désactivée. Mais ils ne fonctionneront pas tant que vous n'avez pas activé la fonction.

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

```
enable ns feature LB
show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```

Pour activer l'équilibrage de charge à l'aide de l'utilitaire de configuration

Accédez à **Système > Paramètres** et, dans Configurer les fonctionnalités de base, sélectionnez **Équilibrage de charge**.

Configurer un service générique pour chaque pare-feu

Pour configurer un service générique pour chaque pare-feu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```


Pour configurer un service générique pour chaque pare-feu à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services** et ajoutez un service. Spécifiez **ANY** dans le champ **Protocole** et * dans le champ Port.

Configurer un moniteur pour chaque service générique

Un moniteur PING est lié par défaut au service. Vous devez configurer un moniteur transparent pour surveiller les hôtes du côté approuvé via des pare-feu individuels. Vous pouvez ensuite lier le moniteur transparent aux services. Le moniteur PING par défaut surveille la connectivité uniquement entre l'appliance Citrix ADC et le périphérique en amont. Le moniteur transparent surveille tous les périphériques existants dans le chemin d'accès entre l'appliance et le périphérique qui possède l'adresse IP de destination spécifiée dans le moniteur. Si un moniteur transparent n'est pas configuré et que l'état du pare-feu est UP mais que l'un des périphériques de saut suivants de ce pare-feu est en panne, l'appliance inclut le pare-feu lors de l'équilibrage de charge et transmet le paquet au pare-feu. Cependant, le paquet n'est pas livré à la destination finale car l'un des périphériques de saut suivants est en panne. En liant un moniteur transparent, si l'un des périphériques (y compris le pare-feu) est en panne, le service est marqué comme étant DOWN et le pare-feu n'est pas inclus lorsque l'appliance effectue l'équilibrage de charge du pare-feu.

La liaison d'un moniteur transparent remplace le moniteur PING. Pour configurer un moniteur PING en plus d'un moniteur transparent, après avoir créé et lié un moniteur transparent, vous devez lier un moniteur PING au service.

Pour configurer un moniteur transparent à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

```
1 add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
     transparent (YES | NO )]
2 bind lb monitor <monitorName> <serviceName>
3 <!--NeedCopy-->
```

Exemple :

```
1 add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
2 bind monitor monitor-HTTP-1 fw-svc1
3 <!--NeedCopy-->
```

Pour créer et lier un moniteur transparent à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs** et créez un moniteur.
2. Dans la boîte de dialogue **Créer un moniteur**, entrez les paramètres requis, puis sélectionnez **Transparent**.

Configurer un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu

Pour configurer un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Pour configurer un serveur virtuel générique pour le trafic provenant d'Internet à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et créez un serveur virtuel générique.
2. Spécifiez **ANY** dans le champ Protocole et ***** dans le champ Port.

Pour configurer un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), spécifiez les valeurs des paramètres suivants comme indiqué :
   - Name—name
4. Dans Protocole, sélectionnez ANY, et dans Adresse IP et port, sélectionnez *.
5. Cliquez sur Créer, puis sur Fermer. Le serveur virtuel que vous avez créé apparaît dans le volet Serveurs virtuels d'équilibrage de charge.

Configurer le serveur virtuel en mode réécriture MAC

Pour configurer le serveur virtuel en mode réécriture MAC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

Pour configurer le serveur virtuel en mode réécriture MAC à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, vServer-LB-1).
2. Modifiez la section **Paramètres de base**, puis cliquez sur **plus**.
3. Dans la liste déroulante **Mode de redirection**, sélectionnez **Base MAC**.

Liez les services de pare-feu au serveur virtuel générique

Pour lier des services de pare-feu au serveur virtuel générique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier des services de pare-feu au serveur virtuel générique à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis sélectionnez un serveur virtuel.
2. Cliquez dans la section Service, puis sélectionnez un service à lier.

Remarque : Vous pouvez lier un service à plusieurs serveurs virtuels.

Configurer un service pour chaque serveur virtuel

Pour configurer un service pour chaque serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <name> <serverName> HTTP <port>
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 10.102.29.5 HTTP 80
<!--NeedCopy-->
```

Pour configurer un service pour chaque serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et configurez un service pour chaque serveur virtuel.
2. Spécifiez **HTTP** dans le champ **Protocole**, puis sélectionnez **HTTP** sous **Moniteurs disponibles**.

Pour configurer un service pour chaque serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un service, spécifiez les valeurs des paramètres suivants comme indiqué :
   - Nom du service : nom
   - serveur—Nom du serveur
   - port : port
4. Dans Protocole, spécifiez HTTP. Sous Moniteurs disponibles, sélectionnez HTTP.
5. Cliquez sur Créer, puis sur Fermer. Le service que vous avez créé apparaît dans le volet Services.

Configurer un moniteur pour chaque service

Pour lier un moniteur à un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```


Exemple :

```
bind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier un moniteur à un service à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services**, double-cliquez sur un service et ajoutez un moniteur.

Configurer un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs

Pour configurer un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb vserver <name> HTTP <ip> <port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

Pour configurer un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Virtual Services**et configurez un serveur virtuel HTTP.
2. Spécifiez **HTTP** dans le champ **Protocole** .

Pour configurer un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), spécifiez les valeurs des paramètres suivants comme indiqué :
    - Name—name

- Adresse IP : Adresse IP
  Note : Si le serveur virtuel utilise IPv6, activez la case à cocher IPv6 et entrez l'adresse au format IPv6 (par exemple, **1000:0000:0000:0000:0005:0600:700 a:888b**).
- port : port

4. Sous Protocole, sélectionnez HTTP.
5. Cliquez sur Créer, puis sur Fermer. Le serveur virtuel que vous avez créé apparaît dans le volet Serveurs virtuels d'équilibrage de charge.

Enregistrer et vérifier la configuration

Lorsque vous avez terminé les tâches de configuration, veillez à enregistrer la configuration. Vous devez également vérifier que les paramètres sont corrects.

Pour enregistrer et vérifier la configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

- `save ns config`
- `show vserver`

Exemple :

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
```



```
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: DOWN     Weight: 1
                Probes: 9       Failed [Total: 9 Current: 9]
                Last response: Failure - Time out during TCP connection
                    establishment stage
                Response Time: 2000.0 millisec
2)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 3       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.275 millisec
 Done
<!--NeedCopy-->
```

Pour enregistrer et vérifier la configuration à l'aide de l'utilitaire de configuration

1. Dans le volet **Détails**, cliquez sur **Enregistrer**.
2. Dans la boîte de dialogue **Enregistrer la configuration**, cliquez sur **Oui**.
3. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
4. Dans le volet **Détails**, sélectionnez le serveur virtuel que vous avez créé à l'étape 5.
5. Vérifiez que les paramètres affichés dans le volet **Détails** sont corrects.
6. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
7. Dans le volet **Détails**, sélectionnez les services que vous avez créés à l'étape 5.

8. Vérifiez que les paramètres affichés dans le volet **Détails** sont corrects.

Surveillance d'un équilibrage de charge du pare-feu configuré dans un environnement sandwich

Une fois la configuration terminée, vous devez afficher les statistiques de chaque service et serveur virtuel pour vérifier les éventuels problèmes.

Affichage des statistiques d'un serveur virtuel

Pour évaluer les performances des serveurs virtuels ou pour résoudre les problèmes, vous pouvez afficher les détails des serveurs virtuels configurés sur l'appliance Citrix ADC. Vous pouvez afficher un résumé des statistiques pour tous les serveurs virtuels ou spécifier le nom d'un serveur virtuel pour afficher les statistiques uniquement pour ce serveur virtuel. Vous pouvez afficher les détails suivants :

- Nom
- Adresse IP
- Port
- Protocole
- État du serveur virtuel
- Taux de demandes reçues
- Taux de succès

Pour afficher les statistiques du serveur virtuel à l'aide de l'interface de ligne de commande

Pour afficher un résumé des statistiques de tous les serveurs virtuels actuellement configurés sur Citrix ADC, ou pour un seul serveur virtuel, à l'invite de commandes, tapez :

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Exemple :

```
>stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
         0/s
Two                          *     0          TCP         DOWN      0/s
         0/s
```



```
6  Three                        *  2598          TCP          DOWN       0/s
           0/s
7  dnsVirtualNS    10.102.29.90    53           DNS          DOWN       0/s
           0/s
8  BRVSERV            10.10.1.1    80          HTTP          DOWN       0/s
           0/s
9  LBVIP           10.102.29.66    80          HTTP            UP       0/s
           0/s
10  Done
11
12 <!--NeedCopy-->
```

Pour afficher les statistiques du serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Statistiques**.
2. Si vous souhaitez afficher les statistiques pour un seul serveur virtuel, dans le volet d'informations, sélectionnez le serveur virtuel, puis cliquez sur **Statistiques**.

Affichage des statistiques d'un service

Vous pouvez afficher le taux de demandes, de réponses, d'octets de demande, d'octets de réponse, de connexions client actuelles, de demandes dans la file d'attente de surtension, de connexions serveur actuelles, etc. à l'aide des statistiques de service.

Pour afficher les statistiques d'un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 stat service <name>
2 <!--NeedCopy-->
```

Exemple :

```
1 stat service Service-HTTP-1
2 <!--NeedCopy-->
```

Pour afficher les statistiques d'un service à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services > Statistiques**.
2. Si vous souhaitez afficher les statistiques pour un seul service, sélectionnez-le, puis cliquez sur **Statistiques**.

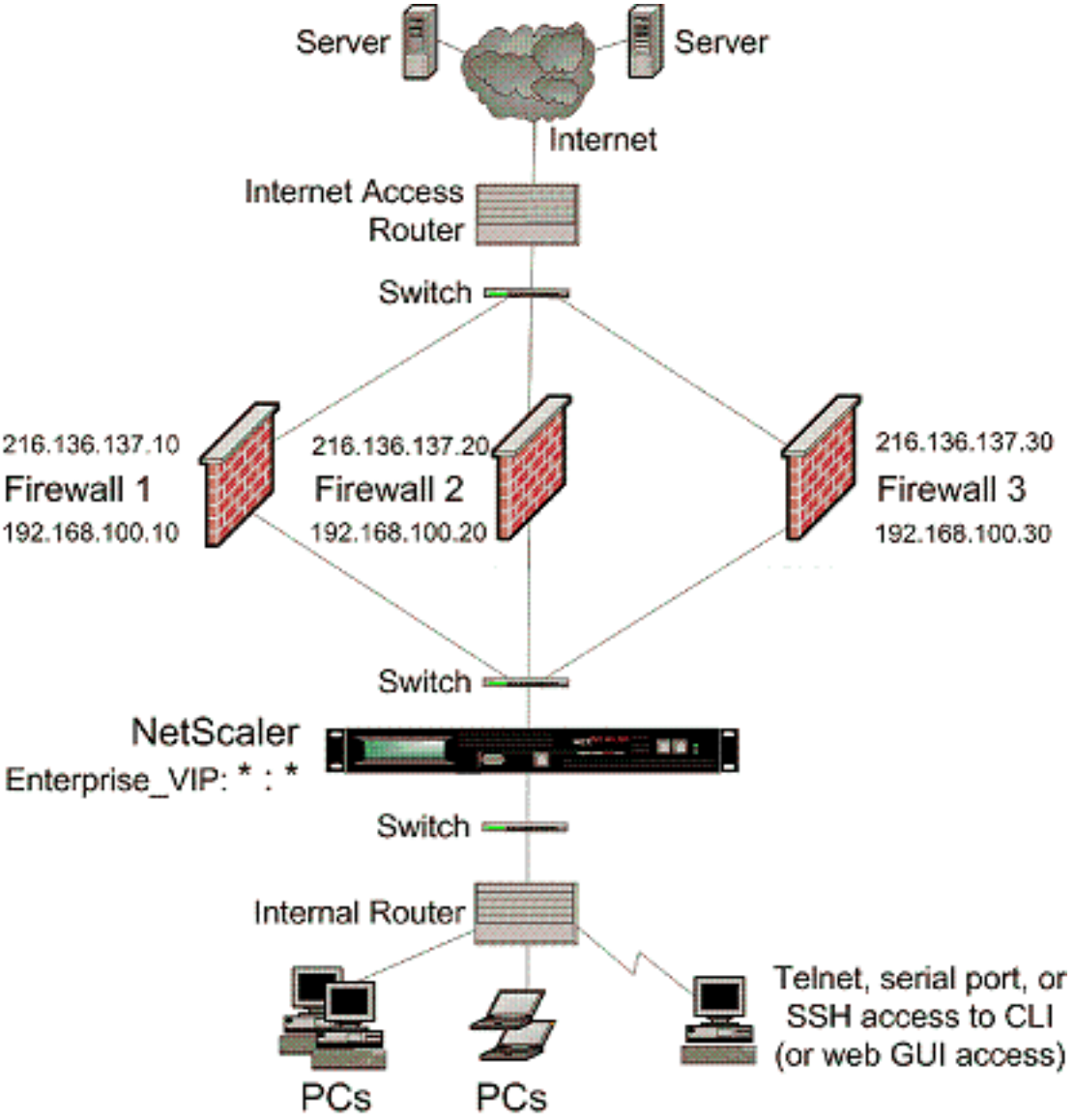
Environnement d’entreprise

August 20, 2021

Dans la configuration d’entreprise, Citrix ADC est placé entre les pare-feu se connectant à Internet public et au réseau privé interne et gère le trafic de sortie. Citrix ADC sélectionne le meilleur pare-feu en fonction de la stratégie d’équilibrage de charge configurée.

Le diagramme suivant illustre l’environnement d’équilibrage de charge du pare-feu d’entreprise

Figure 1. Équilibrage de charge du pare-feu (Enterprise)



Le type de service ANY configure Citrix ADC pour accepter tout le trafic.

Pour bénéficier des avantages liés à HTTP et TCP, configurez le service et vserver avec le type HTTP

ou TCP. Pour que FTP fonctionne, configurez le service avec le type FTP.

Configuration de Citrix ADC dans un environnement d'entreprise

Effectuez les tâches suivantes pour configurer un Citrix ADC dans un environnement d'entreprise.

Pour le trafic à partir du serveur (sortie)

- Activez la fonction d'équilibrage de charge.
- Configurez un service générique pour chaque pare-feu.
- Configurez un moniteur pour chaque service générique.
- Configurez un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu.
- Configurez le serveur virtuel en mode réécriture MAC.
- Liez les services de pare-feu au serveur virtuel générique.

Pour le trafic sur les serveurs de réseau privé

- Configurez un service pour chaque serveur virtuel.
- Configurez un moniteur pour chaque service.
- Configurez un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs.
- Liez les services HTTP au serveur virtuel HTTP.
- Enregistrez et vérifiez la configuration.

Activer la fonction d'équilibrage de charge

Vous pouvez configurer des entités d'équilibrage de charge telles que des services et des serveurs virtuels lorsque la fonctionnalité d'équilibrage de charge est désactivée, mais elles ne fonctionneront pas tant que vous n'avez pas activé la fonctionnalité.

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

- activer la fonction ns LB
- show ns feature

Exemple :

```
1 > enable ns feature LoadBalancing
2  Done
3 > show ns feature
4
5         Feature                       Acronym             Status
6         -------                       -------             ------
```



```
1)     Web Logging                    WL                  OFF
2)     Surge Protection               SP                  ON
3)     Load Balancing                 LB                  ON
.
.
.
24)    NetScaler Push                 push                OFF
Done
<!--NeedCopy-->
```

Pour activer l'équilibrage de charge à l'aide de l'utilitaire de configuration

Accédez à Système > Paramètres et, dans Configurer les fonctionnalités de base, sélectionnez Équilibrage de charge.

Configurer un service générique pour chaque pare-feu

Pour configurer un service générique pour chaque pare-feu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```

Pour configurer un service générique pour chaque pare-feu à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un service, spécifiez les valeurs des paramètres suivants comme indiqué :
   - Nom du service : nom
   - serveur—Nom du serveur
4. Dans Protocole, sélectionnez ANY et dans Port, sélectionnez *.
5. Cliquez sur Créer, puis sur Fermer. Le service que vous avez créé apparaît dans le volet Services.

Configurer un moniteur pour chaque service générique

Un moniteur PING est lié par défaut au service. Vous devrez configurer un moniteur transparent pour surveiller les hôtes du côté approuvé via des pare-feu individuels. Vous pouvez ensuite lier le moniteur transparent aux services. Le moniteur PING par défaut surveille la connectivité uniquement entre l'appliance Citrix ADC et le périphérique en amont. Le moniteur transparent surveille tous les périphériques existants dans le chemin d'accès entre l'appliance et le périphérique qui possède l'adresse IP de destination spécifiée dans le moniteur. Si un moniteur transparent n'est pas configuré et que l'état du pare-feu est UP mais que l'un des périphériques de saut suivants de ce pare-feu est en panne, l'appliance inclut le pare-feu lors de l'équilibrage de charge et transmet le paquet au pare-feu. Cependant, le paquet n'est pas livré à la destination finale car l'un des périphériques de saut suivants est en panne. En liant un moniteur transparent, si l'un des périphériques (y compris le pare-feu) est en panne, le service est marqué comme étant DOWN et le pare-feu n'est pas inclus lorsque l'appliance effectue l'équilibrage de charge du pare-feu.

La liaison d'un moniteur transparent remplace le moniteur PING. Pour configurer un moniteur PING en plus d'un moniteur transparent, après avoir créé et lié un moniteur transparent, vous devez lier un moniteur PING au service.

Pour configurer un moniteur transparent à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

```
1 add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
     transparent (YES | NO )]
2 bind lb monitor <monitorName> <serviceName>
3 <!--NeedCopy-->
```

Exemple :

```
1 add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
2 bind monitor monitor-HTTP-1 fw-svc1
3 <!--NeedCopy-->
```

Pour créer et lier un moniteur transparent à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Moniteurs.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un moniteur, spécifiez les valeurs comme indiqué :
    - Nom*

- Type*—type
- IP destination
- Transparent

-* Un paramètre obligatoire

4. Cliquez sur Créer, puis sur Fermer. Dans le volet Moniteurs, sélectionnez le moniteur que vous venez de configurer et vérifiez que les paramètres affichés en bas de l'écran sont corrects.

Configurer un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu

Pour configurer un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Pour configurer un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), spécifiez les valeurs des paramètres suivants comme indiqué :
   - Name—name
4. Dans Protocole, sélectionnez ANY, et dans Adresse IP et port, sélectionnez *.
5. Cliquez sur Créer, puis sur Fermer. Le serveur virtuel que vous avez créé apparaît dans le volet Serveurs virtuels d'équilibrage de charge.

Configurer le serveur virtuel en mode réécriture MAC

Pour configurer le serveur virtuel en mode réécriture MAC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

Pour configurer le serveur virtuel en mode réécriture MAC à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, vServer-lb-1), puis cliquez sur Ouvrir.
3. Sous l'onglet Avancé, sous Mode de redirection, cliquez sur Mac.
4. Cliquez sur OK.

Liez les services de pare-feu au serveur virtuel générique

Pour lier des services de pare-feu au serveur virtuel générique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier des services de pare-feu au serveur virtuel générique à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels, puis sélectionnez un serveur virtuel.
2. Cliquez dans la section Service, puis sélectionnez un service à lier.

Remarque : Vous pouvez lier un service à plusieurs serveurs virtuels.

Configurer un service pour chaque serveur virtuel

Pour configurer un service pour chaque serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <name> <serverName> HTTP <port>
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 10.102.29.5 HTTP 80
<!--NeedCopy-->
```

Pour configurer un service pour chaque serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un service, spécifiez les valeurs des paramètres suivants comme indiqué :
   - Nom du service : nom
   - serveur—Nom du serveur
   - port : port
4. Dans Protocole, spécifiez HTTP. Sous Moniteurs disponibles, sélectionnez HTTP.
5. Cliquez sur Créer, puis sur Fermer. Le service que vous avez créé apparaît dans le volet Services.

Configurer un moniteur pour chaque service

Pour lier un moniteur à un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Exemple :

```
bind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```


Pour lier un moniteur à un service à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Ouvrez le service et ajoutez un moniteur.

Configurer un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs

Pour configurer un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb vserver <name> HTTP <ip> <port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

Pour configurer un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), spécifiez les valeurs des paramètres suivants comme indiqué :
   - Name—name
   - IP Address—IPAddress
     Remarque : si le serveur virtuel utilise IPv6, activez la case à cocher IPv6 et entrez l'adresse au format IPv6 (par exemple, **1000:0000:0000:0000:0005:0600:700a:888b**).
   - port : port
4. Sous Protocole, sélectionnez HTTP.
5. Cliquez sur Créer, puis sur Fermer. Le serveur virtuel que vous avez créé apparaît dans le volet Serveurs virtuels d'équilibrage de charge.

Liez les services HTTP au serveur virtuel HTTP

Pour lier des services HTTP au serveur virtuel générique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier des services HTTP au serveur virtuel générique à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels, puis sélectionnez un serveur virtuel.
2. Cliquez dans la section Service, puis sélectionnez un service à lier.

Remarque : Vous pouvez lier un service à plusieurs serveurs virtuels.

Enregistrer et vérifier la configuration

Lorsque vous avez terminé les tâches de configuration, veillez à enregistrer la configuration. Vous devez également vérifier que les paramètres sont corrects.

Pour enregistrer et vérifier la configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

- save ns config
- show vserver

Exemple :

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
```



```
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: DOWN     Weight: 1
                Probes: 9       Failed [Total: 9 Current: 9]
                Last response: Failure - Time out during TCP connection
                    establishment stage
                Response Time: 2000.0 millisec
2)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 3       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.275 millisec
 Done
<!--NeedCopy-->
```


Pour enregistrer et vérifier la configuration à l'aide de l'utilitaire de configuration

1. Dans le volet d'informations, cliquez sur Enregistrer.
2. Dans la boîte de dialogue Enregistrer la configuration, cliquez sur Oui.
3. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
4. Dans le volet d'informations, sélectionnez le serveur virtuel que vous avez créé à l'étape 5 et vérifiez que les paramètres affichés dans le volet d'informations sont corrects.
5. Accédez à Gestion du trafic > Équilibrage de charge > Services.
6. Dans le volet d'informations, sélectionnez le service que vous avez créé à l'étape 5 et vérifiez que les paramètres affichés dans le volet d'informations sont corrects.

Surveillance d'une configuration d'équilibrage de charge de pare-feu dans un environnement d'entreprise

Une fois la configuration terminée, vous devez afficher les statistiques de chaque service et serveur virtuel pour vérifier les éventuels problèmes.

Affichage des statistiques d'un serveur virtuel

Pour évaluer les performances des serveurs virtuels ou pour résoudre les problèmes, vous pouvez afficher les détails des serveurs virtuels configurés sur l'appliance Citrix ADC. Vous pouvez afficher un résumé des statistiques pour tous les serveurs virtuels ou spécifier le nom d'un serveur virtuel pour afficher les statistiques uniquement pour ce serveur virtuel. Vous pouvez afficher les détails suivants :

- Nom
- Adresse IP
- Port
- Protocole
- État du serveur virtuel
- Taux de demandes reçues
- Taux de succès

Pour afficher les statistiques du serveur virtuel à l'aide de l'interface de ligne de commande

Pour afficher un résumé des statistiques de tous les serveurs virtuels actuellement configurés sur l'appliance Citrix ADC, ou pour un seul serveur virtuel, à l'invite de commandes, tapez :

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Exemple :


```
>stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
        0/s
Two                          *     0          TCP         DOWN      0/s
        0/s
Three                        *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done


<!--NeedCopy-->
```

Pour afficher les statistiques du serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Statistiques.
2. Si vous souhaitez afficher les statistiques pour un seul serveur virtuel, dans le volet d'informations, sélectionnez le serveur virtuel, puis cliquez sur Statistiques.

Affichage des statistiques d'un service

Mise à jour : 2013-08-28

Vous pouvez afficher le taux de demandes, de réponses, d'octets de demande, d'octets de réponse, de connexions client actuelles, de demandes dans la file d'attente de surtension, de connexions serveur actuelles, etc. à l'aide des statistiques de service.

Pour afficher les statistiques d'un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat service <name>
<!--NeedCopy-->
```

Exemple :


```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Pour afficher les statistiques d'un service à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Services > Statistiques.
2. Si vous souhaitez afficher les statistiques pour un seul service, sélectionnez-le, puis cliquez sur Statistiques.

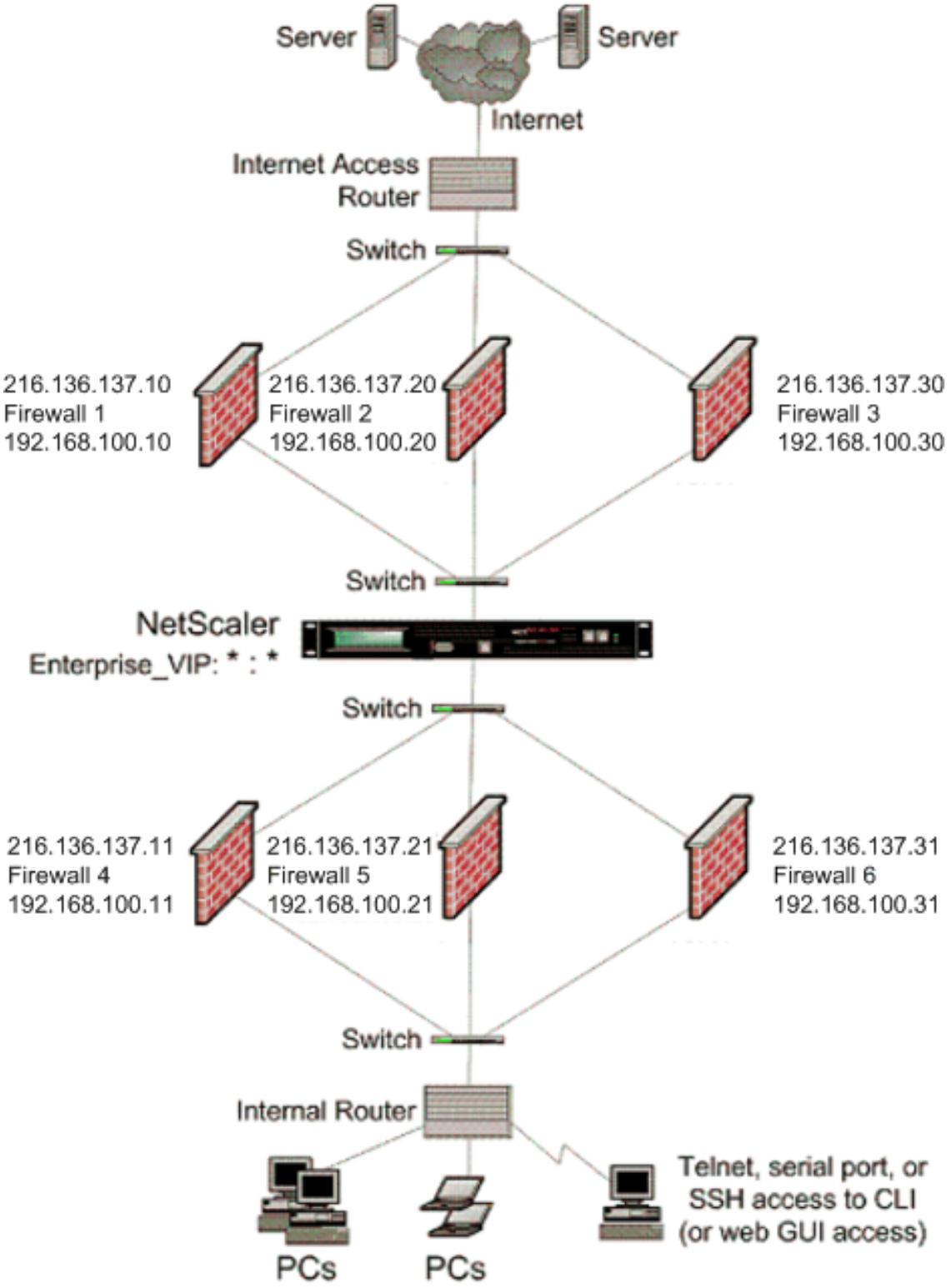
Environnement de pare-feu multiple

August 20, 2021

Dans un environnement à pare-feu multiples, l'appliance Citrix ADC est placée entre deux ensembles de pare-feu, l'ensemble externe se connectant à Internet public et l'ensemble interne se connectant au réseau privé interne. L'ensemble externe gère généralement le trafic de sortie. Ces pare-feu implémentent principalement des listes de contrôle d'accès pour autoriser ou refuser l'accès à des ressources externes. L'ensemble interne gère généralement le trafic entrant. Ces pare-feu mettent en œuvre la sécurité pour protéger l'intranet contre les attaques malveillantes en dehors de l'équilibrage de charge du trafic entrant. L'environnement de pare-feu multiple vous permet d'équilibrer la charge du trafic provenant d'un autre pare-feu. Par défaut, le trafic provenant d'un pare-feu n'est pas équilibré de charge sur l'autre pare-feu sur une appliance Citrix ADC. L'équilibrage de charge du pare-feu activé des deux côtés de Citrix ADC améliore le flux de trafic dans le sens de sortie et d'entrée et assure un traitement plus rapide du trafic.

La figure suivante illustre un environnement d'équilibrage de charge multipare-feu

Figure 1. Équilibrage de la charge du pare-feu (pare-feu multiple)



Avec une configuration comme celle illustrée à la figure 1, vous pouvez configurer Citrix ADC pour équilibrer la charge du trafic via un pare-feu interne, même s'il est équilibré par un pare-feu externe.

Par exemple, avec cette fonctionnalité configurée, le trafic provenant des pare-feu externes (pare-feu 1, 2 et 3) est équilibré sur les pare-feu internes (pare-feu 4, 5 et 6) et vice versa.

L'équilibrage de charge du pare-feu est pris en charge uniquement pour le serveur virtuel LB en mode MAC.

Le type de service ANY configure Citrix ADC pour accepter tout le trafic.

Pour bénéficier des avantages liés à HTTP et TCP, configurez le service et le serveur virtuel avec le type HTTP ou TCP. Pour que FTP fonctionne, configurez le service avec le type FTP.

Configuration de Citrix ADC dans un environnement à pare-feu multiple

Pour configurer une appliance Citrix ADC dans un environnement à pare-feu multiples, vous devez activer la fonction d'équilibrage de charge, configurer un serveur virtuel pour équilibrer la charge du trafic de sortie sur les pare-feu externes, configurer un serveur virtuel pour équilibrer la charge du trafic d'entrée sur les pare-feu internes et activer l'équilibrage de charge du pare-feu sur l'appliance Citrix ADC. Pour configurer un serveur virtuel pour équilibrer la charge du trafic sur un pare-feu dans l'environnement à pare-feu multiple, vous devez :

1. Configurer un service générique pour chaque pare-feu
2. Configurer un moniteur pour chaque service générique
3. Configurer un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu
4. Configurer le serveur virtuel en mode réécriture MAC
5. Liez les services de pare-feu au serveur virtuel générique

Activation de la fonction d'équilibrage de charge

Pour configurer et implémenter des entités d'équilibrage de charge telles que les services et les serveurs virtuels, vous devez activer la fonctionnalité d'équilibrage de charge sur le périphérique Citrix ADC.

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

```
enable ns feature <featureName>
show ns feature
<!--NeedCopy-->
```

Exemple :

```
enable ns feature LoadBalancing
Done
```



```
3 show ns feature
4 Feature Acronym Status
5 ------- ------- ------
6 1) Web Logging WL OFF
7 2) Surge Protection SP ON
8 3) Load Balancing LB ON
9 .
10 .
11 .
12 24) NetScaler Push push OFF
13 Done
14 <!--NeedCopy-->
```

Pour activer l'équilibrage de charge à l'aide de l'interface graphique :

1. Dans le volet de navigation, développez Système, puis cliquez sur Paramètres.
2. Dans le volet Paramètres, sous Modes et fonctionnalités, cliquez sur Modifier les fonctions de base.
3. Dans la boîte de dialogue Configurer les fonctionnalités de base, activez la case à cocher Équilibrage de charge, puis cliquez sur OK.

Configuration d'un service générique pour chaque pare-feu

Pour accepter le trafic provenant de tous les protocoles, vous devez configurer le service générique pour chaque pare-feu en spécifiant la prise en charge de tous les protocoles et ports.

Pour configurer un service générique pour chaque pare-feu à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante pour configurer la prise en charge de tous les protocoles et ports :

```
1 add service <name>@ <serverName> <serviceType> <port_number>
2 <!--NeedCopy-->
```

Exemple :

```
1 add service fw-svc1 10.102.29.5 ANY *
2 <!--NeedCopy-->
```

Pour configurer un service générique pour chaque pare-feu à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Dans le volet d'informations, cliquez sur Ajouter.

3. Dans la boîte de dialogue Créer des services, spécifiez les valeurs des paramètres suivants comme indiqué :

   - Nom du service : nom
   - serveur—Nom du serveur

   -* Un paramètre obligatoire

4. Dans Protocole, sélectionnez Tout et dans Port, sélectionnez *.
5. Cliquez sur Créer, puis sur Fermer. Le service que vous avez créé apparaît dans le volet Services.

Configuration d'un moniteur pour chaque service

Un moniteur PING est lié par défaut au service. Vous devrez configurer un moniteur transparent pour surveiller les hôtes du côté approuvé via des pare-feu individuels. Vous pouvez ensuite lier le moniteur transparent aux services. Le moniteur PING par défaut surveille la connectivité uniquement entre l'appliance Citrix ADC et le périphérique en amont. Le moniteur transparent surveille tous les périphériques existants dans le chemin d'accès entre l'appliance et le périphérique qui possède l'adresse IP de destination spécifiée dans le moniteur. Si un moniteur transparent n'est pas configuré et que l'état du pare-feu est UP mais que l'un des périphériques de saut suivants de ce pare-feu est en panne, l'appliance inclut le pare-feu lors de l'équilibrage de charge et transmet le paquet au pare-feu. Cependant, le paquet n'est pas livré à la destination finale car l'un des périphériques de saut suivants est en panne. En liant un moniteur transparent, si l'un des périphériques (y compris le pare-feu) est en panne, le service est marqué comme étant DOWN et le pare-feu n'est pas inclus lorsque l'appliance effectue l'équilibrage de charge du pare-feu.

La liaison d'un moniteur transparent remplace le moniteur PING. Pour configurer un moniteur PING en plus d'un moniteur transparent, après avoir créé et lié un moniteur transparent, vous devez lier un moniteur PING au service.

Pour configurer un moniteur transparent à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

```
1 add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
     transparent (YES | NO )]
2 bind lb monitor <monitorName> <serviceName>
3 <!--NeedCopy-->
```

Exemple :

```
1 add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
2 bind monitor monitor-HTTP-1 fw-svc1
3 <!--NeedCopy-->
```


L'appliance Citrix ADC apprend les paramètres L2 du serveur à partir du moniteur lié au service. Pour les moniteurs UDP-ECV, configurez une chaîne de réception pour permettre à l'appliance d'apprendre les paramètres L2 du serveur. Si la chaîne de réception n'est pas configurée et que le serveur ne répond pas, l'appliance n'apprend pas les paramètres L2, mais le service est défini sur UP. Le trafic de ce service est en trou noir.

Pour configurer une chaîne de réception à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
1 add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
     transparent (YES | NO )] [-send <string>] [-recv <string>]
2 <!--NeedCopy-->
```

Exemple :

```
1 add lb monitor monitor-udp-1 udp-ecv -destip 10.10.10.11 -transparent
     YES  - send "test message"  - recv "site_is_up"
2 <!--NeedCopy-->
```

Pour créer et lier un moniteur transparent à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Moniteurs.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un moniteur, spécifiez les valeurs des paramètres suivants comme indiqué :
   - Nom*
   - Type*—type
   - IP destination
   - Transparent

   -* Un paramètre obligatoire
4. Cliquez sur Créer, puis sur Fermer. Dans le volet Moniteurs, sélectionnez le moniteur que vous venez de configurer et vérifiez que les paramètres affichés en bas de l'écran sont corrects.

Configuration d'un serveur virtuel pour équilibrer la charge du trafic envoyé aux pare-feu

Pour équilibrer la charge n'importe quel type de trafic, vous devez configurer un serveur virtuel générique spécifiant le protocole et le port comme n'importe quelle valeur.

Pour configurer un serveur virtuel pour équilibrer la charge du trafic envoyé aux pare-feu à l'aide de l'interface de lignede commande :

À l'invite de commandes, tapez la commande suivante :


```
add lb vserver <name>@ <serviceType> <IPAddress> <port_number>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Pour configurer un serveur virtuel pour équilibrer la charge du trafic envoyé aux pare-feu à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans Protocole, sélectionnez Tout, et dans Adresse IP et port, sélectionnez *.
4. Cliquez sur Créer, puis sur Fermer. Le serveur virtuel que vous avez créé apparaît dans le volet Serveurs virtuels d'équilibrage de charge.

Configuration du serveur virtuel en mode de réécriture MAC

Pour configurer le serveur virtuel pour utiliser l'adresse MAC pour transférer le trafic entrant, vous devez activer le mode de réécriture MAC.

Pour configurer le serveur virtuel en mode réécriture MAC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

Pour configurer le serveur virtuel en mode réécriture MAC à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, vServer-lb1), puis cliquez sur Ouvrir.
3. Sous l'onglet Avancé, sous le mode Redirection Mode, cliquez sur Ouvrir.
4. Cliquez sur OK.

Liaison des services de pare-feu au serveur virtuel

Pour accéder à un service sur l'appliance Citrix ADC, vous devez le lier à un serveur virtuel générique.

Pour lier des services de pare-feu au serveur virtuel à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
bind lb vserver <name>@ <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier des services de pare-feu au serveur virtuel à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, vServer-lb1), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Services, activez la case à cocher Actif en regard du service que vous souhaitez lier au serveur virtuel (par exemple, Service-HTTP-1).
4. Cliquez sur OK.

Configuration de l'équilibrage de charge multipare-feu sur l'appliance Citrix ADC

Pour équilibrer la charge du trafic des deux côtés d'un Citrix ADC à l'aide de l'équilibrage de charge du pare-feu, vous devez activer l'équilibrage de charge de plusieurs pare-feu à l'aide du paramètre vServerSpecificMac.

Pour configurer l'équilibrage de charge de plusieurs pare-feu à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
set lb parameter -vServerSpecificMac <status>
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -vServerSpecificMac ENABLED
<!--NeedCopy-->
```


Pour configurer l'équilibrage de charge de plusieurs pare-feu à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, Configurer les paramètres d'équilibrage de charge).
3. Dans la boîte de dialogue Définir les paramètres d'équilibrage de charge, activez la case à cocher MAC spécifique au serveur virtuel.
4. Cliquez sur OK.

Enregistrement et vérification de la configuration

Lorsque vous avez terminé les tâches de configuration, veillez à enregistrer la configuration. Vous devez également vérifier que les paramètres sont corrects.

Pour enregistrer et vérifier la configuration à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

- save ns config
- show vserver

Exemple :

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
```



```
23          State: DOWN
24          Last state change was at Thu Jul  8 14:44:51 2010
25          Time since last state change: 0 days, 00:01:50.240
26          Server Name: 10.102.29.5
27          Server ID : 0   Monitor Threshold : 0
28          Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
29          Use Source IP: NO
30          Client Keepalive(CKA): NO
31          Access Down Service: NO
32          TCP Buffering(TCPB): NO
33          HTTP Compression(CMP): NO
34          Idle timeout: Client: 120 sec   Server: 120 sec
35          Client IP: DISABLED
36          Cacheable: NO
37          SC: OFF
38          SP: OFF
39          Down state flush: ENABLED
40
41  1)      Monitor Name: monitor-HTTP-1
42                  State: DOWN     Weight: 1
43                  Probes: 9       Failed [Total: 9 Current: 9]
44                  Last response: Failure - Time out during TCP connection
                        establishment stage
45                  Response Time: 2000.0 millisec
46  2)      Monitor Name: ping
47                  State: UP       Weight: 1
48                  Probes: 3       Failed [Total: 0 Current: 0]
49                  Last response: Success - ICMP echo reply received.
50                  Response Time: 1.275 millisec
51   Done
52  <!--NeedCopy-->
```

Pour enregistrer et vérifier la configuration à l'aide de l'interface graphique :

1. Dans le volet d'informations, cliquez sur Enregistrer.
2. Dans la boîte de dialogue Enregistrer la configuration, cliquez sur Oui.
3. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
4. Dans le volet d'informations, sélectionnez le serveur virtuel que vous avez créé à l'étape 5 et vérifiez que les paramètres affichés dans le volet d'informations sont corrects.
5. Accédez à Gestion du trafic > Équilibrage de charge > Services.
6. Dans le volet d'informations, sélectionnez le service que vous avez créé à l'étape 5 et vérifiez que les paramètres affichés dans le volet d'informations sont corrects.

Surveillance d'une configuration d'équilibrage de charge du pare-feu dans un environnement à pare-feu multiple

Une fois la configuration terminée, vous devez afficher les statistiques de chaque service et serveur virtuel pour vérifier les éventuels problèmes.

Affichage des statistiques d'un serveur virtuel

Pour évaluer les performances des serveurs virtuels ou pour résoudre les problèmes, vous pouvez afficher les détails des serveurs virtuels configurés sur l'appliance Citrix ADC. Vous pouvez afficher un résumé des statistiques pour tous les serveurs virtuels ou spécifier le nom d'un serveur virtuel pour afficher les statistiques uniquement pour ce serveur virtuel. Vous pouvez afficher les détails suivants :

- Nom
- Adresse IP
- Port
- Protocole
- État du serveur virtuel
- Taux de demandes reçues
- Taux de succès

Pour afficher les statistiques du serveur virtuel à l'aide de l'interface de ligne de commande

Pour afficher un résumé des statistiques de tous les serveurs virtuels actuellement configurés sur l'appliance Citrix ADC, ou pour un seul serveur virtuel, à l'invite de commandes, tapez :

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Exemple :

```
>stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
        0/s
Two                          *     0          TCP         DOWN      0/s
        0/s
Three                        *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
```



```
8  BRVSERV            10.10.1.1    80         HTTP          DOWN      0/s
          0/s
9  LBVIP           10.102.29.66    80         HTTP            UP      0/s
          0/s
10  Done
11
12
13 <!--NeedCopy-->
```

Pour afficher les statistiques du serveur virtuel à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Statistiques.
2. Si vous souhaitez afficher les statistiques pour un seul serveur virtuel, dans le volet d'informations, sélectionnez le serveur virtuel, puis cliquez sur Statistiques.

Affichage des statistiques d'un service

Vous pouvez afficher le taux de demandes, de réponses, d'octets de demande, d'octets de réponse, de connexions client actuelles, de demandes dans la file d'attente de surtension, de connexions serveur actuelles, etc. à l'aide des statistiques de service.

Pour afficher les statistiques d'un service à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 stat service <name>
2 <!--NeedCopy-->
```

Exemple :

```
1 stat service Service-HTTP-1
2 <!--NeedCopy-->
```

Pour afficher les statistiques d'un service à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Services > Statistiques.
2. Si vous souhaitez afficher les statistiques pour un seul service, sélectionnez-le, puis cliquez sur Statistiques.

Équilibrage de charge globale des serveurs

August 20, 2021

> **Remarques :**
>
> - À partir de la version 13.0 build 41.x, les déploiements GSLB (Global Server Load Balancing) utilisant l'appliance Citrix ADC sont entièrement conformes au jour de l'indicateur DNS 2019.
> - La fonctionnalité GSLB est incluse avec les licences Citrix ADC Advance et Premium. La licence de l'option Citrix ADC est prise en charge avec l'édition Standard.

Les appliances Citrix ADC configurées pour GSLB assurent la reprise après sinistre et assurent la disponibilité continue des applications en protégeant contre les points de défaillance d'un réseau étendu. GSLB équilibre la charge entre les datacenters en orientant les demandes des clients vers le datacenter le plus proche ou le plus performant, ou vers les datacenters survivants en cas de panne.

Dans une configuration standard, un serveur DNS local envoie des demandes client à un serveur virtuel GSLB, auquel sont liés les services GSLB. Un service GSLB identifie un serveur virtuel d'équilibrage de charge ou de commutation de contenu, qui peut se trouver sur le site local ou un site distant. Si le serveur virtuel GSLB sélectionne un serveur virtuel d'équilibrage de charge ou de commutation de contenu sur un site distant, il envoie l'adresse IP du serveur virtuel au serveur DNS. Le serveur DNS l'envoie au client. Le client envoie ensuite la demande au nouveau serveur virtuel à la nouvelle adresse IP.

Les entités GSLB que vous devez configurer sont les sites GSLB, les services GSLB, les serveurs virtuels GSLB, les serveurs virtuels d'équilibrage de charge ou de commutation de contenu et les services DNS (ADNS) faisant autorité. Vous devez également configurer MEP. Vous pouvez également configurer des vues DNS pour exposer différentes parties de votre réseau aux clients accédant au réseau à partir de différents emplacements.

> **Remarque :**
>
> Pour tirer pleinement parti des fonctionnalités GSLB, utilisez les appliances ADC pour l'équilibrage de charge ou la commutation de contenu dans chaque centre de données, afin que votre configuration GSLB puisse utiliser le MEP propriétaire pour échanger des mesures de site.

Fonctionnement du GSLB

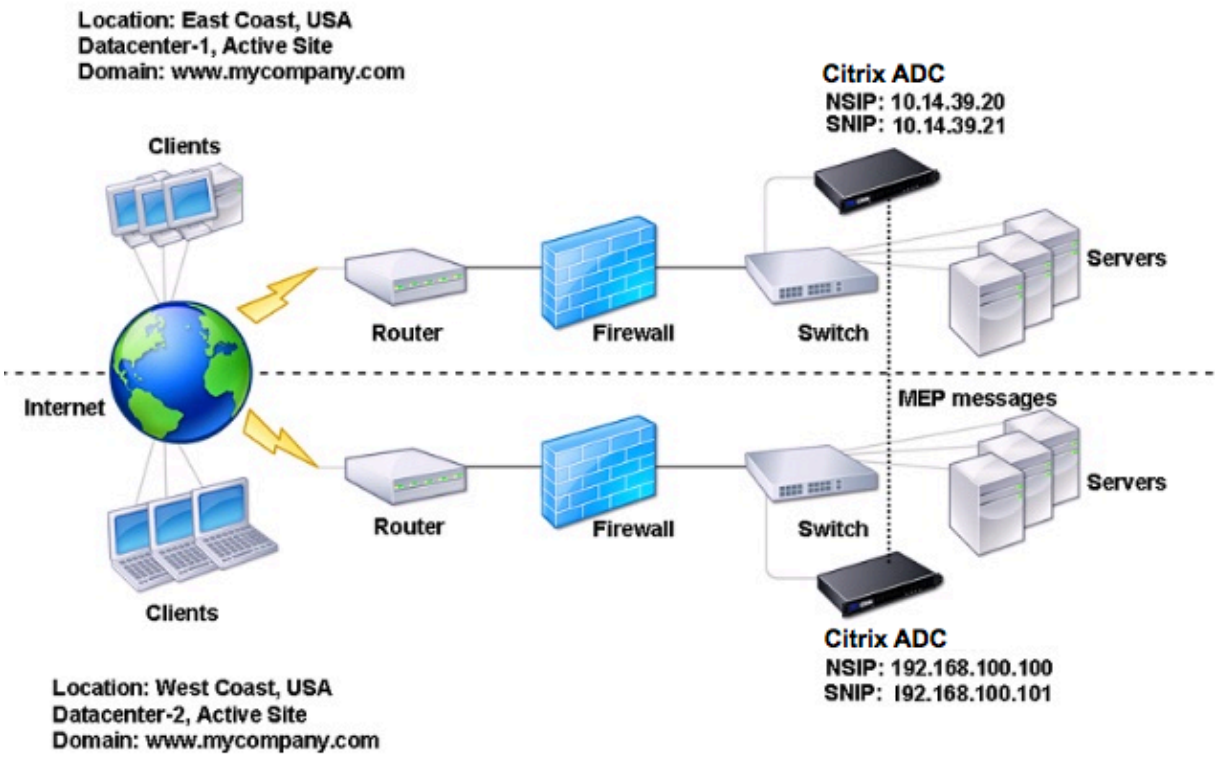
Avec le DNS ordinaire, lorsqu'un client envoie une demande DNS (Domain Name System), il reçoit une liste d'adresses IP du domaine ou du service. Généralement, le client choisit la première adresse IP de la liste et initie une connexion avec ce serveur. Le serveur DNS utilise une technique appelée DNS round robin pour faire pivoter les adresses IP de la liste. Il envoie la première adresse IP à la fin de la liste et promeut les autres après avoir répondu à chaque requête DNS. Cette technique assure une répartition égale de la charge, mais elle ne prend pas en charge la reprise après sinistre, l'équilibrage de charge basé sur la charge ou la proximité des serveurs, ou la persistance.

Lorsque vous configurez GSLB sur des appliances ADC et activez MEP, l'infrastructure DNS est utilisée pour connecter le client au centre de données qui répond le mieux aux critères définis. Les critères peuvent désigner les éléments suivants :

- Centre de données le moins chargé
- Centre de données le plus proche
- Centre de données qui répond le plus rapidement aux demandes provenant de l'emplacement du client
- Combinaison de ces mesures et de ces mesures SNMP.

Une appliance assure le suivi de l'emplacement, des performances, de la charge et de la disponibilité de chaque centre de données. Il utilise ces facteurs pour sélectionner le centre de données à envoyer la demande du client.

La figure suivante illustre une topologie GSLB de base.



Une configuration GSLB consiste en un groupe d'entités GSLB sur chaque appliance de la configuration. Ces entités comprennent les sites GSLB, les services GSLB, les groupes de services GSLB, les serveurs virtuels GSLB, les serveurs d'équilibrage de charge, les serveurs de commutation de contenu et les services ADNS.

Types de déploiement GSLB

January 21, 2021

Les appliances Citrix ADC configurées pour l'équilibrage global de la charge des serveurs (GSLB) assurent la reprise après sinistre et assurent la disponibilité continue des applications en protégeant contre les points de défaillance d'un réseau étendu (WAN). GSLB peut équilibrer la charge entre les datacenters en orientant les demandes des clients vers le datacenter le plus proche ou le plus performant, ou vers les datacenters survivants en cas de panne.

Voici quelques-uns des types de déploiement GSLB typiques :

- Déploiement de site actif-actif
- Déploiement de site actif-passif
- Déploiement de topologie parent-enfant

Déploiement de site actif-actif

August 20, 2021

Un site actif-actif se compose de plusieurs centres de données actifs. Les demandes des clients sont équilibrées de charge entre les datacenters actifs. Ce type de déploiement peut être utilisé lorsque vous avez besoin d'une distribution globale du trafic dans un environnement distribué.

Tous les sites d'un déploiement actif-actif sont actifs, et tous les services d'une application/domaine particulier sont liés au même serveur virtuel GSLB. Les sites échangent des mesures via le protocole MEP (Metrics Exchange Protocol). Les mesures de site échangées entre les sites incluent l'état de chaque serveur virtuel d'équilibrage de charge et de commutation de contenu, le nombre actuel de connexions, le taux actuel de paquets et l'utilisation actuelle de la bande passante. L'appliance Citrix ADC a besoin de ces informations pour effectuer l'équilibrage de charge sur les sites.

Un déploiement actif-actif peut inclure un maximum de 32 sites GSLB, car le MEP ne peut pas synchroniser plus de 32 sites. Aucun site de sauvegarde n'est configuré dans ce type de déploiement.

L'appliance Citrix ADC envoie des demandes client au site GSLB approprié, tel que déterminé par la méthode GSLB spécifiée dans la configuration GSLB.

Pour un déploiement actif-actif, vous pouvez configurer les méthodes GSLB suivantes.

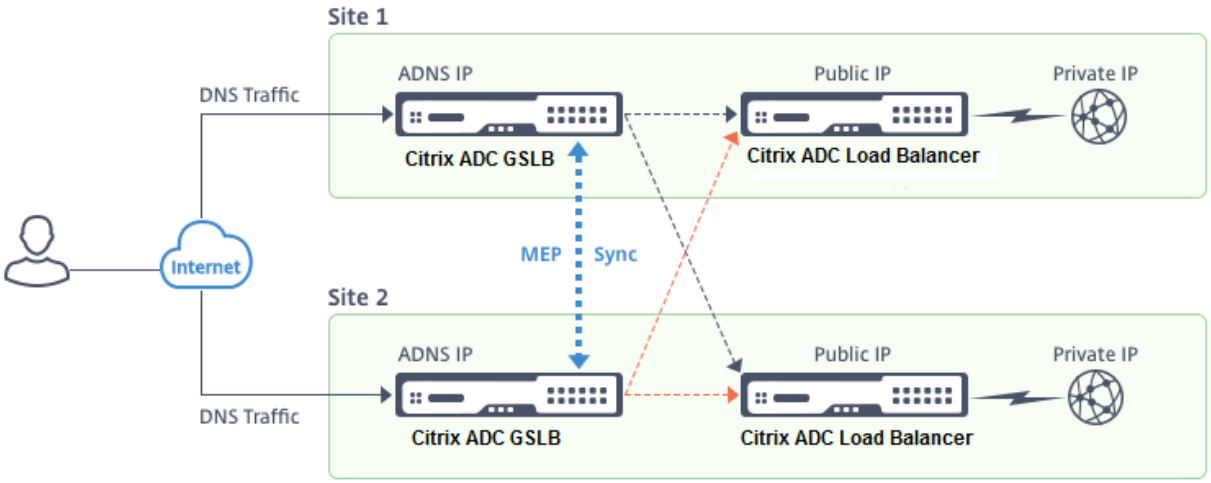
- Round Robin
- Connexions moindres
- Temps de réponse le plus faible
- Moins de bande passante

- Moins de paquets
- Hash IP source
- Chargement personnalisé
- Temps aller-retour (RTT)
- Proximité statique

> Remarque :
>
> - Si MEP est désactivé, les méthodes GSLB suivantes sont par défaut la méthode Round Robin.
>   - RTT
>   - Moins de connexions
>   - Moins de bande passante
>   - Moins de paquets
>   - Temps de réponse minimal
> - Dans la méthode GLSB de proximité statique, l'appliance envoie la demande à l'adresse IP du site qui correspond le mieux aux critères de proximité.
> - Dans la méthode Round Trip Time, les valeurs de temps d'aller-retour dynamique (RTT) sont de sélectionner l'adresse IP du site le plus performant. RTT est une mesure du retard dans le réseau entre le serveur DNS local du client et une ressource de données.

Topologie de centre de données actif-actif GSLB

Dans le diagramme, le site 1 et le site 2 sont des sites actifs de la DGGLSB.



Lorsque le client envoie une requête DNS, il atterrit sur l'un des sites actifs.

Si Site 1 reçoit la demande du client, le serveur virtuel GSLB du Site 1 sélectionne un serveur virtuel d'équilibrage de charge ou de commutation de contenu et envoie l'adresse IP du serveur virtuel au serveur DNS, qui l'envoie au client. Le client renvoyer la demande au nouveau serveur virtuel à la nouvelle adresse IP.

Comme les deux sites sont actifs, l'algorithme GSLB évalue les services sur les deux sites lors d'une sélection déterminée par la méthode GSLB configurée.

Déploiement de site actif-passif

August 20, 2021

Un site actif-passif est constitué d'un centre de données actif et passif. Ce type de déploiement est idéal pour la reprise après sinistre.

Dans ce type de déploiement, certains sites (sites distants) sont réservés uniquement à la reprise après sinistre. Ces sites ne participent à aucune prise de décision tant que tous les sites actifs ne sont pas en panne. Un site passif ne devient opérationnel que si un événement de sinistre déclenche un basculement.

Une fois que vous avez configuré le centre de données principal, répliquez la configuration du centre de données de sauvegarde et désignez-le comme site GSLB passif en désignant un serveur virtuel GSLB sur ce site comme serveur virtuel de sauvegarde.

Un déploiement actif-passif peut inclure un maximum de 32 sites GSLB, car le MEP ne peut pas synchroniser plus de 32 sites.

Pour un déploiement actif-passif, vous pouvez configurer les méthodes GSLB suivantes.

- Round Robin
- Connexions moindres
- Temps de réponse le plus faible
- Moins de bande passante
- Moins de paquets
- Hash IP source
- Chargement personnalisé
- Temps aller-retour (RTT)
- Proximité statique

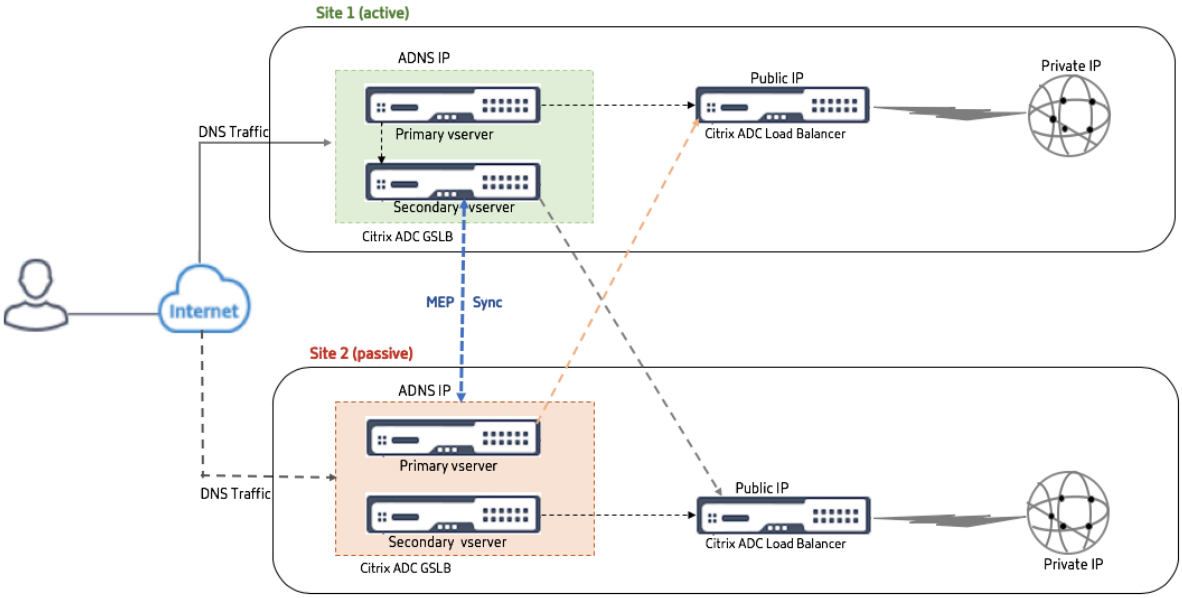
Remarque :

- Si MEP est désactivé, les méthodes d'algorithme suivantes sont par défaut Round Robin.
  - RTT
  - Connexions moindres
  - Moins de bande passante
  - Moins de paquets
  - Temps de réponse le plus faible

- Dans la méthode GLSB de proximité statique, l'appliance envoie la demande à l'adresse IP du site qui correspond le mieux aux critères de proximité.
- Dans la méthode Round Trip Time, les valeurs de temps d'aller-retour dynamique (RTT) sont de sélectionner l'adresse IP du site le plus performant. RTT est une mesure du retard dans le réseau entre le serveur DNS local du client et une ressource de données.

Topologie de centre de données actif-passif GSLB

Dans le diagramme, le site 1 est un site actif et le site 2 est un site passif, dont la configuration est identique à celle du Site 1.



Si le site 1 tombe en panne, le site 2 devient opérationnel.

Lorsque le client envoie une demande DNS, la demande peut atterrir sur n'importe lequel des sites. Cependant, les services sont sélectionnés uniquement à partir du site actif (Site1) tant qu'il est UP.

Les services du site passif (Site 2) ne sont sélectionnés que si le site actif (Site 1) est DOWN.

Déploiement de topologie parent-enfant à l'aide du protocole MEP

August 20, 2021

Citrix ADC GSLB assure l'équilibrage global de la charge des serveurs et la reprise après sinistre en créant des connexions maillées entre tous les sites concernés et en prenant des décisions d'équilibrage de charge intelligentes. Chaque site communique avec les autres pour échanger des

mesures de serveur et réseau via Metric Exchange Protocol (MEP), à intervalles réguliers. Toutefois, avec l'augmentation du nombre de sites homologues, le volume du trafic MEP augmente de façon exponentielle en raison de la topologie de maillage. Pour surmonter cela, vous pouvez utiliser une topologie parent-enfant. La topologie parent-enfant prend également en charge les déploiements plus importants. En plus des 32 sites parents, vous pouvez configurer 1024 sites enfants.

La topologie parent-enfant GSLB est une conception hiérarchique à deux niveaux avec les caractéristiques suivantes :

- Au niveau supérieur, il y a des sites parents, qui entretiennent des relations avec d'autres parents.
- Chaque parent peut avoir plusieurs sites enfants.
- Chaque site parent échange des informations sur la santé avec ses sites enfants et avec d'autres sites parents.
- Un site enfant communique uniquement avec son site parent.
- Dans une relation parent-enfant pour GSLB, seul le site parent répond aux requêtes ADNS. Les sites enfants agissent comme des sites d'équilibrage de charge normaux.
- Configurez un service ADNS ou un serveur virtuel d'équilibrage de charge DNS uniquement dans le site parent.
- Un site parent peut avoir une configuration GSLB normale, c'est-à-dire des services provenant de sites locaux et distants, mais un site enfant ne peut avoir que des services locaux. En outre, seuls les sites parents ont des serveurs virtuels GSLB configurés.

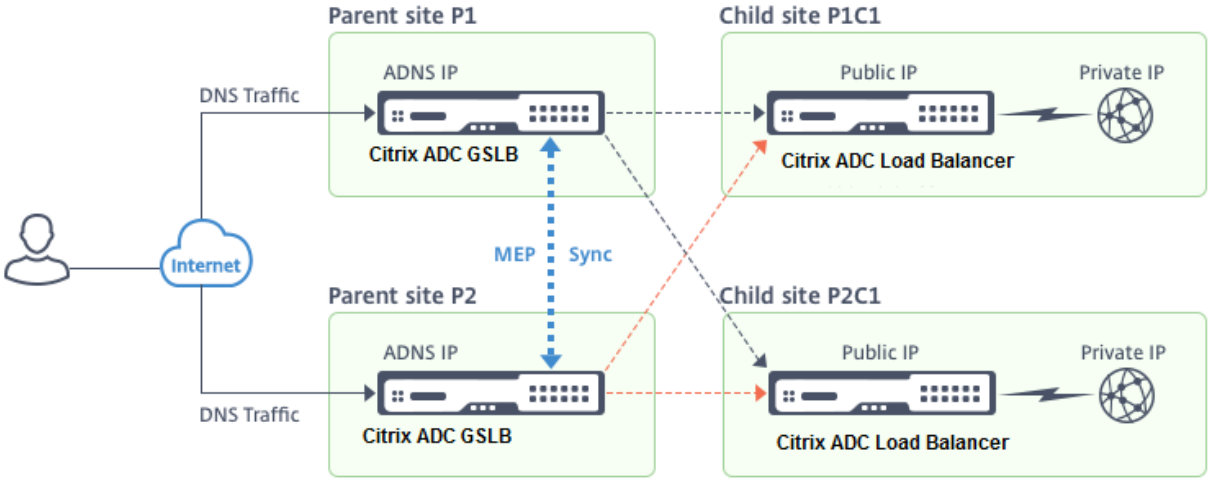
> **Remarque**
>
> - Dans une topologie parent-enfant, l'échange de mesures de site est initié à partir de la plus faible des deux adresses IP. Toutefois, à partir de Citrix ADC version 11.1 build 51.x, les sites parents initient des connexions aux sites enfants, et non de la manière inverse. Parce que les sites parents contiennent des informations sur tous les sites enfants dans la configuration GSLB.

- Dans une connexion parent-parent, l'échange de mesures de site est toujours initié à partir de l'IP inférieure de deux adresses IP.
- Dans une topologie parent-enfant, les services GSLB ne doivent pas toujours être configurés sur un site enfant. Toutefois, si vous disposez d'une configuration plus importante, telle que l'authentification client, l'insertion d'adresse IP du client ou toute autre exigence spécifique à SSL, vous devez ajouter un service GSLB explicite sur le site enfant et le configurer en conséquence.
- Dans une topologie parent-enfant, le site parent et le site enfant peuvent être sur différentes versions du logiciel Citrix ADC. Toutefois, pour utiliser l'option GSLB AutomaticConfigSync pour synchroniser la configuration entre les sites parents, tous les sites parents doivent se trouver sur les mêmes versions du logiciel Citrix ADC. Si vous n'utilisez pas l'option automaticConfigSync,

le site parent et le site enfant peuvent se trouver sur des versions différentes du logiciel ADC Citrix, mais assurez-vous que vous n'utilisez aucune des nouvelles fonctionnalités de la dernière version. Cela s'applique également, en général, à deux nœuds Citrix ADC participant à GSLB.

Topologie parent-enfant de base

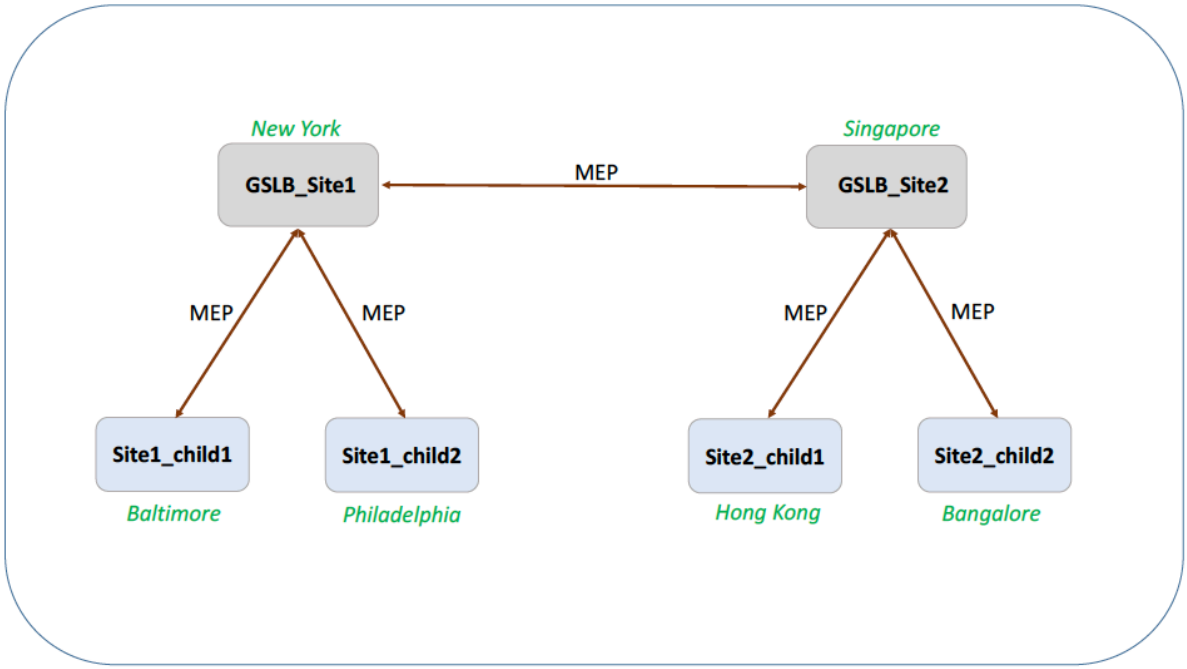
Dans le diagramme, SiteP1 et SiteP2 sont des sites parents dans une relation homologue. Les sites P1C1 et P2C1 sont respectivement les sites enfants de P1 et P2.



Configuration d'une configuration parent-enfant pour GSLB

Si un pare-feu est configuré sur un site GSLB, assurez-vous que le port 3011 est ouvert.

Le diagramme suivant affiche un exemple de configuration parent-enfant.



- La configuration d'un site enfant inclut le site enfant et son site parent, mais aucun autre site parent ou enfant.
- Les mesures réseau, telles que RTT et les informations de session de persistance, sont synchronisées uniquement sur les sites parents. Par conséquent, les paramètres tels que NWMetricExchange et SessionExchange sont désactivés par défaut sur tous les sites enfants.
- Pour vérifier la configuration parent-enfant correcte, vérifiez les états de tous les services GSLB liés aux sites parents.

Pour configurer une configuration parent-enfant pour GSLB à l'aide de l'interface de ligne de commande :

1. Sur chaque site parent, entrez les commandes suivantes :

```
add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
    ipv6_addr|*>]

add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
    ipv6_addr|*>] [-parentSite <string>]
<!--NeedCopy-->
```

Exemple :

```
add gslb site GSLB_Site1 10.1.1.1 - publicIP 10.1.1.1

add gslb site Site1_child1 1 10.1.1.2 -publicIP 10.1.1.2 -
    parentSite GSLB_Site1
<!--NeedCopy-->
```


2. Sur chaque site enfant, entrez les commandes suivantes :

```
add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
   ipv6_addr|*>]

add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
   ipv6_addr|*>] [-parentSite <string>]
<!--NeedCopy-->
```

Exemple :

```
add gslb site GSLB_Site1 10.1.1.1 - publicIP 10.1.1.1

add gslb site Site1_child1 1 10.1.1.2 -publicIP 10.1.1.2 -
   parentSite GSLB_Site1
<!--NeedCopy-->
```

Pour obtenir un exemple complet de configuration parent-enfant, à l'aide de l'interface de ligne de commande, voir Exemple de configuration Parent-Enfant complète, Utilisation de l'interface de ligne de commande

> **Remarque**
>
> Si l'adresse IP du serveur virtuel d'équilibrage de charge est une adresse IP privée et que l'adresse IP publique est différente de cette adresse IP, vous devez configurer un service GSLB pour le serveur virtuel d'équilibrage de charge local sur le site enfant. Ceci est requis pour la collecte de statistiques entre le site parent et le site enfant.
>
> Sur le site enfant, à l'invite de commandes, tapez :
>
> `add gslb service <name> <private IP/lb vserver IP> http 80 -sitename <childsite name> -publicip <public IP of LB vserver>`
>
> **Exemple :**
>
> add gslb service Service-GSLB 192.168.1.3 http 80 -GSLB_Site11 site 11_lb1 172.16.1.1
>
> Où 192.168.1.3 est une adresse IP privée du serveur virtuel d'équilibrage de charge et 172.16.1.1 est une adresse IP publique du serveur virtuel d'équilibrage de charge.

Sauvegarde d'un site parent

Remarque : cette fonctionnalité a été introduite dans Citrix ADC version 11.1 build 51.x. Pour utiliser la topologie du site parent de sauvegarde, assurez-vous que le site parent et les sites enfants sont sur Citrix ADC 11.1 build 51.x et versions ultérieures.

La topologie de site parent de sauvegarde est utile dans les scénarios où de nombreux sites enfants

sont associés à un site parent. Si ce site parent est en panne, tous ses sites enfants deviennent indisponibles. Pour éviter cela, vous pouvez maintenant configurer un site parent de sauvegarde auquel les sites enfants peuvent se connecter si le site parent d'origine est DOWN. Le site parent envoie la liste parent de sauvegarde aux sites enfants via les messages MEP.

Lorsqu'un site parent est DOWN, les autres sites parents de la GSLB savent qu'un site parent particulier est DOWN via MEP car MEP vers ce site parent est DOWN. Les autres sites parents de la configuration GSLB recherchent la chaîne de sauvegarde du parent pair. Le site parent avec la préférence la plus élevée adopte les sites enfants du parent qui est tombé en panne. Le nouveau parent initie ensuite une connexion avec le site enfant. Un site enfant peut accepter ou rejeter la connexion après avoir évalué ses connexions existantes et les informations de la liste de sauvegarde. Il faut quelques secondes pour que le parent de sauvegarde adopte les sites enfants.
Lorsque le site parent d'origine est de nouveau disponible, il tente d'établir des connexions avec ses sites enfants qui ont migré vers un parent différent. Lorsqu'une tentative de connexion réussit, le site enfant est réaffecté à son site parent d'origine.

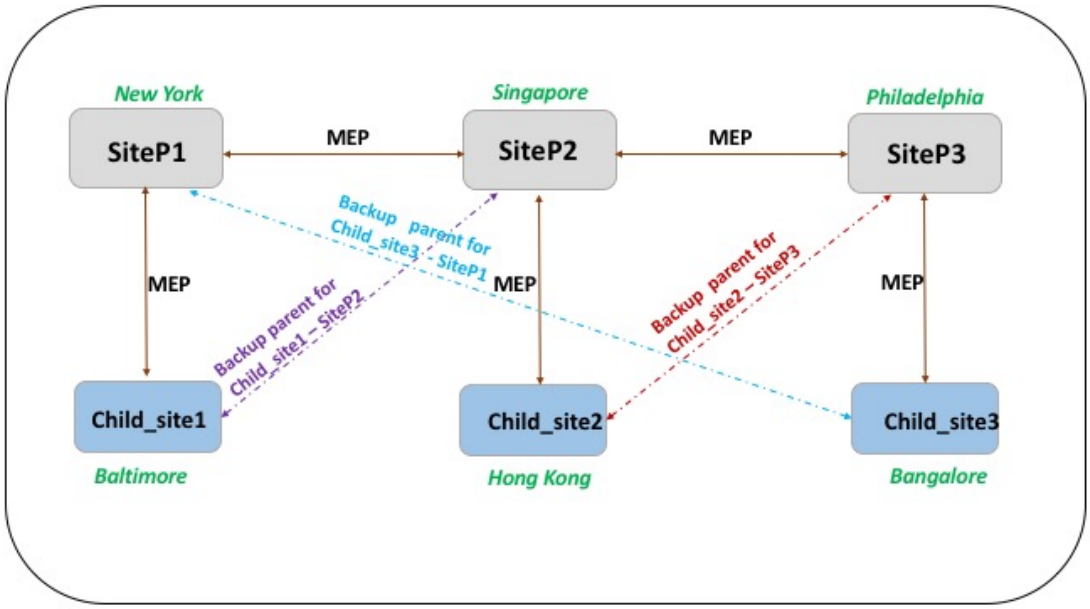
Remarque :

- Seuls les sites parents peuvent être configurés en tant que sauvegardes, et cette configuration ne peut être effectuée que sur le site parent.
- Tous les sites enfants utilisent le jeu parent de sauvegarde.
- La synchronisation est effectuée uniquement sur les sites parents. La configuration des sites enfants GSLB n'est pas affectée par la synchronisation. En effet, les configurations de site parent et de site enfant ne sont pas identiques. La configuration des sites enfants se compose uniquement de ses propres détails et de son site parent. En outre, les services GSLB ne doivent pas toujours être configurés dans les sites enfants.

Considérez la configuration indiquée dans la figure suivante, dans laquelle :

- SiteP1, SiteP2 et SiteP3 sont les sites parents.
- Child_site1, Child_site2 et Child_site3 sont les sites enfants de SiteP1, SiteP2 et SiteP3 respectivement.
- sites parents de sauvegarde ;
  - SiteP1 parents de sauvegarde - SiteP2 (préférence supérieure) et SiteP3
  - SiteP2 parents de sauvegarde — SiteP3 (préférence supérieure) et SiteP1
  - Parents de sauvegarde SiteP3 — SiteP1 (préférence supérieure) et SiteP2

Remarque : Àdes fins d'illustration, la figure ne montre qu'un seul parent de sauvegarde pour chaque site parent.



La liste suivante résume le comportement des sites parents et enfants dans différents scénarios :

- Scénario 1 : SiteP1 est en panne.
  - SiteP2 et SiteP3 détectent que la connexion MEP de SiteP1 est DOWN. SiteP2 est plus élevé dans la liste des préférences des parents de sauvegarde pour SiteP1, de sorte qu'il essaie d'initier une connexion à Child_Site1. SiteP3 suppose que Child_Site1 est désormais le site enfant du site parent SiteP2.
  - SiteP2 envoie Child_Site1 la liste des parents de sauvegarde de SiteP1 (SiteP2 et SiteP3) à Child_Site1. Child_site1 utilise la liste pour décider s'il faut accepter ou rejeter la connexion à partir de SiteP2. Il accepte la connexion et devient un enfant de SiteP2.
  - Lorsque SiteP1 est de nouveau disponible, il envoie Child_Site1 une demande de connexion. La nouvelle demande a priorité et Child_Site 1 migre vers SiteP1.
- Scénario 2 : Seule la connexion MEP entre SiteP1 et SiteP2 est DOWN. Child_site1 rejette la demande de connexion de SiteP2, car son parent, SiteP1, est toujours UP.
- Scénario 3 : SiteP3 et Child_Site1 détectent que SiteP1 est DOWN et que la connexion MEP entre SiteP3 et SiteP2 est également DOWN. Toutefois, SiteP2 détecte que SiteP1 est UP et que la connexion MEP entre SiteP1 et SiteP2 est UP.
  - SiteP2 ne prend aucune action.
  - SiteP3 vérifie la liste de sauvegarde de SiteP1 et constate que SiteP2 a une préférence plus élevée que SiteP3. Mais SiteP2 est DOWN, donc SiteP3 essaie d'établir une connexion avec Child_Site1. Child_site1 a détecté que SiteP1 est DOWN, il accepte donc la demande de connexion de SiteP3.

- Maintenant, la connexion entre SiteP1 et SiteP2 est suspendue. SiteP2 vérifie la liste de sauvegarde de SiteP1 et se trouve comme la sauvegarde la plus préférée. Il essaie donc de se connecter à Child_Site1. Child_site1 évalue la nouvelle demande de connexion en fonction de la liste de SiteP1 et trouve SiteP2 comme sauvegarde préférée, de sorte qu'il migre vers SiteP2 à partir de SiteP3.

Pour configurer un site parent de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb site <sitename> -backupParentlist <bkp_site1> <bkp_site2> ... <
   bkp_site5>
<!--NeedCopy-->
```

<sitename> est le site parent actuel.

Exemple :

Pour le site parent (SiteP1), les sites (SiteP2 et SiteP3) sont configurés en tant que sites parents de sauvegarde.

```
set gslb site SiteP1 -backupParentlist SiteP2 SiteP3
<!--NeedCopy-->
```

Remarque :

- Vous ne pouvez pas ajouter un nouveau site en tant que parent de sauvegarde. Vous devez d'abord ajouter tous les sites, puis configurer le site en tant que parent de sauvegarde.
- Pour supprimer un parent de sauvegarde, vous devez utiliser la commande unset, qui désinstalle tous les sites précédemment configurés en tant que sites parents de sauvegarde.

Pour configurer un site parent de sauvegarde à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Sites** .
2. Ajoutez un nouveau site ou sélectionnez un site existant.
3. Sélectionnez la zone d'option **Sauvegarder les sites parents** lors de la création ou de la configuration du site GSLB.

Entités de configuration GSLB

August 20, 2021

Une configuration GSLB consiste en un groupe d'entités GSLB sur chaque appliance de la configuration. Ces entités sont les suivantes :

- Sites GSLB
- Services GSLB
- Serveurs virtuels GSLB
- Équilibrage de charge ou serveurs virtuels de commutation de contenu
- Services ADNS
- VIP DNS

Sites GSLB

Une configuration GSLB typique se compose de centres de données, dont chacun possède divers matériels réseau pouvant être ou non des appliances Citrix ADC. Les centres de données sont appelés sites GSLB. Chaque site GSLB est géré par une appliance Citrix ADC locale de ce site. Chacune de ces appliances traite son propre site comme le site local et tous les autres sites, gérés par d'autres appliances, comme des sites distants.

Si l'appliance qui gère un site est la seule appliance Citrix ADC dans ce centre de données, le site GSLB hébergé sur cette appliance agit comme un espace réservé comptable à des fins d'audit, car aucune mesure ne peut être collectée. Généralement, cela se produit lorsque l'appliance est utilisée uniquement pour GSLB et que d'autres produits du centre de données sont utilisés pour l'équilibrage de charge ou la commutation de contenu.

Relations entre les sites GSLB

Le concept de sites est au cœur des implémentations de Citrix ADC GSLB. Sauf indication contraire, les sites forment une relation entre eux. Cette relation est utilisée d'abord pour échanger des informations sur l'intégrité, puis pour répartir la charge comme déterminé par l'algorithme sélectionné. Toutefois, dans de nombreuses situations, il n'est pas souhaitable d'établir une relation entre les pairs entre tous les sites du GSLB. Les raisons de ne pas avoir une mise en œuvre de tous les pairs pourraient être ;

- Pour séparer clairement les sites GSLB. Par exemple, pour séparer les sites qui participent à la résolution des requêtes DNS des sites de gestion du trafic.
- Réduire le volume du trafic MEP (Metric Exchange Protocol), qui augmente de manière exponentielle avec un nombre croissant de sites homologues.

Ces objectifs peuvent être atteints en utilisant les sites GSLB parents et enfants.

Services GSLB

Un service GSLB est généralement une représentation d'un serveur virtuel d'équilibrage de charge ou de commutation de contenu, bien qu'il puisse représenter n'importe quel type de serveur virtuel. Le service GSLB identifie l'adresse IP, le numéro de port et le type de service du serveur virtuel. Les services GSLB sont liés aux serveurs virtuels GSLB sur les appliances Citrix ADC qui gèrent les sites GSLB. Un service GSLB lié à un serveur virtuel GSLB dans le même centre de données est local au serveur virtuel GSLB. Un service GSLB lié à un serveur virtuel GSLB dans un centre de données différent est distant de ce serveur virtuel GSLB.

> **Remarque**
>
> Les sites et services sont intrinsèquement liés pour indiquer la proximité entre les deux. Autrement dit, tous les services doivent appartenir à un site et sont supposés être situés au même endroit que le site du GSLB aux fins de proximité. De même, les services et les serveurs virtuels sont liés, de sorte que la logique est liée aux ressources disponibles.

Serveurs virtuels GSLB

Un serveur virtuel GSLB a un ou plusieurs services GSLB qui lui sont liés, et la charge équilibre le trafic entre ces services. Il évalue les méthodes GSLB configurées (algorithmes) pour sélectionner le service approprié auquel envoyer une demande client. Étant donné que les services GSLB peuvent représenter des serveurs locaux ou distants, la sélection du service GSLB optimal pour une requête a pour effet de sélectionner le centre de données qui doit servir la demande client.

Le domaine pour lequel l'équilibrage de charge du serveur global est configuré doit être lié au serveur virtuel GSLB, car un ou plusieurs services liés au serveur virtuel répondront aux demandes faites pour ce domaine.

Contrairement aux autres serveurs virtuels configurés sur une appliance Citrix ADC, un serveur virtuel GSLB ne possède pas sa propre adresse IP virtuelle (VIP).

Équilibrage de charge ou serveurs virtuels de commutation de contenu

Un serveur virtuel d'équilibrage de charge ou de commutation de contenu représente un ou plusieurs serveurs physiques sur le réseau local. Les clients envoient leurs demandes à l'adresse IP virtuelle (VIP) du serveur virtuel d'équilibrage de charge ou de commutation de contenu, et le serveur virtuel équilibre la charge entre les serveurs physiques. Après qu'un serveur virtuel GSLB sélectionne un service GSLB représentant un serveur virtuel d'équilibrage de charge ou de commutation de contenu local ou distant, le client envoie la demande à l'adresse VIP de ce serveur virtuel.

Pour plus d'informations sur l'équilibrage de charge ou les serveurs et services virtuels de commutation de contenu, voir Équilibrage de charge ou commutation de contenu.

Services ADNS

Un service ADNS est un type de service spécial qui répond uniquement aux demandes DNS pour les domaines pour lesquels l'appliance Citrix ADC fait autorité. Lorsqu'un service ADNS est configuré, l'appliance possède cette adresse IP et la publie. Lors de la réception d'une demande DNS par un service ADNS, l'appliance vérifie la présence d'un serveur virtuel GSLB lié à ce domaine. Si un serveur virtuel GSLB est lié au domaine, il est interrogé pour obtenir la meilleure adresse IP à laquelle envoyer la réponse DNS.

VIP DNS

Une adresse IP virtuelle DNS est une adresse IP virtuelle (VIP) qui représente un serveur virtuel DNS équilibrant la charge sur l'appliance Citrix ADC. Les demandes DNS pour les domaines pour lesquels l'appliance Citrix ADC fait autorité peuvent être envoyées à un VIP DNS.

Méthodes GSLB

August 20, 2021

Contrairement aux serveurs DNS traditionnels qui répondent simplement avec les adresses IP des serveurs configurés, une appliance Citrix ADC configurée pour GSLB répond avec les adresses IP des services, comme déterminé par la méthode GSLB configurée. Par défaut, le serveur virtuel GSLB est défini sur la méthode de connexion minimale. Si tous les services GSLB sont en panne, l'appliance répond avec les adresses IP de tous les services GSLB configurés.

Les méthodes GSLB sont des algorithmes que le serveur virtuel GSLB utilise pour sélectionner le service GSLB le plus performant. Une fois le nom d'hôte dans l'adresse Web résolu, le client envoie le trafic directement à l'adresse IP du service résolu.

L'appliance Citrix ADC fournit les méthodes GSLB suivantes :

- Round Robin
- Connexions moindres
- Temps de réponse le plus faible
- Moins de bande passante
- Moins de paquets
- Hash IP source
- Chargement personnalisé
- Temps aller-retour (RTT)
- Proximité statique

Pour que les méthodes GSLB fonctionnent avec un site distant, MEP doit être activé ou les moniteurs explicites doivent être liés aux services distants. Si MEP est désactivé, les méthodes RTT, Moins de connexions, Moins de bande passante, Moins de paquets et Moins de temps de réponse par défaut sont Round Robin.

Les méthodes de proximité statique et d'équilibrage de charge RTT sont spécifiques à GSLB.

Spécification d'une méthode GSLB autre que la proximité statique ou la RTT dynamique

Pour plus d'informations sur la méthode Round Robin, Last Connections, Moindres Temps de réponse, Moins de bande passante, Moins de paquets, Hash IP source ou Charge personnalisée, reportez-vous à la section Équilibrage de charge.

Pour modifier la méthode GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb vserver <name> -lbMethod GSLBMethod
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -lbMethod ROUNDROBIN
<!--NeedCopy-->
```

Pour modifier la méthode GSLB à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez un serveur virtuel GSLB et cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue Configurer le serveur virtuel GSLB, sous l'onglet Méthode et persistance, sous Méthode, sélectionnez une méthode dans la liste Choisir une méthode.
4. Cliquez sur **OK**et vérifiez que la méthode sélectionnée apparaît sous Détails au bas de l'écran.

Algorithmes GSLB

August 20, 2021

L'algorithme suivant est pris en charge pour GSLB.

- **Round Robin** : Lorsqu'un serveur virtuel GSLB est configuré pour utiliser la méthode round robin, il fait pivoter en permanence une liste des services qui lui sont liés. Lorsque le serveur virtuel reçoit une demande, il affecte la connexion au premier service de la liste, puis déplace ce service au bas de la liste.
- **Temps de réponse le moins**élevé : Lorsque le serveur virtuel GSLB est configuré pour utiliser la méthode de temps de réponse le moins élevé, il sélectionne le service avec la valeur la plus faible. Où, valeur la plus basse = connexions actives actuelles X temps de réponse moyen.

  Vous pouvez configurer cette méthode uniquement pour les services HTTP et SSL (Secure Sockets Layer). Le temps de réponse (également appelé Time to First Byte, ou TTFB) est l'intervalle de temps entre l'envoi d'un paquet de requête à un service et la réception du premier paquet de réponse du service. L'appliance NetScaler utilise le code de réponse 200 pour calculer le TTFB.
- **Moins de connexions** : Lorsqu'un serveur virtuel GSLB est configuré pour utiliser l'algorithme GSLB de connexion (ou méthode) le moins important, il sélectionne le service avec le moins de connexions actives. Il s'agit de la méthode par défaut, car, dans la plupart des cas, elle fournit les meilleures performances.
- **Moins de bande passante** : un serveur virtuel GSLB configuré pour utiliser la méthode la plus faible bande passante sélectionne le service qui dessert actuellement le moins de trafic, mesuré en mégabits par seconde (Mbps).
- **Moins de paquets** : Un serveur virtuel GSLB configuré pour utiliser la méthode des paquets les moins sélectionne le service qui a reçu le moins de paquets au cours des 14 dernières secondes.
- **Hash IP source** : Un serveur virtuel GSLB configuré pour utiliser la méthode de hachage IP source utilise la valeur hachée de l'adresse IPv4 ou IPv6 client pour sélectionner un service. Pour diriger toutes les demandes provenant d'adresses IP source appartenant à un réseau particulier vers un serveur de destination spécifique, vous devez masquer l'adresse IP source. Pour les adresses IPv4, utilisez le paramètre netMask. Pour les adresses IPv6, utilisez le paramètre V6NetMaskLength.
- **Charge personnalisée** : l'équilibrage de charge personnalisé est effectué sur les paramètres du serveur tels que l'utilisation du processeur, la mémoire et le temps de réponse. Lors de l'utilisation de la méthode de chargement personnalisée, l'appliance Citrix ADC sélectionne généralement un service qui ne gère aucune transaction active. Si tous les services de la configuration GSLB gèrent des transactions actives, l'appliance sélectionne le service avec la charge la plus faible. Un type spécial de moniteur, connu sous le nom de moniteur de charge, calcule la charge sur chaque service du réseau. Les moniteurs de charge ne marquent pas l'état d'un service, mais ils retirent les services de la décision GSLB lorsque ces services ne sont pas UP.

Pour plus de détails, voir Équilibrage de charge.

Proximité statique

August 20, 2021

La méthode de proximité statique pour GSLB utilise une base de données de proximité statique basée sur l'adresse IP pour déterminer la proximité entre le serveur DNS local du client et les sites GSLB. L'appliance Citrix ADC répond avec l'adresse IP d'un site qui correspond le mieux aux critères de proximité.

Si plusieurs sites GSLB situés à des emplacements géographiques différents servent le même contenu, l'appliance Citrix ADC gère une base de données de plages d'adresses IP et utilise la base de données pour prendre des décisions concernant les sites GSLB vers lesquels diriger les demandes clients entrantes.

Pour que la méthode de proximité statique fonctionne, vous devez soit configurer l'appliance Citrix ADC pour qu'elle utilise une base de données de proximité statique existante remplie via un fichier d'emplacement, soit ajouter des entrées personnalisées à la base de données de proximité statique. Après avoir ajouté des entrées personnalisées, vous pouvez définir leurs qualificatifs d'emplacement. Après avoir configuré la base de données, vous êtes prêt à spécifier la proximité statique comme méthode GSLB.

Pour plus d'informations sur la configuration de la proximité statique, reportez-vous à la section Configuration de la proximité statique.

Méthode de temps aller-retour dynamique

August 20, 2021

Le temps aller-retour dynamique (RTT) est une mesure du temps ou du retard dans le réseau entre le serveur DNS local du client et une ressource de données. Pour mesurer la RTT dynamique, l'appliance Citrix ADC sonde le serveur DNS local du client et recueille des informations de mesure RTT. L'appliance utilise ensuite cette mesure pour prendre sa décision d'équilibrage de charge. L'équilibrage global de charge du serveur surveille l'état en temps réel du réseau et dirige dynamiquement la demande du client vers le centre de données avec la valeur RTT la plus faible.

Lorsque la demande DNS d'un client pour un domaine vient à l'appliance Citrix ADC configurée comme DNS faisant autorité pour ce domaine, l'appliance utilise la valeur RTT pour sélectionner l'adresse IP du site le plus performant pour l'envoyer en réponse à la demande DNS.

L'appliance Citrix ADC utilise différents mécanismes, tels que PING ou demande d'écho ICMP, UDP et TCP pour collecter les mesures RTT pour les connexions entre le serveur DNS local et les sites participants. L'appliance envoie d'abord une sonde ping pour déterminer le RTT. Si la sonde ping échoue,

une sonde DNS UDP est utilisée. Si cette sonde échoue également, l'appliance utilise une sonde TCP DNS.

Ces mécanismes sont représentés sur l'appliance Citrix ADC sous la forme de moniteurs d'équilibrage de charge et sont facilement identifiés grâce à l'utilisation du préfixe « ldns ». Les trois moniteurs, dans leur ordre par défaut, sont :

- `ldns-ping`
- `ldns-dns`
- `ldns-tcp`

Ces moniteurs sont intégrés à l'appliance et sont réglés sur des valeurs par défaut sûres. Mais ils sont personnalisables comme n'importe quel autre moniteur de l'appareil.

Vous pouvez modifier l'ordre par défaut en le définissant explicitement en tant que paramètre GSLB. Par exemple, pour définir l'ordre d'être la requête UDP DNS suivie du PING puis du TCP, tapez la commande suivante :

```
1 set gslb parameter -ldnsprobeOrder DNS PING TCP
2 <!--NeedCopy-->
```

À moins qu'elles n'aient été personnalisées, l'appliance Citrix ADC effectue des sondes UDP et TCP sur le port 53. Toutefois, contrairement aux moniteurs d'équilibrage de charge réguliers, les sondes ne doivent pas fournir des informations RTT valides. Les messages indisponibles du port ICMP, les réinitialisations TCP et les réponses d'erreur DNS, qui constitueraient généralement un échec, sont tous acceptables pour le calcul de la valeur RTT.

Une fois les données RTT compilées, l'appliance utilise le protocole d'échange de mesures propriétaire (MEP) pour échanger des valeurs RTT entre les sites participants. Après avoir calculé les mesures RTT, l'appliance trie les valeurs RTT pour identifier le datacenter avec la meilleure (la plus petite) mesure RTT.

Si les informations RTT ne sont pas disponibles (par exemple, lorsque le serveur DNS local d'un client accède au site pour la première fois), l'appliance Citrix ADC sélectionne un site à l'aide de la méthode round robin et dirige le client vers le site.

Pour configurer la méthode dynamique, vous configurez le serveur virtuel GSLB du site pour RTT dynamique. Vous pouvez également définir l'intervalle auquel les serveurs DNS locaux sont sondés à une valeur autre que la valeur par défaut.

Configurer un serveur virtuel GSLB pour RTT dynamique

Pour configurer un serveur virtuel GSLB pour RTT dynamique, spécifiez la méthode d'équilibrage de charge RTT.

L'appliance Citrix ADC valide régulièrement les informations de synchronisation pour un serveur local donné. Si une modification de la latence dépasse le facteur de tolérance configuré, l'appliance met à jour sa base de données avec les nouvelles informations de synchronisation et envoie la nouvelle valeur à d'autres sites GSLB en effectuant un échange MEP. Le facteur de tolérance par défaut est de 5 millisecondes (ms).

Le facteur de tolérance RTT doit être le même dans tout le domaine GSLB. Si vous le modifiez pour un site, vous devez configurer des facteurs de tolérance RTT identiques sur toutes les appliances Citrix ADC déployées dans le domaine GSLB.

Pour configurer un serveur virtuel GSLB pour RTT dynamique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb vserver <name> -lbMethod RTT -tolerance <value>
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -lbMethod RTT -tolerance 10
<!--NeedCopy-->
```

Pour configurer un serveur virtuel GSLB pour RTT dynamique à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel.

Définir l'intervalle de sondage des serveurs DNS locaux

L'appliance Citrix ADC utilise différents mécanismes, tels que PING ou demande d'écho ICMP, TCP et UDP pour obtenir des mesures RTT pour les connexions entre le serveur DNS local et les sites GSLB participants. Par défaut, l'appliance utilise un moniteur ping et sonde le serveur DNS local toutes les 5 secondes. L'appliance attend ensuite 2 secondes pour la réponse. Si une réponse n'est pas reçue pendant ce temps, elle utilise le moniteur DNS TCP pour sonder.

Toutefois, vous pouvez modifier l'intervalle de temps pour l'exploration du serveur DNS local afin de tenir compte de votre configuration.

Pour modifier l'intervalle de sondage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set lb monitor <monitorName> <type> -interval <integer> <units> -
    resptimeout <integer> <units>
<!--NeedCopy-->
```

Exemple :

```
set lb monitor ldns-tcp LDNS-TCP -interval 10 sec -resptimeout 5 sec
<!--NeedCopy-->
```

Pour modifier l'intervalle de sondage à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**, puis double-cliquez sur le moniteur que vous souhaitez modifier (par exemple, ping).

Méthode API

August 20, 2021

Vous pouvez utiliser la méthode API pour déterminer le service GSLB le plus performant. La méthode API pour GSLB utilise une API REST pour déterminer le service GSLB le plus performant.

Dans la méthode API, lorsque GSLB reçoit une demande DNS d'un client, il évalue la demande par rapport à la règle spécifiée. Si GSLB rencontre l'expression de légende HTTP, SYS.HTTP_CALLOUT (<name>), il appelle une requête d'API REST à un agent de légende HTTP. GSLB utilise la réponse de l'agent de légende HTTP pour décider du service le plus performant. Dans la réponse DNS, GSLB renvoie l'adresse IP du service le plus performant, au client.

Pour configurer une méthode d'API GSLB à l'aide de l'interface de ligne de commande

Effectuez les opérations suivantes pour configurer la méthode d'API GSLB :

1. Configurez une légende HTTP.

   Pour plus d'informations, voir Configuration d'une légende HTTP.

   À l'invite de commandes, tapez :

   ```
   add policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-
       port <port>] [-vServer <string>] [-returnType <returnType>] [-
       httpMethod (GET | POST)] [-hostExpr <string>] [-urlStemExpr <
       string>] [-headers <name(value)> ...] [-parameters <name(value)
       > ...] [-bodyExpr <string>] [-fullReqExpr <string>] [-scheme (
   ```



```
    http | https)] [-resultExpr <string>] [-cacheForSecs <secs>] [-
    comment <string>]
<!--NeedCopy-->
```

Exemple :

```
add policy httpCallout GSLB_Method_API -IPAddress 208.111.39.237 -
    port 443 -returnType TEXT -hostExpr  "\" hopx.gslb.com\ ""  -
    urlStemExpr  "\" /zones/1/customers/92395/apps/6/decision\ ""
    -headers Authorization( "Basic 19fbe6db-4332-4e3f-a8bc-
    ee47bdc726f8") -parameters ip(DNS.REQ.OPT.ECS.IP.
    TYPECAST_TEXT_T ALT CLIENT.IP.SRC.TYPECAST_TEXT_T) -scheme
    https -resultExpr  "HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).
    XPATH_JSON(xp%/providers/Val[1]/provider%)"  -cacheForSecs 30
<!--NeedCopy-->
```

2. Spécifiez la méthode API pour l'équilibrage de charge. GSLB évalue la demande DNS par rapport à la règle spécifiée.

   À l'invite de commandes, tapez :

```
add gslb vserver <name> <serviceType>  [-lbMethod <lbMethod>] [-
    backupLBMethod <backupLBMethod>] -rule <expression>
<!--NeedCopy-->
```

   Exemple :

```
add gslb vserver vs1 HTTP -lbMethod API -backupLBMethod ROUNDROBIN
     -rule  "sys.http_callout(GSLB_Method_API)"
<!--NeedCopy-->
```

Exemple de configuration pour intégrer GSLB et ITM à l'aide de l'API comme méthode LB

Cette configuration permet à GSLB d'utiliser les aspects de visibilité Internet de Citrix Intelligent Traffic Management (ITM) pour déterminer le service GSLB le plus performant.

```
/* Enable ns features */

enable ns feature lb gslb cs

/* This is a named expression that is used in the HTTP callout, used
    for result expression. */

```



```
add policy expression exp1 "HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).XPATH_JSON(xp%/providers/Val[1]/provider%)"

/* This is a named expression that is used in HTTP callout, used for host expression. */

add policy expression exp2 ""hopx.cedexis.com""

/* This is the HTTP callout configured to request the ITM for the GSLB decision. */

add policy httpCallout ITM_OpenMix_API -IPAddress 208.111.39.237 -port 80 -returnType TEXT -hostExpr exp2 -urlStemExpr ""/zones/1/customers/61770/apps/3/decision"" -headers Authorization("Basic a310697a-1d69-48bf-8f36-55742a8e894e") -parameters ip(DNS.REQ.OPT.ECS.IP.TYPECAST_TEXT_T ALT CLIENT.IP.SRC.TYPECAST_TEXT_T) -scheme http -resultExpr exp1 -cacheForSecs 30

/* Add service 1 */
add service sg1 98.136.103.24 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

/* Add service 2 */
add service sg2 172.217.194.113 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

/* Add ADNS service */

add service adns1 10.102.217.106 ADNS 53 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport NO -sp OFF -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO

/* Add lb vserver 1 for service 1 */
add lb vserver lbvs1 HTTP 10.102.217.116 80 -persistenceType NONE -cltTimeout 180

/* Add lb vserver 2 for service 2 */
add lb vserver lbvs2 HTTP 10.102.217.117 80 -persistenceType NONE -cltTimeout 180

/* Bind service 1 to lb vserver 1 */

bind lb vserver lbvs1 sg1
```



```
36
37 /* Bind service 2 to lb vserver 2 */
38
39 bind lb vserver lbvs2 sg2
40
41 /* Configure API GSLB method on GSLB virtual server to call the HTTP
      callout. This HTTP callout requests the ITM for the GSLB decision
      and returns GSLB service name, which should serve the request. */
42
43 add gslb vserver vs1 HTTP -lbMethod API -backupLBMethod ROUNDROBIN -
      rule "sys.http_callout(ITM_OpenMix_API)" -tolerance 0
44
45 /* Add GSLB site */
46
47 add gslb site site1 10.102.217.106 -publicIP 10.102.217.106
48
49 /* Add GSLB service 1 */
50
51 add gslb service aws_ec2_ap_south_1_asia_pacific_mumbai_1
      10.102.217.116 HTTP 80 -publicIP 10.102.217.116 -publicPort 80 -
      maxClient 0 -siteName site1 -sitePersistence HTTPRedirect -
      sitePrefix gs2. -cltTimeout 180 -svrTimeout 360 -downStateFlush
      ENABLED
52
53 /* Add GSLB service 2 */
54
55 add gslb service aws_ec2_ap_south_1_asia_pacific_mumbai 10.102.217.117
      HTTP 80 -publicIP 10.102.217.117 -publicPort 80 -maxClient 0 -
      siteName site1 -sitePersistence HTTPRedirect -sitePrefix gs1. -
      cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
56
57 /* Bind the GSLB service 1 to GSLB server 1 */
58 bind gslb vserver vs1 -serviceName
      aws_ec2_ap_south_1_asia_pacific_mumbai_1
59
60 /* Bind the GSLB service 2 to GSLB server 2 */
61 bind gslb vserver vs1 -serviceName
      aws_ec2_ap_south_1_asia_pacific_mumbai
62
63 /* Bind a domain name to the GSLB virtual server */
64 bind gslb vserver vs1 -domainName testruchit104.com -TTL 5
65
66 <!--NeedCopy-->
```


Configurer la proximité statique

January 21, 2021

Pour que la méthode de proximité statique fonctionne, vous devez soit configurer l'appliance Citrix ADC pour qu'elle utilise une base de données de proximité statique existante remplie via un fichier d'emplacement, soit ajouter des entrées personnalisées à la base de données de proximité statique. Après avoir ajouté des entrées personnalisées, vous pouvez définir leurs qualificatifs d'emplacement. Après avoir configuré la base de données, vous êtes prêt à spécifier la proximité statique comme méthode GSLB.

Ce document contient les renseignements suivants :

- Ajout d'un fichier d'emplacement pour créer une base de données de proximité statique
- Ajout d'entrées personnalisées à une base de données de proximité statique
- Définition des qualificatifs d'emplacement
- Spécification de la méthode de proximité
- Synchronisation de la base de données de proximité statique GSLB

Ajouter un fichier d'emplacement pour créer une base de données de proximité statique

August 20, 2021

Une base de données de proximité statique est un fichier ASCII basé sur UNIX. Les entrées ajoutées à cette base de données à partir d'un fichier d'emplacement sont appelées entrées statiques. Un seul fichier d'emplacement peut être chargé sur une appliance Citrix ADC. L'ajout d'un nouveau fichier d'emplacement remplace le fichier existant. Le nombre d'entrées dans la base de données de proximité statique est limité par la mémoire configurée dans l'appliance Citrix ADC.

La base de données de proximité statique peut être créée au format par défaut ou dans un format dérivé de bases de données tierces configurées commercialement (telles que www.maxmind.com et www.ip2location.com).

L'appliance Citrix ADC comprend les deux fichiers de base de données de géolocalisation IP suivants. Ce sont des fichiers GeoLite2, publiés par MaxMind.

- Citrix_Netscaler_InBuilt_GeoIP_DB_IPv4
- Citrix_Netscaler_InBuilt_GeoIP_DB_IPv6

Ces fichiers de base de données sont disponibles dans un format pris en charge par l'appliance Citrix ADC dans le répertoire /var/netscaler/inbuilt_db.

Vous pouvez utiliser ces bases de données de géolocalisation IP comme fichier d'emplacement pour la méthode GSLB basée sur la proximité statique ou dans des stratégies basées sur l'emplacement.

Ces bases de données varient dans les détails qu'elles fournissent. Il n'y a pas d'application stricte du format de fichier de base de données, sauf que le fichier par défaut comporte des balises de format. Les fichiers de base de données sont des fichiers ASCII qui utilisent une virgule comme séparateur de champ. Il existe des différences dans la structure des champs et la représentation des adresses IP dans les emplacements.

Le paramètre format décrit la structure du fichier à l'appliance Citrix ADC. La spécification d'une valeur incorrecte pour l'option de format peut endommager les données internes.

> **Remarque**
>
> - Après une mise à niveau, si le répertoire /var/netscaler/inbuilt_db/ contient le fichier de base de données (Citrix_Netscaler_inbuilt_geoip_db.csv) des versions antérieures du logiciel Citrix ADC, le fichier est conservé.
> - L'emplacement par défaut du fichier de base de données est /var/netscaler/locdb, et sur une configuration haute disponibilité (HA), une copie identique du fichier doit être présente au même emplacement sur les deux appliances Citrix ADC.
> - Si le fichier d'emplacement est stocké dans un emplacement autre que l'emplacement par défaut, spécifiez le chemin d'accès du fichier d'emplacement.
> - Pour les partitions d'administration, le chemin par défaut est : /var/partitions/<partitionName>/netscaler/locdb.
> - Certaines bases de données fournissent des noms de pays courts selon la norme ISO-3166 et des noms de pays longs également. Citrix ADC utilise des noms courts lors du stockage et de la correspondance de qualificatifs.
> - Pour créer une base de données de proximité statique, ouvrez une session sur le shell UNIX de l'appliance Citrix ADC et utilisez un éditeur pour créer un fichier avec les détails d'emplacement dans l'un des formats pris en charge par Citrix ADC.

Pour ajouter un fichier d'emplacement statique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add locationFile <locationFile> [-format <format>]
-  show locationFile
<!--NeedCopy-->
```

Exemple :


```
add locationFile /var/netscaler/locdb/nsgeo1.0 -format netscaler
Done

show locationFile
Location File: /var/netscaler/locdb/nsgeo1.0
Format: netscaler
 Done
>
<!--NeedCopy-->
```

Exemple :

```
add locationFile /var/netscaler/inbuilt_db/
   Citrix_Netscaler_InBuilt_GeoIP_DB_IPv4 -format netscaler

add locationFile6 /var/netscaler/inbuilt_db/
   Citrix_Netscaler_InBuilt_GeoIP_DB_IPv6 -format netscaler
<!--NeedCopy-->
```

Pour ajouter un fichier d'emplacement statique à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Emplacement**, cliquez sur l'onglet **Base de données statique**.
2. Cliquez sur **Ajouter** pour ajouter un fichier d'emplacement statique.

Vous pouvez afficher une base de données de fichiers d'emplacement importée à l'aide de la boîte **de dialogue Afficher la base** de données de l'utilitaire de configuration. Il n'y a pas d'équivalent CLI.

Pour afficher un fichier d'emplacement statique à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Emplacement**, cliquez sur l'onglet **Base de données statique**.
2. Sélectionnez un fichier d'emplacement statique et, dans la liste **Action**, cliquez sur **Afficher la base de données** .

Pour convertir un fichier d'emplacement au format Citrix ADC :

Par défaut, lorsque vous ajoutez un fichier d'emplacement, il est enregistré au format Citrix ADC. Vous pouvez convertir un fichier d'emplacement d'autres formats au format Citrix ADC.

> **Remarque** : L'option nsmap est accessible uniquement à partir de l'interface de ligne de commande. La conversion n'est possible qu'au format Citrix ADC.

Pour convertir le format de base de données statique, à l'invite CLI, tapez la commande suivante :

```
nsmap -f <inputFileFormat> -o <outputFileName> <inputFileName>
<!--NeedCopy-->
```


Exemple :

```
1  nsmap -f ip-country-region-city -o nsfile.ns ip-country-region-city.
      csv
2 <!--NeedCopy-->
```

Script pour convertir le format de base de données Maxmind GeoLite2 au format de base de données Citrix ADC

La base de données MaxMind GeoIP ne peut pas être utilisée directement dans Citrix ADC. La base de données MaxMind GeoIP doit être convertie au format Citrix ADC, puis chargée pour la détection de localisation IP dans la méthode de proximité statique GSLB et d'autres fonctionnalités telles que les stratégies.
Vous pouvez utiliser un script pour convertir le format de base de données GeoLite2 au format de base de données Citrix ADC. Ce script peut être utilisé pour convertir les fichiers IPv4 et IPv6.
Le script est disponible à l'emplacement :https://github.com/citrix/MaxMind-GeoIP-Database-Conversion-Citrix-ADC-Format

Étapes pour convertir la base de données GeoIP2 au format Citrix ADC

1. Téléchargez la base de données GeoLite2 City ou GeoLite2 Country au format .csv à partir dehttps://dev.maxmind.com/geoip/geoip2/geolite2/.
2. Copiez le fichier dans un répertoire Citrix ADC (disons /var). Décompressez le fichier à l'aide de la commande shell suivante, qui créerait un répertoire portant le même nom.

   ```
   tar -xf <filename>
   ```

3. Téléchargez le script Convert_GeoIPDB_TO_NetScaler_Format.pl à partir dehttps://github.com/citrix/MaxMind-GeoIP-Database-Conversion-Citrix-ADC-Format et copiez-le dans le répertoire créé à l'étape #2.
4. Pour vérifier les options acceptables pour l'exécution du script, exécutez la commande suivante :

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl -help
   ```

   Diverses options sont disponibles :

   - Fichier de sortie<filename> IPv4. Nom du fichier de sortie par défaut : NetScaler_Maxmind_GeoIP_db
   - Fichier de sortie-p <filename> IPv6. Nom du fichier de sortie par défaut : NetScaler_Maxmind_GeoIP
   - -logfile <filename> Fichier contenant la liste des événements/messages
   - -debug Imprime tous les messages sur STDOUT

5. Exécutez la commande suivante pour convertir le format de base de données GeoLite2 au format de base de données Citrix ADC.

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl
   ```

   > **Remarque :** L'opération peut prendre jusqu'à 5 minutes.

   Les noms de fichiers par défaut utilisés dans le script sont ceux de la base de données basée sur Maxmind GeoLite2 City. Si vous avez téléchargé la base de données GeoLite2 Country, vous devez fournir les noms de fichiers d'entrée en conséquence comme indiqué dans la liste.

   - `-b <filename>` nom du fichier bloc IPv4 à convertir. Nom du fichier par défaut : GeoLite2-City-blocks-IPv4.csv
   - `-i <filename>` nom du fichier bloc IPv6 à convertir. Nom du fichier par défaut : GeoLite2-City-blocks-IPv6.csv
   - `-l <filename>` nom du fichier d'emplacement à convertir. Nom du fichier par défaut : Geolite2-City-locations-fr.csv

   Exemple :

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl -b GeoLite2-Country-Blocks-IPv4.csv -i GeoLite2-Country-Blocks-IPv6.csv -l GeoLite2-Country-Locations-en.cs
   <!--NeedCopy-->
   ```

   Voici les fichiers de sortie générés après l'exécution du script.

   - Netscaler_Maxmind_GeoIP_DB_IPv4.csv
   - Netscaler_Maxmind_GeoIP_DB_IPv6.csv

6. Une fois la conversion de la base de données au format Citrix ADC terminée, utilisez la commande suivante pour commencer à l'utiliser.

   ```
   add locationFile <locationFile>
   ```

Ajouter un fichier de base de données statique tiers sur une appliance Citrix ADC

Procédez comme suit pour ajouter un fichier de base de données statique tiers sur une appliance Citrix ADC.

1. Obtenez le fichier de base de données d'emplacement auprès d'un fournisseur tiers, tel que www.maxmind.com ou www.ip2location.com.
2. Copiez le fichier de base de données d'emplacement sur l'appliance Citrix ADC à l'aide de l'utilitaire WinSCP.

> **Remarque**
>
> L'emplacement par défaut du fichier de base de données sur l'appliance est **/var/netscaler/locdb**.

3. Exécutez la commande suivante pour ajouter un fichier d'emplacement statique :

```
add location file <locationfile Name> -format LocationFormat
<!--NeedCopy-->
```

4. Exécutez la commande suivante pour vous assurer que la base de données d'emplacement est chargée :

```
show location parameter
<!--NeedCopy-->
```

Cette commande affiche les paramètres, tels que le nombre d'entrées statiques. Si la base de données n'est pas chargée correctement, cette commande affiche également un message d'erreur. Un maximum de 3M-1 (3 millions moins une) entrées peuvent être chargées.

5. Exécutez la commande suivante pour afficher l'emplacement du site GSLB :

```
show gslb service
<!--NeedCopy-->
```

> **Remarque**
>
> ```
> -  Si la base de données est chargée correctement, l'
>    emplacement des sites GSLB est automatiquement renseigné
>    dans la base de données.
> ```
>
> - Vous ne pouvez spécifier qu'un seul fichier d'emplacement dans la configuration de l'appliance.
> - Si les appliances sont dans une configuration haute disponibilité, une appliance doit copier la base de données à partir de l'autre appliance.
> - Si aucune correspondance n'est trouvée pour une adresse IP entrante, la demande est traitée à l'aide de la méthode Round Robin.

6. Exécutez la commande suivante pour configurer la méthode GSLB sur l'appliance :

```
set gslb vserver GSLBVserverName -lbMethod MethodType
<!--NeedCopy-->
```


Ajouter des entrées personnalisées à une base de données de proximité statique

August 20, 2021

Les entrées personnalisées ont priorité sur les entrées statiques dans la base de données de proximité. Vous pouvez ajouter un maximum de 500 entrées personnalisées. Pour une entrée personnalisée, indiquez tous les qualificatifs omis avec un astérisque (*) et, si les qualificatifs ont un point ou un espace dans le nom, placez le paramètre entre guillemets doubles. Les 31 premiers caractères sont évalués pour chaque qualificatif. Vous pouvez également fournir la longitude et la latitude de l'emplacement géographique de la plage d'adresses IP pour sélectionner un service avec la méthode GSLB de proximité statique.

Pour ajouter des entrées personnalisées à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter une entrée personnalisée à la base de données de proximité statique et vérifier la configuration :

```
add location < IPfrom> < IPto> <preferredLocation> [-longitude <integer
   >[-latitude <integer>]]
show location
<!--NeedCopy-->
```

Exemple :

```
>add location 192.168.100.1 192.168.100.100 *.us.ca.mycity
<!--NeedCopy-->
```

```
>show location
<!--NeedCopy-->
```

Paramètres d'ajout d'entrées personnalisées

- IPFrom

  Première adresse IP dans la plage, en notation décimale pointillée. Il s'agit d'un argument obligatoire.

- IPto

  Dernière adresse IP de la plage, en notation décimale pointillée. Il s'agit d'un argument obligatoire.

- preferredLocation

  Chaîne de qualificatifs, en notation pointillée, décrivant l'emplacement géographique de la plage d'adresses IP. Chaque qualificatif est plus spécifique que celui qui le précède, comme dans continent.country.region.city.isp.organization. Par exemple, "na.us.ca.San Jose.att.Citrix ».

  Note : Un qualificatif qui inclut un point (.) ou un espace () doit être placé entre guillemets doubles.

  Il s'agit d'un argument obligatoire. Longueur maximale : 197

- longitude

  Valeur numérique, en degrés, spécifiant la longitude de l'emplacement géographique de la plage d'adresses IP.

  Remarque : Les paramètres de longitude et de latitude sont utilisés pour sélectionner un service avec la méthode GSLB de proximité statique. S'ils ne sont pas spécifiés, la sélection est basée sur les qualificatifs spécifiés pour l'emplacement.

  Valeur maximale : 180

- latitude

  Valeur numérique, en degrés, spécifiant la latitude de l'emplacement géographique de la plage d'adresses IP.

  Remarque : Les paramètres de longitude et de latitude sont utilisés pour sélectionner un service avec la méthode GSLB de proximité statique. S'ils ne sont pas spécifiés, la sélection est basée sur les qualificatifs spécifiés pour l'emplacement.

  Valeur maximale : 180

Pour ajouter des entrées personnalisées à l'aide de l'utilitaire de configuration

Accédez à **AppExpert** > **Emplacement**, cliquez sur l'onglet **Entrées personnalisées** et ajoutez les entrées personnalisées.

Définir les paramètres de localisation

October 5, 2021

La base de données utilisée pour implémenter la proximité statique contient l'emplacement des sites GSLB. Chaque emplacement contient une plage d'adresses IP et jusqu'à six qualificatifs pour cette

plage. Les qualificatifs sont des chaînes littérales et sont comparés dans un ordre prescrit au moment de l'exécution. Chaque emplacement doit comporter au moins un qualificatif. Les étiquettes de qualificatifs définissent la signification des qualificatifs (contexte), qui sont définis par l'utilisateur. Citrix ADC dispose de deux contextes intégrés :

Contexte géographique, qui comporte les libellés de qualificateurs suivants :

- Qualificateur 1 — « Continent »
- Qualificateur 2 — « Pays »
- Qualificateur 3 — « État »
- Qualificateur 4 — « Ville »
- Qualificateur 5 — « FAI »
- Qualificateur 6 — « Organisation »

Entrées personnalisées, qui comportent les étiquettes de qualificateur suivantes :

- Qualificateur 1 — « Qualifier 1 »
- Qualificateur 2 — « Qualifier 2 »
- Qualificateur 3 — « Qualifier 3 »
- Qualificateur 4 — « Qualifier 4 »
- Qualificateur 5 — « Qualifier 5 »
- Qualificateur 6 — « Qualifier 6 »

Si le contexte géographique est défini sans qualificateur de continent, Continent est dérivé de Country. Même les libellés de qualificatifs intégrés sont basés sur le contexte, et les étiquettes peuvent être modifiées. Ces étiquettes de qualificatifs spécifient les emplacements mappés avec les adresses IP utilisées pour prendre des décisions de proximité statiques.

Pour prendre une décision statique basée sur la proximité, l'appliance Citrix ADC compare les attributs d'emplacement (qualificatifs) dérivés de l'adresse IP du résolveur de serveur DNS local avec les attributs d'emplacement des sites participants. Si un seul site correspond, la solution matérielle-logicielle renvoie l'adresse IP de ce site. S'il y a plusieurs correspondances, le site sélectionné est le résultat d'un tournoi à la ronde sur les sites GSLB correspondants. S'il n'y a pas de correspondance, le site sélectionné est le résultat d'un tourniquet sur tous les sites configurés. Un site qui n'a pas de qualificatifs est considéré comme une correspondance.

Les règles GEO pour l'expression de stratégie basée sur l'emplacement vous permettent de vérifier les correspondances avec des caractères génériques. Cette fonctionnalité vérifie si les qualificatifs génériques correspondent à n'importe quel autre qualificatif, y compris non générique ou non. La correspondance avec caractères génériques est effectuée à l'aide de l'`matchWildcardtoany` attribut ajouté à la `set locationParameter` commande.

L'`matchWildcardtoany` attribut peut être défini sur les valeurs suivantes :

- **Oui :** les qualificatifs Wildcard correspondent à tous les autres qualificatifs.

- **Non :** les qualificatifs génériques ne correspondent pas aux qualificatifs non génériques, mais à d'autres qualificatifs génériques. L'option par défaut est **Non**.
- **Expression :** les qualificatifs génériques d'une expression correspondent à n'importe quel qualificatif d'un emplacement LDNS, mais les qualificatifs génériques de l'emplacement LDNS ne correspondent pas aux qualificatifs non génériques d'une expression.

Exemple :

```
add dns policy1 "CLIENT.IP.SRC.MATCHES_LOCATION("Continent.country
    \*.\*.\*.\* \ “)”  <action>
<!--NeedCopy-->
```

Pour définir les paramètres d'emplacement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set locationparameter -context <context> -q1label <string> [-q2label <
    string>] [-q3label <string>] [-q4label <string>] [-q5label <string>]
     [-q6label <string>] -matchWildcardtoany [Yes | No | Expression]
<!--NeedCopy-->
```

Exemple :

```
set locationparameter -context custom -q1label asia -matchWildcardtoany
    Yes
<!--NeedCopy-->
```

Pour définir les paramètres de localisation à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > GSLB > Base de données et entrées**.
2. Sous **Paramètres**, cliquez sur **Modifier les paramètres d'emplacement**.
3. Dans la page **Configurer les paramètres d'emplacement**, définissez les paramètres d'emplacement.

Spécifier la méthode de proximité

August 20, 2021

Lorsque vous avez configuré la base de données de proximité statique, vous êtes prêt à spécifier la proximité statique comme méthode GLSB.

Pour spécifier la proximité statique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la proximité statique et vérifier la configuration :

```
set gslb vserver <name> -lbMethod STATICPROXIMITY
show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -lbMethod STATICPROXIMITY
show gslb vserver
<!--NeedCopy-->
```

Pour spécifier la proximité statique à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Serveurs virtuels et double-cliquez sur le serveur virtuel.
2. Cliquez sur la section **Méthode** et, dans la liste déroulante **Choisir une méthode**, sélectionnez **STATICPROXIMITY**.

Synchroniser la base de données de proximité statique GSLB

January 21, 2021

La synchronisation d'une base de données de proximité statique GSLB (Global Server Load Balancing) nécessite que l'un des sites soit identifié comme étant le nœud GSLB maître. Tout site de la topologie peut être désigné comme nœud maître. Le reste des nœuds GSLB sont automatiquement désignés comme nœuds esclaves.

La synchronisation des bases de données de proximité statique GSLB synchronise les fichiers du répertoire /var/netscaler/locdb sur les nœuds esclaves. Pendant le processus de synchronisation, le nœud maître récupère la configuration en cours d'exécution à partir de chacun des nœuds esclaves et la compare à la configuration du nœud maître. Le nœud GSLB maître utilise le programme rsync pour synchroniser la base de données de proximité statique entre les nœuds esclaves. Pour accélérer le processus de synchronisation, le programme rsync ne fait que suffisamment de modifications pour éliminer les différences entre les deux fichiers. Le processus de synchronisation ne peut pas être annulé.

L'exemple suivant synchronise Site2, qui est un site esclave, avec le site maître Site1. L'administrateur entre la commande **sync gslb config** sur Site1 :


```
sync gslb config -nowarn
Sync Time: Feb 24 2014 14:56:16
Retrieving local site info: ok
Retrieving all participating gslb sites info:
0 bytes in 0 blocks
ok
site1[Master]:
        Getting Config: ok
site2[Slave]:
        Syncing gslb static proximity database: ok
        Getting Config: ok
        Comparing config: ok
        Applying changes: ok
 Done
<!--NeedCopy-->
```

Configurer la communication site à site

August 20, 2021

La communication site à site GSLB se fait entre les nœuds RPC (Remote Procedure Call) associés aux sites communicants. Un site GSLB maître établit des connexions avec des sites esclaves afin de synchroniser les informations de configuration GSLB et d'échanger des mesures de site.

Un nœud RPC est créé automatiquement lorsqu'un site GSLB est créé et reçoit un nom d'utilisateur et un mot de passe générés en interne. L'appliance Citrix ADC utilise ce nom d'utilisateur et ce mot de passe pour s'authentifier auprès des sites GSLB distants lors de l'établissement de la connexion. Aucune étape de configuration n'est nécessaire pour un nœud RPC, mais vous pouvez spécifier un mot de passe de votre choix, améliorer la sécurité en chiffrant les informations échangées par les sites GSLB et spécifier une adresse IP source pour le nœud RPC.

L'appliance a besoin d'une adresse IP appartenant à Citrix ADC à utiliser comme adresse IP source lors de la communication avec d'autres sites GSLB. Par défaut, les nœuds RPC utilisent soit une adresse IP de sous-réseau (SNIP), mais vous pouvez spécifier une adresse IP de votre choix.

Les rubriques suivantes décrivent le comportement et la configuration des nœuds RPC sur l'appliance Citrix ADC :

Modification du mot de passe d'un nœud RPC

Citrix vous recommande de sécuriser la communication entre les sites dans votre configuration GSLB en modifiant le mot de passe de chaque nœud RPC. Après avoir modifié le mot de passe du nœud RPC du site local, vous devez propager manuellement la modification au nœud RPC sur chacun des sites distants.

Le mot de passe est stocké sous forme cryptée. Vous pouvez vérifier que le mot de passe a changé en utilisant la commande show rpcNode pour comparer la forme chiffrée du mot de passe avant et après la modification.

> **Remarque :** GSLB utilise un compte d'utilisateur interne. Pour une sécurité renforcée, Citrix vous recommande également de modifier le mot de passe du compte utilisateur interne. Le mot de passe du compte d'utilisateur interne est modifié via le mot de passe du nœud RPC.

Pour modifier le mot de passe d'un nœud RPC à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour modifier le mot de passe d'un nœud RPC :

```
set ns rpcNode <IPAddress> {
 -password }

show ns rpcNode
<!--NeedCopy-->
```

Exemple :

```
> set rpcNode 192.0.2.4 -password mypassword
 Done
> show rpcNode
.
.
.
2)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
    SrcIP:  *               Secure:  OFF
Done
>

<!--NeedCopy-->
```


Pour annuler le mot de passe d'un nœud RPC à l'aide de l'interface de ligne de commande

Pour annuler le mot de passe d'un nœud RPC à l'aide de l'interface de ligne de commande, tapez la commande unset RPCNode, l'adresse IP du nœud RPC et le paramètre password, sans valeur.

Pour modifier le mot de passe d'un nœud RPC à l'aide de l'utilitaire de configuration

Accédez à Système > Réseau > RPC, sélectionnez le nœud RPC et modifiez le mot de passe.

Chiffrer l'échange de mesures de site

Vous pouvez sécuriser les informations échangées entre les sites GSLB en définissant l'option sécurisée pour les nœuds RPC dans la configuration GSLB. Avec l'option sécurisée définie, l'appliance Citrix ADC chiffre toutes les communications envoyées depuis le nœud vers d'autres nœuds RPC.

Pour chiffrer l'échange de mesures de site à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour chiffrer l'échange de mesures de site et vérifier la configuration :

```
set ns rpcNode <IPAddress> [-secure ( YES | NO )]
show rpcNode
<!--NeedCopy-->
```

Exemple :

```
> set rpcNode 192.0.2.4 -secure YES
 Done
>
> show rpcNode
.
.
.
3)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e SrcIP:
    192.0.2.3     Secure:  ON
 Done
>
<!--NeedCopy-->
```

Pour annuler la définition du paramètre secure à l'aide de l'interface de ligne de commande

Pour annuler la définition du paramètre secure à l'aide de l'interface de ligne de commande, tapez la commande unset RPCNode, l'adresse IP du nœud RPC et le paramètre secure, sans valeur.

Pour chiffrer l'échange de mesures de site à l'aide de l'utilitaire de configuration Citrix ADC

1. Accédez à Système > Réseau > RPC et double-cliquez sur un nœud RPC.
2. Sélectionnez l'option **Sécuriser**, puis cliquez sur **OK** .

Configurer l'adresse IP source pour un nœud RPC

Par défaut, l'appliance Citrix ADC utilise une adresse SNIP de sous-réseau (SNIP) appartenant à Citrix ADC comme adresse IP source d'un nœud RPC, mais vous pouvez configurer l'appliance pour qu'elle utilise une adresse SNIP spécifique. Si une adresse SNIP n'est pas disponible, le site GSLB ne peut pas communiquer avec d'autres sites. Dans un tel scénario, vous devez configurer l'adresse NSIP ou une adresse IP virtuelle (VIP) comme adresse IP source pour un nœud RPC. Une adresse VIP peut être utilisée comme adresse IP source d'un nœud RPC uniquement si le nœud RPC est un nœud distant. Si vous configurez une adresse VIP comme adresse IP source et supprimez l'adresse VIP, l'appliance utilise une adresse SNIP.

> **Remarque**
>
> À partir de la version NetScaler 11.0.64.x, vous pouvez configurer l'appliance pour qu'elle utilise l'adresse IP du site GSLB comme adresse IP source d'un nœud RPC.

Pour spécifier une adresse IP source pour un nœud RPC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour modifier l'adresse IP source d'un nœud RPC et vérifier la configuration :

```
set ns rpcNode <IPAddress> [-srcIP <ip_addr|ipv6_addr|*>]
show ns rpcNode
<!--NeedCopy-->
```

Exemple :

```
set rpcNode 192.0.2.4 -srcIP 192.0.2.3
Done
show rpcNode
<!--NeedCopy-->
```

```
IPAddress: 192.0.2.4 Password: d336004164d4352ce39e SrcIP: 192.0.2.3
   Secure: OFF
Done
<!--NeedCopy-->
```


Pour annuler la définition du paramètre d'adresse IP source à l'aide de l'interface de ligne de commande

Pour annuler la définition du paramètre d'adresse IP source à l'aide de l'interface de ligne de commande, tapez le RPCNodeCommand non défini, l'adresse IP du nœud RPC et le paramètre SRCip, sans valeur.

Pour spécifier une adresse IP source pour un nœud RPC à l'aide de l'utilitaire de configuration Citrix ADC

1. Accédez à Système > Réseau > RPC et double-cliquez sur un nœud RPC.
2. Dans le champ Adresse IP source, entrez l'adresse IP que vous souhaitez que le nœud RPC utilise comme adresse IP source et cliquez sur OK.

> **Important**
>
> L'adresse IP source ne peut pas être synchronisée entre les sites participant à GSLB car l'adresse IP source d'un nœud RPC est spécifique à chaque appliance Citrix ADC. Par conséquent, après avoir forcé une synchronisation (à l'aide de la commande sync gslb config —ForceSync ou en sélectionnant l'option ForceSync dans l'interface graphique), vous devez modifier manuellement les adresses IP source sur les autres appliances Citrix ADC.

Configuration du protocole d'échange de mesures

August 20, 2021

Les centres de données d'une mesure d'installation GSLB échangent entre eux via le protocole MEP (Metrics Exchange Protocol), qui est un protocole propriétaire pour l'appliance Citrix ADC. L'échange des informations de mesure commence lorsque vous créez un site GSLB. Ces mesures comprennent les informations de charge, de réseau et de persistance.

Le MEP est requis pour la vérification de l'état des centres de données afin de s'assurer de leur disponibilité. Une connexion pour l'échange de mesures réseau (aller-retour) peut être initiée par l'un ou l'autre des datacenters impliqués dans l'échange, mais une connexion pour l'échange de mesures de site est toujours initiée par le datacenter dont l'adresse IP est inférieure. Par défaut, le centre de données utilise une adresse IP de sous-réseau (SNIP) pour établir une connexion à l'adresse IP d'un centre de données différent. Toutefois, vous pouvez configurer un SNIP, une adresse IP virtuelle (VIP) spécifique ou l'adresse NSIP, comme adresse IP source pour l'échange de mesures. Le processus de communication entre les sites GSLB utilise le port TCP 3011 ou 3009. Ce port doit donc être ouvert sur les pare-feu qui se trouvent entre les appliances Citrix ADC.

Remarque : Vous pouvez configurer une adresse IP de site SNIP ou GSLB comme adresse IP source pour l'échange de mesures. Pour plus d'informations, voir Configurer l'adresse IP source pour un nœud RPC.

Si les sites source et cible (le site qui initie une connexion MEP et le site qui reçoit la demande de connexion, respectivement) ont des adresses IP privées et publiques configurées, les sites échangent des informations MEP à l'aide des adresses IP publiques.

Vous pouvez également lier des moniteurs pour vérifier l'état de santé des services distants, comme décrit dans « Surveillance des services GSLB ». « Lorsque les moniteurs sont liés, l'échange de mesures ne contrôle pas l'état du service distant. Si un moniteur est lié à un service distant et que l'échange de mesures est activé, le moniteur contrôle l'état d'intégrité. La liaison des moniteurs au service distant permet à l'appliance Citrix ADC d'interagir avec un périphérique d'équilibrage de charge ADC autre que Citrix. L'appliance Citrix ADC peut surveiller les périphériques ADC autres que Citrix, mais ne peut pas effectuer l'équilibrage de charge sur eux, à moins que les moniteurs ne soient liés à tous les services GSLB et que seules des méthodes d'équilibrage de charge statique (telles que les méthodes d'équilibrage de charge statique, de proximité statique ou de hachage) sont utilisées.

Avec NetScaler version 11.1.51.x ou ultérieure, pour éviter toute perturbation inutile des services, vous pouvez définir un délai pour marquer les services GSLB comme étant DOWN lorsqu'une connexion MEP tombe en panne.

État MEP dans une configuration haute disponibilité

Dans une configuration haute disponibilité, le nœud principal établit des connexions avec les sites distants et l'état MEP n'est pas synchronisé du nœud principal aux nœuds secondaires. Par conséquent, l'état MEP dans le nœud secondaire reste en panne. Lorsque le nœud secondaire devient principal, il établit des connexions MEP avec le nouveau site GSLB et met à jour l'état MEP en conséquence.

Activer l'échange de mesures de site

Les mesures de site échangées entre les sites GSLB incluent l'état de chaque serveur virtuel d'équilibrage de charge ou de commutation de contenu, le nombre actuel de connexions, le débit de paquets actuel et les informations d'utilisation de la bande passante actuelle.

L'appliance Citrix ADC a besoin de ces informations pour effectuer l'équilibrage de charge entre les sites. L'intervalle d'échange de mesures de site est de 1 seconde. Un service GSLB distant doit être lié à un serveur virtuel GSLB local pour permettre l'échange de mesures de site avec le service distant.

Pour activer ou désactiver l'échange de mesures de site à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver l'échange de mesures de site et vérifier la configuration :

```
set gslb site <siteName> -metricExchange (ENABLED|DISABLED)
show gslb site** <siteName>
<!--NeedCopy-->
```

Exemple :

```
set gslb site Site-GSLB-East-Coast -metricExchange ENABLED
set gslb site Site-GSLB-East-Coast -metricExchange DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Pour activer ou désactiver l'échange de mesures de site à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Sites**, puis sélectionnez le site.
2. Dans la boîte de dialogue **Configurer le site GSLB**, sélectionnez l'**option Exchange de mesures** .

Activer l'échange de mesures réseau

Si vos sites GSLB utilisent la méthode d'équilibrage de charge aller-retour (RTT), vous pouvez activer ou désactiver l'échange d'informations RTT sur le service DNS local du client. Ces informations sont échangées toutes les 5 secondes.

Pour plus d'informations sur la modification de la méthode GSLB par une méthode basée sur RTT, voir Méthodes GSLB.

Pour activer ou désactiver l'échange d'informations de mesure réseau à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver l'échange d'informations sur les métriques réseau et vérifier la configuration :

```
set gslb site <siteName> -nwmetricExchange (ENABLED|DISABLED)
show gslb site <<siteName>
<!--NeedCopy-->
```

Exemple :


```
set gslb site Site-GSLB-East-Coast -nwmetricExchange ENABLED
set gslb site Site-GSLB-East-Coast -nwmetricExchange DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Pour activer ou désactiver l'échange d'informations de mesure réseau à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Sites**.
2. Dans la boîte de dialogue **Configurer le site GSLB**, sélectionnez l'option **Exchange métrique réseau** .

Configuration d'un délai pour que les services GSLB soient marqués comme DOWN lorsqu'une connexion MEP se désactive

Si l'état d'une connexion MEP à un site distant passe à DOWN, l'état de chaque service GSLB sur ce site distant est marqué comme DOWN, bien que le site ne soit pas réellement DOWN.

Vous pouvez maintenant définir un délai pour laisser un certain temps pour rétablir la connexion MEP avant que le site ne soit marqué comme DOWN. Si la connexion MEP est de nouveau disponible avant l'expiration du délai, les services ne sont pas affectés.

Par exemple, si vous définissez le délai 10, les services GSLB sont marqués comme DOWN jusqu'à ce que la connexion MEP ait été DOWN pendant 10 secondes. Si la connexion MEP est de nouveau disponible en 10 secondes, les services GSLB restent à l'état UP.

Remarque : Ce délai s'applique uniquement aux services non liés à un moniteur. Le délai n'affecte pas les moniteurs de déclenchement.

Pour définir un délai à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set gslb parameter** - GSLBSvcStateDelayTime <sec>
<!--NeedCopy-->
```

Exemple :

set gslb parameter - GSLBSvcStateDelayTime 10

> **Remarque**
>
> Dans un déploiement hiérarchique (topologie parent-enfant), si vous configurez le service GSLB

> sur les sites parent et enfant, définissez le paramètre GSLB sur les sites parent et enfant. Si vous ne configurez pas le service GSLB sur le site enfant, définissez le paramètre GSLB uniquement sur le site parent.

Pour définir un délai à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Modifier les paramètres GSLB**.
2. Dans la zone **Temps de retard (secondes) de l'état du service GSLB**, tapez le délai en secondes.

Configurer un temps d'apprentissage pour les services GSLB lorsque l'état de la connexion MEP apparaît pour éviter les volets sur les services GSLB

Lorsqu'un nœud redémarre ou pendant le basculement HA, le système est initialisé. Ensuite, le nœud doit connaître les informations actuelles sur les services locaux et enfants configurés pour communiquer l'état du service aux nœuds distants via MEP. Le nœud prend un certain temps pour apprendre les informations correctes. Dans le même temps, si un nœud homologue se connecte à ce nœud et demande une mise à jour, le nœud peut envoyer un état de service et des statistiques incorrects. Ces informations incorrectes peuvent entraîner des problèmes liés à la fonctionnalité et à d'autres problèmes liés aux fonctionnalités sur les nœuds homologues distants. Pour éviter ce scénario, vous pouvez désormais définir un temps d'apprentissage pour le service GSLB local et enfant.

Lorsqu'un délai d'attente d'apprentissage est configuré, le site GSLB reçoit un certain temps de tampon (délai d'attente d'apprentissage) pour connaître les statistiques correctes sur ses services locaux et enfants. Lorsqu'un service est en phase d'apprentissage, le site GSLB distant obtient ces informations dans la mise à jour MEP, et ne respecte pas l'état du site principal et les statistiques reçues via MEP pour ce service.

Les services GSLB entrent dans la phase d'apprentissage dans l'un des scénarios suivants.

- L'appliance Citrix ADC est redémarrée
- Le basculement à haute disponibilité s'est produit
- Le nœud propriétaire d'une configuration GSLB de cluster est modifié
- MEP est activé sur un nœud local
- Le site GSLB est issu d'un scénario insulaire. Un site GSLB devient un îlot lorsqu'il n'est connecté à aucun autre site.

Dans un déploiement parent-enfant, le parent de sauvegarde (s'il est configuré) déplace sélectivement les services GSLB du site enfant adopté vers la phase d'apprentissage lorsque le parent principal tombe en panne.

Pour définir un temps d'apprentissage de l'état du service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set gslb parameter - SvcStateLearningTime <sec>
<!--NeedCopy-->
```

Vous pouvez définir « SVCStateLearningTime » en quelques secondes. La valeur par défaut est 0 et la valeur maximale est 3600. Ce paramètre est applicable uniquement si les moniteurs ne sont pas liés aux services GSLB.

Exemple :

```
set gslb parameter - SvcStateLearningTime 10
<!--NeedCopy-->
```

Pour définir un temps d'apprentissage de l'état du service à l'aide de l'interface graphique

1. Accédez à **Configuration > Gestion du trafic > GSLB > Tableau de bord > Modifier les paramètres GSLB**.

   La page **Définir les paramètres GSLB** apparaît.

2. Dans le champ **Durée d'apprentissage de l'état du service GSLB (secondes)**, saisissez le temps d'apprentissage en secondes.

Activer l'échange d'informations de persistance

Vous pouvez configurer l'appliance Citrix ADC pour qu'elle fournisse des connexions persistantes, de sorte qu'une transmission client vers n'importe quel serveur virtuel d'un groupe puisse être dirigée vers un serveur ayant reçu des transmissions précédentes du même client.

Vous pouvez activer ou désactiver l'échange d'informations de persistance sur chaque site. Ces informations sont échangées toutes les 5 secondes entre les appliances Citrix ADC participant à GSLB.

Pour plus d'informations sur la configuration de la persistance, voir Configuration des connexions persistantes.

Pour activer ou désactiver l'échange d'informations de persistance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver l'échange d'informations de persistance et vérifier la configuration :


```
set gslb site <siteName> -sessionExchange (ENABLED|DISABLED)
show gslb site** <siteName>
<!--NeedCopy-->
```

Exemple :

```
set gslb site Site-GSLB-East-Coast -sessionExchange  ENABLED
set gslb site Site-GSLB-East-Coast -sessionExchange  DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Pour activer ou désactiver l'échange d'informations de persistance à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Sites**, puis double-cliquez sur le site.
2. Dans la boîte de dialogue **Configurer le site GSLB**, activez ou désactivez la case à cocher **Échange d'entrée de session de persistance**.

Configurer GSLB à l'aide d'un assistant

January 21, 2021

Vous pouvez maintenant utiliser un assistant pour configurer les types de déploiement GSLB : actif-actif, actif-passif et parent-enfant.

Cet Assistant est disponible dans l'interface graphique. Pour accéder à l'Assistant, accédez à **Configuration** > **Gestion du trafic** > **GSLB** et cliquez sur **Démarrer** .

Vous pouvez également accéder à cet Assistant à partir du tableau de bord GSLB. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Tableau de bord** et cliquez sur **Configurer GSLB** .

Remarque : Vous pouvez également configurer les entités GSLB individuellement.

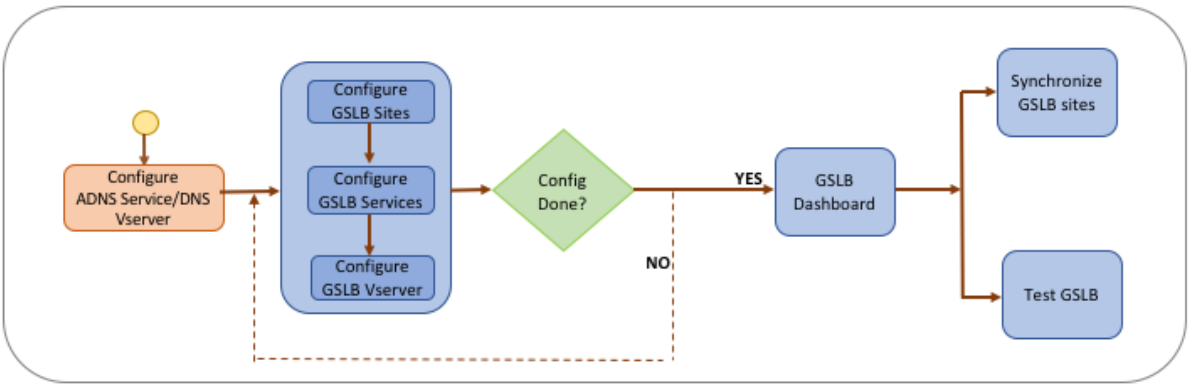
- Configuration active du site
- Configuration du site actif-passif
- Configuration de la topologie parent-enfant

> **Important**
>
> Cette fonctionnalité est prise en charge dans le déploiement haute disponibilité et non dans les déploiements de partition d'administration et de cluster.

Configurer le site actif-actif

January 21, 2021

La figure suivante illustre le flux de travail impliqué dans une configuration de site actif GSLB.



Avant de commencer à configurer un site actif, assurez-vous d'avoir configuré une configuration standard d'équilibrage de charge pour chaque batterie de serveurs ou centre de données.

De plus, pour synchroniser la configuration GSLB entre les sites GSLB dans le déploiement, assurez-vous que :

- Les sites GLSB locaux sont configurés sur toutes les appliances de la configuration GSLB.
- Vous avez activé l'accès à la gestion sur tous les sites GSLB de la configuration.
- Vous avez configuré le pare-feu pour accepter la synchronisation automatique et les connexions MEP.
- Les appliances principales et esclave Citrix ADC exécutent les mêmes versions logicielles Citrix ADC.
- Toutes les appliances Citrix ADC participant en tant que sites doivent avoir la même version du logiciel Citrix ADC (les sites ne sont pas dans une relation maître-esclave).
- Le mot de passe du nœud RPC est le même sur tous les sites GSLB de la configuration GSLB.

Pour configurer un site actif à l'aide de l'assistant

Sous l'onglet Configuration, procédez comme suit :

1. Accédez à **Gestion du trafic** > **GSLB**, puis cliquez sur **Démarrer**.
2. Si vous n'avez pas configuré de service ADNS ou de serveur virtuel DNS pour le site, vous pouvez le faire maintenant.
   a) Cliquez sur **Affichage**, puis sur **Ajouter**.
   b) Entrez le nom du service, l'adresse IP et sélectionnez le protocole (ADNS/ADNS_TCP) par lequel les données sont échangées avec le service.

3. Sélectionnez **Site actif**.
4. Entrez le nom de domaine complet et spécifiez la période pendant laquelle l'enregistrement doit être mis en cache par les proxy DNS.
5. Configurez les sites GSLB. Chaque site doit être configuré avec un site GSLB local, et la configuration de chaque site doit inclure tous les autres sites en tant que sites GSLB distants. Il ne peut y avoir qu'un seul site local et tous les autres sites sont des sites distants.
   a) Entrez les détails du site, tels que le nom du site et l'adresse IP du site.
   b) Sélectionnez le type de site REMOTE ou LOCAL.
   c) Vous pouvez également modifier le mot de passe RPC et, si nécessaire, le sécuriser.
   d) Si un moniteur doit être lié au service GSLB, sélectionnez la condition dans laquelle le moniteur doit surveiller le service. Cela ne sera efficace qu'une fois qu'un moniteur est lié aux services. Les conditions possibles sont :
      - **ALWAYS**. Surveillez le service GSLB en tout temps.
      - **Échec de MEP**. Surveillez le service GSLB uniquement lorsque l'échange de mesures via MEP échoue.
      - **Échec de MEP et ID de service Down**. L'échange de mesures via MEP est activé, mais le statut du service, mis à jour via l'échange de mesures, est DOWN.
6. Configurez les services GSLB. Pour créer un site actif, vous devez ajouter au moins deux services GSLB.
   a) Entrez les détails du service, tels que le nom du service, le type de service et le numéro de port.
   b) Associez le service à un site (local ou distant) en sélectionnant le site GSLB auquel appartient le service GSLB.
   c) Sélectionnez le moniteur qui doit être lié au service en cas d'échec de MEP, si nécessaire. Le service peut être un serveur existant ou vous pouvez créer un nouveau serveur ou un serveur virtuel.
   d) Pour associer un serveur existant, sélectionnez le nom du serveur. L'adresse IP du service est automatiquement renseignée.
      - Si l'adresse IP publique est différente de l'adresse IP du serveur, ce qui peut se produire dans un environnement NAT, entrez l'adresse IP publique et le numéro de port du port public.
      - Pour associer un nouveau serveur, créez un serveur en entrant les détails IP du serveur, son adresse IP publique et le numéro de port public.
      - Pour associer un serveur virtuel, sélectionnez un serveur virtuel existant ou cliquez sur + et ajoutez un nouveau serveur virtuel. Ce vserver est le vserver d'équilibrage de charge auquel ce service GSLB sera associé.
7. Configurez les serveurs virtuels GSLB.
   a) Entrez le nom du serveur virtuel GSLB et sélectionnez le type d'enregistrement DNS.
   b) Cliquez sur **>** dans la zone **Sélectionner un service** et choisissez les services GSLB à lier

au serveur virtuel GSLB.

c) Cliquez sur **>** dans la zone **Liaison** de domaine pour sélectionner le domaine à lier à ce serveur virtuel GSLB.

d) Choisissez la méthode GSLB pour sélectionner le service GSLB le plus performant. Les valeurs par défaut de la méthode GSLB, de la méthode de sauvegarde et de la pondération dynamique sont automatiquement renseignées, par défaut. Vous pouvez les modifier si nécessaire.

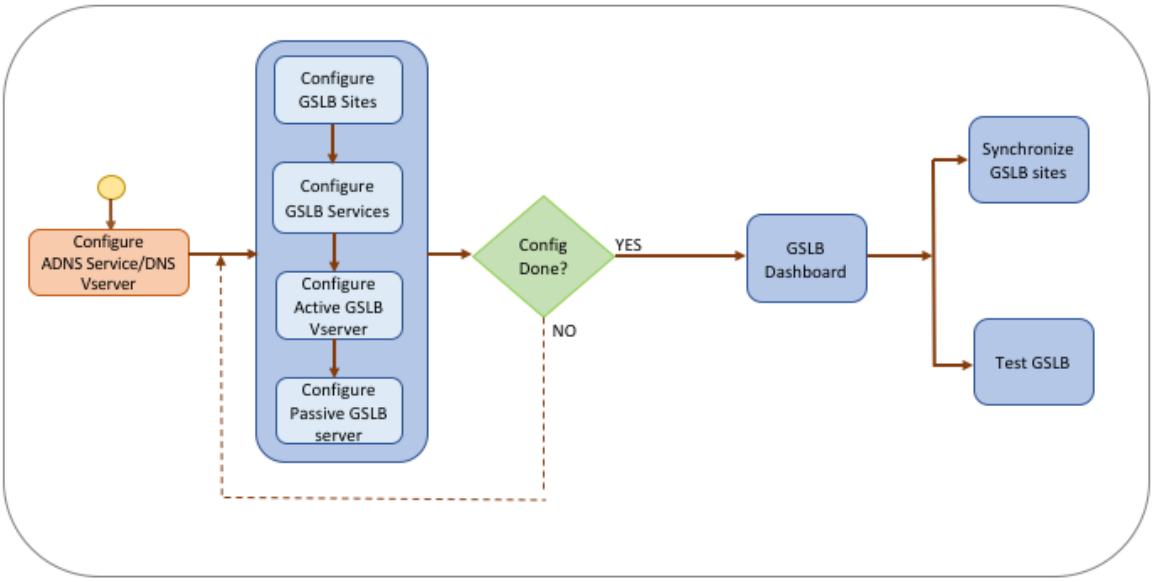
- Si vous choisissez la méthode **basée sur l'algorithme**, sélectionnez les méthodes primaires et de sauvegarde et spécifiez également l'option de pondération dynamique.
- Si vous choisissez la méthode **Proximité statique**, sélectionnez la méthode de sauvegarde et la méthode de pondération dynamique. Indiquez également l'emplacement du fichier de base de données en cliquant sur l'icône > ou ajoutez un nouvel emplacement en cliquant sur **+** dans la zone Sélectionner une base de données d'emplacement.
- Si vous choisissez la méthode de **proximité dynamique (RTT)**, sélectionnez la méthode de sauvegarde et spécifiez l'option de pondération dynamique et la valeur de temps aller-retour en fonction de laquelle le service le plus performant doit être sélectionné.

8. Cliquez sur **Terminé** si la configuration est terminée. Le tableau de bord GSLB s'affiche.
9. Si vous avez modifié la configuration du site GSLB, cliquez sur **Synchroniser automatiquement GSLB** dans le tableau de bord pour synchroniser la configuration avec d'autres sites dans la configuration GSLB.
   - Avant la synchronisation, assurez-vous que la configuration du site local inclut des informations sur les sites distants. En outre, pour que la synchronisation réussisse, le site local doit être configuré sur les autres appliances Citrix ADC.
   - Si la synchronisation en temps réel est activée, vous n'avez pas besoin de cliquer sur **Synchroniser automatiquement GSLB**. La synchronisation se produit automatiquement. Pour activer la synchronisation en temps réel, procédez comme suit :
     a) Accédez à **Gestion du trafic** > **GSLB** > **Tableau de bord** et cliquez sur **Modifier les paramètres GSLB**.
     b) Activez la case à cocher **Synchronisation automatique de la configuration**.
10. Cliquez sur **Tester l'installation GSLB** pour vous assurer que les services ADNS ou les serveurs DNS répondent avec l'adresse IP correcte pour le nom de domaine configuré dans la configuration GSLB.

Configurer le site actif-passif

August 20, 2021

La figure suivante illustre le flux de travail impliqué dans la configuration du site actif-passif.



Avant de commencer à configurer un site actif-passif, assurez-vous d'avoir configuré une configuration standard d'équilibrage de charge pour chaque batterie de serveurs ou centre de données.

De plus, pour synchroniser la configuration GSLB entre les sites GSLB dans le déploiement, assurez-vous que :

- Les sites GLSB locaux sont configurés sur toutes les appliances de la configuration GSLB.
- Vous avez activé l'accès à la gestion sur tous les sites GSLB de la configuration.
- Vous avez configuré le pare-feu pour accepter la synchronisation automatique et les connexions MEP.
- Les appliances principales et esclave Citrix ADC exécutent les mêmes versions logicielles Citrix ADC.
- Toutes les appliances Citrix ADC participant en tant que sites doivent avoir la même version du logiciel Citrix ADC (les sites ne sont pas dans une relation maître-esclave).
- Le mot de passe du nœud RPC est le même sur tous les sites GSLB de la configuration GSLB.

Pour configurer un site actif-passif à l'aide de l'assistant

Sous l'onglet Configuration, procédez comme suit :

1. Accédez à **Gestion du trafic** > **GSLB**, puis cliquez sur **Démarrer**.
2. Si vous n'avez pas configuré de service ADNS ou de serveur virtuel DNS pour le site, vous pouvez le faire maintenant.
   a) Cliquez sur **Affichage**, puis sur **Ajouter**.
   b) Entrez le nom du service, l'adresse IP et sélectionnez le protocole (ADNS/ADNS_TCP) par lequel les données sont échangées avec le service.

3. Sélectionnez **Site actif-passif**.
4. Entrez le nom de domaine complet et spécifiez la période pendant laquelle l'enregistrement doit être mis en cache par les proxy DNS.
5. Configurez les sites GSLB. Chaque site doit être configuré avec un site GSLB local, et la configuration de chaque site doit inclure tous les autres sites en tant que sites GSLB distants. Il ne peut y avoir qu'un seul site local et tous les autres sites sont des sites distants.
   a) Entrez les détails du site, tels que le nom du site et l'adresse IP du site.
   b) Sélectionnez le type de site REMOTE ou LOCAL.
   c) Vous pouvez également modifier le mot de passe RPC et, si nécessaire, le sécuriser.
   d) Si un moniteur doit être lié au service GSLB, sélectionnez la condition dans laquelle le moniteur doit surveiller le service. Cela ne sera efficace qu'une fois qu'un moniteur est lié aux services. Les conditions possibles sont :
      - **ALWAYS**. Surveillez le service GSLB en tout temps.
      - **Échec de MEP**. Surveillez le service GSLB uniquement lorsque l'échange de mesures via MEP échoue.
      - **Échec de MEP et ID de service Down**. L'échange de mesures via MEP est activé, mais le statut du service, mis à jour via l'échange de mesures, est DOWN.
6. Configurez les services GSLB.
   a) Entrez les détails du service, tels que le nom du service, le type de service et le numéro de port.
   b) Associez le service à un site (local ou distant) en sélectionnant le site GSLB auquel appartient le service GSLB.
   c) Sélectionnez le moniteur qui doit être lié au service en cas d'échec de MEP, si nécessaire. Le service peut être un serveur existant ou vous pouvez créer un nouveau serveur ou un serveur virtuel.
   d) Pour associer un serveur existant, sélectionnez le nom du serveur. L'adresse IP du service est automatiquement renseignée.
      - Si l'adresse IP publique est différente de l'adresse IP du serveur, ce qui peut se produire dans un environnement NAT, entrez l'adresse IP publique et le numéro de port du port public.
      - Pour associer un nouveau serveur, créez un serveur en entrant les détails IP du serveur, son adresse IP publique et le numéro de port public.
      - Pour associer un serveur virtuel, sélectionnez un serveur virtuel existant ou cliquez sur **+** et ajoutez un nouveau serveur virtuel. Ce vserver est le vserver d'équilibrage de charge auquel ce service GSLB sera associé.
7. Configurez les serveurs virtuels de sauvegarde GSLB. Les serveurs virtuels de sauvegarde GSLB ne deviennent opérationnels que lorsque les serveurs virtuels GSLB principaux sont inaccessibles ou qu'ils sont marqués DOWN pour une raison quelconque.
   a) Entrez le nom du serveur virtuel GSLB et sélectionnez le type d'enregistrement DNS.

b) Cliquez sur **>** dans **Liaison de service**, puis choisissez les services GSLB qui doivent être liés au serveur virtuel GSLB.

c) Choisissez la méthode GSLB pour sélectionner le service GSLB le plus performant. Les valeurs par défaut de la méthode GSLB, de la méthode de sauvegarde et de la pondération dynamique sont automatiquement renseignées, par défaut. Vous pouvez les modifier si nécessaire.

- Si vous choisissez la méthode **basée sur l'algorithme**, sélectionnez la méthode principale et la méthode de sauvegarde.
- Si vous choisissez la méthode **Proximité statique**, sélectionnez la méthode de sauvegarde et indiquez l'emplacement du fichier de base de données.
- Si vous choisissez la méthode **RTT (Dynamic Proximity)**, sélectionnez la méthode de sauvegarde et spécifiez la pondération du service et la valeur RTT en fonction de laquelle le service le plus performant doit être sélectionné.

8. Configurez les serveurs virtuels GSLB.

a) Entrez le nom du serveur virtuel GSLB et sélectionnez le type d'enregistrement DNS.

b) Cliquez sur **>** dans la zone **Sélectionner un service** et choisissez les services GSLB à lier au serveur virtuel GSLB.

c) Cliquez sur **>** dans la zone **Liaison** de domaine pour sélectionner le domaine à lier à ce serveur virtuel GSLB.

d) Choisissez la méthode GSLB pour sélectionner le service GSLB le plus performant. Les valeurs par défaut de la méthode GSLB, de la méthode de sauvegarde et de la pondération dynamique sont automatiquement renseignées, par défaut. Vous pouvez les modifier si nécessaire.

- Si vous choisissez la méthode **basée sur l'algorithme**, sélectionnez les méthodes primaires et de sauvegarde et spécifiez également l'option de pondération dynamique.
- Si vous choisissez la méthode **Proximité statique**, sélectionnez la méthode de sauvegarde et la méthode de pondération dynamique. Indiquez également l'emplacement du fichier de base de données en cliquant sur l'icône **>** ou ajoutez un nouvel emplacement en cliquant sur **+** dans la zone Sélectionner une base de données d'emplacement.
- Si vous choisissez la méthode de **proximité dynamique (RTT)**, sélectionnez la méthode de sauvegarde et spécifiez l'option de pondération dynamique et la valeur de temps aller-retour en fonction de laquelle le service le plus performant doit être sélectionné.

9. Cliquez sur **Terminé** si la configuration est terminée. Le tableau de bord GSLB s'affiche.
10. Si vous avez modifié la configuration du site GSLB, cliquez sur **Synchroniser automatiquement GSLB** dans le tableau de bord pour synchroniser la configuration avec d'autres sites dans la configuration GSLB.

- Avant la synchronisation, assurez-vous que la configuration du site local inclut des infor-

mations sur les sites distants. En outre, pour que la synchronisation réussisse, le site local doit être configuré sur les autres appliances Citrix ADC.

- Si la synchronisation en temps réel est activée, vous n'avez pas besoin de cliquer sur **Synchroniser automatiquement GSLB**. La synchronisation se produit automatiquement. Pour activer la synchronisation en temps réel, procédez comme suit :
  a) Accédez à **Gestion du trafic** > **GSLB** > **Tableau de bord** et cliquez sur **Modifier les paramètres GSLB**.
  b) Activez la case à cocher **Synchronisation automatique de la configuration**.

11. Cliquez sur **Tester l'installation GSLB** pour vous assurer que les services ADNS ou les serveurs DNS répondent avec l'adresse IP correcte pour le nom de domaine configuré dans la configuration GSLB.

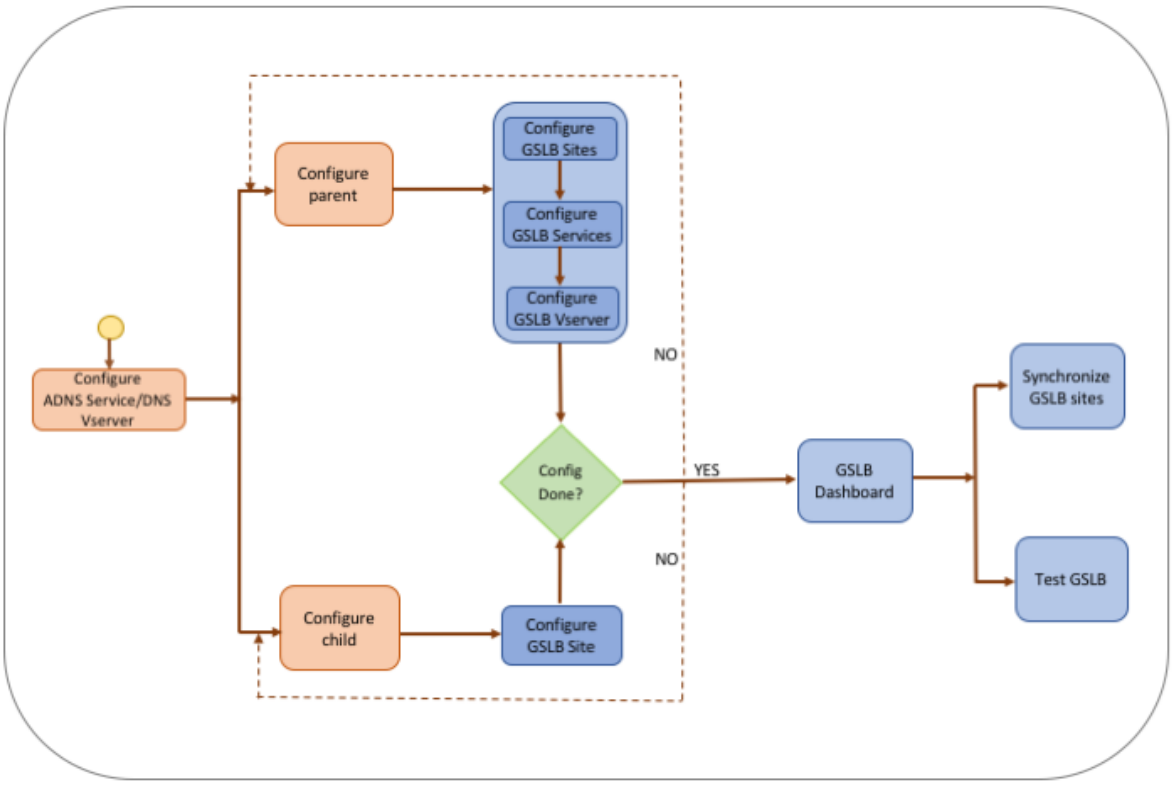
> **Remarque**
>
> Pour plus d'informations sur la configuration des entités GSLB d'une configuration GSLB actif-passive pour la reprise après sinistre, voir Configuration de GSLB pour la reprise après sinistre.

Configurer la topologie parent-enfant

February 12, 2021

Dans une topologie parent-enfant, au niveau supérieur se trouvent les sites parents, qui ont des relations d'homologue avec d'autres parents. Chaque parent peut avoir plusieurs sites enfants et chaque site parent échange des informations d'intégrité avec ses sites enfants et avec d'autres sites parents. Toutefois, un site enfant communique uniquement avec son site parent.

La figure suivante illustre le flux de travail impliqué dans une configuration de topologie parent-enfant GSLB.



Avant de commencer à configurer le déploiement de la topologie parent-enfant, assurez-vous d'avoir configuré une configuration d'équilibrage de charge standard pour chaque batterie de serveurs ou centre de données.

De plus, pour synchroniser la configuration GSLB entre les sites GSLB dans le déploiement, assurez-vous que :

- Les sites GLSB locaux sont configurés sur toutes les appliances de la configuration GSLB.
- Vous avez activé l'accès à la gestion sur tous les sites GSLB de la configuration.
- Vous avez configuré le pare-feu pour accepter la synchronisation automatique et les connexions MEP.
- Toutes les appliances Citrix ADC participant en tant que sites doivent avoir la même version du logiciel Citrix ADC (les sites ne sont pas dans une relation maître-esclave).
- Le mot de passe du nœud RPC est le même sur tous les sites GSLB de la configuration GSLB.

Pour configurer un déploiement parent-enfant à l'aide de l'assistant

Sous l'onglet Configuration, procédez comme suit :

1. Accédez à **Gestion du trafic** > **GSLB**, puis cliquez sur **Démarrer**.
2. Si vous n'avez pas configuré de serveur ADNS ou de serveur virtuel DNS pour le site, vous pouvez le faire maintenant.

a) Cliquez sur **Affichage**, puis sur **Ajouter**.
b) Entrez le nom du service, l'adresse IP et sélectionnez le protocole (ADNS/ADNS_TCP) par lequel les données sont échangées avec le service.

3. Sélectionnez **Topologie parent-enfant**.
4. Dans le champ Sélectionner le type de site, choisissez ;
   - **Parent** : lors de la configuration du site parent, vous devez configurer les sites enfants associés ainsi que les autres sites parents dans la configuration GSLB.
   - **Enfant** — Lors de la configuration du site enfant, vous devez configurer uniquement le site enfant et son site parent.

Pour configurer un site parent

1. Entrez le nom de domaine complet et spécifiez la période pendant laquelle l'enregistrement doit être mis en cache par les proxy DNS.
2. Configurez les sites GSLB. Chaque site doit être configuré avec un site GSLB local, et la configuration de chaque site doit inclure tous les autres sites en tant que sites GSLB distants. Il ne peut y avoir qu'un seul site local. Tous les autres sites sont des sites distants. Si l'adresse IP du site spécifiée appartient à l'appliance (par exemple, une adresse MIP ou une adresse SNIP), le site est un site local. Sinon, il s'agit d'un site distant.
3. Entrez les détails du site, tels que le nom du site et l'adresse IP du site.
   a) Sélectionnez le type de site.
   b) Vous pouvez également modifier le mot de passe RPC et, si nécessaire, le sécuriser.
   c) Si un moniteur doit être lié au service GSLB, sélectionnez la condition dans laquelle le moniteur doit surveiller le service. Cela ne sera efficace qu'une fois qu'un moniteur est lié aux services. Les conditions possibles sont :
      - **Always**. Surveillez le service GSLB en tout temps.
      - **Échec de MEP**. Surveillez le service GSLB uniquement lorsque l'échange de mesures via MEP échoue.
      - **Échec de MEP et le service est DOWN**. L'échange de mesures via MEP est activé, mais le statut du service, mis à jour via l'échange de mesures, est DOWN.
4. Configurez les services GSLB.
   a) Entrez les détails du service, tels que le nom du service, le type de service et le numéro de port.
   b) Associez le service à un site (local ou distant) en sélectionnant le site GSLB auquel appartient le service GSLB.
   c) Sélectionnez le moniteur qui doit être lié au service en cas d'échec de MEP, si nécessaire. Le service peut être un serveur existant ou vous pouvez créer un nouveau serveur ou un serveur virtuel.
      - Pour associer un serveur existant, sélectionnez le nom du serveur. L'adresse IP du service est renseignée automatiquement.

- Pour associer un nouveau serveur, créez un serveur en entrant les détails IP du serveur, son adresse IP publique et le numéro de port public.
- Pour associer un serveur virtuel, sélectionnez un serveur virtuel déjà existant ou cliquez sur **+** et ajoutez un nouveau serveur virtuel. Ce vserver est le vserver d'équilibrage de charge auquel ce service GSLB sera associé. Si l'adresse IP publique est différente de l'adresse IP du serveur, ce qui peut se produire dans un environnement NAT, entrez l'adresse IP publique et le numéro de port public.

5. Configurez les serveurs virtuels GSLB.
   a) Entrez le nom du serveur virtuel GSLB et sélectionnez le type d'enregistrement DNS.
   b) Cliquez sur **>** dans la zone **Sélectionner un service** et choisissez les services GSLB à lier au serveur virtuel GSLB.
   c) Cliquez sur **>** dans la zone **Liaison** de domaine pour afficher le nom de domaine lié au serveur virtuel GSLB.
   d) Choisissez la méthode GSLB pour sélectionner le service GSLB le plus performant. Les valeurs par défaut de la méthode GSLB, de la méthode de sauvegarde et de la pondération dynamique sont automatiquement renseignées par défaut. Vous pouvez les modifier si nécessaire.
      - Si vous choisissez la méthode **basée sur l'algorithme**, sélectionnez les méthodes primaires et de sauvegarde et spécifiez également l'option de pondération dynamique.
      - Si vous choisissez la méthode **Proximité statique**, sélectionnez la méthode de sauvegarde et la méthode de pondération dynamique. Indiquez également l'emplacement du fichier de base de données en cliquant sur l'icône **>** ou ajoutez un nouvel emplacement en cliquant sur **+** dans la zone Sélectionner une base de données d'emplacement.
      - Si vous choisissez la méthode **RTT (Dynamic Proximity)**, sélectionnez la méthode de sauvegarde et spécifiez la pondération du service et la valeur RTT en fonction de laquelle le service le plus performant doit être sélectionné.
6. Cliquez sur **Terminé** si la configuration est terminée. Le tableau de bord GSLB s'affiche.
7. Si vous avez modifié la configuration du site parent GSLB, cliquez sur **Synchroniser automatiquement GSLB** pour synchroniser la configuration avec les autres sites parents dans la configuration GSLB. Dans une topologie parent-enfant, la synchronisation des sites enfants est ignorée.
   - Avant la synchronisation, assurez-vous que la configuration du site local inclut des informations sur les sites distants.
   - Si la synchronisation en temps réel est activée, vous n'avez pas besoin de cliquer sur **Synchroniser automatiquement GSLB**. La synchronisation se produit automatiquement. Pour activer la synchronisation en temps réel, procédez comme suit :
     a) Accédez à **Gestion du trafic** > **GSLB** > **Tableau de bord** et cliquez sur **Modifier les paramètres GSLB**.

b) Activez la case à cocher **Synchronisation automatique de la configuration**.

8. Cliquez sur **Tester l'installation GSLB** pour vous assurer que les services ADNS ou les serveurs DNS répondent avec l'adresse IP correcte pour le nom de domaine configuré dans la configuration GSLB.

Pour configurer un site enfant

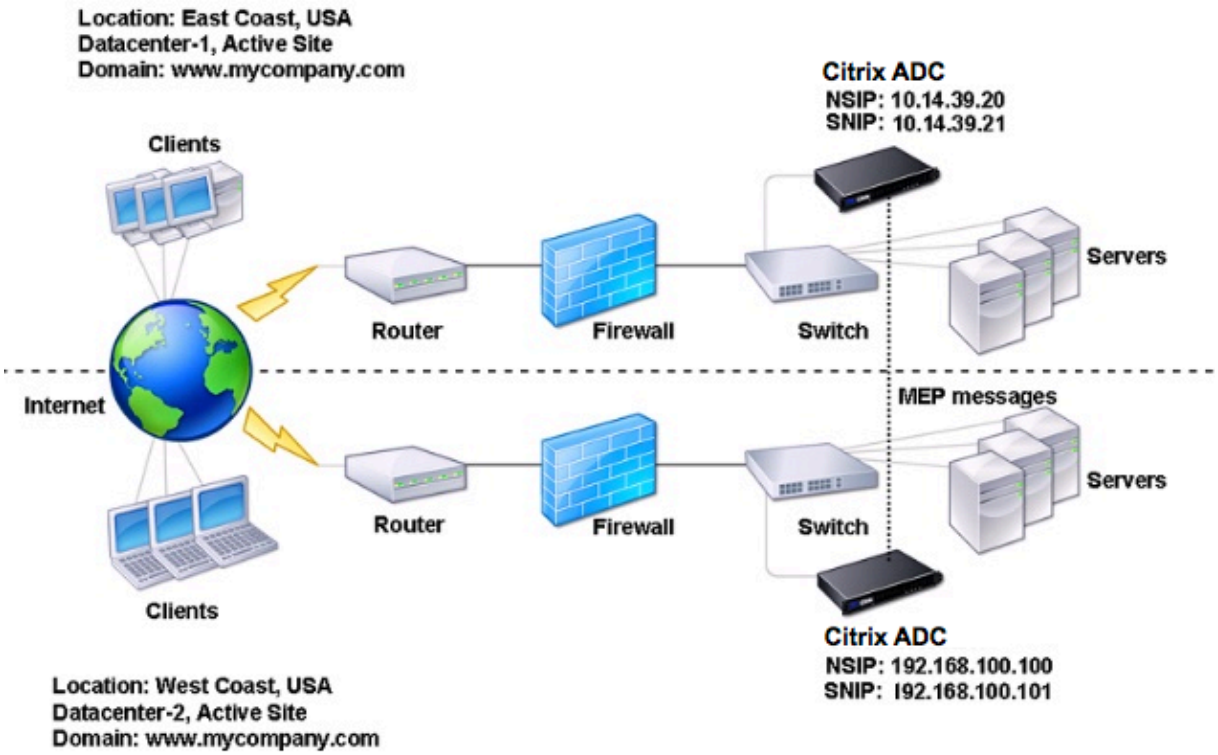
1. Configurez les sites GSLB.
   a) Entrez les détails du site, tels que le nom du site et l'adresse IP du site.
   b) Sélectionnez le type de site.
   c) Vous pouvez également modifier le mot de passe RPC et, si nécessaire, le sécuriser. 4. Si un moniteur est lié au service GSLB, sélectionnez la condition dans laquelle le moniteur doit surveiller le service. Les conditions possibles sont :
      - **Always**. Surveillez le service GSLB en tout temps.
      - **Échec de MEP**. Surveillez le service GSLB uniquement lorsque l'échange de mesures via MEP échoue.
      - **Échec de MEP et le service est DOWN**. L'échange de mesures via MEP est activé, mais le statut du service, mis à jour via l'échange de mesures, est DOWN.
2. Cliquez sur **Terminé** si la configuration est terminée. Le tableau de bord GSLB s'affiche.
3. Cliquez sur **Tester l'installation GSLB** pour vous assurer que les services ADNS ou les serveurs DNS répondent avec l'adresse IP correcte pour le nom de domaine configuré dans la configuration GSLB.

Configurer les entités GSLB individuellement

August 20, 2021

L'équilibrage global de la charge du serveur est utilisé pour gérer le flux de trafic vers un site Web hébergé sur deux batteries de serveurs distinctes qui se trouvent idéalement dans des emplacements géographiques différents. Prenons par exemple un site Web, www.mycompany.com, qui est hébergé sur deux batteries de serveurs ou centres de données géographiquement séparés. Les deux batteries de serveurs utilisent des appliances Citrix ADC. Les appliances Citrix ADC de ces batteries de serveurs sont configurées en mode à bras unique et fonctionnent comme des serveurs DNS faisant autorité pour le domaine www.mycompany.com. La figure suivante illustre cette configuration.

Figure 1. Topologie de base GSLB



Pour configurer une telle configuration GSLB, vous devez d'abord configurer une configuration d'équilibrage de charge standard pour chaque batterie de serveurs ou centre de données. Cela vous permet d'équilibrer la charge entre les différents serveurs de chaque batterie de serveurs. Ensuite, configurez les deux appliances Citrix ADC en tant que serveurs DNS (ADNS) faisant autorité. Ensuite, créez un site GSLB pour chaque batterie de serveurs, configurez des serveurs virtuels GSLB pour chaque site, créez des services GLSB et liez les services GSLB aux serveurs virtuels GSLB. Enfin, liez le domaine aux serveurs virtuels GSLB. Les configurations GSLB sur les deux appliances sur les deux sites différents sont identiques, bien que les configurations d'équilibrage de charge pour chaque site soient spécifiques à ce site.

Remarque : Pour configurer un site GSLB dans une configuration de cluster Citrix ADC, reportez-vous à la section Configuration de GSLB dans un cluster.

Configuration d'une configuration d'équilibrage de charge standard

Un serveur virtuel d'équilibrage de charge équilibre la charge entre différents serveurs physiques du centre de données. Ces serveurs sont représentés en tant que services sur l'appliance Citrix ADC, et les services sont liés au serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la configuration d'une configuration d'équilibrage de charge de base, voir Équilibrage de charge.

Configurer un service DNS faisant autorité

August 20, 2021

Lorsque vous configurez l'appliance Citrix ADC en tant que serveur DNS faisant autorité, il accepte les demandes DNS du client et répond avec l'adresse IP du centre de données auquel le client doit envoyer les demandes.

Remarque : pour que l'appliance Citrix ADC puisse faire autorité, vous devez également créer des enregistrements SOA et NS. Pour plus d'informations sur les enregistrements SOA et NS, voir Système de noms de domaine.

Pour créer un service ADNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service ADNS et vérifier la configuration :

```
add service <name> <IP>@ ADNS <port>

show service <name>
<!--NeedCopy-->
```

Exemple :

```
add service Service-ADNS-1 10.14.39.21 ADNS 53

show service Service-ADNS-1
<!--NeedCopy-->
```

Pour modifier un service ADNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set service <name> <IPAddress> ADNS <port>
<!--NeedCopy-->
```

Exemple :

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
<!--NeedCopy-->
```


Pour supprimer un service ADNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
rm service <name>
<!--NeedCopy-->
```

Exemple :

```
rm service Service-ADNS-1
<!--NeedCopy-->
```

Pour configurer un service ADNS à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Ajoutez un nouveau service ADNS ou sélectionnez un service existant et modifiez ses paramètres.

Configurer un site GSLB de base

August 20, 2021

Un site GSLB est une représentation d'un centre de données dans votre réseau et est un regroupement logique de serveurs virtuels, de services et d'autres entités réseau GSLB. Généralement, dans une configuration GSLB, de nombreux sites GSLB sont équipés pour servir le même contenu à un client. Ceux-ci sont généralement séparés géographiquement pour s'assurer que le domaine est actif même si un site tombe complètement en panne. Tous les sites de la configuration GSLB doivent être configurés sur chaque appliance Citrix ADC hébergeant un site GSLB. En d'autres termes, sur chaque site, vous configurez le site GSLB local et chaque site GSLB distant.

Une fois les sites GSLB créés pour un domaine, l'appliance Citrix ADC envoie les demandes client au site GSLB approprié, comme déterminé par les algorithmes GSLB configurés.

Pour créer un site GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un site GSLB et vérifier la configuration :

```
add gslb site <siteName> <siteIPAddress>
show gslb site <siteName>
<!--NeedCopy-->
```


Exemple :

```
add gslb site Site-GSLB-East-Coast 10.14.39.21
show glsb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Pour modifier ou supprimer un site GSLB à l'aide de l'interface de ligne de commande

- Pour modifier un site GSLB, utilisez la commande set gslb site, qui ressemble à la commande add gslb site, sauf que vous entrez le nom d'un site GSLB existant.
- Pour annuler la définition d'un paramètre de site, utilisez la commande unset gslb site, suivie de la valeur SiteName et du nom du paramètre à réinitialiser à sa valeur par défaut.
- Pour supprimer un site GSLB, utilisez la commande rm gslb site, qui accepte uniquement l'argument <name>.

Pour configurer un site GSLB de base à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Sites**.
2. Ajoutez un nouveau site GSLB ou sélectionnez un site GSLB existant et modifiez ses paramètres.

Pour afficher les statistiques d'un site GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat gslb site <siteName>
<!--NeedCopy-->
```

Exemple :

```
stat gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Pour afficher les statistiques d'un site GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Sites**.
2. Sélectionnez le site GSLB et cliquez sur **Statistiques**.

Configurer un service GSLB

August 20, 2021

Un service GSLB est une représentation d'un serveur virtuel d'équilibrage de charge ou de commutation de contenu. Un service GSLB local représente un serveur virtuel d'équilibrage de charge ou de commutation de contenu local. Un service GSLB distant représente un serveur virtuel d'équilibrage de charge ou de commutation de contenu configuré sur l'un des autres sites de la configuration GSLB. Sur chaque site de la configuration GSLB, vous pouvez créer un service GSLB local et n'importe quel nombre de services GSLB distants.

> **Important**
>
> Si le serveur virtuel d'équilibrage de charge se trouve dans un nœud GSLB lui-même ou dans un nœud enfant (dans le déploiement parent-enfant) et qu'aucun moniteur n'est lié au service GSLB, assurez-vous que les éléments suivants :
>
> L'adresse IP du service GLSB, le numéro de port et le protocole correspondent au que le service représente. Sinon, l'état du service est marqué comme étant DOWN.

Pour créer un service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service GSLB et vérifier la configuration :

```
1 add gslb service <serviceName> <serverName | IP> <serviceType> <port>-
     siteName <string>
2 show gslb service <serviceName>
3 <!--NeedCopy-->
```

Exemple :

```
1 add gslb service Service-GSLB-1 10.14.39.14 HTTP 80  - siteName Site-
     GSLB-East-Coast
2 show gslb service Service-GSLB-1
3 <!--NeedCopy-->
```

Pour modifier ou supprimer un service GSLB à l'aide de l'interface de ligne de commande

- Pour modifier un service GSLB, utilisez la commande <serviceName> set gslb service. Pour cette commande, spécifiez le nom du service GSLB dont vous souhaitez modifier la configuration. Vous pouvez modifier les valeurs existantes des paramètres spécifiés par vous ou définis

par défaut. Vous pouvez modifier la valeur de plusieurs paramètres dans la même commande. Reportez-vous à la commande add gslb service pour plus de détails sur les paramètres. Exemple

```
> set gslb service SKP_GSLB_NOTCNAME_SVC2 -maxBandWidth 25 -
   maxClient 8
Done
> sh gslb service SKP_GSLB_NOTCNAME_SVC2
SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
...
Max Conn: 8  Max Bandwidth: 25 kbits
<!--NeedCopy-->
```

- Pour réinitialiser un paramètre à sa valeur par défaut, vous pouvez utiliser la commande <serviceName> unset gslb service et les paramètres à annuler. Exemple

```
> unset gslb service SKP_GSLB_NOTCNAME_SVC2 maxBandWidth
Done
> sh gslb service SKP_GSLB_NOTCNAME_SVC2
SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
...
Max Conn: 8  Max Bandwidth: 0 kbits
<!--NeedCopy-->
```

- Pour supprimer un service GSLB, utilisez la commande <serviceName> rm gslb service.

Pour créer un service GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Services**.
2. Ajoutez un nouveau service GSLB ou sélectionnez un service existant et modifiez ses paramètres.

Pour afficher les statistiques d'un service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat gslb service <serviceName>
<!--NeedCopy-->
```

Exemple :

```
stat gslb service Service-GSLB-1
<!--NeedCopy-->
```


Pour afficher les statistiques d'un service GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Services**.
2. Sélectionnez le service GSLB et cliquez sur **Statistiques**.

Configurer un groupe de services GSLB

August 20, 2021

Le groupe de services vous permet de gérer un groupe de services aussi facilement qu'un seul service. Par exemple, si vous activez ou désactivez une option, telle que la compression, la surveillance de l'intégrité ou l'arrêt progressif, pour un groupe de services, l'option est activée ou désactivée pour tous les membres du groupe de services.

Après avoir créé un groupe de services, vous pouvez le lier à un serveur virtuel et ajouter des services au groupe. Vous pouvez également lier des moniteurs aux groupes de services.

> **Important**
>
> Si le serveur virtuel d'équilibrage de charge se trouve soit dans un nœud GSLB lui-même, soit dans un nœud enfant (dans le déploiement parent-enfant) et qu'aucun moniteur n'est lié au service GSLB, vérifiez que ce qui suit :
>
> L'adresse IP du groupe de services GLSB, le numéro de port et le protocole correspondent le serveur virtuel représenté par le service. Sinon, l'état du service est marqué comme étant DOWN.

Citrix ADC prend en charge les types de groupes de services GSLB suivants.

- Groupes de services basés sur l'adresse IP
- Groupes de services basés sur un nom de domaine
- Groupes de services de mise à l'échelle automatique basés sur un nom de domaine

Groupes de services de mise à l'échelle automatique basés sur un nom de domaine GSLB

La solution GSLB (hybride et multi-cloud Global Server load Balancing) de Citrix ADC permet aux clients de distribuer le trafic d'application entre plusieurs centres de données dans des clouds hybrides, plusieurs clouds et sur site. La solution Citrix ADC GSLB prend en charge diverses solutions d'équilibrage de charge, telles que l'équilibreur de charge Citrix ADC, Elastic Load Balancing (ELB) pour Amazon Web Services (AWS) et d'autres équilibreurs de charge tiers. En outre, la solution GSLB effectue un équilibrage de charge global même si les couches GSLB et équilibrage de charge sont gérées de manière indépendante.

Dans les déploiements cloud, les utilisateurs reçoivent un nom de domaine comme référence lorsqu'ils accèdent à la solution d'équilibrage de charge à des fins de gestion. Il est recommandé que les entités externes n'utilisent pas les adresses IP auxquelles ces noms de domaine résolvent. En outre, les couches d'équilibrage de charge sont mises à l'échelle vers le haut ou vers le bas en fonction de la charge, et les adresses IP ne sont pas garanties d'être statiques. Par conséquent, il est recommandé d'utiliser le nom de domaine pour faire référence aux points de terminaison d'équilibrage de charge au lieu des adresses IP. Cela nécessite que les services GSLB soient référencés en utilisant le nom de domaine au lieu des adresses IP et il doit consommer toutes les adresses IP renvoyées pour le nom de domaine de la couche d'équilibrage de charge et avoir une représentation pour le même dans GSLB.

Pour utiliser des noms de domaine au lieu des adresses IP lorsque vous faites référence aux points de terminaison d'équilibrage de charge, vous pouvez utiliser les groupes de services basés sur des noms de domaine pour GSLB.

Surveillance des groupes de services basés sur le nom de domaine GSLB

L'appliance Citrix ADC dispose de deux moniteurs intégrés qui surveillent les applications basées sur TCP : tcp-default et ping-default. Le moniteur tcp-default est lié à tous les services TCP et le moniteur ping-default est lié à tous les services non-TCP. Les moniteurs intégrés sont liés par défaut aux groupes de services GSLB. Cependant, il est recommandé de lier un moniteur spécifique à une application aux groupes de services GSLB.

Recommandation pour définir l'option des moniteurs de déclenchement sur MEPDOWN

L'option Trigger Moniteurs peut être utilisée pour indiquer si le site GSLB doit toujours utiliser les moniteurs, ou utiliser des moniteurs lorsque le protocole d'échange de mesures (MEP) est DOWN.

L'option Trigger Moniteurs est définie sur ALWAYS par défaut.

Lorsque l'option Trigger Monitors est définie sur ALWAYS, chaque nœud GSLB déclenche les moniteurs indépendamment. Si chaque nœud GSLB déclenche les moniteurs indépendamment, alors chaque nœud GSLB peut fonctionner sur différents ensembles de services GSLB. Cela peut entraîner des divergences dans les réponses DNS pour les demandes DNS qui atterrissent sur ces nœuds GSLB. En outre, si chaque nœud GSLB surveille indépendamment, le nombre de sondes de moniteur atteignant l'entité d'équilibrage de charge augmente. Les entrées de persistance deviennent également incompatibles entre les nœuds GSLB.

Par conséquent, il est recommandé que l'option Trigger Moniteurs sur l'entité de site GSLB soit définie sur MEPDOWN. Lorsque l'option Trigger Moniteurs est définie sur MEPDOWN, la résolution du domaine d'équilibrage de charge et la propriété de surveillance appartiennent au nœud GSLB local. Lorsque l'option Trigger Moniteurs est définie sur MEPDOWN, la résolution du domaine d'équilibrage de charge et la surveillance subséquente sont effectuées par le nœud GSLB local d'un groupe de services GSLB.

Les résultats sont ensuite propagés à tous les autres nœuds participant à GSLB à l'aide du protocole MEP (Metrics Exchange Protocol).

En outre, chaque fois que le jeu d'adresses IP associé à un domaine d'équilibrage de charge est mis à jour, il est notifié via MEP.

Limites des groupes de services GSLB

- Pour un domaine d'équilibrage de charge, l'adresse IP renvoyée dans la réponse DNS est généralement l'adresse IP publique. L'adresse IP privée ne peut pas être appliquée dynamiquement lorsque le domaine d'équilibrage de charge est résolu. Par conséquent, le port IP public et le port IP privé pour les groupes de services à échelle automatique basés sur le nom de domaine GSLB sont les mêmes liaisons de port IP. Ces paramètres ne peuvent pas être définis explicitement pour les groupes de services de mise à l'échelle automatique basés sur le nom de domaine.
- La persistance du site, les vues DNS et le clustering ne sont pas pris en charge pour les groupes de services GSLB.

Configurer et gérer des groupes de services GSLB à l'aide de l'interface de ligne de commande

Opération	Commande CLI
Pour ajouter un groupe de services GSLB|`add gslb serviceGroup <serviceGroupName>@ <serviceType> [-autoScale (DISABLED	DNS)] -siteName <string>`
	Exemple : **add gslb serviceGroup** Service-Group-1 http -siteName Site1 -autoScale DNS
Pour lier un groupe de services GSLB à un serveur virtuel|`bind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>)| <serverName>@	((-monitorName <string>@`
	Exemple : **bind gslb serviceGroup** Service-Group-1 203.0.113.2; **bind gslb serviceGroup** Service-Group-1 S1 80; **bind gslb serviceGroup** Service-Group-1 -monitorName Mon1
Pour délier un groupe de services GSLB à un serveur virtuel|`unbind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>)| <serverName>@	-monitorName <string>@)`
	Exemple :**unbind gslb ServiceGroup** Service-Group-1 -MonitorName Mon1
Pour définir des paramètres pour un groupe de services GSLB|`set gslb serviceGroup <serviceGroupName>@ [(<serverName>@ <port> [-weight <positive_integer>] [-hashId <positive_integer>] [-publicIP <ip_addr|ipv6_addr|*>] [-publicPort <port>])| -maxClient <positive_integer>	-cip (ENABLED | DISABLED)| <cipHeader>	-cltTimeout <secs>	-svrTimeout <secs>	-maxBandwidth <positive_integer>	-monThreshold <positive_integer>	-downStateFlush (ENABLED | DISABLED)] [-monitorName <string> -weight <positive_integer>] [-healthMonitor (YES | NO)] [-comment <string>] [-appflowLog (ENABLED | DISABLED)]`

|Pour annuler la définition de paramètres d'un groupe de services GSLB|unset gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port> [-weight] [-hashId] [-publicIP] [-publicPort]] [-maxClient] [-cip] [-cltTimeout] [-svrTimeout] [-maxBandwidth] [-monThreshold] [-appflowLog] [-monitorName] [-weight] [-healthMonitor] [-cipHeader] [-downStateFlush] [-comment]
|Pour activer un groupe de services GSLB|enable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>]
||Exemple :**enable gslb serviceGroup** SG1 S1 80
|Pour désactiver un groupe de services GSLB|"'disable gslb serviceGroup @ [@] [-delay] [-graceFul (YES /| NO)]

```
||Exemple :**disable gslb serviceGroup** SRG2 S1 80
||**Remarque** : Le groupe de services qui doit être désactivé doit être un groupe de services DBS et non un groupe de services de mise à l'échelle automatique.
|Pour supprimer un groupe de services GSLB|``rm gslb serviceGroup <serviceGroupName>``
||Exemple :**rm gslb serviceGroup** Service-Group-1
|Pour afficher les statistiques d'un groupe de services GSLB|``stat gslb serviceGroup [<serviceGroupName>]``
||Exemple :**stat gslb ServiceGroup** Service-Group-1
|Pour afficher les propriétés d'un groupe de services GSLB|``show gslb serviceGroup [<serviceGroupName>  -includeMembers]``
||Exemple : **show gslb serviceGroup** SG1; **show gslb serviceGroup** -includeMembers

### Modifications apportées aux commandes de l'interface de ligne de commande GSLB existantes

Le tableau suivant répertorie certaines des modifications apportées aux commandes GSLB existantes aprés l'introduction des groupes de services GSLB.

|Commande CLI|Modification
|--|--|
|bind gslb vserver|Le nom du groupe de services est ajouté à la commande bind.
||Exemple :```bind gslb vserver <name> ((-serviceName <string> [-weight <positive_integer>] ) | <serviceGroupName>@ | | (-domainName <string> [-TTL <secs>] [-backupIP<ip_addr|ipv6_addr|*>] [-cookieDomain <string>] [-cookieTimeout <mins>][-sitedomainTTL <secs>]) | (-policyName <string>@ [-priority<positive_integer>] [-gotoPriorityExpression <expression>] [-type REQUEST | RESPONSE )]))
<!--NeedCopy-->
```


|unbind gslb vserver|Le groupe de services est ajouté à la commande unbind.
|Exemple :|“‘unbind gslb vserver (-serviceName @ /(-domainName [-backupIP] [-cookieDomain]) | -policyName @)

```
|show gslb site|Lorsque cette commande est exécutée, les groupes de services GSLB sont également affichés.
|show gslb vs|Lorsque cette commande est exécutée, les groupes de services GSLB sont affichés.
|stat gslb vs|Lorsque cette commande est exécutée, les statistiques des groupes de services GSLB sont également affichées.
|show lb monitor bindings|Lorsque cette commande est exécutée, les liaisons de groupe de services GSLB sont également affichées.

### Configurer les groupes de services GSLB à l'aide de l'interface graphique

1.  Accédez à **Gestion du trafic** > **GSLB** > **Groupes de services**.
1.  Créez un groupe de services et définissez le mode Mise à l'échelle automatique sur DNS.

### Configurer la persistance du site pour les groupes de services GSLB

Vous pouvez configurer la persistance du site pour les groupes de services basés sur l'adresse IP et le nom de domaine. La persistance du site n'est pas prise en charge pour les groupes de services de mise à l'échelle automatique basés sur un nom de domaine.

#### Pour définir la persistance du site en fonction des cookies HTTP à l'aide de l'interface de ligne de commande

-  Pour la persistance du proxy de connexion, vous n'avez pas à définir le préfixe du site.

 À l'invite de commandes, tapez :
```

set gslb service group [-sitePersistence]

```
-  Pour la persistance de redirection HTTP, vous devez d'abord définir le préfixe de site pour un membre du groupe de services, puis définir le paramétre de persistance HttPreDirect pour le groupe de services.

```



```
À l'invite de commandes, tapez :
```

set gslb servicegroup <serviceGroup member name|Ip> [-sitePrefix]

set gslb servicegroup [-sitePersistence]
“‘

Exemples :

- Persistance du proxy de connexion

  set gslbservicegroup sg1 -sitePersistence connectionProxy

- Persistance HttpRedirect

  set gslb servicegroup sg2 test1 80 -sitePrefix vserver-GSLB-1

  set gslb servicegroup sg2 -sitePersistence hTTPRedirect

Pour définir la persistance du site en fonction des cookies à l’aide de l’interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Groupes de services** et sélectionnez le groupe de services que vous souhaitez configurer pour la persistance du site (par exemple, ServiceGroup-GSLB-1).
2. Cliquez sur la section **Persistance du site** et définissez la persistance qui répond à vos besoins.

> **Conseil**
>
> Pour obtenir un scénario de déploiement et un exemple de configuration de groupes de services GSLB, consultez les rubriques suivantes :
>
> - Cas d’utilisation : Déploiement d’un groupe de services de mise à l’échelle automatique basé sur un nom de domaine
> - Cas d’utilisation : Déploiement d’un groupe de services de mise à l’échelle automatique basé sur l’adresse IP

Configurer un serveur virtuel GSLB

August 20, 2021

Un serveur virtuel GSLB est une entité qui représente un ou plusieurs services GSLB et équilibre le trafic entre eux. Il évalue les méthodes ou algorithmes GSLB configurés pour sélectionner un service GSLB auquel envoyer la demande client.

> **Remarque**
>
> Une exigence de protocole de serveur virtuel GSLB consiste principalement à créer une relation

> entre le serveur virtuel et les services liés au serveur virtuel. Cela permet également de maintenir la cohérence de la CLI/API pour d'autres types de serveurs virtuels. Le paramètre Type de service sur un service ou un serveur virtuel n'est pas utilisé lors du traitement des demandes DNS. Il est plutôt référencé pendant la persistance du site, la surveillance et pour effectuer des recherches via MEP.

Pour créer un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un serveur virtuel GSLB et vérifier la configuration :

```
1 -  add gslb vserver <name> <serviceType> -ipType (IPv4 | IPv6)
2 -  show gslb vserver <name>
3 <!--NeedCopy-->
```

Exemple :

```
1 add gslb vserver Vserver-GSLB-1 HTTP -ipType IPv4
2 add gslb vserver Vserver-GSLB-2 HTTP -ipType IPv6
3 show gslb vserver Vserver-GSLB-1
4 show gslb vserver Vserver-GSLB-2
5 <!--NeedCopy-->
```

Pour modifier ou supprimer un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

- Pour modifier un serveur virtuel GSLB, utilisez la commande `set gslb vserver`. Cette commande fonctionne de la même manière que la commande `add gslb vserver`, sauf que vous entrez le nom d'un serveur virtuel GSLB existant.
- Pour réinitialiser un paramètre à valeur par défaut, vous pouvez utiliser la commande `unset gslb vserver` suivie de la valeur vServerName et du nom du paramètre dont la définition doit être annulée.
- Pour supprimer un serveur virtuel GSLB, utilisez la commande `rm gslb vserver`, qui accepte uniquement l'argument name.

Pour configurer un serveur virtuel GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels**.
2. Ajoutez un nouveau serveur virtuel GSLB ou sélectionnez un serveur virtuel GSLB existant et modifiez ses paramètres.

Pour afficher les statistiques d'un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
stat gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

Pour afficher les statistiques d'un serveur virtuel GSLB à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels**, sélectionnez le serveur virtuel et cliquez sur **Statistiques**.

Statistiques du serveur virtuel GSLB

À partir de Citrix ADC version 12.1 build 51.xx et versions ultérieures, les statistiques du serveur virtuel GSLB affichent également les informations suivantes en plus des détails tels que : accès vserver, session de persistance en cours, octets de demande, octets de réponse, seuil de débordement, accès de débordement, client actuel établi et les accès de sauvegarde vserver ayant échoué.

- **Échecs de la méthode LB primaire** : Nombre de fois où la méthode GSLB principale a échoué.
- **Échec de la méthode de base de sauvegarde** : nombre de fois où la méthode GSLB de sauvegarde a échoué.
- **Vserver Persistence hits** : nombre de fois que la demande est traitée via les sessions de persistance.

Les statistiques du serveur virtuel GSLB affichent également les statistiques des membres du groupe de services liés au serveur virtuel.

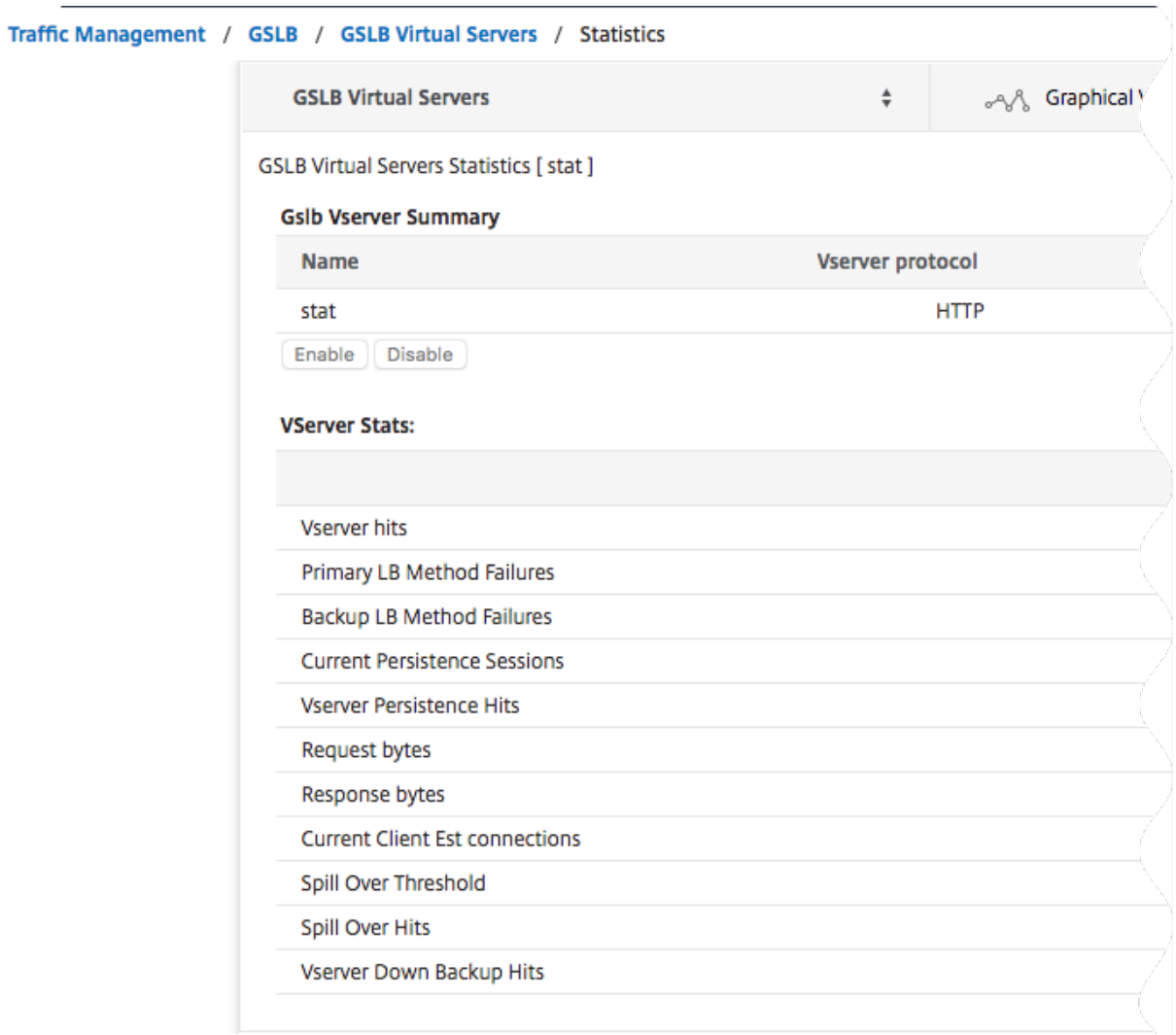
> **Remarque :**
> La méthode principale ou la méthode de sauvegarde peut échouer lorsque la méthode principale est la proximité statique et que la méthode de sauvegarde est RTT. Dans ce scénario, s'il n'y a pas d'emplacement correspondant à l'IP LDNS, la proximité statique échoue et la méthode de sauvegarde est tentée. Les statistiques sont mises à jour en fonction des éléments suivants :
>
> - Si la méthode de sauvegarde réussit, seules les statistiques d'échec de la méthode principale sont incrémentées.
> - Si le calcul RTT ne réussit pas, la méthode de sauvegarde échoue également. Dans ce cas,

> les statistiques de défaillance de la méthode primaire et de la méthode de sauvegarde sont incrémentées.
>
> Lorsque la méthode de sauvegarde échoue, la méthode de dernier recours du round robin est utilisée.

L'image suivante est un exemple de statistiques de serveur virtuel GSLB à partir de l'interface de ligne de commande.

```
Gslb Vserver Summary
                Protocol        State   Health  actSvcs inactSvc
gslbvip             HTTP         DOWN        0        0        0

VServer Stats:
                                        Rate (/s)               Total
Vserver hits                                 0                      0
Primary LB Method Failures                  --                      0
Backup LB Method Failures                   --                      0
Current Persistence Sessions                --                      0
Vserver Persistence Hits                    --                      0
Request bytes                                0                      0
Response bytes                               0                      0
Current Client Est connections              --                      0
Spill Over Threshold                        --                      0
Spill Over Hits                             --                      0
Vserver Down Backup Hits                    --                      0

Note: The above counters are the sum of all bound GSLB services
 Done
```

L'image suivante est un exemple de statistiques de serveur virtuel GSLB à partir de l'interface graphique.



Statistiques des services GSLB

Lorsque vous exécutez la commande stat gslb service à partir de la ligne de commande ou cliquez sur le **lien Statistiques** de l'utilitaire de configuration, les détails suivants du service s'affichent :

- **Demander des octets.** Nombre total d'octets de demande reçus sur ce service ou serveur virtuel.
- **Octets de réponse.** Nombre d'octets de réponse reçus par ce service ou serveur virtuel.
- **Connexions établies par le client actuel.** Nombre de connexions client dans l'état ESTABLISHED.
- **Charge actuelle sur le service.** Chargement sur le service (Calculé à partir du moniteur de charge lié au service).

Les données du nombre de demandes et de réponses, ainsi que le nombre de connexions client et serveur actuelles peuvent ne pas être affichées ou ne pas être synchronisées avec les données du

serveur virtuel d'équilibrage de charge correspondant.

Effacement des statistiques de serveur virtuel ou de service GSLB

Remarque : Cette fonctionnalité est disponible dans NetScaler version 10.5.e.

Vous pouvez désormais effacer les statistiques d'un serveur virtuel et d'un service GSLB. Citrix ADC propose les deux options suivantes pour effacer les statistiques :

- **Base** : efface les statistiques spécifiques au serveur virtuel, mais conserve les statistiques qui sont fournies par le service GLSB lié.
- **Complet** : efface à la fois le serveur virtuel et les statistiques de service GSLB liées.

Pour effacer les statistiques d'un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat gslb vserver <name> -clearstats <basic | full>
<!--NeedCopy-->
```

Exemple :

```
stat gslb vserver Vserver-GSLB-1 - clearstats basic
<!--NeedCopy-->
```

Pour effacer les statistiques d'un service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat gslb service <name> -clearstats <basic | full>
<!--NeedCopy-->
```

Exemple :

```
stat gslb service service-GSLB-1 - clearstats basic
<!--NeedCopy-->
```

Pour effacer les statistiques d'un serveur virtuel GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels**.
2. Sélectionnez le serveur virtuel GSLB, cliquez sur **Statistiques**, puis cliquez sur **Effacer**.
3. Dans la liste déroulante **Effacer**, sélectionnez **Basique** ou **Complet**, puis cliquez sur **OK**.

Pour effacer les statistiques d'un service GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Services**.
2. Sélectionnez le service GSLB, cliquez sur **Statistiques**, puis cliquez sur **Effacer**.
3. Dans la liste déroulante **Effacer**, sélectionnez **Basique** ou **Complet**, puis cliquez sur **OK**.

Activation et désactivation des serveurs virtuels GSLB

Lorsque vous créez un serveur virtuel GSLB, il est activé par défaut. Si vous désactivez le serveur virtuel GSLB, lors de la réception d'une demande DNS, l'appliance Citrix ADC ne prend aucune décision GSLB basée sur la méthode GSLB configurée. Au lieu de cela, la réponse à la requête DNS contient les adresses IP de tous les services liés au serveur virtuel.

Pour activer ou désactiver un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
enable gslb vserver <name>@

disable gslb vserver <name>@
<!--NeedCopy-->
```

Exemple :

```
enable gslb vserver Vserver-GSLB-1
disable gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

Pour activer ou désactiver un serveur virtuel GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels**.
2. Sélectionnez un serveur virtuel et, dans la liste **Action**, sélectionnez **Activer** ou **désactiver** .

Lier les services GSLB à un serveur virtuel GSLB

August 20, 2021

Une fois les services GSLB et le serveur virtuel configurés, les services GSLB pertinents doivent être liés au serveur virtuel GSLB pour activer la configuration.

Pour lier un service GSLB à un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier un service GSLB à un serveur virtuel GSLB et vérifiez la configuration :

```
bind gslb vserver <name> -serviceName <string>

show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
bind gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

Pour délier un service GSLB d'un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind gslb vserver <name> -serviceName <string>
<!--NeedCopy-->
```

Pour lier des services GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur un serveur virtuel.
2. Cliquez dans la section **Domaines**, puis configurez un domaine et liez le domaine.

Lier un domaine à un serveur virtuel GSLB

August 20, 2021

Pour faire d'une appliance Citrix ADC le serveur DNS faisant autorité pour un domaine, vous devez lier le domaine au serveur virtuel GSLB. Lorsque vous liez un domaine à un serveur virtuel GSLB, l'appliance Citrix ADC ajoute un enregistrement d'adresse pour le domaine, contenant le nom du serveur virtuel GSLB. Les enregistrements de début d'autorité (SOA) et de serveur de noms (NS) pour le domaine GSLB doivent être ajoutés manuellement.

Pour plus d'informations sur la configuration des enregistrements SOA et NS, voir Système de noms de domaine.

Pour lier un domaine à un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier un domaine à un serveur virtuel GSLB et vérifiez la configuration :

```
bind gslb vserver <name> -domainName <string>
show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
bind gslb vserver Vserver-GSLB-1 -domainName www.mycompany.com
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

Pour délier un domaine GSLB d'un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind gslb vserver <name> -domainName <string>
<!--NeedCopy-->
```

Pour lier un domaine à un serveur virtuel GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels**.
2. Dans le volet Serveurs virtuels GSLB, sélectionnez le serveur virtuel GSLB auquel vous souhaitez lier le domaine (par exemple, vServer-GSLB-1) et cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel GSLB, sous l'onglet Domaines, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau domaine, cliquez sur **Ajouter**.
   - Pour modifier un domaine existant, sélectionnez le domaine, puis cliquez sur **Ouvrir**.
4. Dans la boîte de dialogue Créer un domaine GSLB ou Configurer un domaine GSLB, spécifiez les valeurs des paramètres suivants comme indiqué :
   - Nom de domaine* : nom de domaine (par exemple, www.monentreprise.fr)

   * Paramètre obligatoire
5. Cliquez sur Créer.
6. Cliquez sur OK.

Pour afficher les statistiques d'un domaine à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat gslb domain <name>
<!--NeedCopy-->
```

Exemple :

```
stat gslb domain www.mycompany.com
<!--NeedCopy-->
```

Remarque : Pour afficher les statistiques d'un domaine GSLB particulier, entrez le nom du domaine exactement tel qu'il a été ajouté à l'appliance Citrix ADC. Si vous ne spécifiez pas le nom de domaine ou si vous spécifiez un nom de domaine incorrect, les statistiques de tous les domaines GSLB configurés s'affichent.

Pour afficher les statistiques d'un domaine à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels**.
2. Dans le volet Serveurs virtuels GSLB, sélectionnez le serveur virtuel GSLB (par exemple, vServer-GSLB-1) et cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel GSLB, sous l'onglet Domaines, sélectionnez le domaine, puis cliquez sur **Statistiques s.**

Pour afficher les détails de configuration des entités liées à un domaine GSLB à l'aide de la ligne de commande

Remarque : Cette fonctionnalité est disponible dans NetScaler version 10.5.e.

À l'invite de commandes, tapez :

```
show gslb domain <name>
<!--NeedCopy-->
```

Exemple :

```
show gslb domain gslb1.com
       gslb1.com
       gvs1 - HTTP    state: DOWN
       DNS Record Type: A
       Configured Method: LEASTCONNECTION
       Backup Method: ROUNDROBIN
```



```
7         Persistence Type: NONE
8         Empty Down Response: DISABLED
9         Multi IP Response: DISABLED
10        Dynamic Weights: DISABLED
11
12        gsvc1 (10.102.239.165: 80)- HTTP State: DOWN    Weight: 1
13               Dynamic Weight: 0    Cumulative Weight: 1
14               Effective State: DOWN
15               Threshold : BELOW
16
17               Monitor Name : http
18                      State: DOWN   Weight: 1
19                      Probes: 144   Failed [Total: 144 Current: 144]
20                      Last response: Failure - TCP syn sent, reset
                           received.
21                      Response Time: 2000 millisec
22
23        gsvc2 (10.102.239.179: 80)- HTTP State: DOWN    Weight: 1
24               Dynamic Weight: 0    Cumulative Weight: 1
25               Effective State: DOWN
26               Threshold : BELOW
27
28               Monitor Name : http-ecv
29                      State: DOWN   Weight: 1
30                      Probes: 141   Failed [Total: 141 Current: 141]
31                      Last response: Failure - TCP syn sent, reset
                           received.
32                      Response Time: 2000 millisec
33 Done
34 <!--NeedCopy-->
```

Pour afficher les détails de configuration des entités liées à un domaine GSLB à l'aide de l'utilitaire de configuration

Remarque : Cette fonctionnalité est disponible dans NetScaler version 10.5.e.

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur un serveur virtuel.
2. Cliquez sur le champ situé sous le volet **Domaines** .
3. Dans la boîte de dialogue **Liaison de domaine de serveur virtuel GSLB**, sélectionnez un domaine, puis cliquez sur **Afficher les liaisons**.

Exemple de configuration et de configuration GSLB

January 21, 2021

Une organisation dispose d'un réseau géographiquement dispersé et dispose de trois centres de données situés aux États-Unis, au Mexique et en Colombie. Dans la configuration liée à ces emplacements, ceux-ci sont appelés respectivement US, MX et CO. À chaque emplacement, l'entreprise dispose d'une batterie de serveurs, qui fournit le même contenu et la configuration fonctionne comme prévu. L'appliance Citrix ADC à chaque emplacement est configurée via un serveur virtuel avec le protocole HTTP sur le port 80.

L'organisation a mis en œuvre la configuration GSLB en ajoutant un identificateur de site à chaque site. L'identificateur de site inclut un nom de site et une adresse IP appartenant à l'appliance Citrix ADC et utilisés pour les communications GSLB.
Chaque site dispose d'un site local à l'appliance. En outre, chaque site dispose de deux sites distants de l'appliance locale. Sur chaque site, un serveur virtuel GSLB est créé avec le même nom. Ce serveur virtuel identifie le site Web de l'organisation à l'échelle mondiale et n'a aucune adresse IP associée à celui-ci.
Le programme d'installation dispose également de services GSLB configurés qui pointent vers les serveurs virtuels d'équilibrage de charge configurés sur chaque site GSLB en spécifiant l'adresse IP, le protocole et le numéro de port du serveur virtuel respectif. Ces services sont liés au serveur virtuel GSLB.

Remarque : Dans la procédure ci-dessous, les commandes utilisent des adresses IP privées pour les sites GSLB. Pour les sites publics et les services GSLB, assurez-vous d'utiliser des adresses IP publiques pour ces sites.

Le tableau suivant répertorie les adresses IP et les emplacements utilisés dans l'exemple :

Adresse IP	Emplacement
10.3.1.101	IP du site de Citrix ADC local.
172.16.1.101	IP du site de l'emplacement distant Site-MX.
192.168.1.101	IP du site de l'emplacement distant Site-co.
172.16.1.100	IP de service de localisation distante Site-MX.
10.3.1.100	IP du service de Citrix ADC local.
192.168.1.100	IP de service de localisation distante Site-co.

Lorsque vous ajoutez un site GSLB, si le site communique uniquement sur Internet, utilisez le champ « IP publique ». Par exemple, lorsqu'il n'y a pas de connectivité VPN de site à site entre les sites GSLB.

Pour configurer l'installation de GSLB avec les appliances Citrix ADC à l'aide des commandes CLI

1. Activez la fonctionnalité GSLB, si ce n'est déjà fait.

```
enable ns feature gslb
<!--NeedCopy-->
```

2. Identifier un SNIP qui pour ajouter un site GSLB local.
3. Ajoutez le site GSLB pour l'appliance Citrix ADC locale.

```
add gslb site site-US 10.3.1.101
<!--NeedCopy-->
```

4. Ajoutez les sites GSLB pour les appliances Citrix ADC distantes.

```
add gslb site site-MX 172.16.1.101
add gslb site site-CO 192.168.1.101
<!--NeedCopy-->
```

5. Ajoutez le serveur virtuel GSLB qui fait référence à un service utilisé dans la configuration GSLB :

```
add gslb vserver gslb-lb HTTP
<!--NeedCopy-->
```

6. Ajoutez les services GSLB pour chaque site participant à la configuration GSLB :

```
add gslb service gslb_SVC30 172.16.1.100 HTTP 80 -siteName site-MX
add gslb service gslb_SVC10 10.3.1.100 HTTP 80 -siteName site-US
add gslb service gslb_SVC20 192.168.1.100 HTTP 80 -siteName site-
   CO
<!--NeedCopy-->
```

7. Liez les services GSLB au serveur virtuel GSLB :

```
bind gslb vserver gslb-lb -serviceName gslb_SVC10
bind gslb vserver gslb-lb -serviceName gslb_SVC20
bind gslb vserver gslb-lb -serviceName gslb_SVC30
<!--NeedCopy-->
```

8. Liez le domaine au serveur virtuel GSLB.

```
bind gslb vserver gslb-lb -domainName www.mycompany.com -TTL 30
<!--NeedCopy-->
```


9. Ajoutez un service ADNS qui écoute les requêtes DNS.

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

Synchroniser la configuration dans une configuration GSLB

August 20, 2021

Généralement, une configuration GSLB comporte quelques centres de données avec un site GSLB configuré pour chaque centre de données. Dans chaque Citrix ADC, participant à GSLB, configurez un site GSLB en tant que site local et les autres en tant que sites distants. Lorsque vous ajoutez un autre site GSLB ultérieurement, vous devez vous assurer que la configuration sur tous les sites GSLB est identique. Vous pouvez utiliser l'option de synchronisation de configuration GSLB de Citrix ADC pour synchroniser la configuration entre les sites GSLB.

L'appliance Citrix ADC à partir de laquelle vous utilisez l'option de synchronisation est appelée « site principal » et les sites GSLB sur lesquels la configuration est copiée en tant que « sites subordonnés ». Lorsque vous synchronisez une configuration GSLB, les configurations de tous les sites GSLB participant à la configuration GSLB sont similaires à celles du site principal.

La synchronisation est effectuée uniquement sur les sites parents. La synchronisation n'affecte pas la configuration des sites enfants GSLB. En effet, les configurations de site parent et de site enfant ne sont pas identiques. La configuration des sites enfants comprend uniquement ses propres informations et celle de son site parent. En outre, les services GSLB ne doivent pas toujours être configurés dans les sites enfants.

- Le nœud principal détecte les différences entre la configuration du nœud principal et du nœud subordonné, et modifie la configuration du nœud subordonné pour le rendre similaire au nœud principal.

  Si vous forcez une synchronisation (utilisez l'option « forcer la synchronisation »), l'appliance supprime la configuration GSLB du nœud subordonné, puis configure le subordonné pour qu'elle soit similaire au nœud principal.

- Pendant la synchronisation, si une commande échoue, la synchronisation n'est pas interrompue et le message d'erreur est enregistré dans un fichier **.err** dans le répertoire **/var/netscaler/gslb** .

- La synchronisation est effectuée uniquement sur les sites parents. La synchronisation n'affecte pas la configuration des sites enfants GSLB. En effet, les configurations de site parent et de site enfant ne sont pas identiques. La configuration des sites enfants comprend uniquement ses

propres informations et celle de son site parent. En outre, les services GSLB ne doivent pas toujours être configurés dans les sites enfants.

- Si vous désactivez la connexion utilisateur interne, la synchronisation automatique GSLB utilise les clés SSH pour synchroniser la configuration. Toutefois, pour utiliser la synchronisation automatique GSLB dans l'environnement de partition, vous devez activer la connexion utilisateur interne et vous assurer que le nom d'utilisateur de la partition dans les sites GSLB locaux et distants est le même.

> **Remarque**
>
> - Sur le nœud RPC du site GSLB distant, configurez le pare-feu pour qu'il accepte les connexions de synchronisation automatique en spécifiant l'adresse IP du site distant (adresse IP du cluster pour la configuration du cluster) et le port (3010 pour RPC et 3008 pour RPC sécurisé). Si la route par défaut pour atteindre les sites distants se trouve dans le sous-réseau de gestion, comme dans la plupart des cas, NSIP est utilisé comme adresse IP source.
>
> Pour configurer une adresse IP source différente, vous devez disposer de l'adresse IP du site GSLB et du SNIP dans un sous-réseau différent. En outre, vous devez disposer d'une route explicite définie vers l'adresse IP du site distant via un sous-réseau IP de site GSLB.
>
> Pour une sécurité renforcée, Citrix vous recommande de modifier le compte d'utilisateur interne et les mots de passe du nœud RPC. Le mot de passe du compte d'utilisateur interne est modifié via le mot de passe du nœud RPC. Pour plus de détails, voir Modifier le mot de passe d'un nœud RPC.

Si vous utilisez l'option saveconfig, les sites qui participent au processus de synchronisation enregistrent automatiquement leur configuration, de la manière suivante :

Sur le nœud RPC du site GSLB distant, configurez le pare-feu pour qu'il accepte les connexions de synchronisation automatique en spécifiant l'adresse IP du site distant (adresse IP du cluster pour la configuration du cluster) et le port (3010 pour RPC et 3008 pour RPC sécurisé). Si la route par défaut pour atteindre les sites distants se trouve dans un sous-réseau de gestion, comme dans la plupart des cas, NSIP est utilisé comme adresse IP source.

Pour configurer une adresse IP source différente, vous devez disposer de l'adresse IP du site GSLB et du SNIP dans un sous-réseau différent. Vous devez également disposer d'une route explicite définie vers l'adresse IP du site distant via le sous-réseau IP du site GSLB. L'adresse IP source ne peut pas être synchronisée entre les sites participant à GSLB car l'adresse IP source d'un nœud RPC est spécifique à chaque appliance Citrix ADC. Par conséquent, après avoir forcé une synchronisation (à l'aide de la commande sync gslb config -ForceSync ou en sélectionnant l'option ForceSync dans l'interface graphique), vous devez modifier manuellement les adresses IP source sur les autres appliances Citrix ADC. Le port 22 est également requis pour synchroniser les fichiers de base de données sur le site distant.

Pour améliorer le temps nécessaire à la synchronisation de la configuration sur tous les sites GSLB

Configurez les paramètres du profil TCP à l'invite de commandes comme suit :

```
1 set tcpprofile nstcp_internal_apps -bufferSize 4194304 -sendBuffsize
     4194304 -tcpmode ENDPOINT
2 <!--NeedCopy-->
```

Limites de la synchronisation

- Sur le site principal, les noms des sites GSLB distants doivent être identiques à ceux des sites configurés sur les appliances Citrix ADC hébergeant ces sites.
- Pendant la synchronisation, des perturbations de trafic peuvent se produire.
- Citrix ADC a été testé pour synchroniser jusqu'à 200 000 lignes de configuration.
- La synchronisation peut échouer :
  - Si la méthode de déversement est passée de CONNECTION à CONNECTION DYNAMIC CONNECTION.
  - Si vous échangez le préfixe de site des services GSLB liés à un serveur virtuel GSLB sur le nœud principal, puis essayez de synchroniser.
  - Si les mots de passe du nœud RPC sont différents pour NSIP et l'adresse IP de bouclage.
  - Si vous effectuez une synchronisation sur des sites GSLB configurés dans différentes partitions de la même appliance Citrix ADC.
- Si vous avez configuré les sites GSLB en tant que paires haute disponibilité (HA), les mots de passe des nœuds RPC des nœuds principal et secondaire doivent être identiques.
- Si vous renommez une entité GLSB faisant partie de votre configuration GSLB (utilisez la commande « show gslb RunningConfig » pour afficher la configuration GSLB). Vous devez utiliser l'option de synchronisation forcée pour synchroniser la configuration avec d'autres sites GSLB.

> **Remarque :**
>
> - Dans la synchronisation incrémentielle, vous n'avez pas besoin d'utiliser l'option de synchronisation forcée pour synchroniser la configuration avec d'autres sites GSLB. Ceci est applicable à partir de Citrix ADC version 13.0 build 79.x.

Remarque : Pour surmonter les limitations dues à certains paramètres de la configuration GSLB, vous pouvez utiliser l'option de synchronisation forcée. Mais, si vous utilisez l'option de synchronisation forcée, les entités GSLB sont supprimées et lues à la configuration et les statistiques GSLB sont réinitialisées à zéro. Par conséquent, le trafic est perturbé lors du changement de configuration.

Points à noter avant de commencer la synchronisation d'une configuration GSLB

Avant de commencer la synchronisation d'une configuration GSLB, assurez-vous que :

- Sur tous les sites GSLB, y compris le site principal, l'accès à la gestion et SSH doivent être activés pour l'adresse IP du site GSLB correspondant. L'adresse IP d'un site GSLB doit être une adresse IP appartenant à l'appliance Citrix ADC. Pour plus d'informations sur l'ajout des adresses IP du site GSLB et l'activation de l'accès à la gestion, voir « Configuration d'un site GSLB de base ».
- La configuration GSLB de l'appliance Citrix ADC considérée comme étant le site principal est complète et appropriée pour être copiée sur tous les sites.
- Si vous synchronisez la configuration GSLB pour la première fois, tous les sites participant à GSLB doivent posséder l'entité de site GSLB de leurs sites locaux respectifs.
- Vous ne synchronisez pas les sites qui, par conception, n'ont pas la même configuration.
- Le site principal et les sites subordonnés exécutent les mêmes versions de Citrix ADC. À partir de la version 12.1, version 50.x, l'appliance vérifie la version du micrologiciel sur les sites principaux et subordonnés avant de lancer la synchronisation. Si les sites principal et les sites subordonnés exécutent différentes versions, la synchronisation est interrompue pour ce site distant afin d'éviter toute modification incompatible entre les versions. En outre, un message d'erreur affichant les détails du site sur lequel la synchronisation a été interrompue s'affiche.

  Les figures suivantes affichent des exemples de messages d'erreur provenant de l'interface de ligne de commande et de l'interface graphique.

```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name                Status      Reason
-------------------------------------------------------------------------------------------------------------
        s2                       Failure     Error: Different netscaler release on the remote site. Local Site: 13.0, Remote Site: 12.1
        s1                       Success     All Done
        s3                       Success     All Done
Done
>
```

```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name                Status      Reason
-------------------------------------------------------------------------------------------------------------
        s2                       Failure     Error: Different netscaler release on the remote site. Local Site: 13.0, Remote Site: 12.1
        s1                       Success     All Done
        s3                       Success     All Done
Done
>
```


> **Important**
>
> Les répertoires suivants sont synchronisés dans le cadre de la synchronisation de configuration GSLB.
>
> - /var/netscaler/locdb/
> - /var/netscaler/ssl/
> - /var/netscaler/inbuilt_db/

Synchronisation manuelle entre les sites participant à GSLB

August 20, 2021

La synchronisation manuelle de la configuration GSLB sur le site maître et les sites esclaves est effectuée de la manière suivante :

- Le site maître détecte les différences entre la configuration de son propre site et le site esclave.
- Le site maître applique la différence de configuration au site esclave.
- Le site maître effectue la synchronisation de configuration avec tous les sites esclaves de la configuration GSLB et termine le processus de synchronisation.

Important : après la synchronisation d'une configuration GSLB, la configuration ne peut pas être restaurée sur aucun des sites GSLB. Effectuez la synchronisation uniquement si vous êtes sûr que le processus de synchronisation ne remplace pas la configuration sur le site distant. La synchronisation de site n'est pas souhaitable lorsque les sites locaux et distants ont des configurations différentes par conception, ce qui entraîne une panne du site. Si certaines commandes échouent et que certaines commandes réussissent, les commandes réussies ne sont pas annulées.

Points à noter

- Si vous forcez une synchronisation (utilisez l'option « forcer la synchronisation »), l'appliance Citrix ADC supprime la configuration GSLB du site esclave. Ensuite, le site maître configure le site esclave pour le rendre similaire à son propre site.
- Pendant la synchronisation, si une commande échoue, la synchronisation n'est pas abandonnée. Les messages d'erreur sont consignés dans un fichier .err dans le répertoire /var/netscaler/gslb.
- Si vous utilisez `saveconfig` cette option, les sites participant au processus de synchronisation enregistrent automatiquement leur configuration, de la manière suivante :
  - Le site maître enregistre sa configuration immédiatement avant d'initier le processus de synchronisation.

- Les sites esclaves enregistrent leur configuration une fois le processus de synchronisation terminé. Un site esclave n'enregistre sa configuration que si la différence de configuration a été appliquée avec succès. Si la synchronisation échoue sur un site esclave, vous devez rechercher manuellement la cause de l'échec et prendre des mesures correctives.

Pour synchroniser une configuration GSLB à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour synchroniser les sites GSLB et vérifier la configuration :

```
sync gslb config [-preview | -forceSync <string> | -nowarn | -
   saveconfig] [-debug]
show gslb syncStatus
<!--NeedCopy-->
```

Exemple :

```
sync gslb config

[WARNING]: Syncing config may cause configuration loss on other site.

Please confirm whether you want to sync-config (Y/N)? [N]:y

Sync Time: Dec 9 2011 10:56:9

Retrieving local site info: ok

Retrieving all participating gslb sites info: ok

Gslb_site1[Master]:

Getting Config: ok

Gslb_site2[Slave]:

Getting Config: ok

Comparing config: ok

Applying changes: ok

Done
<!--NeedCopy-->
```

Pour synchroniser une configuration GSLB à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic > GSLB > Tableau de bord**.
2. Cliquez sur **Auto Synchronization GSLB** et sélectionnez **ForceSYN** .
3. Dans **Nom du site GSLB**, sélectionnez les sites GSLB à synchroniser avec la configuration du nœud maître.

Aperçu de la synchronisation GSLB

En prévisualisant l'opération de synchronisation GSLB, vous pouvez voir les différences entre le nœud maître et chaque nœud esclave. S'il y a des divergences, vous pouvez résoudre les problèmes avant de synchroniser la configuration GSLB.

Pour afficher un aperçu de la sortie de synchronisation GSLB à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
sync gslb config -preview
<!--NeedCopy-->
```

Pour afficher un aperçu de la sortie de synchronisation GSLB à l'aide de l'interface graphique :

1. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Tableau de bord**.
2. Cliquez sur **Synchronisation automatique GSLB** et sélectionnez **Aperçu** .
3. Cliquez sur **Exécuter**.
   Une fenêtre de progression affiche toutes les incohérences dans la configuration.

Débogage des commandes déclenchées lors du processus de synchronisation

Vous pouvez afficher l'état (succès ou échec) de chaque commande déclenchée au cours du processus de synchronisation et résoudre les problèmes en conséquence.

Pour déboguer les commandes de synchronisation GSLB à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
sync gslb config -debug
<!--NeedCopy-->
```

Pour déboguer les commandes de synchronisation GSLB à l'aide de l'interface graphique :

1. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Tableau de bord.**
2. Cliquez sur **Synchronisation automatique GSLB** et sélectionnez **Déboguer** .
3. Cliquez sur **Exécuter**. Une fenêtre de progression affiche l'état de chaque commande déclenchée lors de la synchronisation.

Synchronisation en temps réel entre les sites participant à GSLB

October 5, 2021

Vous pouvez utiliser ce `AutomaticConfigSync` paramètre pour synchroniser automatiquement la configuration GSLB en temps réel du site principal avec tous les sites subordonnés. Il n'est pas nécessaire de déclencher manuellement l'option AutoSync pour synchroniser la configuration.

Vous pouvez synchroniser automatiquement la configuration GSLB du site principal avec tous les sites subordonnés en utilisant la synchronisation incrémentielle ou la synchronisation complète. Le `GSLBSyncMode` paramètre permet de choisir le mode de synchronisation.

> Remarque :
>
> À partir de Citrix ADC version 13.0 build 79.x, la synchronisation incrémentielle de la synchronisation GSLB est prise en charge. Par défaut, la synchronisation est effectuée à l'aide d'une synchronisation incrémentielle. La synchronisation incrémentielle peut être effectuée en activant le `IncrementalSync` paramètre. Pour plus de détails, consultez la section Synchronisation incrémentielle de la configuration GSLB.

Meilleures pratiques pour l'utilisation de la fonction de synchronisation en temps réel

- Il est recommandé que toutes les appliances Citrix ADC participant en tant que sites disposent de la version logicielle SameCitrix ADC.
- Pour modifier le mot de passe du nœud RPC, commencez par modifier le mot de passe sur le site subordonné, puis sur le site principal.
- Configurez les sites GSLB locaux sur chaque site participant à GSLB.
- Activez AutomaticConfigSync sur l'un des sites où la configuration est effectuée. Ce site est finalement synchronisé avec d'autres sites GSLB.
- S'il y a une nouvelle configuration ou si des modifications sont apportées à la configuration existante, vérifiez l'état à l'aide de la `show gslb syncStatus` commande pour confirmer si les modifications sont synchronisées sur tous les sites ou s'il y a eu une erreur.
- La surveillance des ports RSYNC doit être activée.

Pour activer la synchronisation en temps réel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb parameter [ - automaticConfigSync (ENABLED | DISABLED)] [-
    MEPKeepAliveTimeout <secs>]  [-GSLBSyncMode ( IncrementalSync |
    FullSync )] [-GSLBSyncLocFiles ( ENABLED | DISABLED)] [-
```



```
    GslbConfigSyncMonitor ( ENABLED | DISABLED )] [-GSLBSyncInterval <
    secs>] [-GSLBSyncSaveConfigCommand ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Exemple :

```
set gslb parameter  -automaticConfigSync ENABLED
<!--NeedCopy-->
```

La synchronisation en temps réel fournit les paramètres configurables suivants :

- **GSLBSyncMode -Mode**dans lequel la configuration est synchronisée du site principal vers les sites distants.
  - Valeurs possibles : IncrementalSync, FullSync
  - Valeur par défaut : IncrementalSync
- **GSLBSynclocFiles**—Lors de la synchronisation de la configuration GSLB, par défaut, les modifications apportées aux fichiers DB d'emplacement sont détectées et synchronisées automatiquement. Étant donné que les répertoires DB d'emplacement ne changent pas souvent, les administrateurs peuvent désactiver la synchronisation automatique des fichiers DB de localisation. Les administrateurs doivent plutôt copier manuellement les fichiers DB d'emplacement sur les sites subordonnés GSLB. La synchronisation des fichiers DB d'emplacement prend beaucoup de temps. Ainsi, le fait de l'éviter réduit le temps global de synchronisation.

  Exemple de désactivation de la synchronisation automatique des fichiers DB d'emplacement :

  ```
  set gslb parameter -GSLBSyncMode IncrementalSync -
     GSLBSyncLocFiles DISABLED
  <!--NeedCopy-->
  ```

- **GSLBConfigSyncMonitor**—Activez le paramètre GSLB Config Sync Monitor pour surveiller l'état du port RSYNC des sites subordonnés, qui est le port SSH 22 sur l'adresse IP du site GSLB distant. Si le moniteur affiche l'état du site subordonné comme DOWN, l'opération RSYNC vers ce site est ignorée. Cela réduit les retards de synchronisation causés par la tentative de connexion aux sites distants en panne.

  Exemple pour activer la surveillance des ports RSYNC dans l'interface de ligne de commande :

  ```
  set gslb parameter -GSLBSyncMode IncrementalSync -
     GslbConfigSyncMonitor ENABLED
  <!--NeedCopy-->
  ```

- **GSLBSyncInterval**—Définit l'intervalle de temps (en secondes) auquel se produit la synchronisation de la configuration GSLB. Par défaut, la fonction de synchronisation automatique de

configuration GSLB synchronise automatiquement la configuration GSLB toutes les 10 secondes. Vous pouvez modifier l'intervalle de temps sur n'importe quelle valeur souhaitée. Ne pas définir cette valeur sur une valeur inférieure, par exemple, au moins 5 secondes. Parce que la synchronisation fréquente peut augmenter la consommation du processeur de gestion.

> Remarque :
>
> Dans une configuration de partition d'administration, l'intervalle de temps ne peut être défini que dans la partition par défaut car il s'agit d'un paramètre global.

Exemple de définition de l'intervalle de synchronisation :

```
set gslb parameter -AutomaticConfigSync ENABLED -GSLBSyncMode
   IncrementalSync -GSLBSyncInterval 7
<!--NeedCopy-->
```

- **GSLBSyncSaveConfigCommand**—Activez ce paramètre pour synchroniser la `save ns config` commande avec les sites subordonnés, si l' `AutomaticConfigSync` option est activée.

  Exemple pour activer la synchronisation de la commande « Enregistrer la configuration » :

  ```
  set gslb parameter -AutomaticConfigSync ENABLED -
     GSLBSyncSaveConfigCommand ENABLED
  <!--NeedCopy-->
  ```

  La `save ns config` commande n'est pas synchronisée sur les sites subordonnés dans certains scénarios, comme suit :

  - Le site subordonné est en panne ou inaccessible lorsque la configuration est enregistrée sur le site principal.
  - La configuration a échoué sur un site subordonné.

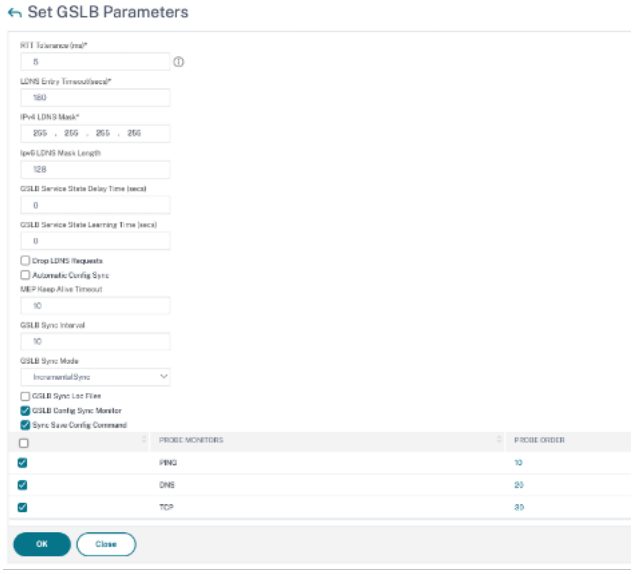
Pour activer la synchronisation en temps réel à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Modifier les paramètres GSLB**.
2. Dans la page **Définir les paramètres GSLB**, vous pouvez effectuer les opérations suivantes :
   - Pour synchroniser automatiquement la configuration GSLB en temps réel, sélectionnez **ConfigSync automatique**.

   Remarque : Cette option doit être activée uniquement sur le site où la configuration est effectuée.

   - Pour définir l'intervalle de synchronisation automatique de configuration GSLB, entrez le temps en secondes dans le champ **Intervalle de synchronisation GSLB** .

- Pour activer la surveillance des ports RSYNC, activez la case à cocher **GSLB Config Sync Monitor** .
- Pour désactiver la synchronisation automatique des fichiers DB d'emplacement, désactivez la case à cocher **GSLB Sync Loc Files** .
- Pour activer la synchronisation de la `save ns config` commande sur les sites subordonnés, activez la case à cocher **Synchroniser la commande Enregistrer la configuration** .



Pour plus d'informations sur les rubriques suivantes, reportez-vous à la section Synchronisation manuelle entre les sites participant à GSLB.

- Aperçu de la synchronisation GSLB
- Débogage des commandes déclenchées pendant le processus de synchronisation

Points à noter

- Le fichier journal consolidé lié à la synchronisation en temps réel est stocké dans le répertoire /var/netscaler/gslb/periodic_sync.log.
- Le fichier de configuration par défaut est stocké dans le répertoire /var/netscaler/gslb_sync/.
- Le site principal utilise la structure de répertoires suivante :
  - Le site principal stocke tous ses fichiers dans le répertoire /var/netscaler/gslb_sync/master.
  - Le site principal stocke son fichier de configuration qui doit être synchronisé avec les sites subordonnés, dans le répertoire /var/netscaler/gslb_sync/master/gslbconf/.
  - Les fichiers d'état extraits de tous les sites subordonnés sont stockés dans le répertoire /var/netscaler/gslb_sync/master/slavestatus/.
- Le site subordonné utilise la structure de répertoires suivante :
  - Le site subordonné reprend le dernier fichier de configuration à appliquer depuis le répertoire /var/netscaler/gslb_sync/slave/gslbconf.

  - Le site subordonné stocke son fichier d'état dans le répertoire /var/netscaler/gslb_sync/slave/gslbstatus
- Dans la configuration d'une partition d'administration, la même structure de répertoire est maintenue à l'emplacement : /var/partitions/`partition name`/netscaler/gslb_sync.
- Les horloges de tous les sites doivent être réglées avec précision selon une norme en temps réel telle que le temps universel coordonné (UTC).

Synchronisation incrémentielle de la configuration GSLB

La fonction de synchronisation automatique de la configuration GSLB vérifie les modifications de configuration sur le site principal toutes les 10 secondes et effectue une synchronisation. Cette valeur d'intervalle de synchronisation est configurable.

Dans la synchronisation incrémentielle, seules les configurations qui ont changé sur le site principal entre la dernière synchronisation et l'intervalle de synchronisation suivant (10 secondes) sont synchronisées sur tous les sites subordonnés. La synchronisation incrémentielle est le comportement par défaut. Le fait de pousser uniquement les configurations incrémentielles réduit considérablement la taille du fichier de configuration, et donc le temps de synchronisation. Si une synchronisation incrémentielle échoue, le système effectue automatiquement une synchronisation complète de la configuration.

La synchronisation incrémentielle est effectuée de la manière suivante :

- Le site principal envoie le fichier de configuration comprenant uniquement ses dernières modifications sur tous les sites subordonnés. La dernière modification concerne les configurations qui ont changé entre la dernière synchronisation et l'intervalle de synchronisation suivant (10 secondes).
- Chaque site subordonné applique la dernière modification à son propre site.
- La synchronisation incrémentielle n'est pas tentée sur les sites subordonnés, qui sont en état DOWN. Lorsque le site revient, la synchronisation est à nouveau effectuée.
- Le site subordonné génère des journaux d'état à chaque étape et les copie dans un fichier à un emplacement spécifique.
- Le site principal extrait les fichiers journaux d'état de l'emplacement spécifié.
- Le site principal prépare un fichier journal avec des journaux combinés à partir de tous les sites subordonnés.
- Ce fichier journal combiné est stocké dans le fichier "/var/netscaler/gslb/periodic_sync.log".

Pour plus d'informations sur les répertoires dans lesquels les fichiers de configuration sont stockés, consultez la section Points à noter .

Pour activer la synchronisation incrémentielle de configuration GSLB à l'aide de l'interface de ligne de commande


```
set gslb parameter -AutomaticConfigSync (ENABLED | DISABLED) -
    GSLBSyncMode (IncrementalSync | FullSync) -GslbConfigSyncMonitor (
    ENABLED | DISABLED) -GSLBSyncInterval <secs> -GSLBSyncLocFiles (
    ENABLED | DISABLED)
<!--NeedCopy-->
```

Exemple :

```
set gslb parameter -AutomaticConfigSync ENABLED -GSLBSyncMode
    IncrementalSync
<!--NeedCopy-->
```

Pour activer la synchronisation incrémentielle GSLB à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > GSLB > Tableau de bord > Modifier les paramètres GSLB**.
2. Dans la page **Définir les paramètres GSLB**, choisissez **IncrementalSync** dans le menu déroulant **Mode de synchronisation GSLB** .

Synchronisation complète de la configuration GSLB

Chaque fois qu'il y a un changement de configuration sur le site principal, la configuration complète en cours d'exécution du GSLB sur le site principal est transférée vers tous les sites subordonnés. Même si la synchronisation incrémentielle est configurée, une synchronisation complète est effectuée lorsque le site principal ne connaît pas l'état de configuration du site subordonné. Certains de ces scénarios sont les suivants :

- Activez la fonction de synchronisation automatique de la configuration GSLB pour la première fois.
- Redémarrez l'appliance Citrix ADC.
- Le déploiement de GSLB comporte plusieurs sites principaux, et un autre site principal devient le site principal actif.
- Ajoutez un nouveau site subordonné au déploiement GSLB.

La synchronisation complète de la configuration GSLB s'effectue de la manière suivante :

- Le site principal envoie son dernier fichier de configuration vers tous les sites subordonnés.
- Chaque site subordonné compare sa propre configuration au dernier fichier de configuration envoyé par le site principal. Le site subordonné identifie la différence de configuration et applique la configuration delta à son propre site.
- Le site subordonné génère des journaux d'état à chaque étape et les copie dans un fichier à un emplacement spécifique.
- Le site principal extrait les fichiers journaux d'état de l'emplacement spécifié.

- Le site principal prépare un fichier journal avec des journaux combinés à partir de tous les sites subordonnés.
- Ce fichier journal combiné est stocké dans le fichier "/var/netscaler/gslb/periodic_sync.log".

Si vous tentez de synchroniser manuellement (avec la `sync gslb config` commande) un site en cours de synchronisation automatique, un message d'erreur « Synchronisation en cours » apparaît. La synchronisation automatique ne peut pas être déclenchée pour un site en cours de synchronisation manuelle.

> **Attention :**
>
> À partir de Citrix ADC 12.1 build 49.37, les interruptions SNMP sont générées lorsque vous synchronisez la configuration GSLB. Dans la synchronisation en temps réel, l'état de synchronisation dans la première interruption SNMP est capturé en tant qu'échec. Vous pouvez ignorer cet état car une deuxième interruption SNMP est automatiquement générée immédiatement après la première interruption avec l'état de synchronisation réel. Toutefois, si la synchronisation a également échoué lors de la deuxième tentative, l'interruption SNMP n'est pas générée car l'état de synchronisation n'a pas changé par rapport à l'état de synchronisation précédent.

Pour plus d'informations sur la configuration de l'appliance Citrix ADC pour générer des interruptions, consultez Configuration de Citrix ADC pour générer des interruptions SNMP.

Pour activer la synchronisation complète GSLB à l'aide de l'interface de ligne de commande

```
set gslb parameter -GSLBSyncMode (IncrementalSync | FullSync)
<!--NeedCopy-->
```

Exemple :

```
set gslb parameter -GSLBSyncMode FullSync
<!--NeedCopy-->
```

Pour activer la synchronisation incrémentielle GSLB à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic > GSLB > Tableau de bord > Modifier les paramètres GSLB**.
2. Dans la page **Définir les paramètres GSLB**, choisissez **FullSync** dans le menu déroulant **Mode de synchronisation GSLB** .

Plusieurs sites principaux dans un déploiement GSLB

L'appliance Citrix ADC prend en charge plusieurs sites principaux dans un déploiement actif-passif. Il est recommandé d'avoir deux sites principaux dans un déploiement GSLB pour faire face à la défaillance du site principal GSLB. Le fait de disposer de deux sites principaux peut éviter un point de

défaillance unique de la synchronisation de la configuration GSLB. À tout moment, un seul site principal peut traiter activement la configuration GSLB à partir de l'utilisateur. Si les modifications de configuration sont effectuées simultanément sur plusieurs sites principaux, cela peut entraîner des incohérences de configuration ou des pertes de configuration. Par conséquent, il est recommandé d'effectuer des modifications de configuration à partir d'un seul site principal à la fois et d'utiliser l'autre site principal comme sauvegarde en cas de défaillance du site principal actif.

> Remarque :
>
> Lorsque plusieurs sites principaux sont utilisés dans un déploiement GSLB, la surveillance RSYNC doit être activée.

Pour faire d'un nœud GSLB l'un des principaux sites de synchronisation de configuration GSLB, exécutez la commande suivante :

```
set gslb parameter -automaticConfigSync Enabled
<!--NeedCopy-->
```

Afficher l'état et le résumé de la synchronisation GSLB

January 21, 2021

Une fois la configuration GSLB synchronisée sur les sites GSLB, vous pouvez afficher l'état détaillé et le résumé de la dernière opération de synchronisation GSLB. Ceci est applicable à la synchronisation GSLB manuelle et en temps réel.

Pour afficher l'état ou le résumé de la synchronisation GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show gslb sync status
<!--NeedCopy-->
```

ou

```
show gslb syncStatus -summary
<!--NeedCopy-->
```

Exemple de sortie de configuration pour la synchronisation manuelle GSLB

La sortie suivante affiche l'état de la synchronisation manuelle de la configuration GSLB.


```
> sh gslb syncStatus
Displaying the status of the manual GSLB configuration synchronization:

gslb_site1[Master]:
        Getting Config:  ok
gslb_site2[Slave]:
        Syncing gslb static proximity database:  ok
        Syncing inbuilt gslb static proximity database : ok
        Getting Config:  ok
        Comparing config:  ok
        Applying changes:  ok
gslb_natsite1[Slave]:
        Syncing gslb static proximity database:  ok
        Syncing inbuilt gslb static proximity database : ok
        Getting Config:  ok
        Comparing config:  ok
        Applying changes:  ok
 Done
>
```

La sortie suivante affiche le récapitulatif de l'état de la synchronisation manuelle de la configuration GSLB.

```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name               Status          Reason
-------------------------------------------------------------------------------------------------------------
        gslb_site1              Success         All Done
        gslb_site2              Failure         Error executing command on gslb site...ERROR: Connection failed
        gslb_natsite1           Success         All Done
Done
>
```

Exemple de sortie de configuration pour la synchronisation en temps réel GSLB

La sortie suivante affiche l'état de la synchronisation de configuration GSLB en temps réel pour le site maître :

```
1  > sh gslb syncStatus
```



```
Displaying the status of the real time GSLB configuration
    synchronization as master node:

site2[Master]:
                New GSLB configuration detected at Fri Jan 23 20:54:24
                    2020
                Fetching current configuration: Done
                Updating default.conf file: Done
site1[Slave]:
                Syncing gslb static proximity database to node site1:
                    Done
                Syncing inbuilt GSLB static proximity database to node
                    site1: Done
                Syncing ssl certificates, keys and CRLS to node site1:
                    Done
                Syncing current configuration to site1: Done
                Pulling status files from site1: Status file not
                    available yet(Sync in progress)
                Pulling status files from site1: Done
                site1 received new configuration from 10.102.217.205 in
                     file 2JNSzClRHK5+pdek6szQ3g-default-10.102.217.210.
                    conf
                Firing set gslb parameter -startConfigSync ENABLED
                    command: Done
                Fetching running GSLB Config: Done
                Comparing config: Done
                Applying changes: Done
                Firing set gslb parameter -startConfigSync DISABLED
                    command: Done
                Updating default.conf file: Done
Done
<!--NeedCopy-->
```

La sortie suivante affiche l'état de la synchronisation de configuration GSLB en temps réel pour le site esclave :

```
> sh gslb syncStatus
Displaying the status of the real time GSLB configuration
    synchronization as slave node:

                site1 received new configuration from 10.102.217.205 in
                     file 2JNSzClRHK5+pdek6szQ3g-default-10.102.217.210.
                    conf
                Firing set gslb parameter -startConfigSync ENABLED
                    command: Done
```



```
6                 Fetching running GSLB Config: Done
7                 Comparing config: Done
8                 Applying changes: Done
9                 Firing set gslb parameter -startConfigSync DISABLED
                     command: Done
10                Updating default.conf file: Done
11 Done
12 <!--NeedCopy-->
```

La sortie suivante affiche le récapitulatif de l'état de la synchronisation de configuration GSLB en temps réel pour le site maître :

```
1  > sh gslb syncStatus -summary
2  Displaying the status summary of the real time GSLB configuration
       synchronization as master node:
3
4  ------------------------------------------------------------------------------

5                 Site Name                                   Status
                                Reason
6  ------------------------------------------------------------------------------

7                 site2                                       Success
                              All Done
8                 site1                                       Success
                              All Done
9
10 Done
11 <!--NeedCopy-->
```

La sortie suivante affiche le récapitulatif de l'état de la synchronisation de configuration GSLB en temps réel pour le site esclave :

```
1  > sh gslb syncStatus  - summary
2  Displaying the status summary of the real time GSLB configuration
       synchronization as slave node:
3
4  ------------------------------------------------------------------------------

5                 Site Name                                   Status
                                Reason
6  ------------------------------------------------------------------------------

7                 site1                                       Success
                              All Done
```



```
8
9  Done
10 <!--NeedCopy-->
```

Pour afficher l'état ou le résumé de la synchronisation GSLB à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Tableau de bord**.
2. Cliquez sur **Afficher le résumé de la synchronisationou Afficher l'état de la synchronisation**, selon les besoins.

Interruptions SNMP pour la synchronisation de la configuration GSLB

August 20, 2021

À partir de Citrix ADC 12.1 build 49.xx, l'appliance Citrix ADC génère des interruptions SNMP pour les sites locaux et distants lorsque vous synchronisez la configuration GSLB. Les interruptions SNMP sont générées à la fois pour la synchronisation manuelle et la synchronisation en temps réel.

Lorsque vous synchronisez la configuration GSLB pour la première fois, les interruptions SNMP sont générées. Lors des tentatives de synchronisation suivantes, les interruptions SNMP sont générées uniquement si le statut de synchronisation est modifié par rapport à l'état de synchronisation précédent. En outre, les interruptions SNMP sont générées uniquement pour les sites pour lesquels l'état de synchronisation a changé par rapport à l'état précédent.

Par exemple, considérez que la première synchronisation de configuration GSLB est réussie. Lorsque vous synchronisez la configuration pour la deuxième fois et si la synchronisation réussit à nouveau, les interruptions SNMP ne sont pas générées car l'état n'est pas modifié. Toutefois, lors de la troisième tentative, si la synchronisation échoue pour l'un des sites, l'interruption SNMP est générée uniquement pour ce site.

Dans le cadre d'une haute disponibilité et d'une configuration de cluster, l'appliance génère les interruptions SNMP lorsque vous synchronisez la configuration GSLB à partir du nouveau nœud, quel que soit l'état de synchronisation précédent. En outre, si l'option d'interruption SNMP a été précédemment désactivée puis activée, les interruptions SNMP sont générées à partir de ce point, quel que soit l'état de synchronisation précédent.

Les interruptions SNMP de la synchronisation de configuration GSLB fournissent les détails suivants :

- Nom du site GSLB pour lequel l'interruption SNMP est envoyée.
- État de synchronisation de la configuration GSLB : succès ou échec.
- Mode de synchronisation de configuration GSLB : synchronisation incrémentielle ou synchronisation complète.

- (Facultatif) Informations détaillées sur les interruptions SNMP.

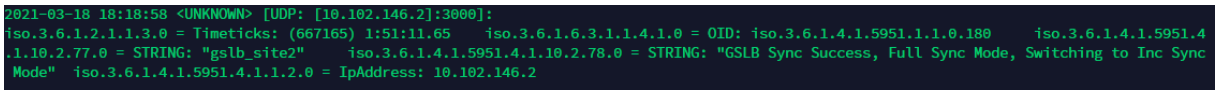
Les interruptions SNMP sont générées dans les scénarios suivants :

- L'état de synchronisation GSLB pour un site GSLB passe de Success to Failure, et inversement.
- Le mode de synchronisation GSLB passe de la synchronisation incrémentielle à la synchronisation complète, et inversement.

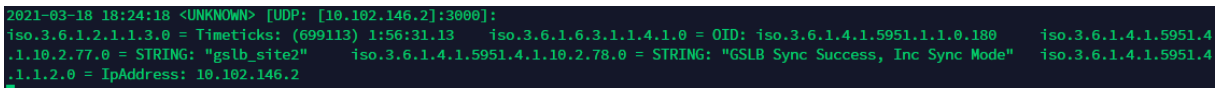
> Remarque :
>
> Même lorsque la synchronisation incrémentielle est activée, si la synchronisation complète est effectuée sur un site GSLB pour une raison quelconque, la raison de la synchronisation complète est mentionnée dans la section « Informations détaillées » du message d'interruption. Par exemple, lorsqu'un nouveau site GSLB est ajouté à la configuration GSLB.

Exemples de messages d'interruption SNMP

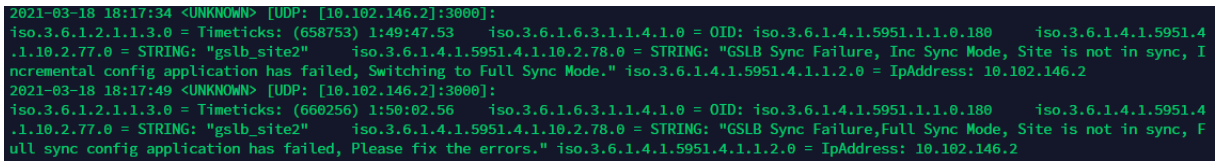
La figure suivante présente un exemple d'interruption SNMP pour gslb_site2, où la synchronisation de la configuration GSLB réussit en mode Synchronisation complète.



La figure suivante présente un exemple d'interruption SNMP pour gslb_site2, où la synchronisation de la configuration GSLB réussit à l'aide du mode de synchronisation incrémentielle.



La figure suivante présente un exemple d'interruption SNMP pour gslb_site2, où la synchronisation de la configuration GSLB à l'aide du mode de synchronisation incrémentielle a échoué. Le message d'erreur indique que vous devez corriger manuellement les erreurs pour terminer la synchronisation.



La figure suivante présente un exemple d'interruption SNMP pour gslb_site2, où la synchronisation de la configuration GSLB à l'aide du mode de synchronisation incrémentielle a échoué. Il indique également la raison de l'échec de la synchronisation, c'est-à-dire que le moniteur de site est en panne.

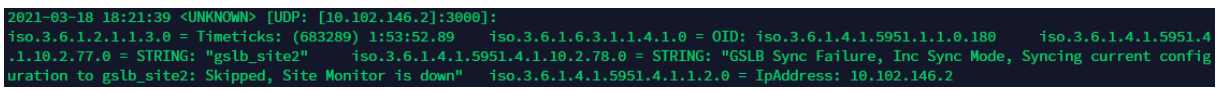


Tableau de bord GSLB

January 21, 2021

Vous pouvez afficher l'état général des sites GSLB participant à GSLB sur le tableau de bord GSLB.

Vous pouvez accéder aux paramètres GSLB à partir du tableau de bord. Vous pouvez également démarrer l'assistant de configuration GSLB à partir du tableau de bord. En outre, vous pouvez effectuer la synchronisation et tester la configuration GSLB à partir du tableau de bord.

Pour accéder au tableau de bord GSLB, accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Tableau de bord**.

Surveillance des services GSLB

August 20, 2021

Lorsque vous liez un service distant à un serveur virtuel GSLB, les sites GSLB échangent des informations de mesure, y compris des informations de mesure réseau, qui sont les informations de temps d'arrêt et de persistance.

Si une connexion d'échange de mesures est momentanément perdue entre l'un des sites participants, le site distant est marqué comme étant DOWN et l'équilibrage de charge est effectué sur les sites restants qui sont UP. Lorsque l'échange de mesures pour un site est DOWN, les services distants appartenant au site sont également marqués comme DOWN.

L'appliance Citrix ADC évalue périodiquement l'état des services GSLB distants en utilisant soit MEP, soit des moniteurs explicitement liés aux services distants. La liaison de moniteurs explicites aux services locaux n'est pas requise, car l'état du service GSLB local est mis à jour par défaut à l'aide du MEP. Toutefois, vous pouvez lier des moniteurs explicites à un service distant. Lorsque les moniteurs sont explicitement liés, l'état du service distant n'est pas contrôlé par l'échange de mesures.

Par défaut, lorsque vous liez un moniteur à un service GSLB distant, l'appliance Citrix ADC utilise l'état du service signalé par le moniteur. Toutefois, vous pouvez configurer l'appliance Citrix ADC pour qu'elle utilise des moniteurs pour évaluer les services dans les situations suivantes :

- Utilisez toujours des moniteurs (paramètre par défaut).
- Utilisez des moniteurs lorsque MEP est DOWN.
- Utilisez des moniteurs lorsque les services distants et MEP sont DOWN.

Les deuxième et troisième paramètres ci-dessus permettent à l'appliance d'arrêter la surveillance lorsque MEP est UP. Par exemple, dans une configuration GSLB hiérarchique, un site GSLB fournit les informations MEP sur ses sites enfants à son site parent. Un tel site intermédiaire peut évaluer

l'état du site enfant comme DOWN en raison de problèmes de réseau, bien que l'état réel du site soit UP. Dans ce cas, vous pouvez lier des moniteurs aux services du site parent et désactiver MEP pour déterminer l'état réel du service distant. Cette option vous permet de contrôler la manière dont les états des services distants sont déterminés.

Pour utiliser des moniteurs, commencez par les créer, puis les lier aux services GSLB.

Configurer le déclencheur du moniteur

Vous pouvez configurer un site GSLB pour toujours utiliser des moniteurs (valeur par défaut), utiliser des moniteurs lorsque le MEP est en panne ou utiliser des moniteurs lorsque le service distant et le MEP sont en panne. Dans les deux derniers cas, l'appliance Citrix ADC cesse de surveiller lorsque MEP revient à l'état UP.

Pour configurer le déclenchement du moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb site <siteName> -triggerMonitor (ALWAYS | MEPDOWN |
    MEPDOWN_SVCDOWN)
<!--NeedCopy-->
```

Exemple :

```
set gslb site Site-GSLB-North-America -triggerMonitor Always
<!--NeedCopy-->
```

Pour configurer le déclenchement du moniteur à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Sites**, puis double-cliquez sur le site.
2. Dans la liste déroulante **Moniteurs de déclenchement**, sélectionnez une option de déclenchement de la surveillance.

Ajouter ou supprimer des moniteurs

Pour ajouter un moniteur, spécifiez le type et le port. Vous ne pouvez pas supprimer un moniteur lié à un service. Vous devez d'abord dissocier le moniteur du service.

Pour ajouter un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un moniteur et vérifier la configuration :


```
add lb monitor <monitorName> -type <monitorType> -destPort <portNumber>

show lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
add lb monitor monitor-HTTP-1 -type HTTP -destPort 80
show lb monitor monitor-HTTP-1
<!--NeedCopy-->
```

Pour supprimer un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm lb monitor <monitorName>
<!--NeedCopy-->
```

Pour ajouter un moniteur à l'aide de l'utilitaire de configuration

Accédez à Gestion
du trafic > Équilibrage de charge > Moniteurs, puis ajoutez ou supprimez un moniteur.

Liaison des moniteurs à un service GSLB

Une fois que vous avez créé des moniteurs, vous devez les lier aux services GSLB. Lorsque vous liez des moniteurs aux services, vous pouvez spécifier un poids pour le moniteur. Après avoir lié un ou plusieurs moniteurs pondérés, vous pouvez configurer un seuil de surveillance pour le service. Ce seuil abaisse le service si la somme des pondérations du moniteur liées tombe en dessous de la valeur du seuil.

Remarque : dans l'utilitaire de configuration, vous pouvez définir à la fois le poids et le seuil de surveillance en même temps que vous liez le moniteur. Lorsque vous utilisez la ligne de commande, vous devez émettre une commande distincte pour définir le seuil de surveillance du service.

Pour lier le moniteur au service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind monitor <name> <serviceName> [ -state (Enabled | Disabled) ] -
    weight <positiveInteger>
<!--NeedCopy-->
```


Exemple :

```
bind monitor monitor-HTTP-1 service-GSLB-1 -state enabled -weight 2
<!--NeedCopy-->
```

Pour définir le seuil de surveillance d'un service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb service <ServiceName> -monThreshold <PositiveInteger>
<!--NeedCopy-->
```

Exemple :

```
set gslb service service-GSLB-1 -monThreshold 9
<!--NeedCopy-->
```

Pour lier le moniteur au service GSLB à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Services.
2. Cliquez sur la section **Moniteur** et liez le moniteur au service GSLB.

Pour définir le seuil de surveillance d'un service GSLB à l'aide de l'utilitaire de configuration

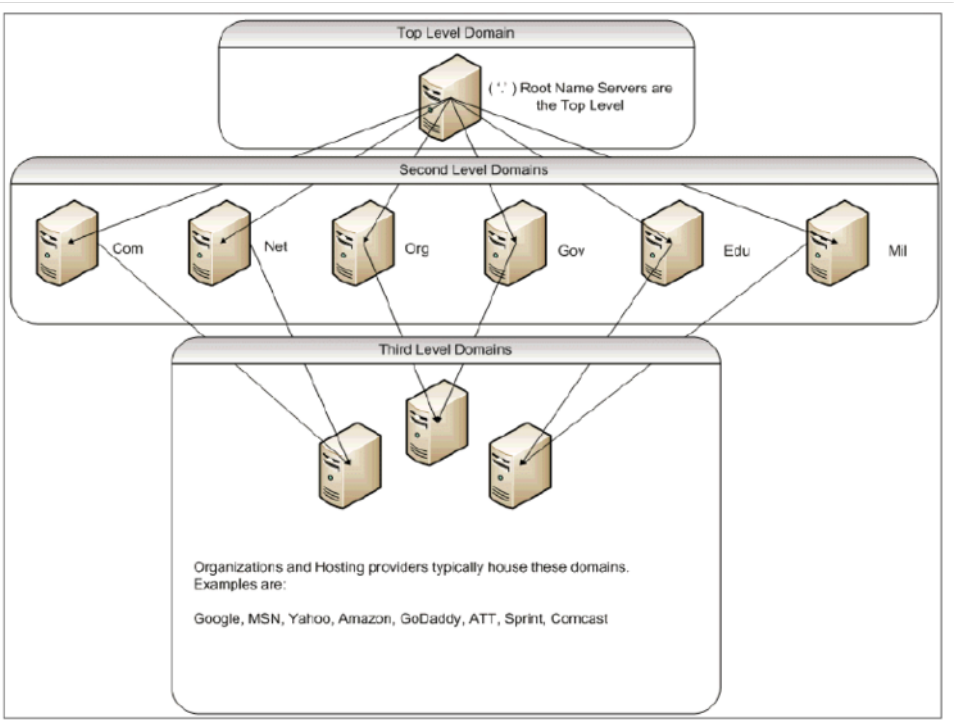
1. Accédez à Gestion du trafic > GSLB > Services.
2. Cliquez sur la section **Surveiller le seuil** et entrez une valeur de seuil.

Comment le système de noms de domaine prend en charge GSLB

October 5, 2021

Le système de noms de domaine (DNS) est considéré comme une base de données distribuée, qui utilise l'architecture Client/Serveur. Les serveurs de noms sont les serveurs de l'architecture, et les résolveurs sont les clients qui sont des routines de bibliothèque installées sur un système d'exploitation qui créent et envoient des requêtes sur le réseau.

La hiérarchie logique du DNS est illustrée dans le diagramme suivant :



> Remarque :
>
> Les serveurs racine de deuxième niveau sont responsables de la gestion des mappages Name Server to Address pour les délégations de serveurs de noms dans les domaines .com, .net, .org, .gov, etc. Chaque domaine des domaines de deuxième niveau est responsable de la gestion des mappages Serveur de noms à adresse pour les domaines organisationnels de niveau inférieur. Au niveau de l'organisation, les adresses d'hôte individuelles sont résolues pour les hôtes www, FTP et autres hôtes fournissant des services.

Délégation

L'objectif principal de la topologie DNS actuelle est d'alléger la charge de gestion de tous les enregistrements d'adresses sur une seule autorité. Cela permet de déléguer un espace de noms d'organisation à cette organisation particulière. L'organisation peut ensuite déléguer davantage son espace à des sous-domaines au sein de l'organisation. Par exemple, sous citrix.com, vous pouvez créer des sous-domaines appelés `sales.citrix.comeducation.citrix.com`, et `support.citrix.com`. Les services correspondants peuvent conserver leur propre ensemble de serveurs de noms qui font autorité pour leur sous-domaine, puis conserver leur propre ensemble de noms d'hôte pour les mappages d'adresses. Aucun service n'est responsable de la gestion de tous les enregistrements d'adresses Citrix. Chaque département peut modifier les adresses et modifier les topologies, sans imposer davantage de travail au domaine ou à l'organisation de niveau supérieur.

Avantages de la topologie hiérarchique

Voici quelques-uns des avantages de la topologie hiérarchique :

- Capacité à monter en charge
- Ajout d'une fonctionnalité de mise en cache dans les serveurs de noms à chaque niveau, où une requête DNS est gérée par un hôte qui ne fait pas autorité pour un domaine particulier, mais qui peut contribuer à la réponse à la requête et réduire la congestion et le temps de réponse.
- La mise en cache crée également une redondance et une résilience face aux défaillances du serveur. Si un serveur de noms échoue, il est toujours possible que des enregistrements soient diffusés à partir d'autres serveurs disposant de copies mises en cache récentes des mêmes enregistrements.

Résolveurs

Les résolveurs sont le composant client du système DNS. Les programmes exécutés sur un hôte qui ont besoin d'informations provenant de l'espace de noms de domaine utilisent le résolveur. Le résolveur gère :

- Interrogation d'un serveur de noms.
- Interprétation des réponses (qui peuvent être des enregistrements de ressources ou une erreur).
- Renvoyer l'information aux programmes qui en ont fait la demande.

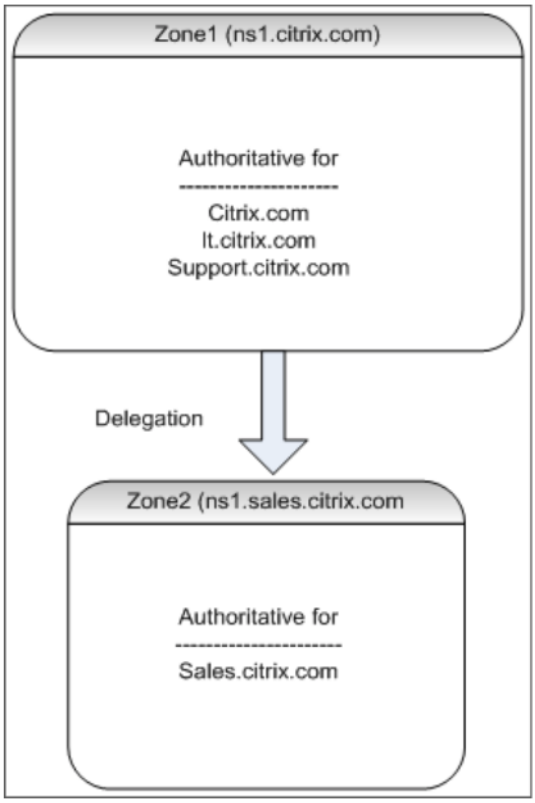
Le résolveur est un ensemble de routines de bibliothèque compilées dans des programmes tels que telnet, FTP et ping. Il ne s'agit pas de processus distincts. Les résolveurs peuvent créer une requête, l'envoyer et attendre une réponse. Et, envoyez-le à nouveau (éventuellement à un serveur de noms secondaire) s'il n'y a pas de réponse dans un certain temps. Ces types de résolveurs sont appelés résolveurs de talon. Certains résolveurs ont la fonctionnalité ajoutée pour mettre en cache les enregistrements et respectent le temps de vie (TTL). Sous Windows, cette fonctionnalité est disponible via le service Client DNS ; elle peut être consultée via la console « services.msc ».

Serveurs de noms

Les serveurs de noms stockent généralement des informations complètes sur une partie particulière d'un espace de noms de domaine (appelée zone). On dit alors que le serveur de noms est autorisé pour cette zone. Ils peuvent également faire autorité pour plusieurs zones.

La différence entre un domaine et une zone est subtile. Un domaine est l'ensemble complet des entités, y compris ses sous-domaines, tandis qu'une zone est uniquement l'information d'un domaine qui n'est pas déléguée à un autre serveur de noms. Un exemple de zone est `citrix.com`, alors qu'il s'`sales.citrix.com` agit d'une zone distincte si cette zone est déléguée à un autre serveur de noms au sein du sous-domaine. Dans ce cas, la zone Citrix principale peut inclure `citrix.comit.citrix.com`, et `support.citrix.com`. Étant donné que le `sales.citrix.com` est délégué, il ne fait pas

partie de la zone sur laquelle le serveur de citrix.com noms fait autorité. Le diagramme suivant montre les deux zones.

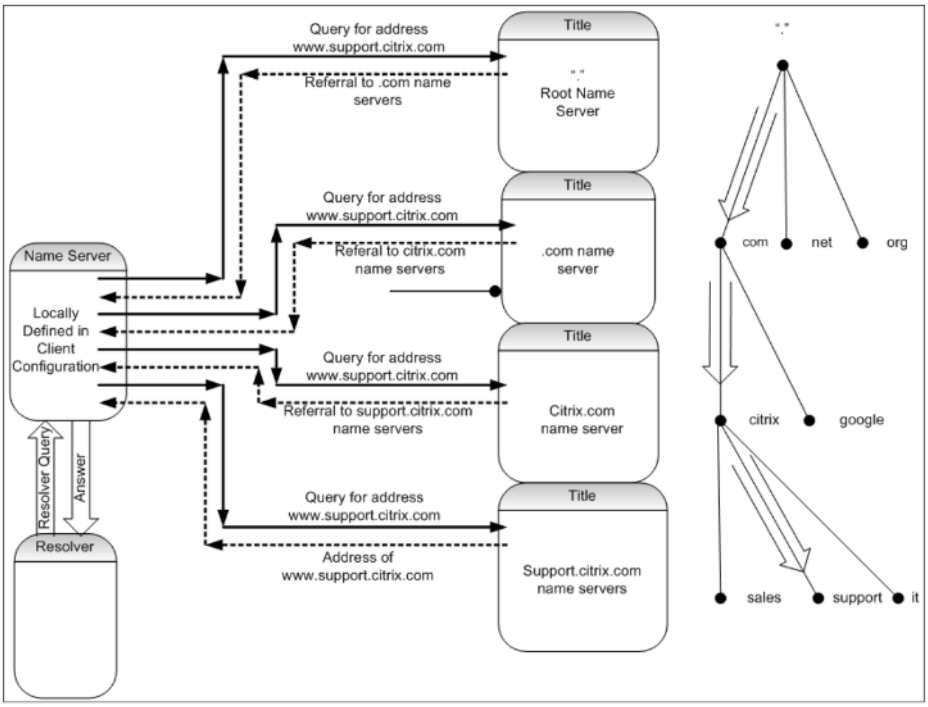


Pour déléguer correctement un sous-domaine, vous devez attribuer des pouvoirs pour ce sous-domaine à différents serveurs de noms. Dans l'exemple précédent, le ns1.citrix.com ne contient pas d'informations sur le sales.citrix.com sous-domaine. Il contient plutôt des pointeurs vers les serveurs de noms qui font autorité pour le ns1.sales.citrix.com sous-domaine.

Serveurs de noms racine et résolution des requêtes

Les serveurs de noms racine connaissent les adresses IP de tous les serveurs de noms faisant autorité pour les domaines de deuxième niveau. Si un serveur de noms ne dispose pas d'informations sur un domaine donné dans ses propres fichiers de données, il n'a qu'à contacter un serveur racine pour commencer à parcourir la branche appropriée de l'arborescence **DNS** afin d'accéder au domaine donné. Il s'agit d'une série de demandes adressées à plusieurs serveurs de noms afin de faciliter la traversée de l'arborescence afin de trouver le prochain serveur de noms faisant autorité, qui doit être contacté pour une résolution ultérieure.

Le diagramme suivant montre une requête DNS typique, en supposant qu'il n'y ait pas d'enregistrement mis en cache pour le nom demandé pendant la traversée. L'exemple suivant utilise une maquette du domaine Citrix.



Requêtes récursives et non récursives

L'exemple précédent illustre les deux types de requêtes pouvant survenir.

- Requête récursive : La requête entre le résolveur et le serveur de noms configuré localement est récursive. Cela signifie que le serveur de noms reçoit la requête et ne répond pas au résolveur tant que la requête n'a pas reçu une réponse complète ou qu'une erreur n'a pas été renvoyée. Si le serveur de noms reçoit une référence vers la requête, le serveur de noms suit la référence jusqu'à ce que le serveur de noms reçoive enfin la réponse (adresse IP) renvoyée.
- Requête non récursive : La requête que le serveur de noms configuré localement effectue sur le serveur de noms de domaine faisant autorité ultérieur est non récursive (ou itérative). Chaque demande est immédiatement répondue par un renvoi vers un serveur faisant autorité de niveau inférieur ou la réponse à la requête, si le serveur de noms interrogé contient la réponse dans ses fichiers de données ou dans son cache.

Mise en cache

Bien que le processus de résolution soit impliqué et peut nécessiter de petites requêtes à plusieurs hôtes, il est rapide. L'un des facteurs qui augmente la vitesse de résolution DNS est la mise en cache. Chaque fois qu'un serveur Name reçoit une requête récursive, il peut devoir communiquer avec d'autres serveurs pour accéder au serveur faisant autorité approprié pour la demande spécifique. Il stocke toutes les informations qu'il reçoit pour référence ultérieure. Lorsque le client suivant émet

une demande similaire, par exemple un hôte différent mais dans le même domaine, il connaît déjà le serveur de noms qui fait autorité pour ce domaine et peut envoyer une demande directement là au lieu de commencer par le serveur de noms racine.

La mise en cache peut également se produire pour les réponses négatives, telles que les requêtes pour les hôtes qui n'existent pas. Dans ce cas, le serveur ne doit pas interroger le serveur de noms faisant autorité pour le domaine demandé pour déterminer que l'hôte n'existe pas. Pour gagner du temps, le serveur de noms vérifie simplement le cache et réagit avec l'enregistrement négatif.

Les serveurs de noms ne mettent pas en cache les enregistrements indéfiniment, sinon vous ne pouvez jamais mettre à jour les adresses IP. Pour éviter les problèmes de synchronisation, les réponses DNS contiennent une durée de vie (TTL). Ce champ décrit l'intervalle de temps pendant lequel le cache peut stocker un enregistrement avant qu'il ne doive l'abandonner et vérifier auprès du serveur de noms faisant autorité pour les enregistrements mis à jour. Si les enregistrements n'ont pas été modifiés, l'utilisation de TTL permet également des réponses dynamiques rapides des appareils exécutant GSLB.

Types d'enregistrements de ressources

Divers RFC fournissent une liste complète des types d'enregistrements de ressources DNS et de leur description. Le tableau suivant répertorie les types d'enregistrements de ressources courants.

Type d'enregistrement de ressource	Description	RFC
Une	Une adresse d'hôte	RFC 1035
NS	Un serveur de noms faisant autorité	RFC 1035
MD	Une destination de messagerie (obsolète - utiliser MX)	RFC 1035
MF	Un redirecteur de courrier (obsolète - utiliser MX)	RFC 1035
CNAME	Le nom canonique d'un alias	RFC 1035
SOA	Marque le début d'une zone d'autorité	RFC 1035
WKS	Une description de service bien connue	RFC 1035
PTR	Un pointeur de nom de domaine	RFC 1035

Type d'enregistrement de ressource	Description	RFC
HINFO	Informations sur l'hôte	RFC 1035
MINFO	Informations sur la boîte aux lettres ou la liste de diffusion	RFC 1035
MX	Échange de courrier	RFC 1035
TXT	chaînes de texte	RFC 1035
AAAA	Adresse IP6	RFC 3596
SRV	Sélection de serveurs	RFC 2782]

Comment GSLB prend en charge le DNS

GSLB utilise des algorithmes et des protocoles qui décident quelle adresse IP doit être envoyée pour une requête DNS. Les sites GSLB sont distribués géographiquement et il existe un serveur de noms faisant autorité DNS sur chaque site exécuté en tant que service sur l'appliance Citrix ADC. Tous les serveurs de noms des différents sites concernés font autorité pour le même domaine. Chacun des domaines GSLB est un sous-domaine pour lequel une délégation est configurée. Par conséquent, les serveurs de noms GSLB font autorité et peuvent utiliser l'un des différents algorithmes d'équilibrage de charge pour décider de l'adresse IP à renvoyer.

Une délégation est créée en ajoutant un enregistrement de serveur de noms pour le domaine GSLB dans les fichiers de base de données du domaine parent et un enregistrement d'adresse ultérieur pour les serveurs de noms utilisés pour la délégation. Par exemple, si vous souhaitez utiliser GSLB pour `www.citrix.com`, le fichier SOA Bind suivant peut être utilisé pour déléguer des demandes `www.citrix.com` à des serveurs de noms : Netscaler1 et Netscaler2.

```
###########################################################################

@ IN SOA citrix.com. hostmaster.citrix.com. (
1 ; serial
3h ; refresh
1h ; retry
1w ; expire
1h ) ; negative caching TTL
IN NS ns1
IN NS ns2
IN MX 10 mail

ns1    IN A 10.10.10.10
ns2    IN A 10.10.10.20
```



```
mail  IN A 10.20.20.50

### Old Configuration if www was not delegated to a GSLB name server
www IN A 10.20.20.50

### Updated Configuration
Netscaler1 IN A xxx.xxx.xxx.xxx
Netscaler2 IN A yyy.yyy.yyy.yyy
www IN NS Netscaler1.citrix.com.
www IN NS Netscaler2.citrix.com.
###
IN MX 20 mail2
mail2 IN A 10.50.50.20
################################################################################


<!--NeedCopy-->
```

La compréhension de BIND n'est pas obligatoire pour configurer DNS. Toutes les implémentations de serveur DNS conformes disposent d'une méthode permettant de créer la délégation équivalente. Les serveurs DNS Microsoft peuvent être configurés pour délégation en utilisant les instructions de la section Créer une délégation de zone.

Ce qui différencie GSLB sur l'appliance Citrix ADC de l'utilisation du service DNS standard pour la distribution du trafic, c'est que les sites Citrix ADC GSLB échangent des données à l'aide d'un protocole propriétaire appelé Metric Exchange Protocol (MEP). Avec MEP, les sites GSLB sont en mesure de conserver des informations sur tous les autres sites. Lorsqu'une demande DNS est reçue, le MEP prend en compte les mesures GSLB pour déterminer les informations suivantes :

- Site avec le moins de connexions actuelles
- Site le plus proche du serveur LDNS, qui a envoyé la demande en fonction des temps aller-retour (RTT).

Plusieurs algorithmes d'équilibrage de charge peuvent être utilisés, mais GSLB est un DNS dont le cerveau est en dessous indiquant au serveur de noms (hébergé sur l'appliance Citrix ADC) quelle adresse doit être envoyée en fonction des mesures des sites participants.

Les autres avantages que GSLB offre sont la capacité de maintenir la persistance (ou l'affinité du site). Les réponses aux requêtes DNS entrantes peuvent être comparées à l'adresse IP source pour déterminer si cette adresse a été dirigée vers un site particulier dans un passé récent. Si c'est le cas, la même adresse est envoyée dans la réponse DNS pour s'assurer que la session client est maintenue.

Une autre forme de persistance est obtenue au niveau du site à l'aide de redirections HTTP ou de proxy HTTP. Ces formes de persistance se produisent après la réponse DNS. Par conséquent, si vous recevez une demande HTTP sur un site contenant un cookie pour diriger la demande vers un autre

site participant, vous pouvez répondre par une redirection ou envoyer un proxy à la demande vers le site approprié.

Protocole d'échange de mesures

Le protocole MEP (Metric Exchange Protocol) est utilisé pour partager les données utilisées dans les calculs GSLB entre sites. À l'aide de connexions MEP, vous échangez trois types de données. Ces connexions n'ont pas besoin d'être sécurisées via le port TCP 3011 ou peuvent être sécurisées à l'aide du port SSL sur le port TCP 3009.

Les trois types de données suivants sont échangés et possèdent leurs propres intervalles et méthodes d'échange.

- **Échange de mesures de site :** Il s'agit d'un modèle d'échange d'interrogation. Par exemple, si site1 dispose d'une configuration pour les services site2, un site1 demande à site2 l'état des services GSLB chaque seconde. Site2 répond avec l'état et d'autres détails de chargement.
- **Échange de mesures réseau :** Il s'agit de l'échange d'informations LDNS RTT, utilisé dans l'algorithme d'équilibrage de charge de proximité dynamique. Il s'agit d'un modèle d'échange push. Toutes les cinq secondes, chaque site transmet ses données vers d'autres sites participants.
- **Échange de persistance :** Il s'agit de l'échange de persistance SOURCEIP. Il s'agit également d'un modèle d'échange push. Toutes les cinq secondes, chaque site transmet ses données vers d'autres sites participants.

Par défaut, les services de site sont surveillés par MEP sur la base des informations d'interrogation uniquement. Si vous liez des moniteurs en fonction de l'intervalle de surveillance, l'état est mis à jour et vous pouvez contrôler la fréquence des mises à jour en définissant l'intervalle de surveillance en conséquence.

Recommandations de mise à niveau pour le déploiement GSLB

October 5, 2021

Cette section fournit des recommandations sur la séquence dans laquelle les nœuds GSLB doivent être mis à niveau dans diverses configurations GSLB. Il aborde également quelques questions fréquentes.

Remarque : L'appliance Citrix ADC à partir de laquelle la synchronisation GSLB est démarrée est appelée « site principal » et les sites GSLB sur lesquels la configuration est copiée en tant que « sites subordonnés ».

Avant de commencer le processus de mise à niveau, lisez les conditions préalables mentionnées dans les rubriques suivantes :

- Avant de commencer
- Mettez à niveau une paire haute disponibilité.
- Mettez à niveau un cluster.

Points à noter lors de la mise à niveau des configurations GSLB

- Dans une configuration HA, commencez par mettre à niveau les sites subordonnés, puis le site principal.
- Dans une configuration HA, les états de service peuvent ne pas se propager d'un nœud principal de génération antérieure vers un nœud secondaire de génération plus récent. Toutefois, si les versions sont de versions différentes, mais qu'elles ont la même version HA, l'état du service peut toujours se propager.
- Si GSLB est configuré au sein d'un cluster, mettez d'abord à niveau les nœuds non propriétaires, puis mettez à niveau le nœud propriétaire. S'il existe un ou plusieurs sites dans un cluster, suivez la même séquence de mise à niveau dans chacun des sites.
- Activez les nouvelles fonctionnalités GSLB uniquement après avoir mis à niveau tous les nœuds vers une version plus récente.
- Mettez à niveau tous les nœuds GSLB vers la dernière version. Il n'y a pas d'impact fonctionnel sur les fonctionnalités disponibles lorsque certains nœuds GSLB utilisent une version plus ancienne et que certains nœuds GSLB sont mis à niveau vers une version plus récente.

FAQ

- **Les états du service GSLB sont-ils propagés lorsque les instances exécutent des versions logicielles différentes ?**

  Le MEP GSLB est fonctionnel lorsque les instances sont exécutées sur différentes versions et que les états de service GSLB sont propagés sur les sites GSLB. Il n'y a aucun impact sur la communication MEP lorsque les instances exécutent différentes versions après une mise à niveau.

- **Est-il recommandé de modifier la configuration pendant une mise à niveau ?**

  In a GSLB setup, when a main site is being upgraded, it is not recommended to do configuration changes on any other GSLB nodes.

Ressources connexes

Les ressources suivantes fournissent des informations sur la mise à niveau d'une instance Citrix ADC à l'aide de Citrix ADM :

- 10 façons dont le service Citrix ADM prend en charge les mises à niveau Citrix ADC simplifiées
- Utiliser le service Citrix ADM pour mettre à niveau les instances Citrix ADC
- Utiliser le logiciel Citrix ADM pour mettre à niveau des instances Citrix ADC

Cas d'utilisation : Déploiement d'un groupe de services de mise à l'échelle automatique basé sur un nom de domaine

August 20, 2021

> **Conseil**
>
> Pour plus d'informations sur les groupes de services GSLB, voir Configuration d'un groupe de services GSLB.

Scénario de déploiement

Deux centres de données sont déployés dans deux régions AWS, l'un à Sydney et l'autre en Virginie du Nord. Un autre centre de données est déployé dans Azure. Un ELB AWS dans chaque région AWS est utilisé pour équilibrer la charge des serveurs d'applications. ALB est utilisé pour Azure pour équilibrer la charge du serveur d'applications. Les appliances Citrix ADC sont configurées pour GSLB pour les ELB et ALB à l'aide d'un groupe de services de mise à l'échelle automatique basé sur un nom de domaine GSLB.

> **Important**
>
> Vous devez configurer les groupes de sécurité requis dans AWS et les attacher à l'instance GSLB. Le port 53 doit être autorisé dans les règles entrantes et sortantes du groupe de sécurité. En outre, les ports (3009 ou 3011 selon la configuration MEP sécurisée) pour la communication MEP doivent être ouverts. Pour la surveillance des applications, les ports correspondants doivent être autorisés dans les règles sortantes du groupe de sécurité.

Les étapes de configuration du scénario de déploiement ci-dessus et des commandes CLI correspondantes sont les suivantes :

1. Créer des centres de données (représentés par des sites GSLB).

   ```
   add gslb site aws-sydney 192.0.2.2

   add gslb site aws-nvirginia 198.51.100.111

   add gslb site alb-southindia 203.0.113.6
   ```

2. Ajoutez un serveur de noms avec l'adresse IP de la passerelle DNS où le nœud GSLB est ajouté. Cela doit être fait dans tous les centres de données.


```
add dns nameServer 8.8.8.8
```

3. Ajouter des serveurs pour ELB et ALB.

```
add server aws-sydney_server lb-sydney-1052691850.ap-southeast-2.elb.amazonaws.com

add server aws-nvirginia_server LB-nvirginia-860559595.us-east-1.elb.amazonaws.com

add server alb-southindia_server alb.southindia.cloudapp.azure.com
```

4. Ajoutez des groupes de services à mise à l'échelle automatique GSLB pour chaque ELB et ALB et liez chaque serveur au groupe de services respectif.

```
add gslb serviceGroup aws-nvirginia_sg HTTP -autoScale DNS -siteName aws-nvirginia

add gslb serviceGroup aws-sydney_sg HTTP -autoScale DNS -siteName aws-sydney

add gslb serviceGroup alb-southindia_sg HTTP -autoScale DNS -siteName alb-southindia

bind gslb serviceGroup aws-nvirginia_sg aws-nvirginia_server 80

bind gslb serviceGroup aws-sydney_sg aws-sydney_server 80

bind gslb serviceGroup alb-southindia_sg alb-southindia_server 80
```

5. Ajoutez un serveur virtuel GSLB et liez le domaine d'application et les groupes de services à ce serveur virtuel.

```
add gslb vserver gv1 HTTP

bind gslb vserver gv1 -serviceGroupName aws-nvirginia_sg

bind gslb vserver gv1 -serviceGroupName aws-sydney_sg

bind gslb vserver gv1 -serviceGroupName alb-southindia_sg
```

Cas d'utilisation : déploiement d'un groupe de services GSLB basé sur une adresse IP

August 20, 2021

> **Conseil**
>
> Pour plus d'informations sur les groupes de services GSLB, voir Configuration d'un groupe de

> services GSLB.

Scénario de déploiement

S'il existe plusieurs applications hébergées sur le même serveur d'applications, le GSLB doit sonder ces applications pour voir si elles répondent ou non. Si une application ne répond pas, l'utilisateur doit être dirigé vers le serveur sur lequel l'application est UP. En outre, si l'une des applications est DOWN, le serveur ne doit pas être marqué DOWN, car les autres applications sont UP.

Dans l'exemple suivant, plusieurs applications (HTTPS) sont hébergées sur un serveur dans chaque site GSLB et donc toutes ces applications se résolvent en une seule adresse IP du site respectif.

À l'aide des groupes de services GSLB, vous pouvez avoir le même serveur avec une adresse IP et un port liés à plusieurs groupes de services où chaque groupe de services représente une application différente.

Un moniteur spécifique à l'application est lié aux groupes de services qui marque le groupe de services comme DOWN si l'application est en panne. Ainsi, chaque fois qu'une application est DOWN, seule cette application est retirée de l'installation et non du serveur.

```
```
add gslb serviceGroup app1_site1 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s1

add gslb serviceGroup app2_site1 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s1

add gslb serviceGroup app1_site2 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s2

add gslb serviceGroup app2_site2 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s2

add lb monitor http_app2 HTTP -respCode 200 -httpRequest "GET /testsite
    /app2.html"

add lb monitor http_app1 HTTP -respCode 200 -httpRequest "GET /testsite
    /app1.html"

bind gslb serviceGroup app1_site1 192.0.2.140 80

bind gslb serviceGroup app1_site1 -monitorName http_app1

bind gslb serviceGroup app2_site1 192.0.2.140 80

```

 
```

```
bind gslb serviceGroup app2_site1 -monitorName http_app2

bind gslb serviceGroup app1_site2 192.0.2.142 80

bind gslb serviceGroup app1_site2 -monitorName http_app1

bind gslb serviceGroup app2_site2 192.0.2.142 80

bind gslb serviceGroup app2_site2 -monitorName http_app2
<!--NeedCopy--> ```
```

Articles pratiques

January 21, 2021

Les articles pratiques GSLB contiennent des informations sur certaines des configurations GSLB importantes telles que la personnalisation de la configuration GSLB, la configuration des connexions persistantes, la reprise après sinistre, etc.

Personnalisation de votre configuration GSLB

Configuration des connexions persistantes

Gestion des connexions client

Configurer GSLB pour la proximité

Protection de la configuration GSLB contre les défaillances

Configuration de GSLB pour la reprise après sinistre

Remplacer le comportement de proximité statique en configurant les emplacements préférés

Configuration de la sélection de service GSLB à l'aide de la commutation de contenu

Configuration de l'équilibrage de la charge du serveur global pour les requêtes DNS avec les enregistrements NAPTR

Utilisation de l'option de sous-réseau client EDNS0 pour l'équilibrage de la charge du serveur global

Exemple de configuration parent-enfant complète à l'aide du protocole Exchange de mesures

Personnaliser votre configuration GSLB

August 20, 2021

Une fois votre configuration GSLB de base opérationnelle, vous pouvez la personnaliser en modifiant la bande passante d'un service GSLB, en configurant les services GSLB basés sur CNAME, la proximité statique, la RTT dynamique, les connexions persistantes ou les pondérations dynamiques pour les services, ou en modifiant la méthode GSLB.

Vous pouvez également configurer la surveillance des services GSLB pour déterminer leur état.

Ces paramètres dépendent de votre déploiement réseau et des types de clients que vous prévoyez de vous connecter à vos serveurs.

Modifier les connexions maximales ou la bande passante maximale pour un service GSLB

Vous pouvez limiter le nombre de nouveaux clients qui peuvent se connecter simultanément à un serveur virtuel d'équilibrage de charge ou de commutation de contenu en configurant le nombre maximal de clients et/ou la bande passante maximale pour le service GSLB qui représente le serveur virtuel.

Pour modifier la largeur maximale des clients ou de la bande passante d'un service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour modifier le nombre maximal de connexions client ou la bande passante maximale d'un service GSLB et vérifier la configuration :

```
set gslb service <serviceName> [-maxClients <positive_integer>] [-
   maxBandwidth <positive_integer>]
show gslb service <serviceName>
<!--NeedCopy-->
```

Exemple :

```
set glsb service Service-GSLB-1 -maxBandwidth 100 -maxClients 100
show gslb service Service-GSLB-1
<!--NeedCopy-->
```

Pour modifier la largeur maximale des clients ou de la bande passante d'un service GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Services**, puis double-cliquez sur un service.
2. Cliquez dans la section **Autres paramètres** et définissez les paramètres suivants :
   - Nombre maximal de clients : MaxClients
   - Largeur de bande maximale : largeur de bande maximale

Créer des services GSLB basés sur CNAME

Pour configurer un service GSLB, vous pouvez utiliser l'adresse IP du serveur ou un nom canonique du serveur. Si vous souhaitez exécuter plusieurs services (comme un FTP et un serveur Web, chacun s'exécutant sur des ports différents) à partir d'une seule adresse IP ou exécuter plusieurs services HTTP sur le même port, avec des noms différents, sur le même hôte physique, vous pouvez utiliser des noms canoniques (CNAMES) pour les services.

Par exemple, vous pouvez avoir deux entrées dans DNS comme ftp.example.com et www.example.com pour les services FTP et les services HTTP sur le même domaine, example.com. Les services GSLB basés sur CNAME sont utiles dans une configuration de résolution de domaine à plusieurs niveaux ou dans l'équilibrage de charge de domaine à plusieurs niveaux. La configuration d'un service GSLB basé sur CNAME peut également aider si l'adresse IP du serveur physique est susceptible de changer.

Si vous configurez des services GSLB basés sur CNAME pour un domaine GSLB, lorsqu'une requête est envoyée pour le domaine GSLB, l'appliance Citrix ADC fournit un CNAME au lieu d'une adresse IP. Si l'enregistrement A de cet enregistrement CNAME n'est pas configuré, le client doit interroger le domaine CNAME pour l'adresse IP. Si l'enregistrement A de cet enregistrement CNAME est configuré, l'appliance Citrix ADC fournit au CNAME l'enregistrement A correspondant (adresse IP). L'appliance Citrix ADC gère la résolution finale de la requête DNS, telle que déterminée par la méthode GSLB. Les enregistrements CNAME peuvent être conservés sur une autre appliance Citrix ADC ou sur un système tiers.

Dans un service GSLB basé sur une adresse IP, l'état d'un service est déterminé par l'état du serveur qu'il représente. Toutefois, un service GSLB basé sur CNAME a son état défini sur UP par défaut ; l'adresse IP du serveur virtuel (VIP) ou le protocole d'échange métrique (MEP) ne sont pas utilisés pour déterminer son état. Si un moniteur de bureau est lié à un service GSLB basé sur CNAME, l'état du service est déterminé en fonction du résultat des sondes de moniteur.

Vous pouvez lier un service GSLB basé sur CNAME uniquement à un serveur virtuel GSLB dont le type d'enregistrement DNS est CNAME. En outre, une appliance Citrix ADC peut contenir au plus un service GSLB avec une entrée CNAME donnée.

Voici quelques-unes des fonctionnalités prises en charge pour un service GSLB basé sur CNAME :

- L'affinité de site basée sur la stratégie GSLB est prise en charge, avec CNAME comme emplacement privilégié.
- La persistance de l'adresse IP source est prise en charge. L'entrée de persistance contient les informations CNAME au lieu de l'adresse IP et du port du service sélectionné.

Voici les limites des services GSLB basés sur CNAME :

- La persistance du site n'est pas prise en charge, car le service référencé par un CNAME peut être présent à n'importe quel emplacement tiers.

- La réponse à plusieurs adresses IP n'est pas prise en charge car un domaine ne peut pas avoir plusieurs entrées CNAME.
- Le hachage IP source et Round Robin sont les seules méthodes d'équilibrage de charge prises en charge. La méthode Proximité statique n'est pas prise en charge car un CNAME n'est pas associé à une adresse IP et la proximité statique ne peut être maintenue qu'en fonction des adresses IP.

Remarque : La fonctionnalité Empty-Down-Response doit être activée sur le serveur virtuel GSLB auquel vous liez le service GSLB basé sur CName-based. Si vous activez la fonctionnalité Empty-Down-Response, lorsqu'un serveur virtuel GSLB est DÉSACTIVÉ ou désactivé, la réponse à une requête DNS, pour les domaines liés à ce serveur virtuel, contient un enregistrement vide sans adresse IP, au lieu d'un code d'erreur.

Pour créer un service GSLB basé sur CNAME à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add gslb service <serviceName> -cnameEntry <string> -siteName <string>
2 <!--NeedCopy-->
```

Exemple :

```
1 add gslb service Service-GSLB-1 -cnameEntry transport.mycompany.com -
     siteName Site-GSLB-East-Coast
2 add gslb service Service-GSLB-2 -cnameEntry finance.mycompany.com -
     siteName Site-GSLB-West-Coast
3 <!--NeedCopy-->
```

Pour créer un service GSLB basé sur CNAME à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Services**.
2. Créez un service et définissez le **Type sur Canonical Name Based**.

Configurer l'état hors service de transition (TROFS) dans GSLB

Lorsque vous configurez la persistance sur un serveur virtuel GSLB auquel un service est lié, le service continue de servir les demandes du client même après sa désactivation, acceptant de nouvelles requêtes ou connexions uniquement pour honorer la persistance. Après une période configurée, connue sous le nom de période d'arrêt gracieux, aucune nouvelle demande ou connexion n'est dirigée vers le service et toutes les connexions existantes sont fermées.

Lorsque vous désactivez un service, vous pouvez spécifier une période d'arrêt gracieuse, en secondes, à l'aide de l'argument delay. Pendant la période d'arrêt gracieux, si le service est lié à un serveur virtuel, son état apparaît comme « hors service ».

Configurer des pondérations dynamiques pour les services

Dans un réseau typique, il existe des serveurs qui ont une capacité de trafic plus élevée que d'autres. Cependant, avec une configuration régulière d'équilibrage de charge, la charge est répartie uniformément entre tous les services, même si différents services représentent des serveurs ayant des capacités différentes.

Pour optimiser vos ressources GSLB, vous pouvez configurer des pondérations dynamiques sur un serveur virtuel GSLB. Les pondérations dynamiques peuvent être basées soit sur le nombre total de services liés au serveur virtuel, soit sur la somme des pondérations des différents services liés au serveur virtuel. La distribution du trafic est ensuite basée sur les poids configurés pour les services.

Lorsque des pondérations dynamiques sont configurées sur le serveur virtuel GSLB, les requêtes sont distribuées selon la méthode d'équilibrage de charge, la pondération du service GSLB et la pondération dynamique. Le produit du poids du service GSLB et du poids dynamique est connu sous le nom de poids cumulatif. Par conséquent, lorsque le poids dynamique est configuré sur le serveur virtuel GSLB, les requêtes sont distribuées sur la base de la méthode d'équilibrage de charge et du poids cumulé.

Lorsque la pondération dynamique d'un serveur virtuel est désactivée, la valeur numérique est définie sur 1. Cela garantit que le poids cumulé est un entier différent de zéro à tout moment.

La pondération dynamique peut être basée sur le nombre total de services actifs liés à des serveurs virtuels d'équilibrage de charge ou sur les pondérations attribuées aux services.

Considérez une configuration avec deux sites GSLB configurés pour un domaine et chaque site dispose de deux services pouvant servir le client. Si un service sur l'un ou l'autre site tombe en panne, l'autre serveur de ce site doit gérer deux fois plus de trafic qu'un service sur l'autre site. Si la pondération dynamique est basée sur le nombre de services actifs, le site dont les deux services sont actifs a deux fois plus de poids que celui du site avec un service en panne et reçoit donc deux fois plus de trafic.

Vous pouvez également envisager une configuration dans laquelle les services du premier site représentent des serveurs deux fois plus puissants que les serveurs du second site. Si la pondération dynamique est basée sur les poids attribués aux services, le trafic peut être envoyé deux fois plus important au premier site que au second.

Remarque : Pour plus d'informations sur l'attribution de poids aux services d'équilibrage de charge, voir Assignation de poids aux services.

Pour illustrer la façon dont le poids dynamique est calculé, considérez un serveur virtuel GSLB auquel un service GSLB est lié. Le service GSLB représente un serveur virtuel d'équilibrage de charge qui, à son tour, a deux services liés à lui. Le poids attribué au service GSLB est 3. Les pondérations attribuées aux deux services sont respectivement de 1 et 2. Dans cet exemple, lorsque le poids dynamique est défini sur :

- **Désactivé:Le**poids cumulé du serveur virtuel GSLB est le produit du poids dynamique (désactivé = 1) et du poids du service GSLB (3), de sorte que le poids cumulé est 3.
- **SERVICECOUNT** : Le nombre est la somme du nombre de services liés aux serveurs virtuels d'équilibrage de charge correspondant au service GSLB (2), et le poids cumulé est le produit du poids dynamique (2) et du poids du service GSLB (3), qui est 6.
- **SERVICEWEIGHT** : Le poids dynamique est la somme des poids des services liés aux serveurs virtuels d'équilibrage de charge correspondant au service GSLB (3), et le poids cumulatif est le produit du poids dynamique (3) et du poids du service GSLB (3), qui est 9.

Remarque : Les pondérations dynamiques ne sont pas applicables lorsque des serveurs virtuels de commutation de contenu sont configurés.

Pour configurer un serveur virtuel GSLB pour utiliser des pondérations dynamiques à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb vserver <name> -dynamicWeight SERVICECOUNT | SERVICEWEIGHT
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver vserver-GSLB-1 -dynamicWeight SERVICECOUNT
<!--NeedCopy-->
```

Pour définir le serveur virtuel GSLB pour qu'il utilise des pondérations dynamiques à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Serveurs virtuels, double-cliquez sur le serveur virtuel GSLB dont vous souhaitez modifier la méthode (par exemple, vServer-GSLB-1).
2. Cliquez sur la section **Méthode** et, dans la liste déroulante **Poids dynamique**, sélectionnez **SERVICECOUNT** ou **SERVICEWEIGHT**.

Comment configurer la persistance dans GSLB

August 20, 2021

La persistance garantit qu'une série de demandes client pour un nom de domaine particulier est envoyée au même centre de données au lieu d'équilibrer la charge. Si la persistance est configurée pour

un domaine particulier, elle a priorité sur la méthode GSLB configurée. Vous pouvez utiliser la persistance pour les déploiements où une information liée à une transaction client est stockée localement sur une instance qui a servi les requêtes initiales. Par exemple, les déploiements pour le commerce électronique qui utilise un panier d'achat, où le serveur doit conserver l'état de la connexion pour suivre la transaction. L'appliance Citrix ADC sélectionne un centre de données pour traiter une demande client. Lorsque la persistance est activée, elle transfère la même adresse IP du centre de données sélectionné pour toutes les demandes DNS (Domain Name System) suivantes. Si une session de persistance pointe vers un centre de données en panne, l'appliance Citrix ADC utilise la méthode GSLB configurée pour sélectionner un nouveau centre de données. Il devient alors persistant pour les demandes ultérieures du client.
Pour la persistance dans GSLB, le même ensemble d'identificateurs de persistance (PersistID) doit être configuré sur les serveurs virtuels GSLB dans tous les centres de données. Le module GSLB utilise l'identificateur de persistance pour identifier de manière unique un serveur virtuel GSLB. Lorsque la persistance IP source est activée sur le serveur virtuel GSLB, les sessions de persistance sont également échangées dans le cadre de l'échange de mesures. Pour que l'appliance Citrix ADC prend en charge la persistance sur tous les sites, la configuration liée à la persistance doit être effectuée sur tous les sites GSLB participants. Citrix recommande la persistance dans GSLB pour les applications avec état, ce qui oblige les clients à se reconnecter à la même instance d'application pour les demandes suivantes.

Vous pouvez obtenir la persistance dans GSLB par les moyens suivants :

- Persistance sur le serveur virtuel GSLB
- Persistance du site sur les services de la GSLB

Persistance sur le serveur virtuel GSLB

La persistance sur le serveur virtuel GSLB est utilisée lors des requêtes DNS. L'adresse IP source de la demande DNS est utilisée pour créer une session de persistance entre le client et le centre de données. Les clients DNS sont généralement les passerelles DNS locales (LDNS) ou DNS qui procurent un ensemble de clients assis derrière eux (dans les FAI). La persistance sur un serveur virtuel GSLB est agnostique du protocole d'application.
En général, plusieurs passerelles DNS ou serveurs LDNS (Local Domain Name Server) sont configurés dans le réseau client. Citrix vous recommande de configurer un masque de persistance approprié car pour les demandes DNS suivantes, quels que soient les périphériques LDNS en amont utilisés pour se connecter à l'appliance ADC, le client peut persister vers le même centre de données qui avait servi les requêtes antérieures. Une fois la session de persistance créée pour une adresse IP LDNS, tous les clients finaux qui se connectent à l'aide de ce LDNS reçoivent la même adresse IP du centre de données.

Persistance du site sur les services de la GSLB

La persistance du site devient effective lors du traitement des demandes de demande. La persistance du site ne fonctionne que pour le trafic HTTP et HTTPS car la persistance est obtenue à l'aide du cookie HTTP. Comme les cookies sont conservés sur les clients HTTP (navigateurs), ils donnent une visibilité sur les clients assis derrière les passerelles DNS. Lorsque vous utilisez des cookies pour obtenir la persistance des clients, aucune ressource n'est consommée sur l'appliance ADC pour chaque client entrant. Lorsque vous mettez un service GSLB hors service avec un délai de retard, le service passe à l'état hors service (TROFS). La persistance est prise en charge tant que le service est à l'état UP ou TROFS. Autrement dit, si le même client envoie une demande pour le même service dans le délai spécifié après qu'un service est marqué TROFS, le même site GSLB (centre de données) assure la maintenance de la demande.

Si vous accédez à une application via un alias, assurez-vous que l'enregistrement CNAME est également configuré sur l'appliance Citrix ADC. Dans une topologie parent-enfant, la persistance du site ne fonctionne pas lorsque vous accédez à une application via un alias.

> Remarque
>
> Si le proxy de connexion est spécifié comme méthode de persistance du site et que vous souhaitez également configurer la persistance sur les serveurs virtuels LB, la persistance IP source n'est pas recommandée. Lorsque la connexion est mise en service par proxy, une adresse IP appartenant à l'appliance ADC est utilisée, et non l'adresse IP réelle du client.
> Configurez une persistance appropriée, qui n'utilise pas l'adresse IP source de la requête HTTP (S) pour identifier le client, par exemple la persistance des cookies ou la persistance basée sur des règles.

Configurer la persistance en fonction de l'adresse IP source

Si la persistance IP source est configurée sur le serveur virtuel GSLB, des sessions de persistance sont créées pour l'adresse IP source de la requête DNS. Selon la fonctionnalité Extended Client Subnet (ECS), l'adresse IP source de la requête DNS provient de l'une des options suivantes :

- L'adresse IP source dans l'en-tête IP du paquet de requête DNS entrant
- L'option ECS de la requête DNS Pour plus d'informations sur ECS, voir Utiliser l'option de sous-réseau client EDNS0 pour Global Server Load Balancing.

Les sessions de persistance d'un client durent jusqu'au délai d'expiration de la persistance. Après l'expiration du délai d'expiration, les sessions de persistance existantes sont effacées. Pour les demandes subséquentes, une nouvelle décision du GSLB est prise et une adresse IP différente du service GSLB peut être sélectionnée.
La persistance IP source sur le serveur virtuel GSLB et la persistance du site sur le service GSLB se complètent mutuellement. Si la persistance IP source est désactivée sur le serveur virtuel GSLB, le

serveur virtuel GSLB choisit un service GSLB différent chaque fois que le DNS tente d'effectuer la résolution. Le client se connecte également à un service GSLB différent et au centre de données qui reçoit la demande d'application proxy la connexion au centre de données qui a servi le client en premier. Cela peut ajouter une certaine latence. Ainsi, en activant la persistance IP source sur le serveur virtuel GSLB peut éviter de fréquents sauts multiples pour les demandes d'application. Si la session de persistance IP source a expiré et que le client se reconnecte après cela, la persistance du site relie le client au centre de données, qui avait initialement servi le client. En outre, si le client se connecte de nouveau via une passerelle DNS, qui n'entre pas dans la plage de masque de persistance configurée, la persistance du site aide les clients à s'en tenir au centre de données qui a servi la première demande.

Pour configurer la persistance en fonction de l'adresse IP source à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb vserver <name> -persistenceType (SOURCEIP|NONE) -persistenceId
    <positive_integer> [-persistMask <netmask>] - [timeout <mins>]
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver vserver-GSLB-1 -persistenceType SOURCEIP -
   persistenceId 23 -persistMask 255.255.255.255 - timeout 2
<!--NeedCopy-->
```

Pour configurer la persistance en fonction de l'adresse IP source à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel GSLB dont vous souhaitez modifier la méthode (par exemple, vServer-GSLB-1).
2. Cliquez sur la section **Persistance** et, dans la liste déroulante **Persistance**, sélectionnez **SOURCEIP** et définissez les paramètres suivants :
   - ID de persistance : persistenceID
   - Délai d'expiration : délai d'expiration
   - Longueur du masque de réseau IPv4 ou du masque IPv6 : masque persistant

Configurer la persistance du site en fonction des cookies HTTP

La persistance du site est obtenue à l'aide de cookies HTTP (appelés « cookies du site ») pour reconnecter le client au même serveur. Lorsque l'appliance GSLB répond à une demande DNS client en envoyant l'adresse IP du site GSLB sélectionné, le client envoie une requête HTTP à ce site GSLB. Point

de terminaison d'application dans ce site GSLB ajoute un cookie de site à l'en-tête HTTP, et la persistance du site est en vigueur.
Si le client envoie une requête DNS après l'expiration du cache client, la requête DNS peut être dirigée vers un autre site GSLB. Le nouveau site GSLB utilise le cookie du site présent dans l'en-tête de requête du client pour implémenter la persistance. La fonctionnalité de persistance du site devient active dans les conditions suivantes :

- Lorsque le nom de domaine dans l'en-tête de l'hôte correspond à l'un des domaines GSLB
- Lorsque la persistance du site est activée sur le service GSLB qui représente le serveur virtuel recevant le trafic de l'application.

Le cookie du site contient des informations sur le service GSLB sélectionné sur lequel le client a une connexion persistante. Si le service GSLB pointé par le cookie est désactivé ou supprimé de la configuration GLSB, le serveur virtuel qui reçoit le trafic continue à traiter le trafic. L'expiration du cookie est basée sur le délai d'expiration du cookie configuré sur l'appliance Citrix ADC. Si les noms de serveur virtuel ne sont pas identiques sur tous les sites, vous devez utiliser l'identificateur de persistance. Les cookies insérés sont conformes à la RFC 2109.

Citrix ADC prend en charge deux types de persistance de site :

- Proxy de connexion
- Redirection HTTP

Proxy de connexion

Dans le mode Proxy de connexion de la persistance du site, le centre de données qui reçoit la demande d'application suivante effectue les tâches suivantes pour établir une connexion :

1. Crée une connexion au site GSLB qui a inséré le cookie du site.
2. Proxie la demande du client vers le site d'origine.

   Remarque :

   Le serveur proxy établit la connexion avec le site d'origine en utilisant les détails suivants :

   ```
   1 -  Le SNIP du nouveau site est l'adresse IP source.
   ```

   - L'adresse IP publique du service GSLB du site d'origine est l'adresse IP de destination.
   - Un port éphémère est le port source et le port de service GSLB est le port de destination.
   - Utilise les protocoles HTTP ou HTTPS en fonction du type de service GSLB.
3. Reçoit une réponse du site GSLB d'origine.
4. Relais cette réponse au client.
5. Ferme la connexion.

Redirection HTTP

Si la configuration GSLB utilise la persistance de redirection HTTP, le nouveau site redirige la requête vers le site qui a initialement inséré le cookie. Le nom de domaine dans l'URL de redirection est le domaine du site. Assurez-vous que les cookies et les certificats SSL sont applicables à la fois au domaine GSLB et au domaine du site. Pour appliquer des cookies à la fois pour GSLB et le domaine du site, le domaine des cookies doit être le site du domaine GSLB. Pour appliquer des certificats SSL à la fois à GSLB et au domaine de site, le certificat lié au serveur virtuel SSL doit être un certificat générique.

Le proxy de connexion se produit lorsque les conditions suivantes sont remplies :

- Les demandes sont envoyées pour un domaine participant à GSLB. Le domaine est obtenu à partir de l'en-tête URL/hôte.
- Le service GSLB local a le proxy de connexion activé.
- La demande inclut un cookie valide qui contient l'adresse IP d'un service GSLB distant actif.

> **Remarque**
>
> Dans une configuration parent-enfant GSLB, le proxy de connexion fonctionne comme prévu même lorsqu'un service GSLB n'est pas configuré sur un site enfant. Toutefois, si vous disposez d'une configuration supplémentaire telle que l'authentification client, l'insertion d'adresse IP du client ou toute autre exigence spécifique à SSL, vous devez ajouter un service GSLB explicite sur le site et le configurer en conséquence.
>
> Pour plus d'informations sur la topologie parent-enfant, voir Déploiement de la topologie parent-enfant à l'aide du protocole MEP.

Pour définir la persistance en fonction des cookies HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb service <serviceName> -sitePersistence (ConnectionProxy [-
   sitePrefix <prefix>] | HTTPredirect -sitePrefix <prefix>)
<!--NeedCopy-->
```

Exemple :

```
set gslb service service-GSLB-1 -sitePersistence ConnectionProxy
set gslb service service-GSLB-1 -sitePersistence HTTPRedirect -
   sitePrefix vserver-GSLB-1
<!--NeedCopy-->
```


Pour définir la persistance en fonction des cookies à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Services** et sélectionnez le service que vous souhaitez configurer pour la persistance du site (par exemple, Service-GSLB-1).
2. Cliquez sur la section **Persistance du site** et définissez la persistance en fonction des cookies.

Gérer les connexions client

October 5, 2021

Pour faciliter la gestion des connexions client, vous pouvez activer le nettoyage différé des connexions au serveur virtuel. Vous pouvez ensuite gérer le trafic DNS local en configurant des stratégies DNS.

Activer le nettoyage différé des connexions aux serveurs virtuels

L'état d'un serveur virtuel dépend des états des services qui lui sont liés, et l'état de chaque service dépend des moniteurs qui lui sont liés. En cas de ralentissement ou d'arrêt d'un serveur, le délai des sondes de surveillance est dépassé et le service qui représente le serveur est marqué comme étant EN PANNE. Un serveur virtuel est marqué comme étant en panne uniquement lorsque tous les services qui lui sont liés sont marqués comme étant en panne. Vous pouvez configurer des services et des serveurs virtuels pour qu'ils mettent fin à toutes les connexions lorsqu'elles tombent en panne ou qu'elles autorisent le passage des connexions. Ce dernier paramètre est destiné aux situations dans lesquelles un service est marqué comme étant en panne en raison d'un serveur lent.

Lorsque vous configurez l'option de vidage de l'état d'arrêt, l'appliance Citrix ADC effectue un nettoyage différé des connexions à un service GSLB en panne.

Pour activer le nettoyage différé des connexions au serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le nettoyage des connexions différées et vérifier la configuration :

```
set gslb service <name> -downStateFlush (ENABLED | DISABLED)
show gslb service <name>
<!--NeedCopy-->
```

Exemple :

```
set gslb service Service-GSLB-1 -downStateFlush ENABLED
Done
```



```
3
4 show gslb service Service-GSLB-1
5 Done
6 <!--NeedCopy-->
```

Pour activer le nettoyage différé des connexions au serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Services** et double-cliquez sur le service.
2. Cliquez sur la section **Autres paramètres** et **sélectionnez l'option Flush de l'état désactivée** .

Gérez le trafic DNS local à l'aide de stratégies DNS

Vous pouvez utiliser des stratégies DNS pour implémenter l'affinité de site en dirigeant le trafic depuis l'adresse IP d'un résolveur DNS local ou d'un réseau vers un site GSLB cible prédéfini. Cela est configuré en créant des stratégies DNS avec des expressions DNS et en liant les stratégies globalement sur l'appliance Citrix ADC.

Expressions DNS

L'appliance Citrix ADC fournit certaines expressions DNS prédéfinies qui peuvent être utilisées pour configurer des actions spécifiques à un domaine. Ces actions peuvent, par exemple, supprimer certaines demandes, sélectionner une vue spécifique pour un domaine spécifique ou rediriger certaines demandes vers un emplacement spécifique.

Ces expressions DNS (également appelées *règles*) sont combinées pour créer des stratégies DNS qui sont ensuite liées globalement sur l'appliance Citrix ADC.

Voici la liste des qualificatifs DNS prédéfinis disponibles sur l'appliance Citrix ADC :

- CLIENT.UDP.DNS.DOMAIN.EQ (« nom de domaine »)
- CLIENT.UDP.DNS.IS_AREC
- CLIENT.UDP.DNS.IS_AAAAREC
- CLIENT.UDP.DNS.IS_SRVREC
- CLIENT.UDP.DNS.IS_MXREC
- CLIENT.UDP.DNS.IS_SOAREC
- CLIENT.UDP.DNS.IS_PTRREC
- CLIENT.UDP.DNS.IS_CNAME
- CLIENT.UDP.DNS.IS_NSREC
- CLIENT.UDP.DNS.IS_ANYREC

L'expression DNS CLIENT.UDP.DNS.DOMAIN peut être utilisée avec des expressions de chaîne. Si vous utilisez des noms de domaine dans l'expression, ils doivent se terminer par un point (.). Par exemple, CLIENT.UDP.DNS.DOMAIN.ENDSWITH (« abc.com. »)

Pour créer une expression à l'aide de l'utilitaire de configuration

1. Cliquez sur l'icône en regard de la zone de texte Expression. Cliquez sur Ajouter. (Laissez les zones de liste déroulante Type de flux et protocole vides.) Suivez ces étapes pour créer une règle.
2. Dans la zone Qualificatif, sélectionnez un qualificatif (par exemple, EMPLACEMENT).
3. Dans la zone Opérateur, sélectionnez un opérateur (par exemple, ==).
4. Dans la zone Valeur, tapez une valeur (par exemple, Asie, Japon…).
5. Cliquez sur OK. Cliquez sur Créer, puis sur Fermer. La règle est créée.
6. Cliquez sur OK.

Configurer les actions DNS

Une stratégie DNS inclut le nom d'une action DNS à exécuter lorsque la règle de stratégie est évaluée à TRUE. Une action DNS peut effectuer l'une des opérations suivantes :

- Envoyez au client une adresse IP pour laquelle vous avez configuré une vue DNS. Pour plus d'informations sur les vues DNS, voir Ajout de vues DNS.
- Envoyez au client l'adresse IP d'un service GSLB après avoir fait référence à une liste d'emplacements préférés qui remplace le comportement de proximité statique. Pour plus d'informations sur les emplacements préférés, reportez-vous à la section Remplace le comportement de proximité statique par configuration des emplacements préférés.
- Envoyez au client une adresse IP spécifique telle que déterminée par l'évaluation de la requête ou de la réponse DNS (réécriture de la réponse DNS).
- Transmettez une demande au serveur de noms sans effectuer de recherche dans le cache DNS de la solution matérielle-logicielle.
- Déposez une demande.

Vous ne pouvez pas créer d'action DNS pour supprimer une demande DNS ou pour contourner le cache DNS sur l'appliance. Si vous souhaitez supprimer une demande DNS, utilisez l'action intégrée DNS_Default_Act_Drop. Si vous souhaitez contourner le cache DNS, utilisez l'action intégrée DNS_Default_Act_CacheBypass. Les deux actions sont disponibles avec les actions personnalisées dans les boîtes de dialogue Créer une stratégie DNS et Configurer la stratégie DNS. Ces actions intégrées ne peuvent pas être modifiées ou supprimées.

Pour configurer une action DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une action DNS et vérifier la configuration :

```
add dns action <actionName> <actionType> (-IPAddress <ip_addr |
    ipv6_addr> ... | -viewName <string> | -preferredLocList <string>
    ...) [-TTL <secs>]

show dns action [<actionName>]
<!--NeedCopy-->
```

Exemples

Exemple 1 : Configuration de la réécriture de la réponse DNS. L'action DNS suivante envoie au client une adresse IP préconfigurée lorsque la stratégie à laquelle l'action est liée est évaluée à true :

```
add dns action dns_act_response_rewrite Rewrite_Response -IPAddress
    192.0.2.20 192.0.2.56 198.51.100.10
 Done

show dns action dns_act_response_rewrite
1)  ActionName:  dns_act_response_rewrite ActionType:  Rewrite_Response
     TTL:  3600              IPAddress:  192.0.2.20 192.0.2.56
    198.51.100.10
 Done
<!--NeedCopy-->
```

Exemple 2 : Configuration d'une réponse basée sur la vue DNS. L'action DNS suivante envoie au client une adresse IP pour laquelle vous avez configuré une vue DNS :

```
add dns action send_ip_from_view_internal_ip ViewName -viewName
    view_internal_ip
Done

show dns action send_ip_from_view_internal_ip
1)  ActionName:  send_ip_from_view_internal_ip ActionType:  ViewName
       ViewName:  view_internal_ip
 Done
<!--NeedCopy-->
```

Exemple 3 : Configuration d'une réponse basée sur une liste d'emplacements préférés. L'action DNS suivante envoie au client l'adresse IP qui correspond à l'emplacement préféré qu'il sélectionne dans la liste d'emplacements spécifiée :


```
add dns action send_preferred_location GslbPrefLoc -preferredLocList NA
    .tx.ns1.\*.\*.* NA.tx.ns2.\*.\*.* NA.tx.ns3.\*.\*.*
Done

show dns action  send_preferred_location
1)  ActionName:  send_preferred_location ActionType:  GslbPrefLoc
    PreferredLocList:  "NA.tx.ns1.\*.\*.\*" "NA.tx.ns2.\*.\*.\*" "NA.tx.
    ns3.\*.\*.*"
 Done
<!--NeedCopy-->
```

Pour configurer une action DNS à l'aide de l'utilitaire de configuration Citrix ADC

1. Accédez à Gestion du trafic > DNS > Actions, créez ou modifiez une action DNS.
2. Dans la boîte de dialogue Créer une action DNS ou Configurer une action DNS, définissez les paramètres suivants :
   - Nom de l'action (ne peut pas être modifié pour une action DNS existante)
   - Type (ne peut pas être modifié pour une action DNS existante)
     Pour définir le paramètre
     Type, effectuez l'une des opérations suivantes :
     - Pour créer une action DNS associée à une vue DNS, sélectionnez Nom de la vue. Ensuite, dans la liste Nom de la vue, sélectionnez la vue DNS que vous souhaitez utiliser dans l'action.
     - Pour créer une action DNS avec une liste d'emplacements préférés, sélectionnez Liste des emplacements préférés. Dans Emplacement préféré, saisissez un lieu, puis cliquez sur Ajouter. Ajoutez autant d'emplacements DNS que vous le souhaitez.
     - Pour configurer une action DNS de réécriture d'une réponse DNS sur la base de l'évaluation de la stratégie, sélectionnez Réécrire la réponse. Dans Adresse IP, saisissez une adresse IP, puis cliquez sur Ajouter. Ajoutez autant d'adresses IP que vous le souhaitez.
   - TTL (applicable uniquement au type d'action Réécrire la réponse)

Configurer les stratégies DNS

Les stratégies DNS fonctionnent sur une base de données d'emplacements qui utilise des adresses IP statiques et personnalisées. Les attributs de la demande DNS locale entrante sont définis dans le cadre d'une expression, et le site cible est défini dans le cadre d'une stratégie DNS. Lorsque vous définissez des actions et des expressions, vous pouvez utiliser une paire de guillemets simples (« ») comme qualificatif générique pour spécifier plusieurs emplacements. Lorsqu'une stratégie DNS est configurée et qu'une demande GSLB est reçue, la base de données d'adresses IP personnalisée est d'abord interrogée pour obtenir une entrée qui définit les attributs d'emplacement de la source :

- Lorsqu'une requête DNS provient d'un LDNS, les caractéristiques du LDNS sont évaluées par rapport aux stratégies configurées. Si elles correspondent, une action appropriée (affinité de site) est exécutée. Si les caractéristiques LDNS correspondent à plusieurs sites, la charge de la demande est équilibrée entre les sites qui correspondent aux caractéristiques LDNS.
- Si l'entrée est introuvable dans la base de données personnalisée, la base de données d'adresses IP statique est interrogée pour une entrée et, en cas de correspondance, l'évaluation de stratégie ci-dessus est répétée.
- Si l'entrée n'est pas trouvée dans les bases de données personnalisées ou statiques, le meilleur site est sélectionné et envoyé dans la réponse DNS sur la base de la méthode d'équilibrage de charge configurée.

Les restrictions suivantes s'appliquent aux stratégies DNS créées sur l'appliance Citrix ADC.

- 64 stratégies au maximum sont prises en charge.
- Les stratégies DNS sont globales pour l'appliance Citrix ADC et ne peuvent pas être appliquées à un serveur virtuel ou à un domaine spécifique.
- La liaison de stratégie spécifique au domaine ou au serveur virtuel n'est pas prise en charge.

Vous pouvez utiliser des stratégies DNS pour diriger les clients qui correspondent à une certaine plage d'adresses IP vers un site spécifique. Par exemple, si vous avez une configuration GSLB avec plusieurs sites GSLB séparés géographiquement, vous pouvez diriger tous les clients dont l'adresse IP se trouve dans une plage spécifique vers un centre de données particulier.

Le trafic DNS basé sur TCP et UDP peut être évalué. Les expressions de stratégie sont disponibles pour le trafic DNS basé sur UDP sur le serveur et pour le trafic DNS UDP et le trafic DNS TCP côté client. En outre, vous pouvez configurer des expressions pour évaluer les requêtes et les réponses qui impliquent uniquement les types de questions DNS (ou valeurs QTYPE) suivants :

- Une
- AAAA
- NS
- SRV
- PTR
- CNAME
- SOA
- MX
- ANY

Les codes de réponse suivants (valeurs RCODE) sont également pris en charge :

- NOERROR - Aucune erreur
- FORMERR - Erreur de format
- SERVFAIL - Défaillance du serveur

- NXDOMAIN - Domaine inexistant
- NOTIMP - Type de requête non implémenté
- REFUSÉ - Requête refusée

Vous pouvez configurer des expressions pour évaluer le trafic DNS. Une expression DNS commence par les préfixes DNS.REQ ou DNS.RES. Des fonctions sont disponibles pour évaluer le domaine interrogé, le type de requête et le protocole transporteur. Pour plus d'informations sur les expressions DNS, voir « Expressions pour évaluer un message DNS et identifier son protocole de transporteur » dans « Configuration et référence des stratégies ».

Pour ajouter une stratégie DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une stratégie DNS et vérifier la configuration :

```
add dns policy <name> <rule> <actionName>
show dns policy <name>
<!--NeedCopy-->
```

Exemple :

```
> add dns policy-GSLB-1 'CLIENT.UDP.DNS.DOMAIN.EQ("domainname")'
   my_dns_action
 Done
> show dns policy-GSLB-1
    Name: policy-GSLB-1
    Rule: CLIENT.UDP.DNS.DOMAIN.EQ("domainname")
    Action Name: my_dns_action
    Hits: 0
    Undef Hits: 0

 Done
<!--NeedCopy-->
```

Pour supprimer une stratégie DNS configurée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm dns policy <name>
<!--NeedCopy-->
```

Pour configurer une stratégie DNS à l'aide de l'utilitaire de configuration Citrix ADC

1. Accédez à Gestion du trafic > DNS > Stratégies et créez une stratégie DNS.
2. Dans la boîte de dialogue Créer une stratégie DNS ou Configurer une stratégie DNS, définissez les paramètres suivants :
   - Nom de la stratégie (ne peut pas être modifié pour une stratégie existante)
   - Action
   - Expression
     Pour spécifier une expression, procédez comme suit :
     a) Cliquez sur Ajouter, puis, dans la zone de liste déroulante qui apparaît, sélectionnez l'élément d'expression par lequel vous souhaitez commencer l'expression. Une deuxième liste apparaît. La liste contient un ensemble d'éléments d'expression que vous pouvez utiliser immédiatement après le premier élément d'expression.
     b) Dans la deuxième liste, sélectionnez l'élément d'expression souhaité, puis entrez un point.
     c) Après chaque sélection, si vous entrez une période, le prochain ensemble d'éléments d'expression valides apparaît dans une liste. Sélectionnez des éléments d'expression et remplissez les arguments des fonctions jusqu'à ce que vous obteniez l'expression souhaitée.
3. Cliquez sur Créer ou sur OK, puis cliquez sur Fermer.

Stratégies de liaison DNS

Les stratégies DNS sont liées globalement sur l'appliance Citrix ADC et sont disponibles pour tous les serveurs virtuels GSLB configurés. Même si les stratégies DNS sont globalement liées, l'exécution des stratégies peut être limitée à un serveur virtuel GSLB spécifique en spécifiant le domaine dans l'expression.

Remarque : Même si la commande bind dns global accepte REQ_OVERRIDE et RES_OVERRIDE comme points de liaison valides, ces points de liaison sont redondants, car les stratégies DNS ne peuvent être liées que globalement. Liez vos stratégies DNS uniquement aux points de liaison REQ_DEFAULT et RES_DEFAULT.

Pour lier une stratégie DNS globalement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une stratégie DNS globalement et vérifier la configuration :

```
bind dns global <policyName> <priority> [-gotoPriorityExpression <
    string>] [-type <type>]
show dns global -type <type>
<!--NeedCopy-->
```

Exemple :


```
bind dns global policy-GSLB-1 10 -gotoPriorityExpression END
 Done
show dns global -type REQ_DEFAULT
1)  Policy Name: policy-GSLB-1
    Priority: 10
    GotoPriorityExpression: END
 Done
<!--NeedCopy-->
```

Pour lier une stratégie DNS globalement à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > DNS > Stratégies.
2. Dans le volet d'informations, cliquez sur Liaisons globales.
3. Dans la boîte de dialogue Lier/délier les stratégies DNS à la stratégie globale, cliquez sur Insérer une stratégie.
4. Dans la colonne Nom de la stratégie, sélectionnez, dans la liste, la stratégie que vous souhaitez lier. Sinon, dans la liste, cliquez sur Nouvelle stratégie, puis créez une stratégie DNS en définissant des paramètres dans la boîte de dialogue Créer une stratégie DNS.
5. Pour modifier une stratégie déjà liée globalement, cliquez sur le nom de la stratégie, puis sur Modifier la stratégie. Ensuite, dans la boîte de dialogue Configurer la stratégie DNS, modifiez la stratégie, puis cliquez sur OK.
6. Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur Délier la stratégie.
7. Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
8. Pour régénérer les priorités affectées, cliquez sur Régénérer les priorités. Les valeurs de priorité sont modifiées pour commencer à 100, avec des incréments de 10, sans affecter l'ordre d'évaluation.
9. Cliquez sur OK.

Pour afficher les liaisons globales d'une stratégie DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show dns global
```

Pour afficher les liaisons globales d'une stratégie DNS à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **DNS** > **Stratégies**.
2. Dans le volet d'informations, cliquez sur **Liaisons globales**. Les liaisons globales de toutes les stratégies DNS apparaissent dans cette boîte de dialogue.

Ajout de vues DNS

Vous pouvez configurer des vues DNS pour identifier différents types de clients et fournir une adresse IP appropriée à un groupe de clients qui interrogent le même domaine GSLB. Les vues DNS sont configurées à l'aide de stratégies DNS qui sélectionnent les adresses IP renvoyées au client.

Par exemple, si vous avez configuré GSLB pour le domaine de votre entreprise et que le serveur est hébergé sur le réseau de votre entreprise, les clients qui demandent le domaine depuis le réseau interne de votre entreprise peuvent recevoir l'adresse IP interne du serveur au lieu de l'adresse IP publique. En revanche, les clients qui interrogent le DNS pour le domaine à partir d'Internet peuvent obtenir l'adresse IP publique du domaine.

Pour ajouter une vue DNS, vous lui attribuez un nom de 31 caractères maximum. Le premier caractère doit être un chiffre ou une lettre. Les caractères suivants sont également autorisés : @ _ -. (point) : (deux-points) # et espace (). Après avoir ajouté la vue, vous configurez une stratégie pour l'associer aux clients et à une partie du réseau, et vous liez la stratégie globalement. Pour configurer et lier une stratégie DNS, consultez **Gestion du trafic DNS local à l'aide de stratégies DNS**.

Pour ajouter une vue DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une vue DNS et vérifier la configuration :

```
add dns view <viewName>
show dns view <viewName>
<!--NeedCopy-->
```

Exemple :

```
add dns view PrivateSubnet
show dns view PrivateSubnet
<!--NeedCopy-->
```

Pour supprimer une vue DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm dns view <viewName>
<!--NeedCopy-->
```

Pour ajouter une vue DNS à l'aide de l'utilitaire de configuration

Accédez à Gestion du trafic > DNS > Vues et ajoutez une vue DNS.

Pour plus d'informations sur la création d'une stratégie DNS et sur la façon de lier des stratégies DNS globalement, voir **Gestion du trafic DNS local à l'aide de stratégies DNS**.

Configurer GSLB pour la proximité

August 20, 2021

Lorsque vous configurez GSLB pour la proximité, les demandes des clients sont transférées au centre de données le plus proche. Le principal avantage de la méthode GSLB basée sur la proximité est des temps de réponse plus rapides résultant de la sélection du datacenter disponible le plus proche. Un tel déploiement est essentiel pour les applications qui nécessitent un accès rapide à de grands volumes de données.

Vous pouvez configurer GSLB pour la proximité en fonction du temps aller-retour (RTT), de la proximité statique ou d'une combinaison des deux.

Configurer la méthode de temps aller-retour dynamique (RTT)

Le temps aller-retour dynamique (RTT) est une mesure du temps ou du retard dans le réseau entre le serveur DNS local du client et une ressource de données. Pour mesurer la RTT dynamique, l'appliance Citrix ADC sonde le serveur DNS local du client et recueille des informations de mesure RTT. L'appliance utilise ensuite cette mesure pour prendre sa décision d'équilibrage de charge. L'équilibrage global de la charge du serveur surveille l'état en temps réel du réseau et dirige dynamiquement la demande du client vers le centre de données avec la valeur RTT la plus faible

Pour configurer GSLB pour la proximité avec la méthode dynamique, vous devez d'abord configurer la configuration GSLB de base, puis configurer RTT dynamique.

Créez d'abord deux sites GSLB, locaux et distants. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB et liez les services au serveur virtuel. Créez ensuite des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB sur le site local. Enfin, créez un serveur virtuel d'équilibrage de charge avec la même adresse IP de serveur virtuel que le service GSLB.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Une fois que vous avez configuré une configuration GSLB de base, configurez la méthode RTT dynamique.

Pour plus d'informations sur la configuration du serveur virtuel GSLB pour utiliser la méthode RTT dynamique pour l'équilibrage de charge, voir Configuration du RTT dynamique.

Configurer la proximité statique

La méthode de proximité statique pour GSLB utilise une base de données de proximité statique basée sur l'adresse IP pour déterminer la proximité entre le serveur DNS local du client et les sites GSLB. L'appliance Citrix ADC répond avec l'adresse IP d'un site qui correspond le mieux aux critères de proximité.

Si plusieurs sites GSLB situés à des emplacements géographiques différents servent le même contenu, l'appliance Citrix ADC gère une base de données de plages d'adresses IP et utilise la base de données pour prendre des décisions concernant les sites GSLB vers lesquels diriger les demandes clients entrantes.

Pour configurer GSLB pour la proximité avec proximité statique, vous devez d'abord configurer la configuration GSLB de base, puis configurer la proximité statique.

Créez d'abord deux sites GSLB, locaux et distants. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB et liez les services au serveur virtuel. Créez ensuite des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB sur le site local. Enfin, créez un serveur virtuel d'équilibrage de charge avec la même adresse IP de serveur virtuel que le service GSLB.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Une fois que vous avez configuré une configuration GSLB de base, configurez la proximité statique.

Pour plus d'informations sur la configuration du serveur virtuel GSLB pour utiliser la proximité statique pour l'équilibrage de charge, reportez-vous à la section Configuration de la proximité statique.

Configurer la proximité statique et la RTT dynamique

Vous pouvez configurer le serveur virtuel GSLB pour utiliser une combinaison de proximité statique et de RTT dynamique lorsque vous avez des clients provenant d'un réseau interne comme une succursale. Vous pouvez configurer GSLB de telle sorte que les clients provenant de la succursale ou de tout autre réseau interne soient dirigés vers un site GSLB particulier géographiquement proche du réseau client. Pour toutes les autres demandes, vous pouvez utiliser RTT dynamique.

Créez d'abord deux sites GSLB, locaux et distants. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB et liez les services au serveur virtuel. Créez ensuite des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB sur le site local. Enfin, créez un serveur virtuel d'équilibrage de charge avec la même adresse IP de serveur virtuel que le service GSLB.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Une fois que vous avez configuré une configuration GSLB de base, configurez le serveur virtuel GSLB pour qu'il utilise la proximité statique pour tout le trafic provenant d'un réseau interne, puis utilisez RTT dynamique pour tout autre trafic.

Pour plus d'informations sur la configuration de la proximité statique, reportez-vous à la section Configuration de la proximité statique et pour plus d'informations sur la configuration du RTT dynamique, voir Configuration du RTT dynamique.

Protéger la configuration GSLB contre les défaillances

August 20, 2021

Vous pouvez protéger votre configuration GSLB contre les défaillances d'un site GSLB ou d'un serveur virtuel GSLB en configurant les éléments suivants :

- Un serveur virtuel GSLB de sauvegarde
- Une appliance Citrix ADC pour répondre avec plusieurs adresses IP
- Une adresse IP de sauvegarde pour un domaine GSLB

Vous pouvez également détourner le trafic excédentaire vers un serveur virtuel de sauvegarde à l'aide de spillover.

Configurer un serveur virtuel GSLB de sauvegarde

La configuration d'une entité de sauvegarde pour un serveur virtuel GSLB garantit que le trafic DNS vers un site n'est pas interrompu si le serveur virtuel GSLB tombe en panne. L'entité de sauvegarde peut être un autre serveur virtuel GSLB ou une adresse IP de sauvegarde. Avec une entité de sauvegarde configurée, si le serveur virtuel GSLB principal tombe en panne, l'entité de sauvegarde gère les demandes DNS. Pour spécifier ce qui doit se produire lorsque le serveur virtuel GSLB principal revient à nouveau, vous pouvez configurer l'entité de sauvegarde pour continuer à gérer le trafic jusqu'à ce que vous autorisiez manuellement le serveur virtuel principal à prendre le relais (à l'aide de l'option DisablePrimaryOnDown).

Remarque : Vous pouvez configurer une seule entité de sauvegarde comme sauvegarde pour plusieurs serveurs virtuels GSLB.

Pour configurer un serveur virtuel GSLB de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur virtuel GSLB en tant que serveur virtuel de sauvegarde et vérifier la configuration :


```
set gslb vserver <name> -backupVServer <name> [-disablePrimaryOnDown (
    ENABLED | DISABLED)]

show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2 -
    disablePrimaryOnDown ENABLED
show gslb vserver vserver-GSLB-1
<!--NeedCopy-->
```

Pour définir le serveur virtuel GSLB comme serveur virtuel de sauvegarde à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels**, puis double-cliquez sur le serveur virtuel GSLB.
2. Sélectionnez la section **Sauvegarde Virtual Server** et choisissez le serveur virtuel de sauvegarde.

Configurer une configuration GSLB pour répondre avec plusieurs adresses IP

Une réponse DNS typique contient l'adresse IP du service GSLB le plus performant. Toutefois, si vous activez plusieurs réponses IP (MIR), l'appliance Citrix ADC envoie le meilleur service GSLB en tant que premier enregistrement de la réponse et ajoute les services actifs restants en tant qu'enregistrements supplémentaires. Si MIR est désactivé (valeur par défaut), l'appliance Citrix ADC envoie le meilleur service en tant que seul enregistrement en réponse.

Pour configurer un serveur virtuel GSLB pour plusieurs réponses IP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur virtuel GSLB pour plusieurs réponses IP et vérifiez la configuration :

```
set gslb vserver<name> -MIR (ENABLED | DISABLED)
-  show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :


```
set gslb vserver vserver-GSLB-1 -MIR ENABLED
 show gslb vserver <vserverName>
<!--NeedCopy-->
```

Pour définir un serveur virtuel GSLB pour plusieurs réponses IP à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel GSLB pour lequel vous souhaitez configurer un serveur virtuel de sauvegarde (par exemple, vServer-GSLB-1).
2. Dans l'onglet **Avancé**, sous Lorsque ce serveur virtuel est « UP », activez la case à cocher Envoyer toutes les adresses IP de service « actives » en réponse (MIR), puis sélectionnez **OK**.

Configuration d'un serveur virtuel GSLB pour répondre avec un enregistrement d'adresse vide en cas de panne

Une réponse DNS peut contenir soit l'adresse IP du domaine demandé, soit une réponse indiquant que l'adresse IP du domaine n'est pas connue par le serveur DNS, auquel cas la requête est transmise à un autre serveur de noms. Ce sont les seules réponses possibles à une requête DNS.

Lorsqu'un serveur virtuel GSLB est désactivé ou dans un état DOWN, la réponse à une requête DNS pour le domaine GSLB lié à ce serveur virtuel contient les adresses IP de tous les services liés au serveur virtuel. Cependant, vous pouvez configurer le serveur virtuel GSLB pour, dans ce cas, envoyer une Empty Down Response (EDR). Lorsque cette option est définie, une réponse DNS d'un serveur virtuel GSLB qui est à l'état DOWN ne contient pas d'enregistrements d'adresse IP, mais le code de réponse réussit. Cela empêche les clients de tenter de se connecter à des sites GSLB qui sont en panne.

Remarque : Vous devez configurer ce paramètre pour chaque serveur virtuel auquel vous souhaitez qu'il s'applique.

Pour configurer un serveur virtuel GSLB pour les réponses vides à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb vserver<name> -EDR (ENABLED | DISABLED)
<!--NeedCopy-->
```

Exemple :

```
> set gslb vserver vserver-GSLB-1 -EDR ENABLED
```



```
2   Done
3 <!--NeedCopy-->
```

Pour définir un serveur virtuel GSLB pour les réponses vides à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel GSLB pour lequel vous souhaitez configurer un serveur virtuel de sauvegarde (par exemple, vServer-GSLB-1).
2. Dans l'onglet Avancé, sous Lorsque ce serveur virtuel est en panne, activez la case à cocher Ne pas envoyer d'adresse IP de service en réponse (EDR).
3. Cliquez sur **OK**.

Configurer une adresse IP de sauvegarde pour un domaine GSLB

Vous pouvez configurer un site de sauvegarde pour votre configuration GSLB. Lorsque cette configuration est en place, si tous les sites principaux tombent en panne, l'adresse IP du site de sauvegarde est fournie dans la réponse DNS.

En règle générale, si un serveur virtuel GSLB est actif, ce serveur virtuel envoie une réponse DNS avec l'une des adresses IP de site actives sélectionnées par la méthode GSLB configurée. Si tous les sites principaux configurés sur le serveur virtuel GSLB sont inactifs (à l'état DOWN), le serveur ADNS (Domain Name System) ou le serveur DNS autoritaire envoie une réponse DNS avec l'adresse IP du site de sauvegarde.

Remarque : Lorsqu'une adresse IP de sauvegarde est envoyée, la persistance n'est pas respectée.

Pour définir une adresse IP de sauvegarde pour un domaine à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir une adresse IP de sauvegarde et vérifier la configuration :

```
1 set gslb vserver <name> -domainName <string> -backupIP <IPAddress>
2 show gslb vserver <name>
3 <!--NeedCopy-->
```

Exemple :

```
1 set gslb vserver vserver-GSLB-1 -domainName www.abc.com -backupIP
     10.102.29.66
2 show gslb vserver vserver-GSLB-1
```



```
<!--NeedCopy-->
```

Pour définir une adresse IP de sauvegarde pour un domaine à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel GSLB auquel vous souhaitez lier le domaine de sauvegarde (par exemple, vServer-GSLB-1).
2. Cliquez sur la section **Domaines**, configurez le domaine GSLB et spécifiez l'adresse IP du domaine de sauvegarde dans le champ **IP de sauvegarde** .

Détourner le trafic excédentaire vers un serveur virtuel de sauvegarde

Une fois que le nombre de connexions à un serveur virtuel GSLB principal dépasse la valeur de seuil configurée, vous pouvez utiliser l'option de débordement pour détourner de nouvelles connexions vers un serveur virtuel GSLB de sauvegarde. Cette valeur de seuil peut être calculée dynamiquement ou définie manuellement. Une fois que le nombre de connexions au serveur virtuel principal tombe en dessous du seuil, le serveur virtuel GSLB principal reprend à traiter les demandes du client.

Vous pouvez configurer la persistance avec spillover. Lorsque la persistance est configurée, les nouveaux clients sont détournés vers le serveur virtuel de sauvegarde si ce client n'est pas déjà connecté à un serveur virtuel principal. Lorsque la persistance est configurée, les connexions qui ont été détournées vers le serveur virtuel de sauvegarde ne sont pas déplacées vers le serveur virtuel principal une fois que le nombre de connexions vers le serveur virtuel principal est inférieur au seuil. Au lieu de cela, le serveur virtuel de sauvegarde continue à traiter ces connexions jusqu'à ce qu'elles soient terminées par l'utilisateur. Pendant ce temps, le serveur virtuel principal accepte de nouveaux clients.

Le seuil peut être mesuré en fonction du nombre de connexions, de la bande passante et de l'état de santé des services.

Si le serveur virtuel de sauvegarde atteint le seuil configuré et ne parvient pas à prendre de charge supplémentaire, le serveur virtuel principal détourne toutes les demandes vers l'URL de redirection désignée. Si une URL de redirection n'est pas configurée sur le serveur virtuel principal, les requêtes suivantes sont supprimées.

La fonctionnalité de débordement empêche le service GSLB de sauvegarde à distance (site GSLB de sauvegarde) d'être inondé de demandes client lorsque le serveur virtuel GSLB principal échoue. Cela se produit lorsqu'un moniteur est lié à un service GSLB distant et que le service rencontre une défaillance qui provoque un état DOWN. Toutefois, le moniteur continue de maintenir l'état du service GSLB distant UP en raison de la fonctionnalité de débordement.

Dans le cadre de la résolution de ce problème, deux États sont maintenus pour un service GSLB, l'état primaire et l'état effectif. L'état principal est l'état du serveur virtuel principal et l'état effectif est l'état

cumulatif des serveurs virtuels (chaîne principale et chaîne de sauvegarde). L'état effectif est défini sur UP si l'un des serveurs virtuels de la chaîne de serveurs virtuels est UP. Un indicateur indiquant que le VIP principal a atteint le seuil est également fourni. Le seuil peut être mesuré en fonction du nombre de connexions ou de la bande passante.

Un service n'est pris en compte pour GSLB que si son état principal est UP. Le trafic est dirigé vers le service GSLB de sauvegarde uniquement lorsque tous les serveurs virtuels principaux sont DOWN. En règle générale, ces déploiements ne comportent qu'un seul service GSLB de sauvegarde.

L'ajout d'états primaires et effectifs à un service GSLB a les effets suivants :

- Lorsque la persistance de l'adresse IP source est configurée, le DNS local est dirigé vers le site précédemment sélectionné uniquement si le serveur virtuel principal sur le site sélectionné est UP et inférieur au seuil. La persistance peut être ignorée en mode Round Robin.
- Si la persistance basée sur les cookies est configurée, les requêtes client sont redirigées uniquement lorsque le serveur virtuel principal sur le site sélectionné est UP.
- Si le serveur virtuel principal a atteint sa saturation et que les VIP de sauvegarde sont absents ou inexistants, l'état effectif est défini sur DOWN.
- Si les moniteurs externes sont liés à un serveur virtuel HTTP-HTTPS, le moniteur décide de l'état principal.
- S'il n'y a pas de serveur virtuel de sauvegarde sur le serveur virtuel principal et que le serveur virtuel principal a atteint son seuil, l'état effectif est défini sur DOWN.

Pour configurer un serveur virtuel GSLB de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le serveur virtuel GSLB de sauvegarde et vérifier la configuration :

```
set gslb vserver <name> -soMethod <method> -soThreshold <threshold> -
    soPersistence ( \*\*ENABLED\*\* | \*\*DISABLED\*\* ) -
    soPersistenceTimeout <timeout>
show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -soMethod CONNECTION -soThreshold 1000
    -soPersistence ENABLED -soPersistenceTimeout 2
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```


Pour configurer un serveur virtuel GSLB de sauvegarde à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel que vous souhaitez configurer en tant que sauvegarde (par exemple, vServer-LB-1).
2. Cliquez sur la section **Spillover** et définissez les paramètres suivants :
   - Méthode— soMethod
   - Seuil — soThreshold
   - Délai d'expiration de la persistance (min) — soPersistenceTimeout
3. Sélectionnez l'option Persistance et cliquez sur **OK**.

Configurer GSLB pour la reprise après sinistre

August 20, 2021

La capacité de reprise après sinistre est essentielle, car les temps d'arrêt sont coûteux. Une appliance Citrix ADC configurée pour GSLB transfère le trafic vers le centre de données le moins chargé ou le centre de données le plus performant. Cette configuration, appelée configuration active-active, améliore non seulement les performances, mais assure également une reprise après sinistre immédiate en acheminant le trafic vers d'autres centres de données si un centre de données faisant partie de la configuration est en panne. Vous pouvez également configurer une configuration GSLB active en veille uniquement pour la reprise après sinistre.

Configurer GSLB pour la reprise après sinistre dans une configuration de centre de données en veille active

Une configuration classique de reprise après sinistre inclut un centre de données actif et un centre de données de secours. Le centre de données de secours est un site distant. Lorsqu'un basculement survient à la suite d'un événement de sinistre entraînant l'inactivité du centre de données actif principal, le centre de données de secours devient opérationnel.

La configuration de la reprise après sinistre dans une configuration de centre de données active de secours comprend les tâches suivantes.

- Créez le centre de données actif.
  - Ajouter un site GSLB local.
  - Ajoutez un vserver GSLB, qui représente le centre de données actif.
  - Liez le domaine au serveur virtuel GSLB.
  - Ajoutez des services gslb et liez les services au serveur virtuel GSLB actif.
- Créez le centre de données de secours.
  - Ajouter un site gslb distant.
  - Ajoutez un vserver gslb, qui représente un centre de données de secours.

- Ajoutez des services gslb qui représentent le centre de données de secours et liez les services au vserver gslb de secours.
- Désignez le centre de données de secours en configurant le serveur virtuel GSLB de secours comme serveur virtuel de sauvegarde pour le serveur virtuel GSLB actif.

Une fois que vous avez configuré le centre de données principal, répliquez la configuration du centre de données de sauvegarde et désignez-la comme site GSLB de secours en désignant un serveur virtuel GSLB sur ce site comme serveur virtuel de sauvegarde.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Pour désigner le site GSLB de secours à l'aide de l'interface de ligne de commande

Sur le site actif et sur le site distant, à l'invite de commandes, tapez :

```
set gslb vserver <name> -backupVserver <string>
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2
<!--NeedCopy-->
```

Pour configurer le site de secours à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Serveurs virtuels et double-cliquez sur le serveur virtuel GSLB pour le site principal.
2. Cliquez sur la section **Sauvegarder le serveur virtuel** et sélectionnez un serveur virtuel de sauvegarde.

Par défaut, une fois que le serveur virtuel principal devient actif, il commence à recevoir du trafic. Toutefois, si vous souhaitez que le trafic soit dirigé vers le serveur virtuel de sauvegarde même après que le serveur virtuel principal soit actif, utilisez l'option
« désactiver le serveur principal à l'inactivité ».

Configurer pour la reprise après sinistre dans un centre de données actif

Un déploiement GSLB actif, dans lequel les deux sites GSLB sont actifs, supprime tout risque pouvant survenir lors de la mise en place d'un centre de données de secours. Avec une telle configuration, le contenu Web ou d'application peut être mis en miroir dans des emplacements géographiquement distincts. Cela garantit que les données sont toujours disponibles dans chaque centre de données distribué.

Pour configurer GSLB pour la reprise après sinistre dans un centre de données actif configuré, vous devez d'abord configurer la configuration GSLB de base sur le premier centre de données, puis configurer tous les autres centres de données.

Créez d'abord au moins deux sites GSLB. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB et liez les services au serveur virtuel. Créez ensuite des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB dans le site local. Enfin, sur le site local, créez un serveur virtuel d'équilibrage de charge avec la même adresse IP de serveur virtuel que le service GSLB.

Une fois que vous avez configuré le premier centre de données, répliquez la configuration pour les autres centres de données partie de la configuration.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Configuration pour la reprise après sinistre avec Weighted Round Robin

Lorsque vous configurez GSLB pour utiliser la méthode de ronde pondérée, des pondérations sont ajoutées aux services GSLB et le pourcentage configuré du trafic entrant est envoyé à chaque site GSLB. Par exemple, vous pouvez configurer votre configuration GSLB pour transférer 80 % du trafic à un site et 20 % du trafic à un autre. Après cela, l'appliance Citrix ADC enverra quatre requêtes au premier site pour chaque demande qu'il envoie au second.

Pour configurer la méthode de round robin pondérée, créez d'abord deux sites GSLB, locaux et distants. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB, et liez les services au serveur virtuel. Configurez la méthode GSLB comme round robin. Ensuite, créez des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB. Enfin, créez un serveur virtuel d'équilibrage de charge avec la même adresse IP de serveur virtuel que le service GSLB.

Chaque service qui représente un serveur physique dans le réseau a des poids associés. Par conséquent, le service GSLB se voit attribuer une pondération dynamique qui est la somme des pondérations de tous les services qui lui sont liés. Le trafic est ensuite réparti entre les services GSLB en fonction du rapport entre la masse dynamique du service en question et la masse totale. Vous pouvez également configurer des pondérations individuelles pour chaque service GSLB au lieu de la pondération dynamique.

Si les services n'ont pas de poids associés, vous pouvez configurer le serveur virtuel GSLB pour qu'il utilise le nombre de services qui lui sont liés pour calculer la pondération dynamiquement.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Une fois que vous avez configuré une configuration GSLB de base, vous devez configurer la méthode pondérée de manière à ce que le trafic soit réparti entre les sites GSLB configurés en fonction des

pondérations configurées pour les services individuels.

Pour configurer un serveur virtuel pour affecter des pondérations aux services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes, selon que vous souhaitez créer un nouveau serveur virtuel d'équilibrage de charge ou en configurer un existant :

```
add lb vserver <name>@ -weight <WeightValue> <ServiceName>
set lb vserver <name>@ -weight <WeightValue> <ServiceName>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
set lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
<!--NeedCopy-->
```

Pour définir le poids dynamique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb vserver <name> -dynamicWeight DynamicWeightType
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -dynamicWeight ServiceWeight
<!--NeedCopy-->
```

Pour ajouter des pondérations aux services GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb vserver <name> -serviceName GSLBServiceName -weight
   WeightValue
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1 -weight 1
<!--NeedCopy-->
```


Pour configurer un serveur virtuel pour affecter des poids aux services à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de la charge > Serveurs virtuels et double-cliquez sur le serveur virtuel (par exemple, vServer-lb-1).
2. Cliquez sur la section Services et définissez le poids d'un service.

Pour ajouter des pondérations aux services GSLB à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Serveurs virtuels et double-cliquez sur le serveur virtuel (par exemple, vServer-GSLB-1)
2. Cliquez sur la section Services et définissez le poids du service dans le champ Poids.

Pour définir le poids dynamique à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Serveurs virtuels et double-cliquez sur le serveur virtuel (par exemple, vServer-GSLB-1).
2. Cliquez sur la section **Méthode** et, dans la liste déroulante **Poids dynamique**, sélectionnez **SERVICEWEIGHT**.

Configuration pour la reprise après sinistre avec la persistance du datacenter

La persistance du datacenter est requise pour les applications Web qui nécessitent le maintien d'une connexion avec le même serveur au lieu d'équilibrer la charge des requêtes. Par exemple, dans un portail de commerce électronique, il est essentiel de maintenir une connexion entre le client et le même serveur. Pour de telles applications, la persistance de redirection HTTP peut être configurée dans une configuration active.

Pour configurer GSLB pour la reprise après sinistre avec persistance du centre de données, vous devez d'abord configurer la configuration GSLB de base, puis configurer la persistance de redirection HTTP.

Créez d'abord deux sites GSLB, locaux et distants. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB et liez les services au serveur virtuel. Ensuite, créez des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB sur le site local. Ensuite, créez un serveur virtuel d'équilibrage de charge avec la même adresse IP de serveur virtuel que le service GSLB. Enfin, dupliquez les étapes précédentes pour la configuration à distance ou configurez l'appliance Citrix ADC pour synchroniser automatiquement votre configuration GSLB.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Une fois que vous avez configuré une configuration GSLB de base, configurez la priorité de redirection HTTP pour activer la persistance du centre de données.

Pour configurer la redirection HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la redirection HTTP et vérifier la configuration :

```
set gslb service <serviceName> -sitePersistence <sitePersistence> -
   sitePrefix <string>
show gslb service <serviceName>
<!--NeedCopy-->
```

Exemple :

```
set gslb service Service-GSLB-1 -sitePersistence HTTPRedirect -
   sitePrefix vserver-GSLB-1
show gslb service Service-GSLB-1
<!--NeedCopy-->
```

Pour configurer la redirection HTTP à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Services et double-cliquez sur le service GSLB à configurer.
2. Cliquez sur la section **Persistance du site**, sélectionnez l'option **HttpRedirect** et, dans la zone de texte **Prefix** du site, entrez le préfixe du site (par exemple, vServer-GSLB-1).

> **Remarque**
>
> Lorsque la persistance du site n'est pas configurée et si un serveur virtuel d'équilibrage de charge configuré en tant que service GSLB local est DOWN, les requêtes HTTP sont redirigées vers d'autres sites GSLB sains à l'aide d'une redirection 302.

Remplacer le comportement de proximité statique en configurant les emplacements préférés

August 20, 2021

Vous pouvez diriger le trafic d'un serveur DNS (LDNS) local ou d'un réseau vers un service GSLB autre que le service GSLB que la méthode de proximité statique sélectionne pour ce trafic. Autrement dit, vous avez un*emplacement*
privilégié pour ce trafic. Pour remplacer la méthode de proximité statique par des emplacements préférés, vous pouvez effectuer les opérations suivantes :

1. Configurez une action DNS qui consiste en une liste d'emplacements préférés. Pour plus d'informations sur la configuration d'une action DNS, voir Configuration d'une action DNS.

2. Configurez une stratégie DNS pour identifier le trafic en provenance du serveur ou du réseau LDNS pour lequel vous souhaitez remplacer la proximité statique, et appliquez l'action dans la stratégie.
3. Liez la stratégie au point de liaison de la demande globale.

Dans l'action DNS, vous pouvez configurer une liste de jusqu'à 8 emplacements préférés. Les emplacements doivent être fournis dans la notation de qualificatif pointillés, qui est la notation dans laquelle vous ajoutez des emplacements personnalisés à la base de données de proximité statique. Les emplacements peuvent inclure des caractères génériques pour les qualificatifs que vous souhaitez omettre. Pour plus d'informations sur la notation de qualificatif pointillé pour les emplacements, voir Ajout d'entrées personnalisées à une base de données de proximité statique. Lorsque vous saisissez les emplacements préférés, vous devez les saisir dans l'ordre décroissant de priorité.

Lorsqu'une stratégie est évaluée à
TRUE, l'appliance Citrix ADC correspond aux emplacements préférés, dans l'ordre de priorité, aux emplacements des services GSLB. Les correspondances sont des deux types suivants :

- Si tous les qualificatifs non génériques dans un emplacement préféré correspondent aux qualificatifs correspondants dans l'emplacement d'un service GSLB, la correspondance est considérée comme une correspondance parfaite. Par exemple, un emplacement de service GSLB de *.UK.*.* ou Europe.UK.*.* correspond parfaitement à l'emplacement préféré *.UK.*.*.
- Si seul un sous-ensemble des qualificatifs non génériques correspond, la correspondance est considérée comme une correspondance partielle. Par exemple, un emplacement de service GSLB d'Europe.eg est une correspondance partielle pour l'emplacement préféré Europe.UK.

Lorsqu'une stratégie DNS évalue la
valeur TRUE, l'algorithme suivant est utilisé pour sélectionner un service GSLB :

1. L'appliance évalue l'emplacement préféré qui a la priorité la plus élevée et descend l'ordre de priorité jusqu'à ce qu'une correspondance parfaite soit trouvée entre un emplacement préféré et l'emplacement d'un service GSLB.

   Si une correspondance parfaite est trouvée, l'appliance vérifie si le service GSLB correspondant est en service. S'il est actif, il renvoie l'adresse IP du service GSLB dans la réponse DNS. Si plusieurs correspondances parfaites sont trouvées (ce qui peut se produire lorsqu'un ou plusieurs caractères génériques sont utilisés dans un emplacement privilégié), l'appliance vérifie l'état de chacun des services GSLB correspondants et équilibre la charge des services GSLB qui sont en place.

2. Si aucune correspondance parfaite n'est trouvée pour l'un des emplacements préférés, l'appliance revient à l'emplacement préféré qui a la priorité la plus élevée et descend l'ordre de priorité jusqu'à ce qu'une correspondance partielle soit trouvée entre un emplacement préféré et l'emplacement d'un service GSLB.

   Si une correspondance partielle est trouvée, l'appliance vérifie si le service GSLB correspon-

dant est en service. S'il est actif, il renvoie l'adresse IP du service GSLB dans la réponse DNS. Si plusieurs correspondances partielles sont trouvées, l'appliance vérifie l'état de chacun des services GSLB correspondants et équilibre la charge des services GSLB qui sont en service.

3. Si aucune des correspondances parfaites et partielles n'est disponible, la charge de l'appliance équilibre tous les autres services GSLB disponibles.

   De cette manière, l'appliance implémente un type d'affinité de site pour le trafic correspondant à la stratégie DNS.

Exemple

Considérez une configuration GSLB comprenant les huit services GSLB suivants :

- Asia.IN
- Asia.jpn
- Asia.HK
- Europe.UK
- Europe.RU
- Europe.EG
- Africa.SD
- Africa.zmb

Considérez en outre l'action DNS et la configuration de stratégie suivantes :

```
1 > add dns action prefLoc11 GslbPrefLoc -preferredLocList "Asia.HK" "
     Europe.UK"
2  Done
3 > add dns policy dnsPolPrefLoc "CLIENT.IP.SRC.MATCHES_LOCATION("\*.ZMB
     .\*.*")" prefLoc11
4  Done
5 <!--NeedCopy-->
```

Lorsque l'appliance reçoit une demande de l'emplacement *.ZMB.*.*, les emplacements préférés sont évalués comme suit :

1. L'appliance tente de trouver un service GSLB dont l'emplacement correspond parfaitement à Asia.hk, qui est l'emplacement préféré qui a la priorité la plus élevée. Il trouve que le service GSLB à Asia.hk est un match parfait. Si le service GSLB est en service, il envoie au client l'adresse IP du service GSLB.
2. Si le service GSLB à Asia.hk est en panne, l'appareil tente de trouver une correspondance parfaite pour le deuxième emplacement préféré, Europe.UK. Il trouve que le service GSLB sur Europe.UK est une correspondance parfaite. Si le service GSLB est en service, il envoie au client l'adresse IP du service.

3. Si le service GSLB sur Europe.UK est en panne, il revient à l'emplacement préféré qui a la priorité la plus élevée, Asia.hk, et recherche des correspondances partielles. Pour Asia.hk, il trouve que Asia.in et Asia.jpn sont des correspondances partielles. Si un seul des services GSLB correspondants est actif, il envoie au client l'adresse IP du service. Si les deux emplacements sont actifs, la charge équilibre les deux services.
4. Si toutes les correspondances partielles pour Asia.hk sont en panne, l'appareil recherche des correspondances partielles pour Europe.UK. Il trouve que Europe.ru et Europe.eg sont des correspondances partielles pour l'emplacement préféré. Si un seul des services GSLB correspondants est actif, il envoie au client l'adresse IP du service. Si les deux emplacements sont actifs, la charge équilibre les deux services.
5. Si toutes les correspondances partielles pour Europe.UK sont en panne, la charge de l'appliance équilibre tous les autres services GSLB disponibles. Dans l'exemple actuel, la charge de l'appareil équilibre Africa.sd et Africa.zmb parce que les six autres services GSLB ont été trouvés en panne.

Configurer la sélection du service GSLB à l'aide du changement de contenu

August 20, 2021

Dans un déploiement GSLB typique, vous pouvez hiérarchiser la sélection d'un ensemble de services GSLB liés à un serveur virtuel GSLB, mais vous ne pouvez pas effectuer les opérations suivantes :

- Restreindre la sélection d'un service GSLB à partir d'un sous-ensemble de services GSLB liés à un serveur virtuel GSLB pour le domaine donné.
- Appliquez différentes méthodes d'équilibrage de charge sur les différents sous-ensembles de services GSLB dans le déploiement.
- Appliquez des stratégies de débordement sur un sous-ensemble de services GSLB et vous ne pouvez pas avoir de sauvegarde pour un sous-ensemble de services GSLB.
- Configurez un sous-ensemble de services GSLB pour servir un contenu différent. Autrement dit, vous ne pouvez pas basculer de contenu entre les serveurs de différents sites GSLB. La configuration GSLB suppose que les serveurs contiennent le même contenu.
- Définissez un service GSLB de sous-ensemble avec des priorités différentes et spécifiez un ordre dans lequel les services du sous-ensemble sont appliqués à une demande.

Vous pouvez maintenant configurer une stratégie de commutation de contenu (CS) pour personnaliser le déploiement GSLB. Configurez d'abord un ensemble de services GSLB et liez-le à un serveur virtuel GSLB. Ensuite, configurez un serveur virtuel CS de type cible GSLB, définissez une stratégie CS et une action avec le serveur virtuel GSLB comme serveur virtuel cible, et liez la stratégie CS au serveur virtuel CS.

> **Important**
>
> - Seules les stratégies CS avec des expressions basées sur DNS peuvent être liées à un serveur virtuel CS de type cible GSLB.
> - Si un service GLSB est lié à un serveur virtuel CS via un serveur virtuel GSLB, vous ne pouvez pas lier un autre serveur virtuel GSLB lié au même service GSLB au serveur virtuel CS.

Exemple

Considérez un déploiement GLSB qui comprend deux sites GSLB. Sur chaque site, quatre services GSLB (S-1, S-2, S-3 et S-4) sont liés au serveur virtuel GSLB VS-1. Vous pouvez configurer un serveur virtuel de commutation de contenu (CS) de type cible GSLB et définir une stratégie et une action CS avec VS-1 comme serveur virtuel cible, de sorte que les demandes de contenu en anglais ne soient traitées que par S-1 et S-2, et que les demandes de contenu dans la langue locale ne soient traitées que par S-3 et S-4.

Vous pouvez donner la priorité S-1 en configurant un serveur virtuel de sauvegarde sur VS-1 et en liant S-2 au serveur virtuel de sauvegarde. S-1 répond aux demandes du client. Si le serveur S-1 représente tombe en panne, S-2 sert les requêtes. Si S-1 et S-2 sont en panne, les clients reçoivent une réponse vide.

Pour configurer la sélection de service GSLB à l'aide de la commutation de contenu :

1. Configurez GSLB. Pour obtenir des instructions, voir Configuration de l'équilibrage de charge global du serveur.
2. Configurez un serveur virtuel CS (Content Switching) de type cible GSLB. Pour plus d'informations, voir Création de serveurs virtuels de commutation de contenu.
3. Configurer les stratégies CS (Content Switching). Pour plus d'informations, voir Configuration des stratégies de commutation de contenu.
4. Configurez les actions CS qui désignent un serveur virtuel GSLB comme serveur virtuel cible. Pour plus d'informations, voir Configuration d'une action de changement de contenu.
5. Liez les stratégies CS au serveur virtuel CS. Pour plus d'informations, voir Liaison de stratégies à un serveur virtuel de commutation de contenu.
6. Liez le domaine au serveur virtuel CS au lieu du serveur virtuel GSLB.

Exemple de configuration

L'exemple de configuration suivant envoie les demandes du client avec l'adresse IP 5.5.5.5 à SERVICE_GSLB1 et SERVICE_GSLB2. SERVICE_GSLB1 a une priorité plus élevée que SERVICE_GSLB2, et SERVICE_GSLB2 ne sert les demandes du client que lorsque SERVICE_GSLB1 est en panne. Si les deux SERVICE_GSLB1 et SERVICE_GSLB2 sont en panne, SERVICE_GSLB3 et Service-GSLB4 ne sont pas pris en compte et une réponse vide est envoyée au client.

```
1 add cs vs CSVSERVER_GSLB http -targettype GSLB
```



```
Done
add gslb vs VSERVER_GSLB1 http
Done
add gslb vs VSERVER_GSLB2 http
Done
add gslb vs VSERVER_GSLB_BACKUP1 http
Done
set gslb vs VSERVER_GSLB1 -backupvserver VSERVER_GSLB_BACKUP1
Done
add gslb service SERVICE_GSLB1 1.1.1.1 HTTP 80 -sitename site1
Done
add gslb service SERVICE_GSLB2 1.1.1.2 HTTP 80 -sitename site1
Done
add gslb service SERVICE_GSLB3 1.1.1.3 HTTP 80 -sitename site2
Done
add gslb service SERVICE_GSLB4 1.1.1.4 HTTP 80 -sitename site2
Done
bind gslb vs VSERVER_GSLB1 -servicename SERVICE_GSLB1
Done
bind gslb vs VSERVER_GSLB_BACKUP1 -servicename SERVICE_GSLB2
Done
bind gslb vs VSERVER_GSLB2 -servicename SERVICE_GSLB3
Done
bind gslb vs VSERVER_GSLB2 -servicename SERVICE_GSLB4
Done
add cs action a1 -targetvserver VSERVER_GSLB1
Done
add cs policy p1 -rule "CLIENT.IP.SRC.EQ(5.5.5.5)" -action a1
Done
bind cs vs CSVSERVER_GSLB -domainName www.abc.com
Done
bind cs vs CSVSERVER_GSLB -policyname p1 -priority 1
Done
add cs action a2 -targetvserver VSERVER_GSLB2
Done
add cs policy p2 -rule "CLIENT.IP.SRC.EQ(6.6.6.6)" -action a2
Done
bind cs vs CSVSERVER_GSLB -policyname p2 -priority 2
Done
<!--NeedCopy-->
```


Associer une expression de serveur virtuel cible à une action de commutation de contenu GSLB

Vous pouvez maintenant associer une expression de serveur virtuel cible à une action de commutation de contenu GSLB. Cela permet au serveur virtuel de commutation de contenu GSLB d'utiliser des expressions de stratégie pour composer le nom du serveur virtuel GSLB cible lors du traitement des demandes DNS.

Pour configurer une action de commutation de contenu qui spécifie une expression à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour configurer l'action de commutation de contenu afin de récupérer la réponse de légende HTTP.

```
1 add cs action <name> -targetVserverExpr <expression>
2 <!--NeedCopy-->
```

Exemple :

```
1 add cs action csact_GSLB_VServer -targetVserverExpr "SYS.HTTP_CALLOUT(
     GSLB_Method_API)"
2 <!--NeedCopy-->
```

Pour configurer une action de commutation de contenu qui spécifie une expression à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Actions**.
2. Configurez une action de commutation de contenu et spécifiez une **expression** qui calcule dynamiquement le nom du serveur virtuel d'équilibrage de charge cible.

Configurer GSLB pour les requêtes DNS avec les enregistrements NAPTR

August 20, 2021

Dans un déploiement GSLB (Global Server Load Balancing) typique, l'appliance Citrix ADC reçoit des requêtes DNS pour les enregistrements A/AAAA, sélectionne le service GSLB le plus approprié selon la méthode d'équilibrage de charge configurée et renvoie l'adresse IP du service en réponse à la requête DNS. Vous pouvez maintenant configurer l'appliance pour recevoir des requêtes DNS pour les enregistrements NAPTR et répondre avec la liste des services configurés pour un domaine. L'appliance

surveille également l'état des services et, dans la réponse, elle fournit une liste des services qui sont en service.

Exemple :

Dans les déploiements Telco, vous pouvez configurer une appliance Citrix ADC pour recevoir des requêtes DNS avec des enregistrements NAPTR de clients tels que des entités de gestion mobile (MME), qui jouent le rôle d'un résolveur DNS pour découvrir tous les services offerts par le nom de domaine. L'appliance répond à la requête avec des enregistrements NAPTR pour tous les services qui sont en service. Le MME peut utiliser cette réponse NAPTR pour exécuter la procédure S-NAPTR pour sélectionner les nœuds en fonction du service offert, de la colocation, de la proximité topologique, etc.

Si plusieurs nœuds peuvent être sélectionnés, le MME peut utiliser le champ de préférence de l'enregistrement NAPTR de l'appliance Citrix ADC pour déterminer le nœud.

Format d'enregistrement NAPTR

Lors de la réponse à une requête DNS avec enregistrement NAPTR, une appliance Citrix ADC construit un enregistrement NAPTR de réponse pour chaque service GSLB.

Le tableau suivant répertorie les fichiers de l'enregistrement NAPTR :

Champ	
Domaine	Le domaine GSLB
TTL	Durée pendant laquelle l'enregistrement NAPTR peut être mis en cache.
Classe	Classe de l'enregistrement. Par défaut, cette valeur est définie sur IN.
Type	Type d'enregistrement DNS.
Order	Spécifie l'ordre dans lequel l'enregistrement NAPTR DOIT être traité. Vous pouvez spécifier l'ordre dans le service GSLB. Sinon, il est défini sur 1.
Préférence	Spécifie l'ordre dans lequel les enregistrements NAPTR avec des valeurs « ordre » égales doivent être traités, les nombres faibles étant traités avant les nombres élevés. Si l'ordre n'est pas spécifié dans le service GSLB, il est défini sur 1.

Champ	
Indicateurs	Contrôle les aspects de la réécriture et de l'interprétation des champs de l'enregistrement. L'appliance Citrix ADC définit cette valeur à A.
Service	Spécifie le (s) service (s) disponible (s).
Expression régulière	Les expressions régulières ne sont pas prises en charge, donc cette valeur est définie sur NULL.
Remplacement	Nom de domaine du nœud qui héberge les services.

Procédure de configuration

Pour obtenir des instructions détaillées de configuration GSLB, reportez-vous à la section Configuration de l'équilibrage de charge globale du serveur (GSLB). Assurez-vous d'effectuer les opérations suivantes :

- Définissez les paramètres suivants lors de l'ajout du serveur virtuel GSLB :
  - serviceType: ANY
  - dnsRecordType: NAPTR
  - lbMethod: CUSTOMLOAD

Exemple :

```
1 add gslb vserver gslb_vs ANY -dnsRecordType NAPTR -lbMethod CUSTOMLOAD
2 <!--NeedCopy-->
```

- Lors de l'ajout d'un site GSLB, définissez le paramètre *NaptrReplacementSuffix* sur le nom de domaine que vous souhaitez intégrer dans les enregistrements NAPTR.

Exemple :

```
1 add gslb site site1 10.102.218.200  -naptrReplacementSuffix example.com
2 <!--NeedCopy-->
```

- Définissez les paramètres suivants lors de l'ajout du service GSLB :
  - naptrreplacement
  - naptrOrder
  - naptrServices
  - naptrDomainTTL

- naptrPreference

Exemple de configuration

```
add gslb vserver gslb_vs ANY -dnsRecordType NAPTR -lbMethod CUSTOMLOAD

Done

add gslb site site1 10.102.218.200  -naptrReplacementSuffix example.com

Done

add gslb service sgw1 3.3.3.13 ANY *  -siteName site1 -naptrreplacement
    sgw1.site1. -naptrOrder 2 -naptrServices x-3gpp-sgw:x-s5-gtp -
   naptrDomainTTL 20 -naptrPreference   200

Done

add gslb service sgw2 3.3.3.11 ANY *  -siteName site1 -naptrreplacement
    sgw2.site1. -naptrOrder 5 -naptrServices x-3gpp-sgw:x-s5-gtp  -
   naptrDomainTTL 20  naptrPreference  100

Done

add gslb service sgw3 3.3.3.12 ANY *  -siteName site2 -naptrreplacement
    sgw3.site1. -naptrOrder 10 -naptrServices x-3gpp-sgw:x-s5-gtp  -
   naptrDomainTTL 20 naptrPreference   300

bind gslb vserver gslb_vs -serviceName sgw1

Done

bind gslb vserver gslb_vs -serviceName sgw2

Done

bind gslb vserver gslb_vs -serviceName sgw3

Done

bind gslb service sgw1 -monitorName ping

Done

```



```
bind gslb service sgw2 -monitorName ping

Done

bind gslb service sgw3 -monitorName ping

Done

bind gslb vserver gslb_vs -domainName gslb.com -TTL 5

Done
<!--NeedCopy-->
```

> **Remarque**
>
> Les requêtes DNS avec enregistrements NAPTR ne sont pas prises en charge dans la configuration parent-enfant.

Configurer GSLB pour le domaine générique

August 20, 2021

Vous pouvez lier un domaine DNS générique à un serveur virtuel GSLB. Les utilisateurs accédant aux applications derrière un domaine générique sont routés vers le meilleur centre de données optimal, qui héberge ces applications. Le domaine générique gère les demandes de domaines et de sous-domaines inexistants. Pour plus d'informations sur les domaines génériques, voir Prise en charge des domaines DNS génériques.

Pour configurer GSLB pour un domaine générique, vous devez d'abord configurer la configuration GSLB de base. Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Pour configurer une configuration GSLB pour le domaine générique à l'aide de l'interface de ligne de commande

Effectuez les étapes suivantes pour configurer une configuration GSLB pour le domaine générique :

1. Créez les sites GSLB.

```
add gslb site site1 10.0.1.10
add gslb site site2 20.0.1.10
<!--NeedCopy-->
```


2. Ajoutez les services GSLB pour chaque site participant à la configuration GSLB.

```
add gslb service svc1 -sitename site1 10.0.1.10  http 80
add gslb service svc2 -sitename site1 10.0.1.10  http 80
add gslb service svc3 -sitename site2 20.0.1.10  http 80
add gslb service svc4 -sitename site2 20.0.1.10  http 80
<!--NeedCopy-->
```

3. Ajoutez le serveur virtuel GSLB qui fait référence à un service utilisé dans la configuration GSLB.

```
add gslb vserver gslb_vs http
<!--NeedCopy-->
```

4. Ajoutez un service ADNS qui écoute les requêtes DNS.

```
add service adns_udp 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

5. Liez les services GSLB au serveur virtuel GSLB.

```
bind gslb vserver gslb_vs -service svc1
bind gslb vserver gslb_vs -service svc2
bind gslb vserver gslb_vs -service svc3
bind gslb vserver gslb_vs -service svc4
<!--NeedCopy-->
```

6. Créez une zone.

```
add dns soaRec test.com -originServer n1.test.com -contact n1.test
    .com
add dns nsrec test.com n1.test.com
add dns nsrec test.com n2.test.com
add dns zone test.com -proxymode no
<!--NeedCopy-->
```

7. Liez le nom de domaine au serveur virtuel GSLB.

```
bind gslb vserver gslb_vs -domainName *.test.com
<!--NeedCopy-->
```


Utiliser l'option de sous-réseau client EDNS0 pour l'équilibrage de charge global du serveur

January 21, 2021

EDNS Client Subnet (ECS) est une extension d'en-tête DNS (Domain Name Server) qui fournit les détails du sous-réseau client. Vous pouvez utiliser ces détails pour améliorer la précision de Citrix ADC Global Server Load Balancing (GSLB) en utilisant l'emplacement réseau du client plutôt que l'emplacement du résolveur DNS pour déterminer la proximité topologique du client.

> **Remarque**
>
> Citrix ADC prend uniquement en charge EDNS0.

Important :

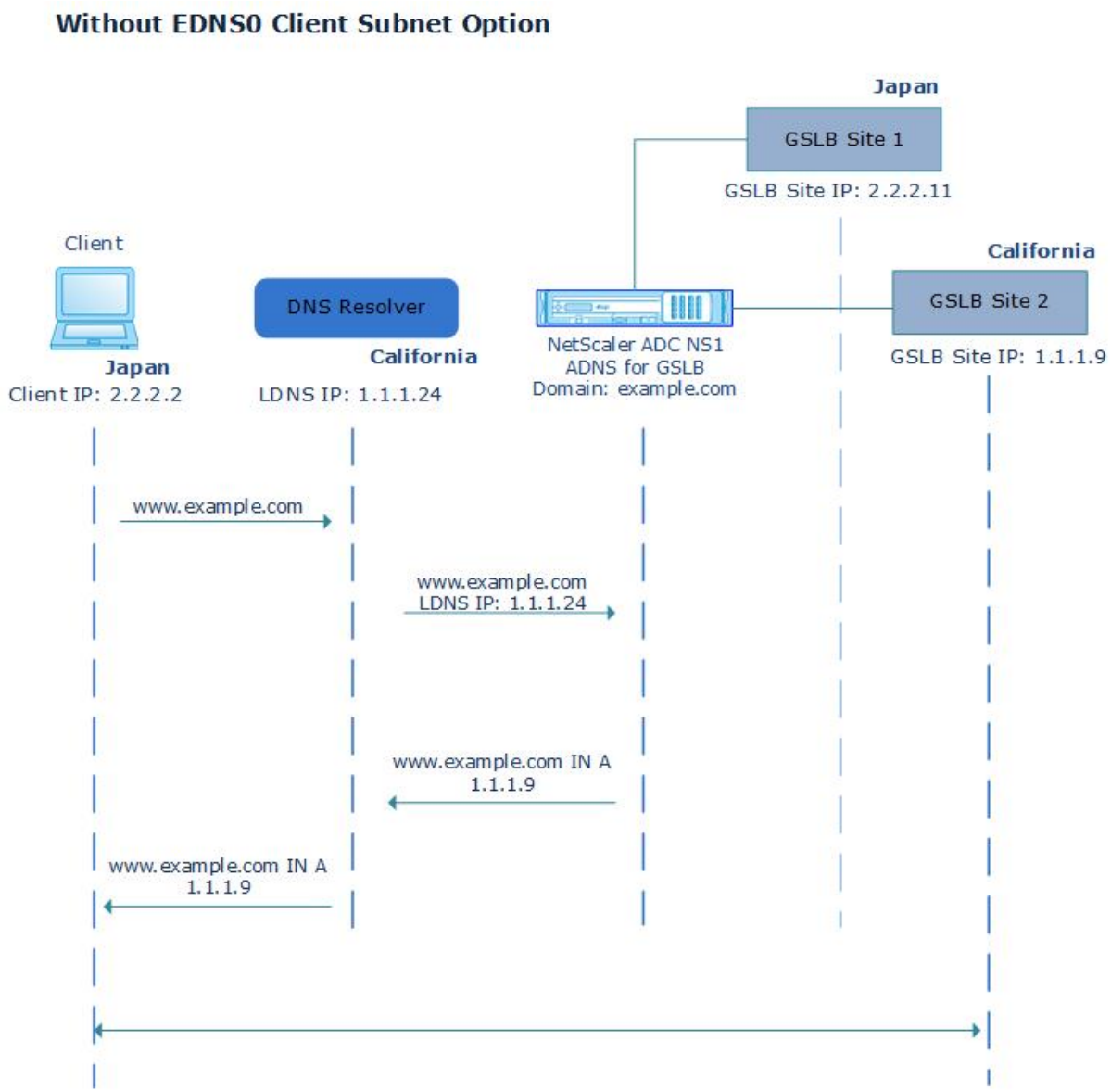
> Assurez-vous que le serveur LDNS (Local Domain Name Server) de votre déploiement prend en charge le sous-réseau client EDNS0 afin que les requêtes DNS entrantes contiennent l'option de sous-réseau client EDNS0 et que l'appliance Citrix ADC utilise l'adresse ECS lors du traitement de la requête DNS.

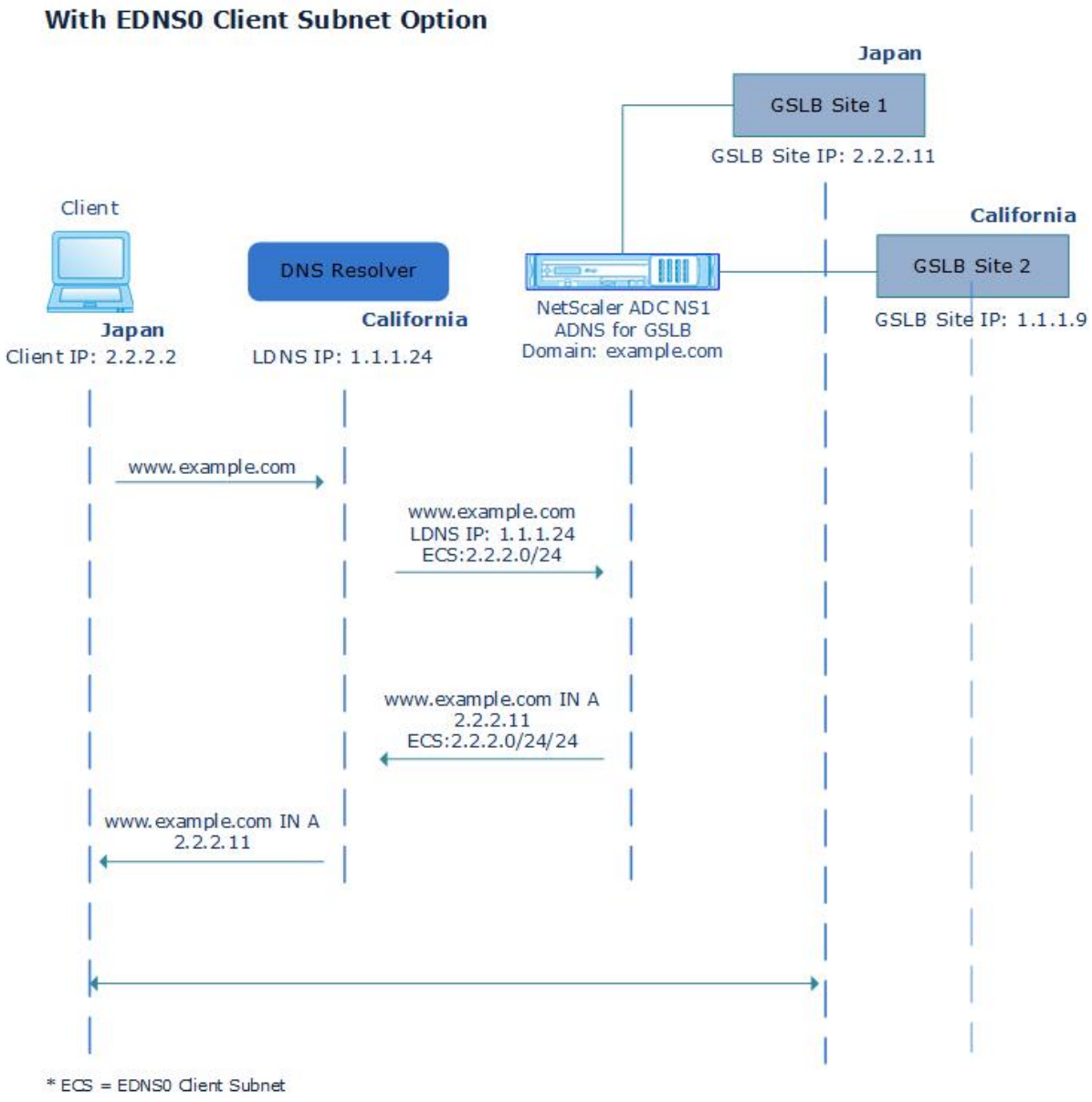
L'appliance Citrix ADC utilise l'adresse IP LDNS pour déterminer la proximité topologique du client et exécute GSLB si, lorsque vous utilisez des méthodes d'équilibrage de charge basées sur la proximité, telles que la proximité statique ou le temps d'aller-retour dynamique (RTT). Cela se produit dans un déploiement GSLB typique. Toutefois, lorsqu'un résolveur DNS centralisé, tel que Google DNS ou OpenDNS, est impliqué dans le déploiement, l'appliance Citrix ADC envoie la demande DNS à un centre de données proche du résolveur DNS centralisé, qui peut ne pas être proche du client. Par exemple, dans un déploiement GSLB Citrix ADC typique utilisant la méthode d'équilibrage de charge de proximité statique, une demande d'utilisateur final provenant du Japon est envoyée à un centre de données au Japon et une demande d'utilisateur final provenant de la Californie est envoyée à un centre de données en Californie. Toutefois, si un résolveur DNS centralisé est impliqué, l'appliance Citrix ADC peut envoyer une demande depuis le Japon à un centre de données en Californie.

Vous pouvez utiliser l'option ECS dans les déploiements qui incluent l'appliance Citrix ADC configurée en tant que serveur DNS (ADNS) faisant autorité pour un domaine GSLB. Si vous utilisez la proximité statique comme méthode d'équilibrage de charge, vous pouvez utiliser le sous-réseau IP dans l'en-tête EDNS au lieu de l'adresse IP LDNS. Cela permet de déterminer la proximité géographique du client. En mode proxy, l'appliance Citrix ADC transfère une requête DNS compatible ECS telle quelle aux serveurs principaux. L'appliance ne met pas en cache les réponses DNS compatibles ECS.

> **Remarque**
>
> L'option ECS n'est pas applicable à tous les autres modes de déploiement, tels que le mode ADNS

> pour les domaines non GSLB, le mode de résolution et le mode de redirection. L'option ECS est ignorée par l'appliance Citrix ADC dans les modes mentionnés ci-dessus. En outre, par défaut, ECS est désactivé pour le déploiement GSLB.





Pour activer l'option de sous-réseau client EDNS0 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
set gslb vserver <vserver_name> **-ECS ENABLED

set gslb vserver vserver-GSLB-1 -ECS ENABLED
<!--NeedCopy-->
```


Validation d'adresse

Vous pouvez configurer un serveur virtuel GSLB pour vérifier que l'adresse renvoyée par l'option EDNS0 Client Subnet (ECS) de la requête DNS n'est pas une adresse IP privée ou non routable. Lorsque la validation d'adresse est activée, l'appliance Citrix ADC ignore l'adresse ECS dans la requête DNS si elle est répertoriée dans le tableau suivant, et utilise plutôt l'adresse IP LDNS pour l'équilibrage global de la charge du serveur.

> **Remarque**
>
> Par défaut, la validation d'adresse est désactivée.

Type d'adresse	Adresse	Description
IPV4	10.0.0.0/8	Pour un usage privé
	172.16.0.0/12	Pour un usage privé
	192.168.0.0/16	Pour un usage privé
	0.0.0.0/8	Fait référence à l'hôte sur le réseau
	100.64.0.0/10	Espace d'adressage partagé
	127.0.0.0/8	Adresse de bouclage
	169.254.0.0/16	Lien adresse IPv4 locale telle que définie dans la RFC 3927
	192.0.0.0/24	Utilisé pour les affectations de protocole IETF, comprend l'espace privé 192.168.0.0/16
	192.0.2.0/24	Utilisé à des fins de documentation
	192.88.99.0/24	Utilisé pour 6to4 Relay Anycast
	198.18.0.0/15	Utilisé dans les tests de benchmark de l'appareil
	198.51.100.0/24	Utilisé à des fins de documentation
	203.0.113.0/24	Utilisé à des fins de documentation
	240.0.0.0/4	Utilisé comme réservé
	255.255.255.255/32	Utilisé pour la diffusion

Type d'adresse	Adresse	Description
IPv6	::1/128	adresse de bouclage
	::/128	adresse non spécifiée
	::ffff:0:0/96	Adresse mappée IPv4
	100::/64	Bloc d'adresse ignoré uniquement
	2001::/23	Utilisé pour les affectations de protocoles IETF
	2001::/32	TEREDO
	2001:2::/48	Utilisé pour l'analyse comparative
	2001:db8::/32	Utilisé à des fins de documentation
	2001:10::/28	ORCHID
	2002::/16	Utilisé pour 6to4 Relay Anycast
	fc00::/7	Unique-local
	fe80::/10	Adresses monodiffusion locales de liaison

Pour activer la validation d'adresse à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

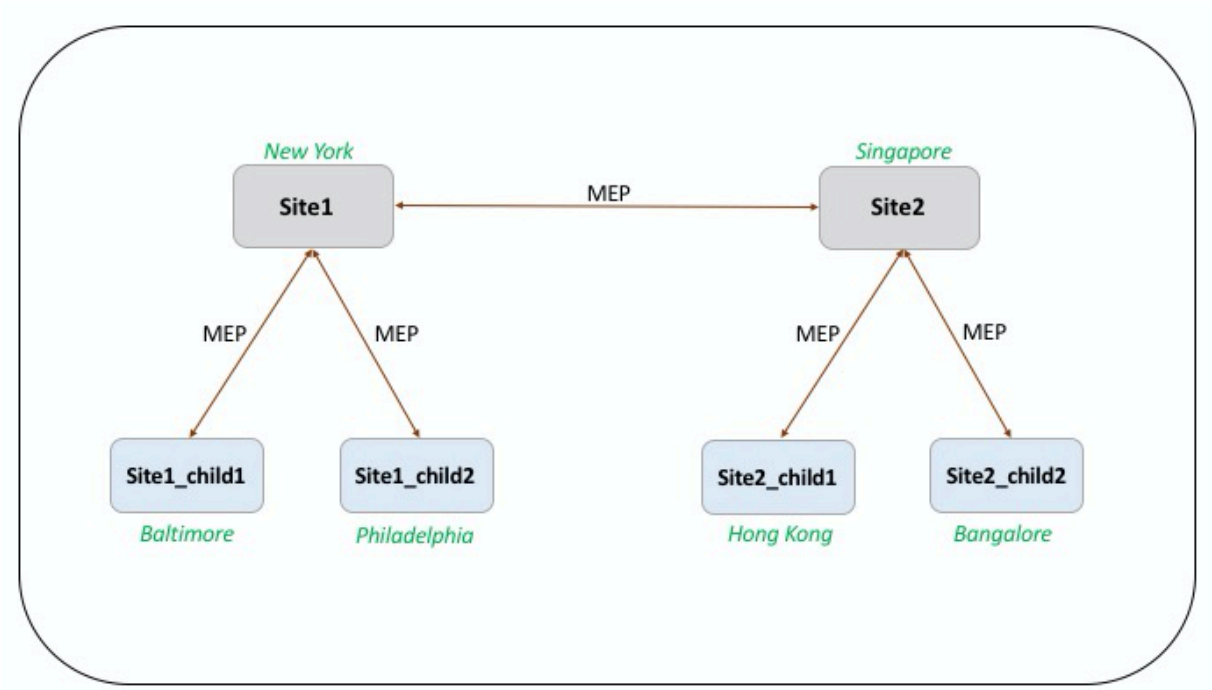
```
set gslb vserver <vserver_name> -ecsAddrValidation ENABLED

set gslb vserver vserver-GSLB-1 -ecsAddrValidation ENABLED
<!--NeedCopy-->
```


Exemple de configuration parent-enfant complète à l'aide du protocole d'échange de mesures

August 20, 2021

Considérons la topologie parent-enfant suivante dans laquelle les sites GSLB sont distribués globalement.

- Site1 et Site2 sont les sites parents.
- Site1_child1 et Site1_child2 sont les sites enfants de Site1.
- Site2_child1 et Site2_child2 sont les sites enfants de Site2.



Les commandes suivantes illustrent la configuration complète de la topologie parent-enfant.

site1

```
1 add gslb site site1 10.102.82.164 -publicIP 10.102.82.164
2
3 add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
4
5 add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1
6
```



```
7  add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site1
8
9  add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
10
11 add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
12
13 add gslb service site1_child1_http_gsvc1 10.102.82.132 HTTP 80 -
       publicIP 10.102.82.132 -publicPort 80 -maxClient 0 -siteName
       site1_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
14
15 add gslb service site1_child2_http_gsvc1 10.102.82.68 HTTP 80 -publicIP
        10.102.82.68 -publicPort 80 -maxClient 0 -siteName site1_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
16
17 add gslb service site2_child1_http_gsvc1 10.106.24.134 HTTP 80 -
       publicIP 10.106.24.134 -publicPort 80 -maxClient 0 -siteName
       site2_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
18
19 add gslb service site2_child2_http_gsvc1 10.106.24.68 HTTP 80 -publicIP
        10.106.24.68 -publicPort 80 -maxClient 0 -siteName site2_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
20
21 add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0 -
       appflowLog DISABLED
22
23 bind gslb vserver gv1 -serviceName site1_child1_http_gsvc1
24
25 bind gslb vserver gv1 -serviceName site1_child2_http_gsvc1
26
27 bind gslb vserver gv1 -serviceName site2_child2_http_gsvc1
28
29 bind gslb vserver gv1 -serviceName site2_child1_http_gsvc1
30
31 bind gslb vserver gv1 -domainName www.gslb.com -TTL 5
32 <!--NeedCopy-->
```

site1_child1


```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1
<!--NeedCopy-->
```

Vous pouvez ajouter les commandes suivantes pour la configuration de l'équilibrage de charge :

```
add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.102.82.132 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
<!--NeedCopy-->
```

site1_child2

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

You can add the following commands for load balancing configuration:

add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.102.82.68 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
<!--NeedCopy-->
```

site2

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164
```



```
2
3  add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
4
5  add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site1
6
7  add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site1
8
9  add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
10
11 add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
12
13 add gslb service site1_child1_http_gsvc1 10.102.82.132 HTTP 80 -
       publicIP 10.102.82.132 -publicPort 80 -maxClient 0 -siteName
       site1_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
14
15 add gslb service site1_child2_http_gsvc1 10.102.82.68 HTTP 80 -publicIP
        10.102.82.68 -publicPort 80 -maxClient 0 -siteName site1_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
16
17 add gslb service site2_child1_http_gsvc1 10.106.24.134 HTTP 80 -
       publicIP 10.106.24.134 -publicPort 80 -maxClient 0 -siteName
       site2_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
18
19 add gslb service site2_child2_http_gsvc1 10.106.24.68 HTTP 80 -publicIP
        10.106.24.68 -publicPort 80 -maxClient 0 -siteName site2_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
20
21 add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0 -
       appflowLog DISABLED
22
23 bind gslb vserver gv1 -serviceName site1_child1_http_gsvc1
24
25 bind gslb vserver gv1 -serviceName site1_child2_http_gsvc1
26
27 bind gslb vserver gv1 -serviceName site2_child2_http_gsvc1
28
29 bind gslb vserver gv1 -serviceName site2_child1_http_gsvc1
```



```
30
31 bind gslb vserver gv1 -domainName www.gslb.com -TTL 5
32 <!--NeedCopy-->
```

site2_child1

```
1 add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
2
3 add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
     nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
     site2
4 <!--NeedCopy-->
```

You can add the following commands for load balancing configuration:

```
1 add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
      -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
     svrTimeout 360 -CKA NO -TCPB NO -CMP NO
2
3 add lb vserver lb1 HTTP 10.106.24.134 80 -persistenceType NONE -
     cltTimeout 180
4
5 bind lb vserver lb1 svc1
6 <!--NeedCopy-->
```

site2_child2

```
1 add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
2
3 add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
     nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
     site2
4 <!--NeedCopy-->
```

You can add the following commands for load balancing configuration:

```
1 add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
      -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
     svrTimeout 360 -CKA NO -TCPB NO -CMP NO
2
3 add lb vserver lb1 HTTP 10.106.24.68 80 -persistenceType NONE -
     cltTimeout 180
```



```
4
5 bind lb vserver lb1 svc1
6 \`\`\`
7 <!--NeedCopy-->
```

Équilibrage de charge de liaison

January 21, 2021

L'équilibrage de charge de liaison (LLB) équilibre le trafic sortant sur plusieurs connexions Internet fournies par différents fournisseurs de services. LLB permet à l'appliance Citrix ADC de surveiller et de contrôler le trafic afin que les paquets soient transmis de manière transparente via la meilleure liaison possible. Contrairement à l'équilibrage de charge du serveur, où un service représente un serveur, avec LLB, un service représente un routeur ou le saut suivant. Un lien est une connexion entre l'appliance Citrix ADC et le routeur.

Pour configurer l'équilibrage de charge de liaison, de nombreux utilisateurs commencent par configurer une configuration de base avec des paramètres par défaut. Une configuration de base implique des services, des serveurs virtuels, des moniteurs, des itinéraires, une méthode LLB et la persistance (facultatif). Une fois qu'une configuration de base est opérationnelle, vous pouvez la personnaliser pour votre environnement.

Les méthodes d'équilibrage de charge applicables à LLB sont le « round robin », le hachage IP de destination, le moins de bande passante et le moins de paquets. Vous pouvez éventuellement configurer la persistance pour que les connexions soient maintenues sur un lien spécifique. Les types de persistance disponibles sont basés sur l'adresse IP source, l'adresse IP de destination et l'adresse IP source et l'adresse IP de destination. PING est le moniteur par défaut, mais il est recommandé de configurer un moniteur transparent.

Vous pouvez personnaliser votre configuration en configurant le NAT inverse (RNAT) et les liens de sauvegarde.

Configuration d'une configuration LLB de base

August 20, 2021

Pour configurer LLB, vous devez d'abord créer des services représentant chaque routeur auprès des fournisseurs de services Internet (FAI). Un moniteur PING est lié par défaut à chaque service. La liaison d'un moniteur transparent est facultative mais recommandée. Ensuite, vous créez un serveur virtuel,

liez les services au serveur virtuel et configurez une route pour le serveur virtuel. L'itinéraire identifie le serveur virtuel comme Gateway vers les routeurs physiques représentés par les services. Le serveur virtuel sélectionne un routeur à l'aide de la méthode d'équilibrage de charge que vous spécifiez. Vous pouvez également configurer la persistance pour vous assurer que tout le trafic d'une session particulière est envoyé via un lien spécifique.

Pour configurer une configuration LLB de base, procédez comme suit :

- Configurer les services
- Configurer un serveur virtuel LLB et lier un service
- Configurer la méthode LLB et la persistance
- Configurer une route LLB
- Créer et lier un moniteur transparent

Configurer les services

Un moniteur par défaut (PING) est automatiquement lié à un type de service ANY lors de la création du service, mais vous pouvez remplacer le moniteur par défaut par un moniteur transparent, comme décrit dans Création et liaison d'un moniteur transparent.

Pour créer un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <name> <IP> <serviceType> <port>

show service <name>
<!--NeedCopy-->
```

Exemple :

```
add service ISP1R_svc_any 10.10.10.254 any *
show service ISP1R_svc_any
        ISP1R_svc_any (10.10.10.254:*) - ANY
        State: DOWN
        Last state change was at Tue Aug 31 04:31:13 2010
        Time since last state change: 2 days, 05:34:18.600
        Server Name: 10.10.10.254
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
```



```
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 244705  Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.322 millisec
 Done
<!--NeedCopy-->
```

Pour créer des services à l'aide de l'utilitaire de configuration

Accédez à Gestion du trafic > Équilibrage de charge > Serviceset créez un service.

Pour créer des services à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un service, spécifiez les valeurs des paramètres suivants :
   - Nom du service* : nom
   - Serveur—IP
   - Protocol* : ServiceType (sélectionnez ANY dans la liste déroulante).
   - Port* : port

Un paramètre obligatoire

1. Cliquez sur Créer.
2. Répétez les étapes 2 à 4 pour créer un autre service.
3. Cliquez sur Fermer.
4. Dans le volet Services, sélectionnez les services que vous venez de configurer et vérifiez que les paramètres affichés en bas de l'écran sont corrects.

Configurer un serveur virtuel LLB et lier un service

Après avoir créé un service, créez un serveur virtuel et liez des services au serveur virtuel. La méthode LB par défaut des connexions minimales n'est pas prise en charge dans LLB. Pour plus d'informations sur la modification de la méthode LB, voir Configuration de la méthode LLB et de la persistance.

Pour créer un serveur virtuel d'équilibrage de charge de liaison et lier un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb vserver <name> <serviceType>

bind lb vserver < name> <serviceName>

show lb vserver < name>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver LLB-vip any
bind lb vserver LLB-vip ISP1R_svc_any
sh lb vserver LLB-vip
        LLB-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: DOWN
        Last state change was at Thu Sep  2 10:51:32 2010
        Time since last state change: 0 days, 17:51:46.770
        Effective State: DOWN
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: ROUNDROBIN
        Mode: IP
        Persistence: NONE
        Connection Failover: DISABLED

1) ISP1R_svc_any (10.10.10.254: *) - ANY State: DOWN    Weight: 1
 Done
<!--NeedCopy-->
```


Pour créer un serveur virtuel d'équilibrage de charge de liaison et lier un service à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**et créez un serveur virtuel pour l'équilibrage de charge des liens. Spécifiez **ANY** dans le champ **Protocole**.
2. Dans la liste déroulante **Type d'adresse IP**, sélectionnez l'option souhaitée. Sélectionnez **Non adressable** pour créer un serveur virtuel qui n'est pas directement accessible.
3. Sous l'onglet **Services**, dans la colonne **Actif**, activez la case à cocher du service que vous souhaitez lier au serveur virtuel.

Configurer la méthode LLB et la persistance

Par défaut, l'appliance Citrix ADC utilise la méthode de connexion minimale pour sélectionner le service permettant de rediriger chaque requête client, mais vous devez définir la méthode LLB sur l'une des méthodes prises en charge. Vous pouvez également configurer la persistance, de sorte que différentes transmissions du même client soient dirigées vers le même serveur.

Pour configurer la méthode LLB et/ou la persistance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set lb vserver <name> -lbMethod <lbMethod> -persistenceType <
   persistenceType>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver LLB-vip -lbmethod ROUNDROBIN -persistencetype SOURCEIP

show lb vserver LLB-vip
        LLB-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: DOWN
        Last state change was at Fri Sep  3 04:46:48 2010
        Time since last state change: 0 days, 00:52:21.200
        Effective State: DOWN
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: ROUNDROBIN
```



```
14          Mode: IP
15          Persistence: SOURCEIP
16       Persistence Mask: 255.255.255.255       Persistence v6MaskLength:
            128   Persistence Timeout: 2 min
17          Connection Failover: DISABLED
18 <!--NeedCopy-->
```

Pour configurer la méthode d'équilibrage de charge de liaison et/ou la persistance à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels et sélectionnez le serveur virtuel pour lequel vous souhaitez configurer la méthode d'équilibrage de charge et/ou les paramètres de persistance.
2. Dans la section **Paramètres avancés**, sélectionnez Méthode et configurez la méthode d'équilibrage de charge.
3. Dans la section **Paramètres avancés**, sélectionnez **Persistance** et configurez les paramètres de persistance.

Configurer une route LLB

Après avoir configuré les services IPv4 ou IPv6, les serveurs virtuels, les méthodes LLB et la persistance, vous configurez une route LLB IPv4 ou IPv6 pour le réseau spécifiant le serveur virtuel LLB comme Gateway. Un itinéraire est un ensemble de liens qui sont équilibrés de charge. Les demandes sont envoyées à l'adresse IP du serveur virtuel LLB qui agit comme la Gateway pour tout le trafic sortant et sélectionne le routeur en fonction de la méthode LLB configurée.

Pour configurer une route LLB IPv4 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lb route <network> <netmask> <gatewayName>
2
3 show lb route [<network> <netmask>]
4 <!--NeedCopy-->
```

Exemple :

```
1 add lb route 0.0.0.0 0.0.0.0 LLB-vip
2 show lb route 0.0.0.0 0.0.0.0
3        Network          Netmask        Gateway/VIP              Flags
4      -----------      -------------   --------------          --------
5 1)     0.0.0.0          0.0.0.0        LLB-vip                UP
```



```
6 <!--NeedCopy-->
```

Pour configurer une route LLB IPv6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lb route6 <network> <gatewayName>
2
3 show lb route6
4 <!--NeedCopy-->
```

Exemple :

```
1 add lb route6 ::/0 llb6_vs show lb route6 Network VIP Flags -----------
      --------- -------- 1) ::/0 llb6_vs UP
2 <!--NeedCopy-->
```

Pour configurer une route LLB à l'aide de l'utilitaire de configuration

Accédez à Système > Réseau > Itinéraires, sélectionnez **LLB**et configurez l'itinéraire LLB.

Remarque : Sélectionnez LLBV6 pour configurer un itinéraire IPV6.

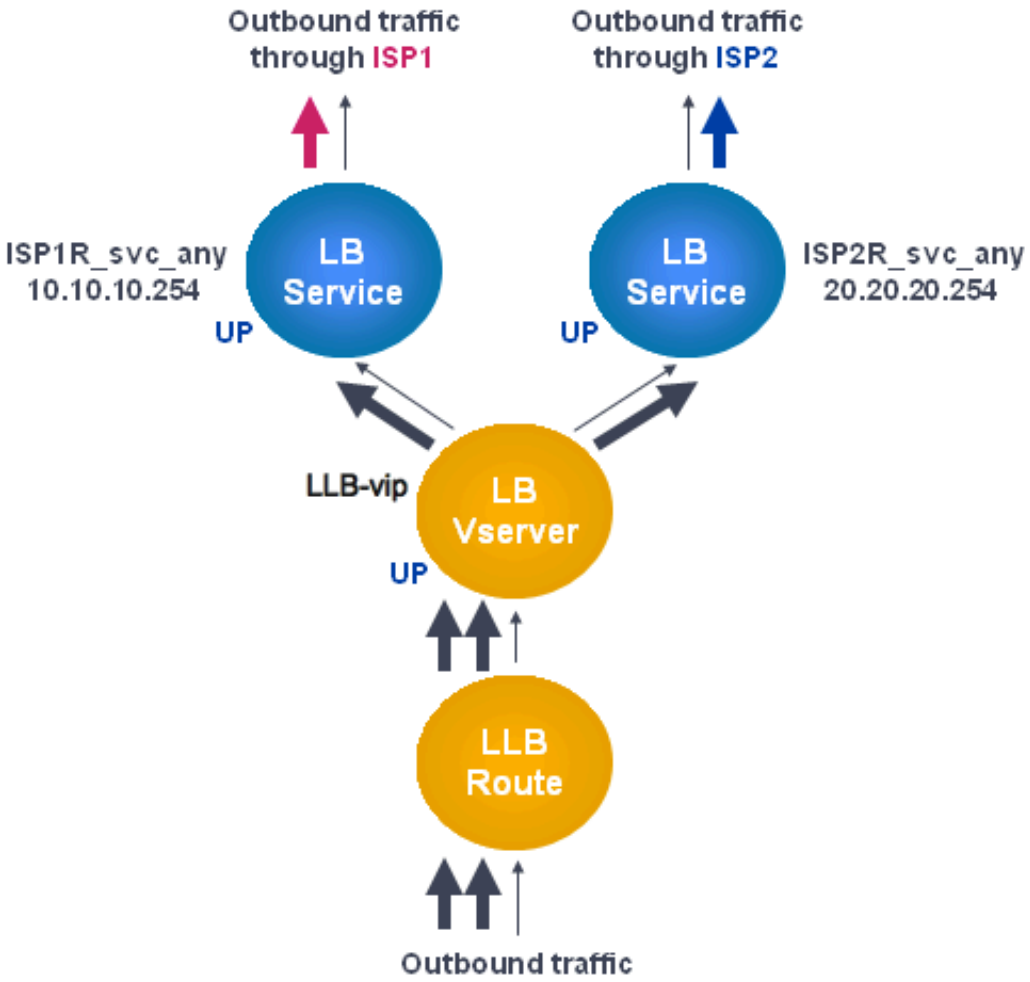
Pour configurer une route LLB à l'aide de l'utilitaire de configuration

1. Accédez à Système > Réseau > Itinéraires.
2. Dans le volet d'informations, sélectionnez l'une des options suivantes :
   - Cliquez sur LLB pour configurer un itinéraire IPv4.
   - Cliquez sur LLBV6 pour configurer un itinéraire IPv4.
3. Dans la boîte de dialogue Créer une route LB ou Créer une routeIPV6 LB, définissez les paramètres suivants :
   - Réseau*
   - Netmask* : requis pour les routes IPV4.
   - Nom de la passerelle *—Nom de la passerelle

     *Paramètre obligatoire
4. Cliquez sur Créer, puis sur Fermer. L'itinéraire que vous venez de créer apparaît dans l'onglet LLB ou LLB6 du volet Itinéraires.

Le diagramme suivant montre une configuration LLB de base. Un service est configuré pour chacun des deux liens (FAI) et les moniteurs PING sont liés par défaut à ces services. Un lien est sélectionné en fonction de la méthode LLB configurée.

Figure 1. Configuration de base LLB



> **Remarque**
>
> Si votre fournisseur de services Internet a fourni une adresse IPv6, remplacez le service IPv4 par un service IPv6 dans la figure ci-dessus.

Créer et lier un moniteur transparent

Vous créez un moniteur transparent pour surveiller l'intégrité des périphériques en amont, tels que les routeurs. Vous pouvez ensuite lier le moniteur transparent aux services. Le moniteur PING par défaut surveille la connectivité uniquement entre l'appliance Citrix ADC et le périphérique en amont. Le moniteur transparent surveille tous les périphériques existants dans le chemin d'accès entre

l'appliance et le périphérique qui possède l'adresse IP de destination spécifiée dans le moniteur. Si un moniteur transparent n'est pas configuré et que l'état du routeur est UP mais que l'un des périphériques de saut suivants de ce routeur est en panne, l'appliance inclut le routeur lors de l'équilibrage de charge et transmet le paquet au routeur. Cependant, le paquet n'est pas livré à la destination finale car l'un des périphériques de saut suivants est en panne. En liant un moniteur transparent, si l'un des périphériques (y compris le routeur) est en panne, le service est marqué comme étant DOWN et le routeur n'est pas inclus lorsque l'appliance effectue l'équilibrage de la charge de liaison.

Pour créer un moniteur transparent à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb monitor <monitorName> <type> -destIP <ip_addr|*> -transparent
   YES

show lb monitor [<monitorName>]
<!--NeedCopy-->
```

Exemple :

```
add lb monitor monitor-1 PING -destIP 10.10.10.11 -transparent YES
> show lb monitor monitor-1
1)   Name.......: monitor-1  Type......:      PING   State....:
   ENABLED
Standard parameters:
  Interval.........:            5 sec   Retries...........:
                    3
  Response timeout.:            2 sec   Down time.........:
      30 sec
  Reverse..........:               NO   Transparent.......:
                  YES
  Secure...........:               NO   LRTM..............:
      ENABLED
  Action...........:   Not applicable   Deviation.........:
      0 sec
  Destination IP...:      10.10.10.11
  Destination port.:    Bound service
  Iptunnel.........:               NO
  TOS..............:               NO   TOS ID...........:
                    0
  SNMP Alert Retries:               0     Success Retries..:
                    1
  Failure Retries..:                0
```



```
<!--NeedCopy-->
```

Pour créer un moniteur transparent à l'aide de l'utilitaire de configuration

Accédez à Gestion du trafic > Équilibrage de charge > Surveille et configurez un moniteur transparent.

Pour créer un moniteur transparent à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Moniteurs.
2. Dans le volet Moniteurs, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un moniteur, définissez les paramètres suivants :
   - Nom*
   - Type *
   - IP destination
   - Transparent

   *Paramètre obligatoire
4. Cliquez sur Créer, puis sur Fermer.
5. Dans le volet Moniteurs, sélectionnez le moniteur que vous venez de configurer et vérifiez que les paramètres affichés dans le volet Détails sont corrects.

Pour lier un moniteur à un service à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Sous l'onglet **Moniteurs**, sous **Disponible**, sélectionnez le moniteur que vous souhaitez lier au service, puis cliquez sur **Ajouter** .

Pour lier un moniteur à un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb monitor <monitorName> <serviceName>

show service <name>
<!--NeedCopy-->
```

Exemple :


```
bind lb monitor monitor-HTTP-1 ISP1R_svc_any
 Done
> show service ISP1R_svc_any
        ISP1R_svc_any (10.10.10.254:*) - ANY
        State: UP
        Last state change was at Thu Sep  2 10:51:07 2010
        Time since last state change: 0 days, 18:41:55.130
        Server Name: 10.10.10.254
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: UP  Weight: 1
                Probes: 1256       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.322 millisec
 Done
<!--NeedCopy-->
```

Pour lier un moniteur à un service à l'aide de l'utilitaire de configuration

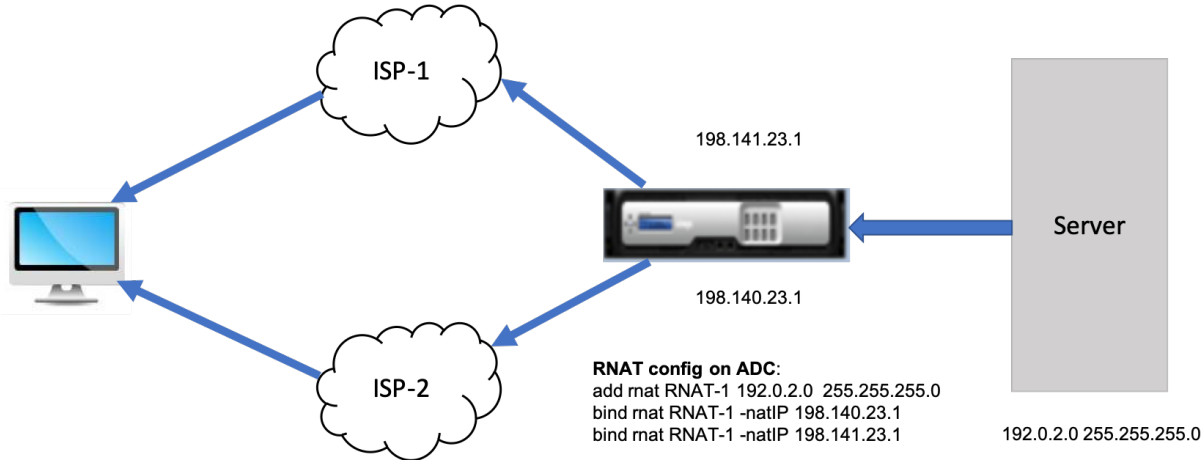
1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Dans le volet d'informations, sélectionnez un service auquel vous souhaitez lier un moniteur, puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le service, sous l'onglet Moniteurs, sous Disponible, sélectionnez le moniteur à lier au service, puis cliquez sur Ajouter.
4. Cliquez sur OK.
5. Dans le volet Services, sélectionnez le service que vous venez de configurer et vérifiez que les paramètres affichés dans le volet Détails sont corrects.

Configurer RNAT avec LLB

August 20, 2021

Vous pouvez configurer une configuration LLB pour la traduction d'adresses réseau inverse (RNAT) pour le trafic sortant. Il garantit que le trafic réseau de retour pour un flux spécifique est acheminé via le même chemin. Configurez d'abord la LLB de base, comme décrit dans Configuration d'un programme d'installation LLB de base, puis configurez RNAT comme décrit dans Configurer RNAT. Activez ensuite le mode « utiliser le sous-réseau IP (USNIP) ».

Dans le diagramme suivant, l'appliance Citrix ADC utilise LLB pour acheminer le trafic sortant vers différents liens. Pendant l'opération RNAT, l'appliance ADC remplace les adresses IP source du trafic sortant par l'adresse IP NAT publique (198.141.23.1) pour acheminer le trafic via ISP-1. De même, l'appliance ADC remplace les adresses IP source par 198.140.23.1 pour acheminer le trafic via ISP-2.



Pour ajouter des SNIP pour les routeurs ISP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add NS IP <subnet of first ISP in the IP router> <subnet mask> -type
    SNIP

add NS IP <subnet of second ISP in the IP router> <subnet mask> -type
    SNIP
<!--NeedCopy-->
```

Exemple :

```
add ns ip 198.140.23.1 255.255.255.0 -type snip

```



```
add ns ip 198.141.23.1 255.255.255.0 -type snip
<!--NeedCopy-->
```

Pour configurer RNAT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))

bind rnat <name> <natIP>@ …

show rnat <name>
<!--NeedCopy-->
```

Exemple :

```
add rnat RNAT-1 192.0.2.0 255.255.255.0
bind rnat RNAT-1 -natIP 198.140.23.1
bind rnat RNAT-1 -natIP 198.141.23.1

> show rnat RNAT-1
    1) RNAT Name: RNAT-1     Network: 192.0.2.0      Netmask:
       255.255.255.0     Traffic Domain: 0
        UseProxyPort: ENABLED

        NatIP: 198.140.23.1
        NatIP: 198.141.23.1
<!--NeedCopy-->
```

Pour configurer RNAT à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **NAT** .
2. Sous l'onglet **RNAT**, cliquez sur **Configurer RNAT** .
3. Spécifiez le réseau sur lequel effectuer RNAT.

> **Remarque**
>
> Vous pouvez également configurer RNAT à l'aide des listes de contrôle d'accès (ACL). Pour plus de détails, reportez-vous à Configuration de RNAT .

Pour activer l'utilisation du mode IP de sous-réseau à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
enable ns mode USNIP

show ns mode
<!--NeedCopy-->
```

Exemple :

```
enable ns mode USNIP

show ns mode
        Mode                            Acronym             Status
        -------                         -------             ------
 1)     Fast Ramp                       FR                  ON
 2)     … .
 8)     Use Subnet IP                   USNIP               ON
 9)     …
<!--NeedCopy-->
```

Pour activer le mode Utiliser le mode IP de sous-réseau à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres** et, sous **Modes et fonctionnalités**, cliquez sur **Configurer les modes** .
2. Dans la boîte de dialogue **Configurer les modes**, sélectionnez **Utiliser l'adresse IP du sous-réseau**, puis cliquez sur **OK** .

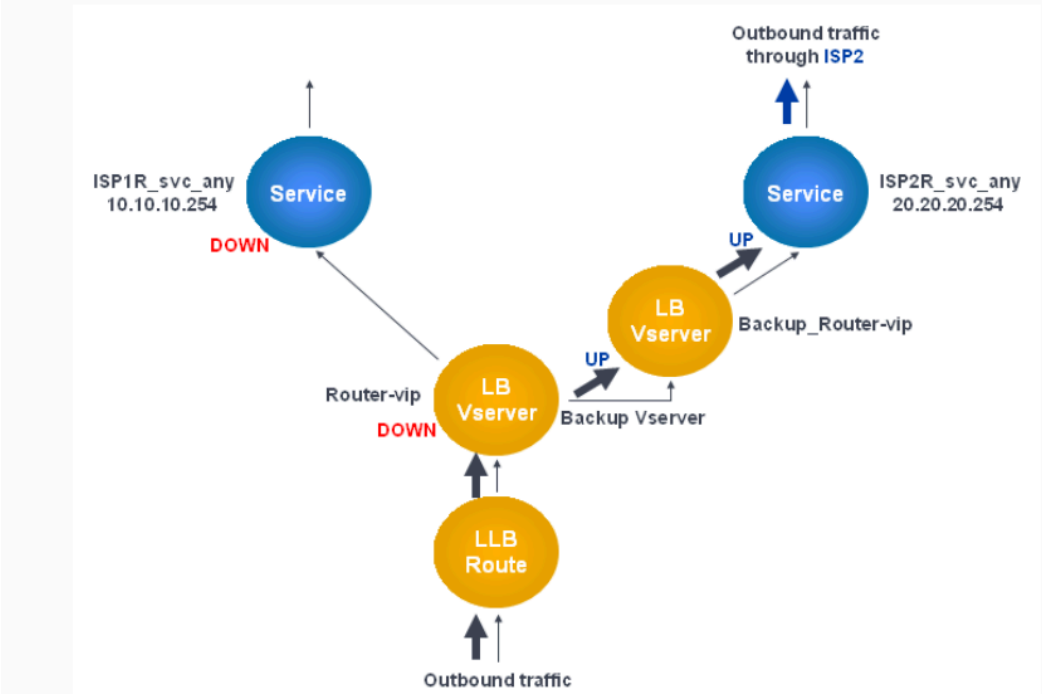
Configurer une route de sauvegarde

August 20, 2021

Pour éviter toute interruption des services lorsque la route principale est en panne, vous pouvez configurer une route de sauvegarde. Une fois la route de sauvegarde configurée, l'appliance Citrix ADC l'utilise automatiquement en cas d'échec de la route principale. Commencez par créer un serveur virtuel principal, comme décrit dans Configuration d'un serveur virtuel LLB et liaison d'un service. Pour configurer une route de sauvegarde, créez un serveur virtuel secondaire similaire à un serveur virtuel principal, puis définissez ce serveur virtuel comme serveur virtuel de sauvegarde (route).

Dans le diagramme suivant, **Router-VIP** est le serveur virtuel principal et **Backup_Router-VIP** est le serveur virtuel secondaire désigné comme serveur virtuel de sauvegarde.

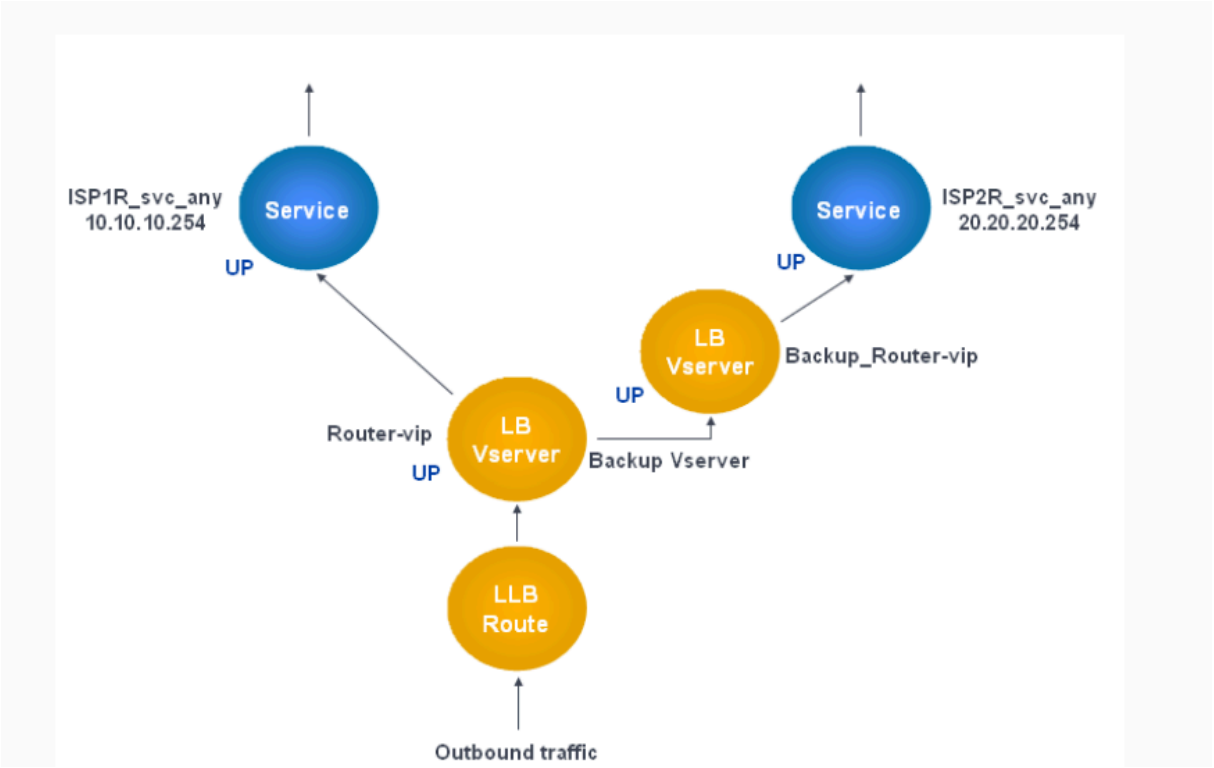
Figure 1. Configuration de l'itinéraire de sauvegarde



Remarque : Si votre fournisseur de services Internet a fourni une adresse IPv6, remplacez le service IPv4 par un service IPv6 dans la figure précédente.

Par défaut, tout le trafic est envoyé par l'itinéraire principal. Toutefois, lorsque l'itinéraire principal échoue, tout le trafic est détourné vers l'itinéraire de sauvegarde, comme indiqué dans le diagramme suivant.

Figure 2. Sauvegardez la gamme en opération



Remarque : Si votre fournisseur de services Internet a fourni une adresse IPv6, remplacez le service IPv4 par un service IPv6 dans la figure précédente.

Pour définir le serveur virtuel secondaire comme serveur virtuel de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -backupVserver <string>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Router-vip -backupVServer Backup_Router-vip
> show lb vserver Router-vip
        Router-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Fri Sep  3 04:46:48 2010
        Time since last state change: 0 days, 03:09:45.600
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       1 (Active)
```



```
12          Configured Method: ROUNDROBIN
13          Mode: IP
14          Persistence: DESTIP     Persistence Mask: 255.255.255.255
                    Persistence v6MaskLength: 128   Persistence Timeout: 2
                min
15          Backup: Router2-vip
16          Connection Failover: DISABLED
17   Done
18  <!--NeedCopy-->
```

Pour définir le serveur virtuel secondaire comme serveur virtuel de sauvegarde à l'aide de l'utilitaire de configuration

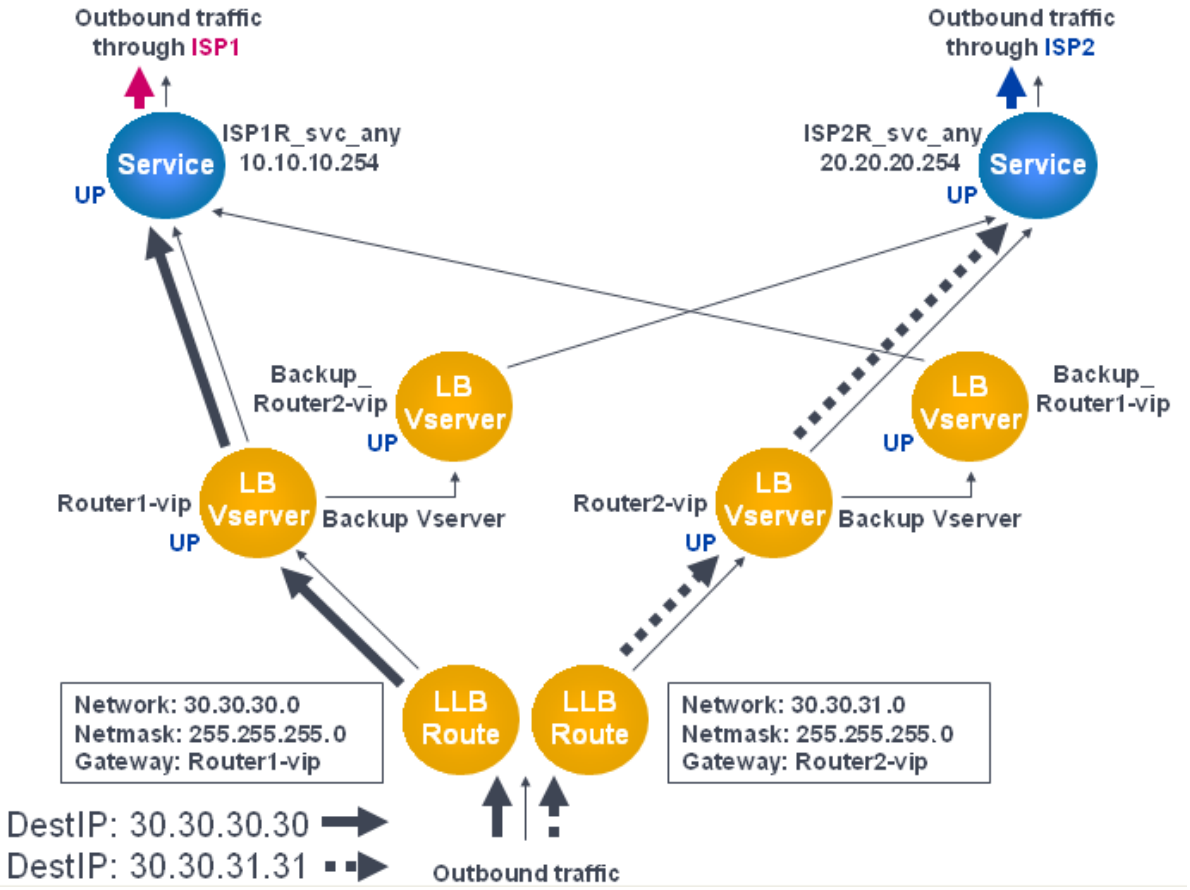
1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et sélectionnez le serveur virtuel secondaire pour lequel vous souhaitez configurer le serveur virtuel de sauvegarde.
2. Dans la boîte de dialogue **Serveur virtuel d'équilibrage** de charge, sous **Avancé**, sélectionnez **Protection** .
3. Dans la liste déroulante **Sauvegarde Virtual Server**, sélectionnez le serveur virtuel de sauvegarde secondaire, puis cliquez sur **OK** .

Scénario de déploiement de LLB résilient

January 21, 2021

Dans le diagramme suivant, il y a deux réseaux : 30.30.30.0 et 30.30.31.0. L'équilibrage de charge de liaison est configuré en fonction de l'adresse IP de destination. Deux itinéraires sont configurés avec les passerelles **Router1-VIP** et **Router2-VIP**, respectivement. **Router1-VIP** est configuré comme une sauvegarde sur **Router2-VIP** et de la manière opposée. Tout le trafic avec l'adresse IP de destination spécifiée comme 30.30.30.30 est envoyé via **Router1-VIP** et le trafic avec l'adresse IP de destination spécifiée comme 30.30.31.31 est envoyé via **Router2-VIP** .

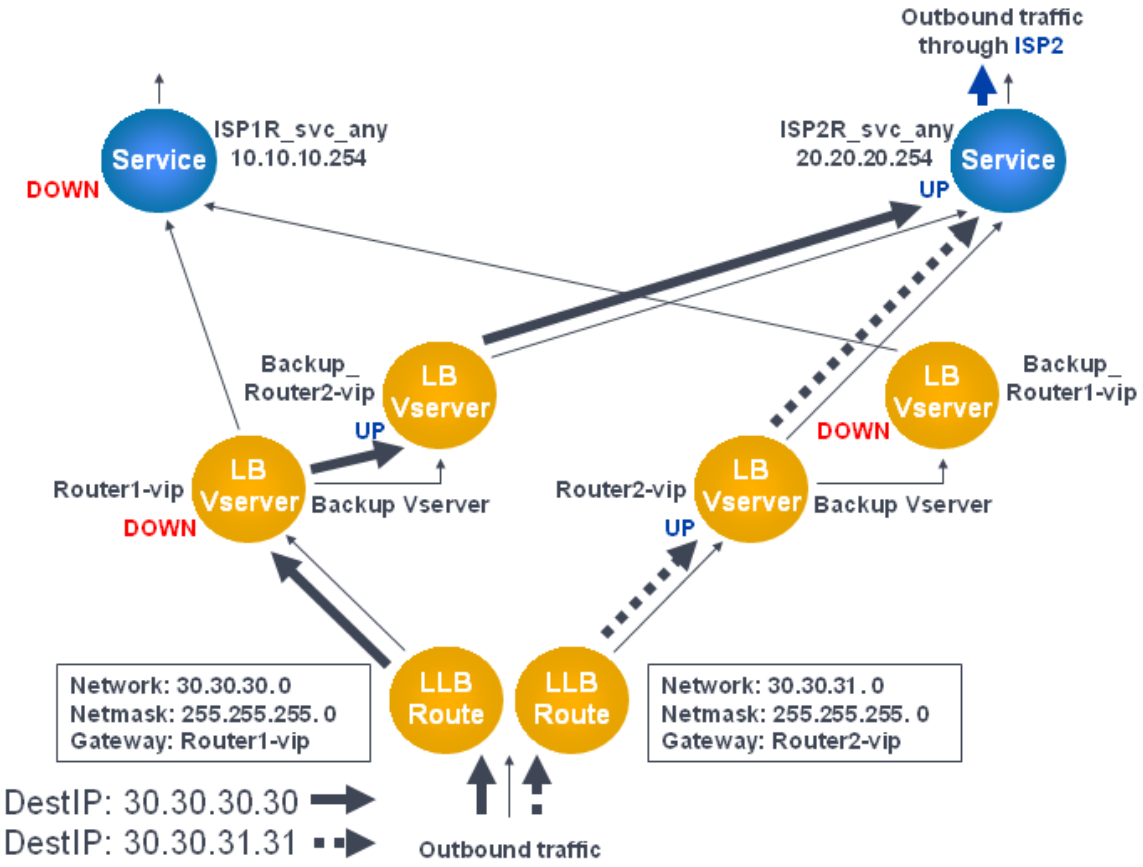
Figure 1. Configuration du déploiement LLB résilient



Remarque : Si votre fournisseur de services Internet a fourni une adresse IPv6, remplacez le service IPv4 par un service IPv6 dans la figure précédente.

Toutefois, si l'une des passerelles (**Router1-VIP** ou **Router2-VIP**) est DOWN, le trafic est acheminé via le routeur de sauvegarde. Dans le diagramme suivant, **Router1-VIP** pour ISP1 est DOWN, donc tout le trafic avec l'adresse IP de destination spécifiée comme 30.30.30.30 est également envoyé via ISP2.

Figure 2. Scénario de déploiement LLB résilient



Remarque : Si votre fournisseur de services Internet a fourni une adresse IPv6, remplacez le service IPv4 par un service IPv6 dans la figure précédente.

Surveiller la configuration d'une LLB

August 20, 2021

Une fois la configuration terminée, vous pouvez afficher les statistiques de chaque service et serveur virtuel pour vérifier les éventuels problèmes.

Afficher les statistiques d'un serveur virtuel

Pour évaluer les performances des serveurs virtuels ou pour résoudre les problèmes, vous pouvez afficher les détails des serveurs virtuels configurés sur l'appliance Citrix ADC. Vous pouvez afficher un résumé des statistiques pour tous les serveurs virtuels. Vous pouvez également spécifier le nom d'un serveur virtuel pour afficher les statistiques uniquement pour ce serveur virtuel. Vous pouvez afficher les détails suivants :

- Nom
- Adresse IP
- Port
- Protocole
- État du serveur virtuel
- Taux de demandes reçues
- Rate of hits

Afficher les statistiques du serveur virtuel à l'aide de l'interface de ligne de commande

Pour afficher un résumé des statistiques de tous les serveurs virtuels actuellement configurés sur Citrix ADC, ou pour un seul serveur virtuel, à l'invite de commandes, tapez :

```
stat lb vserver -detail] [<name>]
<!--NeedCopy-->
```

Exemple :

```
stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
        0/s
Two                          *     0          TCP         DOWN      0/s
        0/s
Three                        *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done
<!--NeedCopy-->
```

Afficher les statistiques de serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Statistiques**.
2. Si vous souhaitez afficher les statistiques pour un seul serveur virtuel, dans le volet d'informations, sélectionnez le serveur virtuel, puis cliquez sur Statistiques.

Afficher les statistiques d'un service

Vous pouvez afficher le taux de demandes, de réponses, d'octets de demande, d'octets de réponse, de connexions client actuelles, de demandes dans la file d'attente de surtension, de connexions au serveur en cours, etc. à l'aide des statistiques de service.

Afficher les statistiques d'un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat service <name>
<!--NeedCopy-->
```

Exemple :

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Afficher les statistiques d'un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services > Statistiques**.
2. Si vous souhaitez afficher les statistiques pour un seul service, sélectionnez-le, puis cliquez sur Statistiques.

Équilibrage de charge

August 20, 2021

La fonction d'équilibrage de charge distribue les demandes des utilisateurs pour des pages Web et autres applications protégées sur plusieurs serveurs hébergeant (ou miroir) le même contenu. Vous utilisez l'équilibrage de charge principalement pour gérer les demandes des utilisateurs vers des applications fortement utilisées, évitant les mauvaises performances et les pannes et vous assurant que les utilisateurs peuvent accéder à vos applications protégées. L'équilibrage de charge offre également une tolérance aux pannes. Lorsqu'un serveur hébergeant une application protégée devient indisponible, la fonctionnalité distribue les demandes des utilisateurs aux autres serveurs hébergeant la même application.

Vous pouvez configurer la fonction d'équilibrage de charge pour :

- Distribuez toutes les demandes pour un site Web, une application ou une ressource protégé spécifique entre deux ou plusieurs serveurs configurés de manière identique.

- Utilisez l'un de plusieurs algorithmes différents pour déterminer quel serveur doit recevoir chaque demande d'utilisateur entrante, en basant la décision sur différents facteurs, tels que le serveur qui possède le moins de connexions utilisateur actuelles ou quel serveur a la charge la plus faible.

La fonction d'équilibrage de charge est une fonctionnalité centrale de l'appliance Citrix ADC. La plupart des utilisateurs configurent d'abord une configuration de base fonctionnelle, puis personnalisent divers paramètres, y compris la persistance des connexions. En outre, vous pouvez configurer des fonctionnalités pour protéger la configuration contre les défaillances, gérer le trafic client, gérer et surveiller les serveurs et gérer un déploiement à grande échelle.

Fonctionnement de l'équilibrage de charge

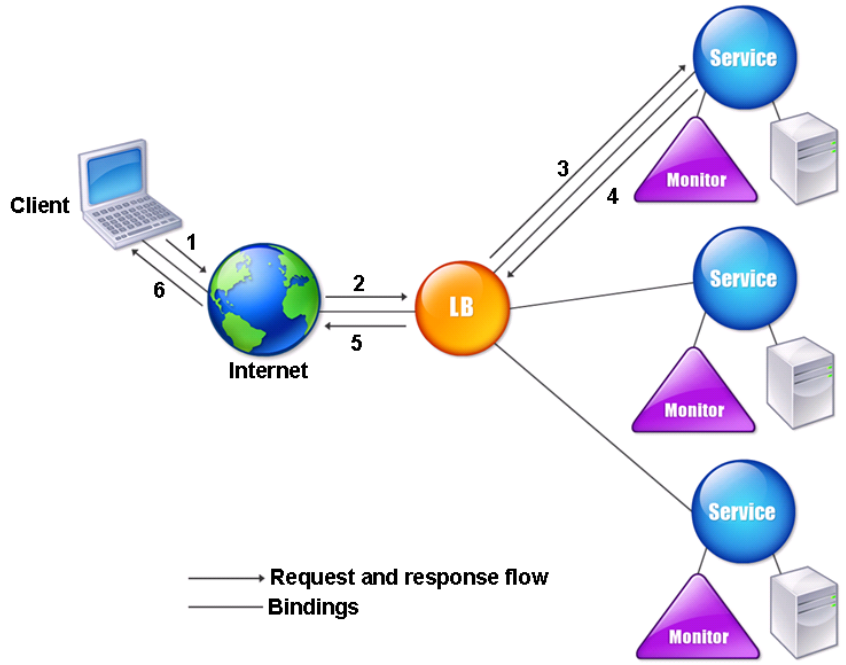
August 20, 2021

Dans une configuration d'équilibrage de charge de base, les clients envoient leurs demandes à l'adresse IP d'un serveur virtuel configuré sur l'appliance Citrix ADC. Le serveur virtuel les distribue aux serveurs d'applications à équilibrage de charge selon un modèle prédéfini, appelé algorithme d'équilibrage de charge. Il peut arriver que vous souhaitiez attribuer au serveur virtuel d'équilibrage de charge une adresse générique au lieu d'une adresse IP spécifique. Pour obtenir des instructions sur la spécification d'un port HTTP global sur l'appliance, consultez **Ports HTTP globaux**.

Principes de base de l'équilibrage de charge

Une configuration d'équilibrage de charge inclut un serveur virtuel d'équilibrage de charge et plusieurs serveurs d'applications équilibrés de charge. Le serveur virtuel reçoit les demandes client entrantes, utilise l'algorithme d'équilibrage de charge pour sélectionner un serveur d'applications et transmet les demandes au serveur d'applications sélectionné. Le dessin conceptuel suivant illustre un déploiement typique d'équilibrage de charge. Une autre variante implique l'attribution d'un port HTTP global.

Figure 1. Architecture d'équilibrage de charge



Le serveur virtuel d'équilibrage de charge peut utiliser plusieurs algorithmes (ou méthodes) pour déterminer comment répartir la charge entre les serveurs à charge équilibrée qu'il gère. La méthode d'équilibrage de charge par défaut est la méthode de connexion la moins élevée, dans laquelle l'appliance Citrix ADC transfère chaque connexion client entrante vers le serveur d'applications à équilibrage de charge qui possède actuellement le moins de connexions utilisateur actives.

Les entités que vous configurez dans une configuration typique d'équilibrage de charge Citrix ADC sont les suivantes :

- **Serveur virtuel d'équilibrage de charge.** Combinaison d'adresse IP, de port et de protocole à laquelle un client envoie des demandes de connexion pour un site Web ou une application à charge équilibrée particulière. Si l'application est accessible à partir d'Internet, l'adresse IP du serveur virtuel (VIP) est une adresse IP publique. Si l'application est accessible uniquement à partir du réseau local ou du WAN, le VIP est généralement une adresse IP privée (non routable de l'ICANN).
- **Service.** Combinaison d'adresse IP, de port et de protocole utilisée pour acheminer les demandes vers un serveur d'applications à équilibrage de charge spécifique. Un service peut être une représentation logique du serveur d'applications lui-même ou d'une application exécutée sur un serveur qui héberge plusieurs applications. Après avoir créé un service, vous le liez à un serveur virtuel d'équilibrage de charge.

- **Objet serveur.** Entité virtuelle qui vous permet d'attribuer un nom à un serveur physique au lieu d'identifier le serveur par son adresse IP. Si vous créez un objet serveur, vous pouvez spécifier son nom au lieu de l'adresse IP du serveur lorsque vous créez un service. Sinon, vous devez spécifier l'adresse IP du serveur lorsque vous créez un service, et l'adresse IP devient le nom du serveur.
- **Moniteur.** Entité sur l'appliance Citrix ADC qui suit un service et assure son fonctionnement correct. Le moniteur sonde périodiquement (ou effectue une vérification de l'état) chaque service auquel vous l'affectez. Si le service ne répond pas dans le délai spécifié par le délai d'expiration et qu'un nombre spécifié de vérifications d'intégrité échoue, ce service est marqué comme DOWN. L'appliance Citrix ADC ignore ensuite ce service lors de l'équilibrage de charge, jusqu'à ce que les problèmes qui ont provoqué la cessation de la réponse du service soient résolus.

Le serveur virtuel, les services et les serveurs d'applications équilibrés de charge dans une configuration d'équilibrage de charge peuvent utiliser des adresses IP IPv4 (Internet Protocol version 4) ou IPv6 (Internet Protocol version 6). Vous pouvez mélanger les adresses IPv4 et IPv6 dans une seule configuration d'équilibrage de charge.

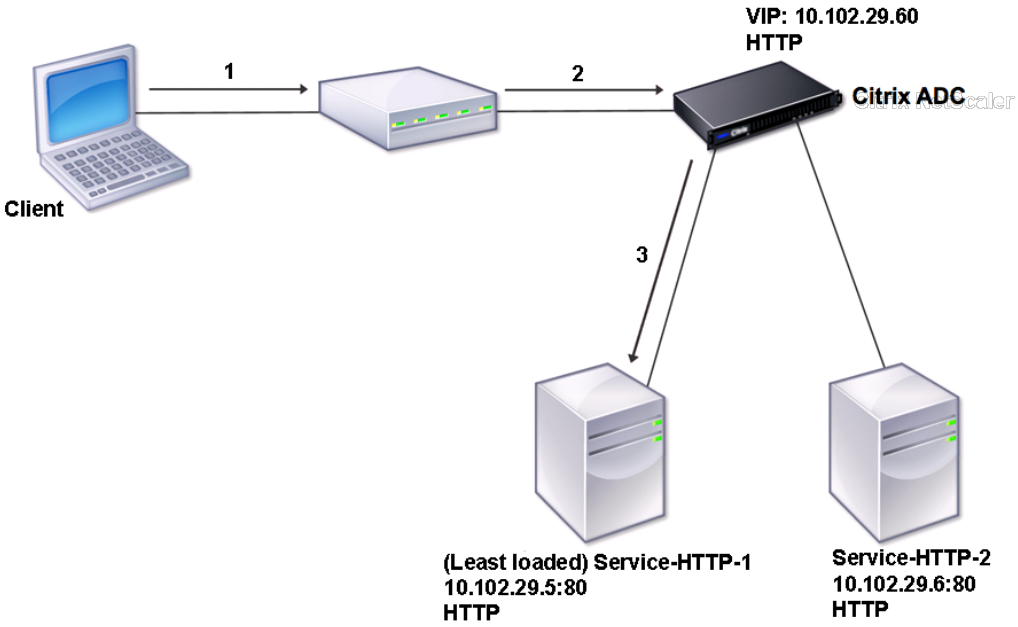
Pour connaître les variations de la configuration d'équilibrage de charge, consultez les cas d'utilisation suivants :

- Configuration de l'équilibrage de charge en mode Retour au serveur direct
- Configuration des serveurs LINUX en mode DSR
- Configuration du mode DSR lors de l'utilisation de TOS
- Configuration de l'équilibrage de charge en mode DSR à l'aide d'IP sur IP
- Configuration de l'équilibrage de charge en mode à un bras
- Configuration de l'équilibrage de charge en mode Inline
- Équilibrage de charge des serveurs système de détection des intrusions
- Équilibrer la charge des serveurs de protocole Bureau à distance

Présentation de la topologie

Dans une configuration d'équilibrage de charge, le serveur d'équilibrage de charge se trouve logiquement entre le client et la batterie de serveurs et gère le flux de trafic vers les serveurs de la batterie de serveurs. Sur l'appliance Citrix ADC, les serveurs d'applications sont représentés par des entités virtuelles appelées services. Le diagramme suivant illustre la topologie d'une configuration d'équilibrage de charge de base.

Figure 2. Topologie d'équilibrage de charge de base

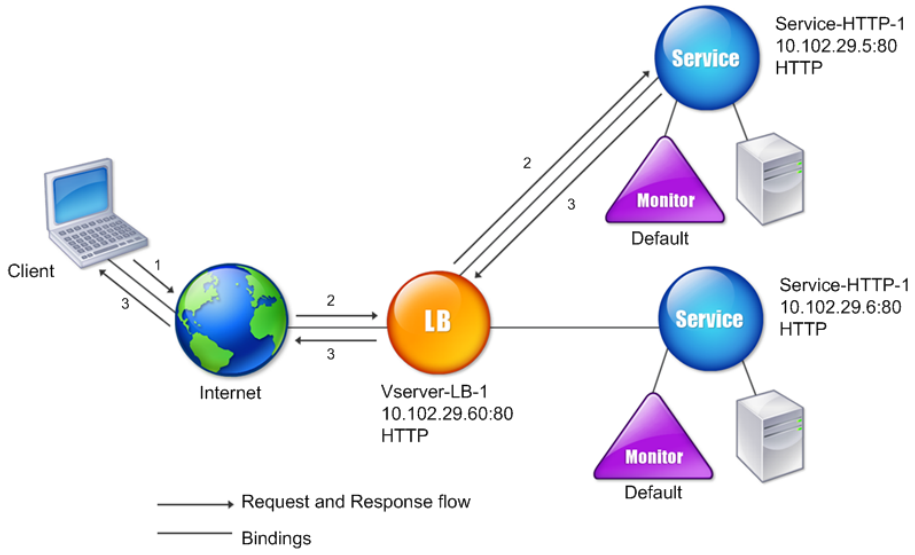


Dans le diagramme, l'équilibrage de charge est utilisé pour gérer le flux de trafic vers les serveurs. Le serveur virtuel sélectionne le service et l'affecte pour répondre aux demandes du client. Considérons un scénario dans lequel les services service-HTTP-1 et service-HTTP-2 sont créés et liés au serveur virtuel nommé vServer-lb-1. VServer-lb-1 transfère la requête client à Service-HTTP-1 ou Service-HTTP-2. L'appliance Citrix ADC utilise la méthode d'équilibrage de charge de connexion la moins élevée pour sélectionner le service pour chaque demande. Le tableau suivant répertorie les noms et les valeurs des entités de base qui doivent être configurées sur l'appliance.

Entité	Nom	Adresse IP	Port	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.60	80	HTTP
Services	Service-HTTP-1	10.102.29.5	80	HTTP
	Service-HTTP-2	10.102.29.6	80	HTTP
Moniteurs	Valeur par défaut	Aucune	Aucune	Aucune

Le diagramme suivant présente les valeurs d'échantillon d'équilibrage de charge et les paramètres obligatoires décrits dans le tableau précédent.

Figure 3. Modèle d'entité d'équilibrage de charge



Utilisation de caractères génériques au lieu d'adresses IP et de ports

Il peut arriver que vous deviez utiliser un caractère générique pour l'adresse IP ou le port d'un serveur virtuel ou pour le port d'un service. Les cas suivants peuvent nécessiter l'utilisation d'un caractère générique :

- Si l'appliance Citrix ADC est configurée comme un passage transparent, qui doit accepter tout le trafic qui lui est envoyé, quel que soit l'adresse IP ou le port vers lequel il est envoyé.
- Si un ou plusieurs services écoutent sur des ports qui ne sont pas bien connus.
- Si un ou plusieurs services, au fil du temps, changent les ports qu'ils écoutent.
- Si vous atteignez la limite pour le nombre d'adresses IP et de ports que vous pouvez configurer sur une seule appliance Citrix ADC.
- Si vous souhaitez créer des serveurs virtuels qui écoutent tout le trafic sur un réseau local virtuel spécifique.

Lorsqu'un serveur ou un service virtuel configuré par caractères génériques reçoit du trafic, l'appliance Citrix ADC détermine l'adresse IP ou le port réel et crée des enregistrements pour le service et le serveur d'applications à charge équilibrée associé. Ces enregistrements créés

dynamiquement sont appelés enregistrements de serveur et de service appris dynamiquement.

Par exemple, une configuration d'équilibrage de charge de pare-feu peut utiliser des caractères génériques pour l'adresse IP et le port. Si vous liez un service TCP générique à ce type de serveur virtuel d'équilibrage de charge, le serveur virtuel reçoit et traite tout le trafic TCP qui ne correspond à aucun autre service ou serveur virtuel.

Le tableau suivant décrit certains des différents types de configurations génériques et le moment où chacune doit être utilisée.

Adresse IP	Port	Protocole	Description
*	*	TCP	Serveur virtuel générique général qui accepte le trafic envoyé à n'importe quelle adresse IP et port de l'appliance Citrix ADC. Lors de l'utilisation d'un serveur virtuel générique, l'appliance apprend dynamiquement l'adresse IP et le port de chaque service et crée les enregistrements nécessaires au cours du traitement du trafic.
*	*	TCP	Serveur virtuel d'équilibrage de charge de pare-feu. Vous pouvez lier des services de pare-feu à ce serveur virtuel et l'appliance Citrix ADC transmet le trafic via le pare-feu à la destination.

Adresse IP	Port	Protocole	Description
Adresse IP	*	TCP, UDP et ANY	Serveur virtuel qui accepte tout le trafic envoyé à l'adresse IP spécifiée, quel que soit le port. Vous devez lier explicitement à ce type de serveur virtuel les services vers lesquels il redirigera le trafic. Il ne les apprend pas dynamiquement. **Remarque** : vous ne configurez pas de services ou de serveurs virtuels pour un port HTTP global. Dans ce cas, vous configurez un port spécifique en tant que port HTTP global (par exemple, définissez ns param -HttpPort 80). L'appliance accepte ensuite tout le trafic correspondant au numéro de port et le traite en tant que trafic HTTP. L'appliance apprend et crée dynamiquement des services pour ce trafic.

Adresse IP	Port	Protocole	Description
*	port	SSL, SSL_TCP	Serveur virtuel qui accepte tout le trafic envoyé à n'importe quelle adresse IP sur un port spécifique. Utilisé pour le déchargement SSL transparent global. Tout le traitement SSL, HTTP et TCP qui est généralement effectué pour un service du même type de protocole est appliqué au trafic qui est dirigé vers ce port spécifique. L'appliance utilise le port pour connaître dynamiquement l'adresse IP du service qu'elle doit utiliser. Si —cleartext n'est pas spécifié, l'appliance Citrix ADC utilise SSL de bout en bout.
*	port	Sans objet	Tous les autres serveurs virtuels pouvant accepter le trafic vers le port. Vous ne liez pas de services à ces serveurs virtuels. L'appliance Citrix ADC les apprend dynamiquement.

Remarque : Si vous avez configuré votre appliance Citrix ADC comme un passage transparent utilisant des ports globaux (génériques), vous pouvez activer le mode Edge.
Pour plus d'informations, reportez-vous à lasection « Configuration du mode Edge ». «

L'appliance Citrix ADC tente de localiser des serveurs et des services virtuels en essayant d'abord une correspondance exacte. Si aucun n'est trouvé, il continue à rechercher une correspondance basée sur des caractères génériques, dans l'ordre suivant :

1. Adresse IP spécifique et numéro de port spécifique
2. Adresse IP spécifique et port * (caractère générique)
3. • (caractère générique) adresse IP et un port spécifique
4. • (caractère générique) adresse IP et un port * (caractère générique)

Si l'appliance ne peut pas sélectionner un serveur virtuel par adresse IP ou numéro de port, elle recherche un serveur virtuel basé sur le protocole utilisé dans la demande, dans l'ordre suivant :

1. HTTP
2. TCP
3. ANY

Configuration des ports HTTP globaux

Vous ne configurez pas de services ou de serveurs virtuels pour un port HTTP global. Au lieu de cela, vous configurez un port spécifique à l'aide de la commande set ns param. Après avoir configuré ce port, l'appliance Citrix ADC accepte tout le trafic correspondant au numéro de port et le traite en tant que trafic HTTP, apprenant dynamiquement et créant des services pour ce trafic.

Vous pouvez configurer plusieurs numéros de port en tant que port HTTP global. Si vous spécifiez plusieurs numéros de port dans une seule commande ns param, séparez les numéros de port par un seul espace blanc. Si un ou plusieurs ports ont déjà été spécifiés en tant que ports HTTP globaux et que vous souhaitez ajouter un ou plusieurs ports sans supprimer les ports actuellement configurés, vous devez spécifier tous les numéros de port, actuels et nouveaux, dans la commande. Avant d'ajouter des numéros de port, utilisez la commande show ns param pour afficher les ports actuellement configurés.

Pour configurer un port HTTP global à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un port HTTP global et vérifier la configuration :

```
set ns param -httpPort <port>

show ns param
```



```
<!--NeedCopy-->
```

Exemple 1 : Configuration d'un port en tant que port HTTP global

Dans cet exemple, le port 80 est configuré en tant que port HTTP global.

```
set ns param -httpPort 80
Done
show ns param
         Global configuration settings:
                            HTTP port(s): 80
                        Max connections: 0
           Max requests per connection: 0
                   Client IP insertion: DISABLED
                        Cookie version: 0
         Persistence Cookie Secure Flag: ENABLED
         ...
         ...
<!--NeedCopy-->
```

Exemple 2 : Ajout de ports lorsqu'un ou plusieurs ports HTTP globaux sont déjà configurés**

Dans cet exemple, le port 8888 est ajouté à la liste globale des ports HTTP. Le port 80 est déjà configuré en tant que port HTTP global.

```
> show ns param
        Global configuration settings:
                            HTTP port(s): 80
                        Max connections: 0
           Max requests per connection: 0
                   Client IP insertion: DISABLED
                        Cookie version: 0
        Persistence Cookie Secure Flag: ENABLED
                            Min Path MTU: 576
        ...
        ...
 Done
> set ns param -httpPort 80 8888
 Done
>  show ns param

        Global configuration settings:
                            HTTP port(s): 80,8888
```



```
                        Max connections: 0
            Max requests per connection: 0
                    Client IP insertion: DISABLED
                         Cookie version: 0
         Persistence Cookie Secure Flag: ENABLED
                           Min Path MTU: 576

         ...
         ...
 Done
>
<!--NeedCopy-->
```

Pour configurer un port HTTP global à l'aide de l'utilitaire de configuration

1. Accédez à **Système > Paramètres > Modifier les paramètres HTTP**, puis ajoutez un numéro de port HTTP.

Configurer l'équilibrage de charge de base

August 20, 2021

Avant de configurer votre configuration initiale d'équilibrage de charge, activez la fonction d'équilibrage de charge. Commencez ensuite par créer au moins un service pour chaque serveur dans le groupe d'équilibrage de charge. Une fois les services configurés, vous êtes prêt à créer un serveur virtuel d'équilibrage de charge et à lier chaque service au serveur virtuel. Cela termine la configuration initiale. Avant de procéder à une configuration supplémentaire, vérifiez votre configuration pour vous assurer que chaque élément a été configuré correctement et fonctionne comme prévu.

Activation de l'équilibrage de charge

Vous pouvez configurer des entités d'équilibrage de charge telles que des services et des serveurs virtuels lorsque la fonctionnalité d'équilibrage de charge est désactivée, mais elles ne fonctionneront pas tant que vous n'avez pas activé la fonctionnalité.

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

- activer la fonction ns LB
- show ns feature

Exemple

```
    > enable ns feature LoadBalancing

     Done

    > show ns feature


            Feature                         Acronym             Status

            -------                         -------             ------

     1)     Web Logging                     WL                  OFF

     2)     Surge Protection                SP                  ON

     3) Load Balancing LB ON

     .

     .

     .

     24)    NetScaler Push                  push                OFF

     Done
<!--NeedCopy-->
```

Pour activer l'équilibrage de charge à l'aide de l'interface graphique

Accédez à **Système** > **Paramètres** et, dans **Configurer les fonctionnalités de base**, sélectionnez **Équilibrage de charge**.

Configuration d'un objet serveur

Créez une entrée pour votre serveur sur l'appliance Citrix ADC. L'appliance Citrix ADC prend en charge les serveurs basés sur les adresses IP et les serveurs basés sur des domaines. Si vous créez un serveur

basé sur l'adresse IP, vous pouvez spécifier le nom du serveur au lieu de son adresse IP lorsque vous créez un service. Pour plus d'informations sur la configuration du DNS pour un serveur basé sur un domaine, voir Système de noms de domaine.

Pour créer un objet serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add server `<name>`@ `<IPAddress>`@ | `<domain>`
<!--NeedCopy-->
```

Exemple d'ajout d'un serveur de noms basé sur une adresse IP :

```
add server web_serv 10.102.27.150
<!--NeedCopy-->
```

Exemple pour ajouter un serveur basé sur un domaine :

```
add server web_serv test.com
<!--NeedCopy-->
```

Pour créer un objet serveur à l'aide de l'interface graphique graphique

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs** et ajoutez un objet serveur.

Configuration des services

Après avoir activé la fonctionnalité d'équilibrage de charge, vous devez créer au moins un service pour chaque serveur d'applications qui doit être inclus dans votre configuration d'équilibrage de charge. Les services que vous configurez fournissent les connexions entre l'appliance Citrix ADC et les serveurs équilibrés de charge. Chaque service a un nom et spécifie une adresse IP, un port et le type de données qui est servi.

Si vous créez un service sans créer d'objet serveur au préalable, l'adresse IP du service est également le nom du serveur qui héberge le service. Si vous préférez identifier les serveurs par nom plutôt que par adresse IP, vous pouvez créer des objets serveur, puis spécifier le nom d'un serveur au lieu de son adresse IP lorsque vous créez un service.

Lorsque vous créez un service qui utilise UDP comme protocole de couche de transport, un moniteur ping est automatiquement lié au service. Un moniteur ping est le moniteur le plus basique des moniteurs intégrés. Lorsque vous créez un service qui utilise TCP comme protocole de couche de transport, un moniteur TCP_Default est automatiquement lié au service. Lorsque vous développez une stratégie

de gestion de votre configuration d'équilibrage de charge, vous pouvez décider de lier un autre type de moniteur, ou plusieurs moniteurs, au service.

Création d'un service

Avant de créer un service, vous devez comprendre les différents types de service et la façon dont chacun est utilisé. La liste suivante décrit les types de services pris en charge par l'appliance Citrix ADC.

HTTP

Utilisé pour les serveurs à charge équilibrée qui acceptent le trafic HTTP, tels que les sites Web standard et les applications Web. Le type de service HTTP permet à l'appliance Citrix ADC de fournir la compression, le filtrage de contenu, la mise en cache et la prise en charge de la conservation du client pour vos serveurs Web de couche 7. Ce type de service prend également en charge l'insertion de port IP du serveur virtuel, la réécriture de port de redirection, le Web 2.0 Push et la prise en charge de la redirection d'URL.

Comme HTTP est un protocole d'application basé sur TCP, vous pouvez également utiliser le type de service TCP pour les serveurs Web. Toutefois, si vous le faites, l'appliance Citrix ADC est capable d'effectuer uniquement l'équilibrage de charge de couche 4. Il ne peut fournir aucun des supports de couche 7 décrits précédemment.

SSL

Utilisé pour les serveurs qui acceptent le trafic HTTPS, tels que les sites Web de commerce électronique et les applications de panier d'achat. Le type de service SSL permet à l'appliance Citrix ADC de chiffrer et de déchiffrer le trafic SSL (effectuer le déchargement SSL) pour vos applications Web sécurisées. Il prend également en charge la persistance HTTP, la commutation de contenu, la réécriture, l'insertion de port IP du serveur virtuel, Web 2.0 Push et la redirection d'URL.

Vous pouvez également utiliser les types de service SSL_BRIDGE, SSL_TCP ou TCP. Dans ce cas, toutefois, l'appliance n'effectue que l'équilibrage de charge de couche 4. Il ne peut pas fournir le déchargement SSL ou l'un des supports de couche 7 décrits.

FTP

Utilisé pour les serveurs qui acceptent le trafic FTP. Le type de service FTP permet à l'appliance Citrix ADC de prendre en charge des détails spécifiques du protocole FTP.

Vous pouvez également utiliser des types de service TCP ou AUY pour les serveurs FTP.

TCP

Utilisé pour les serveurs qui acceptent de nombreux types de trafic TCP différents ou qui acceptent un type de trafic TCP pour lequel un type de service plus spécifique n'est pas disponible.

Vous pouvez également utiliser le type de service ANY pour ces serveurs.

SSL_TCP

Utilisé pour les serveurs qui acceptent le trafic SSL non HTTP, pour prendre en charge le déchargement SSL.

Vous pouvez également utiliser le type de service TCP pour ces services. Dans ce cas, l'appliance Citrix ADC effectue à la fois l'équilibrage de charge de la couche 4 et le déchargement SSL.

UDP

Utilisé pour les serveurs qui acceptent le trafic UDP. Vous pouvez également utiliser le type de service ANY.

SSL_BRIDGE

Utilisé pour les serveurs qui acceptent le trafic SSL lorsque vous ne souhaitez pas que l'appliance Citrix ADC effectue le déchargement SSL. Vous pouvez également utiliser le type de service SSL_TCP.

NNTP

Utilisé pour les serveurs qui acceptent le trafic NNTP (Network News Transfer Protocol), généralement les sites Usenet.

DNS

Utilisé pour les serveurs qui acceptent le trafic DNS, généralement les serveurs de noms. Avec le type de service DNS, l'appliance Citrix ADC valide le format de paquet de chaque requête et réponse DNS. Il peut également mettre en cache les réponses DNS. Vous pouvez appliquer des stratégies DNS aux services DNS.

Vous pouvez également utiliser le type de service UDP pour ces services. Toutefois, si vous le faites, l'appliance Citrix ADC peut uniquement effectuer l'équilibrage de charge de couche 4. Il ne peut pas prendre en charge les fonctionnalités spécifiques au DNS.

ANY

Utilisé pour les serveurs qui acceptent tout type de trafic TCP, UDP ou ICMP. Le paramètre ALY est utilisé principalement avec l'équilibrage de charge du pare-feu et l'équilibrage de charge de liaison.

SIP-UDP

Utilisé pour les serveurs qui acceptent le trafic SIP (Session Initiation Protocol) basé sur UDP. SIP initie, gère et met fin à des sessions de communication multimédia, et est devenu la norme pour la téléphonie Internet (VoIP).

Vous pouvez également utiliser le type de service UDP pour ces services. Toutefois, si vous le faites, l'appliance Citrix ADC effectue uniquement l'équilibrage de charge de couche 4. Il ne peut pas prendre en charge les fonctionnalités spécifiques au SIP.

DNS-TCP

Utilisé pour les serveurs qui acceptent le trafic DNS, où l'appliance Citrix ADC agit comme un proxy pour le trafic TCP envoyé aux serveurs DNS. Avec les services du type de service DNS-TCP, l'appliance Citrix ADC valide le format de paquet de chaque requête et réponse DNS et peut mettre en cache les réponses DNS, comme c'est le cas pour le type de service DNS.

Vous pouvez également utiliser le type de service TCP pour ces services. Toutefois, si vous le faites, l'appliance Citrix ADC effectue uniquement l'équilibrage de charge de couche 4 des serveurs de noms DNS externes. Il ne peut pas prendre en charge les fonctionnalités spécifiques au DNS.

RTSP

Utilisé pour les serveurs qui acceptent le trafic RTSP (Real Time Streaming Protocol). RTSP fournit des données multimédia et d'autres données en continu. Sélectionnez ce type pour prendre en charge l'audio, la vidéo et d'autres types de médias diffusés en continu.

Vous pouvez également utiliser le type de service TCP pour ces services. Toutefois, si vous le faites, l'appliance Citrix ADC effectue uniquement l'équilibrage de charge de couche 4. Il ne peut pas analyser le flux RTSP ni fournir la prise en charge de la persistance RTSPID ou du NAT RTSP.

DHCPRA

Utilisé pour les serveurs qui acceptent le trafic DHCP. Le type de service DHCPRA peut être utilisé pour relayer les demandes DHCP et les réponses entre les VLAN.

DIAMETER

Utilisé pour l'équilibrage de charge Trafic de Diameter entre plusieurs serveurs de Diameter. Diameter utilise l'équilibrage de charge basé sur les messages.

SSL_DIAMETER

Utilisé pour l'équilibrage de charge Trafic de Diameter sur SSL.

Les services sont désignés comme DISABLED jusqu'à ce que l'appliance Citrix ADC se connecte au serveur à équilibrage de charge associé et vérifie qu'il est opérationnel. À ce stade, le service est désigné comme étant « Enabled ». Par la suite, l'appliance Citrix ADC surveille périodiquement l'état des serveurs et place les sondes qui ne répondent pas aux sondes de surveillance (appelées vérifications d'intégrité) dans l'état DISABLED jusqu'à ce qu'elles répondent.

Remarque : Vous pouvez créer une plage de services à partir d'une seule commande CLI ou de la même boîte de dialogue. Les noms de la plage varient en fonction d'un nombre utilisé comme suffixe/préfixe. Par exemple, service1, service2, etc. À partir de l'utilitaire de configuration, vous pouvez spécifier une plage uniquement dans le dernier octet de l'adresse IP, qui est le quatrième dans le cas d'une adresse IPv4 et le huitième dans une adresse IPv6. À partir de la ligne de commande, vous pouvez spécifier la plage dans n'importe quel octet de l'adresse IP.

QUIC

Utilisé par les serveurs d'équilibrage de charge qui acceptent le trafic vidéo QUIC basé sur UDP. Le service permet à l'appliance Citrix ADC d'optimiser le trafic vidéo ABR chiffré via le protocole UDP.

Pour créer un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <name> <serverName> <serviceType> <port>

add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

Pour créer un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic**> **Équilibrage de charge**> **Services**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Créer un service, spécifiez les valeurs des paramètres suivants :

- Nom du service : nom
- serveur—Nom du serveur
- Protocole : Type de service
- port : port

4. Cliquez sur **Créer**, puis sur **Fermer**. Le service que vous avez créé apparaît dans le volet Services.

Création d'un serveur virtuel

Après avoir créé vos services, vous devez créer un serveur virtuel pour accepter le trafic pour les sites Web, applications ou serveurs équilibrés de charge. Une fois l'équilibrage de charge configuré, les utilisateurs se connectent au site Web, à l'application ou au serveur à équilibrage de charge via l'adresse IP ou le nom de domaine complet du serveur virtuel.

Remarque :

- Les noms de serveurs virtuels préfixés par « app_ » n'apparaissent pas dans l'interface graphique bien qu'ils soient présents dans le fichier ns.conf et s'affichent lorsque vous exécutez la commande show. Toutefois, les noms de serveurs virtuels préfixés par « app » sont affichés dans l'interface graphique.
- Le serveur virtuel est désigné comme étant DOWN jusqu'à ce que vous liez les services que vous lui avez créés et jusqu'à ce que l'appliance Citrix ADC se connecte à ces services et vérifie qu'ils sont opérationnels. Ce n'est qu'alors que le serveur virtuel est désigné comme UP.

Pour créer un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lb vserver <name> <serviceType> <ip> <port>
2
3 add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
4 <!--NeedCopy-->
```

Pour créer un serveur virtuel à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis créez un serveur virtuel.

Reliure des services au serveur virtuel

Remarque : Un service peut être lié à un maximum de 500 serveurs virtuels.

Après avoir créé des services et un serveur virtuel, vous devez lier les services au serveur virtuel. Habituellement, les services sont liés à des serveurs virtuels du même type, mais vous pouvez lier certains types de services à certains types différents de serveurs virtuels, comme illustré ci-dessous.

Type de serveur virtuel	Type de service	Commentaire
HTTP	SSL	Vous devez normalement lier un service SSL à un serveur virtuel HTTP pour effectuer le chiffrement.
SSL	HTTP	Vous devez normalement lier un service HTTP à un serveur virtuel SSL pour effectuer le déchargement SSL.
SSL_TCP	TCP	Vous devez normalement lier un service TCP à un serveur virtuel SSL_TCP pour effectuer le déchargement SSL pour d'autres TCP (déchiffrement SSL sans prise de conscience du contenu).

L'état des services liés à un serveur virtuel détermine l'état du serveur virtuel : si tous les services liés sont DOWN, le serveur virtuel est marqué DOWN, et si l'un des services liés est UP ou OUT OF SERVICE, l'état du serveur virtuel est UP.

Pour lier un service à un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb vserver <name> <serviceName>

bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```


Pour lier un service à un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic**> **Équilibrage de charge**> **Serveurs virtuels**, puis sélectionnez un serveur virtuel.
2. Cliquez dans la section **Service**, puis sélectionnez un service à lier.

Remarque : Vous pouvez lier un service à plusieurs serveurs virtuels.

Vérification de la configuration

Une fois votre configuration de base terminée, vous pouvez afficher les propriétés de chaque serveur virtuel d'équilibrage de charge et de service dans votre configuration d'équilibrage de charge pour vérifier que chacun est correctement configuré. Une fois la configuration en cours d'exécution, vous pouvez afficher les statistiques de chaque serveur virtuel d'équilibrage de charge et de service pour vérifier les problèmes éventuels.

Affichage des propriétés d'un objet serveur

Vous pouvez afficher des propriétés telles que le nom, l'état et l'adresse IP de n'importe quel objet serveur dans la configuration de votre appliance Citrix ADC.

Pour afficher les propriétés des objets serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show server <serverName>

show server server-1
<!--NeedCopy-->
```

Pour afficher les propriétés des objets serveur à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs**. Les valeurs des paramètres des serveurs disponibles apparaissent dans le volet d'informations.

Affichage des propriétés d'un serveur virtuel

Vous pouvez afficher des propriétés telles que le nom, l'état, l'état effectif, l'adresse IP, le port, le protocole, la méthode et le nombre de services liés pour vos serveurs virtuels. Si vous avez configuré

plus que les paramètres d'équilibrage de charge de base, vous pouvez afficher les paramètres de persistance de vos serveurs virtuels, les stratégies qui leur sont liées, ainsi que les serveurs virtuels de redirection de cache et de commutation de contenu liés aux serveurs virtuels.

Pour afficher les propriétés d'un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show lb vserver <name>

show lb vserver Vserver-LB-1
<!--NeedCopy-->
```

Pour afficher les propriétés d'un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur un serveur virtuel pour afficher ses propriétés en bas du volet d'informations.
3. Pour afficher les serveurs virtuels de redirection du cache et de commutation de contenu liés à ce serveur virtuel, cliquez sur **Afficher les liaisons CS/CR**.

Affichage des propriétés d'un service

Vous pouvez afficher le nom, l'état, l'adresse IP, le port, le protocole, la connexion client maximale, le nombre maximal de demandes par connexion et le type de serveur des services configurés, et utiliser ces informations pour résoudre toute erreur dans la configuration du service.

Pour afficher les propriétés des services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show service <name>

show service Service-HTTP-1
<!--NeedCopy-->
```


Pour afficher les propriétés des services à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**. Les détails des services disponibles apparaissent dans le volet Services.

Affichage des liaisons d'un service

Vous pouvez afficher la liste des serveurs virtuels auxquels le service est lié. Les informations de liaison fournissent également le nom, l'adresse IP, le port et l'état des serveurs virtuels auxquels les services sont liés. Vous pouvez utiliser les informations de liaison pour résoudre tout problème lié à la liaison des services aux serveurs virtuels.

Pour afficher les liaisons d'un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show service bindings <name>

show service bindings Service-HTTP-1
<!--NeedCopy-->
```

Pour afficher les liaisons d'un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Dans le volet d'informations, sélectionnez le service dont vous souhaitez afficher les informations de liaison.
3. Dans l'onglet **Action**, cliquez sur **Afficher les liaisons** .

Affichage des statistiques d'un serveur virtuel

Pour évaluer les performances des serveurs virtuels ou pour résoudre les problèmes, vous pouvez afficher les détails des serveurs virtuels configurés sur l'appliance Citrix ADC. Vous pouvez afficher un résumé des statistiques pour tous les serveurs virtuels ou spécifier le nom d'un serveur virtuel pour afficher les statistiques uniquement pour ce serveur virtuel. Vous pouvez afficher les détails suivants :

- Nom
- Adresse IP
- Port
- Protocole
- État du serveur virtuel

- Taux de demandes reçues
- Taux de succès

Pour afficher les statistiques du serveur virtuel à l'aide de l'interface de ligne de commande

Pour afficher un résumé des statistiques de tous les serveurs virtuels actuellement configurés sur l'appliance, ou pour un seul serveur virtuel, à l'invite de commandes, tapez :

```
stat lb vserver [`<name>`]
<!--NeedCopy-->
```

Exemple :

```
stat lb vserver server-1
<!--NeedCopy-->
```

La figure suivante présente un exemple de statistique.


```
> stat lbvserver
[
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
vserver1        10.102.20.200    80          SSL         DOWN      0/s

lb1               203.1.113.5   443         DTLS         DOWN      0/s

vicap                       *     0          TCP         DOWN      0/s

lbicap                2.2.3.4  1344          TCP         DOWN      0/s

app_...stest          0.0.0.0     0         HTTP         DOWN      0/s

app_...ttest          0.0.0.0     0         HTTP         DOWN      0/s

app_...fault          0.0.0.0     0         HTTP         DOWN      0/s

app_...test1          0.0.0.0     0         HTTP         DOWN      0/s

app_...1test          0.0.0.0     0         HTTP         DOWN      0/s

app_...fault          0.0.0.0     0         HTTP         DOWN      0/s

app_...est12          0.0.0.0     0         HTTP         DOWN      0/s

app_...sting          0.0.0.0     0         HTTP         DOWN      0/s

test                  2.2.2.2    80         HTTP         DOWN      0/s

shar...lt-lb          0.0.0.0     0         HTTP         DOWN      0/s

shar...es-lb          0.0.0.0     0         HTTP           UP      0/s

shar...es-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...ts-lb          0.0.0.0     0         HTTP           UP      0/s

shar...ns-lb          0.0.0.0     0         HTTP           UP      0/s

shar...as-lb          0.0.0.0     0         HTTP           UP      0/s

forward-vs            0.0.0.0     0          TCP         DOWN      0/s

tcpcs                 0.0.0.0     0          TCP         DOWN      0/s

test124               0.0.0.0     0          SSL         DOWN      0/s

testssl               0.0.0.0     0          SSL         DOWN      0/s
```


Pour afficher les statistiques du serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Si vous souhaitez afficher les statistiques d'un seul serveur virtuel, dans le volet d'informations, sélectionnez le serveur virtuel dont vous souhaitez afficher les statistiques.
3. Dans le volet d'informations, cliquez sur **Statistiques**.

Affichage des statistiques d'un service

Vous pouvez afficher le taux de demandes, de réponses, d'octets de demande, d'octets de réponse, de connexions client actuelles, de demandes dans la file d'attente de surtension, de connexions au serveur en cours, etc. à l'aide des statistiques de service.

Pour afficher les statistiques d'un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat service <name>
<!--NeedCopy-->
```

Exemple :

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Pour afficher les statistiques d'un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Dans le volet d'informations, sélectionnez le service dont vous souhaitez afficher les statistiques (par exemple, Service-HTTP-1).
3. Cliquez sur **Statistiques**. Les statistiques apparaissent dans une nouvelle fenêtre.

Équilibrer la charge du serveur virtuel et des états de service

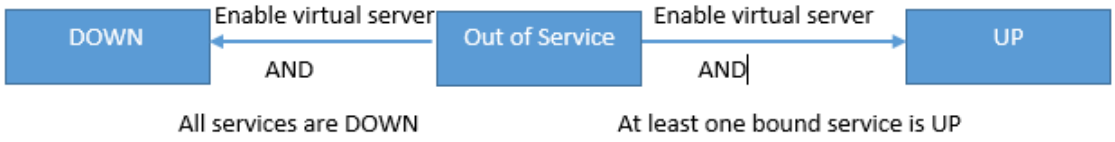
August 20, 2021

Un serveur virtuel d'équilibrage de charge qui ne possède pas de serveur virtuel de sauvegarde peut prendre les états suivants, en fonction de l'état des services qui y sont liés et de sa désactivation administrative :

- **UP** : Au moins un des services liés au serveur virtuel est UP.
- **DOWN** : tous les services liés au serveur virtuel sont DOWN, ou la fonctionnalité d'équilibrage de charge n'est pas activée.
- **Out of Service (OFS)** : Si vous désactivez administrativement le serveur virtuel, il entre dans l'état OFS mais son état effectif est DOWN. L'administrateur peut contrôler la transition vers l'état OFS à partir de l'état DOWN ou UP, ou vers l'état DOWN ou UP à partir de l'état OFS.

L'état et l'état effectif d'un serveur virtuel sont les mêmes si un serveur virtuel de sauvegarde n'est pas configuré. Toutefois, si un serveur virtuel de sauvegarde ou une chaîne de serveurs virtuels de sauvegarde est configuré, l'état effectif est dérivé des états des services liés au serveur virtuel principal et aux serveurs virtuels de sauvegarde. Si l'un des serveurs virtuels de sauvegarde de la chaîne est UP, l'état effectif du serveur virtuel principal est UP, même si tous les services liés au serveur virtuel principal sont DOWN.

Les diagrammes suivants montrent les conditions dans lesquelles un serveur virtuel passe d'un état à un autre.



Un service peut prendre les états suivants :

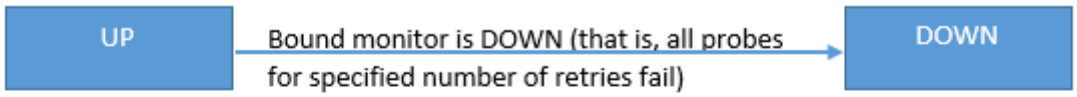
- **UP :** Si les sondes de tous les moniteurs liés au service réussissent.
- **DOWN** : Si les sondes de surveillance vers le service ne sont pas répondues dans le délai configuré.

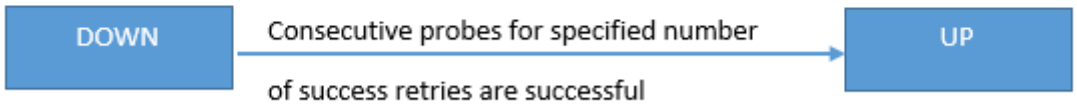
- **OUT OF SERVICE** : si vous désactivez administrativement le service, ou si vous arrêtez correctement le service et qu'il n'y a pas de transactions actives sur le service
- **GOING OUT OF SERVICE (TROFS)** : Si vous désactivez administrativement le service avec un délai, ou si vous arrêtez gracieusement le service et qu'il y a des transactions actives sur le service. Pour plus d'informations, voir Arrêt gracieux des services.
- **ARRÊT EN CAS DE SORTIE DU SERVICE (TROFS_DOWN)[]** Une sonde de surveillance échoue alors que le service est dans l'état « OUT OF SERVICE ».

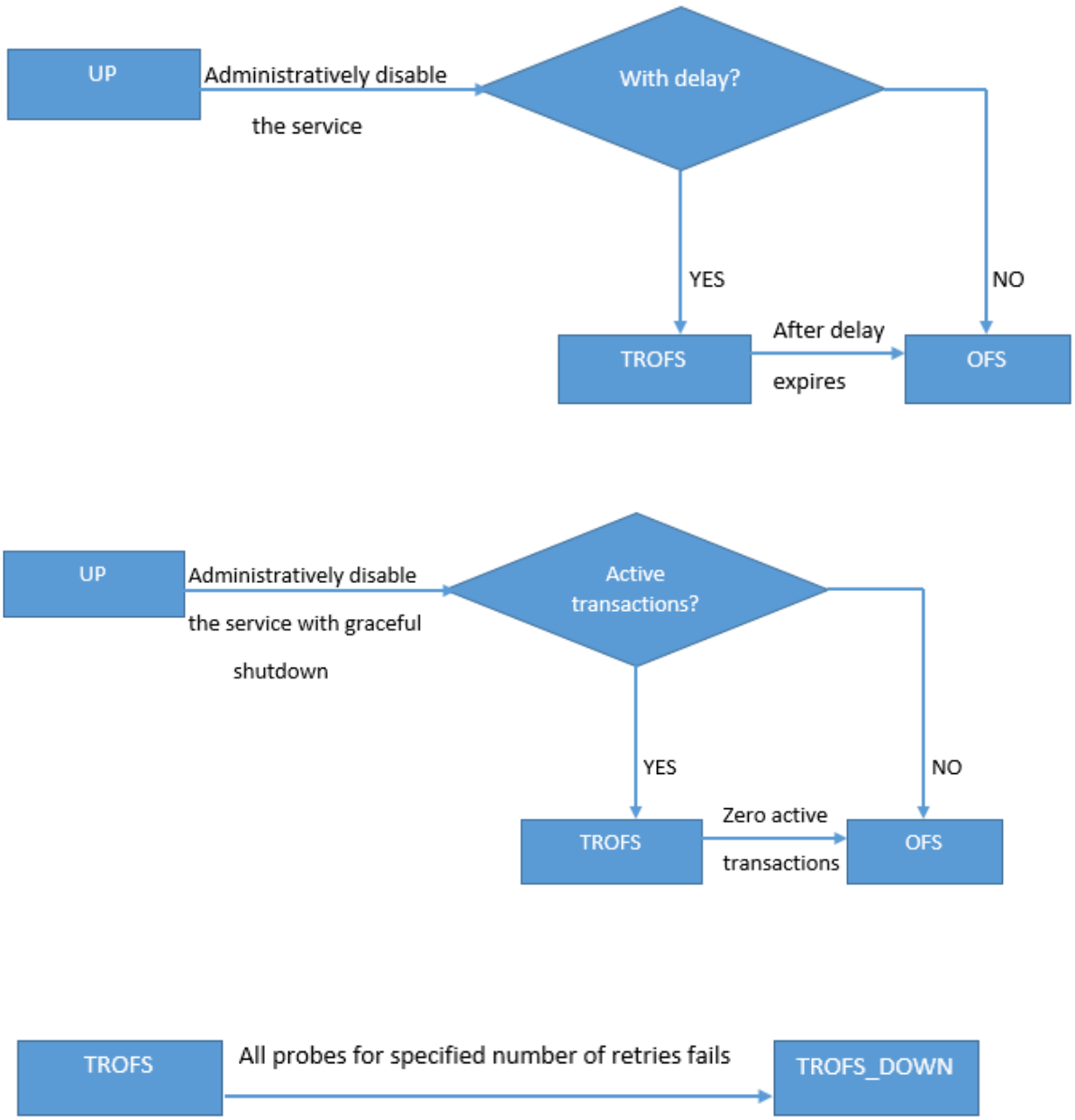
Un service en cours de transition de UP à OFS est dans l'état OUT DU SERVICE. Un service faisant la transition de DOWN à OFS est dans l'état DOWN WHEN GOING OUT OF SERVICE. Par exemple, si un service est DOWN et que vous le désactivez avec un délai, le service passe à DOWN WHEN GOING OUT OF SERVICE, puis à l'état OUT OF SERVICE. Si un service est OUT et que vous le désactivez avec un délai, le service passe à OUT DE SERVICE. Pendant ce temps, si une sonde de surveillance sur le serveur échoue, le service passe à DOWN WHEN GOING OUT OF SERVICE et, après l'expiration du délai, passe à l'état OFS.

> **Remarque**
>
> Vous pouvez configurer le débordement sur un serveur virtuel de sauvegarde en définissant le paramètre « HealthThreshold » sur une valeur positive non nulle. Ensuite, si un service unique lié au serveur virtuel principal passe à l'état DOWN lorsque vous sortez du service et que le seuil d'intégrité n'est pas atteint, le serveur virtuel principal est marqué « DOWN » et les nouvelles connexions sont dirigées vers le serveur virtuel de sauvegarde.

Les diagrammes suivants montrent les conditions dans lesquelles un service passe d'un état à un autre.







Prise en charge du profil d'équilibrage de charge

August 20, 2021

Une configuration d'équilibrage de charge comporte de nombreux paramètres, de sorte que la définition des mêmes paramètres sur plusieurs serveurs virtuels peut devenir fastidieuse. À partir de la

version 11.1, un profil d'équilibrage de charge (LB) facilite cette tâche. Vous pouvez désormais définir des paramètres d'équilibrage de charge dans un profil et associer ce profil à des serveurs virtuels, au lieu de définir ces paramètres sur chaque serveur virtuel.

Les paramètres suivants sont actuellement pris en charge dans un profil LB :

- `HTTPonlyflag`: incluez l'attribut HttpOnly dans les cookies de persistance. L'attribut HttpOnly limite la portée d'un cookie aux requêtes HTTP et contribue à atténuer le risque d'attaques par script intersite.
- UseSecuredPersistenceCookie : chiffrez les valeurs des cookie de persistance à l'aide de l'algorithme de hachage SHA2.
- `Cookiepassphrase`: spécifiez la phrase secrète utilisée pour générer une valeur de cookie de persistance sécurisée.
- DBS_LB : activez l'équilibrage de charge spécifique à la base de données pour les types de service MySQL et MSSQL.
- cl_process_local—Les paquets destinés à un serveur virtuel dans un cluster ne sont pas dirigés. Activez l'option pour le mode de réponse à une demande de paquet unique ou lorsque le périphérique amont exécute un RSS approprié pour la distribution basée sur la connexion.
- LBHashalgorithm : spécifiez l'algorithme de hachage à utiliser pour les méthodes d'équilibrage de charge basées sur le hachage suivantes :
  - Méthode de hachage d'URL
  - Méthode de hachage de domaine
  - Méthode de hachage IP de destination
  - Méthode de hachage IP source
  - Méthode de hachage IP de destination IP source
  - Méthode de hachage du port source IP source
  - Méthode de hachage d'ID d'appel
  - Méthode de jeton

  Valeurs possibles : DEFAULT, PRAC, JARH Valeur
  par défaut : DEFAULT
- LBHashfingers : spécifiez le nombre de doigts à utiliser dans les algorithmes PRAC et JARH pour les méthodes LB basées sur le hachage. L'augmentation du nombre de doigts permet une meilleure répartition du trafic au détriment de la mémoire supplémentaire.

Valeur par défaut : 256 Valeur
minimale : 1 Valeur
maximale : 1024

> **Remarque**
>
> Vous pouvez définir les paramètres DBS_LB et CL_Process_Local sur un serveur virtuel et dans le profil. Si vous activez ces paramètres sur un serveur virtuel, puis que vous définissez un profil sur ce serveur virtuel, les paramètres apparaissent comme désactivés dans la sortie de la "show lb vserver" commande de ce serveur virtuel. Vérifiez le profil pour voir l'état réel de ces paramètres. En outre, si vous définissez puis désactivez un profil sur un serveur virtuel, les paramètres sont définis avec les valeurs par défaut pour ce serveur virtuel.

Pour créer un profil LB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb profile <lbprofilename> -dbsLb ( ENABLED | DISABLED ) -
    processLocal ( ENABLED | DISABLED ) -httpOnlyCookieFlag ( ENABLED |
    DISABLED ) -cookiePassphrase -useSecuredPersistenceCookie ( ENABLED
    | DISABLED ) -lbHashAlgorithm <lbHashAlgorithm> -lbHashFingers <
    positive_integer>
<!--NeedCopy-->
```

Exemple :

```
> sh lb profile p1
LB Profile name:  p1
DBS LB : DISABLED   Process Local: DISABLED
Persistence Cookie HttpOnly Flag: ENABLED
Use Encrypted Persistence Cookie: DISABLED
No of vservers bound: 0
Store MQTT clientid and username in transactional logs: NO
Hash LB algorithm used in LB decision: DEFAULT
Number of fingers for Hash LB algorithm: 256
Done

<!--NeedCopy-->
```

Pour créer un profil LB à l'aide de l'interface graphique

Accédez à **Système** > **Profils** > **Profil LB**, puis ajoutez un profil.

Pour associer un profil LB à un serveur virtuel LB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set lb vserver <name> -lbprofilename <string>
<!--NeedCopy-->
```

Exemple

```
set lbvserver lbvip1 -lbprofile p1

Done

sh lb vserver lbvip1

lbvip1 (203.0.113.1:80) - HTTP       Type: ADDRESS
State: UP
Last state change was at Wed May 25 12:36:20 2016
Time since last state change: 0 days, 00:01:26.140
Effective State: UP  ARP:DISABLED
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Appflow logging: ENABLED
Port Rewrite : DISABLED
No. of Bound Services :  2 (Total)       2 (Active)
Configured Method: LEASTCONNECTION      BackupMethod: ROUNDROBIN
Mode: IP
Persistence: NONE
Vserver IP and Port insertion: OFF
Push: DISABLED  Push VServer:
Push Multi Clients: NO
Push Label Rule: none
L2Conn: OFF
Skip Persistency: None
Listen Policy: NONE
IcmpResponse: PASSIVE
RHIstate: PASSIVE
New Service Startup Request Rate: 0 PER_SECOND, Increment Interval: 0
Mac mode Retain Vlan: DISABLED
DBS_LB: DISABLED
Process Local: DISABLED
Traffic Domain: 0
LB Profile: p1
Done
<!--NeedCopy-->
```


Pour associer un profil LB à un serveur virtuel LB à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Sélectionnez un serveur virtuel, puis cliquez sur **Modifier**.
3. Dans **Paramètres avancés**, cliquez sur **Profils**.
4. Dans la liste **Profil LB**, sélectionnez le profil à associer à ce serveur virtuel.

Algorithmes d'équilibrage de charge

August 20, 2021

L'algorithme d'équilibrage de charge définit les critères utilisés par l'appliance Citrix ADC pour sélectionner le service vers lequel rediriger chaque demande client. Différents algorithmes d'équilibrage de charge utilisent des critères différents. Par exemple, l'algorithme de connexion le moins sélectionne le service avec le moins de connexions actives, tandis que l'algorithme d'arrondis gère une file d'attente en cours d'exécution de services actifs, distribue chaque connexion au service suivant de la file d'attente, puis envoie ce service à la fin de la file d'attente.

Certains algorithmes d'équilibrage de charge sont les mieux adaptés à la gestion du trafic sur les sites Web, d'autres à la gestion du trafic vers les serveurs DNS et d'autres à la gestion d'applications Web complexes utilisées dans le commerce électronique ou sur les réseaux locaux ou les réseaux locaux d'entreprise. Le tableau suivant répertorie chaque algorithme d'équilibrage de charge pris en charge par l'appliance Citrix ADC, avec une brève description de son fonctionnement.

Nom	Sélection du serveur basée sur
LEASTCONNECTION	Quel service a actuellement le moins de connexions client. Il s'agit de l'algorithme d'équilibrage de charge par défaut.
ROUNDROBIN	Quel service est en haut d'une liste de services. Une fois que ce service est sélectionné pour une connexion, il se déplace au bas de la liste.
LEASTRESPONSETIME	Quel serveur équilibré de charge a actuellement le temps de réponse le plus rapide.
URLHASH	Un hachage de l'URL de destination.
DOMAINHASH	Un hachage du domaine de destination.
DESTINATIONIPHASH	Un hachage de l'adresse IP de destination.
SOURCEIPHASH	Un hachage de l'adresse IP source.

Nom	Sélection du serveur basée sur
SRCIPDESTIPHASH	Un hachage des adresses IP source et de destination.
CALLIDHASH	Un hachage de l'ID d'appel dans l'en-tête SIP.
SRCIPSRCPORTHASH	Un hachage de l'adresse IP et du port du client.
LEASTBANDWIDTH	Quel service a actuellement le moins de contraintes de bande passante.
LEASTPACKETS	Quel service reçoit actuellement le moins de paquets.
CUSTOMLOAD	Données provenant d'un moniteur de charge.
TOKEN	Le jeton configuré.
LRTM	Le nombre de connexions actives est faible et le temps de réponse moyen le plus faible.

Selon le protocole du service selon lequel il s'agit d'équilibrage de charge, l'appliance Citrix ADC configure chaque connexion entre le client et le serveur de manière à durer pendant un intervalle de temps différent. Ceci est appelé granularité d'équilibrage de charge, qui sont trois types : la granularité basée sur la demande, la connexion et la granularité basée sur le temps. Le tableau suivant décrit chaque type de granularité et le moment où chacun est utilisé.

Granularité	Types de service équilibré de charge	Spécifie
Sur la base de la demande	HTTP ou HTTPS	Un nouveau service est choisi pour chaque requête HTTP, indépendamment des connexions TCP. Comme pour toutes les requêtes HTTP, une fois que le serveur Web a rempli la demande, la connexion est fermée.

Granularité	Types de service équilibré de charge	Spécifie
Basé sur la connexion	Protocoles TCP et TCP autres que HTTP	Un service est choisi pour chaque nouvelle connexion TCP. La connexion persiste jusqu'à ce qu'elle soit interrompue par le service ou le client.
Basé sur le temps	UDP et autres protocoles IP	Un nouveau service est choisi pour chaque paquet UDP. Lors de la sélection d'un service, une session est créée entre le service et un client pendant une période spécifiée. Lorsque le temps expire, la session est supprimée et un nouveau service est choisi pour les paquets supplémentaires, même si ces paquets proviennent du même client.

Lors du démarrage d'un serveur virtuel ou à chaque fois que l'état d'un serveur virtuel change, le serveur virtuel peut initialement utiliser la méthode round robin pour distribuer les requêtes client entre les serveurs physiques. Ce type de distribution, appelé *startup round robin,* permet d'éviter toute charge inutile sur un serveur unique lorsque les requêtes initiales sont traitées. Après avoir utilisé la méthode round robin au démarrage, le serveur virtuel bascule vers la méthode d'équilibrage de charge spécifiée sur le serveur virtuel.

Le facteur RR de démarrage fonctionne de la manière suivante :

- Si le facteur RR de démarrage est défini sur zéro, l'appliance passe à la méthode d'équilibrage de charge spécifiée en fonction du taux de demande.
- Si le facteur RR de démarrage est différent de zéro, l'appliance utilise la méthode round robin pour le nombre de requêtes spécifié avant de passer à la méthode d'équilibrage de charge spécifiée.
- Par défaut, le facteur RR de démarrage est défini sur zéro.

Remarque : vous ne pouvez pas définir le facteur RR de démarrage pour un serveur virtuel individuel. La valeur que vous spécifiez s'applique à tous les serveurs virtuels de l'appliance Citrix ADC.

Pour définir le facteur d'arrondis de démarrage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb parameter -startupRRFactor <positive_integer>
```

Exemple

```
set lb parameter -startupRRFactor 25000
```

Pour définir le facteur de démarrage à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge**et définissez le facteur RR de démarrage.

Méthode de connexion minimale

August 20, 2021

Lorsqu'un serveur virtuel est configuré pour utiliser l'algorithme d'équilibrage de charge de connexion le moins important (ou méthode), il sélectionne le service avec le moins de connexions actives. Il s'agit de la méthode par défaut, car, dans la plupart des cas, elle fournit les meilleures performances.

Pour les services TCP, HTTP, HTTPS et SSL_TCP, l'appliance Citrix ADC inclut les types de connexion suivants dans sa liste de connexions existantes :

- **Connexions actives à un service.** Connexions représentant les demandes qu'un client a envoyées au serveur virtuel et que le serveur virtuel a transférées à un service. Pour les services HTTP et HTTPS, les connexions actives représentent uniquement les requêtes HTTP ou HTTPS qui n'ont pas encore reçu de réponse.
- **Connexions en attente dans la file d'attente de surtension.** Toutes les connexions au serveur virtuel qui sont en attente dans une file d'attente de surtension et qui n'ont pas encore été transférées à un service. Les connexions peuvent s'accumuler dans la file d'attente de surtension à tout moment, pour l'une des raisons suivantes :
  - Vos services ont des limites de connexion, et tous les services de votre configuration d'équilibrage de charge sont à cette limite.
  - La fonction de protection contre les surtensions est configurée et a été activée par une surtension des demandes adressées au serveur virtuel.
  - Le serveur à équilibrage de charge a atteint une limite interne et n'ouvre donc aucune nouvelle connexion. (Par exemple, la limite de connexion d'un serveur Apache est atteinte.)

Lorsqu'un serveur virtuel utilise la méthode de connexion minimale, il considère les connexions en attente comme appartenant au service spécifique. Par conséquent, il n'ouvre pas de nouvelles connexions à ces services.

Pour les services UDP, les connexions considérées par l'algorithme de connexion le moins important incluent toutes les sessions entre le client et un service. Ces sessions sont des entités logiques basées sur le temps. Lorsque le premier paquet UDP d'une session arrive, l'appliance Citrix ADC crée une session entre l'adresse IP et le port source et l'adresse IP et le port de destination.

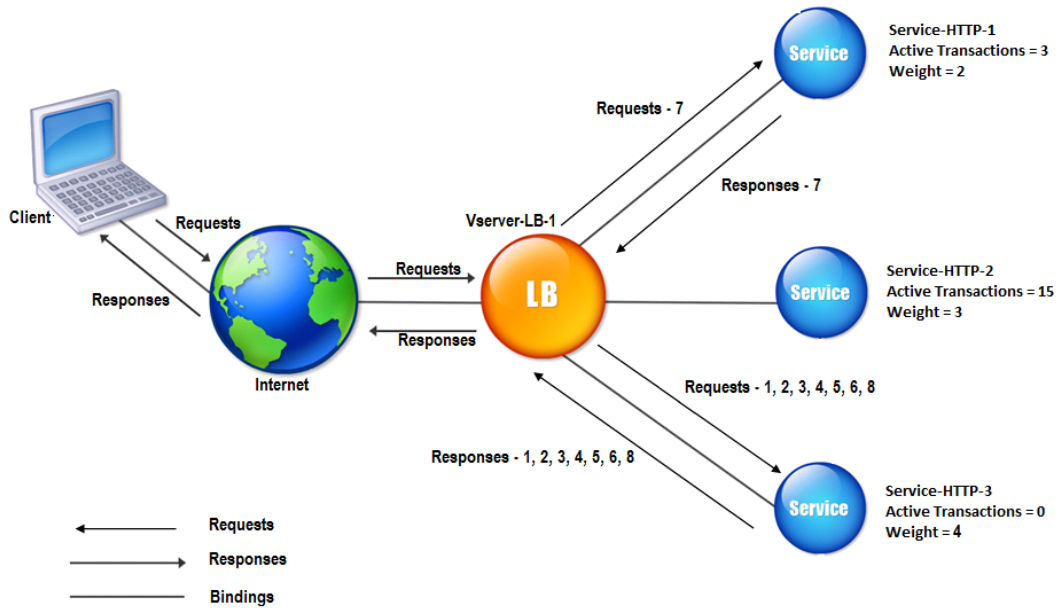
Pour les connexions RTSP (Real-Time Streaming Protocol), l'appliance Citrix ADC utilise le nombre de connexions de contrôle actif pour déterminer le nombre le plus faible de connexions à un service RTSP.

L'exemple suivant montre comment un serveur virtuel sélectionne un service pour l'équilibrage de charge à l'aide de la méthode de connexion minimale. Considérez les trois services suivants :

- Service-HTTP-1 gère 3 transactions actives.
- Service-HTTP-2 gère 15 transactions actives.
- Service-HTTP-3 ne gère aucune transaction active.

Le diagramme suivant illustre la manière dont l'appliance Citrix ADC transmet les demandes entrantes lors de l'utilisation de la méthode de connexion minimale.

Figure 1. Mécanisme de la méthode d'équilibrage de charge des connexions moindres



Dans ce diagramme, le serveur virtuel sélectionne le service pour chaque connexion entrante en choisissant le serveur avec le moins de transactions actives.

Les connexions sont transférées comme suit :

- Service-HTTP-3 reçoit la première requête, car il ne gère aucune transaction active.

  Note : Le service sans mouvement actif est sélectionné en premier.

- Service-HTTP-3 reçoit les deuxième et troisième requêtes parce que le service a le plus petit nombre de transactions actives.
- Service-HTTP-1 reçoit la quatrième demande car Service-HTTP-1 et Service-HTTP-3 ont le même nombre de transactions actives, le serveur virtuel utilise la méthode Round Robin pour choisir entre elles.
- Service-HTTP-3 reçoit la cinquième requête.
- Service-HTTP-1 reçoit la sixième requête, et ainsi de suite, jusqu'à ce que Service-HTTP-1 et Service-HTTP-3 traitent le même nombre de requêtes que Service-HTTP-2. Ensuite, l'appliance Citrix ADC commence à transférer les demandes vers Service-HTTP-2 lorsqu'il s'agit du service le moins chargé ou que son tour arrive dans la file d'attente ronde.

  Remarque : si les connexions à Service-HTTP-2 se ferment, il peut obtenir de nouvelles connexions avant que chacun des deux autres services ait 15 transactions actives.

Le tableau suivant explique comment les connexions sont distribuées dans la configuration d'équilibrage de charge à trois services décrite précédemment.

Connexion entrante	Service sélectionné	Nombre actuel de connexions actives	Remarques
Request-1	Service-HTTP-3 ; (N = 0)	1	Service-HTTP-3 a le moins de connexions actives.
Request-2	Service-HTTP-3 ; (N = 1)	2	Service-HTTP-3 a le moins de connexions actives.
Request-3	Service-HTTP-3; (N = 2)	3	-
Request-4	Service-HTTP-1; (N = 3)	4	Service-HTTP-1 et Service-HTTP-3 ont le même nombre de connexions actives.
Request-5	Service-HTTP-3; (N = 3)	4	Service-HTTP-1 et Service-HTTP-3 ont le même nombre de connexions actives.

Connexion entrante	Service sélectionné	Nombre actuel de connexions actives	Remarques
Request-6	Service-HTTP-1 ; (N = 4)	5	-
Request-7	Service-HTTP-3; (N = 4)	5	-
Request-8	Service-HTTP-1 ; (N = 5)	6	-

Service-HTTP-2 est sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives et que les connexions en cours se ferment, ou lorsque les autres services (Service-HTTP-1 et Service-HTTP-3) ont chacun 15 connexions ou plus.

L'appliance Citrix ADC peut également utiliser la méthode de connexion la moins adaptée lorsque des pondérations sont attribuées aux services. Il sélectionne un service en utilisant la valeur (Nw) de l'expression suivante :

Nw = (Nombre de transactions actives) * (10000/poids)

L'exemple suivant montre comment l'appliance Citrix ADC sélectionne un service pour l'équilibrage de charge à l'aide de la méthode de connexion la moins élevée lorsque des pondérations sont affectées aux services. Dans l'exemple précédent, supposons que Service-HTTP-1 se voit attribuer un poids de 2, Service-HTTP-2 se voit attribuer un poids de 3 et Service-HTTP-3 un poids de 4. Les connexions sont transférées comme suit :

- Service-HTTP-3 reçoit le premier car le service ne gère aucune transaction active.

  Remarque : Si les services ne gèrent aucune transaction active, l'appliance Citrix ADC utilise la méthode ronde, indépendamment des poids attribués à chacun des services.

- Service-HTTP-3 reçoit les deuxième, troisième, quatrième, cinquième, sixième et septième demandes car le service a la valeur Nw la plus faible.
- Service-HTTP-1 reçoit la huitième requête. Étant donné que Service-HTTP-1 et Service-HTTP-3 ont désormais la même valeur Nw, l'appliance effectue un équilibrage de charge de manière ronde. Par conséquent, Service-HTTP-3 reçoit la neuvième requête.

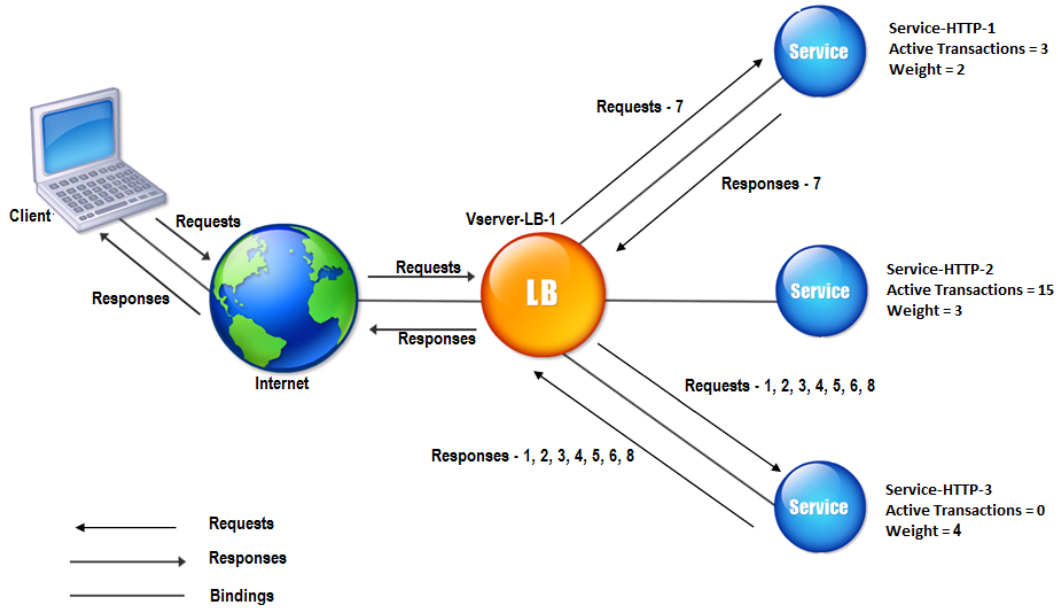
Le tableau suivant explique comment les connexions sont distribuées sur la configuration d'équilibrage de charge à trois services décrite précédemment.

Demande reçue	Service sélectionné	Nw actuel (nombre de transactions actives) * (10000/ poids) valeur	Remarques
Request-1	Service-HTTP-3; (Nw = 0)	Nw = 2500	Service-HTTP-3 a la valeur Nw la plus faible.
Request-2	Service-HTTP-3 ; (Nw = 2500)	Nw= 5000	
Request-3	Service-HTTP-3; (Nw = 5000)	Nw= 7500	
Request-4	Service-HTTP-3; (Nw = 7500)	Nw= 10000	
Request-5	Service-HTTP-3; (Nw = 10000)	Nw= 12500	
Request-6	Service-HTTP-3; (Nw = 12500)	Nw= 15000	
Request-7	Service-HTTP-1; (Nw = 15000)	Nw= 20000	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs Nw
Request-8	Service-HTTP-3; (Nw = 15000)	Nw= 17500	

Service-HTTP-2 est sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives ou lorsque la valeur Nw des autres services (Service-HTTP-1 et Service-HTTP-3) est égale à 50000.

Le diagramme suivant illustre comment l'appliance Citrix ADC utilise la méthode de connexion la moins adaptée lorsque des pondérations sont attribuées aux services.

Figure 2. Mécanisme de la méthode d'équilibrage de charge des connexions moindres lorsque des poids sont affectés



Pour configurer la méthode de connexion la plus faible, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

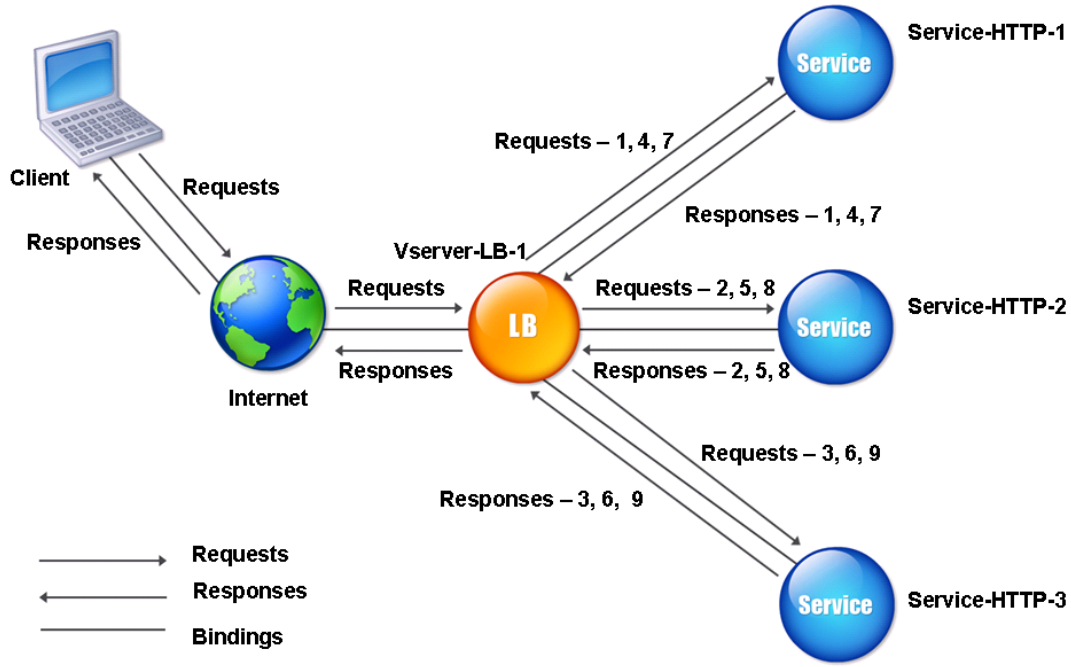
Méthode Round Robin

August 20, 2021

Lorsqu'un serveur virtuel d'équilibrage de charge est configuré pour utiliser la méthode round robin, il fait pivoter en permanence une liste des services qui lui sont liés. Lorsque le serveur virtuel reçoit une demande, il affecte la connexion au premier service de la liste, puis déplace ce service au bas de la liste.

Le diagramme suivant illustre comment l'appliance Citrix ADC utilise la méthode round robin avec une configuration d'équilibrage de charge qui contient trois serveurs équilibrés de charge et leurs services associés.

Figure 1. Fonctionnement de la méthode d'équilibrage de charge Round Robin



Si vous attribuez une pondération différente à chaque service, l'appliance Citrix ADC effectue la distribution ronde pondérée des connexions entrantes. Pour ce faire, il saute les services moins pondérés à des intervalles appropriés.

Par exemple, supposons que vous avez une configuration d'équilibrage de charge avec trois services. Vous définissez Service-HTTP-1 sur un poids de 2, Service-HTTP-2 sur un poids de 3 et Service-HTTP-3 sur un poids de 4. Les services sont liés à vServer-lb-1, qui est configuré pour utiliser la méthode round robin. Avec cette configuration, les demandes entrantes sont livrées comme suit :

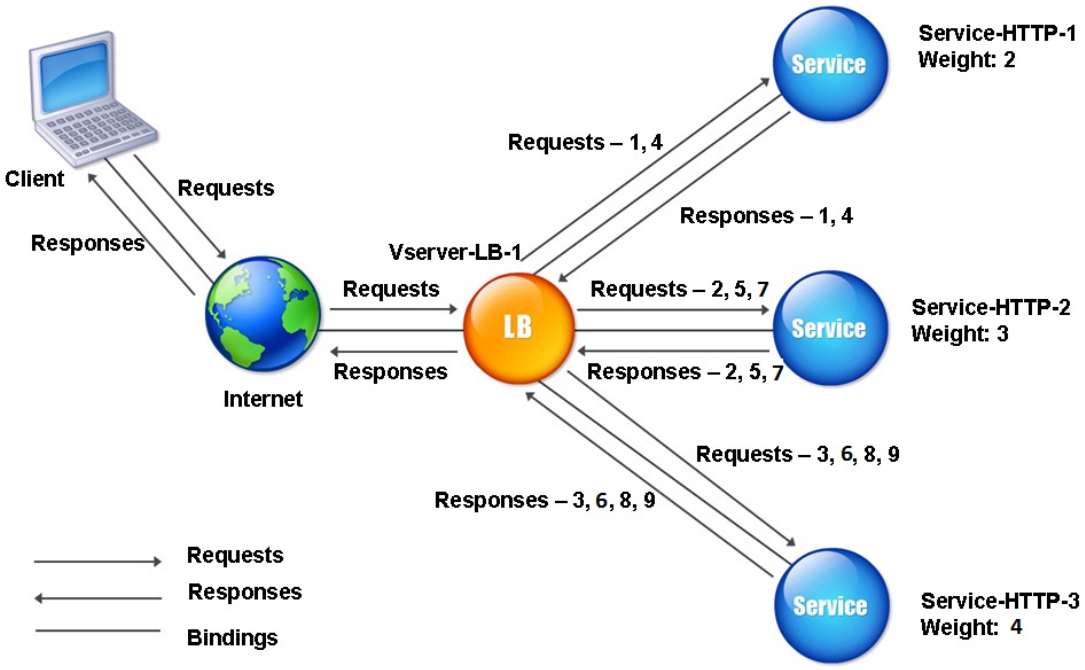
- Service-HTTP-1 reçoit la première requête.
- Service-HTTP-2 reçoit la deuxième requête.
- Service-HTTP-3 reçoit la troisième requête.
- Service-HTTP-1 reçoit la quatrième requête.
- Service-HTTP-2 reçoit la cinquième requête.
- Service-HTTP-3 reçoit la sixième requête.
- Service-HTTP-2 reçoit la septième requête.
- Service-HTTP-3 reçoit à la fois les huitième et neuvième requêtes.

Remarque : Vous pouvez également configurer des pondérations sur les services pour empêcher plusieurs services d'utiliser le même serveur et de surcharger le serveur.

Un nouveau cycle commence alors, en utilisant le même modèle.

Le diagramme suivant illustre la méthode pondérée des robin.

Figure 2. Comment la méthode d'équilibrage de charge Round Robin prend en charge les services pondérés



Pour configurer la méthode ronde, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode du temps de réponse le plus faible

August 20, 2021

Lorsque le serveur virtuel d'équilibrage de charge est configuré pour utiliser la méthode de temps de réponse le moins élevé, il sélectionne le service avec le moins de connexions actives et le plus faible temps de réponse moyen. Vous pouvez configurer cette méthode uniquement pour les serveurs virtuels d'équilibrage de charge HTTP et SSL (Secure Sockets Layer). Le temps de réponse (également appelé Time to First Byte, ou TTFB) est l'intervalle de temps entre l'envoi d'un paquet de requête à un

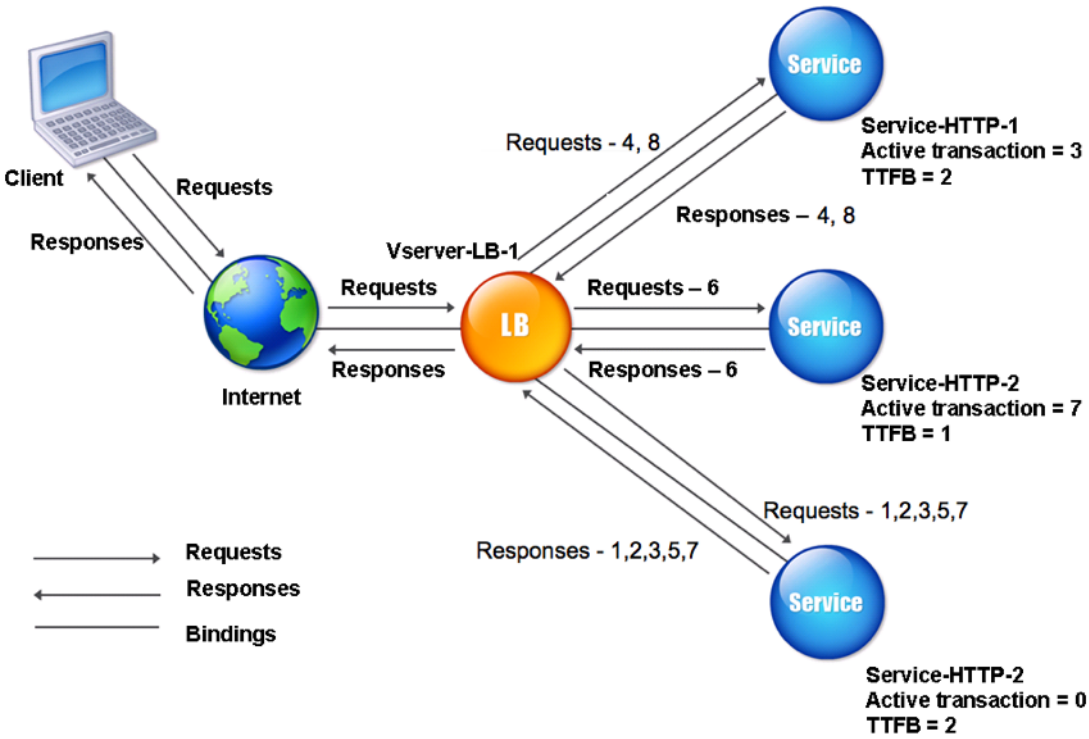
service et la réception du premier paquet de réponse du service. L'appliance Citrix ADC utilise le code de réponse 200 pour calculer le TTFB.

L'exemple suivant montre comment un serveur virtuel sélectionne un service pour l'équilibrage de charge à l'aide de la méthode du temps de réponse le plus faible. Considérez les trois services suivants :

- Service-HTTP-1 gère trois transactions actives et TTFB est de deux secondes.
- Service-HTTP-2 gère sept transactions actives et TTFB est une seconde.
- Service-HTTP-3 ne gère aucune transaction active et TTFB est de deux secondes.

Le diagramme suivant illustre la façon dont l'appliance Citrix ADC utilise la méthode de temps de réponse le plus faible pour transférer les connexions.

Figure 1. Fonctionnement de la méthode d'équilibrage de charge au moindre temps de réponse



Le serveur virtuel sélectionne un service en multipliant le nombre de transactions actives par le TTFB pour chaque service, puis en sélectionnant le service avec le résultat le plus bas. Pour l'exemple illustré ci-dessus, le serveur virtuel transmet les demandes comme suit :

- Service-HTTP-3 reçoit la première demande, car le service ne gère aucune transaction active.
- Service-HTTP-3 reçoit également les deuxième et troisième demandes, car le résultat est le plus bas des trois services.

- Service-HTTP-1 reçoit la quatrième requête. Étant donné que Service-HTTP-1 et Service-HTTP-3 ont le même résultat, l'appliance Citrix ADC choisit entre eux en appliquant la méthode Round Robin.
- Service-HTTP-3 reçoit la cinquième requête.
- Service-HTTP-2 reçoit la sixième requête, car à ce stade, il a le résultat le plus bas.
- Étant donné que Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont tous le même résultat à ce stade, l'appliance passe à la méthode round robin et continue à distribuer les connexions à l'aide de cette méthode.

Le tableau suivant explique comment les connexions sont distribuées dans la configuration d'équilibrage de charge à trois services décrite précédemment.

Demande reçue	Service sélectionné	Valeur N actuelle (nombre de transactions actives * TTFB)	Remarques
Request-1	Service-HTTP-3;(N = 0)	N = 2	Service-HTTP-3 a la valeur N la plus faible.
Request-2	Service-HTTP-3; (N = 2)	N = 4	Service-HTTP-3 a la valeur N la plus faible.
Request-3	Service-HTTP-3; (N = 4)	N = 6	Service-HTTP-3 a la valeur N la plus faible.
Request-4	Service-HTTP-1 ; (N = 6)	N = 8	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N. L'appliance utilise la méthode round robin pour distribuer les requêtes.
Request-5	Service-HTTP-3; (N = 6)	N = 8	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N.
Request-6	Service-HTTP-2; (N = 7)	N = 8	Service-HTTP-2 a la valeur N la plus faible.

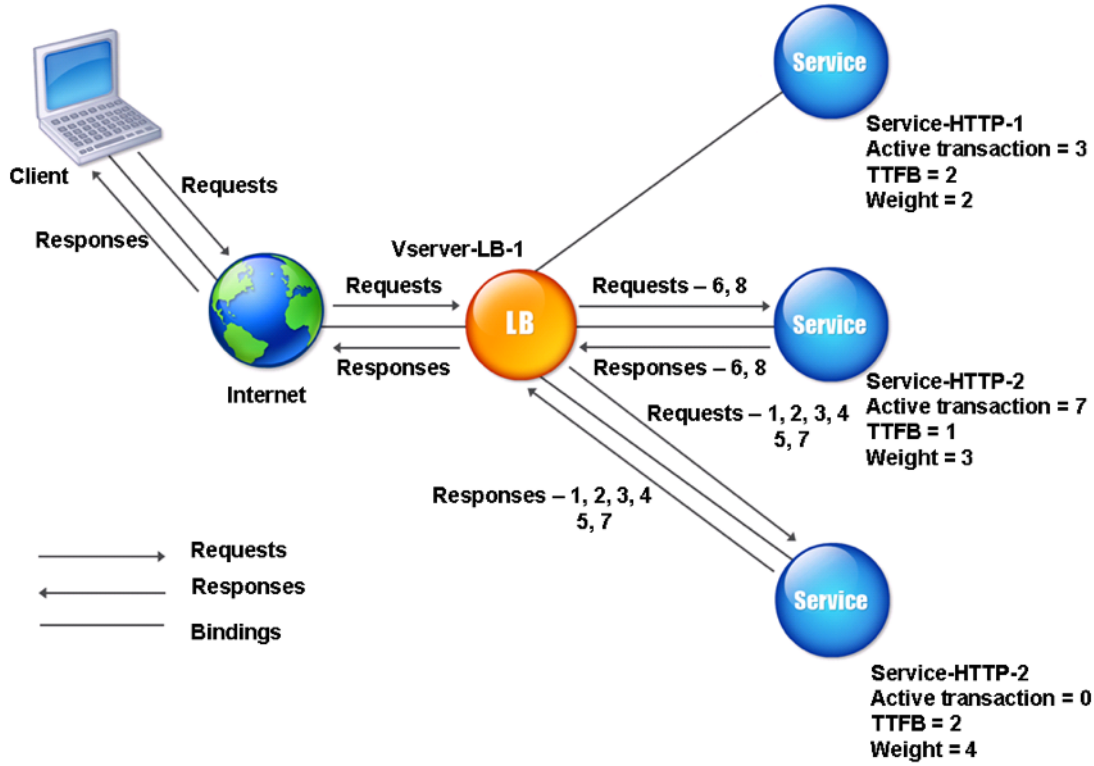
Demande reçue	Service sélectionné	Valeur N actuelle (nombre de transactions actives * TTFB)	Remarques
Request-7	Service-HTTP-3; (N = 8)	N = 10	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N. L'appliance Citrix ADC utilise la méthode round robin pour distribuer les requêtes.
Request-8	Service-HTTP-1 ; (N = 8)	N = 10	Service-HTTP-1 et Service-HTTP-2 ont les mêmes valeurs N, l'appliance utilise la méthode round robin pour distribuer les requêtes.

Service-HTTP-1 est de nouveau sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives ou lorsque sa valeur N est inférieure aux autres services (Service-HTTP-2 et Service-HTTP-3).

Sélection des services lorsque les pondérations sont attribuées

Le diagramme suivant illustre la façon dont l'appliance Citrix ADC utilise la méthode du temps de réponse le plus faible lorsque des pondérations sont affectées.

Figure 2. Fonctionnement de la méthode d'équilibrage de charge du temps de réponse le moins important lorsque des poids sont affectés



Le serveur virtuel sélectionne un service en utilisant la valeur (Nw) dans l'expression suivante :

Nw = (N) ⋆ (10000/poids), où N = (nombre de transactions actives ⋆ TTFB)

Supposons que Service-HTTP-1 se voit attribuer un poids de 2, Service-HTTP-2 un poids de 3 et Service-HTTP-3 un poids de 4.

L'appliance Citrix ADC distribue les demandes comme suit :

- Service-HTTP-3 reçoit la première requête, car il ne gère aucune transaction active.

  Si les services ne gèrent aucune transaction active, l'appliance les sélectionne indépendamment des poids qui leur sont attribués.
- Service-HTTP-3 reçoit les deuxième, troisième, quatrième et cinquième requêtes, car ce service a la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la sixième requête, car ce service a la valeur Nw la plus faible.
- Service-HTTP-3 reçoit la septième requête, car ce service a la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la huitième requête, car ce service a la valeur Nw la plus faible.

Service-HTTP-1 a le poids le plus faible et donc la valeur Nw la plus élevée, de sorte que le serveur virtuel ne le sélectionne pas pour l'équilibrage de charge.

Le tableau suivant explique comment les connexions sont distribuées dans la configuration d'équilibrage de charge à trois services décrite précédemment.

Demande reçue	Service sélectionné	Valeur Nw actuelle = (N) * (10000/Poids)	Remarques
Request-1	Service-HTTP-3; (Nw = 0)	Nw= 5000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-2	Service-HTTP-3; (Nw = 5000	Nw= 10000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-3	Service-HTTP-3; (Nw = 10000)	Nw= 15000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-4	Service-HTTP-3; (Nw = 15000)	Nw= 20000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-5	Service-HTTP-3; (Nw = 20000)	Nw= 25000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-6	Service-HTTP-2; (Nw = 23333.34)	Nw = 26666,67	Service-HTTP-2 a la valeur Nw la plus faible.
Request-7	Service-HTTP-3; (Nw = 25000)	Nw = 30000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-8	Service-HTTP-2; (Nw = 26666.67)	Nw= 30000	Service-HTTP-2 a la valeur Nw la plus faible.

Service-HTTP-1 est sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives ou lorsque sa valeur Nw est inférieure à d'autres services (Service-HTTP-2 et Service-HTTP-3).

Pour configurer la méthode d'équilibrage de charge du temps de réponse le moins possible à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;


```
set lb vserver <name> -lbMethod LEASTRESPONSETIME
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -lbMethod LEASTRESPONSETIME
<!--NeedCopy-->
```

Pour configurer la méthode d'équilibrage de charge du temps de réponse le moins possible à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **LEASTRESPONSETIME**.

Pour plus d'informations sur la configuration des moniteurs, voir Configuration des moniteurs dans une configuration d'équilibrage de charge.

Méthode LRTM

August 20, 2021

Remarque : LRTM signifie « Méthode du temps de réponse le plus faible à l'aide de moniteurs » (LRTM).

Lorsqu'un serveur virtuel d'équilibrage de charge est configuré pour utiliser la méthode LRTM, il utilise l'infrastructure de surveillance existante pour obtenir le temps de réponse le plus rapide. Le serveur virtuel d'équilibrage de charge sélectionne ensuite le service avec le plus petit nombre de transactions actives et le plus faible temps de réponse. Avant d'utiliser la méthode LRTM, vous devez lier des moniteurs spécifiques à l'application à chaque service et activer le mode LRTM sur ces moniteurs. L'appliance Citrix ADC prend ensuite des décisions d'équilibrage de charge en fonction des temps de réponse calculés à partir des sondes de surveillance.

Vous pouvez également utiliser la méthode LRTM pour équilibrer la charge des services non HTTP et non HTTPS. Vous pouvez également utiliser cette méthode lorsque plusieurs moniteurs sont liés à un service. Chaque moniteur détermine le temps de réponse à l'aide du protocole qu'il mesure pour le service qu'il est lié. Le serveur virtuel calcule ensuite un temps de réponse moyen pour ce service en calculant la moyenne des résultats.

Le tableau suivant résume comment les temps de réponse sont calculés pour les différents moniteurs.

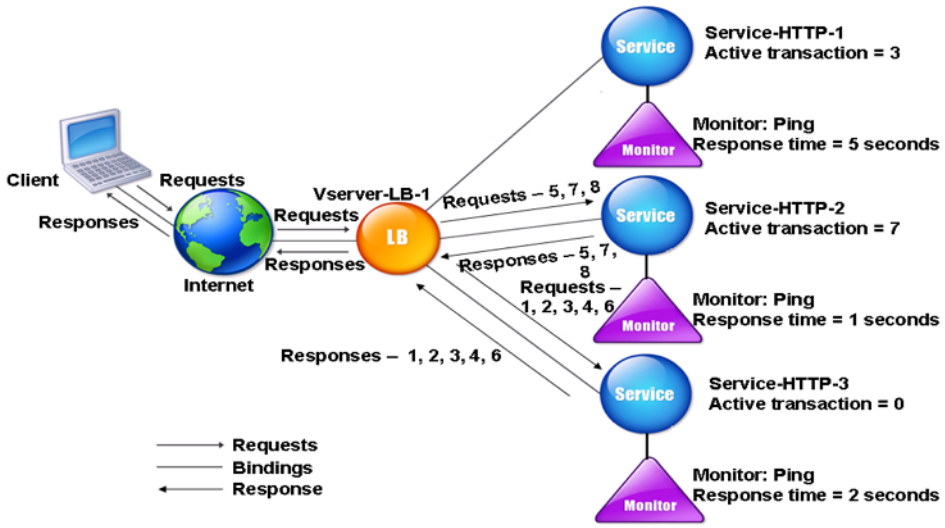
Surveillance	Calcul du temps de réponse
PING	Différence de temps entre la demande ICMP ECHO et la réponse ICMP ECHO.
TCP	Différence de temps entre la requête SYN et la réponse SYN+ACK.
HTTP	Différence de temps entre la requête HTTP (une fois la connexion TCP établie) et la réponse HTTP.
TCP-ECV	Différence de temps entre le moment où la chaîne d'envoi des données est envoyée et la chaîne de réception des données est renvoyée. Un moniteur TCP-ECV sans chaînes d'envoi et de réception est considéré comme ayant une configuration incorrecte.
HTTP-ECV	Différence de temps entre la requête HTTP et la réponse HTTP.
UDP-ECV	Décalage horaire entre la chaîne d'envoi de l'UDP et la chaîne de réception. Un moniteur UDP-ECV sans chaîne de réception est considéré comme ayant une configuration incorrecte.
DNS	Différence de temps entre une requête DNS et la réponse DNS.
TCPS	Différence de temps entre une requête SYN et la fin de la poignée de main SSL.
FTP	Différence de temps entre l'envoi du nom d'utilisateur et l'achèvement de l'authentification de l'utilisateur.
HTTPS (surveille les demandes HTTPS)	Le décalage horaire est le même que pour le moniteur HTTP.
HTTS-ECV (surveille les requêtes HTTPS)	Le décalage horaire est le même que pour le moniteur HTTP-ECV
USER	Différence de temps entre le moment où une demande est envoyée au répartiteur et le moment où la réponse du répartiteur est reçue.

L'exemple suivant montre comment l'appliance Citrix ADC sélectionne un service pour l'équilibrage de charge à l'aide de la méthode LRTM. Considérez les trois services suivants :

- Service-HTTP-1 gère 3 transactions actives et le temps de réponse est de cinq secondes.
- Service-HTTP-2 gère 7 transactions actives et le temps de réponse est d'une seconde.
- Service-HTTP-3 ne gère aucune transaction active et le temps de réponse est de deux secondes.

Le diagramme suivant illustre le processus suivi par l'appliance Citrix ADC lorsqu'elle transfère les demandes.

Figure 1. Fonctionnement de la méthode LRTM



Le serveur virtuel sélectionne un service en utilisant la valeur (N) dans l'expression suivante :

N = (Nombre de transactions actives * Temps de réponse déterminé par le moniteur)

Le serveur virtuel livre les demandes comme suit :

- Service-HTTP-3 reçoit la première demande, car ce service ne gère aucune transaction active.
- Service-HTTP-3 reçoit les deuxième, troisième et quatrième requêtes, car ce service possède la valeur N la plus faible.
- Service-HTTP-2 reçoit la cinquième requête, car ce service a la valeur N la plus faible.
- Étant donné que Service-HTTP-2 et Service-HTTP-3 ont actuellement la même valeur N, l'appliance Citrix ADC passe à la méthode Round Robin. Par conséquent, Service-HTTP-3 reçoit la sixième demande.
- Service-HTTP-2 reçoit les septième et huitième requêtes, car ce service a la valeur N la plus faible.

Service-HTTP-1 n'est pas pris en compte pour l'équilibrage de charge, car il est plus chargé (a la valeur

N la plus élevée) par rapport aux deux autres services. Toutefois, si Service-HTTP-1 termine ses transactions actives, l'appliance Citrix ADC considère à nouveau ce service pour l'équilibrage de charge.

Le tableau suivant résume la façon dont N est calculé pour les services.

Demande reçue	Service sélectionné	Valeur N actuelle (nombre de transactions actives * TTFB)	Remarques
Request-1	Service-HTTP-3;(N = 0)	N = 2	Service-HTTP-3 a la valeur N la plus faible.
Request-2	Service-HTTP-3; (N = 2)	N = 4	Service-HTTP-3 a la valeur N la plus faible.
Request-3	Service-HTTP-3; (N = 4)	N = 6	Service-HTTP-3 a la valeur N la plus faible.
Request-4	Service-HTTP-3; (N = 6)	N = 8	Service-HTTP-3 a la valeur N la plus faible.
Request-5	Service-HTTP-2; (N = 7)	N = 8	Service-HTTP-2 a la valeur N la plus faible.
Request-6	Service-HTTP-3; (N = 8)	N = 10	Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N. L'appliance Citrix ADC passe à la méthode round robin et sélectionne Service-HTTP-3
Request-7	Service-HTTP-2 ; (N = 8)	N = 9	Service-HTTP-2 a la valeur N la plus faible.
Request-8	Service-HTTP-2 ; (N = 9)	N = 10	Service-HTTP-2 a la valeur N la plus faible.

Service-HTTP-1 est de nouveau sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives ou lorsque sa valeur N est inférieure aux autres services (Service-HTTP-2 et Service-HTTP-3).

Sélection des services lorsque les pondérations sont attribuées

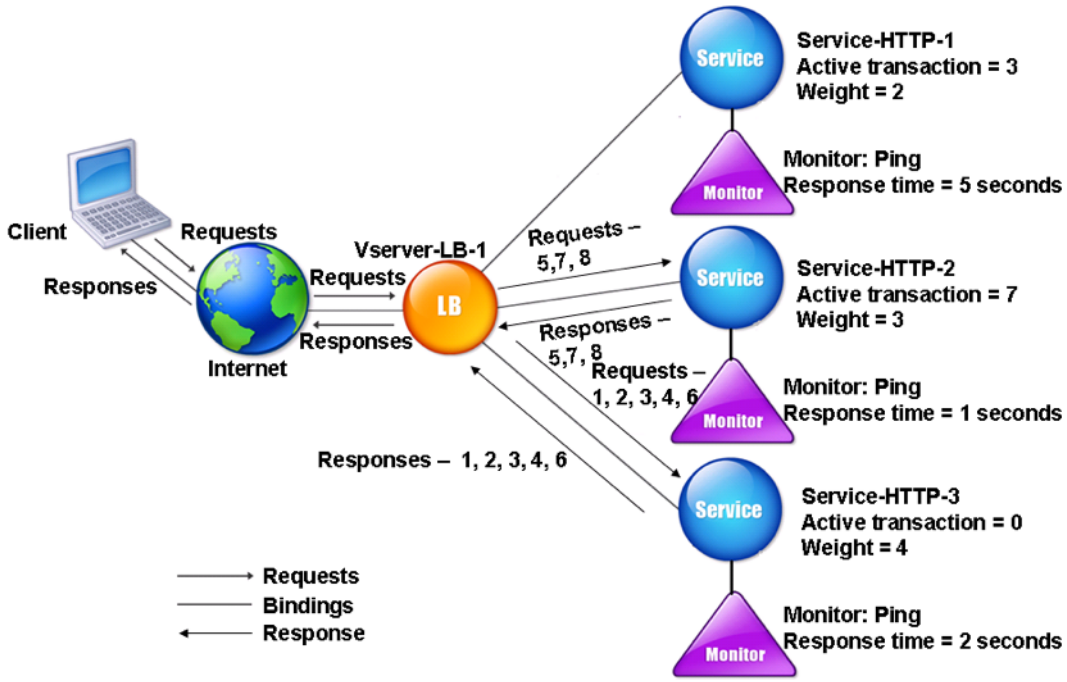
L'appliance Citrix ADC effectue également l'équilibrage de la charge en utilisant le nombre de transactions actives, le temps de réponse et les pondérations si des pondérations différentes sont attribuées aux services. L'appliance Citrix ADC sélectionne le service à l'aide de la valeur (Nw) dans l'expression suivante :

Nw = (N) * (10000/pondération)

Où N = (Nombre de transactions actives * Temps de réponse déterminé par le moniteur)

Le diagramme suivant illustre la façon dont le serveur virtuel utilise la méthode LRTM lorsque des pondérations sont attribuées.

Figure 2. Fonctionnement de la méthode d'équilibrage de charge du temps de réponse le moins important lorsque des poids sont affectés



Dans cet exemple, supposons que Service-HTTP-1 se voit attribuer un poids de 2, Service-HTTP-2 se voit attribuer un poids de 3 et Service-HTTP-3 un poids de 4.

L'appliance Citrix ADC livre les demandes comme suit :

- Service-HTTP-3 reçoit la première requête, car il ne gère aucune transaction active.

- Service-HTTP-3 reçoit les deuxième, troisième, quatrième et cinquième requêtes, car ce service a la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la sixième requête, car ce service a la valeur Nw la plus faible.
- Service-HTTP-3 reçoit la septième requête, car ce service a la valeur Nw la plus faible.
- Service-HTTP-2 reçoit les huitième requêtes, car ce service a la valeur Nw la plus faible.

Service-HTTP-1 a le poids le plus faible et la valeur Nw la plus élevée, de sorte que l'appliance Citrix ADC ne le sélectionne pas pour l'équilibrage de charge.

Le tableau suivant résume la façon dont Nw est calculé pour divers moniteurs.

Demande reçue	Service sélectionné	Valeur Nw actuelle (N) * (10000/Poids)	Remarques
Request-1	Service-HTTP-3; (Nw = 0)	Nw= 5000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-2	Service-HTTP-3; (Nw = 5000	Nw= 10000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-3	Service-HTTP-3; (Nw = 10000)	Nw= 15000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-4	Service-HTTP-3; (Nw = 15000)	Nw= 20000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-5	Service-HTTP-3; (Nw = 20000)	Nw= 25000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-6	Service-HTTP-2; (Nw = 23333.34)	Nw = 26666,67	Service-HTTP-2 a la valeur Nw la plus faible.
Request-7	Service-HTTP-3; (Nw = 25000)	Nw = 30000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-8	Service-HTTP-2; (Nw = 26666.67)	Nw= 30000	Service-HTTP-2 a la valeur Nw la plus faible.

Service-HTTP-1 est sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives

ou lorsque sa valeur Nw est inférieure à d'autres services (Service-HTTP-2 et Service-HTTP-3).

Pour configurer la méthode d'équilibrage de charge LRTM à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;

```
set lb vserver <name> [-lbMethod <lbMethod>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -lbMethod LRTM
<!--NeedCopy-->
```

Pour configurer la méthode d'équilibrage de charge LRTM à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **LRTM**.

Pour activer l'option LRTM dans les moniteurs à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;

```
set lb monitor <monitorName> <type> [-LRTM ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Exemple :

```
set lb monitor monitor-HTTP-1 HTTP -LRTM ENABLED
<!--NeedCopy-->
```

Pour activer l'option LRTM dans les moniteurs à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**, puis ouvrez un moniteur.
2. Dans Paramètres avancés, sélectionnez **LRTM (Temps de réponse minimum à l'aide de la surveillance)**.

Pour plus d'informations sur la configuration des moniteurs, voir Configuration des moniteurs dans une configuration d'équilibrage de charge.

Méthodes de hachage

August 20, 2021

Les méthodes d'équilibrage de charge basées sur des hachages de certaines informations de connexion ou d'en-tête constituent la plupart des méthodes d'équilibrage de charge de l'appliance Citrix ADC. Les hachages sont plus courts et plus faciles à utiliser que les informations sur lesquelles ils sont basés, tout en conservant suffisamment d'informations pour s'assurer qu'aucun élément d'information différent ne génère le même hachage et sont donc confondus les uns avec les autres.

Vous pouvez utiliser les méthodes d'équilibrage de charge de hachage dans un environnement où un cache sert une large gamme de contenu provenant d'Internet ou de serveurs d'origine spécifiés. La mise en cache des demandes réduit la latence des demandes et des réponses et garantit une meilleure utilisation des ressources (CPU), rendant la mise en cache populaire sur les sites Web et serveurs d'applications très utilisés. Comme ces sites bénéficient également de l'équilibrage de charge, les méthodes d'équilibrage de charge de hachage sont largement utiles.

L'appliance Citrix ADC fournit les méthodes de hachage suivantes :

- Méthode de hachage d'URL
- Méthode de hachage de domaine
- Méthode de hachage IP de destination
- Méthode de hachage IP source
- Méthode de hachage IP de destination IP source
- Méthode de hachage du port source IP source
- Méthode de hachage d'ID d'appel
- Méthode de jeton

La plupart des algorithmes de hachage calculent deux valeurs de hachage :

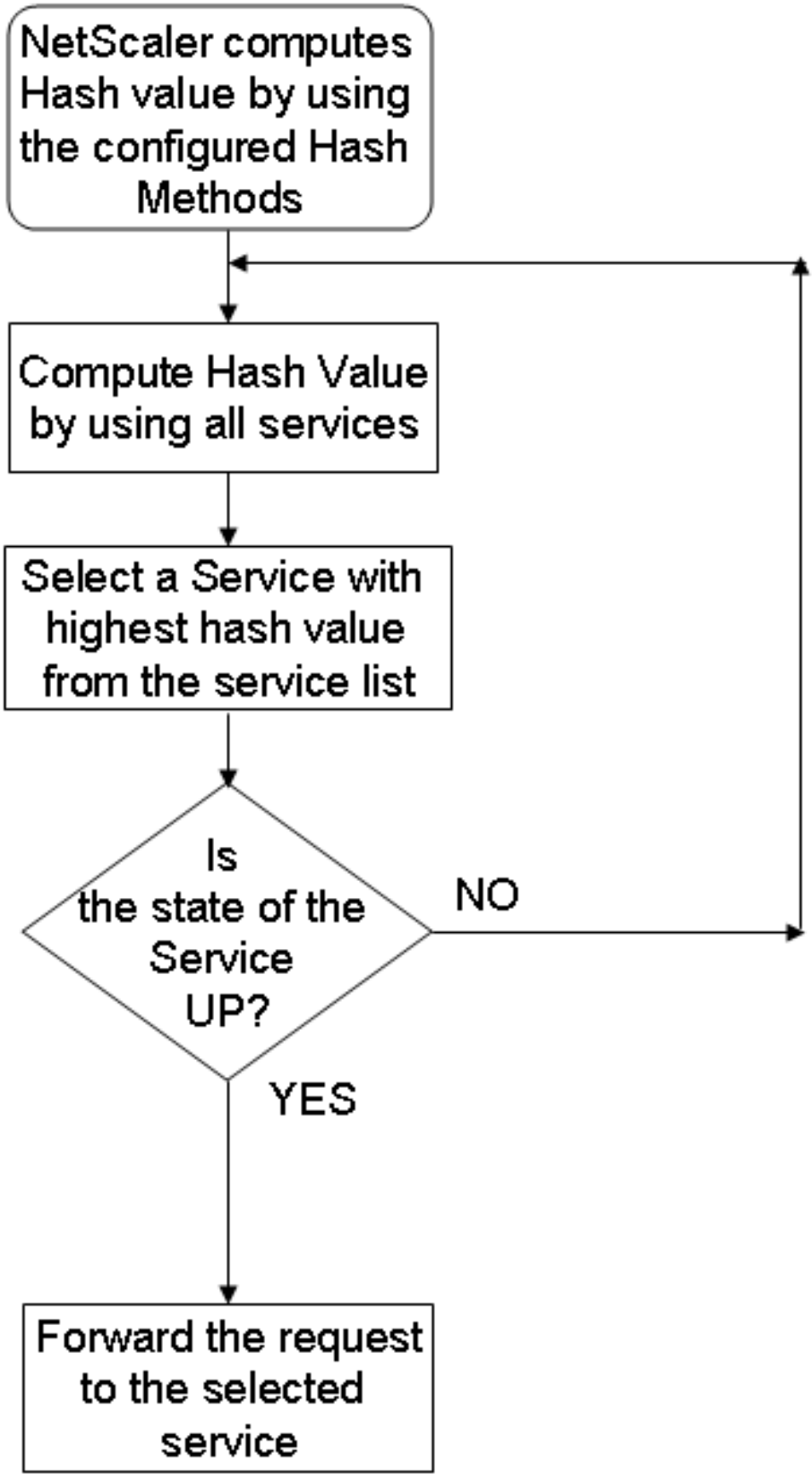
- Un hachage de l'adresse IP et du port du service.
- Hash de l'URL entrante, du nom de domaine, de l'adresse IP source, de l'adresse IP de destination ou des adresses IP source et destination, selon la méthode de hachage configurée.

L'appliance Citrix ADC génère ensuite une nouvelle valeur de hachage en utilisant ces deux valeurs de hachage. Enfin, il transmet la demande au service ayant la valeur de hachage la plus élevée. Lorsque l'appliance calcule une valeur de hachage pour chaque demande et sélectionne le service qui traite la demande, il remplit un cache. Les requêtes suivantes avec la même valeur de hachage sont envoyées au même service. L'organigramme suivant illustre ce processus.

> Remarque
>
> À partir de Citrix ADC version 13.0 build 79.x, les algorithmes de hachage cohérents CARP (PRAC) et Jump Table Assisted Ring Hash (JARH) sont pris en charge. Les algorithmes de hachage co-

> hérents garantissent une interruption minimale lorsque des services sont ajoutés ou supprimés de votre configuration d'équilibrage de charge, ou lors d'un événement de clapet de service dans la configuration d'équilibrage de charge. Pour plus de détails, voir Algorithmes de hachage cohérents.

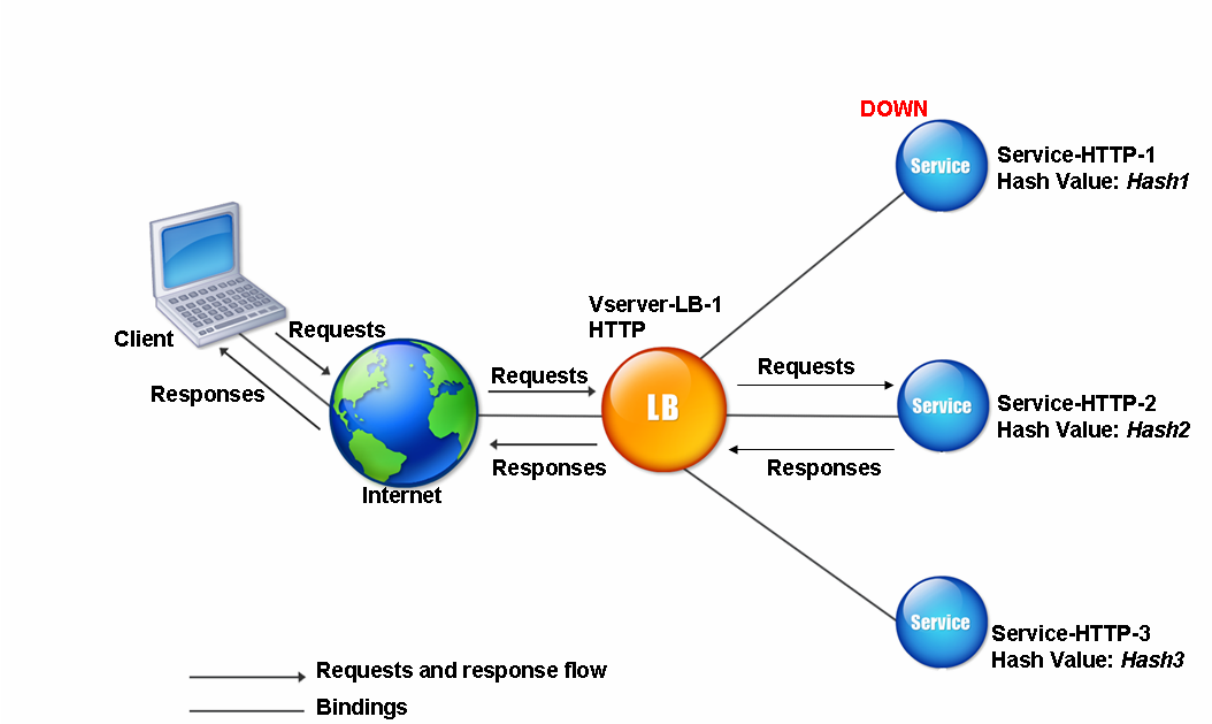
Figure 1. Comment les méthodes de hachage distribuent les demandes



Les méthodes de hachage peuvent être appliquées aux adresses IPv4 et IPv6.

Considérons un scénario dans lequel trois services (Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3) sont liés à un serveur virtuel, toute méthode de hachage est configurée et la valeur de hachage est Hash1. Lorsque les services configurés sont UP, la demande est envoyée à Service-HTTP-1. Si Service-HTTP-1 est en panne, l'appliance Citrix ADC calcule la valeur de hachage du dernier journal du nombre de services. L'appliance sélectionne ensuite le service ayant la valeur de hachage la plus élevée, tel que Service-HTTP-2. Le diagramme suivant illustre ce processus.

Figure 2. Modèle d'entité pour les méthodes de hachage



> Remarque
>
> Si l'appliance Citrix ADC ne parvient pas à sélectionner un service à l'aide d'une méthode de hachage, la méthode de connexion la plus faible est par défaut pour sélectionner un service pour la demande entrante. Ajustez les pools de serveurs en supprimant les services pendant les périodes de faible trafic pour permettre aux caches de se repeupler sans affecter les performances de votre configuration d'équilibrage de charge.

Algorithmes de hachage cohérents

Les algorithmes de hachage cohérents sont utilisés pour obtenir une persistance sans état. Les méthodes LB basées sur le hachage utilisent l'un des trois algorithmes de hachage cohérents suivants :

- **Cache Array Routing Protocol (CARP)**

L'algorithme CARP est utilisé dans l'équilibrage de charge des requêtes HTTP sur plusieurs serveurs de cache proxy. Cet algorithme est activé par défaut.

- **Prime Re-Shuffled Assisted CARP (PRAC)**

  L'appliance Citrix ADC utilise l'algorithme PRAC propriétaire pour fournir une distribution uniforme du trafic.

- **Jump table Assisted Ring Hash (JARH)**

  L'appliance Citrix ADC utilise l'algorithme JARH propriétaire pour assurer la cohérence et la distribution uniforme du trafic. Cet algorithme utilise des doigts de hachage. Un nombre plus élevé de doigts permet une meilleure répartition du trafic. Cependant, l'augmentation du nombre de doigts augmente également l'utilisation de la mémoire.

Pour choisir l'algorithme de hachage cohérent à l'aide de l'interface de ligne de commande

```
1 set lb parameter [-lbHashAlgorithm [DEFAULT|JARH|PRAC] [-lbHashFingers
     <positive_integer>]
2 <!--NeedCopy-->
```

Exemple :

```
1 set lb parameter -lbHashAlgorithm JARH -lbHashFingers 10
2 <!--NeedCopy-->
```

ARGUMENTS :

- **lbHashAlgorithm**-Spécifiez l'algorithme de hachage à utiliser pour les méthodes d'équilibrage de charge basées sur le hachage suivantes :
  - Méthode de hachage d'URL
  - Méthode de hachage de domaine
  - Méthode de hachage IP de destination
  - Méthode de hachage IP source
  - Méthode de hachage IP de destination IP source
  - Méthode de hachage du port source IP source
  - Méthode de hachage d'ID d'appel
  - Méthode de jeton

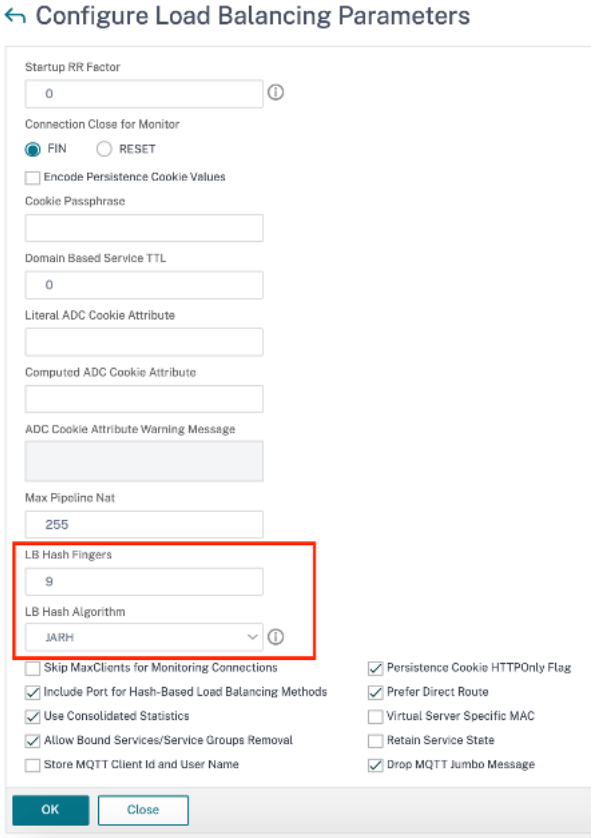
  Valeurs possibles : DEFAULT, PRAC, JARH Valeur
  par défaut : DEFAULT

- **LBHashFingers**-Spécifiez le nombre de doigts à utiliser dans les algorithmes PRAC et JARH pour les méthodes LB basées sur le hachage. L'augmentation du nombre de doigts permet une meilleure répartition du trafic au détriment de la mémoire supplémentaire.

Valeur par défaut : 256 Valeur
minimale : 1 Valeur
maximale : 1024

Pour choisir l'algorithme de hachage cohérent à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Modifier les paramètres d'équilibrage de charge**.
2. Dans le volet **Configurer les paramètres d'équilibrage de charge**, entrez les valeurs appropriées pour les champs suivants en fonction de vos besoins :
   - doigts de hachage LB
   - Dans le champ **Algorithme de hachage LB**, choisissez l'algorithme de hachage cohérent dans le menu déroulant.



La méthode de hachage de l'URL

Lorsque vous configurez l'appliance Citrix ADC pour qu'elle utilise la méthode de hachage URL pour équilibrer la charge des services, pour sélectionner un service, l'appliance génère une valeur de hachage de l'URL HTTP présente dans la demande entrante. Si le service sélectionné par la valeur de

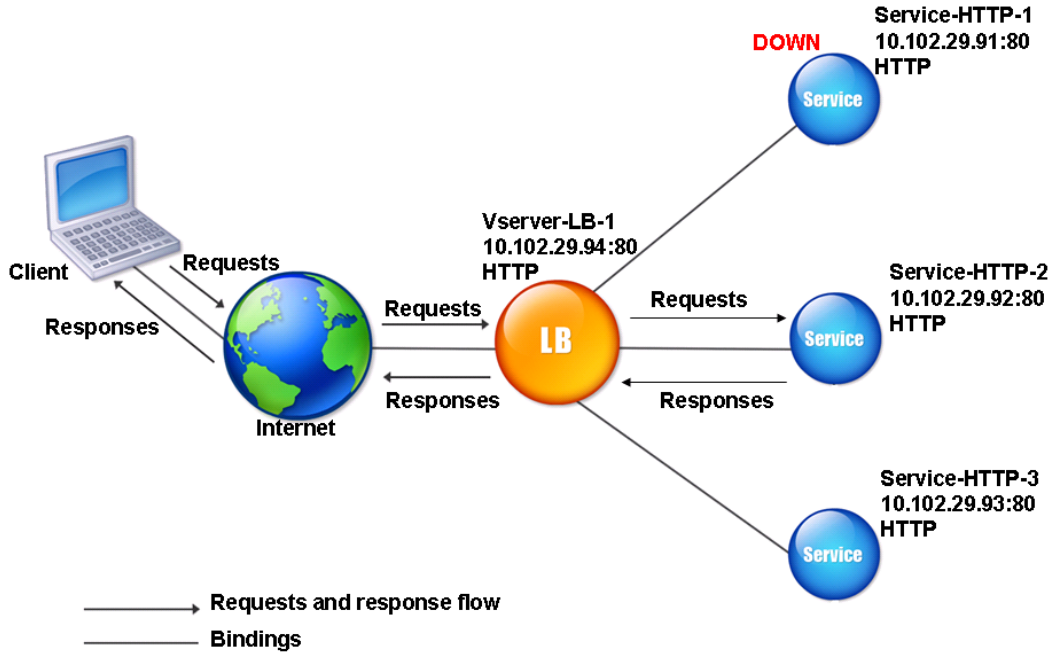
hachage est DOWN, l'algorithme dispose d'une méthode pour sélectionner un autre service dans la liste des services actifs. L'appliance met en cache la valeur hachée de l'URL et, lorsqu'elle reçoit des demandes ultérieures qui utilisent la même URL, elle les transmet au même service. Si l'appliance ne peut pas analyser une requête entrante, elle utilise la méthode round robin pour l'équilibrage de la charge au lieu de la méthode de hachage URL.

Pour générer la valeur de hachage, l'appliance utilise un algorithme spécifique et considère une partie de l'URL. Par défaut, l'appliance prend en compte les 80 premiers octets de l'URL. Si l'URL est inférieure à 80 octets, l'URL complète est utilisée. Vous pouvez spécifier une longueur différente. La longueur de hachage peut aller de 1 octet à 4096 octets. En règle générale, si des URL longues sont utilisées lorsque seuls quelques caractères sont différents, il est judicieux de rendre la longueur de hachage la plus élevée possible afin d'assurer une répartition plus uniforme de la charge.

Considérons un scénario dans lequel trois services, Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3, sont liés à un serveur virtuel, et la méthode d'équilibrage de charge configurée sur le serveur virtuel est la méthode de hachage URL. Le serveur virtuel reçoit une demande et la valeur de hachage de l'URL est U1. L'appliance sélectionne Service-HTTP-1. Si Service-HTTP-1 est DOWN, l'appliance sélectionne Service-HTTP-2.

Le diagramme suivant illustre ce processus.

Figure 3. Fonctionnement du hachage d'URL



Si Service-HTTP-1 et Service-HTTP-2 sont tous deux en panne, l'appliance envoie les demandes avec la valeur de hachage U1 à Service-HTTP-3.

Si Service-HTTP-1 et Service-HTTP-2 sont en panne, les requêtes qui génèrent l'URL1 de hachage sont envoyées à Service-HTTP-3. Si ces services sont UP, les demandes qui génèrent l'URL de hachage 1 sont distribuées de la manière suivante :

- Si le Service-HTTP-2 est en service, la demande est envoyée à Service-HTTP-2.
- Si le Service-HTTP-1 est en service, la demande est envoyée à Service-HTTP-1.
- Si Service-HTTP-1 et Service-HTTP-2 sont mis en service en même temps, la demande est envoyée à Service-HTTP-1.

Pour configurer la méthode de hachage d'URL, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie. Sélectionnez la méthode d'équilibrage de charge en tant qu'URL Hash et définissez la longueur de hachage sur le nombre d'octets à utiliser pour générer la valeur de hachage.

La méthode de hachage du domaine

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage de domaine utilise la valeur hachée du nom de domaine dans la requête HTTP pour sélectionner un service. Le

nom de domaine provient soit de l'URL entrante, soit de l'en-tête Host de la requête HTTP. Si le nom de domaine apparaît à la fois dans l'URL et dans l'en-tête Host, l'appliance donne la préférence à l'URL.

Si vous configurez le hachage de nom de domaine et qu'une requête HTTP entrante ne contient pas de nom de domaine, l'appliance Citrix ADC utilise par défaut la méthode round robin pour cette requête.

Le calcul de la valeur de hachage utilise la longueur de nom ou la valeur de longueur de hachage, la valeur la plus petite étant retenue. Par défaut, l'appliance Citrix ADC calcule la valeur de hachage à partir des 80 premiers octets du nom de domaine. Pour spécifier un nombre différent d'octets dans le nom de domaine lors du calcul de la valeur de hachage, vous pouvez définir le paramètre hashLength (longueur de hachage dans l'utilitaire de configuration) sur une valeur comprise entre 1 et 4096 (octets).

Pour configurer la méthode de hachage de domaine, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode de hachage IP de destination

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage IP de destination utilise la valeur hachée de l'adresse IP de destination pour sélectionner un serveur. Vous pouvez masquer l'adresse IP de destination pour spécifier la partie de celle-ci à utiliser dans le calcul de la valeur de hachage, de sorte que les requêtes provenant de réseaux différents mais destinées au même sous-réseau soient toutes dirigées vers le même serveur. Cette méthode prend en charge les serveurs de destination IPv4 et IPv6.

Cette méthode d'équilibrage de charge est appropriée pour une utilisation avec la fonction de redirection du cache.

Pour configurer la méthode de hachage IP de destination pour un serveur de destination IPv4, définissez le paramètre NetMask. Pour configurer cette méthode pour un serveur de destination IPv6, vous utilisez le paramètre V6NetMasklen. Dans l'utilitaire de configuration, les zones de texte permettant de définir ces paramètres apparaissent lorsque vous sélectionnez la **méthode de hachage IP de destination**.

Pour configurer la méthode de hachage IP de destination, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

La méthode de hachage IP source

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage IP source utilise la valeur hachée de l'adresse IPv4 ou IPv6 client pour sélectionner un service. Pour diriger toutes les demandes provenant d'adresses IP source appartenant à un réseau particulier vers un serveur de destination spécifique, vous devez masquer l'adresse IP source. Pour les adresses IPv4, utilisez le paramètre netMask. Pour les adresses IPv6, utilisez le paramètre V6NetMaskLength.

Pour configurer la méthode de hachage IP source, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode de hachage IP de destination IP source

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage IP de destination IP source utilise la valeur hachée des adresses IP source et destination (IPv4 ou IPv6) pour sélectionner un service. Le hachage est symétrique. La valeur de hachage est la même quel que soit l'ordre des adresses IP source et de destination. Cela garantit que tous les paquets circulant d'un client particulier vers la même destination sont dirigés vers le même serveur.

Pour diriger toutes les demandes appartenant à un réseau particulier vers un serveur de destination spécifique, vous devez masquer l'adresse IP source. Pour les adresses IPv4, utilisez le paramètre netMask. Pour les adresses IPv6, utilisez le paramètre V6NetMaskLength.

Pour configurer la méthode de hachage IP de destination IP source, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode de hachage du port source IP source

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage du port source IP source utilise la valeur de hachage de l'IP source (IPv4 ou IPv6) et du port source pour sélectionner un service. Cela garantit que tous les paquets d'une connexion particulière sont dirigés vers le même service.

Cette méthode est utilisée dans la mise en miroir des connexions et l'équilibrage de charge du pare-feu. Pour plus d'informations sur la mise en miroir des connexions, voir Basculement de connexion.

Pour diriger toutes les demandes appartenant à un réseau particulier vers un serveur de destination spécifique, vous devez masquer l'adresse IP source. Pour les adresses IPv4, utilisez le paramètre netMask. Pour les adresses IPv6, utilisez le paramètre V6NetMaskLength.

Pour configurer la méthode de hachage du port source IP source source, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

La méthode de hachage de l'ID d'appel

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage de l'ID d'appel utilise la valeur de hachage de l'ID d'appel dans l'en-tête SIP pour sélectionner un service. Les paquets d'une session SIP particulière sont donc toujours dirigés vers le même serveur proxy.

Cette méthode est applicable à l'équilibrage de charge SIP. Pour plus d'informations sur l'équilibrage de charge SIP, voir Surveillance des services SIP.

Pour configurer la méthode de hachage de l'ID d'appel, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode de bande passante minimale

August 20, 2021

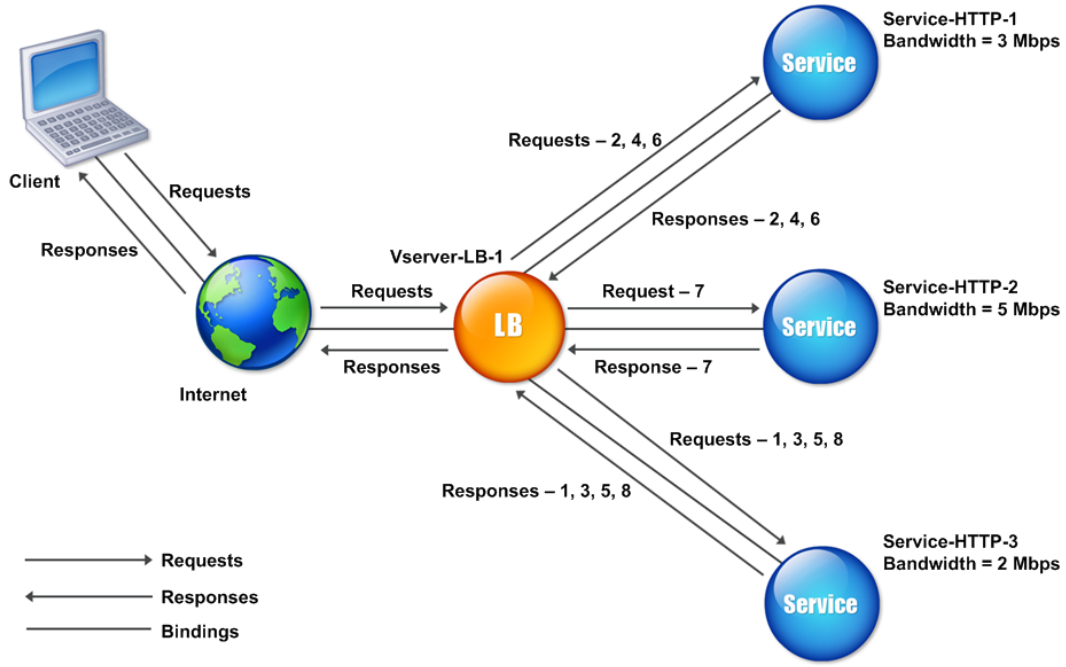
Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode la plus faible bande passante sélectionne le service qui dessert actuellement le moins de trafic, mesuré en mégabits par seconde (Mbps). L'exemple suivant montre comment le serveur virtuel sélectionne un service pour l'équilibrage de charge à l'aide de la méthode la plus faible bande passante.

Considérez trois services, Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3.

- Service-HTTP-1 a 3 Mbps de bande passante.
- Service-HTTP-2 a 5 Mbps de bande passante.
- Service-HTTP-3 a 2 Mbps de bande passante.

Le diagramme suivant illustre comment le serveur virtuel utilise la méthode la plus faible bande passante pour transférer des demandes aux trois services.

Figure 1. Fonctionnement de la méthode d'équilibrage de charge la plus faible bande passante



Le serveur virtuel sélectionne le service en utilisant la valeur de bande passante (N), qui est la somme du nombre d'octets transmis et reçus au cours des 14 secondes précédentes. Si chaque demande nécessite une bande passante de 1 Mbit/s, l'appliance Citrix ADC fournit les demandes comme suit :

- Service-HTTP-3 reçoit la première requête, car ce service a la valeur N la plus faible.
- Étant donné que Service-HTTP-1 et Service-HTTP-3 ont désormais la même valeur N, le serveur virtuel passe à la méthode Round Robin pour ces serveurs, en alternant entre eux. Service-HTTP-1 reçoit la deuxième requête, Service-HTTP-3 reçoit la troisième requête, Service-HTTP-1 reçoit la quatrième requête, Service-HTTP-3 reçoit la cinquième requête et Service-HTTP-1 reçoit la sixième requête.
- Puisque Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont désormais la même valeur N, le serveur virtuel inclut Service-HTTP-2 dans la liste ronde. Par conséquent, Service-HTTP-2 reçoit la septième requête, Service-HTTP-3 reçoit la huitième requête, et ainsi de suite.

Le tableau suivant résume le mode de calcul de N.

Demande reçue	Service sélectionné	Valeur N actuelle	Remarques
Request-1	Service-HTTP-3; (N = 2)	N = 3	Service-HTTP-3 a la valeur N la plus faible.

Demande reçue	Service sélectionné	Valeur N actuelle	Remarques
Request-2	Service-HTTP-1; (N = 3)	N = 4	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N.
Request-3	Service-HTTP-3 ; (N = 3)	N = 4	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N.
Request-4	Service-HTTP-1; (N = 4)	N = 5	-
Request-5	Service-HTTP-3; (N = 4)	N = 5	-
Request-6	Service-HTTP-1 ; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.
Request-7	Service-HTTP-2; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.
Request-8	Service-HTTP-3 ; (N = 5)	N = 6	-

Remarque : Si vous activez l'option RTSP NAT sur le serveur virtuel, l'appliance Citrix ADC utilise le nombre d'octets de données et de contrôle échangés pour déterminer l'utilisation de la bande passante pour les services RTSP. Pour plus d'informations sur l'option NAT RTSP, consultez Gestion des connexions RTSP.

L'appliance Citrix ADC effectue également l'équilibrage de la charge à l'aide de la bande passante et des poids si des poids différents sont attribués aux services. Il sélectionne un service en utilisant la valeur (Nw) dans l'expression suivante :

Nw = (N) * (10000/pondération)

Comme dans l'exemple précédent, supposons que Service-HTTP-1 se voit attribuer un poids de 2, Service-HTTP-2 se voit attribuer un poids de 3 et Service-HTTP-3 un poids de 4. L'appliance Citrix ADC livre les demandes comme suit :

- Service-HTTP-3 reçoit les première deuxième, troisième, quatrième et cinquième requêtes, car ce service a la valeur Nw la plus faible.

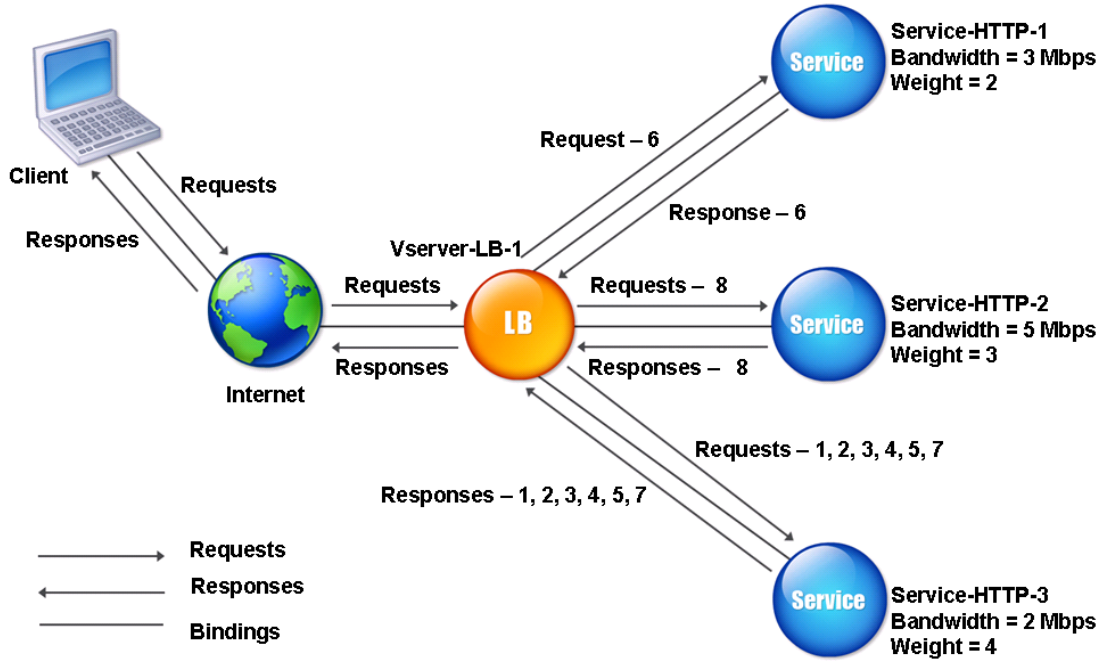
- Service-HTTP-1 reçoit la sixième requête, car ce service a la valeur Nw la plus faible.
- Service-HTTP-3 reçoit la septième requête, car ce service a la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la huitième requête, car ce service a la valeur Nw la plus faible.

Le tableau suivant résume la façon dont Nw est calculé.

Demande reçue	Service sélectionné	Valeur Nw actuelle (nombre de transactions actives) * (10000/pondération)	Remarques
Request-1	Service-HTTP-3; (Nw = 5000)	Nw= 5000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-2	Service-HTTP-3; (Nw = 5000)	Nw= 7500	-
Request-3	Service-HTTP-3; (Nw = 7500)	Nw= 10000	-
Request-4	Service-HTTP-3; (Nw = 10000)	Nw= 12500	-
Request-5	Service-HTTP-3; (Nw = 12500)	Nw= 15000	-
Request-6	Service-HTTP-1; (Nw = 15000)	Nw= 20000	Service-HTTP-1 et Service-HTTP-3 ont la même valeur Nw.
Request-7	Service-HTTP-3; (Nw = 15000)	Nw= 17500	Service-HTTP-1 et Service-HTTP-3 ont la même valeur Nw.
Request-8	Service-HTTP-2; (Nw = 16666.67)	Nw= 20000	Service-HTTP-2 a la valeur Nw la plus faible.

Le diagramme suivant illustre comment le serveur virtuel utilise la méthode de bande passante la moins élevée lorsque des pondérations sont attribuées aux services.

Figure 2. Fonctionnement de la méthode d'équilibrage de charge de la bande passante minimale lorsque des poids sont affectés



Pour configurer la méthode de la moindre bande passante, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Least packets method

August 20, 2021

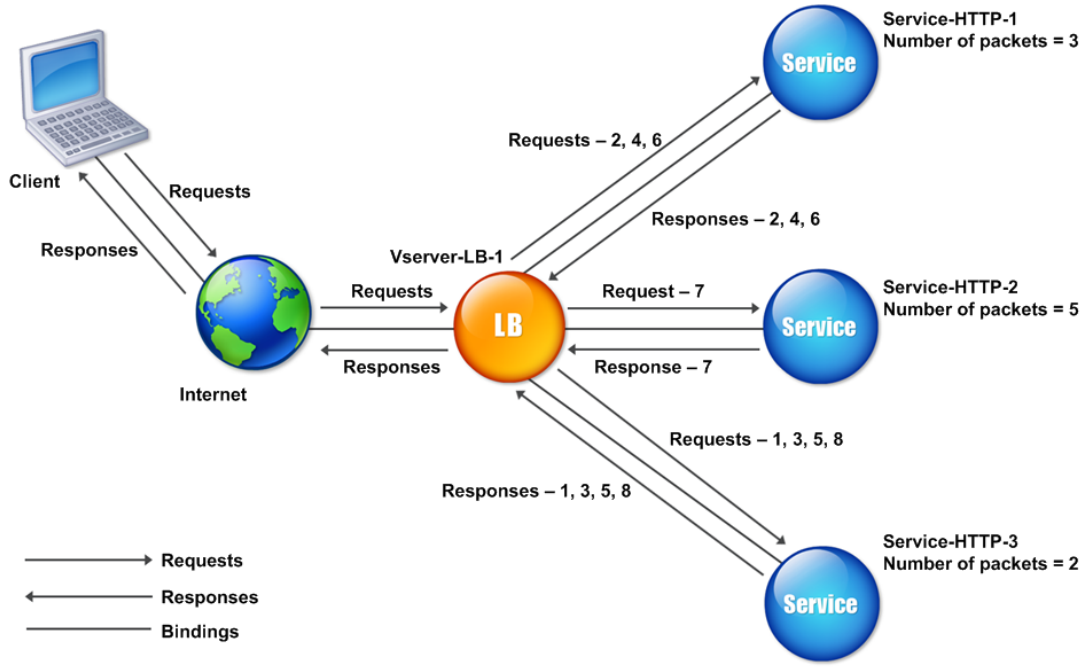
Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode des moindres paquets sélectionne le service qui a reçu le moins de paquets au cours des 14 dernières secondes.

Par exemple, considérez trois services, Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3.

- Service-HTTP-1 a traité trois paquets au cours des 14 dernières secondes.
- Service-HTTP-2 a traité cinq paquets au cours des 14 dernières secondes.
- Service-HTTP-3 a traité deux paquets au cours des 14 dernières secondes.

Le diagramme suivant illustre comment l'appliance Citrix ADC utilise la méthode des moindres paquets pour choisir un service pour chaque demande qu'elle reçoit.

Figure 1. Fonctionnement de la méthode d'équilibrage de charge des moindres paquets



L'appliance Citrix ADC sélectionne un service en utilisant le nombre de paquets (N) transmis et reçus par chaque service au cours des 14 dernières secondes. En utilisant cette méthode, il livre les requêtes comme suit :

- Service-HTTP-3 reçoit la première requête, car ce service a la valeur N la plus faible.
- Puisque Service-HTTP-1 et Service-HTTP-3 ont maintenant la même valeur N, le serveur virtuel bascule vers la méthode round robin. Service-HTTP-1 reçoit donc la deuxième requête, Service-HTTP-3 reçoit la troisième requête, Service-HTTP-1 reçoit la quatrième requête, Service-HTTP-3 reçoit la cinquième requête et Service-HTTP-1 reçoit la sixième requête.
- Puisque Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont tous la même valeur N, le serveur virtuel passe également à la méthode round robin pour Service-HTTP-2, y compris dans la liste ronde. Par conséquent, Service-HTTP-2 reçoit la septième requête, Service-HTTP-3 reçoit la huitième requête, et ainsi de suite.

Le tableau suivant résume le mode de calcul de N.

Demande reçue	Service sélectionné	Valeur N actuelle	Remarques
Request-1	Service-HTTP-3; (N = 2)	N = 3	Service-HTTP-3 a la valeur N la plus faible.

Demande reçue	Service sélectionné	Valeur N actuelle	Remarques
Request-2	Service-HTTP-1; (N = 3)	N = 4	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N.
Request-3	Service-HTTP-3; (N = 3)	N = 4	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N.
Request-4	Service-HTTP-1; (N = 4)	N = 5	-
Request-5	Service-HTTP-3; (N = 4)	N = 5	-
Request-6	Service-HTTP-1 ; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.
Request-7	Service-HTTP-2; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.
Request-8	Service-HTTP-3 ; (N = 5)	N = 6	-

Remarque : Si vous activez l'option NAT RTSP sur le serveur virtuel, l'appliance utilise le nombre de paquets de données et de contrôle pour calculer le nombre de paquets pour les services RTSP. Pour plus d'informations sur l'option NAT RTSP, consultez Gestion des connexions RTSP.

L'appliance Citrix ADC effectue également l'équilibrage de charge en utilisant le nombre de paquets et de poids lorsqu'un poids différent est attribué à chaque service. Il sélectionne un service en utilisant la valeur (Nw) dans l'expression suivante :

Nw = (N) * (10000/pondération)

Comme dans l'exemple précédent, supposons que Service-HTTP-1 se voit attribuer un poids de 2, Service-HTTP-2 se voit attribuer un poids de 3 et Service-HTTP-3 un poids de 4. L'appliance Citrix ADC livre les demandes comme suit :

- Service-HTTP-3 reçoit les première deuxième, troisième, quatrième et cinquième requêtes, car ce service a la valeur Nw la plus faible.
- Service-HTTP-1 reçoit la sixième requête, car ce service a la valeur Nw la plus faible.

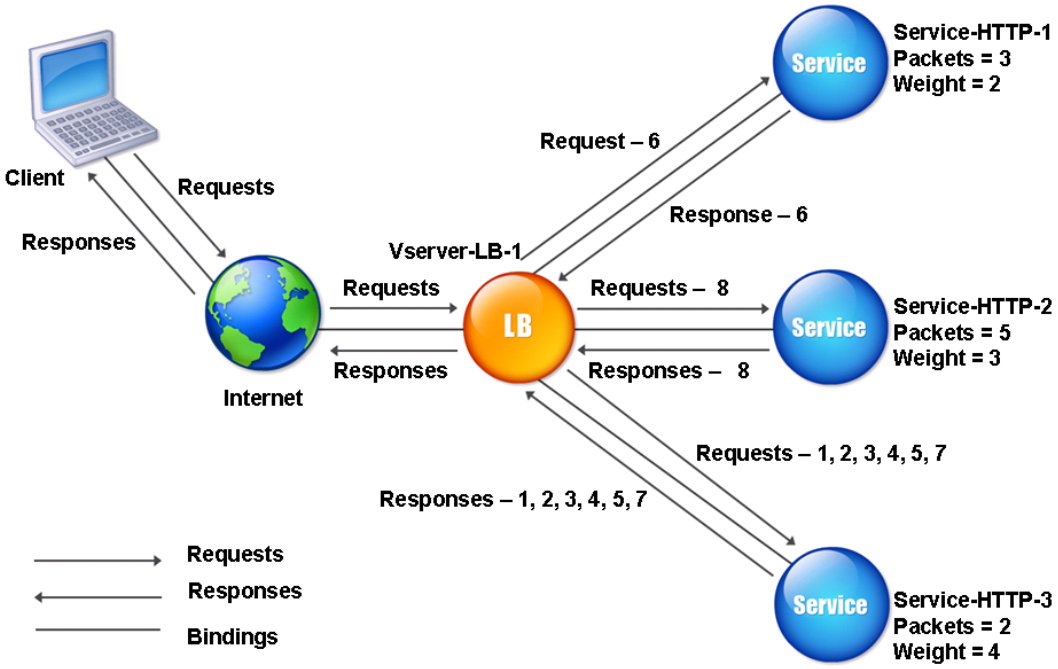
- Service-HTTP-3 reçoit la septième requête, car ce service a la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la huitième requête, car ce service a la valeur Nw la plus faible.

Le tableau suivant résume la façon dont Nw est calculé.

Demande reçue	Service sélectionné	Valeur Nw actuelle (nombre de transactions actives) * (10000/ poids)	Remarques
Request-1	Service-HTTP-3; (Nw = 5000)	Nw= 5000	Service-HTTP-3 a la valeur Nw la plus faible.
Request-2	Service-HTTP-3; (Nw = 5000)	Nw= 7500	-
Request-3	Service-HTTP-3 ; (Nw = 7500)	Nw= 10000	-
Request-4	Service-HTTP-3; (Nw = 10000)	Nw= 12500	-
Request-5	Service-HTTP-3; (Nw = 12500)	Nw= 15000	-
Request-6	Service-HTTP-1; (Nw = 15000)	Nw= 20000	Service-HTTP-1 et Service-HTTP-3 ont la même valeur Nw.
Request-7	Service-HTTP-3; (Nw = 15000)	Nw= 17500	Service-HTTP-1 et Service-HTTP-3 ont la même valeur Nw.
Request-8	Service-HTTP-2; (Nw = 16666.67)	Nw= 20000	Service-HTTP-2 a la valeur Nw la plus faible.

Le diagramme suivant illustre comment le serveur virtuel utilise la méthode des moindres paquets lorsque des pondérations sont attribuées.

Figure 2. Fonctionnement de la méthode des moindres paquets lorsque des poids sont attribués



Pour configurer la méthode des moindres paquets, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

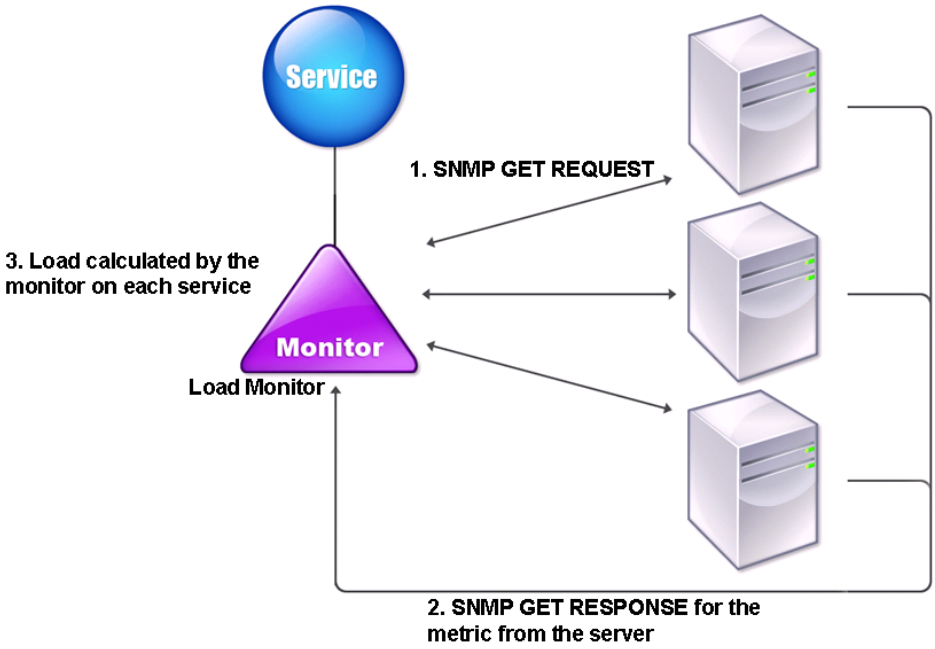
Méthode de chargement personnalisée

October 4, 2021

L'équilibrage de charge personnalisé est effectué sur les paramètres du serveur tels que l'utilisation du processeur, la mémoire et le temps de réponse. Lors de l'utilisation de la méthode de chargement personnalisée, l'appliance Citrix ADC sélectionne généralement un service qui ne gère aucune transaction active. Si tous les services de la configuration d'équilibrage de charge gèrent les transactions actives, l'appliance sélectionne le service avec la charge la plus faible. Un type spécial de moniteur, connu sous le nom de moniteur de charge, calcule la charge sur chaque service du réseau. Les moniteurs de charge ne marquent pas l'état d'un service, mais ils retirent les services de la décision d'équilibrage de charge lorsque ces services ne sont pas UP.

Pour plus d'informations sur les moniteurs de charge, voir Présentation des moniteurs de charge. Le diagramme suivant illustre le fonctionnement d'un moniteur de charge.

Figure 1. Fonctionnement des moniteurs de charge



Le moniteur de charge utilise des sondes SNMP pour calculer la charge sur chaque service en envoyant une demande GET SNMP au service. Cette demande contient un ou plusieurs ID d'objet (OID). Le service répond avec une réponse SNMP GET, avec des mesures correspondant aux OID SNMP. Le moniteur de charge utilise les mesures de réponse pour calculer la charge sur le service.

Le moniteur de charge calcule la charge sur un service en utilisant les paramètres suivants :

- Valeurs de mesures récupérées via les sondes SNMP qui existent sous forme de tables dans l'appliance Citrix ADC.
- Valeur de seuil définie pour chaque mesure.
- Poids attribué à chaque métrique.

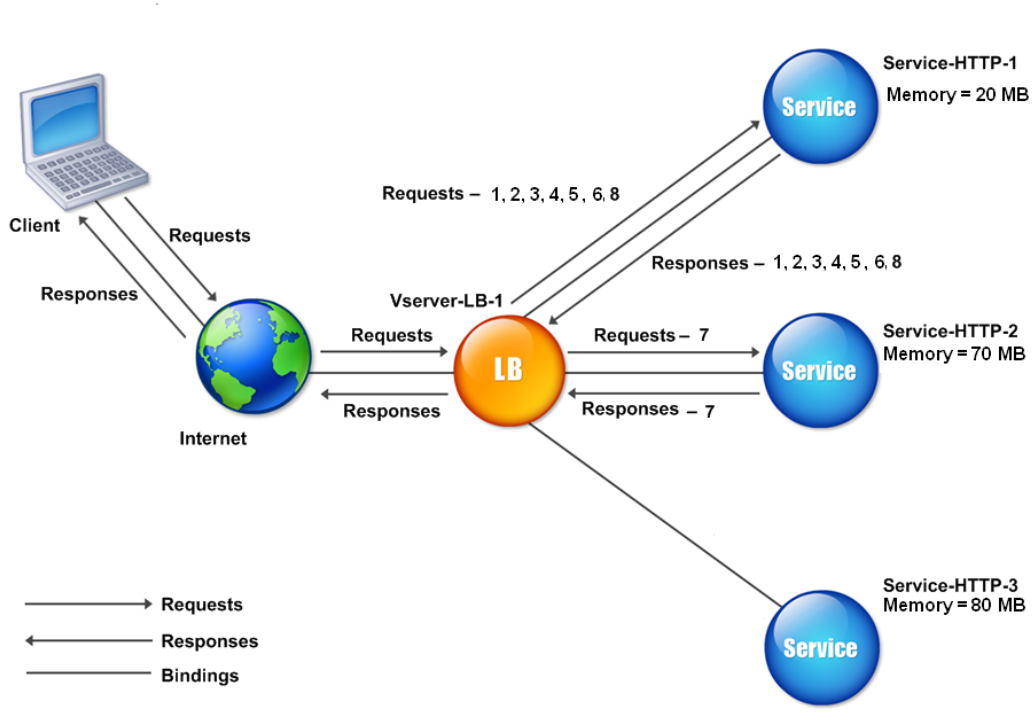
Par exemple, considérez trois services, Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3.

- Le service HTTP-1 utilise 20 Mo de mémoire.
- Service-HTTP-2 utilise 70 Mo de mémoire.
- Service-HTTP-3 utilise 80 Mo de mémoire.

Les serveurs équilibrés de charge peuvent exporter des mesures telles que l'utilisation du processeur et de la mémoire vers les services, qui peuvent à leur tour les fournir au moniteur de charge. Le moniteur de charge envoie aux services une requête GET SNMP contenant les OID

1.3.6.1.4.1.5951.4.1.1.41.1.5, 1.3.6.1.4.1.5951.4.1.1.41.1.4 et 1.3.6.1.4.1.5951.4.1.1.41.1.3. Les OID SNMP de type STRING ne sont pas pris en charge, car vous ne pouvez pas calculer la charge à l'aide d'un OID STRING. Les charges peuvent être calculées à l'aide d'autres types de données, tels que INT et gauge32. Les trois services répondent à la demande. L'appliance Citrix ADC compare les mesures exportées, puis sélectionne Service-HTTP-1 car il dispose de plus de mémoire disponible. Le diagramme suivant illustre ce processus.

Figure 2. Fonctionnement de la méthode de chargement personnalisée



Si chaque requête utilise 10 Mo de mémoire, l'appliance Citrix ADC fournit les demandes comme suit :

- Service-HTTP-1 reçoit les première, deuxième, troisième, quatrième et cinquième requêtes, car ce service a la valeur N la plus faible.
- Service-HTTP-1 et Service-HTTP-2 ont maintenant la même charge, de sorte que le serveur virtuel revient à la méthode round robin pour ces serveurs. Par conséquent, Service-HTTP-2 reçoit la sixième requête, et Service-HTTP-1 reçoit la septième requête.
- Puisque Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont tous la même charge, le serveur virtuel revient également à la méthode round robin pour Service-HTTP-3. Par conséquent, Service-HTTP-3 reçoit la huitième requête.

Le tableau suivant résume le mode de calcul de N.

Demande reçue	Service sélectionné	Valeur N actuelle (nombre de transactions actives)	Remarques
Request-1	Service-HTTP-1 ; (N = 20)	N = 30	Service-HTTP-3 a la valeur N la plus faible.
Request-2	Service-HTTP-1 ; (N = 30)	N = 40	-
Request-3	Service-HTTP-1 ; (N = 40)	N = 50	-
Request-4	Service-HTTP-1 ; (N = 50)	N = 60	-
Request-5	Service-HTTP-1 ; (N = 60)	N = 70	-
Request-6	Service-HTTP-1 ; (N = 70)	N = 80	Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.
Request-7	Service-HTTP-2 ; (N = 70)	N = 80	Service-HTTP-3 ont les mêmes valeurs N.
Request-8	Service-HTTP-1 ; (N = 80)	N = 90	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.

Si des pondérations différentes sont attribuées aux services, l'algorithme de chargement personnalisé tient compte à la fois de la charge sur chaque service et de la pondération attribuée à chaque service. Il sélectionne un service en utilisant la valeur (Nw) dans l'expression suivante :

Nw = (N) * (10000/pondération)

Comme dans l'exemple précédent, supposons que Service-HTTP-1 se voit attribuer un poids de 4, Service-HTTP-2 se voit attribuer un poids de 3 et Service-HTTP-3 un poids de 2. Si chaque requête utilise 10 Mo de mémoire, l'appliance Citrix ADC fournit les demandes comme suit :

- Service-HTTP-1 reçoit les première, deuxième, troisième, quatrième, cinquième, sixième, septième et huitième requêtes, car ce service a la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la neuvième requête, car ce service a la valeur Nw la plus faible.

Service-HTTP-3 a la valeur Nw la plus élevée et n'est donc pas pris en compte pour l'équilibrage de

charge.

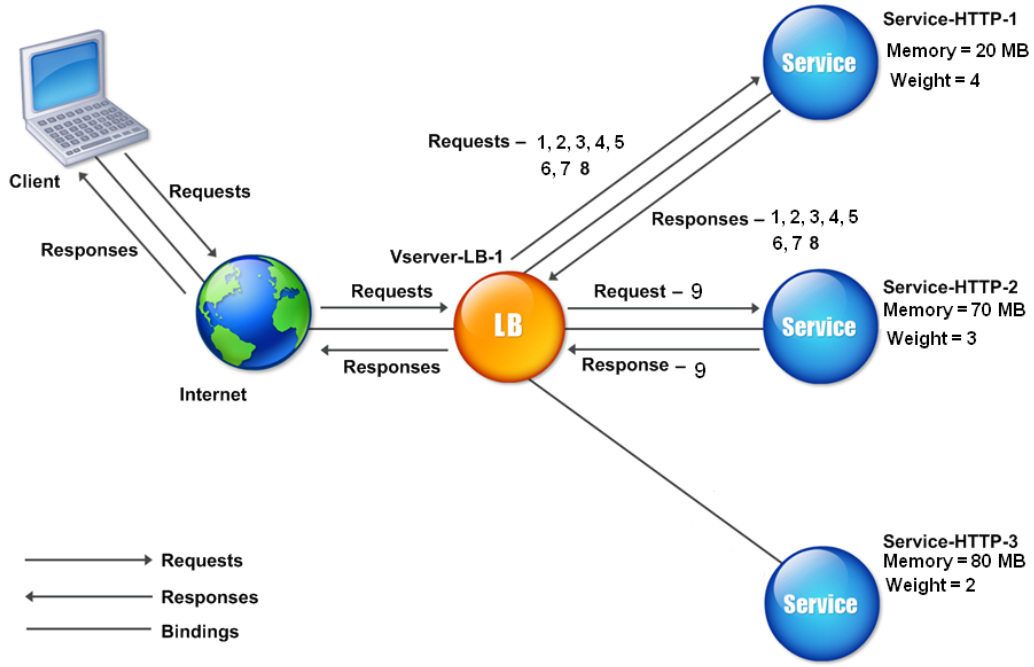
Le tableau suivant résume la façon dont Nw est calculé.

Demande reçue	Service sélectionné	Valeur Nw actuelle (nombre de transactions actives) * (10000/pondération)	Remarques
Request-1	Service-HTTP-1 ; (Nw = 50000)	Nw = 75000	Service-HTTP-1 a la valeur Nw la plus faible.
Request-2	Service-HTTP-1 ; (Nw = 5000)	Nw = 100000	-
Request-3	Service-HTTP-1; (Nw = 15000)	Nw = 125000	-
Request-4	Service-HTTP-1 ; (Nw = 20000)	Nw = 150000	-
Request-5	Service-HTTP-1 ; (Nw = 23333,34)	Nw = 175000	-
Request-6	Service-HTTP-1 ; (Nw = 25000)	Nw = 200000	-
Request-7	Service-HTTP-1 ; (Nw = 23333,34)	Nw = 225000	-
request-8	service-http-1 ; (Nw = 25000)	Nw = 250000	-
request-9	service-http-2 ; (Nw = 233333.34)	Nw = 266666.67	Le service-HTTP-2 a la valeur Nw la plus faible.

Service-HTTP-1 est sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives ou lorsque la valeur Nw des autres services (Service-HTTP-2 et Service-HTTP-3) est égale à 400 000.

Le diagramme suivant illustre la façon dont l'appliance Citrix ADC utilise la méthode de chargement personnalisée lorsque des poids sont affectés.

Figure 3. Fonctionnement de la méthode de chargement personnalisée lorsque des poids sont affectés



Pour configurer la méthode de chargement personnalisée, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode de proximité statique

August 20, 2021

Lorsqu'un serveur virtuel est configuré pour utiliser la méthode de proximité statique, il sélectionne le service qui correspond le mieux aux critères de proximité.

Pour que la méthode de proximité statique fonctionne, vous devez soit configurer l'appliance Citrix ADC pour qu'elle utilise une base de données de proximité statique existante remplie via un fichier d'emplacement, soit ajouter des entrées personnalisées à la base de données de proximité statique. Après avoir ajouté des entrées personnalisées, vous pouvez définir leurs qualificatifs d'emplacement. Après avoir configuré la base de données, vous êtes prêt à spécifier la proximité statique comme méthode d'équilibrage de charge.

Pour plus de détails, consultez les rubriques suivantes.

- Ajout d'un fichier d'emplacement pour créer une base de données de proximité statique
- Ajout d'entrées personnalisées à une base de données de proximité statique
- Définition des qualificatifs d'emplacement
- Spécification de la méthode Proximité statique

Spécification de la méthode de proximité

Lorsque vous avez configuré la base de données de proximité statique, vous êtes prêt à spécifier la proximité statique comme méthode GLSB.

Pour spécifier la proximité statique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la proximité statique et vérifier la configuration :

```
set lb vserver <name> -lbMethod STATICPROXIMITY

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -lbMethod STATICPROXIMITY

show lb vserver
<!--NeedCopy-->
```

Pour spécifier la proximité statique à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et sélectionnez le serveur virtuel.
2. Cliquez sur **Modifier** et développez la section **Méthode** .
3. Dans la liste **Méthode d'équilibrage** de charge, sélectionnez **STATICPROXIMITY**.

Méthode de jeton

August 20, 2021

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode jeton fonde sa sélection d'un service sur la valeur d'un segment de données extrait de la demande client. Le segment de données est appelé le jeton. Vous configurez l'emplacement et la taille du jeton. Pour les demandes suivantes avec le même jeton, le serveur virtuel choisit le même service qui a traité la demande initiale.

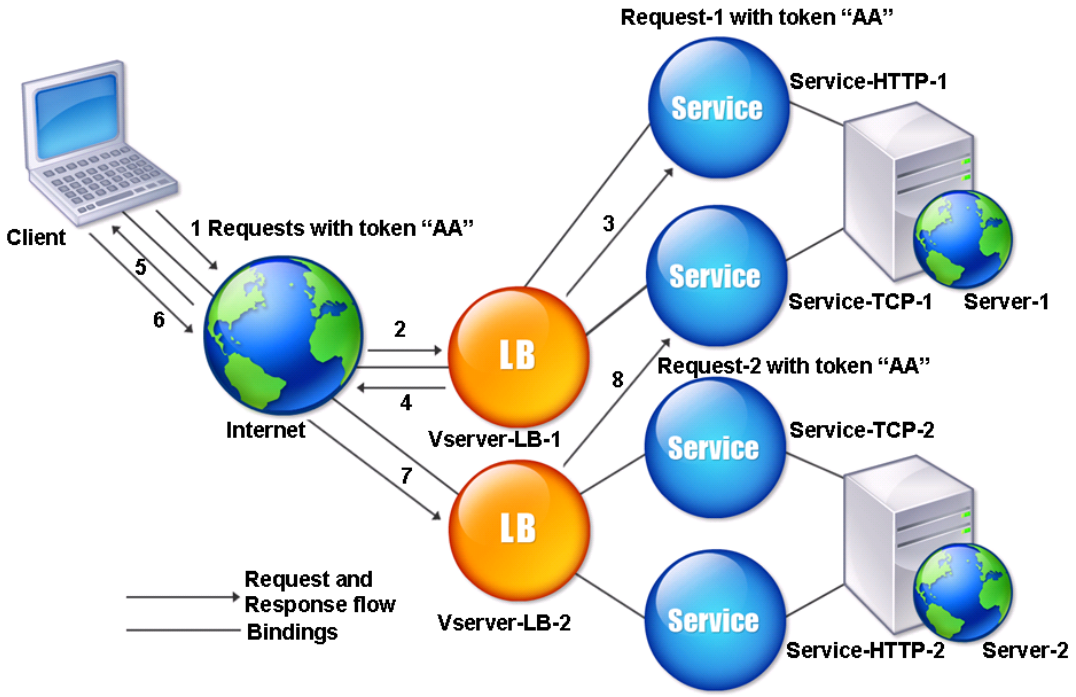
Cette méthode est consciente du contenu. Il fonctionne différemment pour les connexions TCP, HTTP et HTTPS. Pour les services HTTP ou HTTPS, le jeton se trouve dans les en-têtes HTTP, l'URL ou le BODY. Pour localiser le jeton, vous spécifiez ou créez une expression classique ou avancée. Pour plus d'informations sur les expressions classiques ou avancées, voir Configuration et référence des stratégies.

Pour les services HTTP, le serveur virtuel recherche le jeton configuré dans les 24 premiers kilo-octets (Ko) de la charge utile TCP. Pour les services non HTTP (TCP, SSL et SSL_TCP), le serveur virtuel recherche le jeton configuré dans les 16 premiers paquets si la taille totale des 16 paquets est inférieure à 24 Ko. Mais si la taille totale des 16 paquets est supérieure à 24 Ko, l'appliance recherche le jeton dans les 24 premiers Ko de charge utile. Vous pouvez utiliser cette méthode d'équilibrage de charge sur des serveurs virtuels de différents types pour vous assurer que les demandes présentant le même jeton sont dirigées vers les services appropriés, quel que soit le protocole utilisé.

Par exemple, considérez une configuration d'équilibrage de charge composée de serveurs contenant du contenu Web. Vous souhaitez configurer l'appliance Citrix ADC pour rechercher une chaîne spécifique (le jeton) à l'intérieur de la partie requête URL de la requête. Server-1 a deux services, Service-HTTP-1 et Service-TCP-1, et Server-2 a deux services, Service-HTTP-2 et Service-TCP-2. Les services TCP sont liés à vServer-lb-2 et les services HTTP sont liés à vServer-lb-1.

Si vServer-lb-1 reçoit une requête avec le jeton AA, il sélectionne le service service-HTTP-1 (lié au serveur-1) pour traiter la demande. Si VServer-LB-2 reçoit une demande différente avec le même jeton (AA), il dirige cette demande vers le service Service-TCP-1. Le diagramme suivant illustre ce processus.

Figure 1. Fonctionnement de la méthode jeton



Pour configurer la méthode d'équilibrage de charge Token à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la méthode d'équilibrage de charge de jeton et vérifier la configuration :

```
set lb vserver <name> -lbMethod TOKEN -rule <rule> -datalength <length>
    -dataoffset <offset>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver LB-VServer-1 -lbMethod TOKEN -rule 'AA' -datalength 2 -
   dataoffset 25

show lb vserver LB-VServer-1
<!--NeedCopy-->
```


Pour configurer la méthode d'équilibrage de charge de jeton à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans Paramètres avancés, cliquez sur Méthode
3. Dans la liste Méthode d'équilibrage de charge, sélectionnez Token et spécifiez une expression.

Configurer une méthode d'équilibrage de charge qui n'inclut pas de stratégie

August 20, 2021

Après avoir sélectionné un algorithme d'équilibrage de charge pour votre configuration d'équilibrage de charge, vous devez configurer l'appliance Citrix ADC pour qu'elle utilise cet algorithme. Vous pouvez le configurer à l'aide de l'interface de ligne de commande ou de l'utilitaire de configuration.

Remarque :

La méthode jeton est basée sur une stratégie et nécessite plus de configuration que ce qui est décrit ici. Pour configurer la méthode du jeton, reportez-vous à la section Méthode Token.

Pour certaines méthodes basées sur le hachage, vous pouvez masquer une adresse IP pour diriger les requêtes appartenant au même sous-réseau vers le même serveur. Pour plus d'informations, voir Méthodes de hachage.

Pour définir la méthode d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -lbMethod <method>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -lbMethod LeastConnection
<!--NeedCopy-->
```


Pour définir la méthode d'équilibrage de charge à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, cliquez sur **Méthode**et dans la liste Méthode d'équilibrage de charge, sélectionnez une méthode.

Persistance et connexions persistantes

August 20, 2021

Un protocole sans état d'équilibrage de charge, tel que HTTP, perturbe la maintenance des informations d'état relatives aux connexions client si la persistance n'est pas configurée. Différentes transmissions provenant d'un même client peuvent être dirigées vers différents serveurs, même si toutes les transmissions font partie de la même session. Vous pouvez configurer la persistance sur un serveur virtuel d'équilibrage de charge qui gère certains types d'applications Web, telles que les applications de panier d'achat.

Avant de pouvoir configurer la persistance, vous devez comprendre les différents types de persistance, comment ils sont utilisés et quelles sont les implications de chaque type. Vous devez ensuite configurer l'appliance Citrix ADC pour fournir des connexions persistantes aux sites Web et aux applications Web qui en ont besoin.

Vous pouvez également configurer la persistance des sauvegardes, qui prend effet si le type principal de persistance configuré pour un serveur virtuel d'équilibrage de charge échoue. Vous pouvez configurer des groupes de persistance afin qu'une transmission client vers n'importe quel serveur virtuel d'un groupe puisse être dirigée vers un serveur qui a reçu des transmissions précédentes du même client.

Pour plus d'informations sur la persistance avec l'équilibrage de charge RADIUS, voir Configuration de l'équilibrage de charge RADIUS avec persistance.

À propos de la persistance

August 20, 2021

Vous pouvez choisir parmi plusieurs types de persistance pour un serveur virtuel d'équilibrage de charge donné, qui achemine ensuite vers le même service toutes les connexions du même utilisateur vers votre application de panier, votre messagerie Web ou toute autre application réseau. La session de persistance reste en vigueur pendant la durée spécifiée.

Si un serveur participant à une session de persistance est désactivé, le serveur virtuel d'équilibrage de charge utilise la méthode d'équilibrage de charge configurée pour sélectionner un nouveau service et établit une nouvelle session de persistance avec le serveur représenté par ce service. Si le serveur est hors service, il continue de traiter les sessions de persistance existantes, mais le serveur virtuel n'y dirige aucun nouveau trafic. Après l'expiration de la période d'arrêt, le serveur virtuel cesse de diriger les connexions des clients existants vers le service, ferme les connexions existantes et redirige ces clients vers de nouveaux services si nécessaire.

Selon le type de persistance que vous configurez, l'appliance Citrix ADC peut examiner les adresses IP source, les adresses IP de destination, les ID de session SSL, les en-têtes d'hôte ou d'URL, ou une combinaison de ces éléments pour placer chaque connexion dans la session de persistance appropriée. Elle peut également baser la persistance sur un cookie émis par le serveur Web, sur un jeton assigné arbitrairement ou sur une règle logique. Presque tout ce qui permet à l'appliance de faire correspondre les connexions à la session de persistance appropriée et sert de base à la persistance.

Le tableau suivant récapitule les types de persistance disponibles sur l'appliance Citrix ADC.

Type de persistance	Description
IP source	SOURCEIP. Les connexions à partir de la même adresse IP du client font partie de la même session de persistance.
Cookie HTTP	COOKIEINSERT. Les connexions qui ont le même en-tête de cookie HTTP font partie de la même session de persistance.
ID de session SSL	SSLSESSION. Les connexions qui ont le même ID de session SSL font partie de la même session de persistance.
URL passive	URLPASSIVE. Les connexions à la même URL sont traitées comme des parties de la même session de persistance.
ID de serveur personnalisé	CUSTOMSERVERID. Les connexions avec le même en-tête HTTP HOST sont traitées comme des parties de la même session de persistance.
IP destination	DESTIP. Les connexions à la même adresse IP de destination sont traitées comme des parties de la même session de persistance.

Type de persistance	Description
IP source et destination	SRCIPDESTIP. Les connexions qui proviennent à la fois de la même adresse IP source et de la même adresse IP de destination sont traitées comme des parties de la même session de persistance.
ID d'appel SIP	CALLID. Les connexions qui ont le même ID d'appel dans l'en-tête SIP sont traitées comme des parties de la même session de persistance.
ID de session RTSP	RTSPSID. Les connexions qui ont le même ID de session RTSP sont traitées comme des parties de la même session de persistance.
Règle définie par l'utilisateur	RULE. Les connexions qui correspondent à une règle définie par l'utilisateur sont traitées comme des parties de la même session de persistance.

Tableau 1. Types de persistance

Selon le type de persistance que vous avez configuré, le serveur virtuel peut prendre en charge 250 000 connexions persistantes simultanées ou n'importe quel nombre de connexions persistantes jusqu'à concurrence des limites imposées par la quantité de RAM de votre appliance Citrix ADC. Le tableau suivant montre quels types de persistance appartiennent à chaque catégorie.

Type de persistance	Nombre de connexions persistantes simultanées prises en charge
IP source, ID de session SSL, règle, adresse IP de destination, adresse IP source, adresse IP de destination, ID d'appel SIP, ID de session RTSP	250 K
Cookie, ID de serveur URL, ID de serveur personnalisé	Limite de mémoire. Dans CookieInsert, si le délai d'expiration n'est pas 0, le nombre de connexions est limité par la mémoire.

Tableau 2. Types de persistance et nombre de connexions simultanées prises en charge

Certains types de persistance sont spécifiques à des types particuliers de serveur virtuel. Le tableau suivant répertorie chaque type de persistance et indique quels types de persistance sont pris en charge sur quels types de serveur virtuel.

Type de persis-tance	HTTP	HTTPS	TCP	UDP/IP	SSL_Pont	SSL_TCP	RTSP	SIP_UDP
SOURCEI	OUI	OUI	OUI	OUI	OUI	OUI	NON	NON
COOKIEINSERT	OUI	OUI	NON	NON	NON	NON	NON	NON
SSLSESS	NON	OUI	NON	NON	OUI	OUI	NON	NON
URLPASSIVE	OUI	OUI	NON	NON	NON	NON	NON	NON
CUSTOM	OUI	OUI	NON	NON	NON	NON	NON	NON
RULE	OUI	OUI	OUI	NON	NON		NON	NON
SRCIPDE	OUI	OUI	OUI	OUI	OUI	OUI	NON	NON
DESTIP	OUI	OUI	OUI	OUI	OUI	OUI	NON	NON
CALLID	NON	NON	NON	NON	NON	NON	NON	OUI
RTSPID	NON	NON	NON	NON	NON	NON	OUI	NON

Tableau 3. Relation entre le type de persistance et le type de serveur virtuel

Persistance de l’adresse IP source

August 20, 2021

Lorsque la persistance de l’adresse IP source est configurée, le serveur virtuel d’équilibrage de charge utilise la méthode d’équilibrage de charge configurée pour sélectionner un service pour la demande initiale, puis utilise l’adresse IP source (adresse IP du client) pour identifier les demandes suivantes de ce client et les envoyer au même service. Vous pouvez définir une valeur de délai d’attente, qui spécifie la période maximale d’inactivité pour la session. Lorsque la valeur de délai d’expiration expire, la session est ignorée et l’algorithme d’équilibrage de charge configuré est utilisé pour sélectionner un nouveau serveur.

Attention : Dans certains cas, l’utilisation de la persistance basée sur l’adresse IP source peut surcharger vos serveurs. Toutes les demandes adressées à un seul site Web ou à une application sont acheminées via la passerelle unique vers l’appliance Citrix ADC, même si elles sont ensuite redirigées vers plusieurs emplacements. Dans plusieurs environnements proxy, les demandes des clients ont souvent des adresses IP source différentes, même lorsqu’elles sont envoyées à partir du même client, ce qui entraîne une multiplication rapide des sessions de persistance où une seule session doit être créée. Ce problème s’appelle “Mega Proxy problem”. Vous pouvez utiliser la persistance basée sur les cookies HTTP au lieu de la persistance basée sur l’IP source pour empêcher cela de se produire.

Pour configurer la persistance en fonction de l'adresse IP source, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Remarque : si tout le trafic entrant provient derrière un périphérique NAT (Network Address Translation) ou un proxy, le trafic apparaît à l'appliance Citrix ADC comme provenant d'une seule adresse IP source. Cela empêche la persistance de l'IP source de fonctionner correctement. Dans ce cas, vous devez sélectionner un autre type de persistance.

Persistance des cookies HTTP

August 20, 2021

Lorsque la persistance des cookies HTTP est configurée, l'appliance Citrix ADC définit un cookie dans les en-têtes HTTP de la demande client initiale. Le cookie contient l'adresse IP et le port du service sélectionné par l'algorithme d'équilibrage de charge. Comme pour toute connexion HTTP, le client inclut ensuite ce cookie avec toutes les requêtes ultérieures.

Lorsque l'appliance Citrix ADC détecte le cookie, elle transmet la demande à l'adresse IP du service et au port dans le cookie, en conservant la persistance de la connexion. Vous pouvez utiliser ce type de persistance avec des serveurs virtuels de type HTTP ou HTTPS. Ce type de persistance ne consomme pas de ressources d'appliance et peut donc accueillir un nombre illimité de clients persistants.

Remarque : Si le navigateur Web du client est configuré pour refuser les cookies, la persistance basée sur les cookies HTTP ne fonctionne pas. Il peut être conseillé de configurer une vérification des cookie sur le site Web et d'avertir les clients qui ne semblent pas stocker correctement les cookies qu'ils doivent activer les cookies pour le site Web s'ils souhaitent les utiliser.

Le format du cookie que l'appliance Citrix ADC insère est le suivant :

```
NSC_XXXX=<ServiceIP ><ServicePort>
```

Où :

- NSC_XXXX est l'ID du serveur virtuel dérivé du nom du serveur virtuel.
- ServiceIP et ServicePort sont des représentations codées de l'adresse IP du service et du port de service, respectivement. L'adresse IP et le port sont codés séparément.

Vous pouvez définir une valeur de délai d'attente pour ce type de persistance afin de spécifier une période d'inactivité pour la session. Lorsque la connexion est inactive pendant la période spécifiée, l'appliance Citrix ADC rejette la session de persistance. Toute connexion ultérieure à partir du même client entraîne la sélection d'un nouveau serveur en fonction de la méthode d'équilibrage de charge configurée et l'établissement d'une nouvelle session de persistance.

Remarque : si vous définissez la valeur de délai d'expiration sur 0, l'appliance Citrix ADC ne spécifie pas

de délai d'expiration, mais définit un cookie de session qui n'est pas enregistré lorsque le navigateur du client est arrêté.

Par défaut, l'appliance Citrix ADC définit les cookies HTTP version 0 pour une compatibilité maximale avec les navigateurs clients. (Seuls certains proxy HTTP comprennent les cookies de la version 1 ; les navigateurs les plus couramment utilisés ne le font pas.) Vous pouvez configurer l'appliance pour définir les cookies HTTP version 1, afin de respecter la norme RFC2109. Pour les cookies HTTP version 0, l'appliance insère la date et l'heure d'expiration du cookie en tant que temps universel coordonné (GMT) absolu. Il calcule cette valeur comme la somme de l'heure GMT actuelle sur l'appliance et de la valeur de délai d'expiration. Pour les cookies HTTP version 1, l'appliance insère un délai d'expiration relatif en définissant l'attribut « Max-Age » du cookie HTTP. Dans ce cas, le navigateur du client calcule le temps d'expiration réel.

Pour configurer la persistance en fonction d'un cookie inséré par l'appliance, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Dans le cookie HTTP, l'appliance définit par défaut l'`HTTPOnly` indicateur pour indiquer que le cookie n'est pas scriptable et ne doit pas être révélé à l'application cliente. Par conséquent, un script côté client ne peut pas accéder au cookie et le client n'est pas sensible aux scripts intersites.

Cependant, certains navigateurs ne prennent pas en charge l'`HTTPOnly` indicateur et, par conséquent, risquent de ne pas renvoyer le cookie. En conséquence, la persistance est brisée. Pour les navigateurs qui ne prennent pas en charge l'indicateur, vous pouvez omettre l'`HTTPOnly` indicateur dans le cookie de persistance.

Pour modifier le paramètre d'`HTTPOnly` indicateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb parameter -httpOnlyCookieFlag (ENABLED|DISABLED)
<!--NeedCopy-->
```

Exemple :

```
>  set lb parameter -httpOnlyCookieFlag disabled
   Done
> show lb parameter
  Global LB parameters:
       Persistence Cookie HttpOnly Flag: DISABLED
       Use port for hash LB: YES
 Done
<!--NeedCopy-->
```


Pour modifier le paramètre d' HTTPOnly indicateur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge**, puis sélectionnez ou désactivez l'indicateur **HttpOnly Cookie de persistance** .

Cryptage du cookie

À partir de la version 10.5 build 55.8, vous pouvez crypter le cookie en plus de n'importe quel cryptage SSL.

Pour chiffrer le cookie à l'aide de l'interface de ligne de commande, à l'invite de commande, tapez

```
1 set lb parameter -UseEncryptedPersistenceCookie ENABLED -
     cookiePassphrase test
2 <!--NeedCopy-->
```

Pour chiffrer le cookie à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Modifier les paramètres d'équilibrage** de la charge, puis sélectionnez **Encoder les valeurs de cookie de persistance** et entrez une phrase secrète dans la **phrase secrète de cookie** .

Persistance de l'ID de session SSL

August 20, 2021

Lorsque la persistance de l'ID de session SSL est configurée, l'appliance Citrix ADC utilise l'ID de session SSL, qui fait partie du processus de négociation SSL, pour créer une session de persistance avant que la demande initiale ne soit dirigée vers un service. Le serveur virtuel d'équilibrage de charge dirige les demandes suivantes qui ont le même ID de session SSL vers le même service. Ce type de persistance est utilisé pour les services de pont SSL.

Remarque :

Les utilisateurs doivent prendre en compte deux problèmes avant de choisir ce type de persistance. Tout d'abord, ce type de persistance consomme des ressources sur l'appliance Citrix ADC, ce qui limite le nombre de sessions de persistance simultanées qu'il peut prendre en charge. Si vous prévoyez de prendre en charge plusieurs sessions de persistance, vous pouvez choisir un autre type de persistance.

Deuxièmement, si le client et le serveur à charge équilibrée doivent renégocier l'ID de session pendant leurs transactions, la persistance n'est pas maintenue et une nouvelle session de persistance est créée lors de la réception de la prochaine demande du client. Cela peut entraîner l'interruption de l'activité du client sur le site Web et il peut être demandé au client de se réauthentifier ou de redémarrer la session. Cela peut également entraîner un grand nombre de sessions abandonnées si le délai d'attente est défini sur une valeur trop importante.

Pour configurer la persistance en fonction de l'ID de session SSL, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

> **Remarque**
>
> La persistance des ID de session SSL n'est pas prise en charge avec les tickets de session.

Prise en charge de la persistance de sauvegarde pour l'ID de session SSL

À partir de NetScaler version 12.0 build 56.20, la persistance IP source est prise en charge en tant que type de persistance de sauvegarde pour la persistance de l'ID de session SSL. Si le client et le serveur à équilibrage de charge renégocient la session et que la persistance de l'IP source est configurée comme persistance de sauvegarde, les demandes du client sont transmises au même serveur.

Pour prendre en charge la persistance des sauvegardes pour l'ID de session SSL, l'appliance Citrix ADC crée des entrées de session pour l'IP source et l'ID de session SSL lorsqu'une demande client est reçue pour la première fois. Pour les demandes suivantes contenant le même ID de session, l'ID de session SSL est utilisé. Toutefois, lorsque le client et le serveur à équilibrage de charge renégocient la session, la demande du client est transmise au même serveur à l'aide de la persistance IP source et une nouvelle entrée de persistance SSL ID de session est créée.

Pour plus d'informations sur la configuration de la persistance des sauvegardes, voir Configuration de la persistance des sauvegardes.

Persistance du nombre AVP de Diameter

August 20, 2021

Vous pouvez utiliser la persistance basée sur le numéro AVP (Attribute-Valeur Paire) d'un message Diameter pour créer des sessions Diameter persistantes. Lorsque l'appliance Citrix ADC trouve l'AVP dans le message Diameter, il crée une session de persistance basée sur la valeur de l'AVP. Tous les messages suivants qui correspondent à la valeur de l'AVP sont dirigés vers le serveur précédemment sélectionné. Si la valeur de l'AVP ne correspond pas à la session de persistance, une nouvelle session est créée pour la nouvelle valeur.

Remarque : Si le numéro AVP n'est pas défini dans le protocole de base de diamètre RFC 6733, et si le numéro est imbriqué dans un AVP groupé, vous devez définir une séquence de numéros AVP (maximum 3) dans l'ordre parent-enfant. Par exemple, si le numéro AVP X persiste est imbriqué dans AVP Y, qui est imbriqué dans Z, définissez la liste comme Z Y X.

Pour configurer la persistance basée sur le Diameter sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set lb vserver <name> -PersistenceType <type-> persistAVPno <
   positive_integer>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver diameter_vs -persistenceType DIAMETER -persistAVPno 263
<!--NeedCopy-->
```

Persistance de l'ID de serveur personnalisé

August 20, 2021

Dans la méthode de persistance de l'ID de serveur personnalisé, l'ID de serveur spécifié dans la demande client est utilisé pour maintenir la persistance. Pour que ce type de persistance fonctionne, vous devez d'abord définir un ID de serveur sur les services. L'appliance Citrix ADC vérifie l'URL de la demande client et se connecte au serveur associé à l'ID de serveur spécifié. Le fournisseur de services doit s'assurer que les utilisateurs connaissent les ID de serveur à fournir dans leurs demandes de services spécifiques.

Par exemple, si votre site fournit différents types de données, tels que des images, du texte et du multimédia, provenant de différents serveurs, vous pouvez attribuer un ID de serveur à chaque serveur. Sur l'appliance Citrix ADC, vous spécifiez ces ID de serveur pour les services correspondants et vous configurez la persistance de l'ID de serveur personnalisé sur le serveur virtuel d'équilibrage de charge correspondant. Lors de l'envoi d'une demande, le client insère l'ID du serveur dans l'URL indiquant le type de données requis.

Pour configurer la persistance de l'ID de serveur personnalisé :

- Dans votre configuration d'équilibrage de charge, attribuez un ID de serveur à chaque service pour lequel vous souhaitez utiliser l'ID de serveur défini par l'utilisateur pour maintenir la persistance. Les ID de serveur alphanumériques sont autorisés.

- Spécifiez des règles, dans le langage d'expression de syntaxe par défaut, pour examiner les requêtes d'URL pour l'ID du serveur et transférer le trafic vers le serveur correspondant.
- Configurez la persistance de l'ID de serveur personnalisé.

Remarque : la valeur de délai d'expiration de la persistance n'affecte pas le type de persistance de l'ID de serveur personnalisé. Il n'y a pas de limite sur le nombre maximal de clients persistants car ce type de persistance ne stocke aucune information client.

Exemple :

Dans une configuration d'équilibrage de charge avec deux services, attribuez l'ID de serveur 2345-photo-56789 à Service-1 et l'ID de serveur 2345-drawing-abb123 à Service-2. Liez ces services à un serveur virtuel nommé Web11.

```
set service Service-1 10.102.29.5 -CustomServerID 2345-photo-56789

set service Service-2 10.102.29.6 -CustomServerID 2345-drawing-abb123
<!--NeedCopy-->
```

Sur le serveur virtuel Web11, activez la persistance de l'ID de serveur personnalisé.

Créez l'expression suivante afin que toutes les requêtes d'URL contenant la chaîne « sid= » soient examinées.

HTTP.REQ.URL.AFTER_STR (« sid= »)

Exemple :

```
set lb vserver Web11 -persistenceType customserverID -rule "HTTP.REQ.
   URL.AFTER_STR("sid=")"

bind lb vserver Web11 Service-[1-2]
<!--NeedCopy-->
```

Lorsqu'un client envoie une demande avec l'URL suivante à l'adresse IP de Web11, l'appliance dirige la demande vers Service-2 et respecte la persistance.

Exemple :

```
http://www.example.com/index.asp?&sid=2345-drawing-abb123
```

Pour plus d'informations sur les expressions de stratégie de syntaxe par défaut, reportez-vous à la section Configuration et référence des stratégies.

Pour configurer la persistance de l'ID de serveur personnalisé à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.

2. Ouvrez le service et définissez un ID de serveur.
3. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez le serveur virtuel.
4. Dans Paramètres avancés, sélectionnez Persistance.
5. Sélectionnez CUSTOMESERVERID et spécifiez une expression.

Persistance de l'adresse IP

August 20, 2021

Vous pouvez baser la persistance sur les adresses IP de destination, ou sur les adresses IP source et IP de destination.

Persistance basée sur les adresses IP de destination

Avec la persistance basée sur l'adresse IP de destination, lorsque l'appliance Citrix ADC reçoit une demande d'un nouveau client, elle crée une session de persistance basée sur l'adresse IP du service sélectionné par le serveur virtuel (l'adresse IP de destination). Plus tard, il dirige les demandes vers la même adresse IP de destination vers le même service. Ce type de persistance est utilisé avec l'équilibrage de charge de liaison. Pour plus d'informations sur l'équilibrage de charge des liaisons, voir Équilibrage de charge de liaison.

La valeur de délai d'expiration pour la persistance IP de destination est la même que pour la persistance IP source, décrite dans Persistance basée sur l'adresse IP source.

Pour configurer la persistance en fonction de l'adresse IP de destination, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Persistance basée sur les adresses IP source et destination

Avec la persistance basée sur l'adresse IP source et de destination, lorsque l'appliance Citrix ADC reçoit une demande, elle crée une session de persistance basée à la fois sur l'adresse IP du client (l'adresse IP source) et sur l'adresse IP du service sélectionné par le serveur virtuel (l'adresse IP de destination). Plus tard, il dirige les demandes provenant de la même adresse IP source et vers la même adresse IP de destination vers le même service.

La valeur de délai d'expiration pour la persistance IP de destination est la même que pour la persistance IP source, décrite dans Persistance basée sur l'adresse IP source.

Pour configurer la persistance en fonction des adresses IP source et de destination, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Persistance de l'ID d'appel SIP

August 20, 2021

Avec la persistance de l'ID d'appel SIP, l'appliance Citrix ADC choisit un service en fonction de l'ID d'appel dans l'en-tête SIP. Cela lui permet de diriger les paquets d'une session SIP particulière vers le même service et, par conséquent, vers le même serveur équilibré de charge. Ce type de persistance s'applique spécifiquement à l'équilibrage de charge SIP. Pour plus d'informations sur l'équilibrage de charge SIP, voir Surveillance des services SIP.

Pour configurer la persistance en fonction de l'ID d'appel SIP, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Persistance de l'ID de session RTSP

August 20, 2021

Avec la persistance de l'ID de session RTSP, lorsque l'appliance Citrix ADC reçoit une demande d'un nouveau client, elle crée une session de persistance basée sur l'ID de session RTSP (Real-Time Streaming Protocol) dans l'en-tête du paquet RTSP, puis dirige la demande vers le service RTSP sélectionné par l'équilibrage de charge configuré. méthode. Il dirige les demandes suivantes qui contiennent le même ID de session vers le même service. Ce type de persistance s'applique spécifiquement à l'équilibrage de charge SIP. Pour plus d'informations sur l'équilibrage de charge SIP, voir Surveillance des services SIP.

Remarque : la persistance de l'ID de session RTSP est configurée par défaut sur les serveurs virtuels RTSP, et vous ne pouvez pas modifier ce paramètre.

Parfois, différents serveurs RTSP émettent les mêmes ID de session. Lorsque cela se produit, des sessions uniques ne peuvent pas être créées entre le client et le serveur RTSP en utilisant uniquement l'ID de session RTSP. Si plusieurs serveurs RTSP peuvent émettre les mêmes ID de session, vous pouvez configurer l'appliance pour ajouter l'adresse IP du serveur et le port à l'ID de session, créant ainsi un jeton unique qui peut être utilisé pour établir la persistance. Il s'agit du mappage des ID de session.

Pour configurer la persistance en fonction des ID de session RTSP, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Important : si vous devez utiliser le mappage d'ID de session, vous devez définir le paramètre suivant lors de la configuration de chaque service au sein de la configuration d'équilibrage de charge. Assurez-vous également qu'aucune connexion non persistante n'est routée via le serveur virtuel RTSP.

Configurer la persistance passive des URL

August 20, 2021

Avec la persistance passive de l'URL, lorsque l'appliance Citrix ADC reçoit une demande d'un client, elle extrait les informations de port d'adresse IP du serveur (exprimées sous la forme d'un seul nombre hexadécimal) de la demande du client.

La persistance passive des URL nécessite la configuration d'une expression avancée qui spécifie l'élément de requête contenant les informations de port d'adresse IP du serveur. Pour plus d'informations sur les expressions de stratégie classiques et avancées, voir Stratégies et expressions.

L'expression suivante configure l'appliance pour qu'elle examine les requêtes d'URL contenant la chaîne « urlp= », extraire les informations de port d'adresse IP du serveur, les convertit d'une chaîne hexadécimale en adresse IP et numéro de port, puis transfère la requête au service configuré avec cette adresse IP et numéro de port.

HTTP.REQ.URL.AFTER_STR (« urlp= »)

Si la persistance passive d'URL est activée et que l'expression précédente est configurée, une demande avec l'URL et la chaîne de port d'adresse IP du serveur suivantes est dirigée vers 10.102.29.10:80.

```
http://www.example.com/index.asp?&urlp=0A661D0A0050
```

La valeur du délai d'attente de persistance n'affecte pas ce type de persistance. La persistance est maintenue tant que les informations du port d'adresse IP du serveur peuvent être extraites des demandes des clients. Ce type de persistance ne consomme pas de ressources d'appliance, de sorte qu'il peut accueillir un nombre illimité de clients persistants.

Pour configurer la persistance passive des URL, vous devez d'abord configurer la persistance comme décrit dans Configuration des types de persistance qui ne nécessitent pas de règle. Vous définissez le type de persistance sur URLPASSIVE. Vous effectuez ensuite les procédures suivantes.

Pour configurer la persistance passive des URL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

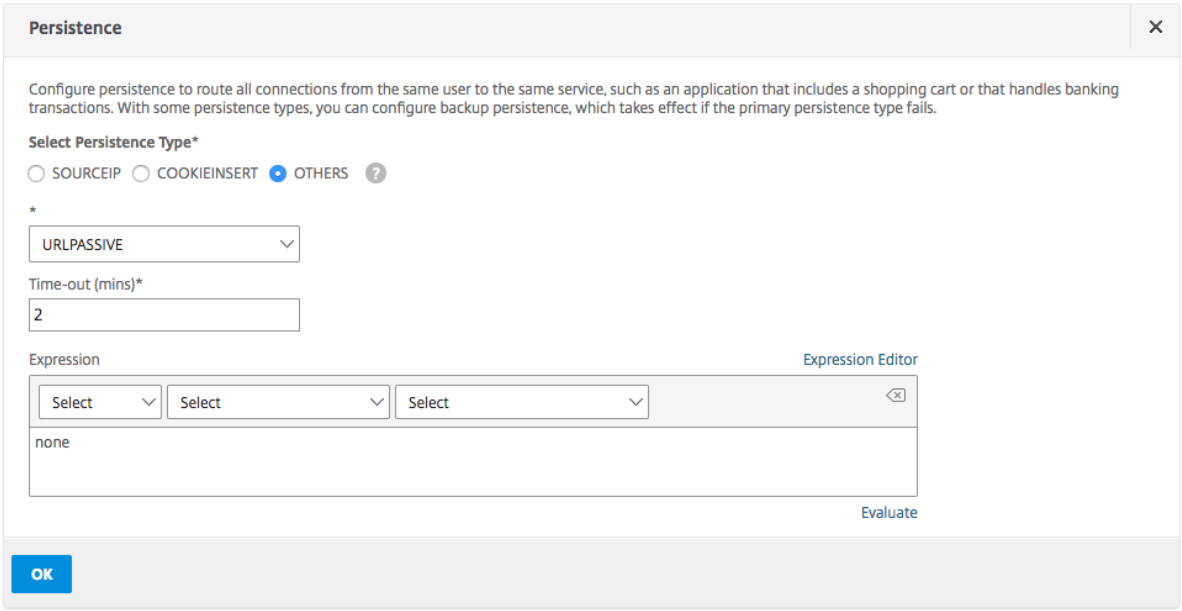
```
set lb vserver <vserverName>  [-persistenceType <persistenceType>]  [-
    rule <expression>]
<!--NeedCopy-->
```

Exemple :


```
set lb vserver LB-VServer-1 -persistenceType URLPASSIVE  - rule HTTP.REQ
    .URL.AFTER_STR( “urlp=” )
<!--NeedCopy-->
```

Pour configurer la persistance sur un serveur virtuel à l’aide de l’interface graphique

1. Accédez à **Gestiondu trafic**>**Équilibrage decharge** > **Serveursvirtuels**, puis ouvrez le serveur virtuel.
2. Dans la section Persistance, choisissez le type de persistance qui répond à vos besoins. Le type de persistance le plus approprié pour le serveur virtuel est disponible sous forme de boutons d’option. D’autres types de persistance applicables au type de serveur virtuel spécifique peuvent être sélectionnés dans la liste Autres.



> **Remarque :**
>
> Avant NetScaler version 12.0 build 56.20, tous les types de persistance sont disponibles dans une seule liste déroulante Persistence sans boutons d’option.

Configuration de la persistance en fonction de règles définies par l’utilisateur

October 5, 2021

> **Avertissement :**
>
> L'utilisation d'expressions classiques pour la règle de persistance dans la fonctionnalité d'équilibrage de charge est supprimée et n'est plus disponible pour la règle de filtrage sur l'appliance Citrix ADC version 13.1. Citrix recommande de ne pas utiliser ces expressions de stratégie via l'interface de ligne de commande Citrix ADC, l'interface graphique Citrix ADC ou l'automatisation Nitro. Pour plus d'informations, consultez les tableaux 1 et 2 de la page FAQ sur la dépréciation des stratégies classiques .

Lorsque la persistance basée sur des règles est configurée, l'appliance Citrix ADC crée une session de persistance basée sur le contenu de la règle appariée avant de diriger la demande vers le service sélectionné par la méthode d'équilibrage de charge configurée. Plus tard, il dirige toutes les demandes correspondant à la règle vers le même service. Vous pouvez configurer la persistance basée sur des règles pour les services de type HTTP, SSL, RADIUS, ANY, TCP et SSL_TCP.

La persistance basée sur des règles nécessite une expression de stratégie classique ou avancée. Vous pouvez utiliser une expression classique pour évaluer les en-têtes de demande, ou vous pouvez utiliser une expression de stratégie avancée pour évaluer les en-têtes de demande, les données de formulaire Web d'une demande, les en-têtes de réponse ou les corps de réponse. Par exemple, vous pouvez utiliser une expression classique pour configurer la persistance en fonction du contenu de l'en-tête de l'hôte HTTP. Vous pouvez également utiliser une expression de stratégie avancée pour configurer la persistance en fonction des informations de session d'application contenues dans un cookie de réponse ou un en-tête personnalisé. Pour plus d'informations sur la création et l'utilisation d'expressions de stratégie classiques et avancées, consultez la section Stratégies et expressions.

Les expressions que vous pouvez configurer dépendent du type de service pour lequel vous configurez la persistance basée sur des règles. Par exemple, certaines expressions spécifiques à RADIUS ne sont pas autorisées pour des protocoles autres que RADIUS, et les expressions basées sur des options TCP ne sont pas autorisées pour des types de service autres que le type AUY. Pour les types de service TCP et SSL_TCP, vous pouvez utiliser des expressions qui évaluent les données du protocole TCP/IP, les données de couche 2, les options TCP et les charges utiles TCP.

Remarque : Pour un cas d'utilisation impliquant la configuration de la persistance basée sur des règles basées sur les données du protocole Financial Information ExCHANGE (« FIX ») transmises via TCP, reportez-vous à la section Configuration de la persistance basée sur une paire nom-valeur dans un flux d'octets TCP.

La persistance basée sur des règles peut être utilisée pour maintenir la persistance avec des entités telles que les appliances Citrix SD-WAN, les plug-ins Citrix SD-WAN, les serveurs de cache et les serveurs d'applications.

Remarque : Sur un serveur virtuel ANY, vous ne pouvez pas configurer la persistance basée sur des règles pour les réponses.

Pour configurer la persistance en fonction d'une règle définie par l'utilisateur, vous devez d'abord configurer la persistance comme décrit dans Configuration des types de persistance qui ne nécessitent pas de règle, puis définissez le type de persistance sur RULE. Vous pouvez ensuite effectuer les procédures suivantes. Vous pouvez configurer la persistance basée sur des règles à l'aide de l'utilitaire de configuration ou de l'interface de ligne de commande.

Pour configurer la persistance en fonction de règles définies par l'utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

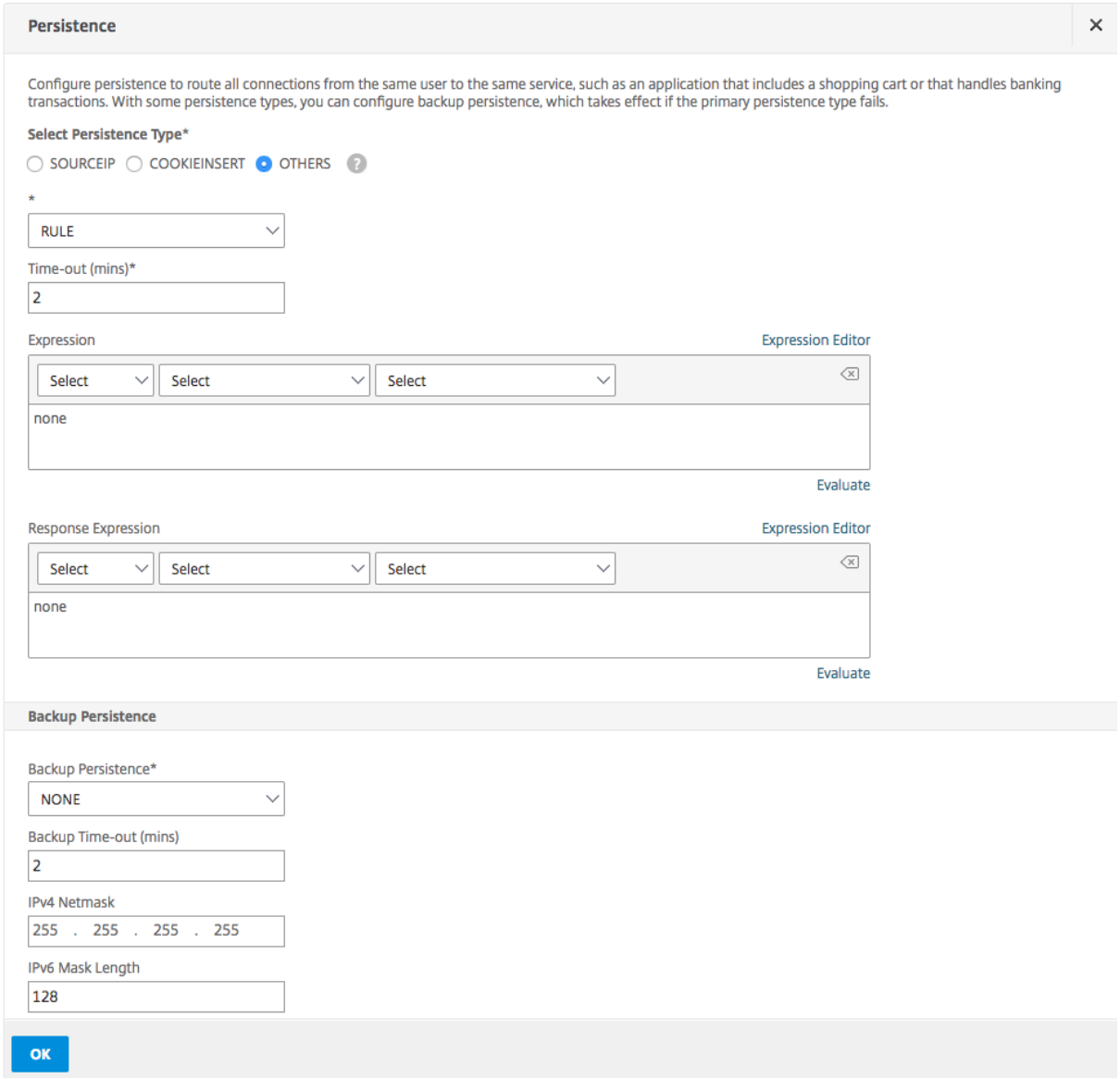
```
set lb vserver <vserverName> [-rule <expression>][-resRule <expression
    >]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vsvr_name -rule http.req.header("cookie").value(0).
    typecast_nvlist_t('=',';').value("server")

set lb vserver vsvr_name -resrule http.res.header("set-cookie").value
    (0).typecast_nvlist_t('=',';').value("server")

<!--NeedCopy-->
```

Pour configurer la persistance en fonction de règles définies par l'utilisateur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans la section Persistence, choisissez le type de persistance qui répond à vos besoins. Le type de persistance le plus approprié pour le serveur virtuel est disponible sous forme de boutons d'option. D'autres types de persistance applicables au type de serveur virtuel spécifique peuvent être sélectionnés dans la liste Autres.



> **Remarque**
>
> Avant NetScaler version 12.0 build 56.20, tous les types de persistance sont disponibles dans une seule liste déroulante Persistence sans boutons d'option.

Exemple : Expression classique pour une charge utile de demande

L'expression classique suivante crée une session de persistance basée sur la présence d'un en-tête HTTP User-Agent contenant la chaîne « MyBrowser » et dirige toutes les demandes client ultérieures contenant cet en-tête et cette chaîne vers le même serveur qui a été sélectionné pour la demande initiale.

```
1 http header User-Agent contains MyBrowser
```



```
<!--NeedCopy-->
```

Exemple : Expression de stratégie avancée pour un en-tête de demande

L'expression de stratégie avancée suivante fait la même chose que l'expression classique précédente.

HTTP.REQ.HEADER("User-Agent").CONTAINS ("MyBrowser")

Exemple : Expression de stratégie avancée pour un cookie de réponse

L'expression suivante examine les réponses pour les cookies « serveur », puis dirige toutes les demandes contenant ce cookie vers le même serveur qui a été sélectionné pour la demande initiale.

HTTP.RES.HEADER("SET-COOKIE").VALUE(0).TYPECAST_NVLIST_T('=';';').VALUE("server")

Configurer les types de persistance qui ne nécessitent pas de règle

August 20, 2021

Pour configurer la persistance, vous devez d'abord configurer un serveur virtuel d'équilibrage de charge, comme décrit dans Configuration de l'équilibrage de charge de base. Vous configurez ensuite la persistance sur le serveur virtuel.

Pour configurer la persistance sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la persistance et vérifier la configuration :

```
set lb vserver <name> -PersistenceType <type> [-timeout <integer>]

show lb vserver
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -persistenceType SOURCEIP -timeout 60

show lb vserver
<!--NeedCopy-->
```


Le délai d'expiration est la période pendant laquelle une session de persistance est en vigueur. Le délai d'expiration par défaut et les valeurs minimales (en minutes) varient en fonction du type de persistance indiqué dans le tableau suivant.

type de persistance	Valeur par défaut	Valeur minimale	Valeur maximale
Insertion de cookie ou insertion de cookie de groupe	2	0	1440
Autres types de persistance	2	2	1440

Remarque

- Le type de persistance d'insertion de cookie de groupe peut être défini sur le groupe d'équilibrage de charge.
- Pour la persistance IP, vous pouvez également définir le paramètre PersistMask.
- Le type de persistance par défaut est défini sur NONE.

Pour configurer la persistance sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans la section Persistance, choisissez le type de persistance qui répond à vos besoins. Le type de persistance le plus approprié pour le serveur virtuel est disponible sous forme de boutons d'option. D'autres types de persistance applicables au type de serveur virtuel spécifique peuvent être sélectionnés dans la liste **Autres**.

Remarque Avant Citrix ADC version 12.0 build 56.20, tous les types de persistance sont disponibles dans une seule liste déroulante Persistance sans boutons d'option.

Configurer la persistance des sauvegardes

August 20, 2021

Vous pouvez configurer un serveur virtuel pour qu'il utilise le type de persistance IP source lorsque le type de persistance principal échoue.

Le tableau suivant décrit les combinaisons de types de persistance de sauvegarde primaire et secondaire, ainsi que les conditions d'utilisation de la persistance de sauvegarde.

Persistance primaire	Persistance des sauvegardes	Lorsque la recherche de persistance principale échoue…
Insertion de cookie	IP source	L'appliance revient à la persistance basée sur la source IP uniquement lorsque le navigateur client ne renvoie aucun cookie dans la requête. Cependant, si le navigateur renvoie un cookie (pas nécessairement le cookie de persistance), il est supposé que le navigateur supporte les cookies et donc la persistance de sauvegarde n'est pas déclenchée.
Règle	IP source	L'appliance utilise la persistance basée sur la source IP lorsque le paramètre spécifié dans la règle est manquant dans la requête entrante.

Remarque

- Si le type de persistance principal est la persistance basée sur un cookie HTTP et que le type de persistance de sauvegarde est basé sur IP source, vous pouvez définir une valeur de délai d'expiration pour la persistance de la sauvegarde. Pour obtenir des instructions, reportez-vous à la section Définition d'une valeur de délai d'attente pour les connexions clientinactives.
- Vous ne pouvez pas définir de valeur de délai d'attente pour la persistance de sauvegarde lorsque la persistance principale est basée sur des règles, car dans ce cas, la valeur de délai d'attente pour la persistance secondaire doit être la même que pour la persistance principale. Par conséquent, le primaire et le secondaire expirent en même temps.

Pour définir la persistance des sauvegardes pour un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set lb vserver <name> -persistenceType <PersistenceType> -
    persistenceBackup <BackupPersistenceType>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -persistenceType CookieInsert -
    persistenceBackup SourceIP

set lb vserver Vserver-LB-1 -persistenceType sslsession -
    persistenceBackup SourceIP

set lb vserver Vserver-LB-1  -persistenceType RULE  -rule http.req.
    header("User-Agent").value(0).contains("MyBrowser")  -
    persistenceBackup SOURCEIP

set lb vserver Vserver-LB-1 -persistenceType sslsession -
    persistenceBackup SourceIP
<!--NeedCopy-->
```

Pour définir la persistance des sauvegardes pour un serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Persistance**et spécifiez un type de persistance de sauvegarde.

Remarque : La persistance principale doit être définie sur COOKIEINSERT, RULE ou SSLSESSION.

Configurer les groupes de persistance

August 20, 2021

Lorsque vous disposez de serveurs équilibrés de charge qui gèrent plusieurs types de connexions différents (tels que des serveurs Web qui hébergent du multimédia), vous pouvez configurer un groupe de serveurs virtuels pour gérer ces connexions. Pour créer un groupe de serveurs virtuels, vous liez différents types de serveurs virtuels, un pour chaque type de connexion accepté par vos serveurs équilibrés de charge, en un seul groupe. Vous configurez ensuite un type de persistance pour l'ensemble du groupe.

Vous pouvez configurer la persistance basée sur IP source ou la persistance basée sur les cookies HTTP pour les groupes de persistance. Après avoir défini la persistance pour l'ensemble du groupe, vous ne pouvez pas la modifier pour les serveurs virtuels individuels du groupe. Si vous configurez la persistance sur un groupe, puis ajoutez un nouveau serveur virtuel au groupe, la persistance du nouveau serveur virtuel est modifiée pour correspondre au paramètre de persistance du groupe.

Lorsque la persistance est configurée sur un groupe de serveurs virtuels, des sessions de persistance sont créées pour les demandes initiales et les demandes suivantes sont dirigées vers le même service que la demande initiale, quel que soit le serveur virtuel du groupe qui reçoit chaque demande client.

Lorsque vous ajoutez un serveur virtuel qui possède des sessions de persistance à un groupe d'équilibrage de charge avec un type de persistance différent, les sessions persistantes existantes spécifiques à un ancien type de persistance sont supprimées. Les sessions persistantes déterminent si le trafic doit être acheminé vers le même serveur virtuel ou vers un autre serveur. Par conséquent, les connexions établies existantes ne sont pas affectées.

Le type de persistance d'un groupe d'équilibrage de charge est appliqué à tous les serveurs virtuels liés à ce groupe, quel que soit le type de protocole des serveurs virtuels. Un groupe d'équilibrage de charge prend en charge les types de persistance suivants :

- IP sourceIP
- CookieInsert
- Règle

Certains serveurs virtuels ne prennent en charge que certains types de persistance. Par exemple, un serveur virtuel de type SSL_BRIDGE peut utiliser uniquement le type de persistance SourceIP pour un groupe LB.

Si vous configurez la persistance basée sur les cookies HTTP, l'attribut de domaine du cookie HTTP est défini. Ce paramètre entraîne le logiciel client à ajouter le cookie HTTP dans les requêtes client si différents serveurs virtuels ont des noms d'hôte publics différents. Pour plus d'informations sur le type de persistance CookieInsert, voir Persistance basée sur les cookies HTTP.

Pour créer un groupe de persistance de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb group <vServerGroupName> <vServerName> -persistenceType <
   PersistenceType>
<!--NeedCopy-->
```

Exemple :


```
bind lb group Vserver-Group-1 Vserver-LB-1 -persistenceType
   CookieInsert
<!--NeedCopy-->
```

Pour modifier un groupe de serveurs virtuels à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Groupes**de persistance, créez un groupe de persistance et spécifiez les serveurs virtuels qui doivent faire partie de ce groupe.

Pour modifier un groupe de serveurs virtuels à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb group <vServerGroupName> -PersistenceBackup <
   BackupPersistenceType> -persistMask <SubnetMaskAddress>
<!--NeedCopy-->
```

Exemple :

```
set lb group vserver-Group-1 -PersistenceBackup SourceIP -persistMask
   255.255.255.255
<!--NeedCopy-->
```

Partager des sessions persistantes entre des serveurs virtuels

August 20, 2021

Dans certains environnements clients (télécommunications et FAI), un serveur unique gère à la fois le contrôle et le trafic de données. Pour une adresse IP client donnée, le trafic de contrôle et de données doit être dirigé vers le même serveur principal. Pour cela, un serveur virtuel est requis pour gérer le trafic d'authentification client, et généralement la persistance basée sur des règles est configurée dessus. Par exemple, Radius.req.avp (8) .value.typecast_text_t'. Le deuxième serveur virtuel pour la gestion du trafic de données. Généralement, la persistance SourceIP est configurée dessus.

Auparavant, les entrées de persistance étaient locales sur le serveur virtuel. Si vous deviez appliquer la persistance sur plusieurs serveurs virtuels, vous deviez ajouter le serveur virtuel à un groupe d'équilibrage de charge, puis appliquer un type de persistance commun au groupe. Cette exigence ne peut pas être atteinte, car tous les serveurs virtuels liés à un groupe d'équilibrage de charge ont hérité de la persistance configurée sur le groupe.

Avec la fonctionnalité de partage de persistance entre serveurs virtuels, vous pouvez définir le nouveau `useVserverPersistency` paramètre pour un groupe d'équilibrage de charge afin de permettre au serveur virtuel du groupe d'utiliser ses propres paramètres de persistance au lieu de les hériter des paramètres de groupe. Vous pouvez configurer une persistance basée sur des règles distinctes sur chaque serveur virtuel.

Vous pouvez également désigner l'un des serveurs virtuels du groupe en tant que serveur virtuel principal. Lorsqu'un serveur virtuel est désigné comme serveur virtuel principal, seul ce serveur virtuel crée les entrées de persistance, qui sont utilisées par tous les serveurs virtuels du groupe. Si le serveur virtuel principal est en panne, l'appliance Citrix ADC ne crée aucune entrée de persistance.

Remarque : Le partage de persistance entre les serveurs virtuels est pris en charge uniquement pour les méthodes de persistance basées sur des règles. Configurez des paramètres de persistance basés sur des règles compatibles sur les serveurs virtuels membres.

Exemple :

Supposons que les v1 et v2 soient liées à un groupe d'équilibrage de charge, la v1 est un serveur virtuel de type RADIUS et v2 est un serveur virtuel de type HTTP. 'Radius.req.avp (8) .value.typecast_text_t' persistency est configuré sur v1 et 'client.ip.src' est configuré sur v2.

Lorsque le trafic passe par le serveur virtuel RADIUS v1, il crée une entrée persistante basée sur la chaîne de règle évaluée. Plus tard, lorsque le trafic atteint le serveur virtuel de type HTTP v2, v2 vérifie les entrées de persistance sur le groupe d'équilibrage de charge et utilise la même session de persistance pour diriger le trafic vers le même serveur principal.

Configuration du partage des sessions persistantes

Pour partager des paramètres de persistance sur le serveur virtuel dans un groupe d'équilibrage de charge, vous devez d'abord activer le paramètre UsevServerPersistency, puis désigner l'un des serveurs virtuels du groupe comme serveur principal.

Pour activer le paramètre USEVServerPersistency à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb group <name> -useVserverPersistency ( ENABLED)
<!--NeedCopy-->
```

Exemple :

```
set lb group lb_grp1 -useVserverPersistency ENABLED
<!--NeedCopy-->
```


Pour activer le paramètre USEVServerPersistency à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Groupes de persistance**.
2. Cliquez sur **Ajouter** pour ajouter un nouveau groupe ou sélectionnez un groupe existant et cliquez sur **Modifier**.
3. Sélectionnez **Utiliser la persistance Vserver**.

Pour désigner un serveur virtuel comme serveur virtuel principal à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb group <name> -useVserverPersistency ( ENABLED ) -masterVserver <
   string>
<!--NeedCopy-->
```

Exemple :

```
set lb group lb_grp1 -useVserverPersistency ENABLED  - masterVserver vs1
<!--NeedCopy-->
```

Pour désigner un serveur virtuel comme serveur virtuel principal à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Groupes de persistance**.
2. Cliquez sur **Ajouter** pour ajouter un nouveau groupe ou sélectionnez un groupe existant et cliquez sur **Modifier**.
3. Sélectionnez **Utiliser la persistance Vserver**.
4. Dans la zone **Nom du serveur virtuel**, cliquez sur **+** pour ajouter le serveur virtuel au groupe. Vous pouvez sélectionner le serveur virtuel disponible ou créer un serveur virtuel.
5. Cliquez sur **Créer** si vous ajoutez un nouveau groupe ou sur **Fermer** si vous modifiez un groupe existant.
6. Sélectionnez le groupe pour lequel vous avez activé le paramètre UsevServerPersistency et cliquez sur **Modifier** pour définir un serveur virtuel comme principal afin de créer des entrées de persistance.
7. Dans la liste **Master vServer**, sélectionnez le serveur virtuel qui doit être désigné comme serveur virtuel principal.

Arguments

USEVServerPersistency

Autoriser les serveurs virtuels d'un groupe à utiliser leurs propres paramètres de persistance pour créer des sessions persistantes, au lieu d'hériter des paramètres de persistance des groupes. Lorsque ce paramètre est activé, la persistance ne peut pas être définie sur le groupe d'équilibrage de charge.

Lorsque ce paramètre est désactivé, les serveurs virtuels du groupe héritent des paramètres de persistance des paramètres de groupe.

Lorsque ce paramètre est activé sur le groupe d'équilibrage de charge, l'appliance Citrix ADC vidé toutes les entrées de persistance correspondantes du groupe et des serveurs virtuels membres.

Valeurs possibles : ENABLED, DISABLED

Par défaut : DISABLED

Exemple :

```
set lb group lb_grp1 -useVserverPersistency ENABLED
<!--NeedCopy-->
```

masterVserver

Désignez un serveur virtuel comme serveur virtuel principal dans son groupe d'équilibrage de charge. Une fois désigné, seul le serveur virtuel principal peut créer les entrées persistantes utilisées par le groupe.

Remarque : Ce paramètre ne peut être défini que si le paramètre useVserverPersistency est activé.

Exemple :

```
set lb group lb_grp1 -masterVserver vs1
<!--NeedCopy-->
```

Exemple de configuration du partage de sessions persistantes à l'aide de l'interface de ligne de commande

Les serveurs virtuels sont créés

```
add lb vs vs1 http 10.1.10.11 80 -persistence rule -rule 'client.ip.
    src'

add lb vs vs2 radius 10.2.2.2 1812 -persistenceType rule -rule '
    Radius.req.avp(8).value.typecast_text_t'
<!--NeedCopy-->
```


Les groupes sont créés.

```
1 add lb group lb_grp1 -persistenceType NONE -useVserverPersistency
     ENABLED
2 <!--NeedCopy-->
```

Un serveur virtuel d'un groupe est désigné comme serveur virtuel principal.

```
1 set lb group lb_grp1 -masterVserver vs1
2 <!--NeedCopy-->
```

Les serveurs virtuels sont liés au groupe.

```
1 bind lb group lb_grp1 vs1
2 bind lb group lb_grp1 vs2
3 <!--NeedCopy-->
```

Pour plus de détails, voir Configuration de l'équilibrage de charge de base et configuration des groupes de persistance.

Configurer l'équilibrage de charge RADIUS avec persistance

August 20, 2021

L'environnement réseau complexe d'aujourd'hui nécessite souvent la coordination d'une configuration d'équilibrage de charge à haut volume et haute capacité avec une authentification et une autorisation robustes. Les utilisateurs d'applications peuvent se connecter à un VPN via des points d'accès mobiles tels que des connexions DSL ou câble de qualité grand public, WiFi ou même des nœuds d'accès à distance. Ces connexions utilisent généralement des adresses IP dynamiques, qui peuvent changer pendant la connexion.

Si vous configurez l'équilibrage de charge RADIUS sur l'appliance Citrix ADC pour prendre en charge les connexions clientes persistantes aux serveurs d'authentification RADIUS, l'appliance utilise l'ouverture de session de l'utilisateur ou l'attribut RADIUS spécifié au lieu de l'adresse IP du client comme ID de session, en dirigeant toutes les connexions et enregistrements associés à sur le même serveur RADIUS. Les utilisateurs peuvent donc se connecter à votre VPN à partir d'emplacements d'accès mobile sans subir de déconnexions lorsque le point d'accès IP ou WiFi du client change.

Pour configurer l'équilibrage de charge RADIUS avec persistance, vous devez d'abord configurer l'authentification RADIUS pour votre VPN. Pour plus d'informations et instructions, reportez-vous au chapitre Authentification, Authentication, Auditing (AAA) dans le trafic d'applications AAA. Choisissez également la fonction d'équilibrage de charge ou de commutation de contenu comme base de votre

configuration, et assurez-vous que la fonctionnalité que vous avez choisie est activée. Le processus de configuration avec l'une ou l'autre des fonctions est presque le même.

Ensuite, vous configurez deux serveurs virtuels d'équilibrage de charge ou deux commutateurs de contenu, l'un pour gérer le trafic d'authentification RADIUS et l'autre pour gérer le trafic de comptabilité RADIUS. Ensuite, vous configurez deux services, un pour chaque serveur virtuel d'équilibrage de charge, et liez chaque serveur virtuel d'équilibrage de charge à son service. Enfin, vous créez un groupe de persistance d'équilibrage de charge et définissez le type de persistance sur RULE.

Activation de la fonction d'équilibrage de charge ou de commutation de contenu

Pour utiliser la fonction Équilibrage de charge ou Commutation de contenu, vous devez d'abord vous assurer que la fonction est activée. Si vous configurez une nouvelle appliance Citrix ADC qui n'a pas encore été configurée, ces deux fonctionnalités sont déjà activées. Vous pouvez donc passer à la section suivante. Si vous configurez une appliance Citrix ADC avec une configuration précédente et que vous n'êtes pas certain que la fonctionnalité que vous utilisez soit activée, vous devez le faire maintenant.

- Pour obtenir des instructions sur l'activation de la fonction d'équilibrage de charge, reportez-vous à Activation de l'équilibra
- Pour obtenir des instructions sur l'activation de la fonction de commutation de contenu, voir Activation du changement

Configuration des serveurs virtuels

Après avoir activé la fonction d'équilibrage de charge ou de commutation de contenu, vous devez ensuite configurer deux serveurs virtuels pour prendre en charge l'authentification RADIUS :

- **Serveur virtuel d'authentification RADIUS.** Ce serveur virtuel et son service associé traitent le trafic d'authentification vers votre serveur RADIUS. Le trafic d'authentification consiste en des connexions associées aux utilisateurs qui se connectent à votre application protégée ou à votre réseau privé virtuel (VPN).
- **Serveur virtuel de comptabilité RADIUS.** Ce serveur virtuel et son service associé gère les connexions comptables à votre serveur RADIUS. Le trafic comptable est constitué de connexions qui suivent les activités d'un utilisateur authentifié sur votre application protégée ou VPN.

Important : vous devez créer une paire de serveurs virtuels d'équilibrage de charge ou une paire de serveurs virtuels de commutation de contenu à utiliser dans votre configuration de persistance RADIUS. Vous ne pouvez pas mélanger les types de serveurs virtuels.

Pour configurer un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel d'équilibrage de charge et vérifier la configuration :

```
add lb vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule
    <rule>

show lb vserver <name>
<!--NeedCopy-->
```

Pour configurer un serveur virtuel d'équilibrage de charge existant, remplacez la `add lb virtual server` commande précédente par la `set lb vserver` commande, qui prend les mêmes arguments.

Pour configurer un serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel de commutation de contenu et vérifier la configuration :

```
add cs vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule
    <rule>

show cs vserver <name>
<!--NeedCopy-->
```

Pour configurer un serveur virtuel de commutation de contenu existant, remplacez la `add cs vserver` commande précédente par la `set cs vserver` commande, qui prend les mêmes arguments.

Exemple :

```
add lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

add lb vserver radius_acct_vs1 RADIUS 192.168.46.34 1813 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

set lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

set lb vserver radius_auth_vs1 RADIUS 192.168.46.34 1813 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
```



```
<!--NeedCopy-->
```

Pour configurer un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** ou accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels>**, puis configurez un serveur virtuel.

Configuration des services

Après avoir configuré vos serveurs virtuels, vous devez ensuite configurer deux services, un pour chacun des serveurs virtuels que vous avez créés.

Remarque : une fois configurés, ces services sont dans l'état DISABLED jusqu'à ce que l'appliance Citrix ADC puisse se connecter aux adresses IP d'authentification et de comptabilité de votre serveur RADIUS et surveiller leur état. Pour obtenir des instructions, reportez-vous à la section Configuration des services.

Liaison de serveurs virtuels aux services

Après avoir configuré vos services, vous devez ensuite lier chacun des serveurs virtuels que vous avez créés au service approprié.Pour obtenir des instructions, reportez-vous à la section Liaison des services au serveur virtuel.

Configuration d'un groupe de persistance pour Rayon

Après avoir lié vos serveurs virtuels d'équilibrage de charge aux services correspondants, vous devez configurer votre configuration d'équilibrage de charge RADIUS pour prendre en charge la persistance. Pour ce faire, vous configurez un groupe de persistance d'équilibrage de charge qui contient vos serveurs et services virtuels d'équilibrage de charge RADIUS, et configurez ce groupe de persistance d'équilibrage de charge pour utiliser la persistance basée sur des règles. Un groupe de persistance est requis car les serveurs virtuels d'authentification et de comptabilité sont différents et le message d'authentification et de comptabilisation pour un seul utilisateur doit atteindre le même serveur RADIUS. Le groupe de persistance permet d'utiliser la même session pour les deux serveurs virtuels. Pour obtenir des instructions, reportez-vous à la section Configuration des groupes de persistance.

Configuration du secret partagé RADIUS

À partir de la version 12.0, une appliance Citrix ADC prend en charge le secret partagé RADIUS. Un client et un serveur RADIUS communiquent entre eux à l'aide d'un secret partagé configuré sur le client et

sur le serveur. Les transactions entre un client RADIUS et un serveur sont authentifiées à l'aide d'un secret partagé. Ce secret est également utilisé pour crypter certaines informations dans le paquet RADIUS.

Scénarios de validation de clé secrète partagée RADIUS

La validation de la clé **secrète partagée RADIUS** se produit dans les scénarios suivants :

- **La clé secrète partagée RADIUS est configurée pour le client radius et le serveur radius :** l'appliance Citrix ADC utilise la clé secrète RADIUS pour le côté client et le côté serveur. Si la vérification réussit, l'appliance autorise le message RADIUS à passer en revue. Sinon, il supprime le message RADIUS.
- La**clé secrète partagée RADIUS n'est configurée ni pour le client radius ni pour le serveur radius :** l'appliance Citrix ADC supprime le message RADIUS, car la validation de la clé secrète partagée ne peut pas être effectuée sur un nœud qui n'a pas de clé radicale configuré.
- **La clé secrète partagée RADIUS n'est pas configurée pour le client RADIUS et le serveur RADIUS :** l'appliance Citrix ADC contourne la validation de la clé secrète RADIUS et permet aux messages RADIUS de passer en revue.

Vous pouvez configurer un secret partagé RADIUS par défaut ou configurer sur une base par client ou sous-réseau. Il est recommandé d'ajouter une clé secrète partagée RADIUS pour tous les déploiements avec la stratégie RADIUS configurée. L'appliance utilise l'adresse IP source du paquet RADIUS pour décider quel secret partagé utiliser. Vous pouvez configurer un client et un serveur RADIUS ainsi que le secret partagé correspondant comme suit :

À l'invite CLI, tapez :

```
1 add radiusNode <clientPrefix/Subnet> -radKey <Shared_secret_key>
2 <!--NeedCopy-->
```

Arguments

Adresse IP

Adresse IP ou sous-réseau du client RADIUS au format CIDR. L'appliance utilise l'adresse IP source d'un paquet de requête entrant pour correspondre à l'adresse IP du client. Au lieu de configurer une adresse IP du client, vous pouvez configurer l'adresse réseau du client. Le préfixe le plus long est mis en correspondance pour identifier le secret partagé pour une demande client entrante.

Radkey

Secret partagé entre le client, l'appliance Citrix ADC et le serveur. Longueur maximale : 31.


```
1  add lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
       TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
2
3  add lb vserver radius_acct_vs1 RADIUS 192.168.46.34 1813 -lbmethod
       TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
4
5  add service radius_auth_service1 192.168.41.68 RADIUS 1812
6
7  add service radius_acct_service1 192.168.41.70 RADIUS 1813
8
9  bind lb vserver radius_auth_vs1 radius_auth_service1
10
11 bind lb vserver radius_acct_vs1 radius_acct_service[1-3]
12
13 add radiusNode 192.168.41.0/24 -radKey  serverkey123
14
15 add radiusNode 203.0.113.0/24 -radkey clientkey123
16 <!--NeedCopy-->
```

Un secret partagé doit être configuré à la fois pour un client et un serveur RADIUS. La commande est la même. Le sous-réseau détermine si le secret partagé est pour un client ou un serveur.

Par exemple, si le sous-réseau spécifié est un sous-réseau client, le secret partagé est pour le client. Si le sous-réseau spécifié est un sous-réseau serveur (192.168.41.0/24 dans l'exemple précédent), le secret partagé concerne le serveur.

Un sous-réseau de 0.0.0.0/0 implique qu'il s'agit du secret partagé par défaut pour tous les clients et serveurs.

> **Remarque :**
>
> Seules les méthodes d'authentification PAP et CHAP sont prises en charge avec le secret partagé RADIUS.

Afficher les sessions de persistance

August 20, 2021

Vous pouvez afficher les différentes sessions de persistance qui sont en vigueur globalement ou pour un serveur virtuel particulier.

> **Remarque** : Une appliance Citrix ADC nCore utilise plusieurs cœurs de processeur pour la gestion des paquets. Le cœur du processeur est propriétaire de chaque session de l'appliance. Si l'appliance reçoit une demande pour laquelle aucune session n'existe, une session est créée et l'un des cœurs est désigné comme propriétaire de cette session.
>
> Les demandes ultérieures qui appartiennent à cette session peuvent ne pas toujours arriver et être traitées par le noyau du propriétaire. Dans ce cas, la messagerie inter-cœur garantit que les informations de session sur le noyau propriétaire sont toujours à jour.

Toutefois, lorsqu'un noyau reçoit une demande appartenant à une session de persistance appartenant à un autre noyau, la messagerie inter-cœur n'actualise pas la valeur de délai d'expiration de la session de persistance.

Par conséquent, dans la sortie des commandes show lb PersistentSessions exécutées successivement, qui affichent uniquement les valeurs de délai d'expiration provenant des cœurs propriétaires, la valeur de délai d'expiration d'une session de persistance peut diminuer à 0 (zéro), même si la session de persistance reste active.

Pour afficher les sessions de persistance à l'aide de l'interface de ligne de commande

À l'invite de commandes, pour afficher les sessions de persistance associées à tous les serveurs virtuels, tapez :

```
show lb persistentSessions [<vServer>]
<!--NeedCopy-->
```

À l'invite de commandes, pour afficher les sessions de persistance liées à un serveur virtuel, tapez :

```
show lb persistentSessions <vServername>
<!--NeedCopy-->
```

Exemple :

```
show lb persistentSessions myVserver
<!--NeedCopy-->
```

Pour afficher les sessions de persistance à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Sessions persistantes du serveur virtuel**.

Effacer les sessions de persistance

August 20, 2021

Vous devrez peut-être effacer les sessions de persistance de l'appliance Citrix ADC si les sessions ne parviennent pas à expiration. Vous pouvez effectuer l'une des opérations suivantes :

- Effacez toutes les sessions de tous les serveurs virtuels à la fois.
- Effacez toutes les sessions d'un serveur virtuel donné à la fois.
- Effacer une session particulière associée à un serveur virtuel donné.

Pour effacer une session de persistance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour effacer les sessions de persistance et vérifier la configuration :

```
clear lb persistentSessions [<vServer> [-persistenceParam <string>]]

show persistentSessions <vServer>
<!--NeedCopy-->
```

Exemples :

L'exemple 1 efface toutes les sessions de persistance pour le serveur virtuel lbvip1 d'équilibrage de charge.

L'exemple 2 affiche d'abord les sessions de persistance pour le serveur virtuel d'équilibrage de charge lbvip1, efface la session avec le paramètre de persistance xls, puis affiche les sessions de persistance pour vérifier que la session a été effacée.

Exemple 1 :

```
> clear persistentSessions lbvip1
 Done
> show persistentSessions
 Done
>
<!--NeedCopy-->
```

Exemple 2 :

```
> show persistentSessions lbvip1
Type        SRC-IP    ...    PERSISTENCE-PARAMETER
RULE        0.0.0.0   ...    xls
RULE        0.0.0.0   ...    txt
```



```
RULE        0.0.0.0    ...    html
 Done
> clear persistentSessions lbvip1 -persistenceParam xls
 Done
> show persistentSessions lbvip1
Type        SRC-IP     ...    PERSISTENCE-PARAMETER
RULE        0.0.0.0    ...    txt
RULE        0.0.0.0    ...    html
 Done
>
<!--NeedCopy-->
```

Pour effacer les sessions de persistance à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Effacer les sessions persistantes**.

Remplacer les paramètres de persistance pour les services surchargés

August 20, 2021

Lorsqu'un service est chargé ou n'est pas disponible, le service aux clients est dégradé. Dans ce cas, vous devrez peut-être configurer l'appliance Citrix ADC pour transférer temporairement à d'autres services les demandes qui seraient autrement incluses dans la session de persistance associée au service surchargé. En d'autres termes, vous devrez peut-être remplacer le paramètre de persistance configuré pour le serveur virtuel d'équilibrage de charge. Vous pouvez obtenir cette fonctionnalité en définissant le paramètre skippersistency. Lorsque ce paramètre de saut de persistance est défini et si le serveur virtuel reçoit de nouvelles connexions pour un service surchargé, ce qui suit se produit.

- Le serveur virtuel ignore les sessions de persistance existantes associées à ce service, jusqu'à ce que le service retourne à un état auquel il peut accepter les demandes.
- Les sessions de persistance associées à d'autres services ne sont pas affectées.

Cette fonctionnalité est disponible uniquement pour les serveurs virtuels de type ANY ou UDP.

Dans les configurations d'équilibrage de charge du répéteur de branche, vous devez également configurer un moniteur de charge et le lier au service. Le moniteur supporte le service des décisions d'équilibrage de charge suivantes jusqu'à ce que la charge sur le service soit ramenée en dessous du seuil configuré. Pour plus d'informations sur la configuration d'un moniteur de charge pour votre serveur virtuel, voir Présentation des moniteurs de charge.

Vous pouvez configurer le serveur virtuel pour effectuer l'une des actions suivantes avec les demandes qui, autrement, feraient partie de la session de persistance :

- **Envoyez chaque demande à l'un des autres services.** Le serveur virtuel prend une décision d'équilibrage de charge et envoie chaque demande à l'un des autres services en fonction de la méthode d'équilibrage de charge. Si tous les services sont surchargés, les demandes sont abandonnées jusqu'à ce qu'un service devienne disponible.

  Les serveurs virtuels basés sur des caractères génériques et des adresses IP prennent en charge cette option. Cette action convient à tous les déploiements, y compris les déploiements dans lesquels le serveur virtuel répartit la charge des appliances Branch Repeater ou des pare-feu.

- **Contournez la configuration du service serveur virtuel.** Le serveur virtuel ne prend pas de décision d'équilibrage de charge. Au lieu de cela, il relie simplement chaque demande à un serveur physique en fonction de l'adresse IP de destination dans la demande.

  Seuls les serveurs virtuels génériques de type ANY et UDP prennent en charge l'option de contournement. Les serveurs virtuels génériques ont une combinaison *:* IP et port. Cette action convient aux déploiements dans lesquels vous utilisez le serveur virtuel pour équilibrer la charge des appliances Branch Repeater ou des pare-feu. Dans ces déploiements, l'appliance Citrix ADC transfère d'abord une demande à un dispositif de répéteur de branche ou à un pare-feu, puis transfère la réponse traitée à un serveur physique. Le serveur virtuel envoie des demandes directement à ses adresses IP de destination dans les conditions suivantes.

  - Vous configurez le serveur virtuel pour contourner la configuration du serveur virtuel—service pour les services surchargés.
  - L'appliance ou le pare-feu Branch Repeater est surchargé.

  Le serveur virtuel envoie des requêtes directement à leurs adresses IP de destination jusqu'à ce que l'appliance Branch Repeater ou le pare-feu puisse accepter les demandes.

Pour remplacer les paramètres de persistance des services surchargés à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour remplacer les paramètres de persistance des services surchargés et vérifier la configuration :

```
set lb vserver <name> -skippersistency <skippersistency>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple

```
> set lb vserver mylbvserver -skippersistency ReLb
 Done
```



```
> show lb vserver mylbvserver
    mylbvserver (\*:\*) - ANY Type: ADDRESS
      . . .
      . . .
 Skip Persistency: ReLb
      . . .
 Done
>
<!--NeedCopy-->
```

Pour remplacer les paramètres de persistance des services surchargés à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et sélectionnez le serveur virtuel de type UDP ou ANY.
2. Dans le volet Paramètres avancés, sélectionnez Paramètres de trafic et spécifiez le type d'Ignorer la persistance.

Résolution des problèmes

August 20, 2021

- **Les statistiques de l'appliance Citrix ADC VPX indiquent que l'appliance a atteint la limite de persistance de la session. Par conséquent, les sessions de persistance échouent. Est-il possible d'augmenter la limite de persistance de session ?**

  Cause : l'appliance Citrix ADC a la limite système de 250 000 sessions de persistance pour un cœur.

  Résolution : Pour résoudre ce problème, vous pouvez effectuer l'une des tâches suivantes :

  - Réduisez la valeur du délai d'attente pour la persistance
  - Augmenter le nombre de cœurs de l'appliance

- **Après avoir configuré la persistance de l'insertion de cookie sur l'appliance Citrix ADC, les utilisateurs signalent que les connexions fonctionnent correctement pendant un certain temps, mais commencent à se déconnecter. Quelles meilleures pratiques dois-je suivre lors de la configuration de la persistance ?**

  Cause : Par défaut, la valeur de délai d'expiration pour la persistance de l'insertion de cookie est de 120 secondes.

Résolution : lorsque vous configurez la persistance pour les applications pour lesquelles le temps d'inactivité ne peut pas être déterminé, définissez la valeur de délai d'expiration de la persistance Insérer cookie sur 0. Avec ce paramètre, la connexion ne s'éteint pas.

- **Après avoir configuré un serveur virtuel HTTP sur l'appliance Citrix ADC, je dois m'assurer qu'un utilisateur se connecte toujours au même serveur pour le contenu demandé. J'ai donc configuré la persistance SourceIP. Maintenant, l'augmentation de la valeur de délai d'attente pour la persistance introduit la latence. Comment puis-je augmenter la valeur de délai d'expiration sans affecter les performances ?**

  Résolution : envisagez d'utiliser la persistance d'insertion de cookie avec la valeur de délai d'expiration définie sur 0. Ce paramètre permet d'activer les paramètres de persistance de longue durée, car l'appliance ne spécifie pas la durée d'expiration du cookie.

- **Après avoir configuré la persistance de l'insertion de cookie sur l'appliance Citrix ADC, cela fonctionne comme prévu lorsque les clients du même fuseau horaire accèdent au contenu. Toutefois, lorsqu'un client d'un autre fuseau horaire tente de se connecter, la connexion est immédiatement temporisée.**

  Cause : La persistance d'insertion de cookie basée sur l'heure fonctionne comme prévu lorsqu'un client du même fuseau horaire établit une connexion. Toutefois, lorsque la machine cliente et l'appliance Citrix ADC se trouvent dans des fuseaux horaires différents, le cookie n'est pas valide. Par exemple, lorsqu'un client du fuseau horaire EST envoie un cookie à 11 h 00 HNE à une appliance Citrix ADC dans le fuseau horaire PST, l'appliance reçoit le cookie à 14 h 00 (HNP). En raison de la différence de temps, le cookie n'est pas valide et la connexion est immédiatement expiré.

  Résolution : définissez la valeur de délai d'expiration pour la persistance de l'insertion de cookie sur 0.

- **Une appliance Citrix ADC est utilisée pour équilibrer la charge des serveurs d'applications, tels que le serveur Oracle Weblogic. Pour vous assurer que les clients obtiennent des connexions persistantes à ces serveurs, la persistance SourceIP est configurée. Il fonctionne comme prévu lorsqu'une connexion est établie à partir d'un ordinateur. Toutefois, lorsque des clients légers tentent de se connecter via un serveur Terminal Server et, par conséquent, l'appliance reçoit des demandes de plusieurs clients à partir de la même adresse IP (l'adresse IP du serveur Terminal Server). Par conséquent, les connexions de tous les clients légers sont dirigées vers le même serveur d'applications. Est-il possible de configurer la persistance des requêtes des clients légers individuels en fonction de l'adresse IP du client ?**

  Cause : l'appliance Citrix ADC reçoit des demandes du serveur Terminal Server et l'adresse IP source de la demande reste la même. Par conséquent, l'appliance ne peut pas faire la distinction entre les demandes reçues des clients légers et fournir une persistance en fonction des

demandes des clients légers.

Résolution : Pour éviter ce problème, vous pouvez configurer la persistance des règles en fonction d'une valeur de paramètre unique pour chaque client léger.

- **L'appliance Citrix ADC est utilisée pour équilibrer la charge des serveurs d'interface Web. Lors de l'accès aux serveurs, l'utilisateur reçoit le message d'erreur « Erreur d'état ». En outre, lorsque l'un des serveurs d'interface Web est arrêté ou non disponible, certains utilisateurs reçoivent un message d'erreur.**

  Cause : Le manque de persistance sur les serveurs de l'interface Web peut entraîner des messages d'erreur lorsqu'un utilisateur tente de se connecter au serveur.

  Résolution : Citrix vous recommande de spécifier la méthode de persistance d'insertion de cookie sur l'appliance Citrix ADC lors de l'équilibrage de charge des serveurs d'interface Web.

Insérer des attributs de cookie aux cookies générés par ADC

August 20, 2021

Les administrateurs Web peuvent insérer d'autres attributs de cookies dans les cookies générés par l'appliance Citrix ADC. Ces attributs de cookies supplémentaires aident à appliquer les politiques requises pour les cookies générés par ADC en fonction du modèle d'accès à l'application.

Les fonctionnalités suivantes utilisent les cookies générés par ADC pour obtenir la persistance.

- Persistance des cookies d'équilibrage de charge
- Persistance des cookies du groupe d'équilibrage de charge
- Persistance du site GSLB
- Persistance des cookies de commutation de contenu

Vous pouvez insérer d'autres attributs de cookie dans les cookies générés par ADC à l'aide des paramètres suivants :

- **LiteralAdcCookieAttribute :** ajoutez d'autres attributs de cookie au cookie généré par ADC, sous forme de chaîne.
- **ComputedAdcCookieAttribute :** Utilisez une variable ADC ns pour ajouter conditionnellement des attributs de cookie au cookie généré par ADC, en fonction des attributs client ou serveur, par exemple, la version de l'agent utilisateur.

> **Remarque**
>
> Vous ne pouvez pas configurer à la fois l'attribut de cookie ADC littéral et l'attribut de cookie ADC calculé, simultanément sur le paramètre d'équilibrage de charge ou dans un seul profil

> d'équilibrage de charge.

Cas d'utilisation : Configurer l'attribut de cookie SameSite

Chaque cookie a un domaine qui lui est associé. Lorsque le domaine d'un cookie correspond au domaine du site Web dans la barre d'adresse de l'utilisateur, cela est considéré comme un contexte de même site (ou de première partie). Si le domaine associé à un cookie correspond à un service externe et non au site Web dans la barre d'adresse de l'utilisateur, cela est considéré comme un contexte intersite (ou tiers).

L'attribut **SameSite** indique au navigateur si le cookie peut être utilisé pour un contexte intersite ou uniquement pour un contexte de même site. De plus, si une application a l'intention d'être consultée dans un contexte intersite, elle ne peut le faire que via la connexion HTTPS. Pour plus de détails, voir RFC6265.

Jusqu'en février 2020, la propriété **SameSite** n'était pas explicitement définie dans Citrix ADC. Le navigateur a pris la valeur par défaut comme None et n'a pas eu d'impact sur les déploiements Citrix ADC.

Cependant, avec la mise à niveau de certains navigateurs, tels que Google Chrome 80, il y a un changement dans le comportement inter-domaines par défaut des cookies. L'attribut **SameSite** peut être défini sur l'une des valeurs suivantes. La valeur par défaut de Google Chrome est définie sur Lax.

- **Aucun :** indique que le navigateur doit utiliser un cookie dans un contexte intersite uniquement sur des connexions sécurisées.
- **Lax :** indique que le navigateur doit utiliser un cookie pour les demandes dans le même contexte de site. Dans le contexte inter-site, seules les méthodes HTTP sûres comme la requête GET peuvent utiliser le cookie.
- **Strict :** Utilisez le cookie uniquement dans le contexte du même site.

S'il n'y a pas d'attribut SameSite dans le cookie, Google Chrome assume la fonctionnalité de SameSite = Lax.

> **Remarque**
>
> Pour certaines versions d'autres navigateurs, la valeur par défaut de l'attribut SameSite peut être définie sur **Aucun**. Dans certaines versions du navigateur, « Samesite = none » peut être traité différemment. Par exemple, les navigateurs suivants rejettent un cookie avec « SameSite = none » :
>
> - Versions de Chrome de Chrome 51 à Chrome 66 (inclus sur les deux extrémités)
> - Versions du navigateur UC sur Android antérieures à la version 12.13.2

Configurer les cookies générés par ADC

Pour configurer les attributs de cookies générés par ADC, vous devez effectuer les opérations suivantes :

1. Créer un serveur virtuel d'équilibrage de charge
2. Définissez les attributs de cookie ADC pour le serveur virtuel d'équilibrage de charge, soit via les paramètres LB soit par le biais du profil LB.
3. Si vous utilisez un profil LB, définissez le profil LB sur un serveur virtuel d'équilibrage de charge.
4. Si vous choisissez d'utiliser l'attribut Cookie ADC calculé, configurez la stratégie de réécriture associée.

> **Remarque**
>
> Si un profil LB est lié à un serveur virtuel LB, la configuration du paramètre de profil est prise en compte au lieu de la configuration globale des paramètres LB.

Vous pouvez définir les attributs de cookie générés par ADC par les méthodes suivantes :

- Définition des attributs des cookie ADC dans les paramètres d'équilibrage de charge
- Définition des attributs des cookie ADC dans le profil d'équilibrage de charge

Définition des attributs des cookie ADC dans les paramètres d'équilibrage de charge à l'aide de l'interface de ligne de commande

Pour appliquer uniformément une stratégie aux cookies générés par ADC de toutes les applications configurées sur l'appliance Citrix ADC, vous pouvez définir l'attribut cookie ADC dans les paramètres LB globaux.

Le paramètre **Literal ADC Cookie Attribut** vous permet d'insérer inconditionnellement les attributs de cookie dans le cookie généré par ADC.

À l'invite de commandes, tapez :

```
set lb parameter -LiteralADCCookieAttribute <string>
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -LiteralADCCookieAttribute SameSite=None
<!--NeedCopy-->
```

Le paramètre **Calculé ADC Cookie Attribut** vous permet d'insérer conditionnellement les attributs de cookie, basés sur les attributs client ou serveur, dans le cookie généré par ADC.

À l'invite de commandes, tapez :

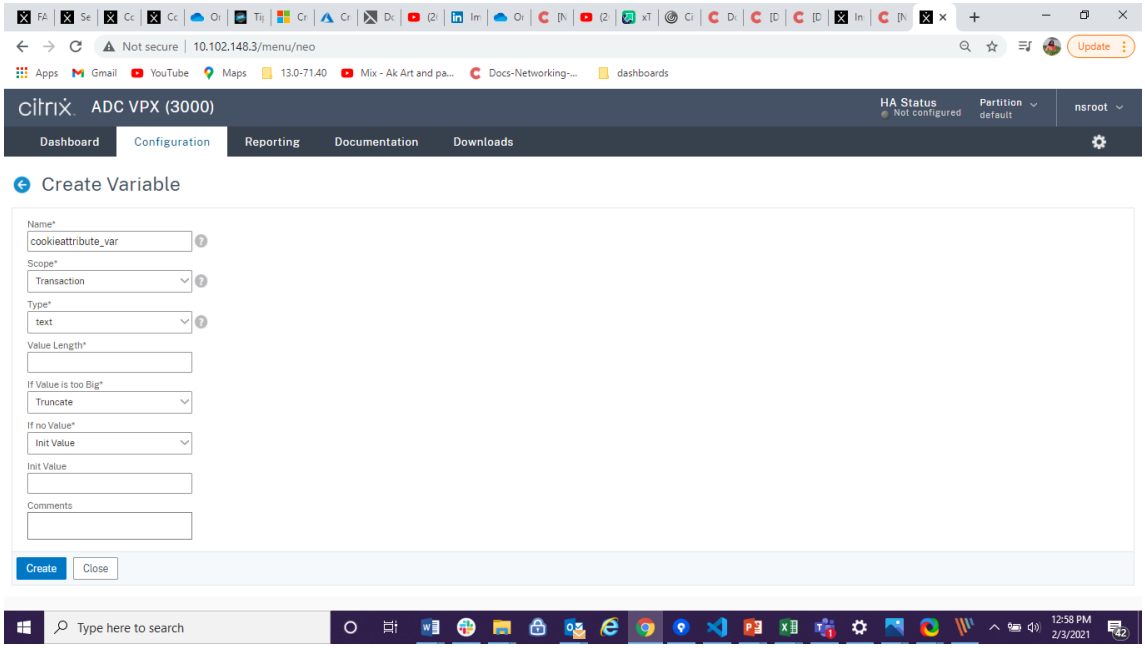
```
set lb parameter -ComputedADCCookieAttribute <ns variable>
<!--NeedCopy-->
```

Exemple :


```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
set lb parameter -ComputedADCCookieAttributE "$cookieattribute_var"
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""

add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
add rewrite policy append_samesite_attribute true samesiteassign

bind rewrite global exception_samesite_attribute 90 110 -type
    RES_OVERRIDE
bind rewrite global append_samesite_attribute 100 110 -type
    RES_OVERRIDE
<!--NeedCopy-->
```

Configurer les variables à l'aide de l'interface graphique

1. Accédez à **AppExpert > Variables**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer une variable**, sélectionnez **Étendue** en tant que **transaction** et **Tapez** comme **texte** dans le menu déroulant.

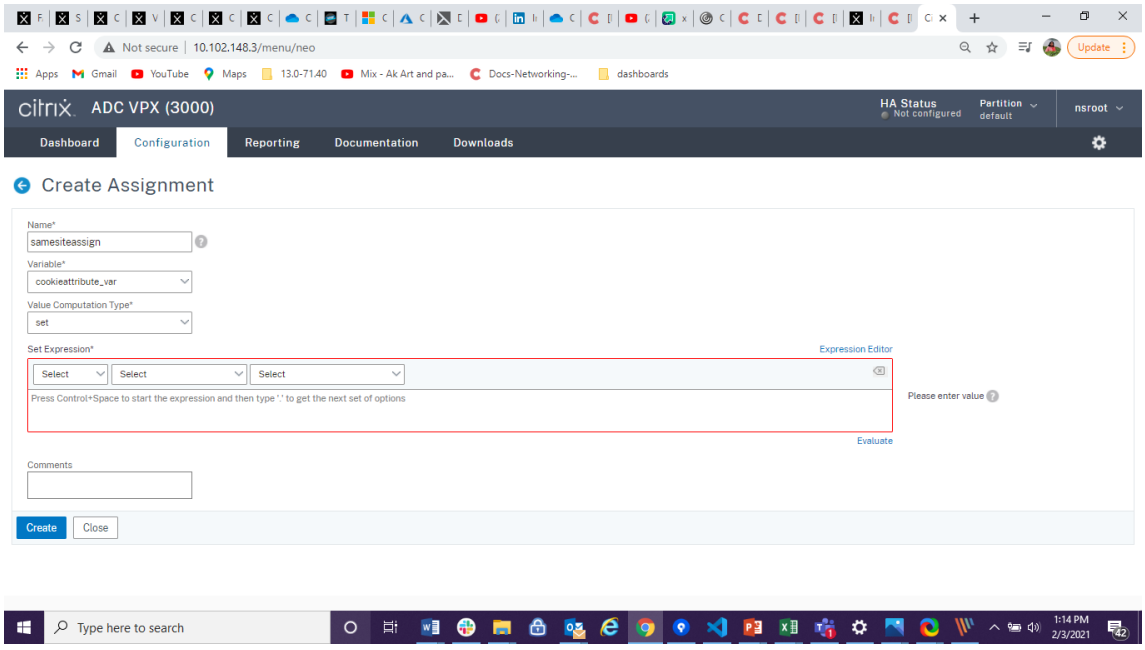


3. Entrez d'autres détails, puis cliquez sur **Créer**.

Créer une affectation à l'aide de l'interface graphique

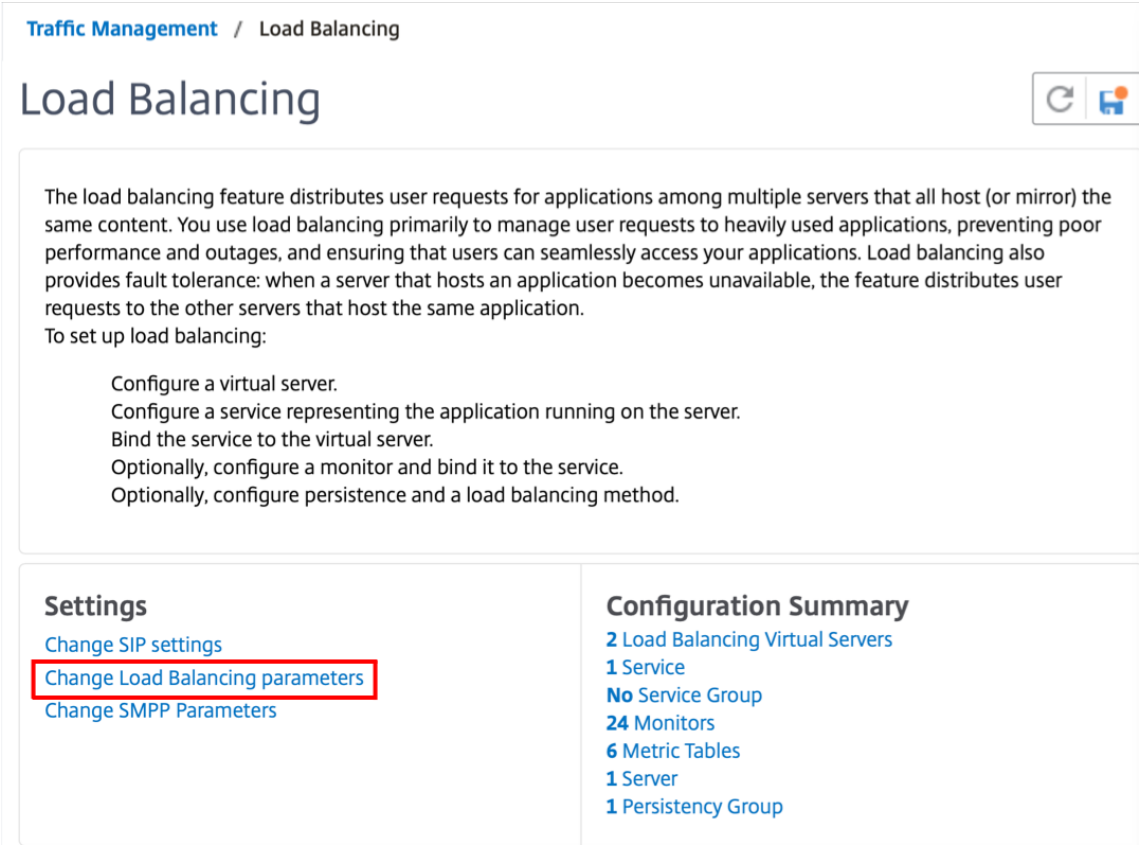
Après avoir configuré une variable, vous pouvez affecter une valeur ou spécifier l'opération à effectuer sur la variable en créant une affectation.

1. Accédez à **AppExpert > Affectations**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un devoir**, entrez les détails, puis cliquez sur **Créer**.



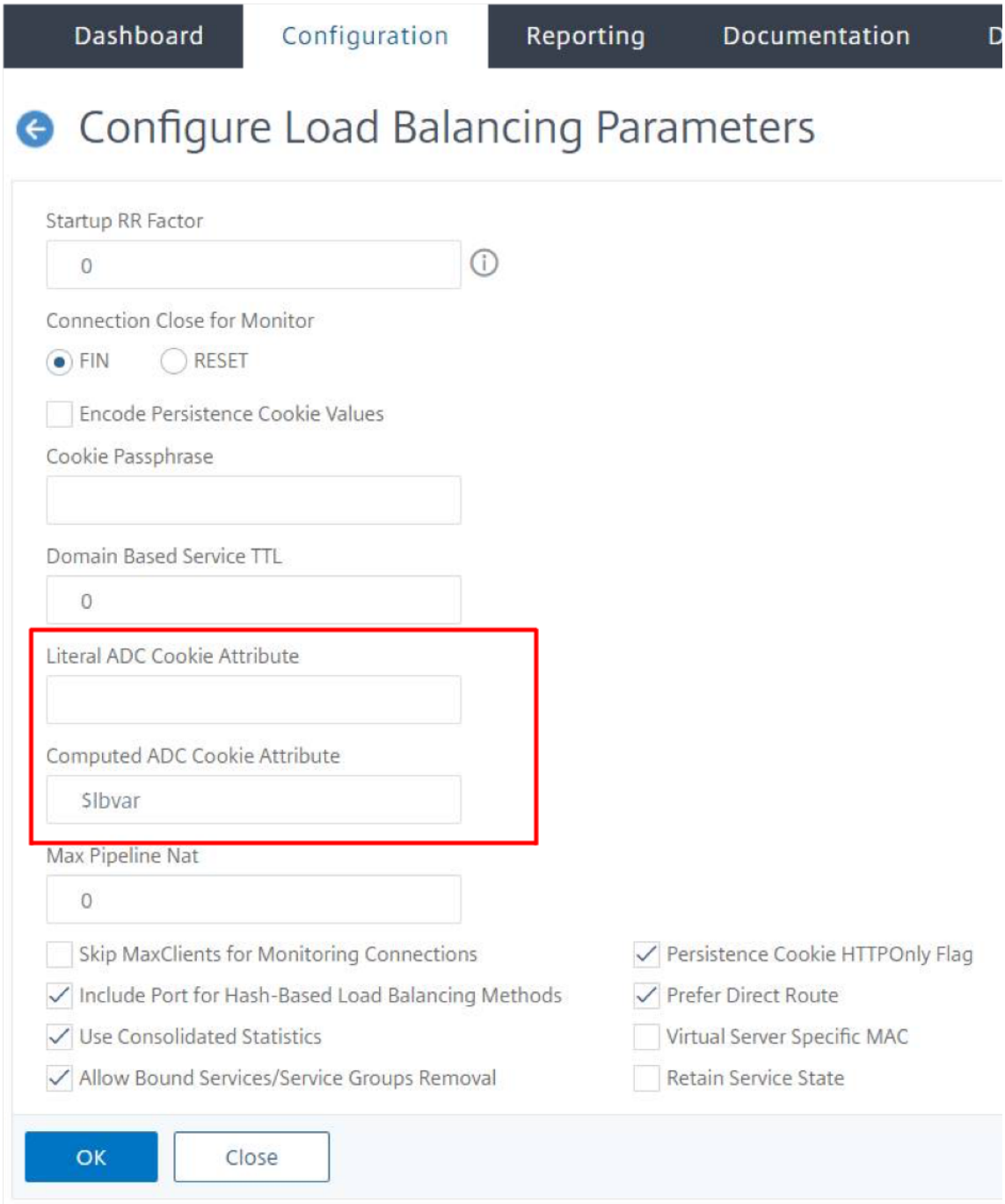
Définition des attributs des cookie ADC dans les paramètres d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Modifier les paramètres d'équilibrage de charge**.



2. Dans le volet **Configurer les paramètres d'équilibrage de charge**, entrez les valeurs appropriées pour l'un des champs en fonction de vos besoins :

   - **Literal ADC Cookie Attribute**
   - **Computed ADC Cookie Attribute**



3. Cliquez sur **OK**.

Définition des attributs des cookie ADC dans le profil d'équilibrage de charge à l'aide de l'interface de ligne de commande

Pour appliquer une stratégie à une application spécifique configurée sur l'appliance Citrix ADC, vous pouvez définir les paramètres de l'attribut de cookie dans le profil LB lié au serveur virtuel LB spéci-

fique à l'application.

Le paramètre d' **attribut Cookie ADC Literal** dans le profil LB vous permet d'insérer inconditionnellement les attributs de cookie dans le cookie généré par ADC spécifique à un serveur virtuel.

À l'invite de commandes, tapez :

```
add lb profile <profile name> -LiteralADCCookieAttribute <string>
<!--NeedCopy-->
```

Exemple :

```
add lb profile LB-Vserver-Profile-1 -LiteralADCCookieAttribute SameSite
    =None
add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
<!--NeedCopy-->
```

Le paramètre **Calculé ADC Cookie Attribut** dans le profil LB vous permet d'insérer conditionnellement les attributs de cookie basés sur les attributs client ou serveur, dans le cookie généré par ADC. Ensuite, définissez ce profil LB sur un serveur virtuel LB.

À l'invite de commandes, tapez :

```
add lb profile <profile name> -ComputedADCCookieAttribute <ns variable>
<!--NeedCopy-->
```

Exemple :

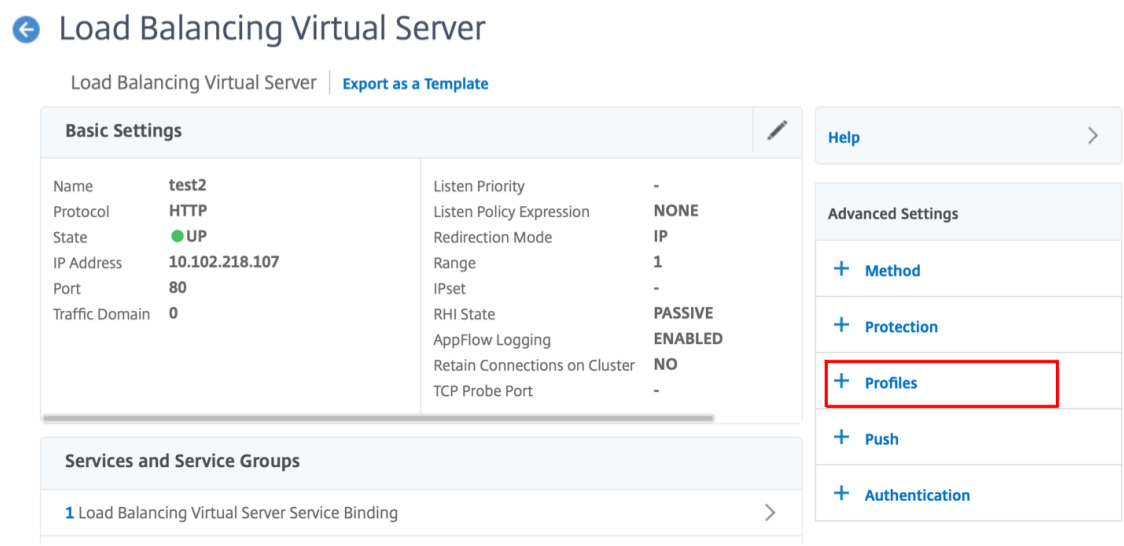
```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""
add lb profile LB-Vserver-Profile-1 -ComputedADCCookieAttributE "
    $cookieattribute_var"

add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
```



```
add rewrite policy append_samesite_attribute true samesiteassign

add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
bind lb vserver LB-VServer-1 -policyName exception_samesite_attribute -
    priority 90 -gotoPriorityExpression 110 -type RESPONSE
bind lb vserver LB-VServer-1 -policyName append_samesite_attribute -
    priority 100 -gotoPriorityExpression 110 -type RESPONSE
<!--NeedCopy-->
```

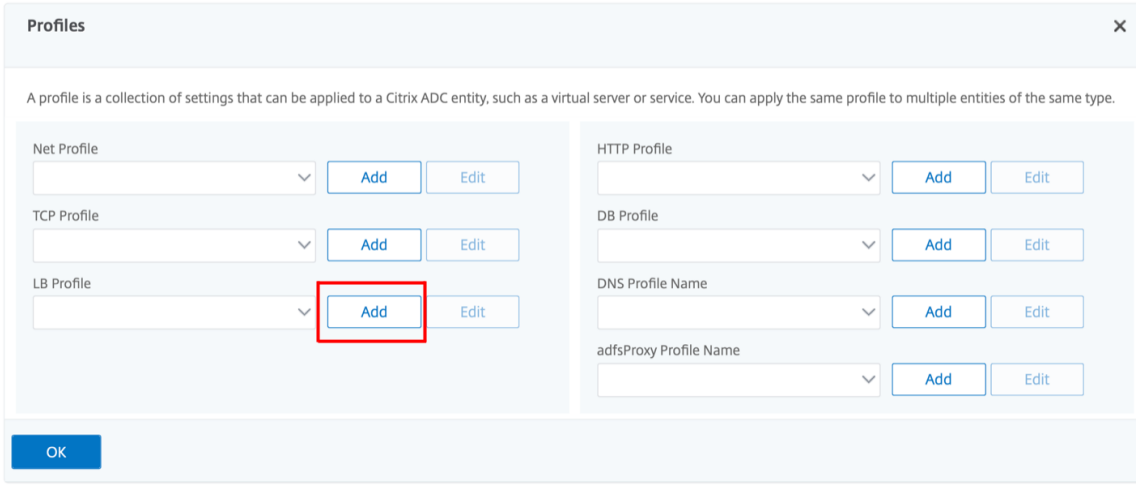
Définition des attributs ADC Cookie dans le profil d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel et cliquez sur **Modifier**.
3. Sous **Paramètres avancés**, cliquez sur **Ajouter des profils**.



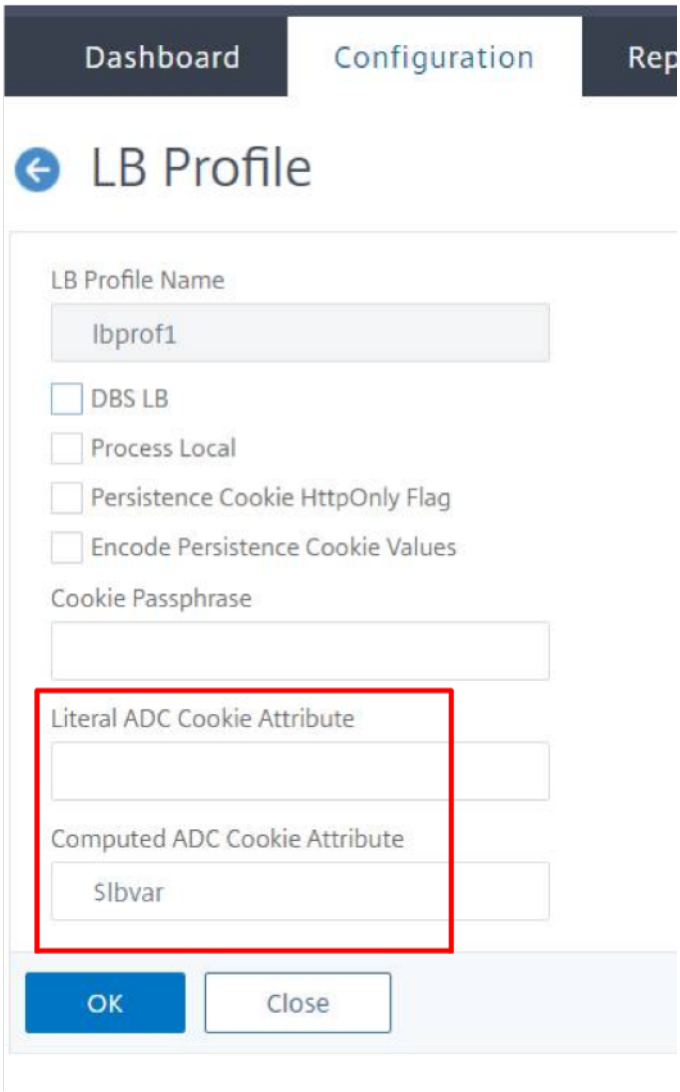
4. Dans la section **Profils**, cliquez sur **Ajouter** pour créer un profil LB.

   Si vous avez déjà créé un profil, choisissez-le dans le menu déroulant **Profil LB**.



5. Dans le volet **Profil LB**, entrez les valeurs appropriées pour l'un des champs en fonction de vos besoins :

- **Literal ADC Cookie Attribute**
- **Computed ADC Cookie Attribute**



1. Cliquez sur **OK**.
2. Définissez le profil LB créé sur le serveur virtuel LB créé à l'**étape 1**.

Vérifier la configuration de la variable ns

Pour vérifier que la variable ADC ns est correctement configurée dans les paramètres LB ou le profil LB, utilisez le paramètre show lb ou show lb profile commandes.

Le tableau suivant répertorie les différents messages d'avertissement et leur cause, lorsque la variable ns n'est pas correctement configurée.

Message d'avertissement	Raisons
La variable NS n'est pas configurée. Configurez-le avec le type text () et la transaction d'étendue pour la variable	La variable NS n'est pas encore configurée.
L'étendue de la variable NS configurée n'est pas une transaction.	La variable est configurée mais l'étendue n'est pas définie sur « transaction ».
Le type de variable n'est pas Texte ().	La variable est configurée mais le type n'est pas défini sur « Texte ».
La taille maximale de valeur configurée pour la variable NS est supérieure à 255.	La valeur configurée pour la variable NS est supérieure à 255 caractères. **Remarque :** une longueur maximale de 255 caractères peut être ajoutée à un cookie généré par ADC. Les caractères qui dépassent la longueur maximale sont tronqués.

Exemple de sortie

Dans l'exemple suivant, le message d'avertissement s'affiche lorsque la variable ns n'est pas configurée.

```
set lb parameter -ComputedADCCookieAttribute "$lbvar"

Warning: NS Variable is not configured. Please configure it with type
    text() and scope transaction
Done
<!--NeedCopy-->
```

Le message d'avertissement s'affiche dans la sortie suivante de la `show lb parameter` commande.

```
show lb parameter

Global LB parameters:
Persistence Cookie HttpOnly Flag: ENABLED
Use Encrypted Persistence Cookie: DISABLED
Use Port For Hash LB: YES
Prefer direct route: YES
Retain Service State: OFF
Start RR Factor: 0
Skip Maxclient for Monitoring: DISABLED
Monitor Connection Close: FIN
```



```
12 Use consolidated stats for LeastConnection: YES
13 Allow mac mode based vserver to pick thereturn traffic from services:
      DISABLED
14 Allow bound service removal: ENABLED
15 TTL for Domain Based Server: 0 secs
16
17 Citrix ADC Cookie Variable Name: $lbvar(NS Variable is not configured.
      Please configure it with type text() and scope transaction)
18
19 Done
20 <!--NeedCopy-->
```

Exemple de configuration pour insérer des attributs de cookie dans le déploiement GSLB

L'exemple de configuration suivant s'applique à la persistance de site configurée sur les services GSLB correspondant à un serveur virtuel LB. Pour ajouter des attributs de cookies supplémentaires aux cookies GSLB, effectuez la configuration suivante.

- Définissez les attributs de cookie ADC dans le profil LB (LB-vserver-profile-1).
- Définissez la valeur de l'attribut Cookie ADC Literal, par exemple « Samesite=none », dans le profil LB.
- Définissez le profil LB sur le serveur virtuel d'équilibrage de charge (LB-vserver-1), qui représente le service GSLB.

```
1  add gslb vserver GSLB-VServer-1 SSL -backupLBMethod ROUNDROBIN -
      tolerance 0 -appflowLog DISABLED
2  add gslb site site1 10.102.148.4 -publicIP 10.102.148.4
3  add gslb service site1_gsvc1 10.102.148.35 SSL 443 -publicIP
      10.102.148.35 -publicPort 443 -maxClient 0 -siteName site1 -
      sitePersistence HTTPRedirect -sitePrefix ss1 -cltTimeout 180 -
      svrTimeout 360 -downStateFlush ENABLED
4
5  bind gslb vserver GSLB-VServer-1 -serviceName site1_gsvc1
6  bind gslb vserver GSLB-VServer-1 -domainName www.gslb.com -TTL 5
7
8  add service service-1 10.102.84.140 SSL 443
9
10 add lb profile LB-Vserver-Profile-1 -LiteralADCCookieAttribute SameSite
      =None
11 add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
      COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
12
13 bind lb vserver LB-VServer-1 service-1
```



```
<!--NeedCopy-->
```

> **Remarque**
>
> Vous pouvez également insérer conditionnellement les attributs de cookie à l'aide de l'attribut Cookie ADC calculé.

Exemple de configuration pour insérer un attribut de cookie dans le déploiement de commutation de contenu

L'exemple de configuration suivant s'applique lorsque plusieurs applications sont hébergées derrière un serveur virtuel de commutation de contenu. Pour appliquer la même stratégie à toutes les applications, liez les stratégies de réécriture au serveur virtuel de commutation de contenu au lieu du serveur virtuel LB, comme suit :

- Définissez les attributs de cookie ADC dans les paramètres LB.

  > **Remarque :**
  >
  > Vous pouvez également définir les attributs de cookie ADC dans le profil LB.

- Configurez la variable ns (cookieattribute_var) de Type définie sur Texte et Étendue définie sur Transaction.
- Définissez l'attribut Cookie ADC calculé dans les paramètres LB globaux à l'aide de la variable ns.
- Définissez les stratégies de réécriture (exception_samesite_attribute et append_samesite_attribute) sur les serveurs virtuels de commutation de contenu pour l'insertion des attributs de cookie.

```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
set lb parameter -ComputedADCCookieAttributE "$cookieattribute_var"
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""

add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
```



```
8  add rewrite policy append_samesite_attribute true samesiteassign
9
10 add lb vserver LB-VServer-1 SSL 10.102.148.35 443
11 add lb vserver LB-VServer-2 SSL 10.102.148.36 443
12
13 add cs vserver CS-VServer-1 SSL 10.102.148.42 443 -persistenceType
      COOKIEINSERT
14
15 add cs action act1 -targetLBVserver v1
16 add cs action act2 -targetLBVserver v2
17 add cs policy CS-policy-1 -rule "HTTP.REQ.URL.CONTAINS("file1.html")" -
      action act1
18 add cs policy CS-policy-2 -rule "HTTP.REQ.URL.CONTAINS("file2.html")" -
      action act2
19
20 bind cs vserver CS-VServer-1 -policyName CS-policy-1 -priority 1
21 bind cs vserver CS-VServer-1 -policyName CS-policy-2 -priority 2
22
23 bind cs vserver -policyname exception_samesite_attribute 90 110 -type
      RES_OVERRIDE
24 bind cs vserver -policyname append_samesite_attribute 100 110 -type
      RES_OVERRIDE
25 <!--NeedCopy-->
```

Personnaliser une configuration d'équilibrage de charge

August 20, 2021

Après avoir configuré une configuration d'équilibrage de charge de base, vous pouvez y apporter plusieurs modifications afin qu'elle répartit la charge exactement comme vous le souhaitez. La fonction d'équilibrage de charge est complexe. Vous pouvez modifier les éléments de base en effectuant une ou plusieurs des opérations suivantes :

- Modification de l'algorithme d'équilibrage de charge
- Configuration des groupes d'équilibrage de charge et utilisation de ces groupes pour créer votre configuration d'équilibrage de charge
- Configuration des connexions client-serveur persistantes
- Configuration du mode de redirection
- Affectation de différentes pondérations à différents services ayant des capacités différentes.

L'algorithme d'équilibrage de charge par défaut sur l'appliance Citrix ADC est la méthode de connexion la plus faible. Dans la méthode de connexion la plus faible, l'appliance envoie chaque connexion

entrante au service qui gère actuellement le moins de connexions. Vous pouvez spécifier différents algorithmes d'équilibrage de charge, chacun étant adapté à différentes conditions.

Pour prendre en charge des applications telles que les chariots d'achat, qui requièrent que toutes les demandes du même utilisateur soient dirigées vers le même serveur, vous pouvez configurer l'appliance pour qu'elle conserve les connexions persistantes entre les clients et les serveurs. Vous pouvez également spécifier la persistance d'un groupe de serveurs virtuels. La persistance permet à l'appliance de diriger les demandes client individuelles vers le même service, quel que soit le serveur virtuel du groupe qui reçoit la demande du client.

Vous pouvez activer et configurer le mode de redirection utilisé par l'appliance lors de la redirection des demandes des utilisateurs, en choisissant entre le transfert sur IP et le transfert sur Mac. Vous pouvez également attribuer des poids à différents services, en spécifiant quel pourcentage de charge entrante doit être dirigé vers chaque service. L'attribution de poids vous permet d'inclure des serveurs de capacités différentes dans la même configuration d'équilibrage de charge sans :

- surcharge des serveurs à faible capacité ou
- ce qui permet aux serveurs de plus grande capacité de rester inactifs.

Personnaliser l'algorithme de hachage pour assurer la persistance sur les serveurs virtuels

August 20, 2021

L'appliance Citrix ADC utilise des algorithmes basés sur le hachage pour maintenir la persistance sur les serveurs virtuels. Par défaut, la méthode d'équilibrage de charge basée sur le hachage utilise une valeur de hachage de l'adresse IP et du numéro de port du service. Si un service est rendu disponible sur différents ports sur le même serveur, l'algorithme génère des valeurs de hachage différentes. Par conséquent, différents serveurs virtuels d'équilibrage de charge peuvent envoyer des demandes pour la même application à différents services, ce qui rompt la pseudo-persistance.

Comme alternative à l'utilisation du numéro de port pour générer la valeur de hachage, vous pouvez spécifier un identificateur de hachage unique pour chaque service. Pour un service, la même valeur d'identificateur de hachage doit être spécifiée sur tous les serveurs virtuels. Si un serveur physique sert plus d'un type d'application, chaque type d'application doit avoir un identifiant de hachage unique.

L'algorithme de calcul de la valeur de hachage pour un service fonctionne comme suit :

- Par défaut, un paramètre global spécifie l'utilisation du numéro de port dans un calcul de hachage.

- Si vous configurez un identificateur de hachage pour un service, il est utilisé et le numéro de port ne l'est pas, quel que soit le paramètre global.
- Si vous ne configurez pas d'identificateur de hachage, mais modifiez la valeur par défaut du paramètre global afin qu'il ne spécifie pas l'utilisation du numéro de port, la valeur de hachage est basée uniquement sur l'adresse IP du service.
- Si vous ne configurez pas d'identificateur de hachage ou ne modifiez pas la valeur par défaut du paramètre global pour utiliser le numéro de port, la valeur de hachage est basée sur l'adresse IP et le numéro de port du service.

Vous pouvez également spécifier des identificateurs de hachage lors de l'utilisation de l'interface de ligne de commande pour lier des services à un groupe de services. Dans l'utilitaire de configuration, vous pouvez ouvrir un groupe de services et ajouter des identifiants de hachage sous l'onglet Membres.

Pour modifier le paramètre global use-port-number à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb parameter -usePortForHashLb (YES          NON)
```

Exemple :

```
1 > set lb parameter -usePortForHashLb NO
2  Done
3 >show lb parameter
4 Global LB parameters:
5         Persistence Cookie HttpOnly Flag: DISABLED
6         Use port for hash LB: NO
7  Done
8 <!--NeedCopy-->
```

Pour modifier le paramètre global use-port-number à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge.
2. Sélectionnez ou désactivez Utiliser le port pour les méthodes LB basées sur hachage.

Pour créer un nouveau service et spécifier un identifiant de hachage pour un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir l'ID de hachage et vérifiez le paramètre :

add service < name > (< ip >	< serverName >) < serviceType > < port > -hashId < positive_integer >

```
show service <name>
<!--NeedCopy-->
```

Exemple :

```
> add service flbkng 10.101.10.1 http 80 -hashId 12345
 Done
>show service flbkng
        flbkng (10.101.10.1:80) - HTTP
        State: DOWN
        Last state change was at Thu Nov  4 10:14:52 2010
        Time since last state change: 0 days, 00:00:15.990
        Server Name: 10.101.10.1
        Server ID : 0   Monitor Threshold : 0

        Down state flush: ENABLED
        Hash Id: 12345

1)      Monitor Name: tcp-default
                State: DOWN     Weight: 1

 Done
<!--NeedCopy-->
```

Pour spécifier un identificateur de hachage pour un service existant à l'aide de l'interface de ligne de commande

Tapez la commande set service, le nom du service et **-hashid** suivi de la valeur ID.

Pour spécifier un identifiant de hachage lors de l'ajout d'un membre de groupe de services

Pour spécifier un identifiant de hachage pour chaque membre à ajouter au groupe et vérifier le paramètre, à l'invite de commandes, tapez les commandes suivantes (Veillez à spécifier un Hashid unique pour chaque membre.) :

```
bind servicegroup <serviceGroupName> <memberName> <port> -hashId <
   positive_integer>

show servicegroup <serviceGroupName>
<!--NeedCopy-->
```

Exemple :

```
 bind servicegroup http_svc_group 10.102.27.153 80 -hashId 2222222

>show servicegroup SRV
        SRV - HTTP
        State: ENABLED  Monitor Threshold : 0
        …

        1)         1.1.1.1:80   State: DOWN     Server Name: 1.1.1.1
              Server ID: 123  Weight: 1
        Hash Id: 32211

                Monitor Name: tcp-default       State: DOWN
        …

        2)         2.2.2.2:80   State: DOWN     Server Name: 2.2.2.2
             Server ID: 123  Weight: 1
        Hash Id: 12345

                Monitor Name: tcp-default       State: DOWN
        …
Done

<!--NeedCopy-->
```

Pour spécifier un identifiant de hachage pour un service à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Créez un nouveau service ou ouvrez un service existant et spécifiez l'ID de hachage.

Pour spécifier un identificateur de hachage pour un membre de groupe de services déjà configuré à l'aide de l'interface graphique graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Groupes de services.
2. Ouvrez un membre et tapez un ID de hachage unique.

Configurer le mode de redirection

October 5, 2021

Le mode de redirection configure la méthode utilisée par un serveur virtuel pour déterminer où transférer le trafic entrant. L'appliance Citrix ADC prend en charge les modes de redirection suivants. Avant de transférer la demande vers un serveur, les modes de redirection fonctionnent comme suit :

- Transfert basé sur IP (par défaut) : l'adresse IP de destination est remplacée par l'adresse IP du serveur.
- Transfert sur Mac : l'adresse MAC de destination est remplacée par l'adresse MAC du serveur. Toutefois, l'adresse IP de destination n'est pas modifiée. Le mode de redirection basé sur Mac est principalement utilisé dans les déploiements d'équilibrage de charge de pare-feu.
- Basé sur le TUNNEL IP : Une encapsulation IP dans IP est effectuée pour les paquets IP clients. Dans les en-têtes IP externes, l'adresse IP de destination est définie sur l'adresse IP du serveur et l'adresse IP source est définie sur l'adresse IP du sous-réseau (SNIP). Les paquets IP du client ne sont pas modifiés. Cela s'applique aux paquets IPv4 et IPv6.
- Basé sur l'ID TOS : L'ID TOS du serveur virtuel est codé dans le champ TOS de l'en-tête IP.

Vous pouvez utiliser l'option IP TUNNEL ou TOS pour implémenter le retour direct du serveur (DSR). Pour plus d'informations, voir :

- Configuration du mode DSR lors de l'utilisation de TOS
- Configurez l'équilibrage de charge en mode DSR pour les réseaux IPv6 à l'aide du champ TOS
- Configurez l'équilibrage de charge en mode DSR à l'aide d'IP sur IP

Vous pouvez configurer le transfert Mac sur les réseaux qui utilisent la topologie DSR, l'équilibrage de charge des liens ou l'équilibrage de charge du pare-feu. Pour plus d'informations sur le transfert Mac pour l'équilibrage de charge, consultez Configurer MBF pour la configuration de l'équilibrage de charge.

Pour configurer le mode de redirection à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -m <RedirectionMode>
```



```
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

> **Remarque**
>
> Pour un service lié à un serveur virtuel sur lequel l' `-m MAC` option est activée, vous devez lier un moniteur non utilisateur.

Pour configurer le mode de redirection à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel et sélectionnez le mode de redirection.

Configurer des serveurs virtuels génériques par VLAN

August 20, 2021

Si vous souhaitez configurer l'équilibrage de charge pour le trafic sur un réseau local virtuel (VLAN) spécifique, vous pouvez créer un serveur virtuel avec une stratégie d'écoute qui le limite au traitement du trafic uniquement sur le VLAN spécifié.

Pour configurer un serveur virtuel avec caractères génériques qui écoute un VLAN spécifique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur virtuel génériques qui écoute un VLAN spécifique et vérifier la configuration :

```
add lb vserver <name> <serviceType> IPAddress * Port * -listenpolicy <
    expression> [-listenpriority <positive_integer>]

show vserver
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-vlan1 ANY -listenpolicy "CLIENT.VLAN.ID.EQ(2)
    " -listenpriority 10

```



```
show vserver Vserver-LB-vlan1
<!--NeedCopy-->
```

Pour configurer un serveur virtuel avec caractères génériques qui écoute un VLAN spécifique à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Créez un nouveau serveur virtuel ou ouvrez un serveur virtuel existant.
3. Spécifiez une priorité et une expression de stratégie d'écoute.

Une fois que vous avez créé ce serveur virtuel, vous le liez à un ou plusieurs services, comme décrit dans Configuration de l'équilibrage de charge de base.

Affecter des pondérations aux services

August 20, 2021

Dans une configuration d'équilibrage de charge, vous affectez des pondérations aux services pour indiquer le pourcentage de trafic qui doit être envoyé à chaque service. Les services ayant des pondérations plus élevées peuvent traiter plus de demandes ; les services ayant des pondérations plus faibles peuvent traiter moins de demandes. L'attribution de poids aux services permet à l'appliance Citrix ADC de déterminer la quantité de trafic que chaque serveur à équilibrage de charge peut gérer, et donc d'équilibrer plus efficacement la charge.

Note : Si vous utilisez une méthode d'équilibrage de charge qui prend en charge la pondération des services (par exemple, la méthode d'arrondi), vous pouvez affecter une pondération au service.

Le tableau suivant décrit les méthodes d'équilibrage de charge qui prennent en charge la pondération et décrit brièvement la manière dont la pondération affecte la sélection d'un service pour chacune d'elles.

Méthodes d'équilibrage de charge	Sélection de service avec poids
Round Robin	Le serveur virtuel donne la priorité à la file d'attente des services disponibles de telle sorte que les services ayant les poids les plus élevés arrivent plus fréquemment à l'avant de la file d'attente que ceux ayant les poids les plus faibles et reçoivent proportionnellement plus de trafic. Pour une description complète, voir La méthode Round Robin.
Moins de connexion	Le serveur virtuel sélectionne le service avec la meilleure combinaison de transactions actives et le poids le plus élevé. Pour une description complète, reportez-vous à la section Méthode de connexion la plus faible.
Moins de temps de réponse et moins de temps de réponse à l'aide de moniteurs	Le serveur virtuel sélectionne le service avec la meilleure combinaison de transactions actives et de temps de réponse moyen le plus rapide. Pour une description complète, reportez-vous à la section Méthode du temps de réponse le plus faible.
Moins de bande passante	Le serveur virtuel sélectionne le service avec la meilleure combinaison de moins de trafic et de bande passante la plus élevée. Pour une description complète, reportez-vous à la section Méthode de la moindre bande passante.
Moins de paquets	Le serveur virtuel sélectionne le service avec la meilleure combinaison de paquets le plus faible et de poids le plus élevé. Pour une description complète, reportez-vous à la section Méthode The Moast Packets.
Chargement personnalisé	Le serveur virtuel sélectionne le service avec la meilleure combinaison de charge la plus faible et de poids le plus élevé. Pour obtenir une description complète, reportez-vous à la section Méthode de chargement personnalisée.

Méthodes d'équilibrage de charge	Sélection de service avec poids
Méthodes de hachage et méthode Token	La pondération n'est pas prise en charge par ces méthodes d'équilibrage de charge.

Pour configurer un serveur virtuel pour affecter des poids aux services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -weight <Value> <ServiceName>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -weight 10 Service-HTTP-1
<!--NeedCopy-->
```

Pour configurer un serveur virtuel pour affecter des poids aux services à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Ouvrez le serveur virtuel, puis cliquez sur dans la section **Services** .
3. Dans la colonne Poids du service, affectez une pondération au service.

Configurer le paramètre de version de serveur MySQL et Microsoft SQL

January 21, 2021

Vous pouvez spécifier la version de Microsoft® SQL Server® et le serveur MySQL pour un serveur virtuel d'équilibrage de charge de type MSSQL et MySQL respectivement. Le paramètre de version est recommandé si vous vous attendez à ce que certains clients n'exécutent pas la même version que votre produit MySQL ou Microsoft SQL Server. Le paramètre de version assure la compatibilité entre les connexions côté client et côté serveur en veillant à ce que toutes les communications soient conformes à la version du serveur.

Pour définir le paramètre de version du serveur Microsoft SQL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir le paramètre de version de Microsoft SQL Server pour un serveur virtuel d'équilibrage de charge et vérifiez la configuration :

```
set lb vserver <name> -mssqlServerVersion <mssqlServerVersion>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple

```
> set lb vserver myMSSQLvip -mssqlServerVersion 2008R2
 Done
> show lb vserver myMSSQLvip
    myMSSQLvip (190.0.2.12:1433) - MSSQL    Type: ADDRESS
 . . .
 . . .
    MSsql Server Version: 2008R2
    . . .
    . . .
 Done
>
<!--NeedCopy-->
```

Pour définir le paramètre de version du serveur MySQL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir le paramètre de version de MySQL Server pour un serveur virtuel d'équilibrage de charge et vérifiez la configuration :

```
set lb vserver <name> -mysqlServerVersion <string>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple

```
> set lb vserver mysqlsvr -mysqlserverversion 5.5.30
 Done
```



```
> sh lb vserver mysqlsvr
     mysqlsvr (2.22.2.222:3306) - MYSQL      Type: ADDRESS
 . . .
 . . .
     Mysql Server Version: 5.5.30
    . . .
    . . .
 Done
>
<!--NeedCopy-->
```

Pour définir le paramètre de version du serveur MySQL ou Microsoft SQL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Ouvrez un serveur virtuel de type MySQL ou MSSQL et définissez la version du serveur.

Serveurs virtuels multi-IP

August 20, 2021

Le Citrix ADC prend en charge la création d'un serveur virtuel d'équilibrage de charge unique avec plusieurs adresses IPv4 et IPv6 non consécutives de type VIP. Chaque adresse VIP liée à un serveur virtuel est traitée comme un serveur virtuel individuel. Ces serveurs virtuels ont le même protocole et d'autres paramètres de niveau serveur virtuel. Un serveur virtuel avec plusieurs adresses VIP est également appelé serveur virtuel multi-IP.

Voici quelques avantages de l'utilisation de serveurs virtuels multi-IP :

- Un serveur virtuel multi-IP décharge le travail de création de nombreux serveurs virtuels avec les mêmes paramètres et liaisons de service.
- Les serveurs virtuels multi-IP réduisent efficacement la possibilité d'atteindre la limite maximale des entités de serveurs virtuels.
- Un serveur virtuel multi-IP peut être utilisé pour les clients de différents sous-réseaux pour se connecter au même ensemble de serveurs.
- Un seul serveur virtuel multi-IP peut être utilisé pour que les clients IPv6 et IPv4 se connectent au même ensemble de serveurs.

Configurer un serveur virtuel multi-IP

La configuration d'un serveur virtuel multi-IP comporte les tâches suivantes :

- Créez un IPSet et liez plusieurs adresses IP à celui-ci.
- Liez l'IPSet pour équilibrer la charge des serveurs virtuels.

Notez les points suivants liés à la configuration IPSet :

- Un IPSet peut avoir :
  - Adresses IPv4 et adresses IPv6 non consécutives ou consécutives
  - combinaisons d'adresses IPv4 et IPv6.
- Toutes les adresses IPv4/IPv6 à associer aux serveurs virtuels utilisant IPSet doivent être de type VIP.
- Un seul IPSet peut être lié à plusieurs serveurs virtuels.
- Les adresses IPv4/IPv6 peuvent être entrantes/sortantes vers/depuis IPset indépendamment des liaisons IPset existantes aux serveurs virtuels.
- Vous devez annuler la liaison IPSet à un serveur virtuel avant de lui lier un nouvel IPSet.

Pour ajouter un IPSet et y lier plusieurs adresses VIP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ipset <name>

bind ipset <name> <IPaddress1 ... >

bind ipset <name> <IPaddress2... >

show ipset <name>
<!--NeedCopy-->
```

Pour lier l'IPSet à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -ipset <ipset name>

show lb vserver <name>
<!--NeedCopy-->
```

Pour ajouter un IPSet et y lier plusieurs adresses VIP à l'aide de l'interface graphique

Accédez à **Système** > **Réseau** > **IPsets** et créez un IPset avec plusieurs adresses VIP.

Pour lier l'IPSet à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et ouvrez un serveur virtuel auquel vous souhaitez lier l'IPSet créé.
2. Dans **Paramètres de base**, définissez le paramètre **IPSet**sur le nom de l'IPSet créé.

```
> add ipset IPSET-1


Done

> bind ipset IPSET-1 9.9.9.10


Done

> bind ipset IPSET-1 1000::20


Done

> add lb vserver LBVS-1 HTTP 8.8.8.10 80  - ipset IPSET-1


Done

> add service SVC-1 3.3.3.10 HTTP 80


Done

> add service SVC-2 3.3.3.100 HTTP 80


Done

> bind lb vserver LBVS-1 SVC-1


Done

> bind lb vserver LBVS-1 SVC-2


Done
```


Prise en charge de GSLB pour les serveurs virtuels multi-IP

Dans les déploiements cloud, les adresses IP flottantes ne sont pas prises en charge. Ces adresses IP sont requises pour les déploiements à haute disponibilité. Avec la prise en charge d'IPSet, vous pouvez associer une adresse IP privée à chacune des instances principale et secondaire. Une des adresses IP privées est ajoutée lors de la création du serveur virtuel. L'autre adresse IP est liée à un IPSet. Cet IPset est ensuite associé au serveur virtuel. Généralement, une adresse IP publique est mappée à l'une des adresses IP privées en fonction de laquelle l'appliance prend le trafic. Pendant le basculement, ce mappage change dynamiquement pour acheminer le trafic vers le nouveau système principal.

Dans les déploiements GSLB, le service GSLB représente l'adresse IP, le numéro de port et le type de service du serveur virtuel. Cette adresse IP peut être l'adresse IP configurée lors de l'ajout du serveur virtuel ou il peut s'agir de l'une des adresses IP de l'IPSet. Indépendamment de l'adresse IP utilisée dans le service GSLB, les statistiques et l'état sont hérités de la même entité de serveur virtuel d'équilibrage de charge.

La topologie enfant parent est également prise en charge avec IPSet. L'IPSet peut être associé aux serveurs virtuels d'équilibrage de charge sur les sites enfants. La communication entre le parent et le site enfant utilise toujours l'adresse IP publique et le port public du service GSLB

En outre, avec la prise en charge IPSet, vous pouvez disposer d'un seul point de terminaison de serveur virtuel pour le trafic IPv4 et IPv6. Auparavant, vous deviez configurer différents serveurs virtuels pour le trafic IPv4 et IPv6. Avec la prise en charge d'IPSet, vous pouvez associer des adresses IP IPv4 et IPv6 au même jeu d'adresses IP. Vous pouvez ajouter différents services GSLB représentant les points de terminaison IPv4 et IPv6.

Remarque : Une seule adresse IP est associée à un service GSLB. Vous ne pouvez pas associer un IPSet à un service GSLB. Pour plus d'informations sur la configuration des entités GSLB, consultez la rubrique Configurer les entités GSLB individuellement.

Limiter le nombre de demandes simultanées sur une connexion client

August 20, 2021

Vous pouvez limiter le nombre de demandes simultanées sur une seule connexion client. Vous pouvez protéger les serveurs contre les vulnérabilités de sécurité en limitant le nombre de demandes simultanées. Lorsque la connexion client atteint la limite maximale spécifiée, l'appliance Citrix ADC supprime les requêtes suivantes sur la connexion jusqu'à ce que le nombre de requêtes en attente soit inférieur à la limite.

Vous pouvez configurer le paramètre MaxPipelineNat pour limiter le nombre de demandes simultanées sur une seule connexion client. Ce paramètre s'applique uniquement aux types de service

suivants et lorsque « svrTimeout » est défini sur zéro :

- ANY
- Tous les types de service UDP sauf DNS

La valeur par défaut du paramètre MaxPipelineNat est 255. La valeur zéro (0) n'applique aucune limite au nombre de demandes simultanées. Lorsqu'aucune limite n'est définie, l'appliance Citrix ADC exécute toutes les demandes.

> **Remarque**
>
> Si vous définissez MaxPipelineNat sur une valeur plus élevée, la probabilité d'attaque d'usurpation peut être plus élevée. Par conséquent, il est recommandé de définir MaxPipelineNat à une valeur inférieure.

Pour limiter le nombre de connexions simultanées pour un client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb parameter -maxPipelineNat <positive_integer>
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -maxPipelineNat 199
<!--NeedCopy-->
```

Pour limiter le nombre de connexions simultanées pour un client à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage**de charge, spécifiez une valeur pour les requêtes NAT Max Pipeline.

Configurer l'équilibrage de charge de Diameter

August 20, 2021

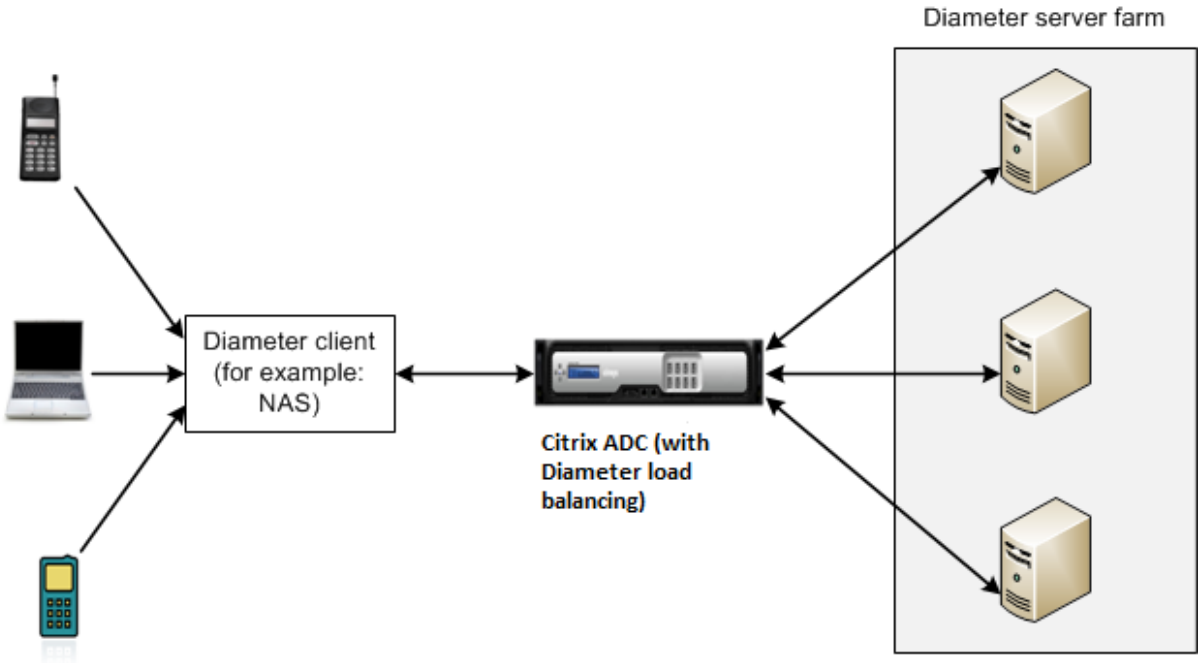
Le protocole Diameter est un protocole de signalisation AAA (Authentication, Authorization and Accounting) de nouvelle génération utilisé principalement sur les appareils mobiles tels que les ordinateurs portables et les téléphones mobiles. Il s'agit d'un protocole peer-to-peer, par opposition au

modèle client-serveur traditionnel utilisé par la plupart des autres protocoles. Toutefois, dans la plupart des déploiements de Diameter, les clients sont à l'origine de la demande et le serveur répond à la demande.

Lorsque les messages Diameter sont échangés, le serveur Diameter effectue généralement beaucoup plus de traitement que le client Diameter. Avec l'augmentation du volume de signalisation du plan de contrôle, le serveur Diameter devient un goulot d'étranglement. Par conséquent, les messages de Diameter doivent être équilibrés de charge sur plusieurs serveurs. Un serveur virtuel effectuant l'équilibrage de charge des messages de Diameter offre les avantages suivants :

- Charge plus légère sur les serveurs Diameter, ce qui se traduit par un temps de réponse plus rapide pour les utilisateurs finaux.
- Surveillance de l'intégrité du serveur et meilleures capacités de basculement.
- Meilleure évolutivité en termes d'ajout de serveur sans modifier la configuration du client.
- Haute disponibilité.
- Déchargement de Diameter SSL.

La figure suivante illustre un système Diameter dans un déploiement de Citrix ADC :



Un système Diameter comporte les composants suivants :

- **Client Diameter.** Prend en charge les applications clientes Diameter en plus du protocole de base. Les clients Diameter sont souvent implémentés dans des appareils situés à la périphérie d'un réseau et fournissent des services de contrôle d'accès pour ce réseau. Des exemples typiques de clients Diameter sont un serveur d'accès réseau (NAS) et l'agent étranger (FA) Mobile IP.

- **Agent Diameter.** Fournit des services de relais, de proxy, de redirection ou de traduction. L'appliance Citrix ADC (configurée avec un serveur virtuel d'équilibrage de charge de Diameter) joue le rôle d'agent de Diameter.
- **Serveur Diameter.** Gère les demandes d'authentification, d'autorisation et de comptabilisation pour un domaine particulier. Un serveur de Diameter doit prendre en charge les applications de serveur de Diameter en plus du protocole de base.

Dans une topologie Diameter typique, lorsqu'un périphérique utilisateur final (tel qu'un téléphone mobile) a besoin d'un service, il envoie une demande à un client Diameter. Chaque client de Diameter établit une connexion unique (connexion TCP — SCTP n'est pas encore pris en charge) avec un serveur de Diameter tel que spécifié par le protocole de base de Diameter RFC 6733. La connexion est longue durée et tous les messages entre les deux nœuds de Diameter (client et serveur) sont échangés sur cette connexion. Citrix ADC utilise l'équilibrage de charge basé sur les messages.

Exemple :

Un fournisseur de services mobiles utilise Diameter pour son système de facturation. Lorsqu'un abonné utilise un numéro prépayé, le client Diameter envoie plusieurs fois des demandes au serveur pour vérifier le solde disponible. Le protocole Diameter établit une connexion entre le client et le serveur, et toutes les demandes sont échangées sur cette connexion. L'équilibrage de charge basé sur la connexion serait inutile, car il n'y a qu'une seule connexion. Cependant, avec le grand nombre de messages sur la connexion, l'équilibrage de charge basé sur les messages accélère le processus de facturation de l'abonné mobile prépayé.

Fonctionnement de l'équilibrage de la charge de Diameter

Une demande d'homologue de déconnexion (DPR) indique l'intention de l'homologue de fermer la connexion, avec la raison de la fermeture de la connexion. L'homologue répond avec un DPA (TCP fournit toujours un DPA réussi).

- Lorsque l'appliance reçoit un DPR du client, elle diffuse le DPR sur tous les serveurs et répond immédiatement avec un DPA au client. Les serveurs répondent avec des DPA, mais l'appliance les ignore. Le client envoie un FIN que l'appliance diffuse à tous les serveurs.
- Lorsque l'appliance reçoit un DPR du serveur, elle répond avec un DPA à ce serveur seul et ne supprime pas le serveur du pool de réutilisation. Lorsque le serveur envoie un FIN, l'appliance répond avec FIN/ACK et supprime les connexions du pool de réutilisation.
- Si l'appliance reçoit un FIN du client, elle lui envoie un FIN/ACK, diffuse le FIN et supprime immédiatement la connexion au serveur du pool de réutilisation.
- Si l'appliance reçoit un FIN du serveur, elle envoie un FIN/ACK et le supprime du pool de réutilisation. Tout nouveau message pour ce serveur est envoyé sur une nouvelle connexion.

Trafic de Diameter d'équilibrage de charge

Lorsqu'un client envoie une demande à l'appliance Citrix ADC, l'appliance analyse la demande et l'équilibre contextuel de la charge vers un serveur Diameter basé sur un AVP persistant. L'appliance a annoncé l'identité du client sur le serveur, de sorte qu'elle n'ajoute pas d'entrées de routage, car le serveur attend des messages directement du client.

Les demandes initiées par le serveur ne sont pas aussi fréquentes que les demandes client. Les demandes initiées par le serveur sont similaires aux demandes initiées par le client, sauf :

- Étant donné que les messages sont reçus de plusieurs serveurs, l'appliance maintient l'état de la transaction en ajoutant un numéro HBYH (Hop by Hop) unique à chaque message de demande transféré. Lorsque la réponse du message arrive (avec le même numéro HBYH), l'appliance convertit ce numéro HBYH en numéro HBYH reçu sur le serveur lorsque la demande est arrivée.
- L'appliance Citrix ADC ajoute une entrée de routage en mettant son identité, car le client voit l'appliance comme un agent de relais.

Remarque : si un message de diamètre couvre plusieurs paquets, l'appliance accumule les paquets dans une file d'attente d'en-tête incomplète et les transmet au serveur lorsque le message complet est accumulé. De même, si un seul paquet contient plusieurs messages de Diameter, l'appliance divise le paquet et transmet les messages aux serveurs, comme déterminé par le serveur virtuel d'équilibrage de charge.

Déconnecter une session

Une demande d'homologue de déconnexion (DPR) indique l'intention de l'homologue de fermer la connexion, avec la raison de la fermeture de la connexion. L'homologue répond avec un DPA (TCP fournit toujours un DPA réussi).

- Lorsque l'appliance Citrix ADC reçoit un DPR du client, il diffuse le DPR sur tous les serveurs et répond immédiatement avec un DPA au client. Les serveurs répondent avec des DPA, mais l'appliance les ignore. Le client envoie un FIN que l'appliance diffuse à tous les serveurs.
- Lorsque l'appliance reçoit un DPR du serveur, elle répond avec un DPA à ce serveur seul et ne supprime pas le serveur du pool de réutilisation. Lorsque le serveur envoie un FIN, l'appliance répond avec FIN/ACK et supprime les connexions du pool de réutilisation.
- Si l'appliance reçoit un FIN du client, elle lui envoie un FIN/ACK, diffuse le FIN et supprime immédiatement la connexion au serveur du pool de réutilisation.
- Si l'appliance reçoit un FIN du serveur, elle envoie un FIN/ACK et le supprime du pool de réutilisation. Tout nouveau message pour ce serveur est envoyé sur une nouvelle connexion.

Configurer l'équilibrage de charge pour le trafic de Diameter

Pour configurer l'appliance Citrix ADC pour équilibrer le trafic de Diameter, vous devez d'abord définir les paramètres de Diameter sur l'appliance, puis ajouter le moniteur de Diameter, ajouter les services de Diameter, lier les services au moniteur, ajouter le serveur virtuel d'équilibrage de charge de Diameter et lier les services au serveur virtuel virtuel virtuel virtuel serveur.

Pour configurer l'équilibrage de charge pour le trafic de Diameter à l'aide de l'interface de ligne de commande

Configurez les paramètres de Diameter.

```
set ns diameter -identity <string> -realm <string> -
   serverClosePropagation <YES|NO>
<!--NeedCopy-->
```

Exemple :

```
set ns diameter -identity mydomain.org -realm org -
   serverClosePropagation YES
<!--NeedCopy-->
```

Ajoutez un moniteur de Diameter.

```
add lb monitor <monitorName> DIAMETER -originHost <string> -originRealm
    <string>
<!--NeedCopy-->
```

Exemple :

```
add lb monitor diameter_mon DIAMETER -originHost mydomain.org -
   originRealm org
<!--NeedCopy-->
```

Créez les services Diameter.

```
add service <name> <IP> DIAMETER <port>
<!--NeedCopy-->
```

Exemple :

```
add service diameter_svc0 10.102.82.86 DIAMETER 3868

add service diameter_svc1 10.102.82.87 DIAMETER 3868

```



```
5 add service diameter_svc2 10.102.82.88 DIAMETER 3868
6
7 add service diameter_svc3 10.102.82.89 DIAMETER 3868
8 <!--NeedCopy-->
```

Liez les services Diameter au moniteur Diameter.

```
1 bind service <name>@ monitorName <monitorName>
2 <!--NeedCopy-->
```

Exemple :

```
1 bind service diameter_svc0 -monitorName diameter_mon
2
3 bind service diameter_svc1 -monitorName diameter_mon
4
5 bind service diameter_svc2 -monitorName diameter_mon
6
7 bind service diameter_svc3 -monitorName diameter_mon
8 <!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge de Diameter avec persistance de Diameter.

```
1 add lb vserver <name> DIAMETER <IPAddress> <port> -persistenceType
     DIAMETER -persistAVPno <positive_integer>
2 <!--NeedCopy-->
```

Exemple :

```
1 add lb vserver diameter_vs DIAMETER 10.102.112.152 3868 -
     persistenceType DIAMETER -persistAVPno 263
2 <!--NeedCopy-->
```

Liez les services Diameter au serveur virtuel d'équilibrage de charge Diameter.

```
1 bind lb vserver <name> <serviceName>
2 <!--NeedCopy-->
```

Exemple :

```
1 bind lb vserver diameter_vs diameter_svc0
2
3 bind lb vserver diameter_vs diameter_svc1
4
5 bind lb vserver diameter_vs diameter_svc2
```



```
6
7 bind lb vserver diameter_vs diameter_svc3
8 <!--NeedCopy-->
```

Enregistrez la configuration.

```
1 save ns config
2 <!--NeedCopy-->
```

Remarque : Vous pouvez également configurer l'équilibrage de charge du trafic de diamètre sur SSL à l'aide du type de service **SSL_DIAMETER**.

Pour configurer l'équilibrage de charge pour le trafic de Diameter à l'aide de l'utilitaire de configuration

1. Accédez à **Système** > **Paramètres** > **Modifier les paramètres de diamètre** et définissez les paramètres de diamètre.
2. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et créez un serveur virtuel d'équilibrage de charge de type Diamètre.
3. Créez un service de type Diameter.
4. Créez un moniteur de type Diameter. Dans Paramètres spéciaux, définissez l'hôte d'origine et le domaine d'origine.
5. Liez le moniteur au service et liez le service au serveur virtuel Diameter.
6. Dans Paramètres avancés, cliquez sur **Persistance**, spécifiez le diamètre et entrez un numéro AVP de persistance.
7. Cliquez sur **Enregistrer**, puis sur **Terminé**.

Configurer l'équilibrage de charge FIX

August 20, 2021

Le protocole FIX (Financial Information Exchange) est une norme de message ouvert utilisée dans le secteur financier pour l'échange électronique d'informations relatives aux transactions de titres entre partenaires commerciaux. Le protocole FIX/SSL_FIX est largement utilisé par les entreprises acheteur et vendeur, les plates-formes de négociation et les régulateurs pour communiquer des informations commerciales.

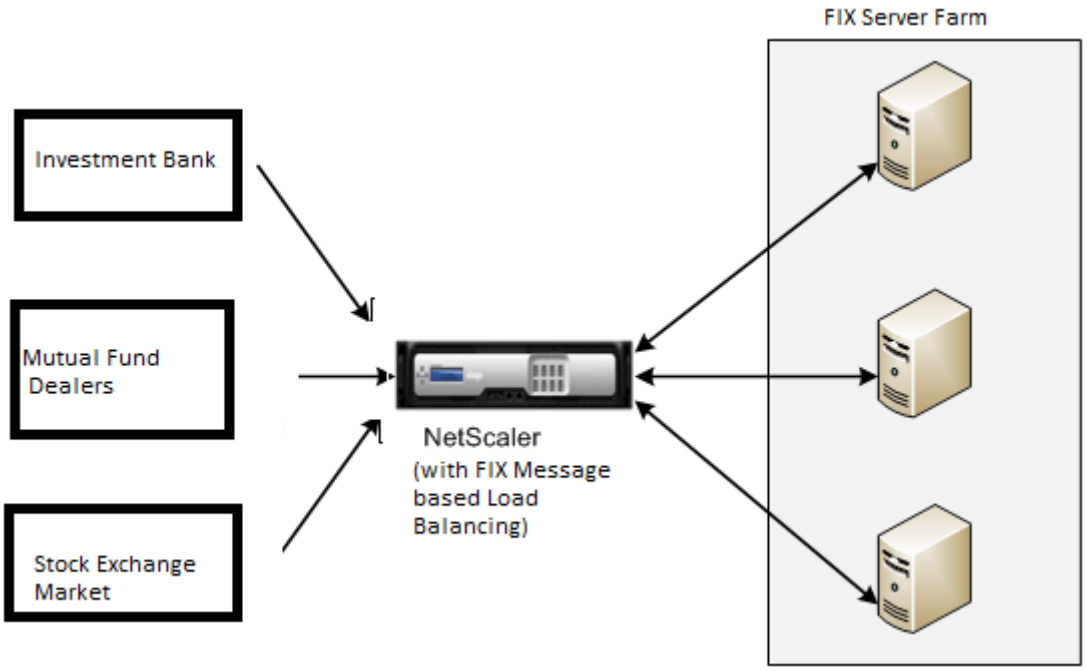
Cette fonctionnalité vous permet de configurer un serveur virtuel d'équilibrage de charge FIX ou SSL_FIX pour distribuer les messages FIX entrants et assurer la sécurité dans la messagerie FIX. Citrix ADC prend en charge l'équilibrage de charge basé sur les messages FIX (MBLB) pour les versions FIX 4.1, FIX 4.2, FIX 4.3 et FIX 4.4.

FIX MBLB sur une appliance Citrix ADC offre les avantages suivants :

1. Gestion efficace des serveurs FIX ou SSL_FIX avec surveillance de l'intégrité et de la haute disponibilité supérieure.
2. Protection SYN pour tous les serveurs FIX ou SSL_FIX.
3. Persistance de la session FIX.

Fonctionnement de l'équilibrage de charge FIX

Une configuration FIX MBLB inclut un serveur virtuel d'équilibrage de charge FIX et plusieurs serveurs FIX équilibrés de charge. Le serveur virtuel FIX reçoit le trafic client entrant, analyse le trafic entrant en messages FIX, sélectionne un serveur FIX pour chaque message FIX et transmet le message au serveur FIX sélectionné. Le dessin conceptuel suivant illustre une configuration typique d'équilibrage de charge FIX.



Dans une configuration de base de FIX MBLB, le serveur virtuel FIX distribue les messages FIX provenant des clients vers les serveurs FIX à charge équilibrée à l'aide de la méthode d'équilibrage de charge ronde. Lorsque la persistance de type FIXSESSION est activée, le serveur virtuel FIX sélectionne le même serveur pour différents messages FIX appartenant à la même session FIX. La session FIX est déterminée en fonction des valeurs des champs **FIX** SenderCompid (balise 49) et TargetCompid (balise 56).

Configurer et surveiller l'équilibrage de charge pour le trafic FIX

Voici les configurations que vous devez faire pour équilibrer la charge du trafic des messages FIX :

1. Configuration du serveur virtuel d'équilibrage de charge FIX
2. Configuration du serveur virtuel d'équilibrage de charge SSL_FIX
3. Configuration du service d'équilibrage de charge FIX
4. Configuration du service d'équilibrage de charge SSL_FIX
5. Configuration de la persistance FIXSESSION
6. Définition du délai d'expiration de la persistance
7. Affichage des statistiques FIX/SSL_FIX
8. Surveillance des sessions persistantes FIX/SSL_FIX

Pour configurer un serveur d'équilibrage de charge FIX à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb vserver <name> FIX <IP> <PORT>
<!--NeedCopy-->
```

Exemple

```
add lb vserver vs1 FIX 10.102.82.86 3868
<!--NeedCopy-->
```

Pour configurer un serveur virtuel d'équilibrage de charge SSL_FIX à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb vserver <name> SSL_FIX <IP> <PORT>
<!--NeedCopy-->
```

Exemple

```
add lb vserver vs1 SSL_FIX 10.102.82.86 3868
<!--NeedCopy-->
```

Pour configurer un service FIX à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <name> <ip-addr> FIX <port>
<!--NeedCopy-->
```


Exemple

```
add service_svc1 10.102.82.86 FIX 3868
<!--NeedCopy-->
```

Pour configurer un service SSL_FIX à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <name> <ip-addr> SSL_FIX <port>
<!--NeedCopy-->
```

Exemple

```
add service svc1 10.102.82.86 SSL_FIX 3868
<!--NeedCopy-->
```

Pour configurer la persistance FIXSESSION à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -persistenceType FIXSESSION
<!--NeedCopy-->
```

Exemple

```
set lb vserver vs1 -persistenceType FIXSESSION
<!--NeedCopy-->
```

Pour définir le délai d'attente de persistance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -timeout <value>
<!--NeedCopy-->
```

Exemple

```
set lb vserver vs1  - timeout 2
<!--NeedCopy-->
```


Pour afficher les statistiques FIX à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat lb vserver <name>
<!--NeedCopy-->
```

Exemple

```
stat lb vserver_svc1
<!--NeedCopy-->
```

Pour lier le service FIX au serveur virtuel FIX à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb vserver <name> <service name>
<!--NeedCopy-->
```

Exemple

```
bind lb vserver vs1 svc1
<!--NeedCopy-->
```

Pour afficher les sessions persistantes FIX à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show lb persistentSessions <name>
<!--NeedCopy-->
```

Exemple

```
show lb persistentSessions vs1
<!--NeedCopy-->
```

> **Remarque**
>
> Remarque : Vous pouvez maintenant configurer l'équilibrage de charge du trafic FIX sur SSL à l'aide du type de service SSL_FIX. Ce service fournit une communication sécurisée pour les messages FIX.

Pour configurer le serveur virtuel d'équilibrage de charge FIX à l'aide de l'interface graphique

1. Accédez à la page **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis cliquez sur **Ajouter** pour créer un serveur virtuel Équilibrage de charge FIX.
2. Dans la page **Serveur virtuel d'équilibrage** de charge, définissez les paramètres du serveur :
   a) Nom du serveur virtuel
   b) Type de protocole comme « FIX »
   c) Type d'adresse IP du serveur
   d) Adresse IP du serveur
   e) Numéro de port du serveur
3. Cliquez sur **OK** et **Continuer** pour définir d'autres paramètres.
4. Dans la section **Services**, sélectionnez ou ajoutez un nouveau service virtuel d'équilibrage de charge FIX et liez-le au serveur FIX.
5. Dans la section **Persistance**, définissez les paramètres suivants :
   a) Type de persistance comme 'FIXSESSION'
   b) Intervalle de temporisation
6. Cliquez sur **OK**, puis sur **Terminé**.

Pour modifier un serveur virtuel d'équilibrage de charge FIX à l'aide de l'interface graphique

Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez un serveur FIX et cliquez sur **Modifier** .

Pour supprimer un serveur virtuel d'équilibrage de charge FIX à l'aide de l'interface graphique

Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez un serveur FIX, puis cliquez sur **Supprimer**.

Pour configurer FIX Load Balancing Virtual Service à l'aide de l'interface graphique

1. Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Services** et cliquez sur **Ajouter** pour créer un service virtuel FIX Load Balancing.
2. Dans la page **Services**, définissez les paramètres suivants. Vous pouvez cliquer sur la flèche « Plus » pour définir d'autres paramètres tels que Domaine du trafic, ID de hachage, ID du serveur, Type de cache et Nombre de connexions actives.
   a) Nom du service — Nom du service virtuel FIX
   b) Choisissez le type de serveur virtuel comme (Nouveau ou existant)

c) Protocole — Type de protocole comme 'FIX'
d) Serveur — Adresse IP du serveur virtuel
e) Port — Numéro de port du serveur

3. Cliquez sur **OK** et **Continuer** pour définir d'autres paramètres tels que Moniteurs, Seuil et délai d'expiration, Profils et Stratégies.
4. Cliquez sur **OK**, puis sur **Terminé**.

Pour modifier un service virtuel d'équilibrage de charge FIX à l'aide de l'interface graphique

Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Services**, sélectionnez un **service FIX** et cliquez sur **Modifier** .

Pour supprimer un service virtuel d'équilibrage de charge FIX à l'aide de l'interface graphique

Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Services**, sélectionnez un service FIX, puis cliquez sur **Supprimer**.

Pour afficher les statistiques du serveur d'équilibrage de charge FIX

Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis cliquez sur **Statistiques** pour afficher les statistiques du serveur FIX.

Pour afficher des sessions persistantes pour un serveur FIX à l'aide de l'interface graphique graphique

Accédez à **la page Configuration** > **Gestion du trafic** et, sous **Surveillance des sessions, cliquez sur Sessionspersistantes du serveur virtuel** .

Pour effacer les sessions persistantes d'un serveur FIX à l'aide de l'interface graphique

1. Accédez à **la page Configuration** > **Gestion du trafic** et, sous **Surveillance des sessions**, cliquez sur **Effacer les sessions persistantes** .
2. Dans la page **Effacer les sessions persistantes**, définissez les paramètres suivants :
   a) Serveur virtuel — Choisir un serveur virtuel FIX
   b) Paramètre de persistance — Choisir un paramètre de persistance FIX
3. Cliquez sur **OK**.

Équilibrage de charge MQTT

August 20, 2021

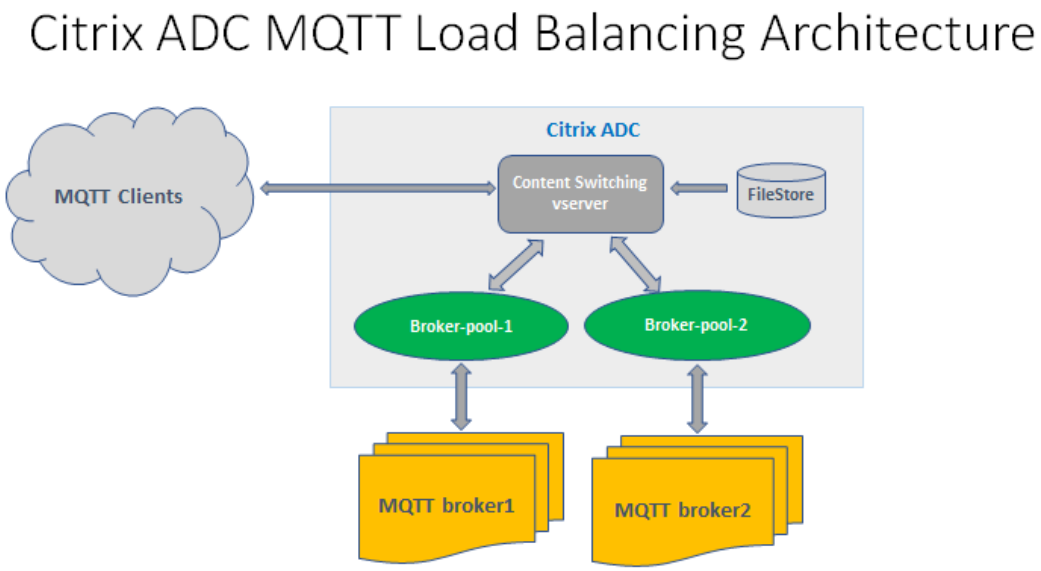
Message Queuing Telemetry Transport (MQTT) est un protocole de messagerie standard OASIS pour l'Internet des objets (IoT). MQTT est une technologie flexible et facile à utiliser qui fournit une communication efficace au sein d'un système IoT. MQTT est un protocole basé sur un courtier et est largement utilisé pour faciliter l'échange de messages entre les clients et le courtier.

Les avantages clés suivants de MQTT en font une option idéale pour votre appareil IoT :

- Fiabilité
- Temps de réponse rapide
- Capacité de prendre en charge des appareils illimités
- Publier ou abonner des messages qui sont parfaits pour les communications plusieurs-à-plusieurs

L'IoT est le réseau d'appareils interconnectés qui sont intégrés avec des capteurs, des logiciels, une connectivité réseau et des appareils électroniques nécessaires. Les composants intégrés permettent aux périphériques IoT de collecter et d'échanger des données. L'augmentation de l'utilisation des périphériques IoT pose de multiples défis pour l'infrastructure réseau, Scale étant le principal. Dans un déploiement à grande échelle d'appareils IoT, les données générées par chaque périphérique IoT doivent être analysées rapidement. Pour atteindre les exigences d'échelle et l'utilisation efficace des ressources, la charge sur le pool de courtiers doit être répartie uniformément. Avec la prise en charge du protocole MQTT, vous pouvez utiliser l'appliance Citrix ADC dans les déploiements IoT pour équilibrer la charge du trafic MQTT.

La figure suivante illustre l'architecture MQTT utilisant une appliance Citrix ADC pour équilibrer la charge du trafic MQTT.



Un déploiement IoT avec protocole MQTT comporte les composants suivants :

- **Courtier MQTT.** Serveur qui reçoit tous les messages des clients, puis achemine les messages vers les clients de destination appropriés. Le courtier est responsable de recevoir tous les messages, de filtrer les messages, de déterminer qui est abonné à chaque message et d'envoyer le message à ces clients abonnés. Le courtier est le centre central par lequel chaque message doit passer.
- **Client MQTT.** Tout appareil, depuis un micro contrôleur jusqu'à un serveur à part entière, qui exécute une bibliothèque MQTT et se connecte à un courtier MQTT sur un réseau. Les éditeurs et les abonnés sont des clients MQTT. Les étiquettes de l'éditeur et de l'abonné désignent si le client publie des messages ou s'est abonné à recevoir des messages.
- **Équilibreur de charge MQTT.** L'appliance Citrix ADC est configurée avec un serveur virtuel d'équilibrage de charge MQTT pour équilibrer la charge du trafic MQTT.

Dans un déploiement IoT typique, le broker (cluster de serveurs) gère le groupe de périphériques IoT (clients IoT). La charge de l'appliance Citrix ADC équilibre le trafic MQTT vers les courtiers en fonction de divers paramètres, tels que l'ID client, la rubrique et le nom d'utilisateur.

Configurer l'équilibrage de charge pour le trafic MQTT

Pour que l'appliance Citrix ADC puisse équilibrer la charge du trafic MQTT, effectuez les tâches de configuration suivantes :

1. Configurez les services MQTT/MQTT_TLS ou les groupes de services.
2. Configurez le serveur virtuel d'équilibrage de charge MQTT/MQTT_TLS.

3. Liez les services MQTT/MQTT_TLS au serveur virtuel d'équilibrage de charge MQTT/MQTT_TLS.
4. Configurer le serveur virtuel de commutation de contenu MQTT/MQTT_TLS.
5. Configurer une action de commutation de contenu qui spécifie le serveur virtuel d'équilibrage de charge cible
6. Configurez une stratégie de commutation de contenu.
7. Liez la stratégie de commutation de contenu à un serveur virtuel de commutation de contenu déjà configuré pour rediriger vers le serveur virtuel d'équilibrage de charge spécifique.
8. Enregistrez la configuration.

Pour configurer l'équilibrage de charge pour le trafic MQTT à l'aide de l'interface de ligne de commande

Configurez les services MQTT/MQTT_TLS ou les groupes de services.

```
add service <name> <IP> <protocol> <port>
add servicegroup <ServiceGroupName> <Protocol>
bind servicegroup <serviceGroupName> <IP> <port>
<!--NeedCopy-->
```

Exemple :

```
add service srvc1 10.106.163.3 MQTT 1883
add servicegroup srvcg1 MQTT
bind servicegroup srvcg1 10.106.163.3 1883
<!--NeedCopy-->
```

Configurez le serveur virtuel d'équilibrage de charge MQTT/MQTT_TLS.

```
add lb vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver lb1 MQTT 10.106.163.9 1883
<!--NeedCopy-->
```

Liez les services ou groupes de services MQTT/MQTT_TLS au serveur virtuel d'équilibrage de charge MQTT.

```
bind lb vserver <name> <serviceName>
bind lb vserver <name> <servicegroupName>
<!--NeedCopy-->
```

Exemple :


```
bind lb vserver lb1 srvc1
bind lb vserver lb1 srvcg1
<!--NeedCopy-->
```

Configurer le serveur virtuel de commutation de contenu MQTT/MQTT_TLS.

```
add cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Exemple :

```
add cs vserver cs1 MQTT 10.106.163.13 1883
<!--NeedCopy-->
```

Configurez une action de commutation de contenu qui spécifie le serveur virtuel d'équilibrage de charge cible.

```
add cs action <name> -targetLBVserver <string> [-comment <string>]
<!--NeedCopy-->
```

Exemple :

```
add cs action act1 -targetlbvserver lbv1
<!--NeedCopy-->
```

Configurez une stratégie de commutation de contenu.

```
add cs policy <policyName> [-url <string> | -rule <expression>] -
    action <actName>
<!--NeedCopy-->
```

Exemple :

```
add cs policy cspol1  -rule   "MQTT.COMMAND.EQ(CONNECT) && MQTT.CONNECT
    .FLAGS.QOS.eq(2)"  -action act1
<!--NeedCopy-->
```

Liez la stratégie de commutation de contenu à un serveur virtuel de commutation de contenu déjà configuré pour rediriger vers le serveur virtuel d'équilibrage de charge spécifique.

```
bind cs vserver <virtualServerName> -policyName <policyName> -priority
    <positiveInteger>
<!--NeedCopy-->
```

Exemple :


```
bind cs vserver cs1 -policyName cspol1 -priority 20
<!--NeedCopy-->
```

Enregistrez la configuration.

```
save ns config
<!--NeedCopy-->
```

Pour configurer l'équilibrage de charge pour le trafic MQTT à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**et créez un serveur virtuel d'équilibrage de charge de type **MQTT** ou **MQTT_TLS**.
2. Créez un service ou un groupe de services de type MQTT.
3. Liez le service au serveur virtuel MQTT.
4. Cliquez sur **Enregistrer**.

Limite de longueur de message MQTT

L'appliance Citrix ADC traite les messages dont la longueur de message est supérieure à 65536 octets comme des paquets jumbo et les rejette par défaut. Le paramètre `dropmqttjumbomessage` lb décide de traiter les paquets jumbo ou non. Ce paramètre est par défaut défini sur **YES**, ce qui implique que les paquets MQTT jumbo sont supprimés par défaut. Si ce paramètre est défini sur **NO**, l'appliance ADC gère même les paquets dont la longueur du message est supérieure à 65536 octets.

Pour configurer l'appliance ADC de manière à gérer les paquets jumbo à l'aide de l'interface de ligne de commande :

```
Set lb parameter -dropMqttJumboMessage [YES | NO]
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -dropMqttJumboMessage no
<!--NeedCopy-->
```

Protéger une configuration d'équilibrage de charge contre les défaillances

August 20, 2021

Lorsqu'un serveur virtuel d'équilibrage de charge échoue ou lorsque le serveur virtuel est incapable de gérer un trafic excessif, la configuration d'équilibrage de charge peut échouer. Vous pouvez protéger votre configuration d'équilibrage de charge contre les défaillances en configurant ;

- l'appliance Citrix ADC pour rediriger le trafic excédentaire vers une autre URL,
- un serveur virtuel d'équilibrage de charge de sauvegarde, et
- un basculement de connexion avec état.

Rediriger les demandes du client vers une autre URL

August 20, 2021

Vous pouvez rediriger les requêtes vers une autre URL à l'aide d'une redirection HTTP 302 si un serveur virtuel d'équilibrage de charge de type HTTP ou HTTPS tombe en panne ou est désactivé. L'URL alternative peut fournir des informations sur l'état du serveur. L'URL de redirection configurée est spécifiée dans l'en-tête d'emplacement de la réponse HTTP. L'URL exacte spécifiée dans la réponse dépend des options de configuration suivantes :

- Si l'URL de redirection configurée contient uniquement le nom de domaine, par exemple http://www.sample1.example.com, l'URL de redirection spécifiée dans la réponse HTTP ajoute l'URI (Uniform Resource Identifier). Il est spécifié dans la requête HTTP au nom de domaine configuré. Par exemple, si la requête contient l'en-tête GET http://www.sample2.example.com/images/site_nav.png, l'en-tête d'emplacement dans la réponse de redirection spécifie l'emplacement : en-tête http://www.sample1.example.com/images/site_nav.png.

  > **Remarque**
  >
  > Les noms de domaine dans la demande et la réponse peuvent différer. Dans cette rubrique, les deux domaines sont appelés sample1.example.com et sample2.example.com pour expliquer le concept.

- Si l'URL de redirection configurée contient un chemin complet, la réponse de redirection spécifie l'URL configurée complète, indépendamment de l'URI de la requête. Par exemple, les URL suivantes sont :
  - URL demandée - http://www.redirect.com/en/index.html
  - URL de redirection - http://www.redirect.com/en/site_down.html

Le tableau suivant répertorie les options de configuration précédentes :

URL de redirection configurée	URL dans la requête HTTP	En-tête dans la réponse HTTP
http://www.sample1.example.com	http://www.sample2.example.com/en/index.html	http://www.sample1.example.com/en/index.html
http://www.sample1.example.com/en/error.html	http://www.sample2.example.com/en/index.html	http://www.sample1.example.com/en/error.html

Remarque

- Lors de la configuration d'une URL de redirection, l' http://example.com URL n'est pas la même que l' http://example.com/ URL, car cette dernière contient le chemin complet du chemin d'accès Webroot, /.
- Si un serveur virtuel d'équilibrage de charge est configuré avec un serveur virtuel de sauvegarde et une URL de redirection, le serveur virtuel de sauvegarde a priorité sur l'URL de redirection. Une redirection n'est utilisée que lorsque les serveurs virtuels principaux et les serveurs virtuels de sauvegarde sont DOWN.

Pour configurer un serveur virtuel pour rediriger la demande du client vers une URL à l'aide de l'interface de ligne de commande

1. Créez un serveur virtuel d'équilibrage de charge.

   ```
   set lb vserver -redirect url
   ```

2. Vérifiez que l'option URL de redirection fonctionne comme prévu. Désactivez le serveur virtuel.

   ```
   disable vserver <vserver_name>
   ```

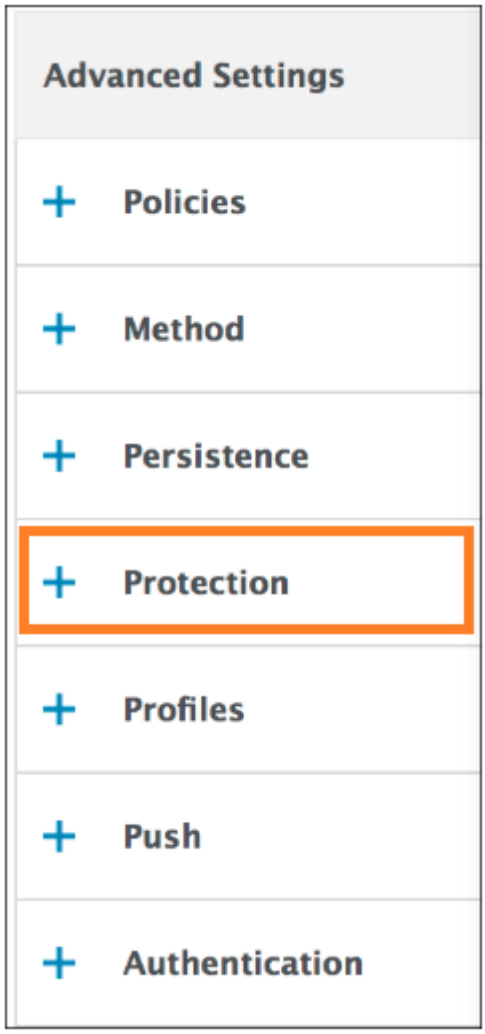
3. Accédez à l'URL du site Web à partir d'un navigateur Web pour vérifier que la demande est redirigée comme prévu. Vous devrez peut-être effacer le cache du navigateur Web et établir une nouvelle connexion avant d'accéder au site Web.
4. Activer le serveur virtuel.

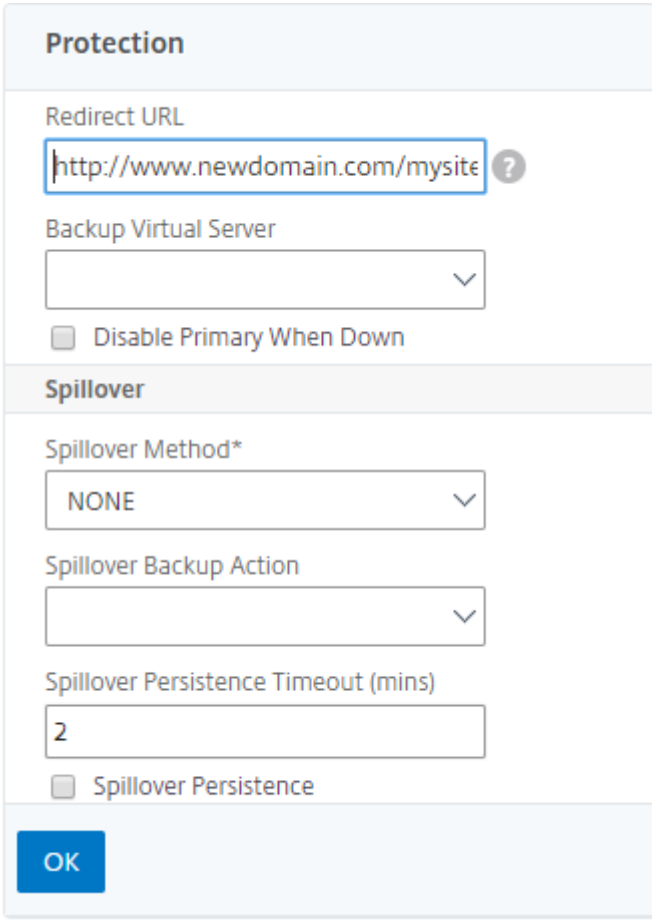
   ```
   enable vserver <vserver_name>
   ```

Pour configurer un serveur virtuel pour rediriger la demande client vers une URL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, pour ajouter un nouveau serveur virtuel, cliquez sur **Ajouter**.
3. Pour modifier un serveur virtuel existant, sélectionnez-le dans la liste et cliquez sur **Modifier**.

4. Sous l'onglet **Paramètres avancés**, cliquez sur **Protection**. Dans le champ **URL de redirection**, tapez l'URL de redirection (par exemple, http://www.newdomain.com/mysite/maintenance).





5. Cliquez sur **OK**.

Configurer un serveur virtuel d'équilibrage de charge de sauvegarde

August 20, 2021

Vous pouvez configurer l'appliance Citrix ADC pour diriger les demandes vers un serveur virtuel de sauvegarde lorsque le serveur virtuel d'équilibrage de charge principal est en panne ou n'est pas disponible. Le serveur virtuel de sauvegarde est un proxy et est transparent pour le client. L'appliance peut également envoyer un message de notification au client concernant la panne du site.

> Remarque :
>
> Le serveur virtuel de sauvegarde continue de gérer les connexions existantes, même après la suppression ou la désactivation du serveur virtuel principal.

Vous pouvez configurer un serveur virtuel d'équilibrage de charge de sauvegarde lorsque vous le créez ou modifier les paramètres facultatifs d'un serveur virtuel existant. Vous pouvez également configurer un serveur virtuel de sauvegarde pour un serveur virtuel de sauvegarde existant, créant ainsi des

serveurs virtuels de sauvegarde en cascade. La profondeur maximale des serveurs virtuels de sauvegarde en cascade est de 10.

Si vous disposez de plusieurs serveurs virtuels qui se connectent à deux serveurs, vous avez le choix entre ce qui se passe si le serveur virtuel principal tombe en panne et revient ensuite. Le comportement par défaut consiste à ce que le serveur virtuel principal reprenne son rôle en tant que serveur principal. Toutefois, vous pouvez configurer le serveur virtuel de sauvegarde pour qu'il reste en contrôle lorsqu'il prend le relais. Par exemple, vous pouvez synchroniser les mises à jour du serveur virtuel de sauvegarde avec le serveur virtuel principal, puis forcer manuellement le serveur principal d'origine à reprendre son rôle. Dans ce cas, vous pouvez désigner le serveur virtuel de sauvegarde pour qu'il reste en contrôle lorsque le serveur virtuel principal tombe en panne, puis revient.

Vous pouvez configurer une URL de redirection sur le serveur virtuel d'équilibrage de charge principal en tant que solution de secours lorsque les serveurs virtuels principal et de sauvegarde sont DOWN ou ont atteint leur seuil de traitement des demandes. Lorsque les services liés à des serveurs virtuels sont OUT DE SERVICE, l'appliance utilise l'URL de redirection.

Remarque : si un serveur virtuel d'équilibrage de charge est configuré à la fois avec un serveur virtuel de sauvegarde et une URL de redirection, le serveur virtuel de sauvegarde a priorité sur l'URL de redirection. Une redirection n'est utilisée que lorsque les serveurs virtuels principaux et de sauvegarde sont en panne.

Pour définir un serveur virtuel de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <vServerName> -backupVserver <BackupVServerName> [-
    disablePrimaryOnDown]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -backupVserver Vserver-LB-2 -
    disablePrimaryOnDown
<!--NeedCopy-->
```

Pour définir un serveur virtuel de sauvegarde à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur **Protection**, puis sélectionnez un serveur virtuel de sauvegarde.

3. Si vous souhaitez que le serveur virtuel de sauvegarde conserve le contrôle jusqu'à ce que vous activez manuellement le serveur virtuel principal, même si le serveur virtuel principal est sauvegardé, sélectionnez **Désactiver le serveur principal en cas d'arrêt**.

> **Remarque :**à partir de Citrix ADC version 12.1 build 51.xx, l'interface graphique affiche l'état effectif de ce serveur indiquant si la sauvegarde est active ou non.
>
> L'état effectif du serveur actuel peut être l'un des éléments suivants :
>
> - **UP** — Indique que le serveur est UP
> - **DOWN** — Indique que le serveur est DOWN
> - **UP (Backup Active)** : indique que le serveur virtuel principal ou secondaire est actif et que le trafic est dirigé vers le serveur virtuel de sauvegarde.
> - **DOWN (Backup Active)** : indique que les serveurs virtuels principaux et les serveurs virtuels de sauvegarde sont en panne et que le trafic est acheminé vers le serveur virtuel de sauvegarde.
>
> Lorsque l'option **Désactiver le serveur principal lors de l'arrêt** est activée sur le serveur virtuel principal et que le serveur principal tombe en panne et est à nouveau activé, le trafic est toujours servi par le serveur virtuel de sauvegarde jusqu'à ce que le serveur virtuel principal soit réactivé explicitement. Vous pouvez utiliser la commande `enable lb vserver <vserver_name>` pour réactiver le serveur virtuel principal.

Configurer le débordement

August 20, 2021

Une configuration de débordement sur l'appliance consiste en un serveur virtuel principal configuré avec une méthode de débordement, un seuil de débordement et un serveur virtuel de sauvegarde. Les serveurs virtuels de sauvegarde peuvent également être configurés pour le débordement, créant ainsi une chaîne de serveurs virtuels de sauvegarde.

La méthode spillover spécifie la condition opérationnelle sur laquelle vous souhaitez baser votre configuration de spillover (par exemple, le nombre de connexions établies, la bande passante ou l'intégrité combinée de la batterie de serveurs). Lorsqu'une nouvelle connexion arrive, l'appliance vérifie que le serveur virtuel principal est opérationnel et compare la condition opérationnelle avec le seuil de débordement configuré. Si le seuil est atteint, la fonction de débordement détourne les nouvelles connexions vers le premier serveur virtuel disponible dans la chaîne de sauvegarde. Le serveur virtuel de sauvegarde gère les connexions qu'il reçoit jusqu'à ce que la charge sur le principal tombe en dessous du seuil.

Si vous configurez la persistance de débordement, le serveur virtuel de sauvegarde continue à traiter

les connexions qu'il a reçues, même après que la charge sur le principal tombe en dessous du seuil. Si vous configurez la persistance des retombées et un délai d'expiration de la persistance des retombées, le serveur virtuel de sauvegarde traite uniquement les connexions pendant la période spécifiée après que la charge sur le principal tombe en dessous du seuil.

Remarque : Généralement, le débordement est déclenché si la valeur associée à la méthode de débordement dépasse le seuil (par exemple, le nombre de connexions). Toutefois, avec la méthode de spillover server-health, le débordement est déclenché si l'intégrité de la batterie de serveurs tombe en dessous du seuil.

Vous pouvez configurer le débordement de l'une des manières suivantes :

- Spécifiez une méthode de débordement prédéfinie. Quatre méthodes prédéfinies sont disponibles et répondent aux exigences courantes de débordement.
- Configurez le débordement basé sur une stratégie. Dans le spillover basé sur une stratégie, vous utilisez une règle Citrix ADC pour spécifier les conditions de débordement. Les règles Citrix ADC vous offrent la flexibilité nécessaire pour configurer le débordement pour diverses conditions opérationnelles.

Utilisez le spillover basé sur des stratégies si une méthode prédéfinie ne répond pas à vos besoins. Si vous configurez les deux pour un serveur virtuel principal, la configuration de spillover basée sur la stratégie a priorité sur la méthode prédéfinie.

Tout d'abord, vous créez le serveur virtuel principal et les serveurs virtuels dont vous avez besoin pour la chaîne de sauvegarde. Vous configurez la chaîne de sauvegarde en spécifiant un serveur virtuel comme sauvegarde pour le principal (c'est-à-dire que vous créez un serveur virtuel secondaire), un serveur virtuel comme sauvegarde pour le secondaire (c'est-à-dire que vous créez un serveur virtuel tertiaire), etc. Ensuite, vous configurez le spillover en spécifiant une méthode de spillover prédéfinie ou en créant et en liant des stratégies de spillover.

Pour obtenir des instructions sur l'attribution d'un serveur virtuel comme sauvegarde pour un autre serveur virtuel, reportez-vous à la section Configuration d'un serveur virtuel d'équilibrage de charge de sauvegarde.

Configurer une méthode de débordement prédéfinie

Les méthodes de débordement prédéfinies répondent à certaines des exigences les plus courantes. Pour utiliser l'une des méthodes de spillover prédéfinies, vous configurez les paramètres de spillover sur le serveur virtuel principal. Pour créer une chaîne de serveurs virtuels de sauvegarde, vous configurez également les paramètres de débordement sur les serveurs virtuels de sauvegarde.

Si les serveurs virtuels de sauvegarde atteignent leurs propres valeurs de seuil et que le type de service est TCP, l'appliance Citrix ADC envoie aux clients une réinitialisation TCP. Pour les types de service HTTP, SSL et RTSP, il détourne les nouvelles demandes vers l'URL de redirection configurée pour le

serveur virtuel principal. Une URL de redirection ne peut être spécifiée que pour les serveurs virtuels HTTP, SSL et RTSP. Si une URL de redirection n'est pas configurée, l'appliance Citrix ADC envoie aux clients une réinitialisation TCP (si le serveur virtuel est de type TCP) ou une réponse HTTP 503 (si le serveur virtuel est de type HTTP ou SSL).

Remarque : Avec les serveurs virtuels RTSP, l'appliance Citrix ADC utilise uniquement des connexions de données pour le débordement. Si le serveur virtuel RTSP de sauvegarde n'est pas disponible, les demandes sont redirigées vers une URL RTSP et un message de redirection RTSP est envoyé au client.

Pour configurer une méthode de débordement prédéfinie pour un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 set lb vserver <vServerName> -soMethod <spillOverType> -soThreshold <
     positiveInteger> -soPersistence ENABLED -soPersistenceTimeout <
     positiveInteger>
2 <!--NeedCopy-->
```

Exemple

```
1 set lb vserver Vserver-LB-1 -soMethod Connection -soThreshold 1000 -
     soPersistence enabled -soPersistenceTimeout 2
2 <!--NeedCopy-->
```

Pour configurer une méthode de débordement prédéfinie pour un serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur **Protection**, puis définissez les paramètres de débordement.

Configurer le débordement basé sur une stratégie

Les stratégies de débordement, basées sur des règles (expressions), vous permettent de configurer l'appliance pour un plus grand nombre de scénarios de débordement. Par exemple, vous pouvez configurer des retombées en fonction du temps de réponse du serveur virtuel ou en fonction du nombre de connexions dans la file d'attente de surtension du serveur virtuel.

Pour configurer le débordement basé sur une stratégie, commencez par créer une action de débordement. Vous sélectionnez ensuite l'expression que vous souhaitez utiliser dans la stratégie de spillover, configurez la stratégie et associez l'action à celle-ci. Enfin, vous liez la stratégie de débordement à un serveur virtuel d'équilibrage de charge, de commutation de contenu ou d'équilibrage de charge de serveur global. Vous pouvez lier plusieurs stratégies de débordement à un serveur virtuel, avec des numéros de priorité. L'appliance évalue les stratégies de débordement par ordre croissant des numéros de priorité et exécute l'action associée à la dernière stratégie pour évaluer la valeur TRUE.

Un serveur virtuel peut également avoir une action de sauvegarde. L'action de sauvegarde est effectuée si le serveur virtuel ne dispose pas d'un ou plusieurs serveurs virtuels de sauvegarde, ou si tous les serveurs virtuels de sauvegarde sont en panne, désactivés ou ont atteint leurs propres limites de débordement.

Lorsqu'une stratégie de débordement entraîne une condition UNDEF (exception levée lorsque le résultat de l'évaluation de la stratégie n'est pas défini), une action UNDEF est exécutée. L'action UNDEF est toujours ACCEPT. Vous ne pouvez pas spécifier une action UNDEF de votre choix.

Configuration d'une action de débordement

Une action de débordement est effectuée lorsque la stratégie de débordement à laquelle elle est associée est évaluée à TRUE. Actuellement, SPILLOVER est la seule action de débordement prise en charge.

Pour configurer le débordement basé sur une stratégie à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une stratégie de débordement et vérifier la configuration :

```
add spillover action <name> -action SPILLOVER

show spillover action <name>
<!--NeedCopy-->
```

Exemple

```
add spillover action mySoAction -action SPILLOVER
Done
<!--NeedCopy-->
```

```
show spillover action mySoAction
1) Name: mySoAction Action: SPILLOVER
Done
```



```
<!--NeedCopy-->
```

Sélection d'une expression pour la stratégie de débordement

Dans l'expression de stratégie, vous pouvez utiliser n'importe quelle expression basée sur un serveur virtuel qui renvoie une valeur booléenne. Par exemple, vous pouvez utiliser l'une des expressions suivantes :

```
SYS.VSERVER("vserver").RESPTIME.GT(<int>)
SYS.VSERVER("vserver").STATE.EQ( " <string> " ), and
SYS.VSERVER("vserver").THROUGHPUT.LT    (<int>)
<!--NeedCopy-->
```

Outre les fonctions existantes telles que RESPTIME, STATE et THROUGHPUT, vous pouvez utiliser les fonctions serveur virtuel suivantes qui ont été introduites avec cette fonctionnalité :

`Averagesurgecount`

Renvoie le nombre moyen de requêtes dans les files d'attente de surtension des services actifs. Renvoie 0 (zéro) s'il n'y a pas de services actifs. Lance une condition UNDEF si elle est utilisée avec un serveur virtuel de commutation de contenu ou d'équilibrage de charge de serveur global.

`Activeservices`

Renvoie le nombre de services actifs. Lance une condition UNDEF si elle est utilisée avec un serveur virtuel de commutation de contenu ou d'équilibrage de charge de serveur global.

`Activetransactions`

Renvoie la valeur du compteur de niveau serveur virtuel pour les transactions actives en cours.

is_dynamic_limit_reached

Renvoie une valeur booléenne TRUE si le nombre de connexions que le serveur virtuel gère est égal au seuil calculé dynamiquement. Le seuil dynamique est la somme des paramètres client maximum (clients max) des services liés qui sont UP.

Vous pouvez utiliser une expression de stratégie pour implémenter l'une des méthodes de spillover prédéfinies. Le tableau suivant mappe les méthodes de spillover prédéfinies aux expressions que vous pouvez utiliser pour les implémenter :

Tableau 1. Conversion de méthodes de débordement prédéfinies en expressions de stratégie

Méthode de débordement prédéfinie	Expression correspondante
CONNECTION	SYS.VSERVER(“<vserver-name>”).CONNECTIONS, utilisé avec la fonction arithmétique GT(int).
BANDWIDTH	SYS.VSERVER(“<vserver-name>”).THROUGHPUT, utilisé avec la fonction arithmétique GT(int).
HEALTH	SYS.VSERVER(“<vserver-name>”).HEALTH, utilisé avec la fonction arithmétique LT(int).
DYNAMICCONNECTION	SYS.VSERVER (»<vserver-name>«) .IS_DYNAMIC_LIMIT_READED **Remarque** : Si vous implémentez un débordement basé sur des stratégies à l’aide de la fonction IS_DYNAMIC_LIMIT_READED, vous devez également configurer la méthode DYNAMICCONNECTION prédéfinie pour le serveur virtuel, de sorte que les statistiques nécessaires au débordement fonctionnent. sont collectés.

Configuration d’une stratégie de débordement

Une stratégie de débordement utilise une expression booléenne comme règle pour spécifier les conditions qui doivent être remplies pour que le débordement se produise.

Pour configurer une stratégie de débordement à l’aide de l’interface de ligne de commande

À l’invite de commandes, tapez les commandes suivantes pour configurer une stratégie de débordement et vérifier la configuration :

```
1 add spillover policy <name> -rule <expression> -action <string> [-
      comment <string>]
2
3 show spillover policy <name>
4 <!--NeedCopy-->
```

Exemple


```
> add spillover policy mySoPolicy -rule SYS.VSERVER("v1").RESPTIME.GT
    (50) -action mySoAction -comment "Triggers spillover when the
    vserver's response time is greater than 50 ms."
Done

> show spillover policy mySoPolicy

1)  Name: mySoPolicy Rule: "SYS.VSERVER("v1").RESPTIME.GT(50)" Action:
    mySoAction Hits: 0 ActivePolicy: 0
Comment: "Triggers spillover when the vserver's response time is
    greater than 50 ms."
Done
>
<!--NeedCopy-->
```

Liaison d'une stratégie de débordement à un serveur virtuel

Vous pouvez lier une stratégie de débordement à des serveurs virtuels d'équilibrage de charge, de commutation de contenu ou d'équilibrage de charge de serveur global). Vous pouvez lier plusieurs stratégies à un serveur virtuel, avec des expressions Goto contrôlant le flux d'évaluation.

Pour lier une stratégie de débordement à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une stratégie de débordement à un serveur virtuel d'équilibrage de charge, de commutation de contenu ou d'équilibrage de charge de serveur global et vérifiez la configuration :

```
bind (lb | cs | gslb) vserver <name> -policyName <string> -priority <
    positive_integer> [-gotoPriorityExpression <expression>]

show (lb | cs | gslb) vserver <name>
<!--NeedCopy-->
```

Exemple

```
> bind lb vserver vserver1 -policyName mySoPolicy -priority 5
Done
> show lb vserver vserver1
vserver1 (2.2.2.12:80) - HTTP Type: ADDRESS
. . .
```



```
6
7  1)  Spillover Policy Name: mySoPolicy Priority: 5
8  GotoPriority Expression: END
9  Flowtype: REQUEST
10 Done
11 >
12 <!--NeedCopy-->
```

Configuration d'une action de sauvegarde pour un événement de débordement

Une action de sauvegarde spécifie ce qu'il faut faire lorsque le seuil de débordement est atteint, mais qu'un ou plusieurs serveurs virtuels de sauvegarde ne sont pas configurés ou sont en panne, désactivés ou ont atteint leurs propres seuils.

Remarque : Pour les méthodes de débordement prédéfinies configurées directement sur le serveur virtuel (en tant que valeurs du paramètre Méthode de débordement), l'action de sauvegarde n'est pas configurable. Par défaut, l'appliance envoie aux clients une réinitialisation TCP (si le serveur virtuel est de type TCP) ou une réponse HTTP 503 (si le serveur virtuel est de type HTTP ou SSL).

L'action de sauvegarde est configurée sur le serveur virtuel. Vous pouvez configurer le serveur virtuel pour qu'il accepte les demandes (une fois que le seuil spécifié par la stratégie est atteint), rediriger les clients vers une URL ou simplement supprimer les demandes avant même d'établir des connexions TCP ou SSL jusqu'à ce que le nombre de demandes tombe en dessous du seuil. Par conséquent, des ressources de mémoire moins importantes sont utilisées lorsque les connexions sont réinitialisées avant même d'allouer des structures de données.

Pour configurer une action de sauvegarde pour le débordement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une action de sauvegarde et vérifier la configuration :

```
1 set lb vserver <name> -soBackupAction <soBackupAction>
2
3 show lb vserver <name>
4 <!--NeedCopy-->
```

Exemple :

```
1 set lb vserver vs1 -soBackupAction REDIRECT -redirectURL `http://www.
     mysite.com/maintenance`
2 Done
3 > show lb vserver vs1
```



```
vs1 (10.102.29.76:80) - HTTP Type: ADDRESS
State: UP
. . .
Redirect URL: `http://www.mysite.com/maintenance`
. . .
Done
<!--NeedCopy-->
```

Pour configurer une action de sauvegarde pour le débordement à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur **Protection**, puis spécifiez une action de sauvegarde de débordement.

Basculement de connexion

August 20, 2021

Le basculement de connexion permet d'éviter la perturbation de l'accès aux applications déployées dans un environnement distribué. Dans une configuration de Citrix ADC High Availability (HA), le *basculement* de *connexion (ou mise en miroir* de connexion *-CM*) fait référence au maintien actif d'une connexion TCP ou UDP établie lorsqu'un basculement se produit. La nouvelle appliance Citrix ADC principale contient des informations sur les connexions établies avant le basculement et continue de servir ces connexions. Après le basculement, le client reste connecté au même serveur physique. La nouvelle appliance principale synchronise les informations avec la nouvelle appliance secondaire. Si le paramètre L2Conn est défini, les paramètres de connexion de couche 2 sont également synchronisés avec le paramètre secondaire.

> Remarque :
>
> Pensez à une configuration HA, dans laquelle un client établit une session avec le nœud principal, qui à son tour établit une session avec le serveur principal. Lorsqu'un basculement est déclenché dans cet état, les paquets reçus sur un nouveau nœud principal à partir du client et des nœuds serveur existants sont traités comme des paquets défectueux, et les connexions client et serveur sont réinitialisées. Si le basculement de connexion sans état est activé (USIP est activé), après le basculement, les connexions ne sont pas réinitialisées lorsque vous recevez des

> paquets provenant de nœuds client ou serveur. Au lieu de cela, les connexions client et serveur sont créées dynamiquement.

Vous pouvez configurer le basculement de connexion en mode stateless ou stateful. En mode de basculement de connexion sans état, les nœuds HA n'échangent aucune information sur les connexions qui ont échoué. Cette méthode n'a pas de surcharge d'exécution.

En mode de basculement de connexion avec état, l'appliance principale synchronise les données des connexions avec basculement avec la nouvelle appliance secondaire.

Le basculement de connexion est utile si votre déploiement dispose de connexions durables. Par exemple, si vous téléchargez un fichier volumineux sur FTP et qu'un basculement se produit pendant le téléchargement, la connexion se rompt et le téléchargement est interrompu. Toutefois, si vous configurez le basculement de connexion en mode avec état, le téléchargement se poursuit même après le basculement.

Fonctionnement du basculement de connexion sur les appliances Citrix ADC

Dans un basculement de connexion sans état, la nouvelle appliance principale tente de recréer le flux de paquets en fonction des informations contenues dans les paquets qu'elle reçoit.

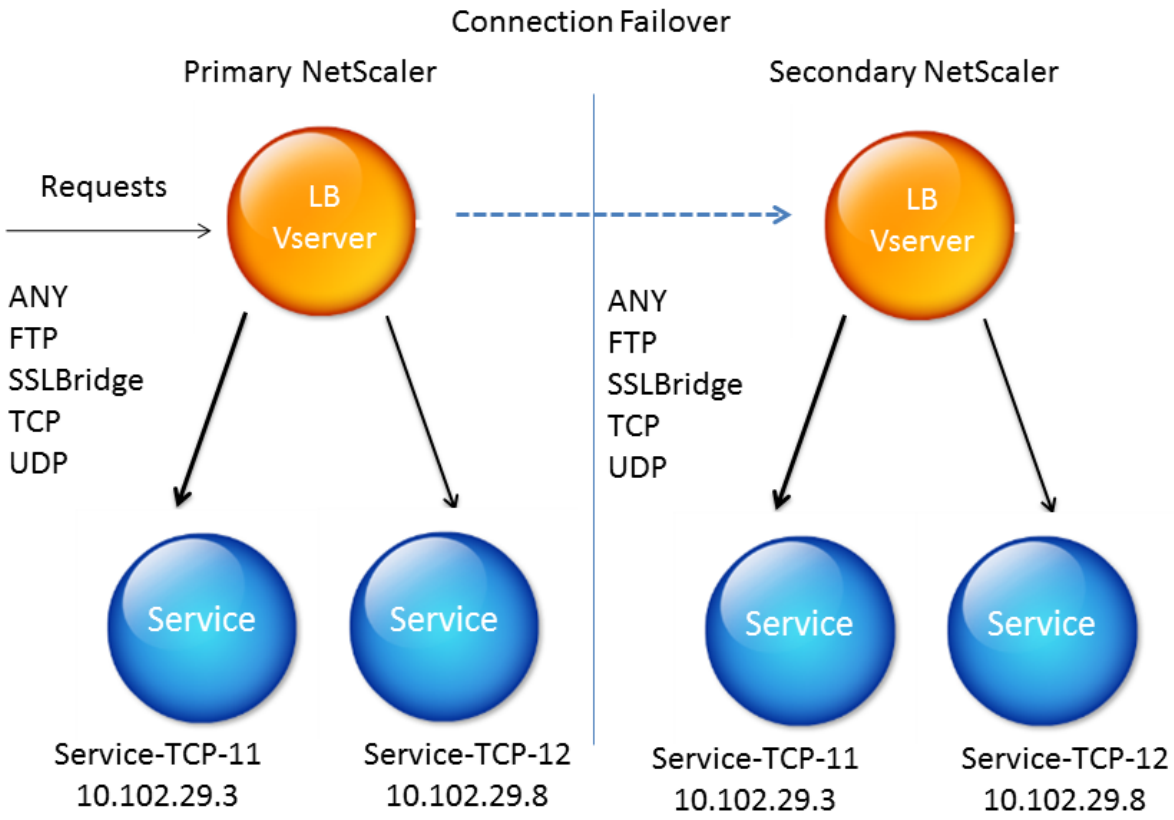
En cas de basculement sur incident avec état, pour gérer les informations actuelles sur les connexions mises en miroir, l'appliance principale envoie des messages à l'appliance secondaire. L'appliance secondaire conserve les données relatives aux paquets mais les utilise uniquement en cas de basculement sur incident. En cas de basculement sur incident, la nouvelle appliance principale (ancienne solution secondaire) commence à utiliser les données stockées sur les connexions en miroir et à accepter le trafic. Pendant la période de transition, le client et le serveur peuvent rencontrer une brève interruption et retransmissions.

Remarque :

Vérifiez que l'appliance principale est en mesure de s'autoriser sur l'appliance secondaire. Pour vérifier la configuration correcte des mots de passe, utilisez la `rpcnode` commande show depuis la ligne de commande ou utilisez l'option RPC du menu **Réseau** de l'interface graphique.

Une configuration HA de base avec basculement de connexion contient les entités illustrées dans la figure suivante.

Figure 1. Diagramme d'entité de basculement de connexion



Remarque

Le basculement de connexion n'est pas pris en charge après l'un des événements suivants :

```
1 - An upgrade to a later release.
2 - An upgrade to a later build within the same release, if the new
      build uses a different HA version.
```

Configuration prise en charge

Le basculement de connexion peut être configuré uniquement sur des serveurs virtuels d'équilibrage de charge. Il ne peut pas être configuré sur des serveurs virtuels de commutation de contenu. Si vous activez le basculement de connexion sur des serveurs virtuels d'équilibrage de charge connectés à un serveur virtuel de commutation de contenu, le basculement de connexion ne fonctionne pas car les serveurs virtuels d'équilibrage de charge n'acceptent pas initialement le trafic.

Le tableau suivant décrit le programme d'installation pris en charge pour le basculement de connexion.

Tableau 1. Basculement de connexion - Installation prise en charge

Paramètre	Sans état	Avec état
Type de service	ANY.	ANY, UDP, TCP, FTP, SSL_BRIDGE.
Méthodes d'équilibrage de charge	Toutes les méthodes prises en charge pour le type de service ANY. Toutefois, si la persistance IP source n'est pas définie, la méthode SRCIPSRCPORTHASH doit être utilisée.	Toutes les méthodes applicables aux types de service pris en charge.
Types de persistance	Persistance SOURCEIP.	Tous les types applicables aux types de service pris en charge sont pris en charge.
USIP	Doit être ON.	Aucune restriction. Peut être ON ou OFF.
Fixations de service	Le service peut être lié à un seul serveur virtuel.	Le service peut être lié à un ou plusieurs serveurs virtuels.
Versions de protocole Internet (IP)	IPv4 et IPv6	IPV4 et IPv6
Prise en charge de la redondance	Clustering et haute disponibilité	Haute disponibilité

> Remarque :
>
> Le basculement de connexion avec état n'est pris en charge que pour les services de commutation basés sur la connexion, par exemple TCP. Étant donné que HTTP utilise la commutation basée sur les requêtes, il ne prend pas en charge le basculement de connexion. Dans SSL, les connexions existantes sont réinitialisées après le basculement.

Fonctionnalités affectées par le basculement de connexion

Le tableau suivant répertorie les fonctionnalités affectées si le basculement de connexion est configuré.

Tableau 2. Comment le basculement de connexion affecte les fonctionnalités de Citrix ADC

Fonctionnalité	Impact du basculement de connexion
Protection SYN	Pour n'importe quelle connexion, si un basculement survient après la sortie de SYN-ACK par l'appliance, mais avant qu'elle ne reçoive l'ACK final, la connexion n'est pas prise en charge par le basculement de connexion. Le client doit réémettre la demande pour établir la connexion.
Protection contre les surtensions	Si le basculement se produit avant l'établissement d'une connexion avec le serveur, le nouveau dispositif principal tente d'établir la connexion avec le serveur. Il retransmet également tous les paquets détenus pendant la protection contre les surtensions.
Access down	Si cette option est activée, la fonctionnalité d'accès est prioritaire sur le basculement de connexion.
Pare-feu d'application	La fonctionnalité de pare-feu d'application n'est pas prise en charge.
INC	La configuration réseau indépendante n'est pas prise en charge en mode haute disponibilité.
TCP mise en mémoire tampon	La mise en mémoire tampon TCP n'est pas compatible avec la mise en miroir de connexion.
Clôture de la réponse	Après basculement, les NATPCB peuvent ne pas être fermés lors de la réponse.

Pour configurer le basculement de connexion à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**. Ouvrez le serveur virtuel et, dans **Paramètres avancés**, cliquez sur **Protection**, puis sélectionnez **Basculement de connexion**en tant qu' **état**.

Pour configurer le basculement de connexion à l'aide de l'interface de ligne de commande

À l'invite de commandes :

```
set lb vserver <vServerName> -connFailover <Value>
show lb vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -connFailover stateful
Done
<!--NeedCopy-->
```

Lorsque le basculement de connexion est désactivé sur un serveur virtuel, les ressources allouées au serveur virtuel sont libérées.

Pour désactiver le basculement de connexion à l'aide de l'interface de ligne de commande

À l'invite de commandes :

```
set lb vserver <vServerName> -connFailover <Value>
show lb vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -connFailover disable
Done
<!--NeedCopy-->
```

Pour désactiver le basculement de connexion à l'aide de l'interface graphique

Accédez à **Gestion du trafic**> **Équilibrage de charge**> **Serveurs virtuels**. Ouvrez le serveur virtuel, dans **Protection**, sélectionnez **Basculement de connexion en**tant que désactivé.

Vider la file d'attente de surtension

August 20, 2021

Lorsqu'un serveur physique reçoit un sursaut de demandes, il devient lent à répondre aux clients qui lui sont actuellement connectés, ce qui laisse les utilisateurs insatisfaits et mécontents. Souvent, la

surcharge provoque également les clients à recevoir des pages d'erreur. L'appliance Citrix ADC fournit des fonctionnalités telles que la protection contre les surtensions, qui contrôle la vitesse à laquelle de nouvelles connexions à un service peuvent être établies et évite ainsi les surcharges.

L'appliance effectue le multiplexage des connexions entre les clients et les serveurs physiques. Lorsqu'elle reçoit une demande client pour accéder à un service sur un serveur, l'appliance recherche une connexion déjà établie au serveur qui est libre. S'il trouve une connexion libre, il utilise cette connexion pour établir un lien virtuel entre le client et le serveur. S'il ne trouve pas de connexion libre existante, l'appliance établit une nouvelle connexion avec le serveur et établit un lien virtuel entre le client et le serveur. Toutefois, si l'appliance ne peut pas établir de nouvelle connexion avec le serveur, elle envoie la demande client à une file d'attente de surtension. Si tous les serveurs physiques liés au serveur virtuel d'équilibrage de charge ou de commutation de contenu atteignent la limite supérieure des connexions client (valeur maximale du client, seuil de protection contre les surtensions ou capacité maximale du service), l'appliance ne peut pas établir de connexion avec un serveur. La fonction de protection contre les surtensions utilise la file d'attente pour réguler la vitesse d'ouverture des connexions avec les serveurs physiques. L'appliance gère une file d'attente de surtension différente pour chaque service lié au serveur virtuel.

La longueur d'une file d'attente de surtension augmente chaque fois qu'une demande survient pour laquelle l'appliance ne peut pas établir de connexion. La longueur d'une file d'attente de surtension diminue dans l'une des conditions suivantes :

- Une demande dans la file d'attente est envoyée au serveur.
- Une demande est dépassée et est supprimée de la file d'attente.

Si la file d'attente de surtension d'un service ou d'un groupe de services devient trop longue, vous pouvez la vider. Vous pouvez vider la file d'attente de surtension d'un service ou d'un groupe de services spécifique, ou de tous les services et groupes de services liés à un serveur virtuel d'équilibrage de charge. Le vidange d'une file d'attente de surtension n'affecte pas les connexions existantes. Seules les requêtes présentes dans la file d'attente de surtension sont supprimées. Pour ces demandes, le client doit faire une nouvelle demande.

Vous pouvez également vider la file d'attente de surtension d'un serveur virtuel de commutation de contenu. Si un serveur virtuel de commutation de contenu transfère certaines requêtes à un serveur virtuel d'équilibrage de charge particulier, et que le serveur virtuel d'équilibrage de charge reçoit également d'autres demandes, lorsque vous videz la file d'attente de surtension du serveur virtuel de commutation de contenu, seules les demandes reçues de ce changement de contenu serveur virtuel sont vidé. Les autres requêtes de la file d'attente de surtension du serveur virtuel d'équilibrage de charge ne sont pas vidées.

Remarque : Vous ne pouvez pas vider les files d'attente de redirection de cache, d'authentification, de VPN ou de serveurs virtuels GSLB ou de services GSLB.

Remarque : N'utilisez pas la fonction de protection contre les surtensions si l'option Use Source IP

(USIP) est activée.

Pour vider une file d'attente de surtension à l'aide de l'interface de ligne de commande

La commande flush ns surgeQ fonctionne de la manière suivante :

- Vous pouvez spécifier le nom d'un service, d'un groupe de services ou d'un serveur virtuel dont la file d'attente de surtension doit être vidé.
- Si vous spécifiez un nom lors de l'exécution de la commande, la file d'attente de surtension de l'entité spécifiée est vidé. Si plusieurs entités portent le même nom, l'appliance vide les files d'attente de surtension de toutes ces entités.
- Si vous spécifiez le nom d'un groupe de services, ainsi qu'un nom de serveur et un port lors de l'exécution de la commande, l'appliance vide la file d'attente de surtension du membre du groupe de services spécifié uniquement.
- Vous ne pouvez pas spécifier directement un membre du groupe de services (<serverName> et <port>) sans spécifier le nom du groupe de services (<name>) et vous ne pouvez pas spécifier <port> sans un <serverName>. Spécifiez le <serverName> et <port> si vous souhaitez vider la file d'attente de surtension pour un membre du groupe de services spécifique.
- Si vous exécutez la commande sans spécifier de nom, l'appliance vide les files d'attente de surtension de toutes les entités présentes sur l'appliance.
- Si un membre du groupe de services est identifié par un nom de serveur, vous devez spécifier le nom du serveur dans cette commande ; vous ne pouvez pas spécifier son adresse IP.

À l'invite de commandes, tapez :

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]
<!--NeedCopy-->
```

Exemples

```
flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80
<!--NeedCopy-->
```

La commande précédente vide la file d'attente de surtension du service ou du serveur virtuel appelé SVC1ANZGB et dont l'adresse IP est 10.10.10.

```
flush ns surgeQ
<!--NeedCopy-->
```

La commande précédente vide toutes les files d'attente de surtension de l'appliance.

Pour vider une file d'attente de surtension à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels**, sélectionnez un serveur virtuel et, dans la liste Action, sélectionnez **Vider la file d'attente de surtension**.

Gestion d'une configuration d'équilibrage de charge

August 20, 2021

Une configuration d'équilibrage de charge existante ne nécessite pas beaucoup de travail à maintenir tant qu'elle est inchangée, mais la plupart ne restent pas inchangées longtemps. L'augmentation de la charge nécessite de nouveaux serveurs équilibrés de charge et, éventuellement, de nouvelles appliances Citrix ADC, qui doivent être configurées et ajoutées à l'installation existante. Les anciens serveurs s'usent et doivent être remplacés, ce qui nécessite la suppression de certains serveurs et l'ajout d'autres. Les mises à niveau de votre équipement réseau ou les modifications apportées à la topologie peuvent également nécessiter des modifications de votre configuration d'équilibrage de charge. Par conséquent, vous devez effectuer des opérations sur des objets serveur, des services et des serveurs virtuels. Le Visualizer peut afficher votre configuration graphiquement et vous pouvez effectuer des opérations sur les entités de l'affichage. Vous pouvez également profiter d'autres fonctionnalités qui facilitent la gestion du trafic via votre configuration d'équilibrage de charge.

Gérer les objets serveur

August 20, 2021

Lors de la configuration de base de l'équilibrage de charge, lorsque vous créez un service, un objet serveur avec l'adresse IP du service est créé, s'il n'en existe pas. Si vous préférez les objets de service nommés avec des noms de domaine plutôt que des adresses IP, vous pouvez également avoir créé manuellement un ou plusieurs objets serveur. Vous pouvez activer, désactiver ou supprimer n'importe quel objet serveur.

Lorsque vous activez ou désactivez un objet serveur, vous activez ou désactivez tous les services associés à l'objet serveur. Lorsque vous actualisez l'appliance Citrix ADC après la désactivation d'un objet serveur, l'état de son service apparaît comme OUT OF SERVICE. Si vous spécifiez un temps d'attente lors de la désactivation d'un objet serveur, l'objet serveur continue de gérer les connexions établies pendant la durée spécifiée, mais rejette les nouvelles connexions. Si vous supprimez un objet serveur, le service auquel il est lié est également supprimé.

Pour activer un serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
enable server <name>
<!--NeedCopy-->
```

Exemple :

```
enable server 10.102.29.5
<!--NeedCopy-->
```

Pour activer ou désactiver un objet serveur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs**.
2. Sélectionnez le serveur et, dans la liste Action, sélectionnez **Activer** ou **Désactiver**.

Pour désactiver un objet serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
disable server <name> <delay>
<!--NeedCopy-->
```

Exemple :

```
disable server 10.102.29.5 30
<!--NeedCopy-->
```

Pour supprimer un objet serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm server <name>
<!--NeedCopy-->
```

Exemple :

```
rm server 10.102.29.5
<!--NeedCopy-->
```


Pour supprimer un objet serveur à l'aide de l'interface graphique graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs**.
2. Sélectionnez un serveur, puis cliquez sur **Supprimer**.

Gérer les services

January 21, 2021

Les services sont activés par défaut lorsque vous les créez. Vous pouvez désactiver ou activer chaque service individuellement. Lors de la désactivation d'un service, vous spécifiez normalement un temps d'attente pendant lequel le service continue à gérer les connexions établies, mais en rejette les nouvelles, avant de s'arrêter. Si vous ne spécifiez pas de temps d'attente, le service s'arrête immédiatement. Pendant le temps d'attente, l'état du service est OUT DE SERVICE.

Vous pouvez supprimer un service lorsqu'il n'est plus utilisé. Lorsque vous supprimez un service, il est indépendant de son serveur virtuel et supprimé de la configuration de Citrix ADC.

Pour activer ou désactiver un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
enable service <name>

disable service <name> <DelayInSeconds>
<!--NeedCopy-->
```

Exemples :

```
enable service Service-HTTP-1
disable service Service-HTTP-1 30
<!--NeedCopy-->
```

Pour activer ou désactiver un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Ouvrez un service et, dans la liste **Action**, sélectionnez **Activer** ou **Désactiver** .

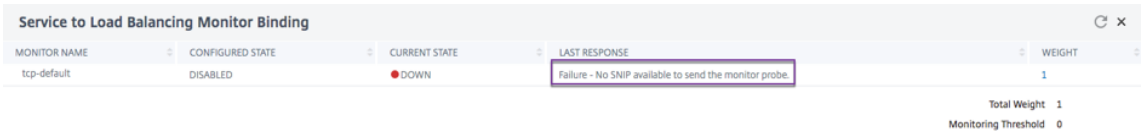
Identifier la cause de l'état de service marqué comme DOWN à l'aide de l'interface graphique

À partir de Citrix ADC version 13.0 build 41.20, vous pouvez afficher les informations de la sonde du moniteur sur l'interface graphique pour les services qui sont DOWN sans accéder à l'interface de liaison du moniteur. Vous pouvez cliquer sur la valeur de la colonne **État du serveur** de la page Services. Vous pouvez cliquer sur **DOWN** pour identifier la cause principale à cause de laquelle le service est marqué comme DOWN.

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Cliquez sur **DOWN** dans la colonne **État du serveur** correspondant au service DOWN.

La page Liaison du moniteur d'équilibrage de charge s'affiche.

La colonne **Dernière réponse** affiche le motif pour lequel le service est marqué comme DOWN.



Gérer un serveur virtuel d'équilibrage de charge

August 20, 2021

Les serveurs virtuels sont activés par défaut lorsque vous les créez. Vous pouvez désactiver et activer manuellement les serveurs virtuels. Si vous désactivez un serveur virtuel, l'état du service virtuel apparaît comme OUT DU SERVICE. Lorsque cela se produit, le serveur virtuel met fin à toutes les connexions, soit immédiatement, soit après avoir autorisé les connexions existantes à se terminer, en fonction du paramètre DownStateFlush. Si DownStateFlush est ENABLED (valeur par défaut), toutes les connexions sont vidé. En cas de désactivation, le serveur virtuel continue de servir les demandes sur les connexions existantes.

Vous supprimez un serveur virtuel uniquement lorsque vous n'avez plus besoin du serveur virtuel. Avant de le supprimer, vous devez en dissocier tous les services.

Pour activer ou désactiver un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
enable lb vserver <name>
<!--NeedCopy-->
```

```
disable lb vserver <name>
<!--NeedCopy-->
```

Exemples :

```
enable lb vserver Vserver-LB-1
disable lb vserver Vserver-LB-1
<!--NeedCopy-->
```

Pour activer ou désactiver un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel et, dans la liste **Action**, sélectionnez **Activer** ou **Désactiver** .

Pour dissocier un service d'un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
unbind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

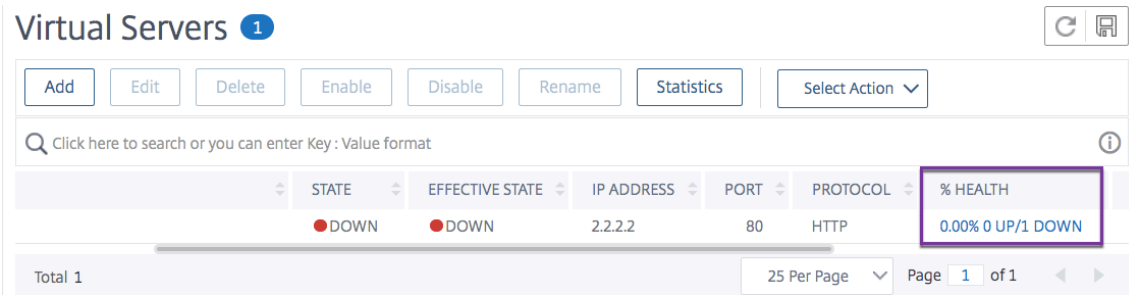
Pour dissocier un service d'un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel, puis cliquez dans la section **Services** .
3. Sélectionnez un service et cliquez sur **Unlier**.

Identifier la cause de l'état du serveur virtuel marqué comme DOWN à l'aide de l'interface graphique

À partir de Citrix ADC version 13.0 build 41.20, vous pouvez afficher les informations de la sonde de moniteur sur l'interface graphique des serveurs virtuels en panne sans accéder à l'interface de liaison du moniteur. La valeur de la colonne **% HEALTH** de la page Serveur virtuel est cliquable. Vous pouvez cliquer sur la valeur dans la colonne **% HEALTH** pour identifier la cause principale à cause de laquelle le serveur virtuel est marqué comme DOWN.

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur la valeur dans la colonne **% HEALTH** correspondant au serveur virtuel en panne.

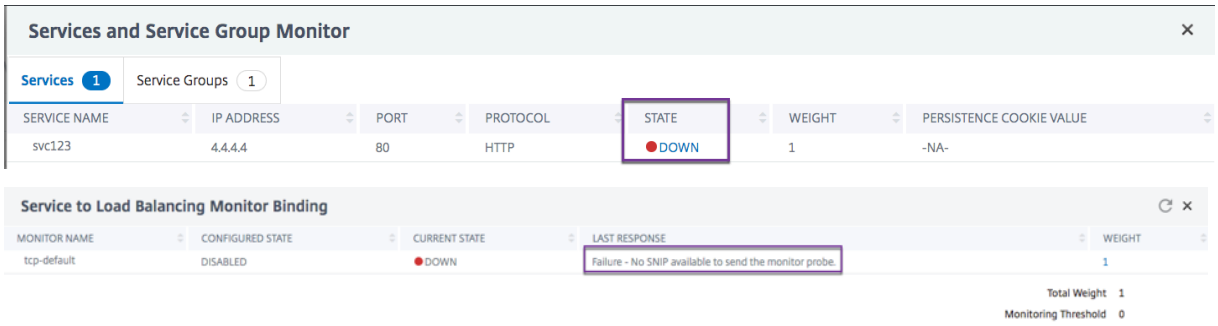


La page Surveillance des services et des groupes de services s'affiche. Les services et groupes de services liés à ce serveur virtuel sont affichés dans les onglets respectifs.

Si vous utilisez des services liés à l'équilibrage de charge virtuel, effectuez les opérations suivantes :

Dans l'onglet **Services**, cliquez sur **DOWN** correspondant au service qui est en panne.

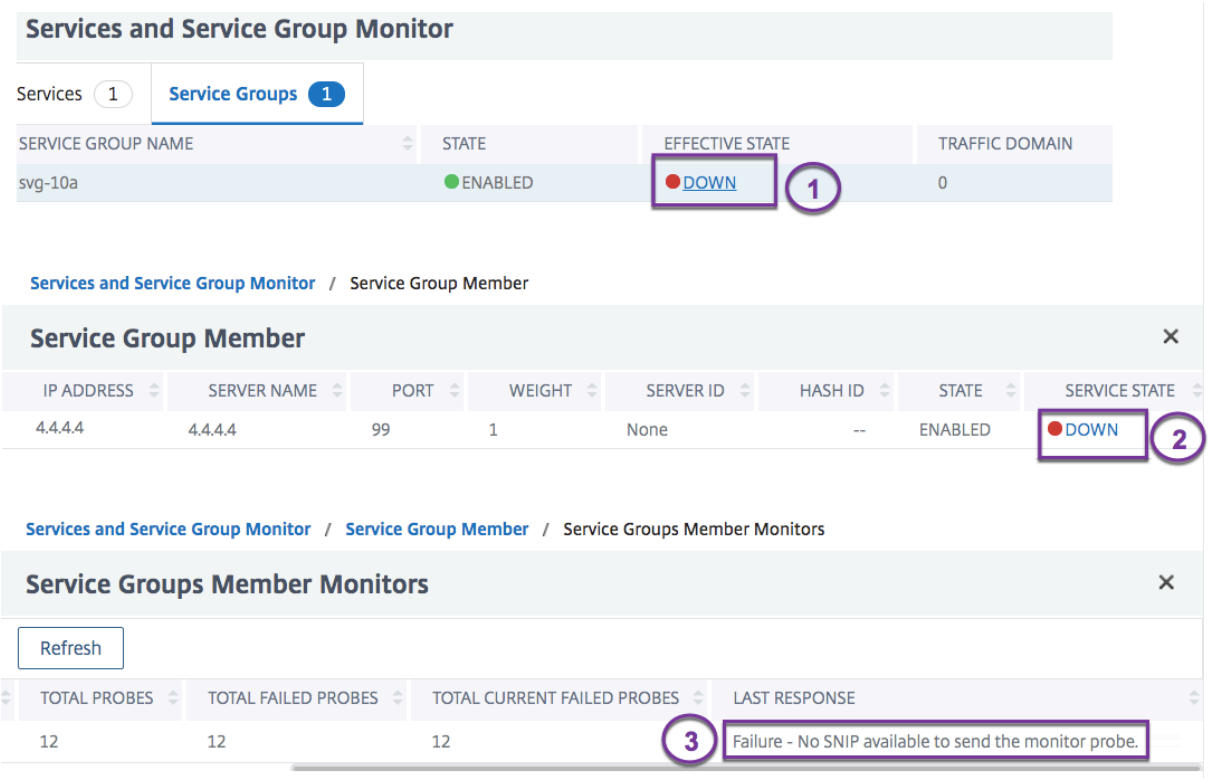
La colonne **Dernière réponse** de la page Liaison du moniteur Service à équilibrage de charge affiche la raison pour laquelle le serveur virtuel est marqué comme DOWN.



Si vous utilisez des groupes de services liés à l'équilibrage de charge virtuel, effectuez les opérations suivantes :

Dans l'onglet **Groupes de services**, cliquez sur **DOWN** dans la page Surveillance des services et des groupes de services, puis cliquez sur **DOWN** dans la page Membre du groupe de services.

La colonne **Dernière réponse** de la page Service Groups Member Monitors affiche la raison pour laquelle le serveur virtuel est marqué comme DOWN.



Visualiseur d'équilibrage de charge

August 20, 2021

Le visualiseur d'équilibrage de charge est un outil que vous pouvez utiliser pour afficher et modifier la configuration d'équilibrage de charge dans un format graphique. Voici un exemple de l'affichage Visualizer.

Figure 1. Affichage du visualiseur d'équilibrage de charge

Vous pouvez utiliser le visualiseur pour afficher les éléments suivants :

- Services et groupes de services liés à un serveur virtuel.
- Les moniteurs liés à chaque service.
- Stratégies liées au serveur virtuel.
- Les étiquettes de stratégie, si elles sont configurées.
- Détails de configuration de tout élément affiché.

Vous pouvez également utiliser le visualiseur pour ajouter et lier de nouveaux objets, modifier des objets existants et activer ou désactiver des objets. La plupart des éléments de configuration affichés

dans Visualizer apparaissent sous les mêmes noms que dans d'autres parties de l'utilitaire de configuration. Toutefois, contrairement au reste de l'utilitaire de configuration, Visualizer regroupe les services qui ont les mêmes détails de configuration et surveillent les liaisons dans une entité appelée conteneur de service.

Un conteneur de service est un ensemble de services et de groupes de services similaires liés à un seul serveur virtuel d'équilibrage de charge. Les services du conteneur ont les mêmes propriétés, à l'exception du nom, de l'adresse IP et du port, et leurs liaisons de moniteur doivent avoir le même poids et l'état de liaison. Lorsque vous liez un nouveau service à un serveur virtuel, il est placé dans un conteneur existant si ses liaisons de configuration et de surveillance correspondent à celles d'autres services. Sinon, il est placé dans son propre conteneur.

Les procédures suivantes fournissent uniquement les étapes de base de l'utilisation du visualiseur. Étant donné que le Visualizer duplique des fonctionnalités dans d'autres zones de la fonction d'équilibrage de charge, d'autres méthodes d'affichage ou de configuration de tous les paramètres pouvant être configurés dans le Visualizer sont fournies dans la documentation d'équilibrage de charge.

Remarque : Le Visualizer nécessite une interface graphique, de sorte qu'il n'est disponible que via l'utilitaire de configuration.

Pour afficher les propriétés du serveur virtuel d'équilibrage de charge à l'aide du Visualizer

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel que vous souhaitez afficher, puis cliquez sur **Visualiseur**.

Pour afficher les détails de configuration des services, des groupes de services et des moniteurs à l'aide du Visualizer

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel que vous souhaitez afficher, puis cliquez sur **Visualiseur**.
3. Dans la boîte de dialogue Load Balancing Visualizer, double-cliquez sur l'entité pour afficher les détails de configuration de l'entité liée à ce serveur virtuel, vous pouvez effectuer les opérations suivantes :

Pour afficher les détails de configuration des stratégies et des étiquettes de stratégie à l'aide du Visualizer dans l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

2. Dans le volet d'informations, sélectionnez le serveur virtuel que vous souhaitez afficher, puis cliquez sur Visualiseur.
3. Dans la boîte de dialogue Visualiseur d'équilibrage de charge, double-cliquez sur l'entité de stratégies pour afficher les stratégies liées à ce serveur virtuel.

Pour modifier une ressource dans une configuration d'équilibrage de charge à l'aide du Visualizer

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel à configurer, puis cliquez sur Visualizer.
3. Dans la boîte de dialogue Load Balancing Visualizer, sur l'image Visualizer, double-cliquez sur la ressource à modifier.

Pour ajouter une configuration d'équilibrage de charge à l'aide du Visualizer

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel à configurer, puis cliquez sur Visualizer.
3. Dans la boîte de dialogue Load Balancing Visualizer, cliquez sur **+** pour ajouter la ressource.

Gérer le trafic client

October 5, 2021

La gestion correcte des connexions client permet de garantir que vos applications restent disponibles pour les utilisateurs, même lorsque votre appliance Citrix ADC subit des charges élevées. Diverses fonctions d'équilibrage de charge et autres fonctionnalités disponibles sur l'appliance peuvent être intégrées dans une configuration d'équilibrage de charge pour traiter la charge plus efficacement, la détourner si nécessaire et hiérarchiser les tâches que l'appliance doit effectuer :

- **Équilibrage de charge sans session.** Vous pouvez configurer des serveurs virtuels d'équilibrage de charge sans session et effectuer l'équilibrage de charge sans créer de sessions dans des configurations utilisant DSR ou des systèmes de détection d'intrusion (IDS).
- **Mise en cache intégrée.** Vous pouvez rediriger les requêtes HTTP vers un cache.
- **Nettoyage retardé.** Vous pouvez configurer le nettoyage différé des connexions de serveur virtuel pour empêcher le processus de nettoyage d'utiliser les cycles du processeur pendant les périodes où l'appliance Citrix ADC subit des charges élevées.

- **Réécriture.** Vous pouvez utiliser la fonction de réécriture pour modifier le port et le protocole lors de la redirection HTTP, ou insérer l'adresse IP et le port du serveur virtuel dans un en-tête de demande personnalisé.
- **RTSP NAT.**
- **Surveillance basée sur les tarifs.** Vous pouvez activer la surveillance basée sur le débit pour détourner le trafic excédentaire.
- **Paramètres de la couche 2.** Vous pouvez configurer un serveur virtuel pour qu'il utilise les paramètres L2 pour identifier une connexion.
- **Réponse ICMP**. Vous pouvez configurer l'appliance pour qu'elle envoie des réponses ICMP aux demandes PING en fonction de vos paramètres. Sur l'adresse IP correspondant au serveur virtuel, définissez la RÉPONSE ICMP sur VSVR_CNTRLD et, sur le serveur virtuel, définissez le `ICMP VSERVER RESPONSE`.

  Les paramètres suivants peuvent être définis sur un serveur virtuel :
  - Lorsque vous définissez `ICMP VSERVER RESPONSE` la valeur PASSIVE sur tous les serveurs virtuels, l'appliance répond toujours.
  - Lorsque vous définissez `ICMP VSERVER RESPONSE` la valeur ACTIVE sur tous les serveurs virtuels, l'appliance répond même si un serveur virtuel est activé.
  - Lorsque vous définissez `ICMP VSERVER RESPONSE` la valeur ACTIVE sur certains et PASSIVE sur d'autres, l'appliance répond même si un serveur virtuel défini sur ACTIVE est activé.

Configurer des serveurs virtuels d'équilibrage de charge sans session

August 20, 2021

Lorsque l'appliance Citrix ADC effectue l'équilibrage de charge, elle crée et gère des sessions entre les clients et les serveurs. La maintenance des informations de session entraîne une charge importante sur les ressources de l'appliance, et les sessions peuvent ne pas être nécessaires dans des scénarios tels que la configuration de DSR (Direct Server Return) et l'équilibrage de charge des systèmes de détection d'intrusion (IDS). Pour éviter de créer des sessions lorsqu'elles ne sont pas nécessaires, vous pouvez configurer un serveur virtuel sur l'appliance pour l'équilibrage de charge sans session. En équilibrage de charge sans session, l'appliance effectue l'équilibrage de charge par paquet.

L'équilibrage de charge sans session peut fonctionner en mode de transfert basé sur Mac ou en mode de transfert basé sur IP.

Pour le transfert basé sur Mac, l'adresse IP du serveur virtuel sans session doit être spécifiée sur tous les serveurs physiques vers lesquels le trafic est transféré.

Pour le transfert basé sur IP dans l'équilibrage de charge sans session, l'adresse IP et le port du serveur virtuel n'ont pas besoin d'être spécifiés sur les serveurs physiques, car ces informations sont

incluses dans les paquets transférés. Lors du transfert d'un paquet du client vers le serveur physique, l'appliance laisse inchangés les détails du client, tels que l'adresse IP et le port, et ajoute l'adresse IP et le port de la destination.

Configuration prise en charge

L'équilibrage de charge sans session Citrix ADC prend en charge les types de service et les méthodes d'équilibrage de charge suivants :

Types de services

- N'importe quel pour la redirection basée sur Mac
- ANY, DNS et UDP pour la redirection IP

Méthodes d'équilibrage de charge

- Round Robin
- Moins de bande passante
- LRTM (méthode du temps de réponse le plus faible)
- Hash IP source
- Hash IP de destination
- Hash IP de destination IP source
- Hachage du port source IP source
- Chargement personnalisé

Limitations

L'équilibrage de charge sans session présente les limitations suivantes :

- L'appliance doit être déployée en mode à deux bras.
- Un service doit être lié à un seul serveur virtuel.
- L'équilibrage de charge sans session n'est pas pris en charge pour les groupes de services.
- L'équilibrage de charge sans session n'est pas pris en charge pour les services basés sur le domaine (services DBS).
- L'équilibrage de charge sans session en mode IP n'est pas pris en charge pour un serveur virtuel configuré en tant que sauvegarde sur un serveur virtuel principal.
- Vous ne pouvez pas activer le mode de débordement.
- Pour tous les services liés à un serveur virtuel d'équilibrage de charge sans session, l'option Use Source IP (USIP) doit être activée.
- Pour un serveur ou un service virtuel générique, l'adresse IP de destination n'est pas modifiée.

Remarque :

- Lors de la configuration d'un serveur virtuel pour l'équilibrage de charge sans session, spécifiez explicitement une méthode d'équilibrage de charge prise en charge. La méthode par défaut, la connexion minimale, ne peut pas être utilisée pour l'équilibrage de charge sans session.
- Pour configurer l'équilibrage de charge sans session en mode de redirection basé sur Mac sur un serveur virtuel, l'option de transfert basé sur Mac doit être activée sur l'appliance Citrix ADC.

Pour ajouter un serveur virtuel sans session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un serveur virtuel sans session et vérifier la configuration :

```
1 add lb vserver <name>@ <serviceType> <IPAddress>@ <port> -m <
     redirectionMode> -sessionless <(ENABLED|DISABLED)> -lbMethod <
     load_balancing_method>
2
3 show lb vserver <name>
4 <!--NeedCopy-->
```

Exemple :

```
1  add lb vserver sesslessv1 any 11.11.12.123 54 -sessionless ENABLED -
      lbMethod roundrobin -m ip
2       Done
3  show lb vserver sesslessv1
4       sesslessv1 (11.11.12.123:54) - ANY Type: ADDRESS
5       State: DOWN
6       ...
7       Effective State: DOWN
8       Client Idle Timeout: 120 sec
9       Down state flush: ENABLED
10      ...
11      Persistence: NONE
12      Sessionless LB: ENABLED
13      Connection Failover: DISABLED
14      L2Conn: OFF
15      1) Policy : cmp_text Priority:8680 Inherited
16      2) Policy : cmp_nocmp_ie60 Priority:8690 Inherited
17 <!--NeedCopy-->
```


Pour configurer l'équilibrage de charge sans session sur un serveur virtuel existant

À l'invite de commandes, tapez :

```
set lb vserver <name>@ -m <redirectionMode> -sessionless <(ENABLED|
   DISABLED)> -lbMethod <load_balancing_method>
<!--NeedCopy-->
```

Exemple

```
set lb vserver sesslessv1 -m mac -sessionless ENABLED -lbmethod lrtm
  Done
<!--NeedCopy-->
```

> **Remarque**
>
> Pour un service lié à un serveur virtuel sur lequel l' `-m MAC` option est activée, vous devez lier un moniteur non utilisateur.

Pour configurer un serveur virtuel sans session à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez le serveur virtuel, puis dans Paramètres avancés, cliquez sur Paramètres de trafic, puis sélectionnez Équilibrage de charge sans session.

Rediriger les requêtes HTTP vers un cache

August 20, 2021

La fonctionnalité de redirection de cache Citrix ADC redirige les requêtes HTTP vers un cache. Vous pouvez réduire considérablement l'impact de la réponse aux demandes HTTP et améliorer les performances de votre site Web grâce à la mise en œuvre correcte de la fonctionnalité de redirection du cache.

Un cache stocke le contenu HTTP fréquemment demandé. Lorsque vous configurez la redirection du cache sur un serveur virtuel, l'appliance Citrix ADC envoie des requêtes HTTP pouvant être mises en cache au cache, et des requêtes HTTP non mises en cache au serveur Web d'origine.

Pour configurer la redirection du cache sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set lb vserver <name> -cacheable <Value>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -cacheable yes
<!--NeedCopy-->
```

Pour configurer la redirection du cache sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur Paramètres de trafic, puis sélectionnez Cacheable.

Activer le nettoyage des connexions au serveur virtuel

August 20, 2021

Sous certaines conditions, vous pouvez configurer le paramètre DownStateFlush pour mettre fin immédiatement aux connexions existantes lorsqu'un service ou un serveur virtuel est marqué « DOWN ». La fin des connexions existantes libère des ressources et, dans certains cas, accélère la récupération des configurations d'équilibrage de charge surchargées.

L'état d'un serveur virtuel dépend des états des services qui lui sont liés. L'état de chaque service dépend des réponses des serveurs équilibrés de charge aux sondes et aux vérifications d'intégrité envoyées par les moniteurs liés à ce service. Parfois, les serveurs équilibrés de charge ne répondent pas. Si un serveur est lent ou occupé, les sondes de surveillance peuvent s'écouler. Si les sondes de surveillance répétées ne sont pas répondues dans le délai d'expiration configuré, le service est marqué DOWN.

Un serveur virtuel est marqué comme DOWN uniquement lorsque tous les services qui lui sont liés sont marqués comme DOWN. Lorsqu'un serveur virtuel est en panne, il met fin à toutes les connexions, soit immédiatement, soit après avoir autorisé les connexions existantes à se terminer.

N'activez pas le paramètre DownStateFlush sur les serveurs d'applications qui doivent terminer leurs transactions. Vous pouvez activer ce paramètre sur les serveurs Web dont les connexions peuvent être interrompues en toute sécurité lorsqu'ils sont marqués comme DOWN.

Le tableau suivant résume l'effet de ce paramètre sur un exemple de configuration constitué d'un serveur virtuel, vServer-LB-1, avec un service qui lui est lié, Service-TCP-1. Dans le tableau, E et D

indiquent l'état du paramètre downStateFlush : E signifie Activé et D signifie Désactivé.

Vserver-LB-1	Service-TCP-1	État des connexions
E	E	Les connexions client et serveur sont toutes deux terminées.
E	D	Pour certains types de services, tels que TCP, pour lesquels l'appliance Citrix ADC ne prend pas en charge la réutilisation des connexions, les connexions client et serveur sont toutes deux interrompues. Pour les types de services, tels que HTTP, pour lesquels l'appliance prend en charge la réutilisation des connexions, les connexions client et serveur ne sont interrompues que si une transaction est active sur ces connexions. Si une transaction n'est pas active, seules les connexions client sont interrompues.

Vserver-LB-1	Service-TCP-1	État des connexions
D	E	Pour certains types de services, tels que TCP, pour lesquels l'appliance Citrix ADC ne prend pas en charge la réutilisation des connexions, les connexions client et serveur sont toutes deux interrompues. Pour les types de services, tels que HTTP, pour lesquels l'appliance prend en charge la réutilisation des connexions, les connexions client et serveur ne sont interrompues que si une transaction est active sur ces connexions. Si une transaction n'est pas active, seules les connexions serveur sont interrompues.
D	D	Ni les connexions client ni serveur ne sont interrompues.

Si vous souhaitez désactiver un service uniquement lorsque toutes les connexions établies sont fermées par le serveur ou le client, vous pouvez utiliser l'option d'arrêt gracieux. Pour plus d'informations sur l'arrêt gracieux d'un service, voir Arrêt gracieux des services.

Pour configurer le paramètre de vidage d'état en panne sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -downStateFlush <Value>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -downStateFlush enabled
```



```
<!--NeedCopy-->
```

Pour configurer le paramètre de vidage d'état en panne sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur Paramètres de trafic, puis sélectionnez Déclenchement de l'état.

Réécriture des ports et des protocoles pour la redirection HTTP

August 20, 2021

Les serveurs virtuels et les services qui y sont liés peuvent utiliser différents ports. Lorsqu'un service répond à une connexion HTTP avec une redirection, vous devrez peut-être configurer l'appliance Citrix ADC pour modifier le port et le protocole pour vous assurer que la redirection se déroule correctement. Pour ce faire, activez et configurez le paramètre redirectPortRewrite.

Ce paramètre affecte uniquement le trafic HTTP et HTTPS. Si ce paramètre est activé sur un serveur virtuel, le serveur virtuel réécrit le port lors des redirections, en remplaçant le port utilisé par le service par le port utilisé par le serveur virtuel.

Si le serveur virtuel ou le service est de type SSL, vous devez activer la redirection SSL sur le serveur virtuel ou le service. Si le serveur virtuel et le service sont tous les deux de type SSL, activez la redirection SSL sur le serveur virtuel.

Le paramètre redirectPortRewrite peut être utilisé dans les scénarios suivants :

- Le serveur virtuel est de type HTTP et les services sont de type SSL.
- Le serveur virtuel est de type SSL et les services sont de type HTTP.
- Le serveur virtuel est de type HTTP et les services sont de type HTTP.
- Le serveur virtuel est de type SSL et les services sont de type SSL.

Scénario 1 : Le serveur virtuel est de type HTTP et les services sont de type SSL. La redirection SSL, et éventuellement la réécriture de port, est activée sur le service. Si la réécriture du port est activée, le port des URL HTTPS est réécrit. Les URL HTTP du serveur sont envoyées telles qu'elles sont au client.

Seule la redirection SSL est activée. Le serveur virtuel peut être configuré sur n'importe quel port. Voir le tableau suivant :

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirection SSL et la réécriture de port sont activées. Le serveur virtuel est configuré sur le port 80. Voir le tableau suivant :

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com/

La redirection SSL et la réécriture de port sont activées. Le serveur virtuel est configuré sur le port 8080. Voir le tableau suivant :

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	http://domain.com:8080/
https://domain.com:444/	http://domain.com:8080/

Scénario 2 : Le serveur virtuel est de type SSL et les services sont de type HTTP. Si la réécriture de port est activée, seul le port des URL HTTP est réécrit. Les URL HTTPS du serveur sont envoyées telles qu'elles au client.

La redirection SSL est activée sur le serveur virtuel. Le serveur virtuel peut être configuré sur n'importe quel port. Voir le tableau suivant.

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com/	https://domain.com/
http://domain.com:8080/	https://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirection SSL et la réécriture de port sont activées sur le serveur virtuel. Le serveur virtuel est configuré sur le port 443. Voir le tableau suivant :

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com/	https://domain.com/
http://domain.com:8080/	https://domain.com/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirection SSL et la réécriture de port sont activées. Le serveur virtuel est configuré sur le port 444. Voir le tableau suivant :

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com/	https://domain.com:444/
http://domain.com:8080/	https://domain.com:444/
https://domain.com/	https://domain.com/
https://domain.com:445/	https://domain.com:445/

Scénario 3 : Le serveur virtuel et le service sont de type HTTP. La réécriture de port doit être activée sur le serveur virtuel. Seul le port des URL HTTP est réécrit. Les URL HTTPS du serveur sont envoyées telles qu'elles au client.

Le serveur virtuel est configuré sur le port 80. Voir le tableau suivant :

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com/	http://domain.com/

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com:8080/	http://domain.com/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

Le serveur virtuel est configuré sur le port 8080. Voir le tableau suivant :

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com/	http://domain.com:8080/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:445/	https://domain.com:445/

Scénario 4 : Le serveur virtuel et le service sont de type SSL. Si la réécriture de port est activée, seul le port des URL HTTPS est réécrit. Les URL HTTP du serveur sont envoyées telles qu'elles sont au client.

La redirection SSL est activée sur le serveur virtuel. Le serveur virtuel peut être configuré sur n'importe quel port. Voir le tableau suivant :

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirection SSL et la réécriture de port sont activées sur le serveur virtuel. Le serveur virtuel est configuré sur le port 443. Voir le tableau suivant :

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
https://domain.com:444/	https://domain.com/

La redirection SSL et la réécriture de port sont activées sur le serveur virtuel. Le serveur virtuel est configuré sur le port 444. Voir le tableau suivant :

Rediriger l'URL à partir du serveur	Rediriger l'URL envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com:444/
https://domain.com:445/	https://domain.com:444/

Pour configurer la redirection HTTP sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -redirectPortRewrite (ENABLED | DISABLED)
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -redirectPortRewrite enabled
<!--NeedCopy-->
```

Pour configurer la redirection HTTP sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez le serveur virtuel et, dans le volet Paramètres avancés, cliquez sur Paramètres de trafic, puis sélectionnez Réécrire.

Pour configurer la redirection SSL sur un serveur virtuel ou un service SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set ssl vserver <vServerName> - sslRedirect (ENABLED | DISABLED)

set ssl service <serviceName> - sslRedirect (ENABLED | DISABLED)
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver Vserver-SSL-1 -sslRedirect enabled

set ssl service service-SSL-1 -sslRedirect enabled
<!--NeedCopy-->
```

Pour configurer la redirection SSL et la réécriture du port SSL sur un serveur virtuel ou un service SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur Paramètres SSL, puis sélectionnez Redirection SSL.

Insérer l'adresse IP et le port d'un serveur virtuel dans l'en-tête de requête

August 20, 2021

Si plusieurs serveurs virtuels communiquent avec différentes applications sur le même service, vous devez effectuer les opérations suivantes :

Configurez l'appliance Citrix ADC pour ajouter l'adresse IP et le numéro de port du serveur virtuel approprié aux requêtes HTTP envoyées à ce service. Ce paramètre permet aux applications exécutées sur le service d'identifier le serveur virtuel qui a envoyé la demande.

Si le serveur virtuel principal est en panne et que le serveur virtuel de sauvegarde est en service, les paramètres de configuration du serveur virtuel de sauvegarde sont ajoutés aux demandes du client. Si vous souhaitez ajouter la même balise d'en-tête, que les demandes proviennent du serveur virtuel principal ou du serveur virtuel de sauvegarde, vous devez configurer la balise d'en-tête requise sur les deux serveurs virtuels.

Remarque : cette option n'est pas prise en charge pour les serveurs virtuels génériques ou les serveurs virtuels factices.

Pour insérer l'adresse IP et le port du serveur virtuel dans les demandes du client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -insertVserverIPPort <insertVserverIPPort> [<
   vipHeader>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -insertVserverIPPort VipAddr
<!--NeedCopy-->
```

Pour insérer l'adresse IP et le port du serveur virtuel dans les demandes du client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez le serveur virtuel et, dans le volet Paramètres avancés, cliquez sur Paramètres de **trafic**, puis sélectionnez Insertion de port IP Virtual Server et spécifiez un en-tête de port IP du serveur virtuel.

Utiliser une adresse IP source spécifiée pour la communication back-end

August 20, 2021

Pour la communication avec les serveurs physiques ou d'autres périphériques homologues, l'appliance Citrix ADC utilise une adresse IP qui lui appartient comme adresse IP source. L'appliance Citrix ADC gère un pool d'adresses IP et sélectionne dynamiquement une adresse IP lors de la connexion à un serveur. En fonction du sous-réseau dans lequel le serveur physique est placé, l'appliance décide de l'adresse IP à utiliser. Ce pool d'adresses est utilisé pour envoyer du trafic et surveiller les sondes.

Dans de nombreux cas, vous pouvez souhaiter que l'appliance utilise une adresse IP spécifique ou n'importe quelle adresse IP provenant d'un ensemble spécifique d'adresses IP pour les communications back-end. Voici quelques exemples :

- Un serveur peut distinguer les sondes de surveillance du trafic si l'adresse IP source utilisée pour les sondes de surveillance appartient à un ensemble spécifique.

- Pour améliorer la sécurité du serveur, un serveur peut être configuré pour répondre à des demandes provenant d'un ensemble spécifique d'adresses IP ou, parfois, d'une seule adresse IP spécifique. Dans ce cas, l'appliance peut utiliser uniquement les adresses IP acceptées par le serveur comme adresse IP source.
- L'appliance peut gérer efficacement ses connexions internes si elle peut distribuer ses adresses IP dans des ensembles d'adresses IP et utiliser une adresse d'un ensemble uniquement pour se connecter à un service spécifique.

Pour configurer l'appliance pour qu'elle utilise une adresse IP source spécifiée, créez des profils réseau (profils réseau) et configurez les entités de l'appliance pour qu'elles utilisent le profil. Un profil réseau peut être lié à des serveurs virtuels d'équilibrage de charge ou de commutation de contenu, aux serveurs virtuels Citrix Gateway VPN, aux services, aux groupes de services ou aux moniteurs. Un profil réseau possède des adresses IP appartenant à Citrix ADC (SNIP et VIP) qui peuvent être utilisées comme adresse IP source. Il peut s'agir d'une seule adresse IP ou d'un ensemble d'adresses IP, appelé ensemble d'adresses IP. Si un profil réseau possède un jeu d'adresses IP, l'appliance sélectionne dynamiquement une adresse IP dans le jeu d'adresses IP au moment de la connexion. Si un profil possède une seule adresse IP, la même adresse IP est utilisée comme adresse IP source.

Si un profil réseau est lié à un serveur virtuel d'équilibrage de charge ou de commutation de contenu, le profil est utilisé pour envoyer du trafic à tous les services qui lui sont liés. Si un profil réseau est lié à un groupe de services, l'appliance utilise le profil pour tous les membres du groupe de services. Si un profil réseau est lié à un moniteur, l'appliance utilise le profil pour toutes les sondes envoyées à partir du moniteur.

Remarque :

- Lorsqu'une appliance Citrix ADC utilise une adresse VIP pour communiquer avec un serveur, elle utilise des entrées de session pour déterminer si le trafic destiné à l'adresse VIP est une réponse d'un serveur ou une demande d'un client.
- Vous pouvez lier un profil réseau à des serveurs virtuels Citrix Gateway VPN. Toutefois, vous devez noter certains points lorsque vous liez un profil net. Pour plus d'informations, voir Points à noter lors de la liaison d'un profil réseau à un serveur virtuel VPN.

Utilisation d'un profil net pour l'envoi de trafic

Si l'option Utiliser l'adresse IP source (USIP) est activée, l'appliance utilise l'adresse IP du client et ignore tous les profils réseau. Si l'option USIP n'est pas activée, l'appliance sélectionne l'adresse IP source de la manière suivante :

- S'il n'y a pas de profil net sur le serveur virtuel ou le groupe de services/services, l'appliance utilise la méthode par défaut.
- S'il existe un profil net uniquement sur le groupe de services/services, l'appliance utilise ce profil net.

- S'il existe un profil net uniquement sur le serveur virtuel, l'appliance utilise le profil net.
- S'il existe un profil net à la fois sur le serveur virtuel et le groupe de services/services, l'appliance utilise le profil net lié au groupe de services/services.

Utilisation d'un profil réseau pour l'envoi de sondes de moniteur :

Pour les sondes de moniteur, l'appliance sélectionne l'adresse IP source de la manière suivante :

- Si un profil réseau est lié au moniteur, l'appliance utilise le profil réseau du moniteur. Il ignore les profils réseau liés au serveur virtuel ou au groupe de services/services.
- S'il n'y a pas de profil net lié au moniteur,
  - S'il existe un profil net sur le groupe de services/services, l'appliance utilise le profil net du groupe de services/services.
  - S'il n'y a pas de profil net même sur le groupe de services/services, l'appliance utilise la méthode par défaut de sélection d'une adresse IP source.

Note : S'il n'y a pas de profil net lié à un service, l'appliance recherche un profil net sur le groupe de services si le service est lié à un groupe de services.

Pour utiliser une adresse IP source spécifiée pour la communication, procédez comme suit :

1. Créez des jeux d'adresses IP à partir du pool de SNIP et de VIP appartenant à l'appliance Citrix ADC. Un jeu d'adresses IP peut être constitué à la fois d'adresses SNIP et VIP. Pour obtenir des instructions, voir Création de jeux d'adresses IP.
2. Créez des profils réseau. Pour obtenir des instructions, reportez-vous à la section Création d'un profil réseau.
3. Liez les profils réseau aux entités de l'appliance. Pour obtenir des instructions, reportez-vous à la section Liaison d'un profil Net à une entité Citrix ADC.

> **Remarque :**
>
> - Un profil réseau ne peut avoir que les adresses IP spécifiées en tant que SNIP et VIP sur l'appliance Citrix ADC.
> - La persistance IP source n'est pas respectée pour les paquets initiés par Citrix ADC.

Gérer les profils réseau

Un profil réseau (ou profil réseau) contient une adresse IP ou un jeu d'adresses IP. Lors de la communication avec des serveurs physiques ou des homologues, l'appliance Citrix ADC utilise les adresses spécifiées dans le profil comme adresse IP source.

- Pour obtenir des instructions sur la création d'un profil réseau, reportez-vous à la section Création d'un profil réseau.
- Pour obtenir des instructions sur la liaison d'un profil réseau à une entité Citrix ADC, reportez-vous à la section Liaison d'un profil réseau à une entité Citrix ADC.

Créer un jeu d'adresses IP

Un ensemble d'adresses IP est un ensemble d'adresses IP configurées sur l'appliance Citrix ADC en tant qu'adresses IP de sous-réseau (SNIP) ou adresses IP virtuelles (VIP). Un ensemble d'adresses IP est identifié avec un nom significatif qui aide à identifier l'utilisation des adresses IP qu'il contient. Pour créer un ensemble d'adresses IP, ajoutez un ensemble d'adresses IP et liez des adresses IP appartenant à Citrix ADC. Les adresses SNIP et VIP peuvent être présentes dans le même ensemble d'adresses IP.

Pour créer un jeu d'adresses IP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
add ipset <name>

bind ipset <name> <IPAddress>
<!--NeedCopy-->
```

Ou

```
bind ipset <name> <IPAddress>

show ipset [<name>]
<!--NeedCopy-->
```

La commande précédente affiche les noms de tous les ensembles d'adresses IP de l'appliance si vous ne transmettez aucun nom. Il affiche les adresses IP liées au jeu d'adresses IP spécifié si vous transmettez un nom.

Exemples

```
1.
> add ipset skpnwipset
 Done
> bind ipset skpnwipset 21.21.20.1
 Done

2.
 > add ipset testnwipset
 Done
> bind ipset testnwipset 21.21.21.[21-25]
 IPAddress "21.21.21.21" bound
 IPAddress "21.21.21.22" bound
 IPAddress "21.21.21.23" bound
 IPAddress "21.21.21.24" bound
```



```
 IPAddress "21.21.21.25" bound
 Done

3.
 > bind ipset skpipset 11.11.11.101
 ERROR: Invalid IP address
[This IP address could not be added because this is not an IP address
   owned by the Citrix ADC appliance]
 > add ns ip 11.11.11.101 255.255.255.0 -type SNIP
 ip "11.11.11.101" added
 Done
 > bind ipset skpipset 11.11.11.101
 IPAddress "11.11.11.101" bound
 Done
4.
> sh ipset
1) Name: ipset-1
2) Name: ipset-2
3) Name: ipset-3
4) Name: skpnewipset
 Done

5.
> sh ipset skpnewipset
IP:21.21.21.21
IP:21.21.21.22
IP:21.21.21.23
IP:21.21.21.24
IP:21.21.21.25
 Done
<!--NeedCopy-->
```

Pour créer un jeu d'adresses IP à l'aide de l'interface graphique

Accédez à **Système > Réseau > Jeux d'adresses IP**et créez un jeu d'adresses IP.

Créer un profil net

Un profil réseau (profil réseau) consiste en une ou plusieurs adresses SNIP ou VIP de l'appliance Citrix ADC.

Pour créer un profil réseau à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add netprofile <name> [-srcIp <srcIpVal>]
<!--NeedCopy-->
```

Si le srcIpVal n'est pas fourni dans cette commande, il peut être fourni ultérieurement à l'aide de la commande `set netprofile`.

Exemples

```
add netprofile skpnetprofile1 -srcIp 21.21.20.1
Done

add netprofile baksnp -srcIp bakipset
Done

set netprofile yahnp -srcIp 12.12.23.1
Done

set netprofile citkbnp -srcIp citkbipset
Done
<!--NeedCopy-->
```

Lier un profil net à une entité Citrix ADC

Un profil réseau peut être lié à un serveur virtuel d'équilibrage de charge, un service, un groupe de services ou un moniteur.

Remarque : Vous pouvez lier un profil net au moment de la création d'une entité Citrix ADC ou le lier à une entité existante.

Pour lier un profil net à un serveur à l'aide de l'interface de ligne de commande

Vous pouvez lier un profil net pour équilibrer la charge des serveurs virtuels et des serveurs virtuels de commutation de contenu. Spécifiez le serveur virtuel approprié.

À l'invite de commandes, tapez :

```
set lb vserver <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Ou


```
set cs vserver <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Exemples

```
set lb vserver skpnwvs1 -netProfile gntnp
 Done
set cs vserver mmdcsv -netProfile mmdnp
 Done
<!--NeedCopy-->
```

Pour lier un profil réseau à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur **Profils** et définissez un profil réseau.

Pour lier un profil réseau à un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Exemple

```
set service brnssvc1 -netProfile brnsnp
 Done
<!--NeedCopy-->
```

Pour lier un profil réseau à un service à l'aide de l'interface graphique graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, cliquez sur **Profils** et définissez un profil réseau.

Pour lier un profil réseau à un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set servicegroup <serviceGroupName> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Exemple

```
set servicegroup ndhsvcgrp -netProfile ndhnp
 Done
<!--NeedCopy-->
```

Pour lier un profil réseau à un groupe de services à l'aide de l'interface graphique graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Groupes**de services et ouvrez un groupe de services.
2. Dans Paramètres avancés, cliquez sur **Profils** et définissez un profil réseau.

Pour lier un profil réseau à un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set monitor <monitor_name> -netProfile <net_profile_name>
```

Exemple

```
set monitor brnsecvmon1 -netProfile brnsmonnp
 Done
<!--NeedCopy-->
```

Pour lier un profil réseau à un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Ouvrez un moniteur et définissez le profil net.

Définir une valeur de délai d'attente pour les connexions client inactives

August 20, 2021

Vous pouvez configurer un serveur virtuel pour qu'il mette fin aux connexions client inactives après l'expiration d'un délai d'attente configuré (en secondes). Lorsque vous configurez ce paramètre,

l'appliance Citrix ADC attend le temps que vous spécifiez et, si le client est inactif après cette période, il ferme la connexion client. Par défaut, la valeur du délai d'inactivité du client est définie sur 180 secondes.

Pour définir une valeur de délai d'expiration pour les connexions client inactives à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -cltTimeout <Value>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -cltTimeout 100
<!--NeedCopy-->
```

Pour définir une valeur de délai d'expiration pour les connexions client inactives à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans **Paramètres avancés,** cliquez sur **Paramètres de trafic**, puis définissez la valeur de délai d'inactivité du client en secondes.

Gérer les connexions RTSP

August 20, 2021

L'appliance Citrix ADC peut utiliser l'une des deux topologies suivantes : le mode NAT-On ou le mode NAT-Off pour équilibrer la charge des serveurs RTSP. En mode NAT, la traduction d'adresses réseau (NAT) est activée et configurée sur l'appliance. Les demandes et les réponses RTSP transitent toutes les deux par l'appliance. Vous devez donc configurer l'appliance pour effectuer la traduction d'adresses réseau (NAT) afin d'identifier la connexion de données.

Pour plus d'informations sur l'activation et la configuration de NAT, consultez Addressage IP.

En mode NAT désactivé, NAT n'est pas activé et configuré. L'appliance reçoit les demandes RTSP du client et les achemine vers le service qu'elle sélectionne à l'aide de la méthode d'équilibrage de charge configurée. Les serveurs RTSP équilibrés envoient leurs réponses directement au client, en

contournant l'appliance. Vous devez donc configurer l'appliance pour qu'elle utilise le mode DSR (Direct Server Return) et attribuer des noms de domaine complets accessibles au public dans DNS à vos serveurs RTSP à charge équilibrée.

Pour plus d'informations sur l'activation et la configuration du mode DSR, reportez-vous à la section Configuration de l'équilibrage de charge en mode de retour direct du serveur. Pour plus d'informations sur la configuration du DNS, voir Système de noms de domaine. Dans les deux cas, lorsque vous configurez l'équilibrage de charge RTSP, vous devez également configurer RTSPnat pour qu'il corresponde à la topologie de votre configuration d'équilibrage de charge.

Pour configurer RTSP NAT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name>  -RTSPNAT <ValueOfRTSPNAT>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vserver-LB-1  -RTSPNAT ON
<!--NeedCopy-->
```

Pour configurer RTSP NAT à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et ouvrez un serveur virtuel de type RTSP.
2. Dans Paramètres avancés, cliquez sur **Paramètres de trafic**, puis sélectionnez **Natting RTSP**.

Gérer le trafic client en fonction du taux de trafic

August 20, 2021

Vous pouvez surveiller le débit de trafic qui circule à travers les serveurs virtuels d'équilibrage de charge et contrôler le comportement de l'appliance Citrix ADC en fonction du débit de trafic. Par exemple :

- Régulez le flux de trafic s'il est trop élevé.
- Les informations de cache sont basées sur le débit de trafic.
- Si le taux de trafic est trop élevé, redirigez le trafic excédentaire vers un autre serveur virtuel d'équilibrage de charge.

- Appliquez une surveillance basée sur les taux aux demandes HTTP et DNS (Domain Name System).

Pour plus d'informations sur les stratégies basées sur les taux, voir Limitation de taux.

Identifier une connexion avec les paramètres de couche 2

August 20, 2021

En règle générale, pour identifier une connexion, l'appliance Citrix ADC utilise le 4-tuple de l'adresse IP du client, du port client, de l'adresse IP de destination et du port de destination. Lorsque vous activez l'option Connexion L2, les paramètres de couche 2 de la connexion (numéro de canal, adresse MAC et ID VLAN) sont utilisés en plus du 4-tuple normal.

l'activation du paramètre L2Conn pour un serveur virtuel d'équilibrage de charge permet plusieurs connexions TCP et non-TCP avec le même 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) pour coexister sur l'appliance Citrix ADC. L'appliance utilise à la fois les paramètres 4-tuple et Layer 2 pour identifier les connexions TCP et non-TCP.

Vous pouvez activer l'option L2Conn dans les scénarios suivants :

- Plusieurs VLAN sont configurés sur l'appliance Citrix ADC et un pare-feu est configuré pour chaque VLAN.
- Vous souhaitez que le trafic provenant des serveurs d'un VLAN et lié à un serveur virtuel d'un autre VLAN passe par les pare-feu configurés pour les deux VLAN.

Par conséquent, lorsqu'une appliance nCore Citrix ADC sur laquelle le paramètre L2conn est défini pour un ou plusieurs serveurs virtuels d'équilibrage de charge est rétrogradée vers une version classique ou vers une version nCore qui ne prend pas en charge le paramètre L2conn, les configurations d'équilibrage de charge qui utilisent le paramètre L2conn deviennent inefficaces.

Pour configurer l'option de connexion L2 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb vserver <name> <serviceType> <IPAddress>@ <port> -l2Conn ON
<!--NeedCopy-->
```

Exemple

```
 add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -l2Conn ON
<!--NeedCopy-->
```


Pour configurer l'option de connexion L2 à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez Paramètres de trafic, puis Paramètres de couche 2.

Configurer l'option Préférer le routage direct

August 20, 2021

Sur un serveur virtuel d'équilibrage de charge générique si vous configurez explicitement un itinéraire vers une destination, par défaut, l'appliance Citrix ADC transfère le trafic en fonction de l'itinéraire configuré. Si vous souhaitez que l'appliance ne recherche pas l'itinéraire configuré, vous pouvez définir l'option Préférer l'itinéraire direct sur NO.

Si un périphérique est directement connecté à un dispositif Citrix ADC, celui-ci transfère directement le trafic vers le périphérique. Par exemple, si la destination d'un paquet est un pare-feu, le paquet n'a pas besoin d'être routé via un autre pare-feu. Cependant, il se peut que vous souhaitiez parfois que le trafic passe par le pare-feu même si l'appareil y est directement connecté. Dans de tels cas, vous pouvez définir l'option Préférer un itinéraire direct sur NO.

Remarque : le paramètre preferDirectRoute s'applique à tous les serveurs virtuels génériques de l'appliance Citrix ADC.

Pour définir l'option Préférer l'itinéraire direct à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb parameter -preferDirectRoute (YES | NO)
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -preferDirectRoute YES
<!--NeedCopy-->
```

Pour définir l'option Préférer l'itinéraire direct à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge**.
2. Sélectionnez Préférer un itinéraire direct.

Utiliser un port source provenant d'une plage de ports spécifiée pour la communication back-end

August 20, 2021

Par défaut, pour les configurations avec l'option USIP désactivée ou avec USIP et utiliser les options de port proxy activées, l'appliance Citrix ADC communique aux serveurs à partir d'un port source aléatoire (supérieur à 1024).

L'appliance prend en charge l'utilisation d'un port source à partir d'une plage de ports spécifiée pour communiquer avec les serveurs. L'un des cas d'utilisation de cette fonctionnalité concerne les serveurs configurés pour identifier le trafic reçu appartenant à un ensemble spécifique basé sur le port source à des fins de journalisation et de surveillance. Par exemple, identifier le trafic interne et externe à des fins de journalisation.

La configuration de l'appliance Citrix ADC pour qu'elle utilise un port source à partir d'une plage de ports pour communiquer avec les serveurs comporte les tâches suivantes :

- **Créez un profil net et définissez le paramètre de plage de ports source**. Un paramètre de plage de ports source spécifie une ou plusieurs plages de ports. L'appliance sélectionne au hasard l'un des ports libres dans les plages de ports spécifiées et l'utilise comme port source pour chaque connexion aux serveurs.
- **Liez le profil réseau à des serveurs virtuels, des services ou des groupes de services d'équilibrage de charge** : Un profil réseau avec un paramètre de plage de ports source peut être lié à un serveur virtuel, un service ou un groupe de services d'une configuration d'équilibrage de charge. Pour une connexion à un serveur virtuel, l'appliance sélectionne aléatoirement l'un des ports libres parmi les plages de ports spécifiées d'un profil réseau et utilise ce port comme port source pour se connecter à l'un des serveurs liés.

Pour spécifier une ou plusieurs plages de ports source à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind netProfile <name> (-srcPortRange <int[-int]> ...)

show netprofile <name>
<!--NeedCopy-->
```

Pour spécifier une ou plusieurs plages de ports source à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **Profils réseau**.

2. Définissez le paramètre **Plage de ports source** lors de l'ajout ou de la modification de NetProfiles.

Exemple de configuration

Dans l'exemple de configuration suivant, le profil net PARTIAL-NAT-1 a des paramètres NAT partiels et est lié à l'équilibrage de charge du serveur virtuel LBVS-1, qui est de type ANY. Pour les paquets reçus sur LBVS-1 à partir de 192.0.0.0/8, l'appliance Citrix ADC traduit le dernier octet de l'adresse IP source du paquet en 100. Par exemple, un paquet avec l'adresse IP source 192.0.2.30 reçu sur LBVS-1, l'appliance Citrix ADC convertit l'adresse IP source en 100.0.2.30 avant de lui envoyer l'un des serveurs liés.

```
```
> add netprofile CUSTOM-SRCPORT-NP-1
Done
> bind netprofile CUSTOM-SRCPRT-NP-1 -srcportrange 2000-3000

Done
> bind netprofile CUSTOM-SRCPRT-NP-1 -srcportrange 5000-6000

Done
> add lb vserver LBVS-1 ANY 203.0.113. 61 * -netprofile PARTIAL-NAT-1

Done
<!--NeedCopy--> ```
```

## Configurer la persistance IP source pour les communications back-end

August 20, 2021

Par défaut, pour une configuration d'équilibrage de charge avec l'option USIP désactivée et un profil réseau lié à un serveur virtuel ou à des services ou groupes de services, l'appliance Citrix ADC utilise l'algorithme d'arrondi pour sélectionner une adresse IP dans le profil réseau pour communiquer avec les serveurs. En raison de cette méthode de sélection, l'adresse IP sélectionnée peut être différente pour différentes sessions d'un client spécifique.

Certaines situations nécessitent que l'appliance Citrix ADC achemine tout le trafic d'un client spécifique à partir de la même adresse IP lors de l'envoi du trafic aux serveurs. Les serveurs peuvent alors, par exemple, identifier le trafic appartenant à un ensemble spécifique à des fins de journalisation et de surveillance.

 
```

L'option de persistance IP source d'un profil net permet à l'appliance Citrix ADC d'utiliser la même adresse, spécifiée dans le profil net, pour communiquer avec les serveurs sur toutes les sessions initiées depuis un client spécifique vers un serveur virtuel.

Pour activer la persistance de l'adresse IP source dans un profil net à l'aide de l'interface de ligne de commande

Pour activer la persistance de l'adresse IP source lors de l'ajout d'un profil net, à l'invite de commandes, tapez :

```
add netProfile <name> -srcippersistency ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Pour activer la persistance de l'adresse IP source dans un profil net existant, à l'invite de commandes, tapez :

```
set netProfile <name> -srcippersistency ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Pour activer la persistance de l'adresse IP source dans un profil net à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **Profils réseau**.
2. Sélectionnez **Source IP persistency** lors de l'ajout ou de la modification d'un profil net.

Exemple

Dans l'exemple de configuration suivant, le profil net NETPROFILE-IPPRSTNCY-1 a l'option de persistance IP source activée et est lié à l'équilibrage de charge du serveur virtuel LBVS-1.

L'appliance Citrix ADC utilise toujours la même adresse IP (dans cet exemple, 192.0.2.11) pour communiquer avec les serveurs liés à LBVS-1, pour toutes les sessions initiées d'un client spécifique vers le serveur virtuel.

```
```
> add ipset IPSET-1

Done
```

 
```

```
> bind ipset IPSET-1 192.0.2.[11-15]
 IPAddress "192.0.2.11" bound
 IPAddress "192.0.2.12" bound
 IPAddress "192.0.2.13" bound
 IPAddress "192.0.2.14" bound
 IPAddress "192.0.2.15" bound
 Done
> add netprofile NETPROFILE-IPPRSTNCY-1 -srcIp IPSET-1 -
   srcippersistency ENABLED

Done
> set lb vserver LBVS-1 -netprofile NETPROFILE-IPPRSTNCY-1

 Done
<!--NeedCopy--> ```
```

Utiliser les adresses locales de liaison IPv6 côté serveur d'une configuration d'équilibrage de charge

August 20, 2021

L'adresse locale de liaison IPv6 est prise en charge pour les services, les groupes de services et les serveurs d'une configuration d'équilibrage de charge. Vous pouvez spécifier une adresse IPv6 locale de liaison avec l'ID VLAN associé dans les configurations de services, de groupes de services et de serveurs. L'appliance Citrix ADC utilise l'adresse SNIP6 locale du même VLAN que celle spécifiée dans les configurations de services, de groupes de services et de serveurs pour communiquer avec eux.

Une adresse IPv6 locale de liaison et l'ID VLAN associé sont spécifiés dans le format suivant dans les configurations des services, des groupes de services et des serveurs :`<IPv6_Addrs>%<vlan_id>`

Par exemple, `fe80:123:4567::a%2048:`, `fe80:123:4567::a` est l'adresse locale du lien ET 2048 est l'ID VLAN.

```
> add service SERVICE-1 fe80:123:4567::a%2048 HTTP 80

Done
> bind servicegroup SERVICE-GROUP-1 fe80::1%24 80

Done
> add server SERVER-1 fe80:b:c:d::e:f:a/64%1028

Done
```


Paramètres avancés d'équilibrage de charge

January 21, 2021

Outre la configuration des serveurs virtuels, vous pouvez configurer des paramètres avancés pour les services.

Pour configurer des paramètres avancés d'équilibrage de charge, consultez les sections suivantes :

- Augmenter progressivement la charge sur un nouveau service avec un démarrage lent au niveau du serveur virtuel
- Option sans moniteur pour les services
- Protéger les applications sur les serveurs protégés contre les surtensions de trafic
- Activer le nettoyage des connexions de serveur virtuel et de service
- Arrêt gracieux des services
- Activer ou désactiver la session de persistance sur les services TROFS
- Demandes directes vers une page Web personnalisée
- Activer l'accès aux services en cas de panne
- Activer la mise en mémoire tampon TCP des réponses
- Activer la compression
- Maintenir la connexion client pour plusieurs demandes client
- Insérer l'adresse IP du client dans l'en-tête de la requête
- Récupérer les détails de localisation à partir de l'adresse IP de l'utilisateur à l'aide de la base de données de géolocalisation
- Utiliser l'adresse IP source du client lors de la connexion au serveur
- Configurer le port source pour les connexions côté serveur
- Définir une limite sur le nombre de connexions client
- Définir une limite sur le nombre de requêtes par connexion au serveur
- Définir une valeur de seuil pour les moniteurs liés à un service
- Définir une valeur de délai d'attente pour les connexions client inactives
- Définir une valeur de délai d'attente pour les connexions au serveur inactif
- Définir une limite sur l'utilisation de la bande passante par les clients
- Rediriger les requêtes client vers un cache
- Conserver l'identificateur VLAN pour la transparence VLAN
- Configurer la transition automatique de l'état en fonction du pourcentage d'intégrité des services liés

Augmenter progressivement la charge sur un nouveau service avec un démarrage lent au niveau du serveur virtuel

August 20, 2021

Vous pouvez configurer l'appliance Citrix ADC pour augmenter progressivement la charge sur un service (nombre de demandes reçues par seconde) immédiatement après que le service a été ajouté à une configuration d'équilibrage de charge ou qu'il ait subi un changement d'état de DOWN à UP (dans ce document, le terme « nouveau service » est utilisé pour les deux situations). Vous pouvez augmenter la charge manuellement avec les valeurs de charge et les intervalles de votre choix (démarrage lent manuel) ou configurer l'appliance pour augmenter la charge à un intervalle spécifié (démarrage lent automatisé) jusqu'à ce que le service reçoive autant de demandes que les autres services de la configuration. Pendant la période de mise en service du nouveau service, l'appliance utilise la méthode d'équilibrage de charge configurée.

Cette fonctionnalité n'est pas disponible dans le monde entier. Il doit être configuré pour chaque serveur virtuel. La fonctionnalité est disponible uniquement pour les serveurs virtuels qui utilisent l'une des méthodes d'équilibrage de charge suivantes :

- Robin à la ronde
- Connexion minimale
- Temps de réponse le plus faible
- Bande passante minimale
- Moins de paquets
- LRTM (méthode du temps de réponse le moins important)
- Chargement personnalisé

Pour cette fonctionnalité, vous devez définir les paramètres suivants :

- Le nouveau taux de demande de service, qui correspond au montant auquel il faut augmenter le nombre ou le pourcentage de demandes envoyées à un nouveau service chaque fois que le tarif est incrémenté. Autrement dit, vous spécifiez la taille de l'incrément en termes de nombre de requêtes par seconde ou de pourcentage de charge supportée, à ce moment, par les services existants. Si cette valeur est définie sur 0 (zéro), le démarrage lent n'est pas effectué sur les nouveaux services.

  Remarque : Dans un mode de démarrage lent automatisé, l'incrément final est inférieur à la valeur spécifiée si la valeur spécifiée entraînerait une charge plus lourde sur le nouveau service que sur les autres services.

- Intervalle d'incrément, en secondes. Si cette valeur est définie sur 0 (zéro), la charge n'est pas incrémentée automatiquement. Vous devez l'incrémenter manuellement.

Avec un démarrage lent automatisé, un service est retiré de la phase de démarrage lent lorsque l'une des conditions suivantes s'applique :

- Le tarif réel des demandes est inférieur au nouveau tarif des demandes de service.
- Le service ne reçoit pas de trafic pendant trois intervalles successifs.
- Le taux de demande a été incrémenté 200 fois.
- Le pourcentage de trafic que le nouveau service doit recevoir est supérieur ou égal à 100.

Avec le démarrage lent manuel, le service reste dans la phase de démarrage lent jusqu'à ce que vous le sortiez de cette phase.

Démarrage lent manuel

Si vous souhaitez augmenter manuellement la charge sur un nouveau service, ne spécifiez pas d'intervalle d'incrémentation pour le serveur virtuel d'équilibrage de charge. Spécifiez uniquement le nouveau taux de demande de service et les unités. Si aucun intervalle n'est spécifié, l'appliance n'incrémente pas la charge périodiquement. Il maintient la charge sur le nouveau service à la valeur spécifiée par la combinaison du nouveau taux de demande de service et des unités jusqu'à ce que vous modifiiez manuellement l'un ou l'autre des paramètres. Par exemple, si vous définissez respectivement le taux de demande de service et les paramètres d'unité sur 25 et « par seconde », l'appliance maintient la charge sur le nouveau service à 25 requêtes par seconde jusqu'à ce que vous modifiiez l'un ou l'autre des paramètres. Lorsque vous souhaitez que le nouveau service quitte le mode de démarrage lent et reçoive autant de demandes que les services existants, définissez le nouveau paramètre de débit de demande de service sur 0.

Par exemple, supposons que vous utilisez un serveur virtuel pour équilibrer la charge de 2 services, Service1 et Service2, en mode rond. Supposons en outre que le serveur virtuel reçoit 240 requêtes par seconde et qu'il répartit la charge uniformément entre les services. Lorsqu'un nouveau service, Service3, est ajouté à la configuration, vous pouvez augmenter la charge manuellement via des valeurs de 10, 20 et 40 requêtes par seconde avant de lui envoyer sa part complète de la charge. Le tableau suivant présente les valeurs auxquelles vous définissez les trois paramètres.

Tableau 1. Valeurs des paramètres

Paramètre	Valeur
Intervalle en secondes	0
Nouveau tarif de demande de service	10, 20, 40 et 0, à intervalles que vous choisissez
Unités pour le nouveau taux de demande de service	Demandes par seconde

Lorsque vous définissez le nouveau paramètre de taux de demande de service sur 0, Service3 n'est plus considéré comme un nouveau service et reçoit sa part entière de la charge.

Supposons que vous ajoutez un autre service, Service4, pendant la période de transition pour Service3. Dans cet exemple, Service4 est ajouté lorsque le nouveau paramètre de taux de demande de service est défini sur 40. Par conséquent, Service4 commence à recevoir 40 demandes par seconde.

Le tableau suivant présente la répartition de la charge sur les services pendant la période décrite dans cet exemple.

Tableau 2. Distribution de charge sur les services lors de l'intensification manuelle de la charge

	nouveau taux de demande de service = 10 req/sec (Service3added)	nouveau taux de demande de service = 20 requis/sec	nouveau taux de demande de service = 40 req/sec (Service4added)	nouveau taux de demande de service = 0 req/sec (les nouveaux services quittent le mode de démarrage lent)
Service1	115	110	80	60
Service2	115	110	80	60
Service3	10	20	40	60
Service4	-	-	40	60
Nombre total de demandes/s (charge sur le serveur virtuel)	240	240	240	240

Démarrage lent automatisé

Si vous souhaitez que l'appliance augmente automatiquement la charge sur un nouveau service à intervalles spécifiés jusqu'à ce que le service puisse être considéré comme capable de gérer sa part entière de la charge, définissez le nouveau paramètre de débit de demande de service, le paramètre unités et l'intervalle d'incrémentation. Lorsque tous les paramètres sont définis sur des valeurs autres que 0, l'appliance incrémente la charge sur un nouveau service en fonction de la valeur du nouveau taux de demande de service, à l'intervalle spécifié, jusqu'à ce que le service reçoive toute sa part de la charge.

Par exemple, supposons que quatre services, Service1, Service2, Service3 et Service4, sont liés à un

serveur virtuel d'équilibrage de charge, vserver1. Supposons en outre que vserver1 reçoit 100 requêtes par seconde et qu'il répartit la charge uniformément entre les services (25 requêtes par seconde par service). Lorsque vous ajoutez un cinquième service, Service5, à la configuration, vous pouvez souhaiter que l'appliance envoie le nouveau service 4 demandes par seconde pendant les 10 premières secondes, 8 demandes par seconde pendant les 10 secondes suivantes, etc., jusqu'à ce qu'elle reçoive 20 demandes par seconde. Pour cette exigence, le tableau suivant indique les valeurs auxquelles vous définissez les trois paramètres :

Tableau 3. Valeurs des paramètres

Paramètre	**Valeur**
Intervalle en secondes	10
Valeur d'incrémentation	4
Unités pour le nouveau taux de demande de service	Demandes par seconde

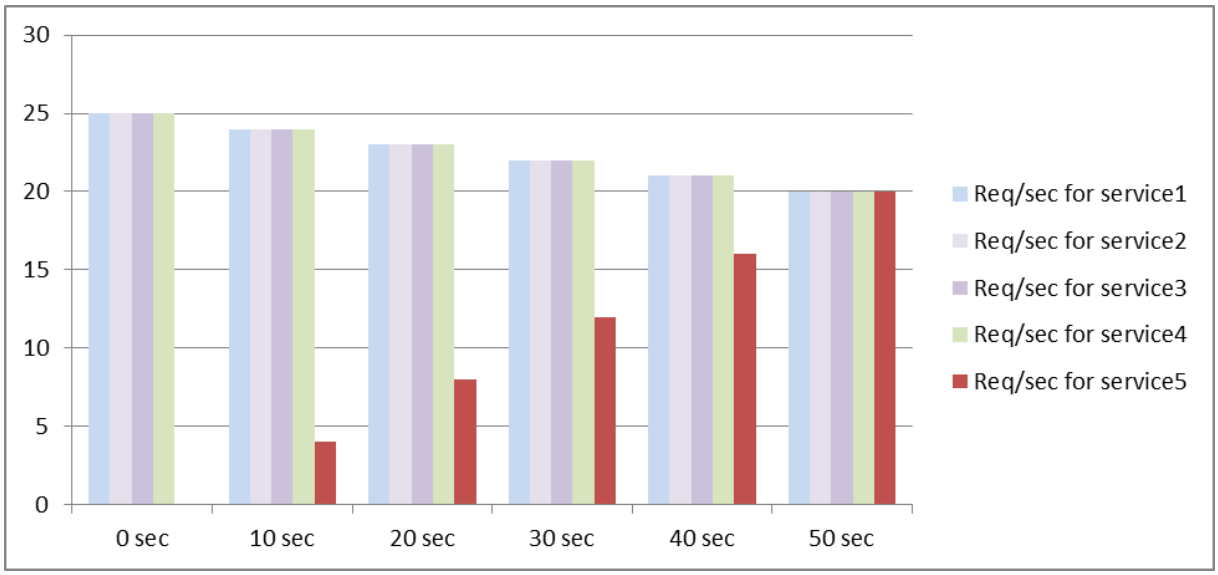
Avec cette configuration, le nouveau service commence à recevoir autant de demandes que les services existants 50 secondes après son ajout ou son état est passé de DOWN à UP. Au cours de chaque intervalle de cette période, l'appliance distribue aux serveurs existants l'excédent de demandes qui auraient été envoyées au nouveau service en l'absence d'incréments pas à pas. Par exemple, en l'absence d'incréments progressifs, chaque service, y compris le Service5, aurait reçu 20 demandes chacune par seconde. Avec des incréments pas à pas, pendant les 10 premières secondes, lorsque Service5 ne reçoit que 4 demandes par seconde, l'appliance distribue l'excédent de 16 demandes par seconde aux services existants, ce qui donne lieu au schéma de distribution indiqué dans le tableau et la figure suivants sur la période de 50 secondes. Après la période de 50 secondes, Service5 n'est plus considéré comme un nouveau service et reçoit sa part normale du trafic.

Tableau 4. Modèle de répartition de charge sur tous les services pour la période de 50 secondes Immédiatement après l'ajout du Service5

	0 seconde	10 secondes	20 seconde	30 secondes	40 seconde	50 seconde
Req/sec forService1	25	24	23	22	21	20
Req/sec forService2	25	24	23	22	21	20

	0 seconde	10 secondes	20 seconde	30 secondes	40 seconde	50 seconde
Req/sec forSer-vice3	25	24	23	22	21	20
Req/sec forSer-vice4	25	24	23	22	21	20
Req/sec forSer-vice5	0	4	8	12	16	20
Nombre total de deman-des/s (charge sur le serveur virtuel)	100	100	100	100	100	100

Figure 1. Graphique du modèle de répartition de charge sur tous les services pour la période de 50 secondes immédiatement après l'ajout du service5



Une autre exigence pourrait consister à ce que l'appliance envoie le Service5 25 % de la charge sur les services existants dans les 5 premières secondes, 50 % dans les 5 secondes suivantes, etc., jusqu'à ce qu'elle reçoive 20 demandes par seconde. Pour cette exigence, le tableau suivant indique les valeurs

auxquelles vous définissez les trois paramètres.

Tableau 5. Valeurs des paramètres

Paramètre	Valeur
Intervalle en secondes	5
Valeur d'incrémentation	25
Unités pour le nouveau taux de demande de service	Pourcentage

Avec cette configuration, le service commence à recevoir autant de demandes que les services existants 20 secondes après son ajout ou son état est passé de DOWN à UP. La répartition du trafic au cours de la période de rampe pour le nouveau service est identique à celle décrite précédemment, où l'unité pour les incréments d'échelon était « demandes par seconde ».

Définir les paramètres de démarrage lent

Vous définissez les paramètres de démarrage lent à l'aide de la commande `set lb vserver` ou de la `add lb vserver` commande. La commande suivante permet de définir des paramètres de démarrage lent lors de l'ajout d'un serveur virtuel.

Pour configurer des incréments de charge pas à pas pour un nouveau service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer les incréments pas à pas dans la charge d'un service et vérifiez la configuration :

```
1 add lb vserver <name> <serviceType> <IPAddress> <port> [-
     newServiceRequest <positive_integer>] [<newServiceRequestUnit>] [-
     newServiceRequestIncrementInterval <positive_integer>]
2
3 show lb vserver <name>
4 <!--NeedCopy-->
```

Exemple

```
1 set lb vserver BR_LB -newServiceRequest 5 PER_SECOND -
     newServiceRequestIncrementInterval 10
2 Done
```



```
3
4 show lb vserver BR_LB
5 BR_LB (192.0.2.33:80) - HTTP Type: ADDRESS
6 State: UP
7 ...
8 ...
9 New Service Startup Request Rate: 5 PER_SECOND, Increment Interval: 10
10 ...
11 ...
12 Done
13 <!--NeedCopy-->
```

Pour configurer des incréments de charge pas à pas pour un nouveau service à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez Méthode et définissez les paramètres de démarrage lent suivants :
   - Nouveau taux de demande de démarrage du service.
   - Nouvelle unité de demande de service.
   - Intervalle d'incrémentation.

Option sans moniteur pour les services

August 20, 2021

Si vous utilisez un système externe pour effectuer des vérifications d'intégrité sur les services et que vous ne souhaitez pas que l'appliance Citrix ADC surveille l'intégrité d'un service, vous pouvez définir l'option sans moniteur pour le service. Dans ce cas, l'appliance n'envoie pas de sondes pour vérifier l'état du service, mais affiche le service sous la forme UP. Même si le service est en panne, l'appliance continue d'envoyer du trafic depuis le client vers le service, comme spécifié par la méthode d'équilibrage de charge.

Le moniteur peut être dans l'état ENABLED ou DISABLED lorsque vous définissez l'option no-monitor et lorsque vous supprimez l'option no-monitor, l'état antérieur du moniteur est repris.

Vous pouvez définir l'option sans moniteur pour un service lors de la création du service. Vous pouvez également définir l'option sans moniteur sur un service existant.

Voici les conséquences de la définition de l'option sans moniteur :

- Si un service pour lequel vous avez activé l'option sans moniteur tombe en panne, l'appliance continue d'afficher le service en mode UP et de transférer le trafic vers le service. Une connexion persistante au service peut aggraver la situation. Dans ce cas, ou si de nombreux services affichés comme UP sont réellement DOWN, le système peut échouer. Pour éviter une telle situation, lorsque le mécanisme externe qui surveille les services signale un service comme DOWN, supprimez le service de la configuration Citrix ADC.
- Si vous configurez l'option sans moniteur sur un service, vous ne pouvez pas configurer l'équilibrage de charge en mode DSR (Direct Server Return). Pour un service existant, si vous définissez l'option sans moniteur, vous ne pouvez pas configurer le mode DSR pour le service.

Pour définir l'option sans moniteur pour un nouveau service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service avec l'option Analyseur de santé et vérifiez la configuration :

```
add service <serviceName> <IP | serverName> <serviceType> <port> -
   healthMonitor (YES|NO)
<!--NeedCopy-->
```

Exemple :

```
add service nomonsrvc 10.102.21.21 http 80 -healthMonitor no
Done

show service nomonsrvc
nomonsrvc (10.102.21.21:80) - HTTP
State: UP
Last state change was at Mon Nov 15 22:41:29 2010
Time since last state change: 0 days, 00:00:00.970
Server Name: 10.102.21.21
 Server ID : 0 Monitor Threshold : 0
...
Access Down Service: NO
...
Down state flush: ENABLED
Health monitoring: OFF

1 bound monitor:
1) Monitor Name: tcp-default
State: UNKNOWN Weight: 1
Probes: 3 Failed [Total: 3 Current: 3]
Last response: Probe skipped - Health monitoring is turned off.
```



```
Response Time: N/A
Done
<!--NeedCopy-->
```

Pour définir l'option sans moniteur pour un service existant à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour définir l'option du moniteur de santé :

```
set service <name> -healthMonitor (YES|NO)
<!--NeedCopy-->
```

Exemple :

```
By default, the state of a service and the state of the corresponding
   monitor are UP.
 >show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP


1) Monitor Name: http-ecv
 State: UP Weight: 1
Probes: 99992 Failed [Total: 0 Current: 0]
Last response: Success - Pattern found in response.
Response Time: 3.76 millisec
Done

When the no-monitor option is set on a service, the state of the
   monitor changes to UNKNOWN.
set service LB-SVC1 -healthMonitor NO
Done

show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP
Last state change was at Fri Dec 10 10:17:37 2010.
Time since last state change: 5 days, 18:55:48.710
Health monitoring: OFF

1) Monitor Name: http-ecv
   State: UNKNOWN Weight: 1
         Probes: 100028 Failed [Total: 0 Current: 0]
   Last response: Probe skipped - Health monitoring is turned off.
```



```
29       Response Time: 0.0 millisec
30     Done
31 When the no-monitor option is removed, the earlier state of the monitor
       is resumed.
32 > set service LB-SVC1 -healthMonitor YES
33 Done
34 >show service LB-SVC1
35 LB-SVC1 (10.102.29.5:80) - HTTP
36 State: UP
37 Last state change was at Fri Dec 10 10:17:37 2010
38 Time since last state change: 5 days, 18:57:47.880
39 1) Monitor Name: http-ecv
40    State: UP Weight: 1
41    Probes: 100029 Failed [Total: 0 Current: 0]
42    Last response: Success - Pattern found in response.
43    Response Time: 5.690 millisec
44    Done
45 <!--NeedCopy-->
```

Pour définir l'option sans moniteur pour un service à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Ouvrez le service et désactivez la fonction Surveillance de l'état.

Protéger les applications sur les serveurs protégés contre les surtensions de trafic

August 20, 2021

L'appliance Citrix ADC fournit l'option de protection contre les surtensions pour maintenir la capacité d'un serveur ou d'un cache. L'appliance régule le flux des demandes des clients vers les serveurs et contrôle le nombre de clients pouvant accéder simultanément aux serveurs. L'appliance bloque toutes les surtensions transmises au serveur, empêchant ainsi la surcharge du serveur.

Pour que la protection contre les surtensions fonctionne correctement, vous devez l'activer globalement. Pour plus d'informations sur la protection contre les surtensions, voir Protection contre les surtensions.

Pour définir la protection contre les surtensions sur le service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -sp <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -sp ON
<!--NeedCopy-->
```

Pour définir la protection contre les surtensions sur le service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez une source.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**, puis **Protection contre les surtensions**.

Activer le nettoyage des connexions de serveur virtuel et de service

August 20, 2021

L'état d'un serveur virtuel dépend des états des services qui lui sont liés. L'état de chaque service dépend des réponses des serveurs équilibrés de charge aux sondes ou aux vérifications d'intégrité envoyées par les moniteurs liés à ce service. Parfois, les serveurs équilibrés de charge ne répondent pas. Si un serveur est lent ou occupé, les sondes de surveillance peuvent s'écouler. Si les sondes de surveillance répétées ne sont pas répondues dans le délai d'expiration configuré, le service est marqué DOWN. Si un service ou un serveur virtuel est marqué BAS, les connexions côté serveur et client doivent être vides. La fin des connexions existantes libère des ressources et, dans certains cas, accélère la récupération des configurations d'équilibrage de charge surchargées.

Sous certaines conditions, vous pouvez configurer le paramètre **DownStateFlush** pour mettre fin immédiatement aux connexions existantes lorsqu'un service ou un serveur virtuel est marqué « DOWN ». N'activez pas le paramètre DownStateFlush sur les serveurs d'applications qui doivent terminer leurs transactions. Vous pouvez activer ce paramètre sur les serveurs Web dont les connexions peuvent être interrompues en toute sécurité lorsqu'ils sont marqués comme DOWN.

Le tableau suivant résume l'effet de ce paramètre sur un exemple de configuration constitué d'un serveur virtuel, vServer-LB-1, avec un service qui lui est lié, Service-1. Dans le tableau, E et D indiquent l'état du paramètre downStateFlush : E signifie Activé et D signifie Désactivé.

Vserver-LB-1	Service-1	État des connexions
E	E	Les connexions client et serveur sont toutes deux terminées.
E	D	Pour certains types de services, tels que TCP, pour lesquels l'appliance Citrix ADC ne prend pas en charge la réutilisation des connexions, les connexions client et serveur sont toutes deux interrompues. Pour les types de services, tels que HTTP, pour lesquels l'appliance prend en charge la réutilisation des connexions, les connexions client et serveur ne sont interrompues que si une transaction est active sur ces connexions. Si une transaction n'est pas active, seules les connexions client sont interrompues.

Vserver-LB-1	Service-1	État des connexions
D	E	Pour certains types de services, tels que TCP, pour lesquels l'appliance Citrix ADC ne prend pas en charge la réutilisation des connexions, les connexions client et serveur sont toutes deux interrompues. Pour les types de services, tels que HTTP, pour lesquels l'appliance prend en charge la réutilisation des connexions, les connexions client et serveur ne sont interrompues que si une transaction est active sur ces connexions. Si une transaction n'est pas active, seules les connexions serveur sont interrompues.
D	D	Ni les connexions client ni serveur ne sont interrompues.

Si vous souhaitez désactiver un service uniquement lorsque toutes les connexions établies sont fermées par le serveur ou le client, vous pouvez utiliser l'option d'arrêt gracieux. Pour plus d'informations sur l'arrêt gracieux d'un service, voir Arrêt gracieux des services.

Pour définir le vidage d'état sur le service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name>  -downStateFlush (ENABLED | DISABLED )
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -downStateFlush enabled
<!--NeedCopy-->
```


Pour définir le vidage d'état sur le service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**et sélectionnez **Vidage de l'état dévalant**.

Pour définir le vidage d'état sur le serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name>  -downStateFlush (ENABLED | DISABLED )
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vsvr1 -downStateFlush enabled
<!--NeedCopy-->
```

Pour définir le vidage d'état sur le serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**et sélectionnez **Vidage de l'état dévalant**.

Arrêt gracieux des services

August 20, 2021

Lors de pannes réseau planifiées, telles que les mises à niveau du système ou la maintenance matérielle, vous devrez peut-être fermer ou désactiver certains services. Vous pouvez ensuite activer le service en utilisant la commande " enable service <name>.

Pour éviter d'interrompre les sessions établies, vous pouvez placer un service dans l'état Transition Out of Service (TROFS) en procédant de l'une des manières suivantes :

- Ajout d'un code ou d'une chaîne TROFS au moniteur : configurez le serveur pour qu'il envoie un code ou une chaîne spécifique en réponse à une sonde de moniteur.
- Désactivez explicitement le service et :
  - Définissez un délai (en secondes).
  - Activez l'arrêt progressif.

Ajout d'un code ou d'une chaîne TROFS

Si vous ne liez qu'un seul moniteur à un service et que le moniteur est compatible TroFS, il peut placer le service dans l'état TROFS en fonction de la réponse du serveur à une sonde de moniteur. Cette réponse est comparée à la valeur du paramètre trofsCode pour un moniteur HTTP ou le paramètre trofsString pour un moniteur HTTP ECV ou TCP-ECV. Si le code correspond, le service est placé dans l'état TROFS. Dans cet état, il continue d'honorer les connexions persistantes.

Si plusieurs moniteurs sont liés à un service, l'état effectif du service est calculé sur la base de l'état de tous les moniteurs liés au service. Lors de la réception d'une réponse TROFS, l'état du moniteur compatible TROFS est considéré comme UP aux fins de ce calcul. Pour plus d'informations sur la façon dont une appliance Citrix ADC désigne un service comme UP, reportez-vous à la section Définition d'une valeur de seuil pour les moniteurs liés à un service.

Important :

- Vous pouvez lier plusieurs moniteurs à un service, mais vous ne devez pas activer TroFS plusieurs d'entre eux.
- Vous pouvez convertir un moniteur compatible TroFS en un moniteur qui n'est pas compatible TroFS, mais pas l'inverse.

Pour configurer un code ou une chaîne TROFS dans un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
add lb monitor <monitor-name> HTTP -trofsCode <respcode>

add lb monitor <monitor-name> HTTP-ECV  -trofsString <resp string>

add lb monitor <monitor-name> TCP-ECV  -trofsString <resp string>
<!--NeedCopy-->
```

Pour modifier le code ou la chaîne TROFS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
set lb monitor <trofs monitorname> HTTP -trofscode <newcode>

set lb monitor <trofs monitorname> HTTP-ECV -trofsstring <new string>

set lb monitor <trofs monitorname> TCP-ECV -trofsstring <new string>
<!--NeedCopy-->
```


Remarque : Vous pouvez utiliser la commande set uniquement si un moniteur compatible TroFS a été ajouté précédemment. Vous ne pouvez pas utiliser cette commande pour définir le code ou la chaîne TROFS pour un moniteur qui n'est pas activé TroFS.

Pour configurer un code ou une chaîne TROFS dans un moniteur à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Moniteurs.
2. Dans le volet Moniteurs, cliquez sur Ajouter, puis effectuez l'une des opérations suivantes :
    - Sélectionnez Type as HTTP, puis spécifiez un code TROFS.
    - Sélectionnez Type en tant que HTTP-ECV ou TCP-ECV, puis spécifiez une chaîne TROFS.

Désactivation d'un service

Souvent, cependant, vous ne pouvez pas estimer le temps nécessaire à toutes les connexions à un service pour effectuer les transactions existantes. Si une transaction n'est pas terminée à l'expiration du temps d'attente, l'arrêt du service peut entraîner une perte de données. Dans ce cas, vous pouvez spécifier un arrêt progressif pour le service, de sorte que le service n'est désactivé que lorsque toutes les connexions clientes actives actuelles sont fermées par le serveur ou le client. Consultez le tableau suivant pour connaître le comportement si vous spécifiez un temps d'attente en plus de l'arrêt progressif.

La persistance est maintenue selon la méthode spécifiée même si vous activez l'arrêt gracieux. Le système continue de servir tous les clients persistants, y compris les nouvelles connexions des clients, sauf si le service est marqué comme DOWN pendant l'état d'arrêt gracieux à la suite des vérifications effectuées par un moniteur.

Le tableau suivant décrit les options d'arrêt gracieuses.

State	Résultats
L'arrêt progressif est activé et un temps d'attente est spécifié.	Le service est arrêté après que la dernière des connexions client actives en cours est servie, même si le temps d'attente n'a pas expiré. L'appliance vérifie l'état des connexions une fois par seconde. Si le temps d'attente expire, toutes les sessions ouvertes sont fermées.
L'arrêt gracieux est désactivé et un temps d'attente est spécifié.	Le service n'est arrêté qu'après l'expiration du temps d'attente, même si toutes les connexions établies sont desservies avant l'expiration.

State	Résultats
L'arrêt progressif est activé et aucun temps d'attente n'est spécifié.	Le service n'est arrêté qu'une fois que la dernière des connexions précédemment établies est servie, quel que soit le temps nécessaire pour servir la dernière connexion.
L'arrêt gracieux est désactivé et aucun temps d'attente n'est spécifié.	Pas d'arrêt gracieux. Le service est arrêté immédiatement après le choix de l'option disable ou l'émission de la commande disable. (Le temps d'attente par défaut est de zéro seconde.)

Pour mettre fin à des connexions existantes lorsqu'un service ou un serveur virtuel est marqué comme DOWN, vous pouvez utiliser l'option Down State Flush. Pour plus d'informations, reportez-vous à la section Activation du nettoyage des connexions aux serveurs virtuels.

Pour configurer l'arrêt progressif d'un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour arrêter correctement un service et vérifier la configuration :

```
disable service <name> [<delay>] [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Exemple :

```
> disable service svc1 6000 -graceFul YES
Done
>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: GOING OUT OF SERVICE (Graceful, Out Of Service in 5998 seconds)
Last state change was at Mon Nov 15 22:44:15 2010
Time since last state change: 0 days, 00:00:01.160
...
Down state flush: ENABLED

1 bound monitor:
1) Monitor Name: tcp-default
State: UP              Weight: 1
```



```
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - live traffic to service.
Response Time: N/A
Done

>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: OUT OF SERVICE
Last state change was at Mon Nov 15 22:44:19 2010
Time since last state change: 0 days, 00:00:03.250
Down state flush: ENABLED

1 bound monitor:
1)  Monitor Name: tcp-default
State: UNKNOWN           Weight: 1
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - service state OFS.
Response Time: N/A
Done
<!--NeedCopy-->
```

Pour configurer l'arrêt progressif d'un service à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Ouvrez le service et, dans la liste Action, cliquez sur Désactiver. Entrez un temps d'attente, puis sélectionnez Graceful.

Activer ou désactiver la session de persistance sur les services TROFS

August 20, 2021

Vous pouvez définir l'indicateur TrofsPersistence pour spécifier si un service en état de transition hors service (TROFS) doit conserver des sessions persistantes. Lorsqu'un moniteur est activé par TROFS, il peut placer un service dans l'état TROFS en fonction de la réponse du serveur à une sonde de moniteur. Cette réponse est comparée à la valeur du paramètre trofsCode pour un moniteur HTTP ou le paramètre trofsString pour un moniteur HTTP ECV ou TCP-ECV. Si le code correspond, le service est placé dans l'état TROFS. Dans cet état, il continue d'honorer les connexions clientes actives. Dans certains cas, les sessions actives honorées peuvent devoir inclure des sessions persistantes. Mais dans d'autres cas, en particulier ceux impliquant des sessions de persistance de longue durée ou des méthodes de persistance telles que l'ID de serveur personnalisé, le respect des sessions persistantes peut empêcher le service de passer à l'état hors service.

Si vous définissez l'indicateur TrofsPersistence sur Enabled, les sessions persistantes sont honorées. Si vous le définissez sur DISABLED, ils ne le sont pas.

Pour définir l'indicateur TrofsPersistence à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour définir l'indicateur `trofsPersistence` d'un nouveau serveur virtuel ou d'un serveur virtuel existant, ou pour renvoyer le paramètre à sa valeur par défaut :

```
add lb vserver <name> [-trofsPersistence ( ENABLED | DISABLED )]

set lb vserver <name> [-trofsPersistence ( ENABLED | DISABLED )]

unset lb vserver <name> [-trofsPersistence]
<!--NeedCopy-->
```

Argument

trofsPersistence. Honorer les connexions clientes actives actuelles et les nouvelles demandes sur les sessions de persistance lorsque le service est dans l'état TROFS.

Valeurs possibles : ENABLED, DISABLED. Par défaut : ENABLED.

Exemples :

```
add lb vserver v1 http 10.102.217.42 80 -persistencetype SOURCEIP -
    trofsPersistence ENABLED

set lb vserver v1 -trofsPersistence DISABLED

unset lb vserver v1 -trofsPersistence
<!--NeedCopy-->
```

Demandes directes vers une page Web personnalisée

September 8, 2021

> **Avertissement**
>
> SureConnect (SC) est obsolète à partir de NetScaler 12.0 build 56.20 et Citrix vous recommande d'utiliser la fonctionnalité AppQoE. Pour plus d'informations, voirAppQoE.

Pour que SureConnect fonctionne correctement, vous devez le définir globalement. Le Citrix ADC fournit l'option SureConnect pour garantir la réponse d'une application.
Pour plus d'informations sur l'option SureConnect, voir Sure Connect.

Pour définir SureConnect sur le service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -sc <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -sc ON
<!--NeedCopy-->
```

Pour définir SureConnect sur le service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez Paramètres de trafic, puis **Sure Connect**.

Activer l'accès aux services en cas de panne

August 20, 2021

Vous pouvez activer l'accès à un service lorsqu'il est désactivé ou dans un état DOWN en configurant l'appliance Citrix ADC pour qu'elle utilise le mode de couche 2 pour relier les paquets envoyés au service. Normalement, lorsque les demandes sont transférées vers des services DOWN, les paquets de requête sont supprimés. Toutefois, lorsque vous activez le paramètre **Access Down**, ces paquets de demandes sont envoyés directement aux serveurs à charge équilibrée.

Pour plus d'informations sur les modes de couche 2 et de couche 3, voir Adressage IP.

Pour que l'appliance relie les paquets envoyés aux services DOWN, activez le mode Couche 2 avec le paramètre AccessDown.

Pour activer l'accès sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -accessDown <Value>
<!--NeedCopy-->
```


Exemple :

```
set service Service-HTTP-1 -accessDown YES
<!--NeedCopy-->
```

Pour activer l'accès sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**, puis **Access Down**.

Activer la mise en mémoire tampon TCP des réponses

August 20, 2021

L'appliance Citrix ADC fournit une option de mise en mémoire tampon TCP qui ne met en mémoire tampon que les réponses du serveur à équilibrage de charge. Cela permet à l'appliance de fournir des réponses serveur au client à la vitesse maximale que le client peut accepter. L'appliance alloue de 0 à 4 095 Mo (Mo) de mémoire tampon pour la mise en mémoire tampon TCP et de 4 à 2 480 kilo-octets (Ko) de mémoire par connexion.

Remarque : La mise en mémoire tampon TCP au niveau du service a priorité sur le paramètre global. Pour plus d'informations sur la configuration globale de la mise en mémoire tampon TCP, voir TCP Buffering.

Pour activer la mise en mémoire tampon TCP sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -TCPB <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -TCPB YES
<!--NeedCopy-->
```

Pour activer la mise en mémoire tampon TCP sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.

2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**, puis **Buffering TCP**.

Activer la compression

August 20, 2021

L'appliance Citrix ADC fournit une option de compression pour compresser de manière transparente les fichiers HTML et texte à l'aide d'un ensemble de stratégies de compression intégrées. La compression réduit les besoins en bande passante et peut améliorer considérablement la réactivité du serveur dans les configurations soumises à des contraintes de bande passante. Les stratégies de compression sont associées aux services liés au serveur virtuel. Les stratégies déterminent si une réponse peut être compressée et envoyer du contenu compressible à l'appliance, qui la compresse et l'envoie au client.

Remarque : Pour que la compression fonctionne correctement, vous devez l'activer globalement. Pour plus d'informations sur la configuration globale de la compression, voir Compression.

Pour activer la compression sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -CMP <YES | NO>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -CMP YES
<!--NeedCopy-->
```

Pour activer la compression sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**, puis **Compression**.

Activer la vérification de l'état TCP externe pour les serveurs virtuels UDP

August 20, 2021

Dans les clouds publics, vous pouvez utiliser l'appliance Citrix ADC comme équilibreur de charge de deuxième niveau lorsque l'équilibreur de charge natif est utilisé comme premier niveau. L'équilibreur de charge natif peut être un équilibrage de charge d'application (ALB) ou un équilibreur de charge réseau (NLB). La plupart des clouds publics ne prennent pas en charge les sondes de santé UDP dans leurs équilibreurs de charge natifs. Pour surveiller l'intégrité de l'application UDP, les clouds publics recommandent d'ajouter un point de terminaison basé sur TCP à votre service. Le point de terminaison reflète l'intégrité de l'application UDP.

L'appliance Citrix ADC prend en charge le contrôle d'intégrité basé sur TCP externe pour un serveur virtuel UDP. Cette fonctionnalité introduit un écouteur TCP sur le VIP du serveur virtuel et le port configuré. L'écouteur TCP reflète l'état du serveur virtuel.

Pour activer un contrôle de santé TCP externe pour les serveurs virtuels UDP par CLI

À l'invite de commandes, tapez la commande suivante pour activer une vérification d'intégrité TCP externe avec l'option tcpProbePort :

```
1 add lb vserver <name> <serviceType> <IPAddress> <port> -tcpProbePort <
     tcpProbePort>
2 <!--NeedCopy-->
```

Exemple :

```
1 add lb vserver Vserver-UDP-1 UDP 10.102.29.60 80 tcpProbePort 5000
2 <!--NeedCopy-->
```

Pour activer un contrôle de santé TCP externe pour les serveurs virtuels UDP par interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis créez un serveur virtuel.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel.
3. Dans le volet **Paramètres de base**, ajoutez le numéro de port dans le champ **Port de sonde TCP**.
4. Cliquez sur **OK**.

Maintenir la connexion client pour plusieurs demandes client

August 20, 2021

Vous pouvez définir le paramètre Keep-Alive du client pour configurer un service HTTP ou SSL afin de maintenir une connexion client à un site Web ouverte sur plusieurs demandes client. Si le client keep-alive est activé, même lorsque le serveur Web à équilibrage de charge ferme une connexion, l'appliance Citrix ADC maintient la connexion entre le client et lui-même ouverte. Ce paramètre permet aux services de servir plusieurs requêtes client sur une seule connexion client.

Si vous n'activez pas ce paramètre, le client ouvre une nouvelle connexion pour chaque demande envoyée au site Web. Le paramètre Keep-alive du client permet d'économiser le temps de trajet aller-retour des paquets requis pour établir et fermer les connexions. Ce paramètre réduit également le temps nécessaire pour terminer chaque transaction. Le client Keep-alive ne peut être activé que sur les types de service HTTP ou SSL.

Client keep-alive défini au niveau du service a priorité sur le paramètre global keep-alive du client. Pour plus d'informations sur le service Keep-Alive du client, voir Keep-Alivedu client.

Pour activer le maintien en vie du client sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -CKA <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -CKA YES
<!--NeedCopy-->
```

Pour activer le maintien en vie du client sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**et sélectionnez **Client Keep-Alive**.

Insérer l'adresse IP du client dans l'en-tête de la requête

August 20, 2021

Un Citrix ADC utilise l'adresse IP du sous-réseau (SNIP) pour se connecter au serveur. Le serveur n'a pas besoin d'être au courant du client.

Cependant, dans certaines situations, le serveur doit être conscient du client qu'il doit servir. Lorsque vous activez le paramètre IP du client, l'appliance insère l'adresse IPv4 ou IPv6 du client lors du transfert des demandes au serveur. Le serveur insère cette adresse IP du client dans l'en-tête des réponses. Le serveur est donc au courant du client.

> **Remarque** : Pour insérer plusieurs en-têtes, vous devez effectuer l'une des opérations suivantes :
>
> - Ajoutez des stratégies de réécriture pour vérifier CLIENT.IS_SSL et insérer l'en-tête approprié.
> - Liez la stratégie de réécriture appropriée pour chaque serveur virtuel en fonction du type.

Pour insérer l'adresse IP du client dans la demande du client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -CIP <Value> <cipHeader>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -CIP enabled X-Forwarded-For
<!--NeedCopy-->
```

Pour insérer l'adresse IP du client dans la demande du client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services** et modifiez un service.
2. Dans le volet **Paramètres de service**, cliquez sur l'**icône Modifier**.
3. Dans le volet **Service d'équilibrage de charge**, activez la case à cocher **Insérer une adresse IP du client**.

Récupérer les détails de localisation à partir de l'adresse IP de l'utilisateur à l'aide de la base de données

October 5, 2021

> **Remarque** Cette fonctionnalité est disponible à partir de Citrix ADC version 12.1 build 50.x et ultérieure.

L'appliance Citrix ADC peut obtenir des informations sur l'emplacement de l'utilisateur, telles que le continent, le comté et la ville. Pour toute adresse IP publique provenant d'une base de données de géolocalisation. Il est exécuté à l'aide de l'infrastructure de stratégie avancée. Les détails de localisation récupérés sont ensuite utilisés dans une action de réécriture ou une action de répondeur pour effectuer les cas d'utilisation suivants.

- Insérez un en-tête HTTP avec les détails de l'emplacement de l'utilisateur (tels que le pays, la ville) lors de l'envoi de la demande du client au serveur principal.
- Ajoutez le nom du pays dans la réponse de la page HTML pour un utilisateur non valide.

La solution matérielle-logicielle peut également consigner les détails de l'emplacement à l'aide du mécanisme de journalisation d'audit.

Obtention des détails de localisation des utilisateurs à l'aide des fonctions de géolocalisation

Les composants interagissent comme suit :

1. L'utilisateur envoie une demande client à partir d'un emplacement géographique particulier.
2. L'appliance Citrix ADC recherche l'adresse IP de l'utilisateur à partir de la demande du client et récupère les détails de la géolocalisation. Les détails incluent le continent, le pays, la région, la ville, le FAI, l'organisation ou les détails personnalisés d'une base de données de géolocalisation.
3. Une fois les détails de l'emplacement récupérés, la solution matérielle-logicielle utilise une stratégie de répondeur ou une stratégie de réécriture pour évaluer la demande.
4. Dans une stratégie de réécriture, la solution matérielle-logicielle ajoute un en-tête avec les détails de l'emplacement géographique et l'envoie au serveur principal. Par exemple, insérez un en-tête HTTP personnalisé avec des informations de pays.
5. Dans une stratégie de répondeur, la solution matérielle-logicielle évalue la demande HTTP et, en fonction de l'évaluation de la stratégie, autorise l'accès aux utilisateurs ou redirige l'utilisateur vers une page d'erreur. Il indique que la région à partir de laquelle ils accèdent à l'application n'a pas accès.

Configuration de la base de données de géolocalisation

En tant que condition préalable, vous devez disposer d'une base de données de géolocalisation pour pouvoir être exécutée sur l'appliance Citrix ADC. Les fichiers de base de données de géolocalisation sont disponibles avec le microprogramme Citrix ADC. Pour télécharger les fichiers de base de données à partir d'un fournisseur, convertissez-les au format Citrix ADC et importez-les dans votre appliance. Pour plus d'informations sur la base de données de géolocalisation, consultez la rubrique Ajouter un fichier d'emplacement pour créer une base de données de proximité statique .

Fonctions de géolocalisation

Le tableau suivant répertorie les fonctions de géolocalisation qui récupèrent les détails de localisation de n'importe quelle adresse IP publique. Ces fonctions peuvent être utilisées dans les stratégies de réécriture ou de répondeur.

Fonction de géolocalisation	Exemple
CLIENT.IP.SRC.LOCATION	Asia.In.Karnataka.Bangalore
CLIENT.IP.SRC.LOCATION.GET (1) .LOCATION_LONG	Inde
CLIENT.IP.SRC.LOCATION (3)	Asia.In.Karnataka
CLIENT.IP.SRC.LAT_LONG	12,77
CLIENT.IPV6.SRC.LOCATION	Amérique du Nord .US.Californie.Santa Clara.Verizon.Citrix
CLIENT.IPV6.SRC.LOCATION(3)	Amérique du Nord, États-Unis, Californie
CLIENT.IPV6.SRC.LOCATION.GET (1) .LOCATION_LONG	États-Unis
CLIENT.IPV6.SRC.LOCATION.GET (3)	Californie
CLIENT.IPV6.SRC.LAT_LONG	36, -119

Configuration des fonctions de géolocalisation

Pour configurer les fonctions de géolocalisation à l'aide d'une infrastructure de stratégie avancée, vous devez activer les fonctionnalités d'équilibrage de charge, de réécriture et de répondeur, puis compléter les cas d'utilisation suivants.

Activer les fonctionnalités d'équilibrage de charge, de répondeur et de réécriture

Si vous souhaitez que l'appliance Citrix ADC autorise l'accès des utilisateurs à partir d'un emplacement géographique particulier, vous devez activer les fonctionnalités d'équilibrage de charge, de réécriture et de répondeur.

```
1 enable ns feature loadbalancing rewrite responder
2 <!--NeedCopy-->
```


Cas d'utilisation 1 : Configuration de la fonction de géolocalisation pour rediriger les utilisateurs non valides en dehors de la géolocalisation

Lorsqu'un utilisateur indien demande l'accès à une page Web, bloquez la demande et répondez avec une page HTML avec le nom du pays.

Les étapes suivantes vous aident à terminer la configuration de ce cas d'utilisation.

- Ajouter une action du répondeur
- Ajouter une stratégie de répondeur
- Lier la stratégie du répondeur au serveur d'équilibrage de charge

Pour plus d'informations sur les procédures de l'interface graphique pour l'action de réécriture et la configuration de la stratégie de réécriture, consultez la rubrique Responder

Ajouter une action du répondeur

Ajoutez une action de répondeur pour répondre avec une page HTML avec le nom du pays.
À l'invite de commandes, tapez :

```
1 add responder action <name> <type> (<target> | <htmlpage>) [-comment <
     string>] [-responseStatusCode <positive_integer>][-reasonPhrase <
     string>]
2 <!--NeedCopy-->
```

Exemple :

```
1 add responder action responder_act respondwith "HTTP.REQ.VERSION + "
     304 Requested Page not allowed in your country - " + CLIENT.IP.SRC.
     LOCATION.GET (1).LOCATION_LONG + "\r\n""
2 <!--NeedCopy-->
```

Ajouter une action de message journal d'audit

Vous pouvez configurer les actions de message d'audit pour consigner les messages à différents niveaux de journal, soit au format Syslog uniquement, soit en syslog et en newnslog formats. Les actions de message d'audit utilisent des expressions pour spécifier le format des messages d'audit. Pour créer une action de message d'audit à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add audit messageaction <name> <logLevel> <stringBuilderExpr> [-logtoNewnslog
 (YES|NO)]
```

Exemple :


```
add audit messageaction msg1 DEBUG ""Request Location: "+CLIENT.IP.SRC.
    LOCATION"
<!--NeedCopy-->
```

Ajouter une stratégie de répondeur

Ajoutez une stratégie de répondeur pour identifier les demandes provenant de l'Inde et associez l'action de répondeur à cette stratégie.
À l'invite de commandes, tapez :

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>] [-appflowAction <string>]
<!--NeedCopy-->
```

Exemple :

```
add responder policy responder_pol CLIENT.IP.SRC.MATCHES_LOCATION("Asia
    .India.\*.\*.\*.\*") responder_act -logaction msg1
<!--NeedCopy-->
```

Lier la stratégie du répondeur au serveur d'équilibrage de charge

Liez la stratégie de répondeur à un serveur virtuel d'équilibrage de charge de type HTTP/SSL.
À l'invite de commandes, tapez :

```
bind lb vserver <vserver name> -policyName < policy_name >  -priority
    <> -type <L7InlineREQUEST | L4Inline-REQUEST>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver http_vserver -policyName responder_pol -priority 100 -
    type REQUEST
<!--NeedCopy-->
```

Cas d'utilisation 2 : Configuration de la fonction de géolocalisation pour insérer un nouvel en-tête HTTP avec des détails d'emplacement pour que le back-end réponde

Imaginons un scénario dans lequel une appliance Citrix ADC doit insérer l'emplacement de l'utilisateur dans l'en-tête HTTP d'une demande envoyée au serveur d'applications afin que le serveur puisse utiliser les informations pour une certaine logique métier.
Les étapes suivantes vous aident à terminer la configuration de ce cas d'utilisation.

- Ajouter une action de réécriture
- Ajouter une stratégie de réécriture
- Lier la stratégie de réécriture à l'équilibrage de charge

Pour plus d'informations sur les procédures de l'interface graphique pour l'action de réécriture et la configuration de la stratégie de réécriture, consultez la rubrique Répondeur .

Ajouter une action de réécriture

Ajoutez une action de réécriture pour insérer un en-tête HTTP personnalisé avec les détails de géolocalisation de l'utilisateur dans la demande et envoyez-lui des serveurs principaux.
À l'invite de commandes, tapez :

```
add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-
    search <expression>] [-refineSearch <string>][-comment <string>]
<!--NeedCopy-->
```

Exemple :

```
add rewrite action rewrite_act insert_http_header "User_location"
    CLIENT.IP.SRC.LOCATION
<!--NeedCopy-->
```

Ajouter une stratégie de réécriture

Ajoutez une stratégie de réécriture pour déterminer si l'action de réécriture doit être exécutée. Dans ce cas, toutes les requêtes envoyées au serveur d'applications doivent comporter un en-tête HTTP personnalisé, de sorte que la règle peut être « true ».
À l'invite de commandes, tapez :

```
add rewrite policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>]
<!--NeedCopy-->
```

Exemple :

```
add rewrite policy rewrite_pol true rewrite_act -logaction log_act
<!--NeedCopy-->
```

Lier la stratégie de réécriture à l'équilibrage de charge

Liez la stratégie de réécriture au serveur virtuel d'équilibrage de charge requis de type HTTP/SSL.
À l'invite de commandes, tapez :


```
bind lb vserver <vserver name> -policyName < policy_name >  -priority
    <> -type <L7InlineREQUEST | L4Inline-REQUEST>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver http_vserver -policyName rewrite_pol -priority 100 -
    type REQUEST
<!--NeedCopy-->
```

Prise en charge de Syslog pour la journalisation des détails de géolocalisation (facultatif)

Si vous préférez consigner les détails de géolocalisation de l'utilisateur, vous devez spécifier l'action SYSLOG à exécuter lorsqu'une demande correspond à la stratégie. L'appliance stocke les détails sous forme de message de journal dans le fichier ns.log.
Pour plus d'informations sur l'audit SYSLOG et NSLOG, consultez la rubrique Journalisation des audits
.

Sortie pour les détails de géolocalisation utilisateur

La sortie suivante est enregistrée dans l'appliance à l'aide du SYSLOG ou de l' `newnslog` action si vous essayez d'accéder à une application depuis l'emplacement Bangalore et si l'appliance utilise la fonction de géolocalisation, « CLIENT.IP.SRC.LOCATION'.

```
Asia.India.Karnataka.Banglore
<!--NeedCopy-->
```

Exemple de journal de sortie :

```
07/23/2018:19:03:54 GMT  Debug 0-PPE-0 : default REWRITE Message 22 0 :
     "Request Location: asia.in.karnataka.bangalore.\*.\*"
07/23/2018:19:23:55 GMT  Debug 0-PPE-0 : default RESPONDER Message 32 0
Done
<!--NeedCopy-->
```

Utiliser l'adresse IP source du client lors de la connexion au serveur

August 20, 2021

Vous pouvez configurer l'appliance Citrix ADC pour qu'elle transfère les paquets du client vers le serveur sans modifier l'adresse IP source. Ceci est utile lorsque vous ne pouvez pas insérer l'adresse IP du client dans un en-tête, par exemple lorsque vous travaillez avec des services non HTTP.

Pour plus d'informations sur la configuration globale d'USIP, consultez Activation de l'utilisation du mode IP source.

Pour activer le mode USIP pour un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -usip (YES | NO)
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -usip YES
<!--NeedCopy-->
```

Pour activer le mode USIP pour un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis ouvrez un service.
2. Dans Paramètres avancés, dans la section Paramètres du service, sélectionnez **Utiliser l'adresse IP source**.

Utiliser l'adresse IP source du client pour la communication principale dans une configuration d'équilibrage de charge v4-v6

August 20, 2021

Dans une configuration d'équilibrage de charge v4-v6, pour les services avec USIP désactivés, l'appliance Citrix ADC communique avec les serveurs associés à partir de l'une des adresses SNIP IPv6 (SNIP6) configurées.

Pour les services avec USIP activé, vous devez définir le paramètre global de préfixe USIP NAT pour informer les serveurs associés de l'adresse IP du client des paquets de requête. Le préfixe NAT USIP est un préfixe IPv6 global de longueur 32/40/48/56/64/96 bits configuré sur l'appliance Citrix ADC.

Pour un service d'équilibrage de charge sur lequel USIP est activé, l'appliance convertit le paquet de requête IPv4 en paquet IPv6 et définit l'adresse IP source du paquet IPv6 traduit sur une concaténation de :

- le préfixe NAT USIP de longueur 32/40/48/56/64/96 bits.
- zéros rembourrés si la longueur du préfixe NAT USIP est inférieure à 96 bits. Nombre de bits rembourrés avec zéros = longueur du préfixe NAT 96-USIP. Par exemple, si la longueur du préfixe NAT USIP est 64, le nombre de bits rembourrés avec des zéros = 96-64 = 32.
- l'adresse source IPv4 [32 bits] qui a été reçue dans le paquet de requête. En d'autres termes, les 32 derniers bits de l'adresse IPv6 source sont définis sur l'adresse IPv4 du client.

À la réception d'un paquet de réponse IPv6 à partir du serveur, l'appliance Citrix ADC convertit le paquet IPv6 en paquet IPv4 et définit l'adresse IP de destination du paquet IPv4 traduit sur les 32 derniers bits de l'adresse IP de destination du paquet IPv6.

> **Remarque** : cette fonctionnalité n'est pas prise en charge pour la configuration Citrix Gateway et les configurations de commutation de contenu et d'équilibrage de charge de redirection de cache.

Étapes de configuration

La configuration d'USIP pour une configuration d'équilibrage de charge v4-v6 comporte les tâches suivantes :

- **Ajouter le préfixe NAT global USIP**. Il s'agit d'un préfixe IPv6 global de longueur 32/40/48/56/64/96 bits à configurer sur l'appliance.
- **Activer le mode global USIP**. Pour plus d'informations, voir Activer l'utilisation du mode IP source.
- **Activez le mode USIP pour les services d'équilibrage**de charge. Pour plus d'informations, voir Utiliser l'adresse IP source du client lors de la connexion au serveur.

Pour ajouter un préfixe NAT global USIP à l'aide de l'interface de ligne de commande :

- `set ipv6 -usipnatprefix <prefix/prefix_length>`
- `show ipv6`

Pour ajouter un préfixe NAT global USIP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau**, puis cliquez sur **Modifier les paramètres IPv6** .
2. Dans l'écran **Configurer la configuration pour IPV6**, définissez le paramètre **USIP NAT Prefix** .

Exemple de configuration

```
1 > set ipv6 -usipnatprefix 2001:DB8:90::/64
2 Done
3
4 > enable ns mode USIP
```



```
Done

> add lb vserver LBVS-1 HTTP 203.0.113.90 80
Done

> add service SVC-1 2001:DB8:5001::30 HTTP 80 -usip yes
Done

> add service SVC-2 2001:DB8:5001::60 HTTP 80 -usip yes
Done

> bind lb vserver LBVS-1 SVC-1
Done

> bind lb vserver LBVS-1 SVC-2
Done

<!--NeedCopy-->
```

Configurer le port source pour les connexions côté serveur

August 20, 2021

Lorsque l'appliance Citrix ADC se connecte à un serveur physique, elle peut utiliser le port source de la demande du client ou utiliser un port proxy comme port source de la connexion. Vous pouvez définir le paramètre Use Proxy Port sur YES pour gérer des situations telles que le scénario suivant :

- L'appliance Citrix ADC est configurée avec deux serveurs virtuels d'équilibrage de charge, LBVS1 et LBVS2.
- Les deux serveurs virtuels sont liés au même service, S-ANY.
- Utiliser (l'adresse IP source du client) est activée sur le service.
- Le client C1 envoie deux demandes, Req1 et Req2, pour le même service.
- LBVS1 reçoit Req1 et LBVS2 reçoit Req2.
- LBVS1 et LBVS2 transmettent la demande à S-ANY, et lorsque S-ANY envoie la réponse, LBVS1 et LBVS2 transmettent la réponse au client.
- Considérez deux cas :
  - Utilisez le port client. Lorsque l'appliance utilise le port client, les serveurs virtuels utilisent l'adresse IP du client (car USIP est ON) et le port du client lors de la connexion au serveur. Par conséquent, lorsque le service envoie la réponse, l'appliance ne peut pas déterminer quel serveur virtuel doit recevoir la réponse.

- Utiliser le port proxy. Lorsque l'appliance utilise un port proxy, les serveurs virtuels utilisent l'adresse IP du client (car USIP est ON), mais des ports différents lors de la connexion au serveur. Par conséquent, lorsque le service envoie la réponse, le numéro de port identifie le serveur virtuel qui doit recevoir la réponse.

Toutefois, si vous avez besoin d'une configuration entièrement transparente, telle qu'une configuration de redirection de cache entièrement transparente, vous devez désactiver le paramètre Utiliser le port proxy afin que l'appliance Citrix ADC puisse utiliser le port source à partir de la demande du client.

L'option Utiliser le port proxy devient pertinente si l'option Utiliser l'adresse IP source (USIP) est activée. Pour les types de service TCP, tels que TCP, HTTP et SSL, l'option est activée par défaut. Pour les types de service UDP, tels que UDP et DNS, y compris ANY, l'option est désactivée par défaut. Pour plus d'informations sur l'option USIP, reportez-vous à la section « Activation de l'utilisation du mode IP source ». «

Vous pouvez configurer le paramètre **Utiliser le port proxy** soit globalement, soit sur un service donné.

Configurer le paramètre d'utilisation du port proxy sur un service

Vous configurez le paramètre **Utiliser ProxyPort** sur le service si vous souhaitez remplacer le paramètre global.

Pour configurer le paramètre Utiliser le port proxy sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -useProxyPort (YES | NO)
<!--NeedCopy-->
```

Exemple :

```
set service svc1 -useproxyport YES
Done

show service svc1
svc1 (10.102.29.30:80) - HTTP
State: UP
. . .
Use Source IP: YES Use Proxy Port: YES
. . .
Done
```



```
<!--NeedCopy-->
```

Pour configurer le paramètre Utiliser le port proxy sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez Paramètres de trafic et sélectionnez **Utiliser le port proxy**.

Configurer globalement le paramètre d'utilisation du port proxy

Vous configurez le paramètre **Utiliser le port proxy** globalement si vous souhaitez appliquer le paramètre à tous les services de l'appliance Citrix ADC. Les paramètres **Use Proxy Port** spécifiques au service remplacent le paramètre global.

Pour configurer globalement le paramètre Utiliser le port proxy à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le paramètre **Utiliser le port proxy** globalement et vérifier la configuration :

```
set ns param -useproxyport ( ENABLED | DISABLED )`
show ns param`
<!--NeedCopy-->
```

Exemple :

```
set ns param -useproxyport ENABLED

Done

show ns param
Global configuration settings:
. . .
Use Proxy Port: ENABLED
Done
<!--NeedCopy-->
```


Pour configurer globalement le paramètre Utiliser le port proxy à l'aide de l'interface graphique

Accédez à **Système > Paramètres > Modifier les paramètres système globaux**, puis sélectionnez ou désactivez Utiliser le port proxy.

Définir une limite sur le nombre de connexions client

August 20, 2021

Vous pouvez spécifier un nombre maximal de connexions client que chaque serveur à équilibrage de charge peut gérer. L'appliance Citrix ADC ouvre ensuite les connexions client à un serveur uniquement jusqu'à ce que cette limite soit atteinte. Lorsque le serveur équilibré de charge atteint sa limite, les sondes du moniteur sont ignorées et le serveur n'est pas utilisé pour l'équilibrage de charge tant qu'il n'a pas terminé le traitement des connexions existantes et libère de la capacité.

Pour plus d'informations sur le paramètre **Maximum Client**, reportez-vous à la section Services basés sur des noms de domaine d'équilibrage de charge.

Remarque : Les connexions en cours de fermeture ne sont pas prises en compte pour cette limite.

Pour définir une limite au nombre de connexions client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -maxclient <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -maxClient 1000
<!--NeedCopy-->
```

Pour définir une limite au nombre de connexions client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Seuils et délais d'attente**, puis sélectionnez **Maximum Clients**.

Définir une limite sur le nombre de requêtes par connexion au serveur

August 20, 2021

L'appliance Citrix ADC peut être configurée pour réutiliser les connexions afin d'améliorer les performances. Dans certains scénarios, cependant, les serveurs Web à charge équilibrée peuvent rencontrer des problèmes lorsque les connexions sont réutilisées pour un trop grand nombre de demandes. Pour les services HTTP ou SSL, utilisez l'option de requête max pour limiter le nombre de requêtes envoyées via une seule connexion à un serveur Web à charge équilibrée.

Remarque : Vous pouvez configurer l'option de requête max pour les services HTTP ou SSL uniquement.

Pour limiter le nombre de requêtes client par connexion à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <ServiceName> -maxReq <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -maxReq 100
<!--NeedCopy-->
```

Pour limiter le nombre de requêtes client par connexion à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Seuils et délais d'attente**, puis sélectionnez **Maximum Requêtes**.

Définir une valeur de seuil pour les moniteurs liés à un service

August 20, 2021

L'appliance Citrix ADC désigne un service comme étant UP uniquement lorsque la somme des pondérations de tous les moniteurs qui lui sont liés et qui sont UP est égale ou supérieure à la valeur

de seuil configurée sur le service. Le poids d'un moniteur spécifie combien ce moniteur contribue à désigner le service auquel il est lié comme UP.

Par défaut, le seuil du moniteur est défini sur 0 et les poids du moniteur sont définis sur 1. Tous les moniteurs ont alors un poids égal et un service peut tomber en panne lorsque l'un des moniteurs tombe en panne.

Par exemple, supposons que trois moniteurs, nommés Monitor-HTTP-1, Monitor-HTTP-2 et Monitor-HTTP-3 respectivement, sont liés à Service-HTTP-1 et que le seuil configuré sur le service est trois. Supposons que les poids suivants soient affectés à chaque moniteur :

- Le poids de Monitor-HTTP-1 est 1.
- Le poids de Monitor-HTTP-2 est de 3.
- Le poids de Monitor-HTTP-3 est de 1.

Le service est marqué UP uniquement si l'un des éléments suivants est vrai :

- Monitor-HTTP-2 est UP.
- Monitor-HTTP-2 et Monitor-HTTP-1 ou Monitor-HTTP-3 sont UP
- Les trois moniteurs sont UP.

Pour définir la valeur de seuil du moniteur sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -monThreshold <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -monThreshold 100
<!--NeedCopy-->
```

Pour définir la valeur de seuil du moniteur sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Seuils et délais d'attente**, puis sélectionnez **Surveiller le seuil**.

Définir une valeur de délai d'attente pour les connexions client inactives

August 20, 2021

Vous pouvez configurer le service avec une valeur de délai d'attente pour mettre fin aux connexions client inactives lorsque le temps configuré s'écoule. Si le client est inactif pendant la période configurée, l'appliance Citrix ADC ferme la connexion client.

Pour définir une valeur de délai d'expiration pour les connexions client inactives à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -cltTimeout <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -cltTimeout 100
<!--NeedCopy-->
```

Pour définir une valeur de délai d'attente pour les connexions client inactives à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Seuils et délais d'attente**, puis sélectionnez **Délai d'attente d'inactivité du client**.

Définir une valeur de délai d'attente pour les connexions au serveur inactif

August 20, 2021

Vous pouvez configurer un service avec une valeur de délai d'expiration pour mettre fin aux connexions de serveur inactives lorsque le temps configuré (en secondes) s'écoule. Si le serveur est inactif pendant la durée configurée, l'appliance Citrix ADC ferme la connexion au serveur.

Pour définir une valeur de délai d'expiration pour les connexions de serveur inactives à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -svrTimeout <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -svrTimeout 100
<!--NeedCopy-->
```

Pour définir une valeur de délai d'expiration pour les connexions de serveur inactives à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Seuils et délais**d'attente et sélectionnez **Délai d'inactivité du serveur**.

Définir une limite sur l'utilisation de la bande passante par les clients

August 20, 2021

Parfois, les serveurs peuvent avoir une bande passante limitée pour gérer les demandes des clients et peuvent être surchargés. Pour éviter la surcharge d'un serveur, vous pouvez spécifier une limite maximale sur la bande passante, en Kbps, traitée par le serveur. L'appliance Citrix ADC transfère les demandes à un serveur à équilibrage de charge uniquement jusqu'à ce que cette limite soit atteinte.

Pour définir une limite de bande passante maximale sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -maxBandwidth <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -maxBandwidth 100
<!--NeedCopy-->
```


Pour définir une limite de bande passante maximale sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Seuils et délais d'attente**et sélectionnez **Bande passante maximale**.

Rediriger les requêtes client vers un cache

August 20, 2021

Vous pouvez configurer un service pour rediriger les demandes client vers un cache et transférer les demandes non mises en cache vers un service choisi par la méthode d'équilibrage de charge configurée.

Pour définir la redirection du cache sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -cacheable <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -cacheable YES
<!--NeedCopy-->
```

Pour définir la redirection du cache sur un service à l'aide de l'interface graphique graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Ouvrez un service et définissez le type de cache.

Conserver l'identificateur VLAN pour la transparence VLAN

August 20, 2021

Vous pouvez configurer un serveur virtuel d'équilibrage de charge pour conserver l'identificateur VLAN du client dans les paquets à transférer aux serveurs. Le serveur virtuel doit être un serveur virtuel générique de type ANY et doit fonctionner en mode MAC.

Pour configurer un serveur virtuel d'équilibrage de charge afin de conserver l'ID VLAN client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour configurer un serveur virtuel d'équilibrage de charge afin de conserver l'ID VLAN client et vérifier la configuration :

```
set lb vserver <name> -m MAC -macmodeRetainvlan ENABLED

show lb vserver <name>
<!--NeedCopy-->
```

> **Remarque**
>
> Pour un service lié à un serveur virtuel sur lequel l' `-m MAC` option est activée, vous devez lier un moniteur non utilisateur.

Pour configurer un serveur virtuel d'équilibrage de charge afin de conserver l'ID VLAN client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**, puis **Conserver l'ID VLAN**.

Configurer la transition automatique de l'état en fonction du pourcentage d'intégrité des services liés

August 20, 2021

Vous pouvez configurer un serveur virtuel d'équilibrage de charge pour qu'il passe automatiquement de l'état UP à l'état DOWN si le pourcentage de services actifs tombe en dessous d'un seuil configuré. Par exemple, si vous liez 10 services à un serveur virtuel d'équilibrage de charge et que vous configurez un seuil de 50 % pour ce serveur virtuel, il passe de HUP à DOWN si six services ou plus sont DOWN. Lorsque le pourcentage d'intégrité dépasse la valeur du seuil, le serveur virtuel revient à l'état UP.

Vous pouvez également activer une alarme SNMP appelée ENTITY-STATE si vous souhaitez que l'appliance Citrix ADC vous avertisse lorsque le pourcentage d'intégrité des services liés entraîne un changement d'état d'un serveur virtuel.

Pour configurer la transition automatique d'état basée sur le pourcentage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une transition automatique d'état pour un serveur virtuel et vérifier la configuration :

```
set lb vserver <name> -healthThreshold <positive_integer>

show lb vserver <name>
<!--NeedCopy-->
```

Pour configurer la transition automatique d'état basée sur le pourcentage à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**et définissez un **seuil de santé**.

Pour activer l'alarme ENTITY-STATE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer l'alarme SNMP ENTITY-STATE et vérifier la configuration :

```
enable snmp alarm ENTITY-STATE

show snmp alarm
<!--NeedCopy-->
```

Pour activer l'alarme ENTITY-STATE à l'aide de l'interface graphique

1. Accédez à **Système > SNMP > Alarmes**.
2. Sélectionnez **ENTITY-STATE** et, dans la liste Action, sélectionnez **Activer**.

Moniteurs intégrés

August 20, 2021

L'appliance Citrix ADC contient divers moniteurs intégrés que vous pouvez utiliser pour surveiller vos services. Ces moniteurs intégrés gèrent la plupart des protocoles courants. Ils offrent des options permettant de modifier certains paramètres, tels que l'intervalle, le délai de réponse pour répondre

à vos besoins. Toutefois, vous ne pouvez pas modifier le nom et le protocole du moniteur. Pour plus d'informations, voir Modification des moniteurs. Vous pouvez également lier un moniteur intégré à un service et le dissocier du service.

> **Remarque**
>
> Vous pouvez créer un moniteur personnalisé basé sur un moniteur intégré. Pour savoir comment créer des moniteurs personnalisés, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des applications basée sur TCP

September 8, 2021

L'appliance Citrix ADC dispose de deux moniteurs intégrés qui surveillent les applications basées sur TCP : `tcp-default` et `ping-default`. Lorsque vous créez un service, le moniteur par défaut approprié lui est automatiquement lié, de sorte que le service peut être utilisé immédiatement s'il est UP. Le moniteur TCP par défaut est lié à tous les services TCP. Le moniteur Ping-Default est lié à tous les services autres que TCP.

Vous ne pouvez pas supprimer ou modifier les moniteurs par défaut. Lorsque vous liez un autre moniteur à un service TCP, le moniteur par défaut n'est pas lié du service. Le tableau suivant répertorie les types de moniteurs, ainsi que les paramètres et les processus de surveillance associés à chaque type.

Type de moniteur	Paramètres spécifiques	Processus
tcp	Sans objet	L'appliance Citrix ADC établit une liaison tridirectionnelle avec la destination du moniteur, puis ferme la connexion. Si l'appliance observe le trafic TCP vers la destination, elle n'envoie pas de demandes de surveillance TCP. Cela se produit si LRTM est désactivé. Par défaut, le LRTM est désactivé sur ce moniteur.

Type de moniteur	Paramètres spécifiques	Processus
http	httpprequest [« HEAD/»] - requête HTTP envoyée au service. respcode [200] - Un ensemble de codes de réponse HTTP est attendu du service.	L'appliance Citrix ADC établit une liaison à trois voies avec la destination du moniteur. Une fois la connexion établie, l'appliance envoie des requêtes HTTP, puis compare le code de réponse avec l'ensemble de codes de réponse configuré.
tcp-ecv	send [« »] - est les données envoyées au service. La longueur maximale autorisée de la chaîne est de 512 octets. Recv [« »] - réponse attendue du service. La longueur maximale autorisée de la chaîne est de 128 octets. Le dernier caractère est la terminaison NULL.	L'appliance Citrix ADC établit une liaison à trois voies avec la destination du moniteur. Lorsque la connexion est établie, l'appliance utilise le paramètre d'envoi pour envoyer des données spécifiques au service et attend une réponse spécifique via le paramètre de réception. Différents serveurs envoient des segments de tailles différentes. Toutefois, le motif doit se situer dans 16 segments TCP.

Type de moniteur	Paramètres spécifiques	Processus
http://ecv	send [« »] - données HTTP envoyées au service ; recv [« »] - données de réponse HTTP attendues du service	L'appliance Citrix ADC établit une liaison à trois voies avec la destination du moniteur. Lorsque la connexion est établie, l'appliance utilise le paramètre d'envoi pour envoyer les données HTTP au service et attend la réponse HTTP spécifiée par le paramètre de réception. (partie du corps HTTP sans en-tête HTTP). Les données de réponse vides correspondent à n'importe quelle réponse. Les données attendues peuvent se trouver n'importe où dans les 24 000 premiers octets du corps HTTP de la réponse.
ping	Non applicable	L'appliance Citrix ADC envoie une demande d'écho ICMP à la destination du moniteur et attend une réponse d'écho ICMP.

Pour configurer des moniteurs intégrés pour des applications basées sur TCP, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Pour configurer des moniteurs basés sur TCP à l'aide de CLI

Exécutez la commande suivante :

```
1 add lb monitor <monitorName> <type> -respCode <int[-int]> -httpRequest
     <string> -resptimeout <integer> [<units>] -retries <integer> -
     downTime <integer> [<units>] -action <action>
2 <!--NeedCopy-->
```

Exemple pour le type de moniteur TCP :


```
add lb monitor Exch2010-RPC-AddressBook TCP -LRTM ENABLED -interval 10
    -resptimeout 5 -destPort 59601
<!--NeedCopy-->
```

Exemple de type de moniteur HTTP :

```
add lb monitor Mon_S4B_FE_2 HTTP -respCode 200 -httpRequest "GET /
    Autodiscover/XFrame/XFrame.html" -LRTM ENABLED -retries 10 -secure
    YES
<!--NeedCopy-->
```

Exemple pour le type de moniteur HTTP-ECV :

```
add lb monitor STM_EXC2016_SSLBridge_MON HTTP-ECV -send "GET /owa/
    healthcheck.htm" -recv "200 OK" -LRTM ENABLED -destPort 443 -secure
    YES
<!--NeedCopy-->
```

Exemple de type de moniteur PING :

```
add lb monitor lbmon-localhost-ping PING -LRTM DISABLED -destIP
    127.0.0.1
<!--NeedCopy-->
```

Surveillance des services SSL

August 20, 2021

L'appliance Citrix ADC dispose de moniteurs sécurisés, TCPS et HTTPS intégrés. Vous pouvez utiliser les moniteurs sécurisés pour surveiller le trafic HTTP et non-HTTP. Pour configurer un moniteur HTTP sécurisé, sélectionnez le type de moniteur comme HTTP, puis définissez l'indicateur sécurisé. Pour configurer un moniteur TCP sécurisé, sélectionnez le type de moniteur en tant que TCP, puis définissez l'indicateur sécurisé. Les moniteurs sécurisés fonctionnent comme suit :

- **Surveillance TCP sécurisée.** L'appliance Citrix ADC établit une connexion TCP. Une fois la connexion établie, l'appliance effectue une liaison SSL avec le serveur. Une fois la poignée de main terminée, l'appliance ferme la connexion.
- **Surveillance HTTP sécurisée.** L'appliance Citrix ADC établit une connexion TCP. Une fois la connexion établie, l'appliance effectue une liaison SSL avec le serveur. Lorsque la connexion SSL est établie, l'appliance envoie des requêtes HTTP sur le canal crypté et vérifie les codes de réponse.

Le tableau suivant décrit les moniteurs intégrés disponibles pour la surveillance des services SSL.

Type de moniteur	Sonde	Critères de réussite (condition directe)
TCP	Connexion TCP ; poignée de main SSL	Connexion TCP réussie établie et liaison SSL réussie.
HTTP	Connexion TCP ; poignée de main SSL ; requête HTTP cryptée	Une connexion TCP réussie est établie, une liaison SSL réussie est effectuée et le code de réponse HTTP attendu dans la réponse HTTP du serveur est crypté.
TCP-ECV	Connexion TCP. Poignée de contact SSL (Les données envoyées à un serveur sont chiffrées.)	Une connexion TCP réussie est établie, une liaison SSL réussie est effectuée et les données TCP attendues sont reçues du serveur.
HTTP-ECV	Connexion TCP ; poignée de main SSL (requête HTTP cryptée)	Une connexion TCP réussie est établie, une liaison SSL réussie est effectuée et les données HTTP attendues sont reçues du serveur.

Exemple de configuration pour le moniteur de vérification de l'état HTTS-ECV

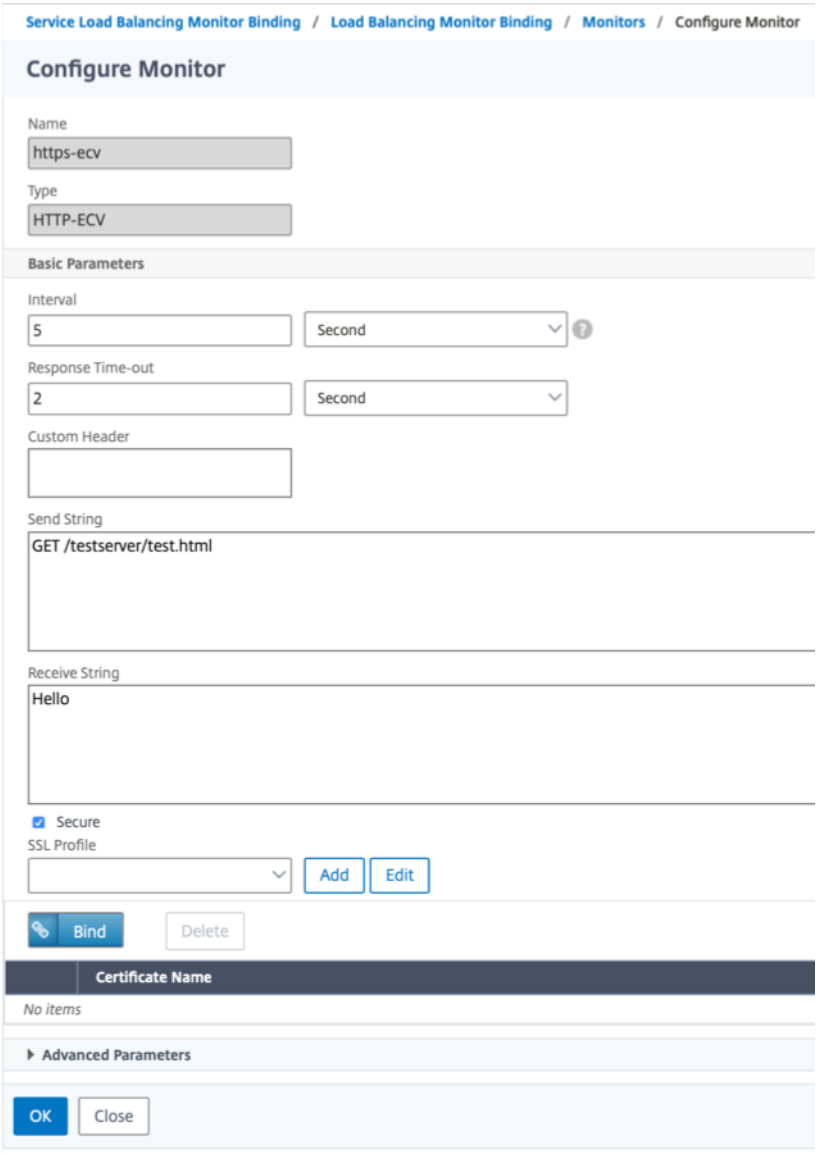
Les services HTTP ont des moniteurs prédéfinis capables de vérifier le contenu étendu (ECV).
Ces moniteurs sont utilisés lorsqu'une validation est requise au-delà d'une connexion TCP réussie.
Ces moniteurs valident le service comme UP, lorsque tous les critères suivants sont remplis :

- Connexion TCP réussie.
- Un type particulier de demande doit être généré.
- Un message spécifique est attendu en réponse de la **chaîne de réception**.

Pour ces moniteurs, une chaîne de requête est configurée avec une chaîne de réponse. Si la chaîne de réponse reçue par le moniteur Citrix ADC correspond à la chaîne configurée, le service est marqué UP.

Liez un moniteur à un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, créez un service et spécifiez le protocole comme **SSL**. Cliquez sur **OK**.
2. Cliquez dans le volet **Liaison du moniteur Service à équilibrage** de charge, puis cliquez sur **Ajouter une liaison** .
3. Choisissez le type de moniteur comme **HTTPS-ECV** et cliquez sur **Modifier** .
4. Dans le volet **Configurer le moniteur** sous l'onglet **Paramètres de base**, entrez des valeurs pour les paramètres suivants :
   - **Send String** — Chaîne que le moniteur doit envoyer au service.
   - **Chaîne de réception** — Chaîne que le moniteur doit recevoir pour marquer le service comme UP.



5. Cliquez sur **OK** pour terminer la configuration du moniteur.
6. Cliquez sur **Sélectionner**.
7. Cliquez sur **Bind** pour lier le moniteur **HTTS-ECV** au service.
8. Cliquez sur **Fermer**.

Liez un moniteur à un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind service <servicename> -monitorName https-ecv
<!--NeedCopy-->
```

Exemple :

```
bind services1 -monitorName https-ecv
<!--NeedCopy-->
```

Surveillance du service HTTP/2

August 20, 2021

L'appliance Citrix ADC prend en charge les moniteurs HTTP/2 pour surveiller l'état de santé des services HTTP/2.

Le moniteur HTTP/2 peut être configuré de deux manières différentes. Selon le type de trafic, vous pouvez configurer un moniteur HTTP/2.

- **HTTP/2 Direct.** Vous pouvez configurer HTTP/2 Direct pour surveiller les services HTTP/2 non sécurisés.
- **HTTP/2 SSL.** Vous pouvez configurer SSL HTTP/2 pour surveiller le trafic sécurisé via SSL. Activez le paramètre Secure Flag dans le HTTP/2 pour surveiller le trafic SSL.

Le http2direct et http2ssl sont les deux moniteurs intégrés différents pris en charge par le protocole HTTP/2.

Le tableau suivant répertorie les types de configuration et les processus de surveillance associés à chaque type.

Type de configuration	Sonde	Les critères de succès
HTTP/2 Direct	Connexion TCP ; préface de connexion HTTP2 et négociation des paramètres ; demande HTTP2	Le code d'état de réponse HTTP/2 doit correspondre au code de réponse configuré.
HTTP/2 SSL	Connexion TCP ; Handshake SSL ; préface de connexion HTTP2 & Négociation des paramètres ; demande HTTP2	Le serveur doit toujours sélectionner ALPN avec le protocole HTTP/2 et le code d'état de réponse HTTP/2 doit correspondre au code de réponse configuré.

Liez le moniteur HTTP/2 à un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `bind service <servicename> -monitorName <name>`
- `bind service <servicename> -monitorName <name>`

Exemple :

- `bind service s1 -monitorName http2direct`
- `bind service s2 -monitorName http2ssl`

Surveillance du service de protocole proxy

August 20, 2021

L'appliance Citrix ADC avec protocole proxy prend en charge la vérification du moniteur. La vérification du moniteur garantit que le serveur principal prend également en charge le protocole proxy. L'appliance Citrix ADC dispose de quatre types de moniteurs intégrés pour les services associés HTTP ou TCP : HTTP, HTTPS, HTTP-ECV et TCP-ECV.

Le tableau suivant répertorie les types de moniteurs, ainsi que les paramètres et les processus de surveillance associés à chaque type.

Type de configuration	Sonde	Les critères de succès
HTTP	`httprequest` [« HEAD/»] - requête HTTP envoyée au service. `respcode` [200] - Un ensemble de codes de réponse HTTP est attendu du service.	L'appliance Citrix ADC établit une liaison à trois voies avec la destination du moniteur. Une fois la connexion établie, l'appliance envoie des requêtes HTTP, puis compare le code de réponse avec l'ensemble de codes de réponse configuré.
HTTPS	`httprequest` [« HEAD/»] - Demande HTTPS envoyée au service. `respcode` [200] - Un ensemble de codes de réponse HTTPS est attendu du service.	L'appliance Citrix ADC établit une liaison à trois voies avec la destination du moniteur. Une fois la connexion établie, l'appliance envoie des requêtes HTTPS, puis compare le code de réponse à l'ensemble de codes de réponse configuré.
HTTP-ECV	send [» »] - données HTTP envoyées au service. Reçu [» »] : données de réponse HTTP attendues du service	L'appliance Citrix ADC établit une liaison à trois voies avec la destination du moniteur. Lorsque la connexion est établie, l'appliance utilise le paramètre send pour envoyer les données HTTP au service et attend la réponse HTTP spécifiée par le paramètre receive. (partie du corps HTTP sans inclure les en-têtes HTTP). Les données de réponse vides correspondent à n'importe quelle réponse. Les données attendues peuvent se trouver n'importe où dans les 24 000 premiers octets du corps HTTP de la réponse.

Type de configuration	Sonde	Les critères de succès
TCP-ECV	send [» »] - données qui sont envoyées au service. La longueur maximale autorisée de la chaîne est de 512 K octets. reçu [» »] - réponse attendue du service. La longueur maximale autorisée de la chaîne est de 128 K octets.	L'appliance Citrix ADC établit une liaison à trois voies avec la destination du moniteur. Lorsque la connexion est établie, l'appliance utilise le paramètre send pour envoyer des données spécifiques au service et attend une réponse spécifique via le paramètre receive. Différents serveurs envoient des segments de différentes tailles. Toutefois, le motif doit se situer dans 16 segments TCP.

Vous pouvez configurer le moniteur de protocole proxy à l'aide de `netprofile`.

Configuration du moniteur de protocole proxy à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

1. Ajouter un profil réseau avec le protocole proxy activé

   ```
   add netprofile <name> -proxyProtocol ( ENABLED | DISABLED )
   ```

Exemple :

```
1 add netprofile profile1 - proxyProtocol ENABLED
```

1. Liez le profil réseau à un service.

   ```
   set service <name> -netprofile <netprofile-name>
   ```

Exemple :

```
1 set service S1 - netprofile profile1
```

> **Remarque**

> Vous pouvez exécuter la commande précédente si vous souhaitez que le profil réseau soit lié à un service.

1. Liez le profil net à un moniteur.

```
set lb monitor <monitor-name> <type> -netprofile <netprofile-name>
```

Exemple :

```
1 set lb monitor http1 HTTPS  - netprofile profile1
```

> **Remarque**
>
> - Vous pouvez exécuter la commande précédente si vous souhaitez que le profil réseau soit lié à un moniteur.
> - Vous pouvez sélectionner le type de moniteur de votre choix. Il peut s'agir de HTTP, HTTPS, TCP-ECV ou HTTP-ECV.
>
> **Important**
>
> - Dans un cas général, le profil réseau (protocole proxy activé) lié à un service est pris en compte.
> - Si le profil réseau est lié à la fois au moniteur et au service, le profil net lié à la surveillance est pris en compte. Le profil réseau lié au service est ignoré.

Surveillance des services FTP

August 20, 2021

Pour surveiller les services FTP, l'appliance Citrix ADC ouvre deux connexions au serveur FTP. Il se connecte d'abord au port de contrôle, qui est utilisé pour transférer des commandes entre un client et un serveur FTP. Après avoir reçu la réponse attendue, il se connecte au port de données, qui est utilisé pour transférer des fichiers entre un client et un serveur FTP. Seulement lorsque le serveur FTP répond comme prévu, sur les deux connexions, il est marqué UP.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

L'appliance Citrix ADC dispose de deux moniteurs intégrés pour les services FTP : le moniteur FTP et le moniteur FTP-EXTENDED. Le moniteur FTP-EXTENDED est un moniteur scriptable. Il utilise le script nsftp.pl. Le script de moniteur FTP-EXTENDED est amélioré pour envoyer des sondes sécurisées aux services FTP. Vous pouvez créer un moniteur de type FTP-EXTENDED. Le script nsftp.pl est automatiquement extrait du répertoire par défaut.

Pour envoyer des sondes FTP sécurisées aux services FTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lb monitor <monitorName> <type> -username <string> -password <
     string> -filename <filename>
2 <!--NeedCopy-->
```

Exemple

```
1 add monitor mon1 FTP-EXTENDED -username root -password freebsd -
     filename fsdf
2 <!--NeedCopy-->
```

Pour envoyer des sondes FTP sécurisées aux services FTP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**.
2. Spécifiez le type de moniteur comme **FTP-EXTENDED**et définissez les paramètres.
3. Dans **Paramètres spéciaux**, spécifiez un nom de **fichier, un nomd'utilisateur**et un**mot de passe**.

Pour configurer des moniteurs intégrés afin de vérifier l'état des services FTP, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance sécurisée des serveurs à l'aide de SFTP

August 20, 2021

Un script utilisateur 'nssftp.pl'est ajouté pour prendre en charge la surveillance SFTP (SSH File Transfer Protocol). Il est disponible dans la liste actuelle des moniteurs utilisateur Citrix ADC intégrés et se trouve dans le répertoire /netscaler/moniteurs. Le moniteur SFTP utilise le nom d'utilisateur et le mot de passe spécifiés pour vérifier si le fichier est présent sur le serveur.

Pour configurer la surveillance sécurisée à l'aide de SFTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
1 add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
    string> -secure ( YES | NO )
2 <!--NeedCopy-->
```

Exemple :

```
1 add monitor SFTP_MON USER -scriptname nssftp.pl -scriptargs "file=
    example.txt;user=sam;password=sam_passwd"
2 <!--NeedCopy-->
```

Pour configurer la surveillance sécurisée à l'aide de SFTP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs** et dans **Type**, spécifiez **USER** .
2. Dans **Paramètres spéciaux**, dans **Nom du script**, sélectionnez nssftp.pl.
3. Spécifiez les **arguments de script**.

Définir les paramètres SSL sur un moniteur sécurisé

August 20, 2021

> **Important**
>
> Cette fonctionnalité est prise en charge uniquement sur les nouveaux profils par défaut. Pour plus d'informations sur ces profils, consultez Présentation de l'infrastructure des profils SSL améliorés.

Un moniteur hérite des paramètres globaux ou du service auquel il est lié. Si un moniteur est lié à un service non SSL ou non SSL_TCP, tel que SSL_BRIDGE, vous ne pouvez pas le configurer avec des paramètres SSL tels que la version du protocole ou les chiffrements à utiliser. Par conséquent, si votre déploiement nécessite une surveillance SSL des serveurs back-end, la surveillance est inefficace.

Vous pouvez avoir plus de contrôle sur la surveillance basée sur SSL des serveurs back-end, en liant un profil SSL à un moniteur. Un profil SSL contient des paramètres SSL, des liaisons chiffrées et des liaisons ECC. Par exemple, vous pouvez définir l'authentification du serveur, les chiffrements et la version du protocole dans un profil SSL et lier le profil à un moniteur. Pour effectuer l'authentification du serveur, vous devez également lier un certificat d'autorité de certification à un moniteur. Pour effectuer l'authentification du client, vous devez lier un certificat client au moniteur. De nouveaux paramètres pour la commande « bind lb monitor » vous permettent de le faire.

> **Remarque**
>
> Les paramètres SSL ne prennent effet que si vous ajoutez un moniteur sécurisé. En outre, le type de profil SSL doit être **BackEnd**.

Types de surveillance prenant en charge les profils SSL

Les profils SSL peuvent être liés aux types de moniteurs suivants :

- HTTP
- HTTP-ECV
- TCP
- TCP-ECV
- HTTP-INLINE

Pour spécifier un profil SSL lors de l'ajout d'un moniteur à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
add lb monitor <monitorName> <type> -secure  YES   -sslprofile <string>

set lb monitor <monitorName> <type> -secure YES -sslprofile <string>
<!--NeedCopy-->
```

Exemple :

```
add ssl profile prof1 -sslProfileType  BackEnd

add lb monitor mon1 HTTP -secure  YES -sslprofile prof1
<!--NeedCopy-->
```

Pour lier une paire de clés de certificat à un moniteur à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
bind monitor  <monitor name> -certkeyName <string>  [(-CA  [-crlCheck (
    Mandatory | Optional ) | -ocspCheck ( Mandatory | Optional )]
<!--NeedCopy-->
```


Surveillance des services SIP

August 20, 2021

Un contrôleur de Citrix ADC dispose de deux moniteurs intégrés que vous pouvez utiliser pour surveiller les services SIP : les moniteurs **SIP-UDP** et **SIP-TCP** . Un moniteur SIP vérifie périodiquement le service SIP auquel le moniteur SIP est lié, en envoyant des méthodes de demande SIP au service SIP. Si le service SIP répond avec un code de réponse, le moniteur marque le service comme UP. Si le service SIP ne répond pas ou ne répond pas correctement, il est marqué comme DOWN.

Paramètre	Spécifie
sipURI	Schéma d'adressage SIP du serveur SIP.
`sipmethod`	Type de demande SIP utilisée pour sonder le service SIP. Spécifiez l'une des méthodes suivantes : INVITE, OPTION (valeur par défaut), REGISTER
`respcode`	Code de réponse SIP avec lequel le service SIP répond à la demande de sonde. Par défaut : 200.

Surveillance des services RADIUS

August 20, 2021

Le moniteur RADIUS de l'appliance Citrix ADC vérifie périodiquement l'état du service RADIUS auquel il est lié en envoyant une demande d'authentification au service. Le serveur RADIUS authentifie le moniteur RADIUS et envoie une réponse. Par défaut, le moniteur s'attend à recevoir un code de réponse 2, la réponse Access-Accept par défaut, du serveur RADIUS. Tant que le moniteur reçoit la réponse appropriée, il marque le service UP.

Remarque : le moniteur RADIUS ne prend en charge que l'authentification de type PAP.

- Si le client s'est authentifié correctement, le serveur RADIUS envoie une réponse Access-Accept. Le code de réponse d'acceptation d'accès par défaut est 2 et il s'agit du code utilisé par l'appliance.
- Si le client ne parvient pas à s'authentifier correctement (par exemple lorsqu'il y a une incompatibilité entre le nom d'utilisateur, le mot de passe ou la clé secrète), le serveur RADIUS envoie une réponse Access-Rejeter. Le code de réponse accès-rejet par défaut est 3, et il s'agit du code

utilisé par l'appliance.

Paramètre	Spécifie
`userName`	Nom d'utilisateur sur le serveur RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3. Ce nom d'utilisateur est utilisé dans la sonde.
Mot de passe	Mot de passe utilisé dans la surveillance des serveurs RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP.
radKey	Valeur de clé secrète partagée utilisée par le serveur RADIUS lors de l'authentification du client.
radNASid	ID NAS-ID qui est encapsulé dans la charge utile lorsqu'une demande d'accès est effectuée.
radNASip	Adresse IP encapsulée dans la charge utile lorsqu'une requête d'accès est effectuée. Lorsque radNASip n'est pas configuré, l'appliance Citrix ADC envoie l'adresse IP mappée (MIP) au serveur RADIUS en tant qu'adresse IP NAS.

Pour surveiller un service RADIUS, vous devez configurer le serveur RADIUS auquel il est lié comme suit :

1. Ajoutez le nom d'utilisateur et le mot de passe du client que le moniteur utilise pour l'authentification à la base de données d'authentification RADIUS.
2. Ajoutez l'adresse IP et la clé secrète du client à la base de données RADIUS appropriée.
3. Ajoutez les adresses IP utilisées par l'appliance pour envoyer des paquets RADIUS à la base de données RADIUS. Si l'appliance Citrix ADC possède plusieurs adresses IP mappées ou si une adresse IP de sous-réseau (SNIP) est utilisée, vous devez ajouter la même clé secrète pour toutes les adresses IP.

   Attention : Si l'adresse IP utilisée par l'appliance n'est pas ajoutée à la base de données RADIUS, le serveur RADIUS rejette tous les paquets.

Pour configurer des moniteurs intégrés afin de vérifier l'état du serveur RADIUS, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveiller la diffusion des informations comptables à partir d'un serveur RADIUS

August 20, 2021

Vous pouvez configurer un moniteur appelé moniteur de *comptabilité RADIUS* pour déterminer si le serveur RADIUS utilisé pour l'authentification, l'autorisation et la comptabilité (Citrix ADC AAA) fournit des informations comptables comme prévu. Le moniteur est de type RADIUS_ACCOUNTING. La sonde est générée par un script Perl appelé nsbmradius.pl, situé dans le répertoire /nsconfig/monitors/. Le script envoie des sondes de demande de comptabilité successives au serveur RADIUS. La sonde n'est considérée comme réussie que si le serveur de comptabilité RADIUS répond avec un paquet dont le champ Code est défini sur 5, ce qui, selon la RFC 2866, indique un paquet Accounting-Response.

Lors de la configuration d'un moniteur de comptabilité RADIUS, vous devez spécifier une clé secrète. Vous pouvez spécifier des paramètres facultatifs, chacun représentant un attribut RADIUS, tel que Acct-Status-Type et Framed-IP-Address. Pour plus d'informations sur ces attributs, voir RFC 2865, « Remote Authentication Dial In User Service (RADIUS) » et RFC 2866, "RADIUS Accounting."

Pour configurer un moniteur de comptabilité RADIUS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur comptable RADIUS et vérifier la configuration :

```
add lb monitor <monitorName> RADIUS_ACCOUNTING [-userName <string>] {
 -password  }
  {
 -radKey  }
  [-radNASip <ip_addr>] [-radAccountType <positive_integer>] [-
     radFramedIP <ip_addr>] [-radAPN <string>] [-radMSISDN <string>] [-
     radAccountSession <string>]

show lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple

```
add lb monitor radAccntMon RADIUS_ACCOUNTING -radKey "8d#>9jr4rV)L7%a2-
   zW13sM"
<!--NeedCopy-->
```


Surveillance des services DNS et DNS-TCP

August 20, 2021

L'appliance Citrix ADC dispose de deux moniteurs intégrés qui peuvent être utilisés pour surveiller les services DNS : DNS et DNS-TCP. Lorsqu'il est lié à un service, l'un ou l'autre contrôle vérifie périodiquement l'état de ce service DNS en lui envoyant une requête DNS. La requête se résout à une adresse IPv4 ou IPv6. Cette adresse IP est ensuite vérifiée par rapport à la liste des adresses IP de test que vous configurez. La liste peut contenir jusqu'à cinq adresses IP. Si l'adresse IP résolue correspond à au moins une adresse IP de la liste, le service DNS est marqué comme étant mis en valeur. Si l'adresse IP résolue ne correspond à aucune adresse IP de la liste, le service DNS est marqué comme étant hors service.

Paramètre	Description
requête	Requête DNS (nom de domaine) envoyée au service DNS surveillé. Valeur par défaut : « \ 007 » Si la requête DNS réussit, le service est marqué comme UP. Sinon, il est marqué comme DOWN. Pour un moniteur inversé, si la requête DNS réussit, le service est marqué comme DOWN. Sinon, il est marqué comme UP. Si aucune réponse n'est reçue, le service est marqué comme étant DOWN.
queryType	Type de requête DNS envoyée. Valeurs possibles : Adresse, Zone.
`IPAddress`	Liste des adresses IP vérifiées par rapport à la réponse à la sonde de surveillance DNS.
IPv6	Activez cette case à cocher si l'adresse IP utilise le format IPv6.

Pour configurer les moniteurs DNS ou DNS-TCP intégrés, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des services LDAP

August 20, 2021

L'appliance Citrix ADC dispose d'un moniteur intégré qui peut être utilisé pour surveiller les services LDAP : le moniteur LDAP. Il vérifie périodiquement le service LDAP auquel il est lié en s'authentifiant et en lui envoyant une requête de recherche. Si la recherche réussit, le service est marqué UP. Si le serveur LDAP ne trouve pas l'entrée, un message d'échec est envoyé au moniteur LDAP et le service est marqué comme DOWN.

Configurez le moniteur LDAP pour définir la recherche qu'il doit effectuer lors de l'envoi d'une requête. Vous pouvez utiliser le paramètre DN de base pour spécifier un emplacement dans la hiérarchie d'annuaires où le serveur LDAP doit démarrer la requête de test. Vous pouvez utiliser le paramètre Attribute pour spécifier un attribut de l'entité cible.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Paramètre	Spécifie
baseDN	Nom de base du moniteur LDAP à partir duquel la recherche LDAP doit commencer. Si le serveur LDAP s'exécute localement, la valeur par défaut de base est dc=`netscaler`, dc=com.
bindDN	Nom BDN du moniteur LDAP.
filtre	Filtre pour le moniteur LDAP. Utilisez le paramètre de filtre dans une requête pour limiter le nombre de résultats. Si vous ne spécifiez pas ce paramètre dans la requête, le filtre s'applique à l'ensemble de la classe d'objets, ce qui peut s'avérer coûteux, comme une utilisation élevée du processeur.
Mot de passe	Mot de passe utilisé pour surveiller les serveurs LDAP.
attribut	Attribut du moniteur LDAP.

Pour configurer le moniteur LDAP intégré, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des services MySQL

August 20, 2021

L'appliance Citrix ADC dispose d'un moniteur intégré qui peut être utilisé pour surveiller les services MySQL : le moniteur MySQL. Il vérifie périodiquement le service MySQL auquel il est lié en lui envoyant une requête de recherche. Si la recherche réussit, le service est marqué UP. Si le serveur MySQL ne répond pas ou si la recherche échoue, un message d'échec est envoyé au moniteur MySQL et le service est marqué comme DOWN.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Paramètre	Spécifie
base de données	Base de données utilisée pour le moniteur MySQL.
sqlQuery	Requête SQL utilisée pour le moniteur MySQL.

Pour configurer un moniteur MySQL intégré, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Pour configurer des moniteurs MySQL à l'aide de la CLI

Exécutez la commande suivante :

```
1 add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
     string>
2 <!--NeedCopy-->
```

Exemple :

```
1 add lb monitor mysql1 USER -scriptName nsmysql.pl -scriptArgs "database
     =cloud;user=cloud;password=password;query=show tables from cloud"
2 <!--NeedCopy-->
```

Surveillance des services SNMP

January 21, 2021

L'appliance Citrix ADC dispose d'un moniteur intégré qui peut être utilisé pour surveiller les services SMNP : le moniteur SNMP. Il vérifie périodiquement l'agent SNMP sur le service auquel il est lié en envoyant une requête pour l'ID d'identification d'entreprise (OID) que vous configurez pour la surveillance. Si la requête réussit, le service est marqué UP. Si le service SNMP trouve l'OID que vous avez

spécifié, la requête réussit et le moniteur SNMP marque le service UP. S'il ne trouve pas l'OID, la requête échoue et le moniteur SNMP marque le service DOWN.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Paramètre	Spécifie
SNMPOID	OID utilisé pour le moniteur SNMP.
snmpCommunity	Communauté utilisée pour le moniteur SNMP.
snmpThreshold	Seuil utilisé pour le moniteur SNMP.
snmpVersion	Version SNMP utilisée pour la surveillance de la charge. Valeurs possibles : V1, V2.

Pour configurer le moniteur SNMP intégré, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des services NNTP

August 20, 2021

L'appliance Citrix ADC dispose d'un moniteur intégré qui peut être utilisé pour surveiller les services NNTP : le moniteur NNTP. Il vérifie périodiquement le service NNTP auquel il est lié en se connectant au service et en vérifiant l'existence du groupe de discussion que vous spécifiez. Si le groupe de discussion existe, la recherche réussit et le service est marqué UP. Si le service NNTP ne répond pas ou si la recherche échoue, le service est marqué comme DOWN.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Le moniteur NNTP peut également être configuré pour publier un message de test dans le groupe de discussion.

Paramètre	Spécifie
`userName`	Nom d'utilisateur sur le serveur RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3. Ce nom d'utilisateur est utilisé dans la sonde.
Mot de passe	Mot de passe utilisé dans la surveillance des serveurs RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP.

Paramètre	Spécifie
groupe	Nom du groupe à interroger pour le moniteur NNTP.

Pour configurer le moniteur NNTP intégré, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des services POP3

August 20, 2021

L'appliance Citrix ADC dispose d'un moniteur intégré qui peut être utilisé pour surveiller les services POP3 : le moniteur POP3. Il vérifie périodiquement le service POP3 auquel il est lié en ouvrant une connexion avec un serveur POP3. Si le serveur POP3 répond avec les codes de réponse corrects dans la période configurée, il marque le service UP. Si le service POP3 ne répond pas ou ne répond pas correctement, il marque le service comme DOWN.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Paramètre	Spécifie
userName	Nom d'utilisateur serveur POP3. Ce nom d'utilisateur est utilisé dans la sonde.
Mot de passe	Mot de passe utilisé dans la surveillance des serveurs POP3.
Nom du script	Chemin d'accès et nom du script à exécuter.
dispatcherIP	Adresse IP du répartiteur auquel la sonde est envoyée.
dispatcherPort	Port du répartiteur vers lequel la sonde est envoyée.

Pour configurer le moniteur POP3 intégré, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Pour configurer des moniteurs POP3 à l'aide de CLI

Exécutez la commande suivante :


```
1 add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
     string>
2 <!--NeedCopy-->
```

Exemple :

```
1 add lb monitor pop31 USER -scriptName nspop3.pl -scriptArgs "user=
     test@lbmon1.net;password=Freebsd123"
2
3 <!--NeedCopy-->
```

Surveillance des services SMTP

August 20, 2021

L'appliance Citrix ADC dispose d'un moniteur intégré qui peut être utilisé pour surveiller les services SMTP : le moniteur SMTP. Le moniteur vérifie le service SMTP auquel il est lié en ouvrant une connexion avec lui et en effectuant une série de poignées de main pour s'assurer que le serveur fonctionne correctement. Si le service SMTP termine correctement les poignées de main, le moniteur marque le service UP. Sinon, si le service SMTP ne répond pas ou ne répond pas correctement, il marque le service DOWN.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Paramètre	Spécifie
Nom du script	Le chemin et le nom du script à exécuter.
dispatcherIP	Adresse IP du répartiteur auquel la sonde est envoyée.
dispatcherPort	Port du répartiteur vers lequel la sonde est envoyée.

Pour configurer le moniteur SMTP intégré, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des services RTSP

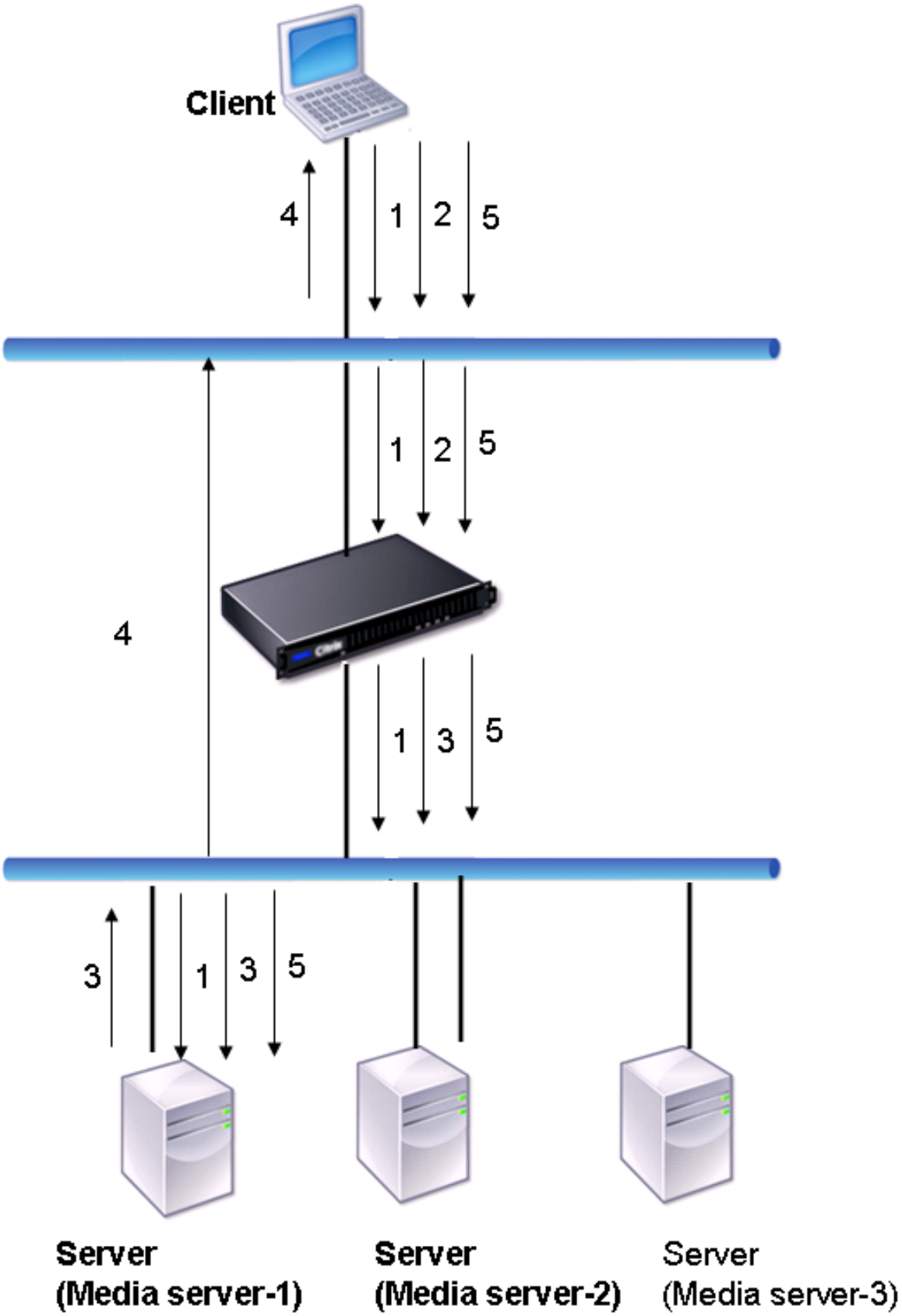
January 21, 2021

L'appliance Citrix ADC dispose d'un moniteur intégré qui peut être utilisé pour surveiller les services RTSP : le moniteur RTSP. Il vérifie périodiquement le service RTSP auquel il est lié en ouvrant une connexion avec le serveur RTSP équilibré de charge. Le type de connexion qu'il ouvre et la réponse qu'il attend diffèrent en fonction de la configuration du réseau. Si le service RTSP répond comme prévu dans la période configurée, il marque le service UP. Si le service ne répond pas ou ne répond pas correctement, il marque le service comme DOWN.

L'appliance Citrix ADC peut être configurée pour équilibrer la charge des serveurs RTSP à l'aide de deux topologies : NAT Off et NAT ON. Les serveurs RTSP envoient leurs réponses directement au client, en contournant l'appliance. L'appliance doit être configurée pour surveiller les services RTSP différemment en fonction de la topologie utilisée par votre réseau. L'appliance peut être déployée en mode Inline ou Non-Inline en mode Nat-Off et Nat-On.

En mode NAT Off, l'appliance fonctionne comme un routeur : elle reçoit les demandes RTSP du client et les achemine vers le service qu'elle sélectionne à l'aide de la méthode d'équilibrage de charge configurée. Si vos serveurs RTSP à équilibrage de charge se voient attribuer des noms de domaine complets accessibles au public dans DNS, les serveurs à équilibrage de charge envoient leurs réponses directement au client, en contournant l'appliance. La figure suivante illustre cette configuration.

Figure 1. RTSP en mode Nat-Off



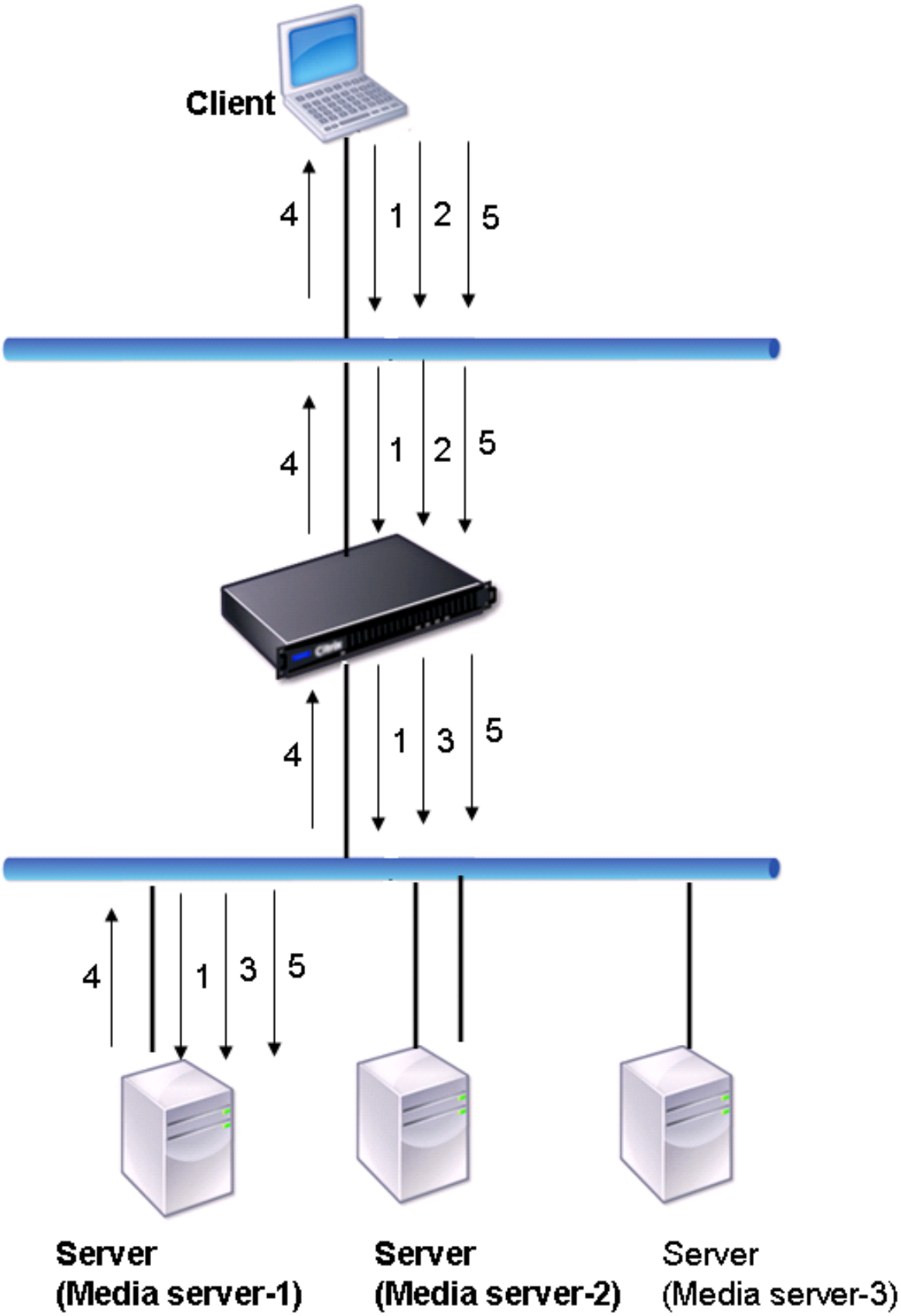
Le flux des demandes et des réponses dans ce scénario est le suivant :

1. Le client envoie une requête DESCRIBE à l'appliance. L'appliance utilise la méthode d'équilibrage de charge configurée pour choisir un service et achemine la demande vers Media Server-1.
2. Le client envoie une demande SETUP à l'appliance. Si l'ID de session RTSP est échangé dans la requête DESCRIBE, l'appliance, à l'aide de la persistance RTSPSID, achemine la demande vers Media Server-1. Si l'ID de session RTSP est échangé dans la demande SETUP, l'appliance effectue l'une des opérations suivantes :
   - Si la requête RTSP vient sur la même connexion TCP, elle achemine la requête vers Media Server-1, en conservant la persistance.
   - Si la demande arrive sur une connexion TCP différente, elle utilise la méthode d'équilibrage de charge configurée pour choisir un service et envoie la demande à ce service, sans maintenir la persistance. Cela signifie que la demande peut être envoyée à un autre service.
3. Media Server-1 reçoit la demande SETUP de l'appliance, alloue des ressources pour traiter la demande RTSP et envoie l'ID de session approprié au client.

   Remarque : l'appliance n'effectue pas NAT pour identifier la connexion RTSP, car les connexions RTSP la contournent.
4. Pour les demandes suivantes, le client utilise ensuite l'ID de session pour identifier la session et envoyer des messages de contrôle au serveur multimédia. Media Server-1 effectue les actions demandées, telles que lecture, avance ou rembobinage.

En mode NAT, l'appliance reçoit les demandes RTSP du client et les achemine vers le serveur de médias approprié à l'aide de la méthode d'équilibrage de charge configurée. Le serveur de médias envoie ensuite ses réponses au client via l'appliance, comme illustré dans le diagramme suivant.

Figure 2. RTSP en mode NAT



Le flux des demandes et des réponses dans ce scénario est le suivant :

1. Le client envoie une requête DESCRIBE à l'appliance. L'appliance utilise la méthode d'équilibrage de charge configurée pour choisir un service et achemine la demande vers Media Server-1.
2. Le client envoie une demande SETUP à l'appliance. Si l'ID de session RTSP est échangé dans la requête DESCRIBE, l'appliance, à l'aide de la persistance RTSPSID, achemine la demande vers Media Server-1. Si l'ID de session RTSP est échangé dans la demande SETUP, l'appliance effectue l'une des opérations suivantes :
   - Si la requête RTSP vient sur la même connexion TCP, elle achemine la requête vers Media Server-1, en conservant la persistance.
   - Si la demande arrive sur une connexion TCP différente, elle utilise la méthode d'équilibrage de charge configurée pour choisir un service et envoie la demande à ce service, sans maintenir la persistance. Cela signifie que la demande peut être envoyée à un autre service.
3. Media Server-1 reçoit la demande SETUP de l'appliance, alloue des ressources pour traiter la demande RTSP et envoie l'ID de session approprié au client.
4. L'appliance effectue NAT pour identifier le client pour les connexions de données RTSP, et les connexions RTSP passent par l'appliance et sont routées vers le client approprié.
5. Pour les demandes suivantes, le client utilise ensuite l'ID de session pour identifier la session et envoyer des messages de contrôle à l'appliance. L'appliance utilise la persistance RTSPSID pour identifier le service approprié et achemine la demande vers Media Server-1. Media Server-1 effectue l'action demandée, telle que lecture, avance ou rembobinage.

Le moniteur RTSP utilise le protocole RTSP pour évaluer l'état des services RTSP. Le moniteur RTSP se connecte au serveur RTSP et effectue une séquence de poignées de main pour s'assurer que le serveur fonctionne correctement.

Paramètre	Spécifie
rtspRequest	Chaîne de requête RTSP envoyée au serveur RTSP (par exemple, OPTIONS *). La valeur par défaut est 07. La longueur de la demande ne doit pas dépasser 163 caractères.
respCode	Ensemble de codes de réponse attendus du service.

Pour obtenir des instructions sur la configuration d'un moniteur RTSP, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance du service XML Broker

August 20, 2021

L'appliance Citrix ADC dispose d'un type de moniteur intégré, CITRIX-XML-SERVICE, avec lequel vous pouvez créer des moniteurs pour surveiller les services XML Broker. Les services XML Broker sont utilisés par Citrix XenApp. Le moniteur ouvre une connexion au service et sonde périodiquement les services XML auxquels il est lié. Si le serveur répond comme prévu dans la période configurée, le moniteur marque le service UP. Si le service ne répond pas ou ne répond pas correctement, le moniteur marque le service comme DOWN.

Pour configurer un moniteur CITRIX-XML-SERVICE, vous devez spécifier le nom de l'application en plus de définir les paramètres standard. Le nom de l'application est le nom de l'application qui doit être exécutée pour surveiller l'état du service XML Broker. L'application par défaut est le Bloc-notes.

Pour configurer des moniteurs pour XML Broker Services, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

> **Remarque**
>
> Le paramètre « Nom de l'application » du moniteur Citrix-XML Service n'est pas valide pour XenApp et Citrix Virtual Desktops versions 7 et ultérieures. Il est recommandé de ne pas utiliser ce paramètre dans XA/XD 7. Si vous configurez ce paramètre, ce paramètre n'est pas utilisé en interne. Le critère de sondage est différent à partir de XA/XD 7. Cependant, vous pouvez utiliser les paramètres « Nom de l'application » dans les versions antérieures à XA/XD 7.

Surveillance des demandes ARP

August 20, 2021

L'appliance Citrix ADC dispose d'un moniteur intégré qui peut être utilisé pour surveiller les demandes ARP : le moniteur ARP. Ce moniteur envoie périodiquement une demande ARP au service auquel il est lié et écoute la réponse attendue. S'il reçoit la réponse attendue, il marque le service UP. S'il ne reçoit aucune réponse ou la mauvaise réponse, il marque le service DOWN.

ARP localise une adresse matérielle pour un serveur à équilibrage de charge lorsque seule l'adresse de la couche réseau est connue. ARP est compatible avec IPv4 pour traduire les adresses IP en adresses MAC Ethernet. La surveillance ARP n'est pas pertinente pour les réseaux IPv6 et n'est donc pas prise en charge sur ces réseaux.

Il n'y a pas de paramètres spéciaux pour le moniteur ARP.

Pour obtenir des instructions sur la configuration d'un moniteur ARP, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance du service XenDesktop Delivery Controller

August 20, 2021

Dans la virtualisation des postes de travail, l'appliance Citrix ADC peut être utilisée pour équilibrer la charge des serveurs WI et XenDesktop Delivery Controller déployés par l'environnement Citrix XenDesktop. L'appliance Citrix ADC fournit un moniteur intégré, `CITRIX-XD-DDC` un moniteur qui surveille les serveurs XenDesktop Delivery Controller. En plus de la vérification de l'état, vous pouvez également vérifier si la sonde est envoyée par un utilisateur valide du serveur XenDesktop Delivery Controller.

Le moniteur envoie une sonde au serveur XenDesktop Delivery Controller sous la forme d'un message XML. Si le serveur répond à la sonde avec l'identité de la batterie de serveurs, la sonde est considérée comme réussie et l'état du serveur est marqué comme UP. Si la réponse HTTP n'a pas de code de réussite ou si l'identité de la batterie de serveurs n'est pas présente dans la réponse, la sonde est considérée comme un échec et l'état du serveur est marqué comme DOWN.

L'option Valider les informations d'identification détermine la sonde à envoyer par le moniteur au serveur XenDesktop Delivery Controller, c'est-à-dire s'il faut demander uniquement le nom du serveur ou valider également les informations d'identification de connexion.

Remarque : Que les informations d'identification de l'utilisateur (nom d'utilisateur, mot de passe et domaine) soient spécifiées sur le `CITRIX-XD-DDC` moniteur, le serveur XenDesktop Delivery Controller ne valide les informations d'identification de l'utilisateur que si l'option de validation des informations d'identification est activée sur le moniteur.

Si vous utilisez l'assistant pour configurer l'équilibrage de charge des serveurs XenDesktop, le `CITRIX-XD-DDC` moniteur est automatiquement créé et lié aux services XenDesktop Delivery Controller.

Pour ajouter un moniteur XD-DDC avec l'option de validation des informations d'identification à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un moniteur XD-DDC et vérifier la configuration :

```
1 add lb monitor <monitorName> <monitorType> -userName <userName> -
      password <password> -domain <domain_name> -validateCred YES
2
```



```
show lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
 > add lb monitor xdddcmon Citrix-xd-ddc -userName Administrator -
    password E12Dc35450a1 -domain dhop -validateCred YES
 Done
> show lb monitor xdddcmon
1) Name......:xdddcmon Type......:CITRIX-XD-DDC State......: ENABLED

Standard parameters:
Interval......:..5 sec...Retries......:..3
Response timeout......:..2 sec...Down time......:..30 sec
Reverse......:..NO...Transparent......:..NO
Secure......:..NO...LRTM......:..ENABLED
Action......:..Not applicable...Deviation......:..0 sec
Destination IP......:..Bound service
Destination port......:..Bound service
Iptunnel......:..NO
TOS......:..NO...TOS ID......:..0
SNMP Alert Retries......:..0...Success Retries......:..1
Failure Retries......:..0

Special parameters:
User Name..........:"Administrator"
Password..........:*****
DDC Domain.........: "dhop"
Done
<!--NeedCopy-->
```

Pour spécifier l'option de validation des informations d'identification sur un moniteur XD-DDC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb monitor <monitorName> <monitorType> -userName -password -domain
   <domain_name> -validateCred YES
<!--NeedCopy-->
```

Exemple :

```
 set lb monitor XD_DDC_21.21.21.22_443_mn CITRIX-xd-ddc -userName
    Administrator -password D123S1R2A123 -domain dhop -validateCred YES
```



```
2 Done
3 <!--NeedCopy-->
```

Pour configurer un moniteur XD-DDC avec l'option de validation des informations d'identification à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**et créez un moniteur de type `Citrix-XD-DDC`.

Surveillance des magasins Citrix StoreFront

August 20, 2021

Vous pouvez configurer un moniteur utilisateur pour un magasin Citrix StoreFront. Le moniteur détermine l'état du magasin StoreFront en analysant successivement le service de compte, le service de découverte et le point de terminaison d'authentification (si le magasin Citrix StoreFront est un magasin authentifié). Si l'un de ces services ne répond pas à la sonde, la sonde du moniteur échoue et le magasin StoreFront est marqué comme étant DOWN. Le moniteur envoie des sondes à l'adresse IP et au port du service lié. Pour plus d'informations, consultez l' API Citrix StoreFront Store Services.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP. Toutefois, si le sous-réseau d'un serveur StoreFront est différent de celui de l'appliance, l'adresse IP du sous-réseau (SNIP) est utilisée.

À partir de la version 10.1 build 120.13, vous pouvez également lier un moniteur StoreFront à un groupe de services. Un moniteur est lié à chaque membre du groupe de services et des sondes sont envoyées à l'adresse IP et au port du membre lié (service). En outre, étant donné que chaque membre d'un groupe de services est désormais surveillé à l'aide de l'adresse IP du membre, vous pouvez désormais utiliser le moniteur StoreFront pour surveiller les nœuds de cluster StoreFront ajoutés en tant que membres du groupe de services.

Dans les versions antérieures, le moniteur StoreFront a essayé d'authentifier les magasins anonymes. Par conséquent, un service peut être marqué comme étant DOWN et vous ne pouvez pas lancer XenApp ou XenDesktop à l'aide de l'URL du serveur virtuel d'équilibrage de charge.

À partir de la version 64.x, l'ordre de la sonde a changé. Le moniteur détermine maintenant l'état du magasin StoreFront en analysant successivement le service de compte, le document de découverte, puis le service d'authentification, et ignore l'authentification pour les magasins anonymes.

Le paramètre de nom d'hôte des moniteurs StoreFront est obsolète. Le paramètre secure est maintenant utilisé pour déterminer s'il faut utiliser HTTP (valeur par défaut) ou HTTPS pour envoyer des sondes de moniteur.

Pour utiliser HTTPS, définissez l'option sécurisée sur Oui.

Pour créer un moniteur StoreFront à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur StoreFront et vérifier la configuration :

```
add lb monitor <monitorName> STOREFRONT <string> -storeName <string> [-
   storefrontacctservice ( YES | NO )] -secure ( YES | NO )

show lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple

```
add lb monitor storefront_ssl STOREFRONT -storename myStore -
   storefrontacctservice YES -secure YES
<!--NeedCopy-->
```

Pour créer un moniteur StoreFront à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**et créez un moniteur de type **STOREFRONT**.

> **Remarque**
>
> Pour plus d'informations sur les moniteurs StoreFront, consultez la documentation StoreFront.

Moniteurs personnalisés

August 20, 2021

En plus des moniteurs intégrés, vous pouvez utiliser des moniteurs personnalisés pour vérifier l'état de vos services. L'appliance Citrix ADC fournit plusieurs types de moniteurs personnalisés basés sur des scripts inclus dans le système d'exploitation Citrix ADC. Les scripts peuvent être utilisés pour déterminer l'état des services en fonction de la charge sur le service ou le trafic réseau envoyé au service. Les moniteurs personnalisés sont les moniteurs en ligne, les moniteurs utilisateur et les moniteurs de charge.

Avec ces types de moniteurs, vous pouvez utiliser la fonctionnalité fournie ou créer vos propres scripts et utiliser ces scripts pour déterminer l'état du service auquel le moniteur est lié.

Configurer les moniteurs HTTP-Inline

August 20, 2021

Les moniteurs en ligne analysent et sondent les réponses des services auxquels ils sont liés uniquement lorsque ces services reçoivent des demandes client. Le moniteur en ligne est de type HTTP-INLINE et ne peut être configuré qu'avec les services HTTP et HTTPS. Un moniteur en ligne détermine que le service auquel il est lié est UP en vérifiant ses réponses aux demandes qui lui sont envoyées. Lorsqu'aucune demande client n'est envoyée au service, le moniteur en ligne sonde le service à l'aide de l'URL configurée.

Remarque : les moniteurs en ligne ne peuvent pas être liés aux services distants ou locaux HTTP ou HTTPS Global Server Load Balancing (GSLB) car ces services représentent des serveurs virtuels plutôt que des serveurs Web équilibrés en charge réelle.

Les moniteurs en ligne ont une valeur de délai d'attente et un nombre de tentatives en cas d'échec des sondes. Vous pouvez sélectionner l'un des types d'action suivants que l'appliance Citrix ADC doit effectuer en cas de panne :

- **AUCUN.** Aucune mesure explicite n'est prise. Vous pouvez afficher le service et le moniteur, et le moniteur indique le nombre de réponses d'erreur contiguës actuelles et de réponses cumulées vérifiées.
- **LOG.** Consigne l'événement dans ns/syslog et affiche les compteurs.
- **DOWN.** Marque le service comme DOWN et ne dirige aucun trafic vers le service. Ce paramètre rompt toutes les connexions persistantes au service. Cette action enregistre également l'événement et affiche les compteurs.

Une fois le service arrêté, le service reste en panne pendant les temps d'arrêt configurés. Une fois le temps d'arrêt écoulé, le moniteur en ligne utilise l'URL configurée pour sonder le service afin de vérifier s'il est à nouveau disponible. Si la sonde réussit, l'état du service devient UP. Le trafic est dirigé vers le service, et la surveillance reprend comme avant.

Pour configurer des moniteurs en ligne, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Pour configurer des moniteurs HTTP en ligne à l'aide de l'interface de ligne de commande

Exécutez la commande suivante :

```
1 add lb monitor <monitorName> <type> -respCode <int[-int]> -httpRequest
     <string> -resptimeout <integer> [<units>] -retries <integer> -
     downTime <integer> [<units>] -action <action>
2 <!--NeedCopy-->
```


Exemple :

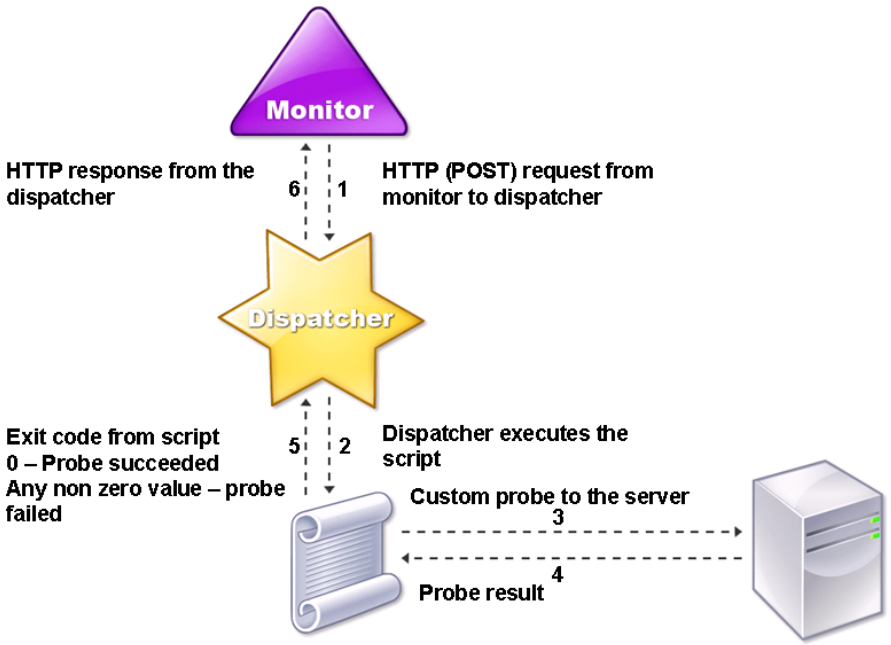
```
add lb monitor http_inline HTTP-INLINE -respCode 200 304 -httpRequest "
    HEAD /var/static/empty.htm" -resptimeout 4 -retries 1 -downTime 2 -
    action NONE
<!--NeedCopy-->
```

Comprendre les moniteurs utilisateur

October 5, 2021

Les moniteurs utilisateur étendent la portée des moniteurs personnalisés. Vous pouvez créer des moniteurs utilisateur pour suivre l'état des applications et protocoles personnalisés que l'appliance Citrix ADC ne prend pas en charge. Le diagramme suivant illustre le fonctionnement d'un moniteur utilisateur.

Figure 1. Moniteurs utilisateur



Un moniteur utilisateur nécessite les composants suivants.

Dispatcher. Un processus, sur la solution matérielle-logicielle, qui écoute les demandes de surveillance. Un répartiteur peut se trouver sur l'adresse IP de bouclage (127.0.0.1) et sur le port 3013. Les répartiteurs sont également appelés répartiteurs internes. Un répartiteur peut également être un serveur Web prenant en charge l'interface CGI (Common Gateway Interface). Ces répartiteurs sont également connus sous le nom de répartiteurs externes. Ils sont utilisés pour les scripts personnalisés qui ne s'exécutent pas dans l'environnement FreeBSD, tels que les scripts .NET.

> Remarque :
>
> Vous pouvez configurer le moniteur et le répartiteur pour qu'ils utilisent HTTPS au lieu de HTTP en activant l'option « sécurisé » sur le moniteur et en le configurant en tant que répartiteur externe. Toutefois, un répartiteur interne ne comprend que le protocole HTTP et ne peut pas utiliser le protocole HTTPS.

Dans une configuration HA, le répartiteur s'exécute sur les appliances Citrix ADC principales et secondaires. Le répartiteur reste inactif sur la solution matérielle-logicielle secondaire.

script. Le script est un programme qui envoie des sondes personnalisées au serveur à charge équilibrée et renvoie le code de réponse au répartiteur. Le script peut renvoyer n'importe quelle valeur au répartiteur, mais si une sonde réussit, le script doit renvoyer la valeur zéro (0). Le répartiteur considère toute autre valeur comme une défaillance de la sonde.

L'appliance Citrix ADC est fournie avec des exemples de scripts pour les protocoles couramment utilisés. Les scripts se trouvent dans le répertoire /nsconfig/moniteurs/. Si vous souhaitez ajouter un script, ajoutez-le ici. Pour personnaliser un script existant, créez une copie portant un nouveau nom et modifiez-la.

Important :

- À partir de Citrix ADC version 13.0 build 41.20, vous pouvez utiliser le `nsntlm-lwp.pl` script pour créer un moniteur de surveillance d'un serveur NTLM sécurisé.
- À partir de la version 10.1 122.17, les fichiers de script des moniteurs utilisateur se trouvent dans un nouvel emplacement.

  Si vous mettez à niveau un dispositif virtuel MPX ou VPX vers la version 10.1 build 122.17 ou ultérieure, les modifications sont les suivantes :

  - Un nouveau répertoire nommé conflicts est créé dans /nsconfig/monitors/ et tous les scripts intégrés des versions précédentes sont déplacés vers ce répertoire.
  - Tous les nouveaux scripts intégrés sont disponibles dans le répertoire /netscaler/monitors/. Tous les scripts personnalisés sont disponibles dans le répertoire /nsconfig/monitors/.
  - Enregistrez un nouveau script personnalisé dans le répertoire /nsconfig/monitors/.
  - Une fois la mise à niveau terminée, si un script personnalisé est créé et enregistré dans le répertoire /nsconfig/monitors/, avec le même nom que le script intégré, le script du

répertoire /netscaler/monitors/ est prioritaire. Le script personnalisé n'est pas exécuté.

Si vous provisionnez un dispositif virtuel avec la version 10.1 version 122.17 ou ultérieure, les modifications sont les suivantes :

- Tous les scripts intégrés sont disponibles dans le répertoire /netscaler/monitors/.
- Le répertoire /nsconfig/monitors/ est vide.
- Si vous créez un script personnalisé, vous devez l'enregistrer dans le répertoire /nsconfig/-monitors/.

Pour que les scripts fonctionnent correctement :

- Le nombre maximal de caractères dans le nom du script ne doit pas dépasser 63.
- Le nombre maximal d'arguments de script pouvant être fournis à un script ne doit pas dépasser 512.
- Le nombre maximal de caractères pouvant être fournis dans les arguments du script de paramètre ne doit pas dépasser 639.

Pour déboguer le script, vous devez l'exécuter à l'aide du script nsumon-debug.pl de l'interface de ligne de commande. Vous utilisez le nom du script (avec ses arguments), l'adresse IP et le port comme arguments du script nsumon-debug.pl. Les utilisateurs doivent utiliser le nom du script, l'adresse IP, le port, le délai d'expiration et les arguments de script pour le script nsumon-debug.pl.

À l'interface de ligne de commande, tapez :

```
1 nsumon-debug.pl <scriptname> <IP> <port> <timeout> <partitionID> [
     scriptarguments][is_secure]
2 <!--NeedCopy-->
```

Important : à partir de la version 10.5 build 57.x et des fichiers de script 11.0 pour les moniteurs utilisateur prennent en charge les adresses IPv6 et incluent les modifications suivantes :

- Pour les protocoles suivants, de nouveaux protocoles `pm files` ont été inclus pour la prise en charge d'IPv6.
  - RADIUS
  - NNTP
  - POP3
  - SMTP
- Les exemples de scripts suivants dans /netscaler/monitors/ ont été mis à jour pour la prise en charge d'IPv6 :
  - nsbmradius.pl
  - nsldap.pl
  - nsnntp.pl

- nspop3 nssf.pl
- nssnmp.pl
- nswi.pl
- nstftp.pl
- nssmtp.pl
- nsrdp.pl
- nsntlm-lwp.pl
- nsftp.pl
- nsappc.pl

Après la mise à niveau vers la version 10.5 build 57.x ou 11.0, si vous souhaitez utiliser vos scripts personnalisés existants avec les services IPv6, assurez-vous de mettre à jour les scripts personnalisés existants avec les modifications fournies dans les exemples de scripts mis à jour dans /netscaler/monitors/.

Remarque : L'exemple de script nsmysql.pl ne prend pas en charge l'adresse IPv6. Si un service IPv6 est lié à un moniteur utilisateur qui utilise nsmysql.pl, la sonde échoue.

- Les types de moniteurs LB suivants ont été mis à jour pour prendre en charge les adresses IPv6 :
  - USER
  - SMTP
  - NNTP
  - LDAP
  - SNMP
  - POP3
  - FTP_EXTENDED
  - StoreFront
  - APPC
  - CITRIX_WI_EXTENDED

  Si vous créez un script personnalisé qui utilise l'un de ces types de moniteurs LB, veillez à inclure la prise en charge IPv6 dans le script personnalisé. Reportez-vous à l'exemple de script associé dans /netscaler/monitors/ pour connaître les modifications que vous devez apporter au script personnalisé pour la prise en charge d'IPv6.

Pour suivre l'état du serveur, le moniteur envoie une requête HTTP POST au répartiteur configuré. Cette demande POST contient l'adresse IP et le port du serveur, ainsi que le script à exécuter. Le répartiteur exécute le script en tant que processus enfant, avec des paramètres définis par l'utilisateur (le cas échéant). Ensuite, le script envoie une sonde au serveur. Le script envoie l'état de la sonde (code de réponse) au répartiteur. Le répartiteur convertit le code de réponse en réponse HTTP et l'envoie au moniteur. En fonction de la réponse HTTP, le moniteur marque le service comme étant en hausse ou en panne.

L'appliance Citrix ADC enregistre les messages d'erreur dans le fichier /var/nslog/nsumond.log lorsque les sondes du moniteur utilisateur échouent. Ces messages d'erreur détaillés sont affichés dans l'interface graphique et dans l'interface de ligne de commande pour les `show service`/ `service group` commandes.

Le tableau suivant répertorie les moniteurs utilisateur et les raisons possibles de l'échec.

Type de moniteur utilisateur	Raisons de défaillance
SMTP	Le moniteur ne parvient pas à établir une connexion au serveur.
NNTP	Le moniteur ne parvient pas à établir une connexion au serveur.
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	Le moniteur ne parvient pas à trouver le groupe NNTP.
LDAP	Le moniteur ne parvient pas à établir une connexion au serveur.
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	Le moniteur ne parvient pas à se lier au serveur LDAP.
	Le moniteur ne parvient pas à localiser une entrée pour l'entité cible sur le serveur LDAP.
FTP	La connexion au serveur est dépassé.

Type de moniteur utilisateur	Raisons de défaillance
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	L'ouverture de session échoue.
	Le moniteur ne parvient pas à trouver le fichier sur le serveur.
POP3	Le moniteur ne parvient pas à établir une connexion à la base de données.
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	L'ouverture de session échoue.
POP3	Le moniteur ne parvient pas à établir une connexion à la base de données.
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	L'ouverture de session échoue.
	La préparation de la requête SQL échoue.
	L'exécution de la requête SQL échoue.
SNMP	Le moniteur ne parvient pas à établir une connexion à la base de données.
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	L'ouverture de session échoue.
	Le moniteur ne parvient pas à créer la session SNMP.
	Le moniteur ne parvient pas à trouver l'identifiant d'objet.

Type de moniteur utilisateur	Raisons de défaillance
	Le paramètre de valeur de seuil du moniteur est supérieur ou égal au seuil réel du moniteur.
RDP (Windows Terminal Server)	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	Le moniteur ne parvient pas à créer un socket.
	Les versions ne correspondent pas.
	Le moniteur n'arrive pas à confirmer la connexion.

Vous pouvez afficher le fichier journal à partir de l'interface de ligne de commande à l'aide des commandes suivantes, qui ouvrent un shell BSD, affichent le fichier journal à l'écran, puis ferment le shell BSD et vous renvoient à l'interface de ligne de commande :

```
> shell
root@ns# cat /var/nslog/nsumond.log
root@ns# exit
>
<!--NeedCopy-->
```

Avant la version 13.0 de Citrix ADC build 52.X, la commande `show service/service group` affichait un message d'erreur générique indiquant « échec de la sonde » comme cause de l'échec de la sonde du moniteur utilisateur.

Exemple :

```
show service ftp

Monitor Name: mon2
State: UNKNOWN  Weight: 1   Passive: 0
Probes: 3    Failed [Total: 0 Current: 0]
Last response: Failure - Probe failed.
Response Time: 1071.838 millisec
<!--NeedCopy-->
```

À partir de Citrix ADC version 13.0 build 52.X, la commande `show service/service group` affiche la cause réelle de la défaillance de la sonde du moniteur utilisateur.

Exemple :


```
show service ftp

Monitor Name: mon2
State: DOWN   Weight: 1   Passive: 0
Probes: 729   Failed [Total: 726 Current: 726]
Last response: Failure - Login failed.
Response Time: 8000.0 millisec
<!--NeedCopy-->
```

Les moniteurs utilisateur ont également une valeur de délai d'expiration et un nombre de relances pour les échecs de sonde. Vous pouvez utiliser des moniteurs utilisateur avec des moniteurs non utilisateurs. En cas d'utilisation élevée du processeur, un moniteur non utilisateur permet de détecter plus rapidement une panne de serveur.

Si la sonde du moniteur de l'utilisateur expire en cas d'utilisation élevée du processeur, l'état du service reste inchangé.

Example1:

```
add lb monitor <name> USER -scriptname <script-name> -resptimeout 5
    seconds
<!--NeedCopy-->
```

> Remarque
>
> Pour les moniteurs scriptables, le délai d'attente de réponse doit être configuré à une valeur égale au délai d'expiration attendu de 1 seconde. Par exemple, si vous vous attendez à ce que le délai d'attente soit de 4 secondes, configurez le délai d'attente de réponse sur 5 secondes.

Example2:

```
add lb monitor <name> USER -scriptname <script-name> -scriptargs <
    Arguments> -secureargs <Arguments>
<!--NeedCopy-->
```

> Remarque
>
> Citrix vous recommande d'utiliser le paramètre `secureargs` au lieu du paramètre `scriptargs` pour toutes les données sensibles liées aux scripts.

Comment utiliser un moniteur utilisateur pour vérifier les sites Web

August 20, 2021

Vous pouvez configurer un moniteur utilisateur pour vérifier les problèmes spécifiques de sites Web signalés par les serveurs HTTP à l'aide de codes HTTP spécifiques. Le tableau suivant répertorie les codes de réponse HTTP que ce moniteur utilisateur attend.

Code de réponse HTTP	Sens
200 - succès	Succès de la sonde.
503 - service indisponible	Échec de la sonde.
404 - introuvable	Script introuvable ou impossible à exécuter.
500 - Erreur interne du serveur	Erreur/contraintes de ressources internes dans le répartiteur (mémoire insuffisante, trop de connexions, erreur système inattendue ou trop de processus). Le service n'est pas marqué comme DOWN.
400 - mauvaise demande	Erreur lors de l'analyse de la requête HTTP.
502 - mauvaise Gateway	Erreur de décodage de la réponse du script.

Vous configurez le moniteur utilisateur pour HTTP à l'aide des paramètres suivants.

Paramètre	Spécifie
Nom du script	Le chemin et le nom du script à exécuter.
scriptArgs	Les chaînes qui sont ajoutées dans les données POST. Ils sont copiés dans la requête verbatim.
dispatcherIP	Adresse IP du répartiteur auquel la sonde est envoyée.
dispatcherPort	Port du répartiteur vers lequel la sonde est envoyée.
localfileName	Nom d'un fichier de script de moniteur sur le système local.
destPath	Emplacement particulier sur l'appliance Citrix ADC où le fichier local téléchargé est stocké.

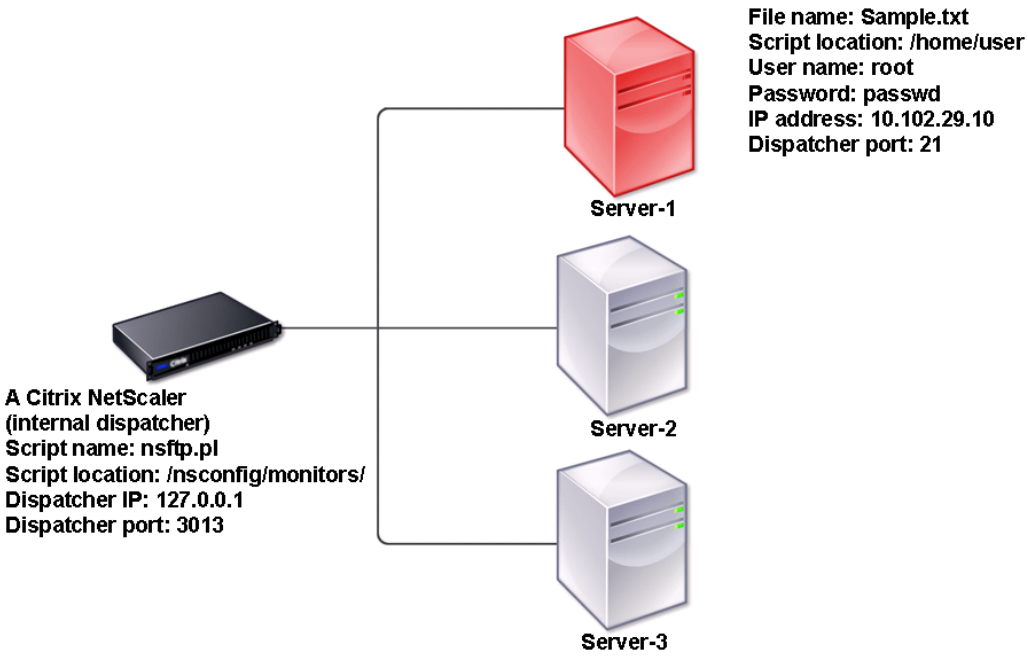
Pour créer un moniteur utilisateur pour surveiller HTTP, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Comprendre le répartiteur interne

August 20, 2021

Vous pouvez utiliser un moniteur utilisateur personnalisé avec le répartiteur interne. Considérons un cas où vous devez suivre l'état d'un serveur en fonction de la présence d'un fichier sur le serveur. Le diagramme suivant illustre ce scénario.

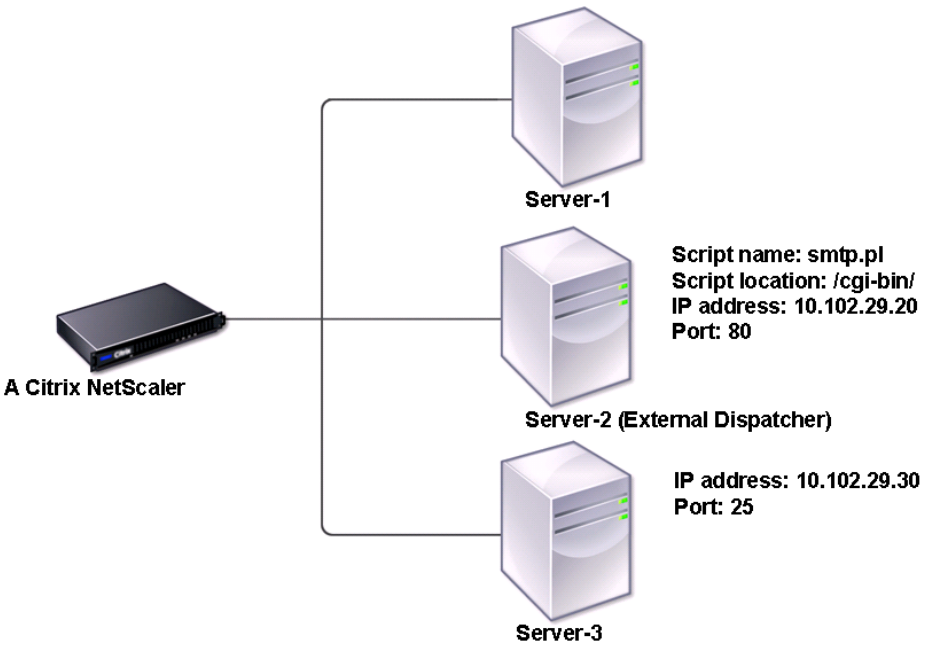
Figure 1. Utilisation d'un moniteur utilisateur avec le répartiteur interne



Une solution possible consiste à utiliser un script Perl qui initie une session FTP avec le serveur et vérifie la présence du fichier. Vous pouvez ensuite créer un moniteur utilisateur qui utilise le script Perl. L'appliance Citrix ADC inclut un tel script Perl (nsftp.pl), dans le répertoire /nsconfig/monitors/.

Vous pouvez utiliser un moniteur utilisateur avec un répartiteur externe. Considérons un cas où vous devez suivre l'état d'un serveur en fonction de l'état d'un service SMTP sur un autre serveur. Ce scénario est illustré dans le diagramme suivant.

Figure 2. Utilisation d'un moniteur utilisateur avec un répartiteur externe



Une solution possible serait de créer un script Perl qui vérifie l'état du service SMTP sur le serveur. Vous pouvez ensuite créer un moniteur utilisateur qui utilise le script Perl.

Configuration du moniteur utilisateur

October 5, 2021

Les moniteurs utilisateur suivent l'état de santé des applications et protocoles personnalisés qu'une appliance Citrix ADC ne prend pas en charge. Il s'agit d'une gamme étendue de moniteurs personnalisés. Pour configurer un moniteur utilisateur, vous devez effectuer les étapes suivantes :

- Écrivez un script qui peut surveiller les services qui lui sont liés.
- Téléchargez le script `/nsconfig/monitors` dans le répertoire de l'appliance Citrix ADC.
- Fournissez une autorisation exécutable sur le script.

Si le type de moniteur est un protocole que la solution matérielle-logicielle ne prend pas en charge, vous devez utiliser un moniteur de type **USER**. Les moniteurs utilisateur ne prennent en charge que les scripts de type Perl et Bash. Ils ne prennent pas en charge les scripts Python.

> **Remarque**
>
> Les sondes de surveillance proviennent de l'adresse NSIP. La `scriptargs` configuration pour le type de moniteur **USER** est affichée dans les fichiers de configuration et ns.conf en cours d'exécution.

Pour plus d'informations sur les moniteurs, voir Configurer les moniteurs.

Pour configurer un moniteur utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb monitor <monitorName> USER -scriptname <NameOfScript> -
    scriptargs <Arguments> -secureargs <Arguments>
<!--NeedCopy-->
```

Example1:

```
add monitor Monitor-User-1 USER -scriptname nsftp.pl -scriptargs "file
    =/home/user/
sample.txt;user=root;password=passwd"
<!--NeedCopy-->
```

Example2:

```
add monitor Monitor-User-1 USER -scriptname nsftp.pl -scriptargs "file
    =/home/user/
sample.txt -secureargs "user=root;password=passwd"
<!--NeedCopy-->
```

> Remarque
>
> Le `secureargs` paramètre stocke les arguments du script dans un format chiffré au lieu du format texte brut. Citrix vous recommande d'utiliser le `secureargs` paramètre au lieu du paramètre scriptargs pour toutes les données sensibles liées aux scripts, par exemple, le nom d'utilisateur et le mot de passe. Si vous choisissez d'utiliser les deux paramètres ensemble, le script spécifié dans `-scriptname` doit accepter les arguments dans l'ordre : `<scriptargs> <secureargs>`. Spécifiez les premiers arguments du `<scriptargs>` paramètre et le reste des arguments dans le `<secureargs>` paramètre. En d'autres termes, maintenez l'ordre défini pour les arguments. Les arguments sécurisés ne s'appliquent qu'au répartiteur interne. Si vous souhaitez utiliser un répartiteur externe, Citrix recommande de sécuriser les données vulnérables dans vos scripts.

Exemple 3 :

Supposons que vous ayez déjà configuré le `scriptargs` paramètre avec les arguments : « a=b ; c=d ; e=f ».

```
add monitor mon1 USER -scriptargs "a=b;c=d;e=f"
<!--NeedCopy-->
```

Si vous souhaitez utiliser le `secureargs` paramètre au lieu du `scriptargs` paramètre, procédez comme suit :

- Annule le `scriptargs` paramètre.
- Indiquez tous les arguments sous `secureargs` paramètre.

```
set monitor mon1 USER -scriptargs "" -secureargs "a=b;c=d;e=f"
<!--NeedCopy-->
```

Pour configurer un moniteur utilisateur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un moniteur**, procédez comme suit :
   - Sélectionnez le type de moniteur en tant qu' **UTILISATEUR**.
   - Choisissez le script dans le menu déroulant ou téléchargez votre propre script.
   - Entrez les valeurs appropriées pour les champs **Arguments de script** et **Arguments sécurisés** .
   - Cliquez sur **Create**.

   Un moniteur utilisateur est créé.

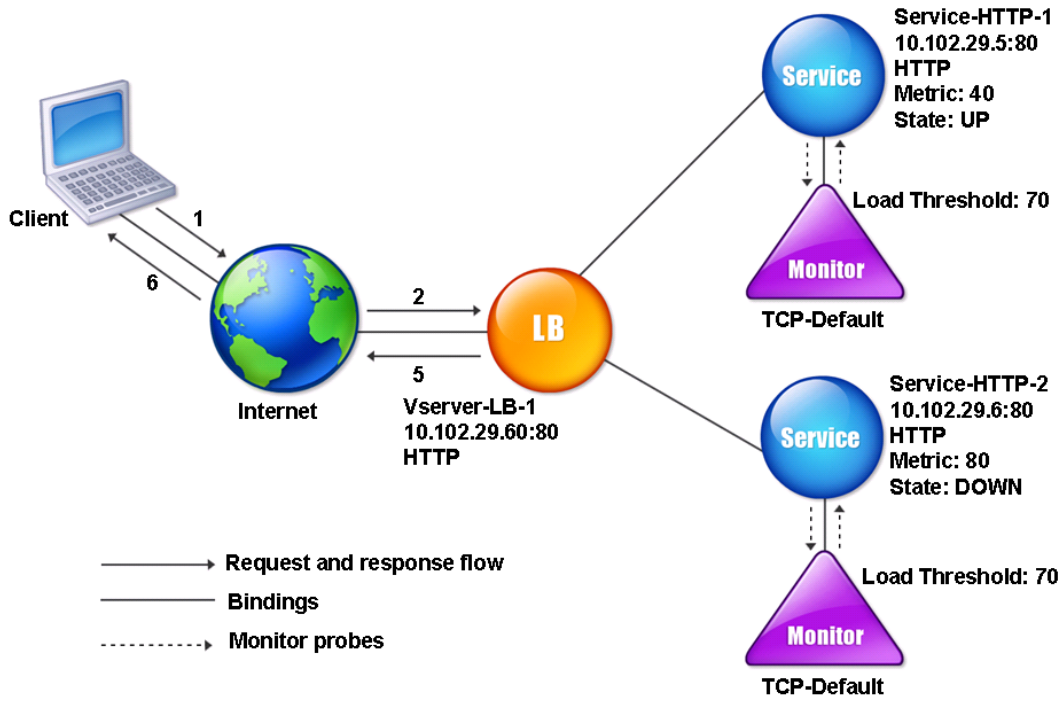
Comprendre les moniteurs de charge

August 20, 2021

Les moniteurs de charge utilisent les OID interrogés SNMP pour calculer la charge. Le moniteur de charge utilise l'adresse IP du service auquel il est lié (l'adresse IP de destination) pour l'interrogation. Il envoie une requête SNMP au service, en spécifiant l'OID d'une mesure. Les mesures peuvent être CPU, mémoire ou nombre de connexions serveur. Le serveur répond à la requête avec une valeur de mesure. La valeur de mesure dans la réponse est comparée à la valeur de seuil. L'appliance Citrix ADC prend en compte le service pour l'équilibrage de charge uniquement si la mesure est inférieure à la valeur seuil. Le service avec la valeur de charge la plus faible est considéré en premier.

Le diagramme suivant illustre un moniteur de charge configuré pour les services décrits dans la configuration d'équilibrage de charge de base discutée dans Configuration de l'équilibrage de charge de base.

Figure 1. Fonctionnement des moniteurs de charge



Remarque : le moniteur de charge ne détermine pas l'état du service. Elle permet uniquement à l'appliance de prendre en compte le service pour l'équilibrage de charge.

Après avoir configuré le moniteur de charge, vous devez ensuite configurer les mesures que le moniteur utilisera. Pour l'évaluation de la charge, le moniteur de charge prend en compte les paramètres du serveur connus sous le nom de mesures, qui sont définis dans les tables de mesures de la configuration de l'appliance. Les tables de mesures peuvent être de deux types :

- **Locaux.** Par défaut, cette table existe dans l'appliance. Il se compose de quatre mesures : connexions, paquets, temps de réponse et bande passante. L'appliance spécifie ces mesures pour un service, et les requêtes SNMP ne sont pas issues de ces services. Ces mesures ne peuvent pas être modifiées.
- **Personnalisé.** Table définie par l'utilisateur. Chaque mesure est associée à un OID.

Par défaut, l'appliance génère les tableaux suivants :

- NetScaler

- RADWARE
- CISCO-CSS
- LOCAL
- FOUNDRY
- ALTEON

Vous pouvez soit ajouter les tables de mesures générées par l'appliance, soit ajouter les tables de votre choix, comme indiqué dans le tableau suivant. Les valeurs de la table de mesures ne sont fournies qu'à titre d'exemples. Dans un scénario réel, considérez les valeurs réelles des mesures.

Nom de la mesure	OID	Poids	Seuil
UC	1.2.3.4	2	70
Mémoire	4.5.6.7	3	80
Connexions	5.6.7.8	4	90

Pour calculer la charge d'une ou de plusieurs mesures, vous affectez une pondération à chaque mesure. Le poids par défaut est 1. Le poids représente la priorité donnée à chaque métrique. Si le poids est élevé, la priorité est élevée. L'appliance choisit un service basé sur l'algorithme de hachage SOURCEIPDESTIP.

Vous pouvez également définir la valeur de seuil pour chaque mesure. La valeur de seuil permet à l'appliance de sélectionner un service pour l'équilibrage de charge si la valeur de mesure du service est inférieure à la valeur de seuil. La valeur de seuil détermine également la charge sur chaque service.

Configurer les moniteurs de charge

August 20, 2021

Pour configurer un moniteur de charge, créez d'abord le moniteur de charge. Pour obtenir des instructions sur la création d'un moniteur, voir Création de moniteurs. Ensuite, sélectionnez ou créez la table de mesures pour définir un ensemble de mesures qui déterminent l'état du serveur, et (si vous créez une table de mesures) liez chaque mesure à la table de mesures.

Pour créer une table de mesures à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
add lb metricTable <metricTableName>
```



```
bind lb metricTable <metricTableName> <metric> <SNMPOID>
<!--NeedCopy-->
```

Exemple :

```
add metricTable Table-Custom-1

bind metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5 11
<!--NeedCopy-->
```

Pour créer une table de mesures et y lier des mesures à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Tables de mesures** et créez une table de mesures.
2. Pour lier des mesures, cliquez sur **Lier et spécifiez une mesure et un OID** SNMP.

Dissocier les mesures d'une table de mesures

August 20, 2021

Vous pouvez dissocier les mesures d'une table de mesures si elles doivent être modifiées ou si vous souhaitez supprimer entièrement la table de mesures.

Pour dissocier les mesures d'une table de mesures à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind lb metricTable <metricTable> <metric>
<!--NeedCopy-->
```

Exemple :

```
unbind metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5
<!--NeedCopy-->
```

Pour dissocier les mesures d'une table de mesures à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de la charge** > **Tables** de mesures.

2. Ouvrez une table de mesures, sélectionnez une mesure, puis cliquez sur **Supprimer**.

Vous pouvez afficher les détails de toutes les tables de mesures configurées, telles que le nom et le type, pour déterminer si la table de mesures est interne ou si elle est créée et configurée.

Configurer la surveillance inverse pour un service

August 20, 2021

Un moniteur inverse marque un service comme DOWN si les critères de sonde sont satisfaits et UP s'ils ne sont pas satisfaits. Par exemple, si vous souhaitez qu'un service de sauvegarde reçoive du trafic uniquement lorsque le service principal est DOWN, vous pouvez lier un moniteur inverse au service secondaire mais le configurer pour sonder le service principal.

L'appliance Citrix ADC prend en charge les moniteurs inverses suivants :

- HTTP
- ICMP
- TCP (à partir de la version 11.1 build 49.x)

Configuration de la surveillance inverse HTTP pour un service

Le tableau suivant décrit les conditions de la surveillance directe et inverse HTTP pour un service :

Condition	Direct	Inverser
Connexion non établie.	Échec	Échec
Le code de réponse HTTP correspond aux spécifications de la sonde.	Succès	Échec
Le code de réponse HTTP ne correspond pas aux spécifications de la sonde.	Échec	Succès
La sonde a expiré.	Échec	Échec

Pour configurer la surveillance inverse HTTP pour un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
add lb monitor <Monitor_Name> HTTP -respCode 200 -httpRequest "HEAD /"
    -destIP <Primary_Service_IP_Address> -destPort 80 -reverse YES

bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
<!--NeedCopy-->
```

Configuration de la surveillance inversée ICMP pour un service

Le tableau suivant décrit les conditions de la surveillance directe et inversée ICMP pour un service :

Condition	Direct	Inverser
La réponse d'écho ICMP est reçue.	Succès	Échec
La sonde a expiré.	Échec	Succès

Pour configurer la surveillance inversée ICMP pour un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb monitor <Monitor_Name> PING -destIP <Primary_Service_IP_Address>
    -reverse YES

bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
<!--NeedCopy-->
```

Configuration de la surveillance inverse TCP pour un service

Si un moniteur TCP direct reçoit un RESET en réponse à une sonde de moniteur, le service est marqué comme DOWN. Toutefois, si un moniteur TCP inverse reçoit une réponse RESET, la sonde est considérée comme réussie et le service est marqué UP.

Le tableau suivant décrit les conditions de la surveillance inverse TCP pour un service :

Condition	Direct	Inverser
La connexion TCP est établie.	Succès	Échec
La sonde a expiré.	Échec	Échec

Condition	Direct	Inverser
La réponse à la sonde est RESET.	Échec	Succès

Pour configurer la surveillance inverse TCP pour un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb monitor <Monitor_Name> TCP  -destip <Primary_Service_IP_Address>
    -destport <primary_service_port>  -reverse YES

bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
<!--NeedCopy-->
```

Pour configurer la surveillance inverse à l'aide de l'interface graphique

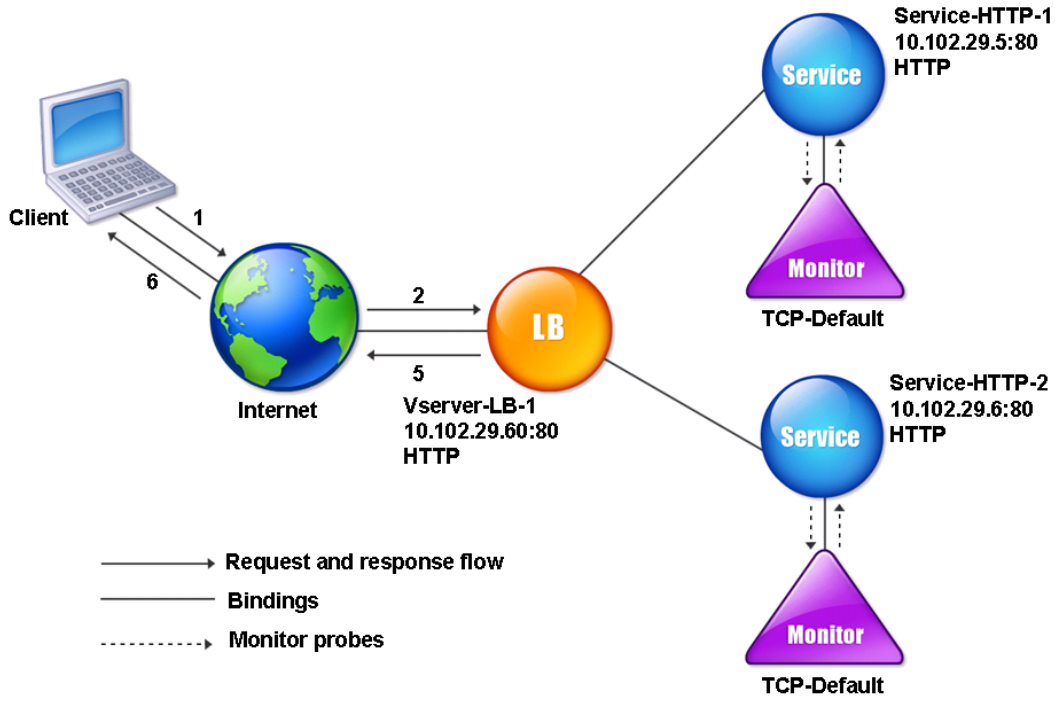
1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**.
2. Créez un moniteur HTTP, ICMP ou TCP et sélectionnez **Inverser**.

Configurer les moniteurs dans une configuration d'équilibrage de charge

August 20, 2021

Pour configurer des moniteurs sur un site Web, vous décidez d'abord d'utiliser un moniteur intégré ou de créer votre propre moniteur. Si vous créez un moniteur, vous pouvez choisir entre créer un moniteur basé sur un moniteur intégré ou créer un moniteur personnalisé utilisant un script que vous écrivez pour surveiller le service. Pour plus d'informations sur la création de moniteurs personnalisés, voir Moniteurs personnalisés. Une fois que vous avez choisi ou créé un moniteur, vous le liez ensuite au service approprié. Les noms de moniteur peuvent contenir jusqu'à 255 caractères. Le diagramme conceptuel suivant illustre une configuration d'équilibrage de charge de base avec des moniteurs.

Figure 1. Fonctionnement des moniteurs



Comme indiqué, chaque service est associé à un moniteur. Le moniteur sonde le serveur à équilibrage de charge via son service. Tant que le serveur à équilibrage de charge répond aux sondes, le moniteur le marque comme UP. Si le serveur à charge équilibrée ne répond pas au nombre de sondes désigné au cours de la période désignée, le moniteur le marque DOWN.

Cette section comprend les détails suivants :

- Création de moniteurs
- Configuration des paramètres de surveillance pour déterminer l'intégrité du service
- Liaison des moniteurs aux services
- Modification des moniteurs
- Activation et désactivation des moniteurs
- Moniteurs sans liaison
- Suppression de moniteurs
- Affichage des moniteurs
- Fermeture des connexions du moniteur
- Ignorer la limite supérieure des connexions client pour les sondes de moniteur

Créer des moniteurs

August 20, 2021

L'appliance Citrix ADC fournit un ensemble de moniteurs intégrés. Il vous permet également de créer des moniteurs personnalisés, basés sur les moniteurs intégrés ou à partir de zéro.

Pour créer un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb monitor <monitorName> <monitorType> [<interval>]

add lb mon monitor-HTTP-1 HTTP

add lb mon monitor-HTTP-2 TCP 2
<!--NeedCopy-->
```

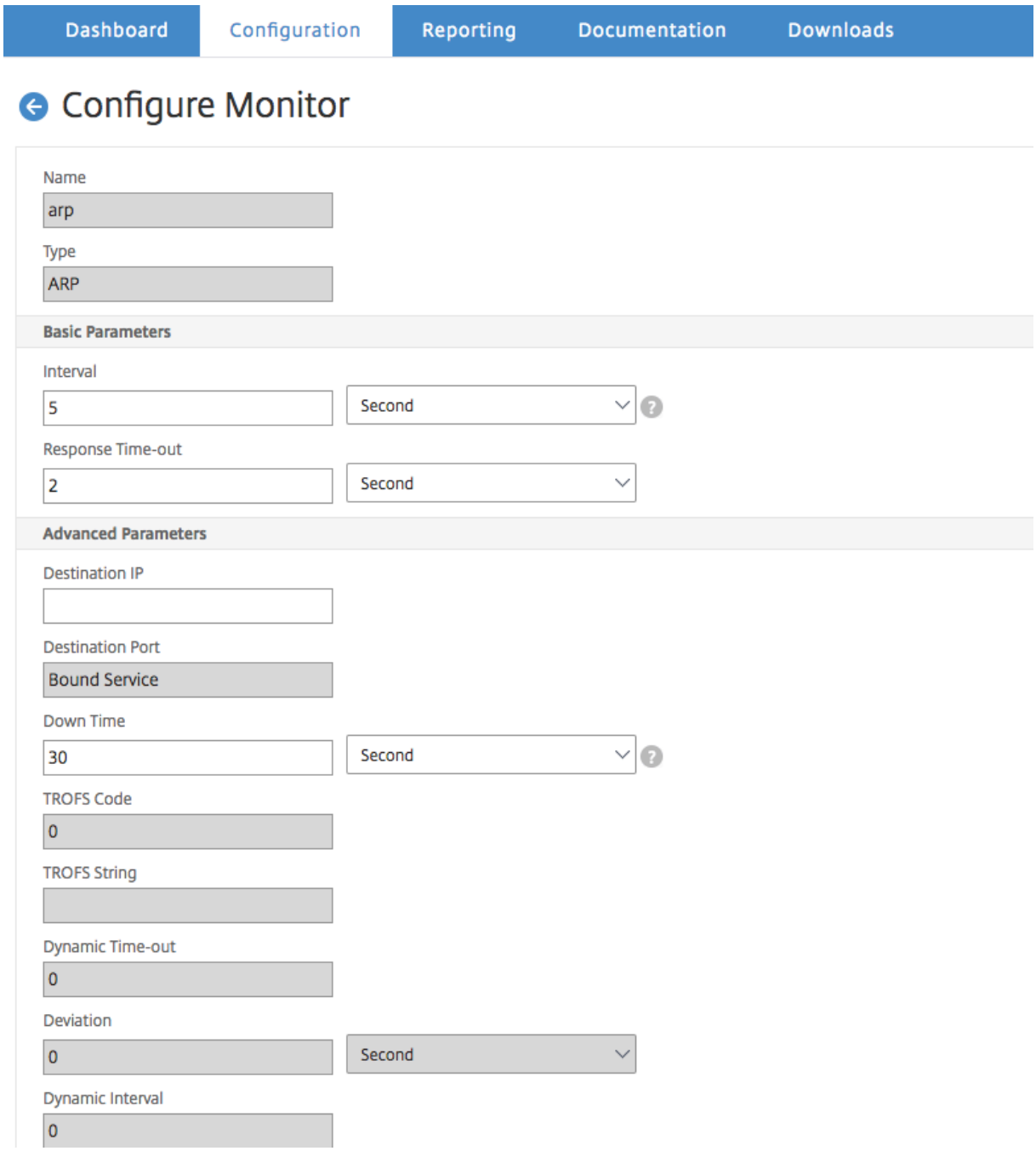
Pour créer un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic**> **Équilibrage de charge**> **Moniteurs**.
2. Cliquez sur **Ajouter** et créez un type de moniteur qui répond à vos besoins.

L'écran Créer un moniteur contient deux sections, **Paramètres de base** et **Paramètres avancés** .

Selon le type de moniteur, la section **Paramètres de base** contient les paramètres qui doivent être définis pour chaque moniteur. La section **Paramètres avancés** contient les paramètres qui peuvent être utilisés dans des cas d'utilisation avancés.

La figure suivante est un exemple de page Créer un moniteur du type de moniteur ARP.



Remarque

Avant NetScaler version 12.0 build 56.20, les paramètres de base et les paramètres avancés sont respectivement nommés paramètres standard et paramètres spéciaux.

Configurer les paramètres du moniteur pour déterminer l'intégrité du service

August 20, 2021

Vous pouvez configurer les paramètres de surveillance suivants pour marquer un service comme étant DOWN en fonction des sondes de surveillance.

Retries

Nombre maximal de sondes à envoyer pour établir l'état d'un service pour lequel une sonde de surveillance échoue.

failureRetries

Nombre de tentatives qui doivent échouer, hors du nombre spécifié pour le paramètre Retries, pour qu'un service soit marqué comme étant DOWN. Par exemple, si le paramètre Retries est défini sur 10 et que le paramètre Failure Retries est défini sur 6, sur les 10 sondes envoyées, au moins six sondes doivent échouer si le service doit être marqué comme DOWN.

alertRetries

Nombre d'échecs de sonde consécutifs après lesquels l'appliance génère une interruption SNMP appelée monProbeFailed.

Définition d'AlertEtries sur une valeur supérieure à la valeur Retries

Le paramètre alertRetries, qui spécifie le nombre maximal d'échecs consécutifs de sonde de surveillance après lesquels l'appliance Citrix ADC génère une interruption SNMP appelée monProbeFailed, peut désormais être défini sur une valeur supérieure à la valeur Retries (qui spécifie le nombre maximal de sondes à envoyer pour établir le paramètre état d'un service pour lequel une sonde de surveillance a échoué). Si la valeur alertRetries est supérieure à la valeur Retries, l'interruption SNMP n'est envoyée qu'après que le service ait été DOWN.

Par exemple, si vous définissez Retries sur 3, alertRetries sur 12 et l'intervalle de temps sur 5 secondes, le service est marqué comme DOWN après 15 secondes (3*5), mais aucune alerte n'est générée. Si les sondes du moniteur échouent toujours après 60 secondes (12*5), l'appliance Citrix ADC génère une interruption monProbeFailed. Si une sonde réussit à un moment donné entre 15 et 60 secondes, le service est marqué UP et aucune alerte n'est générée.

La définition de la valeur alertRetries sur une valeur supérieure à la valeur Retries permet de générer uniquement des alertes authentiques et d'éviter les faux positifs lors des redémarrages planifiés.

Pour définir la valeur du paramètre alertRetries sur une valeur supérieure à la valeur Retries à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb monitor <monitorName> [-retries <integer>] [-alertRetries <
    integer>]
<!--NeedCopy-->
```

Exemple :

add lb monitor monitor-HTTP-1 HTTP -retries 3 -alertRetries 12

Pour définir la valeur du paramètre AlertRetries sur une valeur supérieure à la valeur Retries à l'aide de l'interface graphique graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**.
2. Cliquez sur **Ajouter** pour ajouter un nouveau moniteur ou sélectionnez un moniteur existant et cliquez sur **Modifier**.
3. Dans la zone **Retries**, tapez la valeur du paramètre Retries.
4. Dans la zone **SNMP Alert Retries**, tapez la valeur du paramètre `alertRetries`.

Lier les moniteurs aux services

August 20, 2021

Après avoir créé un moniteur, vous le liez à un service. Vous pouvez lier un ou plusieurs moniteurs à un service. Si vous liez un moniteur à un service, ce moniteur détermine si le service est marqué comme UP ou DOWN.

Si vous liez plusieurs moniteurs à un service, l'appliance Citrix ADC vérifie l'état de tous les moniteurs, puis décide de l'état du service. Vous pouvez configurer différentes pondérations pour un moniteur. Le poids d'un moniteur spécifie dans quelle mesure ce moniteur contribue à désigner le service comme étant UP ou DOWN. Un moniteur avec un poids plus élevé a une préférence plus élevée pour marquer le service comme UP ou DOWN. Le poids par défaut est 1. Par conséquent, même si l'un des moniteurs échoue, le service est marqué comme DOWN. Pour plus d'informations, voir Définir une valeur de seuil pour les moniteurs liés à un service.

Remarque : L'adresse IP de destination d'une sonde de moniteur peut être différente de l'adresse IP du serveur et du port.

Pour lier un moniteur à un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind service <name> (-monitorName <string>)
<!--NeedCopy-->
```

Exemple :

```
bind service s1 -monitorName tcp
<!--NeedCopy-->
```

Pour lier un moniteur à un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Ouvrez le service et ajoutez un moniteur.

Modifier les moniteurs

August 20, 2021

Vous pouvez modifier les paramètres de n'importe quel moniteur que vous avez créé.

Remarque : Deux ensembles de paramètres s'appliquent aux moniteurs : ceux qui s'appliquent à tous les moniteurs, quel que soit leur type, et ceux qui sont spécifiques à un type de moniteur. Pour plus d'informations sur les paramètres d'un type de moniteur spécifique, consultez la description de ce type de moniteur.

Pour modifier un moniteur existant à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb monitor <monitorName> <type> -interval <interval> -resptimeout <
    resptimeout>
<!--NeedCopy-->
```

Exemple :


```
set mon monitor-HTTP-1 HTTP -interval 50 milli
-resptimeout 20 milli
<!--NeedCopy-->
```

Pour modifier un moniteur existant à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**, puis ouvrez un moniteur à modifier.

Activer et désactiver les moniteurs

August 20, 2021

Par défaut, les moniteurs liés aux services et aux groupes de services sont activés. Lorsque vous activez un moniteur, celui-ci commence à sonder les services auxquels il est lié. Si vous désactivez un moniteur lié à un service, l'état du service est déterminé à l'aide des autres moniteurs liés au service. Si le service est lié à un seul moniteur et si vous le désactivez, l'état du service est déterminé à l'aide du moniteur par défaut.

Pour activer un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
enable lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
enable lb mon monitor-HTTP-1
<!--NeedCopy-->
```

Pour activer un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Sélectionnez un moniteur et, dans la liste Action, sélectionnez Activer ou Désactiver.

Pour désactiver un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
disable lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
disable lb mon monitor-HTTP-1
<!--NeedCopy-->
```

Dissocier les moniteurs

August 20, 2021

Vous pouvez dissocier les moniteurs d'un service et d'un groupe de services. Lorsque vous dissociez un moniteur du groupe de services, les moniteurs sont dissociés des services individuels qui constituent le groupe de services. Lorsque vous dissociez un moniteur d'un service ou d'un groupe de services, le moniteur ne sonde pas le service ou le groupe de services.

Remarque : Lorsque vous dissociez tous les moniteurs configurés par l'utilisateur d'un service ou d'un groupe de services, le moniteur par défaut est lié au service et au groupe de services. Les moniteurs par défaut sonde ensuite le service ou les groupes de services.

Pour dissocier un moniteur d'un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
unbind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour dissocier un moniteur d'un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service à modifier.
2. Cliquez dans la section Moniteurs, sélectionnez un moniteur, puis cliquez sur **Délier**.

Supprimer les moniteurs

August 20, 2021

Après avoir délié un moniteur que vous avez créé à partir de son service, vous pouvez supprimer ce moniteur de la configuration de Citrix ADC. (Si un moniteur est lié à un service, il ne peut pas être supprimé.)

Remarque : Lorsque vous supprimez des moniteurs liés à un service, le moniteur par défaut est lié au service. Vous ne pouvez pas supprimer les moniteurs par défaut.

Pour supprimer un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm lb monitor <monitorName> <type>
<!--NeedCopy-->
```

Exemple :

```
rm lb monitor monitor-HTTP-1 HTTP
<!--NeedCopy-->
```

Pour supprimer un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Sélectionnez un moniteur, puis cliquez sur **Supprimer**.

Afficher les moniteurs

August 20, 2021

Vous pouvez afficher les services et les groupes de services liés à un moniteur. Vous pouvez vérifier les paramètres d'un moniteur pour dépanner votre configuration Citrix ADC. La procédure suivante décrit les étapes pour afficher les liaisons d'un moniteur aux services et groupes de services.

Pour afficher les liaisons de moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
show lb monbindings <MonitorName>
<!--NeedCopy-->
```

Exemple :

```
show lb monbindings monitor-HTTP-1
<!--NeedCopy-->
```

Pour afficher les liaisons de moniteurs à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Sélectionnez un moniteur, puis dans la liste Action, cliquez sur **Afficher les liaisons**.

Pour afficher des moniteurs à l'aide de la CLI

À l'invite de commandes, tapez :

```
show lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
show lb mon monitor-HTTP-1
<!--NeedCopy-->
```

Pour afficher des moniteurs à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**. Les détails des moniteurs disponibles apparaissent dans le volet Moniteurs.

Fermer les connexions du moniteur

August 20, 2021

L'appliance Citrix ADC envoie des sondes aux services via les moniteurs liés aux services. Par défaut, le moniteur de l'appliance et le serveur physique suivent la procédure de prise de main complète, même pour les sondes du moniteur. Toutefois, cette procédure ajoute des frais généraux au processus de surveillance et peut ne pas être toujours nécessaire.

Pour le moniteur de type TCP, vous pouvez configurer l'appliance pour fermer une connexion moniteur-sonde après avoir reçu SYN-ACK du service. Pour ce faire, définissez la valeur du paramètre MonitorConnectionClose sur RESET. Si vous souhaitez que la connexion moniteur-sonde passe par la procédure complète, définissez la valeur sur FIN.

Remarque : Le paramètre MonitorConnectionClose s'applique uniquement aux moniteurs TCP et TCP par défaut.

Pour configurer la fermeture de la connexion moniteur à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
set lb parameter -monitorConnectionClose <monitor_conn_close_option>
<!--NeedCopy-->
```

Exemple

```
set lb parameter -monitorConnectionClose RESET
<!--NeedCopy-->
```

Pour configurer la fermeture de la connexion moniteur à l'aide de l'utilitaire de configuration :

1. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge**.
2. Sélectionnez **FIN** ou **Réinitialiser** .

Fermeture des connexions du moniteur au niveau du service ou du groupe de services

Vous pouvez également configurer l'appliance pour fermer une connexion de sonde moniteur au niveau du service et du groupe de services en définissant le paramètre MonConnectionClose. Si ce paramètre n'est pas défini, la connexion du moniteur est fermée à l'aide de la valeur définie dans les paramètres d'équilibrage de charge globale. Si ce paramètre est défini au niveau du service ou du groupe de services, la connexion du moniteur est fermée en envoyant un message de fin de connexion, avec le bit FIN ou RESET défini, au service ou au groupe de services.

Pour configurer la fermeture de la connexion moniteur au niveau du service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <service_name> -monConnectionClose ( RESET | FIN )
<!--NeedCopy-->
```


Pour configurer la fermeture de la connexion moniteur au niveau du groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1  set serviceGroup <service_name> -monConnectionClose ( RESET | FIN )
2 <!--NeedCopy-->
```

Pour configurer la fermeture de la connexion moniteur au niveau du service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Ajoutez ou modifiez un service et, dans **Paramètres de base**, définissez le **bit de fermeture de la connexion de surveillance**.

Pour configurer la fermeture de la connexion moniteur au niveau du groupe de services à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Ajoutez ou modifiez un groupe de services et, dans **Paramètres de base**, définissez le **bit de fermeture de la connexion de surveillance**.

> **Remarque :** Pour fermer une connexion moniteur-sonde à l'aide de paramètres d'équilibrage de charge globaux, vous pouvez configurer MonitorConnectionClose sur FIN ou RESET. Lorsque vous configurez le paramètre MonitorConnectionClose sur ;
>
> - FIN : L'appliance effectue une liaison TCP complète.
> - RESET : l'appliance ferme la connexion après avoir reçu le SYN-ACK du service.
>
> Dans la version plus légère de Citrix ADC CPX, la valeur du paramètre MonitorConnectionClose est définie sur RESET par défaut et ne peut pas être modifiée en FIN au niveau global. Toutefois, vous pouvez modifier le paramètre MonitorConnectionClose en FIN au niveau du service.

Ignorer la limite supérieure des connexions client pour les sondes de moniteur

August 20, 2021

En fonction de considérations telles que la capacité d'un serveur physique, vous pouvez spécifier une limite sur le nombre maximal de connexions client effectuées à n'importe quel service. Si vous avez défini une telle limite sur un service, l'appliance Citrix ADC cesse d'envoyer des demandes au service

lorsque le seuil est atteint et reprend l'envoi de connexions au service après que le nombre de connexions existantes ait atteint les limites. Vous pouvez configurer l'appliance pour ignorer cette vérification lorsqu'elle envoie des connexions moniteur-sonde à un service.

Remarque : vous ne pouvez pas ignorer la vérification des connexions client-maximum pour un service individuel. Si vous spécifiez cette option, elle s'applique à tous les moniteurs liés à tous les services configurés sur l'appliance Citrix ADC.

Pour définir l'option Skip MaxClients for Monitor Connections à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb parameter -monitorSkipMaxClient (ENABLED|DISABLED)
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -monitorSkipMaxClient enabled
<!--NeedCopy-->
```

Pour définir l'option Skip MaxClients for Monitor Connections à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge**.
2. Sélectionnez **Ignorer MaxClients pour la surveillance des connexions**.

Gérer un déploiement à grande échelle

August 20, 2021

L'appliance Citrix ADC contient plusieurs fonctionnalités utiles lors de la configuration d'un déploiement d'équilibrage de charge volumineux. Au lieu de configurer des serveurs et des services virtuels individuellement, vous pouvez créer des groupes de serveurs et de services virtuels. Vous pouvez également créer une gamme de serveurs et de services virtuels, et traduire ou masquer des adresses IP de serveur virtuel et de service.

Vous pouvez définir la persistance d'un groupe de serveurs virtuels. Vous pouvez lier des moniteurs à un groupe de services. La création d'une gamme de serveurs virtuels et de services de type iden-

tique vous permet de configurer et de configurer ces serveurs en une seule procédure. Cela réduit considérablement le temps nécessaire à la configuration de ces serveurs et services virtuels.

En traduisant ou en masquant des adresses IP, vous pouvez retirer des serveurs et des services virtuels. Vous pouvez ensuite apporter des modifications à votre infrastructure, sans reconfiguration étendue de votre service ni de définitions de serveurs virtuels.

Gammes de serveurs virtuels et de services

August 20, 2021

Lorsque vous configurez l'équilibrage de charge, vous pouvez créer des plages de serveurs et de services virtuels, éliminant ainsi la nécessité de configurer des serveurs et des services virtuels individuellement. Par exemple, vous pouvez utiliser une procédure unique pour créer trois serveurs virtuels avec trois adresses IP correspondantes. Lorsque plusieurs arguments utilisent une plage, les plages doivent être de même taille.

Voici les types de plages que vous pouvez spécifier lors de l'ajout de services et de serveurs virtuels à votre configuration :

- **Gammes numériques.** Au lieu de taper un seul nombre, vous pouvez spécifier une plage de nombres consécutifs.

  Par exemple, vous pouvez créer une plage de serveurs virtuels en spécifiant une adresse IP de départ, telle que 10.102.29.30, puis en tapant une valeur pour le dernier octet qui indique la plage, telle que 34. Dans cet exemple, cinq serveurs virtuels sont créés avec des adresses IP comprises entre 10.102.29.30 et 10.102.29.34.

  Remarque : Les adresses IP des serveurs et services virtuels doivent être consécutives.

- **Gammes alphabétiques.** Au lieu de saisir une lettre littérale, vous pouvez remplacer une plage par une lettre unique, par exemple [C-G]. Il en résulte que toutes les lettres de la fourchette sont incluses, dans ce cas C, D, E, F et G.

  Par exemple, si vous avez trois serveurs virtuels nommés et `Vserver-xVserver-yVserver-z`, au lieu de les configurer séparément, vous pouvez taper `vserver [x-z]` pour les configurer tous.

Création d'une gamme de serveurs virtuels

Pour créer une plage de serveurs virtuels à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :


```
add lb vserver <name>@ <protocol> -range <rangeValue> <IPAddress> [<
    port>]

add lb vserver <name>@[<rangeValue>]> <protocol> <IPAddress[<rangeValue
    >]> [<port>]
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-2 http -range 6 10.102.29.30 80
<!--NeedCopy-->
```

OU

```
add lb vserver vserver[P-R] http 10.102.29.[26-28] 80

vserver "vserverP" added

vserver "vserverQ" added

vserver "vserverR" added

Done
<!--NeedCopy-->
```

Pour créer une plage de serveurs virtuels à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
add lb vserver <name>@ <protocol> -range <rangeValue> <IPAddress> [<
    port>]

add lb vserver <name>@\*\*[\*\*<rangeValue>\*\*]\*\*> <protocol> <
    IPAddress[<rangeValue>]> [<port>]
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-2 http -range 6 10.102.29.30 80
<!--NeedCopy-->
```

OU

```
add lb vserver vserver[P-R] http 10.102.29.[26-28] 80
```



```
vserver "vserverP" added
vserver "vserverQ" added
vserver "vserverR" added
Done
<!--NeedCopy-->
```

Pour créer une gamme de serveurs virtuels à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ajoutez un serveur virtuel et spécifiez une plage.

Création d'une gamme de services

Si vous spécifiez une plage pour le nom du service, spécifiez également une plage pour l'adresse IP.

Pour créer une gamme de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande :

```
add service <name>@ <IP>@ <protocol> <port>
<!--NeedCopy-->
```

Exemple :

```
> add service serv[1-3] 10.102.29.[102-104] http 80
service "serv1" added
service "serv2" added
service "serv3" added
 Done
<!--NeedCopy-->
```

Configurer des groupes de services

August 20, 2021

La configuration d'un groupe de services vous permet de gérer un groupe de services aussi facilement qu'un seul service. Par exemple, si vous activez ou désactivez une option quelconque, telle que la compression, la surveillance de l'état ou l'arrêt gracieux, pour un groupe de services, l'option est activée pour tous les membres du groupe de services.

Après avoir créé un groupe de services, vous pouvez le lier à un serveur virtuel et ajouter des services au groupe. Vous pouvez également lier des moniteurs à des groupes de services.

Les membres d'un groupe de services sont identifiés par une adresse IP ou un nom de serveur.

L'utilisation de membres de groupe DBS (Domain-name based service) est avantageuse car vous n'avez pas besoin de reconfigurer le membre sur l'appliance Citrix ADC si l'adresse IP du membre change. L'appliance détecte automatiquement ces modifications via le serveur de noms configuré. Cette fonctionnalité est utile dans les scénarios cloud, où le fournisseur de services peut modifier un serveur physique ou modifier l'adresse IP d'un service. Si vous spécifiez un membre du groupe DBS, l'appliance apprend l'adresse IP de manière dynamique.

Vous pouvez lier les membres IP et DBS au même groupe de services.

Remarque : Si vous utilisez des membres du groupe de services DBS, assurez-vous qu'un serveur de noms est spécifié ou qu'un serveur DNS est configuré sur l'appliance Citrix ADC. Un nom de domaine est résolu en adresse IP uniquement si l'enregistrement d'adresse correspondant est présent sur l'appliance ou le serveur de noms.

Créer des groupes de services

Vous pouvez configurer jusqu'à 8192 groupes de services sur l'appliance Citrix ADC.

Pour créer un groupe de services à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
add servicegroup <ServiceGroupName> <Protocol>
<!--NeedCopy-->
```

Exemple :

```
add servicegroup Service-Group-1 HTTP
<!--NeedCopy-->
```

Pour créer un groupe de services à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**, puis ajoutez un groupe de services.

Lier un groupe de services à un serveur virtuel

Lorsque vous liez un groupe de services à un serveur virtuel, les services membres sont liés au serveur virtuel.

Pour lier un groupe de services à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb vserver <name>@ <serviceGroupName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-Group-1
<!--NeedCopy-->
```

Pour lier un groupe de services à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **Groupes de services**.

Lier un membre à un groupe de services

L'ajout de services à un groupe de services permet au groupe de services de gérer les serveurs. Vous pouvez ajouter les serveurs à un groupe de services en spécifiant les adresses IP ou les noms des serveurs.

Dans l'interface graphique, si vous souhaitez ajouter un membre du groupe de services basé sur un nom de domaine, sélectionnez **Serveur**.

Avec cette option, vous pouvez ajouter n'importe quel serveur auquel un nom a été attribué, qu'il s'agisse d'une adresse IP ou d'un nom attribué par l'utilisateur.

Pour ajouter des membres à un groupe de services à l'aide de l'interface de ligne de commande

Pour configurer un groupe de services, à l'invite de commandes, tapez :

```
bind servicegroup <serviceGroupName> (<IP>@ | <serverName>) <port>
<!--NeedCopy-->
```

Exemples :

```
bind servicegroup Service-Group-1 10.102.29.30 80

bind servicegroup Service-Group-2 1000:0000:0000:0000:0005:0600:700a
    :888b 80
```



```
4
5 bind servicegroup CitrixEdu s1.citrite.net
6 <!--NeedCopy-->
```

Pour ajouter des membres à un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Groupes de services** et ouvrez un groupe de services.
2. Cliquez dans la section Groupe de services et effectuez l'une des opérations suivantes :
   - Pour ajouter un membre de groupe de services IP, sélectionnez IP Based.
   - Pour ajouter un membre de groupe de services basé sur un nom de serveur, sélectionnez Basé sur le serveur.

   Si vous souhaitez ajouter un membre de groupe de services basé sur un nom de domaine, sélectionnez **Serveur**. Avec cette option, vous pouvez ajouter n'importe quel serveur auquel un nom a été attribué, qu'il s'agisse d'une adresse IP ou d'un nom attribué par l'utilisateur.
3. Si vous ajoutez un nouveau membre IP, tapez l'adresse IP dans la zone de texte Adresse IP. Si l'adresse IP utilise le format IPv6, activez la case à cocher IPv6, puis entrez l'adresse dans la zone de texte Adresse IP

   Remarque : Vous pouvez ajouter une plage d'adresses IP. Les adresses IP de la plage doivent être consécutives. Spécifiez la plage en entrant l'adresse IP de départ dans la zone de texte Adresse IP (par exemple, 10.102.29.30). Spécifiez l'octet de fin de la plage d'adresses IP dans la zone de texte sous Plage (par exemple, 35). Dans la zone de texte Port, tapez le port (par exemple, 80), puis cliquez sur Ajouter.
4. Cliquez sur Créer.

Lier un moniteur à un groupe de services

Lorsque vous créez un groupe de services, le moniteur par défaut du type approprié pour le groupe y est automatiquement lié. Les moniteurs sondent périodiquement les serveurs du groupe de services auquel ils sont liés et mettent à jour l'état des groupes de services.

Vous pouvez lier un moniteur différent de votre choix au groupe de services.

Pour lier un moniteur à un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 bind serviceGroup <serviceGroupName> -monitorName <string> -monState (
      ENABLED | DISABLED)
```



```
<!--NeedCopy-->
```

Exemple :

```
bind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1
<!--NeedCopy-->
```

Pour un moniteur de liaison à un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Ouvrez un groupe de services et, dans Paramètres avancés, cliquez sur **Moniteurs**.

Conserver l'état d'origine d'un membre du groupe de services après la désactivation et l'activation d'un serveur virtuel

À partir de la version 64.x, une nouvelle option globale, —retainDisableServer, vous permet de conserver l'état d'un membre d'un groupe de services lorsqu'un serveur est désactivé et réactivé.

Auparavant, l'état d'un membre passe de DISABLED à ENABLED dans les conditions suivantes :

- Deux applications sont déployées sur le même port sur un serveur virtuel.
- Deux groupes de services avec un membre commun sont liés à ce serveur virtuel, et le membre commun est activé dans un groupe et désactivé dans l'autre.
- Le serveur est désactivé, puis réactivé.

Dans ces conditions, la désactivation du serveur désactive tous les membres du groupe de services et la réactivation du serveur active tous les membres, par défaut, quel que soit leur état antérieur. Pour ramener les membres à l'état d'origine, vous devez désactiver manuellement ces membres dans le groupe de services. C'est une tâche lourde et sujette aux erreurs.

Gérer les groupes de services

October 5, 2021

Vous pouvez modifier les paramètres des services d'un groupe de services et effectuer des tâches telles que l'activation, la désactivation et la suppression de groupes de services. Vous pouvez également dissocier les membres d'un groupe de services. Pour plus d'informations sur les groupes de services, voir Configurer les groupes de services.

Modifier un groupe de services

Vous pouvez modifier les attributs des membres du groupe de services. Vous pouvez définir plusieurs attributs du groupe de services, tels que le nombre maximal de clients et la compression. Les attributs sont définis sur les serveurs individuels du groupe de services. Vous ne pouvez pas définir de paramètres sur le groupe de services tels que les informations de transport (adresse IP et port), le poids et l'ID du serveur.

Remarque : Un paramètre que vous définissez pour un groupe de services est appliqué aux serveurs membres du groupe, et non aux services individuels.

Pour modifier un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante avec un ou plusieurs des paramètres facultatifs :

```
set servicegroup <serviceGroupName> [-type <type>] [-maxClient <
    maxClient>] [-maxReq <maxReq>] [-cacheable (YES|NO)] [-cip (ENABLED|
    DISABLED)] [-cipHeader <cipHeader>] [-usip (YES|NO)] [-sc (ON|OFF)]
    [-sp (ON|OFF)] [-cltTimeout <cltTimeout>] [-svrTimeout <svrTimeout>]
     [-cka (YES|NO)] [-TCPB (YES|NO)] [-CMP (\*\*YES\*\*|\*\*NO\*\*)] [-
    maxBandwidth <maxBandwidth>] [-maxThreshold <maxThreshold>] [-state
    (ENABLED|DISABLED)] [-downStateFlush (ENABLED|DISABLED)
<!--NeedCopy-->
```

Exemple :

```
set servicegroup Service-Group-1 -type TRANSPARENT

set servicegroup Service-Group-1 -maxClient 4096

set servicegroup Service-Group-1 -maxReq 16384

set servicegroup Service-Group-1 -cacheable YES
<!--NeedCopy-->
```

Pour modifier un groupe de services à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**, puis ouvrez le groupe de services à modifier.

Supprimer un groupe de services

Lorsque vous supprimez un groupe de services, les serveurs liés au groupe conservent leurs paramètres individuels et continuent d'exister sur l'appliance Citrix ADC.

Pour supprimer un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Exemple :

```
rm servicegroup Service-Group-1
<!--NeedCopy-->
```

Pour supprimer un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Sélectionnez un groupe de services, puis cliquez sur **Supprimer**.

Délier un membre d'un groupe de services

Lorsque vous dissociez un membre du groupe de services, les attributs définis sur le groupe de services ne s'appliquent plus au membre que vous dissociez. Toutefois, les services membres conservent leurs paramètres individuels et continuent d'exister sur l'appliance Citrix ADC.

Pour dissocier des membres d'un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind servicegroup <serviceGroupName> <IP>@ [<port>]
<!--NeedCopy-->
```

Exemple :

```
unbind servicegroup Service-Group-1 10.102.29.30 80
<!--NeedCopy-->
```


Pour dissocier des membres d'un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Ouvrez un groupe de services et cliquez sur dans la section Membres du groupe de services.
3. Sélectionnez un membre du groupe de services, puis cliquez sur **Unbind (Délier)**.

Délier un groupe de services d'un serveur virtuel

Lorsque vous dissociez un groupe de services d'un serveur virtuel, les services membres sont déliés du serveur virtuel et continuent d'exister sur l'appliance Citrix ADC.

Pour dissocier un groupe de services d'un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind lb vserver <name>@ <ServiceGroupName>
<!--NeedCopy-->
```

Exemple :

```
unbind lb vserver Vserver-LB-1 Service-Group-1
<!--NeedCopy-->
```

Pour dissocier un groupe de services d'un serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Ouvrez le serveur virtuel et cliquez sur dans la section Groupe de services.
3. Sélectionnez le groupe de services, puis cliquez sur **Unbind (Délier)**.

Délier les moniteurs des groupes de services

Lorsque vous dissociez un moniteur d'un groupe de services, le moniteur que vous dissociez ne surveille plus les services individuels qui constituent le groupe.

Pour dissocier un moniteur d'un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
unbind serviceGroup <serviceGroupName> -monitorName <string>
<!--NeedCopy-->
```

Exemple :

```
unbind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1
<!--NeedCopy-->
```

Pour dissocier un moniteur d'un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Ouvrez un groupe de services, puis cliquez sur dans la section Moniteurs.
3. Sélectionnez un moniteur, puis cliquez sur **Unbind (Délier)**.

Activer ou désactiver un groupe de services

Lorsque vous activez un groupe de services et les serveurs, les services appartenant au groupe de services sont activés. De même, lorsqu'un service appartenant à un groupe de services est activé, le groupe de services et le service sont activés. Par défaut, les groupes de services sont activés.

Après avoir désactivé un service activé, vous pouvez afficher le service à l'aide de l'utilitaire de configuration ou de la ligne de commande pour voir le temps restant avant que le service ne tombe en panne.

Pour désactiver un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
disable servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Exemple :

```
disable servicegroup Service-Group-1
<!--NeedCopy-->
```

Pour désactiver un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Sélectionnez un groupe de services, puis dans la liste Action, cliquez sur **Désactiver**.

Pour activer un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
enable servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Exemple :

```
enable servicegroup Service-Group-1
<!--NeedCopy-->
```

Pour activer un groupe de services à l'aide de l'utilitaire de configuration

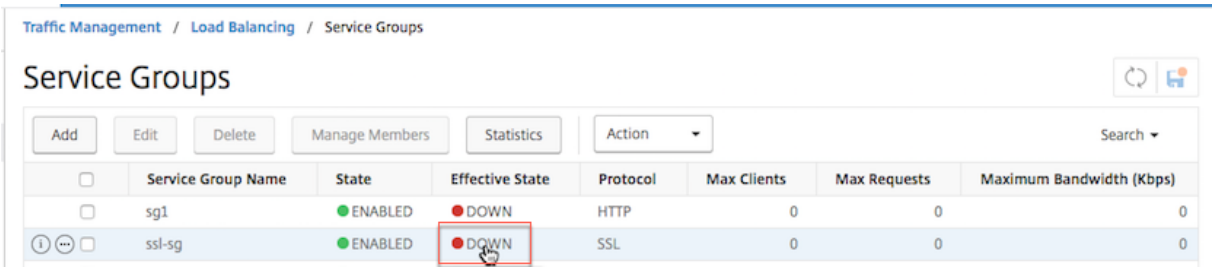
1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Sélectionnez un groupe de services, puis dans la liste Action, cliquez sur **Activer**.

Afficher le statut des membres des groupes de services

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.

Dans la page Groupes de services, la colonne **État effectif** affiche le statut des groupes de services. L'état HAUS/BAS dans la colonne **État effectif** est cliquable. Vous pouvez cliquer sur le statut et obtenir la liste des membres ainsi que leur statut dans la même vue. Sélectionnez un membre et cliquez sur le bouton **Surveiller les détails** pour afficher la raison de l'état en PANNE.

Remarque : Avant la version 12.0 de NetScaler version 56.20, l'état de la colonne **État effectif** n'était pas cliquable.



Affichage des propriétés d'un groupe de services

Vous pouvez afficher les paramètres suivants des groupes de services configurés :

- Nom
- Adresse IP
- State

- Protocole
- Connexions client maximales
- Nombre maximal de demandes par connexion
- Bande passante maximale
- Seuil de surveillance

L'affichage des détails de la configuration peut être utile pour résoudre les problèmes de votre configuration.

Pour afficher les propriétés d'un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour afficher les propriétés du groupe ou les propriétés et les membres du groupe :

```
show servicegroup <ServiceGroupName>

show servicegroup <ServiceGroupName> -includemembers
<!--NeedCopy-->
```

Exemple :

```
show servicegroup Service-Group-1
<!--NeedCopy-->
```

Pour afficher les propriétés d'un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Cliquez sur la flèche en regard du groupe de services.

Affichage des statistiques des groupes de services

Vous pouvez afficher les données statistiques du groupe de services, telles que le taux de demandes, les réponses, les octets de demande et les octets de réponse. L'appliance Citrix ADC utilise les statistiques d'un groupe de services pour équilibrer la charge sur les services.

Pour afficher les statistiques d'un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
stat servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Exemple :

```
stat servicegroup Service-Group-1
<!--NeedCopy-->
```

Pour afficher les statistiques d'un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Sélectionnez un groupe de services, puis cliquez sur **Statistiques**.

Serveurs virtuels d'équilibrage de charge liés à un groupe de services

Dans les déploiements à grande échelle, le même groupe de services peut être lié à plusieurs serveurs virtuels d'équilibrage de charge. Dans ce cas, au lieu d'afficher chaque serveur virtuel pour voir le groupe de services auquel il est lié, vous pouvez afficher la liste de tous les serveurs virtuels d'équilibrage de charge liés à un groupe de services. Vous pouvez afficher les détails suivants de chaque serveur virtuel :

- Nom
- State
- Adresse IP
- Port

Pour afficher les serveurs virtuels liés à un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour afficher les serveurs virtuels liés à un groupe de services :

```
show servicegroupbindings <serviceGroupName>
<!--NeedCopy-->
```

Exemple :

```
> show servicegroupbindings SVCGRPDTLS
SVCGRPDTLS - State :ENABLED
1) Test-pers (10.10.10.3:80) - State : DOWN
2) BRVSERV (10.10.1.1:80) - State : DOWN
3) OneMore (10.102.29.136:80) - State : DOWN
```



```
4) LBVIP1 (10.102.29.66:80) - State : UP
Done
>
<!--NeedCopy-->
```

Pour afficher les serveurs virtuels liés à un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Sélectionnez un groupe de services et, dans la liste Action, cliquez sur **Afficher les liaisons**.

Configurer un ensemble de membres de groupe de services souhaité pour un groupe de services dans un appel d'API NITRO

August 20, 2021

La prise en charge est ajoutée pour configurer un ensemble de membres de groupe de services souhaité pour un groupe de services dans un appel d'API NITRO. Une nouvelle API, Desired State API, est ajoutée pour prendre en charge cette configuration. En utilisant l'API d'état désiré, vous pouvez :

- Fournissez une liste des membres du groupe de services dans une seule requête PUT sur la ressource « servicegroup_servicegroupmemberlist_binding ».
- Indiquez leur poids et leur état (facultatif) dans cette requête PUT.
- Synchronisez efficacement la configuration de l'appliance avec les modifications de déploiement autour des serveurs d'applications.

L'appliance Citrix ADC compare le jeu de membres souhaité demandé avec le jeu de membres configuré. Ensuite, il lie automatiquement les nouveaux membres et délie les membres qui ne sont pas présents dans la demande.

Remarque :

- Cette fonctionnalité est prise en charge uniquement pour les groupes de services de type`API`.
- Vous pouvez uniquement lier des services basés sur l'adresse IP à l'aide de l'API État désiré, les services basés sur le nom de domaine ne sont pas autorisés.
- Auparavant, un seul membre du groupe de services peut être lié dans un appel NITRO.

> **Important**
>
> L'API d'état souhaitée pour l'appartenance à ServiceGroup est prise en charge dans le déploiement de cluster Citrix ADC.

Cas d'utilisation : Synchroniser les modifications de déploiement vers l'appliance Citrix ADC dans des déploiements à grande échelle, tels que Kubernetes

Dans les déploiements à grande échelle et hautement dynamiques (par exemple Kubernetes), le défi consiste à maintenir la configuration de l'appliance à jour en fonction du rythme de changement des déploiements afin de servir avec précision le trafic applicatif. Dans de tels déploiements, les contrôleurs (Ingress ou E-W Controller) sont responsables de la mise à jour de la configuration de ADC. Chaque fois que des modifications sont apportées au déploiement, `kube-api server` envoie l'ensemble effectif de points de terminaison via l' « événement Endpoints » au contrôleur. Le Controller utilise l'approche Read-Delta-Modify où il effectue les opérations suivantes :

- Récupère le jeu de points de terminaison actuellement configuré (ensemble de membres de groupe de services d'un groupe de services) pour le service à partir de l'appliance ADC.
- Compare le jeu de points de terminaison configuré avec l'ensemble de l'événement reçu.
- Lie les nouveaux points de terminaison (membres du groupe de services) ou délie les points de terminaison supprimés.

Étant donné que le taux de modification et la taille des services sont élevés dans cet environnement, cette méthode de configuration n'est pas efficace et peut retarder les mises à jour de configuration.

L'API d'état désiré résout le problème en acceptant le jeu de membres prévu pour un groupe de services dans une seule API, et met à jour efficacement la configuration.

Créer un groupe de services de type API à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
1 add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
     autoScale>]
```

Exemple :

```
1 add serviceGroup svg1 HTTP -autoScale API
```

Vous pouvez configurer les paramètres `autoDisablegraceful`, `autoDisabledelay` et `autoScale` à l'aide de la commande add serviceGroup ou set serviceGroup.

```
1 add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
     autoScale>] [-autoDisablegraceful ( YES | NO)] [-autoDisabledelay <
     secs>]
2
3 add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale (API |
     CLOUD | DISABLED| DNS |POLICY)]
4
```



```
5 set serviceGroup <serviceGroupName [-autoDisablegraceful ( YES | NO)]
     [-autoDisabledelay <secs>]
6
7 set serviceGroup <serviceGroupName [-autoScale (API |CLOUD | DISABLED|
     DNS |POLICY)]
```

Exemple :

```
1 add serviceGroup svg1 HTTP autoDisablegraceful YES -autoDisabledelay
     100
2
3 add serviceGroup svg1 HTTP -autoScale API
4
5 set serviceGroup svg1 -autoDisablegraceful  YES -autoDisabledelay 100
6
7 set serviceGroup svg1 -autoScale API
```

Arguments

autoDisablegraceful

Indique l'arrêt progressif du service. Si cette option est activée, l'appliance attend la fermeture de toutes les connexions en attente à ce service avant de supprimer le service. Pour les clients qui ont déjà une session persistante sur le système, de nouvelles connexions ou demandes continuent d'être envoyées à ce service. Le membre de service est supprimé uniquement s'il n'y a pas de connexions en attente. Valeur par défaut : NO

autoDisabledelay

Indique le temps autorisé (en secondes) pour un arrêt progressif. Pendant cette période, de nouvelles connexions ou demandes continuent d'être envoyées à ce service pour les clients qui ont déjà une session persistante sur le système. Les connexions ou les demandes de nouveaux clients qui n'ont pas de session de persistance sur le système ne sont pas envoyées au service. Au lieu de cela, ils sont équilibrés entre les autres services disponibles. Après l'expiration du délai, le membre du service est supprimé.

API Autoscale

Active l'utilisation de l'API État désiré pour lier le jeu de membres à un groupe de services prévu. Vous pouvez définir le groupe de services de non-mise à l'échelle automatique au type Mise à l'échelle automatique de l'API État désiré, si toutes les conditions fournies correspondent.

La commande set ServiceGroup Autoscale peut échouer si les liaisons de membres existantes remplissent l'une des conditions suivantes :

- Si le serveur lié au groupe de services est un serveur de noms ou un serveur de domaine.
- Si le nom du serveur lié au groupe de services est une adresse IP, il doit correspondre à l'adresse IP du serveur réelle. Dans l'exemple suivant, le nom du serveur et l'adresse IP du serveur ne correspondent pas.
  - **CLI :** ajout du *nom du serveur d'adresses IP du serveur*
  - **Exemple :** add server 1.2.3.4 4.3.2.1
- Si le nom du serveur de bouclage est autre que 127.0.0.1 ou 0000:0000:0000:0000:0000:0000:0000:0001.
- Si vous choisissez différents types de mise à l'échelle automatique (Cloud, API, DNS et stratégie) dans une commande set ServiceGroup et ajoutez la commande ServiceGroup.

Important :

- Les paramètres AutoDisableGraceful et AutoDisableDelay ne s'appliquent qu'aux groupes de services de type Autoscale « API » et « CLOUD ».
- Si les paramètres autoDisablegraceful ou autoDisabledelay ne sont pas configurés, les membres du service sont immédiatement supprimés.

Délier gracieusement un membre du groupe de services

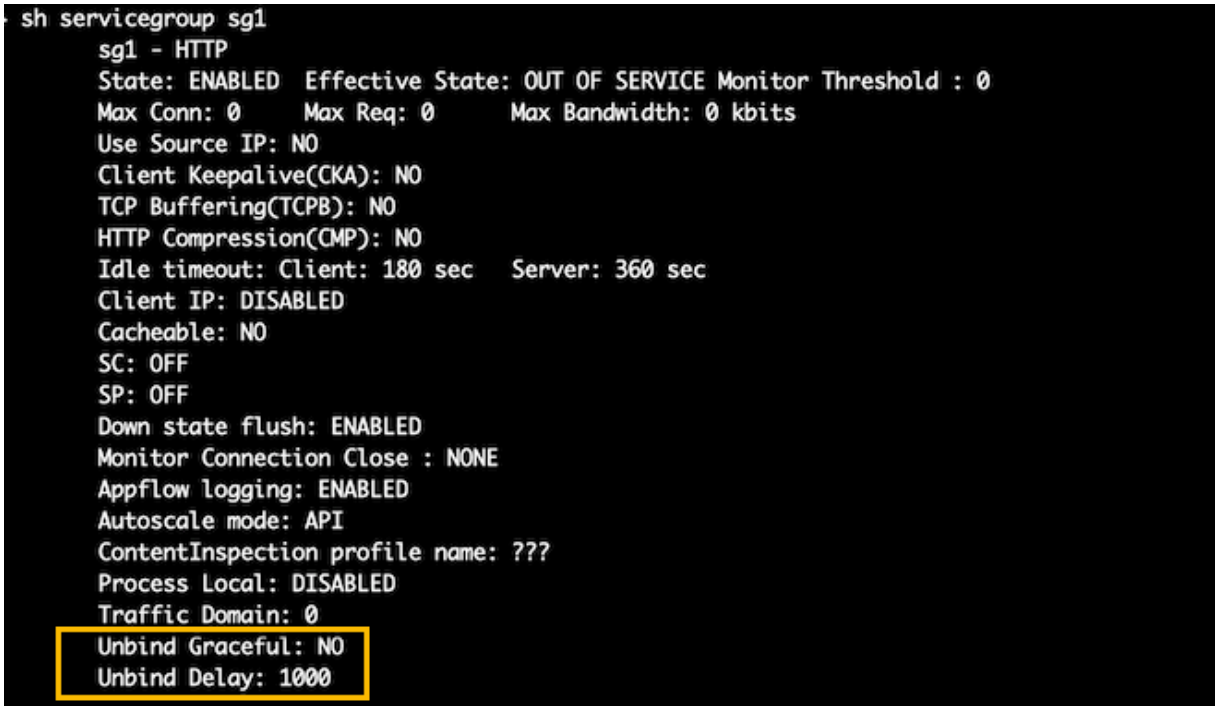
Si l'un des membres du groupe de services ne figure pas dans la liste d'état souhaitée, ces membres sont gracieusement non liés en fonction de la configuration des paramètres `autoDisablegraceful` ou `autoDisabledelay`.

- Si l'un de ces paramètres est défini, le membre du groupe de services est non lié gracieusement.
- Si aucun de ces paramètres n'est défini, le membre du groupe de services est immédiatement indépendant.

Remarque :

- Les membres du groupe de services identifiés pour une déliaison gracieuse sont affichés uniquement lorsque la commande show service group est exécutée.
- Vous ne pouvez pas effectuer d'opération (définie, non définie, par exemple) sur le membre du groupe de services identifié pour la déliaison gracieuse.

La figure suivante présente un exemple de commande show service group.

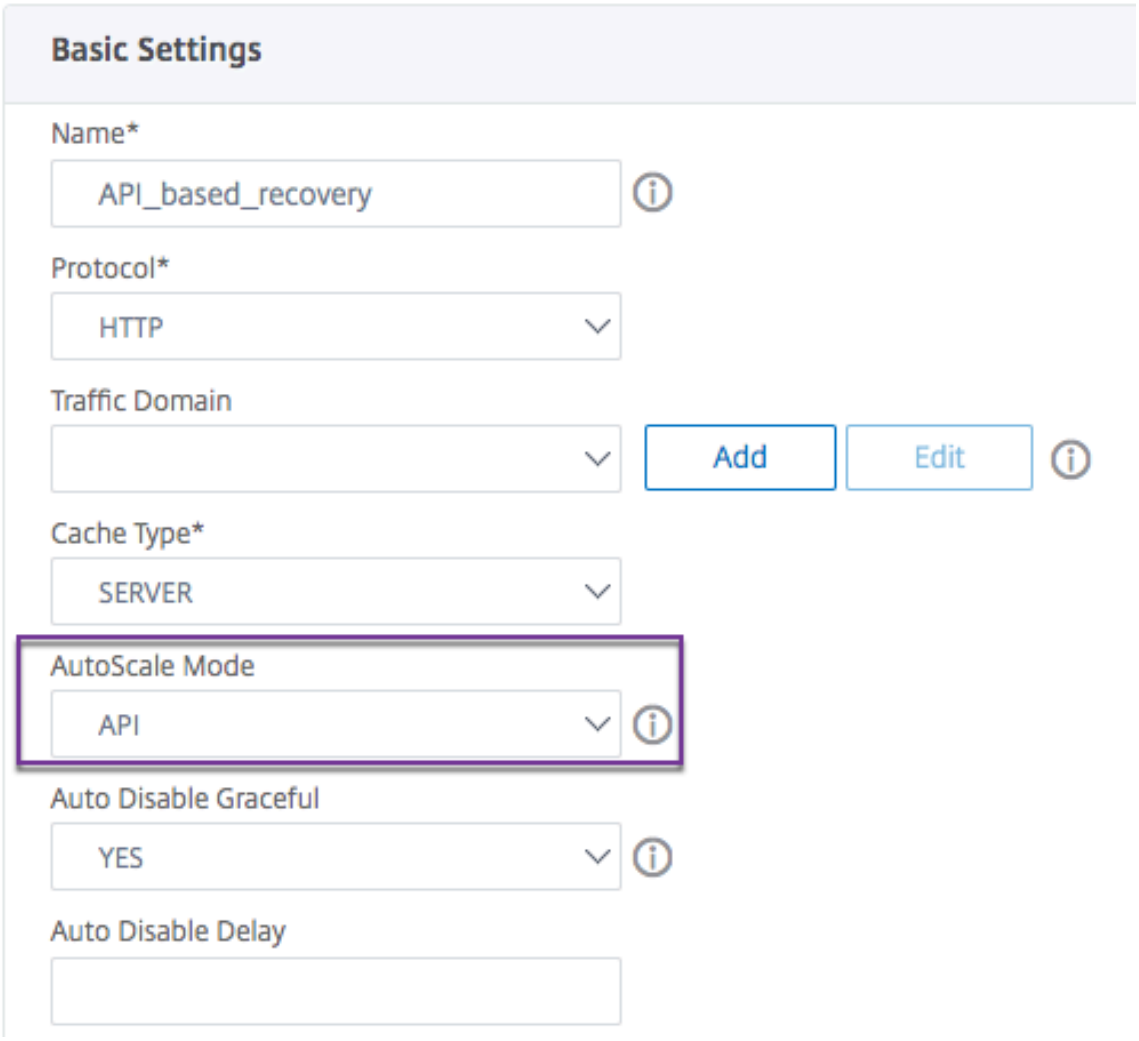


Créer un groupe de services de type API à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Groupes de services**, puis cliquez sur **Ajouter**.
2. En **mode AutoScale**, sélectionnez **API**.

Configurez l'arrêt progressif ou un délai pour un groupe de services de type API à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Groupes de services**.



2. En **mode AutoScale**, sélectionnez **API**.
3. Dans **Auto Disable Graceful**, sélectionnez **YES**.
4. Dans **Auto Disable Delay**, entrez le temps d'attente pour un arrêt progressif.

Remarque : Les champs **Auto Disable Graceful** ou **Auto Display Delay** sont activés uniquement si vous sélectionnez **API** ou **CLOUD** en **mode AutoScale**.

Configurer la mise à l'échelle automatique du groupe de services basé sur le domaine

August 20, 2021

Un groupe de services basé sur un domaine est constitué de membres dont les adresses IP sont obtenues en résolvant les noms de domaine des serveurs liés au groupe de services. Les noms de

domaine sont résolus par un serveur de noms dont vous configurez les détails sur l'appliance. Un groupe de services basé sur un domaine peut également inclure des membres basés sur l'adresse IP.

Le processus de résolution de noms pour un serveur basé sur un domaine peut renvoyer plusieurs adresses IP. Le nombre d'adresses IP dans la réponse DNS est déterminé par le nombre d'enregistrements d'adresse (A) configurés pour le nom de domaine, sur le serveur de noms. Même si le processus de résolution de noms renvoie plusieurs adresses IP, une seule adresse IP est liée au groupe de services. Pour augmenter ou réduire l'échelle d'un groupe de services, vous devez lier et dissocier manuellement d'autres serveurs basés sur un domaine vers et depuis le groupe de services, respectivement.

Toutefois, vous pouvez configurer un groupe de services basé sur un domaine pour qu'il soit mis à l'échelle automatiquement en fonction de l'ensemble complet des adresses IP renvoyées par un serveur de noms DNS pour un serveur basé sur un domaine. Pour configurer la mise à l'échelle automatique, lors de la liaison d'un serveur basé sur un domaine à un groupe de services, activez l'option de mise à l'échelle automatique. Voici les étapes de configuration d'un groupe de services basé sur le domaine qui évolue automatiquement :

- Ajoutez un serveur de noms pour résoudre les noms de domaine. Pour plus d'informations sur la configuration d'un serveur de noms sur l'appliance, voir Ajout d'un serveur de noms.
- Ajoutez un serveur basé sur un domaine. Pour plus d'informations sur l'ajout d'un serveur basé sur un domaine, voir Configuration d'un objet serveur.
- Ajoutez un groupe de services et associez le serveur basé sur le domaine au groupe de services, l'option Mise à l'échelle automatique étant définie sur DNS. Pour plus d'informations sur l'ajout d'un groupe de services, reportez-vous à la section Configuration des groupes de services.

Lorsqu'un serveur basé sur un domaine est lié à un groupe de services et que l'option de mise à l'échelle automatique est définie sur la liaison, un moniteur UDP et un moniteur TCP sont automatiquement créés et liés au serveur basé sur le domaine. Les deux moniteurs fonctionnent comme des résolveurs. Le moniteur TCP est désactivé par défaut et l'appliance utilise le moniteur UDP pour envoyer des requêtes DNS au serveur de noms afin de résoudre le nom de domaine. Si la réponse DNS est tronquée (l'indicateur TC est défini sur 1), l'appliance revient à TCP et utilise le moniteur TCP pour envoyer les requêtes DNS via TCP. Par la suite, l'appliance continue d'utiliser uniquement le moniteur TCP.

La réponse DNS du serveur de noms peut contenir plusieurs adresses IP pour le nom de domaine. Lorsque l'option de mise à l'échelle automatique est définie, l'appliance interroge chacune des adresses IP à l'aide du moniteur par défaut, puis inclut dans le groupe de services uniquement les adresses IP disponibles. Une fois les enregistrements d'adresse IP expirés, tels que définis par leurs valeurs de durée de vie (TTL), le moniteur UDP (ou le moniteur TCP, si l'appliance est revenue à utiliser le moniteur TCP) interroge le serveur de noms pour la résolution de domaine et inclut toute nouvelle adresse IP dans le groupe de services. Si une adresse IP faisant partie du groupe de services n'est pas présente dans la réponse DNS, l'appliance supprime cette adresse du groupe de services

après la fermeture gracieuse des connexions existantes au membre du groupe, processus au cours duquel elle ne permet pas d'établir de nouvelles connexions avec le membre. Si un nom de domaine qui s'est résolu avec succès dans le passé donne lieu à une réponse NXDOMAIN, tous les membres du groupe de services associés à ce domaine sont supprimés.

Les membres statiques (basés sur l'adresse IP) et les membres basés sur le domaine à mise à l'échelle dynamique peuvent coexister dans un groupe de services. Vous pouvez également lier des membres ayant des noms de domaine différents à un groupe de services avec l'option de mise à l'échelle automatique définie. Toutefois, chaque nom de domaine associé à un groupe de services doit être unique au sein du groupe de services. Vous devez activer l'option de mise à l'échelle automatique pour chaque serveur basé sur le domaine que vous souhaitez utiliser pour la mise à l'échelle automatique du groupe de services. Si une adresse IP est commune à un ou plusieurs domaines, l'adresse IP n'est ajoutée qu'une seule fois au groupe de services.

> **Important**
>
> - La mise à l'échelle automatique DNS est prise en charge dans un déploiement de cluster.
> - La surveillance des chemins pour les groupes de services à l'échelle automatique n'est pas prise en charge dans le déploiement de cluster

Pour configurer un groupe de services pour qu'il évolue automatiquement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le groupe de services et vérifier la configuration :

```
add serviceGroup <serviceGroupName> -autoScale (YES | NO)

show serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Exemple

Dans l'exemple suivant, server1 est un serveur basé sur le domaine. La réponse DNS contient plusieurs adresses IP. Cinq adresses sont disponibles et sont ajoutées au groupe de services.

```
> add serviceGroup servGroup server1 80 -autoScale YES
 Done
> sh servicegroup servGroup
       servGroup - HTTP
        State: ENABLED  Monitor Threshold : 0
              . . .
              . . .
```



```
        1)   192.0.2.31:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        2)   192.0.2.32:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        3)   192.0.2.36:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        4)   192.0.2.55:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        5)   192.0.2.80:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.
 Done
<!--NeedCopy-->
```

Pour configurer un groupe de services pour qu'il évolue automatiquement à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Créez un groupe de services et définissez le mode Mise à l'échelle automatique sur DNS.

Remplacer les valeurs TTL

> **Remarque** : Cette option est prise en charge par Citrix ADC 12.1 build 51.xx et versions ultérieures.

L'appliance Citrix ADC est configurée pour interroger périodiquement le serveur DNS pour toute mise à jour de l'enregistrement SRV associé à l'application au démarrage de l'application. Par défaut, la périodicité de cette requête dépend de la TTL publiée dans l'enregistrement SRV. Dans les applications microservice ou cloud world, les déploiements changent de manière plus dynamique. Par conséquent, les proxys doivent être plus rapides dans l'absorption des modifications apportées au déploiement des applications. Par conséquent, il est recommandé aux utilisateurs de définir explicitement le paramètre TTL de service basé sur le domaine sur une valeur inférieure à la TTL d'enregistrement SRV et optimale pour votre déploiement. Vous pouvez remplacer la valeur TTL par deux méthodes :

- Lors de la liaison d'un membre au groupe de services
- Définition de la valeur TTL globalement à l'aide de la commande set lb parameter.

Si la valeur TTL est configurée à la fois lors de la liaison du membre du groupe de services et également globalement, la valeur TTL spécifiée lors de la liaison du membre du groupe de services est prioritaire. Si la valeur TTL n'est pas spécifiée lors de la liaison d'un membre d'un groupe de services ou au niveau global, l'intervalle de surveillance DBS est dérivé de la valeur TTL dans la réponse DNS.

Remplacer les valeurs TTL à l'aide de l'interface de ligne de commande

- Pour écraser la valeur TTL lors de la liaison, à l'invite de commandes, tapez :

```
bind serviceGroup <serviceGroupName> (<serverName> [-dbsTTL <secs
    >])
<!--NeedCopy-->
```

Exemple :

```
bind servicegroup svc_grp_1 web_serv -dbsTTL 10
<!--NeedCopy-->
```

- Pour écraser globalement la valeur TTL, à l'invite de commandes, tapez :

```
set lb parameter [-dbsTTL <secs>]
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -dbsTTL 15
<!--NeedCopy-->
```


Remplacer les valeurs TTL à l'aide de l'interface graphique

Pour remplacer la valeur TTL lors de la liaison :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Dans la page **Groupes de services**, sélectionnez le groupe de services que vous avez créé et cliquez sur **Modifier**.
3. Dans la page **Groupes de services d'équilibrage** de charge, cliquez sur **Membres du groupe de services**.
4. Dans la page **Liaison de membres du groupe de services**, sélectionnez le serveur que vous avez créé et cliquez sur **Modifier**.
5. Dans **TTL de service basé sur le domaine**, entrez la valeur TTL.

Pour remplacer la valeur TTL au niveau global :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Modifier les paramètres d'équilibrage** de charge.
2. Dans **TTL de service basé sur le domaine**, entrez la valeur TTL.

> **Remarque :** Si la valeur TTL du serveur basé sur le domaine est définie sur 0, alors la valeur TTL du paquet de données est utilisée.

Spécification de différents serveurs de noms pour les liaisons de groupes de services et de noms de domaine

> **Remarque :** Cette option est prise en charge par Citrix ADC 12.1 build 51.xx et versions ultérieures.

Vous pouvez configurer différents serveurs de noms pour différents noms de domaine dans un groupe spécifique. La définition du paramètre NameServer est facultative lors de la liaison d'un serveur DBS au groupe de services. Lorsqu'un serveur de noms n'est pas spécifié lors de la liaison d'un membre au groupe de services, le serveur de noms configuré globalement est pris en compte.

Spécification de serveurs de noms lors de la liaison d'un serveur à des groupes de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 bind serviceGroup <serviceGroupName> (<serverName> [-nameServer <
     ip_addr>] [-dbsTTL <secs>])
2 <!--NeedCopy-->
```

Exemple :


```
bind servicegroup svc_grp_1 web_serv  -ns.nameserver.com 10.102.27.155
    -dbsTTL 10
<!--NeedCopy-->
```

Spécification de serveurs de noms lors de la liaison d'un serveur à des groupes de services à l'aide de l'interface graphique graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Dans la page **Groupes de services**, sélectionnez le groupe de services que vous avez créé et cliquez sur **Modifier**.
3. Dans la page **Groupes de services d'équilibrage** de charge, cliquez sur **Membres du groupe de services**.
4. Dans la page **Liaison de membres du groupe de services**, sélectionnez le serveur que vous avez créé et cliquez sur **Modifier**.
5. Dans **Name Server**, spécifiez le nom du serveur de noms auquel la requête du domaine lié doit être envoyée.

Découverte de service à l'aide d'enregistrements SRV DNS

August 20, 2021

Un enregistrement SRV (enregistrement de service) est une spécification de données dans le système de noms de domaine qui définit l'emplacement, c'est-à-dire le nom d'hôte et le numéro de port des serveurs pour les services spécifiés. L'enregistrement définit également le poids et la priorité de chaque serveur.

Exemple d'enregistrement SRV :

_http._tcp.example.com. 100 IN SRV 10 60 5060 a.example.com.

Le tableau suivant décrit chaque élément d'un enregistrement SRV :

Service	Protocol	Name	TTL	Class	SRV	Priority	Weight	Port	Target
HTTP	TCP	example.com	100	IN	SRV	10	60	5060	a.example.com

Vous pouvez utiliser les enregistrements SRV DNS pour découvrir les points de terminaison du service. L'appliance Citrix ADC est configurée pour interroger périodiquement les serveurs DNS avec l'enregistrement SRV associé à un service. Lors de la réception de l'enregistrement SRV, chaque hôte cible publié dans l'enregistrement SRV est lié à un groupe de services associé au service. Chacune des

liaisons hérite du port, de la priorité et du poids de l'enregistrement SRV. Pour chaque déploiement de service, l'utilisateur doit configurer l'appliance Citrix ADC une fois lors de sa mise en service, ce qui en fait un déploiement tactile unique pour les applications.

Important : le poids des membres du groupe de services appris dynamiquement ne peut pas être modifié à l'aide de l'interface de ligne de commande ou de l'interface graphique.

Cas d'utilisation : microservices d'équilibrage de charge

Les applications évoluent vers l'architecture microservice à partir d'architectures monolithiques. Le passage à l'architecture de microservices avec une solution d'échelle automatique du serveur back-end rend le déploiement d'applications plus dynamique. Pour prendre en charge un tel déploiement dynamique, les proxy ou ADC doivent être en mesure de détecter dynamiquement l'application ou les instances de service back-end et de les absorber dans la configuration du proxy.
La découverte de service à l'aide de DNS SRV enregistre la fonctionnalité facilite la configuration de l'appliance Citrix ADC dans un tel scénario de déploiement dynamique. Les développeurs d'applications peuvent utiliser certaines des plates-formes d'orchestration pour déployer l'application. Les plates-formes d'orchestration lors de l'instanciation de conteneurs pendant le déploiement d'applications peuvent ne pas attribuer le port standard spécifique au protocole pour chacun de ces conteneurs. Dans de tels scénarios, la découverte des informations de port devient la clé de la configuration de l'appliance Citrix ADC. Les enregistrements SRV sont utiles dans un tel scénario. Les paramètres d'enregistrement SRV tels que la priorité et le poids peuvent être utilisés pour un meilleur équilibrage de charge des applications.

- Le paramètre de priorité peut être utilisé pour dicter la priorité du pool de serveurs.
- Le paramètre de poids peut être utilisé pour dicter la capacité des instances de service back-end et peut donc être utilisé pour l'équilibrage de charge pondérée.
- Chaque fois qu'il y a une modification dans le pool de serveurs back-end, par exemple une instance back-end est supprimée du pool, l'instance n'est gracieusement supprimée qu'une fois toutes les connexions client existantes honorées.

> **Remarque :**
>
> - Une découverte de service basée sur les enregistrements A/AAAA, toutes les adresses IP résolues ont le même poids car vous affectez le poids au domaine en cours de résolution.
> - Si la pondération dans la réponse SRV est supérieure à 100, les services ne sont pas créés.

Équilibrage de charge basé sur la priorité à l'aide d'enregistrements SRV

Vous pouvez utiliser les enregistrements SRV pour effectuer un équilibrage de charge basé sur la priorité. Le pool de serveurs basé sur la priorité peut être une alternative pour les serveurs virtuels de

sauvegarde. Le fichier ns.conf nécessite une configuration minimale par rapport aux serveurs virtuels de sauvegarde.

Dans l'équilibrage de charge basé sur la priorité à l'aide d'enregistrements SRV, un numéro de priorité est attribué à chaque pool de serveurs. Le nombre le plus faible a la priorité la plus élevée. L'un des serveurs du pool de priorité la plus élevée est sélectionné pour l'équilibrage de charge en fonction de l'intégrité et de la disponibilité du serveur. Si tous les serveurs du pool de serveurs de priorité la plus élevée sont en panne, les serveurs qui ont la priorité la plus élevée sont sélectionnés pour l'équilibrage de charge. Toutefois, si les serveurs du pool de serveurs de priorité la plus élevée sont à nouveau activés, les serveurs sont de nouveau sélectionnés dans le pool de priorité la plus élevée.

Le passage d'un pool de serveurs prioritaires à un autre pool de serveurs se produit gracieusement en saignant les transactions client existantes. Par conséquent, les clients actuels ne voient aucune rupture dans l'accès à l'application.

Pour activer l'interrogation des enregistrements SRV à l'aide de l'interface de ligne de commande

Effectuez les tâches suivantes pour activer l'interrogation des enregistrements SRV :

1. Créez un serveur en spécifiant le paramètre de type de requête comme SRV.

   À l'invite de commandes, tapez :

   ```
   add server <name> <domain> [-queryType <queryType>])
   <!--NeedCopy-->
   ```

   Exemple :

   ```
   add server web_serv example.com -queryType SRV
   <!--NeedCopy-->
   ```

   Remarque :

   - Par défaut, les requêtes IPv4 sont envoyées. Pour envoyer des requêtes IPv6, vous devez activer le domaine IPv6.
   - Le nom de domaine cible SRV ne doit pas dépasser 127 caractères.

2. Créez un groupe de services avec le mode de mise à l'échelle automatique en tant que DNS.

   À l'invite de commandes, tapez :

   ```
   add serviceGroup <serviceGroupName> <serviceType> [-autoScale <
       autoScale>]
   <!--NeedCopy-->
   ```

   Exemple :


```
add servicegroup svc_grp_1 http -autoscale dns
<!--NeedCopy-->
```

3. Liez le serveur créé à l'étape 1 au groupe de services en tant que membre.

   À l'invite de commandes, tapez :

```
bind serviceGroup <serviceGroupName> <serverName>
<!--NeedCopy-->
```

   Exemple :

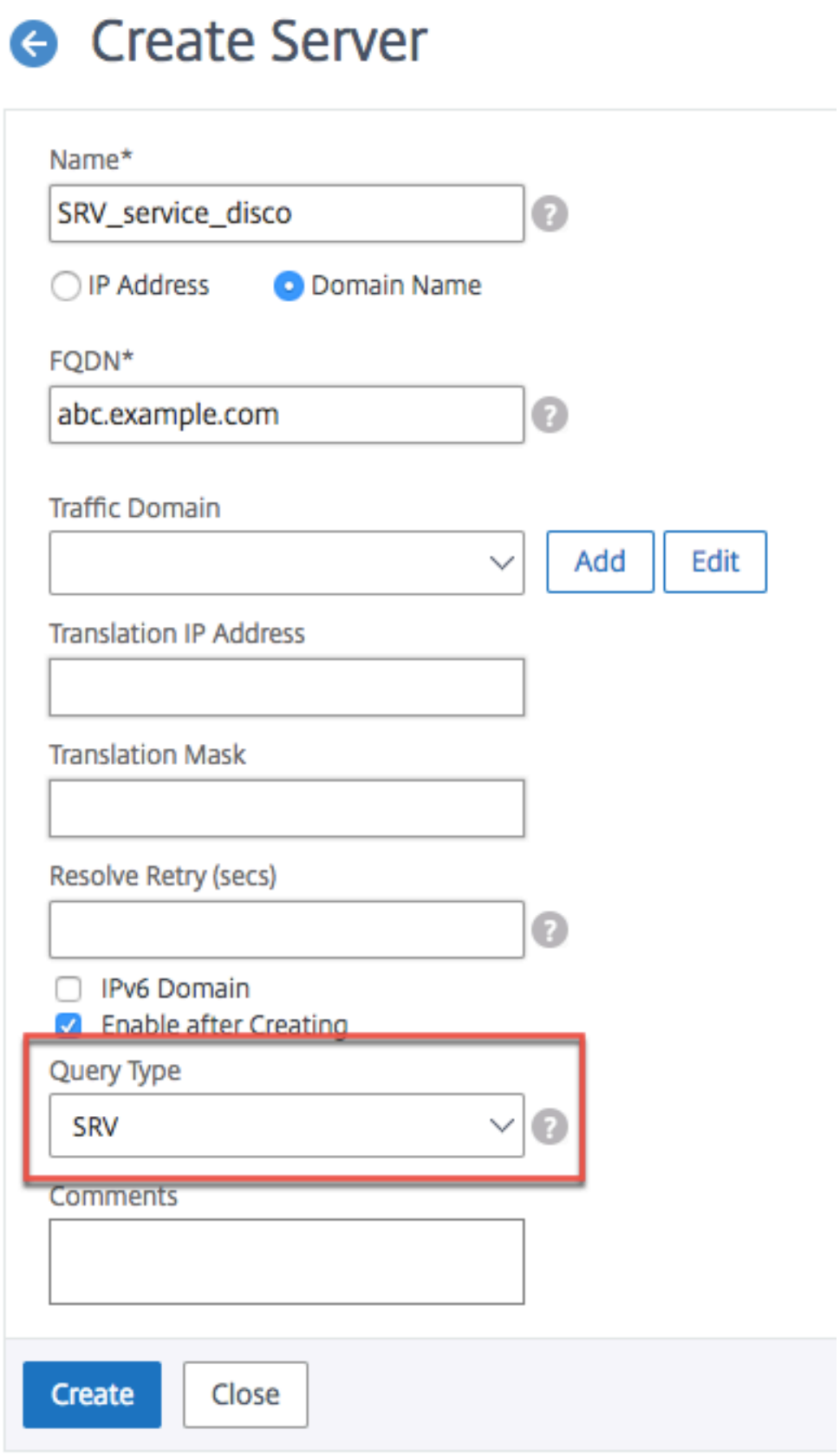
```
bind servicegroup svc_grp_1 web_serv
<!--NeedCopy-->
```

> **Remarque :**
>
> - Lorsque vous liez des serveurs à des membres du groupe de services, vous n'avez pas à entrer le numéro de port pour les types de serveurs SRV. Si vous spécifiez un numéro de port pour le type de serveur SRV, un message d'erreur s'affiche.
> - Vous pouvez éventuellement spécifier un serveur de noms et une valeur TTL tout en liant un serveur au groupe de services.

Pour activer l'interrogation des enregistrements SRV à l'aide de l'interface graphique

Créer un serveur

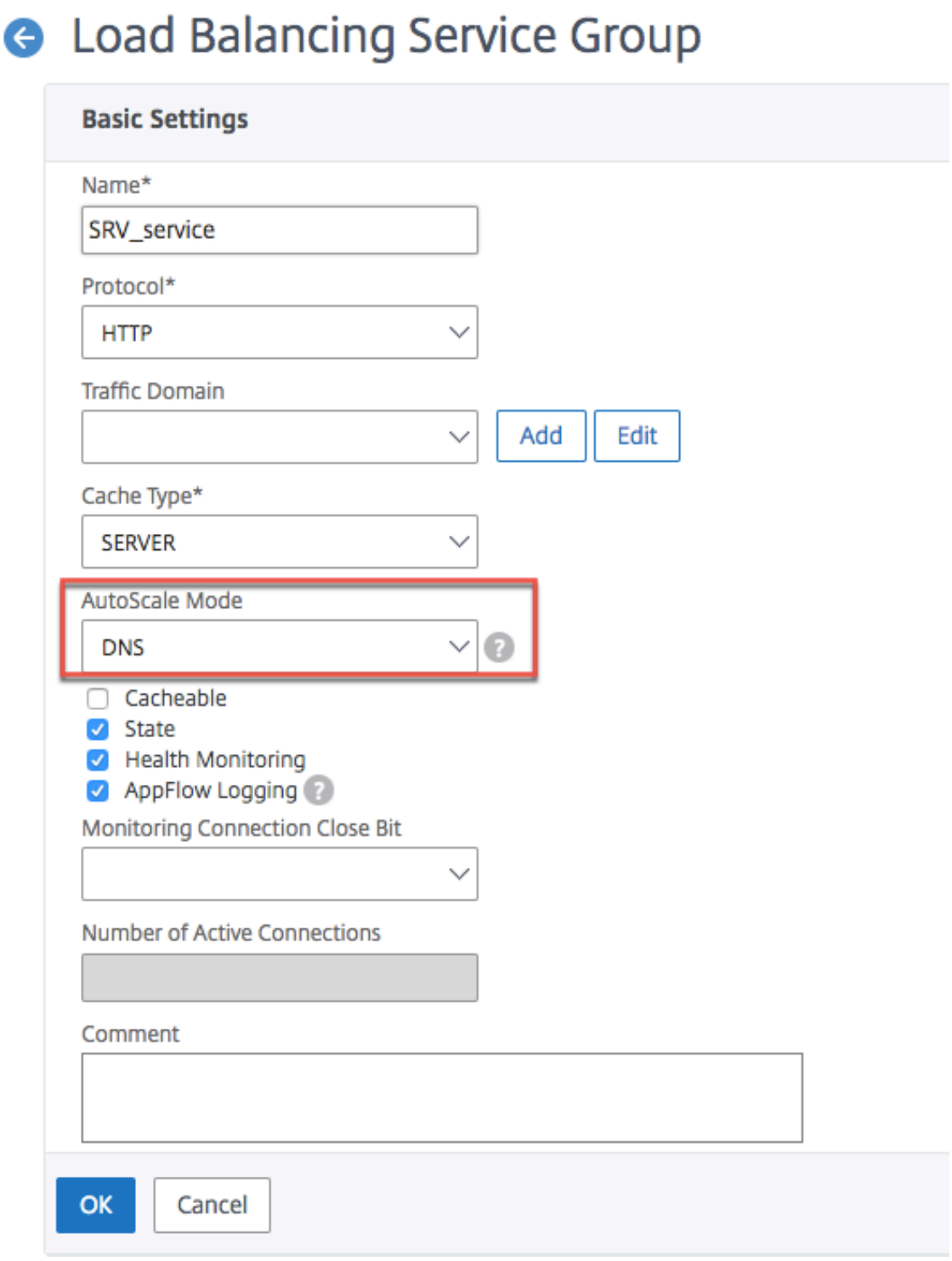
1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs**, puis cliquez sur **Ajouter** .



2. Dans la page **Créer un serveur**, sélectionnez nom de domaine.
3. Entrez les détails de tous les paramètres requis.
4. Dans **Type de requête**, sélectionnez **SRV**.
5. Cliquez sur **Créer**.

Créer un groupe de services avec le mode de mise à l'échelle automatique en tant que DNS

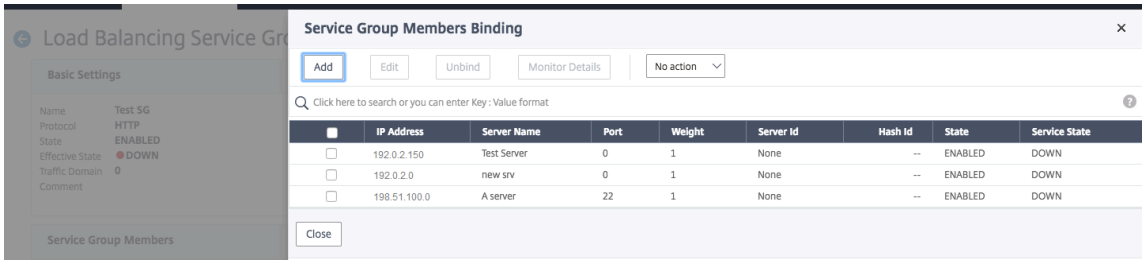
1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Dans la page **Groupe de services d'équilibrage** de charge, entrez les détails de tous les paramètres requis.
3. En **mode Mise à l'échelle automatique**, sélectionnez **DNS**.



4. Cliquez sur **OK**.

Lier le serveur au membre du groupe de services

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Dans la page **Groupes de services**, sélectionnez le groupe de services que vous avez créé et cliquez sur **Modifier**.
3. Dans la page **Groupes de services d'équilibrage** de charge, cliquez sur **Membres du groupe de services**.
4. Dans la page **Liaison de membres du groupe de services**, sélectionnez le serveur que vous avez créé et cliquez sur **Fermer** .



Remarque :

- Lors de la liaison, vous n'avez pas à entrer le numéro de port pour les types de serveur SRV. Si vous entrez un numéro de port pour le type de serveur SRV, un message d'erreur s'affiche.
- Vous pouvez éventuellement spécifier un serveur de noms et une valeur TTL tout en liant un serveur au groupe de services.

Remplacer les valeurs TTL

L'appliance Citrix ADC est configurée pour interroger périodiquement le serveur DNS pour toute mise à jour de l'enregistrement SRV associé à l'application au démarrage de l'application. Par défaut, la périodicité de cette requête dépend de la TTL publiée dans l'enregistrement SRV. Dans les applications microservice ou cloud world, les déploiements changent de manière plus dynamique. Par conséquent, les proxys doivent être plus rapides dans l'absorption des modifications apportées au déploiement des applications. Par conséquent, il est recommandé aux utilisateurs de définir explicitement le paramètre TTL de service basé sur le domaine sur une valeur inférieure à la TTL d'enregistrement SRV et optimale pour votre déploiement. Vous pouvez remplacer la valeur TTL par deux méthodes :

- Lors de la liaison d'un membre au groupe de services
- Définition de la valeur TTL globalement à l'aide de la commande set lb parameter.

Si la valeur TTL est configurée à la fois lors de la liaison du membre du groupe de services et également globalement, la valeur TTL spécifiée lors de la liaison du membre du groupe de services est prioritaire. Si la valeur TTL n'est pas spécifiée lors de la liaison d'un membre d'un groupe de services ou au niveau global, l'intervalle de surveillance DBS est dérivé de la valeur TTL dans la réponse DNS.

Remplacer les valeurs TTL à l'aide de l'interface de ligne de commande

- Pour écraser la valeur TTL lors de la liaison, à l'invite de commandes, tapez :

```
bind serviceGroup <serviceGroupName> (<serverName> [-dbsTTL <secs
   >])
<!--NeedCopy-->
```

Exemple :

```
bind servicegroup svc_grp_1 web_serv -dbsTTL 10
<!--NeedCopy-->
```

- Pour écraser globalement la valeur TTL, à l'invite de commandes, tapez :

```
set lb parameter [-dbsTTL <secs>]
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -dbsTTL 15
<!--NeedCopy-->
```

Remplacer les valeurs TTL à l'aide de l'interface graphique

Pour remplacer la valeur TTL lors de la liaison :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Dans la page **Groupes de services**, sélectionnez le groupe de services que vous avez créé et cliquez sur **Modifier**.
3. Dans la page **Groupes de services d'équilibrage** de charge, cliquez sur **Membres du groupe de services**.
4. Dans la page **Liaison de membres du groupe de services**, sélectionnez le serveur que vous avez créé et cliquez sur **Modifier**.
5. Dans **TTL de service basé sur le domaine**, entrez la valeur TTL.

Pour remplacer la valeur TTL au niveau global :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Modifier les paramètres d'équilibrage** de charge.
2. Dans **TTL de service basé sur le domaine**, entrez la valeur TTL.

> **Remarque** : Si la valeur TTL du serveur basé sur un domaine est définie sur 0, la valeur TTL du paquet de données est utilisée.

Spécification de différents serveurs de noms pour les liaisons de groupes de services et de noms de domaine

Vous pouvez configurer différents serveurs de noms pour différents noms de domaine dans un groupe spécifique. La définition du paramètre NameServer est facultative lors de la liaison d'un serveur DBS au groupe de services. Lorsqu'un serveur de noms n'est pas spécifié lors de la liaison d'un membre au groupe de services, le serveur de noms configuré globalement est pris en compte.

Spécification de serveurs de noms lors de la liaison d'un serveur à des groupes de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind serviceGroup <serviceGroupName> (<serverName> [-nameServer <
    ip_addr>] [-dbsTTL <secs>])
<!--NeedCopy-->
```

Exemple :

```
bind servicegroup svc_grp_1 web_serv  -ns.nameserver.com 10.102.27.155
    -dbsTTL 10
<!--NeedCopy-->
```

Spécification de serveurs de noms lors de la liaison d'un serveur à des groupes de services à l'aide de l'interface graphique graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Dans la page **Groupes de services**, sélectionnez le groupe de services que vous avez créé et cliquez sur **Modifier**.
3. Dans la page **Groupes de services d'équilibrage** de charge, cliquez sur **Membres du groupe de services**.
4. Dans la page **Liaison de membres du groupe de services**, sélectionnez le serveur que vous avez créé et cliquez sur **Modifier**.
5. Dans **Name Server**, spécifiez le nom du serveur de noms auquel la requête du domaine lié doit être envoyée.

Traduire l'adresse IP d'un serveur basé sur un domaine

August 20, 2021

Pour simplifier la maintenance sur l'appliance Citrix ADC et sur les serveurs de domaine qui lui sont connectés, vous pouvez configurer des masques d'adresses IP et des adresses IP de traduction. Ces fonctions fonctionnent ensemble pour analyser les paquets DNS entrants et remplacer une nouvelle adresse IP par une adresse IP résolue par le DNS.

Lorsqu'elle est configurée pour un serveur basé sur un domaine, la traduction d'adresses IP permet à l'appliance de localiser une autre adresse IP de serveur lorsque vous arrêtez le serveur pour maintenance ou si vous effectuez d'autres modifications d'infrastructure affectant le serveur.

Lors de la configuration du masque, vous devez utiliser des valeurs de masque IP standard (une puissance de deux, moins un) et des zéros, par exemple, 255.255.0.0. Les valeurs non nulles ne sont autorisées que dans les octets de départ.

Lorsque vous configurez une adresse IP de traduction pour un serveur, vous créez une correspondance 1:1 entre une adresse IP de serveur et un autre serveur qui partage des octets de début ou de fin dans son adresse IP. Le masque bloque des octets particuliers dans l'adresse IP du serveur d'origine. L'adresse IP résolue par le DNS est transformée en une nouvelle adresse IP en appliquant l'adresse IP de traduction et le masque de traduction.

Par exemple, vous pouvez configurer une adresse IP de traduction 10.20.0.0 et un masque de traduction 255.255.0.0. Si une adresse IP résolue par DNS pour un serveur est 40.50.27.3, cette adresse est transformée en 10.20.27.3. Dans ce cas, l'adresse IP de traduction fournit les deux premiers octets de la nouvelle adresse, et le masque passe par les deux derniers octets de l'adresse IP d'origine. La référence à l'adresse IP d'origine, telle que résolue par DNS, est perdue. Surveille tous les services auxquels le serveur est lié également un rapport sur l'adresse IP transformée.

Lors de la configuration d'une adresse IP de traduction pour un serveur basé sur un domaine, vous spécifiez un masque et une adresse IP vers laquelle l'adresse IP résolue par le DNS doit être traduite.

Remarque : La traduction de l'adresse IP n'est possible que pour les serveurs basés sur le domaine. Vous ne pouvez pas utiliser cette fonctionnalité pour les serveurs IP. Le modèle d'adresse peut être basé uniquement sur les adresses IPv4.

Pour configurer une adresse IP de traduction pour un serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
add server <name>@ <serverDomainName> -translationIp <
    translationIPAddress> -translationMask <netMask> -state <ENABLED|
    DISABLED>
<!--NeedCopy-->
```

Exemple :

```
add server myMaskedServer www.example.com -translationIp 10.10.10.10 -
    translationMask
255.255.0.0 -state ENABLED
<!--NeedCopy-->
```

Pour configurer une adresse IP de traduction pour un serveur à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs**, créez un serveur basé sur un domaine et spécifiez une adresse IP de traduction.

Masquer l'adresse IP d'un serveur virtuel

October 5, 2021

Vous pouvez configurer un masque et un modèle au lieu d'une adresse IP fixe pour un serveur virtuel. Cela permet de rediriger le trafic dirigé vers n'importe quelle adresse IP correspondant au masque et au modèle vers un serveur virtuel particulier. Par exemple, vous pouvez configurer un masque qui autorise la variable des trois premiers octets d'une adresse IP, de sorte que le trafic vers 111.11.11.198, 22.22.22.198 et 33.33.33.198 soit envoyé au même serveur virtuel.

En configurant un masque pour l'adresse IP d'un serveur virtuel, vous pouvez éviter la reconfiguration de vos serveurs virtuels en raison d'une modification du routage ou d'une autre modification de l'infrastructure. Le masque permet au trafic de continuer à circuler sans reconfiguration étendue de vos serveurs virtuels.

Le masque d'adresse IP d'un serveur virtuel fonctionne différemment d'une définition de modèle IP pour un serveur décrite dans la section Traduction de l'adresse IP d'un serveur de domaine. Pour un masque d'adresse IP de serveur virtuel, un masque non nul est interprété comme un octet considéré. Pour un service, la valeur non nulle est bloquée.

De plus, pour un masque d'adresse IP de serveur virtuel, les valeurs principales ou de fin peuvent être prises en compte. Si le masque d'adresse IP du serveur virtuel considère les valeurs de gauche de l'adresse IP, il s'agit d'un masque de transfert. Si le masque prend en compte les valeurs situées à droite de l'adresse, il s'agit d'un masque inversé.

Remarque : L'appliance Citrix ADC évalue tous les serveurs virtuels de masque avant d'évaluer les serveurs virtuels à masque inverse.

Lorsque vous masquez l'adresse IP d'un serveur virtuel, vous devez également créer un modèle d'adresse IP pour faire correspondre le trafic entrant avec le serveur virtuel approprié. Lorsque la solution matérielle-logicielle reçoit un paquet IP entrant, elle met en correspondance l'adresse IP de destination du paquet avec les bits pris en compte dans le modèle d'adresse IP, et après avoir trouvé une correspondance, elle applique le masque d'adresse IP pour construire l'adresse IP de destination finale.

Prenons l'exemple suivant :

- Adresse IP de destination dans le paquet entrant : 10.102.27.189
- Modèle d'adresse IP : 10.102.0.0
- Masque IP : 255.255.0.0
- Adresse IP de destination (finale) construite : 10.102.27.189.

Dans ce cas, les 16 premiers bits de l'adresse IP de destination d'origine correspondent au modèle d'adresse IP de ce serveur virtuel, de sorte que ce paquet entrant est routé vers ce serveur virtuel.

Si une adresse IP de destination correspond aux modèles IP de plusieurs serveurs virtuels, la correspondance la plus longue est prioritaire. Prenons l'exemple suivant :

- Serveur virtuel 1 : modèle IP 10.10.0.0, masque IP 255.255.0.0
- Serveur virtuel 2 : modèle IP 10.10.10.0, masque IP 255.255.255.0
- Adresse IP de destination dans le paquet : 10.10.10.45.
- Serveur virtuel sélectionné : Serveur virtuel 2.

Le modèle associé à Virtual Server 2 correspond à plus de bits que celui associé au serveur virtuel 1, de sorte que les adresses IP correspondantes sont envoyées à Virtual Server 2.

Remarque : Les ports sont également pris en compte si un disjoncteur est nécessaire.

Pour configurer un masque d'adresse IP de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lb vserver <name>@ http -ipPattern <ipAddressPattern> -ipMask <
     ipMask> <listenPort>
2 <!--NeedCopy-->
```

Exemple :

Correspondance de motifs basée sur des octets de préfixe :


```
add lb vserver myLBVserver http -ippattern 10.102.0.0 -ipmask
   255.255.0.0 80
<!--NeedCopy-->
```

Correspondance de motifs basée sur les octets de fin :

```
add lb vserver myLBVserver1 http -ippattern 0.0.22.74 -ipmask
   0.0.255.255 80
<!--NeedCopy-->
```

Modifier un serveur virtuel basé sur des modèles :

```
set lb vserver myLBVserver1 -ippattern 0.0.22.74 -ipmask 0.0.255.255
<!--NeedCopy-->
```

Si vous configurez le serveur virtuel 1 comme suit :

```
add lb vserver vs1 HTTP -ippattern 100.1.1.0 -ipmask 255.255.255.0 80
<!--NeedCopy-->
```

L'appliance Citrix ADC ne répond pas à une demande ARP sur toutes les adresses IP. Toutefois, il répond au trafic du serveur virtuel acheminé vers toutes les adresses IP de ce modèle.

Pour configurer un masque d'adresse IP de serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans la liste Type d'adresse, sélectionnez Modèle IP et spécifiez un modèle IP et un masque IP.

Configurer l'équilibrage de charge pour les protocoles couramment utilisés

August 20, 2021

Outre les sites Web et les applications Web, d'autres types d'applications déployées en réseau qui utilisent d'autres protocoles courants reçoivent souvent de grandes quantités de trafic et bénéficient donc de l'équilibrage de charge. Plusieurs de ces protocoles nécessitent des configurations spécifiques pour que l'équilibrage de charge fonctionne correctement. Parmi eux figurent FTP, DNS, SIP et RTSP.

Si vous configurez votre appliance Citrix ADC pour qu'elle utilise des noms de domaine pour vos serveurs plutôt que des adresses IP, vous devrez peut-être également configurer la traduction et le masquage IP pour ces serveurs.

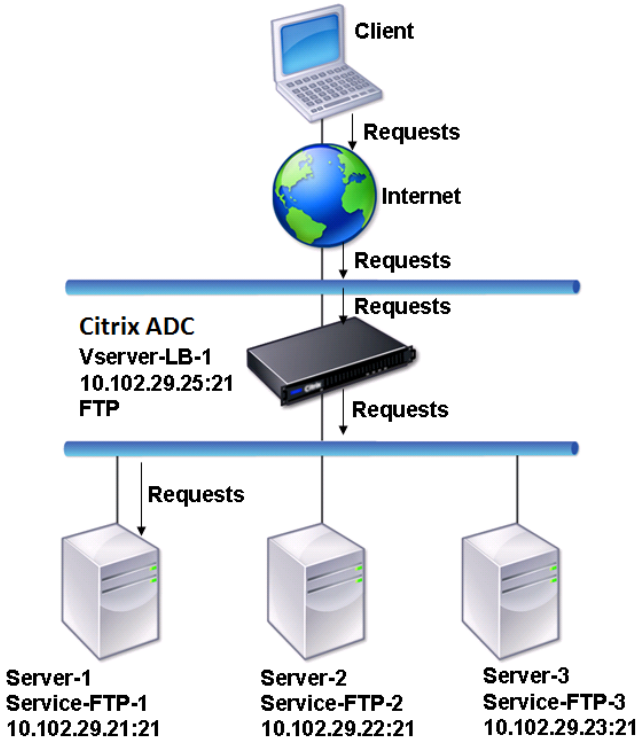
Équilibrer la charge d'un groupe de serveurs FTP

August 20, 2021

L'appliance Citrix ADC peut être utilisée pour équilibrer la charge des serveurs FTP. FTP exige que l'utilisateur initie deux connexions sur deux ports différents vers le même serveur : la connexion de contrôle, via laquelle le client envoie des commandes au serveur, et la connexion de données, via laquelle le serveur envoie des données au client. Lorsque le client lance une session FTP en ouvrant une connexion de contrôle au serveur FTP, l'appliance utilise la méthode d'équilibrage de charge configurée pour sélectionner un service FTP et lui transmet la connexion de contrôle. Le serveur FTP à équilibrage de charge ouvre ensuite une connexion de données au client pour l'échange d'informations.

Le diagramme suivant décrit la topologie d'une configuration d'équilibrage de charge pour un groupe de serveurs FTP.

Figure 1. Topologie d'équilibrage de charge de base pour les serveurs FTP



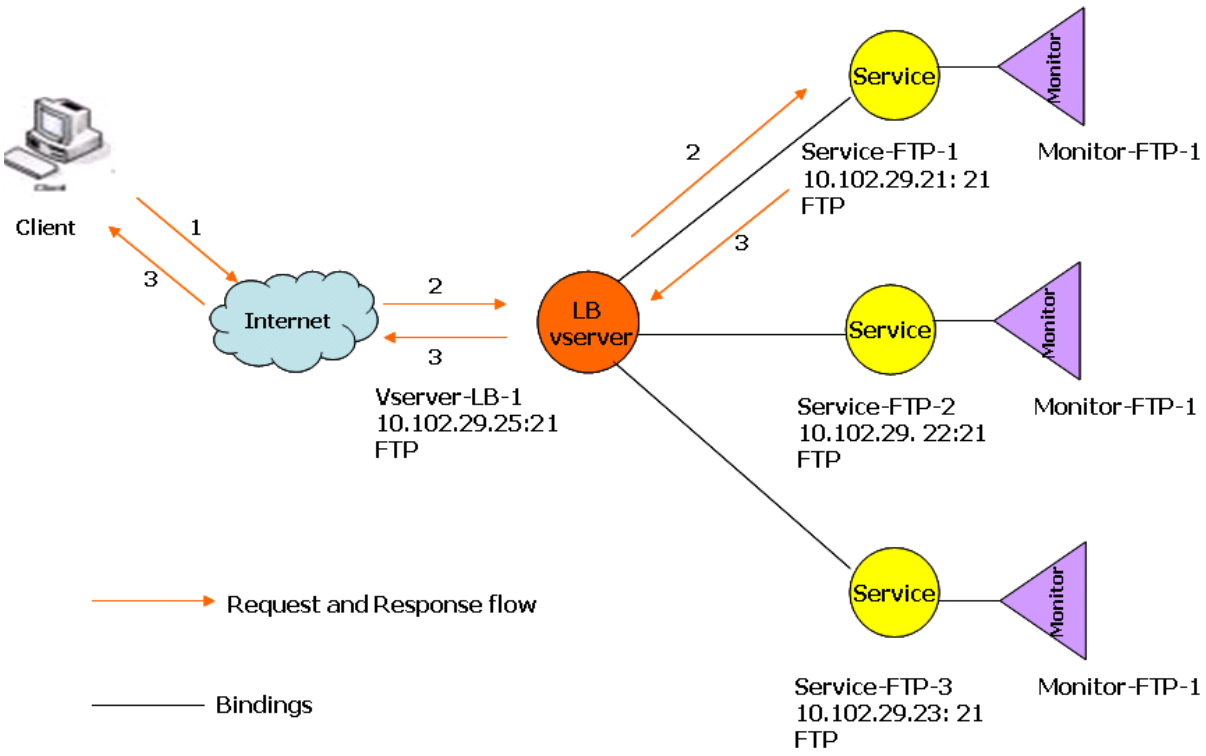
Dans le diagramme, les services Service-FTP-1, Service-FTP-2 et Service-FTP-3 sont liés au serveur virtuel vServer-LB-1. VServer-LB-1 transfère la demande de connexion du client à l'un des services en utilisant la méthode d'équilibrage de charge de connexion la moins élevée. Les demandes suivantes sont transférées au service initialement sélectionné par l'appliance pour l'équilibrage de charge.

Le tableau suivant répertorie les noms et les valeurs des entités de base configurées sur l'appliance.

Type d'entité	Nom	Adresse IP	Port	Protocole
`Vserver`	Vserver-LB-1	10.102.29.25	21	FTP
Services	Service-FTP-1	10.102.29.21	21	FTP
	Service-FTP-2	10.102.29.22	21	FTP
	Service-FTP-3	10.102.29.23	21	FTP
Moniteurs	FTP	Aucune	Aucune	Aucune

Le diagramme suivant présente les entités d'équilibrage de charge et les valeurs des paramètres qui doivent être configurés sur l'appliance.

Figure 2. Modèle d'entité des serveurs FTP d'équilibrage de charge



L'appliance peut également fournir une option FTP passive permettant d'accéder aux serveurs FTP depuis l'extérieur d'un pare-feu. Lorsqu'un client utilise l'option FTP passive et initie une connexion de contrôle au serveur FTP, le serveur FTP initie également une connexion de contrôle au client. Il initie ensuite une connexion de données pour transférer un fichier via le pare-feu.

Pour créer des services et des serveurs virtuels de type FTP, reportez-vous à la section Configuration de l'équilibrage de charge de base. Nommez les entités et définissez les paramètres sur les valeurs décrites dans les colonnes de la table précédente. Lorsque vous configurez une configuration d'équilibrage de charge de base, un moniteur par défaut est lié aux services.

Ensuite, liez le moniteur FTP aux services en suivant la procédure décrite dans la section Liaison des moniteurs aux services.

Pour créer des moniteurs FTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lb monitor <MonitorName> FTP -interval <Interval> -userName <
     UserName> -password <Password>
2 <!--NeedCopy-->
```

Exemple :


```
1 add lb monitor monitor-FTP-1 FTP -interval 360 -userName User -password
      User
2 <!--NeedCopy-->
```

Pour créer des moniteurs FTP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Créez un moniteur de type FTP, et dans Paramètres spéciaux, spécifiez un nom d'utilisateur et un mot de passe.

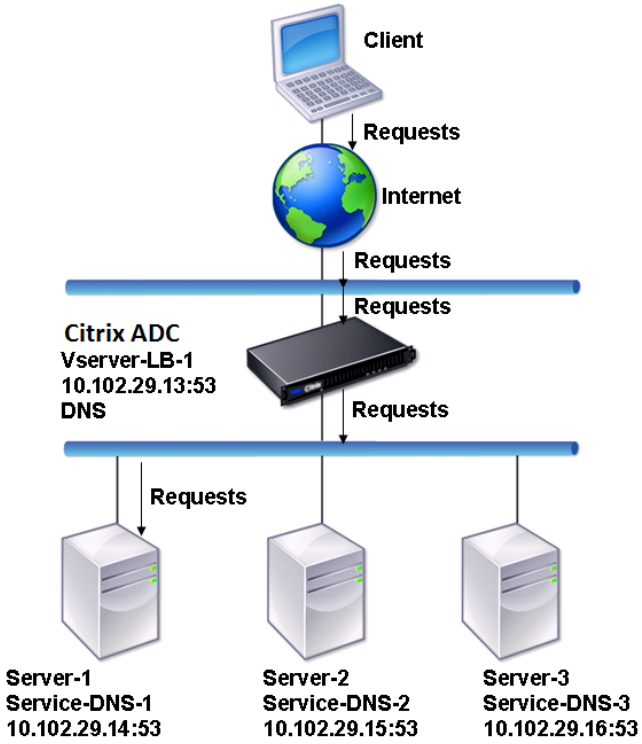
Équilibrer la charge de serveurs DNS

August 20, 2021

Lorsque vous demandez la résolution DNS d'un nom de domaine, l'appliance Citrix ADC utilise la méthode d'équilibrage de charge configurée pour sélectionner un service DNS. Le serveur DNS auquel le service est lié résout ensuite le nom de domaine et renvoie l'adresse IP comme réponse. L'appliance peut également mettre en cache les réponses DNS et utiliser les informations mises en cache pour répondre aux futures demandes de résolution du même nom de domaine. Les serveurs DNS d'équilibrage de charge améliorent les temps de réponse DNS.

Le diagramme suivant décrit la topologie d'une configuration d'équilibrage de charge qui équilibre la charge d'un groupe de services DNS.

Figure 1. Topologie d'équilibrage de charge de base pour les serveurs DNS

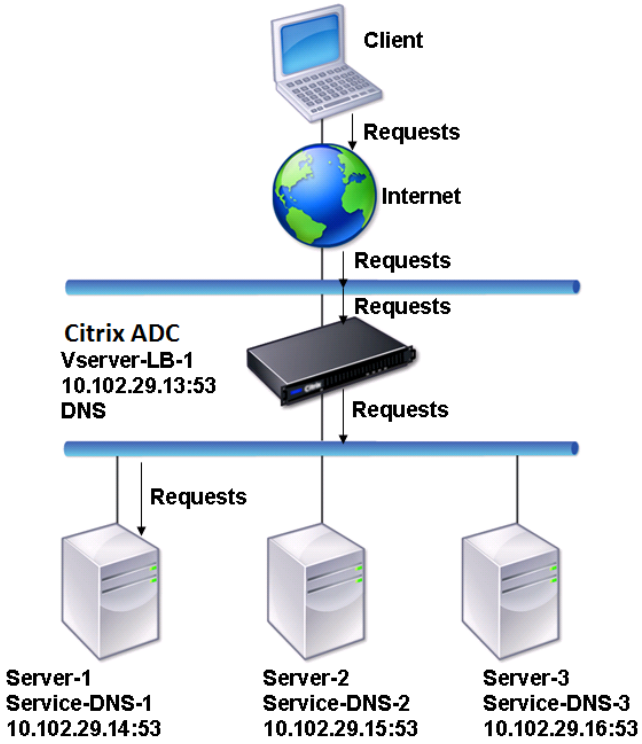


Dans le diagramme, les services Service-DNS-1, Service-DNS-2 et Service-DNS-3 sont liés au serveur virtuel vServer-LB-1. Le serveur virtuel vServer-LB-1 transfère les demandes du client à un service en utilisant la méthode d'équilibrage de charge de connexion la moins élevée. Le tableau suivant répertorie les noms et les valeurs des entités de base configurées sur l'appliance.

Type d'entité	Nom	Adresse IP	Port	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.13	53	DNS
Services	Service-DNS-1	10.102.29.14	53	DNS
	Service-DNS-2	10.102.29.15	53	DNS
	Service-DNS-3	10.102.29.16	53	DNS
Moniteurs	monitor-DNS-1	Aucune	Aucune	Aucune

Le diagramme suivant présente les entités d'équilibrage de charge et les valeurs des paramètres qui doivent être configurés sur l'appliance.

Figure 2. Modèle d'entité des serveurs DNS d'équilibrage de charge



Pour configurer une configuration d'équilibrage de charge DNS de base, reportez-vous à la section Configuration de l'équilibrage de charge de base. Suivez les procédures pour créer des services et des serveurs virtuels de type DNS, nommez les entités et définissez les paramètres à l'aide des valeurs décrites dans le tableau précédent. Lorsque vous configurez une configuration d'équilibrage de charge de base, le moniteur ping par défaut est lié aux services. Pour obtenir des instructions sur la liaison d'un moniteur DNS aux services DNS, vous pouvez également consulter la section Liaison des moniteurs aux services.

La procédure suivante décrit les étapes de création d'un moniteur qui mappe un nom de domaine à l'adresse IP en fonction d'une requête.

Pour configurer des moniteurs DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lb monitor <monitorName> DNS -query <domainName> -queryType <
     Address|ZONE> -IPAddress <ipAddress>
2 <!--NeedCopy-->
```

Exemple :


```
add lb monitor monitor-DNS-1 DNS -query www.citrix.com -queryType
    Address -IPAddress 10.102.29.66

add lb monitor monitor-DNS-2 DNS -query www.citrix2.com -queryType
    Address -IPAddress
1000:0000:0000:0000:0005:0600:700a::888b-888d
<!--NeedCopy-->
```

Pour configurer des moniteurs DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Créez un moniteur de type DNS et, dans Paramètres spéciaux, spécifiez un type de requête et de requête.

Équilibrer la charge de services basés sur un nom de domaine

August 20, 2021

Lorsque vous créez un service pour l'équilibrage de charge, vous pouvez fournir une adresse IP. Vous pouvez également créer un serveur à l'aide d'un nom de domaine. Le nom du serveur (nom de domaine) peut être résolu à l'aide d'un serveur de noms IPv4 ou IPv6, ou en ajoutant un enregistrement DNS faisant autorité (enregistrement pour IPv4 ou AAAA pour IPv6) à la configuration de Citrix ADC.

Lorsque vous configurez des services avec des noms de domaine au lieu d'adresses IP, et si le serveur de noms résout le nom de domaine en une nouvelle adresse IP, le moniteur lié au service exécute une vérification de l'état de la nouvelle adresse IP et met à jour l'adresse IP du service uniquement lorsque l'adresse IP est jugée saine. Le moniteur peut être le moniteur par défaut lié au service ou vous pouvez lier n'importe quel autre moniteur pris en charge. Il sonde le service à intervalles réguliers définis dans les paramètres du moniteur. Si le nom de domaine se résout à une nouvelle adresse IP, le moniteur envoie une nouvelle sonde pour vérifier l'état du service. Toutes les sondes suivantes sont à l'intervalle prédéfini.

Remarque : Lorsque vous modifiez l'adresse IP d'un serveur, le service correspondant est marqué comme DOWN pour la première requête client. Le serveur de noms résout l'adresse IP du service en l'adresse IP modifiée pour la requête suivante, et le service est marqué UP.

Les services basés sur des noms de domaine ont les restrictions suivantes :

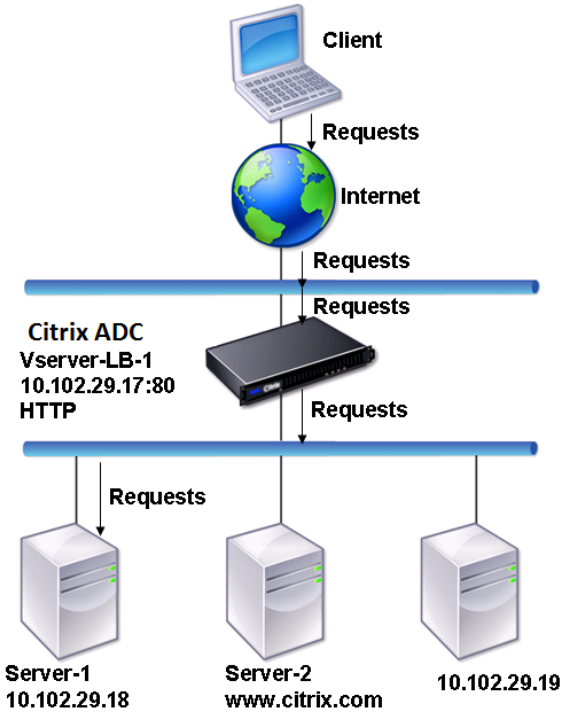
- La longueur maximale du nom de domaine est de 255 caractères.
- Le paramètre Client maximum est utilisé pour configurer un service qui représente le serveur basé sur le nom de domaine. Par exemple, un MaxClient de 1000 est défini pour les services liés

à un serveur virtuel. Lorsque le nombre de connexions sur le serveur virtuel atteint 2000, le résolveur DNS modifie l'adresse IP des services. Toutefois, comme le compteur de connexion sur le service n'est pas réinitialisé, le serveur virtuel ne peut pas prendre de nouvelles connexions tant que toutes les anciennes connexions ne sont pas fermées.

- Lorsque l'adresse IP du service change, la persistance est difficile à maintenir.
- Si la résolution du nom de domaine échoue en raison d'un délai d'expiration, l'appliance utilise les anciennes informations (adresse IP).
- Lorsque la surveillance détecte qu'un service est en panne, l'appliance effectue une résolution DNS sur le service (représentant le serveur basé sur le nom de domaine) pour obtenir une nouvelle adresse IP.
- Les statistiques sont collectées sur un service et ne sont pas réinitialisées lorsque l'adresse IP change.
- Si une résolution DNS renvoie un code « erreur de nom » (3), l'appliance marque le service comme DOWN et change l'adresse IP à zéro.

Lorsque l'appliance reçoit une demande de service, elle sélectionne le service cible. De cette façon, l'appliance équilibre la charge sur vos services. Le diagramme suivant décrit la topologie d'une configuration d'équilibrage de charge qui équilibre la charge d'un groupe de serveurs basés sur des noms de domaine (DBS).

Figure 1. Topologie d'équilibrage de charge de base pour les serveurs DBS



Les services Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 sont liés au serveur virtuel vServer-LB-1. Le serveur virtuel vServer-LB-1 utilise la méthode d'équilibrage de charge la moins élevée pour choisir le service. L'adresse IP du service est résolue à l'aide du serveur de noms vServer-LB-2.

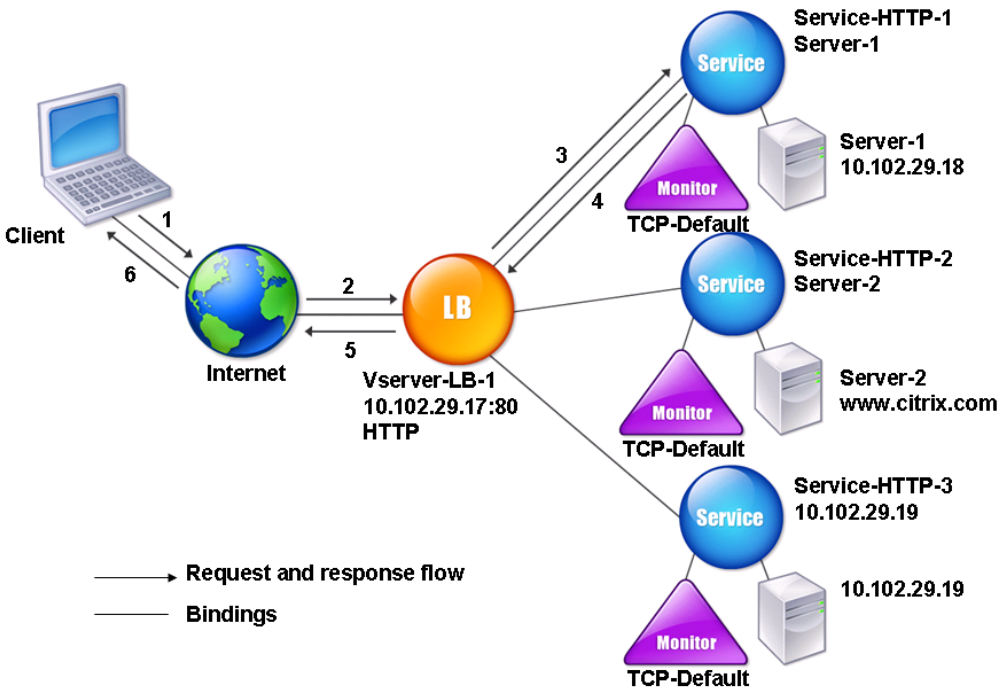
Le tableau suivant répertorie les noms et les valeurs des entités de base configurées sur l'appliance.

Type d'entité	Nom	Adresse IP	Port	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.17	80	HTTP
	Vserver-LB-2	10.102.29.20	53	DNS
Serveurs	server-1	10.102.29.18	80	HTTP
	server-2	www.citrix.com	80	HTTP
Services	Service-HTTP-1	server-1	80	HTTP
	Service-HTTP-2	server-2	80	HTTP
	Service-HTTP-2	10.102.29.19	80	HTTP
Moniteurs	Valeur par défaut	Aucune	Aucune	Aucune

Type d'entité	Nom	Adresse IP	Port	Protocole
Serveur de noms	Aucune	10.102.29.19	Aucune	Aucune

Le diagramme suivant présente les entités d'équilibrage de charge et les valeurs des paramètres qui doivent être configurés sur l'appliance.

Figure 2. Modèle d'entité des serveurs DBS d'équilibrage de charge



Pour configurer une configuration d'équilibrage de charge de base, reportez-vous à la section Configuration de l'équilibrage de charge de base. Créez les services et les serveurs virtuels de type HTTP, nommez les entités et définissez les paramètres à l'aide des valeurs décrites dans le tableau précédent.

Vous pouvez ajouter, supprimer, activer et désactiver des serveurs de noms externes. Vous pouvez créer un serveur de noms en spécifiant son adresse IP ou configurer un serveur virtuel existant en tant que serveur de noms.

Pour ajouter un serveur de noms à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add dns nameServer <dnsVserverName>
<!--NeedCopy-->
```

Exemple :

```
add dns nameServer Vserver-LB-2
<!--NeedCopy-->
```

Pour ajouter un serveur de noms à l'aide de l'utilitaire de configuration

1. Accédez à **Gestiondu trafic**>**DNS**>**Serveurs de **noms****.
2. Créez un serveur de noms DNS de type Serveur virtuel DNS et sélectionnez un serveur dans la liste Serveur virtuel DNS.

Vous pouvez également ajouter un serveur de noms faisant autorité qui résout le nom de domaine en une adresse IP.

> **Remarque**
>
> Vous pouvez ajouter un serveur de noms de type TCP, UDP ou UDP_TCP aux sondes DBS du résolveur. Toutefois, si les serveurs de noms TCP et UDP coexistent et qu'un serveur de noms UDP reçoit une réponse avec le bit tronqué, cette réponse n'est pas retentée sur le serveur de noms TCP.

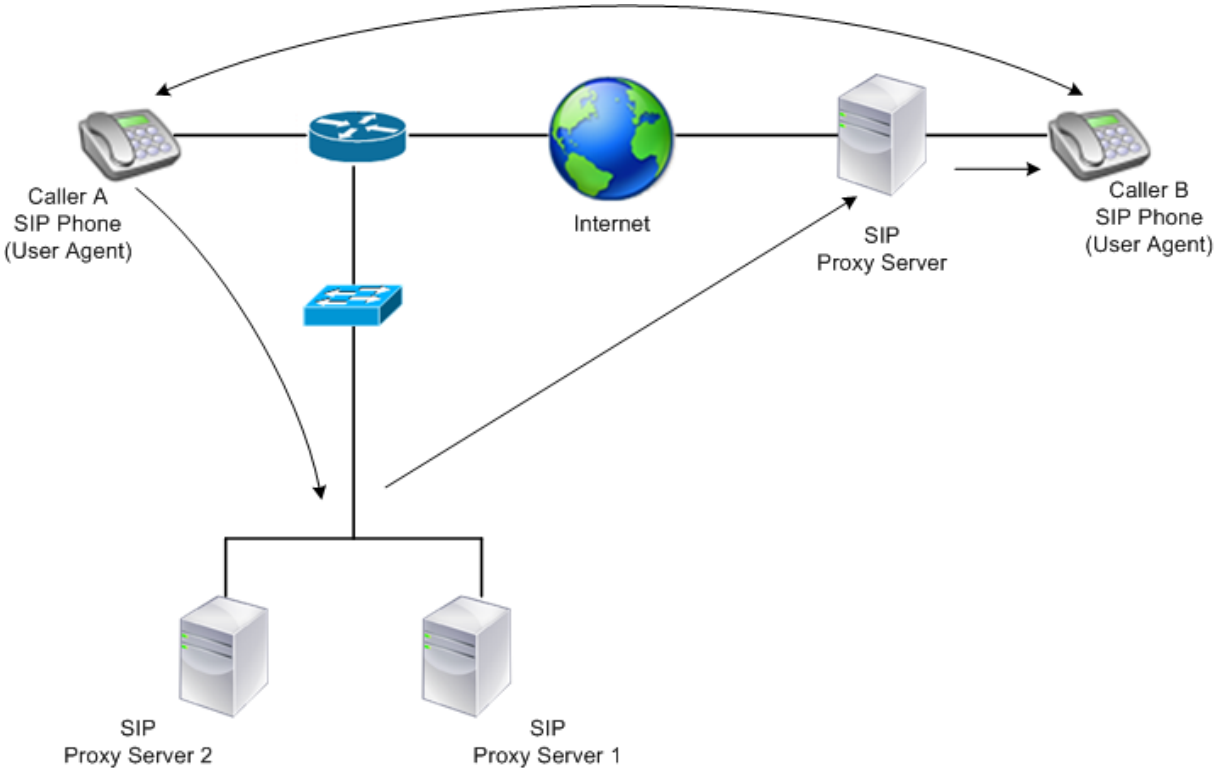
Équilibrer la charge d'un groupe de serveurs SIP

August 20, 2021

Le protocole SIP (Session Initiation Protocol) est conçu pour initier, gérer et mettre fin à des sessions de communication multimédia. Il est devenu la norme pour la téléphonie Internet (VoIP). Les messages SIP peuvent être transmis via TCP ou UDP. Les messages SIP sont de deux types : les messages de demande et les messages de réponse.

Le trafic dans un système de communication basé sur SIP est acheminé par des périphériques et des applications (entités) dédiés. Dans une session de communication multimédia, ces entités échangent des messages. La figure suivante montre un système de communication basé sur SIP de base :

Figure 1. Système de communication basé sur SIP



Un Citrix ADC vous permet d'équilibrer la charge des messages SIP sur UDP ou sur TCP (y compris TLS). Vous pouvez configurer Citrix ADC pour équilibrer la charge des demandes SIP vers un groupe de serveurs proxy SIP. Pour ce faire, vous créez un serveur virtuel d'équilibrage de charge avec la méthode d'équilibrage de charge et le type de persistance défini sur l'une des combinaisons suivantes :

- Méthode d'équilibrage de la charge de hachage d'ID d'appel sans paramètre de persistance
- Persistance basée sur l'ID d'appel avec la méthode d'équilibrage de charge de connexion minimale ou d'arrondi
- Persistance basée sur des règles avec une méthode d'équilibrage de charge de connexion minimale ou d'arrondi

De plus, par défaut, Citrix ADC ajoute RPORT via l'en-tête de la demande SIP, de sorte que le serveur renvoie la réponse à l'adresse IP source et au port d'où provient la demande.

Remarque : Pour que l'équilibrage de charge fonctionne, vous devez configurer les proxys SIP afin qu'ils n'ajoutent pas d'adresses IP privées ou de domaines privés à l'en-tête/charge utile SIP. Les proxys SIP doivent ajouter à l'en-tête SIP un nom de domaine qui se résout à l'adresse IP du serveur virtuel SIP. En outre, les mandataires SIP doivent communiquer avec une base de données commune pour partager les informations d'inscription.

Trafic initié par le serveur

Pour le trafic sortant initié par le serveur SIP, configurez RNAT sur Citrix ADC de sorte que les adresses IP privées utilisées par les clients soient traduites en adresses IP publiques.

Si vous avez configuré des paramètres SIP qui incluent le port source ou de destination RNAT, l'appliance compare les valeurs des ports source et destination des paquets de requête avec le port source RNAT et le port de destination RNAT. Si l'une des valeurs correspond, l'appliance met à jour l'en-tête VIA avec RPORT. La réponse SIP du client traverse ensuite le même chemin que la demande.

Pour le trafic SSL initié par le serveur, Citrix ADC utilise une paire de clés de certificat intégrée. Si vous souhaitez utiliser une paire de clés certificat-clé personnalisée, liez la paire certificat-clé personnalisée au service interne Citrix ADC nommé **nsrnatsip-127.0.0.1-5061**.

Prise en charge des stratégies et expressions

Le langage des expressions par défaut Citrix ADC contient plusieurs expressions qui fonctionnent sur des connexions SIP (Session Initiation Protocol). Ces expressions peuvent être liées uniquement aux serveurs virtuels SIP (sip_udp, sip_tcp ou sip_ssl) et aux points de liaison globaux. Vous pouvez utiliser ces expressions dans les stratégies de commutation de contenu, de limitation de débit, de répondeur et de réécriture.

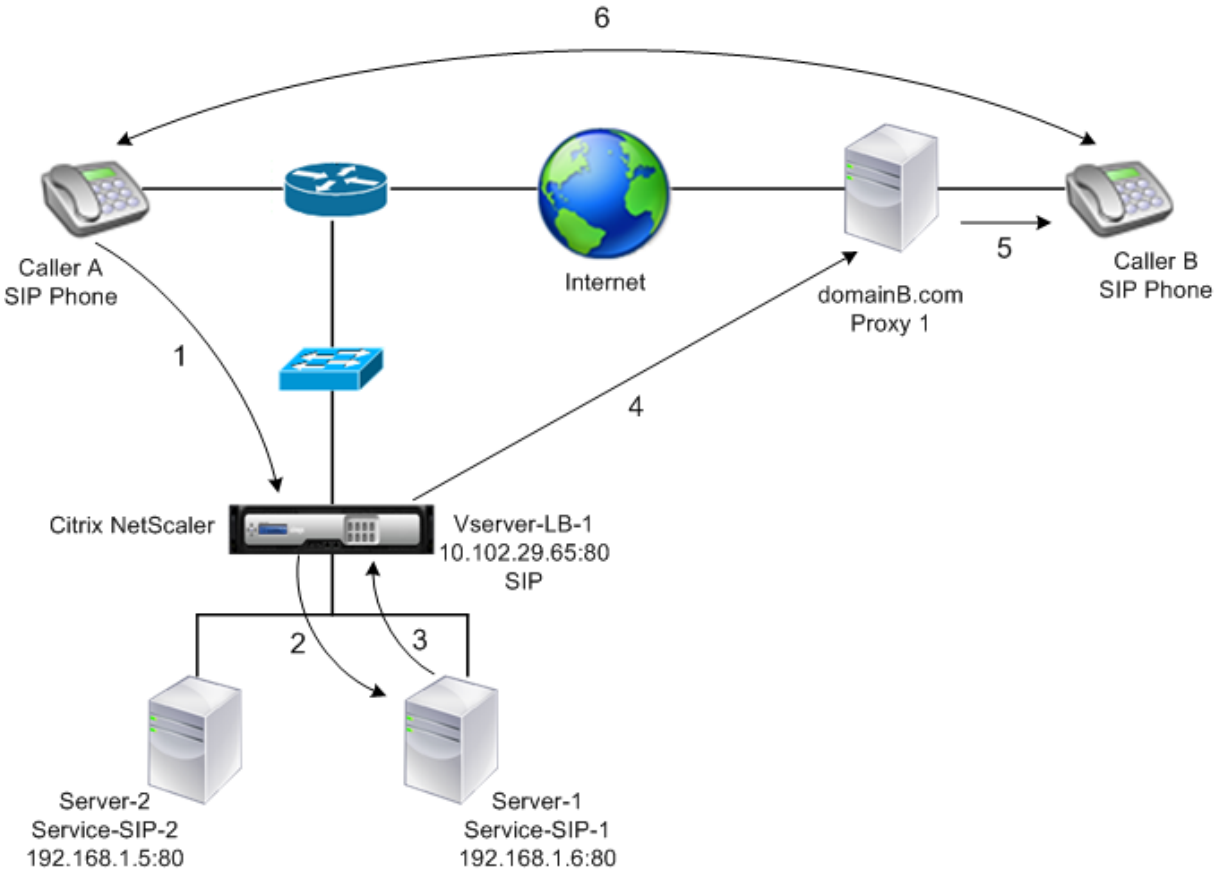
Configuration de l'équilibrage de charge pour le trafic de signalisation SIP sur TCP ou UDP

Citrix ADC peut équilibrer la charge des serveurs SIP qui envoient des demandes via UDP ou TCP, y compris le trafic TCP sécurisé par TLS. ADC fournit les types de service suivants pour équilibrer la charge des serveurs SIP :

- SIP_UDP — Utilisé lorsque les serveurs SIP envoient des messages SIP via UDP.
- SIP_TCP — Utilisé lorsque les serveurs SIP envoient des messages SIP via TCP.
- SIP_SSL — Utilisé pour sécuriser le trafic de signalisation SIP sur TCP à l'aide de SSL ou TLS. Le Citrix ADC prend en charge les modes suivants :
  - Connexion TLS de bout en bout entre le client, ADC et le serveur SIP.
  - Connexion TLS entre le client et ADC, et connexion TCP entre ADC et le serveur SIP.
  - Connexion TCP entre le client et ADC, et connexion TLS entre ADC et le serveur SIP.

La figure suivante illustre la topologie d'un programme d'installation configuré pour équilibrer la charge d'un groupe de serveurs SIP envoyant des messages SIP via TCP ou UDP.

Figure 2. Topologie d'équilibrage de charge SIP



Type d'entité	Nom	Adresse IP	Port	Type de service/Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.65	80	SIP_UDP / SIP_TCP / SIP_SSL
Services	Service-SIP-1	192.168.1.6	80	SIP_UDP / SIP_TCP / SIP_SSL
	Service-SIP-2	192.168.1.5	80	SIP_UDP / SIP_TCP / SIP_SSL
Moniteurs	Valeur par défaut	Aucune	80	SIP_UDP / SIP_TCP / SIP_SSL

Voici une vue d'ensemble de la configuration de l'équilibrage de charge de base pour le trafic SIP :

1. Configurez les services et configurez un serveur virtuel pour chaque type de trafic SIP que vous souhaitez équilibrer la charge :

   - **SIP_UDP** — Si vous équilibrez la charge du trafic SIP sur UDP.
   - **SIP_TCP** — Si vous équilibrez la charge du trafic SIP sur TCP.
   - **SIP_SSL** — Si vous êtes en train d'équilibrer la charge et de sécuriser le trafic SIP sur TCP.

   Remarque : Si vous utilisez SIP_SSL, veillez à créer une paire de clés de certificat SSL. Pour plus d'informations, voir Ajout d'une paire de clés de certificat.

2. Liez les services aux serveurs virtuels.
3. Si vous souhaitez surveiller les états des services avec un moniteur autre que le moniteur par défaut (**tcp-default**), créez un moniteur personnalisé et liez-le aux services. Le Citrix ADC fournit deux types de moniteurs personnalisés, **SIP-UDP** et **SIP-TCP**, pour la surveillance des services SIP.
4. Si vous utilisez un serveur virtuel SIP_SSL, liez une paire de clés de certificat SSL au serveur virtuel.
5. Si vous utilisez Citrix ADC comme Gateway pour les serveurs SIP dans votre déploiement, configurez RNAT.
6. Si vous souhaitez ajouter RPORT aux messages SIP initiés à partir du serveur SIP, configurez les paramètres SIP.

Pour configurer une configuration d'équilibrage de charge de base pour le trafic SIP à l'aide de l'interface de ligne de commande

Créez un ou plusieurs services. À l'invite de commandes, tapez :

```
add service <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>
<!--NeedCopy-->
```

Exemple :

```
add service Service-SIP-UDP-1 192.0.2.5 SIP_UDP 80
<!--NeedCopy-->
```

Créez autant de serveurs virtuels que nécessaire pour gérer les services que vous avez créés. Le type de serveur virtuel doit correspondre au type de services que vous lui liez. À l'invite de commandes, tapez :

```
add lb vserver <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>
<!--NeedCopy-->
```


Exemple :

```
add lb vserver Vserver-LB-1 SIP_UDP 10.102.29.60 80
<!--NeedCopy-->
```

Liez chaque service à un serveur virtuel. À l'invite de commandes, tapez :

```
bind lb vserver <name> <serverName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-SIP-UDP-1
<!--NeedCopy-->
```

(Facultatif) Créez un moniteur personnalisé de type SIP-UDP ou SIP-TCP et liez le moniteur au service. À l'invite de commandes, tapez :

```
add lb monitor <monitorName> <monitorType> [<interval>]

bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Exemple :

```
add lb monitor mon1 sip-UDP -sipMethod REGISTER -sipuRI sip:mon@test.
    com -sipregURI sip:mon@test.com -respcode 200

bind monitor mon1 Service-SIP-UDP-1
<!--NeedCopy-->
```

Si vous avez créé un serveur virtuel SIP_SSL, liez une paire de clés de certificat SSL au serveur virtuel. À l'invite de commandes, tapez : À l'invite de commandes, tapez :

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -
    CA - skipCAName
<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1
<!--NeedCopy-->
```

Configurez RNAT comme requis par la topologie de votre réseau. À l'invite de commandes, tapez l'une des commandes suivantes pour créer respectivement une entrée RNAT qui utilise une adresse réseau

comme condition et SNIP comme adresse IP NAT, une entrée RNAT qui utilise une adresse réseau comme condition et une adresse IP unique comme adresse IP NAT, une entrée RNAT qui utilise une ACL comme la condition et un SNIP comme adresse IP NAT, ou une entrée RNAT qui utilise une ACL comme condition et une adresse IP unique comme adresse IP NAT :

```
add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))

bind rnat <name> <natIP>@ …

show rnat
<!--NeedCopy-->
```

Exemple :

```
add rnat RNAT-1 192.168.1.0 255.255.255.0

bind rnat RNAT-1 -natip 10.102.29.50
<!--NeedCopy-->
```

Si vous souhaitez utiliser une paire de clés certificat-clé personnalisée, liez la paire certificat-clé personnalisée au service interne Citrix ADC nommé nsrnatsip-127.0.0.1-5061.

```
add ssl certKey <certkeyName> -cert <string> [-key <string>]

bind ssl service <serviceName> -certkeyName <string>
<!--NeedCopy-->
```

Exemple :

```
add ssl certKey c1 -cert cert.epm -key key.ky

bind ssl service nsrnatsip-127.0.0.1-5061 -certkeyName c1
<!--NeedCopy-->
```

Si vous souhaitez ajouter RPORT aux messages SIP initiés par le serveur SIP, tapez la commande suivante à l'invite de commandes :

```
set lb sipParameters -rnatSrcPort <rnatSrcPort> -rnatDstPort<
    rnatDstPort> -retryDur <integer> -addRportVip <addRportVip> -
    sip503RateThreshold <sip503_rate_threshold_value>
<!--NeedCopy-->
```

Exemple de configuration pour l'équilibrage de charge du trafic SIP sur UDP


```
add service service-UDP-1 10.102.29.5 SIP_UDP 80

Done

add lb vserver vserver-LB-1 SIP_UDP 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-UDP-1

Done

add lb mon mon1 sip-udp -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-UDP-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done

set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
     -addRportVip ENABLED -sip503RateThreshold 1000

Done
<!--NeedCopy-->
```

Exemple de configuration pour l'équilibrage de charge du trafic SIP sur TCP

```
add service service-TCP-1 10.102.29.5 SIP_TCP 80

Done

add lb vserver vserver-LB-1 SIP_TCP 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-TCP-1

```



```
Done

add lb mon mon1 sip-tcp -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-TCP-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done

set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
     -addRportVip ENABLED -sip503RateThreshold 1000

Done
<!--NeedCopy-->
```

Exemple de configuration pour l'équilibrage de charge et la sécurisation du trafic SIP sur TCP

```
add service service-SIP-SSL-1 10.102.29.5 SIP_SSL 80

Done

add lb vserver vserver-LB-1 SIP_SSL 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-SIP-SSL

Done

add lb mon mon1 sip-tCP -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-SIP-SSL

```



```
Done

bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done

set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
    -addRportVip ENABLED -sip503RateThreshold 1000

Done
<!--NeedCopy-->
```

Pour configurer une configuration d'équilibrage de charge de base pour le trafic SIP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ajoutez un serveur virtuel de type SIP_UDP, SIP_TCP ou SIP_SSL.
2. Cliquez sur la section **Service** et ajoutez un service de type SIP_UDP, SIP_TCP ou SIP_SSL.
3. **(Facultatif) Cliquez sur la section Moniteur et ajoutez un moniteur du type SIP-UDP ou SIP-TCP.**
4. Liez le moniteur au service et liez le service au serveur virtuel.
5. Si vous avez créé un serveur virtuel SIP_SSL, liez une paire de clés de certificat SSL au serveur virtuel. Cliquez sur la section Certificats et liez une paire de clés de certificat au serveur virtuel.
6. Configurez RNAT comme requis par la topologie de votre réseau. Pour configurer RNAT :
   a) Accédez à **Système > Réseau > Routes**.
   b) Sur la page Routes, cliquez sur l'onglet **RNAT** .
   c) Dans le volet d'informations, cliquez sur **Configurer le RNAT**.
   d) Dans la boîte de dialogue Configurer RNAT, effectuez l'une des opérations suivantes :
      - Si vous souhaitez utiliser l'adresse réseau comme condition pour créer une entrée RNAT, cliquez sur **Réseau** et définissez les paramètres suivants :
        - Réseau
        - Masque réseau
      - Si vous souhaitez utiliser une ACL étendue comme condition pour créer une entrée RNAT, cliquez sur **ACL** et définissez les paramètres suivants :
        - Nom ACL

- Port de redirection

e) Pour définir une adresse SNIP en tant qu'adresse IP NAT, passez à l'étape 7.

f) Pour définir une adresse IP unique comme IP NAT, dans la liste IP NAT disponible (s), sélectionnez l'adresse IP que vous souhaitez définir comme IP NAT, puis cliquez sur Ajouter. L'IP NAT que vous avez sélectionnée apparaît dans la liste IP NAT configurée.

g) Cliquez sur Créer, puis sur Fermer.

Si vous souhaitez utiliser une paire de clés certificat-clé personnalisée, liez la paire certificat-clé personnalisée au service interne Citrix ADC nommé **nsrnatsip-127.0.0.1-5061**. Pour lier la paire :

a) Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis cliquez sur l'onglet Services internes.

b) Sélectionnez nsrnatsip-127.0.0.1-5061 et cliquez sur **Modifier**.

c) Cliquez sur la section **Certificats** et liez une paire de clés de certificat au service interne.

7. Si vous souhaitez ajouter RPORT aux messages SIP initiés par le serveur SIP, configurez les paramètres SIP. Accédez à **Gestion du trafic > Équilibrage de charge**, puis cliquez sur Modifier les paramètres SIP, définissez les différents paramètres SIP.

Exemple d'expression et de stratégie SIP : compression activée dans les demandes client

Un Citrix ADC ne peut pas traiter les demandes SIP client compressées, de sorte que la demande SIP client échoue.

Vous pouvez configurer une stratégie de répondeur qui intercepte le message SIP NEGOTIATE du client et recherche l'en-tête de compression. Si le message inclut un en-tête de compression, la stratégie répond avec « 400 Bad Request », de sorte que le client renvoie la demande sans la compresser.

À l'invite de commandes, tapez les commandes suivantes pour créer la stratégie de répondeur :

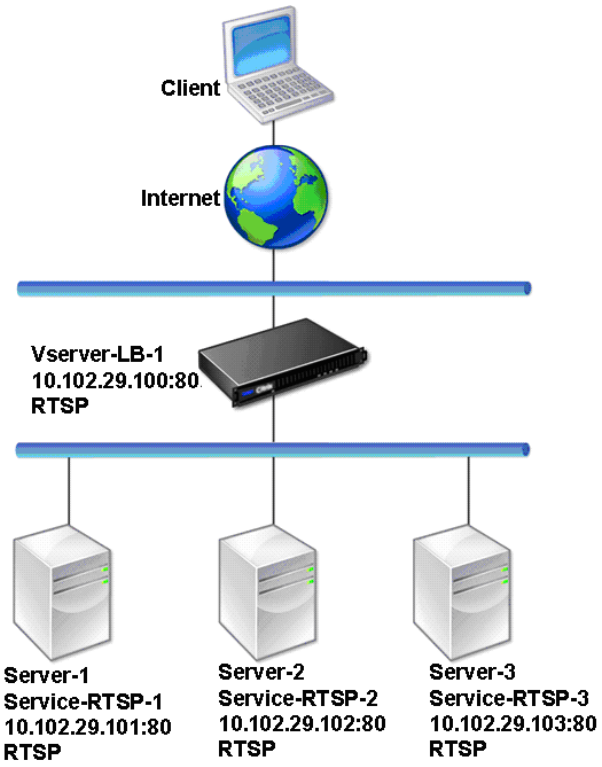
```
1  add responder action sipaction1 respondwith q{
2   "SIP/2.0 400 Bad Requestrnrn" }
3
4
5  Done
6
7  add responder policy sippol1
8
9  add responder policy sippol1 "SIP.REQ.METHOD.EQ("NEGOTIATE")&&SIP.REQ.
       HEADER("Compression").EXISTS" sipaction1
10 <!--NeedCopy-->
```


Équilibrer la charge de serveurs RTSP

August 20, 2021

L'appliance Citrix ADC peut équilibrer la charge sur les serveurs RTSP afin d'améliorer les performances des flux audio et vidéo sur les réseaux. Le diagramme suivant décrit la topologie d'une configuration d'équilibrage de charge configurée pour équilibrer la charge d'un groupe de serveurs RTSP.

Figure 1. Topologie d'équilibrage de charge pour RTSP



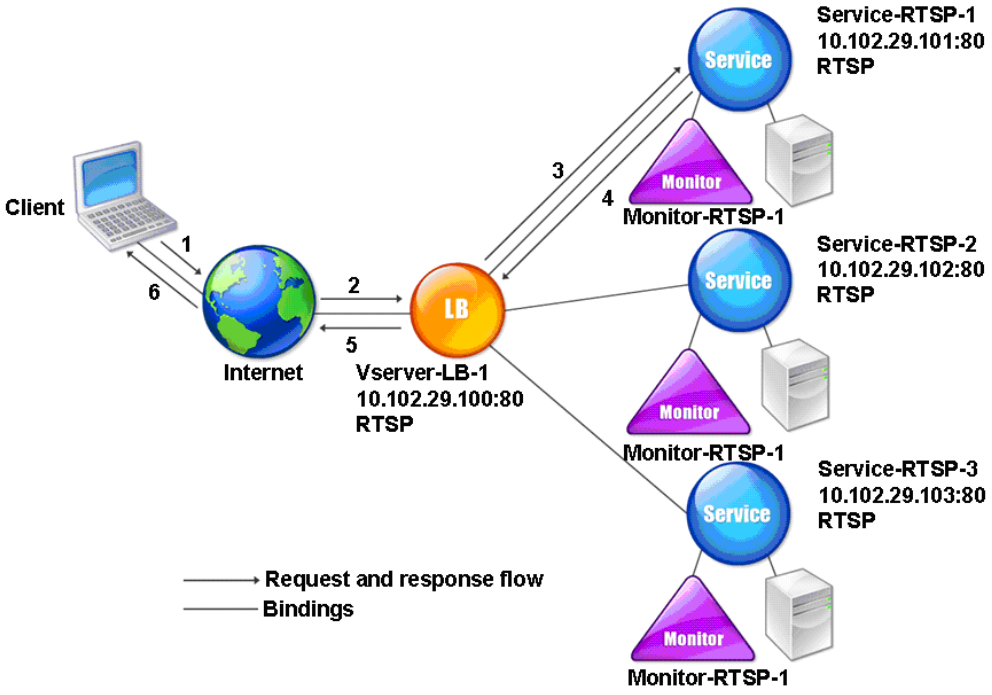
Dans l'exemple, les services Service-RTSP-1, Service-RTSP-2 et Service-RTSP-3 sont liés au serveur virtuel vServer-LB-1. Le tableau suivant répertorie les noms et les valeurs des entités d'exemple.

Type d'entité	Nom	Adresse IP	Port	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.100	554	RTSP
Services	Service-RTSP-1	10.102.29.101	554	RTSP
	Service-RTSP-2	10.102.29.102	554	RTSP

Type d'entité	Nom	Adresse IP	Port	Protocole
	Service-RTSP-3	10.102.29.103	554	RTSP
Moniteurs	Monitor-RTSP-1	Aucune	554	RTSP

Le diagramme suivant montre les entités d'équilibrage de charge utilisées dans la configuration RTSP.

Figure 2. Modèle d'entité des serveurs RTSP d'équilibrage de charge



Pour configurer une configuration d'équilibrage de charge de base pour les serveurs RTSP, reportez-vous à la section Configuration de l'équilibrage de charge de base. Créez des services et des serveurs virtuels de type RTSP. Lorsque vous configurez une configuration d'équilibrage de charge de base, le moniteur par défaut TCP est lié aux services. Pour lier un moniteur RTSP à ces services, reportez-vous à la section Liaison des moniteurs aux services. La procédure suivante décrit comment créer un moniteur qui vérifie les serveurs RTSP.

Pour configurer des moniteurs RTSP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
add lb monitor <monitorName> <type>
<!--NeedCopy-->
```

Exemple :

```
add lb monitor Monitor-RTSP-1 RTSP
<!--NeedCopy-->
```

Pour configurer des moniteurs RTSP à l'aide de l'interface graphique

Accédez à Gestion du trafic > Équilibrage de charge > Moniteurs et créez un moniteur de type RTSP.

Équilibrer la charge des serveurs de protocole Bureau à distance

August 20, 2021

Le protocole RDP (Remote Desktop Protocol) est un protocole compatible multicanal qui permet de disposer de canaux virtuels distincts pour transporter des données de présentation, des communications de périphérique série, des informations de licence, des données hautement cryptées (activité du clavier et de la souris), etc.

RDP est utilisé pour fournir une interface graphique à un autre ordinateur du réseau. RDP est utilisé avec les serveurs Terminal Server Windows pour fournir un accès rapide avec transmission presque en temps réel des mouvements de souris et des touches pressées même sur des connexions à faible bande passante.

Lorsque plusieurs serveurs Terminal Server sont déployés pour fournir des services Bureau à distance, l'appliance Citrix ADC assure l'équilibrage de charge des serveurs Terminal Server (Windows 2003 et 2008 Server Enterprise Editions). Parfois, un utilisateur qui accède à une application à distance peut vouloir laisser l'application en cours d'exécution sur la machine distante mais arrêter l'ordinateur local. L'utilisateur ferme donc l'application locale sans se déconnecter de l'application distante. Une fois reconnecté à la machine distante, l'utilisateur doit pouvoir continuer avec l'application distante. Pour fournir cette fonctionnalité, l'implémentation Citrix ADC RDP respecte le jeton de routage (cookie) défini par le répertoire de session des services Terminal Server ou Broker afin que le client puisse se reconnecter au même serveur Terminal Server auquel il était précédemment connecté. Le répertoire de session, implémenté sur Windows 2003 Terminal Server, est appelé Broker sur Windows 2008 Terminal Server.

Lorsqu'une connexion TCP est établie entre le client et le serveur virtuel d'équilibrage de charge, Citrix ADC applique la méthode d'équilibrage de charge spécifiée et transfère la demande à l'un des serveurs

Terminal Server. Le serveur Terminal Server vérifie le répertoire de session pour déterminer si le client dispose d'une session exécutée sur un autre serveur Terminal Server du domaine.

S'il n'y a pas de session active sur un autre serveur Terminal Server, le serveur Terminal Server répond en servant la demande client et l'appliance Citrix ADC transmet la réponse au client.

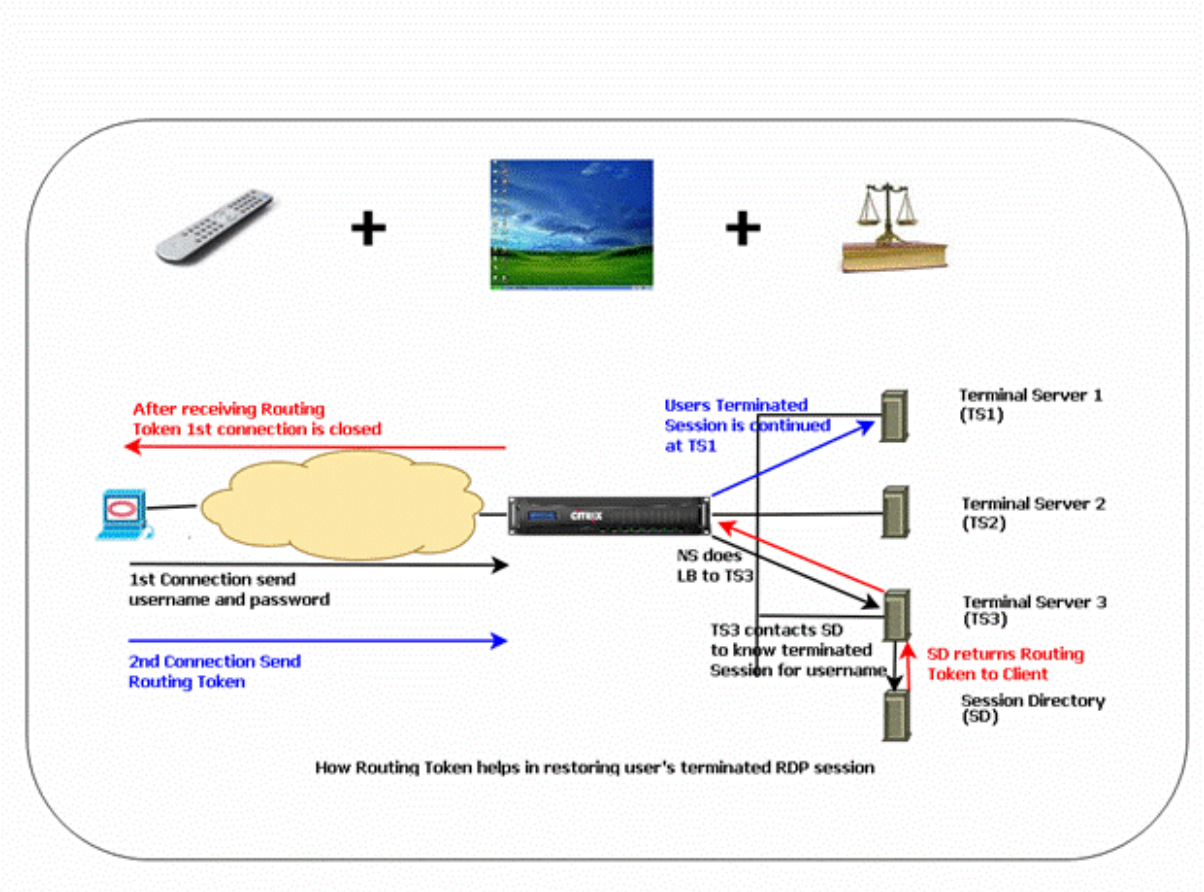
S'il existe une session active sur un autre serveur Terminal Server, le serveur Terminal Server qui reçoit la demande insère un cookie (appelé jeton de routage) avec les détails de la session active et renvoie les paquets à l'appliance Citrix ADC, qui renvoie le paquet au client. Le serveur ferme la connexion avec le client. Lorsque le client tente de se connecter à nouveau, Citrix ADC lit les informations de cookie et transmet le paquet au serveur Terminal Server sur lequel le client a une session active.

L'utilisateur sur la machine cliente subit une continuation du service et n'a pas à prendre d'action spécifique.

Remarque : La fonctionnalité Répertoire de sessions Windows nécessite le client Bureau à distance qui a été publié pour la première fois avec Windows XP. Si une session avec un client Terminal Server Windows 2000 ou Windows NT 4.0 est déconnectée et que le client se reconnecte, le serveur avec lequel la connexion est établie est sélectionné par l'algorithme d'équilibrage de charge.

Le diagramme suivant décrit l'équilibrage de charge RDP.

Figure 1. Topologie d'équilibrage de charge pour RDP



Remarque

- Lorsqu'un service RDP est configuré, la persistance est automatiquement maintenue à l'aide d'un jeton de routage. Vous n'avez pas besoin d'activer explicitement la persistance.
- L'appliance Citrix ADC prend uniquement en charge les cookies IP.
- Le script nsrdp.pl n'est pas pris en charge sur aucune version actuelle des serveurs Windows.

Assurez-vous que les sessions RDP déconnectées sont effacées sur les serveurs Terminal Server au niveau du back-end afin d'éviter les battements entre deux serveurs Terminal Server lorsqu'une session RDP est déconnectée sans déconnexion. Pour de plus amples informations, consultez `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758177(v=ws.10)##BKMK_2`

Lorsque vous ajoutez un service RDP, par défaut, Citrix ADC ajoute un moniteur du type TCP et le lie au service. Le moniteur par défaut est un moniteur TCP simple qui vérifie si un processus d'écoute existe sur le port 3389 du serveur spécifié pour le service RDP. S'il y a un processus d'écoute à 3389, Citrix ADC marque ce service comme UP et s'il n'y a pas de processus d'écoute, il marque le service comme DOWN.

Pour une surveillance plus efficace d'un service RDP, en plus du moniteur par défaut, vous pouvez

configurer un moniteur de script destiné au protocole RDP. Lorsque vous configurez le moniteur de script, le Citrix ADC ouvre une connexion TCP au serveur spécifié et envoie un paquet RDP. Le moniteur marque le service comme UP uniquement s'il reçoit une confirmation de la connexion du serveur physique. Par conséquent, à partir du moniteur de script, Citrix ADC peut savoir si le service RDP est prêt à traiter une demande.

Le moniteur est un moniteur de type utilisateur et le script se trouve sur Citrix ADC à l'adresse /nsconfig/monitors/nsrdp.pl. Lorsque vous configurez le moniteur utilisateur, le Citrix ADC exécute le script automatiquement. Pour configurer le moniteur de script, ajoutez le moniteur et liez-le au service RDP.

Pour configurer l'équilibrage de charge RDP, créez des services de type RDP et liez-les à un serveur virtuel RDP.

Pour configurer les services d'équilibrage de charge RDP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une configuration d'équilibrage de charge RDP et vérifier la configuration :

```
add service <name>@ <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Remarque : Répétez la commande précédente pour ajouter d'autres services.

Exemple

```
> add service ser1 10.102.27.182 RDP 3389
Done
> add service ser2 10.102.27.183 RDP 3389
Done
>show service ser1
ser1 (10.102. 27.182:3389) - RDP
        State: UP
…
            Server Name: 10.102.27.182
            Server ID : 0           Monitor Threshold : 0
        Down state flush: ENABLED
…
1)      Monitor Name: tcp-default
                State: UP       Weight: 1
…
                Response Time: 4.152 millisec
 Done
<!--NeedCopy-->
```


Pour configurer les services d'équilibrage de charge RDP à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services**et créez des services de type RDP.

Pour configurer un serveur virtuel d'équilibrage de charge RDP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur virtuel d'équilibrage de charge RDP et vérifier la configuration :

```
add lb vserver <name>@ <serviceType> <ipAddress> <port>

bind lb vserver <name>@ <serviceName>

Bind all the RDP services to be load balanced to the virtual server.
<!--NeedCopy-->
```

Exemple :

Cet exemple comporte deux services RDP liés au serveur virtuel RDP.

```
add lb vs v1 rdP 10.102.27.186 3389
Done

bind lb vs v1 ser1
service "ser1" bound

bind lb vs v1 ser2
service "ser2" bound
Done

sh lb vs v1
v1 (10.102.27.186:3389) - RDP   Type: ADDRESS
State: UP
…
No. of Bound Services :  2 (Total)       2 (Active)
Configured Method: LEASTCONNECTION
  Current Method: Round Robin, Reason: A new service is bound
Mode: IP
Persistence: NONE
  L2Conn: OFF

1) ser1 (10.102.27.182: 3389) - RDPState: UP   Weight: 1
2) ser2 (10.102.27.183: 3389) - RDPState: UP   Weight: 1
```



```
24 Done
25 <!--NeedCopy-->
```

Pour configurer un serveur virtuel d'équilibrage de charge RDP à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, créez un serveur virtuel de type RDP et liez les services RDP à ce serveur virtuel.

Pour configurer un moniteur de script pour les services RDP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
1 add lb monitor <monitorName> USER -scriptName nsrdp.pl
2
3 bind lb monitor <monitorName> <rdpServiceName>
4 <!--NeedCopy-->
```

Exemple :

```
1 add service ser1 10.102.27.182 RDP 3389
2
3 add lb monitor RDP_MON USER -scriptName nsrdp.pl
4
5 bind lb monitor RDP_MON ser1
6
7 <!--NeedCopy-->
```

Pour configurer un moniteur de script pour les services RDP à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**et créez un moniteur de type USER.
2. Dans Paramètres spéciaux, dans la liste Nom du script, sélectionnez nsrdp.pl, puis liez ce moniteur à un service RDP.

Équilibre de charge du serveur Microsoft Exchange

October 5, 2021

Ce document fournit les exemples de configuration recommandés pour l'équilibrage de charge du serveur Microsoft Exchange à l'aide de l'appliance Citrix ADC.

Citrix ADM StyleBooks simplifie les configurations d'équilibrage de charge Citrix ADC pour Exchange. Pour plus d'informations, voir StyleBook Microsoft Exchange.

> Remarque :
>
> L'équilibrage de charge de Microsoft Exchange n'est pas possible à l'aide d'un seul serveur virtuel d'équilibrage de charge. Suivez plutôt les configurations recommandées fournies dans ce document.

Différences entre Microsoft Exchange 2016 et les versions plus récentes

- Il n'est pas nécessaire de configurer les ports RPC (Remote Procedure Call) statiques sur Exchange 2016 car les ports RPC ne sont pas utilisés.
- Toutes les sections nommées « pour les versions d'Exchange inférieures à 2016 » ne sont pas nécessaires avec Exchange 2016.
- Si vous avez déjà configuré l'une des versions autres que 2016 et que vous migrez vers 2016, vous n'avez pas besoin de les supprimer. Parce que même s'ils existent, il n'y a aucun problème.

Points à noter

- Pour les appels de procédure à distance (RPC) avec le serveur Exchange au-dessous de 2016, les serveurs CAS Exchange doivent être configurés pour les affectations de ports statiques. Pour plus d'informations, consultez la documentation Microsoft Exchange 2010 Client Access Server : Configurer les ports RPC statiques .
- Cette configuration suppose l'utilisation de l'appliance Citrix ADC pour le déchargement SSL. Pour plus d'informations, consultez Comment configurer le déchargement SSL dans Exchange 2010 ou Configuration du déchargement SSL dans Exchange 2013.
- Si vous ne souhaitez pas utiliser la fonction de déchargement SSL de l'appliance Citrix ADC, modifiez le groupe de services `CAS_servicegroup_http` et les moniteurs par type `SSL` et ses liaisons sur port `443`.
- La protection contre les surtensions n'est pas compatible avec Microsoft Exchange. Ne l'activez pas sur aucun service ou groupe de services lié à Microsoft Exchange. L'activation de la protection contre les surtensions engendre des problèmes de connectivité et
- Remplacez les variables suivantes par les informations appropriées :
  - {HTTP Public IP} : adresse IP du point de terminaison HTTP Exchange public

- {IP publique RPC} —Adresse IP du point de terminaison RPC Exchange public (peut être la même que HTTP Public IP)
- {Timeout} : délai d'expiration souhaité (en secondes). Il est recommandé d'être aussi long que le temps de travail standard (c'est-à-dire 8 heures)
- {PerstimeOut} : délai d'expiration souhaité (en minutes). Doit correspondre au paramètre de délai d'attente précédent.
- {Port AB} : port TCP du carnet d'adresses RPC (généralement 59601)
- {Port CA} : port TCP d'accès client RPC (généralement 59600)
- {CertKey} —Clé de certificat SSL
- {Serveur CAS-1} : adresse IP du serveur CAS
- {Serveur CAS-2} : adresse IP du serveur CAS

Exemples de configuration recommandés pour toutes les versions de Microsoft Exchange Server

Groupes de services :

```
add serviceGroup CAS_servicegroup_http HTTP -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout { Timeout }
 -svrTimeout { Timeout }
 -CKA NO -TCPB NO -CMP YES
add serviceGroup CAS_servicegroup_rpc_epm TCP -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout { Timeout }
 -svrTimeout { Timeout }
 -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_http {
 CAS-1 Server }
  80 -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_http {
 CAS-2 Server }
  80 -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_epm {
 CAS-1 Server }
  135 -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_epm {
 CAS-2 Server }
  135 -CustomServerID ""None""
<!--NeedCopy-->
```


Moniteurs :

```
add lb monitor CAS_monitor_rpc_epm TCP -LRTM ENABLED -destPort 135
set lb monitor http-ecv HTTP-ECV -recv 403 -LRTM DISABLED
bind serviceGroup CAS_servicegroup_http -monitorName http-ecv
bind serviceGroup CAS_servicegroup_rpc_epm -monitorName
   CAS_monitor_rpc_epm
<!--NeedCopy-->
```

Serveurs virtuels d'équilibrage de charge :

```
add lb vserver CAS_vserver_owa SSL 0.0.0.0 0 -persistenceType
   COOKIEINSERT -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add lb vserver CAS_vserver_as SSL 0.0.0.0 0 -persistenceType RULE -
   timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -rule "HTTP.REQ.HEADER("Authorization")" -
     cltTimeout {
 Timeout }

add lb vserver CAS_vserver_oa SSL 0.0.0.0 0 -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add lb vserver CAS_vserver_ews SSL 0.0.0.0 0 -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add lb vserver CAS_vserver_ad SSL 0.0.0.0 0 -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

set ssl vserver CAS_vserver_owa -sslRedirect ENABLED
bind ssl vserver CAS_vserver_owa -certkeyName {
 CertKey }

bind ssl vserver CAS_vserver_oab -certkeyName {
 CertKey }
```



```
32
33 bind ssl vserver CAS_vserver_as -certkeyName {
34  CertKey }
35
36 bind ssl vserver CAS_vserver_oa -certkeyName {
37  CertKey }
38
39 bind ssl vserver CAS_vserver_ews -certkeyName {
40  CertKey }
41
42 bind ssl vserver CAS_vserver_ad -certkeyName {
43  CertKey }
44
45 bind lb vserver CAS_vserver_owa CAS_servicegroup_http
46 bind lb vserver CAS_vserver_oab CAS_servicegroup_http
47 bind lb vserver CAS_vserver_as CAS_servicegroup_http
48 bind lb vserver CAS_vserver_oa CAS_servicegroup_http
49 bind lb vserver CAS_vserver_ews CAS_servicegroup_http
50 bind lb vserver CAS_vserver_ad CAS_servicegroup_http
51 add lb vserver CAS_vserver_rpc_epm TCP {
52  RPC Public IP }
53   135 -timeout {
54  PersTimeout }
55   -cltTimeout {
56  Timeout }
57   -comment "vserver for RPC End Point Mapper"
58 bind lb vserver CAS_vserver_rpc_epm CAS_servicegroup_rpc_epm
59 <!--NeedCopy-->
```

Groupe de persistance :

```
1 add lb group CAS_persistency_group_sourceip
2 bind lb group CAS_persistency_group_sourceip CAS_vserver_oa
3 bind lb group CAS_persistency_group_sourceip CAS_vserver_oab
4 bind lb group CAS_persistency_group_sourceip CAS_vserver_ews
5 bind lb group CAS_persistency_group_sourceip CAS_vserver_ad
6 bind lb group CAS_persistency_group_sourceip CAS_vserver_rpc_epm
7 set lb group CAS_persistency_group_sourceip -persistenceType SOURCEIP -
     timeout {
8  PersTimeout }
9
10 <!--NeedCopy-->
```

Commutation de contenu pour les services HTTP :


```
add cs vserver CAS_vserver_cs SSL {
 Public IP }
  443 -cltTimeout {
 Timeout }
  -caseSensitive OFF -comment "Exchange CS VServer"
bind ssl vserver CAS_vserver_cs -certkeyName {
 CertKey }

add cs action CAS_action_cs_owa -targetLBVserver CAS_vserver_owa
add cs action CAS_action_cs_oab -targetLBVserver CAS_vserver_oab
add cs action CAS_action_cs_as -targetLBVserver CAS_vserver_as
add cs action CAS_action_cs_oa -targetLBVserver CAS_vserver_oa
add cs action CAS_action_cs_ews -targetLBVserver CAS_vserver_ews
add cs action CAS_action_cs_autodiscover -targetLBVserver
   CAS_vserver_ad
add cs policy CAS_policy_cs_owa -rule "HTTP.REQ.URL.SET_TEXT_MODE(
   IGNORECASE).STARTSWITH("/owa")" -action CAS_action_cs_owa
add cs policy CAS_vserver_oab -rule "HTTP.REQ.URL.SET_TEXT_MODE (
   IGNORECASE).STARTSWITH("/OAB")"
add cs policy CAS_policy_cs_as -rule "HTTP.REQ.URL.SET_TEXT_MODE(
   IGNORECASE).STARTSWITH("/Microsoft-Server-ActiveSync")" -action
   CAS_action_cs_as
add cs policy CAS_policy_cs_autodiscover -rule "HTTP.REQ.URL.
   SET_TEXT_MODE(IGNORECASE).STARTSWITH("/Autodiscover")" -action
   CAS_action_cs_autodiscover
add cs policy CAS_policy_cs_oa -rule "HTTP.REQ.URL.SET_TEXT_MODE(
   IGNORECASE).STARTSWITH("/rpc")" -action CAS_action_cs_oa
add cs policy CAS_policy_cs_ews -rule "HTTP.REQ.URL.SET_TEXT_MODE(
   IGNORECASE).STARTSWITH("/EWS")" -action CAS_action_cs_ews

bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_oa -priority
   90
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_owa -priority
   100
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_oab -priority
   100
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_as -priority
   110
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_autodiscover -
   priority 120
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_ews -priority
   130
bind cs vserver CAS_vserver_cs -lbvserver CAS_vserver_owa
<!--NeedCopy-->
```


Exemples de configuration recommandés pour les versions de Microsoft Exchange Server inférieures à 2016

Groupes de services supplémentaires :

```
add serviceGroup CAS_servicegroup_rpc_ca TCP -maxClient 0 -maxReq 0 -
    cip DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
  -svrTimeout {
 Timeout }
  -CKA NO -TCPB NO -CMP NO
add serviceGroup CAS_servicegroup_rpc_ab TCP -maxClient 0 -maxReq 0 -
    cip DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
  -svrTimeout {
 Timeout }
  -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_rpc_ca {
 CAS-1 Server }
  {
 CA Port }
  -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_ca {
 CAS-2 Server }
  {
 CA Port }
  -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_ab {
 CAS-1 Server }
  {
 AB Port }
  -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_ab {
 CAS-2 Server }
  {
 AB Port }
  -CustomServerID ""None""
<!--NeedCopy-->
```

Moniteurs supplémentaires :

```
add lb monitor CAS_monitor_rpc_ca TCP -LRTM ENABLED -destPort {
 CA Port }

add lb monitor CAS_monitor_rpc_ab TCP -LRTM ENABLED -destPort {
```



```
 AB Port }

bind serviceGroup CAS_servicegroup_rpc_ca -monitorName
   CAS_monitor_rpc_ca
bind serviceGroup CAS_servicegroup_rpc_ab -monitorName
   CAS_monitor_rpc_ab
<!--NeedCopy-->
```

Serveurs virtuels d'équilibrage de charge supplémentaires :

```
add lb vserver CAS_vserver_rpc_ab TCP {
 RPC Public IP }
  {
 AB Port }
  -timeout {
 PersTimeout }
  -cltTimeout {
 Timeout }
  -comment "vserver for  RPC Address Book"
add lb vserver CAS_vserver_rpc_ca TCP {
 RPC Public IP }
  {
 CA Port }
  -timeout {
 PersTimeout }
  -cltTimeout {
 Timeout }
  -comment "vserver for  RPC Client Access"
bind lb vserver CAS_vserver_rpc_ab CAS_servicegroup_rpc_ab
bind lb vserver CAS_vserver_rpc_ca CAS_servicegroup_rpc_ca
<!--NeedCopy-->
```

Groupe de persistance supplémentaire :

```
bind lb group CAS_persistency_group_sourceip CAS_vserver_rpc_ab
bind lb group CAS_persistency_group_sourceip CAS_vserver_rpc_ca
<!--NeedCopy-->
```

Exemples de configuration recommandés pour les versions de Microsoft Exchange Server 2016 et plus récentes

Serveur virtuel d'équilibrage de charge supplémentaire :

```
add lb vserver CAS_vserver_mapi SSL 0.0.0.0 0 -timeout {
```



```
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

bind ssl vserver CAS_vserver_mapi -certkeyName {
 CertKey }

bind lb vserver CAS_vserver_mapi CAS_servicegroup_http
<!--NeedCopy-->
```

Groupe de persistance supplémentaire :

```
bind lb group CAS_persistency_group_sourceip CAS_vserver_mapi
<!--NeedCopy-->
```

Changement de contenu pour les services HTTP :

```
add cs action CAS_action_cs_mapi -targetLBVserver CAS_vserver_mapi
add cs policy CAS_policy_cs_mapi -rule "HTTP.REQ.URL.SET_TEXT_MODE(
   IGNORECASE).STARTSWITH("/mapi")" -action CAS_action_cs_mapi
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_mapi -priority
    140
<!--NeedCopy-->
```

Configurations optionnelles

Redirection HTTPS pour Outlook Web App (OWA) :

```
add lb vserver CAS_vserver_owa_http_redirect HTTP {
 HTTP Public IP }
  80 -persistenceType COOKIEINSERT -timeout {
 PersTimeout }
  -lbMethod ROUNDROBIN -redirectURL "https://mail.example.com/owa" -
     cltTimeout {
 Timeout }

<!--NeedCopy-->
```

REMARQUE : Remplacez par une URL de redirection HTTPS appropriée.

Politique de réécriture /owa :

```
add rewrite action owa_rewrite replace http.REQ.URL ""/owa""
add rewrite policy owa_rewrite_policy "http.req.url.eq("/")"
   owa_rewrite
```



```
bind lb vserver CAS_vserver_owa -policyName owa_rewrite_policy -
    priority 100 -gotoPriorityExpression END -type REQUEST
add responder action action_responder_owa redirect ""https://www.
    example.com/owa""
add responder policy_responder_owa HTTP.REQ.IS_VALID
    action_responder_owa
set responder param -undefAction NOOP
bind lb vserver CAS_vserver_owa -policyName policy_responder_owa -
    priority 100 -gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

REMARQUE : Remplacez par une URL de redirection HTTPS appropriée.

Prise en charge de SMTP :

Pour la configuration suivante, USIP doit être activé afin que les serveurs CAS puissent voir l'adresse IP du serveur SMTP d'envoi pour validation. Cette configuration nécessite également que la passerelle par défaut du serveur CAS soit configurée pour pointer vers l'adresse SNIP de l'appliance ADC.

```
add lb vserver CAS_vserver_smtp TCP {
 HTTP Public IP }
  25 -persistenceType SOURCEIP -timeout 60 -lbMethod LEASTCONNECTION -
     cltTimeout 30
add serviceGroup CAS_servicegroup_smtp TCP -maxClient 0 -maxReq 0 -cip
    DISABLED -usip YES -SP OFF -useproxyport YES -cltTimeout 30 -
    svrTimeout 30 -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_smtp {
 CAS-1 Server }
  25 -CustomServerID ""None"" bind serviceGroup CAS_servicegroup_smtp {
 CAS-2 Server }
  25 -CustomServerID ""None""
bind lb vserver CAS_vserver_smtp CAS_servicegroup_smtp
<!--NeedCopy-->
```

Prise en charge de Post Office Protocol version 3 (POP3) :

```
add lb vserver CAS_vserver_pop3 TCP {
 HTTP Public IP }
  110 -persistenceType SOURCEIP -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add serviceGroup CAS_servicegroup_pop3 TCP -maxClient 0 -maxReq 0 -cip
    DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
```



```
 -svrTimeout {
 Timeout }
 -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_pop3 {
 CAS-1 Server }
 110 -CustomServerID ""None"" bind serviceGroup CAS_servicegroup_pop3
     {
 CAS-2 Server }
 110 -CustomServerID ""None""
bind lb vserver CAS_vserver_pop3 CAS_servicegroup_pop3
<!--NeedCopy-->
```

> Remarque :
>
> Vous pouvez effectuer la configuration précédente pour POP3 chiffré SSL en modifiant le port sur 995 et les types de serveur/service virtuel en SSL. Liez également un certificat SSL approprié.

Prise en charge de l'IMAP :

```
add lb vserver CAS_vserver_imap TCP {
 HTTP Public IP }
 143 -persistenceType SOURCEIP -timeout {
 PersTimeout }
 -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add serviceGroup CAS_servicegroup_imap TCP -maxClient 0 -maxReq 0 -cip
    DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
 -svrTimeout {
 Timeout }
 -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_imap {
 CAS-1 Server }
 143 -CustomServerID ""None"" bind serviceGroup CAS_servicegroup_imap
     {
 CAS-2 Server }
 143 -CustomServerID ""None""
bind lb vserver CAS_vserver_imap CAS_servicegroup_imap
<!--NeedCopy-->
```

> Remarque :
>
> Vous pouvez effectuer la configuration précédente pour IMAP crypté SSL en modifiant le port sur 993 et les types de serveur/service virtuel en SSL. Liez également un certificat SSL approprié.

Autres ressources

- Configuration de serveurs d'équilibrage de charge pour Microsoft Exchange avec filtrage de sécurité de la messagerie
- Déploiement de NetScaler avec Microsoft Exchange 2016

Cas d'utilisation 1 : Équilibrage de charge SMPP

August 20, 2021

Des millions de messages courts sont échangés quotidiennement entre des particuliers et des fournisseurs de services à valeur ajoutée, tels que les banques, les annonceurs et les services d'annuaire, à l'aide du protocole SMPP (Short Message peer to peer). Souvent, la remise des messages est retardée parce que les serveurs sont surchargés et que le trafic n'est pas réparti de manière optimale entre les serveurs. Le Citrix ADC prend en charge l'équilibrage de charge SMPP et fournit une distribution optimale des messages sur vos serveurs, évitant ainsi les mauvaises performances et les pannes.

Citrix ADC effectue l'équilibrage de charge côté serveur lorsque les messages sont reçus des clients et côté client lorsque les messages sont reçus des serveurs.

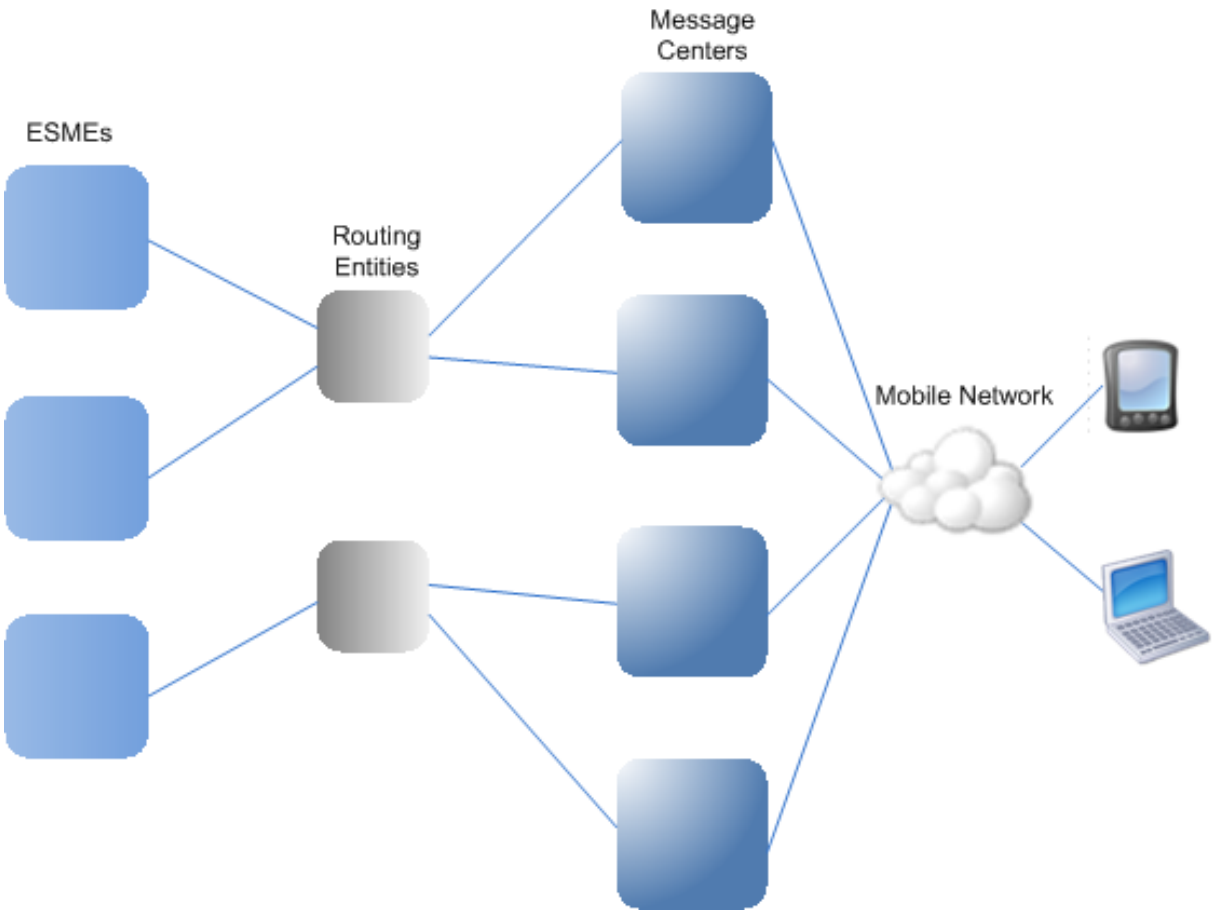
L'équilibrage de charge des messages SMPP par Citrix ADC offre les avantages suivants :

- Meilleure distribution de la charge sur les serveurs, ce qui se traduit par un temps de réponse plus rapide pour les utilisateurs finaux
- Surveillance de l'intégrité des serveurs et meilleures capacités de basculement
- Ajout rapide et facile de nouveaux serveurs (centres de messagerie) sans modifier la configuration du client
- Haute disponibilité

Introduction à SMPP

SMPP est un protocole de couche d'application pour le transfert de messages courts entre les entités de messages courts externes (ESME), les entités de routage (RE) et les centres de messages (MC) via des connexions TCP à longue durée de vie. Il est utilisé pour l'envoi de messages courts (SMS) entre amis, contacts et tiers tels que les banques (banque mobile), les annonceurs (commerce mobile) et les services d'annuaire. Les messages provenant d'une ESME (entité non mobile) arrivent au MC, qui les distribue aux entités de messages courts (PME) telles que les téléphones mobiles. SMPP est également utilisé par les PME pour envoyer des messages courts à des tiers (par exemple, pour l'achat de produits, le paiement de factures et le transfert de fonds). Ces messages arrivent au MC et sont transmis au MC de destination ou à l'ESME.

Le diagramme suivant montre les différentes entités SMPP : ESME, RE et MCs, dans un réseau mobile.



Présentation de l'architecture des différentes entités SMPP dans un réseau mobile

Remarque : Les termes client et ESME sont utilisés de manière interchangeable dans tout le document.

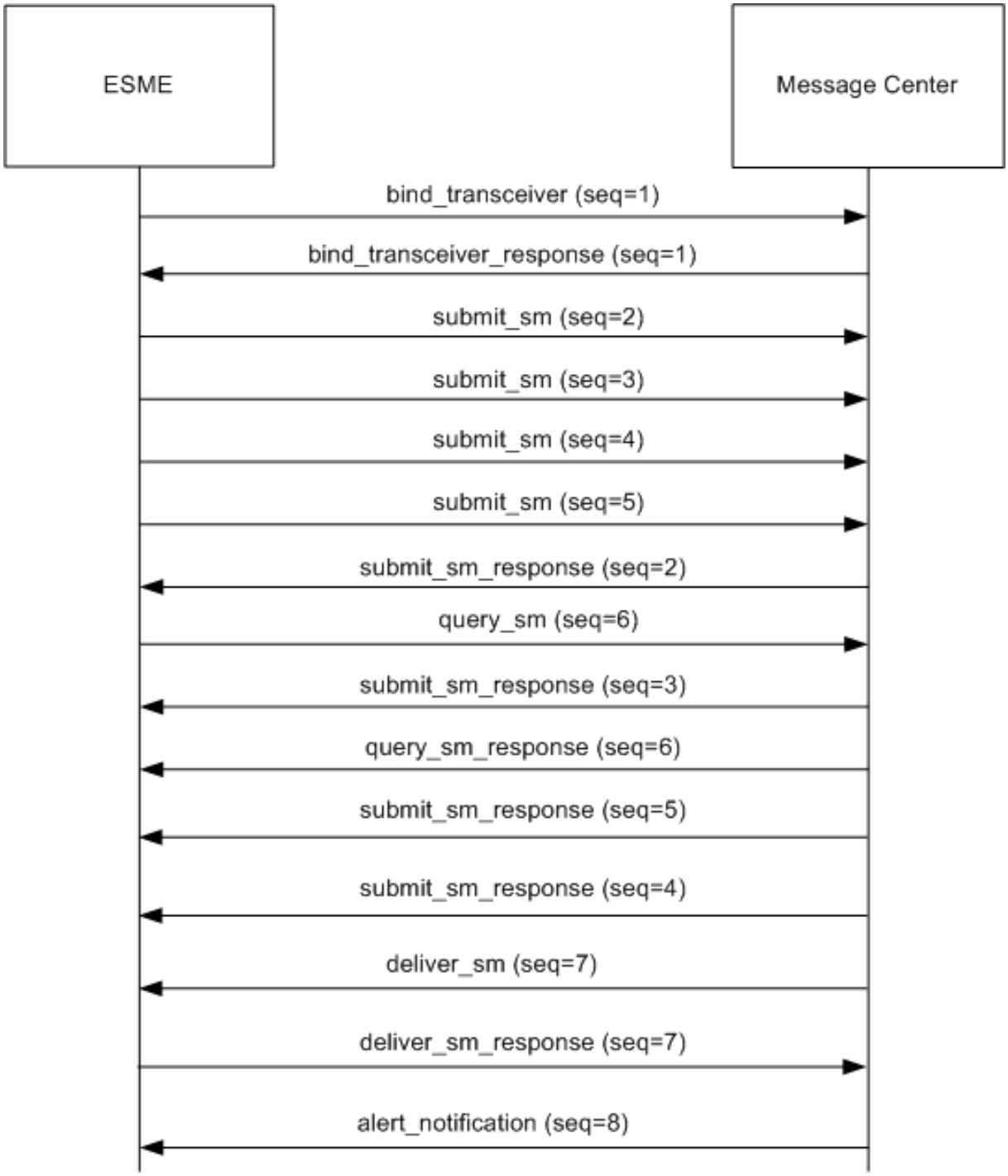
Un ESME (client) ouvre une connexion au MC dans l'un des trois modes suivants : émetteur, récepteur ou émetteur-récepteur. En tant qu'émetteur, il ne peut envoyer que des messages pour la livraison. En tant que récepteur, il ne peut recevoir que des messages. En tant qu'émetteur-récepteur, l'ESME peut envoyer et recevoir des messages. L'ESME envoie au MC l'un des trois messages (également appelés PDU) : bind_transmitter, bind_receiver ou bind_transceiver. Le MC répond avec un bind_transmitter_resp, bind_receiver_resp ou bind_transceiver_resp, selon le cas pour la requête.

Une fois la connexion établie, l'ESME peut, selon le mode dans lequel il est lié au MC, envoyer un message submit_sm ou data_sm, recevoir un message deliver_sm ou data_sm, ou envoyer et recevoir n'importe lequel de ces types de messages. L'ESME peut également envoyer des messages auxiliaires, tels que query_sm, replace_sm et cancel_sm, pour interroger l'état d'une remise de message antérieure, remplacer un message antérieur par un nouveau message ou annuler un message non remis.

Si un message n'est pas remis parce qu'un ESME n'est pas disponible ou qu'un abonné mobile n'est pas en ligne, le message est mis en file d'attente. Plus tard, lorsque le MC détecte que l'abonné mobile est maintenant accessible, il envoie une PDU alert_notification à l'ESME via une session de récepteur ou d'émetteur-récepteur, demandant la remise des messages en file d'attente.

Chaque PDU de demande a un numéro de séquence unique. La PDU de réponse a le même numéro de séquence que la demande d'origine. Étant donné que l'échange de messages sur SMPP peut être en mode asynchrone, un ESME ou un MC peut envoyer plusieurs requêtes à la fois. Le numéro de séquence joue un rôle crucial dans le retour de la réponse dans la même session SMPP. En d'autres termes, le numéro de séquence rend possible la correspondance des demandes et des réponses.

Le diagramme suivant montre comment le flux de trafic utilise les différentes PDU lorsque l'ESME se lie en tant qu'émetteur-récepteur.



Limitation :

L'appliance Citrix ADC ne prend pas en charge les opérations sortantes. Autrement dit, un centre de messages ne peut pas lancer une session SMPP avec un ESME via l'appliance Citrix ADC.

Fonctionnement de l'équilibrage de charge SMPP sur Citrix ADC

Un ESME (client) envoie un message de liaison pour ouvrir une connexion au Citrix ADC. ADC authentifie chaque ESME et, en cas de succès, répond avec un message approprié. Citrix ADC établit une connexion avec chaque centre de messages et équilibre la charge de tous les messages entre ces centres de messages. Lorsque ADC reçoit un message d'un client, il réutilise une connexion ouverte au centre de messages ou envoie une requête de liaison à un centre de messages si une connexion ouverte n'est pas disponible.

ADC peut équilibrer la charge des messages provenant des clients et des serveurs. Il peut surveiller l'état des centres de messages et gérer les messages concaténés. Il fournit également une prise en charge de la commutation de contenu pour les centres de messages.

Messages provenant des ESME

Chaque ESME doit être ajouté en tant qu'utilisateur sur Citrix ADC pour l'authentification. Le client établit une connexion TCP avec un serveur virtuel SMPP configuré sur ADC en envoyant une requête de liaison. ADC authentifie le client et, en cas de succès, analyse le message de liaison. ADC envoie ensuite la demande au centre de messages sélectionné par la méthode d'équilibrage de charge configurée. Si une connexion au centre de messages n'est pas disponible pour réutilisation, l'ADC ouvre une connexion TCP avec le centre de messages en envoyant une nouvelle requête de liaison au centre de messages.

Avant de transférer la réponse (submit_sm_resp ou data_sm_resp) du centre de messages au client, ADC ajoute un ID de serveur personnalisé à l'ID du message afin d'identifier le centre de messages pour les opérations auxiliaires, telles que la requête, le remplacement ou l'annulation des demandes d'un message, par le client. Les demandes d'autres clients sont équilibrées de la même manière.

Dans la requête de liaison d'origine, un client spécifie la plage d'adresses qu'il peut servir. Cette plage est utilisée pour transférer les messages deliver_sm ou data_sm des centres de messages vers les clients.

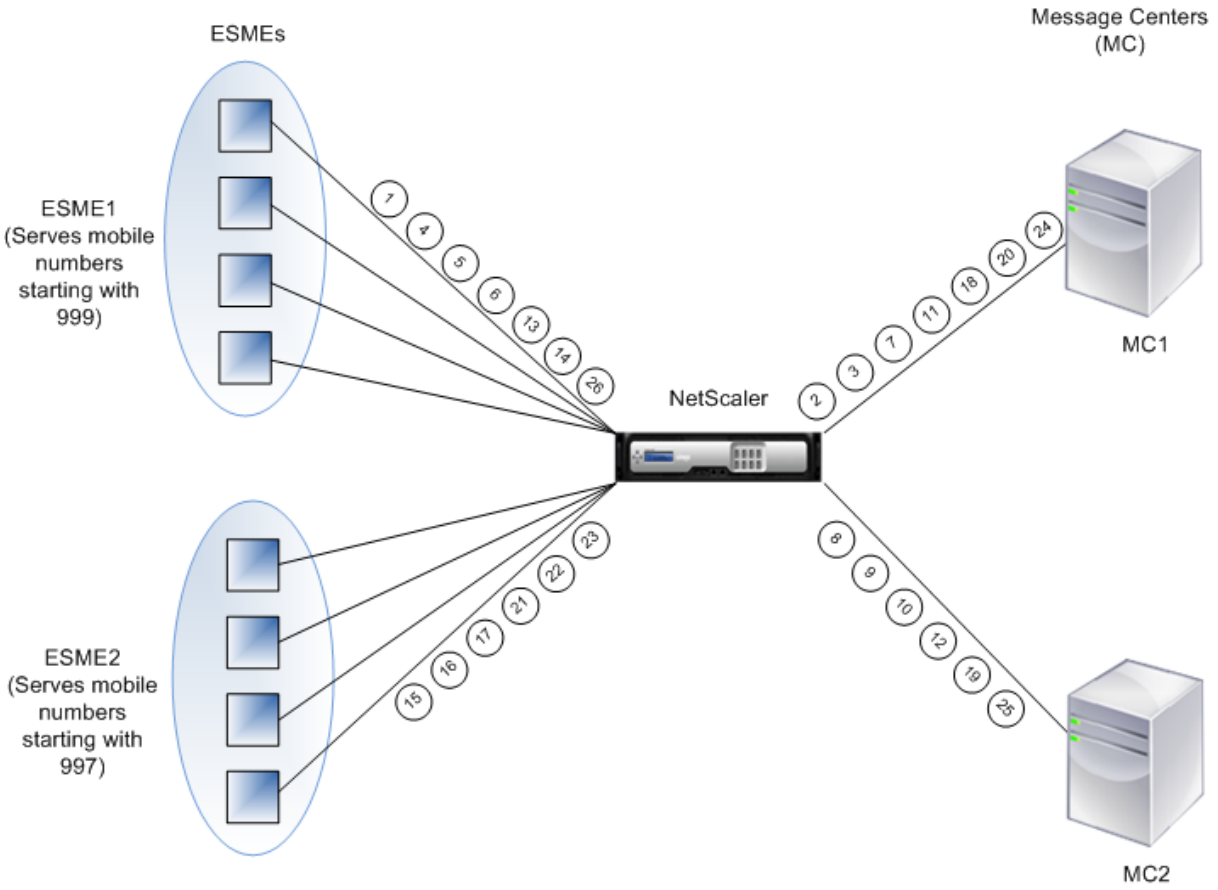
Messages provenant d'un centre de messages

Les ESME qui peuvent gérer une plage d'adresses spécifique sont regroupés dans un cluster. Tous les nœuds d'un cluster fournissent les mêmes informations d'identification. Dans un cluster, seule la méthode round robin est utilisée pour l'équilibrage de charge. Pour envoyer des messages d'origine mobile (MO), le centre de messages envoie un message deliver_sm au Citrix ADC. Si un cluster pouvant servir la plage d'adresses de destination (par exemple, les nombres commençant par 998) est lié à ADC, il sélectionne ce cluster, puis équilibre la charge entre les nœuds ESME de ce cluster.

Si un ESME qui peut servir des messages deliver_sm pour la plage d'adresses n'est pas lié à ADC et que la mise en file d'attente des messages est activée, le message est mis en file d'attente jusqu'à ce qu'un

tel client se lie à ADC en mode récepteur ou émetteur-récepteur. Vous pouvez spécifier la taille de la file d'attente.

Le diagramme suivant illustre le flux interne des PDU entre les ESME, Citrix ADC et les centres de messages. Par souci de simplicité, seuls deux ESME et deux centres de messages sont affichés.



Flux de messages (PDU) :

1. ESME1 envoie une requête de liaison à NetScaler
2. NetScaler envoie une requête de liaison à MC1
3. MC1 envoie une réponse de liaison à NetScaler
4. NetScaler envoie une réponse de liaison à ESME1
5. ESME1 envoie submit_sm (1) à NetScaler
6. ESME1 envoie submit_sm (2) à NetScaler
7. NetScaler transfère submit_sm (1) à MC1
8. NetScaler envoie une requête de liaison à MC2
9. MC2 envoie une réponse de liaison à NetScaler
10. NetScaler transfère submit_sm (2) à MC2
11. MC1 envoie submit_sm_resp (1) à NetScaler
12. MC2 envoie submit_sm_resp (2) à NetScaler
13. NetScaler transfère submit_sm_resp (1) à ESME1

14. NetScaler transfère submit_sm_resp (2) à ESME1
15. ESME2 envoie une requête de liaison à NetScaler
16. NetScaler envoie une réponse de liaison à ESME2
17. ESME2 envoie submit_sm (3) à NetScaler
18. NetScaler transfère submit_sm (3) à MC1
19. MC2 envoie deliver_sm à NetScaler (ESME2 sert la plage d'adresses spécifiée dans le message)
20. MC1 envoie submit_sm_resp (3) à NetScaler
21. NetScaler transfère submit_sm_resp (3) à ESME2
22. NetScaler transfère deliver_sm à ESME2
23. ESME2 envoie deliver_sm_resp à NetScaler
24. MC1 envoie alert_notification à NetScaler (ESME1 sert la plage d'adresses spécifiée dans le message)
25. NetScaler transfère deliver_sm_resp vers MC2
26. NetScaler transmet la notification alert_notification à ESME1

Surveillance de la santé des centres de messages

Par défaut, un moniteur TCP_Default est lié à un service SMPP, mais vous pouvez lier un moniteur personnalisé de type SMPP. Le moniteur personnalisé ouvre une connexion TCP au centre de messages et envoie un paquet enquire_link. En fonction du succès ou de la défaillance de la sonde, le service est marqué comme UP ou DOWN.

Commutation de contenu sur les centres de messages

Les centres de messagerie peuvent accepter plusieurs connexions (ou lier des demandes) provenant d'ESME. Vous pouvez configurer Citrix ADC pour changer de contenu ces demandes en fonction des paramètres de liaison SMPP. Voici quelques expressions courantes pour configurer les méthodes de sélection d'un centre de messages :

- En fonction de la plage d'adresses : Dans l'exemple d'expression suivant, ADC sélectionne un centre de messages spécifique si la plage d'adresses commence à 988.

Exemple :

SMPP.BINDINFO.ADDRESS_RANGE.CONTAINS("^988")

- Basé sur l'ID ESME : Dans l'exemple d'expression suivant, ADC sélectionne un centre de messages spécifique si l'ID ESME est égal à ESME1.

Exemple :

SMPP.BINDINFO.SYSTEM_ID.EQ("ESME1")

- Selon le type ESME : Dans l'exemple d'expression suivant, ADC sélectionne un centre de messages spécifique si le type ESME est VMS. VMS signifie système de messagerie vocale.

Exemple :

SMPP.BINDINFO.SYSTEM_TYPE.EQ(“VMS”)

- En fonction du type de numéro (TON) de l’ESME : Dans l’exemple d’expression suivant, l’ADC sélectionne un centre de messages spécifique si TON est égal à 1 (1 signifie un numéro international).

Exemple :

SMPP.BINDINFO.ADDR_TON.EQ(1)

- Basé sur l’indicateur de plan numérique (NPI) de l’ESME : Dans l’exemple d’expression suivant, ADC sélectionne un centre de messages spécifique si NPI est égal à 0 (0 signifie une connexion inconnue).

Exemple :

SMPP.BINDINFO.ADDR_NPI.EQ(0)

- En fonction du type de liaison : Dans l’exemple d’expression suivant, l’ADC sélectionne un centre de messages spécifique si le type de liaison est TRANSCEIVER. (Un émetteur-récepteur peut envoyer et recevoir des messages.)

Exemple :

SMPP.BINDINFO.TYPE.EQ(TRANSCEIVER)

Gestion des messages concaténés

Un SMS peut contenir un maximum de 140 octets. Les messages plus longs doivent être divisés en petites parties. Si le mobile de destination est capable, les messages sont combinés et livrés en un seul SMS. Citrix ADC transfère les fragments d’un message au même centre de messages. Chaque message contient un numéro de référence, un numéro de séquence et le nombre total de fragments. Le numéro de référence est le même pour chaque fragment d’un message long. Le numéro de séquence spécifie la position du fragment particulier dans le message complet. Une fois tous les fragments reçus, l’ESME combine les fragments en un seul long message et envoie le message à l’abonné mobile.

Si un client se déconnecte d’une connexion active, la connexion au centre de messages n’est pas fermée. Il est réutilisé pour les demandes d’autres clients.

Limitation

Les ID de message, provenant du centre de message, de plus de 59 octets ne sont pas pris en charge. Si la longueur de l’ID de message renvoyée par le centre de messages est supérieure à 59 octets, les opérations auxiliaires échouent et Citrix ADC répond avec un message d’erreur.

Configuration de l'équilibrage de charge SMPP sur Citrix ADC

Effectuez les tâches suivantes pour configurer l'équilibrage de charge SMPP sur ADC :

1. Ajouter un utilisateur SMPP. ADC authentifie l'utilisateur avant d'accepter une demande de liaison de l'utilisateur. L'utilisateur est généralement un ESME.
2. Ajoutez un serveur virtuel d'équilibrage de charge, en spécifiant le protocole comme SMPP.
3. Ajoutez un service, en spécifiant le protocole comme SMPP, et un ID de serveur personnalisé unique pour chaque serveur. Liez le service au serveur virtuel d'équilibrage de charge créé précédemment.
4. Le cas échéant, créez un groupe de services et ajoutez des services au groupe de services.
5. Vous pouvez également ajouter un moniteur de type SMPP-ECV et le lier au service. Un moniteur TCP par défaut est lié par défaut.
6. Définissez les paramètres SMPP, tels que le mode client et la file d'attente de messages.

Pour configurer l'équilibrage de charge SMPP à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
add smpp user <username> -password <password>
add service <name> <IP> SMPP <port>  - customserverID <customserverID>
add lb vserver <name> <IP> SMPP <port>
bind lb vserver <name> <service name>
set smpp param
<!--NeedCopy-->
```

Exemple

```
add smpp user smppclient1 -password c03ebb540695b6110eb31172f32245a1 -
    encrypted -encryptmethod ENCMTHD_2
add smpp user smppclient2 -password c03ebb540695b6110eb31172f32245a1 -
    encrypted -encryptmethod ENCMTHD_2
add service smmpsvc 10.102.84.140 SMPP 2775 -gslb NONE -maxClient 0 -
    maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
     180 -svrTimeout 360 -CustomServerID ab -CKA NO -TCPB NO -CMP NO
add service smmpsvc2 10.102.81.175 SMPP 2775 -gslb NONE -maxClient 0 -
    maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
     180 -svrTimeout 360 -CustomServerID xy -CKA NO -TCPB NO -CMP NO
add lb vserver smppvs SMPP 10.102.239.179 2775 -persistenceType NONE -
    cltTimeout 180
bind lb vserver smppvs smmpsvc2
bind lb vserver smppvs smmpsvc
set smpp param -addrrange "d*"
```



```
<!--NeedCopy-->
```

Pour configurer l'équilibrage de charge SMPP à l'aide de l'utilitaire de configuration

1. Accédez à **Système > Administration des utilisateurs > Utilisateurs SMPP**, puis ajoutez un utilisateur SMPP.
2. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres SMPP**et définissez les paramètres comme requis par votre déploiement.
3. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ajoutez un serveur virtuel de type SMPP.
4. Cliquez dans la section Service, ajoutez un service de type SMPP et spécifiez un ID de serveur.

Cas d'utilisation 2 : Configurer la persistance basée sur une règle basée sur une paire nom-valeur dans un flux d'octets TCP

August 20, 2021

Certains protocoles transmettent des paires nom-valeur dans un flux d'octets TCP. Le protocole du flux d'octets TCP dans cet exemple est le protocole FIX (Financial Information eXchange). Dans une implémentation non XML, le protocole FIX permet à deux hôtes communiquant via un réseau d'échanger des informations commerciales ou liées au commerce sous forme de liste de paires nom-valeur (appelées « champs FIX »). Le format du champ est <tag>=<value><delimiter>. Ce format de marque-valeur traditionnel rend le protocole FIX idéal pour le cas d'utilisation.

La balise dans un champ FIX est un identifiant numérique qui indique la signification du champ. Dans cet exemple ;

- La balise 35 indique le type de message.
- La valeur après le signe égal a une signification spécifique pour la balise donnée et est associée à un type de données. La valeur A pour la balise 35 indique que le message est un message d'ouverture de session.
- Le délimiteur est le caractère ASCII « Start of Header » (SOH) non imprimable (0x01), qui est le symbole de curseur (^).
- Un nom est également attribué à chaque champ. Le champ portant la balise 35 est le champ MsgType.

Voici un exemple de message d'ouverture de session.

8=FIX.4.1 9=61 35=A 49=INVMGR 56=BRKR 34=1 52=20000426-12:05:06 98=0 108=30 10=157

Votre choix de type de persistance pour une liste de valeurs de balise telle que celle présentée ci-dessus est déterminé par les options disponibles pour extraire une chaîne particulière de la liste. Les méthodes de persistance basées sur des jetons nécessitent que vous spécifiez le décalage et la longueur du jeton que vous souhaitez extraire de la charge utile. Le protocole FIX ne vous permet pas de le faire, car le décalage d'un champ donné et la longueur de sa valeur peuvent varier d'un message à l'autre. Cette variation dépend du type de message, des champs précédents et de la longueur des valeurs précédentes. Il varie également en fonction de l'implémentation de l'un à l'autre, selon que des champs personnalisés ont été définis ou non. De telles variations rendent impossible de prédire le décalage exact d'un champ donné ou de spécifier la longueur de la valeur à extraire comme jeton. Dans ce cas, la persistance basée sur des règles est donc le type de persistance préféré.

Supposons qu'un serveur virtuel fixlb1 équilibrage la charge des connexions TCP à une batterie de serveurs hébergeant des instances d'une application compatible FIX. Vous souhaitez configurer la persistance des connexions sur la base de la valeur du champ SenderCompid, qui identifie l'entreprise qui envoie le message. La balise de ce champ FIX est 49 (illustrée dans l'exemple de message d'ouverture de session précédent).

Pour configurer la persistance basée sur des règles pour le serveur virtuel d'équilibrage de charge, définissez le type de persistance du serveur virtuel d'équilibrage de charge sur RULE et configurez le paramètre de règle avec une expression. L'expression doit être celle qui extrait la partie de la charge utile TCP dans laquelle vous prévoyez de trouver le champ SenderCompid, compose la chaîne résultante dans une liste nom-valeur basée sur les délimiteurs, puis extrait la valeur du champ SenderCompid (balise 49), comme suit :

```
set lb vserver fixlb1 -persistenceType RULE -rule "CLIENT.TCP.PAYLOAD(300).
TYPECAST_NVLIST_T('=','^').VALUE("\49\")"
```

Remarque : Les barres obliques inverses ont été utilisées dans l'expression car il s'agit d'une commande CLI. Si vous utilisez l'utilitaire de configuration, n'entrez pas les barres obliques inverses.

Si le client envoie un message FIX contenant la liste nom-valeur de l'exemple précédent de message d'ouverture de session, l'expression extrait la valeur INVMGR et l'appliance Citrix ADC crée une session de persistance basée sur cette valeur.

L'argument de la fonction PAYLOAD () peut être aussi grand que vous le jugez nécessaire pour inclure le champ SenderCompid dans la chaîne extraite par la fonction. Vous pouvez également utiliser la fonction SET_TEXT_MODE (IGNORECASE) si vous souhaitez que l'appliance ignore la casse lors de l'extraction de la valeur du champ, et que la fonction HASH crée une session de persistance basée sur un hachage de la valeur extraite. L'expression suivante utilise les fonctions SET_TEXT_MODE (IGNORECASE) et HASH :

```
CLIENT.TCP.PAYLOAD(500).TYPECAST_NVLIST_T('=','^').SET_TEXT_MODE(IGNORECASE
).VALUE("49").HASH
```


Voici d'autres exemples de règles que vous pouvez utiliser pour configurer la persistance des connexions FIX (remplacez<tag> par la balise du champ dont vous souhaitez extraire la valeur) :

- Pour extraire la valeur d'un champ FIX dans les 300 premiers octets de la charge utile TCP, vous pouvez utiliser l'expression CLIENT.TCP.PAYLOAD(300).BEFORE_STR("^").AFTER_STR("<tag>=").
- Pour extraire une chaîne de 20 octets au décalage 80, convertissez la chaîne dans une liste nom-valeur, puis extrayez la valeur du champ souhaité, utilisez l'expression CLIENT.TCP.PAYLOAD(100).SUBSTR(80,
  tag>").
- Pour extraire les 100 premiers octets de la charge utile TCP, convertissez la chaîne dans une liste nom-valeur et extraire la valeur de la troisième occurrence du champ souhaité, utilisez l'expression CLIENT.TCP.PAYLOAD(100).TYPECAST_NVLIST_T('=','^').VALUE("<tag>",2).
  Remarque : Si le second argument transmis à la fonction
  VALUE() est
  n, l'appliance extrait la valeur de l'instance
  (n+1)
  th du champ car le nombre commence à zéro (
  0).

Voici d'autres exemples de règles que vous pouvez utiliser pour configurer la persistance. Seules les expressions basées sur la charge utile peuvent évaluer les données transmises via le protocole FIX. Les autres expressions sont des expressions plus générales pour configurer la persistance basée sur des protocoles de mise en réseau inférieurs.

- CLIENT.TCP.PAYLOAD (100)
- CLIENT.TCP.PAYLOAD (100) .HASH
- CLIENT.TCP.PAYLOAD (100) .SUBSTR (5,10)
- CLIENT.TCP.SRCPORT
- CLIENT.TCP.DSTPORT
- CLIENT.IP.SRC
- CLIENT.IP.DST
- CLIENT.IP.SRC.GET4
- CLIENT.IP.DST.GET4
- CLIENT.ETHER.SRCMAC.GET6
- CLIENT.ETHER.DSTMAC.GET5
- CLIENT.VLAN.ID

Cas d'utilisation 3 : Configurer l'équilibrage de charge en mode de retour direct du serveur

August 20, 2021

L'équilibrage de charge en mode DSR (Direct Server Return) permet au serveur de répondre directement aux clients à l'aide d'un chemin de retour qui ne passe pas par l'appliance Citrix ADC. Toutefois, en mode DSR, l'appliance peut continuer à effectuer des vérifications de l'état des services. Dans un environnement à volume élevé de données, l'envoi de trafic serveur directement au client en mode DSR augmente la capacité globale de gestion des paquets de l'appliance, car les paquets ne transitent pas par l'appliance.

Le mode DSR présente les caractéristiques et limitations suivantes :

- Il prend en charge le mode à un bras et le mode en ligne.
- L'appliance vieillit les sessions en fonction du délai d'inactivité.
- Étant donné que l'appliance ne fournit pas de proxy aux connexions TCP (c'est-à-dire qu'elle n'envoie pas SYN-ACK au client), elle n'arrête pas les attaques SYN. En utilisant le filtre de débit de paquets SYN, vous pouvez contrôler le taux de SYN sur le serveur. Pour contrôler le taux de syns, définissez un seuil pour le taux de syns. Pour obtenir une protection contre les attaques SYN, vous devez configurer l'appliance pour les connexions TCP par proxy. Toutefois, cela nécessite que le trafic inverse circule à travers l'appliance.
- Dans une configuration DSR, l'appliance Citrix ADC ne remplace pas l'adresse IP du serveur virtuel d'équilibrage de charge par l'adresse IP du serveur de destination. Au lieu de cela, il transfère les paquets à un service en utilisant l'adresse MAC du serveur. Le VIP doit être configuré sur le serveur et ARP doit être désactivé pour le VIP configuré sur le serveur. Cela empêche la demande du client de contourner l'appliance lorsqu'elle est configurée en mode à bras unique. Par exemple, un utilisateur doit configurer VIP dans l'interface de bouclage et désactiver l'ARP pour le même VIP.
- L'appliance obtient l'adresse MAC du serveur à partir du moniteur lié au service. Toutefois, les moniteurs utilisateur personnalisés (moniteurs de type USER), qui utilisent des scripts stockés sur l'appliance Citrix ADC, n'apprennent pas l'adresse MAC d'un serveur. Si vous utilisez uniquement des moniteurs personnalisés dans une configuration DSR, pour chaque demande reçue par le serveur virtuel, l'appliance tente de résoudre l'adresse IP de destination en une adresse MAC (en envoyant des demandes ARP). Étant donné que l'adresse IP de destination est une adresse IP virtuelle appartenant à l'appliance Citrix ADC, les demandes ARP se résolvent toujours à l'adresse MAC de l'interface Citrix ADC. Par conséquent, tout le trafic reçu par le serveur virtuel est renvoyé en boucle vers l'appliance. Si vous utilisez des moniteurs utilisateur dans une configuration DSR, vous devez également configurer un autre moniteur d'un type différent (par exemple, un moniteur PING) pour les services, idéalement avec un intervalle plus long entre les

sondes, afin que l'adresse MAC des serveurs puisse être apprise.

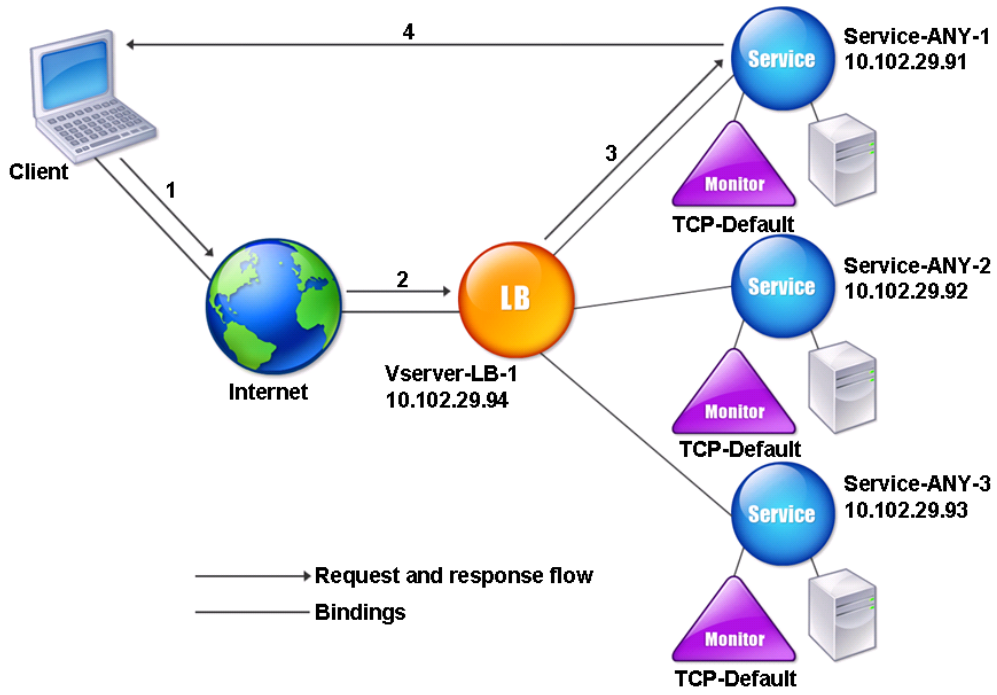
- L'appliance Citrix ADC apprend les paramètres L2 du serveur à partir du moniteur lié au service. Pour les moniteurs UDP-ECV, configurez une chaîne de réception pour permettre à l'appliance d'apprendre les paramètres L2 du serveur. Si la chaîne de réception n'est pas configurée et que le serveur ne répond pas, l'appliance n'apprend pas les paramètres L2, mais le service est défini sur UP. Le trafic de ce service est en trou noir.

Dans l'exemple de scénario, les services Service-ANY-1, Service-ANY-2 et Service-ANY-3 sont créés et liés au serveur virtuel Vserver-LB-1. La charge du serveur virtuel équilibre la demande du client vers un service et le service répond directement aux clients, en contournant l'appliance Citrix ADC. Le tableau suivant répertorie les noms et les valeurs des entités configurées sur l'appliance Citrix ADC en mode DSR.

Type d'entité	Nom	Adresse IP	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.94	ANY
Services	Service-ANY-1	10.102.29.91	ANY
	Service-ANY-2	10.102.29.92	ANY
	Service-ANY-3	10.102.29.93	ANY
Moniteurs	TCP	Aucune	Aucune

Le diagramme suivant présente les entités d'équilibrage de charge et les valeurs des paramètres à configurer sur l'appliance.

Figure 1. Modèle d'entité pour l'équilibrage de charge dans le modèle DSR



Pour que l'appliance fonctionne correctement en mode DSR, l'adresse IP de destination dans la requête client doit être inchangée. Au lieu de cela, l'appliance modifie le MAC de destination en celui du serveur sélectionné. Ce paramètre permet au serveur de déterminer l'adresse MAC du client pour transférer les demandes au client tout en contournant le serveur.

Ensuite, vous configurez une configuration d'équilibrage de charge de base comme décrit dans Configuration de l'équilibrage de chargede base, nommer les entités et définir les paramètres à l'aide des valeurs décrites dans le tableau précédent.

Après avoir configuré la configuration d'équilibrage de charge de base, vous devez la personnaliser pour le mode DSR. Pour ce faire, vous configurez une méthode d'équilibrage de charge prise en charge, telle que la méthode de hachage IP source avec un serveur virtuel sans session. Vous devez également définir le mode de redirection pour permettre au serveur de déterminer l'adresse MAC du client pour transférer les réponses et de contourner l'appliance.

Après avoir configuré la méthode d'équilibrage de charge et le mode de redirection, vous devez activer le mode USIP sur chaque service. Le service utilise ensuite l'adresse IP source lors du transfert des réponses.

Pour configurer la méthode d'équilibrage de charge et le mode de redirection pour un serveur virtuel sans session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <
   RedirectionMode> -sessionless <Value>
<!--NeedCopy-->
```

Exemple

```
set lb vserver Vserver-LB-1 -lbMethod SourceIPHash -m MAC -sessionless
   enabled
<!--NeedCopy-->
```

> **Remarque**
>
> Pour un service lié à un serveur virtuel sur lequel l'option -m MAC est activée, vous devez lier un moniteur non-utilisateur.

Pour configurer la méthode d'équilibrage de charge et le mode de redirection pour un serveur virtuel sans session à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel, sélectionnez Mode de redirection comme basé sur MAC et méthode comme SOURCEIPHASH.
3. Dans Paramètres de trafic, sélectionnez Équilibrage de charge sans session.

Pour configurer un service pour utiliser l'adresse IP source à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <ServiceName> -usip <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-ANY-1 -usip yes
<!--NeedCopy-->
```


Pour configurer un service pour utiliser l'adresse IP source à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Ouvrez un service, puis dans Paramètres de trafic, sélectionnez **Utiliser l'adresse IP source**.

Certaines étapes supplémentaires sont nécessaires dans certaines situations, décrites dans les sections suivantes.

Cas d'utilisation 4 : Configurer les serveurs LINUX en mode DSR

August 20, 2021

Le système d'exploitation LINUX nécessite la configuration d'une interface de bouclage avec l'adresse IP virtuelle (VIP) de l'appliance Citrix ADC sur chaque serveur équilibré de charge dans le cluster DSR.

Pour configurer le serveur LINUX en mode DSR

Pour créer une interface de retour en boucle avec le VIP de l'appliance Citrix ADC sur chaque serveur à équilibrage de charge, à l'invite du système d'exploitation Linux, tapez les commandes suivantes :

```
ifconfig dummy0 up

ifconfig dummy0:0 inet <netscaler vip> netmask 255.255.255.255 up

echo 1 > /proc/sys/net/ipv4/conf/dummy0/arp_ignore

echo 2 > /proc/sys/net/ipv4/conf/dummy0/arp_announce
<!--NeedCopy-->
```

Ensuite, exécutez le logiciel qui remappe l'identifiant TOS en VIP.

Remarque : ajoutez les mappages corrects au logiciel avant de l'exécuter. Dans les commandes précédentes, le serveur LINUX utilise dummy0 pour se connecter au réseau. Lorsque vous utilisez cette commande, tapez le nom de l'interface utilisée par votre serveur LINUX pour se connecter au réseau.

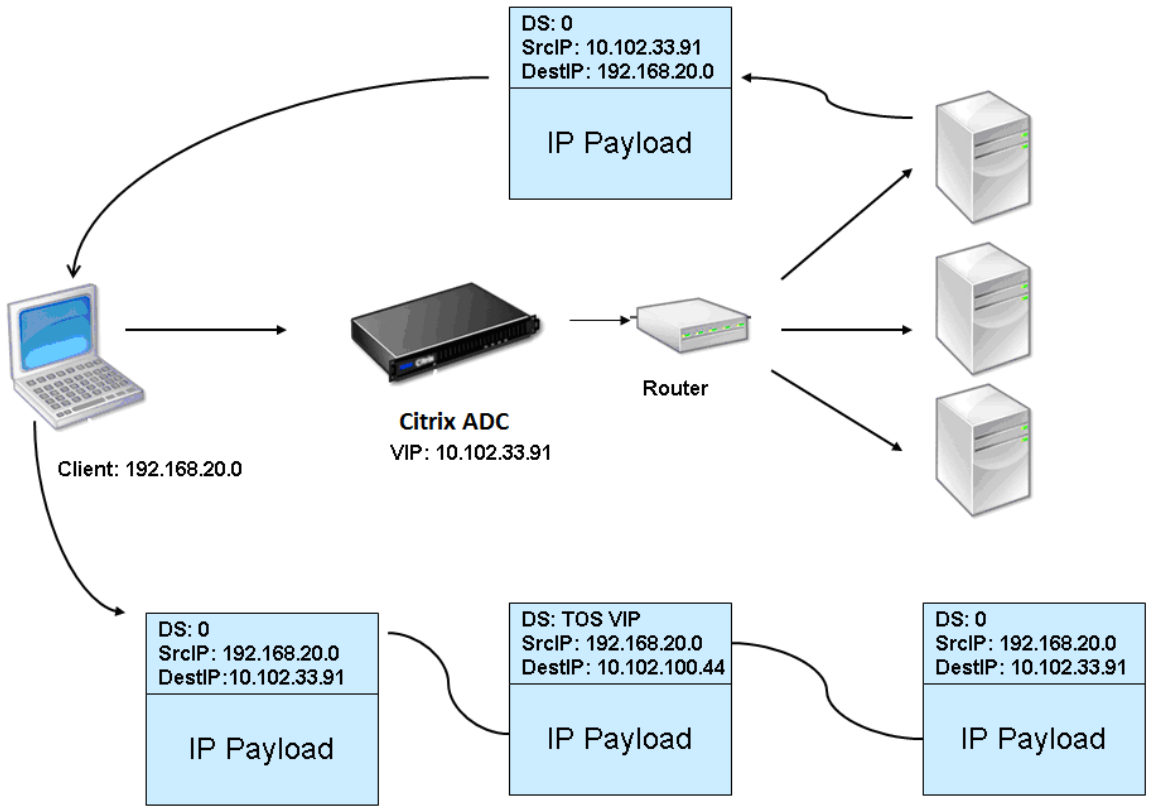
Cas d'utilisation 5 : Configurer le mode DSR lors de l'utilisation de TOS

August 20, 2021

Les services différenciés (DS), également appelés TOS (Type of Service), sont un champ qui fait partie de l'en-tête de paquet IPv4. Le champ équivalent dans l'en-tête IPv6 est Classe de trafic. TOS est utilisé par les protocoles de couche supérieure pour optimiser le chemin d'accès d'un paquet. Les informations TOS code l'adresse IP virtuelle (VIP) de l'appliance Citrix ADC, et les serveurs à équilibrage de charge en extraient le VIP.

Dans le scénario suivant, l'appliance ajoute le VIP au champ **TOS** du paquet, puis transmet le paquet au serveur d'équilibrage de charge. Le serveur à équilibrage de charge répond ensuite directement au client, en contournant l'appliance, comme illustré dans le diagramme suivant.

Figure 1. L'appliance Citrix ADC en mode DSR avec TOS



La fonctionnalité TOS est personnalisée pour un environnement contrôlé comme suit :

- L'environnement ne doit pas comporter de périphériques avec état, tels que pare-feu avec état et passerelles TCP, dans le chemin entre l'appliance et les serveurs équilibrés de charge.
- Les routeurs de tous les points d'entrée du réseau doivent supprimer le champ TOS de tous les paquets entrants pour s'assurer que le serveur à équilibrage de charge ne confond pas un autre champ TOS avec celui ajouté par l'appliance.
- Chaque serveur ne peut avoir que 63 VIP.
- Le routeur intermédiaire ne doit pas envoyer de messages d'erreur ICMP concernant la fragmen-

tation. Le client ne comprend pas le message, car l'adresse IP source est l'adresse IP du serveur équilibré de charge et non le VIP Citrix ADC.

- Les TOS sont valides uniquement pour les services basés sur IP. Vous ne pouvez pas utiliser de services basés sur un nom de domaine avec TOS.

Dans l'exemple, Service-any-1 est créé et lié au serveur virtuel vServer-lb-1. La charge du serveur virtuel équilibre la demande du client au service et le service répond directement aux clients, en contournant l'appliance. Le tableau suivant répertorie les noms et les valeurs des entités configurées sur l'appliance en mode DSR.

Type d'entité	Nom	Adresse IP	Protocole
Serveur virtuel	Vserver-LB-1	10.102.33.91	ANY
Services	Service-ANY-1	10.102.100.44	ANY
Moniteurs	PING	Aucune	Aucune

DSR avec TOS nécessite que l'équilibrage de charge soit configuré sur la couche 3. Pour configurer une configuration d'équilibrage de charge de base pour la couche 3, reportez-vous à la section Configuration de l'équilibrage de charge de base. Nommez les entités et définissez les paramètres à l'aide des valeurs décrites dans le tableau précédent.

Après avoir configuré la configuration d'équilibrage de charge, vous devez personnaliser la configuration d'équilibrage de charge pour le mode DSR en configurant le mode de redirection pour permettre au serveur de décapsuler le paquet de données, puis de répondre directement au client et de contourner l'appliance.

Après avoir spécifié le mode de redirection, vous pouvez éventuellement autoriser l'appliance à surveiller le serveur de manière transparente. Cela permet à l'appliance de surveiller de manière transparente les serveurs équilibrés de charge.

Pour configurer le mode de redirection pour le serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <vServerName> -m <Value> -tosId <Value>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -m TOS -tosId 3
<!--NeedCopy-->
```


Pour configurer le mode de redirection du serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel et, en mode redirection, sélectionnez ID TOS.

Pour configurer le moniteur transparent pour TOS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add monitor <MonitorName> <Type> -destip <DestinationIP> -tos <Value> -
     tosId <Value>
2 <!--NeedCopy-->
```

Exemple :

```
1 add monitor mon1 PING -destip 10.102.33.91 -tos Yes  -tosId 3
2 <!--NeedCopy-->
```

Pour créer le moniteur transparent pour TOS à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Créez un moniteur, sélectionnez TOS et tapez l'ID TOS que vous avez spécifié pour le serveur virtuel.

Moniteurs de TOS génériques

Dans une configuration d'équilibrage de charge en mode DSR utilisant le champ TOS, la surveillance de ses services nécessite la création d'un moniteur TOS et lié à ces services. Un moniteur TOS distinct est requis pour chaque configuration d'équilibrage de charge en mode DSR à l'aide du champ TOS, car un moniteur TOS nécessite l'adresse VIP et l'ID TOS pour créer une valeur codée de l'adresse VIP. Le moniteur crée des paquets de sonde dans lesquels le champ **TOS** est défini sur la valeur codée de l'adresse VIP. Il envoie ensuite les paquets de sonde aux serveurs représentés par les services d'une configuration d'équilibrage de charge.

Avec de nombreuses configurations d'équilibrage de charge, la création d'un moniteur TOS personnalisé distinct pour chaque configuration est une tâche lourde et importante. La gestion de ces moniteurs du PE est également une tâche importante. Maintenant, vous pouvez créer des moniteurs de TOS génériques. Créez un seul moniteur TOS générique pour toutes les configurations d'équilibrage de charge qui utilisent le même protocole (par exemple, TCP ou UDP).

Un moniteur de TOS générique possède les paramètres obligatoires suivants :

- Type = <protocol>
- TOS = Oui

Les paramètres suivants peuvent être définis sur une valeur ou peuvent être laissés vides :

- IP destination
- Port de destination
- ID TOS

Un moniteur TOS générique (avec IP de destination, port de destination et ID TOS non définis) lié à un service DSR apprend automatiquement l'ID TOS et l'adresse VIP du serveur virtuel d'équilibrage de charge. Le moniteur crée des paquets de sonde avec le champ TOS défini sur l'adresse VIP codée, puis envoie les paquets de sonde au serveur représenté par le service DSR.

Pour créer un moniteur de TOS générique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lb monitor <monitorName> <Type> -tos YES
2
3 show lb monitor <monitorName>
4 <!--NeedCopy-->
```

Pour lier un moniteur de TOS générique à un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 bind lb monitor <monitorName> <serviceName>
2
3 show lb monitor <monitorName>
4 <!--NeedCopy-->
```

Pour créer un moniteur de TOS générique à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**.
2. Ajoutez un moniteur avec les paramètres suivants :
   - Type = <protocol>
   - TOS = OUI

Pour lier un moniteur de TOS générique à un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.

2. Ouvrez un service et liez un moniteur de TOS générique à celui-ci.

Dans l'exemple de configuration suivant, V1, V2 et V3 sont des serveurs virtuels d'équilibrage de charge de type ANY et dont l'ID TOS est défini sur 1, 2 et 3 respectivement. S1, S2, S3, S4 et S5 sont des services de type ANY. S1 et S2 sont liés à V1 et V2. S3, S4 et S5 et liés à V1 et V3. WLCD-TOS-MON est un moniteur TOS générique de type TCP et est lié à S1, S2, S3, S4 et S5.

WLCD-TOS-MON apprend automatiquement l'ID TOD et l'adresse VIP des serveurs virtuels liés à S1, S2, S3, S4 et S5.

Étant donné que S1 est lié à V1 et V2, WLCD-TOS-MON crée deux types de paquets de sonde pour S1, l'un avec le champ **TOS** défini sur l'adresse VIP codée (203.0.113.1) de V1 et l'autre avec l'adresse VIP (203.0.113.2) de V2. Citrix ADC envoie ensuite ces paquets de sonde au serveur représenté par S1. De même, WLCD-TOS-MON crée des paquets de sonde pour S2, S3, S4 et S5.

```
1  add lb monitor WLCD-TOS-MON  TCP -tos YES
2
3  Done
4
5  add lb vserver V1 ANY 203.0.113.1 * -m TOS  - tosID 1
6
7  Done
8
9  add lb vserver V2 ANY 203.0.113.2 * -m TOS  - tosID 2
10
11 Done
12
13 add lb vserver V3 ANY 203.0.113.3 * -m TOS  - tosID 3
14
15 Done
16
17 add service S1 198.51.100.1 ANY *
18
19 Done
20
21 add service S2 198.51.100.2 ANY *
22
23 Done
24
25 add service S3 198.51.100.3 ANY *
26
27 Done
28
29 add service S4 198.51.100.4 ANY *
30
31 Done
```



```
32
33 add service S5 198.51.100.5 ANY *
34
35 Done
36
37 bind lb monitor WLCD-TOS-MON S1
38
39 Done
40
41 bind lb monitor WLCD-TOS-MON S2
42
43 Done
44
45 bind lb monitor WLCD-TOS-MON S3
46
47 Done
48
49 bind lb monitor WLCD-TOS-MON S4
50
51 Done
52
53 bind lb monitor WLCD-TOS-MON S5
54
55 Done
56
57 bind lb vserver V1 S1, S2, S3, S4, S5
58
59 Done
60
61 bind lb vserver V2, S1, S2
62
63 Done
64
65 bind lb vserver V3 S3, S4, S5
66
67 Done
68 <!--NeedCopy-->
```


Cas d'utilisation 6 : Configurer l'équilibrage de charge en mode DSR pour les réseaux IPv6 à l'aide du champ TOS

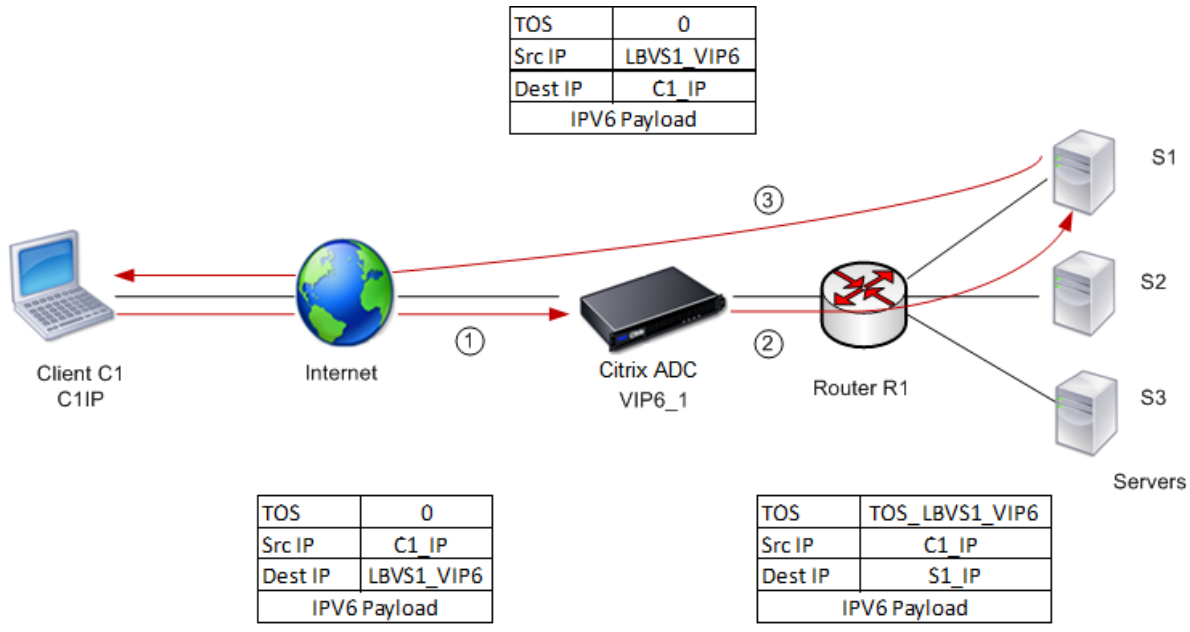
August 20, 2021

Vous pouvez configurer l'équilibrage de charge en mode DSR (Direct Server Return) pour les réseaux IPv6 à l'aide du champ Type de service (TOS) lorsque l'appliance Citrix ADC et les serveurs se trouvent dans des réseaux différents.

Remarque : Le champ TOS est également appelé champ Classe de trafic.

En mode DSR, lorsqu'un client envoie une demande à une adresse VIP6 sur une appliance Citrix ADC, l'appliance transmet cette demande au serveur en changeant l'adresse IPv6 de destination du paquet à l'adresse IPv6 du serveur et en définissant une valeur codée de l'adresse VIP6 dans le TOS (également appelée classe de trafic) de l'en-tête IPv6. Vous pouvez configurer le serveur pour qu'il utilise les informations du champ TOS pour dériver l'adresse VIP6 de la valeur codée, qui est ensuite utilisée comme adresse IP source dans les paquets de réponse. Le trafic de réponse est directement acheminé vers le client, en contournant l'appliance.

Prenons un exemple où un serveur virtuel d'équilibrage de charge LBVS1, configuré sur une appliance Citrix ADC NS1, est utilisé pour équilibrer le trafic entre les serveurs S1, S2 et S3. L'appliance Citrix ADC NS1 et les serveurs S1, S2 et S3 se trouvent dans des réseaux différents, de sorte que le routeur R1 est déployé entre NS1 et les serveurs.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Entités	Nom
Adresse IPv6 du client C1	C1_IP (à titre de référence uniquement)
Serveur virtuel d'équilibrage de charge sur NS1	LBVS1
Adresse IPv6 de LBVS1	LBVS1_VIP6 (à des fins de références uniquement)
Valeur TOS	TOS_LBVS1_VIP6 (à des fins de référence uniquement)
Service pour le serveur S1 sur NS1	SVC_S1
Adresse IPv6 pour le serveur S1	S1_IP (à des fins de références uniquement)
Service pour le serveur S2 sur NS1	SVC_S2
Adresse IPv6 pour le serveur S1	S2_IP (à des fins de références uniquement)
Service pour le serveur S3 sur NS1	SVC_S3
Adresse IPv6 pour le serveur S1	S3_IP (à des fins de références uniquement)

Voici le flux de trafic dans l'exemple de scénario :

1. Le client C1 envoie une requête au serveur virtuel LBVS1.
2. L'algorithme d'équilibrage de charge de LBVS1 sélectionne le serveur S1 et l'appliance ouvre une connexion à S1. NS1 envoie la demande à S1 avec :
   - Champ TOS défini sur TOS_LBVS1_VIP6.
   - Adresse IP source en tant que C1_IP.
3. Le serveur S1, à la réception de la demande, utilise les informations du champ TOS pour dériver l'adresse LBVS1_VIP6, qui est l'adresse IP du serveur virtuel LBVS1 sur NS1. Le serveur envoie directement la réponse à C1, en contournant l'appliance, avec :
   - Adresse IP source définie sur l'adresse Derivedlbvs1_VIP6 afin que le client communique au serveur virtuel LBVS1 sur NS1 et non au serveur S1.

Pour configurer l'équilibrage de charge en mode DSR à l'aide de TOS, effectuez les opérations suivantes sur l'appliance

1. Activer le mode USIP globalement.
2. Ajoutez les serveurs en tant que services.
3. Configurez un serveur virtuel d'équilibrage de charge avec une valeur TOS.
4. Liez les services au serveur virtuel.

Pour configurer l'équilibrage de charge en mode DSR à l'aide de TOS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
enable ns mode USIP

add service <serviceName> <IP> <serviceType> <port>
<!--NeedCopy-->
```

Répétez la commande précédente autant de fois que nécessaire pour ajouter chaque serveur en tant que service sur l'appliance Citrix ADC.

```
add lb vserver <name> <serviceType> <ip> <port> -m <redirectionMode> -
    tosId <positive_integer>

bind lb vserver <vserverName> <serviceName>
<!--NeedCopy-->
```

Pour activer le mode USIP à l'aide de l'utilitaire de configuration

Accédez à **Système > Paramètres > Configurer les modes**, puis sélectionnez **Utiliser l'adresse IP source**.

Pour créer des services à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis créez un service.

Pour créer un serveur virtuel d'équilibrage de charge et lier des services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et créez un serveur virtuel.
2. Cliquez dans la section Service pour lier un service à ce serveur virtuel.

Cas d'utilisation 7 : Configurer l'équilibrage de charge en mode DSR à l'aide d'IP sur IP

August 20, 2021

Vous pouvez configurer une appliance Citrix ADC pour qu'elle utilise le mode DSR (Direct Server Return) sur les réseaux de couche 3 à l'aide d'un tunnel IP, également appelé configuration *IP sur IP* . Comme pour les configurations standard d'équilibrage de charge pour le mode DSR, cela permet aux serveurs de répondre directement aux clients au lieu d'utiliser un chemin de retour via l'appliance Citrix ADC. Cela améliore le temps de réponse et le débit. Comme pour le mode DSR standard, l'appliance Citrix ADC surveille les serveurs et effectue des vérifications de l'état des ports de l'application.

Avec la configuration IP sur IP, l'appliance Citrix ADC et les serveurs n'ont pas besoin d'être sur le même sous-réseau de couche 2. Au lieu de cela, l'appliance Citrix ADC encapsule les paquets avant de les envoyer au serveur de destination. Une fois que le serveur de destination reçoit les paquets, il les décapsule, puis envoie ses réponses directement au client. C'est souvent ce que l'on appelle L3DSR.

Pour configurer le mode L3-DSR sur votre appliance Citrix ADC :

- Créez un serveur virtuel d'équilibrage de charge. Définissez le mode sur IPTUNNEL et activez le suivi sans session.
- Créez des services. Créez un service pour chaque application principale et liez les services au serveur virtuel.
- Configurez pour la décapsulation. Configurez une appliance Citrix ADC ou un serveur principal pour.

> Remarque :
>
> Lorsque vous utilisez une appliance Citrix ADC, la configuration de la décapsulation est un tunnel IP entre les appliances ADC, le backend exécutant L2DSR vers les vrais serveurs.

Configurer un serveur virtuel d'équilibrage de charge

Configurez un serveur virtuel pour traiter les demandes adressées à vos applications. Attribuez le type de service correspondant au service ou utilisez un type de ANY pour plusieurs services.
Définissez la méthode de transfert sur IPTUNNEL et permettez au serveur virtuel de fonctionner en mode sans session. Configurez n'importe quelle méthode d'équilibrage de charge que vous souhaitez utiliser.

Pour créer et configurer un serveur virtuel d'équilibrage de charge pour DSR IP sur IP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour configurer un serveur virtuel d'équilibrage de charge pour IP sur IP DSR et vérifier la configuration :

```
add lb vserver <name> serviceType <serviceType> IPAddress <ip> Port <
    port> -lbMethod <method> -m <ipTunnelTag> -sessionless [ENABLED |
    DISABLED]
```



```
2
3 show lb vserver <name>
4 <!--NeedCopy-->
```

Exemple :

Dans l'exemple suivant, nous avons sélectionné la méthode d'équilibrage de charge comme Sourceİphash et configuré l'équilibrage de charge sans session.

```
1 add lb vserver Vserver-LB-1 ANY 1.1.1.80 * -lbMethod SourceIPHash -m
     IPTUNNEL -sessionless ENABLED
2 <!--NeedCopy-->
```

Pour créer et configurer un serveur virtuel d'équilibrage de charge pour IP sur IP DSR à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Créez un serveur virtuel et spécifiez le mode de redirection comme **base de tunnel IP**.

Configurer les services pour le DSR IP sur IP

Après avoir créé votre serveur à charge équilibrée, configurez un service pour chacune de vos applications. Le service gère le trafic entre l'appliance Citrix ADC et ces applications et permet à l'appliance Citrix ADC de surveiller l'intégrité de chaque application.

Affectez les services à utiliser le mode USIP et liez un moniteur de type IPTUNNEL au service pour une surveillance basée sur un tunnel.

Pour créer et configurer un service pour DSR IP sur IP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service et éventuellement créer un moniteur et le lier au service :

```
1 add service <serviceName> <serverName> <serviceType> <port> -usip <usip
     >
2
3 add monitor <monitorName> <monitorType> -destip <ip> -iptunnel <
     iptunnel>
4
5 bind service <serviceName> -monitorName <monitorName>
6 <!--NeedCopy-->
```


Exemple :

Dans l'exemple suivant, un moniteur de type IPTUNNEL est créé.

```
add monitor mon_DSR PING -destip 1.1.1.80 -iptunnel yes
add service svc_DSR01 2.2.2.100 ANY * -usip yes
bind service svc_DSR01 -monitorName mon_DSR
<!--NeedCopy-->
```

Une autre approche pour simplifier le routage au niveau du serveur et de l'appliance ADC consiste à configurer l'ADC et le serveur pour qu'ils utilisent une adresse IP provenant du même sous-réseau. Cela garantit que tout trafic ayant une destination d'un point de terminaison de tunnel est envoyé au-dessus du tunnel. Dans cet exemple, 10.0.1.0/30 est utilisé.

> **Remarque :**
>
> Le but du moniteur est de s'assurer que le tunnel est actif en atteignant le bouclage de chaque serveur via le tunnel IP. Si le service n'est pas en service, vérifiez si le routage IP externe entre ADC et le serveur est bon. Vérifiez également si les adresses IP internes sont accessibles via le tunnel IP. Des routes peuvent être requises sur le serveur, ou PBR est ajouté à ADC en fonction de l'implémentation choisie.

Exemple :

```
add ns ip 10.0.1.2 255.255.255.252 -vServer DISABLED
add netProfile netProfile_DSR -srcIP 10.0.1.2
add lb monitor mon_DSR PING -LRTM DISABLED -destIP 1.1.1.80 -ipTunnel
    YES -netProfile netProfile_DSR
<!--NeedCopy-->
```

Pour configurer un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Créez un moniteur et sélectionnez **Tunnel IP**.

Pour créer et configurer un service pour IP sur IP DSR à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Créez un service et, dans l'onglet **Paramètres**, sélectionnez **Utiliser l'adresse IP source**.

Pour lier un service à un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :


```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-DSR-1
<!--NeedCopy-->
```

Pour lier un service à un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel et cliquez dans la section **Services** pour lier un service au serveur virtuel.

Utilisation de l'adresse IP du client dans l'en-tête externe des paquets de tunnel

Citrix ADC prend en charge l'utilisation de l'adresse IP source client-source comme adresse IP source dans l'en-tête externe des paquets de tunnel liés au mode de retour direct du serveur à l'aide du tunnel IP. Cette fonctionnalité est prise en charge pour le DSR avec IPv4 et le DSR avec les modes de tunneling IPv6. Pour activer cette fonctionnalité, activez le paramètre **d'adresse IP source du client** pour IPv4 ou IPv6. Ce paramètre est appliqué globalement à toutes les configurations DSR qui utilisent le tunneling IP.

Pour utiliser une adresse IP source client-source comme adresse IP source à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set iptunnelparam -useclientsourceip [YES | NO]`
- `show iptunnelparam`

Pour utiliser l'adresse IP source du client comme adresse IP source à l'aide de l'interface graphique

1. Accédez à **Système > Réseau**.
2. Dans l'onglet **Paramètres**, cliquez sur **Paramètres globaux du tunnel IPv4**.
3. Dans la page **Configurer les paramètres globaux du tunnel IPv4**, activez la case à cocher **Utiliser l'adresse IP source client**.
4. Cliquez sur **OK**.

Pour utiliser l'adresse IP source du client comme adresse IP source à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set ip6tunnelparam -useclientsourceip [YES | NO]`
- `show ip6tunnelparam`

Pour utiliser l'adresse IP source du client comme adresse IP source à l'aide de l'interface graphique

1. Accédez à **Système > Réseau**.
2. Dans l'onglet **Paramètres**, cliquez sur **Paramètres globaux du tunnel IPv6**.
3. Dans la page **Configurer les paramètres globaux du tunnel IPv6**, activez la case à cocher **Utiliser l'adresse IP source du client**.
4. Cliquez sur **OK**.

Configuration de décapsulation

Vous pouvez configurer une appliance Citrix ADC ou un serveur principal en tant que décapsulation.

Décapsulation Citrix ADC

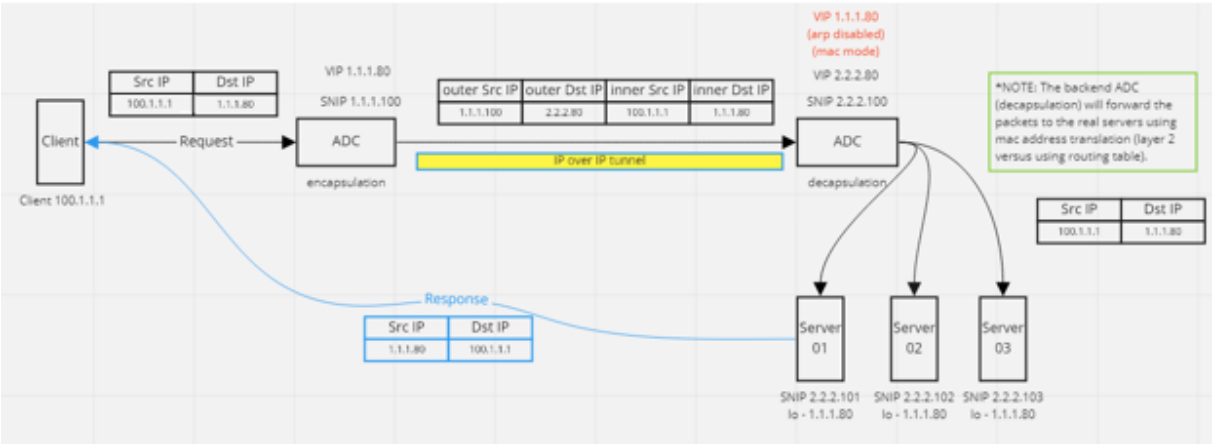
Lorsqu'une appliance Citrix ADC est utilisée comme décapsulation, un tunnel IP doit être créé dans l'appliance Citrix ADC. Pour plus de détails, voir Configuration des tunnels IP.

La configuration de la décapsulation Citrix ADC comprend les deux serveurs virtuels suivants :

- Le premier serveur virtuel reçoit le paquet encapsulé et supprime l'encapsulation IP externe.
- Le deuxième serveur virtuel dispose de l'adresse IP du service d'origine sur l'ADC frontal et utilise la traduction MAC pour transférer le paquet vers le serveur principal en utilisant l'adresse MAC des services liés. Cette configuration est généralement appelée L2DSR. Assurez-vous de désactiver ARP sur ce serveur virtuel.

Exemple de configuration :

L'illustration suivante montre une configuration de décapsulation à l'aide des appliances ADC.



La configuration complète requise pour la configuration est la suivante.

Configuration ADC frontale :

```
add service svc_DSR01 2.2.2.80 ANY * -usip YES -useproxyport NO
add lb vserver vip_DSR_ENCAP ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
    IPTUNNEL -sessionless ENABLED
bind lb vserver vip_DSR_ENCAP svc_DSR01
<!--NeedCopy-->
```

Configuration ADC back-end :

```
add ipTunnel DSR-IPIP 1.1.1.100 255.255.255.255 *

add service svc_DSR01_01 2.2.2.101 ANY * -usip YES -useproxyport NO
add service svc_DSR01_02 2.2.2.102 ANY * -usip YES -useproxyport NO
add service svc_DSR01_03 2.2.2.103 ANY * -usip YES -useproxyport NO

add lb vserver vs_DSR_DECAP ANY 2.2.2.80 * -lbMethod SOURCEIPHASH -m
    IPTUNNEL -sessionless ENABLED -netProfile netProf_DSR_MBF_noIP

add ns ip 1.1.1.80 255.255.255.255 -type VIP -arp DISABLED -snmp
    DISABLED
add lb vserver vs_DSR_Relay ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
    MAC -sessionless ENABLED

bind lb vserver vs_DSR_DECAP svc_DSR01_01
bind lb vserver vs_DSR_DECAP svc_DSR01_02
bind lb vserver vs_DSR_DECAP svc_DSR01_03

bind lb vserver vip_DSR_Relay svc_DSR01_01
bind lb vserver vip_DSR_Relay svc_DSR01_02
bind lb vserver vip_DSR_Relay svc_DSR01_03
```



```
19
20 add netProfile netProf_DSR_MBF_noIP -MBF ENABLED
21 add lb monitor mon_DSR_MAC PING -netProfile netProf_DSR_MBF_noIP
22 bind service svc_DSR01_01 -monitorName mon_DSR_MAC
23 bind service svc_DSR01_02 -monitorName mon_DSR_MAC
24 bind service svc_DSR01_03 -monitorName mon_DSR_MAC
25 <!--NeedCopy-->
```

L'exemple suivant montre une configuration de test utilisant Ubuntu et les serveurs Red Hat exécutant apache2. Ces commandes sont configurées sur chaque serveur principal.

```
1 sudo ip addr add 1.1.1.80 255.255.255.255 dev lo
2 sudo sysctl net.ipv4.conf.all.arp_ignore=1
3 sudo sysctl net.ipv4.conf.all.arp_announce=2
4 sudo sysctl net.ipv4.conf.eth4.rp_filter=2 (The interface has the
     external IP with route towards the ADC)
5 sudo sysctl net.ipv4.conf.all.forwarding=1
6 sudo ip link set dev lo arp on
7 <!--NeedCopy-->
```

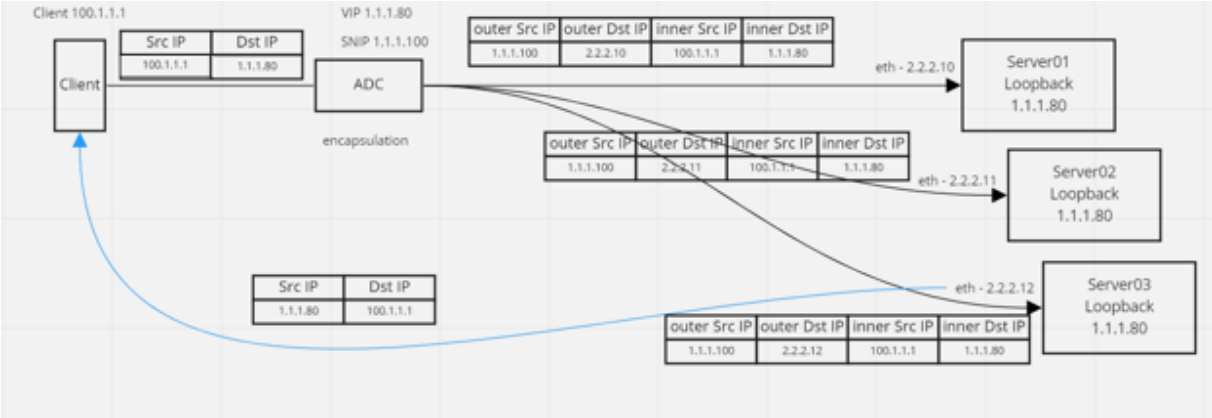
Décapsulation du serveur back-end

Lorsque vous utilisez les serveurs principaux comme décapsulation, la configuration principale varie en fonction du type de système d'exploitation du serveur. Vous pouvez configurer un serveur principal en tant que décapsulation en procédant comme suit :

1. Configurez une interface de boucle arrière avec IP pour IP de service.
2. Créez une interface de tunnel.
3. Ajouter un itinéraire via l'interface tunnel.
4. Configurez les paramètres d'interface nécessaires pour le trafic.

> Remarque :
>
> Les serveurs du système d'exploitation Windows ne peuvent pas effectuer de tunnels IP en mode natif. Les commandes sont donc fournies à titre d'exemple pour les systèmes Linux. Toutefois, les plug-ins tiers sont disponibles pour les serveurs Windows OS, ce qui ne relève pas du champ d'application de cet exemple.

L'illustration suivante montre une configuration de décapsulation à l'aide des serveurs principaux.



Exemple de configuration :

Dans cet exemple, 1.1.1.80 est l'adresse IP virtuelle (VIP) Citrix ADC et 2.2.2.10-2.2.2.12 sont les adresses IP du serveur principal. L'adresse VIP est configurée dans l'interface de bouclage et un itinéraire est ajouté via l'interface du tunnel. Les moniteurs utilisent l'adresse IP du serveur et placent les paquets du moniteur sur le tunnel IP à l'aide des points de terminaison du tunnel.

La configuration complète requise pour la configuration est la suivante.

Configuration ADC frontale :

La configuration suivante crée un moniteur qui utilise le point de terminaison du tunnel comme source. Ensuite, envoyez des pings par tunnel à l'adresse IP du service.

```
1 add ns ip 10.0.1.2 255.255.255.252 -vServer DISABLED
2 add netProfile netProfile_DSR -srcIP 10.0.1.2
3 add lb monitor mon_DSR PING -LRTM DISABLED -destIP 1.1.1.80 -ipTunnel
     YES -netProfile netProfile_DSR
4 <!--NeedCopy-->
```

La configuration suivante crée un service VIP pour service qui utilise l'adresse IP source d'origine. Ensuite, transfère le trafic via un tunnel IP vers les serveurs back-end.

```
1  add service svc_DSR01 2.2.2.10 ANY * -usip YES -useproxyport NO
2  bind service svc_DSR01 -monitorName mon_DSR
3
4  add service svc_DSR02 2.2.2.11 ANY * -usip YES -useproxyport NO
5  bind service svc_DSR02 -monitorName mon_DSR
6
7  add service svc_DSR03 2.2.2.12 ANY * -usip YES -useproxyport NO
8  bind service svc_DSR03 -monitorName mon_DSR
9
10 add lb vserver vip_DSR_ENCAP ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
     IPTUNNEL -sessionless ENABLED
11 bind lb vserver vip_DSR_ENCAP svc_DSR01
```



```
bind lb vserver vip_DSR_ENCAP svc_DSR02
bind lb vserver vip_DSR_ENCAP svc_DSR03
<!--NeedCopy-->
```

Configuration du serveur principal de chaque serveur :

Les commandes suivantes sont requises pour que le serveur principal reçoive le paquet IPIP, supprime l'encapsulation externe, puis réagisse depuis le bouclage à l'adresse IP du client d'origine. Cela garantit que les adresses IP du paquet reçu par le client correspondent aux adresses IP de la demande d'origine.

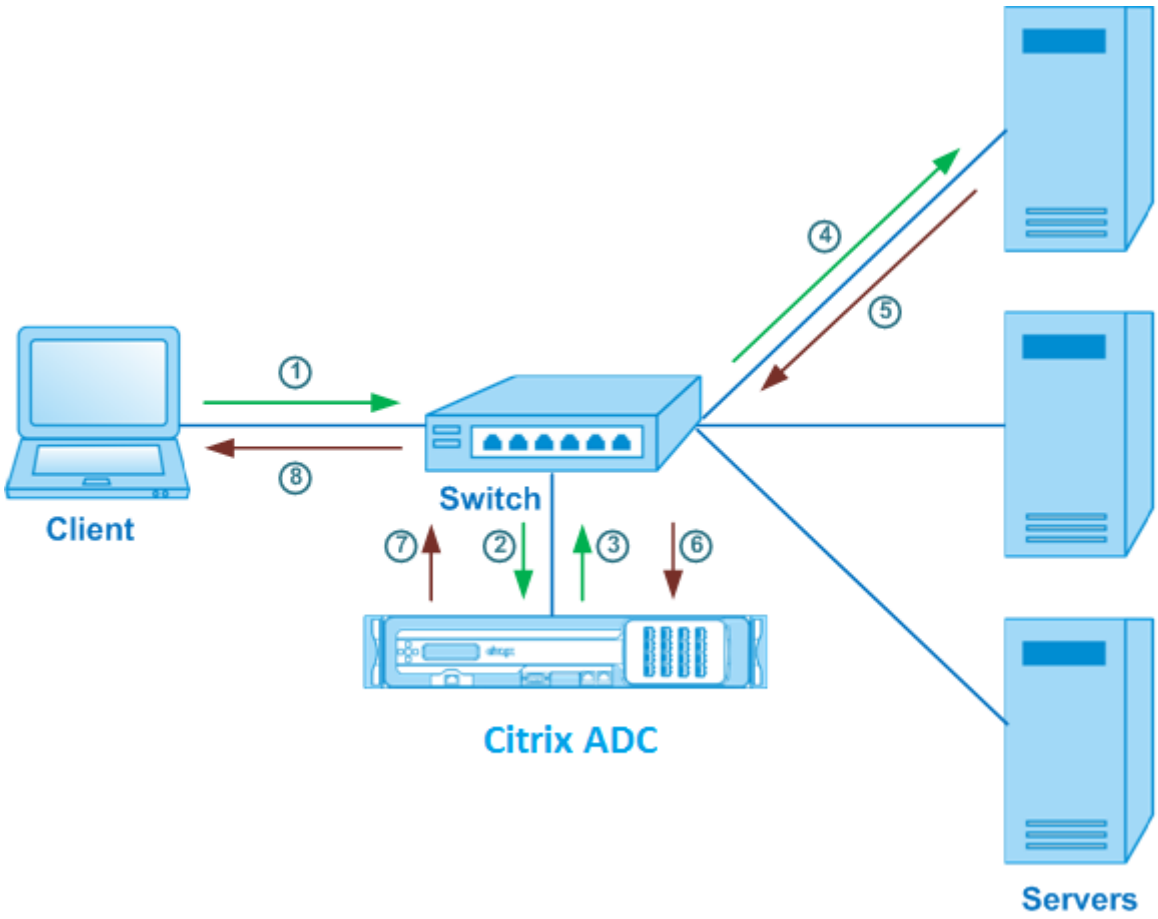
```
modprobe ipip
sudo ip addr add 1.1.1.80 255.255.255.255 dev lo
nmcli connection add type ip-tunnel ip-tunnel.mode ipip con-name tun0
ifname tun0 remote 198.51.100.5 local 203.0.113.10
nmcli connection modify tun0 ipv4.addresses '10.0.1.1/30'
nmcli connection up tun0
sudo sysctl net.ipv4.conf.all.arp_ignore=1
sudo sysctl net.ipv4.conf.all.arp_announce=2
sudo sysctl net.ipv4.conf.tun0.rp_filter=2
sudo sysctl net.ipv4.conf.all.forwarding=1
sudo ip link set dev lo arp off
<!--NeedCopy-->
```

Cas d'utilisation 8 : Configurer l'équilibrage de charge en mode à un bras

August 20, 2021

Dans une configuration à un bras, vous connectez l'appliance Citrix ADC au réseau via un seul VLAN. L'appliance reçoit la demande du client sur un seul VLAN et envoie la demande au serveur sur le même VLAN. Il s'agit de l'un des scénarios de déploiement les plus simples, où le routeur, les serveurs et l'appliance sont tous connectés au même commutateur. Les demandes des clients au niveau du commutateur sont transférées à l'appliance, qui utilise la méthode d'équilibrage de charge configurée pour sélectionner le service.

Figure 1. Équilibrage de charge en mode à bras unique



Dans l'exemple de scénario, les services Service-ANY-1, Service-ANY-2 et Service-ANY-3 sont créés et liés au serveur virtuel Vserver-LB-1. La charge du serveur virtuel équilibre la demande du client vers un service. Le tableau suivant répertorie les noms et les valeurs des entités configurées sur l'appliance en mode monobras.

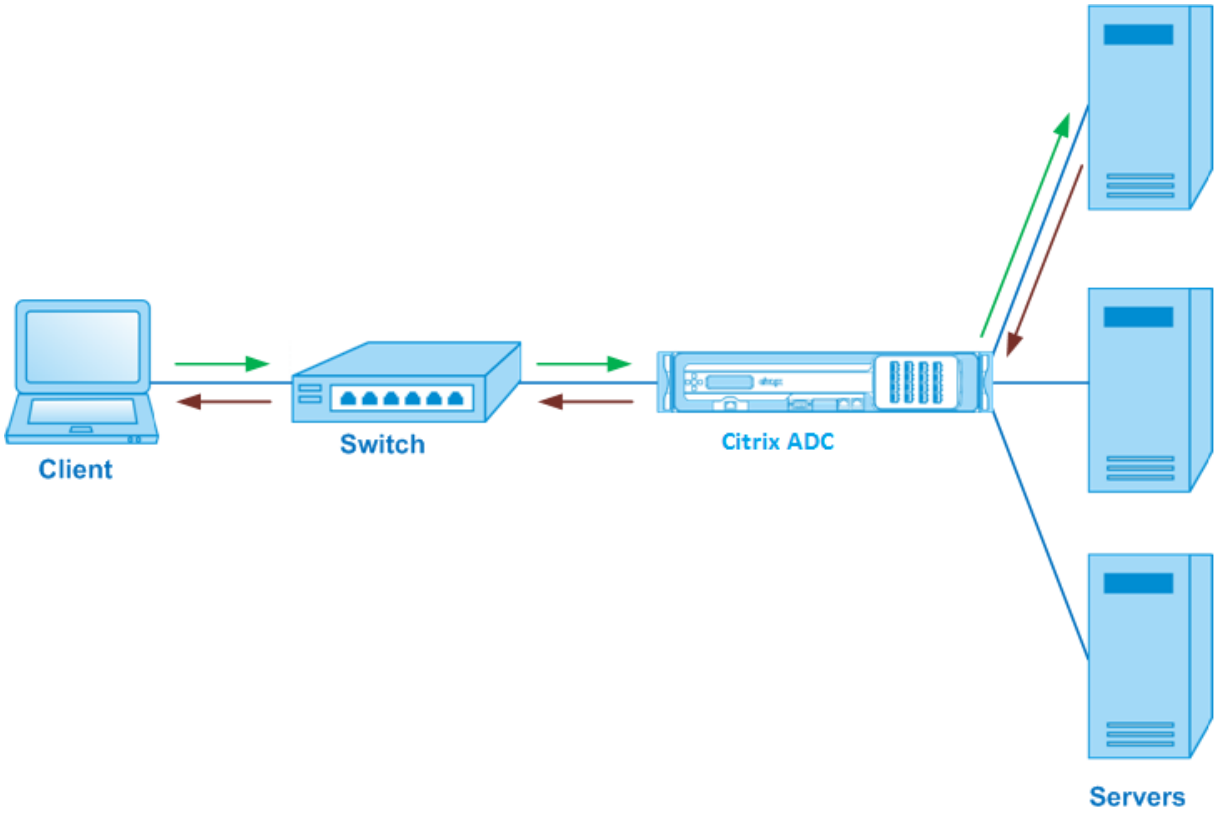
Type d'entité	Nom	Adresse IP	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.94	ANY
Services	Service-ANY-1	10.102.29.91	ANY
	Service-ANY-2	10.102.29.92	ANY
	Service-ANY-3	10.102.29.93	ANY
Moniteurs	TCP	Aucune	Aucune

Pour configurer une configuration d'équilibrage de charge en mode à bras unique, reportez-vous à la section Configuration de l'équilibrage de charge de base.

Cas d'utilisation 9 : Configurer l'équilibrage de charge en mode Inline

August 20, 2021

Dans un mode en ligne (également appelé mode à deux bras), vous connectez l'appliance Citrix ADC au réseau via plusieurs VLAN. L'appliance reçoit la demande du client sur un VLAN et envoie la demande au serveur sur un autre VLAN. Dans la configuration à deux bras, l'appliance est connectée entre les serveurs et le client. Les demandes des clients au niveau du commutateur sont transférées à l'appliance, qui utilise la méthode d'équilibrage de charge configurée pour sélectionner le service.



La configuration et le diagramme d'entités pour le mode en ligne sont les mêmes que ceux décrits dans Configuration de l'équilibrage de charge en mode à bras unique.

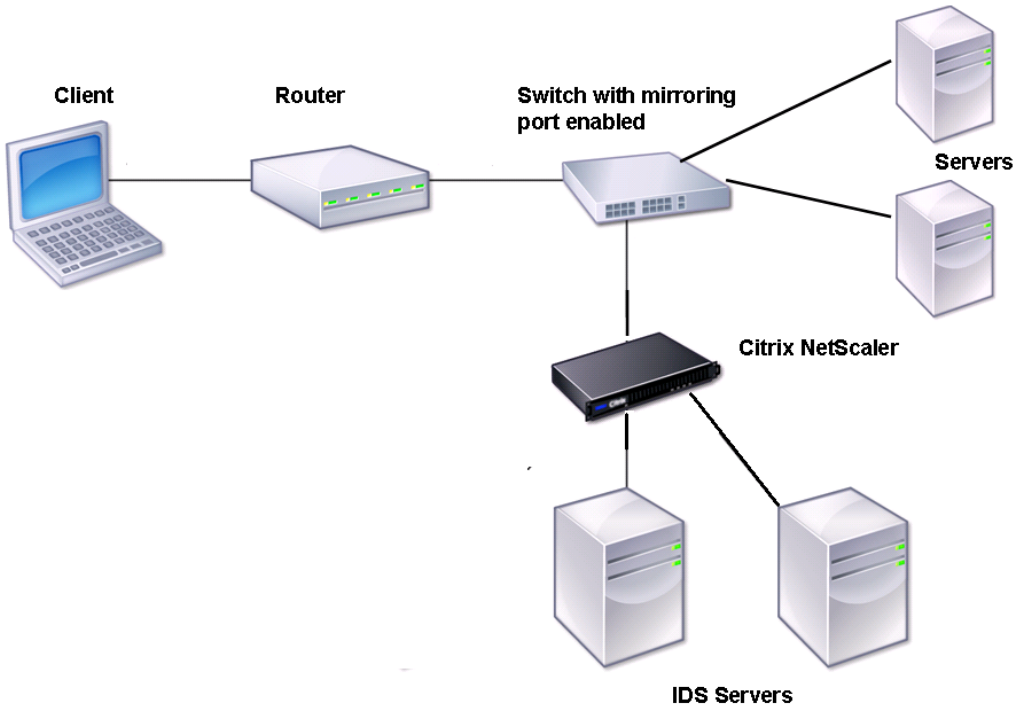
Cas d'utilisation 10 : Équilibrage de la charge des serveurs du système de détection d'intrusion

August 20, 2021

Pour permettre à l'appliance Citrix ADC de prendre en charge l'équilibrage de charge des serveurs IDS (Intrusion Detection System), les serveurs et les clients IDS doivent être connectés via un commu-

tateur dont la mise en miroir des ports est activée. Le client envoie une requête au serveur. Étant donné que la mise en miroir des ports est activée sur le commutateur, les paquets de requête sont copiés ou envoyés au port du serveur virtuel de l'appliance Citrix ADC. L'appliance utilise ensuite la méthode d'équilibrage de charge configurée pour sélectionner un serveur IDS, comme indiqué dans le diagramme suivant.

Figure 1. Topologie des serveurs IDS à charge équilibrée



Remarque : Actuellement, l'appliance prend en charge l'équilibrage de charge des périphériques IDS passifs uniquement.

Comme illustré dans le diagramme précédent, la configuration de l'équilibrage de charge IDS fonctionne comme suit :

1. La demande du client est envoyée au serveur IDS, et un commutateur doté d'un port de mise en miroir activé transfère ces paquets au serveur IDS. L'adresse IP source est l'adresse IP du client et l'adresse IP de destination est l'adresse IP du serveur. L'adresse MAC source est l'adresse MAC du routeur et l'adresse MAC de destination est l'adresse MAC du serveur.
2. Le trafic qui circule à travers le commutateur est mis en miroir vers l'appliance. L'appliance utilise les informations de couche 3 (adresse IP source et adresse IP de destination) pour transférer le paquet au serveur IDS sélectionné sans modifier l'adresse IP source ou l'adresse IP de

destination. Il modifie l'adresse MAC source et l'adresse MAC de destination à l'adresse MAC du serveur IDS sélectionné.

Remarque : lors de l'équilibrage de charge des serveurs IDS, vous pouvez configurer les méthodes d'équilibrage de charge SRCIPHASH, DESTIPHASH ou SRCIPDESTIPHASH. La méthode SRCIPDESTIPHASH est recommandée car les paquets circulant du client vers un service sur l'appliance doivent être envoyés à un seul serveur IDS.

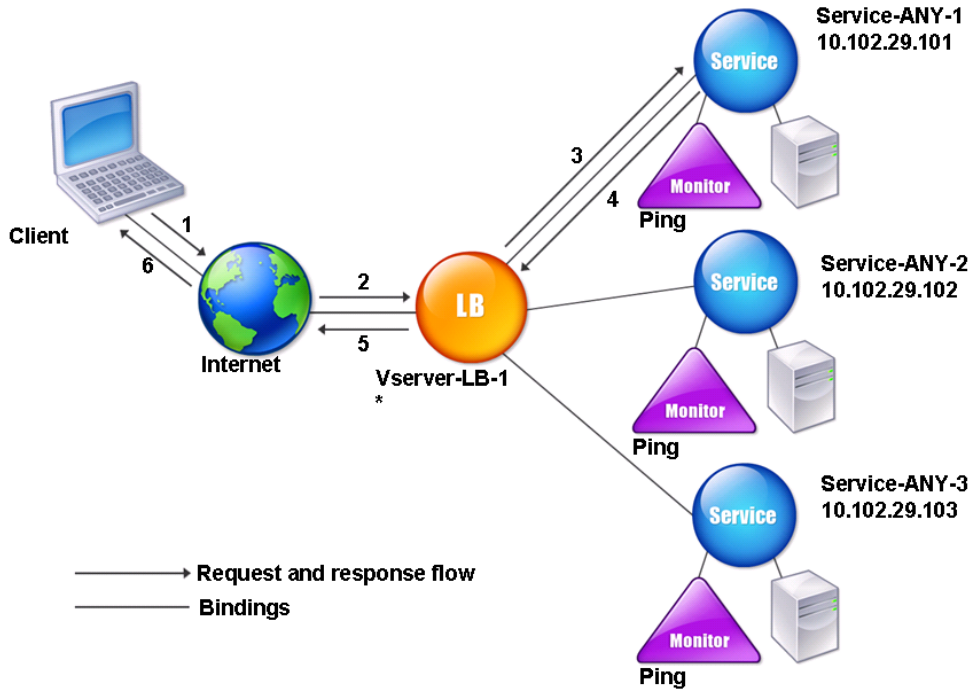
Supposons que Service-any-1, Service-any-2 et Service-any-3 soient créés et liés à vServer-lb-1. Le serveur virtuel équilibre la charge sur les services. Le tableau suivant répertorie les noms et les valeurs des entités configurées sur l'appliance.

Type d'entité	Nom	Adresse IP	Port	Protocole
Serveur virtuel	Vserver-LB-1	*	*	ANY
Services	Service-ANY-1	10.102.29.101	*	ANY
	Service-ANY-2	10.102.29.102	*	ANY
	Service-ANY-3	10.102.29.103	*	ANY
Moniteurs	Ping	Aucune	Aucune	Aucune

Remarque : Vous pouvez utiliser le mode en ligne ou le mode à un bras pour une configuration d'équilibrage de charge IDS.

Le diagramme suivant présente les entités d'équilibrage de charge et les valeurs des paramètres à configurer sur l'appliance.

Figure 2. Modèle d'entité pour les serveurs IDS d'équilibrage de charge



Pour configurer une configuration d'équilibrage de charge IDS, vous devez d'abord activer le transfert basé sur Mac. Désactivez également les modes de couche 2 et 3 sur l'appliance.

Pour activer le transfert basé sur Mac à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
enable ns mode <ConfigureMode>
<!--NeedCopy-->
```

Exemple :

```
enable ns mode MAC
<!--NeedCopy-->
```

Pour activer le transfert basé sur Mac à l'aide de l'utilitaire de configuration

Accédez à **Système > Paramètres > Configurer les modes**, puis sélectionnez **Transfert basé sur MAC**.

Ensuite, reportez-vous à la section « Configuration de l'équilibrage de chargede base » pour configurer une configuration d'équilibrage de charge de base.

Après avoir configuré la configuration d'équilibrage de charge de base, vous devez la personnaliser pour IDS en configurant une méthode d'équilibrage de charge prise en charge (telle que la méthode de hachage SRCIPDESTIP sur un serveur virtuel sans session) et en activant le mode MAC. L'appliance ne conserve pas l'état de la connexion et transfère uniquement les paquets aux serveurs IDS sans les traiter. L'adresse IP et le port de destination restent inchangés car le serveur virtuel est en mode MAC.

Pour configurer une méthode d'équilibrage de charge et un mode de redirection pour un serveur virtuel sans session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <
    RedirectionMode> -sessionless <Value>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -lbMethod SourceIPDestIPHash -m MAC -
    sessionless enabled
<!--NeedCopy-->
```

> **Remarque**
>
> Pour un service lié à un serveur virtuel sur lequel l'option -m MAC est activée, vous devez lier un moniteur non utilisateur.

Pour configurer une méthode d'équilibrage de charge et un mode de redirection pour un serveur virtuel sans session à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel et, en mode redirection, sélectionnez basé sur MAC.
3. Dans Paramètres avancés, cliquez sur Méthodes, puis sélectionnez SRCIPDESTIPHASH. Cliquez sur Paramètres de trafic, puis sélectionnez Équilibrage de charge sans session.

Pour définir un service pour utiliser l'adresse IP source à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <ServiceName> -usip <Value>
```



```
<!--NeedCopy-->
```

Exemple :

```
set service Service-ANY-1 -usip yes
<!--NeedCopy-->
```

Pour définir un service pour utiliser l'adresse IP source à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Ouvrez un service et, dans Paramètres, sélectionnez **Utiliser l'adresse IP source**.

Pour que USIP fonctionne correctement, vous devez le définir globalement. Pour plus d'informations sur la configuration globale d'USIP, consultez Addressage IP.

Cas d'utilisation 11 : Isolation du trafic réseau à l'aide de stratégies d'écoute

August 20, 2021

> **Remarque**
>
> La solution d'isolation du trafic utilisant des serveurs virtuels clichés pour simuler l'isolement multilocataire n'est plus recommandée. Citrix vous recommande également d'utiliser la fonctionnalité Citrix ADC Admin Partitioning pour de tels déploiements. Pour plus d'informations, voir Partitionnement administrateur.

Une exigence de sécurité courante dans un centre de données consiste à maintenir l'isolement du chemin réseau entre le trafic de diverses applications ou locataires. Le trafic d'une application ou d'un locataire doit être isolé du trafic d'autres applications ou locataires. Par exemple, une société de services financiers voudrait garder le trafic des applications de son service d'assurance distinct de celui de ses applications de services financiers. Par le passé, cela a été facilement réalisé grâce à la séparation physique des périphériques de service réseau tels que les pare-feu, les équilibreurs de charge et les IdP, ainsi qu'à la surveillance du réseau et à la séparation logique dans la structure de commutation.

À mesure que les architectures de datacenter évoluent vers des datacenters virtualisés multilocataires, les services de mise en réseau dans la couche d'agrégation d'un datacenter sont consolidés. Ce développement a fait de l'isolation des chemins de réseau un composant essentiel pour les périphériques de service réseau et conduit à la nécessité pour les ADC de pouvoir isoler le trafic aux

niveaux L4 à L7. En outre, tout le trafic d'un locataire particulier doit passer par un pare-feu avant d'atteindre la couche de service.

Pour répondre à la nécessité d'isoler les chemins réseau, une appliance Citrix ADC identifie les domaines réseau et contrôle le trafic entre les domaines. La solution Citrix ADC comporte deux composants principaux : les stratégies d'écoute et les serveurs virtuels instantanés.

Chaque chemin réseau à isoler se voit attribuer un serveur virtuel sur lequel une stratégie d'écoute est définie afin que le serveur virtuel écoute uniquement le trafic à partir d'un domaine réseau spécifié.

Pour isoler le trafic, les stratégies d'écoute peuvent être basées sur plusieurs paramètres client ou leurs combinaisons, et les stratégies peuvent se voir attribuer des priorités. Le tableau suivant répertorie les paramètres qui peuvent être utilisés dans les stratégies d'écoute pour identifier le trafic.

Catégorie	Paramètres
Protocole Ethernet	Adresse MAC source, adresse MAC de destination
Interface réseau	ID réseau, débit de réception, débit d'envoi, débit de transmission
Protocole IP	Adresse IP source, adresse IP de destination
Protocole IPv6	Adresse IPv6 source, adresse IPv6 de destination
Protocole TCP	Port source, port de destination, taille maximale du segment, charge utile et autres options
Protocole UDP	Port source, port de destination
VLAN	ID

Tableau 1. Paramètres client utilisés pour définir des stratégies d'écoute

Sur l'appliance Citrix ADC, un serveur virtuel est configuré pour chaque domaine, avec une stratégie d'écoute spécifiant que le serveur virtuel doit écouter uniquement le trafic de ce domaine. Un serveur virtuel d'équilibrage de charge instantanée est également configuré pour chaque domaine, qui écoute le trafic destiné à n'importe quel domaine. Chacun des serveurs virtuels d'équilibrage de charge instantanée a une adresse IP et un port génériques (*), et son type de service est défini sur ANY.

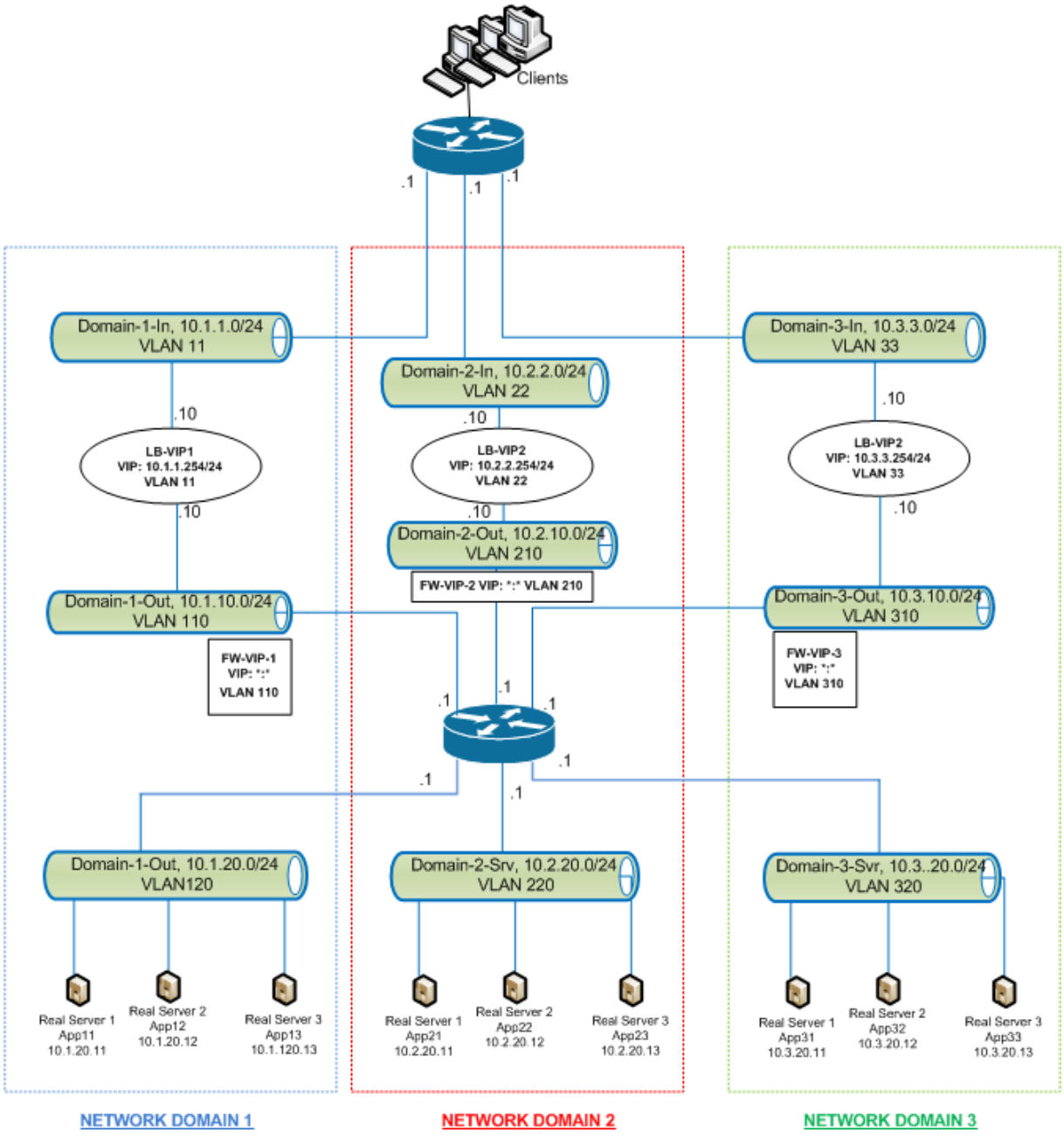
Dans chaque domaine, un pare-feu pour le domaine est lié en tant que service au serveur virtuel d'équilibrage de charge instantanée, qui transfère tout le trafic via le pare-feu. Le trafic local est transféré vers sa destination et le trafic destiné à un autre domaine est transféré vers le pare-feu de ce domaine. Les serveurs virtuels d'équilibrage de charge instantanée sont configurés pour la redirection

en mode MAC.

Comment les chemins réseau sont isolés

La figure suivante montre un flux de trafic typique entre les domaines. Tenez compte du flux de trafic dans le domaine réseau 1 et entre le domaine réseau 1 et le domaine réseau 2.

Figure 1. Isolation du chemin d'accès réseau



Trafic au sein du domaine réseau 1

Le domaine réseau 1 comporte trois VLAN : VLAN 11, VLAN110 et VLAN120. Les étapes suivantes décrivent le flux de trafic.

- Un client de VLAN 11 envoie une demande pour un service disponible à partir du pool de services dans VLAN 120.
- Le serveur virtuel d'équilibrage de charge LB-VIP1, qui est configuré pour écouter le trafic du VLAN 11, reçoit la demande et transmet la demande au VLAN 110. Le serveur virtuel du VLAN 110 transmet la demande au serveur virtuel d'équilibrage de charge instantanée FW-VIP-1.
- FW-VIP-1, qui est configuré pour écouter le trafic à partir du VLAN 110, reçoit la demande et la transmet au VLAN 120.
- Le serveur virtuel d'équilibrage de charge dans VLAN 120 équilibre la charge de la demande à l'un des serveurs physiques, App11, App12 ou App13.
- La réponse envoyée par le serveur physique renvoie par le même chemin d'accès au client dans VLAN 11.

Cette configuration garantit que le trafic est toujours séparé à l'intérieur de Citrix ADC pour tout le trafic provenant d'un client.

Trafic entre le domaine réseau 1 et le domaine réseau 2

Le domaine réseau 1 comporte trois VLAN : VLAN 11, VLAN110 et VLAN120. Le domaine réseau 2 dispose également de trois VLAN : VLAN 22, VLAN 210 et VLAN 220. Les étapes suivantes décrivent le flux de trafic entre VALN 11 et VLAN 22.

- Un client de VLAN 11, qui appartient au domaine réseau 1, envoie une demande pour un service disponible à partir du pool de services dans VLAN 220, qui appartient au domaine réseau 2.
- Dans le domaine réseau 1, le serveur virtuel d'équilibrage de charge LB-VIP1, qui est configuré pour écouter le trafic du VLAN 11, reçoit la demande et transmet la demande au VLAN 110.
- Le serveur virtuel d'équilibrage de charge instantanée FW-VIP-1, qui est configuré pour écouter le trafic VLAN 110 destiné à tout autre domaine, reçoit la demande et la transmet au serveur virtuel FW-VIP-2 de pare-feu car la demande est destinée à un serveur physique dans le domaine réseau 2.
- Dans le domaine réseau 2, FW-VIP-2 transmet la demande au VLAN 220.
- Le serveur virtuel d'équilibrage de charge dans VLAN 220 équilibre la charge de la demande à l'un des serveurs physiques, App21, App22 ou App23.
- La réponse envoyée par le serveur physique renvoie par le même chemin d'accès via le pare-feu dans le domaine réseau 2, puis vers le domaine réseau 1 pour atteindre le client dans VLAN 11.

Étapes de configuration

Pour configurer l'isolement de chemin réseau à l'aide de stratégies d'écoute, procédez comme suit :

- Ajouter des expressions de stratégie d'écoute. Chaque expression spécifie un domaine auquel le trafic est destiné. Vous pouvez utiliser l'ID VLAN ou d'autres paramètres pour identifier le trafic.
- Pour chaque domaine réseau, configurez deux serveurs virtuels comme suit :
  - Créez un serveur virtuel d'équilibrage de charge pour lequel vous spécifiez une stratégie d'écoute qui identifie le trafic destiné à ce domaine. Vous pouvez spécifier le nom d'une expression créée précédemment ou vous pouvez créer une expression lors de la création du serveur virtuel.
  - Créez un autre serveur virtuel d'équilibrage de charge, appelé serveur virtuel instantané, pour lequel vous spécifiez une expression de stratégie d'écoute qui s'applique au trafic destiné à n'importe quel domaine. Sur ce serveur virtuel, définissez le type de service sur ANY et l'adresse IP et le port sur un astérisque (*). Activez le transfert basé sur Mac sur ce serveur virtuel.
  - Activez l'option Connexion L2 sur les deux serveurs virtuels.
    En règle générale, pour identifier une connexion, l'appliance Citrix ADC utilise le 4-tuple de l'adresse IP du client, du port client, de l'adresse IP de destination et du port de destination. Lorsque vous activez l'option Connexion L2, les paramètres de couche 2 de la connexion (numéro de canal, adresse MAC et ID VLAN) sont utilisés en plus du 4-tuple normal.
- Ajoutez des services représentant les pools de serveurs dans le domaine et liez-les au serveur virtuel.
- Configurez le pare-feu pour chaque domaine en tant que service et liez tous les services de pare-feu au serveur virtuel Shadow.

Pour isoler le trafic réseau à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
1 add policy expression <expressionName> <listenPolicyExpression>
2
3 add lb vserver <name> <serviceType> <ip> <port> -l2conn ON -
     listenPolicy <expressionName>
4 <!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge pour chaque domaine. Ce serveur virtuel est destiné au trafic du même domaine.

```
1 add lb vserver <name> ANY * * -l2conn ON -m MAC -listenPolicy <
     expressionName>
```



```
<!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge instantanée pour chaque domaine. Ce serveur virtuel est destiné au trafic d'autres domaines.

Exemple :

```
add policy expression e110 client.vlan.id==110
add policy expression e210 client.vlan.id==210
add policy expression e310 client.vlan.id==310
add policy expression e11 client.vlan.id==11
add policy expression e22 client.vlan.id==22
add policy expression e33 client.vlan.id==33

add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -persistenceType NONE -
    listenPolicy e11
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP2 HTTP 10.2.2.254 80 -persistenceType NONE -
    listenPolicy e22
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP3 HTTP 10.3.3.254 80 -persistenceType NONE -
    listenPolicy e33
-cltTimeout 180 -l2Conn ON


add lb vserver FW-VIP-1 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e110 -Listenpriority 1 -m MAC -cltTimeout
    120

add lb vserver FW-VIP-2 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e210 -Listenpriority 2 -m MAC -cltTimeout
    120

add lb vserver FW-VIP-3 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e310 -Listenpriority 3 -m MAC -cltTimeout
    120


add service RD-1 10.1.1.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO

```



```
28 add service RD-2 10.2.2.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
      DISABLED
29 -usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
      NO -TCPB NO -CMP NO
30
31 add service RD-3 10.3.3.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
      DISABLED
32 -usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
      NO -TCPB NO -CMP NO
33
34
35 bind lb vserver FW-VIP-1 RD-1
36
37 bind lb vserver FW-VIP-2 RD-2
38
39 bind lb vserver FW-VIP-3 RD-3
40 <!--NeedCopy-->
```

Pour isoler le trafic réseau à l'aide de l'utilitaire de configuration

1. Ajoutez des services représentant les serveurs, comme décrit dans la section Création d'un service.
2. Ajoutez chaque pare-feu en tant que service :
   a) Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
   b) Créez un service en spécifiant le protocole ANY, le serveur comme adresse IP du pare-feu et le port 80.
3. Configurez un serveur virtuel d'équilibrage de charge.
4. Configurez le serveur virtuel d'équilibrage de charge instantanée.
5. Pour chaque domaine réseau, répétez les étapes 3 et 4.
6. Dans le volet Serveurs virtuels d'équilibrage de charge, ouvrez les serveurs virtuels que vous avez créés et vérifiez les paramètres.

Cas d'utilisation 12 : Configurer XenDesktop pour l'équilibrage de charge

August 20, 2021

Pour améliorer les performances de livraison des applications de bureau virtuel, vous pouvez intégrer l'appliance Citrix ADC avec Citrix XenDesktop et utiliser la fonctionnalité d'équilibrage de charge Citrix

ADC pour répartir la charge entre les serveurs d'interface Web et les serveurs DDC (Desktop Delivery Controller).

Généralement, vous utilisez XenDesktop dans des situations où les applications ne sont pas compatibles avec l'exécution sur un serveur Terminal Server ou XenApp, ou si chaque bureau virtuel a des exigences uniques. Dans de tels cas, vous avez besoin d'un hôte de bureau pour chaque utilisateur qui se connecte. Toutefois, les hôtes peuvent être regroupés de sorte que vous n'avez besoin que d'un seul hôte pour chaque utilisateur actuellement connecté.

Le service d'application principal déployé pour XenDesktop est Desktop Delivery Controller (DDC). La DDC est installée sur un serveur, et sa fonction principale est d'enregistrer les hôtes de bureau et de courtier les connexions client à eux.

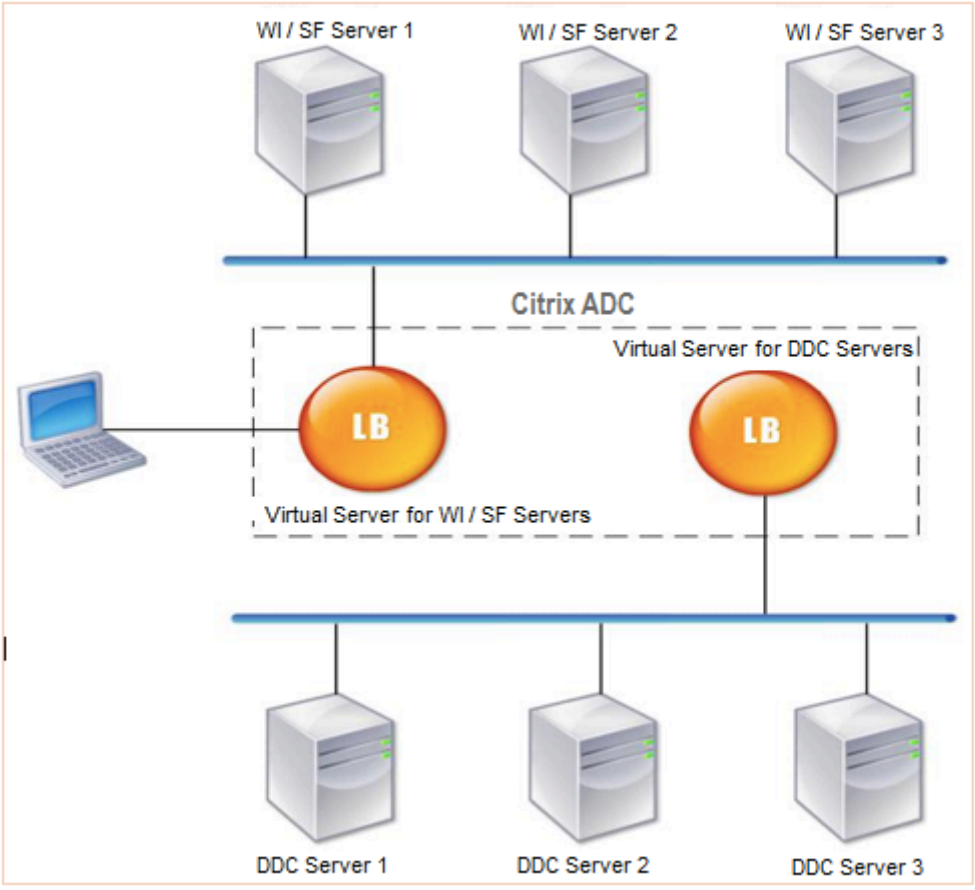
La DDC authentifie également les utilisateurs et gère l'assemblage des environnements de bureau virtuel des utilisateurs en contrôlant l'état des postes de travail, en démarrant et en arrêtant les postes de travail.

En général, plusieurs DDC sont installés pour améliorer la disponibilité.

Les serveurs d'interface Web fournissent un accès sécurisé aux bureaux virtuels. L'interface Web est le portail de connexion initial au Desktop Delivery Controller (DDC). Le navigateur Web sur le périphérique de l'utilisateur envoie des informations au serveur Web, qui communique avec la batterie de serveurs pour lui permettre d'accéder au bureau virtuel.

La figure suivante illustre la topologie d'un dispositif Citrix ADC fonctionnant avec XenDesktop.

Figure 1. Équilibrage de charge de XenDesktop



> **Remarque**
>
> Bien que vous puissiez utiliser le protocole HTTP, Citrix vous recommande d'utiliser SSL pour la communication entre le client et l'appliance Citrix ADC. Vous pouvez utiliser le protocole HTTP pour la communication entre le Citrix ADC et les serveurs DDC même si vous utilisez le protocole SSL pour la communication avec le client.

Pour configurer l'équilibrage de charge pour XenDesktop à l'aide de l'interface graphique

1. Créez un service.
   a) Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
   b) Créez un service en spécifiant un nom, une adresse IP, un port et un type de protocole, puis cliquez sur **OK**.
2. Créez un serveur virtuel d'équilibrage de charge.
   a) Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis cliquez sur **Ajouter**.

b) Créez un serveur virtuel en spécifiant un nom, une adresse IP, un port et un type de protocole, puis cliquez sur **OK**.

3. Liez le service au serveur virtuel d'équilibrage de charge.
4. Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et sélectionnez un serveur.
   a) Cliquez sur **Modifier**.
   b) Dans les **Services et groupes de services**, cliquez sur **>**et cliquez sur **Ajouter une liaison**.
   c) Sélectionnez le service que vous souhaitez lier et entrez la valeur de pondération.
   d) Cliquez sur **Bind**.

Pour configurer l'équilibrage de charge pour XenDesktop à l'aide de l'interface de ligne de commande

- Pour créer un service, à l'invite de commandes, tapez :

```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

- Pour créer un serveur virtuel, à l'invite de commandes, tapez :

```
add lb vserver <name> <serviceType> <ip> <port>
<!--NeedCopy-->
```

Exemple :

add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80

- Pour lier un service à un serveur virtuel d'équilibrage de charge, à l'invite de commandes, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

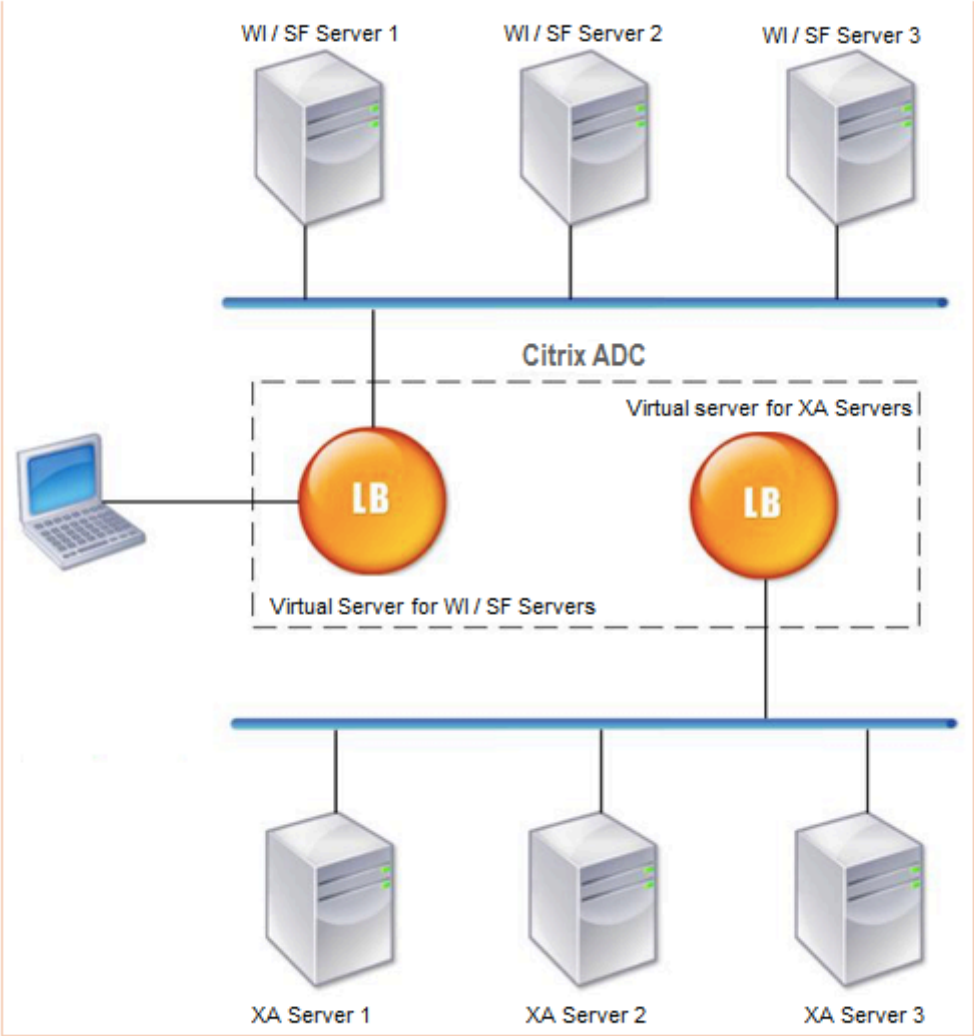
```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```


Cas d'utilisation 13 : Configurer XenApp pour l'équilibrage de charge

August 20, 2021

Pour une livraison efficace des applications, vous pouvez intégrer l'appliance Citrix ADC avec Citrix XenApp et utiliser la fonctionnalité d'équilibrage de charge Citrix ADC pour répartir la charge entre les batteries de serveurs XenApp. La figure suivante est un diagramme topologique d'une telle configuration.

Figure 1. Équilibrage de charge de XenApp



Les serveurs d'interface Web fournissent un accès sécurisé aux ressources d'application XenApp via le navigateur Web de l'utilisateur. Le client d'interface Web présente aux utilisateurs toutes les ressources, telles que les applications, le contenu et les postes de travail disponibles dans les

batteries de serveurs XenApp. Les utilisateurs peuvent accéder aux ressources publiées via un navigateur Web standard ou via le plug-in en ligne Citrix.

Le navigateur Web sur le périphérique de l'utilisateur envoie des informations au serveur Web, qui communique avec les serveurs de la batterie de serveurs pour lui permettre d'accéder aux ressources.

L'interface Web et le courtier XML sont des services complémentaires. L'interface Web permet aux utilisateurs d'accéder aux applications et XML Broker évalue les autorisations de l'utilisateur pour déterminer quelles applications apparaissent dans l'interface Web.

Le service XML est installé sur tous les serveurs de la batterie de serveurs. Le service XML spécifié dans l'interface Web fonctionne en tant que courtier XML. Sur la base des informations d'identification de l'utilisateur transmises par le serveur d'interface Web, le serveur XML Broker envoie une liste d'applications accessibles à l'utilisateur.

Dans les grandes entreprises où plusieurs serveurs d'interface Web et des serveurs XML Broker sont déployés, Citrix recommande d'équilibrer la charge de ces serveurs à l'aide de l'appliance Citrix ADC. Configurez un serveur virtuel pour équilibrer la charge des serveurs de l'interface Web et un autre pour les serveurs XML Broker. La méthode d'équilibrage de charge et d'autres fonctionnalités peuvent être configurées sur le serveur virtuel si nécessaire.

> **Remarque**
>
> Bien que vous puissiez utiliser le protocole HTTP, Citrix vous recommande d'utiliser SSL pour la communication entre le client et Citrix ADC. Vous pouvez utiliser le protocole HTTP pour la communication entre le Citrix ADC et les serveurs WI même si vous utilisez le protocole SSL pour la communication avec le client.

Pour configurer l'équilibrage de charge pour XenApp à l'aide de l'interface graphique

1. Créez un service.
   a) Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
   b) Créez un service en spécifiant un nom, une adresse IP, un port et un type de protocole, puis cliquez sur **OK**.
2. Créez un serveur virtuel d'équilibrage de charge.
   a) Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis cliquez sur **Ajouter**.
   b) Créez un serveur virtuel en spécifiant un nom, une adresse IP, un port et un type de protocole, puis cliquez sur **OK**.
3. Liez le service au serveur virtuel d'équilibrage de charge.
4. Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et sélectionnez un serveur.
   a) Cliquez sur **Modifier**.

b) Dans les **Services et groupes de services**, cliquez sur **>**et cliquez sur **Ajouter une liaison**.
c) Sélectionnez le service que vous souhaitez lier et entrez la valeur de pondération.
d) Cliquez sur **Bind**.

Pour configurer l'équilibrage de charge pour XenApp à l'aide de l'interface de ligne de commande

- Pour créer un service, à l'invite de commandes, tapez :

```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

- Pour créer un serveur virtuel, à l'invite de commandes, tapez :

```
add lb vserver <name> <serviceType> <ip> <port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

- Pour lier un service à un serveur virtuel d'équilibrage de charge, à l'invite de commandes, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

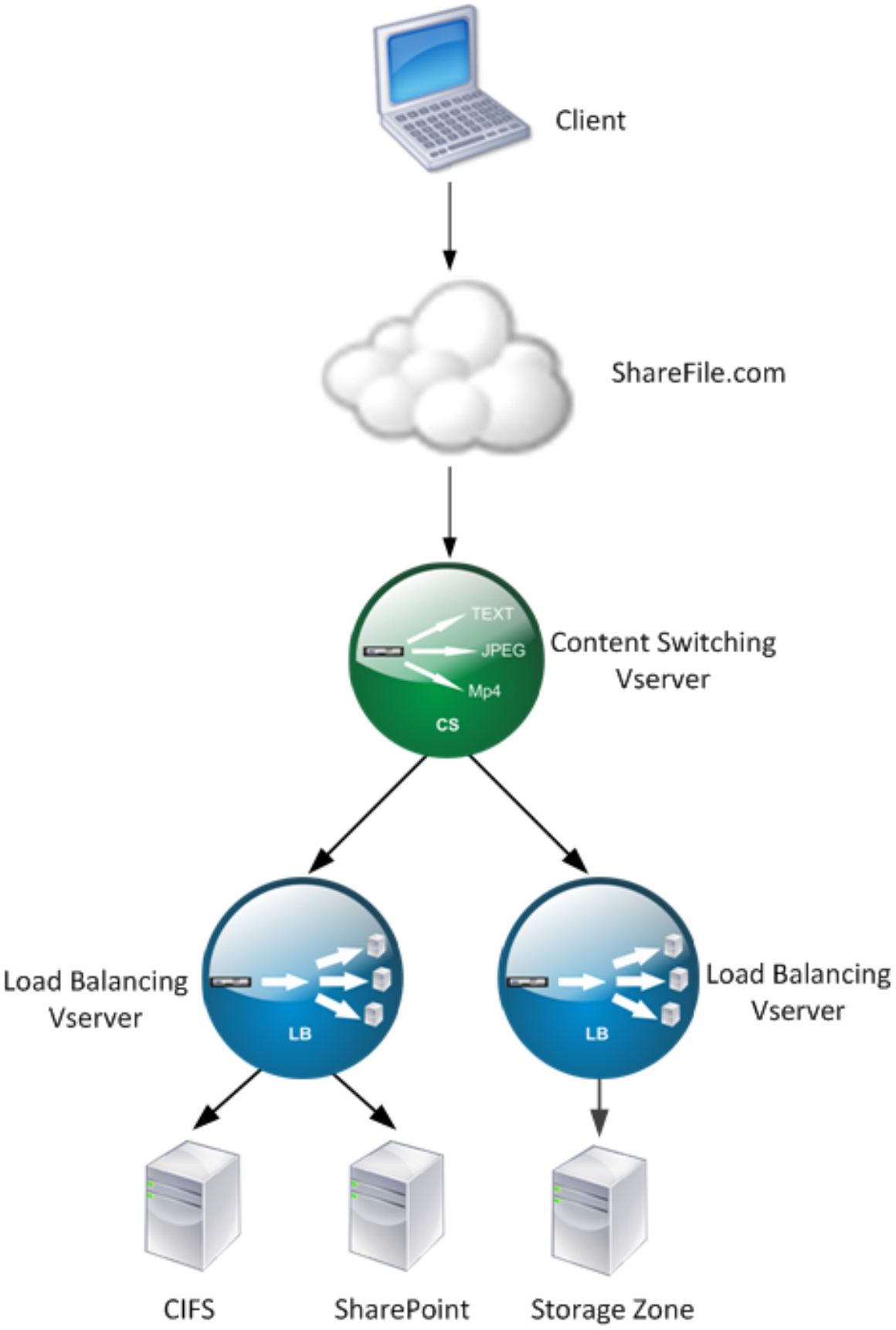
Cas d'utilisation 14 : Assistant ShareFile pour l'équilibrage de charge Citrix ShareFile

August 20, 2021

Vous pouvez configurer l'équilibrage de charge pour Citrix ShareFile à l'aide de l'Assistant. L'assistant Citrix ShareFile aide à configurer la configuration d'équilibrage de charge pour le site ShareFile en fonction du type de contenu demandé. Le serveur de commutation de contenu dirige la demande selon qu'il s'agit d'une requête StorageZone, CIFS ou SharePoint. Le changement de contenu est basé sur des stratégies. L'Assistant génère automatiquement les stratégies pour identifier si la demande concerne StorageZone, CIFS ou SharePoint. Le serveur virtuel de commutation de contenu utilise ces stratégies pour diriger la demande vers le serveur d'équilibrage de charge correct.

Un flux de données typique peut être représenté comme illustré dans le diagramme suivant.

Figure 1. Équilibrage de la charge des données ShareFile

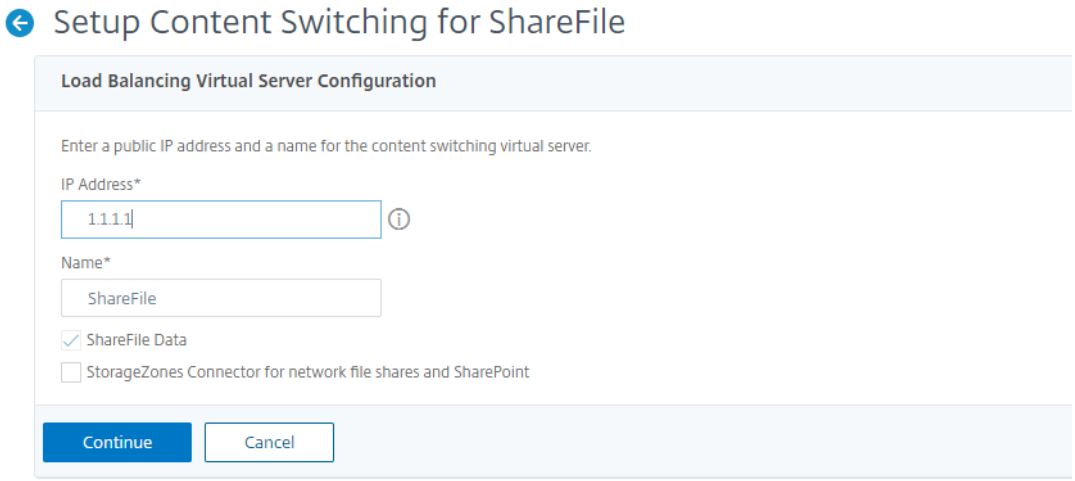


Vous pouvez afficher les serveurs virtuels d'équilibrage de charge créés par l'assistant ShareFile en accédant à **Gestion du trafic > Serveurs virtuels** et **services > Serveurs virtuels**. Vous ne pouvez pas supprimer manuellement les serveurs virtuels créés à l'aide de l'Assistant ShareFile. Utilisez l'Assistant pour supprimer les serveurs virtuels.

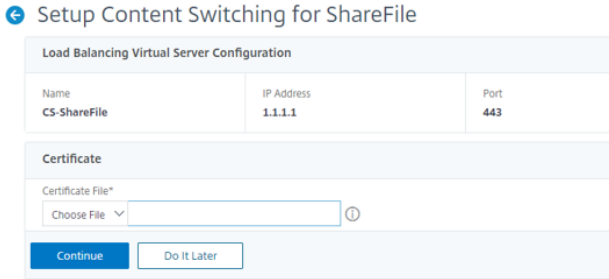
Citrix ADC utilise l'authentification LDAP pour la demande SharePoint ou CIFS. L'authentification par hachage est utilisée pour authentifier les demandes de StorageZones.

Pour configurer un dispositif Citrix ADC pour l'équilibrage de charge Citrix ShareFile

1. Dans le volet de navigation, cliquez sur **Gestion du trafic**.
2. Sous **Citrix ShareFile** section, cliquez sur **Configurer Citrix ADC pour ShareFile**.
3. Sur la page **Setup Content Switching for ShareFile**, fournissez les informations suivantes :
   - Adresse IP : adresse IP du serveur virtuel de commutation de contenu.
   - Nom : Nom du serveur virtuel de commutation de contenu.
   - Si vous souhaitez configurer l'équilibrage de charge pour CIFS ou SharePoint, activez la case à cocher **StorageZone Connector for Network File Share/SharePoint**, puis cliquez sur **Continuer**. Par défaut, la case à cocher **ShareFile Data** est activée.



4. Fournir un certificat valide. Si vous possédez un certificat, cliquez sur **Choisir un certificat** et sélectionnez le certificat dans la liste déroulante. Si vous devez installer un certificat, cliquez sur **Installer le certificat** et fournissez la paire Certificat-clé.

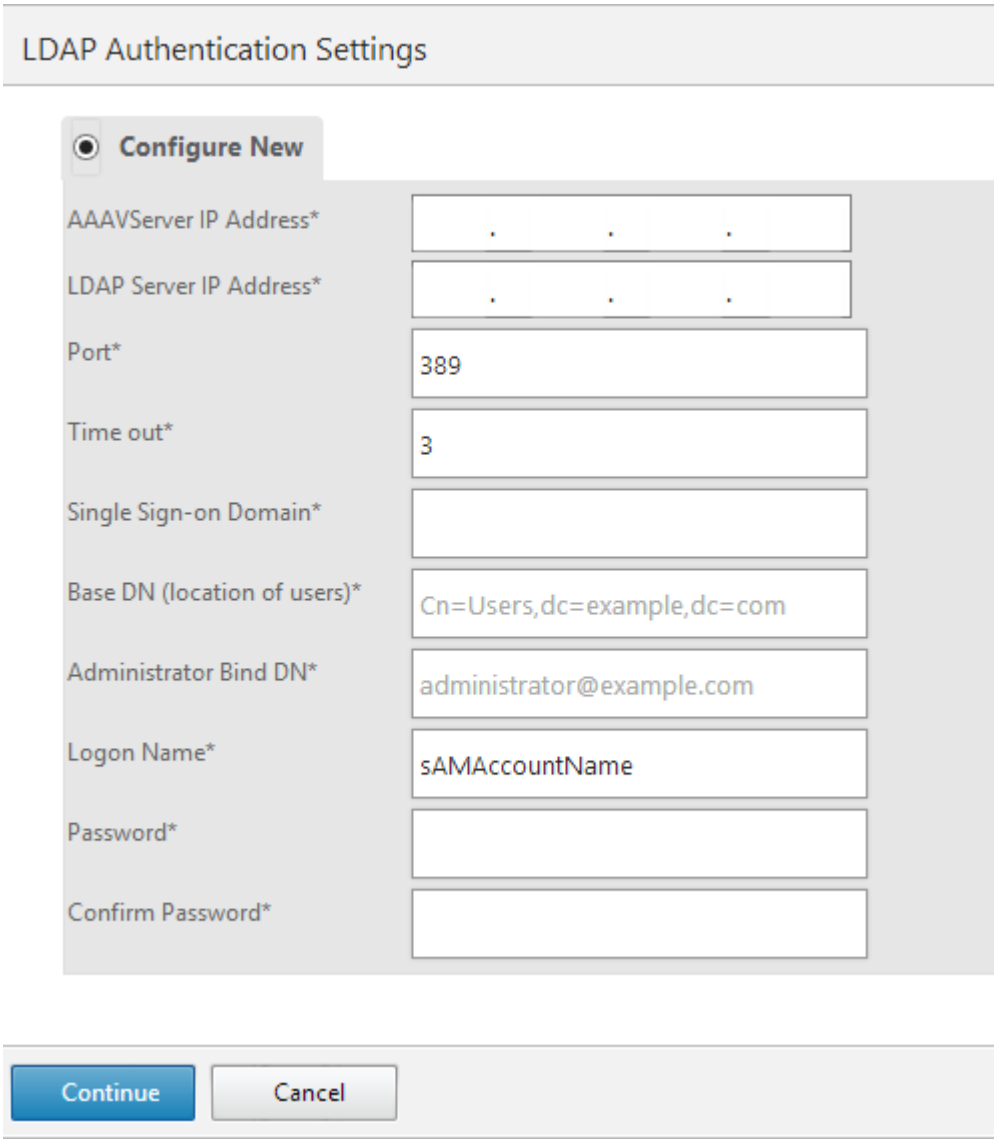


5. Cliquez sur **Continuer**.
6. Dans la boîte de dialogue **Ajouter un nouveau contrôleur StorageZone**, spécifiez les valeurs

des paramètres suivants :

- Adresse IP du contrôleur StorageZone : adresse IP
- Port—Numéro de port. La valeur par défaut est 443.
- Protocole : sélectionnez la

7. Cliquez sur **Créer**, puis sur **Terminé**. L'Assistant crée automatiquement un service et génère automatiquement le nom du service.
8. Si vous avez choisi l'équilibrage de charge pour CIFS ou SharePoint à l'étape 4.c, spécifiez les valeurs des paramètres d'authentification LDAP :
   - Adresse IP du serveur virtuel Citrix ADC AAA : adresse IP du serveur virtuel Citrix ADC AAA
   - Adresse IP du serveur LDAP : adresse IP du serveur LDAP
   - Port—Numéro de port. La valeur par défaut est 389
   - Timeout : valeur du délai d'attente en minutes
   - Domaine d'authentification unique : nom de domaine d'authentification unique
   - DN de base : nom de domaine de base
   - Administrator Bind DN : nom de compte LDAP avec le nom de domaine, par exemple, administrator@domainname.com
   - Nom d'ouverture de session : le nom d'ouverture de session est le nom SamAccountName
   - Mot de passe et confirmation du mot de passe : entrez le mot de passe et confirmez



9. Cliquez sur **Continuer**, puis sur **Terminé**.

Pour supprimer la configuration d'équilibrage de charge pour ShareFile

1. Dans le volet de navigation, cliquez sur **Gestion du trafic**.
2. Sous **Citrix ShareFile** section, cliquez sur **Supprimer la configuration ShareFile**.

Cas d'utilisation 15 : configurer l'équilibrage de charge de couche 4 sur l'appliance Citrix ADC

October 5, 2021

L'équilibreur de charge de couche 4 (ports TCP et UDP) utilise les informations fournies dans la couche de transport réseau pour acheminer les demandes des clients entre les groupes de serveurs.

Lorsqu'une connexion de couche 4 est établie entre un client et un serveur, elle dispose d'une vue par paquets du trafic échangé entre eux. L'équilibreur de charge de couche 4 prend ses décisions de routage en fonction des informations d'adresse extraites des premiers paquets du flux TCP, et n'inspecte pas le contenu des paquets. Par conséquent, l'équilibrage de charge de la couche 4 est également appelé équilibrage de charge basé sur la connexion.

L'équilibreur de charge de couche 4 surveille la santé d'un serveur. Le trafic n'est pas acheminé vers le serveur s'il est en panne.

L'équilibrage de charge de couche 4 est utile pour diverses applications utilisant des charges utiles TCP ou UDP. De tels protocoles échangent des données sous forme de charge utile TCP et n'ont pas de structure spécifique à suivre.

Pour configurer l'équilibrage de charge de la couche 4 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

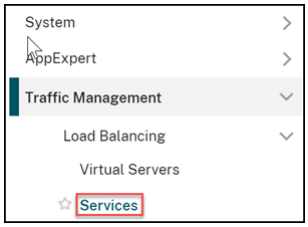
```
add service <name> <serverName> <serviceType> <port>
add lb vserver <name> <serviceType> <ip> <port>
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
add service TCPservice 192.0.2.3 TCP 1
add lb vserver TCPserver TCP 192.0.2.4 1
bind lb vserver TCPserver TCPservice
<!--NeedCopy-->
```

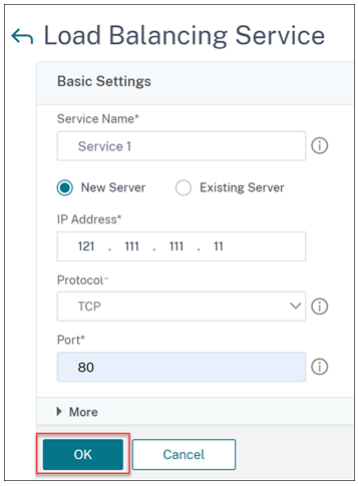
Pour configurer l'équilibrage de charge de la couche 4 à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Services**.



2. Cliquez sur **Ajouter** pour créer un service.

3. Spécifiez les détails requis dans **Nom du service** et **adresse IP**.
4. Sélectionnez **TCP** ou **UDP** dans **Protocol**.
5. Cliquez sur **OK**.



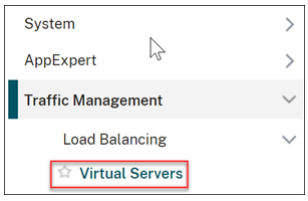
6. Cliquez sur **Terminé**.

   Un service est créé.

   Lorsque vous créez un service en utilisant UDP comme protocole de couche de transport, un moniteur ping (moniteur intégré) est automatiquement lié au service. Lorsque vous créez un service en utilisant TCP comme protocole de couche de transport, un moniteur **tcp_default** est automatiquement lié au service.

   Pour la configuration de l'équilibrage de charge, vous pouvez lier votre service à un autre type de moniteur ou à plusieurs moniteurs. Pour les exigences de surveillance avancée, vous pouvez utiliser le moniteur **tcp-ecv** et configurer les messages de demande et de réponse.

7. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

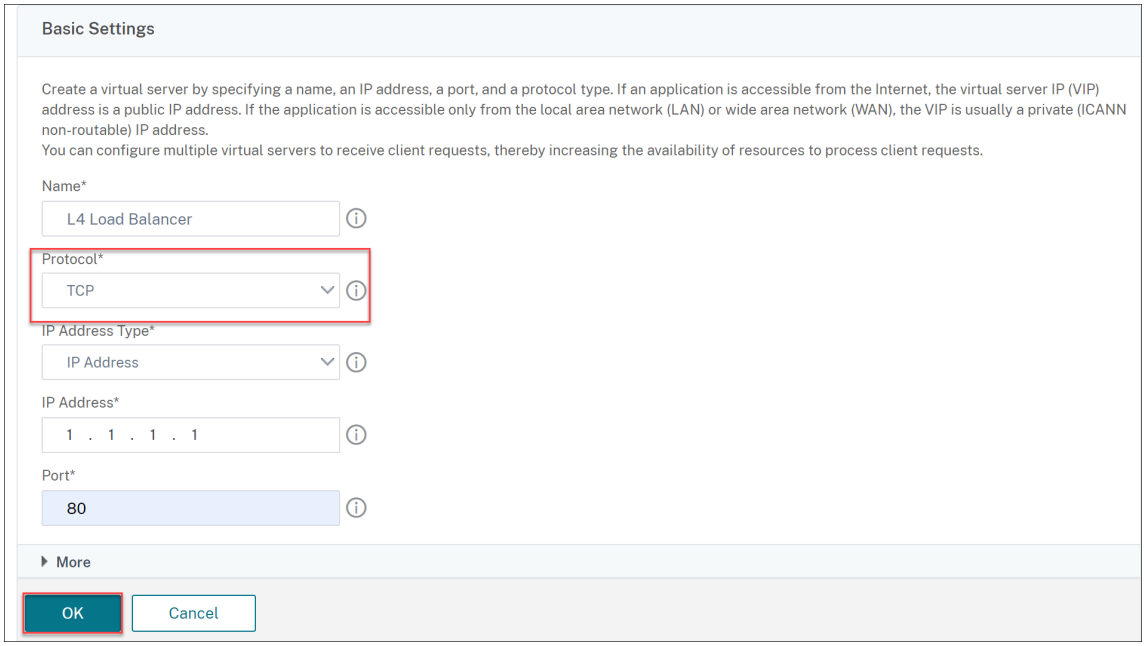


8. Cliquez sur **Ajouter** pour créer un nouveau serveur virtuel.

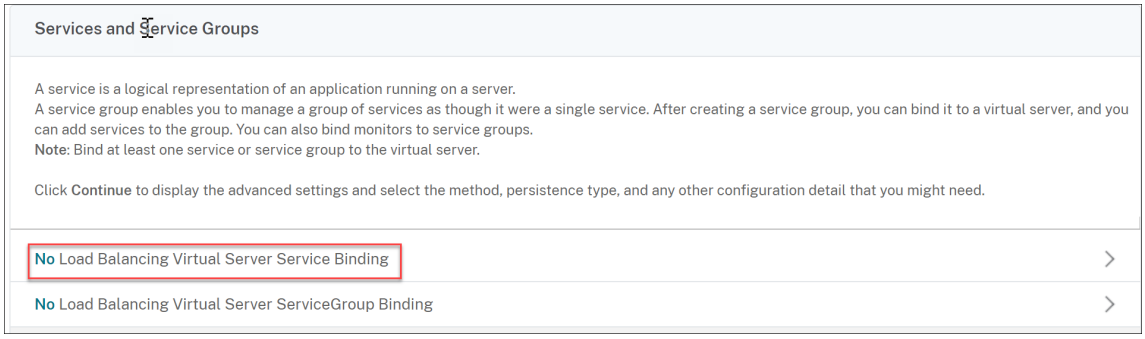
   Lorsque l'équilibrage de charge est configuré, vous pouvez vous connecter au site Web, à l'application ou au serveur à charge équilibrée via l'adresse IP ou le nom de domaine complet du serveur virtuel.

9. Spécifiez les détails requis dans **Nom**, **Type d'adresse IP**et **Adresse IP**.
10. Sélectionnez **TCP** ou **UDP** dans **Protocol**.

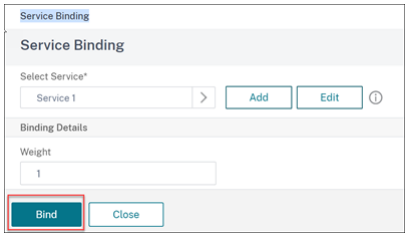
11. Tapez un numéro de port (de 0 à 1023 en fonction du type de service) dans **Port**.
12. Cliquez sur **OK**.



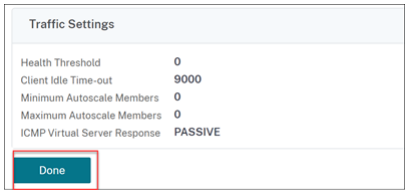
13. Cliquez **sur Liaison de service de serveur virtuel sans équilibrage** de charge dans **Services et groupes de services**.



14. Dans la page **Liaison de services**, sélectionnez **Cliquez pour sélectionner** dans **Sélectionner un service**.
15. Sélectionnez le service à lier, puis cliquez sur **Sélectionner**.
16. Cliquez sur **Liaison pour lier** le service au serveur virtuel.



17. Cliquez sur **Continuer**.
18. Cliquez sur **Terminé**.



La configuration du serveur virtuel d'équilibrage de charge de couche 4 est terminée.

Résolution des problèmes

August 20, 2021

Si l'équilibrage de charge ne fonctionne pas comme prévu après l'avoir configuré, vous pouvez utiliser certains outils courants pour accéder aux ressources Citrix ADC et diagnostiquer le problème.

Ressources pour le dépannage de l'équilibrage de charge

Pour obtenir de meilleurs résultats, utilisez les ressources suivantes pour résoudre un problème de commutation de contenu sur une appliance Citrix ADC :

- Dernier fichier ns.conf
- `newnslog` Fichiers pertinents
- Traces de paquets éthéré enregistrées sur l'appliance et le client concerné, si possible
- Le fichier ns.log

En plus des ressources ci-dessus, les outils suivants permettent d'accélérer le dépannage :

- Outil complémentaire de navigateur qui peut afficher les en-têtes HTTP. Cela peut être utilisé pour résoudre les problèmes liés à la persistance.
- Application Wireshark personnalisée pour les fichiers de trace Citrix ADC.

Résolution des problèmes d'équilibrage de charge

- **Problème**

L'utilisation du processeur atteint 100 % lorsqu'un moniteur utilisateur est lié à un service lié à un serveur virtuel sur lequel l'option -m MAC est activée.

- **Résolution**

Liez un moniteur non-utilisateur au service.

- **Problème**

  J'ai créé un script utilisateur pour la surveillance, mais cela ne fonctionne pas.

  Résolution

  Vérifiez le nombre d'arguments dans le script. La limite est de 512. Un script avec plus de 512 arguments peut ne pas fonctionner correctement. Utilisez le script nsumon-debug.pl de l'interface de ligne de commande pour déboguer le script.

- **Problème**

  Je vois beaucoup de sondes de moniteur, et ils semblent augmenter le trafic réseau inutilement. Existe-t-il un moyen de désactiver les sondes du moniteur ?

  Résolution

  Vous pouvez désactiver les connexions de la sonde du moniteur en désactivant le moniteur ou en définissant la valeur du paramètre HealthMonitor dans la commande set service sur NO. Avec l'option NO, l'appliance affiche le service comme UP à tout moment.

- **Problème**

  J'ai configuré des moniteurs pour les services, mais les connexions sont toujours dirigées vers des serveurs qui sont DOWN.

  Résolution

  Vous devez probablement réduire les intervalles de sonde du moniteur. L'appliance Citrix ADC ne détecte pas l'état DOWN tant que le moniteur n'envoie pas une sonde.

- **Problème**

  Une mesure liée au moniteur est présente dans les tables de mesures locales et personnalisées.

  Résolution

  Ajoutez le préfixe local au nom de mesure si la mesure est choisie dans la table de mesure locale. Toutefois, si la mesure est choisie dans la table personnalisée, vous n'avez pas besoin d'ajouter de préfixe.

- **Problème**

  Les sondes du moniteur à un service n'atteignent pas le service.

  Résolution

  Vérifiez si vous avez défini une limite sur le nombre de connexions pour un service. Si oui, exemptez les connexions moniteur-sonde de cette limite en définissant le paramètre MonitorSkipMaxClient sur Enabled.

- **Problème**

Je suis capable de ping les serveurs, mais l'état des services est toujours affiché comme DOWN.

Résolution

Vérifiez le type de moniteurs configurés. Par exemple, si un serveur n'est pas configuré pour SSL et que vous utilisez un moniteur HTTPS, l'état du service est marqué comme étant DOWN. Dans ce cas, l'utilisation d'un moniteur TCP doit changer l'état du service sur UP.

- **Problème**

  Définir un poids pour les moniteurs de charge n'aide pas à décider de l'état du service.

  Résolution

  Les moniteurs de charge ne peuvent pas décider de l'état du service. Par conséquent, définir un poids sur les moniteurs de charge n'est pas approprié.

- **Problème**

  Un service n'est pas stable.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez qu'un serveur correct est lié au service.
  - Vérifiez le type de moniteur lié au service.
  - Vérifiez les raisons des défaillances du moniteur. Vous pouvez ouvrir un service à partir de la page Services et vérifier les détails du nombre de sondes, de défaillances et de l'état de la dernière réponse du moniteur dans l'onglet Monitors de la boîte de dialogue Configurer le service. Pour afficher les détails, cliquez sur le moniteur configuré.
  - S'il s'agit d'un moniteur personnalisé, liez un moniteur TCP ou ping au service et vérifiez l'état du moniteur. Si cela résout le problème, il y a un problème avec le moniteur personnalisé et le moniteur nécessite une enquête plus approfondie.
  - Vous pouvez enregistrer des traces de paquets sur l'appliance Citrix ADC et vérifier les sondes du moniteur et la réponse du serveur pour une enquête plus approfondie.

- **Problème**

  L'adresse IP virtuelle (VIP) n'est pas stable ou son état est affiché comme DOWN.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez que la fonction d'équilibrage de charge est sous licence.
  - Vérifiez que la fonctionnalité est activée.
  - Vérifiez qu'un service approprié est lié au serveur virtuel.
  - Si le statut de l'adresse VIP est affiché comme DOWN, vérifiez qu'un administrateur a activé le service. Si ce n'est pas le cas, le statut du service doit être hors service. Dans ce cas, vous devez activer le service et vérifier si le problème est résolu.

- Vérifiez le (s) service (s) lié (s) au serveur virtuel et suivez les étapes de dépannage mentionnées pour le problème de service non stable.
- Si l'adresse VIP n'est pas stable, tous les services liés au serveur virtuel doivent échouer. Par conséquent, vérifiez si tous les services échouent en même temps. Si tel est le cas, il existe un problème de réseau entre l'appliance Citrix ADC et les serveurs.

- **Problème**

  Le site connaît un équilibrage de charge inégal.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez la méthode d'équilibrage de charge configurée sur l'appliance.
  - Vérifiez que les poids associés aux services sont comme prévu.
  - Si la méthode d'équilibrage de charge est autre que Round Robin, vérifiez le nombre de connexions au serveur connecté dans le `newnslog` fichier. Vous pouvez exécuter la commande suivante pour vérifier le numéro du `newnslog` fichier :

    ```
    ## nsconmsg -K <newnslog_file> -s ConLb=2 -d oldconmsg
    ```

    Vérifiez les services du serveur virtuel spécifique et vérifiez le temps de réponse, les connexions ouvertes établies (OE), le nombre de demandes, les demandes persistantes et le taux persistant (P) pour résoudre davantage le problème.
  - Si la méthode d'équilibrage de charge est ronde, vérifiez les demandes persistantes comme mentionné à l'étape précédente. En outre, vérifiez si le service n'est pas stable. Si ce n'est pas le cas, effectuez les étapes de dépannage mentionnées pour le problème de service non stable
  - Vérifiez si la persistance est configurée sur l'appliance.
  - Vérifiez si un service n'est pas stable. Si oui, suivez les étapes de dépannage mentionnées pour le problème de service non stable.

- **Problème**

  L'état du service est affiché comme DOWN.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez si une adresse SNIP est configurée.
  - Vérifiez que les moniteurs appropriés sont liés au service.
  - Si des moniteurs personnalisés sont liés au service, liez un moniteur TCP ou ping au service et vérifiez l'état du moniteur. Si cela résout le problème, il y a un problème avec le moniteur personnalisé et le moniteur nécessite une enquête plus approfondie.

- Vérifiez si l'état du service est affiché comme DOWN pour le serveur qui se trouve dans un autre sous-réseau. Si oui, vérifiez si Use Subnet IP (USNIP) résout le problème car cela peut être dû au fait que l'adresse MIP ne peut pas communiquer avec le serveur.

- **Problème**

  Il y a un problème avec le temps de réponse.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez le temps de réponse du serveur à partir des statistiques de service en exécutant la commande suivante :

    ```
    ## nsconmsg -K <newnslog_file> -s ConLb=2 -d oldconmsg
    ```

  - Vérifiez que le service n'est pas stable et que l'état du service est affiché en tant que problèmes DOWN.

- **Problème**

  L'un des serveurs sert plus de demandes que les autres serveurs équilibrés de charge.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez la méthode d'équilibrage de charge. Utilisez la méthode round robin pour distribuer la requête client de manière égale quelle que soit la charge sur les serveurs.
  - Déterminez si la persistance est activée pour la configuration d'équilibrage de charge. Si la persistance est activée, un serveur donné peut supporter une charge plus lourde pour maintenir sa session, surtout si les sessions de persistance sont longues.
  - Vérifiez si des pondérations sont affectées à chaque service. L'attribution de poids appropriés aide à une bonne répartition de la charge.

- **Problème**

  Les connexions à un serveur équilibré de charge spécifique sont bloquées. Par exemple, toutes les connexions à un serveur Outlook peuvent être bloquées.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez la méthode d'équilibrage de charge. S'il s'agit d'un round robin, envisagez de changer la méthode en moins de connexions.
  - Envisagez de réduire le délai d'attente du moniteur. Un délai d'attente plus court permet de marquer un service comme étant DOWN plus tôt, ce qui aiderait à diriger le trafic vers le serveur qui est fonctionnel.

- Si les connexions sont bloquées pendant une longue période, une file d'attente de surtension peut s'accumuler. Envisagez de vider la file d'attente des surtensions pour éviter un pic soudain de charge sur le serveur.
- Si les serveurs fonctionnent à leur niveau maximal, envisagez d'ajouter un nouveau serveur pour de meilleures performances.

- **Problème**

  La majorité des connexions sont dirigées vers un serveur particulier, même lorsque la méthode de connexion minimale pour l'équilibrage de charge est configurée.

  Résolution

  Déterminez si la persistance est configurée et est de type IP source. Si la persistance de l'adresse IP source est configurée même avec la méthode de connexion minimale, les requêtes vont à un serveur spécifique. L'adresse IP du serveur est requise pour gérer les informations de session. Envisagez d'utiliser la persistance basée sur les cookies HTTP.

- **Conseils de dépannage**
  Pour d'autres problèmes, prenez en compte les conseils suivants pour résoudre un problème non répertorié ci-dessus :

  - Si plusieurs moniteurs de charge sont liés à un service, la charge sur le service est la somme de toutes les valeurs sur les moniteurs de charge qui lui sont liés. Pour que l'équilibrage de charge fonctionne correctement, vous devez lier le même ensemble de moniteurs à tous les services.
  - Si vous désactivez un moniteur de charge lié au service et que le service est lié à un serveur virtuel, le serveur virtuel utilise la méthode Round Robin pour l'équilibrage de charge.
  - Lorsque vous liez un service à un serveur virtuel où la méthode d'équilibrage de charge est CUSTOMLOAD et où l'état du service est UP, le serveur virtuel utilise la méthode Round Robin initiale pour l'équilibrage de charge. Il continue d'être en ronde ronde si le service ne dispose pas de moniteurs de charge personnalisés ou si l'état d'au moins un des moniteurs de charge personnalisés n'est pas UP.
  - Tous les services liés à un serveur virtuel où la méthode d'équilibrage de charge est CUSTOMLOAD, les services doivent avoir des moniteurs de charge liés à eux.
  - La méthode d'équilibrage de charge CUSTOMLOAD suit également la ronde de démarrage.
  - Si vous désactivez une liaison basée sur des mesures et qu'il s'agit de la dernière mesure active, le serveur virtuel spécifique utilise la méthode round robin pour l'équilibrage de charge. Une mesure est désactivée en définissant le seuil de mesure sur zéro.
  - Lorsqu'une mesure liée à un moniteur franchit la valeur de seuil, ce service particulier n'est pas pris en compte pour l'équilibrage de charge. Si tous les services ont atteint le seuil, le serveur virtuel utilise la méthode round robin pour l'équilibrage de charge et un message d'erreur « 5xx - server busy error » s'affiche.
  - Un maximum de 10 mesures d'une table personnalisée peut être lié au moniteur.

- Les OID doivent être des variables scalaires.
- Pour un équilibrage de charge réussi, l'intervalle doit être aussi bas que possible. Si l'intervalle est élevé, la période de récupération de la valeur de charge augmente. Par conséquent, l'équilibrage de charge a lieu en utilisant des valeurs incorrectes.
- Un utilisateur ne peut pas modifier la table locale.

Questions fréquentes sur l'équilibrage de la charge

August 20, 2021

Quelles sont les différentes stratégies d'équilibrage de charge que je peux créer sur l'appliance Citrix ADC

Vous pouvez créer les types de stratégies d'équilibrage de charge suivants sur l'appliance Citrix ADC :

- Connexions moindres
- Round Robin
- Temps de réponse le plus faible
- Bande passante minimale
- Moins de paquets
- hachage d'URL
- Hachage de nom de domaine
- Hachage de l'adresse IP source
- Hachage de l'adresse IP de destination
- IP source - Hachage IP de destination
- Jeton
- LRTM

Puis-je assurer la sécurité de la batterie de serveurs Web en implémentant l'équilibrage de charge à l'aide de l'appliance Citrix ADC ?

Oui. Vous pouvez assurer la sécurité de la batterie de serveurs Web en implémentant l'équilibrage de charge à l'aide de l'appliance Citrix ADC. L'appliance Citrix ADC vous permet d'implémenter les options suivantes de la fonctionnalité d'équilibrage de charge :

- Masquage des adresses IP : vous permet d'installer les serveurs réels sur un espace d'adressage IP privé pour des raisons de sécurité et pour la conservation des adresses IP. Ce processus est transparent pour l'utilisateur final car l'appliance Citrix ADC accepte les demandes au nom du serveur. En mode de masquage d'adresses, l'appliance isole complètement les deux réseaux.

Par conséquent, un client peut accéder à un service s'exécutant sur le sous-réseau privé, tel que FTP ou un serveur Telnet, via un autre VIP sur l'appliance pour ce service.

- Mappage de ports : permet d'héberger les services TCP réels sur des ports non standard pour des raisons de sécurité. Ce processus est transparent pour l'utilisateur final car l'appliance Citrix ADC accepte les demandes au nom du serveur sur l'adresse IP et le numéro de port annoncés standard.

Quels sont les différents appareils que je peux utiliser pour équilibrer la charge avec une appliance Citrix ADC ?

Vous pouvez équilibrer la charge des appareils suivants avec une appliance Citrix ADC :

- Batteries de serveurs
- Caches ou Proxies inversées
- Périphériques de pare-feu
- Systèmes de détection des intrusions
- Dispositifs de déchargement SSL
- Dispositifs de compression
- Serveurs d'inspection de contenu

Pourquoi dois-je implémenter la fonctionnalité d'équilibrage de charge pour le site Web ?

Vous pouvez implémenter la fonctionnalité d'équilibrage de charge pour le site Web afin de tirer les avantages suivants :

- Réduisez le temps de réponse : lorsque vous implémentez la fonction d'équilibrage de charge pour le site Web, l'un des principaux avantages est l'augmentation que vous pouvez attendre avec impatience dans le temps de chargement. Avec deux serveurs ou plus partageant la charge du trafic Web, chacun des serveurs exécute moins de charge de trafic qu'un seul serveur. Cela signifie qu'il y a plus de ressources disponibles pour répondre aux demandes des clients. Cela se traduit par un site Web plus rapide.
- Redondance : La mise en œuvre de la fonction d'équilibrage de charge introduit un peu de redondance. Par exemple, si le site est équilibré sur trois serveurs et que l'un d'eux ne répond pas du tout, les deux autres peuvent continuer à fonctionner et les visiteurs du site ne remarquent même pas de temps d'arrêt. Toute solution d'équilibrage de charge cesse immédiatement d'envoyer du trafic vers le serveur principal qui n'est pas disponible.

Pourquoi dois-je désactiver l'option MBF (Mac Based Forwarding) pour Link Load Balancing (LLB) ?

- Si vous activez l'option MBF, l'appliance Citrix ADC considère que le trafic entrant en provenance du client et le trafic sortant vers le même client passent par le même routeur en amont. Toutefois, la fonctionnalité LLB nécessite le meilleur chemin d'accès pour le trafic retour.
- L'activation de l'option MBF rompt cette conception de topologie en envoyant le trafic sortant via le routeur qui a transféré le trafic client entrant.

Mise en réseau

August 20, 2021

Les rubriques suivantes fournissent une référence conceptuelle et des instructions pour configurer les différents composants réseau sur l'appliance Citrix ADC.

Adressage IP	Découvrez les différents types d'adresses IP détenues par Citrix ADC et comment les créer, les personnaliser et les supprimer.
Interfaces	Configurez certaines des configurations réseau de base qui doivent être effectuées pour démarrer.
Listes de contrôle d'accès (ACL)	Configurez les différents types de listes de contrôle d'accès et comment les créer, les personnaliser et les supprimer.
Routage IP	Apprenez et configurez la fonctionnalité de routage de l'appliance Citrix ADC, statique et dynamique.
Protocole Internet version 6 (IPv6)	Découvrez comment l'appliance Citrix ADC prend en charge IPv6.
Domaines de trafic	Apprenez et configurez les domaines de trafic pour segmenter le trafic réseau pour différentes applications.
VXLAN	Apprenez et configurez les VXLAN pour répondre aux besoins d'évolutivité de votre centre de données.

Adressage IP

January 21, 2021

Avant de pouvoir configurer l'appliance Citrix ADC, vous devez affecter l'adresse NSIP, également appelée adresse IP de gestion. Vous pouvez également créer d'autres adresses IP appartenant à Citrix ADC pour abstraire les serveurs et établir des connexions avec les serveurs. Dans ce type de configuration, l'appliance sert de proxy pour les serveurs abstraits. Vous pouvez également utiliser des connexions proxy à l'aide de traductions d'adresses réseau (INAT et RNAT). Lors de la connexion par proxy, l'appliance peut se comporter comme un périphérique de pontage (couche 2) ou comme un périphérique de transfert de paquets (couche 3). Pour rendre le transfert de paquets plus efficace, vous pouvez configurer des entrées ARP statiques. Pour IPv6, vous pouvez configurer la découverte de voisins (ND).

Configuration des adresses IP appartenant à Citrix ADC

January 21, 2021

Les adresses IP appartenant à Citrix ADC, à savoir l'adresse NSIP, les adresses IP virtuelles (VIP), les adresses IP de sous-réseau (SNIP) et les adresses IP du site d'équilibrage de charge du serveur global (GSLBips), existent uniquement sur l'appliance Citrix ADC. Le NSIP identifie de manière unique le Citrix ADC sur votre réseau et donne accès à l'appliance. Un VIP est une adresse IP publique à laquelle un client envoie des demandes. Citrix ADC met fin à la connexion client au VIP et initie une connexion avec un serveur. Cette nouvelle connexion utilise un SNIP ou un MIP comme adresse IP source pour les paquets transférés au serveur. Si vous disposez de plusieurs centres de données répartis géographiquement, chaque centre de données peut être identifié par un GSLBIP unique. Vous pouvez configurer certaines adresses IP appartenant à Citrix ADC pour fournir l'accès aux applications de gestion.

Configuration de l'adresse NSIP

August 20, 2021

L'adresse NSIP est l'adresse IP à laquelle vous accédez à l'appliance Citrix ADC à des fins de gestion. L'appliance ne peut avoir qu'un seul NSIP, également appelé adresse IP de gestion. Vous devez ajouter cette adresse IP lorsque vous configurez Citrix ADC pour la première fois. Vous ne pouvez pas supprimer une adresse NSIP. Pour des raisons de sécurité, le NSIP doit être une adresse IP non routable sur le réseau local de votre organisation.

Si vous modifiez cette adresse, vous devez redémarrer l'appliance Citrix ADC. Si l'adresse de sous-réseau de la nouvelle adresse NSIP est différente de la précédente, vous devez ajouter un itinéraire par défaut pour ce sous-réseau afin que la nouvelle adresse NSIP devienne accessible à partir d'autres réseaux sur le réseau local.

> **Important**
>
> La configuration de l'adresse NSIP est obligatoire.

La modification de l'adresse NSIP d'une appliance Citrix ADC comporte les tâches suivantes :

- Modifiez l'adresse du NSIP.
- Ajoutez un itinéraire par défaut pour l'adresse de sous-réseau de l'adresse NSIP, s'il n'en existe pas.
- Enregistrez la configuration.
- Redémarrez l'appliance.

Procédures de ligne de commande

Pour modifier l'adresse NSIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **définir ns config -IPAddress** <netmask> <ip_addr> **-netmask**
- **show ns config**

Pour ajouter un itinéraire par défaut à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **ajouter route 0 0** <gateway IP address>
- **Afficher l'itinéraire**

Pour enregistrer la configuration à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **save config**

Pour redémarrer l'appliance Citrix ADC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **reboot**

Procédures GUI

Pour configurer l'adresse NSIP à l'aide de l'interface graphique :

1. Cliquez sur l'icône en forme de roue dentée dans le coin supérieur droit de la page **Configuration** .
2. Cliquez sur le**volet d'adresses** NSIP.
3. Sur la page d'**adresse NSIP**, définissez les paramètres suivants, puis cliquez sur **Terminé** :
   - Adresse du NSIP
   - Masque réseau

Pour ajouter un itinéraire par défaut à l'aide de l'interface graphique :

Accédez à **Système** >**Réseau** > **Itinéraires** et, sous l'onglet De **base**, ajoutez un itinéraire par défaut avec les paramètres suivants, puis cliquez sur **Créer** .

- Réseau (défini sur zéro)
- Masque de réseau (défini sur zéro)
- Passerelle (adresse IP de la Gateway)

Pour redémarrer Citrix ADC à l'aide de l'interface graphique :

1. Dans la page de l'onglet **Informations système** du nœud **Système**, cliquez sur **Redémarrer** .
2. Lorsque vous êtes invité à redémarrer, sélectionnez **Enregistrer la configuration** pour vous assurer que vous ne perdez aucune configuration.

Exemple de configuration

Dans l'exemple suivant, l'adresse NSIP d'une appliance Citrix ADC est remplacée par 192.0.2.90, qui a une adresse de sous-réseau différente (192.0.2.0/24) de l'adresse NSIP précédente. Par conséquent, une route par défaut est ajoutée pour ce sous-réseau, de sorte que la nouvelle adresse NSIP devient accessible à partir d'autres réseaux.

```
1  > set nsconfig -ipAddress 192.0.2.90 -netmask 255.255.255.0
2
3   Warning: The configuration must be saved and the system rebooted for
       these settings to take effect
4  > add route 0 0 192.0.2.1
5
6   Warning: The configuration must be saved and the system rebooted for
       these settings to take effect
7  > save config
8
9   Done
10 > reboot
```


Configuration et gestion des adresses IP virtuelles (VIP)

August 20, 2021

La configuration d'une adresse IP de serveur virtuel (VIP) n'est pas obligatoire lors de la configuration initiale du Citrix ADC. Lorsque vous configurez l'équilibrage de charge, vous affectez des adresses VIP aux serveurs virtuels.

Pour plus d'informations sur la configuration d'une configuration d'équilibrage de charge, voir Équilibrage de charge.

Dans certains cas, vous devez personnaliser les attributs VIP ou activer ou désactiver une adresse VIP. Une adresse VIP est généralement associée à un serveur virtuel et certains attributs VIP sont personnalisés pour répondre aux exigences du serveur virtuel. Vous pouvez héberger le même serveur virtuel sur plusieurs appliances Citrix ADC résidant sur le même domaine de diffusion, à l'aide des attributs ARP et ICMP. Après avoir ajouté un VIP (ou toute adresse IP), l'appliance envoie des demandes ARP, puis y répond. Les VIP sont les seules adresses IP appartenant à Citrix ADC qui peuvent être désactivées. Lorsqu'une adresse VIP est désactivée, le serveur virtuel qui l'utilise tombe en panne et ne répond pas aux demandes de service ARP, ICMP ou L4. Comme alternative à la création d'adresses VIP une par une, vous pouvez spécifier une plage consécutive d'adresses VIP.

Pour créer une adresse VIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add ns ip <IPAddress> <netmask> -type <type>
- montrer ns ip <IPAddress>

Exemple :

```
1 > add ns ip 10.102.29.59 255.255.255.0 -type VIP
2  Done
3 <!--NeedCopy-->
```

Pour créer une plage d'adresses VIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add ns ip <IPAddress> <netmask> -type <type>
- montrer ns ip <IPAddress>

Exemple :

```
1 > add ns ip 10.102.29.[60-64] 255.255.255.0 -type VIP
2 ip "10.102.29.60" added
3 ip "10.102.29.61" added
4 ip "10.102.29.62" added
```



```
ip "10.102.29.63" added
ip "10.102.29.64" added
 Done
<!--NeedCopy-->
```

Pour activer ou désactiver une adresse VIP IPv4 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants pour activer ou désactiver un VIP et vérifiez la configuration :

- enable ns ip <IPAddress>
- montrer ns ip <IPAddress>
- disable ns ip <IPAddress>
- montrer ns ip <IPAddress>

Exemple :

```
> enable ns ip 10.102.29.79
 Done
> show ns ip 10.102.29.79

        IP: 10.102.29.79
        Netmask: 255.255.255.255
        Type: VIP
        state: Enabled
        arp: Enabled
        icmp: Enabled
        vserver: Enabled
        management access: Disabled
          telnet: Disabled
          ftp: Disabled
          ssh: Disabled
          gui: Disabled
          snmp: Disabled
        Restrict access: Disabled
        dynamic routing: Disabled
        hostroute: Disabled
 Done
> disable ns ip 10.102.29.79
 Done
> show ns ip 10.102.29.79

        IP: 10.102.29.79
        Netmask: 255.255.255.255
        Type: VIP
        state: Disabled
```



```
30          arp: Enabled
31          icmp: Enabled
32          vserver: Enabled
33          management access: Disabled
34            telnet: Disabled
35            ftp: Disabled
36            ssh: Disabled
37            gui: Disabled
38            snmp: Disabled
39          Restrict access: Disabled
40          dynamic routing: Disabled
41          hostroute: Disabled
42
43   Done
44  <!--NeedCopy-->
```

Pour configurer une adresse VIP à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **IP** > **IPv4s**, puis ajoutez une nouvelle adresse IP ou modifiez une adresse existante.

Pour créer une plage d'adresses VIP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IPs> IPv4**.
2. Dans la liste **Action**, sélectionnez **Ajouter une plage**.

Pour activer ou désactiver une adresse VIP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IPs> IPv4**.
2. Procédez comme suit :
   - Sélectionnez une adresse VIP.
   - Maintenez la touche **Ctrl** enfoncée et sélectionnez plusieurs entrées d'adresse de serveur.
   - Maintenez la touche **Maj enfoncée** et sélectionnez une plage d'entrées d'adresse de serveur.
   - Sélectionnez toutes les adresses en cochant la case située à gauche de la ligne d'en-tête.
3. Dans la liste **Action**, sélectionnez **Désactiver** ou **Activer** .

Détection d'une appliance Citrix ADC dans un programme d'équilibrage de charge UDP via les mises à jour TTL

Le tableau suivant montre comment une appliance Citrix ADC gère la valeur TTL des paquets reçus dans différentes fonctionnalités.

Fonctionnalité	Valeur TTL
Serveur virtuel	TTL est définie sur 255 lors du transfert de la demande aux serveurs back-end. TTL est décrémenté de 1 lors de la transmission de la réponse au client.
Mode L2	TTL n'est pas modifié.
Mode L3	TTL est défini sur 255.
INAT	TTL est définie sur 255 lors du transfert de la demande au serveur principal. TTL est décrémenté de 1 lors de la transmission de la réponse au client.

Certaines entreprises/scénarios exécutant une application de surveillance nécessitent que l'appliance Citrix ADC d'une configuration d'équilibrage de charge soit détectée comme l'un des sauts d'un traceroute. Une appliance Citrix ADC d'une configuration d'équilibrage de charge n'est pas détectée dans un traceroute car l'appliance, par défaut, définit la valeur TTL sur 255 au lieu de la décrémenter lors du transfert de la requête à un serveur principal.

Pour répondre à cette exigence, le paramètre **TTL Decrement** d'une adresse VIP peut être utilisé. Ce paramètre s'applique à tous les serveurs virtuels UDP utilisant ce VIP.

Lorsque vous activez le paramètre **TTL Decrement** d'un VIP, l'appliance Citrix ADC décrémente la valeur TTL de 1 au lieu de la définir sur 255 lors du transfert de demandes, qui sont reçues sur les serveurs virtuels UDP qui utilisent ce VIP.

La surveillance des applications à l'aide de données traceroute permet désormais de détecter la présence d'une appliance Citrix ADC d'une configuration d'équilibrage de charge UDP.

Avant de commencer

Avant de commencer à configurer un dispositif Citrix ADC à détecter dans un traceroute d'une configuration d'équilibrage de charge, notez les points suivants :

- Le paramètre TTL de décrémentation est pris en charge uniquement pour les serveurs virtuels d'équilibrage de charge UDP.
- Le paramètre TTL de décrémentation est pris en charge pour les adresses IPv4 VIP ainsi que IPv6 VIP (VIP6).
- Le paramètre TTL de décrémentation est pris en charge pour les appliances Citrix ADC autonomes ainsi que pour les configurations de haute disponibilité (HA) et de cluster.

Étapes de configuration

La configuration d'une appliance Citrix ADC à détecter dans un traceroute d'une configuration d'équilibrage de charge UDP comporte les tâches suivantes :

- Créer une configuration d'équilibrage de charge UDP
- Activer le paramètre TTL Decrement pour l'adresse VIP

Procédures CLI

Pour activer l'option TTL de décrémentation pour une adresse VIP à l'aide de l'interface de ligne de commande :

- Pour activer l'option TTL de décrémentation pour une adresse VIP lors de l'ajout de l'adresse VIP, à l'invite de commandes, tapez :
  - **add ns ip** <ip> <mask> -**type VIP** -**decrementTTL ENABLED**
  - **show ns ip** <VIP address>
- Pour activer l'option TTL de décrémentation pour une adresse VIP existante, à l'invite de commandes, tapez :
  - **set ns ip** <ip> <mask> -**decrementTTL ENABLED**
  - **show ns ip** <VIP address>

Pour activer l'option TTL de décrémentation pour une adresse VIP6 à l'aide de l'interface de ligne de commande :

- Pour activer l'option TTL de décrémentation pour une adresse VIP6 lors de l'ajout de l'adresse VIP6, à l'invite de commandes, tapez :
  - **add ns ip6** <IP6/prefix> <mask> -**type VIP** -**decrementTTL ENABLED**
  - **show ns ip6** <VIP6/prefix>
- Pour activer l'option TTL de décrémentation pour une adresse VIP6 existante, à l'invite de commandes, tapez :
  - **set ns ip6** <ip6/prefix> <mask> -**decrementTTL ENABLED**
  - **show ns ip6** <VIP6 address>

```
1      > add ns ip 203.0.113.30 -type VIP -decrementTTL ENABLED
2       Done
3
4      > add ns ip6  2001:DB8:5001::30 -type VIP -decrementTTL ENABLED
5       Done
6  <!--NeedCopy-->
```

Procédures GUI

Pour activer l'option TTL de décrémentation pour une adresse VIP à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **IP** > **IPv4s** et activez le paramètre **Decrement TTL** tout en ajoutant une nouvelle adresse VIP ou en modifiant une adresse existante.

Pour activer l'option TTL de décrémentation pour une adresse VIP6 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **IP** > **IPv6s** et activez le paramètre **Decrement TTL** tout en ajoutant une nouvelle adresse VIP6 ou en modifiant une adresse existante.

Configuration de la suppression de réponse ARP pour les adresses IP virtuelles (VIP)

August 20, 2021

Vous pouvez configurer l'appliance Citrix ADC pour qu'elle réponde ou ne réponde pas aux demandes ARP pour une adresse IP virtuelle (VIP) en fonction de l'état des serveurs virtuels associés à ce VIP.

Par exemple, si des serveurs virtuels V1, de type HTTP et V2, de type HTTPS, partagent l'adresse VIP 10.102.29.45 sur une appliance Citrix ADC, vous pouvez configurer l'appliance pour ne pas répondre à une requête ARP pour VIP 10.102.29.45 si V1 et V2 sont à l'état DOWN.

Les trois options suivantes sont disponibles pour configurer la suppression de réponse ARP pour une adresse IP virtuelle.

- **AUCUN**. L'appliance Citrix ADC répond à toute demande ARP pour l'adresse VIP, quel que soit l'état des serveurs virtuels associés à l'adresse.
- **UN VSERVER**. L'appliance Citrix ADC répond à toute demande ARP pour l'adresse VIP si au moins un des serveurs virtuels associés est en état UP.
- **ALL VSERVER**. L'appliance Citrix ADC répond à toute demande ARP pour l'adresse VIP si tous les serveurs virtuels associés sont en état UP.

Le tableau suivant présente l'exemple de comportement de l'appliance Citrix ADC pour un VIP configuré avec deux serveurs virtuels :

Serveurs virtuels associés pour un VIP	ÉTAT 1	ÉTAT 2	ÉTAT 3	ÉTAT 4
NONE				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Répondre à une demande ARP pour ce VIP ?	Oui	Oui	Oui	Oui

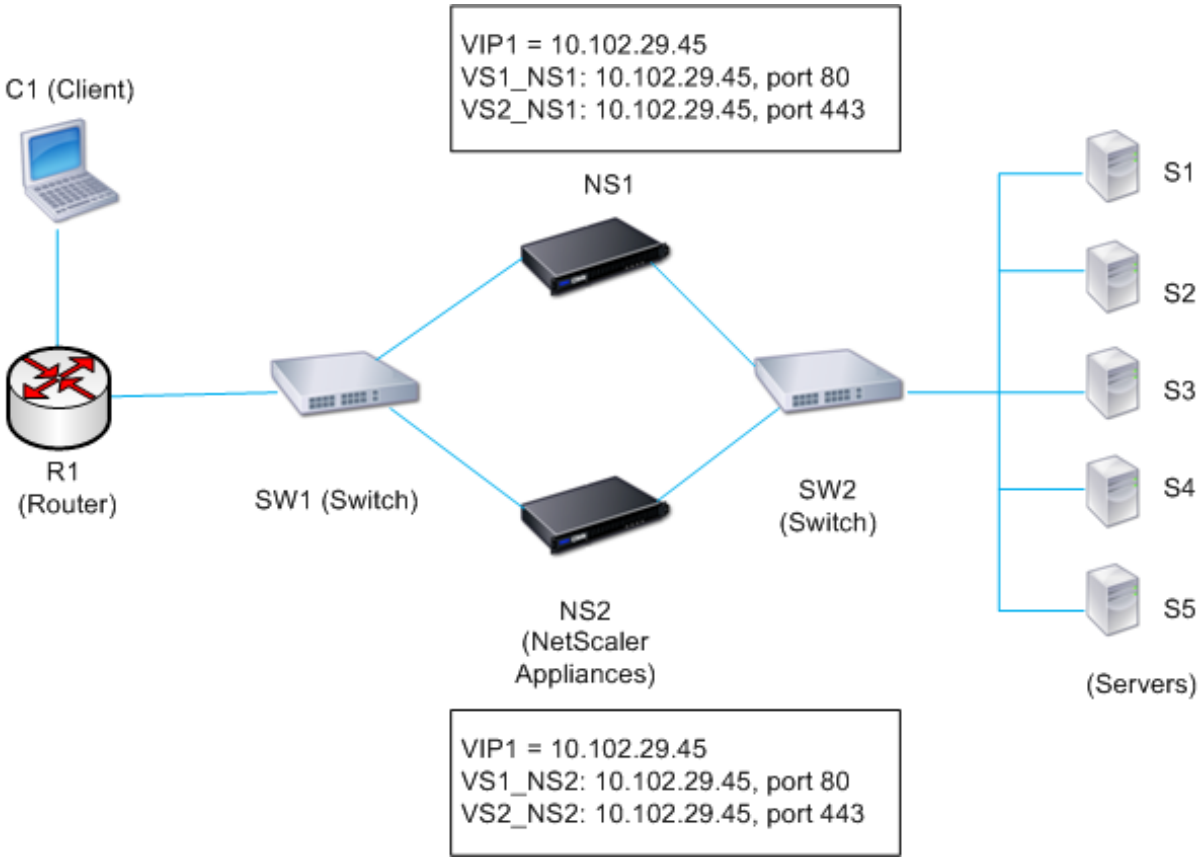
Serveurs virtuels associés pour un VIP	ÉTAT 1	ÉTAT 2	ÉTAT 3	ÉTAT 4
UN VSERVER				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Répondre à une demande ARP pour ce VIP ?	Oui	Oui	Oui	Non
ALL VSERVER				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Répondre à une demande ARP pour ce VIP ?	Oui	Non	Non	Non

Prenons un exemple où vous souhaitez tester les performances de deux serveurs virtuels, V1 et V2, qui ont la même adresse VIP mais sont de types différents et sont chacun configurés sur les appliances Citrix ADC NS1 et NS2. Appelons l'adresse VIP partagée *VIP1*.

V1 équilibre la charge des serveurs S1, S2 et S3. V2 équilibre la charge des serveurs S4 et S5.

Sur NS1 et NS2, pour VIP1, le paramètre de suppression ARP est défini sur ALL_VSERVER. Si vous souhaitez tester les performances de V1 et V2 sur NS1, vous devez désactiver manuellement V1 et V2 sur NS2, afin que NS2 ne réponde pas à aucune demande ARP pour VIP1.

Figure 1.



Le flux d'exécution est le suivant :

1. Le client C1 envoie une demande à V1. La requête atteint R1.
2. R1 n'a pas d'entrée APR pour l'adresse IP (VIP1) de V1, donc R1 diffuse une demande ARP pour VIP1.
3. NS1 répond avec l'adresse MAC source MAC1 et l'adresse IP source VIP1. NS2 ne répond pas à la demande ARP.
4. SW1 apprend le port pour VIP1 à partir de la réponse ARP et met à jour sa table de pont, et R1 met à jour l'entrée ARP avec MAC1 et VIP1.
5. R1 transmet le paquet à l'adresse VIP1 sur NS1.
6. L'algorithme d'équilibrage de charge de NS1 sélectionne le serveur S2, et NS1 ouvre une connexion entre l'une de ses adresses SNIP et S2. Lorsque S2 envoie une réponse au client, la réponse retourne par le même chemin.
7. Maintenant, vous voulez tester les performances de V1 et V2 sur NS2, de sorte que vous activez V1 et V2 sur NS2 et les désactivez sur NS1. NS2 diffuse désormais un message ARP pour VIP1. Dans le message, MAC2 est l'adresse MAC source et VIP1 est l'adresse IP source.
8. SW1 apprend le numéro de port pour atteindre MAC2 à partir de la diffusion ARP et met à jour sa table de pont pour envoyer les demandes clientes suivantes pour VIP1 à NS2. R1 met à jour sa table ARP.
9. Supposons maintenant que l'entrée ARP pour VIP1 expire dans la table ARP de R1, et le client

C1 envoie une requête pour V1. Étant donné que R1 n'a pas d'entrée APR pour VIP1, il diffuse une demande ARP pour VIP1.

10. NS2 répond avec une adresse MAC source et VIP1 comme adresse IP source. NS1 ne répond pas à la demande ARP.

Pour configurer la suppression des réponses ARP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set ns ip** -**arpResponse** <arpResponse>]
- **sh ns IP** <IPAddress>

Exemple :

```
1 > set ns ip 10.102.29.96 -arpResponse ALL_VSERVERS
2  Done
3 <!--NeedCopy-->
```

Pour configurer la suppression des réponses ARP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IPs> IPv4**.
2. Ouvrez une entrée d'adresse IP et sélectionnez le type de réponse ARP.

Configuration des adresses IP de sous-réseau (SNIP)

August 20, 2021

Une adresse IP de sous-réseau (SNIP) est une adresse IP appartenant à Citrix ADC qui est utilisée par Citrix ADC pour communiquer avec les serveurs.

Citrix ADC utilise l'adresse IP du sous-réseau comme adresse IP source pour les connexions client proxy aux serveurs. Il utilise également l'adresse IP du sous-réseau lors de la génération de ses propres paquets, tels que les paquets liés aux protocoles de routage dynamique, ou pour envoyer des sondes de surveillance pour vérifier l'état des serveurs. Selon la topologie de votre réseau, vous devrez peut-être configurer un ou plusieurs SNIP pour différents scénarios.

Pour configurer une adresse SNIP sur un Citrix ADC, ajoutez l'adresse SNIP, puis activez le mode global Use Subnet IP (USNIP). Comme alternative à la création de SNIP un par un, vous pouvez spécifier une plage consécutive de SNIP.

Pour configurer une adresse SNIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add ns ip <IPAddress> <netmask> -type SNIP
- montrer ns ip <IPAddress>

Exemple :

```
> add ns ip 10.102.29.203 255.255.255.0 -type SNIP
 Done
<!--NeedCopy-->
```

Pour créer une plage d'adresses SNIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add ns ip <IPAddress> <netmask> -type SNIP
- montrer ns ip <IPAddress>

Exemple :

```
> add ns ip 10.102.29.[205-209] 255.255.255.0 -type SNIP
ip "10.102.29.205" added
ip "10.102.29.206" added
ip "10.102.29.207" added
ip "10.102.29.208" added
ip "10.102.29.209" added
 Done
<!--NeedCopy-->
```

Pour activer ou désactiver le mode USNIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- enable ns modeUSNIP
- disable ns modeUSNIP

Pour configurer une adresse SNIP à l'aide de l'interface graphique :

Accédez à Système > Réseau > IP > IPv4s, puis ajoutez une nouvelle adresse SNIP ou modifiez une adresse existante.

Pour créer une plage d'adresses SNIP à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > IPs> IPv4.
2. Dans la liste Action, sélectionnez Ajouter une plage.

Pour activer ou désactiver le mode USNIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- enable ns mode USNIP
- disable ns mode USNIP

Pour activer ou désactiver le mode USNIP à l'aide de l'interface graphique :

1. Accédez à Système > Paramètres, dans le groupe Modes et fonctionnalités, cliquez sur Modifier les modes.
2. Sélectionnez ou désactivez l'option Utiliser l'adresse IP du sous-réseau.

Utilisation de SNIP pour un sous-réseau de serveur directement connecté

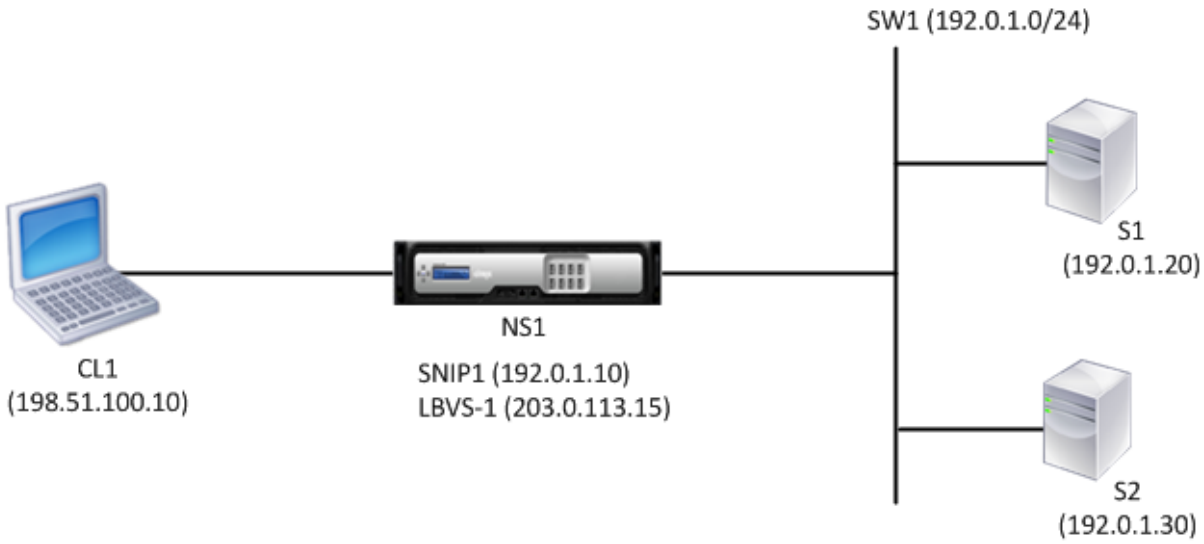
Pour activer la communication entre le Citrix ADC et un serveur connecté directement à ADC Citrix ou connecté uniquement via un commutateur L2, vous devez configurer une adresse IP de sous-réseau qui appartient au sous-réseau du serveur. Vous devez configurer au moins une adresse IP de sous-réseau pour chaque sous-réseau directement connecté, à l'exception du sous-réseau de gestion directement connecté qui est connecté via NSIP.

Prenons un exemple de configuration d'équilibrage de charge dans lequel le serveur virtuel d'équilibrage de charge LBVS1 sur Citrix ADC NS1 est utilisé pour équilibrer la charge des serveurs S1 et S2, qui sont connectés à NS1 via le commutateur L2 SW1. S1 et S2 appartiennent au même sous-réseau.

L'adresse SNIP SNIP1, qui appartient au même sous-réseau que S1 et S2, est configurée sur NS1. Dès que SNIP1 est configuré, NS1 diffuse des paquets ARP pour SNIP1.

Les services SVC-S1 et SVC-S2 sur NS1 représentent S1 et S2. Dès que ces services sont configurés, NS1 diffuse des demandes ARP pour S1 et S2 pour résoudre le mappage IP-MAC. Après que S1 et S2 répondent, NS1 leur envoie des sondes de surveillance à intervalles réguliers, à partir de l'adresse SNIP1, pour vérifier leur état de santé.

Pour plus d'informations sur la configuration de l'équilibrage de charge sur un Citrix ADC, voir Équilibrage de charge.



Voici le flux de trafic dans cet exemple :

1. Le client C1 envoie un paquet de requête à LBVS-1. Le paquet de requête a :

- IP source = adresse IP du client (198.51.100.10)
- IP de destination = adresse IP de LBVS-1 (203.0.113.15)

2. LBVS1 de NS1 reçoit le paquet de requête.
3. L'algorithme d'équilibrage de charge de LBVS1 sélectionne le serveur S2.
4. Comme S2 est directement connecté à NS1 et SNIP1 (192.0.1.10) est la seule adresse IP sur NS1 qui appartient au même sous-réseau que S2, NS1 ouvre une connexion entre SNIP1 et S2.
5. NS1 envoie le paquet de requête à S2 à partir de SNIP1. Le paquet de requête a :
   - IP source = SNIP1 (192.0.1.10)
   - IP de destination = adresse IP de S2 (192.0.1.30)
6. La réponse de S2 renvoie par le même chemin.

Utilisation de SNIP pour les sous-réseaux de serveur connectés via un routeur

Pour activer la communication entre Citrix ADC et les serveurs dans des sous-réseaux connectés via un routeur, vous devez configurer au moins une adresse IP de sous-réseau appartenant au sous-réseau de l'interface directement connectée au routeur. ADC utilise cette adresse IP de sous-réseau pour communiquer avec les serveurs des sous-réseaux accessibles via le routeur.

Prenons un exemple de configuration d'équilibrage de charge dans lequel le serveur virtuel d'équilibrage de charge LBVS1 sur Citrix ADC NS1 est utilisé pour équilibrer la charge des serveurs S1, S2, S3 et S4, qui sont connectés à NS1 via le routeur R1.

S1 et S2 appartiennent au même sous-réseau, 192.0.2.0/24, et sont connectés à R1 via le commutateur L2 SW1. S3 et S4 appartiennent à un autre sous-réseau, 192.0.3.0/24, et sont connectés à R1 via le commutateur L2 SW2.

Citrix ADC NS1 est connecté au routeur R1 via le sous-réseau 192.0.1.0/24. L'adresse SNIP SNIP1, qui appartient au même sous-réseau que l'interface directement connectée au routeur (192.0.1.0/24), est configurée sur NS1. NS1 utilise cette adresse pour communiquer avec les serveurs S1 et S2 et avec les serveurs S3 et S4.

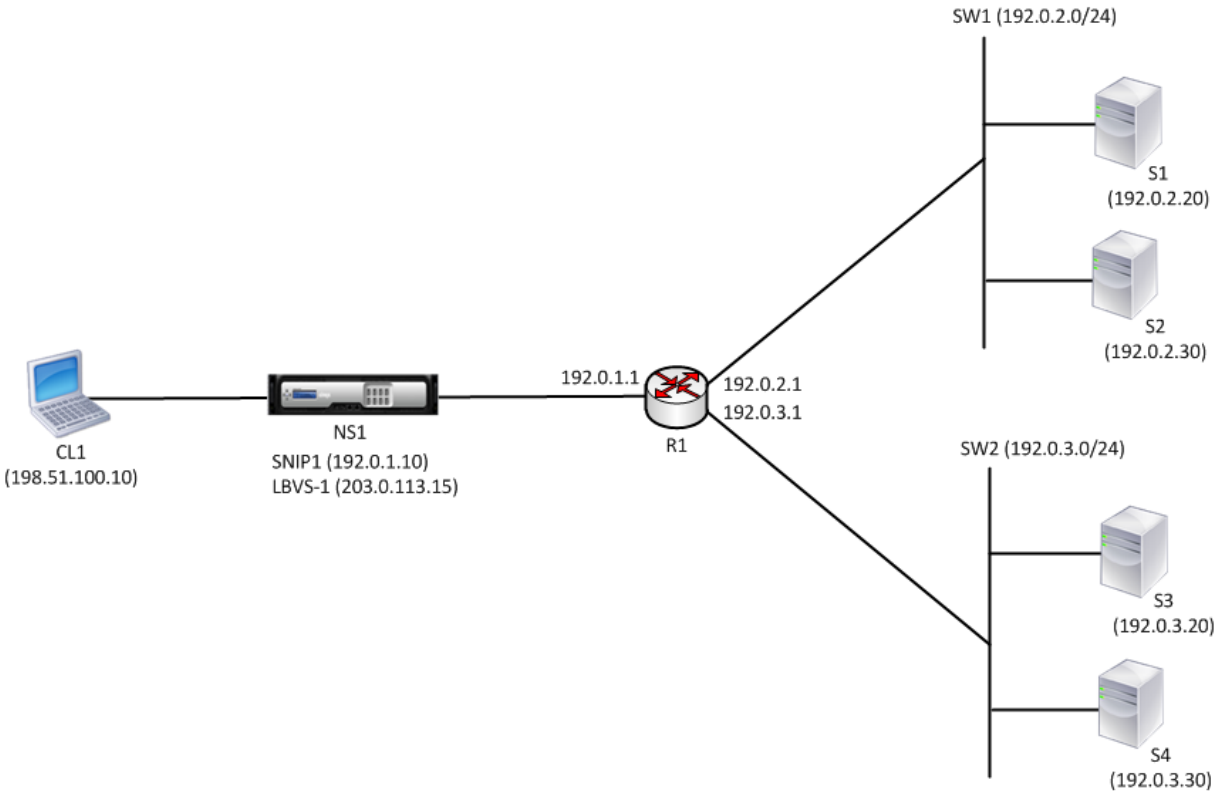
Pour plus d'informations sur la configuration de l'équilibrage de charge sur un Citrix ADC, voir Équilibrage de charge.

Dès que l'adresse SNIP1 est configurée, NS1 diffuse les paquets d'annonce ARP pour SNIP1.

La table de routage de NS1 se compose d'entrées de routage pour S1, S2, S3 et S4 à R1. Ces entrées d'itinéraire sont soit des entrées d'itinéraire statiques, soit annoncées par R1 vers NS1, à l'aide de protocoles de routage dynamiques.

Les services SVC-S1, SVC-S2, SVC-S3 et SVC-S4 sur NS1 représentent les serveurs S1, S2, S3 et S4. NS1 détecte, dans ses tables de routage, que ces serveurs sont accessibles via R1. NS1 leur envoie des sondes de surveillance à intervalles réguliers, à partir de l'adresse SNIP1, pour vérifier leur état de santé.

Pour plus d'informations sur le routage IP sur un Citrix ADC, consultez Routage IP.



Voici le flux de trafic dans cet exemple :

1. Le client C1 envoie un paquet de requête à LBVS-1. Le paquet de requête a :
   - IP source = adresse IP du client (198.51.100.10)
   - IP de destination = adresse IP de LBVS-1 (203.0.113.15)
2. LBVS1 de NS1 reçoit le paquet de requête.
3. L'algorithme d'équilibrage de charge de LBVS1 sélectionne le serveur S3.
4. NS1 vérifie sa table de routage et trouve que S3 est accessible via R1. SNIP1 (192.0.1.10) est la seule adresse IP sur NS1 qui appartient au même sous-réseau que le routeur R1, NS1 ouvre une connexion entre SNIP1 et S3 via R1.
5. NS1 envoie le paquet de requête à R1 à partir de SNIP1. Le paquet de requête a :
   - Adresse IP source = SNIP1 (192.0.1.10)
   - Adresse IP de destination = adresse IP de S3 (192.0.3.20)
6. La requête atteint R1, qui vérifie sa table de routage et transfère le paquet de requête à S3.
7. La réponse de S3 renvoie par le même chemin.

Utilisation de SNIP pour plusieurs sous-réseaux de serveurs (VLAN) sur un commutateur L2

Lorsque vous disposez de plusieurs sous-réseaux de serveur (VLAN) sur un commutateur L2 connecté à un Citrix ADC, vous devez configurer au moins une adresse SNIP pour chacun des sous-réseaux de serveur, afin que l'ADC Citrix puisse communiquer avec ces sous-réseaux de serveur.

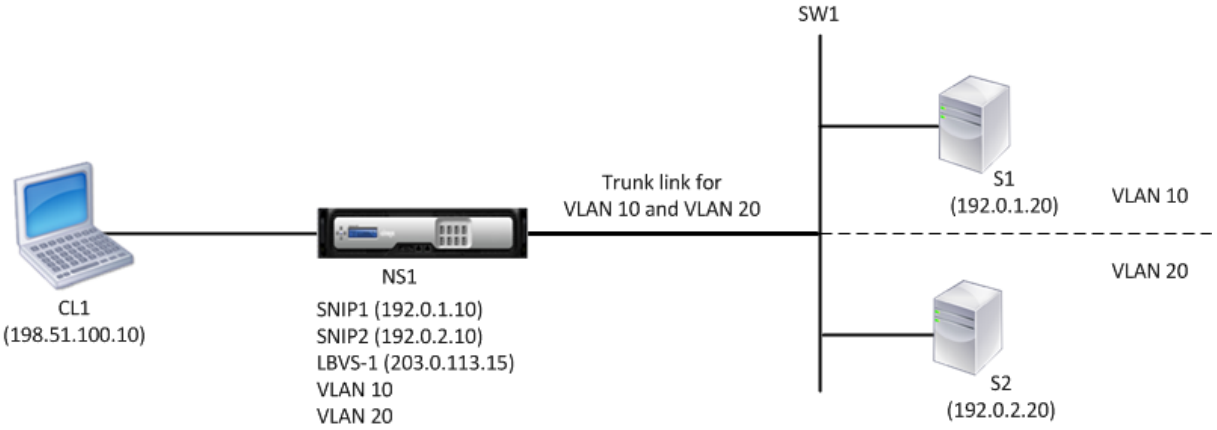
Prenons un exemple de configuration d'équilibrage de charge dans lequel le serveur virtuel d'équilibrage de charge LBVS1 sur Citrix ADC NS1 est utilisé pour équilibrer la charge des serveurs S1 et S2, qui sont connectés à NS1 via le commutateur L2 SW1. S1 et S2 appartiennent à différents sous-réseaux et font partie de VLAN 10 et VLAN20, respectivement. La liaison entre NS1 et SW1 est une liaison de jonction et est partagée par VLAN10 et VLAN20.

Pour plus d'informations sur la configuration de l'équilibrage de charge sur un Citrix ADC, voir Équilibrage de charge.

Les adresses IP de sous-réseau SNIP1 (à des fins de référence uniquement) et SNIP2 (à des fins de référence uniquement) sont configurées sur NS1. NS1 utilise SNIP1 (sur VLAN 10) pour communiquer avec le serveur S1, et SNIP2 (sur VLAN 20) pour communiquer avec S2. Dès que SNIP1 et SNIP2 sont configurés, NS1 diffuse des paquets d'annonce ARP pour SNIP1 et SNIP2.

Pour plus d'informations sur la configuration des VLAN sur un Citrix ADC, consultez Configuration d'un VLAN.

Les services SVC-S1 et SVC-S2 sur NS1 représentent les serveurs S1 et S2. Dès que ces services sont configurés, NS1 diffuse des demandes ARP pour eux. Une fois que S1 et S2 répondent, NS1 leur envoie des sondes de surveillance à intervalles réguliers pour vérifier leur état de santé. NS1 envoie des sondes de surveillance à S1 depuis l'adresse SNIP1 et à S2 depuis l'adresse SNIP2.



Voici le flux de trafic dans cet exemple :

1. Le client C1 envoie un paquet de requête à LBVS-1. Le paquet de requête a :
   - IP source = adresse IP du client (198.51.100.10)
   - IP de destination = adresse IP de LBVS-1 (203.0.113.15)

2. LBVS1 de NS1 reçoit le paquet de requête.
3. L'algorithme d'équilibrage de charge de LBVS1 sélectionne le serveur S2.
4. Comme S2 est directement connecté à NS1 et SNIP2 (192.0.2.10) est la seule adresse IP sur NS1 qui appartient au même sous-réseau que S2, NS1 ouvre une connexion entre SNIP2 et S2. Remarque : Si S1 est sélectionné, NS1 ouvre une connexion entre SNIP1 et S1.
5. NS1 envoie le paquet de requête à S2 à partir de SNIP2. Le paquet de requête a :
   - IP source = SNIP1 (192.0.2.10)
   - IP de destination = adresse IP de S2 (192.0.2.20)
6. La réponse de S2 renvoie par le même chemin.

Configuration des adresses IP de site GSLB (GSLBIP)

August 20, 2021

Une adresse IP de site GSLB (GSLBIP) est une adresse IP associée à un site GSLB. Il n'est pas obligatoire de spécifier une adresse GSLBIP lorsque vous configurez initialement l'appliance Citrix ADC. Une adresse GSLBIP n'est utilisée que lorsque vous créez un site GSLB.

Pour plus d'informations sur la création d'une adresse IP de site GSLB, consultez Global Server Load Balancing.

Suppression d'une adresse IP appartenant à Citrix ADC

August 20, 2021

Vous pouvez supprimer n'importe quelle adresse IP à l'exception du NSIP. Le tableau suivant fournit des informations sur les processus que vous devez suivre pour supprimer les différents types d'adresses IP. Avant de supprimer un VIP, supprimez le serveur virtuel associé.

Type d'adresse IP	Incidences
Adresse IP du sous-réseau (SNIP)	Si l'adresse IP supprimée est la dernière adresse IP du sous-réseau, l'itinéraire associé est supprimé de la table de routage. Si l'adresse IP supprimée est la Gateway dans l'entrée d'itinéraire correspondante, la Gateway de cette route de sous-réseau est remplacée par une autre adresse IP appartenant à Citrix ADC.
Adresse IP du serveur virtuel (VIP)	Avant de supprimer un VIP, vous devez d'abord supprimer le serveur virtuel qui lui est associé. Pour plus d'informations sur la suppression du serveur virtuel, reportez-vous à la section Équilibrage de charge.
Adresse IP du site GSLB-Site-IP	Avant de supprimer une adresse IP de site GSLB, vous devez supprimer le site qui lui est associé. Pour plus d'informations sur la suppression du site, consultez Global Server Load Balancing.

Pour supprimer une adresse IP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

<IPaddress>rm ns ip

Exemple :

```
1 > rm ns ip 10.102.29.54
2 Done
3 <!--NeedCopy-->
```

Pour supprimer une adresse IP à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **IP** > **IPv4s**, supprimez l'adresse IP.

Configuration des contrôles d'accès aux applications

August 20, 2021

Les contrôles d'accès aux applications, également appelés contrôles d'accès de gestion, constituent un mécanisme unifié pour gérer l'authentification des utilisateurs et mettre en œuvre des règles qui déterminent l'accès des utilisateurs aux applications et aux données. Vous pouvez configurer des SNIP pour fournir un accès aux applications de gestion. L'accès de gestion pour le NSIP est activé par défaut et ne peut pas être désactivé. Vous pouvez toutefois le contrôler à l'aide des ACL.

Pour plus d'informations sur l'utilisation des ACL, consultez Listes de contrôle d'accès (ACL).

L'appliance Citrix ADC ne prend pas en charge l'accès de gestion aux VIP.

Le tableau suivant résume l'interaction entre l'accès à la gestion et les paramètres de service spécifiques pour Telnet.

Accès à la gestion	Telnet (État configuré sur Citrix ADC)	Telnet (État effectif au niveau IP)
Activer	Activer	Activer
Activer	Désactiver	Désactiver
Désactiver	Activer	Désactiver
Désactiver	Désactiver	Désactiver

Le tableau suivant donne une vue d'ensemble des adresses IP utilisées comme adresses IP source dans le trafic sortant.

Application/ IP	NSIP	SNIP	VIP
ARP	Oui	Oui	Non
Trafic côté serveur	Non	Oui	Non
RNAT	Non	Oui	Oui
PING ICMP	Oui	Oui	Non
Routage dynamique	Oui	Oui	Oui

Le tableau suivant donne un aperçu des applications disponibles sur ces adresses IP.

Application/ IP	NSIP	SNIP	VIP
SNMP	Oui	Oui	Oui
Accès au système	Oui	Oui	Non

Vous pouvez accéder à Citrix ADC et le gérer à l'aide d'applications telles que Telnet, SSH, GUI et FTP.

Remarque : Telnet et FTP sont désactivés sur Citrix ADC pour des raisons de sécurité. Pour les activer, contactez le support client. Une fois les applications activées, vous pouvez appliquer les contrôles au niveau IP.

Pour configurer Citrix ADC pour qu'il réponde à ces applications, vous devez activer les applications de gestion spécifiques. Si vous désactivez l'accès de gestion pour une adresse IP, les connexions existantes qui utilisent l'adresse IP ne sont pas terminées, mais aucune nouvelle connexion ne peut être initiée.

En outre, les applications non gérées exécutées sur le système d'exploitation FreeBSD sous-jacent sont ouvertes aux attaques de protocole, et ces applications ne tirent pas parti des capacités de prévention des attaques de l'appliance Citrix ADC.

Vous pouvez bloquer l'accès à ces applications non gérées sur un SNIP ou un NSIP. Lorsque l'accès est bloqué, un utilisateur qui se connecte à un Citrix ADC à l'aide du SNIP ou du NSIP ne peut pas accéder aux applications non gérées exécutées sur le système d'exploitation sous-jacent.

Pour configurer l'accès de gestion pour une adresse IP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

set ns ip <IPAddress> -mgmtAccess <value> -**telnet** <value> -**ftp** <value> -**gui** <value> -**ssh** <value> -**snmp** <value> -**restrictAccess** (**ENABLED** | **DÉSACTIVÉ**)

Exemple :

```
1  > set ns ip 10.102.29.54 -mgmtAccess enabled -restrictAccess ENABLED
2   Done
3 <!--NeedCopy-->
```

Pour activer l'accès de gestion pour une adresse IP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IPs> IPv4**.
2. Ouvrez une entrée d'adresse IP et sélectionnez l'option **Activer le contrôle d'accès à la gestion** pour prendre en charge les applications répertoriées.

Activer l'accès sécurisé à l'interface graphique Citrix ADC à l'aide d'une adresse IP de sous-réseau (SNIP)

L'accès sécurisé à l'interface graphique Citrix ADC est activé par défaut pour Citrix ADC IP (NSIP). Vous pouvez également activer l'accès sécurisé à l'appliance Citrix ADC à l'aide d'une adresse IP de sous-réseau de l'appliance.

Après avoir configuré une adresse SNIP pour un accès sécurisé à une paire haute disponibilité, l'accès sécurisé est disponible pour l'appliance principale, si vous accédez à l'adresse SNIP.

Procédure CLI Citrix ADC

Pour activer l'accès sécurisé à l'interface graphique Citrix ADC à l'aide d'une adresse IP de sous-réseau (SNIP) à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

set ns ip <SNIP_Address>**-type SNIP -gui SECUREONLY -MGMTaccess ACTIVÉ**

Exemple :

```
1   > set ns ip 203.0.113.99 -mgmtAccess enabled -restrictAccess ENABLED
2
3    Done
4  <!--NeedCopy-->
```

Comment Citrix ADC utilise un proxy pour les connexions

August 20, 2021

Lorsqu'un client initie une connexion, l'appliance Citrix ADC met fin à la connexion client, initie une connexion à un serveur approprié et envoie le paquet au serveur. L'appliance n'effectue pas cette action pour le type de service UDP ou ANY.

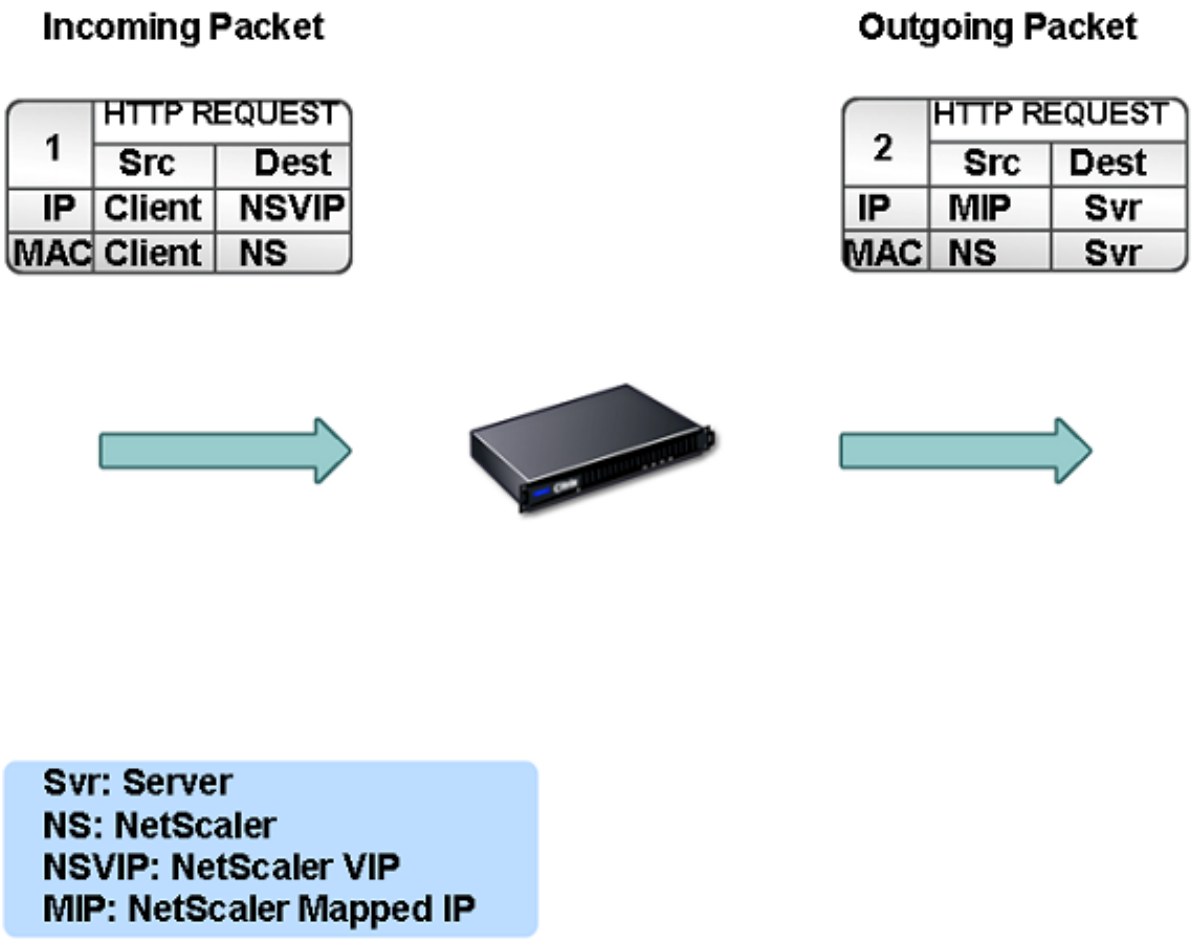
Pour plus d'informations sur les types de service, voir Équilibrage de charge.

Vous pouvez configurer Citrix ADC pour qu'il traite le paquet avant d'initier la connexion avec un serveur. Le comportement par défaut consiste à modifier les adresses IP source et destination d'un paquet avant d'envoyer le paquet au serveur. Vous pouvez configurer Citrix ADC pour qu'il conserve l'adresse IP source des paquets en activant le mode Use Source IP.

Mode de sélection de l'adresse IP de destination

Le trafic envoyé à l'appliance Citrix ADC peut être envoyé à un serveur virtuel ou à un service. L'appliance gère différemment le trafic vers les serveurs et services virtuels. Citrix ADC met fin au trafic reçu à une adresse IP du serveur virtuel (VIP) et modifie l'adresse IP de destination en adresse IP du serveur avant de transférer le trafic au serveur, comme indiqué dans le diagramme suivant.

Figure 1. Connexions proxy aux VIP



Les paquets destinés à un service sont envoyés directement au serveur approprié et Citrix ADC ne modifie pas les adresses IP de destination. Dans ce cas, Citrix ADC fonctionne comme un proxy.

Mode de sélection de l'adresse IP source

Lorsque l'appliance Citrix ADC communique avec les serveurs physiques ou les périphériques homologues, par défaut, elle n'utilise pas l'adresse IP du client. Citrix ADC gère un pool d'adresses IP de sous-réseau (SNIP) et sélectionne une adresse IP de ce pool à utiliser comme adresse IP source d'une connexion au serveur physique. En fonction du sous-réseau dans lequel le serveur physique est placé, Citrix ADC sélectionne une adresse SNIP spécifique.

Remarque : si l'option Use Source IP (USIP) est activée, l'appliance utilise l'adresse IP du client.

Activer l'utilisation du mode IP source

August 20, 2021

Lorsque l'appliance Citrix ADC communique avec les serveurs physiques ou les périphériques homologues, par défaut, elle utilise l'une de ses propres adresses IP comme adresse IP source. L'appliance gère un pool d'adresses IP de sous-réseau (SNIP) et sélectionne une adresse IP de ce pool à utiliser comme adresse IP source pour une connexion au serveur physique. La décision de sélectionner une adresse SNIP dépend du sous-réseau dans lequel réside le serveur physique.

Si nécessaire, vous pouvez configurer l'appliance Citrix ADC pour qu'elle utilise l'adresse IP du client comme adresse IP source. Certaines applications ont besoin de l'adresse IP réelle du client. Les cas d'utilisation suivants sont quelques exemples :

- L'adresse IP du client dans le journal d'accès Web est utilisée à des fins de facturation ou d'analyse d'utilisation.
- L'adresse IP du client est utilisée pour déterminer le pays d'origine du client ou le fournisseur de services Internet d'origine du client. Par exemple, de nombreux moteurs de recherche tels que Google fournissent du contenu correspondant à l'emplacement auquel appartient l'utilisateur.
- L'application doit connaître l'adresse IP du client pour vérifier que la demande provient d'une source fiable.
- Parfois, même si un serveur d'applications n'a pas besoin de l'adresse IP du client, un pare-feu placé entre le serveur d'applications et Citrix ADC peut avoir besoin de l'adresse IP du client pour filtrer le trafic.

Activez le mode Use IP source (USIP) si vous souhaitez que Citrix ADC utilise l'adresse IP du client pour la communication avec les serveurs.

La figure suivante montre comment l'appliance utilise les adresses IP en mode USIP.

Avant de commencer

Avant d'activer le mode USIP, notez les points suivants :

- Activez USIP dans les situations suivantes :
  - Équilibrage de charge des serveurs IDS (Intrusion Detection System)
  - Équilibrage de charge SMTP
  - Basculement de connexion sans état
  - Équilibrage de charge sans session
  - Si vous utilisez le mode Direct Server Return (DSR)
- Le paramètre global USIP s'applique uniquement aux services créés après la création du paramètre global USIP. En d'autres termes, le paramètre global USIP ne s'applique pas aux services existants lorsque le paramètre global USIP est défini. Par exemple, la désactivation globale d'USIP ne désactive pas USIP sur les services existants. Mais cela empêche les services créés ultérieurement d'avoir USIP activé automatiquement.

  Pour activer ou désactiver USIP sur un ensemble de services existants, vous devez activer ou désactiver USIP sur chacun de ces services.
- Lorsque USIP est activé, vous devez définir la Gateway du serveur sur l'une des adresses IP appartenant à Citrix ADC (de type IP de sous-réseau (SNIP) afin que la réponse du serveur passe toujours par l'appliance Citrix ADC.
- Si vous activez USIP, définissez le délai d'inactivité pour les connexions serveur sur une valeur inférieure à la valeur par défaut, afin que les connexions inactives soient effacées rapidement du côté serveur.
- Pour la redirection transparente du cache, si vous activez USIP, activez également L2CONN.
- Étant donné que les connexions HTTP ne sont pas réutilisées lorsque USIP est activé, un grand nombre de connexions côté serveur peuvent s'accumuler. Les connexions au serveur inactif peuvent bloquer les connexions pour d'autres clients. Par conséquent, définissez des limites sur le nombre maximal de connexions à un service. Citrix recommande également de définir la valeur de délai d'expiration du serveur HTTP, pour un service sur lequel USIP est activé, sur une valeur inférieure à la valeur par défaut, afin que les connexions inactives soient effacées rapidement du côté serveur.
- Comme alternative au mode USIP, vous avez la possibilité d'insérer l'adresse IP (CIP) du client dans l'en-tête de requête de la connexion côté serveur pour un serveur d'applications qui a besoin de l'adresse IP du client.
- Dans les versions antérieures de Citrix ADC, le mode USIP avait les options de port source suivantes pour les connexions côté serveur :

- **Utilisez le port du client**. Avec cette option, les connexions ne peuvent pas être réutilisées. Pour chaque requête du client, une nouvelle connexion est établie avec le serveur physique.
- **Utiliser le port proxy**. Avec cette option, la réutilisation de la connexion est possible pour toutes les demandes du même client.

Dans les versions ultérieures de Citrix ADC, si USIP est activé, la valeur par défaut est d'utiliser un port proxy pour les connexions côté serveur et de ne pas réutiliser les connexions. Le fait de ne pas réutiliser les connexions peut ne pas affecter la vitesse d'établissement des connexions.

Par défaut, l'option Utiliser le port proxy est activée si le mode USIP est activé.

Remarque : Si vous activez le mode USIP, il est recommandé d'activer l'option Utiliser le port proxy.

Pour plus d'informations sur l'option Utiliser le port proxy, voir Configurer le port source pour les connexions côté serveur.

Étapes de configuration

Activez le mode Use IP source (USIP) si vous souhaitez que Citrix ADC utilise l'adresse IP du client pour la communication avec les serveurs. Par défaut, le mode USIP est désactivé. Le mode USIP peut être activé globalement sur Citrix ADC ou sur un service spécifique. Si vous l'activez globalement, USIP est activé par défaut pour tous les services créés ultérieurement. Si vous activez USIP pour un service spécifique, l'adresse IP du client est utilisée uniquement pour le trafic dirigé vers ce service.

Procédures CLI

Pour activer ou désactiver globalement le mode USIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- **enable ns mode USIP**
- **disable ns mode USIP**

Pour activer le mode USIP pour un service à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

set service <name>@ -**usip** (**YES** | **NON**)

Exemple :

```
1 > set service Service-HTTP-1 -usip YES
2 Done
3 <!--NeedCopy-->
```


Procédures GUI

Pour activer ou désactiver globalement le mode USIP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, dans le groupe **Modes et fonctionnalités**, cliquez sur **Modifier les modes** .
2. Sélectionnez ou désactivez l'option **Utiliser l'adresse IP source** .

Pour activer le mode USIP pour un service à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services** et modifiez un service.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres du service**et sélectionnez **Utiliser l'adresse IP source**.

Configuration de la traduction d'adresses réseau

January 21, 2021

La traduction d'adresses réseau (NAT) implique la modification des adresses IP source et/ou destination et/ou des numéros de port TCP/UDP des paquets IP qui passent par l'appliance Citrix ADC. L'activation de NAT sur l'appliance améliore la sécurité de votre réseau privé et le protège d'un réseau public tel qu'Internet, en modifiant les adresses IP source de vos réseaux lorsque les données passent par Citrix ADC. En outre, avec l'aide d'entrées NAT, l'ensemble de votre réseau privé peut être représenté par quelques adresses IP publiques partagées. Le Citrix ADC prend en charge les types de traduction d'adresses réseau suivants :

- **NAT entrant (NAT).** Citrix ADC remplace l'adresse IP de destination dans les paquets générés par le client par l'adresse IP privée du serveur.
- **NAT inverse (RNAT).** Citrix ADC remplace l'adresse IP source dans les paquets générés par les serveurs par les adresses IP NAT publiques.

Traduction d'adresses réseau entrantes

August 20, 2021

Lorsqu'un client envoie un paquet à une appliance Citrix ADC configurée pour la traduction d'adresses réseau entrantes (INAT), l'appliance convertit l'adresse IP de destination publique du paquet en adresse IP de destination privée et transfère le paquet au serveur à cette adresse.

Les configurations suivantes sont prises en charge :

- **Mappage IPv4-IPv4** : une adresse IPv4 publique sur l'appliance Citrix ADC écoute les demandes de connexion au nom d'un serveur IPv4 privé. L'appliance Citrix ADC convertit l'adresse IP de destination publique du paquet en adresse IP de destination du serveur. Ensuite, l'appliance transmet le paquet au serveur à cette adresse.
- **Mappage IPv4-IPv6** : une adresse IPv4 publique sur l'appliance Citrix ADC écoute les demandes de connexion au nom d'un serveur IPv6 privé. L'appliance Citrix ADC crée un paquet de requête IPv6 avec l'adresse IP du serveur IPv6 comme adresse IP de destination.
- **Mappage IPv6-IPv4** : une adresse IPv6 publique sur l'appliance Citrix ADC écoute les demandes de connexion au nom d'un serveur IPv4 privé. L'appliance Citrix ADC crée un paquet de requête IPv4 avec l'adresse IP du serveur IPv4 comme adresse IP de destination.
- **Mappage IPv6-IPv6** : une adresse IPv6 publique sur l'appliance Citrix ADC écoute les demandes de connexion au nom d'un serveur IPv6 privé. L'appliance Citrix ADC convertit l'adresse IP de destination publique du paquet en adresse IP de destination du serveur. Ensuite, l'appliance transmet le paquet au serveur à cette adresse.

Lorsque l'appliance transfère un paquet à un serveur, l'adresse IP source attribuée au paquet est déterminée comme suit :

- Si le mode USNIP (USNIP) est activé et si le mode USIP source est désactivé, l'appliance utilise une adresse IP de sous-réseau (SNIP) comme adresse IP source.
- Si le mode USIP est activé et que le mode USNIP est désactivé, l'appliance utilise l'adresse IP du client (CIP) comme adresse IP source.
- Si les deux modes USIP et USNIP sont activés, le mode USIP est prioritaire.
- Vous pouvez également configurer Citrix ADC pour qu'il utilise une adresse IP unique comme adresse IP source, en définissant le paramètre ProxyIP.
- Si aucun des modes ci-dessus n'est activé et qu'une adresse IP unique n'a pas été spécifiée, Citrix ADC tente d'utiliser un MIP comme adresse IP source.
- Si les modes USIP et USNIP sont activés et qu'une adresse IP unique a été spécifiée, l'ordre de priorité est le suivant : USIP-unique IP-USNIP-MIP-Error.

Pour protéger Citrix ADC contre les attaques DoS, vous pouvez activer le proxy TCP. Toutefois, si d'autres mécanismes de protection sont utilisés dans votre réseau, vous pouvez les désactiver.

Configurer les règles INAT

Vous pouvez créer, modifier ou supprimer une entrée INAT.

Procédures CLI

Pour créer une entrée INAT à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour créer une entrée INAT et vérifier sa configuration :

- **add inat** <name><publicIP><privateIP>[-**tcpproxy** (**ACTIVÉ** | **DÉSACTIVÉ**)] [-**ftp** (**ACTIVÉ** | **DÉSACTIVÉ**)] [-**usip** (**ON** | **OFF**)] [-**usnip** (****ACTIVÉ** | OFF**)] [-**ProxyIP** ** \< ip_addr **ipv6_addr>**]
- **Afficher dans** []<name>

Exemple :

```
> add inat ip4-ip4 172.16.1.2 192.168.1.1 -proxyip 10.102.29.171
 Done
<!--NeedCopy-->
```

Pour modifier une entrée INAT à l'aide de l'interface de ligne de commande :

Pour modifier une entrée INAT, tapez la commande `set inat`, le nom de l'entrée et les paramètres à modifier, avec leurs nouvelles valeurs.

Pour supprimer une configuration INAT à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **rm inat** <name>

Exemple :

```
> rm inat ip4-ip4
 Done
<!--NeedCopy-->
```

Procédures GUI

Pour configurer une entrée INAT à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Itinéraires** > **INAT**, puis ajoutez une entrée INAT ou modifiez une entrée INAT existante.

Pour supprimer une configuration INAT à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Itinéraires** > **INAT**, supprimez la configuration INAT.

Basculement de connexion pour les règles INAT

Le basculement de connexion ou la mise en miroir des connexions permet au nœud principal de dupliquer les informations de connexion et de persistance vers le nœud secondaire dans une haute disponibilité. Les informations d'état de la connexion sont partagées régulièrement avec le nœud secondaire lorsque la mise en miroir de connexion est activée.

L'activation du basculement de connexion offre plus de fiabilité, mais cela se fait au coût d'un temps système utilisé pour partager les informations d'état. Les données de connexion sont synchronisées

avec l'unité de secours avec chaque mise à jour de l'état de paquet ou de flux. Par conséquent, il ne doit être utilisé que dans des endroits où la fiabilité du niveau de connexion est d'une importance primordiale.

Les configurations haute disponibilité de l'appliance Citrix ADC prennent en charge le basculement de connexion pour les connexions INAT. Le nœud principal envoie des mappages INAT et d'autres informations de connexion liées à INAT au nœud secondaire à intervalles réguliers. L'appliance secondaire utilise les informations de mappage et de connexion uniquement en cas de basculement.

Lorsqu'un basculement se produit, le nouveau nœud principal dispose d'informations sur les connexions INAT établies avant le basculement. Par conséquent, il continue à servir ces connexions même après le basculement.

Du point de vue du client, le basculement est transparent. Pendant la période de transition, le client et le serveur peuvent rencontrer une brève interruption et retransmissions. Le basculement de connexion peut être activé par règle INAT.

Pour activer le basculement de connexion sur une règle INAT, vous activez le paramètre `connFailover` de cette règle RNAT spécifique à l'aide de l'interface de ligne de commande.

Procédure CLI

Pour activer le basculement de connexion pour une règle INAT à l'aide de l'interface de ligne de commande :

Pour activer le basculement de connexion lors de l'ajout d'une règle INAT, tapez à l'invite de commandes :

- **add inat** <name><publicIP><privateIP>[-**tcpproxy** (**ACTIVÉ** | **DÉSACTIVÉ**)] [-**ftp** (**ACTIVÉ** | **DÉSACTIVÉ**)] [-**usip** (**ON** | **OFF**)] [-**usnip** (****ACTIVÉ** | OFF**)] [-**ProxyIP** \ <ip_addr|ipv6_addr] -**connfailover** (**ACTIVÉ** | **DÉSACTIVÉ**)
- **montrer inat** <name>

Pour activer le basculement de connexion lors de la modification d'une règle INAT existante, tapez à l'invite de commandes :

- **set inat -connfailover** (**ENABLED** | **DISABLED**)
- **montrer inat** <name>

Coexistence d'INAT et de serveurs virtuels

January 21, 2021

Si INAT et RNAT sont tous deux configurés, la règle INAT a priorité sur la règle RNAT. Si RNAT est configuré avec une adresse IP de traduction d'adresses réseau (IP NAT), l'adresse IP NAT est sélectionnée comme adresse IP source pour ce client RNAT.

L'adresse IP de destination publique par défaut dans une configuration INAT est l'adresse IP virtuelle (VIP) du périphérique Citrix ADC. Les serveurs virtuels utilisent également des VIP. Lorsque INAT et un serveur virtuel utilisent la même adresse IP, la configuration Vserver remplace la configuration INAT.

Voici quelques exemples de scénarios de configuration et leurs effets.

Incident	Résultats
Vous avez configuré un serveur virtuel et un service pour envoyer directement au serveur tous les paquets de données reçus sur un port Citrix ADC spécifique. Vous avez également configuré INAT et activé TCP. La configuration d'INAT de cette manière envoie tous les paquets de données reçus via un moteur TCP avant de les envoyer au serveur.	Tous les paquets reçus sur Citrix ADC, à l'exception de ceux reçus sur le port spécifié, passent par le moteur TCP.
Vous avez configuré un serveur virtuel et un service pour envoyer au serveur tous les paquets de données de type TCP, qui sont reçus sur un port spécifique sur Citrix ADC, après avoir passé par le moteur TCP. Vous avez également configuré INAT et désactivé TCP. La configuration d'INAT de cette manière envoie les paquets de données reçus directement au serveur.	Seuls les paquets reçus sur le port spécifié passent par le moteur TCP.
Vous avez configuré un serveur virtuel et un service pour envoyer tous les paquets de données reçus à l'un ou l'autre des deux serveurs. Vous tentez de configurer INAT pour envoyer tous les paquets de données reçus à un autre serveur.	La configuration INAT n'est pas autorisée.

Incident	Résultats
Vous avez configuré INAT pour envoyer tous les paquets de données reçus directement à un serveur. Vous tentez de configurer un serveur virtuel et un service pour envoyer tous les paquets de données reçus à deux serveurs différents.	La configuration vserver n'est pas autorisée.

NAT46 apatride

August 20, 2021

La fonction NAT46 sans état permet la communication entre les réseaux IPv4 et IPv6 via la traduction de paquets IPv4 vers IPv6, et vice versa, sans conserver d'informations de session sur l'appliance Citrix ADC.

Pour une configuration NAT46 sans état, l'appliance convertit un paquet IPv4 en IPv6 ou un paquet IPv6 en IPv4 tel que défini dans les RFC 6145 et 2765.

Une configuration NAT46 sans état sur l'appliance Citrix ADC comporte les composants suivants :

- **Entrée INAT IPv4-IPv6.** Entrée INAT définissant une relation 1:1 entre une adresse IPv4 et une adresse IPv6. En d'autres termes, une adresse IPv4 de l'appliance écoute les demandes de connexion au nom d'un serveur IPv6. Un paquet de requête IPv4 pour cette adresse IPv4 est traduit en paquet IPv6, puis le paquet IPv6 est envoyé au serveur IPv6.

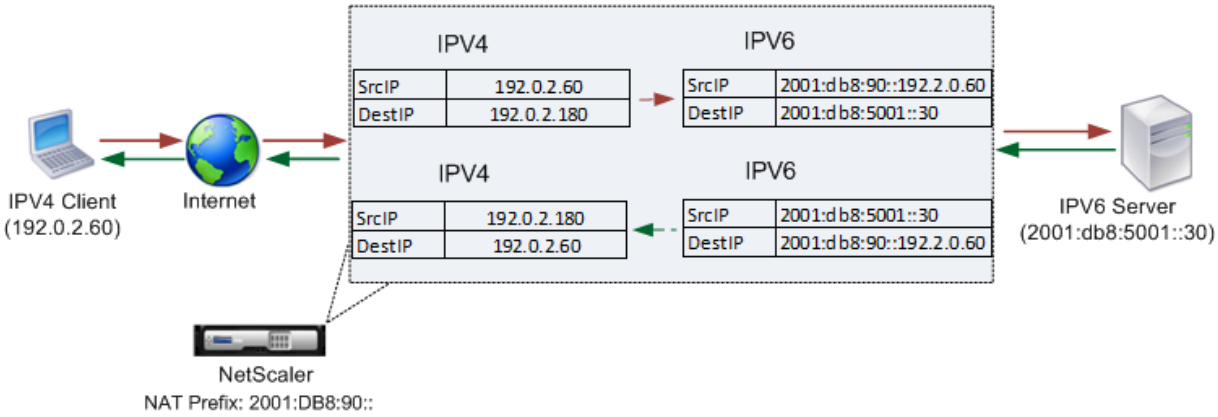
  L'appliance convertit un paquet de réponse IPv6 en paquet de réponse IPv4 dont le champ d'adresse IP source est défini comme adresse IPv4 spécifiée dans l'entrée INAT. Le paquet traduit est ensuite envoyé au client.

- **Préfixe NAT46 IPv6.** Préfixe IPv6 global de longueur 96 bits (128-32=96) configuré sur l'appliance. Lors de la traduction de paquets IPv4 en paquets IPv6, l'appliance définit l'adresse IP source du paquet IPv6 traduit sur une concaténation du préfixe IPv6 NAT46 [96 bits] et de l'adresse source IPv4 [32 bits] qui a été reçue dans le paquet de requête.

  Lors de la traduction de paquets IPv6 vers IPv4, l'appliance définit l'adresse IP de destination du paquet IPv4 traduit sur les 32 derniers bits de l'adresse IP de destination du paquet IPv6.

Prenons un exemple dans lequel une entreprise héberge le site www.example.com sur le serveur S1, qui possède une adresse IPv6. Pour activer la communication entre les clients IPv4 et le serveur IPv6 S1, l'appliance Citrix ADC NS1 est déployée avec une configuration NAT46 sans état qui inclut une entrée INAT IPv4-IPv6 pour le serveur S1 et un préfixe NAT46. L'entrée INAT inclut une adresse IPv4

à laquelle l'appliance écoute les demandes de connexion des clients IPv4 pour le compte du serveur IPv6 S1.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple :

Entités	Nom	Valeur
Adresse IP du client	Client_IPv4 (à titre de référence uniquement)	192.0.2.60
Adresse IPv6 du serveur	SEVR_IPv6 (à titre de référence uniquement)	2001:DB8:5001::30
Adresse IPv4 définie dans l'entrée INAT pour le serveur IPv6 S1	Map-SEVR-IPv4 (à titre de référence uniquement)	192.0.2.180
Préfixe IPv6 pour la traduction NAT 46	NAT46_PREFIX (à titre de référence uniquement)	2001:DB8:90::

Voici le flux de trafic dans cet exemple :

1. IPv4 Client CL1 envoie un paquet de requête à l'adresse Map-SEVR-IPv4 (192.0.2.180) sur l'appliance Citrix ADC.
2. L'appliance reçoit le paquet de requête et recherche dans les entrées INAT NAT46 l'adresse IPv6 mappée à l'adresse Map-SEVR-IPv4 (192.0.2.180). Il trouve l'adresse SEVR-IPv6 (2001:DB 8:5001::30).
3. L'appliance crée un paquet de requête IPv6 traduit avec :
   - Champ adresse IP de destination = SEVR-IPv6 = 2001:DB 8:5001::30
   - Champ d'adresse IP source = Concaténation du préfixe NAT (96 premiers bits) et client_IPv4 (32 derniers bits) = 2001:DB 8:90::192.0.2.60
4. L'appliance envoie la requête IPv6 traduite à SEVR-IPv6.
5. Le serveur IPv6 S1 répond en envoyant un paquet IPv6 à l'appliance Citrix ADC avec :

- Champ d'adresse IP de destination = Concaténation du préfixe NAT (96 premiers bits) et client_IPv4 (32 derniers bits) = 2001:DB 8:90::192.0.2.60
- Champ d'adresse IP source = SEVR-IPv6 = 2001:DB 8:5001::30

6. L'appliance reçoit le paquet de réponse IPv6 et vérifie que son adresse IP de destination correspond au préfixe NAT46 configuré sur l'appliance. Comme l'adresse de destination correspond au préfixe NAT46, l'appliance recherche dans les entrées INAT NAT46 l'adresse IPv4 associée à l'adresse SEVR-IPv6 (2001:DB 8:5001::30). Il trouve l'adresse Map-SEVR-IPv4 (192.0.2.180).
7. L'appliance crée un paquet de réponse IPv4 avec :
   - Champ d'adresse IP de destination = Préfixe NAT46 retiré de l'adresse de destination de la réponse IPv6 = Client_IPv4 (192.0.2.60)
   - Champ d'adresse IP source = adresse Map-SEVR-IPv4 (192.0.2.180)
8. L'appliance envoie la réponse IPv4 traduite au CL1 client.

Limites du NAT46 apatrides

Les restrictions suivantes s'appliquent au NAT46 apatrides :

- La traduction des options IPv4 n'est pas prise en charge.
- La traduction des en-têtes de routage IPv6 n'est pas prise en charge.
- La traduction des en-têtes d'extension hop-by-hop des paquets IPv6 n'est pas prise en charge.
- La traduction des en-têtes ESP et EH des paquets IPv4 n'est pas prise en charge.
- La traduction des paquets de multidiffusion n'est pas prise en charge.
- La traduction des en-têtes d'option de destination et des en-têtes de routage source n'est pas prise en charge.
- La traduction des paquets UDP IPv4 fragmentés qui ne contiennent pas de somme de contrôle UDP n'est pas prise en charge.

Configurer NAT46 sans état

La création des entités requises pour la configuration NAT46 sans état sur l'appliance Citrix ADC implique les procédures suivantes :

1. Créez une entrée INAT de mappage IPv4-IPv6 avec le mode sans état activé.
2. Créez un préfixe IPv6 NAT46.

Procédures CLI

Pour configurer une entrée de mappage INAT à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add inat <name> <publicIPv4> <privateIPv6> -mode STATELESS

- montrer inat <name>

Pour créer un préfixe NAT46 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- set inatparam -nat46v6Prefix <ipv6_addr|*>
- montrer inatparam

Exemple :

```
 > add inat exmpl-com-stls-nat46 192.0.2.180
2001:DB8:5001::30 -mode stateless
Done

> set inatparam -nat46v6Prefix 2001:DB8:90::/96
Done
<!--NeedCopy-->
```

Procédures GUI

Pour créer une entrée de mappage INAT à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > Itinéraires > INAT.
2. Ajoutez une nouvelle entrée INAT ou modifiez une entrée INAT existante.
3. Définissez les paramètres suivants :
   - Nom*
   - Adresse IP publique*
   - Adresse IP privée* (Activez la case à cocher IPv6 et entrez l'adresse au format IPv6.)
   - Mode (sélectionnez Stateless dans la liste déroulante.)

   * Paramètre obligatoire

Pour créer un préfixe NAT46 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Configurer les paramètres INAT**et définissez le paramètre **Préfixe**.

Définition des paramètres globaux pour NAT46 sans état

L'appliance fournit des paramètres globaux facultatifs pour les configurations NAT46 sans état.

Pour définir des paramètres globaux pour NAT46 sans état à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

set inatparam [-**Nat46 Ignoretos** (**OUI**	**NON**)] [-**Nat46ZeroChecksum** (**ACTIVÉ**	**DÉSACTIVÉ**)] [-**NAT46v6MTU**] \ <positive_integer>[-**Nat46Fragheader** (**ACTIVÉ**	**DÉSACTIVÉ**)]

-
- **montrer inatparam**

Exemple :

```
1 > set inatparam -nat46IgnoreTOS YES -nat46ZeroCheckSum DISABLED -
     nat46v6Mtu 1400 -nat46FragHeader DISABLED
2  Done
3 <!--NeedCopy-->
```

Pour définir des paramètres globaux pour NAT46 sans état à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Configurer les paramètres INAT** .

DNS64

August 20, 2021

La fonctionnalité Citrix ADC DNS64 répond avec un enregistrement DNS AAAA synthétisé à un client IPv6 envoyant une requête AAAA pour un domaine IPv4 uniquement. La fonction DNS64 est utilisée avec la fonction NAT64 pour permettre une communication transparente entre les clients IPv6 uniquement et les serveurs IPv4 uniquement. DNS64 permet la découverte du domaine IPv4 par les clients IPV6 uniquement, et NAT64 permet la communication entre les clients et les serveurs.

Pour synthétiser un enregistrement AAAA, l'appliance Citrix ADC récupère un enregistrement DNS A à partir d'un serveur DNS. Le préfixe DNS64 est un préfixe IPv6 96 bits configuré sur l'appliance Citrix ADC. L'appliance Citrix ADC synthétise l'enregistrement AAAA par concaténation du préfixe DNS64 (96 bits) et de l'adresse IPv4 (32 bits).

Pour activer la communication entre les clients IPv6 et les serveurs IPv4, une appliance Citrix ADC avec configuration DNS64 et NAT64 peut être déployée côté client IPv6 ou côté serveur IPv4. Dans les deux cas, la configuration DNS64 sur l'appliance Citrix ADC est similaire et inclut un serveur virtuel d'équilibrage de charge agissant en tant que serveur proxy pour les serveurs DNS. Si l'appliance Citrix

ADC est déployée côté client, le serveur virtuel d'équilibrage de charge doit être spécifié, sur le client IPv6, comme serveur de noms pour un domaine.

Prenons un exemple où une appliance Citrix ADC avec configuration DNS64 et NAT64 est configurée côté IPv4. Dans cet exemple, une entreprise héberge le site www.example.com sur le serveur S1, qui possède une adresse IPv4. Pour activer la communication entre les clients IPv6 et le serveur IPv4 S1, l'appliance Citrix ADC NS1 est déployée avec un DNS64 et une configuration NAT64 avec état.

La configuration DNS64 inclut le serveur virtuel d'équilibrage de charge DNS LBVS-DNS64-1, sur lequel l'option DNS64 est activée. Une stratégie DNS64 nommée DNS64-Policy-1 et une action DNS64 associée nommée DNS64-action-1 sont également configurées sur NS1, et DNS64-Policy-1 est lié à LBVS-DNS64-1. LBVS-DNS64-1 agit comme un serveur proxy DNS pour les serveurs DNS DNS-1 et DNS-2.

Lorsque le trafic arrivant à LBVS-DNS64-1 correspond aux conditions spécifiées dans DNS64-Policy-1, le trafic est traité selon les paramètres de DNS64-action-1. DNS64-action-1 spécifie le préfixe DNS64 utilisé, avec l'enregistrement A reçu d'un serveur DNS, pour synthétiser un enregistrement AAAA.

Les enregistrements de cache du paramètre DNS global sont activés sur l'appliance Citrix ADC, de sorte que l'appliance met en cache les enregistrements DNS. Ce paramètre est nécessaire pour que le DNS64 fonctionne correctement.

Le tableau suivant répertorie les paramètres utilisés dans l'exemple ci-dessus : exemples de paramètres DNS64.

Voici le flux de trafic dans cet exemple :

1. Le client IPv6 CL1 envoie une requête DNS AAAA pour l'adresse IPv6 du site www.example.com.
2. La demande est reçue par le serveur virtuel d'équilibrage de charge DNS LBVS-DNS64-1 sur l'appliance Citrix ADC NS1.
3. NS1 vérifie ses enregistrements de cache DNS pour l'enregistrement AAAA demandé et trouve que l'enregistrement AAAA pour le site www.example.com n'existe pas dans le cache DNS.
4. L'algorithme d'équilibrage de charge de LBVS-DNS64-1 sélectionne le serveur DNS DNS-1 et lui transmet la requête AAAA.
5. Étant donné que le site www.example.com est hébergé sur un serveur IPv4, le serveur DNS DNS-1 n'a pas d'enregistrement AAAA pour le site www.example.com.
6. DNS-1 envoie une réponse DNS AAAA vide ou un message d'erreur à LBVS-DNS64-1.
7. Étant donné que l'option DNS64 est activée sur LBVS-DNS64-1 et que la requête AAAA de CL1 correspond à la condition spécifiée dans DNS64-policy-1, NS1 envoie une requête DNS A à DNS-1 pour l'adresse IPv4 de www.example.com.
8. DNS-1 répond en envoyant l'enregistrement DNS A pour www.example.com à LBVS-DNS64-1. L'enregistrement A inclut l'adresse IPv4 pour www.example.com.
9. NS1 synthétise un enregistrement AAAA pour le site www.example.com avec :
    - Adresse IPv6 pour le site www.example.com = Concaténation du préfixe DNS64 (96 bits) spécifié dans DNS64action associée, et l'adresse IPv4 de l'enregistrement DNS A (32 bits)

= 2001:DB8:300::192.0.2.60

10. NS1 envoie l'enregistrement AAAA synthétisé au client IPv6 CL1. NS1 met également en cache l'enregistrement A dans sa mémoire. NS1 utilise l'enregistrement A mis en cache pour synthétiser les enregistrements AAAA pour les requêtes AAAA suivantes.

Points à prendre en compte pour une configuration DNS64

Avant de configurer DNS64 sur une appliance Citrix ADC, tenez compte des points suivants :

- La fonctionnalité DNS64 de l'appliance Citrix ADC est conforme à la RFC 6174.
- La fonctionnalité DNS64 de l'appliance Citrix ADC ne prend pas en charge DNSSEC. L'appliance Citrix ADC ne synthétise pas un enregistrement AAAA à partir d'une réponse DNSSEC reçue d'un serveur DNS. Une réponse est classée en tant que réponse DNSSEC, uniquement si elle contient des enregistrements RRSIG.
- L'appliance Citrix ADC prend en charge le préfixe DNS64 d'une longueur de 96 bits seulement.
- Bien que la fonctionnalité DNS64 soit utilisée avec la fonctionnalité NAT64, les configurations DNS64 et NAT64 sont indépendantes sur l'appliance Citrix ADC. Pour un flux particulier, vous devez spécifier la même valeur de préfixe IPv6 pour le préfixe DNS64 et les paramètres de préfixe NAT64, de sorte que les adresses IPv6 synthétisées reçues par le client soient routées vers la configuration NAT64 particulière. Pour plus d'informations sur la configuration de NAT64 sur une appliance Citrix ADC, consultez NAT64 avec état.
- Voici les différents cas de traitement DN64 par l'appliance Citrix ADC :
  - Si la réponse AAAA du serveur DNS inclut des enregistrements AAAA, chaque enregistrement de la réponse est vérifié pour l'ensemble de règles d'exclusion configuré sur l'appliance Citrix ADC pour la configuration DNS64 particulière. Citrix ADC supprime de la réponse les adresses IPv6 dont le préfixe correspond à la règle d'exclusion. Si la réponse résultante inclut au moins un enregistrement IPv6, l'appliance Citrix ADC transmet cette réponse au client, sinon l'appliance synthétise une réponse AAAA à partir de l'enregistrement A du domaine et l'envoie au client IPv6.
  - Si la réponse AAAA du serveur DNS est une réponse de réponse vide, l'appliance demande des enregistrements de ressources A portant le même nom de domaine ou recherche dans ses propres enregistrements si l'appliance est un serveur de noms de domaine authentique pour le domaine. Si la demande entraîne une réponse ou une erreur vide, la même chose est transmise au client.
  - Si la réponse du serveur DNS inclut RCODE = 1 (erreur de format), l'appliance Citrix ADC transfère la même chose au client. S'il n'y a pas de réponse avant le délai d'expiration, l'appliance Citrix ADC envoie une réponse avec RCODE = 2 (défaillance du serveur) au client.

  - Si la réponse du serveur DNS inclut un CNAME, la chaîne est suivie jusqu'à ce que l'enregistrement A ou AAAA terminant soit atteint. Si le CNAME ne possède aucun enregistrement de ressource AAAA, l'appliance Citrix ADC récupère l'enregistrement DNS A à utiliser pour synthétiser l'enregistrement AAAA. La chaîne CNAME est ajoutée à la section de réponse avec l'enregistrement AAAA synthétisé, puis envoyée au client.

- La fonctionnalité DNS64 de l'appliance Citrix ADC prend également en charge la réponse à la demande PTR. Lorsqu'une demande PTR pour un domaine d'une adresse IPv6 est reçue sur l'appliance et que l'adresse IPv6 correspond à l'un des préfixes DNS64 configurés, l'appliance crée un enregistrement CNAME mappant le domaine IP6-ARPA dans l'IN-ADDR correspondant. Le domaine ARPA et le domaine IN-ADDR.ARPA nouvellement formé est utilisé pour la résolution. L'appliance recherche les enregistrements PTR locaux et, si les enregistrements ne sont pas présents, elle envoie une demande PTR pour le domaine IN-ADDR.ARPA au serveur DNS. L'appliance Citrix ADC utilise la réponse du serveur DNS pour synthétiser la réponse pour la demande PTR initiale.

Étapes de configuration

La création des entités requises pour la configuration NAT64 avec état sur l'appliance Citrix ADC implique les procédures suivantes :

- **Ajouter des services DNS.** Les services DNS sont une représentation logique des serveurs DNS pour lesquels l'appliance Citrix ADC agit en tant que serveur proxy DNS. Pour plus d'informations sur la définition des paramètres facultatifs d'un service, voir Équilibrage de charge.
- **Ajouter une action DNS64 et une stratégie DNS64, puis liez l'action DNS64 à la stratégie DNS64.** Une stratégie DNS64 spécifie les conditions à mettre en correspondance avec le trafic pour le traitement DNS64 en fonction des paramètres de l'action DNS64 associée. L'action DNS64 spécifie le préfixe DNS64 obligatoire et les paramètres facultatifs de règle d'exclusion et de règle mappée.
- **Créez un serveur virtuel d'équilibrage de charge DNS et liez les services DNS et la stratégie DNS64 à celui-ci.** Le serveur virtuel d'équilibrage de charge DNS agit comme un serveur proxy DNS pour les serveurs DNS représentés par les services DNS liés. Le trafic arrivant sur le serveur virtuel est mis en correspondance avec la stratégie DNS64 liée pour le traitement DNS64. Pour plus d'informations sur la définition des paramètres facultatifs d'un serveur virtuel d'équilibrage de charge, voir Équilibrage de charge.

  Remarque : l'interface de ligne de commande comporte des commandes distinctes pour ces deux tâches, mais l'interface graphique les combine dans une seule boîte de dialogue.

  Activer la mise en cache des enregistrements DNS. Activez le paramètre global de l'appliance Citrix ADC pour mettre en cache les enregistrements DNS, qui sont obtenus via des opérations

de proxy DNS. Pour plus d'informations sur l'activation de la mise en cache des enregistrements DNS, voir Système de noms de domaine.

Procédures CLI

Pour créer un service de type DNS à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add service <name> <IP> <serviceType> <port> …

Pour créer une action DNS64 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- ajouter l'action DNS 64 <actionName>- Préfixe <ipv6_addr|*> [-MappeRule] <expression>[-ExcludeRule]<expression>

Pour créer une stratégie DNS64 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add dns policy64 <name> -rule <expression> -action <string>

Pour créer un serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- ajouter lb vserver <name>DNS <IPAddress><port>-dns64 (ACTIVÉ | DÉSACTIVÉ) [-ByPassaAAA (OUI | NON)]…

Pour lier les services DNS et la stratégie DNS64 au serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- bind lb vserver <name> <serviceName> …
- bind lb vserver <name> -policyName <string> -priority <positive_integer> …

Procédures GUI

Pour créer un service de type DNS à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Services, puis ajoutez un nouveau service.
2. Définissez les paramètres suivants :
   - Nom du service*
   - Serveur*
   - Protocole* (Sélectionnez DNS dans la liste déroulante.)
   - Port*

Pour créer une action DNS64 à l'aide de l'interface graphique :

Accédez à Gestion du trafic > DNS > Actions, sous l'onglet DNS Actions64, ajoutez une nouvelle action DNS64.

Pour créer une stratégie DNS64 à l'aide de l'interface graphique :

Accédez à Gestion du trafic > DNS > Stratégies, sous l'onglet DNS Policies64, ajoutez une nouvelle stratégie DNS64.

Pour créer un serveur virtuel d'équilibrage de charge DNS et lier les services DNS et la stratégie DNS64 à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels, puis ajoutez un nouveau serveur virtuel.
2. Définissez les paramètres suivants :
   - Nom*
   - Adresse IP*
   - Protocole* (Sélectionnez DNS dans la liste déroulante.)
   - Port*
3. Sélectionnez l'option Activer le DNS64.
4. Dans le volet Services, liez le service au serveur virtuel.
5. Dans le volet Stratégies, liez la stratégie au serveur virtuel.

Exemple de configuration

```
 > add service SVC-DNS-1 203.0.113.50 DNS 53
 Done

> add service SVC-DNS-2 203.0.113.60 DNS 53
 Done

> add dns Action64 DNS64-Action-1 -Prefix 2001:DB8:300::/96
 Done

> add dns Policy64 DNS64-Policy-1 -rule "CLIENT.IPv6.SRC.IN_SUBNET
   (2001:DB8:5001::/64)"
-action DNS64-Action-1
 Done

> add lb vserver LBVS-DNS64-1 DNS 2001:DB8:9999::99 53 -dns64 ENABLED
 Done

> bind lb vserver LBVS-DNS64-1 SVC-DNS-1
 Done
```



```
19
20 > bind lb vserver LBVS-DNS64-1 SVC-DNS-2
21  Done
22
23 > bind lb vserver LBVS-DNS64-1 -policyname DNS64-Policy-1 -priority 2
24  Done
25
26 <!--NeedCopy-->
```

Traduction NAT64 avec état

August 20, 2021

La fonction NAT64 avec état permet la communication entre les clients IPv6 et les serveurs IPv4 via la traduction de paquets IPv6 vers IPv4, et vice versa, tout en conservant les informations de session sur l'appliance Citrix ADC.

Une configuration NAT64 avec état sur l'appliance Citrix ADC comporte les composants suivants :

- **Règle NAT64** : entrée composée d'une règle ACL6 et d'un profil réseau, qui consiste en un pool d'adresses SNIP appartenant à Citrix ADC.
- **Préfixe IPv6 NAT64** : préfixe IPv6 global de longueur 96 bits (128-32=96) configuré sur l'appliance.
  Remarque : Actuellement, l'appliance Citrix ADC prend en charge un seul préfixe à utiliser couramment avec toutes les règles NAT 64.

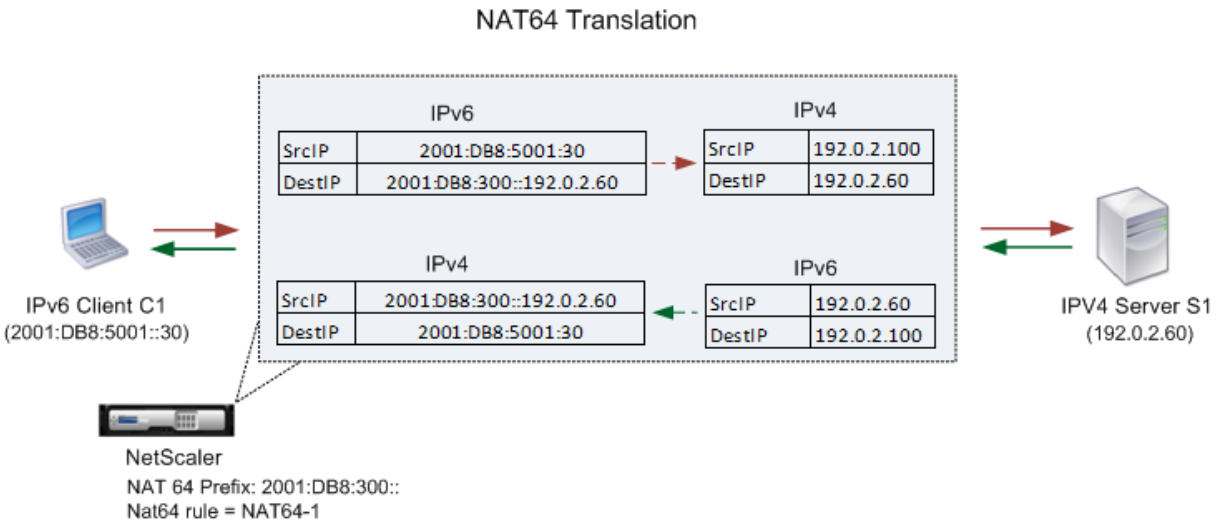
L'appliance Citrix ADC considère un paquet IPv6 entrant pour la traduction NAT64 lorsque toutes les conditions suivantes sont remplies :

- Le paquet IPv6 entrant correspond à la règle ACL6 liée à une règle NAT64.
- L'adresse IP de destination du paquet IPv6 correspond au préfixe IPv6 NAT64.

Lorsqu'un paquet de requête IPv6 reçu par l'appliance Citrix ADC correspond à une norme ACL6 définie dans une règle NAT64 et que l'adresse IP de destination du paquet correspond au préfixe IPv6 NAT64, l'appliance Citrix ADC considère le paquet IPv6 à traduire.

L'appliance convertit ce paquet IPv6 en un paquet IPv4 dont l'adresse IP source correspond à l'une des adresses IP liées au profil réseau défini dans la règle NAT64, et une adresse IP de destination composée des 32 derniers bits de l'adresse IPv6 de destination du paquet de requête IPv6. L'appliance Citrix ADC crée une session NAT64 pour ce flux particulier et transfère le paquet au serveur IPv4. Les réponses ultérieures du serveur IPv4 et les demandes du client IPv6 sont traduites en conséquence par l'appliance, sur la base des informations de la session NAT64 particulière.

Prenons un exemple dans lequel une entreprise héberge le site www.example.com sur le serveur S1, qui a une adresse IPv4. Pour activer la communication entre les clients IPv6 et le serveur IPv4 S1, l'appliance Citrix ADC NS1 est déployée avec une configuration NAT64 avec état qui inclut une règle NAT64 et un préfixe NAT64. Une adresse IPv6 mappée du serveur S1 est formée en concaténant le préfixe IPv6 NAT64 [96 bits] et l'adresse source IPv4 [32 bits]. Cette adresse IPv6 mappée est ensuite configurée manuellement dans les serveurs DNS. Les clients IPv6 obtiennent l'adresse IPv6 mappée à partir des serveurs DNS pour communiquer avec le serveur IPv4 S1.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple : exemples de paramètres de traduction NAT64 avec état.

Voici le flux de trafic dans cet exemple :

1. Le client IPv6 CL1 envoie un paquet de requête à l'adresse Map-SEVR-IPv6 (2001:DB 8:300::192.0.2.60).
2. L'appliance Citrix ADC reçoit le paquet de requête. Si le paquet de requête correspond à l'ACL6 définie dans la règle NAT64 et que l'adresse IP de destination du paquet correspond au préfixe IPv6 NAT64, Citrix ADC considère le paquet IPv6 pour la traduction.
3. L'appliance crée un paquet de requête IPv4 traduit avec :
   - Champ d'adresse IP de destination contenant le préfixe NAT64 retiré de l'adresse de destination de la requête IPv6 (SEVR_IPv4 = 192.0.2.60)
   - Champ d'adresse IP source contenant l'une des adresses IPv4 liées à Netprofile-1 (dans ce cas, 192.0.2.100)
4. L'appliance Citrix ADC crée une session NAT64 pour ce flux et envoie la requête IPv4 traduite au serveur S1.
5. Le serveur IPv64 S1 répond en envoyant un paquet IPv4 à l'appliance Citrix ADC avec :
   - Champ d'adresse IP de destination contenant 192.0.2.100

- Champ d'adresse IP source contenant l'adresse deSevr_IPv4 (192.0.2.60)

6. L'appliance reçoit le paquet de réponse IPv4, recherche toutes les entrées de session et constate que le paquet de réponse IPv6 correspond à l'entrée de session NAT64 créée à l'étape 4. L'appliance considère le paquet IPv4 pour la traduction.
7. L'appliance crée un paquet de réponse IPv6 traduit avec :
   - Destination IP address field=Client_IPv6=2001:DB8:5001::30
   - Source IP address field = Concatenation of NAT64 Prefix (First 96 bits) and Sevr_IPv4 (last 32 bits) =2001:DB8:300::192.0.2.60
8. L'appliance envoie la réponse IPv6 traduite au CL1 client.

Limites de la NAT64 avec état

Les limitations suivantes s'appliquent à la NAT64 avec état :

- La traduction des options IPv4 n'est pas prise en charge.
- La traduction des en-têtes de routage IPv6 n'est pas prise en charge.
- La traduction des en-têtes d'extension hop-by-hop des paquets IPv6 n'est pas prise en charge.
- La traduction des en-têtes ESP et EH des paquets IPv6 n'est pas prise en charge.
- La traduction des paquets de multidiffusion n'est pas prise en charge.
- Les paquets de protocole SCTP (Stream Control Transmission Protocol), DCCP (Datagram Congestion Control Protocol) et IPsec ne sont pas traduits.

Configuration de l'état NAT64

La création des entités requises pour la configuration NAT64 avec état sur l'appliance Citrix ADC implique les procédures suivantes :

1. Ajoutez une règle ACL6 avec l'action ALLOW.
2. Ajoutez un ipset, qui lie plusieurs adresses IP.
3. Ajoutez un netprofile et liez l'ipset à celui-ci. Si vous voulez lier une seule adresse IP, vous n'avez pas besoin de créer une entité ipset. Dans ce cas, liez l'adresse IP directement au netprofile.
4. Ajoutez une règle NAT64, qui inclut la liaison de la règle ACL6 et du profil réseau à la règle NAT 64.
5. Ajoutez un préfixe NAT64 IPv6.

Procédures CLI

Pour ajouter une règle ACL6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add ns acl6 <acl6name> <acl6action> …

Pour ajouter un IPSet et y lier plusieurs adresses IP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add ipset <name>
- bind ipset <name> <IPaddress …>

Pour ajouter un profil réseau à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add netprofile <name> -srcIP <IPaddress or IPset>

Pour ajouter une règle NAT64 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add nat64 <name> <acl6name> -netProfile <string>

Pour ajouter un préfixe NAT64 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- set ipv6 -natprefix <ipv6_addr|*>

Exemple :

```
 > add acl6 ACL6-1 ALLOW -srcIPv6 2001:DB8:5001::30
 Done

> apply acls6
 Done

> add ip 192.0.2.100 255.255.255.0  - type SNIP
 Done

> add ip 192.0.2.102 255.255.255.0   - type SNIP
 Done

> add ipset IPset-1
 Done

> bind ipset IPset-1 192.0.2.100 192.0.2.102
IPAddress "192.0.2.100" bound
IPAddress "192.0.2.102" bound
 Done

> add netprofile Netprofile-1 -srcIP IPset-1
 Done
```



```
23
24 > add nat64 NAT64-1 ACL6-1 -netprofile Netprofile-1
25  Done
26
27 > set ipv6 -natprefix 2001:DB8:300::/96
28  Done
29 <!--NeedCopy-->
```

Procédures GUI

Pour ajouter une règle NAT64 à l'aide de l'interface graphique :

Accédez à Système > Réseau > Routes > NAT64 et à une nouvelle règle NAT64, ou modifiez une règle existante.

Pour ajouter un préfixe NAT64 à l'aide de l'interface graphique :

Accédez à Système > Réseau, dans le groupe Paramètres, cliquez sur Configurer les paramètres INATet définissez le paramètre Préfixe.

RNAT

August 20, 2021

Dans Reverse Network Address Translation (RNAT), l'appliance Citrix ADC remplace les adresses IP source dans les paquets générés par les serveurs avec des adresses IP NAT publiques. Par défaut, l'appliance utilise une adresse SNIP comme adresse IP NAT. Vous pouvez également configurer l'appliance pour qu'elle utilise une adresse IP NAT unique pour chaque sous-réseau. Vous pouvez également configurer RNAT à l'aide des listes de contrôle d'accès (ACL). Les modes IP source (USIP), Use Subnet IP (USNIP) et LLB (Link Load Balancing) affectent le fonctionnement de RNAT. Vous pouvez afficher des statistiques pour surveiller RNAT.

Remarque : La plage de ports éphémères pour RNAT sur l'appliance Citrix ADC est 1024-65535.

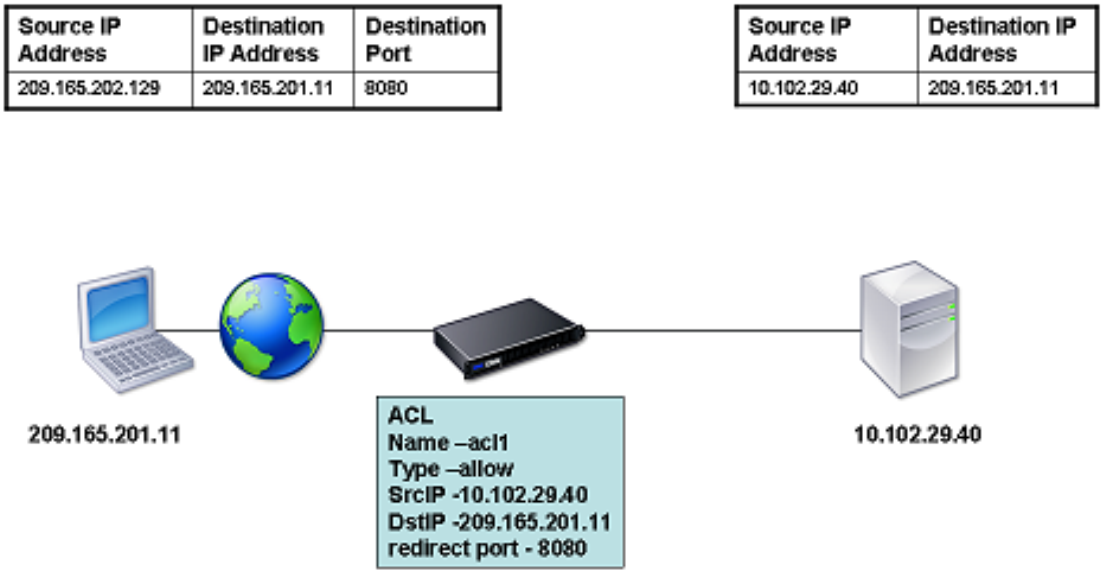
Vous pouvez utiliser une adresse réseau ou une ACL étendue comme condition pour une entrée RNAT :

- **Utilisation d'une adresse réseau.** Lorsque vous utilisez une adresse réseau, le traitement RNAT est effectué sur tous les paquets provenant du réseau spécifié.
- **Utilisation des listes ACL étendues.** Lorsque vous utilisez des ACL, le traitement RNAT est effectué sur tous les paquets qui correspondent aux ACL. Pour configurer l'appliance Citrix ADC pour qu'elle utilise une adresse IP unique pour le trafic correspondant à une liste ACL, vous devez effectuer les trois tâches suivantes :

1. Configurez l'ACL.
2. Configurez RNAT pour modifier l'adresse IP source et le port de destination.
3. Appliquez la liste ACL.

Le diagramme suivant illustre RNAT configuré avec une liste ACL.

Figure 1. RNAT avec une ACL

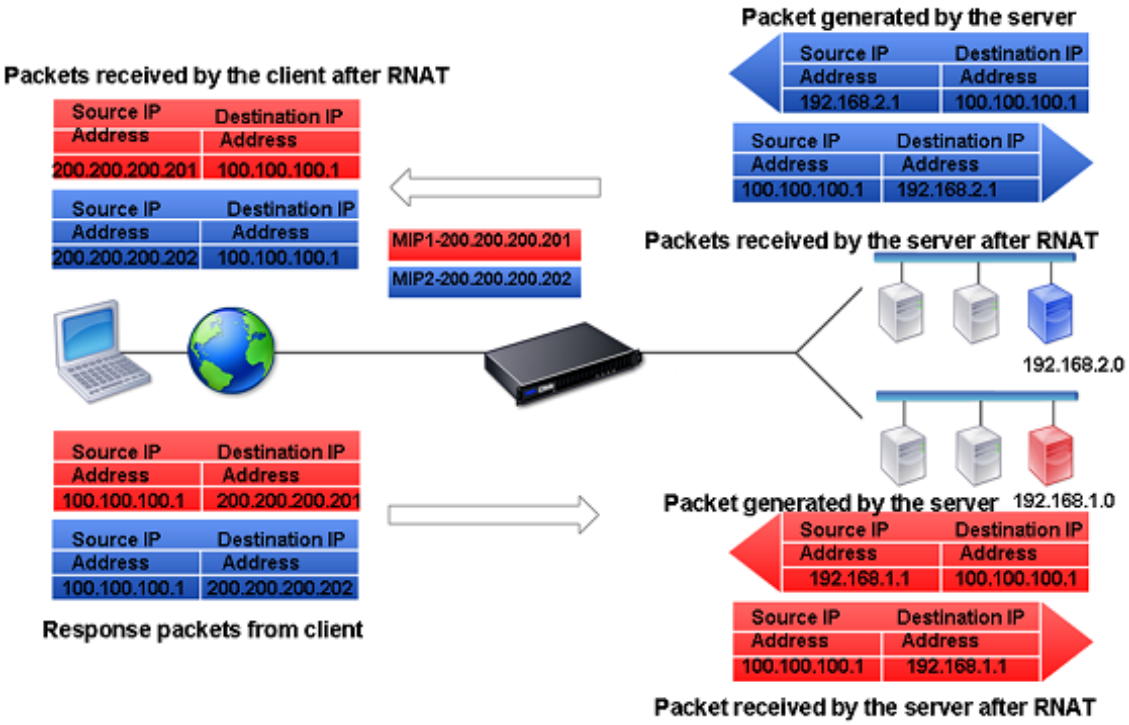


Vous avez les choix de base suivants pour le type d'adresse IP NAT :

- **Utilisation d'un SNIP comme adresse IP NAT.** Lorsque vous utilisez un SNIP comme adresse IP NAT, l'appliance Citrix ADC remplace les adresses IP source des paquets générés par le serveur par un SNIP. Par conséquent, l'adresse SNIP doit être une adresse IP publique. Si le mode Use Subnet IP (USNIP) est activé, Citrix ADC peut utiliser une adresse IP de sous-réseau (SNIP) comme adresse IP NAT.
- **Utilisation d'une adresse IP unique comme adresse IP NAT.** Lorsque vous utilisez une adresse IP unique comme adresse IP NAT, l'appliance Citrix ADC remplace les adresses IP source des paquets générés par le serveur par l'adresse IP unique spécifiée. L'adresse IP unique doit être une adresse IP publique appartenant à Citrix ADC. Si plusieurs adresses IP NAT sont configurées pour un sous-réseau, la sélection d'adresses IP NAT utilise l'algorithme Round Robin.

  Cette configuration est illustrée dans le diagramme suivant.

  Figure 2. Utilisation d'une adresse IP unique comme adresse IP NAT



Avant de commencer

Avant de configurer une règle RNAT, tenez compte des points suivants :

- Lorsque RNAT et Use Source IP (USIP) sont tous deux configurés sur l'appliance Citrix ADC, RNAT a priorité. En d'autres termes, l'adresse IP source des paquets, qui correspond à une règle RNAT, est remplacée selon le paramètre de la règle RNAT.
- Dans une topologie où l'appliance Citrix ADC effectue à la fois l'équilibrage de la charge de liaison (LLB) et le RNAT pour le trafic provenant du serveur, l'appliance sélectionne l'adresse IP source en fonction du routeur. La configuration LLB détermine la sélection du routeur. Pour plus d'informations sur LLB, reportez-vous à la section Équilibrage de charge des liaisons.

Configurer RNAT

Les instructions suivantes fournissent des procédures de ligne de commande distinctes pour créer des entrées RNAT qui utilisent différentes conditions et différents types d'adresses IP NAT. Dans l'interface graphique, toutes les variations peuvent être configurées dans la même boîte de dialogue, donc il n'y a qu'une seule procédure pour les utilisateurs de l'interface graphique.

Procédures CLI

Pour créer une règle RNAT à l'aide de l'interface de ligne de commande :

À l'invite de commandes, pour créer la règle et vérifier la configuration, tapez :

- `add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))`
- `bind rnat <name> <natIP>@ …`
- `show rnat`

Pour modifier ou supprimer une règle RNAT à l'aide de l'interface de ligne de commande :

- Pour modifier une règle RNAT :

  `set rnat <name> (<aclname> [-redirectPort <port>])`

- Pour supprimer une règle RNAT, tapez la commande.

  `rm rnat <name>`

Utilisez la commande suivante pour vérifier la configuration :

- `show rnat`

Exemples :

```
A network address as the condition and a SNIP address as the NAT IP address:

> add rnat RNAT-1 192.168.1.0 255.255.255.0
Done

A network address as the condition and a unique IP address as the NAT IP address:

> add rnat RNAT-2 192.168.1.0 255.255.255.0
Done

> bind rnat RNAT-2 -natip 10.102.29.50
Done

If instead of a single NAT IP address you specify a range, RNAT entries are created with all the Citrix ADC-owned IP addresses, except the NSIP, that fall within the range specified:

> add rnat RNAT-3 192.168.1.0 255.255.255.0
Done

> bind rnat RNAT-3 -natip 10.102.29.[50-110]
Done


An ACL as the condition and a SNIP address as the NAT IP address:
```



```
24
25 > add rnat RNAT-4 acl1
26 Done
27
28 An ACL as a condition and a unique IP address as the NAT IP address:
29
30 > add rnat RNAT-4 acl1
31 Done
32
33 > bind rnat RNAT-4 -natip 10.102.29.50
34 Done
35
36 If instead of a single NAT IP address you specify a range, RNAT entries
       are created with all the Citrix ADC-owned IP addresses, except the
      NSIP, that fall within the range specified:
37
38 > add rnat RNAT-5 acl1
39 Done
40
41 > bind rnat RNAT-5 -natip 10.102.29.[50-70]
42 Done
43
44 <!--NeedCopy-->
```

Procédures GUI

Pour créer une entrée RNAT à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **NAT**, cliquez sur l'onglet **RNAT** et ajoutez une nouvelle règle RNAT ou modifiez une règle existante.

Moniteur RNAT

Vous pouvez afficher les statistiques RNAT pour résoudre les problèmes liés à la traduction d'adresses IP.

Le tableau suivant décrit les statistiques associées à RNAT et RNAT IP.

Statistique	Description
Octets reçus	Octets reçus pendant les sessions RNAT
Octets envoyés	Octets envoyés pendant les sessions RNAT
Paquets reçus	Paquets reçus pendant les sessions RNAT

Statistique	Description
Paquets envoyés	Paquets envoyés pendant les sessions RNAT
Syn envoyé	Demandes de connexions envoyées pendant les sessions RNAT
Sessions en cours	Sessions RNAT actuellement actives

Pour afficher les statistiques RNAT à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **stat rnat**

Exemple :

```
1  > stat rnat
2
3  RNAT summary
4                                Rate (/s)            Total
5  Bytes Received                  0                    0
6  Bytes Sent                      0                    0
7  Packets Received                0                    0
8  Packets Sent                    0                    0
9  Syn Sent                        0                    0
10 Current RNAT sessions           --                   0
11  Done
12 >
13 <!--NeedCopy-->
```

Pour surveiller RNAT à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **NAT**, cliquez sur l'onglet **RNAT**, puis cliquez sur **Statistiques** .

Configurer RNAT6

Les règles RNAT (Inverse Network Address Translation) pour les paquets IPv6 sont appelées RNAT6. Lorsqu'un paquet IPv6 généré par un serveur correspond aux conditions spécifiées dans la règle RNAT6, l'appliance remplace l'adresse IPv6 source du paquet IPv6 par une adresse NAT IPv6 configurée avant de le transférer à la destination. L'adresse IPv6 NAT est l'une des adresses SNIP6 ou VIP6 appartenant à Citrix ADC.

Lors de la configuration d'une règle RNAT6, vous pouvez spécifier un préfixe IPv6 ou un ACL6 comme condition :

- **Utilisation d'une adresse réseau IPv6**. Lorsque vous utilisez un préfixe IPv6, l'appliance effectue un traitement RNAT sur les paquets IPv6 dont l'adresse IPv6 correspond au préfixe.
- **Utilisation d'ACL6**. Lorsque vous utilisez un ACL6, l'appliance effectue un traitement RNAT sur les paquets IPv6 qui correspondent aux conditions spécifiées dans l'ACL6.

Vous disposez de l'une des options suivantes pour définir l'adresse IP NAT :

- Spécifiez un ensemble d'adresses SNIP6 et VIP6 appartenant à Citrix ADC pour une règle RNAT6. L'appliance Citrix ADC utilise l'une des adresses IPv6 de cet ensemble comme adresse IP NAT pour chaque session. La sélection est basée sur l'algorithme de round robin et est effectuée pour chaque session.
- Ne spécifiez aucune adresse SNIP6 ou VIP6 appartenant à Citrix ADC pour une règle RNAT6. L'appliance Citrix ADC utilise l'une des adresses SNIP6 ou VIP6 appartenant à Citrix ADC en tant qu'adresse IP NAT. La sélection est basée sur le réseau de saut suivant auquel un paquet IPv6 correspondant à la règle RNAT est destiné.

Procédures CLI

Pour créer une règle RNAT6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, pour créer la règle et vérifier la configuration, tapez :

- **ajouter rnat6** <name>(<network>| (<acl6name>[-**RedirectPort**]<port>))
- **bind rnat6** <name> <natIP6>@ …
- **show rnat6**

Pour modifier ou supprimer une règle RNAT6 à l'aide de l'interface de ligne de commande :

- Pour modifier une règle RNAT6 dont la condition est une ACL6, tapez la commande **set rnat6** <name>, suivie d'une nouvelle valeur pour le paramètre **RedirectPort** .
- Pour supprimer une règle RNAT6, tapez la commande **clear rnat6** <name>.

Procédures GUI

Pour configurer une règle RNAT6 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **NAT**, cliquez sur l'onglet **RNAT6** et ajoutez une nouvelle règle RNAT6 ou modifiez une règle existante.

Moniteur RNAT6

Vous pouvez afficher des statistiques relatives à la fonctionnalité RNAT6 pour surveiller les performances ou pour résoudre les problèmes liés à la fonctionnalité RNAT6. Vous pouvez afficher un résumé des statistiques des règles RNAT6 ou d'une règle RNAT6 particulière. Les compteurs statistiques

reflètent les événements survenus depuis le dernier redémarrage de l'appliance Citrix ADC. Tous ces compteurs sont réinitialisés à 0 lorsque l'appliance Citrix ADC est redémarrée.

La liste suivante répertorie certains des compteurs de statistiques associés à la fonctionnalité RNAT6 :

- **Octets reçus** - Nombre total d'octets reçus pendant les sessions RNAT6.
- **Octets envoyés** - Nombre total d'octets envoyés pendant les sessions RNAT6.
- **Paquets reçus** - Nombre total de paquets reçus pendant les sessions RNAT6.
- **Paquets envoyés** - Nombre total de paquets envoyés pendant les sessions RNAT6.
- **Syn envoyé** - Nombre total de demandes de connexions envoyées pendant les sessions RNAT6
- **Sessions en cours - Sessions** RNAT6 actuellement actives

Pour afficher une synthèse des statistiques de toutes les règles RNAT6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **Stat Rnat6**

Pour afficher les statistiques d'une règle RNAT6 spécifiée à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **Commencez Rnat6** []<rnat6 rule name>

Pour afficher les statistiques RNAT6 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **NAT**, cliquez sur l'onglet **RNAT6**, puis cliquez sur **Statistiques** .

```
> stat rnat6

RNAT6 summary

                          Rate (/s)               Total

Bytes Received             178                20644

Bytes Sent                 178                20644

Packets Received            5                  401

Packets Sent                5                  401

Syn Sent                    0                    2

Current RNAT6 sessions      --                   1

Done

```



```
21 <!--NeedCopy-->
```

Heure de début du journal et raisons de fermeture de connexion dans les entrées du journal RNAT

Pour diagnostiquer ou résoudre les problèmes liés à RNAT, l'appliance Citrix ADC consigne les sessions RNAT chaque fois qu'elles sont fermées.

Un message de journal pour une session RNAT comprend les informations suivantes :

- Adresse IP appartenant à Citrix ADC (adresse NSIP ou adresse SNIP) à partir de laquelle le message de journal est source
- Horodatage de la création du journal
- Protocole de la session RNAT
- Adresse IP source
- Adresse IP RNAT
- Adresse IP de destination
- Heure de début de la session RNAT
- Heure de clôture de la session RNAT
- Nombre total d'octets envoyés par l'appliance Citrix ADC pour cette session RNAT
- Nombre total d'octets reçus par l'appliance Citrix ADC pour cette session RNAT
- Raison de la clôture de la session RNAT. L'appliance Citrix ADC consigne le motif de fermeture des sessions RNAT TCP qui n'utilisent pas le proxy TCP (proxy TCP désactivé) de l'appliance. Voici le type de raisons de fermeture enregistrées pour les sessions RNAT TCP :
  - FIN**TCP**. La session RNAT a été fermée en raison d'un FIN TCP envoyé par le périphérique source ou de destination.
  - **TCP RST**. La session RNAT a été fermée en raison d'une réinitialisation TCP envoyée par le périphérique source ou de destination.
  - **Délai d'expiration**. La session RNAT a expiré.

Le tableau suivant présente quelques exemples d'entrées de journal pour les sessions RNAT.

Type d'entrée	Exemple d'entrée de journal
Exemple d'entrée de journal pour la session RNAT UDP	Dec 1 15:28:12 10.102.53.114 12/01/2015:15:28:12 GMT 0-PPE-0 : default UDP NAT_OTHERCONN_DELINK 154 0 : Source 1.2.2.5:23431 - Destination 192.168.123.122:22 - NatIP 192.168.123.1:4045 - Destination 192.168.123.122:22 - Start Time 12/01/2015:15:26:58 GMT - Delink Time 12/01/2015:15:28:12 GMT - Total_bytes_send 2511 - Total_bytes_recv 3725
Exemple d'entrée de journal pour la session RNAT TCP. L'entrée du journal indique que la session s'est fermée en raison de la réinitialisation TCP	Dec 1 15:29:59 10.102.53.114 12/01/2015:15:27:59 GMT 0-PPE-0 : default TCP NAT_OTHERCONN_DELINK 152 0 : Source 1.2.2.5:33826 - Destination 192.168.123.122:22 - NatIP 192.168.123.1:2384 - Destination 192.168.123.122:22 - Start Time 12/01/2015:15:27:40 GMT - Delink Time 12/01/2015:15:27:59 GMT - Total_bytes_send 2147 - Total_bytes_recv 3257 - Closure Reason TCP RST
Exemple d'entrée de journal pour la session RNAT TCP. L'entrée du journal indique que la session a expiré	Dec 1 15:30:12 10.102.53.114 12/01/2015:15:30:12 GMT 0-PPE-0 : default TCP NAT_OTHERCONN_DELINK 155 0 : Source 1.2.2.5:64976 - Destination 192.168.123.115:22 - NatIP 192.168.123.1:19636 - Destination 192.168.123.115:22 - Start Time 12/01/2015:15:27:25 GMT - Delink Time 12/01/2015:15:30:12 GMT - Total_bytes_send 0 - Total_bytes_recv 0 - Closure Reason TIMEOUT

Basculement de connexion avec état pour RNAT

Le basculement de connexion permet d'éviter la perturbation de l'accès aux applications déployées dans un environnement distribué. L'appliance Citrix ADC prend désormais en charge le basculement de connexion avec état pour les connexions liées aux règles RNAT dans une configuration Citrix ADC High Availability (HA). Dans une configuration HA, le basculement de connexion (ou mise en miroir de connexion) fait référence au processus de maintien d'une connexion TCP ou UDP établie active lorsqu'un basculement se produit.

L'appliance principale envoie des messages à l'appliance secondaire afin de synchroniser les informations actuelles sur les connexions RNAT. L'appliance secondaire utilise ces informations de connexion uniquement en cas de basculement. Lorsqu'un basculement se produit, la nouvelle appliance Citrix ADC principale dispose d'informations sur les connexions établies avant le basculement et continue donc à desservir ces connexions même après le basculement. Du point de vue du client, ce basculement est transparent. Pendant la période de transition, le client et le serveur peuvent rencontrer une brève interruption et des retransmissions.

Le basculement de connexion peut être activé par règle RNAT. Pour activer le basculement de connexion sur une règle RNAT, vous activez le paramètre ConnFailover (ConnFailover de connexion) de cette règle RNAT spécifique à l'aide de la CLI ou de l'interface graphique.

Pour activer le basculement de connexion pour une règle RNAT à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- `set rnat <name> -connfailover (ENABLED | DISABLED)`
- `show rnat`

Pour activer le basculement de connexion pour une règle RNAT à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **NAT**, puis cliquez sur l'onglet **RNAT** .
2. Sélectionnez **Basculement de connexion** lors de l'ajout d'une nouvelle règle RNAT ou lors de la modification d'une règle existante.

Réservation du port source pour les connexions RNAT aux serveurs

Pour une demande atteignant une configuration RNAT dont une ou plusieurs adresses IP RNAT et le paramètre Utiliser le port proxy est désactivé, l'appliance Citrix ADC utilise l'une des adresses IP RNAT et le port source de la demande RNAT pour se connecter aux serveurs. Avant la version 13.0 47.x, la connexion RNAT (à l'aide du port source du client RNAT) au serveur échoue si le même port source est déjà utilisé dans d'autres connexions.

- **Port source inférieur à 1024**. Par défaut, l'appliance Citrix ADC réserve les 1024 premiers ports de toute adresse IP appartenant à Citrix ADC (y compris les adresses IP RNAT). Avant la version 13.0 47.x, la connexion RNAT (à l'aide du port source du client RNAT) au serveur échoue si le port source de la requête RNAT est inférieur ou égal à 1024. Avec la version 13.0 47.x, la connexion RNAT (à l'aide du port source du client RNAT) au serveur réussit même si le port source de la requête RNAT est inférieur ou égal à 1024.
- **Port source supérieur à 1024**. Avant la version 13.0 47.x, la connexion RNAT (à l'aide du port source du client RNAT) au serveur échoue si le même port source est déjà utilisé dans d'autres connexions. Avec la version 13.0 47.x, vous pouvez spécifier une plage de ports source client RNAT dans le paramètre `Retain Source Port range`

(`retainsourceportrange`) dans le cadre d'une configuration RNAT. L'appliance Citrix ADC réserve ces ports source client RNAT sur l'adresse IP RNAT pour être utilisés uniquement pour la connexion RNAT aux serveurs.

Suppression de sessions RNAT

Vous pouvez supprimer toutes les sessions RNAT indésirables ou inefficaces de l'appliance Citrix ADC. L'appliance libère immédiatement les ressources (telles que le port de l'adresse IP NAT et la mémoire) allouées à ces sessions, ce qui rend les ressources disponibles pour les nouvelles sessions. L'appliance supprime également tous les paquets suivants liés à ces sessions supprimées. Vous pouvez supprimer toutes les sessions RNAT ou sélectionnées de l'appliance Citrix ADC.

Pour effacer toutes les sessions RNAT à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **flush rnatsession**

Pour effacer les sessions RNAT sélectives à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **flush rnatsession** ((-**network** <ip_addr> -**netmask** <netmask>) | -**natIP** <ip_addr> | -**aclname** <string>)

Pour effacer toutes les sessions RNAT ou sélectives à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **NAT**, puis cliquez sur l'onglet **RNAT**.
2. Dans le menu **Actions**, cliquez sur **Vider les sessions RNAT** pour supprimer toutes les sessions RNAT ou sélectives (par exemple, supprimer les sessions RNAT avec une IP RNAT spécifique ou appartenant à une règle RNAT basée sur le réseau ou ACL spécifique).

Exemples de configurations :

```
1     Clear all RNAT sessions existing on a Citrix ADC appliance
2
3     > flush rnatsession
4
5     Done
6
7     Clear all RNAT sessions belonging to network based RNAT rules that
         has 203.0.113.0/24 network as the matching condition.
8
9     > flush rnatsession -network 203.0.113.0 -netmask 255.255.255.0
10
11    Done
12
```



```
13      Clear all RNAT sessions with RNAT IP 192.0.2.90.
14
15      > flush rnatsession -natIP 192.0.2.90
16
17      Done
18
19      Clear all RNAT sessions belonging to ACL based RNAT rules that has
           ACL-RNAT-1 as the matching condition.
20
21      > flush rnatsession -aclname ACL-RNAT-1
22
23      Done
24  <!--NeedCopy-->
```

Configuration de la traduction IPv6-IPv4 basée sur des préréglages

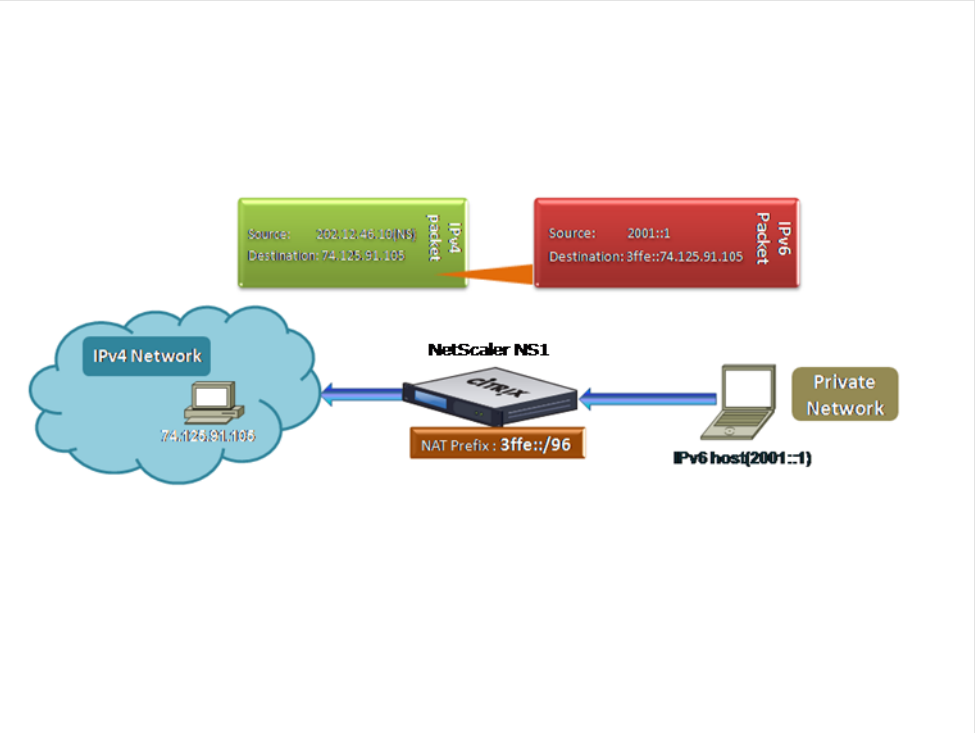
August 20, 2021

La traduction par préfixe est un processus de traduction des paquets envoyés à partir de serveurs IPv6 privés en paquets IPv4, à l'aide d'un préfixe IPv6 configuré dans l'appliance Citrix ADC. Ce préfixe a une longueur de 96 bits (128-32=96). Les serveurs IPv6 intègrent l'adresse IP de destination des serveurs ou des hôtes IPv4 dans les 32 derniers bits du champ d'adresse IP de destination des paquets IPv6. Les 96 premiers bits du champ d'adresse IP de destination sont définis comme préfixe NAT IPv6.

L'appliance Citrix ADC compare les 96 premiers bits de l'adresse IP de destination de tous les paquets IPv6 entrants au préfixe configuré. S'il existe une correspondance, l'appliance Citrix ADC génère un paquet IPv4 et définit l'adresse IP de destination comme les 32 derniers bits de l'adresse IP de destination du paquet IPv6 correspondant. Les paquets IPv6 adressés à ce préfixe doivent être routés vers Citrix ADC afin que la traduction IPv6-IPv4 soit effectuée par l'ADC Citrix.

Dans le diagramme suivant, 3ffe : :/96 est configuré comme préfixe NAT IPv6 sur Citrix ADC NS1. L'hôte IPv6 envoie un paquet IPv6 avec l'adresse IP de destination 3ffe : :74.125.91.105. NS1 compare les 96 premiers bits de l'adresse IP de destination de tous les paquets IPv6 entrants au préfixe configuré, et ils correspondent. NS1 génère ensuite un paquet IPv4 et définit l'adresse IP de destination comme 74.125.91.105.

Figure 1. Traduction par préfixe IPv6-IPv4



Pour configurer la traduction IPv6-IPv4 basée sur préfixe à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
définir le préfixe ipv6 [-natprefix \ <ipv6_addr \ *]
```

-
- show ipv6

Exemple :

```
1 > set ipv6 -natprefix 3ffe::/96
2  Done
3 <!--NeedCopy-->
```

Pour configurer la traduction IPv6-IPv4 basée sur un préfixe à l'aide de l'interface graphique :

Accédez à Système > Réseau, dans le groupe Paramètres, cliquez sur Configurer les paramètres INATet définissez le paramètre Préfixe.

NAT du préfixe IP

January 21, 2021

L'appliance Citrix ADC prend en charge la traduction d'une partie de l'adresse IP source au lieu de l'adresse complète des paquets reçus sur l'appliance. Le NAT du préfixe IP inclut la modification d'un ou plusieurs octets ou bits de l'adresse IP source.

L'appliance Citrix ADC prend en charge le préfixe IP NAT pour les configurations d'équilibrage de charge des types suivants : ANY, UDP, DNS, TCP et HTTP.

Cas d'utilisation : Zonification des clients pour un déploiement d'une appliance Citrix ADC et d'un périphérique d'optimisation

Le NAT du préfixe IP est très utile dans un déploiement qui inclut une appliance Citrix ADC et un périphérique d'optimisation (Citrix ByteMobile, par exemple). Ce type de déploiement a des réseaux clients situés géographiquement différents, qui partagent la même adresse réseau. L'appliance Citrix ADC doit envoyer le trafic reçu de chacun des réseaux clients au périphérique d'optimisation avant de le transférer à la destination.

Le périphérique renvoie le trafic optimisé à l'appliance Citrix ADC. Étant donné que l'exigence d'optimisation est différente pour le trafic de chaque réseau client, le périphérique d'optimisation doit reconnaître le réseau client de chaque paquet qu'il reçoit. La solution consiste à séparer le trafic de chaque réseau client dans une zone différente à l'aide de VLAN. Le préfixe IP NAT avec un paramètre différent est configuré pour chaque zone. L'appliance Citrix ADC traduit le dernier octet de l'adresse IP source de chaque paquet, et la valeur de l'octet traduit est différente pour chaque zone.

Prenons un exemple de deux zones, Z1 et Z2, partageant l'adresse réseau 192.0.2.0/24. Sur l'appliance Citrix ADC, les entités NAT préfixe IP nommées natrule-1 et natrule-2 sont configurées pour ces deux zones. Avant que l'appliance transfère un paquet depuis Z1, natrule-1 traduit le dernier octet de l'adresse IP source du paquet en 100. De même, pour les paquets de Z2, natrule-2 traduit le dernier octet de l'adresse IP source en 200. Pour deux clients, CL1-Z1 dans la zone Z1 et CL1-Z2 dans la zone Z2, chacun ayant une adresse IP 192.0.2.30, l'appliance Citrix ADC traduit l'adresse IP source des paquets de CL1-Z1 en 100.0.2.30 et des paquets de CL1-Z2 en 200.0.2.30. Le périphérique d'optimisation auquel l'appliance Citrix ADC envoie les paquets traduits est configuré pour utiliser l'adresse IP source d'un paquet pour reconnaître la zone, de sorte qu'il applique l'optimisation appropriée configurée pour la zone d'origine du paquet.

Étapes de configuration

La configuration du préfixe IP NAT comprend les étapes suivantes :

- **Créez un profil net et définissez le paramètre Règle NAT d'un profil net**. Une règle NAT spécifie deux adresses IP et un masque réseau. La première adresse IP (spécifiée par le paramètre Adresse IP) est l'adresse IP source qui doit être traduite avec la seconde (spécifiée par le paramètre IP Rewrite). Le masque réseau spécifie la partie de l'adresse IP source à traduire avec la même partie de la deuxième adresse IP.

- **Liez le profil net pour équilibrer la charge des serveurs virtuels ou des services**. Un profil réseau avec paramètre de règle NAT peut être lié à un serveur virtuel ou un service de type ANY, UDP, DNS, TCP et HTTP. Après avoir lié un profil réseau à un serveur ou service virtuel, l'appliance Citrix ADC correspond à l'adresse IP source des paquets entrants liés au serveur virtuel ou au service virtuel avec le paramètre de règle NAT. Citrix ADC exécute ensuite le préfixe IP NAT pour les paquets qui correspondent à la règle NAT.

Pour configurer la traduction NAT du préfixe IP à l'aide de la ligne de commande :

À l'invite de commandes, tapez :

- **bind netProfile** <name> (-**natRule** <ip_addr> <netmask> <rewriteIp>)
- **show netprofile** <name>

Pour configurer le NAT du préfixe IP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **Profils réseau**.
2. Définissez les paramètres suivants sous Règles NAT lors de l'ajout ou de la modification de Net-Profiles.
    - Adresse IP
    - Masque réseau
    - Réécrire IP

Exemple de configuration

Dans l'exemple de configuration suivant, le profil net PARTIAL-NAT-1 a des paramètres NAT de préfixe IP et est lié à l'équilibrage de charge du serveur virtuel LBVS-1, qui est de type ANY. Pour les paquets reçus sur LBVS-1 à partir de 192.0.0.0/8, l'appliance Citrix ADC traduit le dernier octet de l'adresse IP source du paquet en 100. Par exemple, un paquet avec l'adresse IP source 192.0.2.30 reçu sur LBVS-1, l'appliance Citrix ADC convertit l'adresse IP source en 100.0.2.30 avant de lui envoyer l'un des serveurs liés.

```
1 > add netprofile PARTIAL-NAT-1
2 Done
3
4 > bind netprofile PARTIAL-NAT-1  - natrule 192.0.0.0 255.0.0.0 100.0.0.0
5 Done
6
7 > add lb vserver LBVS-1 ANY 203.0.113. 61 * -netprofile PARTIAL-NAT-1
8 Done
9 <!--NeedCopy-->
```


ARP statique

August 20, 2021

Vous pouvez ajouter des entrées ARP statiques à la table ARP et les supprimer. Après avoir ajouté une entrée, vous devez vérifier la configuration. Si l'adresse IP, le port ou l'adresse MAC change après la création d'une entrée ARP statique, vous devez supprimer ou ajuster manuellement l'entrée statique. Par conséquent, la création d'entrées ARP statiques n'est pas recommandée sauf si nécessaire.

Pour ajouter une entrée ARP statique à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **ajouter une adresse IP IP arp** <ip_addr>-**mac**<mac_addr>-**ifnum** <interface_name>
- **show arp** <IPAddress>

Exemple :

```
1 > add arp -ip 10.102.29.6 -mac 00:24:e8:73:ca:ec -ifnum 1/1
2  Done
3 <!--NeedCopy-->
```

Pour supprimer une entrée ARP statique à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande **rm arp** et l'adresse IP.

Pour ajouter une entrée ARP statique à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Table ARP** et ajoutez une entrée ARP statique.

Spécifier un VLAN dans une entrée ARP statique

Dans une entrée ARP statique, vous pouvez spécifier le VLAN via lequel le périphérique de destination est accessible. Cette fonctionnalité est utile lorsque l'interface spécifiée dans l'entrée ARP statique fait partie de plusieurs VLAN balisés et que la destination est accessible via l'un des VLAN. L'appliance Citrix ADC inclut l'ID VLAN spécifié dans les paquets sortants correspondant à l'entrée ARP statique. Si vous ne spécifiez pas d'ID de VLAN dans une entrée ARP et que l'interface spécifiée fait partie de plusieurs VLAN balisés, l'appliance affecte le VLAN natif de l'interface à l'entrée ARP.

Par exemple, disons que l'interface Citrix ADC 1/2 fait partie du VLAN natif 2 et des VLAN balisés 3 et 4, et que vous ajoutez une entrée ARP statique pour le périphérique réseau A, qui fait partie du VLAN 3 et est accessible via l'interface 1/2. Vous devez spécifier le VLAN 3 dans l'entrée ARP du périphérique réseau A. L'appliance Citrix ADC inclut ensuite le VLAN 3 balisé dans tous les paquets destinés au périphérique réseau A et les envoie à partir de l'interface 1/2.

Si vous ne spécifiez pas d'ID de VLAN, l'appliance Citrix ADC attribue un VLAN 2 natif à l'entrée ARP. Les paquets destinés au périphérique A sont abandonnés dans le chemin d'accès réseau, car ils ne spécifient pas le VLAN 3 balisé, qui est le VLAN du périphérique A.

Pour spécifier un VLAN dans une entrée ARP statique à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **ajouter l'adresse IP IP** <ip_addr>**-mac**<mac_addr>**-ifnum** <interface_name>[-**vlan**]<positive_integer>
- **show arp** <IPAddress>

Exemple :

```
1 > add arp -ip 198.51.100.91 -mac 36:db:4b:f6:12:15 -ifnum 1/2 -vlan 3
2 Done
3 <!--NeedCopy-->
```

Définir le délai d'expiration pour les entrées ARP dynamiques

August 20, 2021

Vous pouvez définir globalement un délai de vieillissement (valeur de délai d'attente) pour les entrées ARP apprises dynamiquement. La nouvelle valeur s'applique uniquement aux entrées ARP qui sont apprises dynamiquement après la définition de la nouvelle valeur. Les entrées ARP existantes expirent après la période de vieillissement configurée précédemment. Vous pouvez spécifier une valeur de délai ARP comprise entre 1 et 1 200 secondes.

Pour définir le délai d'expiration des entrées ARP dynamiques à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set arpparam** -**timeout** <positive_integer>]
- **show arpparam**

Exemple :

```
1 > set arpparam -timeout 500
2  Done
3 <!--NeedCopy-->
```

Pour définir le délai d'expiration des entrées ARP dynamiques sur sa valeur par défaut à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **unset arpparam**
- **show arpparam**

Exemple :

```
> unset arpparam
 Done
<!--NeedCopy-->
```

Pour définir le délai d'expiration des entrées ARP dynamiques à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Configurer les paramètres globaux ARP** et définissez le paramètre **Délai d'expiration d'entrée de table ARP**.

Découverte de voisins

August 20, 2021

La découverte des voisins (ND) est l'un des protocoles les plus importants d'IPv6. Il s'agit d'un protocole basé sur des messages qui combine les fonctionnalités du protocole ARP (Address Resolution Protocol), ICMP (Internet Control Message Protocol) et de la découverte du routeur. ND permet aux nœuds de publier leurs adresses de couche de liens et d'obtenir les adresses MAC ou les adresses de couche de liens des nœuds voisins. Ce processus est effectué par le protocole ND6 (Neighbor Discovery Protocol).

La découverte de voisins peut effectuer les fonctions suivantes :

- **Découverte du routeur** : permet à un hôte de découvrir les routeurs locaux sur une liaison attachée et de configurer automatiquement un routeur par défaut.
- **Découverte des préfixes** : permet à l'hôte de découvrir les préfixes réseau pour les destinations locales.

  Remarque : l'appliance Citrix ADC ne prend pas en charge la découverte de préfixes.
- **Découverte des paramètres** : permet à un hôte de découvrir des paramètres d'exploitation supplémentaires, tels que MTU et la limite de saut par défaut pour le trafic sortant.
- **Configuration automatique des adresses** : permet aux hôtes de configurer automatiquement les adresses IP pour les interfaces avec et sans services de configuration des adresses avec état tels que DHCPv6. Citrix ADC ne prend pas en charge la configuration automatique des adresses pour les adresses IPv6 globales.
- **Résolution d'adresse** : Equivalent à ARP dans IPv4, permet à un nœud de résoudre l'adresse IPv6 d'un nœud voisin en son adresse de couche de liaison.

- **Détection de l'inaccessibilité des voisins** : permet à un nœud de déterminer l'état d'accessibilité d'un voisin.
- **Détection d'adresses en double** : permet à un nœud de déterminer si une adresse NSIP est déjà utilisée par un nœud voisin.
- **Redirection** : Equivalent au message IPv4 ICMP Redirection, permet à un routeur de rediriger l'hôte vers une meilleure adresse IPv6 premier saut pour atteindre une destination.

Remarque : l'appliance Citrix ADC ne prend pas en charge la redirection IPv6.

Étapes de configuration

La configuration de la découverte de voisins comporte les tâches suivantes :

- Ajout de voisins IPv6
- (Facultatif) Suppression des voisins IPv6

Procédures CLI

Pour ajouter un voisin IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **ajouter nd6** <neighbor><mac><ifnum>[-**vlan**]<integer>
- **sh nd6**

Exemple :

```
1  > add nd6 2001::1 00:04:23:be:3c:06 1/1  - vlan 1
2   Done
3
4  > show nd6
5     Neighbor                 MAC-Address(Vlan, Interface)       State
                TIME
6     --------                 ---------------------------       -----
              --------
7  1) ::1                      00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE
          PERMANENT
8  2) fe80::2d0:68ff:fe0b:58da 00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE
          PERMANENT
9  3) 2001::1                  00:04:23:be:3c:06(   1,   1/1)   REACHABLE
            STATIC
10  Done
11 <!--NeedCopy-->
```


Pour supprimer une entrée de découverte de voisin à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **rm nd6** <Neighbor> -**vlan** <VLANID>

Exemple :

```
1  rm nd6 3ffe:100:100::1 -vlan 1
2 <!--NeedCopy-->
```

Pour supprimer toutes les entrées de découverte de voisins à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **clear nd6**

Procédures GUI

Pour ajouter un voisin IPv6 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Voisins IPv6** et ajoutez un nouveau voisin IPv6.

Pour supprimer une entrée de découverte de voisin à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Voisins IPv6**, supprimez le voisin IPv6.

Pour supprimer toutes les entrées de découverte de voisins à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Voisins IPv6**, puis cliquez sur **Effacer** .

Tunnels IP

August 20, 2021

Un tunnel IP est un canal de communication, qui peut être créé à l'aide de technologies d'encapsulation, entre deux réseaux qui n'ont pas de chemin de routage. Chaque paquet IP partagé entre les deux réseaux est encapsulé dans un autre paquet, puis envoyé via le tunnel.

L'appliance Citrix ADC implémente le Tunneling IP de la manière suivante :

- **Citrix ADC as a Encapsulator (Load Balancing with DSR Mode)** : envisagez une organisation qui possède plusieurs centres de données dans différents pays, où le Citrix ADC peut être situé à un emplacement et les serveurs back-end sont situés dans un pays différent. Essentiellement, le Citrix ADC et les serveurs back-end sont sur différents réseaux et sont connectés via un routeur.

Lorsque vous configurez Direct Server Return (DSR) sur ce Citrix ADC, le paquet envoyé à partir du sous-réseau source est encapsulé par le Citrix ADC et envoyé via un routeur et un tunnel au serveur principal approprié. Le serveur principal décapsule le paquet et répond directement au client, sans permettre au paquet de passer via Citrix ADC.

- **Citrix ADC en tant que décapsulateur :** envisagez une organisation disposant de plusieurs centres de données disposant chacun d'entre eux d'un Citrix ADC et d'un serveur principal. Lorsqu'un paquet est envoyé du centre de données A au centre de données B, il est généralement envoyé via un intermédiaire, disons un routeur ou un autre Citrix ADC. Citrix ADC traite le paquet, puis transfère le paquet au serveur principal. Toutefois, si un paquet encapsulé est envoyé, Citrix ADC doit être capable de décapsuler le paquet avant de l'envoyer aux serveurs back-end. Pour permettre au Citrix ADC de fonctionner comme un décapsulateur, un tunnel est ajouté entre le routeur et le Citrix ADC. Lorsque le paquet encapsulé, avec des informations d'en-tête supplémentaires, atteint le Citrix ADC, le paquet de données est décapsulé, c'est-à-dire que les informations d'en-tête supplémentaires sont supprimées et le paquet est ensuite transféré aux serveurs back-end appropriés.

  Le Citrix ADC peut également être utilisé comme décapsulateur pour la fonctionnalité d'équilibrage de charge, en particulier dans les scénarios où le nombre de connexions sur un serveur vServer dépasse une valeur seuil et toutes les nouvelles connexions sont ensuite détournées vers un serveur vserver de sauvegarde.

Configurer les tunnels IP

La configuration des tunnels IP sur une appliance Citrix ADC consiste à créer des entités de tunnel IP. Une entité de tunnel IP spécifie les adresses IP locales et distantes du point d'extrémité du tunnel ainsi que le protocole à utiliser pour le tunnel IP.

Remarque : lors de la configuration d'un tunnel IP dans une configuration de cluster, l'adresse IP locale doit être une adresse SNIP par bandes.

Procédures CLI

Pour créer un tunnel IP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add iptunnel** <name> <remote> <remoteSubnetMask> <local> -**type** -**protocol** (**ipoverip** | **GRE**)
- **show iptunnel**

Pour supprimer un tunnel IP à l'aide de l'interface de ligne de commande :

Pour supprimer un tunnel IP, tapez la commande **rm iptunnel** et le nom du tunnel.

Pour créer un tunnel IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ip6tunnel** <name> <remoteIp> <local>
- **show ip6tunnel**

Pour supprimer un tunnel IPv6 à l'aide de l'interface de ligne de commande :

Pour supprimer un tunnel IPv6, tapez la commande **rm ip6tunnel** et le nom du tunnel.

Procédures GUI

Pour créer un tunnel IP à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Tunnels IP**, ajoutez un nouveau tunnel IP.

Pour créer un tunnel IPv6 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Tunnels IP** > **Tunnels IPv6** et ajoutez un nouveau tunnel IPv6.

Personnalisation des tunnels IP à l'échelle mondiale

En spécifiant globalement l'adresse IP source, vous pouvez attribuer une adresse IP source commune dans tous les tunnels. En outre, étant donné que la fragmentation nécessite beaucoup de CPU, vous pouvez spécifier globalement que l'appliance Citrix ADC abandonne tout paquet nécessitant une fragmentation. Sinon, si vous souhaitez fragmenter tous les paquets tant qu'une valeur de seuil CPU n'est pas atteinte, vous pouvez spécifier globalement la valeur de seuil CPU.

Procédures CLI

Pour personnaliser globalement les tunnels IP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **définir IPTunnelParam** -**SrCip** <sourceIPAddress>-**SrcIpRoundRobin** (**OUI** | **NON**) -**DropFrag** [**OUI** | **NON**] -**DropFragCPUThreshold** <Positive integer>
- **show ipTunnelParam**

Exemple :

```
1 > set iptunnelparam  - srcIP 12.12.12.22 -dropFrag Yes  -
     dropFragCpuThreshold 50
2  Done
3
4 > set iptunnelparam -srcIPRoundRobin YES -dropFrag Yes  -
     dropFragCpuThreshold 50
5  Done
6 <!--NeedCopy-->
```


Pour personnaliser globalement les tunnels IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set ip6tunnelparam** -**srcIP** <IPv6Address> -**srcIPRoundRobin** (**YES** | NO)-**dropFrag** [**OUI** | **NON**] -**dropFragCpuThreshold** <Positive integer>
- **show ip6tunnelparam**

Procédures GUI

Pour personnaliser globalement les tunnels IP à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau**, dans le groupe Paramètres, cliquez sur **Paramètres globaux du tunnel IPv4** .

1. Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Paramètres globaux du tunnel IPv6**.
2. Dans la boîte de dialogue **Configurer les paramètres globaux du tunnel IP**, définissez les paramètres.

Pour personnaliser globalement les tunnels IPv6 à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Paramètres globaux du tunnel IPv6**.
2. Dans la boîte de dialogue **Configurer les paramètres globaux du tunnel IP**, définissez les paramètres.

Options de charge utile GRE dans un tunnel IP GRE

Pour un tunnel IP GRE configuré, l'appliance Citrix ADC encapsule l'ensemble du paquet de couche 2, y compris l'en-tête Ethernet et l'en-tête VLAN (balise VLAN dot1q). Les tunnels IP GRE entre les appliances Citrix ADC et certains périphériques tiers peuvent ne pas être stables, car ces périphériques tiers ne sont pas programmés pour traiter certains ou les en-têtes de paquets de couche 2. Pour configurer un tunnel GRE IP stable entre une appliance Citrix ADC et un périphérique tiers, vous pouvez utiliser le paramètre de charge utile GRE du jeu de commandes GRE IP tunnel. Le paramètre de charge utile GRE peut également être appliqué à un GRE avec tunnel IPsec.

Vous pouvez définir le paramètre de charge utile GRE pour effectuer l'une des opérations suivantes avant l'envoi du paquet via le tunnel GRE :

- **Ethernet avec DOT1Q**. Porter l'en-tête Ethernet ainsi que l'en-tête VLAN. C'est le réglage par défaut. Pour un tunnel lié à un réseau netbridge, l'en-tête Ethernet interne et l'en-tête VLAN contiennent des informations provenant de la table ARP et pont de l'appliance Citrix ADC. Pour un tunnel défini comme saut suivant d'une règle PBR, l'adresse MAC de destination Ethernet

interne est définie sur zéro et l'en-tête VLAN spécifie le VLAN par défaut. Le paquet encapsulé (GRE) envoyé à partir du point d'extrémité du tunnel Citrix ADC a le format suivant :

Outer Ethernet Header	Outer IP Header	GRE Header	Inner Ethernet	Inner VLAN header	Inner IP/IPv6/ARP header	Inner TCP/UDP Header	Payload

- **Ethernet**. Portez l'en-tête Ethernet mais supprimez l'en-tête VLAN. Étant donné que les paquets ne transportent aucune information VLAN dans le tunnel, pour un tunnel avec ce paramètre et lié à un netbridge, vous devez lier un VLAN approprié au netbridge afin que, lors de la réception des paquets sur le tunnel, Citrix ADC puisse transférer ces paquets au VLAN spécifié. Si le tunnel est défini comme un saut suivant dans une règle PBR, Citrix ADC achemine les paquets reçus sur le tunnel. Le paquet encapsulé (GRE) envoyé à partir du point d'extrémité du tunnel Citrix ADC a le format suivant :

Outer Ethernet header	Outer IP header	GRE Header	Inner Ethernet header	Inner IP/IPv6/ARP header	Inner TCP/UDP header	Payload

- **IP**. Déposez l'en-tête Ethernet ainsi que l'en-tête VLAN. Étant donné que les tunnels avec ce paramètre ne portent pas d'en-têtes de couche 2, ces tunnels ne peuvent pas être liés à un Netbridge mais peuvent être définis comme un saut suivant dans une règle PBR. Le périphérique de point de terminaison du tunnel homologue lors de la réception du paquet consomme ou l'achemine. Le paquet encapsulé (GRE) envoyé à partir du point d'extrémité du tunnel Citrix ADC a le format suivant :

Outer Ethernet header	Outer IP header	GRE header	Inner IP/IPv6 header	Inner TCP/UDP header	Payload

Pour supprimer les en-têtes de couche 2 de paquets dans un tunnel IP GRE à l'aide de l'interface de ligne de commande :

- **ajouter IPTunnel** <name><remote><remoteSubnetMask><local>[-**protocole** \ [-**vlan**]<GRE><positive_integer>] [-**grepayload**] [-**IPsecProfileName**]\ <string>
- **show iptunnel** <tunnelname>

Exemple :

```
> add iptunnel IPTUNNEL-1 203.0.113.133 255.255.255.0 198.51.100.15 -
    protocol GRE - grepayload Ethernet -ipsecProfileName IPTUNNEL-IPSEC
    -1
Done
<!--NeedCopy-->
```


Trafic IPv6 via les tunnels GRE IPV4

L'appliance Citrix ADC prend en charge le transfert du trafic IPv6 via un tunnel IPV4 GRE. Cette fonctionnalité peut être utilisée pour activer la communication entre des réseaux IPv6 isolés sans mettre à niveau l'infrastructure IPv4 entre eux.

Pour configurer cette fonctionnalité, vous associez une règle PBR6 au tunnel GRE IPv4 configuré via lequel vous souhaitez que Citrix ADC envoie et reçoit du trafic IPv6. Les paramètres d'adresse IPv6 source et d'adresse IPv6 de destination de la règle PBR6 spécifient les réseaux IPv6 dont le trafic doit traverser le tunnel IPv4 GRE.

Remarque : le protocole IPsec n'est pas pris en charge sur les tunnels GRE IPv4 configurés pour transférer des paquets IPv6.

Pour créer un tunnel GRE IPv4 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ipTunnel** <name> <remote> <remoteSubnetMask> <local> -**protocol GRE**
- **show ipTunnel** <name>

Pour associer une règle PBR6 à un tunnel GRE IPv4 à l'aide de l'interface de ligne de commande :

- **add ns pbr6** <pbrName> **ALLOW** -**srcIPv6** <network-range> -**dstIPv6** <network-range> -**ipTunnel** <tunnelName>
- **show pbr**

Exemple de configuration

Dans l'exemple de configuration suivant, le tunnel GRE IP Tunnel-V6onv4 est créé avec l'adresse IP du point de terminaison du tunnel distant 10.10.6.30 et l'adresse IP du point de terminaison du tunnel local 10.10.5.30. Le tunnel est ensuite lié à pbr6 PBR6-v6onv4. SRCIPv6 spécifie le réseau IPv6 connecté au point de terminaison local et DestiPV6 spécifie le réseau IPv6 connecté au point de terminaison distant. Le trafic provenant de ces réseaux IPv6 est autorisé à traverser le tunnel GRE IPv4.

```
1 > add ipTunnel TUNNEL-V6onV4 10.10.6.30 255.255.255.255 10.10.5.30 -
     protocol GRE
2 -ipsecProfileName None
3 Done
4 > add ns pbr6 PBR6-V6onV4 ALLOW -srcIPv6 = 2001:0db8:1::1-2001:0db8
     :1::255 -destIPv6 =
5 1-2001:0db8:4::255 -ipTunnel TUNNEL-V6onV4
6 <!--NeedCopy-->
```


Envoyer le trafic de réponse via un tunnel IP-IP

Vous pouvez configurer une appliance Citrix ADC pour qu'elle envoie le trafic de réponse via un tunnel IP au lieu de le router vers la source. Par défaut, lorsque l'appliance reçoit une demande d'un autre Citrix ADC ou d'un périphérique tiers via un tunnel IP, elle achemine le trafic de réponse au lieu de l'envoyer via le tunnel. Vous pouvez utiliser des routes basées sur des stratégies (PBR) ou activer le transfert basé sur Mac (MBF) pour envoyer la réponse via le tunnel.

Dans une règle PBR, spécifiez les sous-réseaux aux deux points d'extrémité dont le trafic doit traverser le tunnel. Définissez également le saut suivant comme nom du tunnel. Lorsque le trafic de réponse correspond à la règle PBR, l'appliance Citrix ADC envoie le trafic via le tunnel.

Vous pouvez également activer MBF pour répondre à cette exigence, mais la fonctionnalité est limitée au trafic pour lequel l'appliance Citrix ADC stocke les informations de session (par exemple, trafic lié à l'équilibrage de charge ou aux configurations RNAT). L'appliance utilise les informations de session pour envoyer le trafic de réponse via le tunnel.

Procédures CLI

Pour créer une règle PBR et lui associer le tunnel IP-IP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns pbr** <pbr_name> **ALLOW** -**srcIP** = <local_subnet_range> -**destIP** = <remote_subnet_range> -**ipTunnel** <tunnel_name>
- **apply ns pbrs**
- **show ns pbr** <pbr_name>

Pour activer le transfert basé sur Mac à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **enable ns mode MBF**
- **afficher le mode ns**

Procédures GUI

Pour créer une règle PBR et lui associer le tunnel IP-IP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **PBR**. Sous l'onglet **PBR**, créez une règle **PBR** .
2. Lors de la création du PBR, définissez le **type de saut suivant** sur **tunnel IPet le nom** du tunnel IP sur le nom du tunnel IP configuré.

Pour activer le transfert basé sur Mac à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, dans **Modes et fonctionnalités**, cliquez sur **Configurer les modes** .

2. Sur la page **Configurer les modes**, sélectionnez **Transfert basé sur Mac** .

Exemple de configuration

Prenons un exemple de tunnel IPIP, NS1-NS2-IPIP, qui est configuré entre deux appliances Citrix ADC NS1 et NS2.

Par défaut, pour toute demande que NS2 reçoit via le tunnel, son achemine le trafic de réponse vers la source au lieu de l'envoyer (vers NS1) via le tunnel.

Vous pouvez configurer des routes basées sur des stratégies (PBR) ou activer le transfert basé sur Mac (MBF) sur NS2 pour lui permettre d'envoyer la réponse via le tunnel.

Dans l'exemple de configuration suivant sur NS2, NS1-NS2-IPIP est un tunnel IPIP et NS1-NS2-IPIP-PBR est une règle PBR. Pour les demandes (dont l'adresse IP source interne est comprise entre 10.102.147.0-10.102.147.255 et l'adresse IP de destination interne dans la plage 10.102.147.0-10.102.147.255) reçues par NS2 via le tunnel, NS2 envoie la réponse correspondante via le tunnel (vers NS1) au lieu de l'acheminer vers la source. La fonctionnalité est limitée au trafic correspondant à la règle PBR.

```
1 > add iptunnel NS1-NS2-IPIP 192.0.2.99 255.255.255.255 203.0.113.99 -
     protocol IPIP
2
3 Done
4 > add pbr NS1-NS2-IPIP-PBR -srcIP 10.102.147.0-10.102.147.255  - destIP
     10.20.1.0-10.20.1.255  - ipTunnel NS1-NS2-IPIP
5
6 Done
7 > apply pbrs
8
9 Done
```

Vous pouvez également activer MBF sur NS2. La fonctionnalité est limitée au trafic pour lequel NS2 stocke les informations de session (par exemple, le trafic lié à l'équilibrage de charge ou aux configurations RNAT).

```
1 > enable ns mode MBF
2
3 Done
```


Paquets IPv4 de classe E

January 21, 2021

Par défaut, l'appliance Citrix ADC supprime tous les paquets s'ils contiennent une adresse IPv4 de classe E dans les champs IP source ou IP de destination. Si votre installation utilise des adresses IPv4 de classe E, vous pouvez configurer l'appliance Citrix ADC pour traiter les paquets IPv4 de classe E.

Avant de commencer

Avant de commencer à configurer un dispositif Citrix ADC pour traiter les paquets IPv4 de classe E, notez les points suivants :

- Les appliances Citrix ADC ne prennent pas en charge la configuration d'une adresse IPv4 appartenant à Citrix ADC (par exemple, SNIP et VIP) dans la plage de classe E. Les appliances Citrix ADC prennent uniquement en charge le traitement des paquets IPv4 de classe E.
- Une appliance Citrix ADC utilise en interne des adresses IPv4 de classe E pour la fonctionnalité IPv6. L'appliance Citrix ADC ne prend pas en charge les deux fonctionnalités (traitement des paquets IPv4 de classe E et prise en charge IPv6) fonctionnant simultanément. L'appliance Citrix ADC impose une restriction pour ne pas activer la fonction IPv6 lorsque le traitement des paquets IPv4 de classe E est activé, et vice versa.

Étapes de configuration

La configuration d'une appliance Citrix ADC pour traiter les paquets IPv4 de classe E consiste à activer le paramètre de couche 3 des **clients d'adresse IPv4 Classe E** (**allowClassEIPv4**).

Procédures CLI

Pour configurer l'appliance Citrix ADC pour traiter les paquets IPv4 de classe E à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set l3param** -**allowClassEIPv4** (**ENABLED**|**DISABLED**)
- **show l3param**

Exemple de configuration :

```
1 > set l3param -allowClassEIPv4 ENABLED
2
3 Done
4
```



```
> sh l3param

    Network L3 related Configuration Parameters

    icmpgen_rate_threshold      : 100

    srcnat                      : ENABLED

    override_rnat               : DISABLED

    drop_df_flag                : DISABLED

    .

    .

    .

    IPv6DynamicRouting          : DISABLED

    allowClassEIPv4             : ENABLED

Done
<!--NeedCopy-->
```

Procédures GUI

Pour configurer l'appliance Citrix ADC pour traiter les paquets IPv4 de classe E à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau**, puis dans la section **Paramètres**, cliquez sur **Configurer les paramètres de couche 3**.
2. Sélectionnez les **clients d'adresse IPv4 Classe E** et cliquez sur **OK** .

Interfaces

January 21, 2021

Avant de commencer à configurer les interfaces, décidez si votre configuration peut utiliser le mode de transfert basé sur Mac et activez ou désactivez ce paramètre système en conséquence. Le nombre d'interfaces dans votre configuration est différent pour les différents modèles de l'appliance Citrix

ADC. En plus de configurer des interfaces individuelles, vous pouvez logiquement regrouper des interfaces, en utilisant des VLAN pour restreindre le flux de données au sein d'un ensemble d'interfaces, et vous pouvez regrouper des liens dans des canaux. Dans une configuration haute disponibilité, vous pouvez configurer une adresse MAC virtuelle si nécessaire. Si vous utilisez le mode L2, vous pouvez modifier l'âge de la table de pont.

Une fois la configuration terminée, décidez si vous devez activer le paramètre système pour la découverte du MTU de chemin. Les appliances Citrix ADC peuvent être déployées en mode actif à l'aide de VRRP. Un déploiement actif-actif, en plus de prévenir les temps d'arrêt, permet une utilisation efficace de toutes les appliances Citrix ADC dans le déploiement. Vous pouvez utiliser l'outil Visualizer réseau pour afficher la configuration réseau d'un déploiement de Citrix ADC et configurer des interfaces, des canaux, des VLAN et des groupes de ponts.

Configuration du transfert basé sur Mac

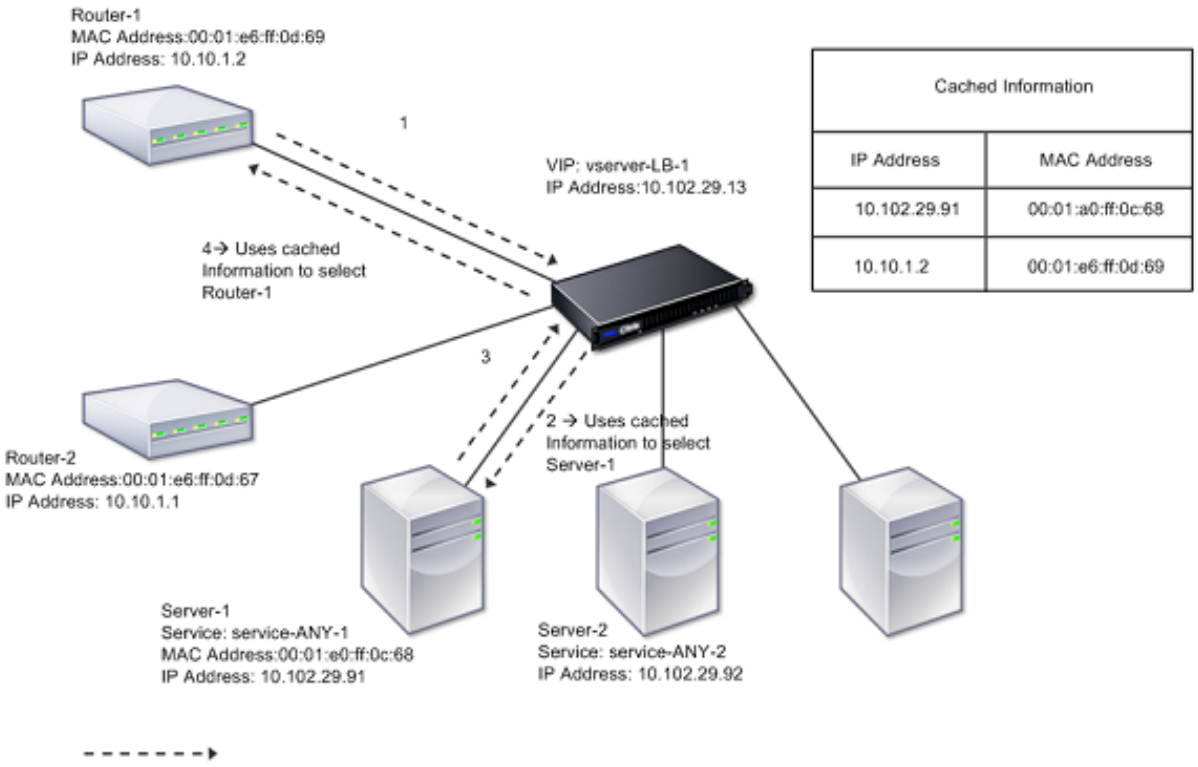
August 20, 2021

Lorsque le transfert basé sur Mac (MBF) est activé, lorsqu'une requête atteint l'appliance Citrix ADC, l'appliance se souvient de l'adresse MAC source du cadre et l'utilise comme adresse MAC de destination pour les réponses obtenues. Le transfert basé sur Mac peut être utilisé pour éviter les recherches multi-routes/ARP et pour éviter les flux de paquets asymétriques. Le transfert basé sur Mac peut être nécessaire lorsque Citrix ADC est connecté à plusieurs périphériques avec état, tels que des VPN ou des pare-feu, car il garantit que le trafic de retour est envoyé au même périphérique d'où provient le trafic initial.

Le transfert basé sur Mac est utile lorsque vous utilisez des périphériques VPN, car il garantit que tout le trafic circulant à travers un VPN passe par le même périphérique VPN.

Le diagramme topologique suivant illustre le processus de transfert basé sur Mac.

Figure 1. Mode de transfert basé sur Mac



Lorsque le transfert basé sur MAC (MBF) est activé, Citrix ADC met en cache l'adresse MAC de :

- Source (un périphérique de transmission tel que routeur, pare-feu ou périphérique VPN) de la connexion entrante.
- Serveur qui répond aux demandes.

Lorsqu'un serveur répond via l'appliance Citrix ADC, l'appliance définit l'adresse MAC de destination du paquet de réponse sur l'adresse mise en cache, en veillant à ce que le trafic circule de manière symétrique, puis transmet la réponse au client. Le processus contourne les fonctions de recherche de table de routage et de recherche ARP. Toutefois, lorsque Citrix ADC initie une connexion, il utilise les tables de routage et ARP pour la fonction de recherche. Dans une configuration de retour direct du serveur, vous devez activer le transfert basé sur Mac.

Pour plus d'informations sur les configurations de retour direct du serveur, voir Équilibrage de charge.

Certaines topologies de déploiement peuvent exiger que les chemins entrants et sortants passent par différents routeurs. Le transfert basé sur Mac romprait cette conception de topologie.

MBF devrait être désactivé dans les situations suivantes :

- **Lorsqu' un serveur utilise l'association de cartes d'interface réseau (NIC) sans utiliser LACP (802.1ad Link Aggregation).** Pour activer le transfert basé sur Mac dans ce cas, vous devez utiliser un périphérique de couche 3 entre Citrix ADC et le serveur.
  Remarque : MBF peut être activé lorsque le serveur utilise l'association de cartes réseau avec LACP, car l'interface virtuelle utilise une adresse MAC.

- **Lorsque le clustering de pare-feu est utilisé**. Le clustering de pare-feu suppose que ARP est utilisé pour résoudre l'adresse MAC du trafic entrant. Parfois, l'adresse MAC entrante peut être une adresse MAC non clusterisée et ne doit pas être utilisée pour le traitement des paquets entrants.

Lorsque MBF est désactivé, l'appliance utilise la connectivité L2 ou L3 pour transférer les réponses des serveurs aux clients. Selon la table de routage, les routeurs utilisés pour la connexion sortante et la connexion entrante peuvent être différents. En cas de trafic inverse (réponse du serveur) :

- Si la source et la destination se trouvent sur des sous-réseaux IP différents, l'appliance utilise la recherche d'itinéraire pour localiser la destination.
- Si la source se trouve sur le même sous-réseau que la destination, Citrix ADC recherche la table ARP pour localiser l'interface réseau et lui transfère le trafic. Si la table ARP n'existe pas, Citrix ADC demande les entrées ARP.

Pour activer ou désactiver le transfert basé sur Mac à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **enable ns mode MBF**
- **disable ns mode MBF**

Pour activer ou désactiver le transfert basé sur Mac à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, dans le groupe **Modes et fonctionnalités**, cliquez sur **Configurer les modes** .
2. Sélectionnez ou désactivez l'option de **transfert basé sur Mac** .

Transfert basé sur MAC pour une configuration d'équilibrage de charge

Certaines configurations d'équilibrage de charge nécessitent que l'appliance Citrix ADC contourne le MBF global (si activé) pour ces configurations et utilise plutôt les recherches Route/ARP pour envoyer des paquets vers la destination.

Le paramètre MBF d'un profil net est utilisé pour activer ou désactiver MBF pour une configuration d'équilibrage de charge spécifique. MBF peut être défini pour le côté client ainsi que pour le côté serveur d'une configuration d'équilibrage de charge en liant les profils réseau (MBF activé ou désactivé) au serveur virtuel et aux services.

Par exemple, si un profil réseau avec MBF désactivé est lié au serveur virtuel d'une configuration d'équilibrage de charge, l'appliance Citrix ADC contourne le MBF global (si activé) et utilise à la place les recherches Route/ARP pour envoyer des paquets de réponse aux clients.

Avant de commencer

Avant de commencer à configurer MBF pour une configuration d'équilibrage de charge, notez les points suivants :

- Dans une configuration d'équilibrage de charge, le côté client (serveur virtuel) et le côté serveur (groupes service/service) peuvent avoir différents paramètres MBF.
- Une configuration d'équilibrage de charge hérite du paramètre MBF global si MBF n'est pas défini explicitement dans les profils réseau liés au serveur virtuel et aux services.
- Dans une configuration d'équilibrage de charge, côté serveur (service) hérite du paramètre MBF côté client du profil net lié au serveur virtuel si aucun profil réseau n'est lié au service.
- Dans une configuration d'équilibrage de charge avec le mode de retour direct du serveur, côté client hérite du paramètre MBF dans le profil net lié au service.
- Dans une configuration de commutation de contenu, côté client prend le paramètre MBF dans le profil net lié au serveur virtuel de commutation de contenu au lieu du serveur virtuel d'équilibrage de charge cible.

Limitations

Avant de commencer à configurer MBF pour une configuration d'équilibrage de charge, notez les limitations suivantes :

- Le paramètre MBF pour les configurations d'équilibrage de charge n'est pas pris en charge dans une configuration de cluster.
- Pour un serveur virtuel d'équilibrage de charge avec les paramètres MAC ou L2Conn, MBF est activé indépendamment du paramètre MBF dans le profil réseau lié au serveur virtuel.
- L'appliance Citrix ADC ne prend pas en charge la définition de MBF pour les moniteurs d'équilibrage de charge utilisant le profil net. En d'autres termes, le paramètre MBF d'un profil net n'est pas appliqué aux moniteurs auxquels le profil net est lié. Le paramètre MBF global est appliqué aux moniteurs quel que soit le paramètre MBF du profil net lié.

Configurer MBF pour la configuration de l'équilibrage de charge

La configuration de MBF pour une configuration d'équilibrage de charge comporte les tâches suivantes :

- Activez le paramètre MBF dans un profil net.
- Liez le profil réseau à un ou plusieurs services virtuels d'équilibrage de charge.

Pour activer MBF dans un profil réseau à l'aide de l'interface de ligne de commande :

- Pour activer MBF lors de l'ajout d'un profil net, à l'invite de commandes, tapez :
  - **add netProfile** <name> -**MBF** (**ENABLED** | **DISABLED**)

  - **show netprofile** <name>
- Pour activer MBF dans un profil réseau existant, à l'invite de commandes, tapez :
  - **set netProfile** <name> -**MBF** (**ENABLED** | **DISABLED**)
  - **show netprofile** <name>

Pour activer MBF dans un profil réseau à l'aide de l'interface graphique**

1. Accédez à **Système** > **Réseau** > **Profils réseau**.
2. Activez le paramètre **MBF** lors de l'ajout ou de la modification d'un profil réseau.

Dans l'exemple de configuration suivant, le profil net NETPROFILE-MBF-LBVS a activé MBF et est lié à l'équilibrage de charge du serveur virtuel LBVS-1. En outre, le profil net NETPROFILE-MBF-SVC a activé MBF et est lié à un service d'équilibrage de charge SVC-1.

```
> add netprofile NETPROFILE-MBF-LBVS -MBF ENABLED

Done

> add netprofile NETPROFILE-MBF-SVC -MBF ENABLED

Done

> set lb vserver LBVS-1 -netprofile NETPROFILE-MBF-LBVS

Done

> set service SVC-1 -netprofile NETPROFILE-MBF-SVC

Done

<!--NeedCopy-->
```

Configurer les interfaces réseau

August 20, 2021

Les interfaces réseau de l'appliance Citrix ADC sont numérotées en notation <slot><port>. Après avoir configuré vos interfaces, affichez les interfaces et leurs paramètres pour vérifier la configuration. Vous pouvez également afficher ces informations pour résoudre un problème dans la configuration.

Pour gérer les interfaces réseau, vous pouvez effectuer les opérations suivantes :

- Activez certaines interfaces et désactivez d'autres.
- Réinitialisez une interface pour renégocier ses paramètres.

- Effacez les statistiques accumulées pour une interface.

Pour vérifier la configuration, vous pouvez afficher les paramètres de l'interface. Vous pouvez afficher les statistiques d'une interface pour évaluer son état.

Définir les paramètres de l'interface réseau

La configuration de l'interface réseau n'est ni synchronisée ni propagée. Pour une paire HA, vous devez effectuer la configuration sur chaque unité indépendamment.

Pour définir les paramètres d'interface réseau à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 -  set interface <id> [-speed <speed>] [-duplex <duplex>] [-flowControl
      <flowControl>] [-autoneg ( DISABLED | ENABLED )] [-haMonitor ( ON |
      OFF )] [ ( ON | OFF )] [-tagall ( ON | OFF )] [-lacpMode <lacpMode
     >] [-lacpKey<positive_integer>] [-lacpPriority <positive_integer>]
     [-lacpTimeout (LONG | SHORT )] [-ifAlias <string>] [-throughput <
     positive_integer>][-bandwidthHigh <positive_integer> [-
     bandwidthNormal <positive_integer>]]
2 -  show interface [<id>]
3 <!--NeedCopy-->
```

Exemple :

```
1 > set interface 1/8 -duplex full
2  Done
3 <!--NeedCopy-->
```

Pour définir les paramètres d'interface réseau à l'aide de l'interface graphique :

Accédez à **Système > Réseau > Interfaces**, sélectionnez l'interface réseau à modifier (par exemple, 1/8), cliquez sur **Modifier**, puis définissez les paramètres.

Réglage de la taille et du type de bague de réception pour une interface

Vous pouvez augmenter la taille et le type d'anneau de réception pour les interfaces IX, F1X, F2X ou F4X sur les plates-formes Citrix ADC MPX et SDX.

Une taille de bague accrue offre plus de coussin pour gérer le trafic en rafale, mais peut avoir un impact sur les performances. Une taille de bague allant jusqu'à 8192 est prise en charge pour les interfaces IX. Une taille d'anneau allant jusqu'à 4096 est prise en charge pour les interfaces F1X, F2X et F4X. La taille de bague par défaut reste 2048.

Les types d'anneau d'interface sont élastiques par défaut. Ils augmentent ou diminuent en taille en fonction du taux d'arrivée des paquets. Vous pouvez configurer le type d'anneau comme « fixe », auquel cas la taille de l'anneau ne change pas en fonction du taux de trafic.

Remarque : cette fonctionnalité est prise en charge à partir de la version 13.0 build 41.x, et prise en charge sur les plates-formes dotées d'interfaces IX, F1X, F2X ou F4X.

Utilisez la commande `show hardware` pour déterminer si votre appliance dispose d'interfaces IX, F1X, F2X ou F4X.

Exemples :

Le modèle suivant a 16 interfaces F1X (10G) et 4 interfaces F4X (40G).

```
1  > sh hardware
2          Platform: NSMPX-25000-40G 20\*CPU+16\*F1X+4\*F4X+2\*E1K+2*CVM
               N3 250040
3          Manufactured on: 12/16/2016
4          CPU: 2800MHZ
5          Host Id: 234913926
6          Serial no: N43RJCRV3X
7          Encoded serial no: N43RJCRV3X
8          Netscaler UUID: 336a32d6-2cfa-11e8-bf01-00e0ed5dd23c
9          BMC Revision: 4.08
10  Done
11 <!--NeedCopy-->
```

Le modèle suivant a 2 interfaces 1X (10G).

```
1  > sh hardware
2          Platform: NSMPX-10500 8\*CPU+2\*E1K+8\*E1K+2\*IX+8*CVM 1620
               760100
3          Manufactured on: 12/27/2010
4          CPU: 2832MHZ
5          Host Id: 1707114630
6          Serial no: 7VZZV1ZXJ4
7          Encoded serial no: 7VZZV1ZXJ4
8          Netscaler UUID: eb1bfd72-5176-11e7-ba18-00e0ed1b0d12
9  Done
10 <!--NeedCopy-->
```

Pour configurer la taille et le type d'anneau
à l'aide de l'interface de ligne de commande, tapez :

```
1  set interface <id> -ringsize <positive_integer> -ringtype ( Elastic |
       Fixed )
2  <!--NeedCopy-->
```


Paramètres :

`ringsize`:

Taille de l'anneau de réception de l'interface. Un nombre plus élevé fournit plus de tampons pour gérer le trafic entrant.

Valeur par défaut : 2048 Valeur
minimale : 512 Valeur
maximale : 16384

`ringtype`:

Type de bague de réception de l'interface. Un type d'anneau fixe préalloue le nombre configuré de tampons, quel que soit le taux de trafic. En revanche, un anneau élastique, se dilate et se rétrécit en fonction du taux de trafic entrant.

Valeurs possibles : Elastique, Fixe

Valeur par défaut : Elastic

Exemple :

```
> set interface 40/2 -ringsize 4096 -ringtype Fixed
 Done
> show interface 40/2

1)      Interface 40/2 (40G Ethernet, CR4, 40 Gbit) #21  flags=0xc020 <
    ENABLED, UP, UP, autoneg, HAMON, HEARTBEAT, 802.1q> MTU=1500, native
     vlan=10, MAC=00:e0:ed:75:14:2a, uptime 119h26m32s
        Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
           throughput 0
        Actual: media UTP, speed 40000, duplex FULL, fctl OFF,
           throughput 40000
        LLDP Mode: NONE, LR Priority: 1024
        RX: Pkts(1443972660032) Bytes(1457207315336105) Errs(0) Drops
           (53319) Stalls(0)
        TX: Pkts(1452311431262) Bytes(1458534011197761) Errs(0) Drops
           (788) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
        Rx Ring: Configured size=4096, Actual size=4096, Type: Fixed
 Done
<!--NeedCopy-->
```

La dernière ligne indique la taille de l'anneau configurée et réelle, ainsi que le type d'anneau.

Pour configurer la taille et le type d'anneau à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > Interfaces**.
2. Sélectionnez votre interface et cliquez sur **Modifier**.
3. Dans **Taille de l'anneau**, spécifiez l'une des options suivantes :
   - **Interfaces IX :** 512, 1024, 2048, 4096 ou 8192.
   - **Interfaces F1X, F2X ou F4X :** 512, 1024, 2048 ou 4096.
4. Dans **Type d'anneau**, sélectionnez Élastique ou Fixe.
5. Cliquez sur **OK**.

Activer et désactiver les interfaces réseau

Par défaut, les interfaces réseau sont activées. Désactivez toute interface réseau qui n'est pas connectée au réseau, afin qu'elle ne puisse pas envoyer ou recevoir de paquets. La désactivation d'une interface réseau connectée au réseau dans une configuration haute disponibilité peut provoquer un basculement.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité.

Pour activer ou désactiver une interface réseau à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 -  enable interface <interface_num>
2 -  show interface <interface_num>
3 -  disable interface <interface_num>
4 -  show interface <interface_num>
5 <!--NeedCopy-->
```

Exemple :

```
1  > enable interface 1/8
2   Done
3  > show interface 1/8
4          Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
5          flags=0x4004000 <ENABLED, DOWN, BOUND to LA/1, down, autoneg,
               802.1q>
6          MTU=1514, MAC=00:d0:68:15:fd:3d, downtime 906h58m40s
7          Requested: media UTP, speed AUTO, duplex FULL, fctl OFF,
               throughput 0
8          RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
9          TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
10         NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
```



```
11          Bandwidth thresholds are not set.
12 Done
13 <!--NeedCopy-->
```

Pour activer ou désactiver une interface réseau à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > Interfaces**.
2. Sélectionnez l'interface réseau et, dans la liste **Action**, sélectionnez Activer ou Désactiver.

Réinitialiser les interfaces réseau

Les paramètres de l'interface réseau contrôlent les propriétés telles que le duplex et la vitesse. Pour renégocier les paramètres d'une interface réseau, vous devez la réinitialiser.

Pour réinitialiser une interface réseau à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 -  reset interface <interface_num>
2 -  show interface <interface_num>
3 <!--NeedCopy-->
```

Exemple :

```
1 > reset interface 1/8
2  Done
3 <!--NeedCopy-->
```

Pour réinitialiser une interface réseau à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > Interfaces**.
2. Sélectionnez l'interface réseau et, dans la liste **Action**, sélectionnez **Réinitialiser l'interface** .

Surveillance d'une interface réseau

Vous pouvez afficher des statistiques d'interface réseau pour surveiller les paramètres et utiliser les informations pour vérifier l'état de l'interface réseau. Vous pouvez surveiller les paramètres, tels que les paquets envoyés et les paquets reçus, le débit, les unités de données LACP (Link Aggregate Control Protocol) et les erreurs. Vous pouvez effacer les statistiques d'une interface réseau pour surveiller ses statistiques à partir du moment où elles sont effacées.

Pour afficher les statistiques des interfaces réseau à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :


```
-  stat interface <interface_num>
<!--NeedCopy-->
```

Exemple :

```
> stat interface 1/8
 Done
<!--NeedCopy-->
```

Pour effacer les statistiques d'une interface réseau à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
-  clear interface <interface_num>
<!--NeedCopy-->
```

Exemple :

```
> clear interface 1/8
 Done
<!--NeedCopy-->
```

Pour afficher les statistiques d'une interface à l'aide de l'interface graphique :

Accédez à **Système > Réseau > Interfaces**, sélectionnez l'interface réseau et cliquez sur **Statistiques d'interface**.

Pour effacer les statistiques d'une interface réseau à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > Interfaces**.
2. Sélectionnez l'interface réseau et, dans la liste **Action**, sélectionnez **Effacer les statistiques** .

Configuration des règles de session de transfert

August 20, 2021

Par défaut, l'appliance Citrix ADC ne crée pas d'entrées de session pour le trafic qu'elle transfère uniquement (mode L3). Dans le cas où une demande client que l'appliance transmet à un serveur entraîne une réponse qui doit être renvoyée par le même chemin, vous pouvez créer une règle de session de transfert. Une règle de session de transfert crée des entrées de session de transfert pour le trafic qui provient ou est destiné à un réseau particulier et qui est transféré par Citrix ADC. Vous pouvez créer des règles de session de transfert pour le trafic IPv4 ainsi que pour le trafic IPv6.

Lors de la configuration d'une règle de session de transfert IPv4, vous pouvez spécifier une adresse réseau IPv4 ou une liste ACL étendue comme condition d'identification du trafic IPv4 pour lequel créer une entrée de session de transfert :

- **Adresse réseau**. Lorsque vous spécifiez une adresse réseau IPv4, l'appliance crée des sessions de transfert pour le trafic IPv4 dont la source ou la destination correspond à l'adresse réseau.
- **Règle ACL étendue**. Lorsque vous spécifiez une règle ACL étendue, l'appliance crée des sessions de transfert pour le trafic IPv4 qui correspondent aux conditions spécifiées dans la règle ACL étendue.

Lors de la configuration d'une règle de session de transfert IPv6, vous pouvez spécifier un préfixe IPv6 ou un ACL6 comme condition d'identification du trafic IPv6 pour lequel créer une entrée de session de transfert :

- **Préfixe IPv6**. Lorsque vous spécifiez un préfixe IPv6, l'appliance crée des sessions de transfert pour le trafic IPv6 dont la source ou la destination correspond au préfixe IPv6.
- **Règle ACL6**. Lorsque vous spécifiez une règle ACL6, l'appliance crée des sessions de transfert pour le trafic IPv6 qui correspondent aux conditions spécifiées dans la règle ACL6.

Pour créer une règle de session de transfert IPv4 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour créer une règle de session de transfert et vérifier la configuration :

- ajouter ForwardingSession <name>[\ \ ] <network><netmask>| [-aclname] <string>-connfailover (ENABLED | DISABLED)
- show forwardingSession

Exemple :

```
A network address as the condition:

> add forwardingSession fs-nw-1 10.102.105.51 255.255.255.255
 Done

An ACL as the condition:

> add forwardingSession fs-acl-1 acl1
 Done
<!--NeedCopy-->
```

Pour configurer une règle de session de transfert IPv4 à l'aide de l'interface graphique :

Accédez à Système > Réseau > Sessions de transfert, ajoutez une nouvelle session de transfert IPv4 ou modifiez une session de transfert existante.

Pour créer une règle de session de transfert IPv6 à l'aide de l'interface de ligne de commande :

- À l'invite de commandes, tapez les commandes suivantes pour créer une règle de session de transfert et vérifier la configuration :
  - ajouter ForwardingSession <name>[] <IPv6 prefix>| [-acl6name]<string>
  - show forwardingSession

  Exemple :

```
    An IPv6 prefix as the condition:

    > add forwardingSession fsv6-pfx-1 3ffe::/64
     Done

    An ACL6 rule as the condition:

    > add forwardingSession fsv6-acl6-1  -acl6name ACL6-FS
     Done
<!--NeedCopy-->
```

Pour configurer une règle de session de transfert IPv6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > Sessions de transfert, ajoutez une nouvelle session de transfert IPv6 ou modifiez une session de transfert existante.

Affectation d'une règle ACL à une règle de session de transfert existante

Vous pouvez affecter une règle ACL à une règle de session de transfert basée sur l'adresse réseau/le préfixe IPv6, auquel cas elle devient une règle de session de transfert basée sur l'ACL. Vous pouvez également modifier une règle ACL existante en une autre règle ACL dans une règle de session de transfert basée sur ACL. Une fois que les entrées de session de transfert liées existantes (le cas échéant) ont expiré, les règles commencent à utiliser la liste ACL nouvellement attribuée pour identifier le trafic IPv4/IPv6 pour lequel créer une entrée de session de transfert.

Pour affecter une règle ACL étendue à une règle de session de transfert IPv4 existante à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez

- `set forwardingSession <name> [-aclname <string>]`
- `show forwardingSession <name>`

Pour affecter une règle ACL6 à une règle de session de transfert IPv6 existante à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez

- `set forwardingSession <name> [-acl6name <string>]`

- `show forwardingSession <name>`

Exemple :

```
> add forwardingSession FS-1 -aclname ACL-9
Done

> add forwardingSession FS6-1  - acl6name ACL6-9
Done
```

Désactivation de la direction pour le transfert de sessions sur une configuration de cluster

Le comportement par défaut d'un cluster Citrix ADC est que le nœud qui reçoit du trafic (récepteur de flux) dirige le trafic vers un autre nœud (processeur de flux), qui traite le trafic. La direction du trafic du récepteur de flux vers le processeur de flux se produit sur le backplane du cluster et est appelée direction.

La direction peut être un surcoût pour le traitement en temps réel ou lorsque la configuration inclut des liaisons à latence élevée.

La direction des sessions de transfert peut désormais être désactivée afin que le traitement devienne local au récepteur de flux. Autrement dit, le récepteur de flux devient le processeur de flux.

Avant de commencer

Notez les points suivants avant de configurer les règles de session de transfert dans une configuration de cluster :

- Vous devez configurer les jeux de liens à utiliser pour le transfert de sessions.
- Vous devez activer le transfert basé sur MAC (MBF) sur la configuration du cluster.

Configuration des règles de session de transfert dans une configuration de cluster

La désactivation de la direction pour le transfert des règles de session dans une configuration de cluster peut être effectuée aux deux niveaux suivants :

- **Niveau de règle de session de transfert spécifique**. Activez le paramètre Process Local lors de l'ajout d'une nouvelle règle de session de transfert ou de la modification d'une règle de session de transfert existante.
- **Au niveau mondial**. Activez le paramètre Process Local lors de l'ajout d'une nouvelle instance de cluster ou de la modification d'une instance de cluster existante. Le paramètre global a priorité sur le paramètre de règle de session de transfert.

Procédures CLI

Pour désactiver la direction d'une règle de session de transfert sur une configuration de cluster à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants :

- Si vous ajoutez une nouvelle règle de session de transfert :
  - **add ForwardingSession** <name>(<network []<netmask>) | -**acl6name** <string>| -**aclname** <string>) -**ProcessLocal ENABLED**
  - **show forwardingSession** <name>
- Si vous reconfigurez une règle de session de transfert existante :
  - **set ForwardingSession** <name> -**ProcessLocal ENABLED**
  - **show forwardingSession** <name>

Pour désactiver la direction de toutes les règles de session de transfert (niveau global) sur une configuration de cluster à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants :

- Si vous ajoutez une nouvelle instance de cluster :
  - **add cluster instance** <clid> -**processLocal Enabled**
  - **show cluster instance** <clid>
- Si vous reconfigurez une instance de cluster existante :
  - **set cluster instance** <clid> -**processLocal Enabled**
  - **show cluster instance** <clid>

Exemple de configuration :

Voici deux exemples de désactivation de la direction au niveau de la règle de session de transfert, et un exemple de désactivation de la direction au niveau global.

```
1  An IPv4 forwarding session rule:
2
3  > add forwardingSession FWD-SESSN-PROCSS-LOCL-IPV4-1 10.102.105.51
       255.255.255.255 -processLocal Enabled
4  Done
5
6  An IPv6 forwarding session rule:
7
8  > add forwardingSession FWD-SESSN-PROCSS-LOCL-IPV6-1  - acl6name ACL6-
       FWD-SESSN-1 -processLocal Enabled
9  Done
10
```



```
A cluster setup, with an instance ID 10, has steering disabled at
    global level:

> set cluster instance 10 -processLocal Enabled
Done
<!--NeedCopy-->
```

Procédures GUI

Pour désactiver la direction d'une règle de session de transfert sur une configuration de cluster à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Sessions de transfert**, sélectionnez **Traiter local** tout en ajoutant une nouvelle règle de session de transfert ou en modifiant une règle de session de transfert existante.

Pour désactiver la direction de toutes les règles de session de transfert (niveau global) sur une configuration de cluster à l'aide de l'interface graphique :

Accédez à **Système** > **Cluster**, puis sélectionnez **Process Local** lors de l'ajout d'une configuration de cluster ou de la modification d'une configuration de cluster existante.

Présentation des VLAN

January 21, 2021

Une appliance Citrix ADC prend en charge le port de couche 2 et les VLAN balisés IEEE 802.1q. Les configurations VLAN sont utiles lorsque vous devez restreindre le trafic à certains groupes de stations. Vous pouvez configurer une interface réseau dans le cadre de plusieurs VLAN à l'aide du balisage IEEE 802.1q.

Vous pouvez configurer des VLAN et les lier à des sous-réseaux IP. Citrix ADC effectue ensuite le transfert IP entre ces VLAN (s'il est configuré comme routeur par défaut pour les hôtes de ces sous-réseaux).

Le Citrix ADC prend en charge les types de VLAN suivants :

- **VLAN basés sur les ports.** L'appartenance à un VLAN basé sur un port est définie par un ensemble d'interfaces réseau qui partagent un domaine de diffusion de couche 2 commun et exclusif. Vous pouvez configurer plusieurs VLAN basés sur des ports. Par défaut, toutes les interfaces réseau du Citrix ADC sont membres du VLAN 1.

  Si vous appliquez le balisage 802.1q au port, l'interface réseau appartient à un VLAN basé sur le port. Le trafic de couche 2 est ponté dans un VLAN basé sur un port, et les diffusions de couche 2 sont envoyées à tous les membres du VLAN si le mode de couche 2 est activé. Lorsque vous

ajoutez une interface réseau non balisée en tant que membre d'un nouveau VLAN, elle est supprimée de son VLAN actuel.

- **VLAN par défaut.** Par défaut, les interfaces réseau sur Citrix ADC sont incluses dans un seul VLAN basé sur le port en tant qu'interfaces réseau non marquées. Ce VLAN est le VLAN par défaut. Il a un ID VLAN (VID) de 1. Ce VLAN existe en permanence. Il ne peut pas être supprimé et son VID ne peut pas être modifié.

  Lorsque vous ajoutez une interface réseau à un autre VLAN en tant que membre non marqué, l'interface réseau est automatiquement supprimée du VLAN par défaut. Si vous dissociez une interface réseau de son VLAN basé sur le port actuel, elle est à nouveau ajoutée au VLAN par défaut.

- **VLAN taggés.** Le balisage 802.1q (défini dans la norme IEEE 802.1q) permet à un périphérique réseau (tel que Citrix ADC) d'ajouter des informations à une trame de couche 2 pour identifier l'appartenance au VLAN de la trame. Le balisage permet aux environnements réseau d'avoir des VLAN qui couvrent plusieurs périphériques. Un périphérique qui reçoit le paquet lit la balise et reconnaît le VLAN auquel appartient la trame. Certains périphériques réseau ne prennent pas en charge la réception de paquets balisés et non balisés sur la même interface réseau, en particulier les commutateurs Force10. Dans de tels cas, vous devez contacter le support client pour obtenir de l'aide.

  L'interface réseau peut être un membre balisé ou non marqué d'un VLAN. Chaque interface réseau est un membre non marqué d'un seul VLAN (son VLAN natif). Cette interface réseau transmet les trames du VLAN natif en tant que trames non marquées. Une interface réseau peut faire partie de plusieurs VLAN si les autres VLAN sont balisés.

  Lorsque vous configurez le balisage, assurez-vous de correspondre à la configuration du VLAN aux deux extrémités de la liaison. Le port auquel le Citrix ADC se connecte doit se trouver sur le même VLAN que l'interface réseau Citrix ADC.

  Remarque : Cette configuration de VLAN n'est ni synchronisée ni propagée, vous devez donc effectuer la configuration sur chaque unité d'une paire HA indépendamment.

Application de règles pour classer des images

Les VLAN ont deux types de règles pour classer les trames :

- **Règles d'entrée.** Les règles d'entrée classent chaque image comme appartenant à un seul VLAN. Lorsqu'une trame est reçue sur une interface réseau, les règles suivantes sont appliquées pour classer la trame :

  - Si la trame n'est pas balisée ou a une valeur de balise égale à 0, le VID de la trame est défini sur le port VID (PVID) de l'interface de réception, qui est classé comme appartenant au VLAN natif. (Les PVID sont définis dans la norme IEEE 802.1q.)

  - Si frame a une valeur de balise égale à FFF, le cadre est supprimé.
  - Si le VID de la trame spécifie un VLAN dont l'interface réseau de réception n'est pas membre, la trame est supprimée. Par exemple, si un paquet est envoyé à partir d'un sous-réseau associé à l'ID VLAN 12 vers un sous-réseau associé à l'ID VLAN 10, le paquet est supprimé. Si un paquet non marqué avec VID 9 est envoyé à partir du sous-réseau associé à l'ID VLAN 10 vers une interface réseau PVID 9, le paquet est supprimé.

- **Règles de sortie.** Les règles de sortie suivantes sont appliquées :
  - Si le VID de la trame spécifie un VLAN dont l'interface réseau de transmission n'est pas membre, la trame est supprimée.
  - Au cours du processus d'apprentissage (défini par la norme IEEE 802.1q), le Src MAC et le VID sont utilisés pour mettre à jour la table de recherche de pont du Citrix ADC.
  - Une trame est supprimée si son VID spécifie un VLAN qui n'a aucun membre. (Vous définissez des membres en liant des interfaces réseau à un VLAN.)

VLAN et transfert de paquets sur Citrix ADC

Le processus de transfert sur l'appliance Citrix ADC est similaire à celui sur n'importe quel commutateur standard. Toutefois, Citrix ADC effectue le transfert uniquement lorsque le mode de couche 2 est activé. Les principales caractéristiques du processus de transmission sont les suivantes :

- Les restrictions topologiques sont appliquées. L'application implique la sélection de chaque interface réseau dans le VLAN en tant que port de transmission (selon l'état de l'interface réseau), des restrictions de pontage (ne pas transférer sur l'interface réseau de réception) et des restrictions MTU.
- Les trames sont filtrées sur la base des informations contenues dans la recherche de table de pont dans la table de base de données de transfert (FDB) de Citrix ADC. La recherche de table de pont est basée sur le MAC de destination et le VID. Les paquets adressés à l'adresse MAC du Citrix ADC sont traités sur les couches supérieures.
- Toutes les trames de diffusion et de multidiffusion sont transférées à chaque interface réseau membre du VLAN, mais le transfert n'a lieu que si le mode L2 est activé. Si le mode L2 est désactivé, les paquets de diffusion et de multidiffusion sont supprimés. Ceci est également vrai pour les adresses MAC qui ne sont pas actuellement dans la table de pontage.
- Une entrée VLAN contient une liste d'interfaces réseau membres qui font partie de son ensemble de membres non marqués. Lors du transfert de trames vers ces interfaces réseau, aucune balise n'est insérée dans la trame.
- Si l'interface réseau est un membre balisé de ce VLAN, la balise est insérée dans la trame lorsque la trame est transférée.

Lorsqu'un utilisateur envoie des paquets de diffusion ou de multidiffusion sans que le VLAN soit identifié, c'est-à-dire lors de la détection d'adresses en double (DAD) pour NSIP ou ND6 pour le prochain

saut de l'itinéraire, le paquet est envoyé sur toutes les interfaces réseau, avec un balisage approprié basé sur les règles d'entrée et d'évacuation. ND6 identifie généralement un VLAN et un paquet de données est envoyé sur ce VLAN uniquement. Les VLAN basés sur les ports sont communs à IPv4 et IPv6. Pour IPv6, Citrix ADC prend en charge les VLAN basés sur préfixe.

Configuration d'un VLAN

August 20, 2021

Vous pouvez implémenter des VLAN dans les environnements suivants :

- Sous-réseau unique
- Sous-réseaux multiples
- Réseau local unique
- VLAN (aucun balisage)
- VLAN (balisage 802.1q)

Si vous configurez des VLAN dont les membres sont uniquement des interfaces réseau non marquées, le nombre total de VLAN possibles est limité au nombre d'interfaces réseau disponibles dans Citrix ADC. Si d'autres sous-réseaux IP sont requis avec une configuration VLAN, le balisage 802.1q doit être utilisé.

Lorsque vous liez une interface réseau à un VLAN, l'interface réseau est supprimée du VLAN par défaut. Si les interfaces réseau doivent faire partie de plusieurs VLAN, vous pouvez lier les interfaces réseau aux VLAN en tant que membres balisés.

Vous pouvez configurer Citrix ADC pour qu'il transporte le trafic entre les VLAN au niveau de la couche 3. Dans ce cas, un VLAN est associé à un seul sous-réseau IP. Les hôtes d'un VLAN appartenant à un seul sous-réseau utilisent le même masque de sous-réseau et une ou plusieurs passerelles par défaut connectées à ce sous-réseau. La configuration de la couche 3 pour un VLAN est facultative. La couche 3 est utilisée pour le transfert IP (routage inter-VLAN). Chaque VLAN possède une adresse IP unique et un masque de sous-réseau qui définissent un sous-réseau IP pour le VLAN. Dans une configuration HA, cette adresse IP est partagée avec les autres appliances Citrix ADC. Le Citrix ADC transfère les paquets entre des sous-réseaux IP configurés (VLAN).

Lorsque vous configurez Citrix ADC, vous ne devez pas créer de sous-réseaux IP superposés. Cela empêche la fonctionnalité de la couche 3.

Chaque VLAN est un domaine de diffusion de couche 2 unique. Deux VLAN, chacun lié à des sous-réseaux IP distincts, ne peuvent pas être combinés en un seul domaine de diffusion. Le transfert du trafic entre deux VLAN nécessite un périphérique de transfert (routage) de couche 3, tel que l'appliance Citrix ADC.

Configuration de VLAN dans un programme d'installation HA

La configuration VLAN pour une configuration haute disponibilité nécessite que les appliances Citrix ADC possèdent la même configuration matérielle et que les VLAN configurés sur eux doivent être des images miroir.

La configuration VLAN correcte est implémentée automatiquement lorsque la configuration est synchronisée entre les appliances Citrix ADC. Le résultat est des actions identiques sur toutes les appliances. Par exemple, l'ajout de l'interface réseau 0/1 au VLAN2 ajoute cette interface réseau au VLAN 2 sur toutes les appliances participant à la configuration haute disponibilité.

Remarque : Si vous utilisez des commandes spécifiques à l'interface réseau dans une configuration HA, les configurations que vous créez ne sont pas propagées à l'autre appliance Citrix ADC. Vous devez exécuter ces commandes sur chaque appliance d'une paire HA pour vous assurer que la configuration des deux appliances de la paire HA reste synchronisée.

Création ou modification d'un VLAN

Pour configurer un VLAN, vous créez une entité VLAN, puis liez les interfaces réseau et les adresses IP au VLAN. Si vous supprimez un VLAN, ses interfaces membres sont ajoutées au VLAN par défaut.

Procédures CLI

Pour créer un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- `add vlan <id> [-aliasName <string>] [-ipv6DynamicRouting (ENABLED|DISABLED)]`
- `sh vlan <id>`

Exemple :

```
1    > add vlan 2  -aliasName "Network A"   Done
2 <!--NeedCopy-->
```

Pour lier une interface à un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- `bind vlan <id> -ifnum <slot/port>`
- `sh vlan <id>`

Exemple :

```
1    > bind vlan 2 -ifnum 1/8   Done
2 <!--NeedCopy-->
```


Pour lier une adresse IP à un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- `bind vlan <id> -IPAddress <IPAddress> <netMask>`
- `sh vlan <id>`

Exemple :

```
1    > bind vlan 2 -IPAddress 10.102.29.54 255.255.255.0   Done
2  <!--NeedCopy-->
```

Pour supprimer un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- `rm vlan <id>`

Procédures GUI

Pour configurer un VLAN à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > VLAN, ajoutez un nouveau VLAN ou modifiez un VLAN existant.
2. Pour lier une adresse IP à un VLAN, sous Liaisons IP, sélectionnez l'option Active correspondant à l'adresse IP que vous souhaitez lier au VLAN (par exemple, 10.102.29.54). La colonne Type affiche le type d'adresse IP (par exemple IP mappée, IP virtuelle ou IP de sous-réseau) pour chaque adresse IP de la colonne Adresse IP.
3. Pour lier une interface réseau à un VLAN, sous Liaisons d'interface, sélectionnez l'option Active correspondant à l'interface que vous souhaitez lier au VLAN.

Surveillance des VLAN

Vous pouvez afficher des statistiques VLAN telles que les paquets reçus, les octets reçus, les paquets envoyés et les octets envoyés, et utiliser les informations pour identifier les anomalies ou déboguer un VLAN.

Pour afficher les statistiques d'un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- `stat vlan <vlanID>`

Exemple :

```
1    stat vlan 2
2  <!--NeedCopy-->
```

Pour afficher les statistiques d'un VLAN à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > VLAN.
2. Sélectionnez le VLAN, puis cliquez sur Statistiques.

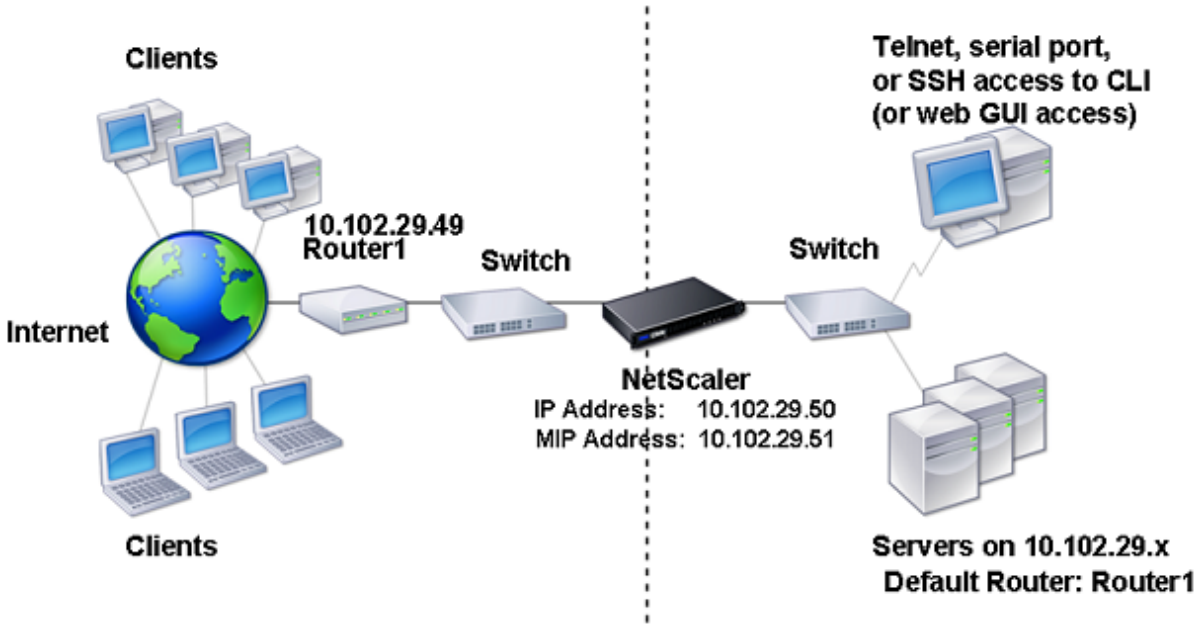
Configuration de VLAN sur un seul sous-réseau

August 20, 2021

Avant de configurer un VLAN sur un seul sous-réseau, assurez-vous que le mode de couche 2 est activé.

La figure suivante montre un environnement de sous-réseau unique

Figure 1. VLAN sur un seul sous-réseau



Dans la figure ci-dessus :

1. Le routeur par défaut pour Citrix ADC et les serveurs est le routeur 1.
2. Le mode de couche 2 doit être activé sur le Citrix ADC pour que ADC Citrix ait un accès direct aux serveurs.
3. Pour ce sous-réseau, un serveur virtuel peut être configuré pour l'équilibrage de charge sur l'appliance Citrix ADC.

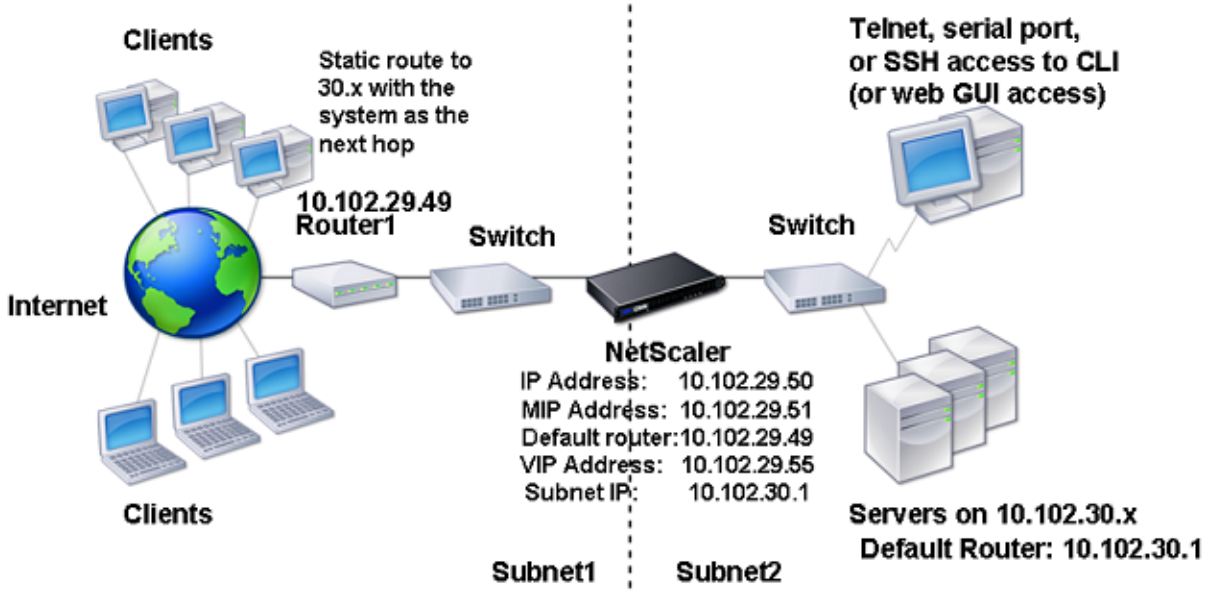
Pour configurer un VLAN sur un seul sous-réseau, suivez les procédures décrites dans Configuration d'un VLAN.

Configuration de VLAN sur plusieurs sous-réseaux

August 20, 2021

Pour configurer un seul VLAN sur plusieurs sous-réseaux, vous devez ajouter un VIP pour le VLAN et configurer le routage de manière appropriée. La figure suivante montre un seul VLAN configuré sur plusieurs sous-réseaux.

Figure 1. Plusieurs sous-réseaux dans un seul VLAN



Pour configurer un seul VLAN sur plusieurs sous-réseaux, effectuez les tâches suivantes :

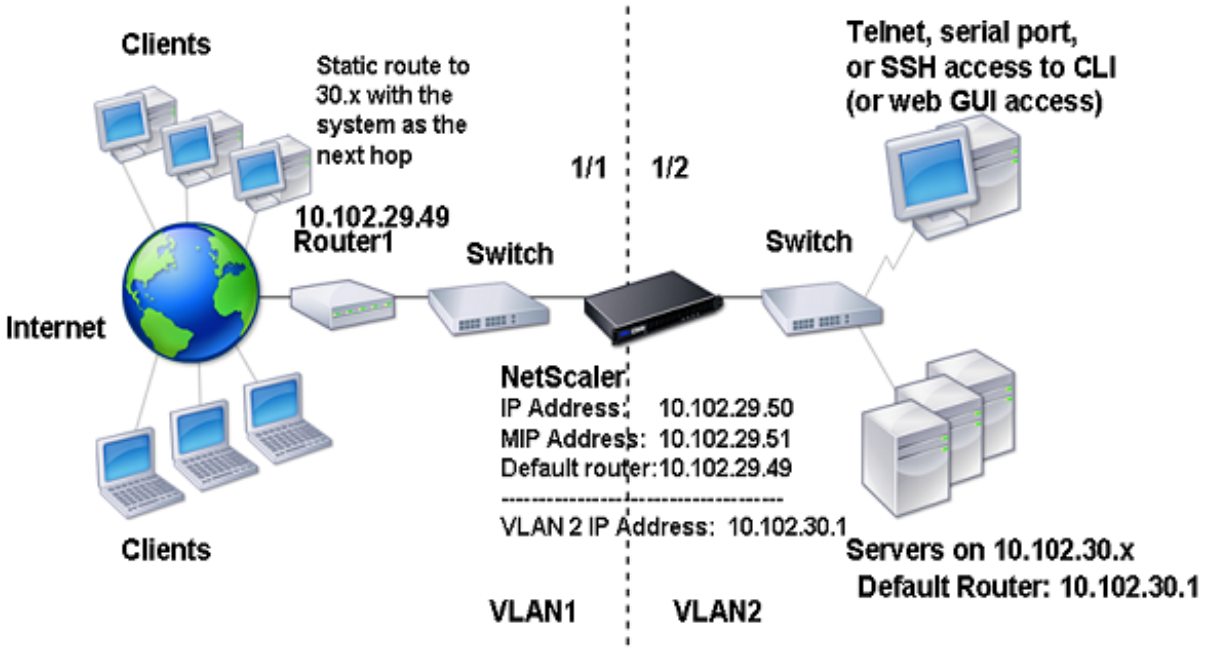
1. Désactivez le mode Couche 2. Pour connaître la procédure de désactivation du mode couche 2, reportez-vous à Modes de transfert de paquets.
2. Ajoutez une adresse VIP. Pour connaître la procédure d'ajout d'une adresse VIP, reportez-vous à la section Configuration et gestion des adresses IP virtuelles (VIP).
3. Configurez la règle RNAT. Pour connaître la procédure de configuration de l'ID RNAT, reportez-vous à la section Configuration de RNAT.

Configuration de plusieurs VLAN non balisés sur plusieurs sous-réseaux

August 20, 2021

Dans les environnements comportant plusieurs VLAN non balisés sur plusieurs sous-réseaux, un VLAN est configuré pour chaque sous-réseau IP. Une interface réseau est liée à un seul VLAN. La figure suivante illustre cette configuration.

Figure 1. Sous-réseaux multiples avec VLAN - Pas de balisage



Pour implémenter la configuration indiquée dans la figure ci-dessus, effectuez les tâches suivantes :

1. Ajouter VLAN 2.
2. Liez l'interface réseau 1/2 du Citrix ADC au VLAN 2 en tant qu'interface réseau non balisée.
3. Liez l'adresse IP et le masque de sous-réseau au VLAN 2.

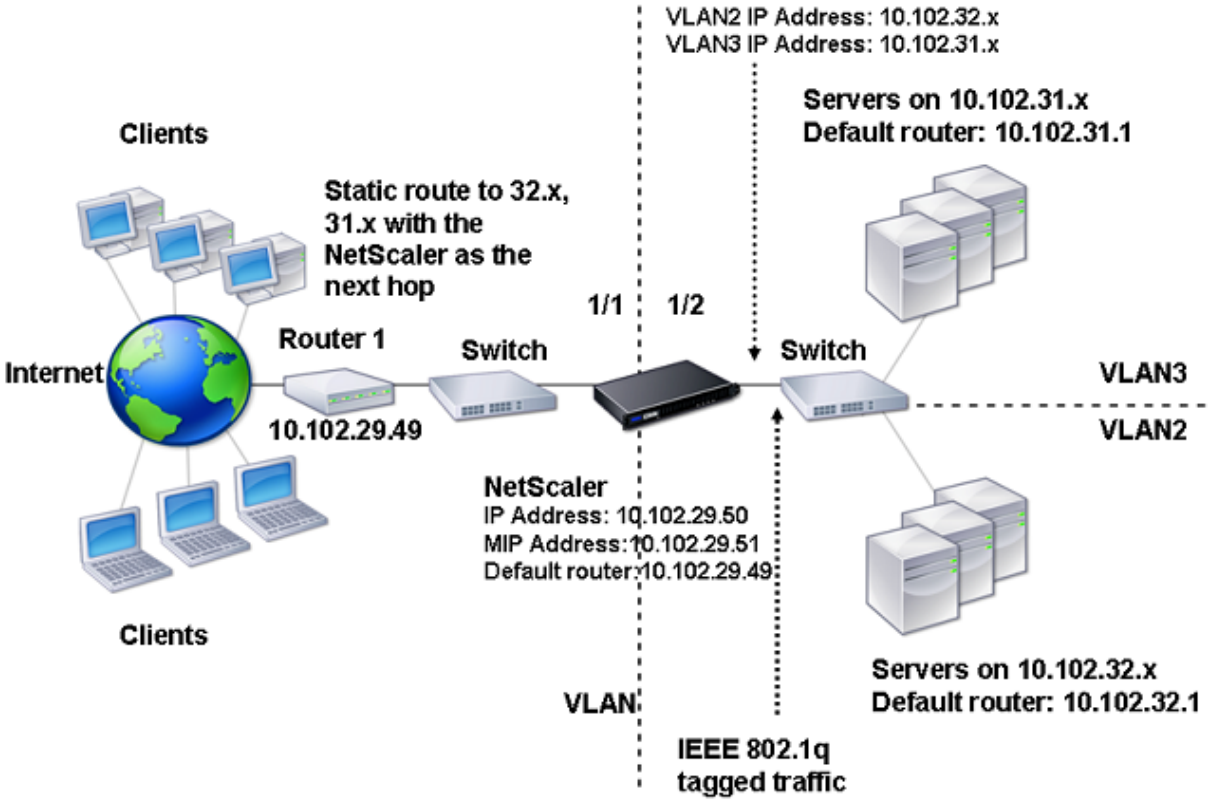
Pour connaître les procédures relatives à ces tâches, reportez-vous à la section Configuration d'un VLAN.

Configuration de plusieurs VLAN avec le balisage 802.1q

August 20, 2021

Pour plusieurs VLAN avec balisage 802.1q, chaque VLAN est configuré avec un sous-réseau IP différent. Chaque interface réseau est dans un VLAN. L'un des VLAN est configuré comme balisé. La figure suivante illustre cette configuration.

Figure 1. Plusieurs VLAN avec balisage IEEE 802.1q



Pour implémenter la configuration indiquée dans la figure ci-dessus, effectuez les tâches suivantes :

1. Ajouter VLAN 2.
2. Liez l'interface réseau 1/2 du Citrix ADC au VLAN 2 en tant qu'interface réseau non balisée.
3. Liez l'adresse IP et le masque de réseau au VLAN 2.
4. Ajouter VLAN 3.
5. Liez l'interface réseau 1/2 du Citrix ADC au VLAN 3 en tant qu'interface réseau balisée.
6. Liez l'adresse IP et le masque de réseau au VLAN 3.

Pour connaître les procédures relatives à ces tâches, reportez-vous à la section Configuration d'un VLAN.

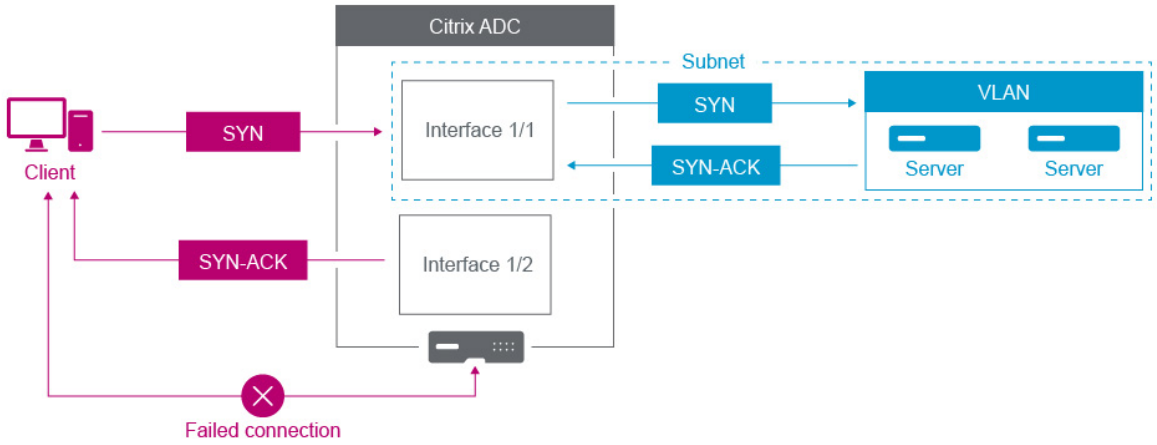
Associer un sous-réseau IP à une interface Citrix ADC à l'aide de VLAN

August 20, 2021

Par défaut, une appliance Citrix ADC ne permet pas de différencier les interfaces réseau. L'appliance fonctionne davantage comme un concentrateur réseau qu'un commutateur. Cela peut conduire à des boucles réseau de couche 3 où le trafic dupliqué est transmis sur plusieurs interfaces.

Dans de tels scénarios, selon la conception du réseau, il est possible qu'une requête puisse être trans-

mise sur une interface et que la réponse correspondante soit reçue sur une interface différente.



Par exemple, un paquet SYN envoyé sur une interface et la réponse SYN-ACK reçue sur une autre interface peuvent entraîner un échec de connexion, car l'appliance prévoit recevoir le SYN-ACK sur la même interface que celle qui a envoyé le paquet SYN d'origine.

Pour résoudre ces problèmes, l'appliance peut utiliser des VLAN internes ou externes pour associer des sous-réseaux spécifiques à des interfaces.

Avant de commencer

Avant de commencer à associer un sous-réseau IP à une interface Citrix ADC à l'aide de VLAN, notez les points suivants :

- La connectivité réseau peut être accidentellement perdue lors de l'association d'un VLAN au sous-réseau ou à l'interface actuellement utilisée pour accéder à l'interface graphique ou à l'interface de ligne de commande Citrix ADC. Par conséquent, dans de tels scénarios, il est fortement recommandé d'effectuer la modification en accédant à l'interface de ligne de commande via la console série d'une appliance Citrix ADC physique ou via la console série virtuelle d'un Citrix ADC VPX.
- Les interfaces de gestion de Citrix ADC manquent de certaines fonctionnalités d'optimisation matérielle, ce qui les rend moins souhaitables pour une utilisation avec le trafic de données de production. À ce titre, il est recommandé de configurer Citrix ADC pour utiliser uniquement les interfaces de gestion pour le trafic NSIP (Management Interfaces for Management). Dans la configuration par défaut, il n'y a pas de différenciation logique entre les interfaces de gestion et les interfaces de données sur un matériel NetScaler. Pour atteindre cet objectif, il est recommandé que le NSIP se trouve sur un VLAN distinct du trafic de données, ce qui permet au trafic de gestion d'être sur une interface distincte.

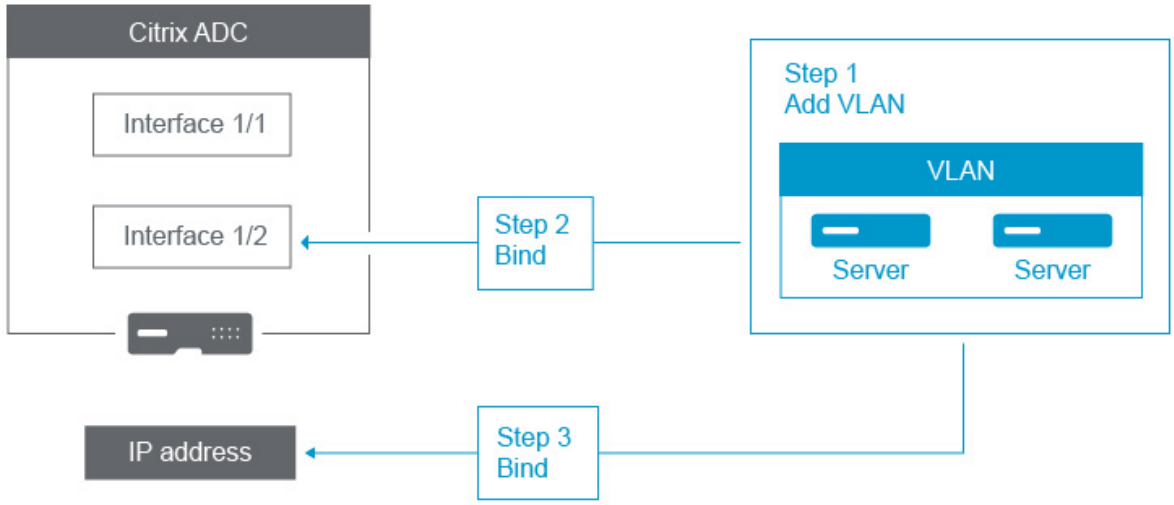
  Bien que le concept soit le même, pour modifier les associations VLAN du sous-réseau qui contient l'adresse NSIP, vous devez configurer NSVLAN au lieu des instructions ci-dessous. De

telles modifications nécessiteront également un redémarrage du Citrix ADC afin de prendre effet. Pour plus d'informations, voir Configuration de NSVLAN.

- Sur Citrix ADC SDX, il est fortement recommandé que le NSIP de chaque instance soit sur le même sous-réseau et VLAN que le SVM (Management Service GUI) et XenServer du SDX. La SVM communique avec les instances via le réseau. Si la SVM, XenServer et les instances ne sont pas sur le même VLAN et sous-réseau, le trafic de gestion doit circuler en dehors du SDX. Dans ce cas, les problèmes de réseau peuvent entraîner l'état de l'instance à apparaître comme jaune ou rouge et peuvent empêcher la gestion et les modifications de configuration des instances de Citrix ADC.

Étapes de configuration

Associer un sous-réseau IP à une interface Citrix ADC comporte les tâches suivantes :



Ajoutez un VLAN. Lors de l'ajout d'un VLAN, si vous balisez le VLAN, vous devez sélectionner un numéro de VLAN défini dans le commutateur réseau pour le port de commutateur associé. Si le VLAN n'est pas étiqueté et qu'il est interne à l'appliance, il est recommandé de sélectionner le numéro de VLAN disponible dans la configuration du commutateur pour une référence facile.

Liez une interface au VLAN. Lors de la liaison, si vous utilisez l'agrégation de liens, associez le VLAN au canal LA (par exemple, LA/1) au lieu de l'interface physique. Le VLAN doit être associé à une seule interface réseau.

Si vous souhaitez marquer le trafic sur l'interface, utilisez l'option balisé (Tag). Sinon, le trafic laisse l'appliance non étiquetée et est associé au VLAN natif du port du commutateur.

Liez une adresse IP au VLAN. Lors de la liaison, si vous liez plusieurs adresses IP à partir du même sous-réseau, une erreur se produit. Lorsqu'une adresse IP est associée à un VLAN, toutes les adresses IP de ce sous-réseau sont automatiquement associées au VLAN.

> **Remarque :**
>
> dans une configuration haute disponibilité (HA), ces configurations VLAN sont ajoutées automatiquement du nœud principal au nœud secondaire lors de la synchronisation HA. Pour plus d'informations sur les configurations haute disponibilité, voir Haute disponibilité.

Procédures CLI

Pour ajouter un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **ajouter vlan** <id>
- **sh vlan** <id>

Pour lier une interface à un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **bind vlan** <id> -**ifnum** <slot/port>
- **sh vlan** <id>

Pour lier une adresse IP à un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **bind vlan** <id> -**IPAddress** <IPAddress> <netMask>
- **sh vlan** <id>

Exemple :

```
1 > add vlan 100
2
3 > bind vlan 100 -ifnum 1/1
4
5 > bind vlan 100 -ipAddress 10.0.1.0 255.255.255.0
6 <!--NeedCopy-->
```

Procédures GUI

Pour configurer un VLAN à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VLAN**, ajoutez un nouveau VLAN.
2. Pour lier une interface réseau à un VLAN, sous **Liaisons d'interface**, sélectionnez l'option **Active** correspondant à l'interface que vous souhaitez lier au VLAN.

3. Pour lier une adresse IP à un VLAN, sous **Liaisons IP**, sélectionnez l'option **Active** correspondant à l'adresse IP que vous souhaitez lier au VLAN (par exemple, 10.102.29.54). La colonne **Type** affiche le type d'adresse IP de chaque adresse IP dans la colonne **Adresse IP** .

Meilleures pratiques en matière de mise en réseau et de VLAN des appliances Citrix ADC

January 21, 2021

Une appliance Citrix ADC utilise des VLAN pour déterminer quelle interface doit être utilisée pour quel trafic. En outre, l'appliance Citrix ADC ne participe pas à Spanning Tree. Sans la configuration VLAN appropriée, l'appliance Citrix ADC n'est pas en mesure de déterminer l'interface à utiliser et il peut fonctionner plus comme un HUB qu'un commutateur ou un routeur. En d'autres termes, l'appliance Citrix ADC peut utiliser toutes les interfaces pour chaque conversation.

Symptômes d'une mauvaise configuration du VLAN

Un problème de configuration erronée du VLAN peut se manifester sous de nombreuses formes, notamment des problèmes de performances, l'incapacité d'établir des connexions, des sessions déconnectées aléatoirement et, dans des situations graves, des perturbations réseau apparemment sans rapport avec l'appliance Citrix ADC elle-même. L'appliance Citrix ADC peut également signaler les déplacements MAC, les interfaces mutées et/ou les dépassements de tampon de l'interface de gestion, selon la nature exacte de l'interaction avec votre réseau.

Déplacements MAC (counter nic_tot_bdg_mac_moves) : ce problème indique que l'appliance Citrix ADC utilise plusieurs interfaces pour communiquer avec le même périphérique (adresse MAC), car il n'a pas pu déterminer correctement quelle interface utiliser.

Interfaces mutées (counter nic_err_bdg_muted) : ce problème indique que l'appliance Citrix ADC a détecté qu'elle crée une boucle de routage en raison de problèmes de configuration de VLAN, et qu'en tant que telle, elle a arrêté une ou plusieurs interfaces incriminées afin d'empêcher un réseau panne.

Dépassements de**tampon d'interface, généralement en référence aux interfaces de gestion (counter nic_err_tx_overflow) : Ce**problème peut être causé si trop de trafic est transmis via une interface de gestion. Les interfaces de gestion de l'appliance Citrix ADC ne sont pas conçues pour gérer de grands volumes de trafic, ce qui peut résulter d'erreurs de configuration réseau et VLAN qui déclenchent l'appliance Citrix ADC à utiliser une interface de gestion pour le trafic de données de production. Cela se produit souvent parce que l'appliance Citrix ADC n'a aucun moyen de différencier le trafic sur le VLAN/sous-réseau du NSIP (NSVLAN) du trafic de production régulier. Il est fortement recommandé que le NSIP se trouve sur un VLAN et un sous-réseau distincts de tous les périphériques de production tels que les stations de travail et les serveurs.

ACK**orphelins (counter tcp_err_orphan_ack)** : ce problème indique que l'appliance Citrix ADC a reçu un paquet ACK qu'elle n'attendait pas, généralement sur une interface différente de celle du trafic ACK'd. Cette situation peut être causée par des erreurs de configuration VLAN lorsque l'appliance Citrix ADC transmet sur une interface différente de celle utilisée par la machine cible pour communiquer avec l'appliance Citrix ADC (souvent vu en conjonction avec des déplacements MAC)

Taux élevés de retransmissions ou d'abandon de retransmission (compteurs : tcp_err_retransmit_giveups, tcp_err_7th_retransmit, divers autres compteurs de retransmission) : L'appliance Citrix ADC tente de retransmettre un paquet TCP 7 fois au total avant d'abandonner et de mettre fin à la connexion. Bien que cette situation puisse être causée par des conditions réseau, elle se produit souvent à la suite d'une mauvaise configuration du VLAN et de l'interface.

Haute disponibilité Split Brain : Split Brain est une condition dans laquelle les deux nœuds haute disponibilité croient qu'ils sont Primary, entraînant des adresses IP dupliquées et la perte des fonctionnalités de l'appliance Citrix ADC. Cela se produit lorsque les deux nœuds haute disponibilité ne peuvent pas communiquer entre eux en utilisant Heartbeats haute disponibilité sur le port UDP 3003 à l'aide du NSIP, sur n'importe quelle interface. Cela est généralement dû à des erreurs de configuration VLAN dans lesquelles le VLAN natif sur les interfaces de l'appliance Citrix ADC n'a pas de connectivité entre les appliances Citrix ADC.

Meilleures pratiques pour les configurations VLAN et réseau

1. Chaque sous-réseau doit être associé à un VLAN.
2. Plusieurs sous-réseaux peuvent être associés au même VLAN (selon la conception de votre réseau).
3. Chaque VLAN doit être associé à une seule interface (aux fins de cette discussion, un canal LA compte comme une seule interface).
4. Si plusieurs sous-réseaux doivent être associés à une interface, les sous-réseaux doivent être balisés.
5. Contrairement à la croyance populaire, la fonctionnalité MBF (Mac-Based-Forwarding) de l'appliance Citrix ADC n'est pas conçue pour atténuer ce type de problème. MBF est conçu principalement pour le mode DSR (Direct Server Return) de l'appliance Citrix ADC, qui est rarement utilisé dans la plupart des environnements (il est conçu pour permettre au trafic de contourner délibérément l'appliance Citrix ADC sur le chemin de retour à partir des serveurs back-end). MBF peut masquer les problèmes de VLAN dans certains cas, mais il ne doit pas être utilisé pour résoudre ce type de problème.
6. Chaque interface de l'appliance Citrix ADC nécessite un VLAN natif (contrairement à Cisco, où les VLAN natifs sont facultatifs), bien que le paramètre TagAll sur une interface puisse être utilisé de sorte qu'aucun trafic non marqué ne quitte l'interface en question.

7. Le VLAN natif peut être balisé si nécessaire pour la conception de votre réseau (il s'agit de l'option tagAll pour l'interface).

8. Le VLAN du sous-réseau du NSIP de votre appliance Citrix ADC est un cas particulier. C'est ce qu'on appelle le NSVLAN. Les concepts sont les mêmes, mais les commandes pour le configurer sont différentes et les modifications apportées au NSVLAN nécessitent un redémarrage de l'appliance Citrix ADC pour prendre effet. Si vous tentez de lier un VLAN à un SNIP qui partage le même sous-réseau que le NSIP, vous obtenez « Opération non autorisée ». C'est parce que vous devez utiliser les commandes NSVLAN à la place. En outre, sur certaines versions de firmware, vous ne pouvez pas définir un NSVLAN si ce numéro de VLAN existe à l'aide de la commande `add VLAN`. Il suffit de supprimer le VLAN, puis de réinstaller le NSVLAN.

9. Les Heartbeats haute disponibilité utilisent toujours le VLAN natif de l'interface respective (éventuellement marqué si l'option tagAll est définie sur l'interface).

10. Il doit y avoir communication entre au moins un ensemble de VLAN natif sur les deux nœuds d'une paire haute disponibilité (ceci peut être direct ou via un routeur). Les VLAN natifs sont utilisés pour les pulsations de haute disponibilité. Si les appliances Citrix ADC ne peuvent pas communiquer entre des VLAN natifs sur n'importe quelle interface, cela entraînera des basculements de haute disponibilité et éventuellement une situation de split-brain où les deux appliances Citrix ADC pensent qu'elles sont primaires (conduisant, entre autres, à des adresses IP en double).

11. L'appliance Citrix ADC ne participe pas à l'arborescence spanning. En tant que tel, il n'est pas possible d'utiliser spanning tree pour assurer la redondance d'interface lors de l'utilisation d'une appliance Citrix ADC. Utilisez plutôt une forme d'agrégation de liens (LACP ou LAG manuelle) à cet effet.

    Remarque : Si vous souhaitez disposer d'une agrégation de liens entre plusieurs commutateurs physiques, les commutateurs doivent être configurés en tant que commutateur virtuel, à l'aide d'une fonctionnalité telle que la pile de commutateurs de Cisco.

12. La synchronisation haute disponibilité et la commande Propagation, par défaut, utilisent le NSIP/NSVLAN. Pour les séparer d'un VLAN différent, vous pouvez utiliser l'option SyncVLAN de la commande `set HA node`.

13. Rien dans la configuration par défaut de l'appliance Citrix ADC n'indique qu'une interface de gestion (0/1 ou 0/2) est limitée au trafic de gestion uniquement. Cette restriction doit être appliquée par l'utilisateur final via la configuration VLAN. Les interfaces de gestion ne sont pas conçues pour gérer le trafic de données, donc votre conception de réseau doit tenir compte de ce point. Les interfaces de gestion, contenues sur la carte mère de l'appliance Citrix ADC, ne disposent pas de diverses fonctionnalités de déchargement, telles que le déchargement CRC, des tampons de paquets plus volumineux et d'autres optimisations, ce qui les rend beaucoup moins efficaces pour gérer de grandes quantités de trafic. Pour séparer les données de produc-

tion et le trafic de gestion, le NSIP ne doit pas être sur le même sous-net/VLAN que votre trafic de données.

14. S'il est souhaitable d'utiliser une interface de gestion pour transporter le trafic de gestion, il est recommandé que l'itinéraire par défaut soit sur un sous-réseau autre que le sous-réseau du NSIP (NSVLAN).

    Dans de nombreuses configurations, l'itinéraire par défaut est utilisé pour la communication des stations de travail (dans un scénario Internet). Si l'itinéraire par défaut se trouve sur le même sous-réseau que le NSIP, l'appliance ADC peut utiliser l'interface de gestion pour envoyer et recevoir du trafic de données. Cette utilisation du trafic de données peut surcharger l'interface de gestion.

15. En outre, un SDX-SVM, XenServer et tous les NSIP d'instance Citrix ADC doivent être sur le même VLAN et sous-réseau. Il n'y a pas de **backplane** dans l'appliance SDX qui permet la communication entre SVM/XEN/instances. S'ils ne sont pas sur le même VLAN/sous-net/interface, le trafic entre eux doit quitter le matériel physique, être routé sur votre réseau et revenir.

    Cette configuration peut entraîner des problèmes de connectivité évidents entre les instances et SVM et, en tant que telle, n'est pas recommandée. Un symptôme courant de ceci est un indicateur d'état d'instance jaune dans la SVM pour l'instance VPX en question, et l'impossibilité d'utiliser la SVM pour reconfigurer une instance VPX.

16. Si certains VLAN sont liés à des sous-réseaux et d'autres ne le sont pas, lors d'un basculement de haute disponibilité, les paquets GARP ne sont pas envoyés pour des adresses IP sur aucun des sous-réseaux qui ne sont pas liés à un VLAN. Cette configuration peut entraîner des problèmes de connexion et de connectivité lors de basculements à haute disponibilité. Ce problème est dû au fait que l'appliance Citrix ADC ne peut pas notifier la modification des adresses IP de propriété MAC réseau sur les appliances Citrix ADC non configurées par VMAC.

    Les symptômes de ceci sont que, pendant ou après un basculement de haute disponibilité, le compteur ip_tot_floating_ip_err incrémente sur l'ancienne appliance principale Citrix ADC pendant plus de quelques secondes, ce qui indique que le réseau n'a pas reçu ou ne traite pas les paquets GARP et que le réseau continue à transmettre des données au nouveau deuxième appliance Citrix ADC.

Configuration de NSVLAN

August 20, 2021

NSVLAN est un VLAN auquel le sous-réseau de l'adresse IP de gestion Citrix ADC (NSIP) est lié. Le sous-réseau NSIP n'est disponible que sur les interfaces associées à NSVLAN. Par défaut, NSVLAN est VLAN 1, mais vous pouvez désigner un VLAN différent comme NSVLAN. Si vous le faites, vous devez

redémarrer l'appliance Citrix ADC pour que la modification prenne effet. Après le redémarrage, le trafic de sous-réseau NSIP est limité au nouveau NSVLAN.

Le trafic provenant du sous-réseau IP Citrix ADC peut être balisé (802.1q) avec l'ID VLAN spécifié pour NSVLAN. Vous devez configurer l'interface du commutateur connecté pour marquer et autoriser ce même ID de VLAN sur l'interface connectée. Si vous supprimez votre configuration NSVLAN, le sous-réseau NSIP est automatiquement lié au VLAN 1, restaurant le NSVLAN par défaut.

Pour configurer NSVLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- set ns config -nsvlan <positive_integer>-ifnum<interface_name>… [-étiqueté (OUI|NON)]
- show ns config

  Remarque : la configuration prend effet après le redémarrage de l'appliance Citrix ADC.

Exemple :

```
1 > set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged NO
2  Done
3
4 > save config
5  Done
6 <!--NeedCopy-->
```

Pour restaurer la configuration NSVLAN par défaut à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- unset ns config -nsvlan
- show ns config

Exemple :

```
1 > unset ns config -nsvlan
2  Done
3 <!--NeedCopy-->
```

Pour configurer NSVLAN à l'aide de l'interface graphique :

Accédez à Système > Paramètres, dans le groupe Paramètres, cliquez sur Modifier les paramètres NSVLAN.

Définition du MTU sur le NSVLAN

Par défaut, la MTU du NSVLAN est définie sur 1500 octets. Vous pouvez modifier ce paramètre pour optimiser les performances du réseau et du réseau. Par exemple, vous pouvez configurer le NSVLAN

pour traiter les trames jumbo.

Pour définir le MTU du NSVLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set vlan** <id> **-mtu** <positive_integer>
- **afficher vlan** <id>

Pour définir le MTU du NSVLAN à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **VLAN**, ouvrez le NSVLAN et définissez le paramètre **Unité de transmission maximale** .

Exemple de configuration :

Dans l'exemple de configuration suivant, VLAN 100 est le NSVLAN.

```
> set ns config -nsvlan 100 -ifnum 1/1 -tagged no

  Warning: The configuration must be saved and the system rebooted for
      these settings to take effect

> set vlan 100 -mtu 1600

  Done

> sh vlan

  1)  VLAN ID: 1

      Link-local IPv6 addr:
    fe80::947b:52ff:fead:12d5/64

      Interfaces : 1/2 LO/1

  2)  VLAN ID: 100    VLAN Alias Name:

      MTU: 1600

      Interfaces : 1/1

      IPs :

          10.102.53.114     Mask: 255.255.255.0

  Done
```



```
30 > save config
31
32   Done
33 <!--NeedCopy-->
```

Configuration de la liste des VLAN autorisés

August 20, 2021

Citrix ADC accepte et envoie des paquets balisés d'un VLAN sur une interface si le VLAN est explicitement configuré sur l'appliance Citrix ADC et que l'interface est liée au VLAN. Certains déploiements (par exemple, Bump in the wire) nécessitent que l'appliance Citrix ADC fonctionne comme un périphérique transparent pour accepter et transférer des paquets étiquetés liés à un grand nombre de VLAN. Pour cette exigence, la configuration et la gestion d'un grand nombre de VLAN n'est pas une solution réalisable.

La liste des VLAN autorisés sur une interface spécifie une liste de VLAN. L'interface accepte et envoie de manière transparente les paquets balisés liés aux VLAN spécifiés sans qu'il soit nécessaire de configurer explicitement ces VLAN sur l'appliance.

Points à prendre en compte avant de configurer la liste des VLAN autorisés

Tenez compte des points suivants avant de configurer la liste des VLAN autorisés

- Dans une configuration haute disponibilité, la liste des VLAN autorisés n'est ni propagée ni synchronisée. Par conséquent, vous devez configurer la liste VLAN autorisé sur les deux nœuds.
- Le trafic d'un VLAN natif peut fuir vers les interfaces non membres qui spécifient le VLAN natif dans sa liste de VLAN autorisé.
- Un maximum de 60 plages de VLAN peut être spécifié dans la liste des VLAN autorisés pour une interface.
- L'appliance Citrix ADC ne prend pas en charge la liste des VLAN autorisés sur les interfaces qui font partie des canaux d'agrégation de liens ou des jeux d'interfaces redondants. Pour plus d'informations sur le jeu d'interfaces redondantes, voir Ensemble d' interfaces redondantes.
- La liste des VLAN autorisés n'est pas prise en charge sur une configuration de cluster Citrix ADC.
- L'appliance Citrix ADC ne prend pas en charge la liste des VLAN autorisés pour les groupes Bridge.
- L'appliance Citrix ADC ne prend pas en charge la liste des VLAN autorisés pour les VXLAN.

Configuration de la liste des VLAN autorisés

Pour configurer la liste des VLAN autorisés à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set interface** <id> **-trunkmode** (ON|OFF) **-trunkAllowedVlan** <int[-int]> …
- **show interface** <id>

Pour configurer la liste des VLAN autorisés à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Interfaces**, sélectionnez une interface réseau, cliquez sur **Modifier**, puis définissez les paramètres suivants :

- Mode Tronc
- VLAN autorisé par le réseau local virtuel

Exemple de configuration :

Dans l'exemple de configuration suivant, les VLAN des plages 100-120, 190-200 et 300-330 sont spécifiés dans la liste des VLAN autorisés pour l'interface 1/2.

```
> set int 1/2 -trunkmode on -trunkallowedVlan 100-120 190-200 300-330

Done

> sh int 1/2

1)      Interface 1/2 (Gig Ethernet 10/100/1000 MBits) #6
        flags=0xc020

        <ENABLED, UP, UP, AUTONEG OFF, HEARTBEAT, 802.1q, trunkmode>

        Trunk Allowed Vlans:  100-120 190-200 300-330

Done

<!--NeedCopy-->
```

Configuration des groupes de ponts

August 20, 2021

En règle générale, lorsque vous souhaitez fusionner deux ou plusieurs VLAN en un seul domaine, vous modifiez la configuration du VLAN sur tous les périphériques des domaines distincts. Cela peut être

une tâche fastidieuse. Pour fusionner plus facilement plusieurs VLAN dans un seul domaine de diffusion, vous pouvez utiliser des groupes de ponts.

La fonctionnalité de groupes de ponts fonctionne de la même manière qu'un VLAN. Plusieurs VLAN peuvent être liés à un seul groupe de ponts, et tous les VLAN liés au même groupe de ponts forment un seul domaine de diffusion. Vous pouvez lier uniquement les VLAN de couche 2 à un groupe de ponts. Pour la fonctionnalité de couche 3, vous devez affecter une adresse IP à un groupe de ponts.

En mode couche 2, un paquet de diffusion reçu sur une interface appartenant à un VLAN particulier est ponté à d'autres VLAN appartenant au même groupe de ponts. Dans le cas d'un paquet monodiffusion, l'appliance Citrix ADC recherche dans sa table de pont les adresses MAC apprises de tous les VLAN appartenant au même groupe de ponts.

En mode de transfert de couche 3, un sous-réseau IP est lié à un groupe de ponts. Citrix ADC accepte les paquets entrants appartenant au sous-réseau lié et transfère les paquets uniquement sur des VLAN liés au groupe de ponts.

Le routage IPv6 peut être activé sur un groupe de ponts configuré.

> **Remarque**
>
> La fonctionnalité de groupe de ponts et le mode BPDU de pont ne peuvent pas fonctionner ensemble.

Étapes de configuration

Procédez comme suit pour configurer un groupe de ponts :

- Activer le mode Couche 2
- Ajouter un groupe de ponts et lier des VLAN au groupe de ponts

Procédures CLI

Pour activer le mode de couche 2 à l'aide de l'interface de ligne de commande :
À l'invite de commandes, tapez :

- **activer le mode ns l2**
- **afficher le mode ns**

Pour ajouter un groupe de ponts et lier des VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **ajouter un groupe de pont** <id>[-**Routage dynamique IPv6** (**ACTIVÉ** | **DÉSACTIVÉ**)]
- **bind bridgegroup** <id> -**vlan** <positive_integer>
- **show bridgegroup** <id>

Exemple :

```
> add bridgegroup 12
 Done
<!--NeedCopy-->
```

Pour supprimer un groupe de ponts à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **rm bridgegroup** <id>

Exemple :

```
 rm bridgegroup 12
<!--NeedCopy-->
```

Procédures GUI

Pour configurer un groupe de ponts à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Groupes** de ponts, ajoutez un nouveau groupe de ponts et liez des VLAN au groupe de ponts, ou modifiez un groupe de ponts existant.

Configuration de MAC virtuels

August 20, 2021

Les nœuds principaux et secondaires d'une configuration haute disponibilité (HA) partagent l'entité flottante d'adresse MAC virtuelle. Le nœud principal possède les adresses IP flottantes (telles que MIP, SNIP et VIP) et répond aux demandes ARP de ces adresses IP avec sa propre adresse MAC. Par conséquent, la table ARP d'un périphérique externe, tel qu'un routeur en amont, est mise à jour avec l'adresse IP flottante et l'adresse MAC du nœud principal.

Lorsqu'un basculement se produit, le nœud secondaire prend la relève en tant que nouveau nœud principal. L'ancien nœud secondaire utilise Gratuitous ARP (GARP) pour annoncer les adresses IP flottantes qu'il avait apprises de l'ancien nœud principal. L'adresse MAC que le nouveau nœud principal annonce est l'adresse MAC de sa propre interface réseau. Certains périphériques (quelques routeurs) n'acceptent pas ces messages GARP. Par conséquent, ces périphériques externes conservent le mappage d'adresse IP vers Mac que l'ancien nœud principal avait annoncé. Cela peut entraîner la chute d'un site GSLB.

Par conséquent, vous devez configurer un MAC virtuel sur les deux nœuds d'une paire HA. Cela signifie que les deux nœuds ont des adresses MAC identiques. Lorsqu'un basculement se produit, l'adresse

MAC du nœud secondaire reste inchangée et les tables ARP sur les périphériques externes n'ont pas besoin d'être mises à jour.

Pour connaître les procédures de configuration d'un MAC virtuel, reportez-vous à la section Configuration des adresses MAC virtuelles.

Configuration de l'agrégation de liens

October 5, 2021

L'agrégation de liens combine les données provenant de plusieurs ports en une seule liaison haute vitesse. La configuration de l'agrégation de liens augmente la capacité et la disponibilité du canal de communication entre l'appliance Citrix ADC et les autres périphériques connectés. Un lien agrégé est également appelé un « canal. » Vous pouvez configurer les canaux manuellement ou utiliser le protocole LACP (Link Aggregation Control Protocol). Vous ne pouvez pas appliquer LACP à un canal configuré manuellement, ni configurer manuellement un canal créé par LACP.

Lorsqu'une interface réseau est liée à un canal, les paramètres du canal ont priorité sur les paramètres de l'interface réseau. (Autrement dit, les paramètres d'interface réseau sont ignorés.) Une interface réseau ne peut être liée qu'à un seul canal.

Lorsqu'une interface réseau est liée à un canal, elle abandonne sa configuration VLAN. Lorsque les interfaces réseau sont liées à un canal, manuellement ou par LACP, elles sont supprimées des VLAN auxquels elles appartenaient à l'origine et ajoutées au VLAN par défaut. Toutefois, vous pouvez lier le canal à l'ancien VLAN, ou à un nouveau. Par exemple, si vous liez les interfaces réseau 1/2 et 1/3 à un VLAN avec ID 2, puis les liez à un canal LA/1, les interfaces réseau sont déplacées vers le VLAN par défaut, mais vous pouvez les relier au VLAN 2.

Configuration manuelle de l'agrégation de liens

Lorsque vous créez un canal d'agrégation de liens, son état est DOWN jusqu'à ce que vous y liez une interface active. Vous pouvez modifier un canal à tout moment. Vous pouvez supprimer des canaux, ou vous pouvez les activer/les désactiver.

Procédures CLI

Pour créer un canal d'agrégation de liens à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- ajouter le canal <id>[-ifnum <interfaceName>…] [-state (ACTIVÉ | DÉSACTIVÉ)] [-speed] <speed>[-Flow Control] [-HamMonitor (ON | OFF)][-tagall (ON | OFF)] [-IFALIAS] <string>[-

débit] <positive_integer>[-bande passante élevée <positive_integer>[- Bande passante normale]<positive_integer>]

- show channel

Exemple :

```
> add channel LA/1 -ifnum 1/8
Done
<!--NeedCopy-->
```

Pour lier une interface à un canal d'agrégation de liens existant ou délier une interface à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- bind channel <id> <interfaceName>
- unbind channel <id> <interfaceName>

Exemple :

```
bind channel LA/1 1/8
<!--NeedCopy-->
```

Pour modifier un canal d'agrégation de liens à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande
set channel, l'ID de canal et les paramètres à modifier, avec leurs nouvelles valeurs.

Pour supprimer un canal d'agrégation de liens à l'aide de l'interface de ligne de commande :

Important : Lorsqu'un canal est supprimé, les interfaces réseau qui lui sont liées induisent des boucles réseau qui diminuent les performances du réseau. Vous devez désactiver les interfaces réseau avant de supprimer le canal.

À l'invite de commandes, tapez :

- rm channel <id>

Exemple :

```
> rm channel LA/1
 Done
<!--NeedCopy-->
```

Procédures GUI

Pour configurer un canal d'agrégation de liens à l'aide de l'interface graphique :

Accédez à Système > Réseau > Canaux, ajoutez un nouveau canal ou modifiez un canal existant.

Pour supprimer un canal d'agrégation de liens à l'aide de l'interface graphique :

> **Important :**
>
> Lorsqu'un canal est supprimé, les interfaces réseau qui lui sont liées induisent des boucles réseau qui diminuent les performances du réseau. Vous devez désactiver les interfaces réseau avant de supprimer le canal.

Accédez à Système > Réseau > Chaînes, sélectionnez le canal à supprimer et cliquez sur Supprimer.

Configuration de l'agrégation de liens à l'aide du protocole de contrôle d'agrégation de liens

Le protocole LACP (Link Aggregation Control Protocol) permet aux périphériques réseau d'échanger des informations d'agrégation de liens en échangeant des unités de données LACP (LACPDU). Par conséquent, vous ne pouvez pas activer LACP sur les interfaces réseau qui sont membres d'un canal que vous avez créé manuellement.

Lorsque vous utilisez LACP pour configurer l'agrégation de liens, vous utilisez des commandes et des paramètres différents pour modifier les canaux d'agrégation de liens que pour créer des canaux d'agrégation de liens. Pour supprimer un canal, vous devez désactiver LACP sur toutes les interfaces qui font partie du canal.

Remarque : Dans une configuration haute disponibilité, les configurations LACP ne sont ni propagées ni synchronisées.

Configuration de la priorité système LACP

La priorité système LACP détermine quel périphérique homologue d'un canal LA LACP peut avoir le contrôle sur le canal LA. Ce numéro est appliqué globalement à tous les canaux LACP de l'appliance. Plus la valeur est basse, plus la priorité est élevée.

Pour configurer la priorité système LACP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour définir la priorité d'une appliance autonome et vérifier la configuration :

- set lacp -sysPriority <positive_integer>
- show lacp

Exemple :

```
1 set lacp -sysPriority 50
2 <!--NeedCopy-->
```


Pour définir la priorité d'un nœud de cluster spécifique, ouvrez une session sur l'adresse IP du cluster et, à l'invite de commandes, tapez les commandes suivantes :

- set lacp -sysPriority <positive_integer> -ownerNode <positive_integer>
- show lacp

Exemple :

```
set lacp -sysPriority 50 -ownerNode 2
<!--NeedCopy-->
```

Pour configurer la priorité système LACP à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > Interfaces et, dans la liste Action, sélectionnez Définir LACP.
2. Spécifiez la priorité système et le nœud propriétaire (applicable uniquement pour une configuration de cluster).

Création de canaux d'agrégation de liens

Pour créer un canal d'agrégation de liens à l'aide de LACP, vous devez activer LACP et spécifier la même clé LACP sur chaque interface que vous voulez faire partie du canal. Par exemple, si vous activez LACP et définissez la clé LACP sur 3 sur les interfaces 1/1 et 1/2, un canal d'agrégation de liens LA/3 est créé et les interfaces 1/1 et 1/2 y sont automatiquement liées.

Remarque :

- Lorsque vous activez LACP sur une interface réseau, vous devez spécifier la clé LACP.
- Par défaut, LACP est désactivé sur toutes les interfaces réseau.

Pour créer un canal LACP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- set interface <id>[-Mode LACP] <lacpMode>[-LAPKey] <positive_integer>[-LACP Priority] <positive_integer>[-LACP Timeout (LONG | COURT)]
- Afficher l'interface []<id>

Pour créer un canal LACP à l'aide de l'interface graphique :

Accédez à Système > Réseau > Interfaces, ouvrez l'interface réseau et définissez les paramètres.

Modification des canaux d'agrégation de liens

Après avoir créé un canal LACP en spécifiant des interfaces, vous pouvez modifier les propriétés du canal.

Pour modifier un canal LACP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- définir le canal <id>[-ifnum <interfaceName>…] [-state (ACTIVÉ | DÉSACTIVÉ)] [-speed] [-Flow Control] [-Hamonitor (ON | OFF)] [-IFALIAS] [-débit] [-tagall (ON | OFF)] [-bande passante élevée <positive_integer>[- Bande passante normale]]
- afficher le canal

Exemple :

```
1 > set channel LA/3 -state ENABLED -speed 10000
2  Done
3 <!--NeedCopy-->
```

Pour modifier un canal LACP à l'aide de l'interface graphique :

Accédez à Système > Réseau > Canaux et modifiez un canal LACP existant.

Suppression d'un canal d'agrégation de liens

Pour supprimer un canal d'agrégation de liens créé à l'aide de LACP, vous devez désactiver LACP sur toutes les interfaces qui font partie du canal.

Pour supprimer un canal LACP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- set interface <id> -lacpMode Disable
- show interface []

Pour supprimer un canal LACP à l'aide de l'interface graphique :

Accédez à Système > Réseau > Interfaces, ouvrez l'interface réseau et désactivez l'option Activer LACP.

Redondance de liaison à l'aide de canaux LACP

La redondance des liens à l'aide de canaux LACP permet à Citrix ADC de diviser un canal LACP en sous-canaux logiques, un sous-canal étant actif et les autres en mode veille. Si le sous-canal actif ne parvient pas à atteindre un seuil minimal de débit, l'un des sous-canaux de secours devient actif et prend le relais.

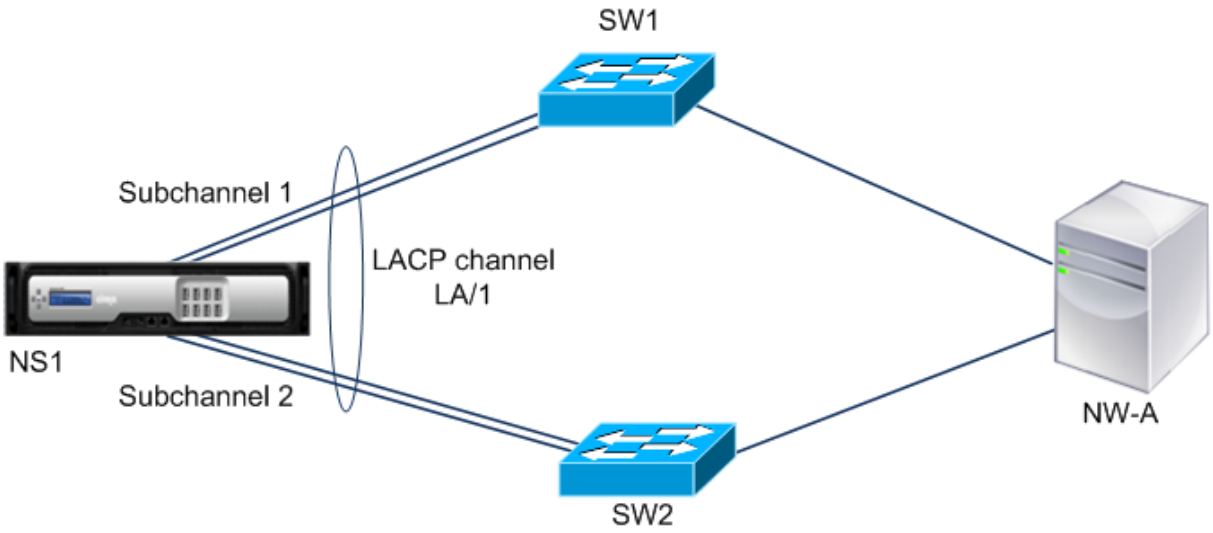
Un sous-canal est créé à partir de liens qui font partie du canal LACP et sont connectés à un périphérique particulier. Par exemple, pour un canal LACP avec quatre interfaces sur un Citrix ADC, deux des interfaces connectées au périphérique A et les deux autres connectées au périphérique B, ADC crée deux sous-canaux logiques, un sous-canal avec deux liaisons au périphérique A et un autre sous-canal avec deux liaisons au périphérique B.

Pour configurer la redondance de liaison pour un canal LACP, définissez le paramètre LRminThroughput, qui spécifie le seuil de débit minimal (en Mbps) à respecter par le sous-canal actif. La définition de ce paramètre crée automatiquement les sous-canaux. Lorsque le débit maximal pris en charge du canal actif est inférieur à la valeur LRminThroughput, le basculement de liaison se produit et un sous-canal de secours devient actif.

Si vous désactivez le paramètre lrminThroughput d'un canal LACP ou si vous définissez la valeur sur zéro, la redondance de liaison pour ce canal est désactivée, ce qui est le paramètre par défaut.

Exemple

Prenons un exemple de redondance de liaison configurée entre Citrix ADC NS1 et les commutateurs SW1 et SW2.



NS1 est connecté au périphérique réseau NW-A via SW1 et SW2.
Sur NS1, le canal LACP LA/1 est créé à partir des interfaces 1/1, 1/2, 1/3 et 1/4. Les interfaces 1/1 et 1/2 de NS1 sont connectées à SW1, et les interfaces 1/3 et 1/4 sont connectées à SW2. Chacune des quatre liaisons prend en charge un débit maximal de 1000Mbps.
Lorsque le paramètre LRminThroughput est défini sur une certaine valeur (par exemple 2000), NS1 crée deux sous-canaux logiques à partir de LA/1, un sous-canal (par exemple sous-canal 1) utilisant les interfaces 1/1 et 1/2 (connectée à SW1), et l'autre sous-canal (sous-canal 2) utilisant les interfaces 1/3 et 1/4 (connectée à SW2).

NS1 applique un algorithme pour rendre un sous-canal (disons le sous-canal 1) actif et mettre l'autre en veille. NS1 et le périphérique réseau NW-A sont accessibles l'un à l'autre via uniquement le sous-canal actif.

Supposons que le sous-canal 1 soit actif et que son débit maximal pris en charge tombe en dessous de la valeur LRminThroughput (par exemple, l'une de ses liaisons échoue et le débit maximal pris en charge tombe à 1000 Mbps). Le sous-canal 2 devient actif et prend le relais.

Redondance de liaison à l'aide de canaux LACP dans une configuration de haute disponibilité

Dans une configuration haute disponibilité (HA), si vous souhaitez configurer le basculement HA basé sur le débit (paramètre débit) et la redondance des liens (paramètre LRminThroughput) sur un canal LACP, vous devez définir le paramètre débit sur une valeur inférieure ou égale à celle du paramètre LRminThroughput.

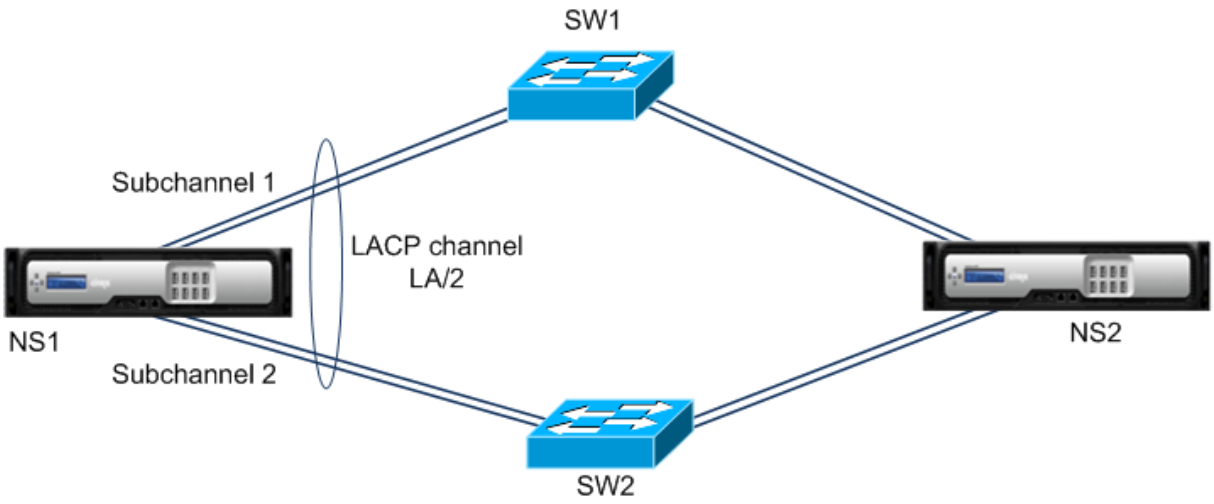
Le débit maximal pris en charge d'un canal LACP est calculé comme le débit maximal pris en charge du sous-canal actif.

Si la valeur du paramètre de débit est égale ou inférieure à la valeur du paramètre lrminthroughput, le basculement HA se produit lorsque les deux conditions suivantes existent simultanément :

- Aucun des débits maximum pris en charge des sous-canaux ne correspond à la valeur du paramètre LRminThroughput.
- Le débit maximal pris en charge du canal LACP ne correspond pas à la valeur du paramètre de débit

Prenons un exemple d'installation HA avec Citrix ADC NS1 et NS2, avec les commutateurs SW1 et SW2. NS1 est connecté à NS2 via SW1 et SW2.

Sur NS1, le canal LACP LA/1 est créé à partir des interfaces 1/1, 1/2, 1/3 et 1/4. Les interfaces 1/1 et 1/2 de NS1 sont connectées à SW1, et les interfaces 1/3 et 1/4 sont connectées à SW2. Chacune des quatre liaisons prend en charge un débit maximal de 1000Mbps.



Voici les paramètres du paramètre LACP dans cet exemple :

Paramètre	Valeur
Débit	2 000
lrminthroughput	2 000

NS1 forme deux sous-canaux de LA/1, un sous-canal (disons sous-canal 1) utilisant les interfaces 1/1 et 1/2 (connectées à SW1), et l'autre sous-canal (sous-canal 2) utilisant les interfaces 1/3 et 1/4 (connectées à SW2). Chacun des deux sous-canaux prend en charge un débit maximal de 2000 Mbps. En appliquant un algorithme, NS1 rend un sous-canal (disons le sous-canal 1) actif et l'autre en veille.

Supposons que le sous-canal 1 soit actif et que son débit maximal pris en charge tombe en dessous de la valeur LRminThroughput (par exemple, l'une de ses liaisons échoue et le débit maximal pris en charge tombe à 1000 Mbps). Le sous-canal 2 devient actif et prend le relais. Le basculement HA ne se produit pas, car le débit maximal pris en charge du canal LACP n'est pas inférieur à la valeur du paramètre de débit :

Débit maximal pris en charge du canal LACP = Débit maximal pris en charge du canal actif = Débit maximal pris en charge du sous-canal 2 = 2000 Mbps

Si le débit maximal pris en charge du sous-canal 2 est également inférieur à la valeur lrminthroughput (par exemple, l'une de ses liaisons échoue et le débit maximal pris en charge tombe à 1000 Mbps), le basculement HA se produit, car le débit maximal pris en charge du canal LACP est alors inférieur au paramètre de débit valeur :

Configurer la redondance des liens à l'aide des canaux LACP

Pour configurer la redondance des liens pour un canal LACP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour configurer le canal et vérifier la configuration :

- **set channel** <id> -lrMinThroughput <positive_integer>
- **afficher le canal**

Exemple :

```
1 > set channel la/1 - lrMinThroughput 2000
2 Done
3 > set channel la/2 - throughput 2000 - lrMinThroughput 2000
4 Done
5 <!--NeedCopy-->
```

Pour configurer la redondance de liaison pour un canal LACP à l'aide de l'interface graphique

1. Accédez à Système > Réseau > Canaux.
2. Dans le volet d'informations, sélectionnez un canal LACP pour lequel vous souhaitez configurer la redondance des liens, puis cliquez sur Modifier.
3. Dans la boîte de dialogue Configurer le canal LACP, définissez le paramètre lrminThroughput.
4. Cliquez sur Fermer.

Jeu d'interfaces redondantes

January 21, 2021

Un ensemble d'interfaces redondantes est un ensemble d'interfaces où l'une des interfaces est active et les autres sont en veille. Si l'interface active échoue, l'une des interfaces de secours prend le relais et devient active.

Les principaux avantages de l'utilisation de jeux d'interfaces redondants sont les suivants :

- Un ensemble d'interfaces redondantes assure la fiabilité de la connexion entre l'appliance Citrix ADC et un périphérique homologue en fournissant des liens de sauvegarde entre eux.
- Contrairement à la redondance de liaison utilisant LACP, aucune configuration n'est requise sur le périphérique homologue pour un ensemble d'interfaces redondantes. Pour le périphérique homologue, l'ensemble d'interfaces redondantes apparaît comme des interfaces individuelles et non comme un ensemble ou une collection.
- Dans une configuration haute disponibilité (HA), les jeux d'interfaces redondantes peuvent réduire le nombre de basculements HA.

> **Remarque**
>
> L'ensemble d'interfaces redondantes était auparavant connu sous le nom de « bundle de cartes réseau » lorsqu'il a été introduit dans la version 10.5.

Fonctionnement de l'ensemble d'interfaces redondantes

Pour un ensemble d'interfaces redondantes, l'appliance Citrix ADC dérive une adresse MAC sur la base d'un algorithme interne et l'affecte au jeu d'interfaces redondantes. Cette adresse MAC est partagée par toutes les interfaces membres et est utilisée uniquement par l'interface active à la fois. L'interface active diffuse des messages GARP, qui contiennent l'adresse MAC attribuée à l'ensemble d'interfaces redondantes et non l'adresse MAC physique de l'interface. Lorsque l'interface active actuelle échoue et est reprise par une autre interface, la nouvelle interface active envoie des messages GARP. Le périphérique homologue met à jour sa table de transfert avec les nouvelles informations de l'interface active. Les interfaces de secours n'envoient aucun message GARP. Les interfaces de secours n'envoient aucun paquet et déposent tous les paquets qu'elles reçoivent.

Dans un ensemble d'interfaces redondantes, la sélection de l'interface membre comme active est basée sur l'un des facteurs suivants :

- **Priorité de l'interface redondante**. Il s'agit d'un paramètre d'une interface et il définit la priorité de l'interface dans une interface redondante définie pour la sélection de membres actifs. Ce paramètre spécifie un entier positif. Réduisez la valeur, plus la priorité de la sélection des membres actifs est élevée. L'interface membre ayant la priorité la plus élevée (valeur la plus basse) est sélectionnée comme interface active du jeu d'interfaces redondantes.

- **Ordre de liaison des interfaces membres**. Si toutes les interfaces membres ont la même priorité d'interface redondante, l'interface membre qui était liée en premier au jeu d'interfaces redondantes est sélectionnée comme interface active du jeu d'interfaces redondantes.

Dans un ensemble d'interfaces redondantes, la sélection active de l'interface est déclenchée dans l'un des événements suivants :

- Lorsque l'interface active actuelle échoue ou que vous la désactivez.
- Lorsque vous définissez la priorité d'une interface de secours sur une valeur inférieure à celle de l'interface active actuelle. L'interface de secours prend le relais comme interface active.
- Lorsque vous liez une interface dont la priorité est inférieure à celle de l'interface active actuelle. L'interface nouvellement liée prend le relais comme interface active.

Points à prendre en considération pour la configuration d'ensembles d'interfaces redondants

Tenez compte des points suivants avant de configurer un ensemble d'interfaces redondantes :

- Dans une appliance autonome ou dans une configuration à haute disponibilité, un jeu redondant de liaison est spécifié dans la notation LR/X, où X peut aller de 1 à 4. Par exemple, LR/1.
- Dans une configuration haute disponibilité, les configurations de jeu d'interface redondantes ne se propagent pas ou ne se synchronisent pas vers le nœud secondaire.
- Vous pouvez configurer un maximum de quatre jeux d'interfaces redondantes sur une appliance Citrix ADC.
- Vous pouvez lier un maximum de 16 interfaces à un ensemble d'interfaces redondantes.
- Les interfaces membres d'un jeu d'interfaces redondantes ne peuvent pas être liées à un autre jeu d'interfaces redondantes.
- Les interfaces membres d'un ensemble d'interfaces redondantes ne peuvent pas être liées à un canal d'agrégat de liaison (LA).
- Les canaux LA ne peuvent pas être liés à un jeu d'interfaces redondantes.
- Les jeux d'interfaces redondants ne peuvent pas être liés à un canal LA.
- Dans une configuration de cluster :
  - Les jeux d'interfaces redondants ne peuvent pas être liés à une agrégation de liens de cluster.
  - Un jeu de liens redondants est spécifié en notation N/LR/X (par exemple, 1/LR/3). Où :
    N est l'ID du nœud de cluster sur lequel l'ensemble d'interfaces redondantes doit être créé.
    X est un identificateur d'ensemble redondant de liaison sur un nœud de cluster. X peut varier de 1-4.
  - Une agrégation de liens de cluster ne peut pas être liée à un ensemble d'interfaces redondantes.
  - Un jeu d'interfaces redondantes peut inclure uniquement les interfaces du nœud auquel appartient le jeu d'interfaces redondantes.

- Une configuration de jeu de redondance elink existant sur une appliance autonome passe automatiquement à la notation de cluster (N/LR/X) après l'ajout de l'appliance à une configuration de cluster.

Étapes de configuration

La configuration de l'interface redondante définie sur une appliance Citrix ADC comporte les tâches suivantes :

- **Créez un ensemble d'interfaces redondantes**. Utilisez l'opération de commande de canal pour créer un ensemble d'interfaces redondantes.

  Dans une appliance autonome ou dans une configuration à haute disponibilité, un jeu redondant de liaison est spécifié dans la notation LR/X, où X peut aller de 1 à 4. Par exemple, LR/1.

  Dans une configuration de cluster, un jeu de liens redondants est spécifié dans N/LR/X (par exemple, 1/LR/3), où : N est l'ID du nœud de cluster sur lequel le jeu d'interfaces redondantes doit être créé, X est l'identifiant de jeu redondant de lien sur un nœud de cluster. X peut varier de 1-4.

- **Liez les interfaces à l'ensemble d'interfaces redondantes**. Associez les interfaces souhaitées au jeu d'interfaces redondantes. Une interface ne peut pas faire partie de plusieurs ensembles d'interfaces redondantes.
- **(Facultatif) Définit une priorité d'interface redondante sur l'interface membre**. Utilisez l'opération de commande d'interface pour définir la priorité d'interface redondante sur une interface membre souhaitée d'un ensemble d'interfaces redondantes.

Pour créer une interface redondante définie à l'aide de l'interface de ligne de commande :

À l'invite de commandes :

- add channel <ID>
- show channel <ID>

Pour lier des interfaces à une interface redondante définie à l'aide de l'interface de ligne de commande :

À l'invite de commandes :

- bind channel <ID> <ifnum>
- show channel <ID>

Pour définir une priorité d'interface redondante d'une interface à l'aide de l'interface de ligne de commande :

À l'invite de commandes :

- set interface <ID> -lrsetpriority <positive_integer>

- show interface <ID>

Exemple de configuration 1 :

Dans l'exemple suivant, le jeu d'interfaces redondantes LR/1 est créé et les interfaces 1/1, 1/2, 1/3 et 1/4 sont liées à LR/1. La priorité d'interface redondante est définie sur une valeur par défaut de 1024 pour toutes ces interfaces membres. La sortie de la commande show channel indique que l'interface 1/1 est l'interface active actuelle pour l'interface redondante lr/1.

```
> add channel lr/1
 Done
> bind channel lr/1 1/1 1/2 1/3 1/4
 Done
> show channel
1)    Interface LR/1 (Link Redundant) #23
        flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON, 802.1q>
        MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0h00m00s
        Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
                 throughput 0
        Actual: throughput 1000
        LLDP Mode: NONE,
        RX: Pkts(1) Bytes(52) Errs(0) Drops(1) Stalls(0)
        TX: Pkts(2) Bytes(84) Errs(0) Drops(4) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
                1/1: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Active Member
                1/2: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/3: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/4: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
Done
<!--NeedCopy-->
```

Exemple de configuration 2 :

Dans l'exemple suivant, la priorité d'interface redondante de l'interface membre 1/4 est définie sur 100, ce qui est inférieur à la priorité d'interface redondante définie de toutes les autres interfaces membres de LR/1.

La sortie de la commande show channel indique que l'interface 1/4 est l'interface active actuelle pour le jeu d'interfaces redondantes LR/1.

```
> set interface 1/4 -lrsetPriority 100
```



```
Done
> show channel
1)      Interface LR/1 (Link Redundant) #23
        flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON, 802.1q>
        MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0h00m00s
        Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
                 throughput 0
        Actual: throughput 1000
        LLDP Mode: NONE,
        RX: Pkts(1) Bytes(52) Errs(0) Drops(1) Stalls(0)
        TX: Pkts(2) Bytes(84) Errs(0) Drops(4) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
                1/1: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/2: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/3: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/4: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Active Member
Done
<!--NeedCopy-->
```

Exemple de configuration 3 :

Envisagez une configuration de cluster de quatre nœuds N1, N2, N3 et N4. Dans cet exemple, le jeu d'interfaces redondantes 1/LR/3 est créé sur le nœud N1 et les interfaces 1/1/1, 1/1/2 et 1/1/3 y sont liées. La priorité d'interface redondante est définie sur une valeur par défaut de 1024 pour toutes ces interfaces membres. La sortie de la commande show channel indique que l'interface 1/1/1 est l'interface active actuelle pour l'ensemble d'interfaces redondantes 1/LR/3.

```
    > add channel 1/LR/3

    Done
    > bind channel 1/LR/3 1/1/1 1/1/2 1/1/3

    Done
    > show channel
    1)    Interface 1/LR/3 (Link Redundant) #14
            flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON,
               802.1q>
            MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0
               h00m00s
            Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
```



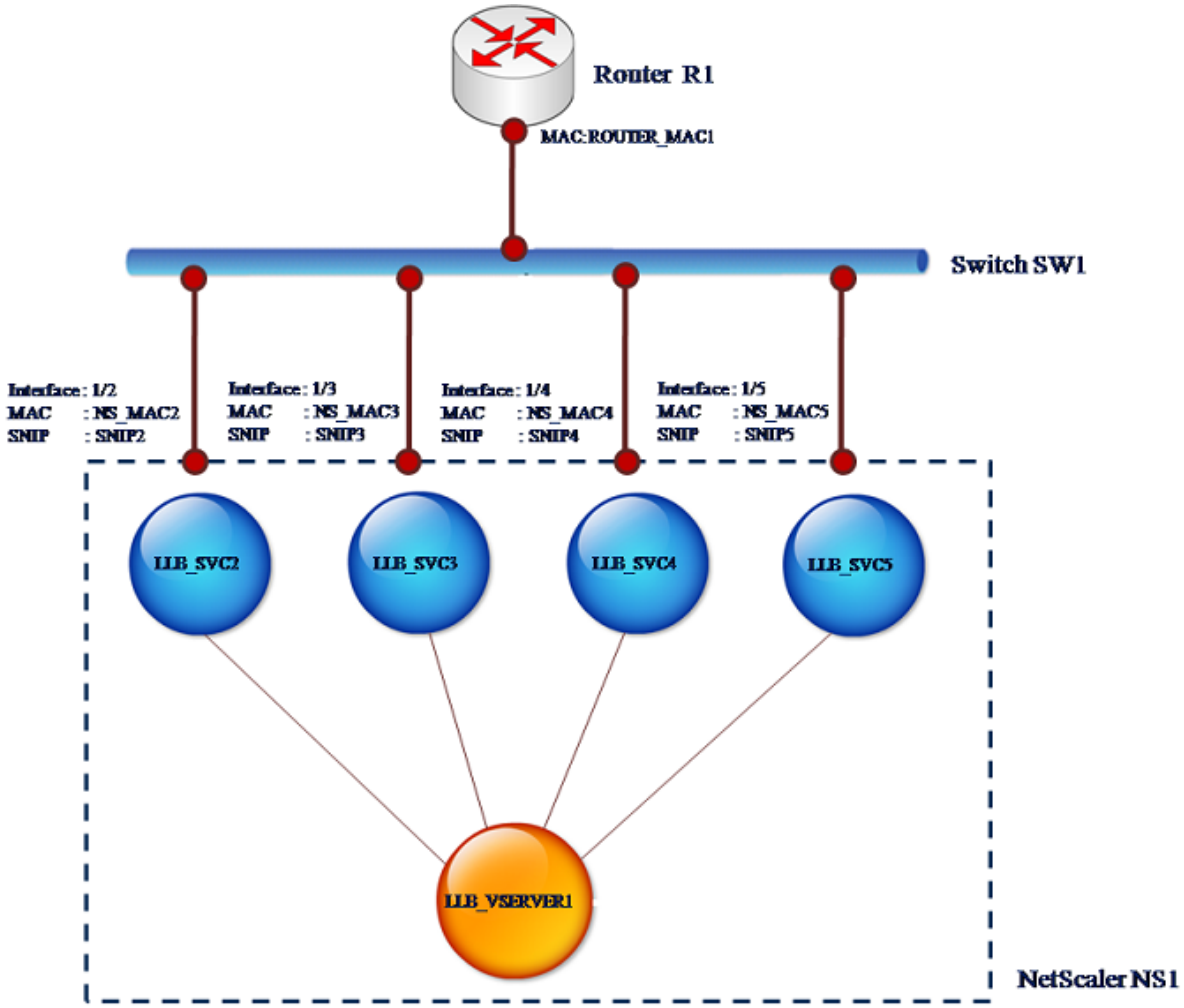
```
12              throughput 0
13              Actual: throughput 1000
14              LLDP Mode: NONE,
15              RX: Pkts(66) Bytes(4406) Errs(0) Drops(82) Stalls(0)
16              TX: Pkts(55) Bytes(2626) Errs(0) Drops(145) Stalls(0)
17              NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted
                    (0)
18              Bandwidth thresholds are not set.
19
20              1/1/1: UTP-1000-FULL-OFF UP  0h14m06s LR Active Member
21              1/1/2: UTP-1000-FULL-OFF UP  0h14m06s LR Inactive Member
22              1/1/3: UTP-1000-FULL-OFF UP  0h14m06s LR Inactive Member
23
24      Done
25  <!--NeedCopy-->
```

Liaison d'une adresse SNIP à une interface

August 20, 2021

Vous pouvez désormais lier une adresse SNIP appartenant à Citrix ADC à une interface sans utiliser de VLAN de couche 3. Tous les paquets liés à l'adresse SNIP passent uniquement par l'interface liée.

Cette fonctionnalité peut être utile dans un scénario où le commutateur en amont ne prend pas en charge les canaux d'agrégation de liens et que vous souhaitez que l'appliance Citrix ADC répartit le trafic provenant d'un serveur sur les quatre liaisons vers le commutateur en amont, comme illustré dans l'illustration suivante.



Les tableaux suivants décrivent les exemples de paramètres pour le scénario :

Entité	Nom	Valeur
Adresses SNIP sur NS1	SNIP2 (à titre de référence uniquement)	10.10.10.2
	SNIP3 (à titre de référence uniquement)	10.10.10.3
	SNIP4 (à titre de référence uniquement)	10.10.10.4
	SNIP5 (à titre de référence uniquement)	10.10.10.5
Serveur virtuel LLB sur NS1	LLB_VSERVER1	-
Moniteur transparent sur NS1	TRANS_MON	-

Entité	Nom	Valeur
Services LLB sur NS1	LLB_SVC2	10.10.10.240
	LLB_SVC3	10.10.10.120
	LLB_SVC4	10.10.10.60
	LLB_SVC5	10.10.10.30
Adresse MAC de l'interface 1/2 sur NS1	NS_MAC_2 (à titre de référence uniquement)	00:e0:ed:0f:bc:e0
Adresse MAC de l'interface 1/3 sur NS1	NS_MAC_3 (à titre de référence uniquement)	00:e0:ed:0f:bc:df
Adresse MAC de l'interface 1/4 sur NS1	NS_MAC_4 (à titre de référence uniquement)	00:e0:ed:0f:bc:de
Adresse MAC de l'interface 1/5 sur NS1	NS_MAC_5 (à titre de référence uniquement)	00:e0:ed:1c:89:53
Adresse IP du routeur R1	Router_IP (à titre de référence uniquement)	10.10.10.1
Adresse MAC de l'interface de R1	ROUTER_MAC1 (à titre de référence uniquement)	00:21:a1:2d:db:cc

Pour configurer les paramètres de l'exemple :

1. Ajoutez quatre SNIP différents dans différentes plages de sous-réseau. Ceci est pour ARP à résoudre sur quatre liens différents. Pour plus d'informations sur la création d'une adresse SNIP, consultez Configuration des adresses IP de sous-réseau (SNIP).

   Exemple CLI :

   ```
   > add ns ip 10.10.10.2 255.255.255.0 -type SNIP
    Done
   > add ns ip 10.10.10.3 255.255.255.128 - type SNIP
   Done
   > add ns ip 10.10.10.4 255.255.255.192 - type SNIP
   Done
   > add ns ip 10.10.10.5 255.255.255.224 - type SNIP
   Done
   <!--NeedCopy-->
   ```

2. Ajoutez quatre services factices différents dans les sous-réseaux SNIP ajoutés. Ceci permet de s'assurer que le trafic est envoyé avec l'adresse IP source comme l'un des quatre SNIP con-

figurés. Pour plus d'informations sur la création d'un service, voir Configurer l'équilibrage de charge de base.

Exemple CLI :

```
> add service LLB_SVC2 10.10.10.240 any *
 Done
> add service LLB_SVC3 10.10.10.120 any *
 Done
> add service LLB_SVC4 10.10.10.60 any *
 Done
> add service LLB_SVC5 10.10.10.30 any *
 Done
<!--NeedCopy-->
```

3. Ajoutez un moniteur ping transparent pour surveiller la Gateway. Liez le moniteur à chacun des services fictifs configurés. Ceci est de rendre l'état des services comme UP. Pour plus d'informations sur la création d'un moniteur transparent, voir Configurer les moniteurs dans une configuration d'équilibrage de charge.

   Exemple CLI :

```
> add monitor TRANS_MON ping -destIP 10.10.10.1 -transparent YES
 Done
> bind monitor TRANS_MON LLB_SVC2
 Done
> bind monitor TRANS_MON LLB_SVC3
 Done
> bind monitor TRANS_MON LLB_SVC4
 Done
> bind monitor TRANS_MON LLB_SVC5
 Done
<!--NeedCopy-->
```

4. Ajoutez un serveur virtuel d'équilibrage de charge de liaison (LLB) et liez les services factices à celui-ci. Pour plus d'informations sur la création d'un serveur virtuel LLB, voir Configuration d'un programme d'installation LLB de base.

   Exemple CLI :

```
> add lb vserver LLB_VSERVER1 any
 Done
> set lb vserver LLB_VSERVER1 -lbmethod ROUNDROBIN
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
```



```
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
<!--NeedCopy-->
```

5. Ajoutez le serveur virtuel LLB comme itinéraire LLB par défaut. Pour plus d'informations sur la création d'une route LLB, consultez Configuration d'une configuration LLB de base.

   Exemple CLI :

```
> add lb route 0.0.0.0 0.0.0.0  LLB_VSERVER1
 Done
<!--NeedCopy-->
```

6. Ajoutez une entrée ARP pour chacun des services factices avec l'adresse MAC de la Gateway. De cette façon, la Gateway est accessible via ces services factices. Pour plus d'informations sur l'ajout d'une entrée ARP, voir Configuration de l'ARP statique.

   Exemple CLI :

```
> add arp -ipaddress 10.10.10.240 -mac 00:21:a1:2d:db:cc -ifnum
   1/2
 Done
> add arp -ipaddress 10.10.10.120 -mac 00:21:a1:2d:db:cc -ifnum
   1/3
 Done
> add arp -ipaddress 10.10.10.60 -mac 00:21:a1:2d:db:cc -ifnum 1/4
 Done
> add arp -ipaddress 10.10.10.30 -mac 00:21:a1:2d:db:cc -ifnum 1/5
 Done
<!--NeedCopy-->
```

7. Liez une interface spécifique à un SNIP en ajoutant une entrée ARP pour chacun de ces SNIP. Ceci permet de s'assurer que le trafic de réponse atteindra la même interface à travers laquelle la requête est sortie. Pour plus d'informations sur l'ajout d'une entrée ARP, voir Configuration de l'ARP statique.

   Exemple CLI :

```
> add arp -ipAddress 10.10.10.2 -mac 00:e0:ed:0f:bc:e0 -ifnum 1/2
 Done
> add arp -ipAddress 10.10.10.3 -mac 00:e0:ed:0f:bc:df -ifnum 1/3
 Done
```



```
> add arp -ipAddress 10.10.10.4 -mac 00:e0:ed:0f:bc:de -ifnum 1/4
 Done
> add arp -ipAddress 10.10.10.5 -mac 00:e0:ed:1c:89:53 -ifnum 1/5
 Done
<!--NeedCopy-->
```

Surveiller la table de pont et modifier le temps de vieillissement

August 20, 2021

L'appliance Citrix ADC relie les trames sur la base de la recherche de table de pont de l'adresse MAC de destination et de l'ID VLAN. Toutefois, l'appliance effectue le transfert uniquement lorsque le mode de couche 2 est activé.

La table de pont est générée dynamiquement, mais vous pouvez l'afficher, modifier la durée de vieillissement de la table de pont et afficher les statistiques de pontage. Toutes les entrées MAC de la table de pont sont mises à jour avec le temps de vieillissement.

Pour définir la durée de vieillissement des entrées de table de pont à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set l2param** -**bridgeagetimeout** <positive_integer>
- **show l2param**

Exemple :

```
> set l2param -bridgeagetimeout 90
 Done
<!--NeedCopy-->
```

Pour afficher les statistiques d'une table de pont à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **stat bridge**

Pour définir la durée de vieillissement des entrées de table de pont à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau**. Dans la page **Réseau**, dans la section **Paramètres**, cliquez sur **Configurer les paramètres de la couche 2** et définissez le paramètre **Valeur d'expiration pour les entrées de table de pont (secondes)**.

Pour afficher les statistiques d'une table de pont à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Table de pont**, sélectionnez l'adresse MAC, puis cliquez sur **Statistiques** .

Appliances Citrix ADC en mode actif-actif à l'aide de VRRP

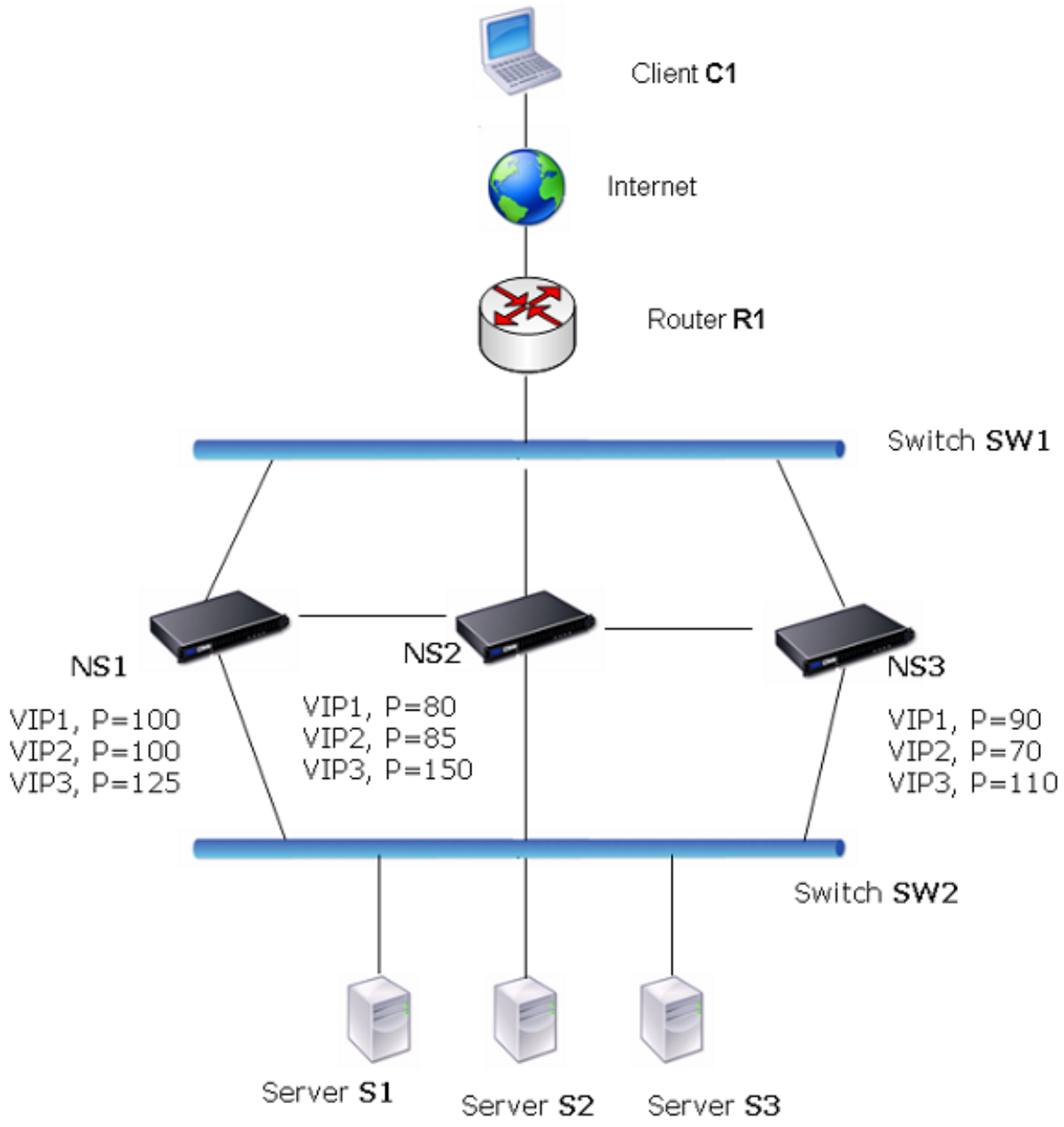
January 21, 2021

Un déploiement actif-actif, en plus de prévenir les temps d'arrêt, permet une utilisation efficace de toutes les appliances Citrix ADC dans le déploiement. En mode de déploiement actif, les mêmes VIP sont configurés sur toutes les appliances Citrix ADC de la configuration, mais avec des priorités différentes, de sorte qu'un VIP donné ne peut être actif que sur une seule appliance à la fois.

Le VIP actif est appelé VIP maître, et les VIP correspondants sur les autres appliances Citrix ADC sont appelés VIP de sauvegarde. Si un VIP maître échoue, le VIP de sauvegarde avec la priorité la plus élevée prend le relais et devient le VIP maître. Toutes les appliances Citrix ADC dans un déploiement actif utilisent le protocole VRRP (Virtual Router Redundancy Protocol) pour annoncer leurs VIP et les priorités correspondantes à intervalles réguliers.

Les appliances Citrix ADC en mode actif peuvent être configurées de manière à ce qu'aucun Citrix ADC ne soit inactif. Dans cette configuration, différents ensembles de VIP sont actifs sur chaque Citrix ADC. Par exemple, dans le diagramme suivant, VIP1, VIP2, VIP3 et VIP4 sont configurés sur les appliances NS1, NS2 et NS3. En raison de leurs priorités, VIP1 et VIP 2 sont actifs sur NS1, VIP3 est actif sur NS2 et VIP 4 est actif sur NS3. Si, par exemple, NS1 échoue, VIP1 sur NS3 et VIP2 sur NS2 deviennent actifs.

Figure 1. Une configuration active-active



Les appliances Citrix ADC dans le diagramme ci-dessus traitent le trafic comme suit :

1. Le client C1 envoie une demande à VIP1. La requête atteint R1.
2. R1 n'a pas d'entrée ARP pour VIP1, il diffuse donc une demande ARP pour VIP1.
3. VIP1 est actif dans NS1, donc NS1 répond avec une adresse MAC source comme MAC virtuel (par exemple MAC1 virtuel) associé à VIP1, et VIP1 comme adresse IP source.
4. SW1 apprend le port pour VIP1 à partir de la réponse ARP et met à jour sa table de pont.
5. R1 met à jour l'entrée ARP avec virtuels MAC1 et VIP1.

6. R1 transmet le paquet au VIP1 sur NS1.
7. L'algorithme d'équilibrage de charge de NS1 sélectionne le serveur S2, et NS1 ouvre une connexion entre l'une de ses adresses SNIP et S2.
8. S2 répond au SNIP sur Citrix ADC.
9. NS1 envoie la réponse de S2 au client. Dans la réponse, NS1 insère l'adresse MAC de l'interface physique comme adresse MAC source et VIP1 comme adresse IP source.
10. Si NS1 échoue, les appliances Citrix ADC utilisent le protocole VRRP pour sélectionner le VIP1 avec la priorité la plus élevée. Dans ce cas, VIP1 sur NS3 devient actif et les deux étapes suivantes mettent à jour la configuration active-active.
11. NS3 diffuse un message GARP pour VIP1. Dans le message, MAC1 virtuel est l'adresse MAC source et VIP1 est l'adresse IP source.
12. SW1 apprend le nouveau port pour MAC1 virtuel à partir de la diffusion GARP et met à jour sa table de pont pour envoyer les demandes clientes suivantes pour VIP1 à NS3. R1 met à jour sa table ARP.

La priorité d'un VIP peut être modifiée par le suivi de l'état de santé. Si vous activez le suivi de l'intégrité, assurez-vous que la préemption est également activée, afin qu'un VIP dont la priorité est abaissée puisse être préempté par un autre VIP.

Dans certaines situations, le trafic peut atteindre un VIP de sauvegarde. Pour éviter de supprimer ce trafic, vous pouvez activer le partage, sur une base par nœud, lorsque vous créez une configuration active-active. Vous pouvez également activer l'option d'envoi global au maître. Sur un nœud sur lequel le partage est activé, il a priorité sur l'envoi au maître.

Suivi de la santé

La priorité de base (plage de BP 1 à 255) détermine ordinairement quel VIP est le VIP principal, mais la priorité effective (EP) peut également influer sur la détermination.

Par exemple, si un VIP sur NS1 a une priorité de 101 et que le même VIP sur NS2 a une priorité de 99, le VIP sur NS1 est actif. Cependant, si deux serveurs vServer utilisent le VIP sur NS1 et que l'un d'eux tombe en panne, le suivi de l'intégrité peut réduire l'EP de VIP sur NS1. VRRP fait ensuite le VIP sur NS2 le VIP actif.

Voici les options de suivi de l'état pour modifier EP :

- **AUCUN.** Pas de suivi. EP = BP
- **ALL.** Si tous les serveurs virtuels sont UP, alors EP = BP. Sinon, EP = 0.
- **ONE.** Si au moins un serveur virtuel est UP, alors EP = BP. Sinon, EP = 0.
- **PROGRESSIVE.** Si TOUS les serveurs virtuels sont UP, alors EP = BP. Si TOUS les serveurs virtuels sont DOWN, EP = 0. Sinon EP = BP (1 - K/N), où N est le nombre total de serveurs virtuels associés au VIP et k le nombre de serveurs virtuels qui sont en panne.

Remarque : si vous spécifiez une valeur autre que NONE, la préemption doit être activée afin que le VIP de sauvegarde avec la priorité la plus élevée devienne actif si la priorité du VIP maître est rétrogradée.

Préemption

La préemption d'un VIP actif par un autre VIP qui atteint une priorité supérieure est activée par défaut et devrait normalement être activée. Dans certains cas, cependant, vous pouvez le désactiver. La préemption est un paramètre par nœud pour chaque VIP.

La préemption peut se produire dans les situations suivantes :

- Un VIP actif tombe en panne et un VIP avec une priorité inférieure prend sa place. Si le VIP ayant la priorité la plus élevée revient en ligne, il préempte le VIP actuellement actif.
- Le suivi de l'intégrité fait que la priorité d'un VIP de sauvegarde devient supérieure à celle du VIP actif. Le VIP de sauvegarde préempte ensuite le VIP actif.

Partage

Si le trafic atteint un VIP de sauvegarde, le trafic est supprimé, sauf si l'option de partage est activée sur le VIP de sauvegarde. Ce comportement est un paramètre par nœud pour chaque VIP et est désactivé par défaut.

Dans la figure **Une configuration active** VIP1 sur NS1 est active et VIP1 sur NS2 et NS3 sont des sauvegardes. Dans certaines circonstances, le trafic peut atteindre VIP1 sur la NS2. Si le partage est activé sur NS2, ce trafic est traité au lieu d'être supprimé.

Configuration du mode actif-actif

August 20, 2021

Sur chaque appliance Citrix ADC que vous souhaitez déployer en mode actif, vous devez ajouter un MAC virtuel et lier le MAC virtuel à un VIP. Le MAC virtuel d'un VIP donné doit être identique sur chaque appliance. Par exemple, si VIP 10.102.29.5 est créé sur les appliances, un ID de routeur virtuel (VRID) doit être créé sur chaque Citrix ADC et lié à VIP 10.102.29.5 sur chaque Citrix ADC. Lorsque vous liez un MAC virtuel à un VIP, l'appliance envoie des publicités VRRP à chaque VLAN lié à ce VIP. Le MAC virtuel peut être partagé par différents VIP configurés sur le même Citrix ADC.

Configuration du mode actif IPv4

Effectuez les tâches suivantes sur chacune des appliances Citrix ADC à inclure dans la configuration active-active :

- **Ajoutez une adresse MAC virtuelle**. Ajoutez une adresse MAC virtuelle en ajoutant un VRID. Vous pouvez également spécifier une priorité et activer ou désactiver la préemption et le partage sur cette adresse VRID.
- **Ajoutez une adresse VIP et associez le VRID du MAC virtuel**. Ajoutez une adresse VIP et définissez le paramètre VRID sur le VRID nouvellement créé. Les attributs du VRID (par exemple, priorité et préemption) sont liés à cette adresse VIP.
  Remarque : La même adresse VIP doit être ajoutée à tous les autres appliances Citrix ADC.

Pour ajouter une adresse MAC virtuelle à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- **ajouter VRID** <id>[-**priorité**] <positive_integer>[-**préemption** (**ACTIVÉ**|**DÉSACTIVÉ**)][-**sharing** (**ENABLED**|**DISABLED**)] [-**suivi**]<tracking>
- **show vrid**

Pour ajouter une adresse VIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns ip** <IPv4Address> -type VIP -vrid <value>
- **show ns ip**

Pour configurer un MAC virtuel à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VMAC**, sous l'onglet **VMAC**, ajoutez un nouveau MAC virtuel ou modifiez un MAC virtuel existant.
2. Définissez les paramètres suivants :
   - ID du routeur virtuel
   - Priority
   - Suivi
   - Préemption
   - Partage

Pour configurer une adresse VIP et y associer le VRID à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IP**, sous l'onglet **IPv4s**, ajoutez une adresse IP de type VIP.
2. Lors de l'ajout de l'adresse IP, sélectionnez l'ID du routeur **virtuel dans la liste déroulante Id du routeur virtuel** .

Exemple de configuration :

L'exemple de configuration suivant permet de déployer les appliances Citrix ADC NS1 et NS2 en mode actif IPv4. L'adresse VIP 203.0.113.10 est configurée sur NS1 et NS2, avec une valeur de priorité dif-

férente sur chaque appliance. Sur chaque appliance, cette adresse VIP est liée à une adresse MAC virtuelle. 203.0.113.10 est maître sur NS2, car sa priorité (200) sur NS2 est supérieure à celle sur NS1 (100).

```
    Settings on NS1

    > add vrid 10 -Priority 100 -Preemption Enabled -sharing Enabled

    Done

    > add ns ip 203.0.113.10 -type VIP -vrid 10

    Done

    Settings on NS2

    > add vrid 10 -Priority 200 -Preemption Enabled -sharing Enabled

    Done

    > add ns ip 203.0.113.10 -type VIP -vrid 10

    Done
<!--NeedCopy-->
```

Configuration du mode actif IPv6

Effectuez les tâches suivantes sur chacune des appliances Citrix ADC à inclure dans la configuration active-active :

- **Ajoutez une adresse MAC6 virtuelle**. Ajoutez une adresse MAC6 virtuelle en ajoutant un VRID6. Vous pouvez également spécifier une priorité et activer ou désactiver la préemption et le partage sur cette adresse VRID6.
- **Ajoutez une adresse VIP6**. Ajoutez une adresse VIP6. Définissez le paramètre VRID6 sur le VRID6 du Mac6 virtuel nouvellement créé. Les attributs du MAC6 virtuel (par exemple, priorité et préemption) sont liés à cette adresse VIP6.
  Remarque : La même adresse VIP6 doit être ajoutée à tous les autres appliances Citrix ADC.

Pour ajouter une adresse MAC6 virtuelle à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **ajouter VriD6** <id>[-**priorité**] [-**préemption** (**ACTIVÉ** | **DÉSACTIVÉ**)] [-**partage** (**ACTIVÉ** | **DÉSACTIVÉ**)]

- **show vrID6**

Pour ajouter une adresse VIP6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns ip6** <IPv6Address> -**type** VIP -**vrid** <value>
- **show ns ip6**

Pour configurer un MAC6 virtuel à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VMAC, sous** l'onglet **VMAC6**, ajoutez un nouveau MAC6 virtuel ou modifiez un **VMAC6** existant.
2. Définissez les paramètres suivants :
   - ID du routeur virtuel
   - Priority
   - Préemption
   - Partage

Pour configurer une adresse VIP6 et y associer le VRID à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IP**, sous l'onglet **IPv6s**, ajoutez une adresse IPv6 de type VIP.
2. Lors de l'ajout de l'adresse VIP6, sélectionnez le VRID6 dans la liste déroulante **Id de routeur virtuel** .

Exemple de configuration :

L'exemple de configuration suivant concerne le déploiement des appliances Citrix ADC NS1 et NS2 en mode actif IPv6. L'adresse VIP6 2001:db8 : :5001 est configurée sur NS1 et NS2, avec une valeur de priorité différente sur chaque appliance. Sur chaque appliance, cette adresse VIP6 est liée à une adresse MAC6 virtuelle. 2001:db8::5001 est maître sur NS2, car sa priorité (200) sur NS2 est supérieure à celle sur NS1 (100).

```
    Settings on NS1
    > add vrid6 10 -Priority 100 -Preemption Enable -sharing Enable

    Done
    > add ns ip6 2001:db8::5001 -type VIP -vrid6 10

    Done
    Settings on NS2
    > add vrid6 10 -Priority 200 -Preemption Enable -sharing Enable

    Done
    > add ns ip6 2001:db8::5001 -type VIP -vrid6 10

    Done
<!--NeedCopy-->
```

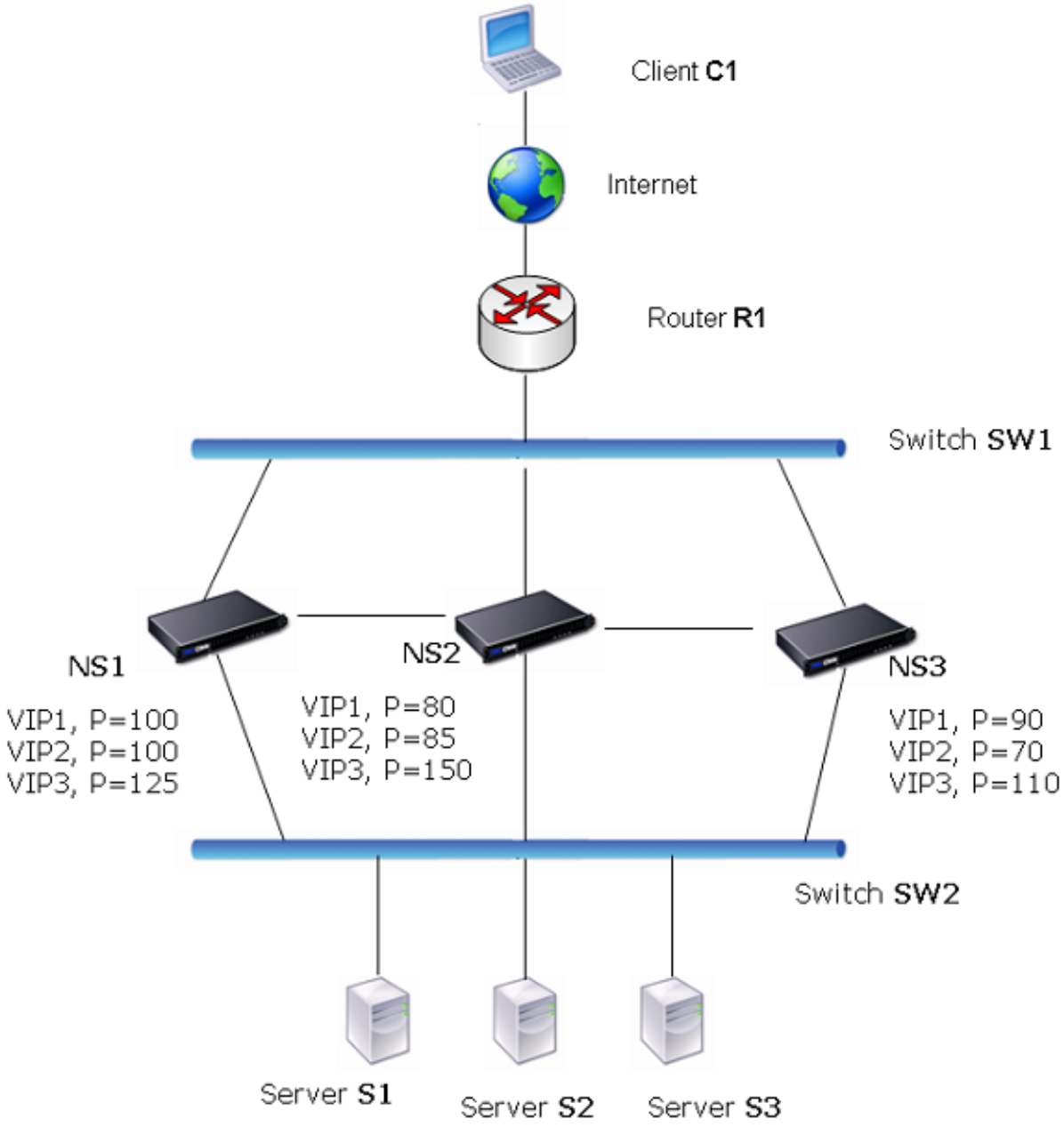

Configuration de l’envoi vers le maître

August 20, 2021

Habituellement, le trafic destiné à un VIP atteint l’appliance Citrix ADC sur laquelle le VIP est actif, car une demande ARP avec le VIP et un MAC virtuel sur cette appliance a atteint le routeur en amont. Mais dans certains cas, comme les routes statiques configurées sur le routeur en amont pour le sous-réseau VIP, ou une topologie qui bloque cet itinéraire, le trafic peut atteindre une appliance Citrix ADC sur laquelle le VIP est en état de sauvegarde. Si vous souhaitez que cette appliance transfère les paquets de données vers l’appliance sur laquelle le VIP est actif, vous devez activer l’option Envoyer au maître. Ce comportement est un paramètre par nœud et est désactivé par défaut.

Par exemple, dans le diagramme suivant, VIP1 est configuré sur NS1, NS2 et NS3 et est actif sur NS1. Dans certaines circonstances, le trafic VIP1 (actif sur NS1) peut atteindre VIP1 sur NS3. Lorsque l’option Envoyer au maître est activée sur NS3, NS3 transfère le trafic vers NS1 via NS2 en utilisant les entrées d’itinéraire pour NS1.

Figure 1. Configuration active active avec option Envoyer au maître activée



Pour activer l'envoi au maître à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
set vrIDParam -sendToMaster (ENABLED          DÉSACTIVÉ)
```

Exemple :


```
> set vrIDParam -sendToMaster ENABLED
 Done
<!--NeedCopy-->
```

Pour activer l'envoi au maître à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Paramètres du routeur virtuel**.
2. Sélectionnez l'option **Envoyer au maître** .

Configuration des intervalles de communication VRRP

August 20, 2021

Dans un déploiement actif, tous les nœuds Citrix ADC utilisent le Virtual Router Redundancy Protocol (VRRP) pour annoncer leurs adresses VIP maîtresses et les priorités correspondantes dans les paquets de publicité VRRP (Hello messages) à intervalles réguliers.

VRRP utilise les intervalles de communication suivants :

- **Hello Interval**. Intervalle entre les messages de bonjour VRRP qu'un nœud d'une adresse VIP maître envoie à ses nœuds homologues.
- **Dead Interval**. Heure après laquelle un noeud d'une adresse VIP de sauvegarde considère l'état de l'adresse VIP principale comme DOWN si les messages de bonjour VRRP ne sont pas reçus du noeud de l'adresse VIP principale. Après l'intervalle mort, l'adresse VIP de sauvegarde prend le relais et devient l'adresse VIP principale.

Vous pouvez modifier ces intervalles en une valeur souhaitée. Ces deux intervalles de communication sont définis par nœud pour toutes les adresses VIP de ce nœud.

Pour configurer les intervalles de communication VRRP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set vrIDParam** [-**helloInterval** <msecs>] [-**deadInterval** <secs>]
- **sh vrIDParam**

Exemple :

```
> set vrIDParam -helloInterval 500 -deadInterval 2
 Done
<!--NeedCopy-->
```

Pour configurer les intervalles de communication VRRP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Paramètres du routeur virtuel**.
2. Dans **Configurer le paramètre Virtual Router**, définissez les paramètres **Hello Interval**et **Dead Interval**.
3. Cliquez sur **OK**.

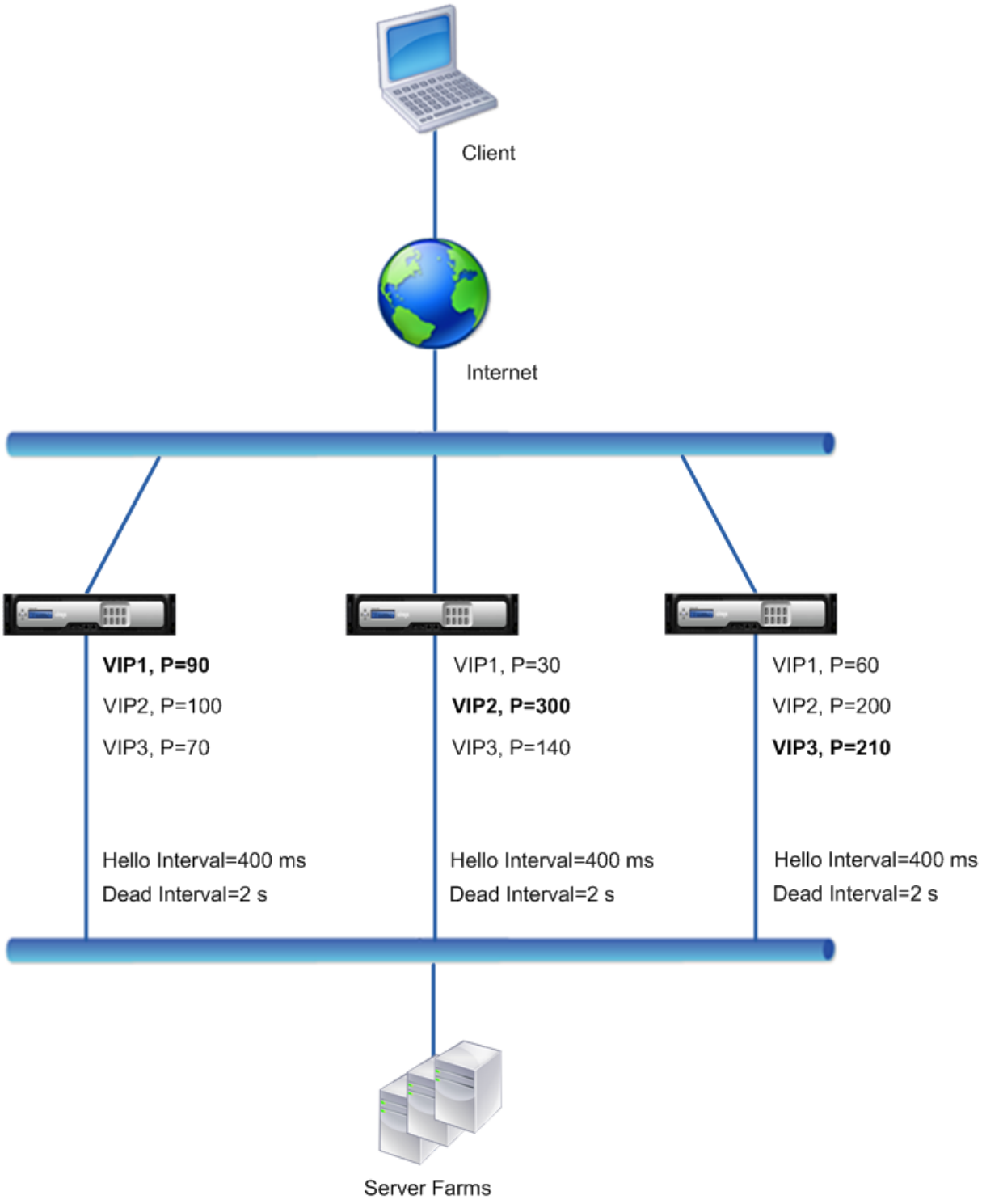
Exemple 1 : Noeuds avec les mêmes intervalles morts VRRP

Envisagez un déploiement actif-actif composé de Citrix ADC NS1, NS2 et NS3. Les adresses IP virtuelles VIP1, VIP2, VIP3 sont configurées sur chacun de ces ADC. En raison de leurs priorités, VIP1 est actif sur NS1, VIP2 est actif sur NS2 et VIP3 est actif sur NS3.

Comme indiqué dans le tableau ci-dessous, l'intervalle mort est défini sur la même valeur (2 secondes) sur les trois nœuds. Les intervalles de communication VRRP (intervalle Bonjour et intervalle mort) d'un nœud s'appliquent à tous les VRID configurés sur le nœud, et à leur tour, s'appliquent à toutes les adresses VIP associées aux VRID sur le nœud.

Sur chaque nœud, les adresses VIP actives (maître) sur ce nœud utilisent l'intervalle Hello, et l'intervalle mort est utilisé par les adresses VIP inactives (sauvegarde) sur ce nœud. La préemption est désactivée pour les adresses VIP des trois nœuds.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple : paramètres de l'exemple 1 de l'intervalle VRRP.



Le flux d'exécution est le suivant :

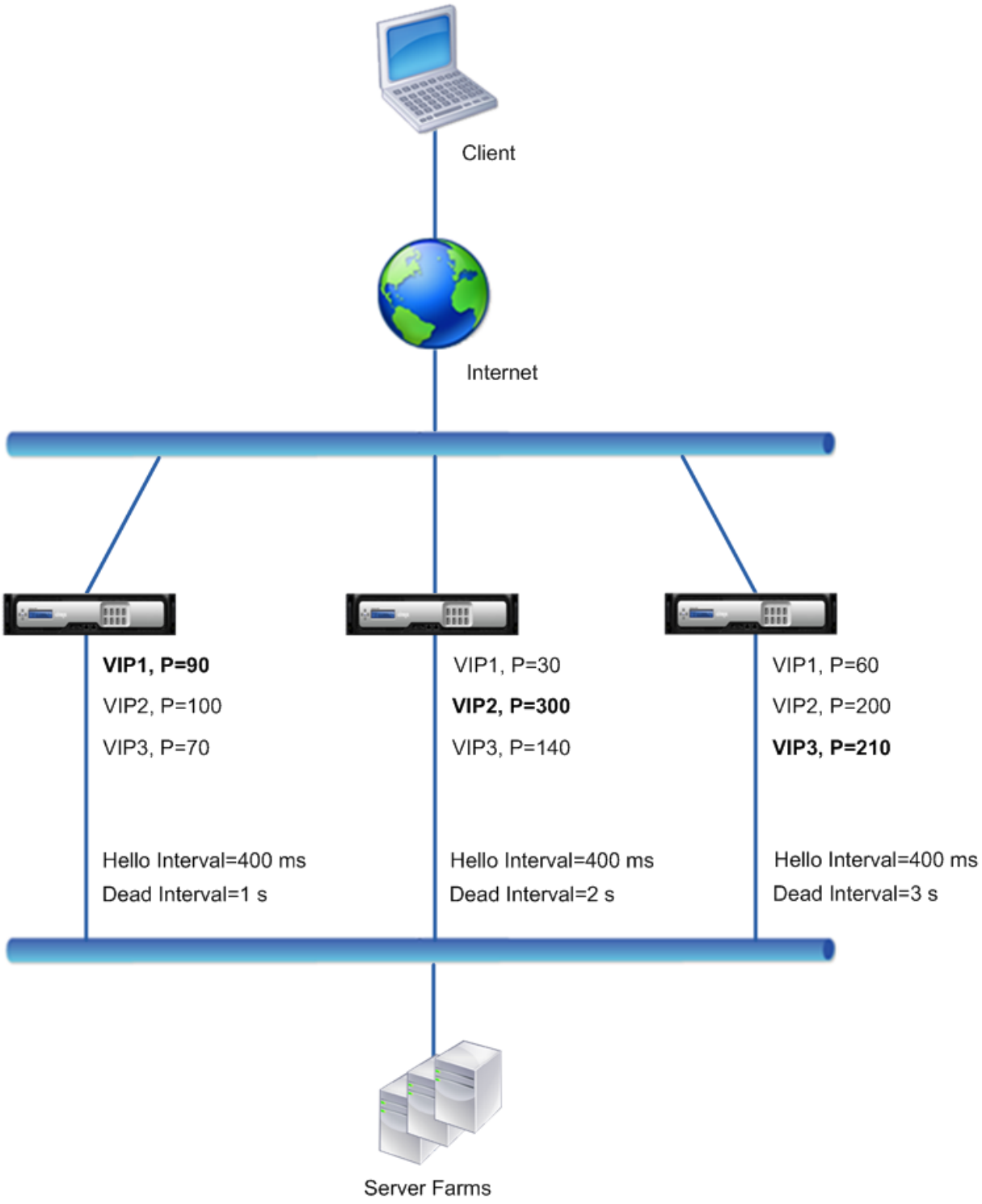
1. NS1 envoie des messages Hello à un intervalle défini de 400 ms à NS2 et NS3 pour l'adresse VIP1, car VIP1 est actif (le maître) sur NS1. De même, NS2 envoie des messages de bonjour pour VIP2 et NS3 envoie des messages de bonjour pour VIP3.

2. Sur NS1, l'intervalle mort défini s'applique aux VIP2 et VIP3, car ils sont inactifs (sauvegardes) sur NS1. De même, sur NS2, l'intervalle mort défini s'applique à VIP1 et VIP3, et sur NS3, l'intervalle mort défini s'applique à VIP1 et VIP2.
3. Si NS1 tombe en panne, NS2 et NS3 considèrent que NS1 est en panne s'ils ne reçoivent aucun message de bonjour de NS1 pendant 2 secondes (intervalle mort). VIP1 sur NS3 prend le relais et devient actif (maître) car sa priorité VRID (60) est supérieure à celle de VIP1 de NS2 (30).

Exemple 2 : Noeuds avec différents intervalles morts VRRP

Considérez un déploiement VRRP similaire au déploiement décrit dans l'Example1, mais avec un intervalle mort différent sur chaque nœud (NS1, NS2 et NS3). La préemption est désactivée pour les adresses VIP des trois nœuds.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple : paramètres de l'exemple 2 de l'intervalle VRRP.



Le flux d'exécution est le suivant lorsque NS1 tombe en panne :

1. NS2 considère que NS1 est en panne après n'avoir reçu aucun message de bonjour de NS1 pendant 2 secondes (intervalle mort de NS2).
2. VIP1 sur NS2 prend le relais et devient actif (master). NS2 commence maintenant à envoyer des

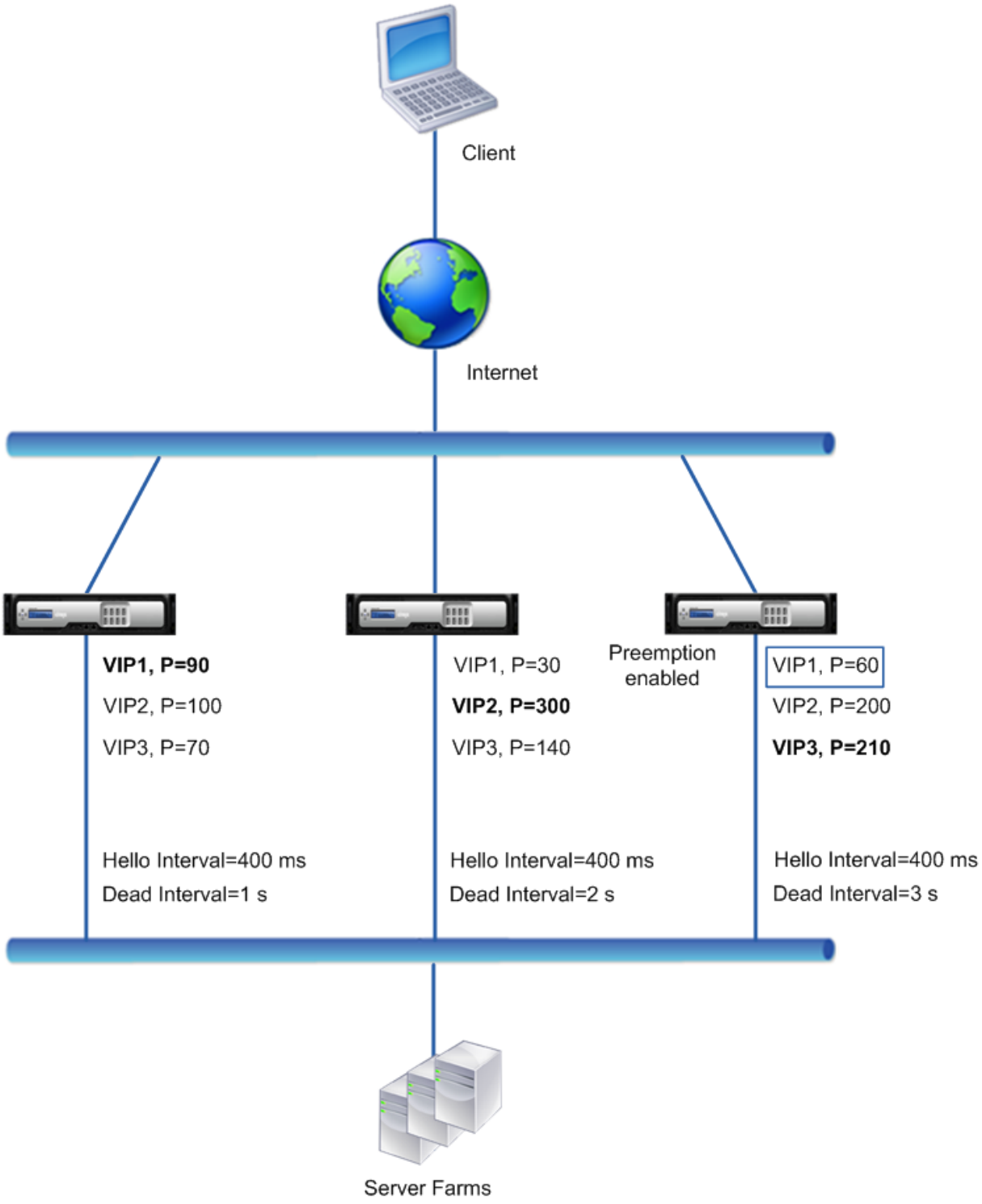
messages hello pour VIP1.

Même si VIP1 sur NS3 a une priorité VRIP plus élevée (60) que VIP1 sur NS2 (30), l'intervalle mort plus grand de NS3 (3 secondes, contre 2 secondes pour NS2) empêche VIP1 sur NS3 de prendre le relais avant que VIP 1 sur NS2 l'ait déjà fait.

Exemple 3 : Noeuds avec différents intervalles morts et préemption activés

Considérez un déploiement VRRP similaire au déploiement décrit dans l'Example1, mais avec des intervalles morts différents sur les trois nœuds, NS1, NS2 et NS3, et avec la préemption activée pour l'adresse VIP1 sur NS3.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple : paramètres de l'exemple 3 de l'intervalle VRRP.



Le flux d'exécution est le suivant lorsque NS1 tombe en panne :

1. NS2 considère NS1 comme arrêt après n'avoir reçu aucun message de bonjour de NS1 pendant 2 secondes (intervalle mort défini de NS2). À ce moment, NS3, avec un intervalle mort de 3 secondes, ne considère pas NS1 comme étant en panne.

2. VIP1 sur NS2 prend le relais et devient actif (master). NS2 commence maintenant à envoyer des messages hello pour VIP1.
3. Lors de la réception de messages bonjour de NS2 pour VIP1, NS3 préempte NS2 pour VIP1 car la préemption est activée pour VIP1 de NS3 et la priorité VRID (60) de VIP1 de NS3 est supérieure à celle (30) de VIP1 de NS2.
4. VIP1 sur NS3 prend le relais et devient actif (maître). NS3 commence maintenant à envoyer des messages de bonjour pour VIP1.

Configuration du suivi de l'intégrité en fonction de l'état de l'interface

August 20, 2021

Pour vous assurer qu'une adresse VIP de sauvegarde prend le relais en tant que VIP maître avant que le nœud de l'adresse VIP maître actuelle ne tombe complètement en panne, vous pouvez configurer un nœud pour modifier la priorité d'une adresse VIP lorsque l'état d'une interface sur le nœud change. Par exemple, le nœud réduit la priorité d'une adresse VIP lorsque l'état d'une interface passe à DOWN et augmente la priorité lorsque l'état de l'interface passe à UP. Cette fonctionnalité est une configuration par nœud pour chaque adresse VIP.

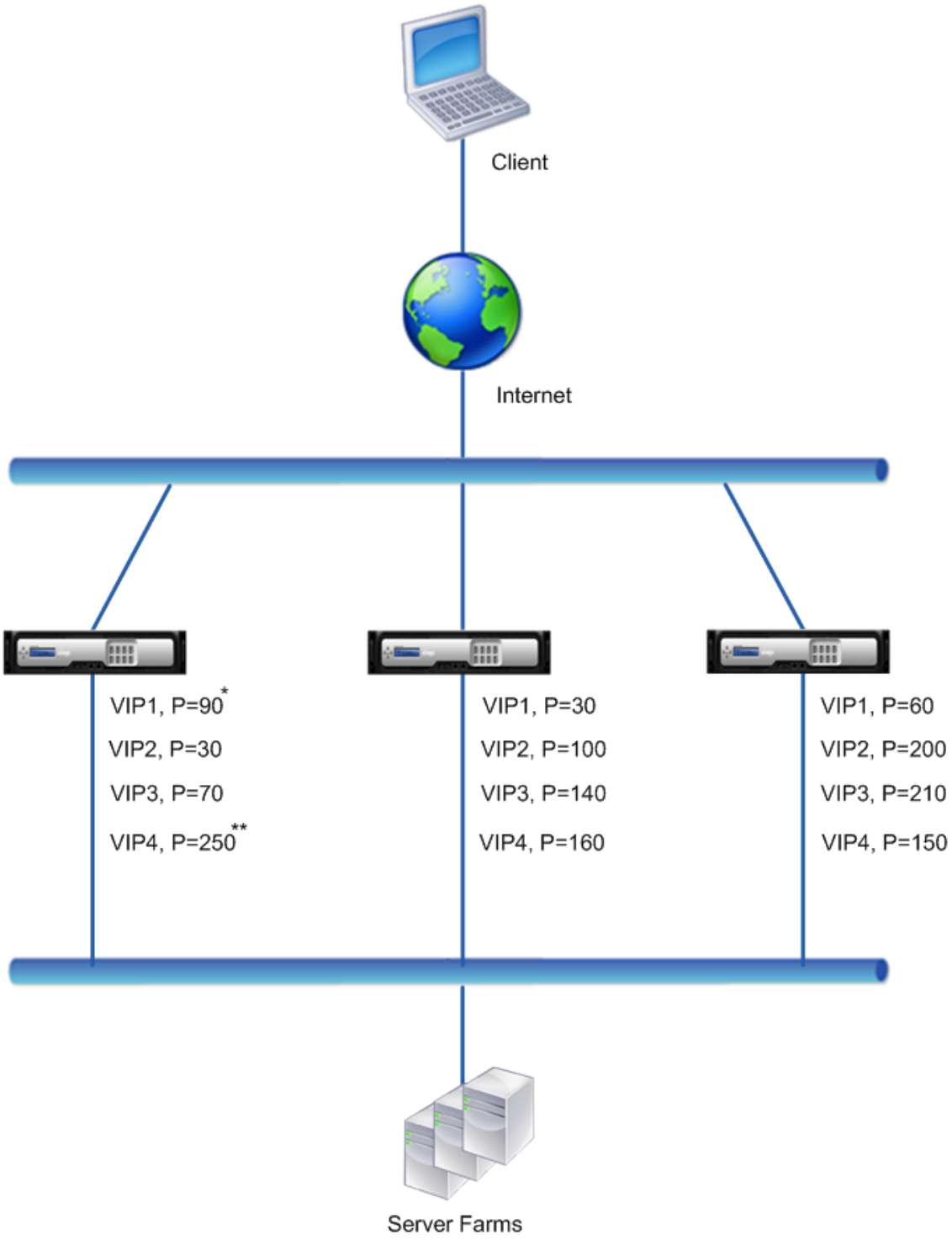
Exemple

Envisagez un déploiement actif-actif composé de Citrix ADC NS1, NS2 et NS3. Les adresses IP virtuelles VIP1, VIP2, VIP3 et VIP4 sont configurées sur chacun de ces ADC. En raison de leurs priorités, VIP1 et VIP4 sont actifs sur NS1, VIP2 est actif sur NS2 et VIP3 est actif sur NS3.

Pour s'assurer que les adresses VIP actives sur NS1 sont prises en charge par NS2 ou NS3 avant que NS1 ne s'arrête complètement, le suivi d'intégrité basé sur l'interface est configuré pour les adresses VIP1 et VIP4 sur NS1. La configuration du suivi d'intégrité basé sur l'interface pour une adresse VIP inclut l'association des interfaces souhaitées et la définition du paramètre de priorité réduite (TrackIFNumPriority) pour le VRID associé de l'adresse VIP. Par exemple, sur NS1, les interfaces 1/2, 1/3 et 1/5 sont associées au VRID de VIP1, et la priorité réduite est définie sur 20.

La préemption est activée pour ces adresses VIP dans les trois nœuds.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple : exemples de paramètres de suivi de l'état de santé.



* Packet Interfaces = 1/2, 1/3, 1/5
Reduced Priority = 20

** Packet Interfaces = 1/5, 1/7
Reduced Priority = 55

Le flux d'exécution est le suivant sur NS1 lorsque plusieurs interfaces sur NS1 tombe en panne :

1. Si l'interface 1/3 tombe en panne, la priorité de l'adresse VIP1 est réduite de 20 (valeur de priorité réduite de VIP1), car l'interface 1/3 est associée à VIP1 :
   - Priorité effective de VIP1 = (Priorité actuelle - priorité réduite) = (90-20) = 70
2. De même, si l'interface 1/5 tombe en panne, la priorité de l'adresse VIP1 est encore réduite :
   - Priorité effective de VIP1 = (Priorité actuelle - priorité réduite) = (70-20) = 50
3. À ce stade, la priorité effective de VIP1 sur NS1 est inférieure à la priorité de VIP1 sur NS3. NS3 préempte NS1 pour VIP1. VIP1 sur NS3 prend le relais et devient actif (maître).
4. En outre, comme l'interface 1/5 est également associée à VIP4, la priorité de VIP4 est réduite par la valeur de priorité réduite du VIP4 (55).
   - Priorité effective de VIP4 = (250 - 55) = 195
5. Si l'interface 1/7 tombe en panne, la priorité de VIP4 est encore réduite :
   - Priorité effective de VIP4 = (Priorité actuelle - priorité réduite) = (195-55) = 145
6. À ce stade, la priorité effective de VIP4 sur NS1 est inférieure à la priorité de VIP4 sur NS2. NS2 préempte NS1 pour VIP4. VIP4 sur NS3 prend le relais et devient actif (master). Cette configuration garantit qu'aucune des quatre adresses VIP n'est active sur NS1 avant qu'elle ne s'arrête complètement.

Étapes de configuration pour le mode actif IPv4

Pour configurer cette fonctionnalité sur un nœud pour une adresse VIP, vous définissez le paramètre Priorité réduite (TrackIFNumPriority), puis associez les interfaces dont l'état doit être suivi pour modifier la priorité de l'adresse VIP. Lorsque l'un des états de l'interface associée passe à DOWN ou UP, le nœud réduit ou augmente la priorité de l'adresse VIP par la valeur Reduced Priority (TrackIFNumPriority) configurée.

Pour définir des interfaces de priorité réduite et de liaison à l'ID du routeur virtuel à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **définir VRID** <id>[-**TrackIfNumpPriority**]<positive_integer>
- **bind vrID** <id> -**trackifNum** <interface_name>
- **show vrID** <id>

Exemple :

```
    > set vrID 125 -trackifNumPriority 10
    Done

    > bind vrID 125 -trackifNum 1/4 1/5
    Done
<!--NeedCopy-->
```


Pour définir des interfaces de priorité réduite et de liaison à l'ID du routeur virtuel à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VMAC.**
2. Sous l'onglet **VMACs**, sélectionnez un ID de routeur virtuel, puis cliquez sur **Modifier** .
3. Sous **Configurer le MAC virtuel**, définissez le paramètre **Priorité réduite**.
4. Sélectionnez l'option **Interfaces suivies pour l'option VRID** et, sous **Associer Interfaces**, ajoutez des interfaces à l'ID du routeur virtuel.

Étapes de configuration pour le mode actif IPv6

Pour configurer cette fonctionnalité sur un nœud pour une adresse VIP6, vous définissez le paramètre Priorité réduite (TrackIFNumPriority), puis associez les interfaces dont l'état doit être suivi pour modifier la priorité de l'adresse VIP6. Lorsque l'un des états de l'interface associée passe à DOWN ou UP, le nœud réduit ou augmente la priorité de l'adresse VIP6 par la valeur Reduced Priority (TrackIFNumPriority) configurée.

Pour modifier automatiquement la priorité d'une adresse VIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants.

- Si vous ajoutez un nouveau MAC6 virtuel :
  - **ajouter VriD6** <id> [-**TrackIfNumpPriority**]
  - **bind vrID6** <id> -**trackifNum** <interface_name>
  - **show vrID6** <id>
- Si vous reconfigurez un MAC6 virtuel existant :
  - **set vrID6** <id> [-**TrackIfNumpPriority**]
  - **bind vrID6** <id> -**trackifNum** <interface_name>
  - **show vrID6** <id>

Exemple :

```
    > set vrID6 130 -trackifNumPriority 10
    Done

    > bind vrID6 130 -trackifNum 1/4 1/5
    Done
<!--NeedCopy-->
```


Retarder la préemption

January 21, 2021

Par défaut, une adresse VIP de sauvegarde préempte l'adresse VIP maître immédiatement après que sa priorité devient supérieure à celle de l'adresse VIP maître. Lors de la configuration d'une adresse VIP de sauvegarde, vous pouvez spécifier un délai pour retarder la préemption. Le délai de préemption est un paramètre par nœud pour chaque adresse VIP de sauvegarde.

Le paramètre de délai de préemption pour un VIP de sauvegarde ne s'applique pas dans les conditions suivantes :

- Le nœud du VIP maître tombe en panne. Dans ce cas, le VIP de sauvegarde prend le relais en tant que VIP maître après l'intervalle mort défini sur le nœud du VIP de sauvegarde.
- La priorité du VIP maître est définie sur zéro. Le VIP de sauvegarde prend le relais en tant que VIP maître après l'intervalle mort défini sur le nœud du VIP de sauvegarde.

Exemple : retarder la préemption

Envisagez un déploiement actif-actif comprenant les appliances Citrix ADC NS1 et NS2. L'adresse IP virtuelle VIP1 est configurée sur chacune de ces appliances. En raison de leurs priorités, VIP1 est maître sur NS2. La préemption est activée et le délai de préemption est défini pour VIP1 sur ces deux nœuds.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Entité et paramètres	Paramètres sur NS1	Paramètres sur NS2
VIP1 (à titre de référence seulement)	**Adresse IP :** 192.0.1.10, **VRID :** 10, **Priorité :** 100, **Préemption :** Activé, **Délai de préemption :** 1000 secondes	**Adresse IP :** 192.0.1.10, **VRID : 10**, **Priorité :** 200, **Préemption :** Activé, **Délai de préemption :** 2000 secondes
Intervalle mort	1 Secondes	2 secondes

Voici quelques exemples de comportement de préemption possible dans cette configuration :

- Si la priorité de VIP1 sur NS1 est définie sur une valeur (par exemple, 210) supérieure à celle de VIP1 sur NS2, VIP1 sur NS1 prend le relais en tant que maître après son délai de préemption défini (1000 secondes).
- Si un troisième nœud NS3 avec les paramètres VRRP suivants est ajouté à ce déploiement, VIP1 sur NS3 devient maître après son délai de préemption défini (3000 secondes).

    - VIP1
        * VRID : 30
        * Adresse IP :
        * Priorité = 300
        * Délai de préemption = 3000 secondes
- Si NS2 tombe en panne, VIP1 sur NS1 prend le relais en tant que maître après 1 seconde (définissez l'intervalle mort sur NS1). Le délai de préemption pour VIP1 sur NS1 ne s'applique pas dans ce cas.
- Si NS2 tombe en panne et que NS1 redémarre, VIP1 sur NS1 devient maître 1 seconde (définissez l'intervalle mort sur NS1) après que NS1 arrive. Le délai de préemption pour VIP1 sur NS1 ne s'applique pas dans ce cas.
- Si la priorité de VIP1 sur NS2 est définie sur zéro, VIP1 passe en mode veille. VIP1 sur NS1 prend le relais en tant que maître après 1 seconde (définir l'intervalle mort sur NS1). Le délai de préemption pour VIP1 sur NS1 ne s'applique pas dans ce cas.

Configuration de la préemption de retard pour le mode actif IPv4

Pour configurer le délai de préemption pour une adresse VIP, vous définissez le paramètre de temporisation de délai de préemption de l'adresse MAC virtuelle associée. Vous pouvez définir ce paramètre lorsque vous ajoutez l'adresse ou modifier une adresse MAC virtuelle existante.

Pour configurer le délai de préemption à l'aide de l'interface de ligne de commande :

- Pour définir le délai de préemption lors de l'ajout d'un MAC virtuel, à l'invite de commandes, tapez :
    - **add vrID** <id> -**preemptiondelaytimer** <secs>
    - **show vrID**
- Pour définir le délai de préemption lors de la modification d'un MAC virtuel, à l'invite de commandes, tapez :
    - **set vrID** <id> -**preemptiondelaytimer** <secs>
    - **show vrID**

Pour configurer le délai de préemption à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VMAC**.
2. Sous l'onglet **VMAC** . Lors de l'ajout d'un nouveau MAC virtuel ou de la modification d'un MAC virtuel existant, définissez le paramètre **Preemption Delay Timer** .

Exemple de configuration :

La configuration suivante utilise les paramètres répertoriés dans le tableau de la section Exemple : Retarder la préemption.

```
1     Settings on NS1
```



```
2
3       > set vrid param  - deadInterval 1
4
5       Done
6
7       > add ns ip 192.0.1.10 255.255.255.255  - type VIP
8
9       Done
10
11      > add vrid 10  - Priority 100  - Preemption Enable  -
           preemptiondelaytimer 1000
12
13      Done
14
15      > bind ns ip 192.0.1.10 255.255.255.255  - vrid 10
16
17      Done
18
19      Settings on NS2
20
21      > set vrid param  - deadInterval 2
22
23      Done
24
25      > add ns ip 192.0.1.10 255.255.255.255  - type VIP
26
27      Done
28
29      > add vrid 20  - Priority 200  - Preemption Enable  -
           preemptiondelaytimer 2000
30
31      Done
32
33      > set ns ip 192.0.1.10 255.255.255.255  - vrid 10
34
35      Done
36  <!--NeedCopy-->
```

Configuration de la préemption de retard pour le mode actif IPv6

Pour configurer le délai de préemption pour une adresse VIP6, vous définissez le paramètre de temporisation de délai de préemption de l'adresse MAC6 virtuelle associée. Vous pouvez définir ce paramètre lorsque vous ajoutez l'adresse MAC6 virtuelle ou modifier une adresse MAC6 virtuelle

existante.

Pour configurer le délai de préemption à l'aide de l'interface de ligne de commande :

- Pour définir le délai de préemption lors de l'ajout d'un MAC6 virtuel, à l'invite de commandes, tapez :
  - **add vrID6** <id> -**preemptiondelaytimer** <secs>
  - **show vrID6**
- Pour définir le délai de préemption lors de la modification d'un MAC6 virtuel, à l'invite de commandes, tapez :
  - **set vrID6** <id> -**preemptiondelaytimer** <secs>
  - **show vrID6**

Pour configurer le délai de préemption à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VMAC**.
2. Sous l'onglet **VMAC6** . Lors de l'ajout d'une adresse MAC6 virtuelle ou de la modification d'une adresse MAC6 virtuelle existante, définissez le paramètre **Preemption Delay Timer** .

Conserver une adresse VIP dans l'état de sauvegarde

January 21, 2021

Vous pouvez forcer une adresse VIP à rester toujours en état de sauvegarde. Cette opération est utile pour la maintenance ou le test d'un déploiement VRRP.

Lorsqu'une adresse VIP est forcée de rester en état de sauvegarde, elle ne participe pas aux transitions d'état VRRP. En outre, il ne peut pas devenir maître même si tous les autres nœuds tombent en panne.

Pour forcer une adresse VIP à rester en état de sauvegarde, définissez la priorité de l'adresse MAC virtuelle associée sur zéro. Pour s'assurer qu'aucune des adresses VIP d'un nœud ne gère le trafic au cours d'un processus de maintenance sur le nœud, définissez toutes les priorités sur zéro.

Vous pouvez définir la priorité d'une adresse MAC virtuelle lors de l'ajout ou de la modification de l'adresse.

Pour forcer une adresse VIP à rester dans l'état de sauvegarde à l'aide de l'interface de ligne de commande :

- Pour définir la priorité lors de l'ajout d'un MAC virtuel, à l'invite de commandes, tapez :
  - **add vrID** <id> -**priority** 0
  - **show vrID**
- Pour définir la priorité lors de la modification d'un MAC virtuel, à l'invite de commandes, tapez :

- **set vrID** <id> -**priority** 0
- **show vrID**

Pour forcer une adresse VIP à rester en état de sauvegarde à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VMAC**.
2. Sous l'onglet **VMAC**, tout en ajoutant un nouveau MAC virtuel ou en modifiant un MAC virtuel existant, définissez le paramètre **Priority** sur zéro.

Visualiseur réseau

January 21, 2021

Le visualiseur réseau affiche une vue graphique de toutes les interfaces, canaux, VLAN, adresses IP et liaisons aux VLAN sur une appliance Citrix ADC. Une interface ou un canal activé a une étiquette noire. Une interface ou un canal désactivé a une étiquette rouge.

Cette image complète des connexions réseau de l'appliance peut être utile pour détecter les défauts dans la conception du réseau et pour optimiser le réseau. Il peut également aider un nouvel administrateur à comprendre facilement la configuration réseau de l'appliance.

Pour ouvrir le visualiseur réseau :

Accédez à **Système** > **Réseau**. Dans **Moniteur des connexions**, cliquez sur **Visualiseur réseau**.

Configuration du protocole de découverte de couche de liens

August 20, 2021

Citrix ADC prend en charge le protocole LLDP (Link Layer Discovery Protocol) standard (IEEE 802.1AB). LLDP est un protocole de couche 2 qui permet à Citrix ADC de faire connaître son identité et ses capacités aux périphériques directement connectés, ainsi que d'apprendre l'identité et les capacités de ces périphériques voisins.

> **Remarque :**
> le protocole LLDP (Link Layer Discovery Protocol) est pris en charge uniquement dans les plates-formes Citrix ADC MPX.

À l'aide de LLDP, le Citrix ADC transmet et reçoit des informations sous la forme de messages LLDP appelés unités de données de paquets LLDP (LLDPU). Un LLDPU est une séquence d'éléments d'information de type, longueur, valeur (TLV). Chaque TLV contient un type spécifique d'informations sur l'appareil qui transmet le LLDPDU. Le Citrix ADC envoie les TLV suivants dans chaque LLDPU :

- ID du châssis
- ID de port
- Valeur du temps de vie
- Nom du système
- Description du système
- Description du port
- Fonctionnalités du système
- Adresse de la direction
- ID de port VLAN
- Agrégation de liens

Remarque : vous ne pouvez pas spécifier les TLV à envoyer dans les messages LLDP.

Les interfaces Citrix ADC prennent en charge les modes LDP suivants :

- **AUCUN**. L'interface ne reçoit ni ne transmet de messages LLDP à l'appareil directement connecté.
- **TRANSMITTER**. L'interface transmet des messages LLDP au périphérique connecté directement, mais ne reçoit pas de messages LLDP du périphérique connecté directement.
- **RECEIVER**. L'interface reçoit les messages LLDP du périphérique connecté directement, mais ne transmet pas les messages LLDP au périphérique connecté directement.
- **TRANSCEIVER**. L'interface transmet les messages LLDP au périphérique directement connecté et reçoit les messages LLDP.

Le mode LLDP d'une interface dépend du mode LLDP configuré aux niveaux global et de l'interface. Le tableau suivant présente les modes résultant des combinaisons disponibles de paramètres au niveau global et de l' interface : modes Interface et LLDP de niveau global.

Notez les points suivants liés aux messages LLDP transmis ou reçus par Citrix ADC :

- **Transmission des messages LLDP.** Le Citrix ADC transmet des LLDPU à partir d'interfaces fonctionnant en mode TRANSMITTER ou TRANSCEIVER LLDP.

  Voici les paramètres de transmission LLDP globaux sur Citrix ADC :

  - **Minuteur**. Intervalle, en secondes, entre les LLDPU que Citrix ADC envoie à un périphérique directement connecté.
  - **Multiplicateur Holdtime**. Multiplicateur pour calculer la durée pendant laquelle le périphérique récepteur stocke les informations LDP dans sa base de données avant de les supprimer ou de les supprimer. La durée est calculée en tant que valeur **du paramètre Multiplicateur de temps** d'arrêt multipliée par la valeur du paramètre Timer.
- **Réception de messages LLDP.** Citrix ADC stocke les informations LLDPDU dans sa base d'informations de gestion (MIB). Les informations LLDP stockées sont classées ou regroupées sous l'ID de l'interface qui a reçu le LLDPDU. Citrix ADC conserve ces informations LDP pour la durée spécifiée dans le LLDPU reçu.

Si ADC reçoit un autre LLDPDU sur une interface avant que les informations LLDP stockées pour cette interface ne soient ignorées, ADC remplace les informations LLDP stockées pour cette interface par des informations dans le nouveau LLDPDU.

Étapes de configuration

La configuration de LLDP sur une appliance Citrix ADC comporte les tâches suivantes :

1. **Définir les paramètres LLDP de niveau global.** Dans cette tâche, vous définissez les paramètres LLDP globaux tels que la minuterie LLDP, le multiplicateur de temps de blocage et le mode LLDP.
2. **Définissez les paramètres LLDP au niveau de l'interface.** Dans cette tâche, vous définissez le mode LLDP pour une interface.
3. **(Facultatif) Afficher les informations sur le périphérique voisin.** Vous pouvez afficher les informations LDP du périphérique voisin collectées sur toutes les interfaces de l'ADC Citrix, ou uniquement les informations LDP collectées sur les interfaces spécifiées. Si vous ne spécifiez pas d'interface, les informations sont affichées pour toutes les interfaces.

Voici les conditions préalables à la configuration de LLDP sur un Citrix ADC :

1. Assurez-vous de bien comprendre le protocole LLDP standard (IEEE 802.1AB).
2. Vérifiez que vous avez configuré LLDP sur les périphériques directement connectés souhaités.

Procédures CLI

Pour définir des paramètres LLDP de niveau global à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- set lldp param [- [-HoldTimeXMult][-timer <positive_integer>] <positive_integer>[-Mode]<Mode>
- show lldp param

Pour configurer une interface pour LLDP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- set interface <id> -lldpmode <lldpmode>
- Afficher l'interface <id>

Pour afficher les informations de périphérique voisin à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- show lldp neighbors
- show lldp neighbors <ifnum>

Procédures GUI

Pour définir les paramètres LLDP de niveau global à l'aide de l'interface graphique :

1. Accédez à Système > Réseau, puis cliquez sur Configurer les paramètres LLDP.
2. Définissez les paramètres suivants :
   - Multiplicateur de minuteur de suspension
   - Minuteur
   - Mode

Pour configurer une interface pour LLDP à l'aide de l'interface graphique :

Accédez à Système > Réseau > Interfaces, ouvrez l'interface et définissez le paramètre de mode LLDP.

Pour afficher les informations de périphérique voisin à l'aide de l'interface graphique :

Accédez à Système > Réseau > Interfaces et, dans la liste Action, sélectionnez Afficher les voisins LLDP.

Prise en charge LDP dans une configuration de cluster

Dans une configuration de cluster, l'interface graphique et l'interface de ligne de commande affichent la configuration voisine LLDP de tous les nœuds de cluster spécifiques ou de tous les nœuds de cluster lorsque l'interface graphique ou l'interface de ligne de commande est accessible via l'adresse IP de cluster (CLIP). Toute modification apportée au mode LLDP de niveau global est appliquée au mode LLDP de niveau global sur chacun des nœuds de cluster.

Prenons un exemple de configuration de cluster de trois nœuds, NS1, NS2 et NS3. Chacun de ces nœuds est connecté à la fois aux routeurs Router-1 et Router2. La sortie suivante s'affiche lorsque l'opération **show lldp neighbor -summary** est exécutée sur l'interface CLI de cluster accessible via l'adresse IP de cluster (CLIP) de la configuration du cluster. La sortie affiche les informations de voisinage LLDP de tous ces nœuds.

```
1  > show lldp neighbor -summary
2
3  Node Id: 1
4  ------------------------------------------------------------
5      Interface    ChassisId           PortId     System name
6  ------------------------------------------------------------
7  1     1/1/1      fe:c7:3b:13:bd:11    1/1         Router-1
8
9  2     1/1/2      12:68:7b:9e:4c:11    1/1         Router-2
10
11 Node Id: 2
12 ------------------------------------------------------------
13     Interface    ChassisId           PortId     System name
```



```
14 ----------------------------------------------------------------
15 1     2/1/1      fe:c7:3b:13:bd:12    1/2        Router-1
16
17 2     2/1/2      12:68:7b:9e:4c:12    1/2        Router-2
18
19 Node Id: 3
20 ----------------------------------------------------------------
21     Interface    ChassisId            PortId     System name
22 ----------------------------------------------------------------
23
24 1     3/1/1       fe:c7:3b:13:bd:13    1/3        Router-1
25
26 2     3/1/2       12:68:7b:9e:4c:13    1/3        Router-2
27
28 Done
29 <!--NeedCopy-->
```

Trames Jumbo

January 21, 2021

Les appliances Citrix ADC prennent en charge la réception et la transmission de trames jumbo contenant jusqu'à 9216 octets de données IP. Les trames Jumbo peuvent transférer des fichiers volumineux plus efficacement qu'il n'est possible avec la taille standard de MTU IP de 1500 octets.

Une appliance Citrix ADC peut utiliser des trames jumbo dans les scénarios de déploiement suivants :

- Jumbo à Jumbo. L'appliance reçoit les données sous forme de trames jumbo et les envoie sous forme de trames jumbo.
- Non Jumbo à Jumbo. L'appliance reçoit les données sous forme de trames régulières et les envoie sous forme de trames jumbo.
- Jumbo à non-Jumbo. L'appliance reçoit les données sous forme de trames jumbo et les envoie en tant que trames régulières.

L'appliance Citrix ADC prend en charge les trames jumbo dans une configuration d'équilibrage de charge pour les protocoles suivants :

- TCP
- Tout protocole sur TCP (par exemple, HTTP)
- SIP
- RADIUS

Configuration de la prise en charge des trames Jumbo sur une appliance Citrix ADC

August 20, 2021

Pour permettre à l'appliance Citrix ADC de prendre en charge les trames jumbo, définissez le MTU sur plus de 1500 sur les interfaces ou les canaux LA et sur les VLAN sur lesquels vous souhaitez que l'appliance Citrix ADC prend en charge les trames jumbo.

Points à prendre en considération avant de définir le MTU des interfaces, des canaux LA ou des VLAN sur une appliance Citrix ADC

1. Lorsque vous créez un canal LA, le canal prend le MTU de la première interface liée si aucune MTU n'est spécifiée pour le canal.
2. Le MTU d'un canal est propagé à toutes les interfaces liées.
3. Lorsqu'une interface est liée au canal dont la MTU est différente de la MTU de l'interface, l'interface passe dans la liste inactive.
4. Lorsque vous modifiez le MTU d'une interface membre, l'interface passe dans la liste inactive.
5. Lorsqu'une interface est déliée du canal, l'interface conserve la valeur MTU du canal.
6. Vous pouvez définir la MTU d'une interface, d'un canal ou d'un VLAN sur une valeur comprise entre 1500-9216.
7. Vous ne pouvez pas définir le MTU sur le VLAN par défaut. L'appliance Citrix ADC utilise le MTU de l'interface via laquelle elle reçoit ou envoie des données depuis ou vers le VLAN par défaut.
8. Pour le trafic basé sur TCP sur une configuration d'équilibrage de charge sur une appliance Citrix ADC, les MSS sont définis en conséquence à chaque point d'extrémité pour la prise en charge des trames jumbo :
    - Pour une connexion entre un client et un serveur virtuel d'équilibrage de charge sur l'appliance Citrix ADC, le MSS sur l'appliance Citrix ADC est défini dans un profil TCP, qui est ensuite lié au serveur virtuel d'équilibrage de charge.
    - Pour une connexion entre l'appliance Citrix ADC et un serveur, le MSS sur NS1 est défini dans un profil TCP, qui est ensuite lié au service représentant le serveur sur l'appliance Citrix ADC.
    - Par défaut, un profil TCP nstcp_default_profile est lié à tous les serveurs et services d'équilibrage de charge basés sur TCP sur l'appliance Citrix ADC.
    - Pour prendre en charge les trames jumbo, vous pouvez soit modifier la valeur MSS du profil TCP nstcp_default_profile, soit créer un profil TCP personnalisé et définir son MSS en conséquence, puis lier le profil TCP personnalisé aux serveurs et services virtuels d'équilibrage de charge souhaités.

- La valeur MSS par défaut de tout profil TCP est 1460.

Procédures CLI

Pour définir le MTU d'une interface à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- set interface <id> -mtu <positive_integer>
- Afficher l'interface <id>

Exemple :

```
1 > set interface 10/1  - mtu 9000
2 Done
3 <!--NeedCopy-->
```

Pour définir le MTU d'un canal à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- set channel <id> -mtu <positive_integer>
- show channel <id>

Exemple :

```
1 > set channel LA/1  - mtu 9000
2 Done
3 <!--NeedCopy-->
```

Pour définir le MTU d'un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add vlan <id> -mtu <positive_integer>
- afficher vlan <id>

Exemple :

```
1 > set vlan 20  - mtu 9000
2 Done
3 <!--NeedCopy-->
```

Procédures GUI

Pour définir le MTU d'une interface à l'aide de l'interface graphique :

Accédez à Système > Réseau > Interfaces, ouvrez l'interface et définissez le paramètre Unité de transmission maximale.

Pour définir la MTU d'un canal à l'aide de l'interface graphique :

Accédez à Système > Réseau > Canaux, ouvrez le canal et définissez le paramètre Unité de transmission maximale.

Pour définir le MTU d'un VLAN à l'aide de l'interface graphique :

Accédez à Système > Réseau > VLAN, ouvrez le VLAN et définissez le paramètre Unité de transmission maximale.

Cas d'utilisation 1 — Configuration Jumbo à Jumbo

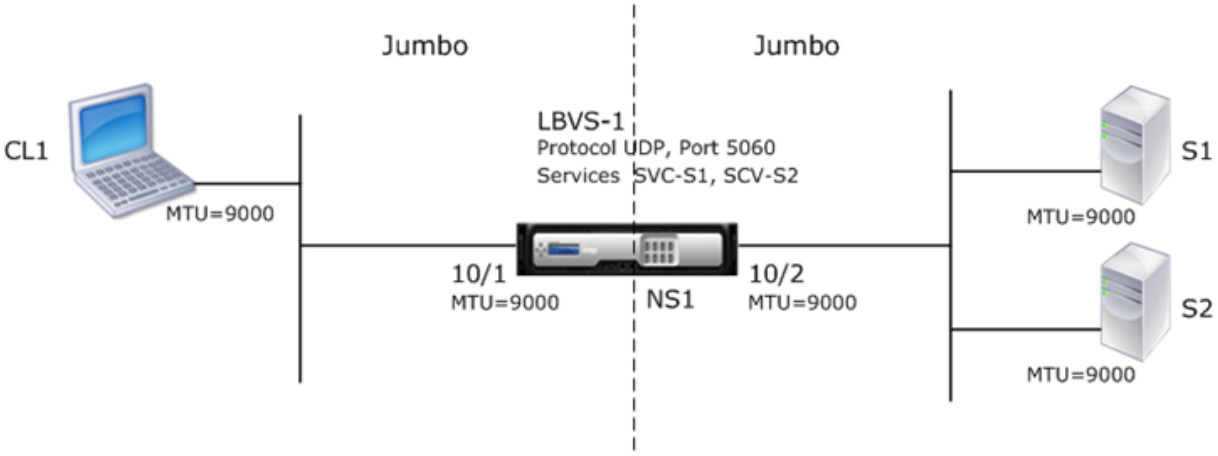
August 20, 2021

Prenons un exemple de configuration jumbo à jumbo dans lequel le serveur virtuel d'équilibrage de charge SIP LBVS-1, configuré sur l'appliance Citrix ADC NS1, est utilisé pour équilibrer la charge du trafic SIP entre les serveurs S1 et S2. La connexion entre le client CL1 et NS1 et la connexion entre NS1 et les serveurs prennent en charge les trames jumbo.

L'interface 10/1 de NS1 reçoit ou envoie du trafic depuis ou vers le client CL1. L'interface 10/2 de NS1 reçoit ou envoie du trafic depuis ou vers le serveur S1 ou S2. Les interfaces 10/1 et 10/2 de NS1 font partie de VLAN 10 et VLAN 20, respectivement.

Pour la prise en charge des trames jumbo, le MTU est défini sur 9216, sur NS1, pour les interfaces 10/1, 10/2 et VLAN 10, VLAN 20.

Tous les autres périphériques réseau, y compris CL1, S1 et S2, dans cet exemple d'installation, sont également configurés pour prendre en charge les trames jumbo.



Le tableau suivant répertorie les paramètres utilisés dans l'exemple.

Entité	Nom	Détails
Adresse IP du client CL1	-	192.0.2.10
Adresse IP des serveurs	S1	198.51.100.19
	S2	198.51.100.20
Adresse SNIP sur NS1		198.51.100.18
MTU spécifié pour les interfaces et les VLAN sur NS1	10/1	9000
	10/2	9000
	VLAN 10	9000
	VLAN 20	9000
Services sur NS1 représentant les serveurs	SVC-S1	**IP address:** 198.51.100.19, **Protocol:** SIP, **Port:** 5060
	SVC-S2	**IP address:** 198.51.100.20, **Protocol:** SIP, **Port:** 5060
Serveur virtuel d'équilibrage de charge sur VLAN 10	LBVS-1	**IP address:** 203.0.113.15, **Protocol:** SIP, **Port:** 5060, **Bound services:** SVC-S1, SVC-S2

Voici le flux de trafic de la demande de CL1 vers NS1 :

1. CL1 crée une requête SIP de 20000 octets à envoyer à LBVS-1 de NS1.
2. CL1 envoie les données de requête en fragments IP à LBVS-1. La taille de chaque fragment IP est égale ou inférieure à la MTU (9000) définie sur l'interface à partir de laquelle CL1 envoie ces fragments à NS1.
    - Taille du premier fragment [IP = en-tête IP+en-tête UDP + segment de données SIP] = [20 + 8 + 8972] = 9000
    - Taille du deuxième fragment [IP = en-tête IP+segment de données SIP] = [20 + 8980] = 9000
    - Taille du dernier fragment IP[IP = en-tête IP+segment de données SIP] = [20 + 2048] = 2068
3. NS1 reçoit les fragments IP de la requête à l'interface 10/1. NS1 accepte ces fragments, car la taille de chacun de ces fragments est égale ou inférieure à la MTU (9000) de l'interface 10/1.
4. NS1 réassemble ces fragments IP pour former la requête SIP de 20000 octets. NS1 traite cette demande.
5. L'algorithme d'équilibrage de charge de LBVS-1 sélectionne le serveur S1.

6. NS1 envoie les données de la requête en fragments IP à S1. La taille de chaque fragment IP est égale ou inférieure à la MTU (9000) de l'interface 10/2, à partir de laquelle NS1 envoie ces fragments à S1. Les paquets IP sont source avec une adresse SNIP de NS1.
    - Taille du premier fragment IP = [IP = en-tête IP+en-tête UDP + segment de données SIP] = [20 + 8 + 8972] = 9000
    - Taille du deuxième fragment IP = [IP = en-tête IP+segment de données SIP] = [20 + 8980] = 9000
    - Taille du dernier fragment IP[IP = en-tête IP+segment de données SIP] = [20 + 2048] = 2068

Voici le flux de trafic de la réponse de S1 à CL1 dans cet exemple :

1. Le serveur S1 crée une réponse SIP de 30000 octets à envoyer à l'adresse SNIP de NS1.
2. S1 envoie les données de réponse en fragments IP à l'adresse SNIP de NS1. La taille de chaque fragment IP est égale ou inférieure à la MTU (9000) définie sur l'interface à partir de laquelle S1 envoie ces fragments à NS1.
    - Taille du premier fragment IP = [IP = en-tête IP+en-tête UDP + segment de données SIP] = [20 + 8 + 8972] = 9000
    - Taille du deuxième et du troisième fragment IP = [IP = en-tête IP+segment de données SIP] = [20 + 8980] = 9000
    - Taille du dernier fragment IP[IP = en-tête IP+segment de données SIP] = [20 + 3068] = 3088
3. NS1 reçoit les fragments IP de réponse à l'interface 10/2. NS1 accepte ces fragments, car la taille de chaque fragment est égale ou inférieure à la MTU (9000) de l'interface 10/2.
4. NS1 réassemble ces fragments IP pour former la réponse SIP de 30000 octets. NS1 traite cette réponse.
5. NS1 envoie les données de réponse en fragments IP à CL1. La taille de chaque fragment IP est égale ou inférieure à la MTU (9000) de l'interface 10/1, à partir de laquelle NS1 envoie ces fragments à CL1. Les fragments IP proviennent de l'adresse IP de LBVS-1.
    - Taille du premier fragment IP = [IP = en-tête IP+en-tête UDP + segment de données SIP] = [20 + 8 + 8972] = 9000
    - Taille du deuxième et du troisième fragment IP = [IP = en-tête IP+segment de données SIP] = [20 + 8980] = 9000
    - Taille du dernier fragment IP =[IP = en-tête IP+segment de données SIP] = [20 + 3068] = 3088

Tâches de configuration

Le tableau suivant répertorie les tâches, les commandes Citrix ADC et les exemples de création de la configuration requise sur l'appliance Citrix ADC.

Tâche	Syntaxe de commande Citrix ADC	Exemple
Définir le MTU des interfaces souhaitées pour la prise en charge des trames jumbo	set interface <id> -mtu <positive_integer>, show interface <id>	set int 10/1 -mtu 9000 set int 10/2 -mtu 9000
Créez des VLAN et définissez le MTU des VLAN souhaités pour la prise en charge des trames jumbo	add vlan <id> -mtu <positive_integer>, show vlan <id>	add vlan 10 -mtu 9000 add vlan 20 -mtu 9000
Liez des interfaces aux VLAN	bind vlan <id> -ifnum <interface_name>, show vlan <id>	bind vlan 10 -ifnum 10/1 bind vlan 20 -ifnum 10/2
Ajouter une adresse SNIP	add ns ip <IPAddress> <netmask> -type SNIP, show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
Créer des services représentant des serveurs SIP	add service <serviceName> <ip> SIP_UDP <port>, show service <name>	add service SVC-S1 198.51.100.19 SIP_UDP 5060 add service SVC-S2 198.51.100.20 SIP_UDP 5060
Créer des serveurs virtuels d'équilibrage de charge SIP et y lier les services	add lb vserver <name> SIP_UDP <ip> <port> bind lb vserver <vserverName> <serviceName>, show lb vserver <name>	add lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060 bind lb vserver LBVS-1 SVC-S1 bind lb vserver LBVS-1 SVC-S2
Enregistrer la configuration	save ns config, show ns config	

Cas d'utilisation 2 — Configuration non Jumbo à Jumbo

August 20, 2021

Prenons un exemple d'installation standard à jumbo dans laquelle le serveur virtuel d'équilibrage de charge LBVS-1, configuré sur une appliance Citrix ADC NS1, est utilisé pour équilibrer le trafic entre les serveurs S1 et S2. La connexion entre le client CL1 et NS1 prend en charge les trames régulières, et la connexion entre NS1 et les serveurs prend en charge les trames jumbo.

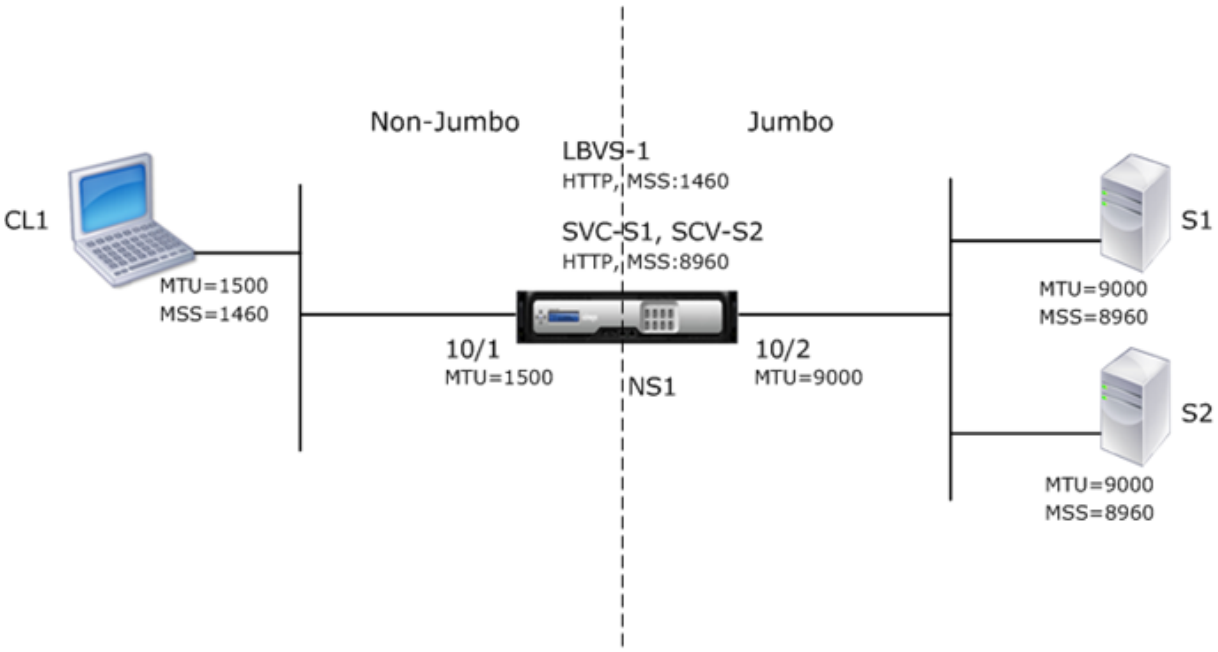
L'interface 10/1 de NS1 reçoit ou envoie du trafic depuis ou vers le client CL1. L'interface 10/2 de NS1 reçoit ou envoie du trafic depuis ou vers le serveur S1 ou S2.

Les interfaces 10/1 et 10/2 de NS1 font partie de VLAN 10 et VLAN 20, respectivement. Pour prendre en charge uniquement les trames régulières entre CL1 et NS1, le MTU est défini sur la valeur par défaut 1500 pour l'interface 10/1 et le VLAN 10

Pour la prise en charge des trames jumbo entre NS1 et les serveurs, la MTU est définie sur 9000 pour l'interface 10/2 et VLAN 20. Les serveurs et tous les autres périphériques réseau entre NS1 et les serveurs sont également configurés pour prendre en charge les trames jumbo.

Puisque le trafic HTTP est basé sur TCP, les MSSS sont définis en conséquence à chaque point d'extrémité pour la prise en charge des trames jumbo.

- Pour prendre en charge les trames jumbo pour la connexion entre une adresse SNIP de NS1 et S1 ou S2, le MSS sur NS1 est défini en conséquence dans un profil TCP personnalisé, qui est lié aux services (SVC-S1 et SVC-S1) représentant S1 et S2 sur NS1.
- Pour prendre en charge uniquement les trames régulières pour la connexion entre CL1 et le serveur virtuel LBVS-1 de NS1, le profil TCP par défaut nstcp_default_profile est utilisé qui est par défaut lié à LBVS-1 et dont le MSS est défini sur la valeur par défaut 1460.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Entité	Nom	Détails
Adresse IP du client CL1		192.0.2.10
Adresse IP des serveurs	S1	198.51.100.19
	S2	198.51.100.20
Adresse SNIP sur NS1		198.51.100.18

Entité	Nom	Détails
MTU spécifié pour les interfaces et les VLAN sur NS1	10/1	1500
	10/2	9000
	VLAN 10	1500
	VLAN 20	9000
Profil TCP par défaut	nstcp_default_profile	MSS:1460
Profil TCP personnalisé	NS1-SERVERS-JUMBO	MSS: 8960
Services sur NS1 représentant les serveurs	SVC-S1	IP address: 198.51.100.19, Protocol: HTTP, Port: 80, TCP profile: NS1-SERVERS-JUMBO (MSS: 8960)
	SVC-S2	IP address: 198.51.100.20, Protocol: HTTP, Port: 80, TCP profile: NS1-SERVERS-JUMBO (MSS: 8960)
Serveur virtuel d'équilibrage de charge sur VLAN 10	LBVS-1	IP address = 203.0.113.15, Protocol: HTTP, Port:80, Bound services: SVC-S1, SVC-S2, TCP Profile: nstcp_default_profile (MSS:1460)

Voici le flux de trafic de la demande de CL1 vers S1 dans cet exemple :

1. Client CL1 crée une requête HTTP de 200 octets à envoyer au serveur virtuel LBVS-1 de NS1.
2. CL1 ouvre une connexion à LBVS-1 de NS1. CL1 et NS1 échangent leurs valeurs MSS TCP respectives lors de l'établissement de la connexion.
3. Étant donné que le MSS de NS1 est plus grand que la requête HTTP, CL1 envoie les données de la demande dans un seul paquet IP à NS1.

   Taille du paquet de requête = [en-tête IP +en-tête TCP + requête TCP] = [20 + 20 + 200] = 240
4. NS1 reçoit le paquet de requête à l'interface 10/1, puis traite les données de requête HTTP dans le paquet.
5. L'algorithme d'équilibrage de charge de LBVS-1 sélectionne le serveur S1 et NS1 ouvre une connexion entre l'une de ses adresses SNIP et S1. NS1 et CL1 échangent leurs valeurs MSS TCP

respectives lors de l'établissement de la connexion.

6. Étant donné que le MSS de S1 est plus grand que la requête HTTP, NS1 envoie les données de la demande dans un seul paquet IP à S1.

   Taille du paquet de demande = [en-tête IP +en-tête TCP + [Demande TCP] = [20 + 20 + 200] = 240

Voici le flux de trafic de la réponse de S1 à CL1 dans cet exemple :

1. Le serveur S1 crée une réponse HTTP de 18 000 octets à envoyer à l'adresse SNIP de NS1.
2. S1 segmente les données de réponse en multiples de MSS de NS1 et envoie ces segments dans des paquets IP à NS1. Ces paquets IP proviennent de l'adresse IP de S1 et sont destinés à l'adresse SNIP de NS1.
   - Taille des deux premiers paquets = [en-tête IP+en-tête TCP + (segment TCP = taille MSS de NS1)] = [20 + 20 + 8960] = 9000
   - Taille du dernier paquet = [en-tête IP+en-tête TCP + (segment TCP restant)] = [20+2080] = 2120
3. NS1 reçoit les paquets de réponse à l'interface 10/2.
4. À partir de ces paquets IP, NS1 assemble tous les segments TCP pour former les données de réponse HTTP de 18000 octets. NS1 traite cette réponse.
5. NS1 segmente les données de réponse en multiples de MSS de CL1 et envoie ces segments dans des paquets IP, de l'interface 10/1, à CL1. Ces paquets IP proviennent de l'adresse IP de LBVS-1 et sont destinés à l'adresse IP de CL1.
   - Taille de tous les paquets sauf le dernier = [En-tête IP + En-tête TCP + (charge utile TCP = taille MSS de CL1)] = [20+20+1460] = 1500
   - Taille du dernier paquet [en-tête IP+en-tête TCP + (segment TCP restant)] = [20 + 20 + 480] = 520

Tâches de configuration

Le tableau suivant répertorie les tâches, les commandes Citrix ADC et les exemples de création de la configuration requise sur l'appliance Citrix ADC.

Tâches	Syntaxe CLI	Exemples
Définir le MTU des interfaces souhaitées pour la prise en charge des trames jumbo	set interface <id> -mtu <positive_integer>, show interface <id>	set int 10/1 -mtu 1500 set int 10/2 -mtu 9000

Tâches	Syntaxe CLI	Exemples
Créez des VLAN et définissez le MTU des VLAN souhaités pour la prise en charge des trames jumbo	add vlan <id> -mtu <positive_integer>, show vlan <id>	add vlan 10 -mtu 1500 add vlan 20 -mtu 9000
Liez des interfaces aux VLAN	bind vlan <id> -ifnum <interface_name>, show vlan <id>	bind vlan 10 -ifnum 10/1 bind vlan 20 -ifnum 10/2
Ajouter une adresse SNIP	add ns ip <IPAddress> <netmask> -type SNIP, show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
Créer des services représentant des serveurs HTTP	add service <serviceName> <ip> HTTP <port>, show service <name>	add service SVC-S1 198.51.100.19 http 80, add service SVC-S2 198.51.100.20 http 80
Créer des serveurs virtuels d'équilibrage de charge HTTP et y lier les services	add lb vserver <name> HTTP <ip> <port>, bind lb vserver <vserverName> <serviceName>, show lb vserver <name>	add lb vserver LBVS-1 http 203.0.113.15 80, bind lb vserver LBVS-1 SVC-S1, bind lb vserver LBVS-1 SVC-S2
Créez un profil TCP personnalisé et définissez son MSS pour la prise en charge des trames jumbo	add tcpProfile <name> -mss <positive_integer>, show tcpProfile <name>	add tcpprofile NS1-SERVERS-JUMBO -mss 8960
Liez le profil TCP personnalisé aux services souhaités	set service <Name> -tcpProfileName <string>, show service <name>	set service SVC-S1 -TCPProfileName NS1-SERVERS-JUMBO, set service SVC-S2 -TCPProfileName NS1-SERVERS-JUMBO
Enregistrer la configuration	save ns config, show ns config	

Cas d'utilisation 3 — Coexistence de flux Jumbo et non-Jumbo sur le même ensemble d'interfaces

August 20, 2021

Prenons un exemple dans lequel les serveurs virtuels d'équilibrage de charge LBVS-1 et LBVS-2 sont configurés sur l'appliance Citrix ADC NS1. LBVS-1 est utilisé pour équilibrer la charge du trafic HTTP entre les serveurs S1 et S2, et LBVS-2 est utilisé pour équilibrer la charge du trafic entre les serveurs S3 et S4.

CL1 est sur VLAN 10, S1 et S2 sur VLAN20, CL2 sur VLAN 30, et S3 et S4 sur VLAN 40. VLAN 10 et VLAN 20 prennent en charge les trames jumbo, et VLAN 30 et VLAN 40 ne prennent en charge que les trames régulières.

En d'autres termes, la connexion entre CL1 et NS1 et la connexion entre NS1 et le serveur S1 ou S2 prennent en charge les trames jumbo. La connexion entre CL2 et NS1 et la connexion entre NS1 et le serveur S3 ou S4 ne prennent en charge que les trames régulières.

L'interface 10/1 de NS1 reçoit ou envoie du trafic depuis ou vers des clients. L'interface 10/2 de NS1 reçoit ou envoie du trafic depuis ou vers les serveurs.

L'interface 10/1 est liée à VLAN 10 et VLAN 30 en tant qu'interface balisée, et l'interface 10/2 est liée à VLAN 20 et VLAN 40 en tant qu'interface balisée.

Pour la prise en charge des trames jumbo, le MTU est réglé sur 9216 pour les interfaces 10/1 et 10/2.

Sur NS1, le MTU est défini sur 9000 pour VLAN 10 et VLAN 20 pour la prise en charge des trames jumbo, et le MTU est défini sur la valeur par défaut 1500 pour VLAN 30 et VLAN 40 pour la prise en charge uniquement des trames régulières.

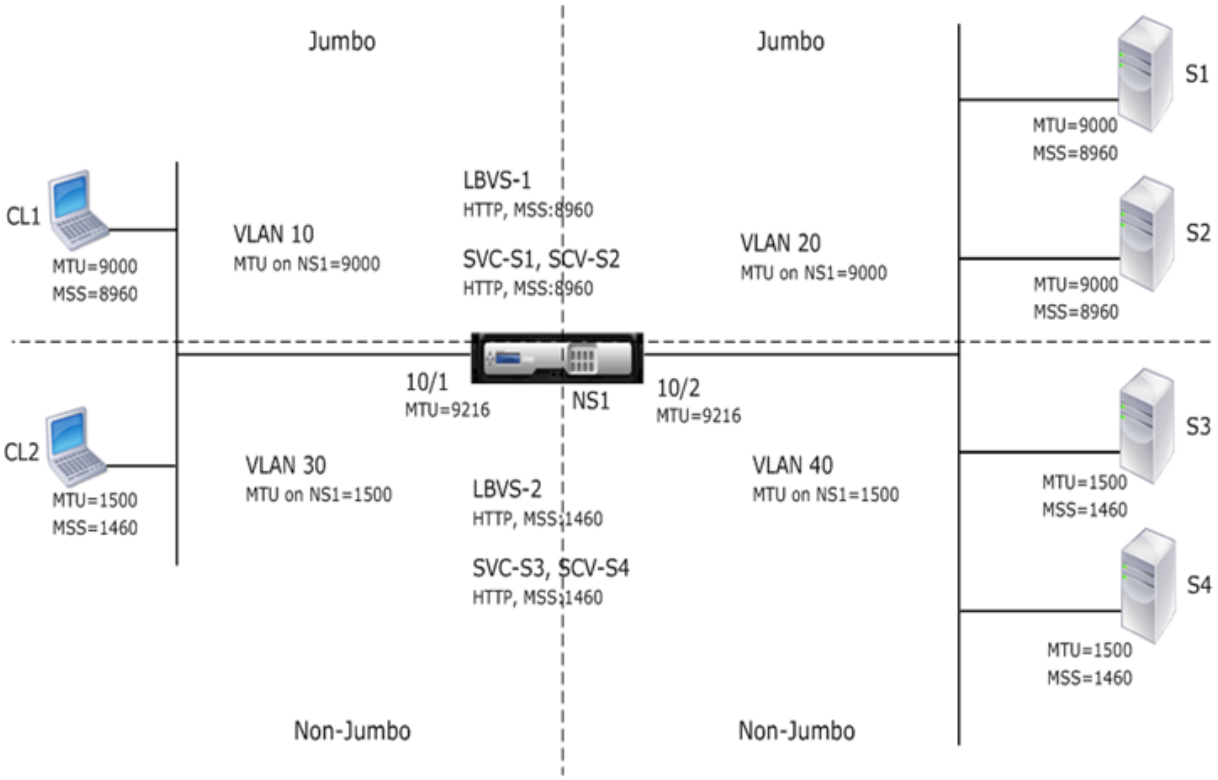
Le MTU effectif sur une interface Citrix ADC pour les paquets balisés VLAN est du MTU de l'interface ou du MTU du VLAN, la valeur la plus faible étant retenue. Par exemple :

- Le MTU de l'interface 10/1 est 9216. Le MTU de VLAN 10 est 9000. Sur l'interface 10/1, le MTU des paquets balisés VLAN 10 est 9000.
- Le MTU de l'interface 10/2 est 9216. Le MTU du VLAN 20 est 9000. Sur l'interface 10/2, le MTU des paquets balisés VLAN 20 est 9000.
- Le MTU de l'interface 10/1 est 9216. Le MTU du VLAN 30 est 1500. Sur l'interface 10/1, le MTU des paquets balisés VLAN 30 est 1500.
- Le MTU de l'interface 10/2 est 9216. Le MTU du VLAN 40 est 1500. Sur l'interface 10/2, le MTU des paquets balisés VLAN 40 est 9000.

CL1, S1, S2 et tous les périphériques réseau situés entre CL1 et S1 ou S2 sont configurés pour les trames jumbo.

Puisque le trafic HTTP est basé sur TCP, les MSSS sont définis en conséquence à chaque point d'extrémité pour la prise en charge des trames jumbo.

- Pour la connexion entre CL1 et le serveur virtuel LBVS-1 de NS1, le MSS sur NS1 est défini dans un profil TCP, qui est ensuite lié à LBVS-1.
- Pour la connexion entre une adresse SNIP de NS1 et S1, le MSS sur NS1 est défini dans un profil TCP, qui est ensuite lié au service (SVC-S1) représentant S1 sur NS1.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple : les cadres Jumbo utilisent des exemples de paramètres de cas 3.

Voici le flux de trafic de la demande de CL1 à S1 :

1. Le client CL1 crée une requête HTTP de 20000 octets à envoyer au serveur virtuel LBVS-1 de NS1.
2. CL1 ouvre une connexion à LBVS-1 de NS1. CL1 et NS1 échangent leurs valeurs MSS TCP tout en établissant la connexion.
3. Étant donné que la valeur MSS de NS1 est inférieure à la requête HTTP, CL1 segmente les données de la demande en multiples de MSS de NS1 et envoie ces segments dans des paquets IP marqués VLAN 10 à NS1.
   - Taille des deux premiers paquets = [en-tête IP +en-tête TCP + (segment TCP = NS1 MSS)] = [20 + 20 + 8960] = 9000
   - Taille du dernier paquet = [en-tête IP+en-tête TCP + (segment TCP restant)] = [20+2080] = 2120
4. NS1 reçoit ces paquets à l'interface 10/1. NS1 accepte ces paquets car la taille de ces paquets

est égale ou inférieure à la MTU effective (9000) de l'interface 10/1 pour les paquets balisés VLAN 10.

5. À partir des paquets IP, NS1 assemble tous les segments TCP pour former la requête HTTP de 20000 octets. NS1 traite cette demande.
6. L'algorithme d'équilibrage de charge de LBVS-1 sélectionne le serveur S1 et NS1 ouvre une connexion entre l'une de ses adresses SNIP et S1. NS1 et CL1 échangent leurs valeurs MSS TCP respectives lors de l'établissement de la connexion.
7. NS1 segmente les données de demande en multiples de MSS de S1 et envoie ces segments dans des paquets IP marqués VLAN 20 vers S1.
    - Taille des deux premiers paquets = [en-tête IP +en-tête TCP + (charge utile TCP = S1 MSS)][20 + 20 + 8960] = 9000
    - Taille du dernier paquet = [en-tête IP+en-tête TCP + (segment TCP restant)] = [20+2080] = 2120

Voici le flux de trafic de la réponse de S1 à CL1 :

1. Le serveur S1 crée une réponse HTTP de 30000 octets à envoyer à l'adresse SNIP de NS1.
2. S1 segmente les données de réponse en multiples de MSS de NS1 et envoie ces segments dans des paquets IP marqués VLAN 20 vers NS1. Ces paquets IP proviennent de l'adresse IP de S1 et sont destinés à l'adresse SNIP de NS1.
    - Taille des trois premiers paquets = [en-tête IP+en-tête TCP + (segment TCP = taille MSS de NS1)][20 + 20 + 8960] = 9000
    - Taille du dernier paquet [en-tête IP+en-tête TCP + (segment TCP restant)] = [20 + 20 + 3120] = 3160
3. NS1 reçoit les paquets de réponse à l'interface 10/2. NS1 accepte ces paquets, car leur taille est égale ou inférieure à la valeur MTU effective (9000) de l'interface 10/2 pour les paquets balisés VLAN 20.
4. À partir de ces paquets IP, NS1 assemble tous les segments TCP pour former la réponse HTTP de 30000 octets. NS1 traite cette réponse.
5. NS1 segmente les données de réponse en multiples de MSS de CL1 et envoie ces segments dans des paquets IP marqués VLAN 10, de l'interface 10/1 à CL1. Ces paquets IP proviennent de l'adresse IP de LBVS et sont destinés à l'adresse IP de CL1.
    - Taille des trois premiers paquets = [en-tête IP+en-tête TCP + [(charge utile TCP = taille MSS de Cl1)][20 + 20 + 8960] = 9000
    - Taille du dernier paquet = = [en-tête IP+en-tête TCP + (segment TCP restant)][20 + 20 + 3120] = 3160

Tâches de configuration

Le tableau suivant répertorie les tâches, les commandes et les exemples de création de la configuration requise sur l'appliance Citrix ADC : les trames Jumbo utilisent les tâches de configuration du cas

3.

Prise en charge de Citrix ADC pour le déploiement de Microsoft Direct Access

August 20, 2021

Microsoft Direct Access est une technologie qui permet aux utilisateurs distants de se connecter de manière transparente et sécurisée aux réseaux internes de l'entreprise, sans avoir à établir une connexion VPN distincte. Contrairement aux connexions VPN, qui nécessitent une intervention de l'utilisateur pour ouvrir et fermer des connexions, un client compatible Accès direct se connecte automatiquement aux réseaux internes de l'entreprise chaque fois que le client se connecte à Internet.

Manage-Out est une fonctionnalité Microsoft Direct Access qui permet aux administrateurs du réseau d'entreprise de se connecter aux clients Direct Access en dehors du réseau et de les gérer (par exemple, effectuer des tâches d'administration, telles que la planification des mises à jour de service et la prise en charge à distance.

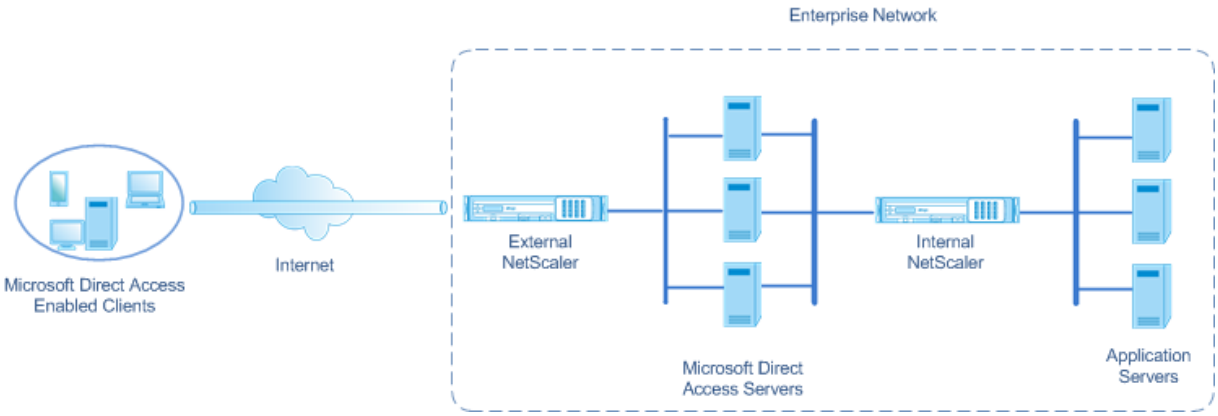
Dans un déploiement Direct Access, les appliances Citrix ADC offrent une haute disponibilité, une évolutivité, des performances élevées et une sécurité. La fonctionnalité d'équilibrage de charge Citrix ADC envoie le trafic client via le serveur le plus approprié. Les appliances peuvent également transférer le trafic Manage-Out via le bon chemin pour atteindre le client.

Architecture

L'architecture d'un déploiement Microsoft Direct Access comprend des clients compatibles Direct Access, des serveurs Direct Access, des serveurs d'applications et des appliances Citrix ADC internes et externes. Les clients se connectent à un serveur d'applications via un serveur d'accès direct. Une appliance Citrix ADC externe équilibre la charge du trafic client vers un serveur Direct Access, et une appliance Citrix ADC interne transfère le trafic client depuis le serveur Direct Access vers le serveur d'applications de destination. L'accès direct est utilisé pour tunneliser le trafic IPv6 du client sur le réseau IPv4. Un serveur virtuel d'équilibrage de charge IPv4 sur l'appliance Citrix ADC externe équilibre le trafic tunnel du client vers l'un des serveurs d'accès direct. Le serveur Direct Access extrait les paquets IPv6 des paquets IPv4 du client reçu et les envoie au serveur d'applications de destination via l'appliance Citrix ADC interne. L'appliance interne Citrix ADC dispose de règles de session de transfert avec l'option de cache de routage source activée pour stocker les informations de connexion de couche 2 et de couche 3 sur le trafic du client à partir du serveur Direct Access. L'appliance Citrix ADC stocke les informations de couche 2 et de couche 3 suivantes dans une table appelée table de cache de routage source :

- Adresse IP source du paquet reçu
- Adresse MAC du serveur d'accès direct qui a envoyé le paquet
- ID VLAN de l'appliance Citrix ADC qui a reçu le paquet
- ID d'interface de l'appliance Citrix ADC qui a reçu le paquet

L'appliance Citrix ADC utilise les informations de la table de cache de routage source pour transférer une réponse au même serveur Direct Access car elle dispose des informations de tunnel pour atteindre le client. En outre, l'appliance interne utilise la table de cache de routage source pour transférer le trafic de sortie du serveur d'applications vers le serveur d'accès direct approprié pour atteindre un client particulier.



Configuration de l'appliance Citrix ADC interne dans un déploiement Microsoft Direct Access

Pour configurer l'appliance Citrix ADC interne pour transférer la réponse d'un serveur d'applications et le trafic de gestion vers la passerelle d'accès direct appropriée, configurez les règles de session de transfert. Dans chaque règle, définissez le paramètre sourceroutecache sur Enabled.

Pour créer une règle de session de transfert à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ForwardingSession** <name>((<network>[]<netmask>) | **-acl6name** <string>| **-aclname** <string>) **-sourceroutecache** (**ACTIVÉ** |DÉSACTIVÉ**]
- **show forwardingsession** <name>

Exemple de configuration :

Dans l'exemple suivant, la règle de session de transfert MS-DA-FW-1 est créée sur l'appliance Citrix ADC interne. La session de transfert stocke les informations de couche 2 et de couche 3 pour tous les paquets IPv6 entrants à partir d'un serveur d'accès direct qui correspond au préfixe IPv6 source 2001:DB8 : :/96.


```
> add forwardingSession MS-DA-FW-1 2001:DB8::/96 -sourceroutecache -
    ENABLED
 Done
```

Affichage de la table du cache de routage source

Vous pouvez afficher la table de cache de routage source pour surveiller ou détecter toute connexion indésirable entre les serveurs d'accès direct et les serveurs d'applications.

Pour afficher la table de cache de routage source à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **show sourceroutecachetable**

Exemple :

```
> show sourceroutecachetable
SOURCEIP            MAC                 VLAN    INTERFACE
2001:DB8:5001:10    56:53:24:3d:02:eb    30        1/2
2001:DB8:5003:30    60:54:35:3e:04:bd    60        1/3
Done
```

Effacement de la table du cache de routage source

Vous pouvez effacer toutes les entrées de la table de cache de routage source sur une appliance Citrix ADC.

Pour effacer la table de cache de routage source à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **flush ns sourceroutecachetable**

Listes de contrôle d'accès

August 20, 2021

Les listes de contrôle d'accès (ACL) filtrent le trafic IP et sécurisent votre réseau contre les accès non autorisés. Une liste ACL est un ensemble de conditions que Citrix ADC évalue pour déterminer s'il faut autoriser l'accès. Par exemple, le service des finances ne veut probablement pas autoriser l'accès à ses ressources par d'autres services, tels que les ressources humaines et la documentation, et ces services veulent restreindre l'accès à leurs données.

Lorsque Citrix ADC reçoit un paquet de données, il compare les informations contenues dans le paquet de données avec les conditions spécifiées dans l'ACL et autorise ou refuse l'accès. L'administrateur de l'organisation peut configurer les ACL pour qu'elles fonctionnent dans les modes de traitement suivants :

- ALLOW : traite le paquet.
- BRIDGE : relie le paquet à la destination sans le traiter. Le paquet est directement envoyé par le transfert de couche 2 et de couche 3.
- DENY : abandonne le paquet.

Les règles ACL constituent le premier niveau de défense sur Citrix ADC.

Citrix ADC prend en charge les types d'ACL suivants :

- **Les listes ACL simples** filtrent les paquets en fonction de leur adresse IP source et, éventuellement, de leur protocole, de leur port de destination ou de leur domaine de trafic. Tout paquet ayant les caractéristiques spécifiées dans la liste ACL est supprimé.
- **Les listes ACL étendues filtrent les** paquets de données en fonction de divers paramètres, tels que l'adresse IP source, le port source, l'action et le protocole. Une liste ACL étendue définit les conditions qu'un paquet doit satisfaire pour que Citrix ADC traite le paquet, pont le paquet ou dépose le paquet.

Nomenclature

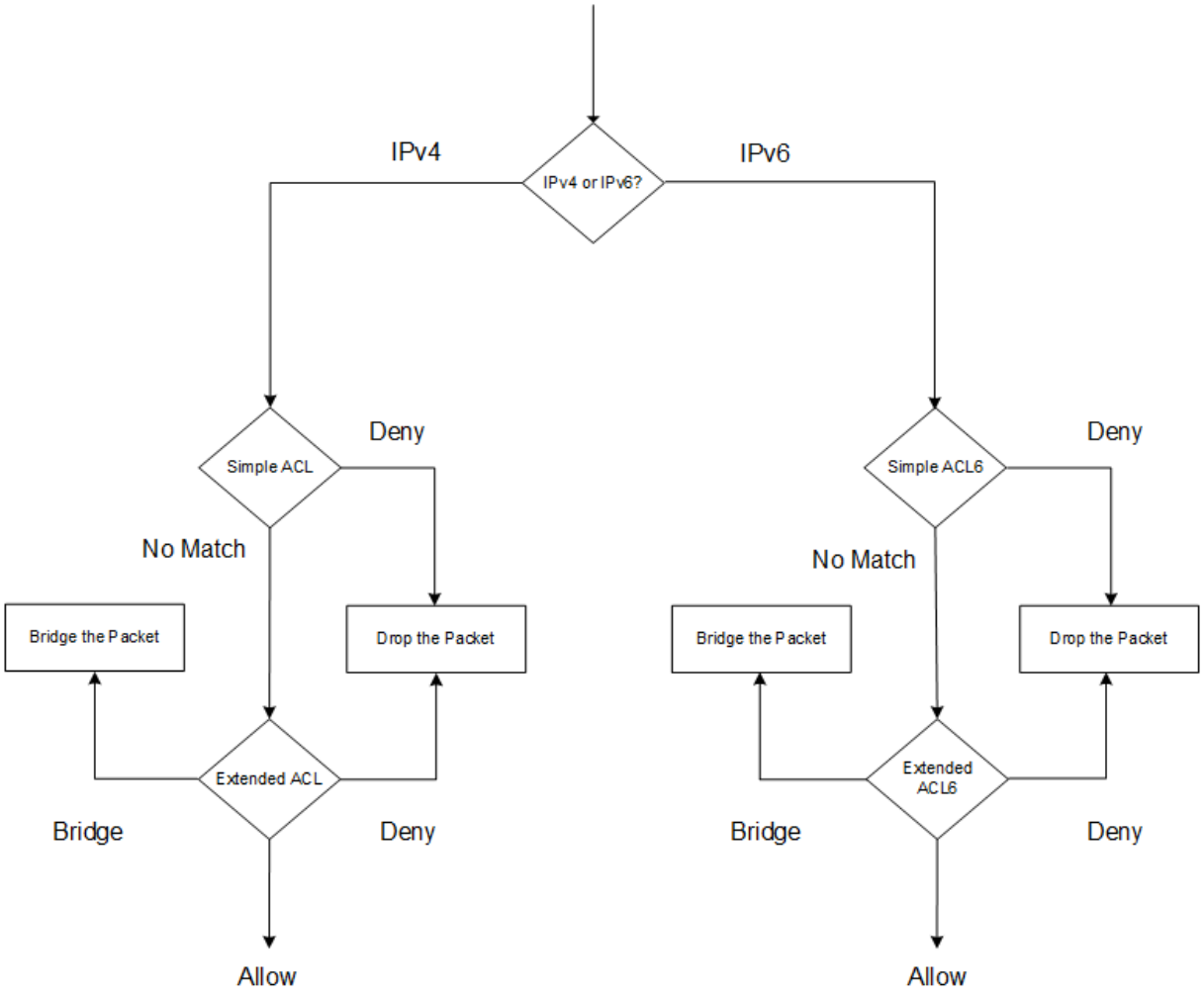
Dans les interfaces utilisateur Citrix ADC, les termes ACL simple et ACL étendue font référence aux listes d'accès qui traitent les paquets IPv4. Une ACL qui traite les paquets IPv6 est appelée ACL6 simple ou ACL6 étendue. Lorsque vous discutez des deux types, cette documentation les désigne parfois comme des ACL simples ou des ACL étendues.

Priorité ACL

Si les ACL simples et étendues sont configurées, les paquets entrants sont comparés aux ACL simples en premier.

Citrix ADC détermine d'abord si le paquet entrant est un paquet IPv4 ou IPv6, puis compare les caractéristiques du paquet à des ACL simples ou ACL6 simples. Si une correspondance est trouvée, le paquet est supprimé. Si aucune correspondance n'est trouvée, le paquet est comparé aux ACL étendues ou aux ACL6 étendues. Si cette comparaison aboutit à une correspondance, le paquet est traité comme spécifié dans l'ACL. Le paquet peut être ponté, abandonné ou autorisé. Si aucune correspondance n'est trouvée, le paquet est autorisé.

Figure 1. Séquence de flux ACL simple et étendue



ACL simples et ACL6 simples

August 20, 2021

Une ACL simple ou un ACL6 simple utilise peu de paramètres et peut être configuré uniquement pour supprimer les paquets IP. Les paquets peuvent être supprimés en fonction de leur adresse IP source et, éventuellement, de leur protocole, de leur port de destination ou de leur domaine de trafic.

Lors de la création d'une ACL simple ou d'une ACL6 simple, vous pouvez spécifier un temps de vie (TTL), en secondes, après quoi l'ACL expire. Les ACL avec des TTL ne sont pas enregistrées lorsque vous enregistrez la configuration. Vous pouvez afficher des ACL simples et des ACL6 simples pour vérifier leur configuration, et vous pouvez afficher leurs statistiques.

Configuration des ACL simples et des ACL6 simples

La configuration d'une ACL simple ou d'un ACL6 simple sur un Citrix ADC peut inclure les tâches suivantes.

- **Créez des ACL simples ou des ACL6**simples. Créer des ACL simples ou des ACL6 simples pour supprimer (refuser) les paquets en fonction de leur adresse IP source et, éventuellement, de leur protocole, de leur port de destination ou de leur domaine de trafic.
- **Supprimez les ACL simples ou les ACL6**simples. Ces ACL ne peuvent pas être modifiées une fois créées. Si vous devez modifier une liste ACL simple ou un ACL6 simple, vous devez la supprimer et en créer une.

Procédures CLI

Pour créer une ACL simple à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 - ns simpleacl <aclname> DENY -srcIP <ip_addr> [-destPort <port> -
    protocol ( TCP | UDP )] [-TTL <positive_integer>]
2 - show ns simpleacl [<aclname>]
3 <!--NeedCopy-->
```

Exemple :

```
1 > add simpleacl rule1 DENY -srcIP 10.102.29.5 -TTL 600
2 Done
3 <!--NeedCopy-->
```

Pour créer un ACL6 simple à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 - add ns simpleacl6 <aclname> DENY - srcIPv6 <ipv6_addr|null> [-
    destPort <port> -protocol ( TCP | UDP )] [-TTL <positive_integer>]
2 - show ns simpleacl6 [<aclname>]
3 <!--NeedCopy-->
```

Exemple :

```
1 > add ns simpleacl6 rule1 DENY - srcIPv6 3ffe:192:168:215::82 -
    destPort 80 -Protocol TCP -TTL 9000
2  Done
3 <!--NeedCopy-->
```

Pour supprimer une seule ACL simple à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **rm ns simpleacl** <aclname>
- **show ns simpleacl**

Pour supprimer un seul ACL6 simple à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **rm ns simpleacl6**<aclname>
- **show ns simpleacl6**

Pour supprimer toutes les listes ACL simples à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **clear ns simpleacl**
- **show ns simpleacl**

Pour supprimer tous les ACL6 simples à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **clear ns simpleacl6**
- **show ns simpleacl6**

Procédures GUI

Pour créer une ACL simple à l'aide de l'interface graphique :

Accédez à **Système > Réseau > ACL** et, sous l'onglet **ACL simples**, ajoutez une nouvelle ACL simple.

Pour créer un ACL6 simple à l'aide de l'interface graphique :

Accédez à **Système > Réseau > ACL** et, sous l'onglet **Simple ACL6s**, ajoutez un nouvel ACL6 simple.

Pour supprimer une seule ACL simple à l'aide de l'interface graphique :

Accédez à **Système > Réseau > ACL** et, sous l'onglet **ACL simples**, supprimez la liste ACL simple.

Pour supprimer une seule ACL6 simple à l'aide de l'interface graphique :

Accédez à **Système > Réseau > ACL** et, sous l'onglet **ACL6s simples**, supprimez l'ACL6 simple.

Pour supprimer toutes les listes ACL simples à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > ACL**.
2. Sous l'onglet **ACL simples**, dans la liste **Action**, cliquez sur **Effacer** .

Pour supprimer tous les ACL6 simples à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > ACL**.
2. Sous l'onglet **Simple ACL6s**, dans la liste **Action**, cliquez sur **Effacer** .

Affichage des statistiques ACL simples et ACL6 simples

Vous pouvez afficher les statistiques ACL simples (ou ACL6 simples), qui incluent le nombre de correspondances, le nombre d'erreurs et le nombre de listes ACL simples configurées.

Le tableau suivant décrit les statistiques que vous pouvez afficher pour les listes ACL simples et les ACL6 simples.

Statistiques	Indique
Match ACL	Paquets correspondant à une ACL
Échecs ACL	Paquets ne correspondant à aucune ACL
Nombre d'ACL	Nombre d'ACL configurées

Procédures CLI

Pour afficher des statistiques ACL simples à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **stat ns simpleacl**

Exemple :

```
1  > stat ns simpleacl
2
3  SimpleACL Statistics
4
5                                              Rate (/s)
                                                  Total
6  SimpleACL hits                                     0
                        0
7  SimpleACL misses                                   0
      51872
8  SimpleACLs count                                  --
                        2
9  Done
10 <!--NeedCopy-->
```

Pour afficher des statistiques ACL6 simples à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **stat ns simpleacl6**

Procédures GUI

Pour afficher des statistiques ACL simples à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **ACL** et, sous l'onglet **ACL simples**, sélectionnez l'ACL et cliquez sur **Statistiques** .

Pour afficher des statistiques ACL6 simples à l'aide de l'interface graphique :

Accédez à **Système > Réseau > ACL** et, sous l'onglet **ACL6s simples**, sélectionnez l'ACL6 simple et cliquez sur **Statistiques**.

Terminer les connexions établies

Pour une ACL simple ou ACL6 simple, Citrix ADC bloque toutes les nouvelles connexions qui correspondent aux conditions spécifiées dans l'ACL. Les paquets liés aux connexions existantes qui ont été établies avant la création de l'ACL ne sont pas bloqués. Pour mettre fin aux connexions précédemment établies qui correspondent à une ACL existante, vous pouvez exécuter une opération de vidage à partir de l'interface de ligne de commande ou de l'interface graphique.

Flush peut être utile dans les cas suivants :

- Vous recevez une liste d'adresses IP sur la liste noire et souhaitez bloquer complètement ces adresses IP d'accéder au Citrix ADC. Dans ce cas, vous créez des ACL simples ou des ACL6 simples pour bloquer toute nouvelle connexion à partir de ces adresses IP, puis vider toutes les connexions existantes associées à ces adresses.
- Vous souhaitez mettre fin à de nombreuses connexions à partir d'un réseau particulier sans prendre le temps de les arrêter une par une.

Avant de commencer

- Lorsque vous exécutez le vidage, Citrix ADC effectue une recherche dans toutes ses connexions établies et met fin aux connexions qui correspondent aux conditions spécifiées dans l'une des listes ACL simples configurées sur l'ADC.
- Si vous envisagez de créer plusieurs ACL simples et de vider les connexions existantes qui correspondent à l'une d'entre elles, vous pouvez minimiser l'effet sur les performances en créant d'abord toutes les listes ACL simples, puis en exécutant le vidage une seule fois.

Procédures CLI

Pour mettre fin à toutes les connexions IPv4 établies qui correspondent à l'une de vos listes d'accès simples configurées à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **flush simpleacl -estSessions**

Pour mettre fin à toutes les connexions IPv6 établies qui correspondent à l'un de vos ACL6 simples configurés à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **flush simpleacl6 -ESTsessions**

Procédures GUI

Pour mettre fin à toutes les connexions IPv4 établies qui correspondent à l'une de vos listes d'accès simples configurées à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > ACL**.
2. Sous l'onglet **ACL simples**, dans la liste **Action**, cliquez sur **Vider** .

Pour mettre fin à toutes les connexions IPv6 établies qui correspondent à l'un de vos ACL6 simples configurés à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > ACL**.
2. Sous l'onglet **Simple ACL6s**, dans la liste **Action**, cliquez sur **Vider** .

ACL étendues et ACL6 étendues

October 5, 2021

Les ACL étendues et les ACL6 étendues fournissent des paramètres et des actions qui ne sont pas disponibles avec les ACL simples. Vous pouvez filtrer les données en fonction de paramètres tels que l'adresse IP source, le port source, l'action et le protocole. Vous pouvez spécifier des tâches pour autoriser un paquet, refuser un paquet ou pont un paquet.

Les ACL étendues et les ACL6 peuvent être modifiées après leur création, et vous pouvez renuméroter leurs priorités pour spécifier l'ordre dans lequel elles sont évaluées.

Remarque : Si vous configurez des ACL simples et étendues, les ACL simples sont prioritaires sur les ACL étendues.

Les actions suivantes peuvent être effectuées sur les ACL étendues et les ACL6 : Modifier, Appliquer, Désactiver, Activer, Supprimer et Renuméroter (priorité). Vous pouvez afficher les listes de contrôle d'accès étendues et les ACL6 pour vérifier leur configuration, et vous pouvez afficher leurs statistiques.

Vous pouvez configurer Citrix ADC pour consigner les détails des paquets qui correspondent à une liste de contrôle d'accès étendue.

Application des ACL étendues et ACL6 étendues : contrairement aux ACL simples et ACL6, les ACL étendues et ACL6 créées sur Citrix ADC ne fonctionnent pas tant qu'elles ne sont pas appliquées. De plus, si vous apportez des modifications à une ACL étendue ou à une ACL6, telles que la désactivation des ACL, la modification d'une priorité ou la suppression des ACL, vous devez réappliquer les listes ACL ou ACL6 étendues. Vous devez les réappliquer après avoir activé la journalisation. La procédure d'application des ACL étendues ou des ACL6 les réapplique toutes. Par exemple, si vous avez appliqué les règles ACL étendues 1 à 10, puis que vous créez et appliquez la règle 11, les 10 premières règles sont appliquées à nouveau.

Si une session est associée à une liste de contrôle d'accès REFUSÉE, cette session est interrompue lorsque vous appliquez les listes de contrôle d'accès.

Les ACL étendues et les ACL6 sont activées par défaut. Lorsqu'ils sont appliqués, Citrix ADC commence à comparer les paquets entrants avec eux. Toutefois, si vous les désactivez, ils ne sont pas utilisés tant que vous ne les avez pas réactivés, même s'ils sont réappliqués.

Renumérotation des priorités des ACL étendues et des ACL6 étendues : les numéros de priorité déterminent l'ordre dans lequel les ACL étendues ou ACL6 sont comparées à un paquet. Une liste de contrôle d'accès dont le numéro de priorité est inférieur a une priorité plus élevée. Il est évalué avant les ACL avec des numéros de priorité plus élevés (priorités inférieures), et la première ACL correspondant au paquet détermine l'action appliquée au paquet.

Lorsque vous créez une ACL étendue ou une ACL6, Citrix ADC lui attribue automatiquement un numéro de priorité multiple de 10, sauf indication contraire. Par exemple, si deux ACL étendues ont des priorités de 20 et 30, respectivement, et que vous souhaitez qu'une troisième ACL ait une valeur comprise entre ces nombres, vous pouvez lui attribuer une valeur de 25. Si vous souhaitez par la suite conserver l'ordre dans lequel les ACL sont évaluées, mais rétablir leur numérotation à des multiples de 10, vous pouvez utiliser la procédure de renumérotation.

Configuration des ACL étendues et des ACL6 étendues

La configuration d'une ACL étendue ou d'une ACL6 sur un Citrix ADC comprend les tâches suivantes.

- **Créez une ACL étendue ou une ACL6.** Créez une ACL étendue ou une ACL6 pour autoriser, refuser ou relier un paquet. Vous pouvez spécifier une adresse IP ou une plage d'adresses IP à mettre en correspondance avec les adresses IP source ou de destination des paquets. Vous pouvez spécifier un protocole à mettre en correspondance avec le protocole des paquets entrants.
- (Facultatif) **Modifiez une ACL étendue ou une ACL6**. Vous pouvez modifier les ACL étendues ou les ACL6 que vous avez précédemment créées. Ou, si vous souhaitez temporairement en mettre un hors d'usage, vous pouvez le désactiver, puis le réactiver ultérieurement.
- **Appliquez des ACL étendues ou des ACL6**. Après avoir créé, modifié, désactivé ou réactivé, ou supprimé une ACL étendue ou une ACL6, vous devez appliquer les ACL ou ACL6 étendues pour les activer.

- (Facultatif) **Renuméroter les priorités des ACL étendues ou des ACL6**. Si vous avez configuré des listes de contrôle d'accès avec des priorités qui ne sont pas des multiples de 10 et que vous souhaitez rétablir la numérotation en multiples de 10, utilisez la procédure de renumérotation.

Procédures CLI

Pour créer une liste de contrôle d'accès étendue à l'aide de l'interface de lignede commande :

À l'invite de commandes, tapez :

- **add ns acl** <aclname> <aclaction> [-**srcIP** [<operator>] <srcIPVal>] [-**srcPort** [<operator>] <srcPortVal>] [-**destIP** [<operator>] <destIPVal>] [-**destPort** [<operator>] <destPortVal>] [-**TTL** <positive_integer>] [-**srcMac** <mac_addr>] [(-**protocol** <protocol> [-established]) | -**protocolNumber** <positive_integer>] [-**vlan** <positive_integer>] [-**interface** <interface_name>] [-**icmpType** <positive_integer> [-**icmpCode** <positive_integer>]] [-**priority** <positive_integer>] [-**state** (ENABLED | DISABLED)] [-**logstate** (ENABLED | DISABLED) [-**ratelimit** <positive_integer>]]
- **show ns acl** [<aclName>]

Pour créer un ACL6 étendu à l'aide de l'interface de lignede commande :

À l'invite de commandes, tapez :

- **add ns acl6** <acl6name> <acl6action> [-**srcIPv6** [<operator>] <srcIPv6Val>] [-**srcPort** [<operator>] <srcPortVal>] [-**destIPv6** [<operator>] <destIPv6Val>] [-**destPort** [<operator>] <destPortVal>] [-**TTL** <positive_integer>] [-**srcMac** <mac_addr>] [(-**protocol** <protocol> [-established]) | -**protocolNumber** <positive_integer>] [-**vlan** <positive_integer>] [-**interface** <interface_name>] [-**icmpType** <positive_integer> [-**icmpCode** <positive_integer>]] [-**priority** <positive_integer>] [-**state** (ENABLED | DISABLED)]
- **show ns acl6** [<aclName>]

Pour modifier une liste de contrôle d'accès étendue à l'aide de l'interface de lignede commande :

Pour modifier une liste de contrôle d'accès étendue, tapez la commande **set ns acl**, le nom de l'ACL étendue et les paramètres à modifier, avec leurs nouvelles valeurs.

Pour modifier un ACL6 étendu à l'aide de l'interface de ligne de commande :

Pour modifier un ACL6 étendu, tapez la commande **set ns acl6**, le nom de l'ACL6 étendu et les paramètres à modifier, avec leurs nouvelles valeurs.

Pour désactiver ou activer une liste de contrôle d'accès étendue à l'aide de l'interface de lignede commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- **disable ns acl** <aclname>
- **enable ns acl** <aclname>

Pour désactiver ou activer un ACL6 étendu à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- **disable ns acl6** <aclname>
- **enable ns acl6** <aclname>

Pour appliquer des listes ACL étendues à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **apply ns acls**

Pour appliquer des ACL6 étendus à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **apply ns acls6**

Pour renuméroter les priorités des ACL étendues à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **renumber ns acls**

Pour renuméroter les priorités des ACL6 étendus à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **renumber ns acls6**

Procédures GUI

Pour configurer une liste de contrôle d'accès étendue à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACL** et, sous l'onglet **ACL étendues**, ajoutez une nouvelle ACL étendue ou modifiez une ACL étendue existante. Pour activer ou désactiver une liste de contrôle d'accès étendue existante, sélectionnez-la, puis sélectionnez **Activer** ou **désactiver** dans la liste **Action** .

Pour configurer un ACL6 étendu à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACLs** et, sous l'onglet **ACL6 étendu**, ajoutez un nouvel ACL6 étendu ou modifiez un ACL6 étendu existant. Pour activer ou désactiver un ACL6 étendu existant, sélectionnez-le, puis sélectionnez **Activer** ou **Désactiver** dans la liste **Action** .

Pour appliquer des listes de contrôle d'accès étendues à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACL** et, sous l'onglet **ACL étendues**, dans la liste **Action**, cliquez sur **Appliquer**.

Pour appliquer des ACL6 étendues à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACL** et, sous l'onglet **ACL6 étendu**, dans la liste **Action**, cliquez sur **Appliquer**.

Pour renuméroter les priorités des listes de contrôle d'accès étendues à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACL** et, sous l'onglet **ACL étendues**, dans la liste **Action**, cliquez sur **Renuméroter la ou les priorités**.

Pour renuméroter les priorités des ACL6 étendues à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACL** et, sous l'onglet **ACL6 étendu**, dans la liste **Action**, cliquez sur **Renuméroter la ou les priorités**.

Exemples de configurations

Le tableau suivant présente des exemples de configuration de règles ACL étendues via l'interface de ligne de commande : exemples de configurations ACL.

Journalisation des listes ACL étendues

Vous pouvez configurer Citrix ADC pour consigner les détails des paquets qui correspondent aux listes de contrôle d'accès étendues.

En plus du nom ACL, les détails consignés incluent des informations spécifiques au paquet, telles que les adresses IP source et de destination. Les informations sont stockées soit dans le fichier syslog, soit dans le `nslog` fichier, en fonction du type de logging global (`syslog or nslog`) activé.

La journalisation doit être activée au niveau global et au niveau ACL. Le paramètre global est prioritaire.

Pour optimiser la journalisation, lorsque plusieurs paquets du même flux correspondent à une ACL, seuls les détails du premier paquet sont consignés et le compteur est incrémenté pour chaque paquet appartenant au même flux. Un flux est défini comme un ensemble de paquets ayant les mêmes valeurs pour l'adresse IP source, l'adresse IP de destination, le port source, le port de destination et les paramètres de protocole. Pour éviter l'inondation des messages de journal, Citrix ADC effectue une limitation de débit interne afin que les paquets appartenant au même flux ne soient pas journalisés de manière répétée. Le nombre total de flux différents pouvant être enregistrés à un moment donné est limité à 10 000.

Remarque : Vous devez appliquer les listes de contrôle d'accès après avoir activé la journalisation.

Procédures CLI

Pour configurer la journalisation ACL étendue à l'aide de l'interface de lignede commande :

À l'invite de commandes, tapez les commandes suivantes pour configurer la journalisation et vérifier la configuration :

- **set ns acl** <aclName> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** <positive_integer>]
- **apply acls**
- **show ns acl** [<aclName>]

Procédures GUI

Pour configurer la journalisation ACL étendue à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > ACL** et, sous l'onglet **ACL étendues**, ouvrez l'ACL étendue.
2. Définissez les paramètres suivants :
   - **État du journal** : activez ou désactivez la journalisation des événements liés à la règle ACL étendue. Les messages de journal sont stockés sur le `syslog or auditlog` serveur configuré.
   - **Limite du nombre de journaux** : nombre maximal de messages de journal à générer par seconde. Si vous définissez ce paramètre, vous devez activer le paramètre Log State.

Exemple de configuration

```
> set ns acl restrict -logstate ENABLED -ratelimit 120
Warning: ACL modified, apply ACLs to activate change

> apply ns acls
Done
<!--NeedCopy-->
```

Journalisation des ACL6 étendues

Vous pouvez configurer l'appliance Citrix ADC pour consigner les détails des paquets qui correspondent à une règle ACL6 étendue. En plus du nom ACL6, les détails consignés incluent des informations spécifiques au paquet, telles que les adresses IP source et de destination. Les informations sont stockées dans un syslog ou dans un fichier `nslog`, en fonction du type de logging (`syslog or nslog`) que vous avez configuré dans l'appliance Citrix ADC.

Pour optimiser la journalisation, lorsque plusieurs paquets du même flux correspondent à un ACL6, seuls les détails du premier paquet sont consignés. Le compteur est incrémenté pour tous les autres paquets appartenant au même flux. Un flux est défini comme un ensemble de paquets qui ont les mêmes valeurs pour les paramètres suivants :

- IP source

- IP destination
- Port source
- Port de destination
- Protocole (TCP ou UDP)

Si un paquet entrant ne provient pas du même flux, un nouveau flux est créé. Le nombre total de flux différents pouvant être enregistrés à un moment donné est limité à 10 000.

Procédures CLI

Pour configurer la journalisation d'une règle ACl6 étendue à l'aide de l'interface de lignede commande :

- Pour configurer la journalisation lors de l'ajout de la règle ACL6 étendue, à l'invite de commandes, tapez :
  - **add acl6** <acl6Name> <acl6action> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** <positive_integer>]
  - **apply acls6**
  - **show acl6** [<acl6Name>]
- Pour configurer la journalisation d'une règle ACL6 étendue existante, à l'invite de commandes, tapez :
  - **set acl6** <acl6Name> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** <positive_integer>]
  - **show acl6** [<acl6Name>]
  - **apply acls6**

Procédures GUI

Pour configurer la journalisation ACL6 étendue à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **ACL**, puis cliquez sur l'onglet **ACL6 étendu** .
2. Définissez les paramètres suivants lors de l'ajout ou de la modification d'une règle ACL6 étendue existante.
   - **État du journal** : activez ou désactivez la journalisation des événements liés à la règle ACL6 étendue. Les messages de journal sont stockés dans le Syslog ou le `auditlog` serveur configuré.
   - **Limite du nombre de journaux** : nombre maximal de messages de journal à générer par seconde. Si vous définissez ce paramètre, vous devez activer le paramètre **Log State** .

Exemple de configuration


```
> set acl6 ACL6-1 -logstate ENABLED -ratelimit 120
Done

> apply acls6
Done
<!--NeedCopy-->
```

Affichage des listes de contrôle d'accès étendues et des statistiques ACL6 étendues

Vous pouvez afficher des statistiques sur les listes de contrôle d'accès étendues et les ACL6.

Le tableau suivant répertorie les statistiques associées aux listes ACL étendues et aux ACL6, ainsi que leurs descriptions.

Statistique	Spécifie
Allow ACL matches	Paquets correspondant aux ACL avec le mode de traitement défini sur Autoriser. Citrix ADC traite ces paquets.
Matchs NAT ACL	Paquets correspondant à une ACL NAT, entraînant une session NAT.
Deny ACL matches	Les paquets ont été supprimés parce qu'ils correspondent aux ACL avec le mode de traitement défini sur DENY.
Matchs ACL Bridge	Paquets correspondant à une liste ACL de pont, qui, en mode transparent, contourne le traitement du service.
ACL matches	Paquets correspondant à une liste ACL.
ACL misses	Paquets ne correspondant à aucune liste de contrôle d'accès.
ACL Count	Nombre total de règles ACL configurées par les utilisateurs.

Statistique	Spécifie
Effective ACL Count	Nombre total d'ACL effectifs configurés en interne. Pour une liste de contrôle d'accès étendue avec une plage d'adresses IP, l'appliance Citrix ADC crée en interne une ACL étendue pour chaque adresse IP. Par exemple, pour une liste de contrôle d'accès étendue avec 1000 adresses IPv4 (plage ou ensemble de données), Citrix ADC crée en interne 1000 ACL étendues.

Procédures CLI

Pour afficher les statistiques de toutes les listes de contrôle d'accès étendues à l'aide de l'interface de lignede commande :

À l'invite de commandes, tapez :

- **stat ns acl**

Pour afficher les statistiques de tous les ACL6 étendus à l'aide de l'interface de lignede commande :

À l'invite de commandes, tapez :

- **stat ns acl6**

Procédures GUI

Pour afficher les statistiques d'une liste de contrôle d'accès étendue à l'aide de l'interface graphique :

- Accédez à **Système > Réseau > ACL**, sous l'onglet **ACL étendues**, sélectionnez l'ACL étendue, puis cliquez sur **Statistiques**.

Pour afficher les statistiques d'un ACL6 étendu à l'aide de l'interface graphique :

- Accédez à **Système > Réseau > ACL**, sous l'onglet **ACL6s étendus**, sélectionnez l'ACL étendue, puis cliquez sur **Statistiques**.

ACL avec état

Une règle ACL avec état crée une session lorsqu'une demande correspond à la règle et autorise les réponses obtenues même si ces réponses correspondent à une règle ACL de refus dans l'appliance

Citrix ADC. Une ACL avec état décharge le travail de création de règles ACL et de règles de session de transfert supplémentaires pour autoriser ces réponses spécifiques.

Les ACL avec état peuvent être utilisées au mieux dans un déploiement de pare-feu Edge d'une appliance Citrix ADC présentant les conditions suivantes :

- L'appliance Citrix ADC doit autoriser les demandes initiées par les clients internes et les réponses associées provenant d'Internet.
- La solution matérielle-logicielle doit supprimer les paquets d'Internet qui ne sont liés à aucune connexion client.

Avant de commencer

Avant de configurer des règles ACL avec état, notez les points suivants :

- L'appliance Citrix ADC prend en charge les règles ACL avec état et les règles ACL6 avec état.
- Dans une configuration haute disponibilité, les sessions d'une règle ACL avec état ne sont pas synchronisées avec le nœud secondaire.
- Vous ne pouvez pas configurer une règle ACL avec état si la règle est liée à une configuration NAT Citrix ADC. Voici quelques exemples de configurations NAT Citrix ADC :
  - RNAT
  - NAT à grande échelle (NAT44 à grande échelle, DS-Lite, NAT64 à grande échelle)
  - NAT64
  - Session de transfert
- Vous ne pouvez pas configurer une règle ACL en tant qu'état si les paramètres TTL et Établi sont définis pour cette règle ACL.
- Les sessions créées pour une règle ACL avec état continuent d'exister jusqu'à l'exode, quelles que soient les opérations ACL suivantes :
  - Supprimer ACL
  - Désactiver l'ACL
  - Effacer l'ACL
- Les listes de contrôle d'accès avec état ne sont pas prises en charge pour les protocoles suivants :
  - FTP actif
  - TFTP

Configurer les règles ACL IPv4 avec état

La configuration d'une règle ACL avec état consiste à activer le paramètre avec état d'une règle ACL.

Pour activer le paramètre avec état d'une règle ACL à l'aide de l'interface de lignede commande :

- Pour activer le paramètre stateful lors de l'ajout d'une règle ACL, à l'invite de commandes, tapez :

- **add acl** <lname> ALLOW -**stateful** (ENABLED | DISABLED)
- **apply acls**
- **show acl** <name>

- Pour activer le paramètre stateful d'une règle ACL existante, à l'invite de commandes, tapez :
  - **set acl** <name> -**stateful** (ENABLED | DISABLED)
  - **apply acls**
  - **show acl** <name>

Pour activer le paramètre avec état d'une règle ACL à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **ACL** et, dans l'onglet **ACL étendues** .
2. Activez le paramètre **Stateful** lors de l'ajout ou de la modification d'une règle ACL existante.

Exemple de configuration

```
> add acl ACL-1 allow -srciP 1.1.1.1 -stateful Yes

Done

> apply acls

Done

> show acl

1)         Name: ACL-1

    Action: ALLOW                          Hits: 0

    srcIP = 1.1.1.1

    destIP

    srcMac:

    Protocol:

    Vlan:                                 Interface:

    Active Status: ENABLED                 Applied Status: NOTAPPLIED

    Priority: 10                           NAT: NO

```



```
29     TTL:
30
31     Log Status: DISABLED
32
33     Forward Session: NO
34
35     Stateful: YES
36 <!--NeedCopy-->
```

Configurer les règles ACL6 avec état

La configuration d'une règle ACL6 avec état consiste à activer le paramètre avec état d'une règle ACL6.

Pour activer le paramètre avec état d'une règle ACL6 à l'aide de l'interface de lignede commande :

- Pour activer le paramètre stateful lors de l'ajout d'une règle ACL6, à l'invite de commandes, tapez :
  - **add acl6** <name> ALLOW -stateful (ENABLED | DISABLD)
  - **apply acls6**
  - **show acl6** <name>
- Pour activer le paramètre stateful d'une règle ACL6 existante, à l'invite de commandes, tapez :
  - **set acl6** <name> -**stateful** (ENABLED | DISABLED)
  - **apply acls6**
  - **show acl6** <name>

Pour activer le paramètre avec état d'une règle ACL6 à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **ACLs** et, dans l'onglet **Extended ACL6s** .
2. Activez le paramètre **Stateful** lors de l'ajout ou de la modification d'une règle ACL6 existante.

Exemple de configuration

```
1 >  add acl6 ACL6-1 allow -srcipv6 1000::1  - stateful Yes
2
3 Done
4
5 >  apply acls6
6
7 Done
8
9 > show acl6
```



```
10
11 1)    Name: ACL6-1
12
13     Action: ALLOW                          Hits: 0
14
15     srcIPv6 = 1000::1
16
17     destIPv6
18
19     srcMac:
20
21     Protocol:
22
23     Vlan:                                 Interface:
24
25     Active Status: ENABLED                 Applied Status: NOTAPPLIED
26
27     Priority: 10                           NAT: NO
28
29     TTL:
30
31     Forward Session: NO
32
33     Stateful: YES
34 <!--NeedCopy-->
```

ACL étendues basées sur un jeu de données

De nombreuses ACL sont nécessaires dans une entreprise. La configuration et la gestion de nombreuses listes de contrôle d'accès sont difficiles et fastidieuses lorsqu'elles nécessitent des modifications fréquentes.

Une appliance Citrix ADC prend en charge les jeux de données dans les ACL étendues. Le jeu de données est une fonctionnalité existante d'une appliance Citrix ADC. Un jeu de données est un tableau de modèles indexés de types : nombre (entier), adresse IPv4 ou adresse IPv6.

La prise en charge des jeux de données dans les listes ACL étendues est utile pour créer plusieurs règles ACL, qui nécessitent des paramètres ACL communs.

Lors de la création d'une règle ACL, au lieu de spécifier les paramètres communs, vous pouvez spécifier un jeu de données, qui inclut ces paramètres communs.

Toutes les modifications apportées au jeu de données sont automatiquement reflétées dans les règles ACL qui utilisent ce jeu de données. Les listes de contrôle d'accès avec jeux de données sont plus faciles à configurer et à gérer. Ils sont également plus petits et plus faciles à lire que les ACL classiques.

Actuellement, l'appliance Citrix ADC prend uniquement en charge les types de jeux de données suivants pour les listes de contrôle d'accès étendues :

- Adresse IPv4 (pour spécifier l'adresse IP source ou l'adresse IP de destination ou les deux pour une règle ACL)
- number (pour spécifier le port source ou le port de destination ou les deux pour une règle ACL)

Avant de commencer

Avant de configurer des règles ACL étendues basées sur des jeux de données, notez les points suivants :

- Assurez-vous que vous êtes familier avec la fonctionnalité de jeu de données d'une appliance Citrix ADC. Pour plus d'informations sur les jeux de données, voir Jeux de modèles et jeux de données.
- L'appliance Citrix ADC prend en charge les jeux de données uniquement pour les ACL étendues IPv4.
- L'appliance Citrix ADC prend uniquement en charge les types de jeux de données suivants pour les listes de contrôle d'accès étendues :
  - Adresse IPv4
  - nombre
- L'appliance Citrix ADC prend en charge les listes de contrôle d'accès étendues basées sur des jeux de données pour toutes les configurations Citrix ADC : autonome, haute disponibilité et cluster.
- Pour une liste de contrôle d'accès étendue avec des jeux de données contenant des plages, l'appliance Citrix ADC crée en interne une ACL étendue pour chaque combinaison de valeurs de jeu de données.
  - **Exemple 1** : Pour une liste de contrôle d'accès étendue basée sur un jeu de données IPv4 avec 1000 adresses IPv4 liées au jeu de données, et le jeu de données est défini sur le paramètre IP source, l'appliance Citrix ADC crée en interne 1000 ACL étendues.
  - **Exemple 2** : liste de contrôle d'accès étendue basée sur un jeu de données avec les paramètres suivants définis :
    - L'adresse IP source est définie sur un ensemble de données contenant 5 adresses IP.
    - L'adresse IP de destination est définie sur un ensemble de données contenant 5 adresses IP.
    - Le port source est défini sur un jeu de données contenant 5 ports.
    - Le port de destination est défini sur un jeu de données contenant 5 ports.

    L'appliance Citrix ADC crée en interne 625 listes de contrôle d'accès étendues. Chacune de ces listes de contrôle d'accès internes contient une combinaison unique des quatre valeurs

de paramètres mentionnées ci-dessus.

- L'appliance Citrix ADC prend en charge un maximum de 10 000 listes de contrôle d'accès étendues. Pour une liste de contrôle d'accès étendue basée sur un jeu de données IPv4 avec une plage d'adresses IP liées au jeu de données, l'appliance Citrix ADC cesse de créer des listes de contrôle d'accès internes une fois que le nombre total de listes ACL étendues atteint la limite maximale.
- Les compteurs suivants sont présents dans le cadre des statistiques ACL étendues :
  * **Nombre d'ACL**. Nombre total de règles ACL configurées par les utilisateurs.
  * Nombre de**LCA effectif**. Nombre total de règles d'ACL effectives configurées par l'appliance Citrix ADC en interne.

  Pour plus d'informations, reportez-vous à la section Affichage des statistiques ACL étendues et ACL6sétendues.

- L'appliance Citrix ADC ne prend pas en charge `set` et `unset` ne fonctionne pas pour associer/dissocier des jeux de données avec les paramètres d'une liste d'accès étendue. Vous pouvez définir les paramètres ACL sur un jeu de données uniquement pendant l' `add` opération.

Configuration des listes ACL étendues basées sur les jeux de données

La configuration d'une règle ACL étendue basée sur un jeu de données comprend les tâches suivantes :

- **Ajoutez un jeu de données**. Un jeu de données est un tableau de modèles indexés de types : nombre (entier), adresse IPv4 ou adresse IPv6. Dans cette tâche, vous créez un type de jeu de données, par exemple un jeu de données de type IPv4.
- **Liez des valeurs au jeu de données**. Spécifiez une valeur ou une plage de valeurs dans le jeu de données. Les valeurs spécifiées doivent être du même type que le type de jeu de données. Par exemple, vous pouvez spécifier une adresse IPv4 ou une plage d'adresses IPv4 pour le jeu de données de type IPv4.
- **Ajoutez une liste d'accès étendue et définissez des paramètres ACL au jeu de données**. Ajoutez une liste de contrôle d'accès étendue et définissez les paramètres ACL requis dans le jeu de données. Ce paramètre entraîne la définition des paramètres sur les valeurs spécifiées dans le jeu de données.
- **Appliquez des listes ACL étendues**. Appliquez les ACL pour activer toutes les listes ACL étendues nouvelles ou modifiées.

Pour ajouter un jeu de données de stratégie à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add policy dataset** <name> <type>

- **show policy dataset**

Pour lier un motif à l'ensemble de données à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **bind policy dataset** <name> <value> [-endRange <string>]
- **show policy dataset**

Pour ajouter une ACL étendue et définir les paramètres ACL sur le jeu de données à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns acl** <aclname> <aclaction> [-**srcIP** [<operator>] <srcIPVal>] [-**srcPort** [<operator>] <srcPortVal>] [-**destIP** [<operator>] <destIPVal>] [-**destPort** [<operator>] <destPortVal>] …
- **show acls**

Pour appliquer des listes ACL étendues à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **apply acls**

Exemple de configuration

Dans l'exemple de configuration suivant d'une liste de contrôle d'accès étendue basée sur un jeu de données, un jeu de données IPv4 `DATASET-IP-ACL-1` et un jeu de données de port `DATASET-PORT-ACL-2` sont créés.

Deux adresses IPv4 : 192.0.2.30 et 192.0.2.60, et deux plages d'adresses IPv4 : (198.51.100.15 - 45) et (203.0.113.60-90) sont liées à DATASET-IP-ACL-1. DATASET-IP-ACL-1 est ensuite spécifié dans les `destIP` paramètres `srcIP` et de l'ACL étendue `ACL-1`.

Deux numéros de port : 2001 et 2004, et deux plages de ports : (5001 - 5040) et (8001 - 8040) sont liés à `DATASET-PORT-ACL-2`. DATASET-PORT-ACL-2 est ensuite spécifié dans les `destPort` paramètres `srcPort` et de l'ACL étendue `ACL-1`.

```
add policy dataset DATASET-IP-ACL-1 IPV4

bind dataset DATASET-IP-ACL-1 192.0.2.30

bind dataset DATASET-IP-ACL-1 192.0.2.60

bind dataset DATASET-IP-ACL-1 198.51.100.15 -endrange 198.51.100.45

bind dataset DATASET-IP-ACL-1 203.0.113.60 -endrange 203.0.113.90

```



```
bind dataset DATASET-PORT-ACL-2 2001

bind dataset DATASET-PORT-ACL-2 2004

bind dataset DATASET-PORT-ACL-2 5001 -endrange 5040

bind dataset DATASET-PORT-ACL-2 8001 -endrange 8040


add ns acl ACL-1 ALLOW -srcIP DATASET-IP-ACL-1 -destIP DATASET-IP-ACL-1
      -srcPort DATASET-PORT-ACL-2 -destPort DATASET-PORT-ACL-2
<!--NeedCopy-->
```

Masque générique d'adresse MAC pour les ACL

August 20, 2021

Un paramètre de masque générique a été introduit pour les ACL étendues et les ACL6 et est utilisé avec le paramètre d'adresse MAC source pour définir une plage d'adresses MAC à correspondre à l'adresse MAC source des paquets entrants.

Les masques génériques spécifient quels chiffres hexadécimaux de l'adresse MAC sont utilisés et quels chiffres hexadécimaux sont ignorés. Le paramètre de masque générique spécifie une série de 1 et de zéros et a une longueur de 12 chiffres. Chaque chiffre est un masque pour le chiffre hexadécimal correspondant de l'adresse MAC. Un chiffre zéro dans le masque générique indique que le chiffre hexadécimal correspondant de l'adresse MAC doit être pris en compte et un chiffre indique que le chiffre hexadécimal correspondant doit être ignoré.

Le masque générique doit répondre aux conditions suivantes :

- A seulement une série de zéros
- A seulement une série de uns
- Commencer par une série de zéros

Voici quelques exemples de masques génériques valides :

- 000000111111
- 000000011111
- 000011111111

Voici quelques exemples de masques génériques non valides :

- 000000111100
- 111110000000

- 010101010101

Pour une ACL, un masque générique 000000111111 pour l'adresse MAC 96:fa: 95:1d:67:4 a définit la plage d'adresses MAC 96:FA:95:00:00:00 - 96:FA:95:FF:FF. Cette plage d'adresses MAC est mise en correspondance avec l'adresse MAC source des paquets entrants.

Pour spécifier une plage d'adresses MAC source dans une règle ACL à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 -  add ns acl <name> <action> -srcMac <mac_addr> -srcMacMask <string>
2 -  show ns acl <aclname>
3 <!--NeedCopy-->
```

Exemple :

```
1 add ns acl ACL-1 ALLOW  - protocol TCP  - srcport 2000-3000 -srcMac 96:fa
     :95:1d:67:4a
2   - srcMacMask 000000111111
3 Done
4 <!--NeedCopy-->
```

Pour spécifier une plage d'adresses MAC source dans une règle ACL6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 -  add ns acl6 <name> <action> -srcMac <mac_addr> -srcMacMask <string>
2 -  show ns acl6 <acl6name>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add ns acl6 ACL6-1 ALLOW -destIPv6 2001::45 -srcMac 96:fa:90:1d:67:4a
2  - srcMacMask 000000001111
3 Done
4 <!--NeedCopy-->
```

Blocage du trafic sur les ports internes

August 20, 2021

Par défaut, une appliance Citrix ADC ne bloque pas un type de trafic interne, même en utilisant des règles ACL.

Le tableau suivant répertorie les types de trafic interne qu'une appliance Citrix ADC ne bloque pas même à l'aide de règles ACL :

Configuration de Citrix ADC	Protocole	Port de destination	Adresse IP de destination
Toutes	TCP	3008–3011	NSIP ou SNIP
Toutes	TCP	179	NSIP ou SNIP
Toutes	UDP	520	NSIP ou SNIP
Haute disponibilité	UDP	3003	NSIP
Haute disponibilité	TCP	4001	NSIP
Haute disponibilité	TCP	22	NSIP
Cluster :	UDP	7000	NSIP

Cette fonctionnalité qui consiste à ne pas bloquer les types de trafic mentionnés précédemment est spécifiée par le paramètre par défaut du paramètre global Layer-3 `Implicit ACL Allow` (`implicitACLAllow`).

Vous pouvez désactiver ce paramètre si vous souhaitez bloquer les types de trafic mentionnés précédemment à l'aide des règles ACL. Une appliance dans une configuration haute disponibilité fait une exception pour son nœud partenaire (principal ou secondaire). Il ne bloque pas le trafic de ce nœud.

Pour désactiver ou activer ce paramètre à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

set l3param -IMPLICITACALLALALLOW [ENABLED	DÉSACTIVÉ]

-
- **sh l3param**

Remarque : Le paramètre implicitACLAllow est activé par défaut.

Exemple :

```
1 > set l3param -implicitACLAllow DISABLED
2 Done
3 <!--NeedCopy-->
```


Routage IP

January 21, 2021

Les appliances Citrix ADC prennent en charge le routage dynamique et statique. Étant donné que le routage simple n'est pas le rôle principal d'un Citrix ADC, l'objectif principal de l'exécution des protocoles de routage dynamique est d'activer l'injection d'intégrité de route (RHI), afin qu'un routeur en amont puisse choisir le meilleur parmi plusieurs routes vers un serveur virtuel distribué sur le plan topographique.

La plupart des implémentations de Citrix ADC utilisent certaines routes statiques pour réduire les frais de routage. Vous pouvez créer des routes statiques de sauvegarde et surveiller des routes pour activer le basculement automatique en cas de panne d'un itinéraire statique. Vous pouvez également affecter des pondérations pour faciliter l'équilibrage de charge entre les routes statiques, créer des routes nulles pour empêcher les boucles de routage et configurer des routes statiques IPv6. Vous pouvez configurer des itinéraires basés sur des stratégies (PBR), pour lesquels les décisions de routage sont basées sur des critères que vous spécifiez.

Configuration d'itinéraires dynamiques

August 20, 2021

Lorsqu'un protocole de routage dynamique est activé, le processus de routage correspondant surveille les mises à jour des itinéraires et annonce les itinéraires. Les protocoles de routage permettent à un routeur en amont d'utiliser la technique ECMP (Equal Cost Multipath) pour équilibrer le trafic vers des serveurs virtuels identiques hébergés sur deux appliances Citrix ADC autonomes. Le routage dynamique sur une appliance Citrix ADC utilise trois tables de routage. Dans une configuration haute disponibilité, les tables de routage de l'appliance secondaire reflètent celles de la solution principale.

Pour connaître les guides de référence des commandes et les commandes non prises en charge sur le protocole de routage dynamique, consultez Guides de référence des commandes du protocole de routage dynamique et commandes non prises en charge.

Le Citrix ADC prend en charge les protocoles suivants :

- Protocole d'information de routage (RIP) version 2
- Ouvrir le chemin le plus court d'abord (OSPF) version 2
- Protocole Border Gateway (BGP)
- RIPng (Routing Information Protocol) nouvelle génération pour IPv6
- Ouvrir le chemin le plus court d'abord (OSPF) version 3 pour IPv6
- Protocole ISIS

Vous pouvez activer plusieurs protocoles simultanément.

Tables de routage dans Citrix ADC

Dans une appliance Citrix ADC, la table de routage du noyau Citrix ADC, la table de routage du noyau FreeBSD et la table de routage NSM FIB contiennent chacun un ensemble différent d'itinéraires et servent un objectif différent. Ils communiquent entre eux en utilisant des sockets de routage UNIX. Les mises à jour de routage ne sont pas automatiquement propagées d'une table de routage à une autre. Vous devez configurer la propagation des mises à jour de routage pour chaque table de routage.

Table de routage du noyau NS

La table de routage du noyau NS contient des routes de sous-réseau correspondant au NSIP et à chaque SNIP et MIP. Habituellement, aucune route correspondant aux VIP n'est présente dans la table de routage du noyau NS. L'exception est un VIP ajouté à l'aide de la commande add ns ip et configuré avec un masque de sous-réseau autre que 255.255.255.255. S'il existe plusieurs adresses IP appartenant au même sous-réseau, elles sont résumées comme une seule route de sous-réseau. En outre, ce tableau contient une route vers le réseau de bouclage (127.0.0.0) et toutes les routes statiques ajoutées via l'interface de ligne de commande (CLI). Les entrées de ce tableau sont utilisées par Citrix ADC dans le transfert de paquets. À partir de l'interface de ligne de commande, ils peuvent être inspectés à l'aide de la commande show route.

Table de routage FreeBSD

Le seul but de la table de routage FreeBSD est de faciliter l'initiation et la fin du trafic de gestion (telnet, ssh, etc.). Dans une appliance Citrix ADC, ces applications sont étroitement couplées à FreeBSD, et il est impératif que FreeBSD dispose des informations nécessaires pour gérer le trafic à destination et en provenance de ces applications. Cette table de routage contient un itinéraire vers le sous-réseau NSIP et un itinéraire par défaut. En outre, FreeBSD ajoute des routes de type WasCloned(W) lorsque Citrix ADC établit des connexions aux hôtes sur les réseaux locaux. En raison de l'utilité hautement spécialisée des entrées de cette table de routage, toutes les autres mises à jour de routage du noyau NS et des tables de routage NSM FIB contournent la table de routage FreeBSD. Ne le modifiez pas avec la commande route. La table de routage FreeBSD peut être inspectée à l'aide de la commande netstat depuis n'importe quel shell UNIX.

FIB du module de services réseau (NSM)

La table de routage FIB NSM contient les itinéraires annonçables qui sont distribués par les protocoles de routage dynamique à leurs homologues du réseau. Il peut contenir :

- **Routes connectées**. Sous-réseaux IP directement accessibles à partir de Citrix ADC. Généralement, les routes correspondant au sous-réseau NSIP et aux sous-réseaux sur lesquels les protocoles de routage sont activés sont présentes dans NSM FIB en tant que routes connectées.
- **Routes du noyau**. Toutes les adresses VIP sur lesquelles l'option -hostRoute est activée sont présentes dans NSM FIB comme routes du noyau si elles satisfont aux niveaux RHI requis. En outre, NSM FIB contient toutes les routes statiques configurées sur l'interface de ligne de commande pour lesquelles l'option - annonce est activée. Sinon, si Citrix ADC fonctionne en mode Publicité d'itinéraire statique (SRADV), tous les itinéraires statiques configurés sur l'interface de ligne de commande sont présents dans NSM FIB. Ces routes statiques sont marquées comme routes du noyau dans NSM FIB, car elles appartiennent en fait à la table de routage du noyau NS.
- **Routes statiques**. Normalement, toute route statique configurée dans VTYSH est présente dans NSM FIB. Si les distances administratives des protocoles sont modifiées, ce n'est peut-être pas toujours le cas. Un point important à noter est que ces routes ne peuvent jamais entrer dans la table de routage du noyau NS.
- **Voies apprises**. Si Citrix ADC est configuré pour apprendre les routes dynamiquement, la FIB NSM contient les routes apprises par les différents protocoles de routage dynamique. Toutefois, les routes apprises par l'OSPF nécessitent un traitement spécial. Ils sont téléchargés sur FIB uniquement si l'option fib-install est activée pour le processus OSPF. Cela peut être fait à partir de la vue router-config dans VTYSH.

Routage dynamique dans une configuration haute disponibilité

Dans une configuration haute disponibilité, le nœud principal exécute le processus de routage et propage les mises à jour de table de routage vers le nœud secondaire. La table de routage du nœud secondaire reflète la table de routage sur le nœud principal.

Transfert sans arrêt

Après le basculement, le nœud secondaire prend un certain temps pour démarrer le protocole, apprendre les routes et mettre à jour sa table de routage. Mais cela n'affecte pas le routage, car la table de routage sur le nœud secondaire est identique à la table de routage sur le nœud principal. Ce mode de fonctionnement est connu sous le nom de transfert non-stop.

Mécanisme d'évitement des trous noirs

Après le basculement, le nouveau nœud principal injecte toutes ses routes VIP dans le routeur en amont. Cependant, ce routeur conserve les routes de l'ancien nœud principal pendant 180 secondes. Comme le routeur n'est pas au courant du basculement, il tente d'équilibrer la charge du trafic entre

les deux nœuds. Pendant les 180 secondes précédant l'expiration des anciennes routes, le routeur envoie la moitié du trafic à l'ancien nœud principal inactif, ce qui est, en fait, un trou noir.

Pour éviter cela, le nouveau nœud principal, lors de l'injection d'un itinéraire, lui attribue une mesure légèrement inférieure à celle spécifiée par l'ancien nœud principal.

Interfaces pour configurer le routage dynamique

Pour configurer le routage dynamique, vous pouvez utiliser l'interface graphique ou une interface de ligne de commande. Citrix ADC prend en charge deux interfaces de ligne de commande indépendantes : l'interface de ligne de commande et l'environnement de ligne de commande virtuel (VTYSH). L'interface de ligne de commande est le shell natif de l'appliance. VTYSH est exposé par ZebOS. La suite de routage Citrix ADC est basée sur ZebOSS, la version commerciale de GNU Zebra.

> **Remarque :**
>
> Citrix recommande d'utiliser VTYSH pour toutes les commandes, sauf celles qui peuvent être configurées uniquement sur l'interface de ligne de commande. L'utilisation de l'interface de ligne de commande doit généralement se limiter aux commandes permettant d'activer les protocoles de routage, de configurer la publicité d'itinéraire hôte et d'ajouter des routes statiques pour le transfert de paquets.

Guides de référence des commandes du protocole de routage dynamique et commandes non prises en charge

Le tableau suivant répertorie les liens du guide de référence des commandes, pour divers protocoles de routage dynamique et les commandes non prises en charge sur l'appliance Citrix ADC : guides de référence du protocole de routage dynamique et commandes non prises en charge.

Configuration de RIP

August 20, 2021

Le protocole RIP (Routing Information Protocol) est un protocole de vecteur de distance. Le Citrix ADC prend en charge RIP tel que défini dans RFC 1058 et RFC 2453. RIP peut s'exécuter sur n'importe quel sous-réseau.

Après avoir activé RIP, vous devez configurer la publicité des itinéraires RIP. Pour le dépannage, vous pouvez limiter la propagation RIP. Vous pouvez afficher les paramètres RIP pour vérifier la configuration.

Activation et désactivation de RIP

Utilisez l'une des procédures suivantes pour activer ou désactiver RIP. Après avoir activé RIP, l'appliance Citrix ADC démarre le processus RIP. Une fois que vous avez désactivé RIP, l'appliance arrête le processus RIP.

Pour activer ou désactiver le routage RIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, entrez l'une des commandes suivantes pour activer ou désactiver RIP :

- **enable ns feature RIP**
- **disable ns feature RIP**

Pour activer ou désactiver le routage RIP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, dans le groupe **Modes et fonctionnalités**, cliquez sur **Modifier les fonctionnalités avancées**.
2. Sélectionnez ou désactivez l'option **RIP Routage** .

Itinéraires publicitaires

RIP permet à un routeur en amont d'équilibrer le trafic entre deux serveurs virtuels identiques hébergés sur deux appliances Citrix ADC autonomes. L'annonce d'itinéraire permet à un routeur en amont de suivre les entités réseau situées derrière Citrix ADC.

Pour configurer RIP pour annoncer des itinéraires à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router rip	Démarrez le processus de routage RIP et entrez en mode de configuration pour le processus de routage.
redistribute static	Redistribute static routes.
redistribute kernel	Redistribute kernel routes.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router rip
```



```
4 NS(config-router)# redistribute static
5 NS(config-router)# redistribute kernel
6 <!--NeedCopy-->
```

Limitation des propagations RIP

Si vous avez besoin de dépanner votre configuration, vous pouvez configurer le mode d'écoute uniquement sur n'importe quelle interface donnée.

Pour limiter la propagation RIP à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router rip	Démarrez le processus de routage RIP et entrez en mode de configuration pour le processus de routage.
passive-interface < vlan_name>	Supprimez les mises à jour de routage sur les interfaces liées au VLAN spécifié.

Exemple :

```
1 >VTYSH
2 NS# configure terminal
3 NS(config)# router rip
4 NS(config-router)# passive-interface VLAN0
5 <!--NeedCopy-->
```

Vérification de la configuration RIP

Vous pouvez afficher la table de routage et d'autres paramètres RIP.

Pour afficher les paramètres RIP à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes dans l'ordre suivant :

Commande	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
sh rip	Afficher la table de routage RIP mise à jour.
sh rip interface <vlan_name>	Affiche les informations RIP pour le VLAN spécifié.

Exemple :

```
NS# VTYSH
NS# sh rip
NS# sh rip interface VLAN0
<!--NeedCopy-->
```

Configuration d'OSPF

August 20, 2021

Le Citrix ADC prend en charge Open Shortest Path First (OSPF) version 2 (RFC 2328). Les fonctionnalités d'OSPF sur Citrix ADC sont les suivantes :

- Si un vserver est actif, l'hôte route vers le vserver peut être injecté dans les protocoles de routage.
- OSPF peut s'exécuter sur n'importe quel sous-réseau.
- L'apprentissage d'itinéraire annoncé par les routeurs OSPF voisins peut être désactivé sur le Citrix ADC.
- Citrix ADC peut annoncer des mesures externes Type-1 ou Type2 pour toutes les routes.
- Citrix ADC peut annoncer les paramètres de mesure spécifiés par l'utilisateur pour les itinéraires VIP. Par exemple, vous pouvez configurer une mesure par VIP sans cartes d'itinéraires spéciales.
- Vous pouvez spécifier l'ID de zone OSPF pour Citrix ADC.
- Le Citrix ADC prend en charge les zones NSSA (not-so-stubby-areas). Un NSSA est similaire à une zone de talon OSPF, mais permet l'injection de voies externes de manière limitée dans la zone de talon. Pour prendre en charge les NSSA, un nouveau bit d'option (le bit N) et un nouveau type (Type 7) de zone LSA (Link State Advertisement) ont été définis. Les LSA de type 7 prennent en charge les informations d'itinéraire externes au sein d'une NSSA. Un routeur de bordure de zone NSSA (ABR) traduit un LSA de type 7 en un LSA de type 5 qui est propagé dans le domaine OSPF. La spécification OSPF définit uniquement les classes générales suivantes de configuration de surface :

- Type 5 LSA : Originaire de routeurs internes à la zone sont inondés dans le domaine par AS routeurs bordeurs (ASBRS).
- Stub : ne permet pas de propager les LSA de type 5 dans/dans toute la zone et dépend plutôt du routage par défaut vers des destinations externes.

Après avoir activé OSPF, vous devez configurer la publicité des itinéraires OSPF. Pour le dépannage, vous pouvez limiter la propagation OSPF. Vous pouvez afficher les paramètres OSPF pour vérifier la configuration.

Activation et désactivation d'OSPF

Pour activer ou désactiver OSPF, vous devez utiliser l'interface de ligne de commande ou l'interface graphique. Lorsque OSPF est activé, le Citrix ADC démarre le processus OSPF. Lorsque OSPF est désactivé, le Citrix ADC arrête le processus de routage OSPF.

Pour activer ou désactiver le routage OSPF à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

1. **activer la fonction ns OSPF**
2. **désactiver la fonctionnalité ns OSPF**

Pour activer ou désactiver le routage OSPF à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, dans le groupe **Modes et fonctionnalités**, cliquez sur **Modifier les fonctionnalités avancées**.
2. Sélectionnez ou désactivez l'option **Routage OSPF** .

Publicité Itinéraires OSPF

OSPF permet à un routeur en amont d'équilibrer le trafic entre deux serveurs virtuels identiques hébergés sur deux appliances Citrix ADC autonomes. La publication d'itinéraire permet à un routeur en amont de suivre les entités réseau situées derrière Citrix ADC.

Pour configurer OSPF pour annoncer des routes à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
configure terminal	Entre en mode de configuration globale.
router OSPF	Démarrez le processus de routage OSPF et entrez en mode de configuration pour le processus de routage.

Commande	Spécifie
network A.B.C.D/M area <0-4294967295>	Activer le routage sur un réseau IP.
redistribute static	Redistribute static routes.
redistribute kernel	Redistribute kernel routes.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router OSPF
NS(config-router)# network 10.102.29.0/24 area 0
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Limitation des propagations OSPF

Si vous avez besoin de dépanner votre configuration, vous pouvez configurer le mode d'écoute uniquement sur n'importe quel VLAN donné.

Pour limiter la propagation OSPF à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router OSPF	Démarrez le processus de routage OSPF et passe en mode de configuration pour le processus de routage.
passive-interface < vlan_name>	Supprimez les mises à jour de routage sur les interfaces liées au VLAN spécifié.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router OSPF
```



```
4 NS(config-router)# passive-interface VLAN0
5 <!--NeedCopy-->
```

Vérification de la configuration OSPF

Vous pouvez afficher les voisins OSPF actuels et les itinéraires OSPF.

Pour afficher les paramètres OSPF à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
sh OSPF neighbor	Affiche les voisins actuels.
sh OSPF route	Affiche les itinéraires OSPF.

Exemple :

```
1 >VTYSH
2 NS# sh ip OSPF neighbor
3 NS# sh ip OSPF route
4 <!--NeedCopy-->
```

Configuration du redémarrage Graceful pour OSPF

Dans une configuration de haute disponibilité (HA) non INC dans laquelle un protocole de routage est configuré, après un basculement, les protocoles de routage sont convergés et les routes entre le nouveau nœud principal et les routeurs voisins adjacents sont apprises. L'apprentissage de chemin prend un certain temps à compléter. Pendant ce temps, le transfert des paquets est retardé, les performances du réseau peuvent être perturbées et les paquets peuvent être abandonnés.

Le redémarrage gracieux permet à une configuration HA lors d'un basculement de demander à ses routeurs adjacents de ne pas supprimer les routes apprises de l'ancien nœud principal de leurs bases de données de routage. En utilisant les informations de routage de l'ancien nœud principal, le nouveau nœud principal et les routeurs adjacents commencent immédiatement à transférer les paquets, sans perturber les performances du réseau.

Pour configurer le redémarrage gracieux pour OSPF à l'aide de la ligne de commande VTYSH, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
VTYSH	VTYSH	Entre l'invite de commande VTYSH.
configure terminal	NS# configure terminal	Entre en mode de configuration globale.
router-id <id>	NS(config)# router-id 1.1.1.1	Définit un identificateur de routeur pour l'appliance Citrix ADC. Cet identificateur est défini pour tous les protocoles de routage dynamique. Le même ID doit être spécifié dans l'autre nœud dans une haute disponibilité configurée pour un redémarrage gracieux pour fonctionner correctement dans la configuration HA.
ospf restart grace-period <1-1800>	NS(config)# ospf restart grace-period 170	Spécifie le délai de grâce, en secondes, pour lequel les routes doivent être conservées dans les périphériques d'assistance. Valeur par défaut : 120 secondes.

Commande	Exemple	Description de la commande
ospf restart helper max-grace-period <1-1800>	NS(config)# ospf restart helper max-grace-period 180	Cette commande est facultative pour limiter la période de grâce maximale pour laquelle l'appliance Citrix ADC sera en mode d'assistance. Si l'appliance Citrix ADC reçoit un LSA opaque avec une période de grâce supérieure à la période d'aide max-grace-period définie, le LSA est ignoré et le Citrix ADC n'est pas placé en mode d'assistance.
router ospf	NS(config)# router ospf	Démarre le processus de routage OSPF et entrez en mode de configuration pour le processus de routage.
network A.B.C.D/M area <0-4294967295>	NS(config-router)# network 192.0.2.0/24 area 0	Active le routage sur un réseau IP.
capability restart graceful	NS(config-router)# capability restart graceful	Active le redémarrage gracieux sur le processus de routage OSPF.
redistribute kernel	NS(config-router)# redistribute kernel	Redistribue les routes du noyau.

Configuration de BGP

August 20, 2021

L'appliance Citrix ADC prend en charge BGP (RFC 4271). Les fonctionnalités de BGP sur Citrix ADC sont les suivantes :

- Le Citrix ADC annonce des routes vers des homologues BGP.
- Le Citrix ADC injecte des routes hôtes vers des adresses IP virtuelles (VIP), déterminées par l'intégrité des serveurs virtuels sous-jacents.

- Le Citrix ADC génère des fichiers de configuration pour exécuter BGP sur le nœud secondaire après un basculement dans une configuration HA.
- Ce protocole prend en charge les échanges de routage IPv6.
- Prise en charge en cas de remplacement dans le protocole de passerelle frontière (BGP)

Après avoir activé BGP, vous devez configurer la publicité des itinéraires BGP. Pour le dépannage, vous pouvez limiter la propagation BGP. Vous pouvez afficher les paramètres BGP pour vérifier la configuration.

Conditions préalables pour IPv6 BGP

Avant de commencer à configurer IPv6 BGP, procédez comme suit :

- Assurez-vous que vous comprenez le protocole IPv6 BGP.
- Activez la fonctionnalité IPv6.

Activation et désactivation de BGP

Pour activer ou désactiver BGP, vous devez utiliser l'interface de ligne de commande ou l'interface graphique. Lorsque BGP est activé, l'appliance Citrix ADC démarre le processus BGP. Lorsque BGP est désactivé, l'appliance arrête le processus BGP.

Pour activer ou désactiver le routage BGP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- activer la fonction ns BGP
- désactiver la fonctionnalité ns BGP

Pour activer ou désactiver le routage BGP à l'aide de l'interface graphique :

1. Accédez à Système > Paramètres, dans le groupe Modes et fonctionnalités, cliquez sur Modifier les fonctionnalités avancées.
2. Sélectionnez ou désactivez l'option Routage BGP.

Publicité IPv4 Itinéraires

Vous pouvez configurer l'appliance Citrix ADC pour annoncer les routes hôtes vers les VIP et annoncer les routes vers les réseaux en aval.

Pour configurer BGP pour annoncer les routes IPv4 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire. Valeurs possibles : 1 à 4 294 967 295.
Voisin < IPv4 address> à distance comme < as-number>	Mettez à jour la table des voisins IPv4 BGP avec l'adresse IPv4 locale du voisin dans le système autonome spécifié.
Famille d'adresses ipv4	Entrez le mode de configuration de la famille d'adresses.
Voisin < IPv4 address> activé	Préfixes d'échange pour la famille de routeurs IPv4 entre l'homologue et le nœud local à l'aide de l'adresse locale du lien.
redistribute kernel	Redistribute kernel routes.
redistribute static	Redistribute static routes.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor 10.102.29.170 remote-as 100
NS(config-router)# Address-family ipv4
NS(config-router-af)# Neighbor 10.102.29.170 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
<!--NeedCopy-->
```

Conditions préalables pour IPv6 BGP

Avant de commencer à configurer IPv6 BGP, procédez comme suit :

- Assurez-vous que vous comprenez le protocole IPv6 BGP.
- Activez la fonctionnalité IPv6.

Publicité IPv6 BGP Itinéraires

Border Gateway Protocol (BGP) permet à un routeur en amont d'équilibrer le trafic entre deux serveurs virtuels identiques hébergés sur deux appliances Citrix ADC autonomes. La publication d'itinéraire permet à un routeur en amont de suivre les entités réseau situées derrière Citrix ADC.

Pour configurer BGP pour annoncer des routes IPv6 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire. Valeurs possibles : 1 à 4 294 967 295.
Voisin < IPv6 address> à distance comme < as-number>	Mettez à jour la table des voisins IPv6 BGP avec l'adresse IPv6 locale du voisin dans le système autonome spécifié.
Famille d'adresses ipv6	Entrez le mode de configuration de la famille d'adresses.
Voisin < IPv6 address> activer	Préfixes d'échange pour la famille de routeurs IPv6 entre l'homologue et le nœud local à l'aide de l'adresse locale du lien.
redistribute kernel	Redistribute kernel routes.
redistribute static	Redistribute static routes.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor a1bc::102 remote-as 100
NS(config-router)# Address-family ipv6
NS(config-router-af)# Neighbor a1bc::102 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
<!--NeedCopy-->
```


Vérification de la configuration BGP

Vous pouvez utiliser VTYSH pour afficher les paramètres BGP.

Pour afficher les paramètres BGP à l'aide de la ligne de commande VTYSH

À l'invite de commandes, tapez :

```
VTYSH
You are now in the VTYSH command prompt. An output similar to the
   following appears:
NS170#
At the VTYSH command prompt, type:
NS170# sh ip BGP
NS170# sh BGP
NS170# sh ip BGP neighbors
NS170# sh ip BGP summary
NS170# sh ip BGP route-map <map-tag>
<!--NeedCopy-->
```

Prise en charge en cas de remplacement dans le protocole de passerelle frontière (BGP)

Dans le cadre de la fonctionnalité de prévention des boucles BGP, si un routeur reçoit un paquet BGP contenant le numéro de système autonome (ASN) du routeur dans le chemin d'accès des systèmes autonomes (AS), le routeur abandonne le paquet. L'hypothèse est que le paquet provient du routeur et a atteint l'endroit d'où il provient.

Si une entreprise possède plusieurs sites avec un même ASN, la prévention des boucles BGP empêche les sites avec un ASN identique d'être liés par un autre ASN. Les mises à jour de routage (paquets BGP) sont supprimées lorsqu'un autre site les reçoit.

Pour résoudre ce problème, la fonctionnalité BGP AS-Override a été ajoutée au module de routage ZebOSS BGP du Citrix ADC.

Lorsque l'AS-Override est activé pour un périphérique homologue, lorsque l'appliance Citrix ADC reçoit un paquet BGP pour le transfert à l'homologue et que l'ASN du paquet correspond à celui de l'homologue, l'appliance remplace l'ASN du paquet BGP par son propre numéro ASN avant de transférer le paquet.

Vous pouvez activer AS-Override pour un voisin spécifique ou un groupe de voisins (groupe homologue) à l'aide de la ligne de commande VTYSH.

Pour configurer BGP AS-Override pour un voisin IPv4 à l'aide de la ligne de commande VTYSH :

Commande	Spécifie
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire.
Voisin < IPv4 address> à distance comme < as-number>	Mettez à jour la table des voisins IPv4 BGP avec l'adresse IPv4 du voisin dans le système autonome spécifié.
Voisin <IPv4 address> en remplacement	Activez BGP en tant que remplacement pour le voisin spécifié.

```
1      > VTYSH NS# configure terminal
2      NS(config)# router BGP 200
3      NS(config-router)# Neighbor 192.0.2.100 remote-as 100
4      NS(config-router)# Neighbor 10.102.29.100 as-override
5  <!--NeedCopy-->
```

Pour configurer BGP AS-Override pour un groupe d'homologues BGP IPv4 à l'aide de la ligne de commande VTYSH :

Commande	Spécifie
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire.
Neighbor <peer group name> **peer-group**	Créez un groupe de pairs BGP.
<IPv4 address> **Groupe de pairs** <peer group name>**Neighbot**	Associez des voisins au groupe d'homologues spécifié.
Neighbor <peer group name> remote-as < as-number>	Mettez à jour la table des voisins IPv4 BGP avec l'adresse IPv4 du voisin dans le système autonome spécifié.
Neighbor <peer group name> as-override	Activez BGP en tant que remplacement pour tous les voisins associés au groupe d'homologues spécifié.

```
1      > VTYSH NS# configure terminal
2      NS(config)# router BGP 200
```



```
3     NS(config-router)# neighbor external-peers-1 peer-group
4     NS(config-router)# neighbor 192.0.2.101 peer-group external-peers-1
5     NS(config-router)# neighbor 192.0.2.102 peer-group external-peers-1
6     NS(config-router)# neighbor 192.0.2.103 peer-group external-peers-1
7     NS(config-router)# Neighbor external-peers-1 remote-as 100
8     NS(config-router)# Neighbor external-peers-1 as-override
9  <!--NeedCopy-->
```

Pour configurer BGP AS-Override pour un voisin IPv6 à l'aide de la ligne de commande VTYSH :

Commande	Spécifie
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire.
Voisin < IPv6 address> à distance comme < as-number>	Mettez à jour la table des voisins IPv4 BGP avec l'adresse IPv4 du voisin dans le système autonome spécifié.
Neighbor <IPv6 address> as-override	Activez BGP en tant que remplacement pour le voisin spécifié.
Famille d'adresses ipv6	Entrez le mode de configuration de la famille d'adresses.
Voisin < IPv6 address> activer	Préfixes Exchange pour la famille de routeurs IPv6 entre le voisin spécifié et Citrix ADC à l'aide de l'adresse locale du lien.
Neighbor <IPv6 address> as-override	Activez BGP en tant que remplacement pour le voisin spécifié.

```
1     > VTYSH NS# configure terminal
2     NS(config)# router BGP 200
3     NS(config-router)# Neighbor a1bc::102 remote-as 100
4     NS(config-router)# Neighbor a1bc::102 as-override
5     NS(config-router)# Address-family ipv6
6     NS(config-router-af)# Neighbor a1bc::102 activate
7     NS(config-router)# Neighbor a1bc::102 as-override
8  <!--NeedCopy-->
```

Pour configurer BGP AS-Override for IPv6 peer group à l'aide de la ligne de commande VTYSH :

Commande	Spécifie
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire.
Neighbor <peer group name> **peer-group**	Créez un groupe de pairs BGP.
<IPv6 address> **Groupe de pairsvoisin** <peer group name>	Associer un voisin au groupe d'homologues spécifié.
Neighbor <peer group name> remote-as < as-number>	Mettez à jour la table des voisins IPv4 BGP avec l'adresse IPv4 du voisin dans le système autonome spécifié.
Neighbor <peer group name> as-override	Activez BGP en tant que remplacement pour tous les voisins associés au groupe d'homologues spécifié.
Famille d'adresses ipv6	Entrez le mode de configuration de la famille d'adresses.
Voisin <peer group name> activé	Échangez les préfixes de la famille de routeurs IPv6 entre les voisins du groupe d'homologues spécifié et Citrix ADC à l'aide de l'adresse locale du lien.
Neighbor <peer group name> as-override	Activez BGP en tant que remplacement pour tous les voisins associés au groupe d'homologues spécifié.

```
1      > VTYSH NS# configure terminal
2      NS(config)# router BGP 200
3      NS(config-router)# neighbor external-peers-2 peer-group
4      NS(config-router)# neighbor 2001::1 peer-group external-peers-2
5      NS(config-router)# neighbor 2001::2 peer-group external-peers-2
6      NS(config-router)# Neighbor external-peers-2 remote-as 100
7      NS(config-router)# Neighbor external-peers-2 as-override
8      NS(config-router)# Address-family ipv6
9      NS(config-router-af)# Neighbor external-peers-2 activate
10     NS(config-router)# Neighbor external-peers-2 as-override
11 <!--NeedCopy-->
```


Redémarrage gracieux

Dans une configuration de haute disponibilité (HA) non INC dans laquelle un protocole de routage est configuré, après un basculement, les protocoles de routage sont convergés et les routes entre le nouveau nœud principal et les routeurs voisins adjacents sont apprises. L'apprentissage de chemin prend un certain temps à compléter. Pendant ce temps, le transfert des paquets est retardé, les performances du réseau peuvent être perturbées et les paquets peuvent être abandonnés.

Le redémarrage gracieux permet à une configuration HA lors d'un basculement de demander à ses routeurs adjacents de ne pas supprimer les routes apprises de l'ancien nœud principal de leurs bases de données de routage. En utilisant les informations de routage de l'ancien nœud principal, le nouveau nœud principal et les routeurs adjacents commencent immédiatement à transférer les paquets, sans perturber les performances du réseau.

Configuration du redémarrage Graceful pour BGP

Pour configurer le redémarrage gracieux pour BGP à l'aide de la ligne de commande VTYSH, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
VTYSH	VTYSH	Entre l'invite de commande VTYSH.
configure terminal	NS# configure terminal	Entre en mode de configuration globale.
router-id <ID>	NS(config)# router-id 1.1.1.1	Identifiant de routeur pour l'appliance Citrix ADC. Cet identificateur est défini pour tous les protocoles de routage dynamique. Le même identifiant doit être spécifié sur l'autre nœud dans une configuration haute disponibilité pour que le redémarrage gracieux fonctionne correctement.
router bgp <AS-number>	NS(config)# router bgp 5	Pénètre en mode de configuration BGP.
bgp graceful-restart	NS(config)# bgp graceful-restart	Active le redémarrage gracieux sur le processus de routage BGP.

Commande	Exemple	Description de la commande
bgp graceful-restart restart-time <1-1800>	NS(config-router)# bgp graceful-restart restart-time 170	Spécifie le délai de grâce, en secondes, pendant lequel les routeurs d'assistance attendent une connexion TCP à partir du nouveau nœud principal après un basculement. Pendant ce temps, les routeurs d'assistance conservent les itinéraires.
bgp graceful-restart stalepath-time <1-1800>	NS(config-router)# bgp graceful-restart stalepath-time 180	Spécifie la durée, en secondes, pendant laquelle l'appliance Citrix ADC en mode assistance conserve les itinéraires périmés pour le redémarrage des routeurs voisins. La valeur par défaut est 360 secondes.
neighbor <IPv4 address of the peer router> remote-as <AS-number>	NS(config-router)# neighbor 192.0.2.30 remote-as 2	Établit l'appairage BGP avec le périphérique de routeur voisin spécifié.
<IPv4 address of the peer router>fonctionnalité voisine gracieuse-redémarrage	NS(config-router)# neighbor 192.0.2.30 capability graceful-restart	Active le redémarrage gracieux avec le voisin spécifié.
redistribute kernel	NS(config-router)# redistribute kernel	Redistribue les routes du noyau.

Configuration du redémarrage Graceful pour IPv6 BGP

Dans une configuration de haute disponibilité (HA) non INC dans laquelle un protocole de routage est configuré, après un basculement, les protocoles de routage sont convergés et les routes entre le nouveau nœud principal et les routeurs voisins adjacents sont apprises. L'apprentissage de chemin prend un certain temps à compléter. Pendant ce temps, le transfert des paquets est retardé, les performances du réseau peuvent être perturbées et les paquets peuvent être abandonnés.

Le redémarrage gracieux permet à une configuration HA lors d'un basculement de demander à ses routeurs adjacents de ne pas supprimer les routes apprises de l'ancien nœud principal de leurs bases

de données de routage. En utilisant les informations de routage de l'ancien nœud principal, le nouveau nœud principal et les routeurs adjacents commencent immédiatement à transférer les paquets, sans perturber les performances du réseau.

Pour configurer le redémarrage gracieux pour IPv6 BGP à l'aide de la ligne de commande VTYSH, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
VTYSH	VTYSH	Entre l'invite de commande VTYSH.
configure terminal	NS# configure terminal	Entre en mode de configuration globale.
router-id <id>	NS(config)# router-id 1.1.1.1	Définit un identificateur de routeur pour l'appliance Citrix ADC. Cet identificateur est défini pour tous les protocoles de routage dynamique. Le même ID doit être spécifié dans l'autre nœud dans une configuration haute disponibilité pour que le redémarrage gracieux fonctionne correctement.
router bgp <AS-number>	NS(config)# router bgp 5	Pénètre en mode de configuration pour le protocole BGP.
bgp graceful-restart	NS(config)# bgp graceful-restart	Active le redémarrage gracieux sur le processus de routage BGP.

Commande	Exemple	Description de la commande
bgp graceful-restart restart-time <1-1800>	NS(config-router)# bgp graceful-restart restart-time 170	Spécifie le délai de grâce, en secondes, pendant lequel les routeurs d'assistance attendent une connexion TCP à partir du nouveau nœud principal après un basculement. Pendant ce temps, les routeurs d'assistance conservent les itinéraires. La valeur par défaut est 360 secondes.
bgp graceful-restart stalepath-time <1-1800>	NS(config-router)# bgp graceful-restart stalepath-time 180	Spécifie la durée, en secondes, pendant laquelle l'appliance Citrix ADC en mode assistance conserve les itinéraires périmés pour le redémarrage des routeurs voisins. La valeur par défaut est 360 secondes.
<AS-number>voisin <IPv6 address> distant en tant que	NS (config-router) # voisin 2001:db8 : :10 distant en tant que 2	Établit l'appairage BGP avec le périphérique de routeur voisin spécifié.
address-family ipv6	NS(config-router)#address-family ipv6	Pénètre le mode de configuration de la famille d'adresses.
neighbor <IPv6 address of the neighbor> activate	NS(config-router-af)#neighbor 2001:db8::10 activate	Active l'échange d'itinéraires de famille d'adresses avec le périphérique de routeur voisin spécifié.
neighbor <IPv6 address of the neighbor> capability graceful-restart	NS(config-router-af)#neighbor 2001:db8::10 capability graceful-restart	Active le redémarrage gracieux avec le périphérique de routeur voisin spécifié.
redistribute kernel	NS(config-router-af)#redistribute kernel	Redistribue les routes du noyau.

Commande	Exemple	Description de la commande
famille d'adresses de sortie	NS (config-router-af) #exit -address-family	Quitte le mode de configuration de la famille d'adresses.

Configuration de l'authentification MD5 pour IPv4 BGP

L'appliance Citrix ADC prend en charge l'authentification MD5 pour Border Gateway Protocol (BGP). Lorsque l'authentification est activée, tout segment TCP appartenant à BGP échangé entre l'appliance Citrix ADC et son périphérique homologue est vérifié et accepté uniquement si l'authentification est réussie. Pour que l'authentification soit réussie, les deux homologues doivent être configurés avec le même mot de passe MD5. Si l'authentification échoue, la relation de voisin BGP n'est pas en cours d'établissement. La prise en charge de l'authentification MD5 pour BGP dans l'appliance Citrix ADC est conforme à la RFC 2385.

Avant de commencer

Avant de commencer à configurer l'authentification BGP MD5, tenez compte des points suivants :

- Assurez-vous que vous comprenez les différents composants de l'authentification BGP MD5, décrits dans la RFC 2385.
- L'authentification BGP MD5 n'est pas prise en charge pour les partitions d'administration Citrix ADC.
- L'authentification BGP MD5 n'est pas prise en charge pour les configurations BGP IPv6.
- L'authentification BGP MD5 est prise en charge pour les configurations de cluster Citrix ADC ainsi que pour les configurations de haute disponibilité.
- En raison du problème suivant dans FreeBSD, Citrix recommande de définir des valeurs de maintien et de maintien faibles (par exemple, 5 et 15) et de configurer un redémarrage gracieux pour une session BGP dans une configuration haute disponibilité de couche 2. Sinon, si l'authentification MD5 est activée, BGP peut prendre plus de temps pour rétablir une connexion avec le voisin après un basculement.
  - Le dernier ACK de FreeBSD ne contient pas md5 digest :
    - https://forums.freebsd.org/threads/11170/
    - http://support.pfsense.narkive.com/povrH5HI/bgp-md5-weird-behavior-when-connection-closes

Configuration de l'authentification MD5 pour IPv4 BGP

Pour configurer l'authentification MD5 pour IPv4 BGP à l'aide de la ligne de commande VTYSH, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
vtych	Affiche l'invite de commande VTYSH.
configure terminal	Entre en mode de configuration globale.
router bgp <AS-number>	Pénètre en mode de configuration pour le protocole BGP. <AS-number>est un numéro de système autonome BGP et est un paramètre obligatoire.
< AS-number >voisin <neighbour IPv4 address> distant en tant que	Met à jour la table BGP IPv4 avec l'adresse IPv4 du voisin dans le système autonome spécifié.
< password in double quotes>mot de< neighbour IPv4 address > passe voisin	Configure l'authentification MD5 pour le voisin spécifié avec le mot de passe MD5 spécifié. Pour que l'authentification MD5 réussisse, vous devez configurer le même mot de passe MD5 sur l'appliance Citrix ADC et l'appliance voisine.

```
1  > vtysh
2
3  ns# configure terminal
4
5  ns(config)#router bgp 5
6
7  ns(config-router)#neighbor 20.20.20.138 remote-as 1
8
9  ns(config-router)#neighbor 20.20.20.138 password  “secret”
10
11 ns(config-router)#redistribute kernel
12
13 ns(config-router)#exit
14
15 <!--NeedCopy-->
```


Configuration du RIP IPv6

August 20, 2021

IPv6 Routing Information Protocol (RIP) ou Ripng est un protocole Distance Vector. Ce protocole est une extension de RIP pour prendre en charge IPv6. Après avoir activé IPv6 RIP, vous devez configurer la publicité des itinéraires RIP IPv6. Pour le dépannage, vous pouvez limiter la propagation RIP IPv6. Vous pouvez afficher les paramètres RIP IPv6 pour vérifier la configuration.

Conditions préalables pour IPv6 RIP

Avant de commencer à configurer IPv6 RIP, procédez comme suit :

- Assurez-vous de bien comprendre le protocole RIP IPv6.
- Installez la licence IPv6pt sur l'appliance Citrix ADC.
- Activez la fonctionnalité IPv6.

Publicité IPv6 RIP Routes

IPv6 RIP permet à un routeur en amont d'équilibrer le trafic entre deux serveurs virtuels identiques hébergés sur deux périphériques autonomes Citrix ADC. L'annonce d'itinéraire permet à un routeur en amont de suivre les entités réseau situées derrière Citrix ADC.

Pour configurer IPv6 RIP pour annoncer les routes IPv6 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router ipv6 rip	Démarrez le processus de routage RIP IPv6 et entrez en mode de configuration pour le processus de routage.
redistribute static	Redistribute static routes.
redistribute kernel	Redistribute kernel routes.

Exemple :

```
>VTYSH
NS# configure terminal
```



```
3 NS(config)# router ipv6 rip
4 NS(config-router)# redistribute static
5 NS(config-router)# redistribute kernel
6 <!--NeedCopy-->
```

Limitation des propagations RIP IPv6

Si vous avez besoin de dépanner votre configuration, vous pouvez configurer le mode d'écoute uniquement sur n'importe quelle interface donnée.

Pour limiter la propagation IPv6 RIP à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router ipv6 rip	Démarrez le processus de routage RIP IPv6 et entrez en mode de configuration pour le processus de routage.
passive-interface < vlan_name>	Supprimez les mises à jour de routage sur les interfaces liées au VLAN spécifié.

Exemple :

```
1 >VTYSH
2 NS# configure terminal
3 NS(config)# router ipv6 rip
4 NS(config-router)# passive-interface VLAN0
5 <!--NeedCopy-->
```

Vérification de la configuration RIP IPv6

Vous pouvez utiliser VTYSH pour afficher la table de routage RIP IPv6 et les informations RIP IPv6 pour un VLAN spécifié.

Pour afficher les paramètres RIP IPv6 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commandes	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
sh ipv6 rip	Afficher la table de routage IPv6 RIP mise à jour.
sh ipv6 rip interface <vlan_name>	Afficher les informations RIP IPv6 pour le VLAN spécifié.

Exemple :

```
NS# VTYSH
NS# sh ipv6 rip
NS# sh ipv6 rip interface VLAN0
<!--NeedCopy-->
```

Configuration d'IPv6 OSPF

August 20, 2021

IPv6 OSPF ou OSPF version 3 (OSPF v3) est un protocole d'état de liaison qui est utilisé pour échanger des informations de routage IPv6. Après avoir activé IPv6 OSPF, vous devez configurer la publicité des routes IPv6 OSPF. Pour le dépannage, vous pouvez limiter la propagation IPv6 OSPF. Vous pouvez afficher les paramètres IPv6 OSPF pour vérifier la configuration.

Conditions préalables pour IPv6 OSPF

Avant de commencer à configurer IPv6 OSPF, procédez comme suit :

- Assurez-vous de bien comprendre le protocole IPv6 OSPF.
- Installez la licence IPv6pt sur l'appliance Citrix ADC.
- Activez la fonctionnalité IPv6.

Publicité Itinéraires IPv6

IPv6 OSPF permet à un routeur en amont d'équilibrer le trafic entre deux serveurs virtuels identiques hébergés sur deux périphériques autonomes Citrix ADC. La publication d'itinéraire permet à un routeur en amont de suivre les entités réseau situées derrière Citrix ADC.

Pour configurer IPv6 OSPF pour annoncer les routes IPv6 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commandes	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router ipv6 OSPF	Démarrez le processus de routage IPv6 OSPF et entrez en mode de configuration pour le processus de routage.
redistribute static	Redistribute static routes.
redistribute kernel	Redistribute kernel routes.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Limitation des propagations IPv6 OSPF

Si vous avez besoin de dépanner votre configuration, vous utilisez VTYSH pour configurer le mode d'écoute uniquement sur un VLAN donné.

Pour limiter la propagation IPv6 OSPF à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commandes	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router ipv6 OSPF	Démarrez le processus de routage IPv6 OSPF et entrez en mode de configuration pour le processus de routage.
passive-interface < vlan_name >	Supprimez les mises à jour de routage sur les interfaces liées au VLAN spécifié.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Vérification de la configuration IPv6 OSPF

Vous utilisez VTYSH pour afficher les voisins actuels IPv6 OSPF et les routes IPv6 OSPF.

Pour afficher les paramètres IPv6 OSPF à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
voisin OSPF sh ipv6	Afficher les voisins actuels.
route sh ipv6 OSPF	Afficher les itinéraires IPv6 OSPF.

Exemple :

```
>VTYSH
NS# sh ipv6 OSPF neighbor
NS# sh ipv6 OSPF route
<!--NeedCopy-->
```

Authentification OSPFv3

Pour garantir l'intégrité, l'authentification d'origine des données et la confidentialité des données des paquets OSPFv3, l'authentification OSPFv3 doit être configurée sur les homologues OSPFv3.

L'appliance Citrix ADC prend en charge l'authentification OSPFv3 et est partiellement conforme à la RFC 4552. L'authentification OSPFv3 est basée sur les deux protocoles IPsec : Authentication Header (AH) et Encapsulating Security Payload (ESP). L'appliance Citrix ADC prend en charge uniquement le protocole AH pour l'authentification OSPFv3.

L'authentification OSPFv3 utilise des associations de sécurité IPSec définies manuellement entre les homologues OSPFv3 et ne repose pas sur le protocole IKE pour former des SA dynamiques. Les SA manuelles définissent les valeurs SPI (Index des paramètres de sécurité), les algorithmes et les clés

à utiliser entre les pairs. Les SA manuelles ne nécessitent aucune négociation entre les pairs ; par conséquent, la même SA doit être définie sur les deux pairs.

Vous pouvez configurer l'authentification OSPFv3 sur un VLAN ou pour une zone OSPFv3. Lorsque vous configurez un VLAN, les paramètres sont appliqués à toutes les interfaces qui sont membres du VLAN. Lorsque vous configurez l'authentification OSPFv3 pour une zone OSPF, les paramètres sont appliqués à tous les VLAN de cette zone. Les paramètres sont à leur tour appliqués à toutes les interfaces qui sont membres de ces VLAN. Ces paramètres ne s'appliquent pas aux VLAN membres sur lesquels vous avez configuré l'authentification OSPFv3 directement.

Tenez compte des points et limitations suivants avant de configurer l'authentification OSPFv3 sur une appliance Citrix ADC :

- Assurez-vous que vous comprenez les différents composants de l'authentification OSPFv3, décrits dans la RFC 4552.
- Seul le protocole d'en-tête d'authentification est pris en charge pour l'authentification OSPFv3. La charge utile de sécurité encapsulée (ESP) n'est pas prise en charge.
- Vous devez définir une SA avec le même paramètre sur l'interface homologue.
- La nouvelle saisie des clés manuelles n'est pas prise en charge.

Pour configurer l'authentification OSPFv3 sur un VLAN à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué : commandes VLAN d'authentification OSPFv3.

Exemple :

```
1 > VTYSH NS# configure terminal
2 NS(config)# interface vlan2
3 NS(config-if)# ipv6 ospf authentication ipsec spi 256 md5 123456789
     ABCDEF0123456789ABCDEF0
4 <!--NeedCopy-->
```

Pour configurer l'authentification OSPFv3 sur une zone OSPF à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué : Authentification OSPFv3 OSPF Area commandes.

Exemple :

```
1 > VTYSH NS# configure terminal
2 ns(config)#router ipv6 ospf 30
3 ns(config-router)# area 1 authentication ipsec spi 256
     md5123456789ABCDEF0123456789ABCDEF0
4 <!--NeedCopy-->
```


Configuration du redémarrage Graceful pour IPv6 OSPF

Dans une configuration de haute disponibilité (HA) non INC dans laquelle un protocole de routage est configuré, après un basculement, les protocoles de routage sont convergés et les routes entre le nouveau nœud principal et les routeurs voisins adjacents sont apprises. L'apprentissage de chemin prend un certain temps à compléter. Pendant ce temps, le transfert des paquets est retardé, les performances du réseau peuvent être perturbées et les paquets peuvent être abandonnés.

Le redémarrage gracieux permet à une configuration HA lors d'un basculement de demander à ses routeurs adjacents de ne pas supprimer les routes apprises de l'ancien nœud principal de leurs bases de données de routage. En utilisant les informations de routage de l'ancien nœud principal, le nouveau nœud principal et les routeurs adjacents commencent immédiatement à transférer les paquets, sans perturber les performances du réseau.

Pour configurer le redémarrage gracieux pour IPv6 OSPF à l'aide de la ligne de commande VTYSH, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
VTYSH	> VTYSH	Entre l'invite de commande VTYSH.
configure terminal	NS# configure terminal	Entre en mode de configuration globale.
router-id id>	NS(config)#router-id 1.1.1.1	Définit un identificateur de routeur pour l'appliance Citrix ADC. Cet identificateur est défini pour tous les protocoles de routage dynamique. Le même ID doit être spécifié dans l'autre nœud dans une haute disponibilité configurée pour un redémarrage gracieux pour fonctionner correctement dans la configuration HA.

Commande	Exemple	Description de la commande
IPv6ospf restart grace-period <1-1800>	NS(config)# IPv6ospf restart grace-period 170	Spécifie le délai de grâce, en secondes, pour lequel les routes doivent être conservées dans les périphériques d'assistance. Valeur par défaut : 120 secondes.
IPv6 ospf restart helper max-grace-period <1-1800>	NS(config)# IPv6 ospf restart helper max-grace-period 180	Cette commande est facultative pour limiter la période de grâce maximale pour laquelle l'appliance Citrix ADC sera en mode d'assistance. Si l'appliance Citrix ADC reçoit un LSA opaque avec une période de grâce supérieure à la période d'aide max-grace-period définie, le LSA est ignoré et le Citrix ADC n'est pas placé en mode d'assistance.
interface <VLANID>	NS(config)#interface vlan3	Entre en mode de configuration VLAN.
ipv6 router ospf area <area_id> tag <tag_id>	NS(config-if)#ipv6 router ospf area 0 tag 1	Démarre le processus de routage IPv6 OSPF sur un VLAN.
exit	NS(config-if)#exit	Quitte le mode de configuration du VLAN.
router ipv6 ospf	NS(config)# router ipv6 ospf 1	Démarre le processus de routage IPv6 OSPF et passe en mode de configuration pour le processus de routage.
capability restart graceful	NS(config-router)#capability restart graceful	Active le redémarrage gracieux sur le processus de routage IPv6 OSPF.

Commande	Exemple	Description de la commande
redistribute kernel	NS(config-router)# redistribute kernel	Redistribue les routes du noyau.

Configuration d'ISIS

August 20, 2021

L'appliance Citrix ADC prend en charge le protocole de routage dynamique Intermediate System-to-Intermediate System (ISIS ou ISIS). Ce protocole prend en charge IPv4 ainsi que les échanges de routage IPv6. IS-IS est un protocole d'état de liaison et est donc moins sujette aux boucles de routage. Avec les avantages d'une convergence plus rapide et la capacité de prendre en charge des réseaux plus grands, ISIS peut être très utile dans les réseaux de fournisseurs d'accès Internet (ISP).

Conditions préalables à la configuration d'ISIS

Avant de commencer à configurer ISIS, procédez comme suit :

- Assurez-vous que vous comprenez le protocole ISIS.
- Pour les itinéraires IPV6, activez :
  - Fonction de traduction de protocole IPv6.
  - Option de routage dynamique IPv6 sur les VLAN sur lesquels vous souhaitez exécuter le protocole ISIS.

Activation de l'ISIS

Utilisez l'une des procédures suivantes pour activer la fonctionnalité de routage ISIS sur l'appliance Citrix ADC.

Pour activer le routage ISIS à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

activer la fonction ns ISIS

Pour activer le routage ISIS à l'aide de l'interface graphique :

1. Accédez à Système > Paramètres, dans le groupe Modes et fonctionnalités, cliquez sur Modifier les fonctionnalités avancées.
2. Sélectionnez ou désactivez l'option de routage ISIS.

Création d'un processus de routage ISIS et démarrage sur un VLAN

Pour créer un processus de routage ISIS, vous devez utiliser la ligne de commande VTYSH.

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Description
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entre dans le mode de configuration global.
[étiquette]ISIS routeur	Crée un processus de routage ISIS et un mode de configuration pour le processus de routage.
net XX….XXXX.YYYY.YYYY.YYYY.00	Spécifie une valeur NET pour le processus de routage, où : · **XX. .. .XXXX** est l'adresse de zone (peut être de 1 à 13 octets), · **YYYY.YYYY.YYYY** est l'ID système (6 octets), · **00** est le sélecteur N (1 octet).
is type (level-1|level-1-2|level-2-uniquement)	Définit le processus de routage ISIS sur le niveau de routage spécifié. Par défaut : niveau 1-2.
ns IPv6 routage	Démarre le démon de routage dynamique IPv6.
<vlan_name>interface	Pénètre en mode de configuration VLAN.
routeur IP ISIS	Active le processus de routage ISIS sur le VLAN pour les échanges de routage IPv4.
routeur ipv6 ISIS	Active le processus de routage ISIS sur le VLAN pour les échanges de routage IPv6.

Exemple :

```
> VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# net 15.aabb.ccdd.0097.00
NS(config-router)# is-type level-1
NS(config-router)# exit
NS(config)# ns IPv6-routing
NS(config)# interface vlan0
NS(config-if)#  ip router isis 11
NS(config-if)# ipv6 router isis 11
<!--NeedCopy-->
```


Itinéraires publicitaires

La publicité d'itinéraire permet à un routeur en amont de suivre les entités réseau situées derrière l'appliance Citrix ADC.

Pour configurer ISIS pour annoncer les routes à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Description
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entre dans le mode de configuration global.
routeur ISIS [étiquette]	Démarre l'instance de routage ISIS et entrez en mode de configuration pour le processus de routage.
redistribute connected (level-1 or level-1-2 or level-2)	Redistribue les routes connectées, où : **niveau 1** : Redistribue les routes connectées en **niveau 1, niveau 1-2** : Redistribue les routes connectées en niveau 1 et niveau 2, **niveau 2** : Redistribue les routes connectées en niveau 2.
redistribuer le noyau (niveau 1 ou niveau 1-2 ou niveau 2)	Redistribue les routes du noyau, où : **niveau -1** : Redistribue les routes du noyau en **niveau -1, niveau 1-2** : Redistribue les routes du noyau en niveau 1 et niveau 2, **niveau 2** : Redistribue les routes du noyau en niveau 2.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# redistribute connected level-1
NS(config-router)# redistribute kernel level-1
<!--NeedCopy-->
```

Limiter les propagations ISIS

Si vous avez besoin de dépanner votre configuration, vous pouvez configurer le mode d'écoute uniquement sur n'importe quel VLAN donné.

Pour limiter la propagation ISIS à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Description
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entre dans le mode de configuration global.
router isis [étiquette]	Entre dans le mode de configuration du processus de routage.
passive-interface <vlan_name>	Supprime les mises à jour de routage sur les interfaces liées au VLAN spécifié.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Vérification de la configuration ISIS

Vous pouvez utiliser VTYSH pour afficher la table de routage ISIS et les informations ISIS pour un VLAN spécifié.

Pour afficher les paramètres ISIS à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commandes	Description
VTYSH	Affiche l'invite de commande VTYSH.
show ip isis route	Affiche la table de routage ISIS IPv4 mise à jour.
show ipv6 isis route	Affiche la table de routage ISIS mise à jour IPv6.
sh isis interface <vlan_name>	Affiche les informations ISIS IPv6 pour le VLAN spécifié.

Exemple :

```
NS# VTYSH
NS#  show ip isis route
```



```
NS#  show ipv6 isis route
NS# sh isis interface VLAN0
<!--NeedCopy-->
```

Installer des itinéraires dans la table de routage Citrix ADC

August 20, 2021

L'appliance Citrix ADC peut utiliser des itinéraires appris par différents protocoles de routage après avoir installé les itinéraires dans la table de routage de l'appliance.

Pour installer diverses routes dans la table de routage interne à l'aide de la ligne de commande VTYSH :

Dans l'interface de ligne de commande, tapez les commandes suivantes en fonction des itinéraires que vous souhaitez installer :

Commandes	Spécifie
VTYSH	Afficher l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
ns route-install Default	Installez les routes par défaut IPv4 dans la table de routage interne.
ns route-install RIP	Installez des routes IPv4 RIP spécifiques à la table de routage interne.
ns route-install BGP	Installez des routes IPv4 BGP spécifiques à la table de routage interne.
ns route-install OSPF	Installez des routes IPv4 OSPF spécifiques à la table de routage interne.
ns route-install IPv6 Default	Installez les itinéraires par défaut IPv6 dans la table de routage interne.
ns route-install IPv6 RIP	Installez des routes IPv6 RIP spécifiques à la table de routage interne.
ns route-install IPv6 BGP	Installez des itinéraires spécifiques à IPv6 BGP dans la table de routage interne.
ns route-install IPv6 OSPF	Installez des routes spécifiques IPv6 OSPF dans la table de routage interne.

Exemple :

```
>VTYSH
NS# configure terminal
NS# ns route-install Default
NS(config)# ns route-install RIP
NS(config)# ns route-install BGP
NS(config)# ns route-install OSPF
NS# ns route-install IPv6 Default
NS(config)# ns route-install IPv6 RIP
NS(config)# ns route-install IPv6 BGP
NS(config)# ns route-install IPv6 OSPF
<!--NeedCopy-->
```

Publication des itinéraires SNIP et VIP vers des zones sélectives

January 21, 2021

Pour annoncer certaines adresses SNIP dans des zones sélectives, l'activation du mode DRADV ou la redistribution des opérations ZebOSS de connexion ne peut pas être utilisée. En effet, ces opérations envoient toutes les routes connectées à ZebOS. En outre, ajouter des routes statiques factices dans ZebOS pour les sous-réseaux requis, ou ajouter des ACL dans ZebOS pour filtrer les routes connectées non désirées, est une tâche lourde et fastidieuse.

Les options Route réseau et Balise permettent de résoudre ce problème. Vous pouvez activer l'option Route réseau pour une seule adresse SNIP par sous-réseau. L'itinéraire connecté pour cette adresse SNIP est envoyé en tant que route du noyau vers ZebOSS.

Pour les adresses VIP et SNIP, Tag, peut recevoir un entier compris entre 1 et 4294967295. Ce paramètre peut être défini uniquement lorsque l'option Route hôte ou Route réseau est activée pour les adresses VIP ou SNIP. La valeur de balise associée aux adresses VIP et SNIP est également envoyée avec leurs itinéraires vers ZebOS. Les balises avec différentes valeurs peuvent être définies pour les routes VIP et SNIP. Ces valeurs de balise peuvent ensuite être appariées dans les cartes de route dans les ZebOS et annoncées dans des zones sélectives.

Publicité des itinéraires SNIP vers des zones sélectives

Pour configurer les paramètres de routage réseau et de balise d'une adresse SNIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- Si vous ajoutez une nouvelle adresse SNIP :

  - **add ns ip** <IPAddress>@ <netmask> -**type SNIP** -**networkroute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **montrer ns ip** <IPAddress>

- Si vous reconfigurez une adresse SNIP existante :
  - **set ns ip** <IPAddress>@ <netmask> -**type SNIP** - **networkroute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **montrer ns ip** <IPAddress>

Pour configurer les paramètres de routage réseau et de balise d'une adresse SNIP à l'aide de l'interface graphique :

1. Accédez à **Système**> **Réseau**> **IP**> **IPv4**.
2. Définissez les paramètres **Route réseau** et **Balise** lors de l'ajout d'une adresse IP de sous-réseau (SNIP) ou de la modification d'une adresse IP de sous-réseau existante.

Annoncer des itinéraires VIP vers des zones sélectives

Pour configurer les paramètres d'itinéraire hôte et de balise d'une adresse VIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants.

- Si vous ajoutez une nouvelle adresse VIP :
  - **add ns ip** <IPAddress>@ <netmask> -**type VIP** -**hostRoute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **montrer ns ip** <IPAddress>
- Si vous reconfigurez une adresse VIP existante :
  - **set ns ip** <IPAddress>@ <netmask> -**type VIP** -**hostRoute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **montrer ns ip** <IPAddress>

Pour configurer les paramètres d'itinéraire réseau et de balise d'une adresse VIP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IPs> IPv4**.
2. Définissez les paramètres **Route de l'hôte** et **Tag** lors de l'ajout d'une adresse VIP ou de la modification d'une adresse VIP existante.

Configuration de la détection de transfert bidirectionnel

January 21, 2021

Le protocole BFD (Bidirectional Forwarding Detection) est un mécanisme de détection rapide des défaillances des chemins de transfert. BFD détecte les échecs de chemin dans l'ordre de millisecondes. BFD est utilisé avec des protocoles de routage dynamique.

En opération BFD, les homologues de routage échangent des paquets BFD à un intervalle négocié. Si un paquet n'est pas reçu d'un pair dans l'intervalle négocié plus l'intervalle de grâce, l'homologue est considéré comme mort et une notification sera envoyée à l'ensemble des protocoles de routage enregistrés. À leur tour, les protocoles de routage recalculent le meilleur chemin d'accès et reprogramment la table de routage. BFD prend en charge un intervalle de temps plus petit, par rapport aux minuteries fournies par les protocoles de routage, ce qui entraîne une détection plus rapide des défaillances.

L'appliance Citrix ADC prend en charge BFD pour les protocoles de routage suivants : BGP (IPv4 et IPv6), OSPFv2 (IPv4) et OSPFv3 (IPv6). La prise en charge BFD dans l'appliance Citrix ADC est conforme aux RFC 5880, 5881 et 5883.

Points à prendre en considération pour la configuration de la détection de transfert bidirectionnel

Avant de commencer à configurer BFD, tenez compte des points suivants :

- Assurez-vous de bien comprendre les différents composants de BFD décrits dans les RFC 5880, 5881 et 5883.
- Le BFD sur une appliance Citrix ADC est pris en charge pour les protocoles de routage suivants :
  - BGP (IPv4 et IPv6)
  - OSPFv2 (IPv4)
  - OSPFv3 (IPv6)
- BFD sur une appliance Citrix ADC n'est pas pris en charge pour les protocoles de routage suivants :
  - ISIS
  - RIP (IPv4)
  - Ripng (IPv6)
- Les fonctionnalités BFD suivantes ne sont pas prises en charge sur un appliance Citrix ADC :
  - Mode Echo BFD
  - Authentification BFD
  - BFD Demander mode asynchrone
- Les valeurs minimales pour les minuteries BFD et BFD Rx sont de 100 millisecondes.
- Lorsque BFD est utilisé dans une topologie avec des adresses IP partagées (par exemple, configuration haute disponibilité de couche 2 avec des adresses SNIP ou configuration de cluster avec des adresses IP par répartition), BFD réduit les sessions actives lors d'un basculement car le temps de détection des défaillances BFD (ordre de millisecondes) est inférieur à l'HA intervalle de détection de basculement (3 à 4 secondes). Par conséquent, Citrix recommande l'utilisation

du redémarrage Graceful dans les topologies HA de couche 2 car les routes sont conservées pendant le processus de basculement.

Étapes de configuration

La configuration de BFD sur une appliance Citrix ADC comporte les tâches suivantes :

- Configurer les paramètres BFD
- Configurer la prise en charge BFD pour les protocoles de routage dynamique

Configurer les paramètres BFD

L'appliance Citrix ADC fournit des paramètres de session BFD distincts pour les sessions à saut unique, les sessions à saut multiple IPv4 et les sessions à saut multiple IPv6. Si vous ne configurez pas les paramètres BFD pour un type de session, les valeurs par défaut sont appliquées pour cette session.

La valeur par défaut de chaque paramètre BFD est identique pour les sessions de saut unique, les sessions de saut multiples IPv4 et les sessions de saut multiples IPv6. Le tableau suivant affiche la valeur par défaut de chaque paramètre BFD.

Nom du paramètre BFD	Valeur par défaut
Intervalle	750 millisecondes
Rx minimum	500 millisecondes
Multiplicateur	3

> **IMPORTANT :**
>
> Les cartes réseau Mellanox dans une appliance Citrix prennent environ 1500 ms à initialiser. Vous devez définir les minuteries BFD sur plus de 1500 ms pour une appliance Citrix ADC avec cartes réseau Mellanox. Citrix recommande de définir les minuteries BFD sur 3000 ms :
>
> - Interval Tx = 600 ms
> - Minimum Rx = 600 ms
> - Multipler = 5

Configuration des paramètres BFD pour une session de saut unique

Pour configurer les paramètres BFD pour une session de saut unique à l'aide de la ligne de commande VTYSH, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de commandes VTYSH.
`configure terminal`	Entrer en mode de configuration globale.
`interface` `vlan ID>`	Entrer le mode de configuration de l'interface.
`bfd singlehop-peer interval <num> minrx <num> multiplier <num>`	Configurer les paramètres BFD sur l'interface spécifiée.

Exemple de configuration :

```
1  > vtysh
2
3  ns# configure terminal
4
5  ns(config)# interface vlan3
6
7  ns(config-if)# bfd singlehop-peer interval 200 minrx 200 multiplier 5
8
9  ns(config-if)# exit
10 <!--NeedCopy-->
```

Configuration des paramètres BFD pour les sessions de saut multiples IPv4

Pour configurer les paramètres BFD pour les sessions de saut multiples IPv4 à l'aide de la ligne de commande VTYSH, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de commandes VTYSH.
`configure terminal`	Entrer en mode de configuration globale.
`bfd multihop-peer <ipv4addr> interval <num> minrx <num> multiplier <num>`	Configurez les paramètres BFD pour les sessions de sauts multiples IPv4.

Exemple de configuration :

```
1      > vtysh
2
3      ns# configure terminal
```



```
4
5     ns(config)# bfd multihop-peer 20.20.20.138 interval 300 minrx 300
          multiplier 5
6
7     ns(config)# exit
8 <!--NeedCopy-->
```

Configuration des paramètres BFD pour les sessions de saut multiples IPv6

Pour configurer les paramètres BFD pour les sessions de saut multiples IPv6 à l'aide de la ligne de commande VTYSH, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de commandes VTYSH.
`configure terminal`	Entrer en mode de configuration globale.
`bfd multihop-peer ipv6 <ipv6addr> interval <num> minrx <num> multiplier <num>`	Configurez les paramètres BFD pour les sessions de sauts multiples IPv6.

Exemple de configuration :

```
1     > vtysh
2
3     ns(config)# bfd multihop-peer ipv6 20fe:125::138 interval 500 minrx
          500 multiplier 5
4
5     ns(config)# exit
6 <!--NeedCopy-->
```

Configurer la prise en charge BFD pour les protocoles de routage dynamique

Vous pouvez activer BFD pour un protocole de routage dynamique pour un type de session avec un homologue. Par exemple, houblon unique et plusieurs houblons. L'appliance Citrix ADC applique les paramètres BFD pertinents à la session.

Configuration de BFD pour une session de saut unique BGP IPv4

Pour configurer BFD pour une session de saut unique BGP IPv4 à l'aide de la ligne de VTYSH commande, à l'invite de commande, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de commandes `VTYSH`.
`configure terminal`	Entrer en mode de configuration globale.
`router bgp <asnumber>`	Système autonome BGP. `asnumber` est un paramètre obligatoire.
`neighbor <ipv4addr> remote-as <num>`	Mettez à jour la table BGP IPv4 avec l'adresse IPv4 du voisin dans le système autonome spécifié.
`neighbor <ipv4addr> fall-over bfd`	Activez BFD pour le voisin spécifié.

Exemple de configuration :

```
1      > vtysh
2
3      ns# configure terminal
4
5      ns(config)#router bgp 1
6
7      ns(config-router)#neighbor 20.20.20.138 remote-as 1
8
9      ns(config-router)#neighbor 20.20.20.138 fall-over bfd
10
11     ns(config-router)#redistribute kernel
12
13     ns(config-router)#exit
14 <!--NeedCopy-->
```

Configuration de BFD pour une session de saut multiple BGP IPv4

Pour configurer BFD pour une session de saut multiple IPv4 BGP à l'aide de la ligne de `VTYSH` commande, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de commandes `VTYSH`.
`configure terminal`	Entrer en mode de configuration globale.
`router bgp <asnumber>`	Système autonome BGP. `asnumber` est un paramètre obligatoire.

Commande	Spécifie
`neighbor <ipv4addr> remote-as <num>`	Mettez à jour la table BGP IPv4 avec l'adresse IPv4 du voisin dans le système autonome spécifié.
`neighbor <ipv4addr> fall-over bfd multihop`	Activez BFD pour le voisin spécifié.

Exemple de configuration :

```
1      > vtysh
2
3      ns# configure terminal
4
5      ns(config)#router bgp 1
6
7      ns(config-router)#neighbor 20.20.20.138 remote-as 1
8
9      ns(config-router)#neighbor 20.20.20.138 fall-over bfd multihop
10
11     ns(config-router)#redistribute kernel
12
13     ns(config-router)#exit
14 <!--NeedCopy-->
```

Configuration de BFD pour une session IPv6 BGP Single Hop

Pour configurer BFD pour une session de saut unique BGP IPv6 à l'aide de la ligne de `VTYSH` commande, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de commandes `VTYSH`.
`configure terminal`	Entrer en mode de configuration globale.
`router bgp <asnumber>`	Système autonome BGP. `asnumber` est un paramètre obligatoire.
`neighbor <ipv6addr> remote-as <num>`	Mettez à jour la table IPv6 BGP avec le lien adresse IPv6 locale du voisin dans le système autonome spécifié.
`neighbor <ipv6addr> fall-over bfd`	Activez BFD pour le voisin spécifié.

Commande	Spécifie
address-family ipv6	Entrez le mode de configuration de la famille d'adresses.
neighbor <ipv6addr> activate	Préfixes d'échange pour la famille de routeurs IPv6 entre l'homologue et le nœud local à l'aide de l'adresse locale du lien.

Exemple de configuration :

```
> vtysh

ns# configure terminal ns(config)#router bgp 1

ns(config-router)#neighbor 30fe:123::124 remote-as 1

ns(config-router)#neighbor 30fe:123::124 fall-over bfd

ns(config-router)#address-family ipv6

ns(config-router-af)#neighbor 30fe:123::124 activate

ns(config-router-af)#redistribute kernel

ns(config-router-af)#exit

<!--NeedCopy-->
```

Configuration de BFD pour une session de saut multiple BGP IPv6

Pour configurer BFD pour une session de saut multiple IPv6 BGP à l'aide de la ligne de VTYSH commande, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
vtysh	Afficher l'invite de commandes VTYSH.
configure terminal	Entrer en mode de configuration globale.
router bgp <asnumber>	Système autonome BGP. asnumber est un paramètre obligatoire.

Commande	Spécifie
`neighbor <ipv6addr> remote-as <num>`	Mettez à jour la table IPv6 BGP avec le lien adresse IPv6 locale du voisin dans le système autonome spécifié.
`neighbor <ipv6addr> fall-over bfd multihop`	Activez BFD pour le voisin spécifié.
`address-family ipv6`	Entrez le mode de configuration de la famille d'adresses.
`neighbor <ipv6addr> activate`	Préfixes d'échange pour la famille de routeurs IPv6 entre le pair et le nœud local à l'aide de l'adresse lien-local.

Exemple de configuration :

```
> vtysh

ns# configure terminal

ns(config)# bfd multihop-peer ipv6 20fe:125::138 interval 500 minrx 500
    multiplier 5

ns(config)#router bgp 1

ns(config-router)#neighbor 20fe:125::138 remote-as 1

ns(config-router)#neighbor 20fe:125::138 fall-over bfd multihop

ns(config-router)#address-family ipv6

ns(config-router-af)#neighbor 20fe:125::138 activate

ns(config-router-af)#redistribute kernel

ns(config-router-af)#end

<!--NeedCopy-->
```

Configuration de BFD pour OSPFv2 (IPv4) sur les interfaces

Vous pouvez activer BFD sur tout ou sur une interface spécifique qui utilise le protocole OSPFv2.

Pour configurer BFD pour OSPFv2 sur toutes les interfaces à l'aide de la ligne de VTYSH commande :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de commandes VTYSH.
`configure terminal`	Entrer en mode de configuration globale.
`router ospf <process tag>`	Entrez le mode de configuration OSPFv2.
`bfd all-interfaces`	Activez BFD sur toutes les interfaces qui utilisent OSPFv2.

Exemple de configuration :

```
1      > vtysh
2
3      ns# configure terminal
4
5      ns(config)#router ospf 1
6
7      ns(config-router)#bfd all-interfaces
8
9      ns(config-router)#redistribute kernel
10
11     ns(config-router)#exit
12 <!--NeedCopy-->
```

Pour configurer BFD pour OSPFv2 sur une interface spécifique à l'aide de la ligne de VTYSH commande :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de commandes VTYSH.
`configure terminal`	Entrer en mode de configuration globale.
`interface` `<vlan ID>`	Entrer le mode de configuration de l'interface.
`ip ospf bfd`	Activez BFD sur l'interface spécifiée qui utilise OSPFv2.

Exemple de configuration :

```
    > vtysh

    ns# configure terminal

    ns(config)# interface vlan5

    ns(config-if)# ip ospf bfd

    ns(config-if)# exit
<!--NeedCopy-->
```

Configuration de BFD pour OSPFv3 (IPv6) sur les interfaces

Vous pouvez activer BFD sur tout ou sur une interface spécifique qui utilise le protocole OSPFv3.

Pour configurer BFD pour OSPFv3 sur toutes les interfaces à l'aide de la ligne de VTYSH commande :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de commandes VTYSH.
`configure terminal`	Entrer en mode de configuration globale.
`router ipv6 ospf <process tag>`	Entrez le mode de configuration OSPFv3.
`bfd all-interfaces`	Activez BFD sur toutes les interfaces qui utilisent OSPFv3.

Exemple de configuration :

```
    > vtysh

    ns# configure terminal

    ns(config)#router ipv6 ospf 10

    ns(config-router)#bfd all-interfaces

    ns(config-router)#redistribute kernel

    ns(config-router)#exit
```



```
<!--NeedCopy-->
```

Pour configurer BFD pour OSPFv3 sur une interface spécifique à l'aide de la ligne de VTYSH commande :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de commandes VTYSH.
`configure terminal`	Entrer en mode de configuration globale.
`interface` <vlan ID>	Entrer le mode de configuration de l'interface.
`ipv6 ospf bfd`	Activez BFD sur l'interface spécifiée qui utilise OSPFv3.

Exemple de configuration :

```
    > vtysh

    ns# configure terminal

    ns(config)# interface vlan15

    ns(config-if)# ipv6 ospf bfd

    ns(config-if)# exit
<!--NeedCopy-->
```

Configuration d'itinéraires statiques

August 20, 2021

Les itinéraires statiques sont créés manuellement pour améliorer les performances de votre réseau. Vous pouvez surveiller les itinéraires statiques pour éviter les interruptions de service. En outre, vous pouvez affecter des pondérations aux itinéraires ECMP et créer des routes nulles pour empêcher les boucles de routage.

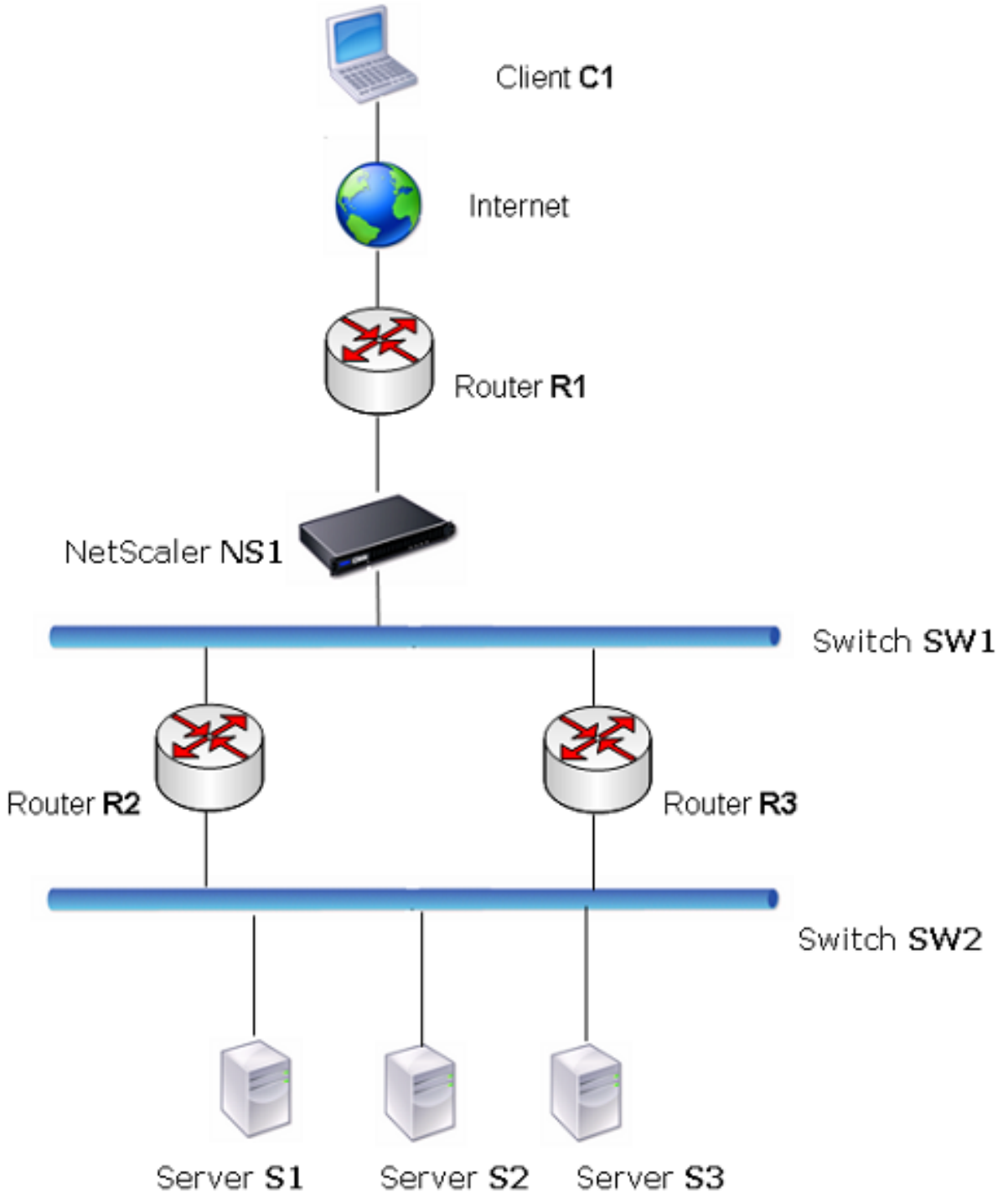
Routes statiques surveillées. Si un itinéraire (statique) créé manuellement tombe en panne, une route de sauvegarde n'est pas automatiquement activée. Vous devez supprimer manuellement

l'itinéraire statique principal inactif. Toutefois, si vous configurez l'itinéraire statique en tant que route surveillée, l'appliance Citrix ADC peut activer automatiquement une route de sauvegarde.

La surveillance statique des itinéraires peut également être basée sur l'accessibilité du sous-réseau. Un sous-réseau est généralement connecté à une seule interface, mais il est logiquement accessible via d'autres interfaces. Les sous-réseaux liés à un VLAN ne sont accessibles que si le VLAN est en service. Les VLAN sont des interfaces logiques par lesquelles les paquets sont transmis et reçus par Citrix ADC. Une route statique est marquée comme DOWN si le saut suivant réside sur un sous-réseau inaccessible.

Remarque : Dans une configuration haute disponibilité (HA), la valeur par défaut pour les routes d'état surveillées (MSRs) sur le nœud secondaire est UP. La valeur est définie pour éviter un écart de transition d'état lors du basculement, ce qui pourrait entraîner la suppression de paquets sur ces routes.

Considérez la topologie simple suivante, dans laquelle un Citrix ADC répartit le trafic de charge vers un site sur plusieurs serveurs.



Le routeur R1 déplace le trafic entre le client et l'appliance Citrix ADC. L'appliance peut atteindre les serveurs S1 et S2 via les routeurs R2 ou R3. Il a deux routes statiques à travers lesquelles atteindre

le sous-réseau des serveurs, l'une avec R2 comme Gateway et l'autre avec R3 comme Gateway. La surveillance de ces deux routes est activée. La distance administrative de l'itinéraire statique avec la Gateway R2 est inférieure à celle de l'itinéraire statique avec la Gateway R3. Par conséquent, R2 est préféré à R3 pour transférer le trafic vers les serveurs. En outre, l'itinéraire par défaut sur Citrix ADC pointe sur R1 afin que tout le trafic Internet se ferme correctement.

Si R2 échoue alors que la surveillance est activée sur la route statique, qui utilise R2 comme Gateway, Citrix ADC le marque comme DOWN. Le Citrix ADC utilise désormais la route statique avec R3 comme Gateway et transmet le trafic aux serveurs via R3.

Le Citrix ADC prend en charge la surveillance des routes statiques IPv4 et IPv6. Vous pouvez configurer Citrix ADC pour surveiller une route statique IPv4 en créant un nouveau moniteur ARP ou PING ou en utilisant des moniteurs ARP ou PING existants. Vous pouvez configurer Citrix ADC pour surveiller un itinéraire statique IPv6 en créant une nouvelle découverte de voisin pour IPv6 (ND6) ou un moniteur PING ou en utilisant les moniteurs ND6 ou PING existants.

Routes statiques pondérées. Lorsque l'appliance Citrix ADC prend des décisions de routage impliquant des itinéraires avec une distance et un coût égaux, c'est-à-dire des itinéraires ECMP (Equal Cost Multi-Path), elle équilibre la charge entre eux à l'aide d'un mécanisme de hachage basé sur les adresses IP source et de destination. Toutefois, pour un itinéraire ECMP, vous pouvez configurer une valeur de pondération. Citrix ADC utilise ensuite à la fois le poids et la valeur hachée pour équilibrer la charge.

Routes nulles. Si l'itinéraire choisi dans une décision de routage est inactif, l'appliance Citrix ADC choisit une route de sauvegarde. Si toutes les routes de sauvegarde deviennent inaccessibles, l'appliance peut réacheminer le paquet vers l'expéditeur, ce qui peut entraîner une boucle de routage conduisant à la congestion du réseau. Pour éviter cette situation, vous pouvez créer une route nulle, qui ajoute une interface null en tant que Gateway. La route nulle n'est jamais l'itinéraire préféré, car elle a une distance administrative plus élevée que les autres routes statiques. Mais il est sélectionné si les autres routes statiques deviennent inaccessibles. Dans ce cas, l'appliance supprime le paquet et empêche une boucle de routage.

Configuration d'itinéraires statiques IPv4

Vous pouvez ajouter une route statique simple ou une route nulle en définissant quelques paramètres, ou vous pouvez définir des paramètres supplémentaires pour configurer une route statique surveillée ou surveillée et pondérée. Vous pouvez modifier les paramètres d'un itinéraire statique. Par exemple, vous pouvez affecter une pondération à un itinéraire non pondéré ou désactiver la surveillance sur un itinéraire surveillé.

Procédures CLI

Pour créer un itinéraire statique à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add route <network> <netmask> <gateway>[-cost <positive_integer>] [-advertise (DISABLED | ENABLED)]
- show route [<network> <netmask> [<gateway>]] [<routeType>] [-detail]

Exemple :

```
> add route 10.102.29.0 255.255.255.0 10.102.29.2 -cost 2 -advertise
   ENABLED
 Done
<!--NeedCopy-->
```

Pour créer un itinéraire statique surveillé à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour créer une route statique surveillée et vérifier la configuration :

- add route <network> <netmask> <gateway> [-distance <positive_integer>] [-weight <positive_integer>][-msr (ENABLED | DISABLED) [-monitor <string>]]
- montrer l'itinéraire [<network> <netmask> [<gateway>]] [<routeType>] [-detail]

Exemple :

```
> add route 10.102.29.0 255.255.255.0 10.102.29.3 -distance 5 -weight 6
    -msr ENBLED -monitor PING
 Done
<!--NeedCopy-->
```

Pour créer une route nulle à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add route <network> <netmask> null
- show route <network> <netmask>

Exemple :

```
> add route 10.102.29.0 255.255.255.0 null
 Done
<!--NeedCopy-->
```

Pour supprimer un itinéraire statique à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

rm route <network> <netmask> <gateway>

Exemple :


```
1 > rm route 10.102.29.0 255.255.255.0 10.102.29.3
2  Done
3 <!--NeedCopy-->
```

Procédures GUI

Pour configurer un itinéraire statique à l'aide de l'interface graphique :

Accédez à Système > Réseau > Itinéraires et, sous l'onglet De base, ajoutez un nouvel itinéraire statique ou modifiez un itinéraire statique existant.

Pour supprimer un itinéraire à l'aide de l'interface graphique :

Accédez à Système > Réseau > Itinéraires et, sous l'onglet De base, supprimez l'itinéraire statique.

Configuration d'itinéraires statiques IPv6

Vous pouvez configurer un maximum de six itinéraires statiques IPv6 par défaut. Les itinéraires IPv6 sont sélectionnés selon que l'adresse MAC du périphérique de destination est accessible. Cela peut être déterminé à l'aide de la fonctionnalité de découverte de voisins IPv6. Les routes sont équilibrées en charge et seuls les mécanismes de hachage basés sur la source/la destination sont utilisés. Par conséquent, les mécanismes de sélection d'itinéraires tels que le round robin ne sont pas pris en charge. L'adresse de saut suivante dans l'itinéraire par défaut n'a pas besoin d'appartenir au sous-réseau NSIP.

Procédures CLI

Pour créer un itinéraire IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour créer une route IPv6 et vérifier la configuration :

- ajouter la route 6 <network>[-vlan]<positive_integer>
- afficher la route 6 [\ []<network>

Exemple :

```
1 > add route6 ::/0 FE80::67 -vlan 5
2  Done
3 <!--NeedCopy-->
```

Pour créer un itinéraire statique IPv6 surveillé à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour créer une route statique IPv6 surveillée et vérifier la configuration :

- ajouter la route6 <network>[-msr (ENABLED | DISABLED) [-monitor]<string>
- show route6 [\ []

Exemple :

```
1 > add route6 ::/0 2004::1 -msr ENABLED -monitor PING
2  Done
3 <!--NeedCopy-->
```

Pour supprimer un itinéraire IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

rm route6 <network> <gateway>

Exemple :

```
1 > rm route6 ::/0 FE80::67
2  Done
3 <!--NeedCopy-->
```

Procédures GUI

Pour configurer un itinéraire IPv6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > Itinéraires et, sous l'onglet IPV6, ajoutez un nouvel itinéraire IPv6 ou modifiez un itinéraire IPv6 existant.

Pour supprimer un itinéraire IPv6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > Itinéraires et, sous l'onglet IPV6, supprimez l'itinéraire IPv6.

RHI (Route Health Injection) basé sur les paramètres du serveur virtuel

August 20, 2021

L'option et le paramètre suivants sont introduits pour contrôler la fonctionnalité RHI (Route Health Injection) de l'appliance Citrix ADC pour la publicité de l'itinéraire d'une adresse VIP.

- **VSVR_CNTRLD**. Il s'agit d'une option pour le paramètre (Vserver RHI Level) d'une adresse VIP. Lorsque cette option est définie sur le paramètre Vserver RHI Level, le comportement RHI pour la publicité de l'itinéraire de l'adresse VIP dépend du paramètre RHI STATE sur tous les serveurs virtuels associés de l'adresse VIP ainsi que leurs états.
- **RHI STATE**. C'est un paramètre de serveur virtuel. Vous pouvez définir le paramètre RHI STATE sur PASSIVE ou ACTIVE. Par défaut, le paramètre RHI STATE est défini sur PASSIVE.

Pour une adresse VIP, lorsque le paramètre RHI (Vserver RHI Level) est défini sur VSVR_CNTRLD, les comportements RHI suivants sont différents pour l'adresse VIP sur la base des paramètres RHI STATE sur les serveurs virtuels associés à l'adresse VIP :

- Si vous définissez RHI STATE sur PASSIVE sur tous les serveurs virtuels, le Citrix ADC annonce toujours l'itinéraire de l'adresse VIP.
- Si vous définissez RHI STATE sur ACTIVE sur tous les serveurs virtuels, le Citrix ADC annonce l'itinéraire de l'adresse VIP si au moins un des serveurs virtuels associés est en état UP.
- Si vous définissez RHI STATE sur ACTIVE sur certains et PASSIVE sur d'autres, le Citrix ADC annonce l'itinéraire de l'adresse VIP si au moins un des serveurs virtuels associés, dont RHI STATE est défini sur ACTIVE, est en état UP.

Le tableau suivant affiche l'exemple de comportement RHI pour une adresse VIP sur la base des paramètres RHI STATE sur les serveurs virtuels associés à l'adresse VIP. L'appliance Citrix ADC dispose de deux serveurs virtuels V1 et V2 associés à l'adresse VIP :

Serveurs virtuels associés pour un VIP	État 1	État 2	État 3	État 4
État RHI défini sur PASSIVE sur tous les serveurs virtuels				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Annoncer l'itinéraire pour cette adresse VIP ?	Oui	Oui	Oui	Oui
État RHI défini sur ACTIVE sur tous les serveurs virtuels				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN

Serveurs virtuels associés pour un VIP	État 1	État 2	État 3	État 4
Annoncer l'itinéraire pour cette adresse VIP ?	Oui	Oui	Oui	Non
État RHI défini sur ACTIVE sur un serveur virtuel et PASSIVE sur l'autre				
V1 (état RHI = ACTIVE)	UP	UP	DOWN	DOWN
V2 (état RHI = PASSIF)	UP	DOWN	UP	DOWN
Annoncer l'itinéraire pour cette adresse VIP ?	Oui	Oui	Non	Non

Pour configurer RHI pour une adresse VIP, en fonction du paramètre RHI (RHI State) des serveurs virtuels associés, effectuez les opérations suivantes :

- Définissez le paramètre RHI (Vserver RHI Level) sur VSVR_CNTRLD pour l'adresse VIP.
- Définissez le paramètre RHI State pour chaque serveur virtuel associé à l'adresse VIP.

Pour définir le niveau RHI vServer pour une adresse VIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set ns ip** <IPAddress> [-**vserverRHILevel** <vserverRHILevel>]

Pour définir le paramètre RHI State d'un serveur virtuel à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set lb vserver** <name> [-**RHIstate** (**PASSIVE** | **ACTIVE**)]

Pour définir le niveau RHI vServer pour une adresse VIP à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **IP**.

2. Sélectionnez une adresse VIP, puis cliquez sur **Modifier**.
3. Définissez le paramètre **VServer RHI Level** sur **VSVR_CNTRLD**, puis cliquez sur **OK** .

Pour définir le paramètre RHI State d'un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Sélectionnez un serveur virtuel d'équilibrage de charge, puis cliquez sur **Modifier**.
3. Définissez le paramètre **RHI State**, puis cliquez sur **OK** .

Configuration d'itinéraires basés sur des stratégies

January 21, 2021

La gamme basée sur des règles base les décisions de gamme sur les critères que vous spécifiez. Une route basée sur des règles (PBR) spécifie les critères de sélection des paquets et, généralement, un saut suivant vers lequel envoyer les paquets sélectionnés. Par exemple, vous pouvez configurer l'appliance Citrix ADC pour acheminer les paquets sortants à partir d'une adresse IP ou d'une plage spécifique vers un routeur de saut suivant particulier. Chaque paquet est mis en correspondance avec chaque PBR configuré, dans l'ordre déterminé par les priorités spécifiées, jusqu'à ce qu'une correspondance soit trouvée. Si aucune correspondance n'est trouvée ou si le PBR correspondant spécifie une action DENY, Citrix ADC applique la table de routage pour un routage basé sur la destination normale.

Un PBR base les décisions de routage des paquets de données sur des paramètres tels que l'adresse IP source, le port source, l'adresse IP de destination, le port de destination, le protocole et l'adresse MAC source. Un PBR définit les conditions qu'un paquet doit satisfaire pour que Citrix ADC achemine le paquet. Ces actions sont connues sous le nom de "modes de traitement." Les modes de traitement sont les suivants :

- **ALLOW.** L'appliance envoie le paquet au routeur de saut suivant désigné.
- **DENY.** Citrix ADC applique la table de routage pour le routage basé sur la destination normale.

Vous pouvez créer des PBR pour le trafic IPv4 et IPv6 sortant.

De nombreux utilisateurs commencent par créer des PBR, puis les modifier. Pour activer un nouveau PBR, vous devez l'appliquer. Pour désactiver un PBR, vous pouvez le supprimer ou le désactiver. Vous pouvez modifier le numéro de priorité d'un PBR pour lui donner une priorité supérieure ou inférieure.

Routes basées sur des stratégies (PBR) pour le trafic IPv4

August 20, 2021

La configuration des PBR implique les tâches suivantes :

- Créez un PBR.
- Appliquer les PBR.
- (Facultatif) Désactivez ou activez un PBR.
- (Facultatif) Renuméroter la priorité du PBR.

Création ou modification d'un PBR

Vous ne pouvez pas créer deux PBR avec les mêmes paramètres. Si vous tentez de créer un doublon, un message d'erreur s'affiche.

Vous pouvez configurer la priorité d'un PBR. La priorité (une valeur entière) définit l'ordre dans lequel l'appliance Citrix ADC évalue les PBR. Lorsque vous créez un PBR sans spécifier de priorité, Citrix ADC attribue automatiquement une priorité qui est un multiple de 10.

Si un paquet correspond à la condition définie par le PBR, Citrix ADC effectue une action. Si le paquet ne correspond pas à la condition définie par le PBR, Citrix ADC compare le paquet au PBR avec la priorité la plus élevée suivante.

Au lieu d'envoyer les paquets sélectionnés à un routeur de saut suivant, vous pouvez configurer le PBR pour les envoyer à un serveur virtuel d'équilibrage de charge de liaison auquel vous avez lié plusieurs sauts suivants. Cette configuration peut fournir une sauvegarde si un lien de saut suivant échoue.

Prenons l'exemple suivant. Deux PBR, p1 et p2, sont configurés sur Citrix ADC et assignés automatiquement les priorités 20 et 30. Vous devez ajouter un troisième PBR, p3, à évaluer immédiatement après le premier PBR, p1. Le nouveau PBR, p3, doit avoir une priorité entre 20 et 30. Dans ce cas, vous pouvez spécifier la priorité 25.

Procédures CLI

Pour créer un PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add ns pbr <name> <action> [-srcIP [<operator>] <srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>] <destPortVal>] [-nextHop <nextHopVal>] [-srcMac <mac_addr>] [-protocol <protocol> |-protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr (ENABLED | DISABLED) [-monitor <string>]] [-state (ENABLED | DISABLED)]
- show ns pbr

Exemple :

```
1 > add ns pbr pbr1  allow -srcip 10.102.37.252 -destip 10.10.10.2 -
     nexthop 10.102.29.77
```



```
2   Done
3 <!--NeedCopy-->
```

Pour modifier la priorité d'un PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour modifier la priorité et vérifier la configuration :

- set ns pbr <name> [-action (ALLOW | DENY)] [-srcIP [<operator>] <srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>] <destPortVal>] [-nextHop <nextHopVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr (ENABLED | DISABLED) [-monitor <string>]] [-state (ENABLED | DISABLED)]
- show ns pbr [<name>]

Exemple :

```
1 > set ns pbr pbr1 -priority 23
2  Done
3 <!--NeedCopy-->
```

Pour supprimer un ou tous les PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- rm ns pbr <name>
- clear ns pbrs

Exemple :

```
1 > rm ns pbr pbr1
2  Done
3
4 > clear ns PBRs
5  Done
6 <!--NeedCopy-->
```

Procédures GUI

Pour créer un PBR à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR, sous l'onglet PBR, ajoutez un nouveau PBR ou modifiez un PBR existant.

Pour supprimer un ou tous les PBR à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR, sous l'onglet PBR, supprimez le PBR.

Application d'un PBR

Vous devez appliquer un PBR pour l'activer. La procédure suivante réapplique tous les PBR que vous n'avez pas désactivés. Les PBR constituent une arborescence de mémoire (table de recherche). Par exemple, si vous créez 10 PBR (p1 - p10), puis que vous créez un autre PBR (p11) et l'appliquez, toutes les PBR (p1 - p11) sont fraîchement appliquées et une nouvelle table de recherche est créée. Si une session est associée à un DENY PBR, la session est détruite.

Vous devez appliquer cette procédure après chaque modification apportée à un RBP. Par exemple, vous devez suivre cette procédure après avoir désactivé un PBR.

Remarque : les PBR créés sur l'appliance Citrix ADC ne fonctionnent pas tant qu'ils ne sont pas appliqués.

Pour appliquer un PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

apply ns PBRs

Pour appliquer un PBR à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > PBR.
2. Sous l'onglet PBR, sélectionnez le PBR, dans la liste Action, sélectionnez Appliquer.

Activation ou désactivation des PBR

Par défaut, les PBR sont activés. Cela signifie que lorsque des PBR sont appliqués, l'appliance Citrix ADC compare automatiquement les paquets entrants aux PBR configurés. Si un PBR n'est pas requis dans la table de recherche, mais qu'il doit être conservé dans la configuration, il doit être désactivé avant l'application des PBR. Une fois les PBR appliqués, Citrix ADC ne compare pas les paquets entrants avec les PBR désactivés.

Pour activer ou désactiver un PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- enable ns pbr <name>
- disable ns pbr <name>

Exemple :

```
> enable ns PBR pbr1
 Done
> show ns PBR pbr1
1)      Name: pbr1
        Action: ALLOW                          Hits: 0
        srcIP = 10.102.37.252
```



```
7          destIP = 10.10.10.2
8          srcMac:                                 Protocol:
9          Vlan:                                   Interface:
10         Active Status: ENABLED                  Applied Status: APPLIED
11         Priority: 10
12         NextHop: 10.102.29.77
13
14  Done
15
16 > disable ns PBR pbr1
17 Warning: PBR modified, use 'apply pbrs' to commit this operation
18
19 > apply pbrs
20  Done
21
22 > show ns PBR pbr1
23 1)       Name: pbr1
24         Action: ALLOW                           Hits: 0
25         srcIP = 10.102.37.252
26         destIP = 10.10.10.2
27         srcMac:                                 Protocol:
28         Vlan:                                   Interface:
29         Active Status: DISABLED                 Applied Status:
               NOTAPPLIED
30         Priority: 10
31         NextHop: 10.102.29.77
32 Done
33 <!--NeedCopy-->
```

Pour activer ou désactiver un PBR à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > PBR.
2. Sous l'onglet PBR, sélectionnez le PBR, dans la liste Action, sélectionnez Activer ou Désactiver.

Renuméroter les PBR

Vous pouvez automatiquement renuméroter les PBR pour définir leurs priorités à des multiples de 10.

Pour renuméroter les PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- renumber ns pbrs

Pour renuméroter les PBR à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR, sous l'onglet PBR, dans la liste Action, sélectionnez Renuméroter les priorités.

Cas d'utilisation - PBR avec plusieurs houblons

Considérons un scénario dans lequel deux PBR, PBR1 et PBR2, sont configurés sur l'appliance Citrix ADC NS1. PBR1 achemine tous les paquets sortants, avec l'adresse IP source 10.102.29.30, vers le routeur de saut suivant R1. PBR2 achemine tous les paquets sortants, avec l'adresse IP source 10.102.29.90, vers le routeur de saut suivant R2. R3 est un autre routeur de saut suivant connecté à NS1.

Si le routeur R1 échoue, tous les paquets sortants correspondant à PBR1 sont supprimés. Pour éviter cette situation, vous pouvez spécifier un serveur virtuel LLB (Link Load Balancing) dans le champ de saut suivant lors de la création ou de la modification d'un PBR. Plusieurs sauts suivants sont liés au serveur virtuel LLB en tant que services (par exemple R1, R2 et R3). Maintenant, si R1 échoue, tous les paquets correspondant à PBR1 sont routés vers R2 ou R3 comme déterminé par la méthode LB configurée sur le serveur virtuel LLB.

L'appliance Citrix ADC génère une erreur si vous tentez de créer un PBR avec un serveur virtuel LLB comme saut suivant dans les cas suivants :

- Ajout d'un autre PBR avec le même serveur virtuel LLB.
- Spécification d'un serveur virtuel LLB inexistant.
- Spécification d'un serveur virtuel LLB pour lequel les services liés ne sont pas des sauts suivants.
- Spécification d'un serveur virtuel LLB pour lequel la méthode LB n'est pas définie sur l'une des options suivantes :
  - ROUNDROBIN
  - DESTINATIONIPHASH
  - SOURCEIPHASH
  - SRCIPDESTIPHASH
  - LEASTPACKETS
  - LEASTBANDWIDTH
  - LTRM
  - CALLIDHASH
  - CUSTOM LOAD
- Spécification d'un serveur virtuel LLB pour lequel le type de persistance LB n'est pas défini sur l'une des options suivantes :
  - DESTIP
  - SOURCEIP
  - SRCDSTIP

Le tableau suivant répertorie les noms et les valeurs des entités configurées sur l'appliance Citrix ADC :

Type d'entité	Nom	Adresse IP
Serveur virtuel d'équilibrage de charge de liaison	LLB1	SO
Services (prochains sauts)	Router1	1.1.1.254
	Router2	2.2.2.254
	Router3	3.3.3.254
PBR	PBR1	SO
	PBR2	SO

Tableau 1. Exemples de valeurs pour la création d'entités

Pour implémenter la configuration décrite ci-dessus, vous devez :

1. Créez des services Router1, Router2 et Router3 qui représentent les routeurs de saut suivants R1, R2 et R3.
2. Créez le serveur virtuel LLB1 d'équilibrage de charge de liaison et liez les services Router1, Router2 et Router3 à celui-ci.
3. Créer PBRS PBR1 et PBR2, avec les champs de saut suivant définis comme LLB1 et 2.2.2.254 (adresse IP du routeur R2), respectivement.

Pour créer un service à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add service <name> <IP> <serviceType> <port>
- show service <name>

Exemple :

```
1 > add service Router1 1.1.1.254 ANY *
2  Done
3 > add service Router2 2.2.2.254 ANY *
4  Done
5 > add service Router3 3.3.3.254 ANY *
6  Done
7 <!--NeedCopy-->
```

Pour créer un service à l'aide de l'interface graphique :

Accédez à Gestion du trafic > Équilibrage de charge > Serviceset créez un service.

Pour créer un serveur virtuel d'équilibrage de charge de liaison et lier un service à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add lb vserver <name> <serviceType>
- bind lb vserver < name> <serviceName>
- show lb vserver < name>

Exemple :

```
> add lb vserver LLB1 ANY
 Done
> bind lb vserver LLB1 Router1 Router2 Router3
 Done
<!--NeedCopy-->
```

Pour créer un serveur virtuel d'équilibrage de charge de liaison et lier un service à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuelset créez un serveur virtuel pour l'équilibrage de charge des liens. Spécifiez **ANY** dans le champ **Protocole**.
   Remarque : Assurez-vous que
   Directement adressable n'est pas cochée.
2. Sous l'onglet **Services**, dans la colonne **Actif**, activez la case à cocher du service que vous souhaitez lier au serveur virtuel.

Pour créer un PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add ns pbr <name> <action> [-srcIP [<operator>] <srcIPVal>] [-nextHop <nextHopVal>]
- show ns pbr

Exemple :

```
> add pbr PBR1 ALLOW -srcIP 10.102.29.30 -nextHop LLB1
 Done
> add pbr PBR2 ALLOW -srcIP 10.102.29.90 -nextHop 2.2.2.254
 Done
<!--NeedCopy-->
```

Pour créer un PBR à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR, sous l'onglet PBR, ajoutez un nouveau PBR.

Itinéraires basés sur des stratégies (PBR6) pour le trafic IPv6

August 20, 2021

La configuration de PBR6s implique les tâches suivantes :

- Créez un PBR6.
- Appliquer PBR6.
- (Facultatif) Désactivez ou activez un PBR6.
- (Facultatif) Renuméroter la priorité du PBR6.

Création ou modification d'un PBR6

Vous ne pouvez pas créer deux PBR6 avec les mêmes paramètres. Si vous tentez de créer un doublon, un message d'erreur s'affiche.

Vous pouvez configurer la priorité d'un PBR6. La priorité (une valeur entière) définit l'ordre dans lequel l'appliance Citrix ADC évalue les PBR6. Lorsque vous créez un PBR6 sans spécifier de priorité, Citrix ADC attribue automatiquement une priorité qui est un multiple de 10.

Si un paquet correspond à la condition définie par le PBR6, Citrix ADC effectue une action. Si le paquet ne correspond pas à la condition définie par le PBR6, Citrix ADC compare le paquet avec le PBR6 avec la priorité la plus élevée suivante.

Procédures CLI

Pour créer un PBR6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns pbr6** <name> <action> [-srcIPv6 [<operator>] <srcIPv6Val>] [-srcPort [<operator>] <srcPortVal>] [-destIPv6 [<operator>] <destIPv6Val>] [-destPort [<operator>] <destPortVal>] [-srcMac <mac_addr>] [-protocol <protocol> |-protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-state (ENABLED | DISABLED)] [-msr (ENABLED | DISABLED) [-monitor <string>]] [-nextHop <nextHopVal>] [-nextHopVlan <positive_integer>]
- show ns pbr

Pour modifier ou supprimer un PBR6 à l'aide de l'interface de ligne de commande :

Pour modifier un PBR6, tapez la commande **set pbr6** <name> et les paramètres à modifier, avec leurs nouvelles valeurs.

Pour supprimer un ou tous les PBR6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- **rm ns pbr6** <name>
- **clear ns pbr6**

Procédures GUI

Pour créer ou modifier un PBR6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR et, sous l'onglet PBR6s, ajoutez un nouveau PBR6 ou modifiez un PBR6 existant.

Pour supprimer un ou tous les PBR6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR et, sous l'onglet PBR6s, supprimez le PBR6.

Application des PBR6

Vous devez appliquer un PBR6 pour l'activer. La procédure suivante réapplique tous les PBR6 que vous n'avez pas désactivés. Les PBR6s constituent une arborescence de mémoire (table de recherche). Par exemple, si vous créez 10 PBR6s (p6_1 - p6_10), puis que vous créez un autre PBR6 (p6_11) et l'appliquez, tous les PBR6s (p6_1 - p6_11) sont fraîchement appliqués et une nouvelle table de recherche est créée. Si une session est associée à un DENY PBR6, la session est détruite.

Vous devez appliquer cette procédure après chaque modification apportée à un PBR6. Par exemple, vous devez suivre cette procédure après avoir désactivé un PBR6.

Remarque : les PBR6 créés sur l'appliance Citrix ADC ne fonctionnent pas tant qu'ils ne sont pas appliqués.

Pour appliquer des PBR6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **apply ns PBR6**

Pour appliquer des PBR6 à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > PBR.
2. Sous l'onglet PBR6s, sélectionnez le PBR6, dans la liste Action, sélectionnez Appliquer.

Activation ou désactivation d'un PBR6

Par défaut, les PBR6 sont activés. Cela signifie que lorsque des PBR6 sont appliqués, l'appliance Citrix ADC compare automatiquement les paquets IPv6 sortants aux PBR6 configurés. Si un PBR6 n'est pas requis dans la table de recherche, mais qu'il doit être conservé dans la configuration, il doit être désactivé avant l'application des PBR6. Une fois les PBR6 appliqués, Citrix ADC ne compare pas les paquets entrants avec les PBR6 désactivés.

Pour activer ou désactiver un PBR6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- **enable ns pbr** <name>

- **disable ns pbr** <name>

Pour activer ou désactiver un PBR6 à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > PBR.
2. Sous l'onglet PBR6s, sélectionnez le PBR6, dans la liste Action, sélectionnez Activer ou Désactiver.

Renumérotation des PBR6s

Vous pouvez automatiquement renuméroter les PBR6 pour définir leurs priorités à des multiples de 10.

Pour renuméroter les PBR6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **renumber ns pbr6**

Pour renuméroter les PBR6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR, sous l'onglet PBR6s, dans la liste Action, sélectionnez Renuméroter les priorités.

Masque générique d'adresse MAC pour PBR

August 20, 2021

Un paramètre de masque générique a été introduit pour les PBR étendus et PBR6 et est utilisé avec le paramètre d'adresse MAC source pour définir une plage d'adresses MAC à comparer avec l'adresse MAC source des paquets sortants.

Les masques génériques spécifient quels chiffres hexadécimaux de l'adresse MAC sont utilisés et quels chiffres hexadécimaux sont ignorés. Le paramètre de masque générique spécifie une série de 1 et de zéros et a une longueur de 12 chiffres. Chaque chiffre est un masque pour le chiffre hexadécimal correspondant de l'adresse MAC. Un chiffre zéro dans le masque générique indique que le chiffre hexadécimal correspondant de l'adresse MAC doit être pris en compte et un chiffre indique que le chiffre hexadécimal correspondant doit être ignoré.

Le masque générique doit répondre aux conditions suivantes :

- A seulement une série de zéros
- A seulement une série de uns
- Commencer par une série de zéros

Voici quelques exemples de masques génériques valides :

- 000000111111
- 000000011111
- 000011111111

Voici quelques exemples de masques génériques non valides :

- 000000111100
- 111110000000
- 010101010101

Pour une règle PBR, un masque générique 000000111111 pour l'adresse MAC 96:fa : 95:1 d : 67:4 a définit la plage d'adresses MAC 96:FA : 95:00:00:00 - 96:FA:95:FF:FF. Cette plage d'adresses MAC est mise en correspondance avec l'adresse MAC source des paquets sortants.

Pour spécifier une plage d'adresses MAC source dans une règle PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns pbr** <name> <action> -**srcMac** <mac_addr> -**srcMacMask** <string>
- **show ns pbr** <pbrname>

Exemple :

```
1 > add ns pbr PBR-1 ALLOW -srcip 192.0.2.34 -srcMac 96:fa:95:1d:67:4a
      - srcMacMask 000000111111 -nexthop 198.51.100.1
2
3  Done
```

Pour spécifier une plage d'adresses MAC source dans une règle PBR6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns pbr6** <name> <action> -**srcMac** <mac_addr> -**srcMacMask** <string>
- **show pbr6** <pbr6name>

Exemple :

```
1 > add ns pbr6 PBR6-1 ALLOW  - srcipv6 2001:db8:0::7 -srcMac 96:fa:95:1d
     :67:4a   - srcMacMask 000000001111 -nexthop 2001:db8:0::1
2  Done
```


Utilisation d'itinéraires basés sur une stratégie NULL pour supprimer des paquets sortants

October 5, 2021

Certaines situations peuvent exiger que l'appliance Citrix ADC supprime des paquets sortants spécifiques au lieu de les router, par exemple dans des cas de test et pendant la migration du déploiement.

Les routes basées sur la stratégie NULL peuvent être utilisées pour supprimer des paquets sortants spécifiques. Un PBR NULL est un type de PBR dont le paramètre nexthop est défini sur NULL. L'appliance Citrix ADC supprime les paquets sortants qui correspondent à un PBR NULL.

Configuration des PBR NULL pour les paquets IPv4

Pour créer un PBR NULL à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns pbr** <name> ALLOW [**-td** <positive_integer>] [-**srcIP** [<operator>] <srcIPVal>] [-**srcPort** [<operator>] <srcPortVal>] [-**destIP** [<operator>] <destIPVal>] [-**destPort** [<operator>] <destPortVal>] (-**nextHop NULL**) [**srcMac** <mac_addr> [-**srcMacMask** <string>]] [-**protocol** <protocol> | -**protocolNumber** <positive_integer>] [-**vlan** <positive_integer> | -**vxlan** <positive_integer>] [-**interface** <interface_name>] [-**priority** <positive_integer>] [-**msr** (**ENABLED** | **DISABLED**) [-**monitor** <string>]] [-**state** (**ENABLED** | **DISABLED**)[-**ownerGroup** <string>]
- **apply ns pbrs**
- **show ns pbr**<id>

Pour configurer un PBR NULL à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **PBR**, sous l'onglet **PBR**, ajoutez un **nouveau PBR NULL** ou modifiez un PBR NULL existant.

Exemple de configuration

Dans l'exemple de configuration suivant, NULL PBR6 PBR6-NULL-EXAMPLE-1 est configuré pour supprimer tous les paquets IPv6 sortants de l'interface 1/5.

```
1 > add ns pbr PBR6-NULL-EXAMPLE-1 ALLOW  - nextHop NULL -interface 1/5
2  Done
3
4 > apply ns pbr6
5  Done
```


Distribution du trafic sur plusieurs routes en fonction des informations de cinq tuples

January 21, 2021

Dans une configuration d'équilibrage de charge, une appliance Citrix ADC peut disposer de plusieurs itinéraires pour envoyer un paquet vers sa destination. Par exemple : à un serveur et à un client.

Une appliance Citrix ADC utilise un algorithme de hachage pour sélectionner une route pour envoyer le paquet à sa destination.

L'algorithme de hachage utilise les deux tuples suivants d'un paquet pour calculer un hachage, sur la base duquel l'appliance Citrix ADC sélectionne une route pour le paquet.

- Adresse IP source
- Adresse IP de destination

La sélection des itinéraires basée sur deux informations tuples peut entraîner une répartition inégale du trafic sur les itinéraires disponibles. Cette répartition inégale du trafic entraîne une surcharge du trafic sur certains itinéraires.

Pour résoudre ce problème, à partir de la version 13.0 71.x, l'appliance Citrix ADC utilise les informations suivantes sur les cinq tuples d'un paquet dans l'algorithme de hachage pour sélectionner une route pour le paquet :

- Adresse IP source (IP du client)
- Port source (port client)
- Adresse IP de destination (IP de service)
- Port de destination (port de service)
- Numéro du protocole

La sélection des itinéraires basée sur cinq informations tuples assure une répartition uniforme du trafic sur les itinéraires disponibles. Cette répartition uniforme du trafic empêche la surcharge du trafic sur un itinéraire.

Prenons un exemple de configuration d'équilibrage de charge où un client envoie une demande à l'adresse VIP. L'appliance Citrix ADC utilise les cinq informations tuples suivantes pour sélectionner une route pour envoyer le paquet de demande au serveur équilibré de charge :

- Adresse IP source (adresse IP du client)
- Port source (port client)
- Adresse IP de destination (adresse IP du service)
- Port de destination (numéro de port de service)
- Numéro du protocole

Priorité concernant les autres fonctionnalités Citrix ADC basées sur la sélection d'itinéraires

Cette section traite de la priorité de la sélection d'itinéraires basée sur la fonctionnalité cinq tuples et d'autres fonctionnalités liées à la sélection d'itinéraires dans une appliance Citrix ADC.

- **Itinéraires basés sur des stratégies (PBR)**. Les règles PBR ont toujours priorité sur la sélection d'itinéraires basée sur cinq tuples.
- **Transfert basé sur Mac (MBF)**. Dans une configuration d'équilibrage de charge, la sélection MBF ou d'itinéraire basée sur cinq tuples a priorité dans les cas suivants :
  - Pour un trafic initié par un client vers l'adresse VIP de la configuration d'équilibrage de charge dans l'appliance Citrix ADC :
    * Demande de trafic destiné à un serveur équilibré de charge. La sélection d'itinéraires basée sur cinq tuples prend la préférence sur MBF.
    * Trafic de réponse destiné au client. MBF prend la préférence sur la sélection d'itinéraires basée sur cinq tuples.
  - Pour un trafic initié par le serveur vers l'adresse SNIP dans l'appliance Citrix ADC :
    * Trafic de réponse destiné au client. La sélection d'itinéraires basée sur cinq tuples prend la préférence sur MBF.
    * Demande de trafic destiné à un serveur équilibré de charge. MBF prend la préférence sur la sélection d'itinéraires basée sur cinq tuples.

Résolution des problèmes de routage

January 21, 2021

Pour rendre votre processus de dépannage aussi efficace que possible, commencez par recueillir des informations sur votre réseau. Vous devez obtenir les informations suivantes sur l'appliance Citrix ADC et les autres systèmes du réseau :

- Diagramme topologique complet, y compris la connectivité de l'interface et les détails des commutateurs intermédiaires.
- Exécution de la configuration. Vous pouvez utiliser la commande show running pour obtenir la configuration en cours d'exécution pour ns.conf et ZebOSs.conf.
- Sortie de la commande Historique, pour déterminer si des modifications de configuration ont été apportées lorsque le problème est survenu.
- Sortie des commandes Top et ps -ax, pour déterminer si un démon de routage utilise le CPU ou se comporte mal.
- Tous les fichiers de base associés au routage dans /var/core - nsm, bgdd, ospfd ou ripd. Vérifiez l'horodatage pour voir s'ils sont pertinents.

- dr_error.log et dr_info.log fichiers de /var/log.
- Sortie de la commande de date et des détails d'heure pour tous les systèmes pertinents. Imprimez les dates sur tous les appareils les uns après les autres, de sorte que les heures sur les messages du journal puissent être corrélées avec divers événements.
- Ns.log pertinent, fichiers newnslog.
- Fichiers de configuration, fichiers journaux et détails de l'historique des commandes des routeurs en amont et en aval.

FAQ sur le routage générique

January 21, 2021

Les utilisateurs ont généralement les questions suivantes sur la façon de résoudre les problèmes de routage génériques :

- Comment enregistrer les fichiers de configuration ?

  La commande write de VTYSH enregistre uniquement ZebOSs.conf. Exécutez la commande save ns config à partir de la CLI pour enregistrer les fichiers ns.conf et ZebOSs.conf.

- Si j'ai configuré à la fois un itinéraire statique par défaut et un itinéraire par défaut appris dynamiquement, quelle est la route par défaut préférée ?

  L'itinéraire appris dynamiquement est l'itinéraire par défaut préféré. Ce comportement est unique aux itinéraires par défaut. Toutefois, dans le cas du Network Services Module (NSM), à moins que les distances administratives ne soient modifiées, un itinéraire configuré statiquement dans le RIB est préféré à un itinéraire dynamique. L'itinéraire qui est téléchargé dans la FIB NSM est l'itinéraire statique.

- Comment bloquer la publicité des itinéraires par défaut ?

  La route par défaut n'est pas injectée dans ZebOS.

- Comment afficher la sortie de débogage des démons réseau ?

  Vous pouvez écrire une sortie de débogage à partir de démons réseau dans un fichier en entrant la commande de fichier journal suivante à partir de la vue de configuration globale dans VTYSH :

  ```
  ns(config)# log file /var/ZebOS.log
  <!--NeedCopy-->
  ```

  Vous pouvez diriger la sortie de débogage vers la console en entrant la commande Terminal Monitor à partir de la vue utilisateur VTYSH :

  ```
  ns# terminal monitor
  ```



```
<!--NeedCopy-->
```

- Comment collecter les cœurs de démons en cours d'exécution ?

  Vous pouvez utiliser l'utilitaire gcore pour collecter les cœurs de démons en cours d'exécution pour traitement par gdb. Cela peut être utile pour déboguer des démons qui se comportent mal sans mettre l'ensemble de l'opération de routage à l'arrêt.

```
gcore [-s] [-c core] [executable] pid
<!--NeedCopy-->
```

  L'option -s arrête temporairement le démon lors de la collecte de l'image principale. Il s'agit d'une option recommandée, car elle garantit que l'image résultante affiche le noyau dans un état cohérent.

```
root@ns#gcore -s -c nsm.core /netscaler/nsm 342
<!--NeedCopy-->
```

- Comment exécuter un lot de commandes ZebOSS ?

  Vous pouvez exécuter un lot de commandes ZebOSS à partir d'un fichier en entrant la commande VTYSH -f <file-name>. Cela ne remplace pas la configuration en cours d'exécution, mais y ajoute. Toutefois, en incluant des commandes pour supprimer la configuration existante dans le fichier de commandes, puis en ajoutant celles pour la nouvelle configuration souhaitée, vous pouvez utiliser ce mécanisme pour remplacer une configuration spécifique :

```
!
router bgp 234
network 1.1.1.1 255.255.255.0
!
route-map bgp-out2 permit 10
 set metric 9900
 set community 8602:300
!
<!--NeedCopy-->
```

Dépannage des problèmes spécifiques à OSPF

January 21, 2021

Avant de commencer à déboguer un problème spécifique à OSPF, vous devez collecter des informations à partir de l'appliance Citrix ADC et de tous les systèmes du réseau local concerné, y compris les routeurs en amont et en aval. Pour commencer, entrez les commandes suivantes :

1. show interface from both nscli and VTYSH
2. show ip ospf interface
3. show ip ospf neighbor detail
4. show ip route
5. show ip ospf route
6. show ip ospf database summary
    - S'il n'y a que quelques LSAs dans la base de données, entrez show ip ospf database routeur, show ip ospf database A. network, show ip ospf database externe, et d'autres commandes pour obtenir tous les détails des LSAs.
    - S'il y a un grand nombre de LSA dans la base de données, entrez la commande d'auto-origine show ip ospf database.
7. show ip ospf
8. show ns ip. Cela garantit que les détails de tous les dignités d'intérêt sont inclus.
9. Obtenez les journaux des périphériques d'appairage et exécutez la commande suivante :

    ```
    gcore -s -c xyz.core /netscaler/ospfd <pid>
    ```

    Remarque : La commande gcore n'est pas perturbatrice.

Collectez des informations supplémentaires à partir de Citrix ADC comme suit :

1. Activez la journalisation des messages d'erreur en entrant la commande suivante à partir de la vue de configuration globale dans VTYSH :

    ```
    ns(config)# log file /var/ospf.log
    <!--NeedCopy-->
    ```

2. Activez le débogage des événements ospf et enregistrez-les à l'aide de la commande suivante :

    ```
    ns(config) #log file /var/ospf.log
    <!--NeedCopy-->
    ```

    Activer le paquet debug ospf lsa uniquement si le nombre de LSA dans la base de données est relativement faible (< 500).

Protocole Internet version 6 (IPv6)

August 20, 2021

Une appliance Citrix ADC prend en charge IPv6 côté serveur et côté client et peut donc fonctionner comme un nœud IPv6. Il peut accepter des connexions à partir de nœuds IPv6 (hôtes et routeurs) et de nœuds IPv4, et peut effectuer la traduction de protocole (RFC 2765) avant d'envoyer du trafic aux services.

Le tableau suivant répertorie certaines des fonctionnalités IPv6 prises en charge par l'appliance Citrix ADC.

Tableau 1. Certaines fonctionnalités IPv6 prises en charge

Fonctionnalités IPv6
Adresses IPv6 pour SNIP (NSIP6, VIP6 et SNIP6)
Découverte des voisins (résolution d'adresses, détection d'adresses dupliquées, détection d'inaccessibilité des voisins, découverte du routeur)
Applications de gestion (ping6, telnet6, ssh6)
Routage statique et routage dynamique (OSPF, BGP, Ripng et ISIS)
VLAN basés sur le port
Listes de contrôle d'accès pour les adresses IPv6 (ACL6)
Protocoles IPv6 (TCP6, UDP6, ICMP6)
Prise en charge côté serveur (adresses IPv6 pour vservers, services)
USIP (Use source IP) et DSR (Direct Server Return) pour IPv6
SNMP et CVPN pour IPv6
HA avec adresse de nœud IPv6 natif
Adresses IPv6 pour les MIP
Découverte Path-MTU pour IPv6

Mise en œuvre de la prise en charge IPv6

Vous devez activer la fonctionnalité IPv6 sur une appliance Citrix ADC avant de pouvoir l'utiliser ou la configurer. Si IPv6 est désactivé, le Citrix ADC ne traite pas les paquets IPv6. Il affiche l'avertissement suivant lorsque vous exécutez une commande non prise en charge :

```
"Warning: Feature(s) not enabled [IPv6PT]"
<!--NeedCopy-->
```

Utilisez l'une des procédures suivantes pour activer ou désactiver IPv6.

Procédures CLI

Pour activer ou désactiver IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- activer la fonction ns ipv6pt
- désactiver la fonctionnalité ns ipv6pt

Procédures GUI

Pour activer ou désactiver IPv6 à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, dans le groupe **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées** .
2. Sélectionnez ou désactivez l'option de **traduction du protocole IPv6** .

Prise en charge de VLAN

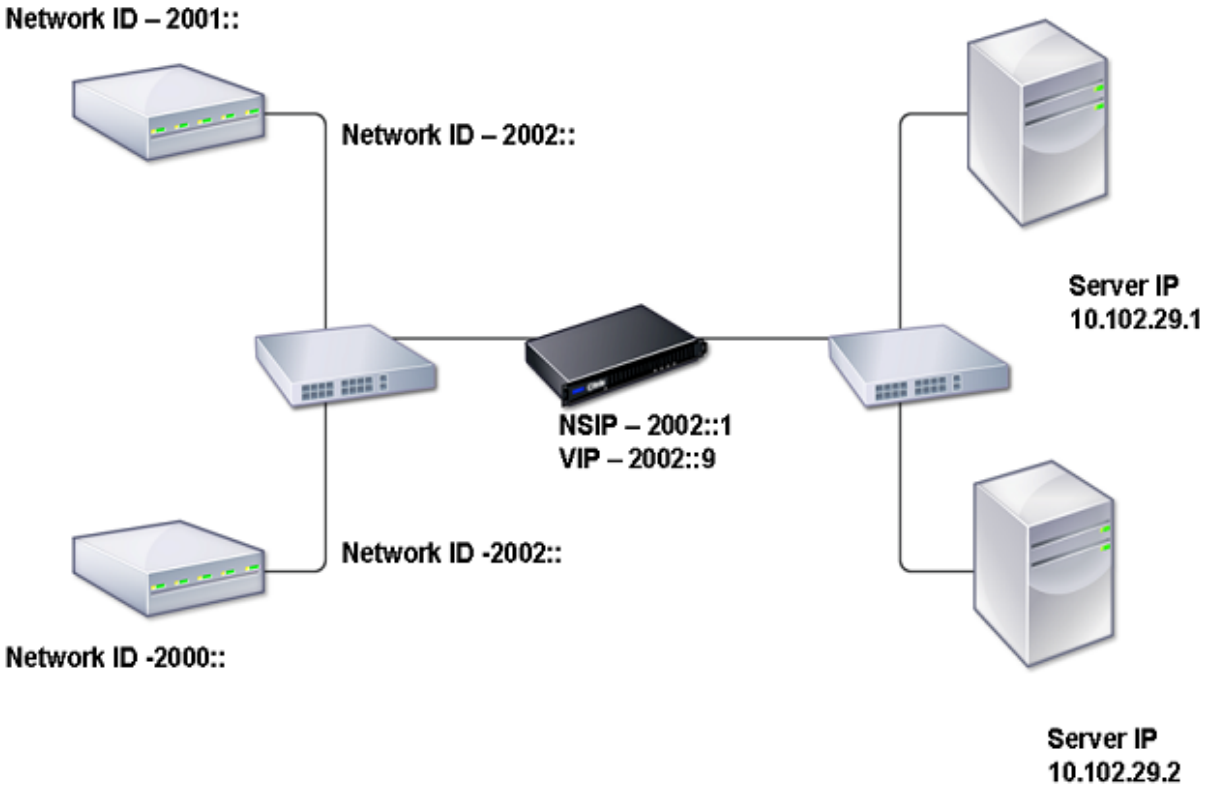
Si vous devez envoyer des paquets de diffusion ou de multidiffusion sans identifier le VLAN (par exemple, pendant DAD pour NSIP ou ND6 pour le prochain saut de la route), vous pouvez configurer l'appliance Citrix ADC pour qu'elle envoie le paquet sur toutes les interfaces avec le balisage approprié. Le VLAN est identifié par ND6 et un paquet de données est envoyé uniquement sur le VLAN. Pour plus d'informations sur ND6 et les VLAN, voir Configuration de la découverte de voisins.

Les VLAN basés sur les ports sont courants pour IPv4 et IPv6. Les VLAN basés sur préfixe sont pris en charge pour IPv6.

Scénario de déploiement simple

Voici un exemple de configuration simple d'équilibrage de charge consistant en un vserver IPv6 et des services IPv4, comme illustré dans le diagramme topologique suivant.

Figure 1. Exemple de topologie IPv6



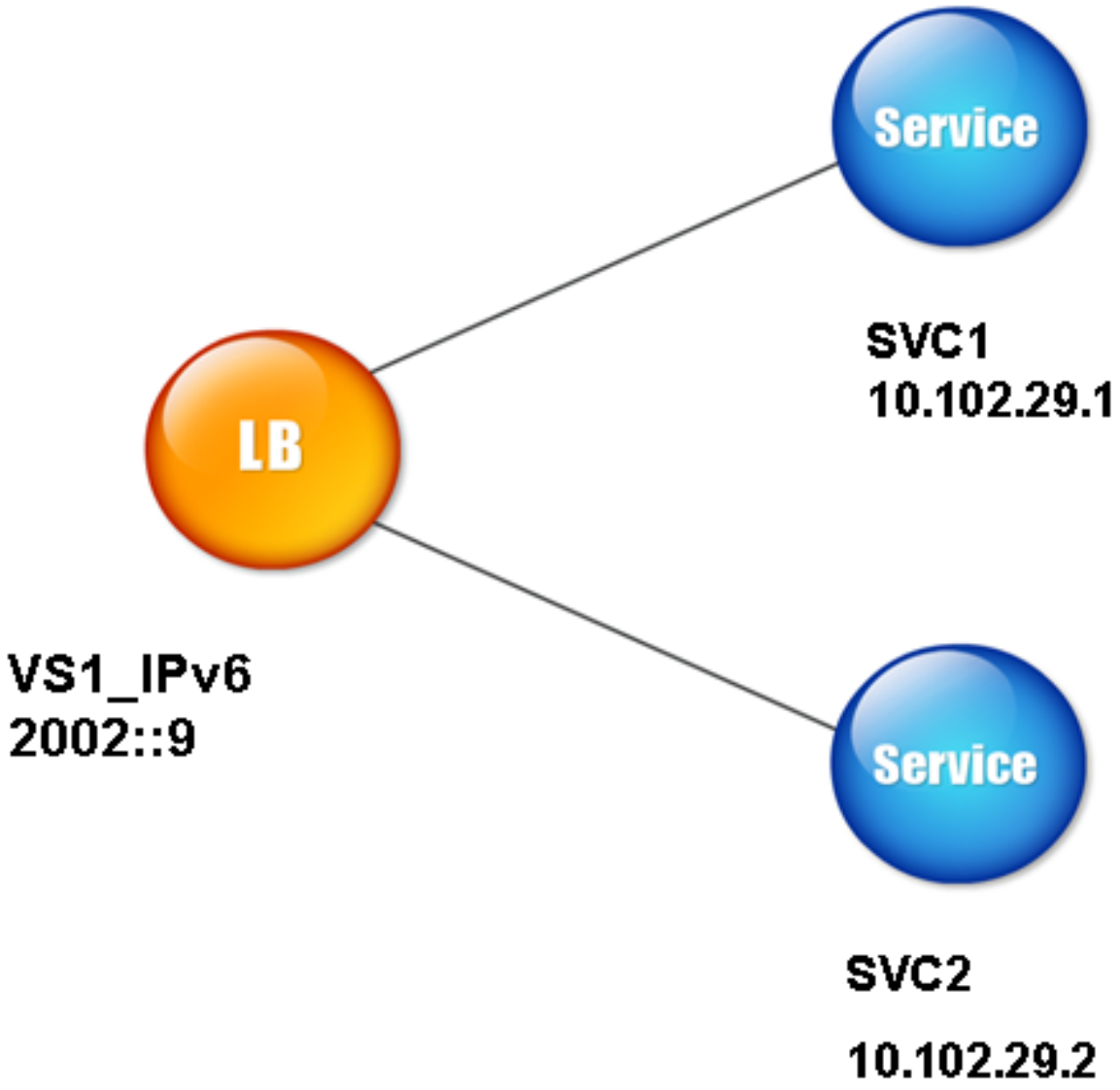
Le tableau suivant récapitule les noms et les valeurs des entités qui doivent être configurées sur Citrix ADC.

Tableau 2. Exemples de valeurs pour la création d'entités

Type d'entité	Nom	Valeur
Serveur serveur LB	VS1_IPv6	2002::9
Services	SVC1	10.102.29.1
	SVC2	10.102.29.2

La figure suivante montre les entités et les valeurs des paramètres à configurer sur Citrix ADC.

Figure 2. Diagramme d'entités IPv6



Pour configurer ce scénario de déploiement, vous devez effectuer les opérations suivantes :

1. Créez un service IPv6.
2. Créez un vserver IPv6 LB.
3. Liez les services au vserver.

Procédures CLI

Pour créer des services IPv4 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add service** <Name> <IPAddress> <Protocol> <Port>
- **sh service** <Name>

Exemple :

```
> add service SVC1 10.102.29.1 HTTP 80
Done

>add service SVC2 10.102.29.2 HTTP 80
Done
<!--NeedCopy-->
```

Pour créer un vserver IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add lb vserver** <Name> <IPAddress> <Protocol> <Port>
- **sh lb vserver** <Name>

Exemple :

```
> add lb vserver VS1_IPv6 2002::9 HTTP 80
Done
<!--NeedCopy-->
```

Pour lier un service à un serveur LB vserver à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **bind lb vserver** <name> <service>
- **sh lb vserver** <name>

Exemple :

```
> bind lb vserver VS1_IPv6 SVC1
Done
<!--NeedCopy-->
```

Procédures GUI

Pour créer des services IPv4 à l'aide de l'interface graphique :

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, cliquez sur **Ajouter**, puis définissez les paramètres suivants :

- Nom du service
- Adresse IP
- Protocole

- Port

Pour créer un vserver IPv6 à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, cliquez sur **Ajouter** et activez la case à cocher **IPv6** .
2. Définissez les paramètres suivants :
   - Nom
   - Protocole
   - Type d'adresse IP
   - Adresse IP
   - Port

Pour lier un service à un serveur LB vserver à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans la page **Serveurs virtuels d'équilibrage** de charge, sélectionnez le vserver pour lequel vous souhaitez lier le service (par exemple, vs1_IPv6).
3. Cliquez sur **Ouvrir**.
4. Dans la boîte de dialogue **Configurer le serveur virtuel (équilibrage de charge)**, sous l'onglet **Services**, activez la case à cocher **Active** correspondant au service que vous souhaitez lier au serveur vserver (par exemple, SVC1).
5. Cliquez sur **OK**.
6. Répétez les étapes 1 à 4 pour lier le service (par exemple, SVC2 au vserver).

Modification de l'en-tête de l'hôte

Lorsqu'une requête HTTP contient une adresse IPv6 dans l'en-tête de l'hôte et que le serveur ne comprend pas l'adresse IPv6, vous devez mapper l'adresse IPv6 à une adresse IPv4. L'adresse IPv4 est ensuite utilisée dans l'en-tête hôte de la requête HTTP envoyée au vserver.

Procédures CLI

Pour modifier l'adresse IPv6 dans l'en-tête de l'hôte en adresse IPv4 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set ns ip6** <IPv6Address> -**map** <IPAddress>
- **sh ns ip6** <IPv6Address>

Exemple :

```
1 > set ns ip6 2002::9 -map 200.200.200.200
2 Done
```



```
<!--NeedCopy-->
```

Procédures GUI

Pour modifier l'adresse IPv6 dans l'en-tête de l'hôte en adresse IPv4 à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IP** et, sous l'onglet **IPv6s**, sélectionnez l'adresse IP pour laquelle vous souhaitez configurer une adresse IP mappée, par exemple, 2002:0:0:0:0:0:0:9, puis cliquez sur Modifier.
2. Dans la zone de texte **IP mappée**, tapez l'adresse IP mappée que vous souhaitez configurer, par exemple 200.200.200.200.

Insertion VIP

Si une adresse IPv6 est envoyée à un serveur IPv4, le serveur peut ne pas comprendre l'adresse IP dans l'en-tête HTTP et peut générer une erreur. Pour éviter cela, vous pouvez mapper une adresse IPv4 au VIP IPv6. Ensuite, vous pouvez activer l'insertion VIP pour activer l'insertion de l'adresse VIP IPv4 et du numéro de port dans les requêtes HTTP envoyées aux serveurs.

Procédures CLI

Pour configurer une adresse IPv6 de carte à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

set ns ip6 <IPv6Address> -**map** <IPAddress>

Exemple :

```
> set ns ip6 2002::9 -map 200.200.200.200
 Done
<!--NeedCopy-->
```

Pour activer l'insertion VIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set lb vserver** <name> -**insertVserverIPPort** <Value>
- **sh lb vserver** <name>

Exemple :

```
> set lb vserver VS1_IPv6 -insertVserverIPPort ON
 Done

<!--NeedCopy-->
```


Procédures GUI

Pour configurer une adresse IPv6 de carte à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IP**, sous l'onglet **IPv6s**, sélectionnez l'adresse IP pour laquelle vous souhaitez configurer une adresse IP de mappage, par exemple, 2002:0:0:0:0:0:0:9, puis cliquez sur **Modifier**.
2. Dans la zone de texte **IP mappée**, tapez l'adresse IP du mappage que vous souhaitez configurer, par exemple 200.200.200.200.

Pour activer l'insertion VIP à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez le serveur virtuel que vous souhaitez activer l'insertion de port, puis cliquez sur **Modifier** .
2. Dans l'onglet **Avancé**, sous **Paramètres de trafic**, dans la zone de liste déroulante **Insertion de port IP Vserver**, sélectionnez **VIPADDR** .
3. Dans la zone de texte **Insertion de port IP Vserver**, tapez l'en-tête vip.

Domaines de trafic

October 5, 2021

> **Avertissement**
>
> Citrix vous recommande d'utiliser les partitions d'administration au lieu d'utiliser les domaines de trafic. Pour plus d'informations, consultez la page Partitionnement administrateur .

Les domaines de trafic sont un moyen de segmenter le trafic réseau pour différentes applications. Vous pouvez utiliser des domaines de trafic pour créer plusieurs environnements isolés au sein d'une appliance Citrix ADC. Une application appartenant à un domaine de trafic spécifique communique avec les entités et traite le trafic au sein de ce domaine. Le trafic appartenant à un domaine de trafic ne peut pas franchir la limite d'un autre domaine de trafic.

Avantages de l'utilisation de Traffic Domains

Les principaux avantages de l'utilisation des domaines de trafic sur une appliance Citrix ADC sont les suivants :

- **Utilisation d'adresses IP dupliquées dans un réseau**. Les domaines de trafic vous permettent d'utiliser une adresse IP en double sur le réseau. Vous pouvez attribuer la même adresse IP ou la même adresse réseau à plusieurs appareils sur un réseau, ou à plusieurs entités sur un dispositif Citrix ADC, à condition que chacune des adresses dupliquées appartienne à un domaine de trafic différent.

- **Utilisation d'entités dupliquées sur l'appliance Citrix ADC**. Les domaines de trafic vous permettent également d'utiliser des entités de fonctionnalités Citrix ADC dupliquées sur l'appliance. Vous pouvez créer des entités avec les mêmes paramètres tant que chaque entité est affectée à un domaine de trafic distinct.
  Remarque : les entités dupliquées portant le même nom ne sont pas prises en charge.
- **Multilocation**. À l'aide des domaines de trafic, vous pouvez fournir des services d'hébergement à plusieurs clients en isolant le type de trafic applicatif de chaque client dans un espace d'adressage défini sur le réseau.

Un domaine de trafic est identifié de manière unique par un identifiant, qui est une valeur entière. Chaque domaine de trafic nécessite un VLAN ou un ensemble de VLAN. La fonctionnalité d'isolation du domaine de trafic dépend des VLAN liés au domaine de trafic. Plusieurs VLAN peuvent être liés à un domaine de trafic, mais le même VLAN ne peut pas faire partie de plusieurs domaines de trafic. Par conséquent, le nombre maximal de domaines de trafic pouvant être créés dépend du nombre de VLAN configurés sur l'appliance.

Domaine de trafic par défaut

Une appliance Citrix ADC possède un domaine de trafic préconfiguré, appelé *domaine de trafic par défaut*, dont l'ID est 0. Tous les paramètres et configurations d'usine font partie du domaine de trafic par défaut. Vous pouvez créer d'autres domaines de trafic, puis segmenter le trafic entre le domaine de trafic par défaut et chacun des autres domaines de trafic. Vous ne pouvez pas supprimer le domaine de trafic par défaut de l'appliance Citrix ADC. Toute entité d'entité que vous créez sans définir l'ID du domaine de trafic est automatiquement associée au domaine de trafic par défaut.

Remarque : Certaines fonctionnalités et configurations sont prises en charge uniquement dans le domaine de trafic par défaut. Ils ne fonctionnent pas dans les domaines de trafic autres que ceux par défaut. Pour obtenir la liste des fonctionnalités prises en charge dans tous les domaines de trafic, consultez Fonctions Citrix ADC prises en charge dans les domaines de trafic.

Fonctionnement des domaines de trafic

Pour illustrer les domaines de trafic, prenons un exemple dans lequel deux domaines de trafic, avec les ID 1 et 2, sont configurés sur l'appliance Citrix ADC NS1.

Dans le domaine de trafic 1, le serveur virtuel d'équilibrage de charge LBVS-TD1 est configuré pour équilibrer la charge du trafic entre les serveurs S1 et S2. Sur l'appliance Citrix ADC, les serveurs S1 et S2 sont représentés par les services SVC1-TD1 et SVC2-TD1, respectivement. Les serveurs S1 et S2 sont connectés à NS1 via le commutateur L2 SW2-TD1. Le client CL-TD1 se trouve sur un réseau privé connecté à NS1 via le commutateur L2 SW1-TD1. SW1-TD1 et SW2-TD1 sont connectés au VLAN 2 de

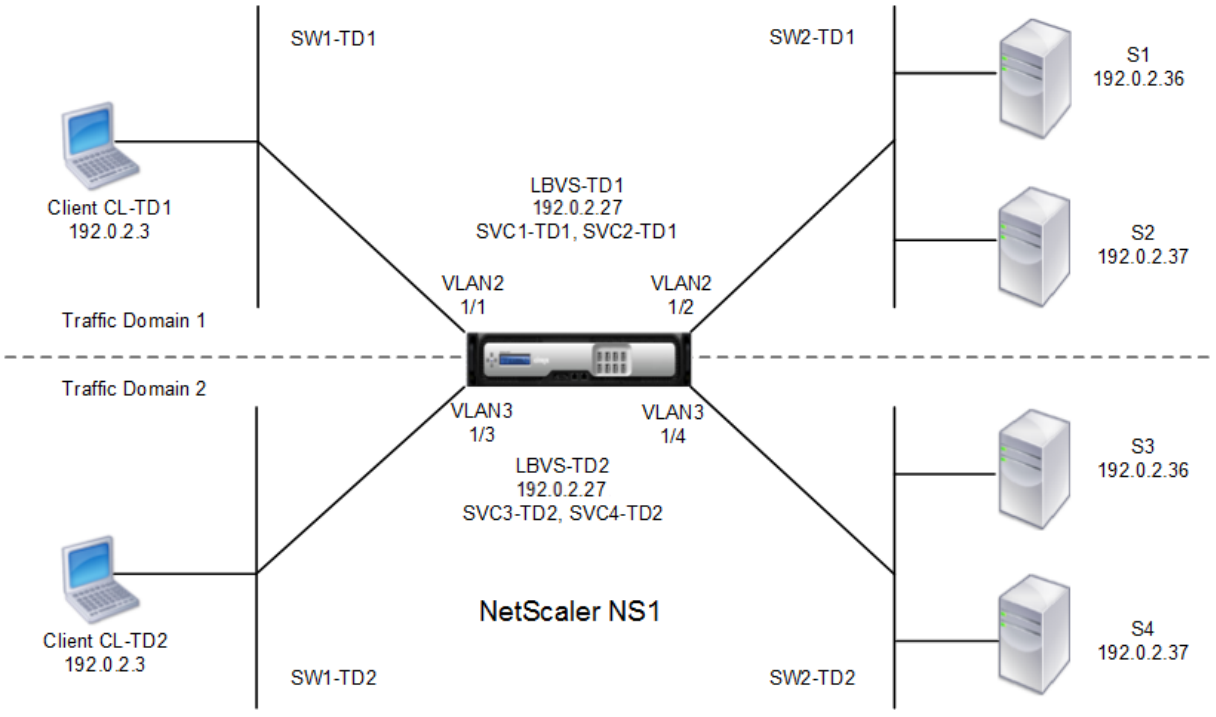
NS1. Le VLAN 2 est lié au domaine de trafic 1, ce qui signifie que le client CL-TD1 et les serveurs S1 et S2 font partie du domaine de trafic 1.

De même, dans le domaine de trafic 2, le serveur virtuel d'équilibrage de charge LBVS-TD2 est configuré pour équilibrer la charge du trafic entre S3 et S4. Sur l'appliance Citrix ADC, les serveurs S3 et S4 sont représentés par les services SVC3-TD2 et SVC4-TD2, respectivement. Les serveurs S3 et S4 sont connectés à NS1 via le commutateur L2 SW2-TD2. Le client CL-TD2 se trouve sur un réseau privé connecté à NS1 via le commutateur L2 SW1-TD2. SW1-TD2 et SW2-TD2 sont connectés au VLAN 3 de NS1. Le VLAN 3 est lié au domaine de trafic 2, ce qui signifie que le client CL-TD2 et les serveurs S3 et S4 font partie du domaine de trafic 2.

Sur l'appliance Citrix ADC, les entités LBVS-TD1 et LBVS-TD2 partagent les mêmes paramètres, y compris l'adresse IP. Il en va de même pour SVC1-TD1 et SVC3-TD2, ainsi que pour SVC2-TD1 et SVC4-TD2. Cela est possible car ces entités se trouvent dans des domaines de trafic différents.

De même, les serveurs S1 et S3, S2 et S4 partagent la même adresse IP, et les clients CL-TD1 et CL-TD2 ont chacun la même adresse IP.

Figure 1. Fonctionnement des domaines de trafic



Le tableau suivant répertorie les paramètres utilisés dans l'exemple.

Entité	Nom	Détails
Paramètres du domaine de trafic 1		

Entité	Nom	Détails
VLAN liés au domaine de trafic 1	VLAN 2	ID VLAN : 2 interfaces liées : 1/1, 1/2
Client connecté à TD1	CL-TD1 (à titre de référence uniquement)	Adresse IP : 192.0.2.3
Serveur virtuel d'équilibrage de charge dans TD1	LBVS-TD1	Adresse IP : 192.0.2.27
Service lié au serveur virtuel LBVS-TD1	SVC1-TD1	Adresse IP : 192.0.2.36
Service lié au serveur virtuel LBVS-TD1	SVC2-TD1	Adresse IP : 192.0.2.37
SNIP	SNIP-TD1 (à des fins de référence uniquement)	Adresse IP : 192.0.2.27
Paramètres du domaine de trafic 2		
VLAN lié au domaine de trafic 2	VLAN 3	ID VLAN : 3 interfaces liées : 1/3, 1/4
Client connecté à TD2	CL-TD2 (à titre de référence uniquement)	Adresse IP : 192.0.2.3
Serveur virtuel d'équilibrage de charge dans TD2	LBVS-TD2	Adresse IP : 192.0.2.27
Service lié au serveur virtuel LBVS-TD2	SVC3-TD2	Adresse IP : 192.0.2.36
Service lié au serveur virtuel LBVS-TD2	SVC4-TD2	Adresse IP : 192.0.2.37
SNIP dans TD2	SNIP-TD2 (à des fins de référence uniquement)	Adresse IP : 192.0.2.29

Voici le flux de trafic dans le domaine de trafic 1 :

1. Le client CL-TD1 diffuse une demande ARP pour l'adresse IP 192.0.2.27 via le commutateur L2 SW1-TD1.
2. La demande ARP atteint NS1 sur l'interface 1/1, qui est liée au VLAN 2. Étant donné que le VLAN 2 est lié au domaine de trafic 1, NS1 met à jour la table ARP du domaine de trafic 1 pour l'adresse IP du client CL-TD1.
3. Étant donné que la demande ARP est reçue sur le domaine de trafic 1, NS1 recherche une entité

configurée sur le domaine de trafic 1 dont l'adresse IP est 192.0.2.27. NS1 détecte qu'un serveur virtuel d'équilibrage de charge LBVS-TD1 est configuré sur le domaine de trafic 1 et possède l'adresse IP 192.0.2.27.

4. NS1 envoie une réponse ARP avec l'adresse MAC de l'interface 1/1.
5. La réponse ARP atteint CL-TD1. CL-TD1 met à jour sa table ARP pour l'adresse IP de LBVS-TD1 avec l'adresse MAC de l'interface 1/1 de NS1.
6. Le client CL-TD1 envoie une demande à 192.0.2.27. La demande est reçue par LBVS-TD1 sur le port 1/1 de NS1.
7. L'algorithme d'équilibrage de charge de LBVS-TD1 sélectionne le serveur S2, et NS1 ouvre une connexion entre un SNIP dans le domaine de trafic 1 (192.0.2.27) et S2.
8. S2 répond à SNIP 192.0.2.27 sur NS1.
9. NS1 envoie la réponse de S2 au client CL-TD1.

Voici le flux de trafic dans le domaine de trafic 2 :

1. Le client CL-TD2 diffuse une demande ARP pour l'adresse IP 192.0.2.27 via le commutateur L2 SW1-TD2.
2. La demande ARP atteint NS1 sur l'interface 1/3, qui est liée au VLAN 3. Étant donné que le VLAN 3 est lié au domaine de trafic 2, NS1 met à jour l'entrée de la table ARP du domaine de trafic 2 pour l'adresse IP du client CL-TD2, même si une entrée ARP pour la même adresse IP (CL-TD1) est déjà présente dans la table ARP du domaine de trafic 1.
3. Étant donné que la demande ARP est reçue dans le domaine de trafic 2, NS1 recherche dans le domaine de trafic 2 une entité dont l'adresse IP est 192.0.2.27. NS1 constate que le serveur virtuel d'équilibrage de charge LBVS-TD2 est configuré dans le domaine de trafic 2 et possède l'adresse IP 192.0.2.27. NS1 ignore LBVS-TD1 dans le domaine de trafic 1, même s'il possède la même adresse IP que LBVS-TD2.
4. NS1 envoie une réponse ARP avec l'adresse MAC de l'interface 1/3.
5. La réponse ARP atteint CL-TD2. CL-TD2 met à jour son entrée de table ARP pour l'adresse IP de LBVS-TD2 avec l'adresse MAC de l'interface 1/3 de NS1.
6. Le client CL-TD2 envoie une demande à 192.0.2.27. La demande est reçue par LBVS-TD2 sur l'interface 1/3 de NS1.
7. L'algorithme d'équilibrage de charge de LBVS-TD2 sélectionne le serveur S3, et NS1 ouvre une connexion entre un SNIP dans le domaine de trafic 2 (192.0.2.29) et S3.
8. S2 répond à SNIP 192.0.2.29 sur NS1.
9. NS1 envoie la réponse de S2 au client CL-TD2.

Fonctionnalités Citrix ADC prises en charge dans les domaines de trafic

Les fonctionnalités Citrix ADC de la liste suivante sont prises en charge dans tous les domaines de trafic.

> **Important**
>
> Toute fonctionnalité Citrix ADC non répertoriée ci-dessous est prise en charge uniquement dans le domaine de trafic par défaut.

- Table ARP
- Tableau ND6
- Table Bridge
- Tous les types d'adresses IPv4 et IPv6
- Routes IPv4 et IPv6
- ACL et ACL6
- PBR & PBR6
- INAT
- RNAT
- RNAT6
- MSR
- MSR6
- Profils de réseau
- MIB SNMP
- Fragmentation
- Moniteurs (les moniteurs scriptables ne sont pas pris en charge)
- Commutation de contenu
- Redirection de cache
- Persistance (les groupes de persistance ne sont pas pris en charge)
- Service (les services basés sur le domaine ne sont pas pris en charge)
- Groupe de services (les groupes de services basés sur un domaine ne sont pas pris en charge)
- Politiques (*)
- PING
- TRACEROUTE
- PMTU
- Haute disponibilité (la mise en miroir des connexions n'est pas prise en charge)
- Cluster (pris en charge sur les clusters L2. Non pris en charge sur les clusters L3)
- Persistance des cookies
- MSS
- Journalisation (Syslog n'est pas pris en charge)
- Protection contre les surtensions
- Équilibrage de charge (Les types suivants ne sont pas pris en charge :)
  - TFTP
  - RTSP
  - Diameter

  - SIP
  - SMPP
- NAT46
- NAT64
- DNS64
- Règles de transfert de session
- SNMP

> **Remarque**
>
> - * Les stratégies n'ont pas de points de liaison globaux pour les domaines de trafic. Toutefois, les stratégies peuvent être liées à un serveur virtuel d'équilibrage de charge spécifique d'un domaine de trafic.
> - Les fonctionnalités Global Server Loading Balancing (GSLB) et ADNS de Citrix ADC ne connaissent pas les domaines de trafic. Si la configuration GSLB doit être partagée entre tous les domaines de trafic, les méthodes GSLB Static Proximity et Round Trip Time (RTT) ne fonctionnent pas. Pour contourner ce scénario, vous pouvez utiliser des méthodes GSLB autres que RTT et Static Proximity. Pour plus d'informations, veuillez consulter http://support.citrix.com/article/CTX202277.

Configuration des domaines de trafic

La configuration d'un domaine de trafic sur l'appliance Citrix ADC comprend les tâches suivantes :

- **Ajoutez des VLAN.** Créez des VLAN et liez-leur des interfaces spécifiées.
- **Créez une entité de domaine de trafic et liez-y des VLAN.** Il s'agit des deux tâches suivantes :
  - Créez une entité de domaine de trafic identifiée de manière unique par un ID, qui est une valeur entière.
  - Liez les VLAN spécifiés à l'entité du domaine de trafic. Toutes les interfaces liées aux VLAN spécifiés sont associées au domaine de trafic. Plusieurs VLAN peuvent être liés à un domaine de trafic, mais un VLAN ne peut pas faire partie de plusieurs domaines de trafic.
- **Créez des entités d'entités sur le domaine de trafic**. Créez les entités d'entités requises dans le domaine de trafic. Les commandes CLI et les boîtes de dialogue de configuration de toutes les fonctionnalités prises en charge dans un domaine de trafic autre que celui par défaut incluent un paramètre appelé *identificateur de domaine de trafic* (td). Lors de la configuration d'une entité d'entités, si vous souhaitez que l'entité soit associée à un domaine de trafic particulier, vous devez spécifier le td. Toute entité d'entité que vous créez sans définir le td est automatiquement associée au domaine de trafic par défaut.

Pour vous donner une idée de la façon dont les entités d'entités sont associées à un domaine de trafic, cette rubrique couvre les procédures de configuration de toutes les entités mentionnées dans la figure intitulée How Traffic Domains Work.

L'interface de ligne de commande comporte deux commandes pour ces deux tâches, mais l'interface graphique les combine dans une seule boîte de dialogue.

Procédures CLI

Pour créer un VLAN et y lier des interfaces à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add vlan** <id>
- **bind vlan** <id>-**ifnum** <slot/port>
- **show vlan** <id>

Pour créer une entité de domaine de trafic et y lier des VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns trafficdomain** <td>
- **bind ns trafficdomain** <td> -**vlan** <id>
- **show ns trafficdomain** <td>

Pour créer un service à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **ajouter un service** <name><IP><serviceType><port>-**td** <id>
- **service de spectacle** <name>

Pour créer un serveur virtuel d'équilibrage de charge et y associer des services à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **ajouter un vserver lb** <name><serviceType><IPAddress><port>-**td** <id>
- **bind lb vserver** <name><serviceName>
- **show lb vserver** <name>

Procédures GUI

Pour créer un VLAN à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **VLAN**, cliquez sur **Ajouter**et définissez les paramètres.

Pour créer une entité de domaine de trafic à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Domaines de trafic**, cliquez sur **Ajouter**, puis dans la boîte de dialogue **Créer un domaine de trafic**, définissez les paramètres.

Pour créer un service à l'aide de l'interface graphique :

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, cliquez sur **Ajouter**et définissez les paramètres.

Pour créer un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique :

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, cliquez sur **Ajouter**et définissez les paramètres.

Liaisons d'entités de domaine inter-trafic

January 21, 2021

Vous pouvez lier des services dans un domaine de trafic à un serveur virtuel dans un autre domaine de trafic. Tous les services devant être liés à un serveur virtuel dans un domaine de trafic différent doivent résider dans le même domaine de trafic.

Vous configurez cette prise en charge à l'aide de la commande bind lb vserver existante ou de la procédure GUI associée.

Cette fonctionnalité peut faciliter l'interaction entre différents domaines de trafic. Dans une entreprise, les serveurs peuvent être regroupés dans différents domaines de trafic. Les serveurs virtuels sont créés dans un domaine de trafic qui fait face à Internet. Un serveur virtuel de ce domaine de trafic peut être configuré pour équilibrer la charge des serveurs dans un autre domaine de trafic. Ce serveur virtuel reçoit des demandes de connexion d'Internet à transférer aux serveurs liés.

Lorsqu'un Citrix ADC est utilisé dans une infrastructure cloud, chaque locataire peut se voir attribuer un domaine de trafic distinct et toutes les ressources (y compris les serveurs) d'un locataire peuvent être regroupées dans le domaine de trafic du locataire. Pour chaque locataire, un serveur virtuel est créé pour les serveurs d'équilibrage de charge dans son domaine de trafic. Tous ces serveurs virtuels sont regroupés dans un seul domaine de trafic faisant face à Internet.

Prenons un exemple de fournisseur de services cloud Exemple-Cloud-A a trois domaines de trafic, avec les ID 10, 20 et 30, configurés sur l'appliance Citrix ADC NS1.

Exemple-Org-A et Example-Org-B sont des locataires de Example-Cloud-A. Le locataire A se voit attribuer le domaine de trafic 20 et le locataire B le domaine 30. Les serveurs S1 et S2 résident dans le domaine de trafic 20 et les serveurs S3 et S4 résident dans le domaine de trafic 30.

Le domaine de trafic 10 fait face à Internet. Les serveurs virtuels LBVS-1 et LBVS-2 sont créés dans le domaine de trafic 10. LBVS-1, dans le domaine de trafic 10, est configuré pour équilibrer la charge des serveurs S1 et S2, qui se trouvent dans le domaine de trafic 20. LBVS-2, dans le domaine de trafic 10, est configuré pour équilibrer la charge des serveurs S3 et S4, qui se trouvent dans le domaine de trafic 30.

Par conséquent, ces serveurs virtuels acceptent les demandes de connexion Internet pour les serveurs qui se trouvent dans un domaine de trafic différent de celui des serveurs virtuels.

Domaines de trafic virtuels basés sur MAC

August 20, 2021

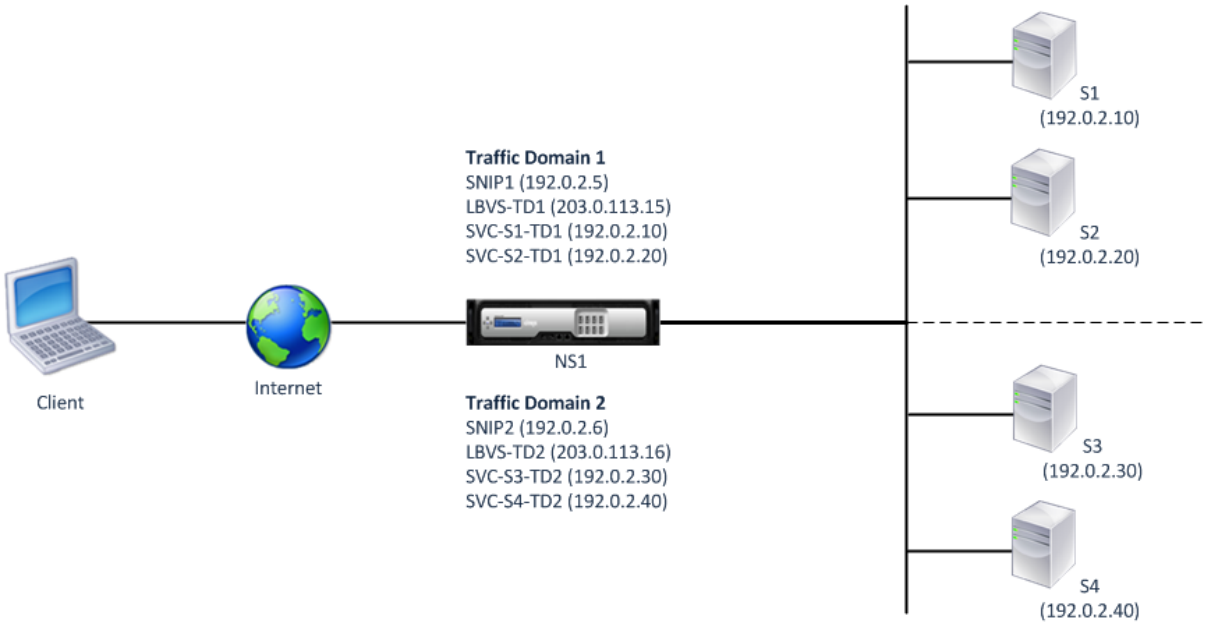
Vous pouvez associer un domaine de trafic à une adresse MAC virtuelle plutôt qu'à des VLAN. Citrix ADC envoie ensuite l'adresse MAC virtuelle du domaine de trafic dans toutes les réponses aux requêtes ARP pour les entités réseau de ce domaine. Par conséquent, ADC peut séparer le trafic entrant suivant pour différents domaines de trafic sur la base de l'adresse MAC de destination, car l'adresse MAC de destination est l'adresse MAC virtuelle d'un domaine de trafic. Après avoir créé des entités sur un domaine de trafic, vous pouvez facilement les gérer et les surveiller en effectuant des opérations au niveau du domaine de trafic.

Prenons un exemple dans lequel deux domaines de trafic, avec les ID 1 et 2, sont configurés sur l'appliance Citrix ADC NS1. Le Citrix ADC crée une adresse MAC virtuelle MAC1 et l'associe au domaine de trafic 1. De même, le Citrix ADC a créé une autre adresse MAC virtuelle MAC2 et s'associe au domaine de trafic 2.

Dans le domaine de trafic 1, le serveur virtuel d'équilibrage de charge LBVS-TD1 est configuré pour équilibrer le trafic entre les serveurs S1 et S2. Sur l'appliance Citrix ADC, les serveurs S1 et S2 sont représentés par les services SVC1-TD1 et SVC2-TD1, respectivement. Une adresse IP de sous-réseau (SNIP) SNIP1 est configurée pour permettre à Citrix ADC de communiquer avec S1 et S2. Étant donné que le MAC1 virtuel est associé au domaine de trafic 1, l'appliance envoie MAC1 virtuel en tant qu'adresse MAC dans toutes les annonces ARP et réponses ARP pour LBVS-TD1 et SNIP1.

De même, dans le domaine de trafic 2, le serveur virtuel d'équilibrage de charge LBVS-TD2 est configuré pour équilibrer la charge du trafic sur S3 et S4. Sur l'appliance Citrix ADC, les serveurs S3 et S4 sont représentés respectivement par les services SVC3-TD2 et SVC4-TD2. Une adresse SNIP SNIP2 est configurée pour permettre à Citrix ADC de communiquer avec S3 et S4. Étant donné que le MAC2 virtuel est associé au domaine de trafic 2, l'appliance envoie MAC2 virtuel en tant qu'adresse MAC dans toutes les annonces ARP et réponses ARP pour LBVS-TD2 et SNIP2.

Citrix ADC sépare le trafic entrant suivant pour les domaines de trafic 1 ou 2 sur la base de l'adresse MAC de destination, si l'adresse MAC de destination est MAC1 virtuel ou MAC2 virtuel.



Le tableau suivant répertorie les paramètres utilisés dans l'exemple : exemples de paramètres de domaine de trafic basé sur MAC virtuel.

Avant de commencer

Voici les points à considérer avant de configurer le domaine de trafic basé sur MAC virtuel :

1. Les domaines de trafic virtuels basés sur MAC sont le moyen le plus simple de parvenir à la ségrégation du trafic réseau.
2. Étant donné que les domaines de trafic basés sur MAC virtuels séparent le trafic réseau en fonction des adresses MAC virtuelles et non des VLAN, vous ne pouvez pas créer d'adresses IP dupliquées sur différents domaines de trafic basés sur MAC virtuels sur un Citrix ADC.
3. Les domaines de trafic virtuels basés sur MAC ne fonctionnent pas lorsque le Citrix ADC est déployé uniquement en mode L2.
4. Les domaines de trafic basés sur VLAN et MAC virtuels peuvent coexister sur un ADC Citrix. Les domaines de trafic basés sur MAC virtuels s'exécutent réellement sur tous les VLAN qui ne sont liés à aucun domaine de trafic basé sur VLAN.

Étapes de configuration

La configuration d'un domaine de trafic basé sur MAC virtuel sur une appliance Citrix ADC comporte les tâches suivantes :

- Créez une entité de domaine de trafic et activez l'option MAC virtuel. Créez une entité de domaine de trafic identifiée de manière unique par un ID, qui est une valeur entière, puis activez

l'option MAC virtuel. Après avoir créé l'entité de domaine de trafic, Citrix ADC crée une adresse MAC virtuelle, puis l'associe à l'entité de domaine de trafic.

- Créez des entités d'entités sur le domaine de trafic. Créez les entités d'entités requises dans le domaine de trafic en spécifiant l'identificateur de domaine de trafic (td) lors de la configuration de ces entités d'entités. Les entités réseau appartenant à Citrix ADC créées dans un domaine de trafic basé sur MAC virtuel sont associées à l'adresse MAC virtuelle, qui est associée au domaine de trafic. Citrix ADC envoie ensuite l'adresse MAC virtuelle du domaine de trafic dans les annonces ARP et les réponses ARP pour ces entités réseau.

Procédures CLI

Pour créer un domaine de trafic virtuel basé sur MAC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
add ns trafficDomain <td> [-vmac ( ENABLED        DISABLED )]
```

-
- show ns trafficdomain <td>

Pour configurer une adresse SNIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add ns ip <IPAddress> <netmask> -type SNIP –td <id>
- show ns ip <IPAddress> -td <id>

Pour créer un service à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add service <name> <IP> <serviceType> <port> -td <id>
- show service <name> -td <id>

Pour créer un serveur virtuel d'équilibrage de charge et y lier des services à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- add lb vserver <name> <serviceType> <IPAddress> <port> -td <id>
- bind lb vserver <name> <serviceName>
- show lb vserver <name> -td <id>

Exemple :

```
1 > add ns trafficDomain 1 -vmac ENABLED
```



```
 Done
> add ns trafficDomain 2 -vmac ENABLED
 Done

> add ns ip 192.0.2.5 255.255.255.0 -type -SNIP -td 1
 Done
> add service  SVC-S1-TD1  192.0.2.10 HTTP 80 -td 1
 Done
> add service  SVC-S2-TD1  192.0.2.20 HTTP 80 -td 1
 Done
> add lb vserver  LBVS-TD1 HTTP   203.0.113.15 80 -td 1
 Done
> bind lb vserver  LBVS-TD1 SVC-S1-TD1
 Done
> bind lb vserver  LBVS-TD1 SVC-S2-TD1
 Done

> add ns ip 192.0.2.6 255.255.255.0 -type -SNIP -td 2
 Done
> add service  SVC-S3-TD2  192.0.2.30 HTTP 80 -td 2
 Done
> add service  SVC-S4-TD2  192.0.2.40 HTTP 80 -td 2
 Done
> add lb vserver  LBVS-TD1 HTTP   203.0.113.16 80 -td 1
 Done
> bind lb vserver  LBVS-TD2 SVC-S3-TD2
 Done
> bind lb vserver  LBVS-TD2 SVC-S3-TD2
 Done
<!--NeedCopy-->
```

Procédures GUI

Pour créer un domaine de trafic basé sur MAC virtuel à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > Interfaces.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la page Créer un domaine de trafic, définissez les paramètres suivants :
   - ID de domaine de trafic *
   - Activer Mac
4. Cliquez sur Créer.

Pour configurer une adresse SNIP à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > IP > IPv4

2. Accédez à Réseau > IP > IPv4
3. Dans le volet d'informations, cliquez sur Ajouter
4. Dans la page Créer une adresse IP, définissez les paramètres suivants. Pour une description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
    - Adresse IP
    - Masque réseau
    - Type IP
    - ID de domaine de trafic
5. Cliquez sur Créer.

Pour créer un service à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Services.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la page Paramètres de base, définissez les paramètres suivants. Pour une description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
    - Nom du service
    - Serveur
    - Protocole
    - Port
    - ID de domaine de trafic
4. Cliquez sur Continuer, puis sur Terminé.
5. Répétez les étapes 2 à 4 pour créer un autre service.
6. Cliquez sur Fermer.

Pour créer un serveur virtuel d'équilibrage de charge et y lier des services à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet Serveurs virtuels d'équilibrage de charge, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer des serveurs virtuels (équilibrage de charge), définissez les paramètres suivants. Pour une description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
    - Nom
    - Adresse IP
    - Protocole
    - Port
    - ID de domaine de trafic
4. Cliquez sur Continuer, dans le volet Service, cliquez sur >.
5. Dans la page Service, cliquez sur Insérer, puis activez la case à cocher pour les services que vous souhaitez lier au serveur virtuel.
6. Cliquez sur Continuer, puis sur Terminé.

7. Répétez les étapes 2 à 5 pour créer un autre serveur virtuel

VXLAN

August 20, 2021

Les appliances Citrix ADC prennent en charge les réseaux locaux virtuels (VxLAN). Un VXLAN superpose des réseaux de couche 2 sur une infrastructure de couche 3 en encapsulant des trames de couche 2 dans des paquets UDP. Chaque réseau de superposition est connu sous le nom de segment VXLAN et est identifié par un identificateur unique 24 bits appelé VXLAN Network Identifier (VNI). Seuls les périphériques réseau d'un même VXLAN peuvent communiquer entre eux.

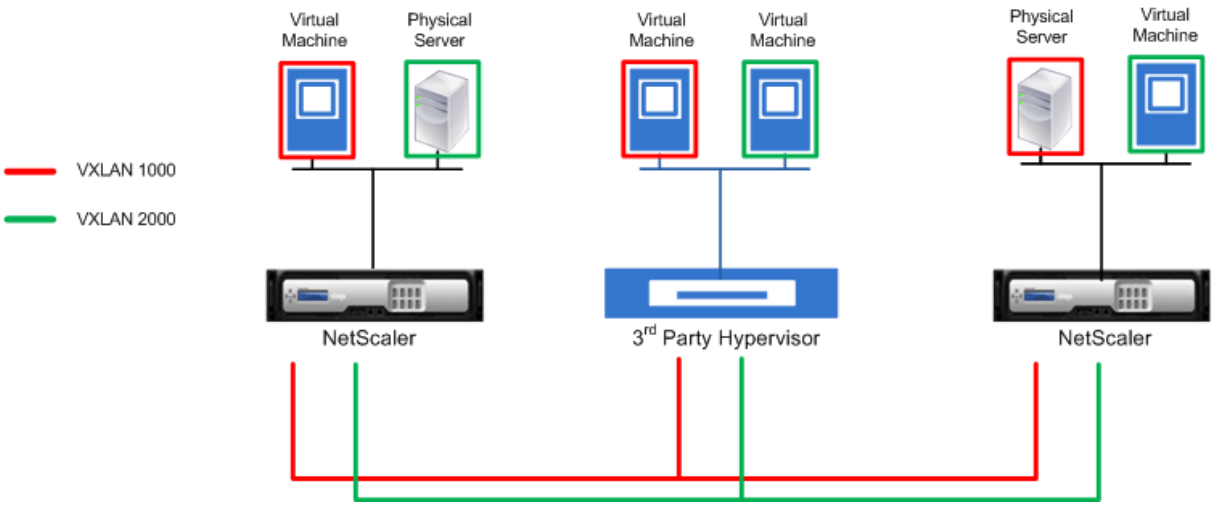
Les VXLAN fournissent les mêmes services réseau Ethernet de couche 2 que les VLAN, mais avec une extensibilité et une flexibilité accrues. Les deux principaux avantages de l'utilisation de VXLAN sont les suivants :

- **Évolutivité supérieure.** La virtualisation des serveurs et les architectures de cloud computing ont considérablement augmenté la demande de réseaux isolés de couche 2 dans un centre de données. La spécification VLAN utilise un ID VLAN 12 bits pour identifier un réseau de couche 2, de sorte que vous ne pouvez pas mettre à l'échelle au-delà de 4094 VLAN. Ce nombre peut être insuffisant lorsqu'il s'agit de milliers de réseaux isolés de couche 2. Le VNI 24 bits peut accueillir jusqu'à 16 millions de segments VXLAN dans le même domaine administratif.
- **Flexibilité accrue.** Étant donné que VXLAN transporte des trames de données de couche 2 sur des paquets de couche 3, les VXLAN étendent les réseaux de niveau 2 entre différentes parties d'un centre de données et entre des centres de données séparés géographiquement. Les applications hébergées dans différentes parties d'un centre de données et dans différents centres de données mais faisant partie du même VXLAN apparaissent comme un réseau contigu.

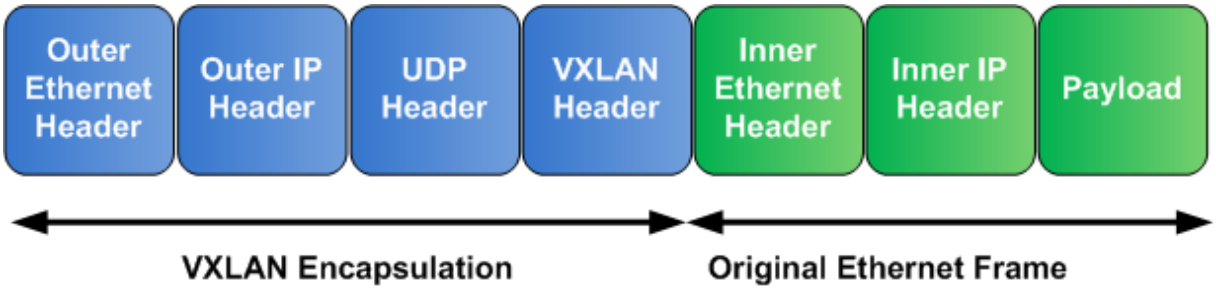
Fonctionnement des VXLAN

Les segments VXLAN sont créés entre les points d'extrémité du tunnel VXLAN (VTEP). Les VTEP prennent en charge le protocole VXLAN et effectuent l'encapsulation et la décapsulation VXLAN. Vous pouvez penser à un segment VXLAN comme un tunnel entre deux VTEP, où un VTEP encapsule une trame Layer2 avec un en-tête UDP et un en-tête IP et l'envoie à travers le tunnel. L'autre VTEP reçoit et décapsule le paquet pour obtenir la trame de couche 2. Un Citrix ADC est un exemple de VTEP. D'autres exemples sont les hyperviseurs tiers, les machines virtuelles compatibles VXLAN et les commutateurs compatibles VXLAN.

L'illustration suivante affiche les machines virtuelles et les serveurs physiques connectés via des tunnels VXLAN.



L'illustration suivante affiche le format d'un paquet VXLAN.



Les VXLAN sur un Citrix ADC utilisent un mécanisme de couche 2 pour l'envoi de trames de diffusion, de multidiffusion et de monodiffusion inconnues. Un VXLAN prend en charge les modes suivants pour l'envoi de ces trames L2.

- **Mode monodiffusion** : dans ce mode, vous spécifiez les adresses IP des VTEP lors de la configuration d'un VXLAN sur un Citrix ADC. Citrix ADC envoie des trames de diffusion, de multidiffusion et de monodiffusion inconnues sur la couche 3 à tous les VTEP de ce VXLAN.
- **Mode de multidiffusion** : dans ce mode, vous spécifiez une adresse IP de groupe de multidiffusion lors de la configuration d'un VXLAN sur un Citrix ADC. Les Citrix ADC ne prennent pas en charge le protocole IGMP (Internet Group Management Protocol). Les Citrix ADC comptent sur le routeur en amont pour rejoindre un groupe de multidiffusion, qui partage une adresse IP de groupe de multidiffusion commune. Citrix ADC envoie des trames de diffusion, de multidiffusion et de monodiffusion inconnues sur la couche 3 à l'adresse IP du groupe de multidiffusion de ce VXLAN.

À l'instar d'une table de pont de couche 2, les Citrix ADC maintiennent les tables de mappage VXLAN en fonction de l'en-tête interne et externe des paquets VXLAN reçus. Ce tableau mappe les adresses MAC d'hôte distant aux adresses IP VTEP pour un VXLAN particulier. Citrix ADC utilise la table de mappage VXLAN pour rechercher l'adresse MAC de destination d'un cadre de couche 2. Si une entrée pour cette adresse MAC est présente dans la table VXLAN, Citrix ADC envoie la trame de couche 2 sur la couche

3, à l'aide du protocole VXLAN, à l'adresse IP VTEP mappée spécifiée dans l'entrée de mappage pour un VXLAN.

Étant donné que les VXLAN fonctionnent de la même manière que les VLAN, la plupart des fonctionnalités Citrix ADC qui prennent en charge le VLAN en tant que paramètre de classification prennent en charge le VXLAN. Ces fonctionnalités incluent un paramètre de paramètre VXLAN facultatif, qui spécifie le VNI VXLAN.

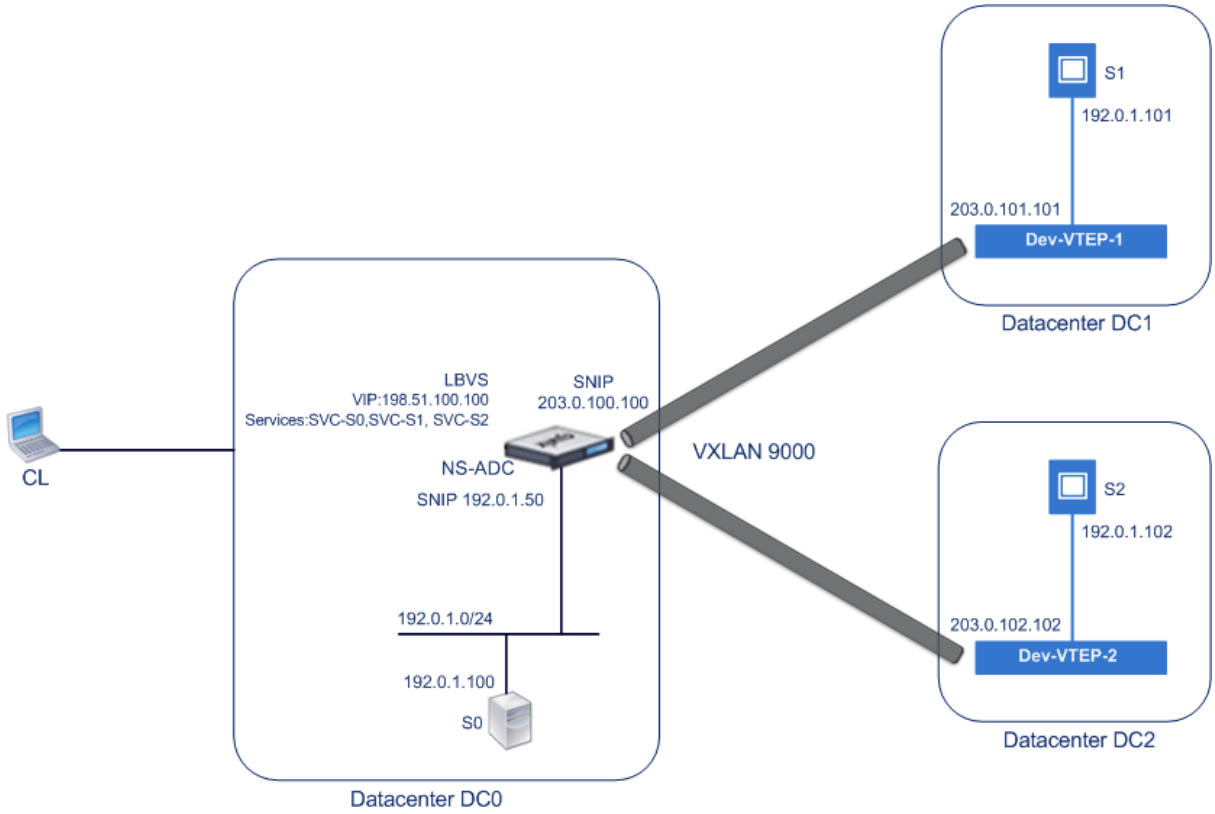
Dans une configuration haute disponibilité (HA), la configuration VXLAN est propagée ou synchronisée vers le nœud secondaire.

Cas d'utilisation VXLAN : équilibrage de charge entre les centres de données

Pour comprendre la fonctionnalité VXLAN d'un Citrix ADC, considérez un exemple dans lequel Example Corp héberge un site sur www.example.com. Pour garantir la disponibilité des applications, le site est hébergé sur trois serveurs, S0, S1 et S2. Un serveur virtuel d'équilibrage de charge, LBVS, sur Citrix ADC NS-ADC est utilisé pour équilibrer la charge de ces serveurs. S0, S1 et S2 résident respectivement dans les centres de données DC0, DC1 et DC2. Dans DC0, le serveur S0 est connecté à NS-ADC.

S0 est un serveur physique, et S1 et S2 sont des machines virtuelles (VM). S1 s'exécute sur le périphérique hôte de virtualisation Dev-VTEP-1 dans le centre de données DC1, et S2 s'exécute sur le périphérique hôte Dev-VTEP-2 dans DC2. NS-ADC, DEV-VTEP-1 et DEV-VTEP-2 prennent en charge le protocole VXLAN.

S0, S1 et S2 font partie du même sous-réseau privé, 192.0.1.0/24. S0, S1 et S2 font partie d'un domaine de diffusion commun, VXLAN 9000 est configuré sur NS-ADC, Dev-VTEP-1 et Dev-VTEP-2. Les serveurs S1 et S2 font partie de VXLAN9000 sur Dev-VTEP-1 et Dev-VTEP-2, respectivement.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple : paramètres VXLAN.

Les services SVC-S0, SVC-S1 et SVC-S2 sur NS-ADC représentent S0, S1 et S2. Dès que ces services sont configurés, NS-ADC diffuse des demandes ARP pour S0, S1 et S2 pour résoudre le mappage IP-MAC. Ces demandes ARP sont également envoyées via VXLAN 9000 à Dev-VTEP-1 et Dev-VTEP-2.

Voici le flux de trafic pour résoudre la demande ARP pour S2 :

1. NS-ADC diffuse une demande ARP pour S2 pour résoudre le mappage IP-MAC. Ce paquet a :
   - Adresse IP source = Adresse IP du sous-réseau SNIP pour serveurs (192.0.1.50)
   - Adresse MAC source = adresse MAC de l'interface du NS-ADC à partir de laquelle le paquet est envoyé = NS-MAC-1
2. NS-ADC prépare le paquet ARP à envoyer via le VXLAN 9000 en encapsulant le paquet avec les en-têtes suivants :
   - En-tête VXLAN avec un ID (VNI) de 9000
   - En-tête UDP standard, somme de contrôle UDP définie sur 0×0000 et port de destination défini sur 4789.
3. NS-ADC envoie le paquet encapsulé résultant à DEV-VTEP-1 et DEV-VTEP-2 sur VXLAN-9000. Le paquet encapsulé a :
   - Adresse IP source = SNIP-VTEP-0 (203.0.100.100).
4. Dev-VTEP-2 reçoit le paquet UDP et décapsule l'en-tête UDP, à partir duquel Dev-VTEP-2 ap-

prend que le paquet est un paquet lié au VXLAN. Dev-VTEP-2 décapsule ensuite l'en-tête VXLAN et apprend l'ID VXLAN du paquet. Le paquet résultant est le paquet de requête ARP pour S2, qui est identique à celui de l'étape 1.

5. À partir de l'en-tête interne et externe du paquet VXLAN, Dev-VTEP-2 crée une entrée dans sa table de mappage VXLAN qui montre le mappage de l'adresse MAC (NS-MAC-1) et SNIP-VTEP-0 (203.0.100.100) pour VXLAN9000.
6. Dev-VTEP-2 envoie le paquet ARP à S2. Le paquet de réponse de S2 atteint Dev-VTEP-2. Dev-VTEP-2 effectue une recherche dans sa table de mappage VXLAN et obtient une correspondance pour l'adresse MAC de destination NS-MAC-1. Le Dev-VTEP-2 sait maintenant que NS-MAC-1 est accessible via SNIP-VTEP-0 (203.0.100.100) sur VXLAN 9000.
7. S2 répond avec son adresse MAC (MAC-S2). Le paquet de réponse ARP a :
   - Adresse IP de destination = Adresse IP du sous-réseau SNIP pour serveurs (192.0.1.50)
   - Adresse MAC de destination = NS-MAC-1
8. Le paquet de réponse de S2 atteint Dev-VTEP-2. Dev-VTEP-2 effectue une recherche dans sa table de mappage VXLAN et obtient une correspondance pour l'adresse MAC de destination NS-MAC-1. Le Dev-VTEP-2 sait maintenant que NS-MAC-1 est accessible via SNIP-VTEP-0 (203.0.100.100) sur VXLAN 9000. Dev-VTEP-2 encapsule la réponse ARP avec les en-têtes VXLAN et UDP et envoie le paquet résultant à SNIP-VTEP-0 (203.0.100.100) de NS-ADC.
9. NS-ADC lors de la réception du paquet, décapsule le paquet en supprimant les en-têtes VXLAN et UDP. Le paquet résultant est la réponse ARP de S2. NS-ADC met à jour la table de mappage VXLAN pour l'adresse MAC de S2 (MAC-S2) avec l'adresse IP de Dev-VTEP-2 (203.0.102.102) pour VXLAN 9000. NS-ADC met également à jour la table ARP pour l'adresse IP de S2 (192.0.1.102) avec l'adresse MAC de S2 (MAC-S2).

Voici le flux de trafic pour le serveur virtuel d'équilibrage de charge LBVS dans cet exemple :

1. Client CL envoie un paquet de requête à LBVS de NS-ADC. Le paquet de requête a :
   - Adresse IP source = adresse IP du client CL (198.51.100.90)
   - Adresse IP de destination = adresse IP (VIP) de LBVS = 198.51.110.100
2. LBVS de NS-ADC reçoit le paquet de requête, et son algorithme d'équilibrage de charge sélectionne le serveur S2 du centre de données DC2.
3. NS-ADC traite le paquet de requête, en changeant son adresse IP de destination à l'adresse IP de S2 et son adresse IP source à l'une des adresses IP de sous-réseau (SNIP) configurées sur NS-ADC. Le paquet de requête a :
   - Adresse IP source = Adresse IP du sous-réseau sur NS-ADC= SNIP pour serveurs (192.0.1.50)
   - Adresse IP de destination = adresse IP de S2 (192.0.1.102)
4. NS-ADC trouve une entrée de mappage VXLAN pour S2 dans sa table de pont. Cette entrée indique que S2 est accessible via le Dev-VTEP-2 sur VXLAN 9000.
5. NS-ADC prépare le paquet à envoyer via le VXLAN 9000 en encapsulant le paquet avec les entêtes suivants :
   - En-tête VXLAN avec un ID (VNI) de 9000

- En-tête UDP standard, somme de contrôle UDP définie sur 0×0000 et port de destination défini sur 4789.

6. NS-ADC envoie le paquet encapsulé résultant à DEV-VTEP-2. Le paquet de requête a :
   - Adresse IP source = adresse SNIP = SNIP = SNIP-VTEP-0 (203.0.100.100)
   - Adresse IP de destination = adresse IP de Dev-VTEP-2 (203.0.102.102)
7. Dev-VTEP-2 reçoit le paquet UDP et décapsule l'en-tête UDP, à partir duquel Dev-VTEP-2 apprend que le paquet est un paquet lié au VXLAN. Dev-VTEP-2 décapsule ensuite l'en-tête VXLAN et apprend l'ID VXLAN du paquet. Le paquet résultant est le même que dans l'étape 3.
8. Dev-VTEP-2 transmet ensuite le paquet à S2.
9. S2 traite le paquet de requête et envoie la réponse à l'adresse SNIP de NS-ADC. Le paquet de réponse a :
   - Adresse IP source = adresse IP de S2 (192.0.1.102)
   - Adresse IP de destination = Adresse IP du sous-réseau sur NS-ADC= SNIP pour serveurs (192.0.1.50)
10. Dev-VTEP-2 encapsule le paquet de réponse de la même manière que NS-ADC encapsulé le paquet de requête dans les étapes 4 et 5. Dev-VTEP-2 envoie ensuite le paquet UDP encapsulé à l'adresse SNIP SNIP pour serveurs (192.0.1.50) de NS-ADC.
11. NS-ADC, à la réception du paquet UDP encapsulé, décapsule le paquet en supprimant les entêtes UDP et VXLAN de la même manière que Dev-VTEP-2 décapsulé le paquet à l'étape 7. Le paquet résultant est le même paquet de réponse que dans l'étape 9.
12. NS-ADC utilise ensuite la table de session pour l'équilibrage de charge LBVS du serveur virtuel et transmet le paquet de réponse au client CL. Le paquet de réponse a :
    - Adresse IP source = adresse IP du client CL (198.51.100.90)
    - Adresse IP de destination = adresse IP (VIP) de LBVS (198.51.110.100)

Points à prendre en considération pour la configuration de VXLAN

Tenez compte des points suivants avant de configurer des VXLAN sur un Citrix ADC :

- Un maximum de 2048 VxLAN peut être configuré sur un Citrix ADC.
- Les VXLAN ne sont pas pris en charge dans un cluster.
- Les adresses IPv6 locales de liaison ne peuvent pas être configurées pour chaque VXLAN.
- Les Citrix ADC ne prennent pas en charge le protocole IGMP (Internet Group Management Protocol) pour former un groupe de multidiffusion. Les Citrix ADC s'appuient sur le protocole IGMP de son routeur en amont pour rejoindre un groupe de multidiffusion, qui partage une adresse IP de groupe de multidiffusion commune. Vous pouvez spécifier une adresse IP de groupe de multidiffusion lors de la création d'entrées de table de pont VXLAN, mais le groupe de multidiffusion doit être configuré sur le routeur en amont. Citrix ADC envoie des trames de diffusion, de multidiffusion et de monodiffusion inconnues sur la couche 3 à l'adresse IP du groupe de

multidiffusion de ce VXLAN. Le routeur en amont transfère ensuite le paquet à tous les VTEP qui font partie du groupe de multidiffusion.

- L'encapsulation VXLAN ajoute une surcharge de 50 octets à chaque paquet :

  En-tête Ethernet externe (14) + en-tête UDP (8) + en-tête IP (20) + en-tête VXLAN (8) = 50 octets

  Pour éviter la fragmentation et la dégradation des performances, vous devez ajuster les paramètres MTU de tous les périphériques réseau d'un chemin VXLAN, y compris les périphériques VTEP VXLAN, pour gérer les 50 octets de surcharge dans les paquets VXLAN.

  Important : les trames jumbo ne sont pas prises en charge sur les appliances virtuelles Citrix ADC VPX, les appliances Citrix ADC SDX et Citrix ADC MPX 15000/17000. Ces appliances prennent en charge une taille MTU de seulement 1500 octets et ne peuvent pas être ajustées pour gérer la surcharge de 50 octets des paquets VXLAN. Le trafic VXLAN peut être fragmenté ou subir une dégradation des performances si l'une de ces appliances se trouve dans le chemin VXLAN ou agit comme un périphérique VXLAN VTEP.
- Sur les appliances Citrix ADC SDX, le filtrage VLAN ne fonctionne pas pour les paquets VXLAN.
- Vous ne pouvez pas définir une valeur MTU sur un VXLAN.
- Vous ne pouvez pas lier des interfaces à un VXLAN.

Étapes de configuration

La configuration d'un VXLAN sur une appliance Citrix ADC comporte les tâches suivantes.

- **Ajoutez une entité VXLAN**. Créez une entité VXLAN identifiée de manière unique par un entier positif, également appelé VXLAN Network Identifier (VNI). Dans cette étape, vous pouvez également spécifier le port UDP de destination du VTEP distant sur lequel le protocole VXLAN est exécuté. Par défaut, le paramètre de port UDP de destination est défini sur 4789 pour l'entité VXLAN. Ce paramètre de port UDP doit correspondre aux paramètres de tous les VTEP distants de ce VXLAN. Vous pouvez également lier des VLAN à ce VXLAN. Le trafic (qui inclut les diffusions, les multidiffusions, les unicasts inconnus) de tous les VLAN liés est autorisé sur ce VXLAN. Si aucun VLAN n'est lié au VXLAN, Citrix ADC autorise le trafic de tous les VLAN, sur ce VXLAN, qui ne font partie d'aucun autre VXLAN.
- **Liez l'adresse IP VTEP locale et l'entité VXLAN**. Liez l'une des adresses SNIP configurées au VXLAN pour fournir des paquets VXLAN sortants.
- **Ajoutez une entrée bridgetable**. Ajoutez une entrée bridgetable spécifiant l'ID VXLAN et l'adresse IP VTEP distante pour le VXLAN à créer.
- **(Facultatif) Liez différentes entités de fonction au VXLAN configuré**. Les VXLAN fonctionnent de la même manière que les VLAN, la plupart des fonctionnalités Citrix ADC qui prennent en charge le VLAN en tant que paramètre de classification prennent également en charge le

VXLAN. Ces fonctionnalités incluent un paramètre de paramètre VXLAN facultatif, qui spécifie le VNI VXLAN.

- **(Facultatif) Affichez la table de mappage VXLAN**. Affichez la table de mappage VXLAN, qui inclut les entrées de mappage de l'adresse MAC de l'hôte distant vers l'adresse IP VTEP pour un VXLAN particulier. En d'autres termes, un mappage VXLAN indique qu'un hôte est accessible via le VTEP sur un VXLAN particulier. Citrix ADC apprend les mappages VXLAN et met à jour sa table de mappage à partir des paquets VXLAN qu'il reçoit. Citrix ADC utilise la table de mappage VXLAN pour rechercher l'adresse MAC de destination d'une trame de couche 2. Si une entrée pour cette adresse MAC est présente dans la table VXLAN, Citrix ADC envoie la trame de couche 2 sur la couche 3, à l'aide du protocole VXLAN, à l'adresse IP VTEP mappée spécifiée dans l'entrée de mappage pour un VXLAN.

Procédures CLI

Pour ajouter une entité VXLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez

- **add vxlan** <id>
- **show vxlan**<id>

Pour lier l'adresse IP VTEP locale au VXLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez

- **lier vxlan** <id> -**srCiP** <IPaddress>
- **show vxlan** <id>

Pour ajouter un pont à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez

- **add bridgetable** -**mac** <macaddress> -**vxlan** <ID> -**vtep** <IPaddress>
- **show bridgetable**

Pour afficher la table de transfert VXLAN à l'aide de la ligne de commande :

À l'invite de commandes, tapez :

- **show bridgetable**

Procédures GUI

Pour ajouter une entité VXLAN et lier une adresse IP VTEP locale à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **VXLAN**et ajoutez une nouvelle entité VXLAN ou modifiez une entité VXLAN existante.

Pour ajouter un pont à l' aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Table de pont**, définissez les paramètres suivants lors de l'ajout ou de la modification d'une entrée de table de pont VXLAN :

- MAC
- VTEP
- ID VXLAN

Pour afficher la table de transfert VXLAN à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Table de pont**.

```
Example
> add vxlan 9000
Done
> bind vxlan 9000 -srcIP 203.0.100.100

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
   203.0.101.101

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
   203.0.102.102

Done
```

Prise en charge des protocoles de routage dynamique IPv6 sur les VXLAN

L'appliance Citrix ADC prend en charge les protocoles de routage dynamique IPv6 pour les VXLAN. Vous pouvez configurer divers protocoles de routage dynamique IPv6 (par exemple, OSPFv3, Ripng, BGP) sur des VxLAN à partir de la ligne de commande VTYSH. Une option IPv6 Dynamic Routing Protocol a été ajoutée au jeu de commandes VXLAN pour activer ou désactiver les protocoles de routage dynamique IPv6 sur un VXLAN. Après avoir activé les protocoles de routage dynamique IPv6 sur un VXLAN, les processus liés aux protocoles de routage dynamique IPv6 doivent être démarrés sur le VXLAN à l'aide de la ligne de commande VTYSH.

Pour activer les protocoles de routage dynamique IPv6 sur un VXLAN à l'aide de l'interface de ligne de commande :

- **ajouter vxlan** <ID>[-**IPv6DynamicRouting** (**ACTIVÉ** | **DÉSACTIVÉ**)]
- **show vxlan**


```
In the following sample configuration, VXLAN-9000 is created and has
    IPv6 dynamic routing protocols enabled on it. Then, using the VTYSH
    command line, process for the IPv6 OSPF protocol is started on the
    VXLAN.

> add vxlan 9000 -ipv6DynamicRouting ENABLED

Done
> bind vxlan 9000 -srcIP 203.0.100.100

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
    203.0.101.101

Done
> VTYSH
NS# configure terminal
NS(config)# ns IPv6-routing
NS(config)# interface VXLAN-9000
NS(config-if)# ipv6 router OSPF area 3
```

Extension de VLAN de plusieurs entreprises vers un cloud à l'aide de cartes VXLAN-VLAN

Les tunnels CloudBridge Connector permettent d'étendre le VLAN d'une entreprise à un cloud. Les VLAN étendus à partir de plusieurs entreprises peuvent avoir des ID VLAN qui se chevauchent. Vous pouvez isoler les VLAN de chaque entreprise en les mappant sur un VXLAN unique dans le cloud. Sur une appliance Citrix ADC, qui est le point de terminaison du connecteur CloudBridge dans le cloud, vous pouvez configurer un mappage VXLAN-VLAN qui relie les VLAN d'une entreprise à un VXLAN unique dans le cloud. Les VXLAN prennent en charge le balisage VLAN pour étendre plusieurs VLAN d'une entreprise depuis CloudBridge Connector vers le même VXLAN.

Effectuez les tâches suivantes pour étendre les VLAN de plusieurs entreprises vers un cloud :

1. Créez un mappage VXLAN-VLAN.
2. Liez le mappage VXLAN-VLAN à une configuration de tunnel CloudBridge Connector basée sur un pont réseau ou PBR sur l'appliance Citrix ADC sur le cloud.
3. (Facultatif) Activez le balisage VLAN dans une configuration VXLAN.

Procédures CLI

Pour ajouter une carte VXLAN-VLAN à l'aide de l'interface de ligne de commande :

- **add vxlanVlanMap** <name>
- **show vxlanVlanMap** <name>

Pour lier un VXLAN et un VLAN à une carte VXLAN-VLAN à l'aide de l'interface de ligne de commande :

- **bind VXLanvlanMap** <name>[-**vxlan** -**vlan** <int [-int]<positive_integer»…]
- **show vxlanVlanMap** <name>

Pour lier un mappage VXLAN-VLAN à un tunnel CloudBridge Connector basé sur un pont réseau à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants.

si vous ajoutez un nouveau pont réseau :

- **add netbridge** <name [-**VXLanVLAN Map**]<string>
- **show netbridge** <name>

si vous reconfigurez un pont réseau existant :

- **set netbridge** <name> [-**VXLanVLAN Map**]
- **show netbridge** <name>

Pour lier un mappage VXLAN-VLAN à un tunnel CloudBridge Connector basé sur PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants.

si vous ajoutez un nouveau PBR :

- **ajouter pbr**ALLOW****<name>(-**IPTunnel** <ipTunnelName>[-**VxLanvlanMap**]<name>)
- **show pbr** <name>

si vous reconfigurez un PBR existant :

- **set pbr** <name> **ALLOW** (-**ipTunnel** <ipTunnelName> [-**VxLanvlanMap**])
- **show pbr** <name>

Pour inclure des balises VLAN dans des paquets liés à un VXLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants.

si vous ajoutez un nouveau VXLAN :

- **add vxlan** <vnid> -**vlanTag** (**ENABLED** | **DISABLED**)
- **show vxlan** <vnid>

si vous reconfigurez un VXLAN existant :

- **set vxlan** <vnid> -**vlanTag** (**ENABLED** | **DISABLED**)
- **show vxlan** <vnid>

Procédures GUI

Pour ajouter une carte VXLAN-VLAN à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **VXLAN Map**, ajoutez un mappage VXLAN VXLAN.

Pour lier un mappage VXLAN-VLAN à un tunnel CloudBridge Connector basé sur Netbridge à l'aide de l'interface graphique :

Accédez à **Système** > **Connecteur CloudBridge** > **Pont réseau**, sélectionnez une carte **VXLAN-VLAN dans la liste déroulante VXLAN VXLAN** tout en ajoutant un nouveau pont réseau ou en reconfigurant un pont réseau existant.

Pour lier un mappage VXLAN-VLAN à un tunnel CloudBridge Connector basé sur PBR à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **PBR**, sous l'onglet Routage basé sur la stratégie (PBR), sélectionnez un mappage **VXLAN-VLAN** dans la liste déroulante **VXLAN VXLAN** tout en ajoutant un nouveau PBR ou en reconfigurant un PBR existant.

Pour inclure des balises VLAN dans des paquets liés à un VXLAN à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **VXLAN**, activez le **balisage VLAN interne** tout en ajoutant un nouveau VXLAN ou en reconfigurant un VXLAN existant.

```
1  > add vxlanVlanMap VXLANVLAN-DC1
2
3  Done
4
5  > bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 3000 -vlan 3
6
7  Done
8
9  > bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 3500 -vlan 4
10
11 Done
12
13 >add vxlanVlanMap VXLANVLAN-DC2
14
15 Done
16
17 > bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 8000 -vlan 3 4
18
19 Done
20
21 > set pbr PBR-CBC-DC-1-CLOUD ALLOW  -ipTunnel  CBC-DC-1-CLOUD -
      vxlanVlanMap VXLANVLAN-DC1
22
```



```
23 Done
24
25 > set pbr PBR-CBC-DC-2-CLOUD ALLOW  -ipTunnel  CBC-DC-2-CLOUD -
      vxlanVlanMap VXLANVLAN-DC2
26
27 Done
```

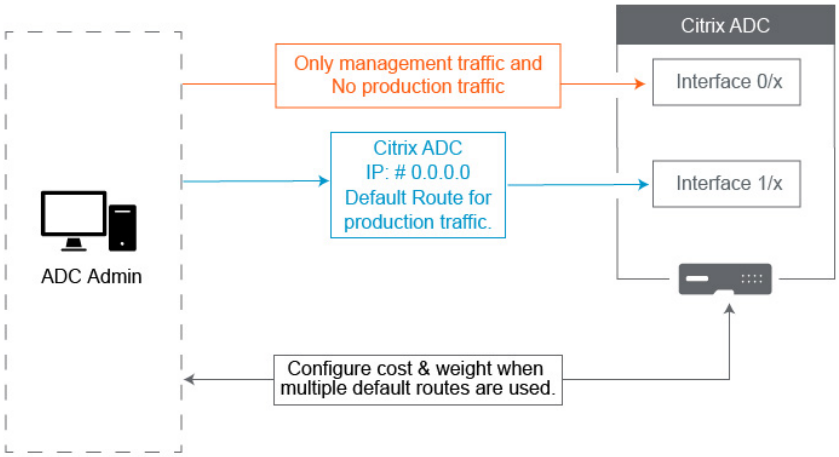
Meilleures pratiques pour les configurations réseau

August 20, 2021

Les sections suivantes traitent des meilleures pratiques pour la configuration des fonctionnalités de mise en réseau sur une appliance Citrix ADC.

Routage et itinéraires par défaut

Voici quelques bonnes pratiques pour configurer les fonctionnalités de couche 3 sur une appliance Citrix ADC.



- **L'interface `0/x` d'une appliance Citrix ADC ou d'une appliance Citrix SDX ne doit pas être utilisée pour le trafic de production**. Sur un MPX ou SDX, les interfaces nommées `0/x` sont référencées aux interfaces de gestion. Cela ne signifie pas que vous devez utiliser ces interfaces pour Management. Cela signifie que ces interfaces ne sont PAS conçues pour le trafic de production. Ils ne disposent pas des tampons matériels et de l'optimisation nécessaires pour atteindre un débit soutenu de 1 Gbit/s. Par conséquent, si votre itinéraire par défaut se trouve dans le même sous-réseau que votre NSIP, vous devez modifier l'itinéraire par défaut ou utiliser une

interface `1/x` pour votre réseau de gestion car les interfaces `1/x` sont entièrement optimisées pour la production 1 Trafic Gbit/s.

> **Remarque** :
>
> Cela ne s'applique pas à une appliance Citrix ADC VPX.

- **Option 1**. Ne pas se connecter aux interfaces`0/x` : déconnectez le câble de l'interface`0/1` . NetScaler écoute le NSIP sur les autres interfaces. (REMARQUE : Ce n'est pas une option pour SDX, car SVM et XenServer ne peuvent parler qu'aux`0/x` interfaces)
- **Option 2**. Changez l'itinéraire par défaut pour une interface différente, comme indiqué dans la section suivante.

- **La Gateway par défaut (route 0.0.0.0) doit se trouver sur un réseau de production et non sur une`0/x` interface** . Lors de la première configuration d'un NetScaler, il vous demande l'adresse NSIP, le masque de sous-réseau et la passerelle. Le problème que cela crée pour les administrateurs est qu'ils ont simplement configuré leur route par défaut pour être sur leur réseau de gestion à l'aide de l'interface 0/1.
  - Pour vérifier quelles sont vos routes, exécutez dans CLI`show route` et votre Gateway par défaut est l'adresse IP dans la ligne où le réseau et le masque de réseau sont 0.0.0.0. Voici un exemple où la passerelle est sur la ligne 1 :

```
1  > sh route
2          Network          Netmask          Gateway/OwnedIP
               State   Traffic Domain  Type
3          -------          -------          ---------------
               -----   --------------  ----
4  1)      0.0.0.0          0.0.0.0          10.25.213.65     UP
            0               STATIC
5  2)      127.0.0.0        255.0.0.0        127.0.0.1        UP
            0               PERMANENT
6  3)      10.25.213.64     255.255.255.192  10.25.213.68     UP
            0               DIRECT
7  4)      172.16.0.0       255.255.255.0    172.16.0.1       UP
            0               DIRECT
8
9  <!--NeedCopy-->
```

  - Pour vérifier l'interface et le VLAN utilisés pour votre passerelle par défaut, vérifiez la table ARP`sh arp` à l'aide de la CLI. Vous pouvez également rechercher l'adresse IP spécifique en utilisant`show arp | grep 10.25.213.65`. Voici un exemple où vous voyez que la passerelle 10.25.213.65 utilise Interface 1/1 et VLAN 1 :

```
1  > sh arp
```



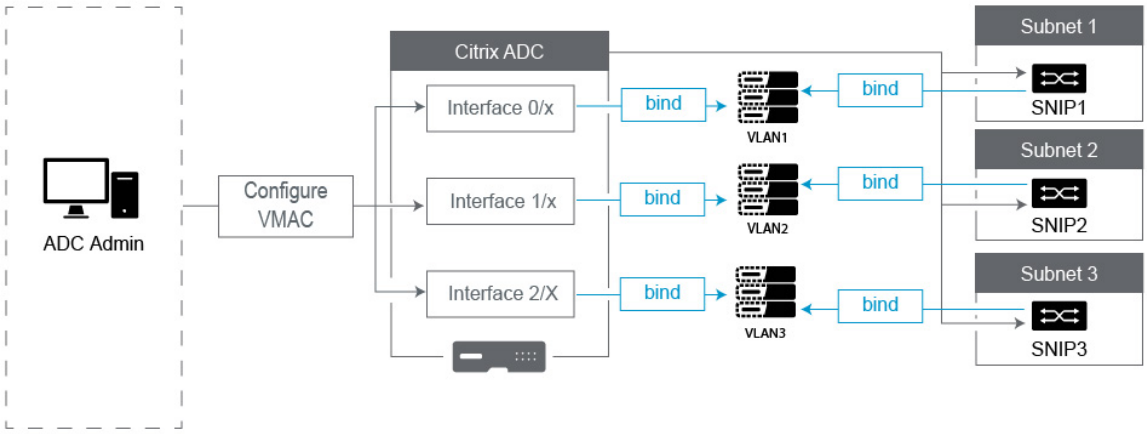
```
2           IP               MAC               Iface VLAN
                Origin     TTL     Traffic Domain
3           --               ---               ----- ----
                ------     ---     --------------
4   1)      127.0.0.1        02:00:18:a4:00:1e  LO/1  1
        PERMANENT  N/A    0
5   2)      10.25.213.70     02:00:0f:46:00:28  1/1   1
        DYNAMIC    967    0
6   3)      10.25.213.68     02:00:18:a4:00:1e  LO/1  1
        PERMANENT  N/A    0
7   4)      10.25.213.67     02:00:0f:46:00:28  1/1   1
        DYNAMIC    641    0
8   5)      10.25.213.65     00:08:e3:ff:fd:90  1/1   1
        DYNAMIC    483    0
9   <!--NeedCopy-->
```

- Modifiez l'itinéraire par défaut pour utiliser une passerelle sur votre sous-réseau et interface de production. Supposons que votre réseau de gestion est 10.0.0.0/24 avec Gateway 10.0.0.1 et que le réseau de production est 10.1.1.0/24 avec Gateway 10.1.1.1. Configurez votre configuration comme ceci :
  - SNIP : (Accès de gestion désactivé) 10.1.1.2
  - NSIP : (Accès de gestion activé) 10.0.0.2
  - Route par défaut : 0.0.0.0 0.0.0.0 10.1.1.1 (Système > Réseau > Routes). Cela utilise un routeur sur le réseau SNIP au lieu du réseau NSIP.

    > **Remarque** :
    >
    > La modification de la Gateway par défaut peut interrompre le trafic de gestion, sauf si vous configurez des routes statiques, une route basée sur une stratégie ou activez le transfert basé sur MAC.

Interfaces, canaux et VLAN

Voici quelques bonnes pratiques pour configurer les fonctionnalités de couche 2 sur une appliance Citrix ADC.



- **Ne connectez pas plusieurs interfaces/canaux au même VLAN, y compris le VLAN 1** :
  - Si vous ne configurez pas correctement vos VLAN, cela peut entraîner un routage de paquets inattendu dans votre réseau et une boucle de couche 2 à chaque fois qu'il existe plusieurs interfaces actives avec le même VLAN (natif ou balisé).
  - Par défaut, toutes les interfaces et les canaux sont sur le VLAN natif 1. Cela crée deux problèmes possibles :
    * Le NetScaler pense que tout le trafic reçu est sur le même réseau, il utilise donc n'importe quelle interface pour envoyer le trafic sur. Si vous avez un VLAN natif différent sur l'interface sur laquelle il a envoyé des données, le trafic ne sera pas routé comme prévu.
    * Si NetScaler reçoit des paquets de diffusion sur un port, il peut retransmettre sur un autre port. Si les deux ports de commutation sont sur le même VLAN, vous venez de créer une boucle de couche 2.
  - Pour supprimer une interface/canal du VLAN 1 :
    * Si vous n'utilisez pas de VLAN natifs sur votre canal d'interface de commutateur/port. Remplacez le VLAN natif sur NetScaler Interface/Channel par un numéro de VLAN inutilisé tel que 999. Vous ne devez pas utiliser le même numéro de VLAN inutilisé pour plusieurs canaux ou interfaces, car il crée une boucle de couche 2.
    * Si vous utilisez des VLAN natifs sur votre canal d'interface de commutateur/port. Modifiez le VLAN natif sur NetScaler Interface/Channel pour qu'il corresponde. Cependant, prenez soin de ne pas avoir plusieurs interfaces ou canaux actifs sur le même VLAN car cela crée des boucles de couche 2.
    * Vous ne pouvez pas supprimer le VLAN natif. Au lieu de cela, vous pouvez le modifier ou définir TagAll pour l'interface ou le canal. Si le port du commutateur n'est pas

configuré avec un VLAN natif non marqué, activez le tagall sur l'interface afin que les paquets de pulsations de haute disponibilité soient balisés.

  - Pour afficher le VLAN natif sur une interface, exécutez `sh interface` dans CLI. Cela vous informera également si l'interface utilise l'option TAGALL.

- **Liez une interface à votre VLAN** - Le NetScaler, par défaut, n'attache pas de nouveau VLAN à une interface. Cela signifie que le VLAN ne sera pas utilisé tant que vous ne le liez pas à une interface. Lorsque le nouveau VLAN n'est pas lié à une interface et que ce VLAN est marqué, NetScaler supprime tout le trafic entrant de ce VLAN. En outre, ne liez pas le même VLAN à plusieurs interfaces.

  - Liez des sous-réseaux à vos VLAN. Le NetScaler ne fonctionne pas comme un routeur typique. La plupart des routeurs attachent des adresses IP aux interfaces. Sur un NetScaler, les adresses IP flottent sur n'importe quelle interface, sauf configuration contraire. Par conséquent, tout sous-réseau que vous souhaitez vous assurer que NetScaler envoie via un VLAN spécifique, en particulier lorsque NetScaler lance ce trafic, vous devez lier un SNIP dans ce sous-réseau au VLAN.

  - Un argument commun que nous entendons contre cela est qu'il fonctionnait bien et maintenant il ne le fait pas sans lier le sous-réseau au VLAN. Cela se produit souvent parce que NetScaler apprend quel VLAN envoyer du trafic, mais cela peut prendre du temps lors de la création de ses tables ARP. Après un redémarrage ou une mise à niveau du microprogramme, alors qu'il commence à construire à nouveau les tables ARP, il peut d'abord apprendre et donc utiliser un chemin différent de celui que vous souhaitez, tel que votre itinéraire par défaut. Il est préférable de lui indiquer quel chemin prendre en liant le SNIP au VLAN. Une fois qu'un SNIP est lié à un VLAN, l'ensemble du sous-réseau de ce SNIP sera lié au VLAN.

  - Assurez-vous que chaque SNIP est lié à un VLAN (sauf dans les cas où vous avez plus d'un SNIP dans un sous-réseau, alors vous ne devez en lier qu'un), et que le VLAN, à son tour, est lié à une seule interface ou canal. Il est également souvent préférable d'avoir un SNIP dans chaque sous-réseau, mais cela n'est pas requis car l'itinéraire le plus spécifique sera utilisé pour tout sous-réseau de destination qui n'a pas de SNIP.

- Pour identifier le VLAN et l'interface utilisés par un sous-réseau :

  1. Accédez à **System>Réseau > VLAN**.
  2. Modifiez chaque VLAN configuré, à son tour, jusqu'à ce que vous trouviez l'adresse IP correcte comme expliqué à l'étape suivante.
  3. Cliquez sur l'onglet Liaisons IP pour voir quelle adresse IP, et donc quel sous-réseau est lié et utilise donc ce VLAN.
  4. Une fois que vous avez identifié le VLAN auquel une adresse IP est liée, où cette adresse

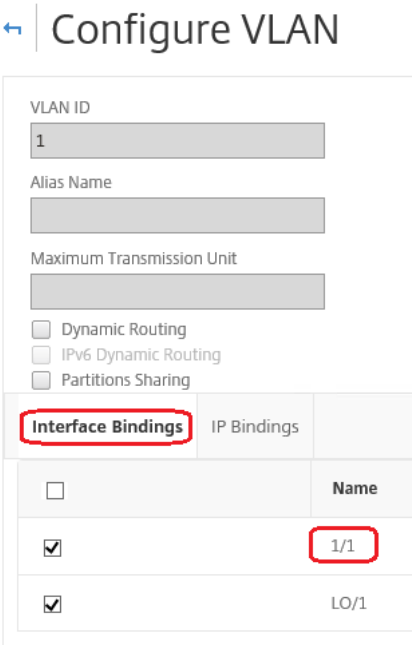
IP se trouve dans le sous-réseau de l'itinéraire par défaut, puis cliquez sur les liaisons d'interface. Chaque interface ou canal lié à ce VLAN sera utilisé.

Exemple

Supposons que l'itinéraire par défaut est`0.0.0.0 0.0.0.0 10.1.1.1`.

Supposons que vous avez deux SNIP de 10.0.0.5 et 10.1.1.69. Puisque 10.1.1.69 se trouve dans le sous-réseau de l'itinéraire par défaut, c'est celui que vous voulez rechercher. Dans les captures d'écran ci-dessous, nous examinons VLAN 1 et nous voyons l'IP 10.1.1.69 est lié à ce VLAN, donc nous savons que nous regardons le VLAN correct.

Cliquez maintenant sur Liaisons d'interface. Dans les liaisons de l'interface VLAN, nous voyons que l'interface`1/1` est utilisée pour ce sous-réseau, et est donc utilisée pour la route par défaut.



> **REMARQUE** :
>
> Si vous n'avez aucune adresse IP liée à vos VLAN, alors par défaut, il sera envoyé VLAN 1. Dans ce cas, regardez quelles interfaces sont liées au VLAN 1. Cela signifie également que NetScaler n'utilisera pas vos VLAN configurés pour le trafic qu'il initie, sauf si vous liez une IP au nouveau VLAN.

ARP gratuit

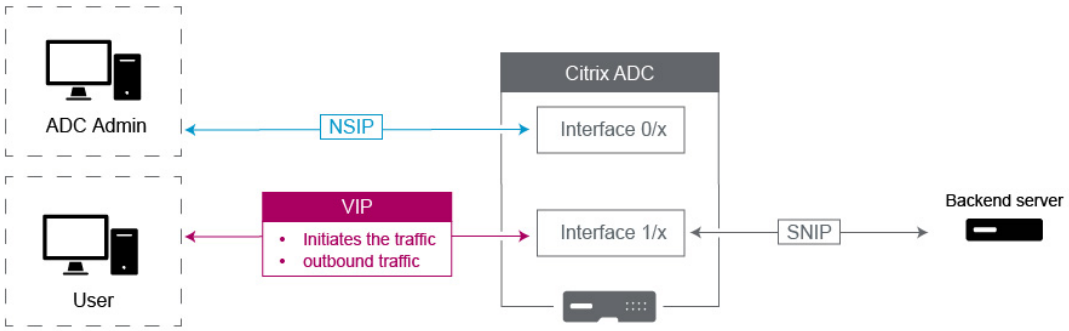
Si GARP ne fonctionne pas, utilisez VMAC - Par défaut, NetScaler utilise GARP pour annoncer ses liaisons d'adresse IP vers MAC sur d'autres périphériques réseau. Cela fonctionne généralement sans problème, cependant, lorsque vous créez plus de services dans NetScaler, vous pouvez commencer à

rencontrer des problèmes lors du basculement sur une paire HA. Le problème le plus courant est que les services restent en panne dans le NetScaler vers lequel vous avez échoué en raison du fait que certains périphériques réseau n'ont pas mis à jour leurs tables ARP avec la nouvelle adresse MAC. Vous pouvez facilement vérifier cela en vérifiant leurs tables ARP pour voir si les adresses MAC correspondent à celles du NetScaler maintenant primaire. Lorsque cela se produit, il est fort probable que certains de vos périphériques réseau limitent le nombre de publicités GARP qu'ils honorent. Dans ce cas, il est nécessaire de configurer VMAC sur toutes vos interfaces et/ou canaux actifs. Si vous prévoyez disposer d'une configuration volumineuse sur votre NetScaler, il peut être préférable de configurer VMAC pour toutes les interfaces et tous les canaux au cours du déploiement initial.

> **REMARQUE** :
>
> N'oubliez pas de configurer VMAC pour l'interface ou le canal utilisé par votre itinéraire par défaut.

Adresses IP détenues par Citrix ADC

Cette section décrit les meilleures pratiques pour configurer les adresses IP appartenant à Citrix ADC :



- **Citrix ADC IP (NSIP)** : Cette adresse IP est généralement utilisée pour la gestion car elle est la seule adresse IP unique à un NetScaler individuel dans un environnement HA ou Cluster. Il est également important de noter que le trafic du moniteur LDAP, RADIUS et User scripted Monitor (tel que le moniteur LDAP et le moniteur StoreFront) s'approvisionnera à partir du NSIP et acheminera ainsi sur le VLAN et l'interface auquel le NSIP est lié (VLAN natif par défaut 1). Si vous avez besoin de la source du trafic LDAP et RADIUS à partir du SNIP, créez un serveur virtuel LB pour vos serveurs back-end.
- **IP du sous-réseau (SNIP)** : Cette adresse IP est utilisée pour initier la communication vers les serveurs back-end et va toujours lancer le trafic. Cela dit, il peut être la destination du trafic

dans ces cas :

- Il peut être utilisé comme adresse de passerelle sur d'autres périphériques lors du routage de couche 3 sur NetScaler.
- Lorsqu'il est activé, il peut accepter des services de gestion, tels que l'accès à l'interface graphique, SSH et SNMP.

- **IP virtuelle (VIP)** : Le VIP est unique en ce sens qu'il ne sera jamais utilisé pour lancer le trafic sortant. Il est destiné à recevoir le trafic uniquement. Une fois qu'il reçoit du trafic, il répond et renvoie le trafic sortant au client. En d'autres termes, l'adresse VIP n'initie pas le trafic sortant.

Notez que cela signifie également qu'il n'est pas utilisé comme source pour communiquer avec les serveurs back-end utilisés dans, par exemple, un serveur virtuel LB.

Configurer pour source de trafic de données Citrix ADC FreeBSD à partir d'une adresse SNIP

August 20, 2021

Certaines fonctionnalités de données Citrix ADC s'exécutent sur le système d'exploitation FreeBSD sous-jacent plutôt que sur le système d'exploitation Citrix ADC. Pour cette raison, ces fonctionnalités envoient du trafic provenant de l'adresse IP Citrix ADC (NSIP) au lieu d'origine d'une adresse SNIP. Il n'est pas souhaitable d'approvisionner le trafic de données à partir de l'adresse NSIP si votre installation dispose de configurations pour séparer l'ensemble du trafic de gestion et de données.

Les fonctionnalités de données Citrix ADC suivantes s'exécutent sur le système d'exploitation FreeBSD sous-jacent et envoient le trafic provenant de l'adresse IP NSIP (Citrix ADC IP) :

- Moniteurs scriptables d'équilibrage de charge
- Synchronisation automatique GSLB

Pour résoudre ce problème, vous pouvez utiliser le paramètre Layer-2 global : `useNetprofileBSDtraffic` . Lorsque vous activez ce paramètre, les fonctionnalités Citrix ADC envoient le trafic provenant de l'une des adresses SNIP d'un profil réseau associé à la fonctionnalité.

Avant de commencer

Avant de configurer l'appliance Citrix ADC pour générer le trafic associé aux fonctionnalités Citrix ADC à partir d'une adresse SNIP, notez les points suivants :

- Actuellement, le paramètre Layer-2 global `useNetprofileBSDtraffic` est pris en charge uniquement pour les moniteurs scriptables d'équilibrage de charge.

Pour configurer l'appliance Citrix ADC de manière à ce que le trafic de synchronisation automatique GSLB source à partir d'une adresse SNIP, vous pouvez utiliser des règles ACL étendues et des règles RNAT comme solution de contournement.

- La `useNetprofileBSDtraffic` prise en charge des moniteurs scriptables d'équilibrage de charge s'applique uniquement aux profils réseau liés aux services associés. La `useNetprofileBSDtraffic` prise en charge ne s'applique pas aux profils réseau liés aux groupes de services associés.

  En d'autres termes, l'appliance Citrix ADC n'utilise aucune adresse SNIP provenant des profils réseau liés aux groupes de services pour l'approvisionnement de l'équilibrage de charge scriptable surveille le trafic.

- La `useNetprofileBSDtraffic` prise en charge ne s'applique pas aux services SSL.

  En d'autres termes, l'appliance Citrix ADC n'utilise aucune adresse SNIP provenant des profils réseau liés aux services SSL pour le script d'équilibrage de charge pour surveiller le trafic.

Configurer l'appliance Citrix ADC pour qu'il surveille le trafic à partir d'une adresse SNIP

La configuration de l'appliance Citrix ADC pour qu'il surveille le trafic à partir d'une adresse SNIP comprend les tâches suivantes :

- Activez le paramètre Layer-2 global `useNetprofileBSDtraffic`.
- Créez un profil réseau et liez au moins une adresse SNIP à celui-ci.
- Liez le profil réseau aux services d'équilibrage de charge qui utilisent des moniteurs scriptables.

Pour activer le paramètre Layer-2 UseNetProfilebSDTraffic à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set l2param** -**useNetprofileBSDtraffic** (**ENABLED** / **DISABLED**)
- **show l2param**

Pour créer un profil réseau et y lier des adresses SNIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add netProfile** <name> -**srcIP** <string>
- **afficher NetProfile**

Pour lier un profil réseau à un service d'équilibrage de charge à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set service** <name> -**netProfile** <string>

- **show service** <name>

Exemple de configuration

L'exemple de configuration suivant permet à une appliance Citrix ADC de surveiller le trafic à partir d'une adresse SNIP. Un profil réseau NETPROFILE-1 est configuré avec l'adresse SNIP 198.51.100.20 qui lui est liée. Un moniteur utilisateur/scriptable USER-MONITOR-1 est créé et est lié à un service d'équilibrage de charge SERVICE-1. NETPROFILE-1 est lié à SERVICE-1. L'appliance Citrix ADC source tous les paquets de moniteurs scriptables de USER-MONITOR-1 à partir de l'adresse SNIP 198.51.100.20.

```
set l2param -useNetprofileBSDtraffic ENABLED

set netprofile NETPROFILE-1 -srcip 198.51.100.20

add lb monitor USER-MONITOR-1 USER -scriptName nsftp.pl -scriptArgs "
    file=Index.png;user=nsroot;password=nsroot" -dispatcherIP 127.0.0.1
    -dispatcherPort 3013 -destIP 203.0.113.90 -destPort 21

bind service SERVICE-1 -monitorName USER-MONITOR-1

set service SERVICE-1 -netProfile NETPROFILE-1

<!--NeedCopy-->
```

Configurer l'appliance Citrix ADC pour générer le trafic de synchronisation automatique GSLB à partir d'une adresse SNIP

La configuration de l'appliance Citrix ADC pour le trafic de synchronisation automatique GSLB source à partir d'une adresse SNIP comprend les tâches de contournement suivantes :

- **Créez une règle ACL étendue**. Une règle ACL étendue identifie les paquets de synchronisation automatique GSLB. Cette identification est basée sur les adresses IP source et IP de destination.
- **Appliquer les listes d'accès**. L'application des listes d'accès active la règle ACL nouvellement créée.
- **Créez une règle RNAT basée sur ACL**. Une règle RNAT change l'adresse IP source de ces paquets de l'adresse NSIP à une adresse SNIP.

> **Remarque :**
>
> Dans une configuration de haute disponibilité ou de cluster, vous devez ajouter des règles ACL et RNAT pour toutes les adresses NSIP du programme d'installation.

Pour créer une liste d'accès étendue à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add acl** <aclname> **ALLOW** -**srcIP** = <NSIP address> -**destIP** = <destination IP address of the packets>
- **show acl** <aclName>

Pour appliquer des ACL étendues à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **apply acls**

Pour créer une règle RNAT basée sur ACL à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add rnat** <name> <aclname>
- **bind rnat** <name> -**natIP** <SNIP address - source IP address for the packets>
- **show rnat** <name>

Exemple de configuration

L'exemple de configuration suivant permet à une appliance Citrix ADC de générer du trafic de synchronisation automatique GSLB à partir d'une adresse SNIP. ACL-2 identifie les paquets de synchronisation automatique GSLB, qui proviennent de l'adresse NSIP 192.0.1.20 et destinés à l'adresse IP du site GSLB 203.0.113.20. RNAT-2 modifie l'adresse IP source en adresse SNIP 198.51.100.20 pour ces paquets identifiés.

```
add acl ACL-2 ALLOW -srcIP = 192.0.1.20  -destIP = 203.0.113.20

apply acls

add rnat RNAT-2 ACL-2

bind rnat RNAT-2 -natIP 198.51.100.20
<!--NeedCopy-->
```

Équilibrage de charge prioritaire

August 20, 2021

La fonction d'équilibrage de charge prioritaire vous permet d'attribuer un numéro de priorité à chacun des services ou groupes de services liés à un serveur virtuel d'équilibrage de charge prioritaire. Un service ou un groupe de services ayant le nombre le plus bas a la priorité la plus élevée. Le trafic

d'application est distribué uniquement à ce service ou à un groupe de services tant que ce service ou le groupe de services est UP. Le service ou le groupe de services auquel est attribué le numéro de priorité suivant ne devient opérationnel que lorsque tous les services ou membres du groupe de services ayant la priorité la plus élevée sont DOWN. Toutefois, lorsqu'un des services ou un membre du groupe de services ayant la priorité la plus élevée redevient disponible, le trafic est redirigé vers ce service ou le groupe de services.

Par exemple, considérez les groupes de services SVG1, SVG2 et SVG3 liés à un serveur virtuel d'équilibrage de charge prioritaire. Le nombre maximal de groupes de priorité est fixé à trois. Vous affectez la priorité à chaque groupe comme suit :

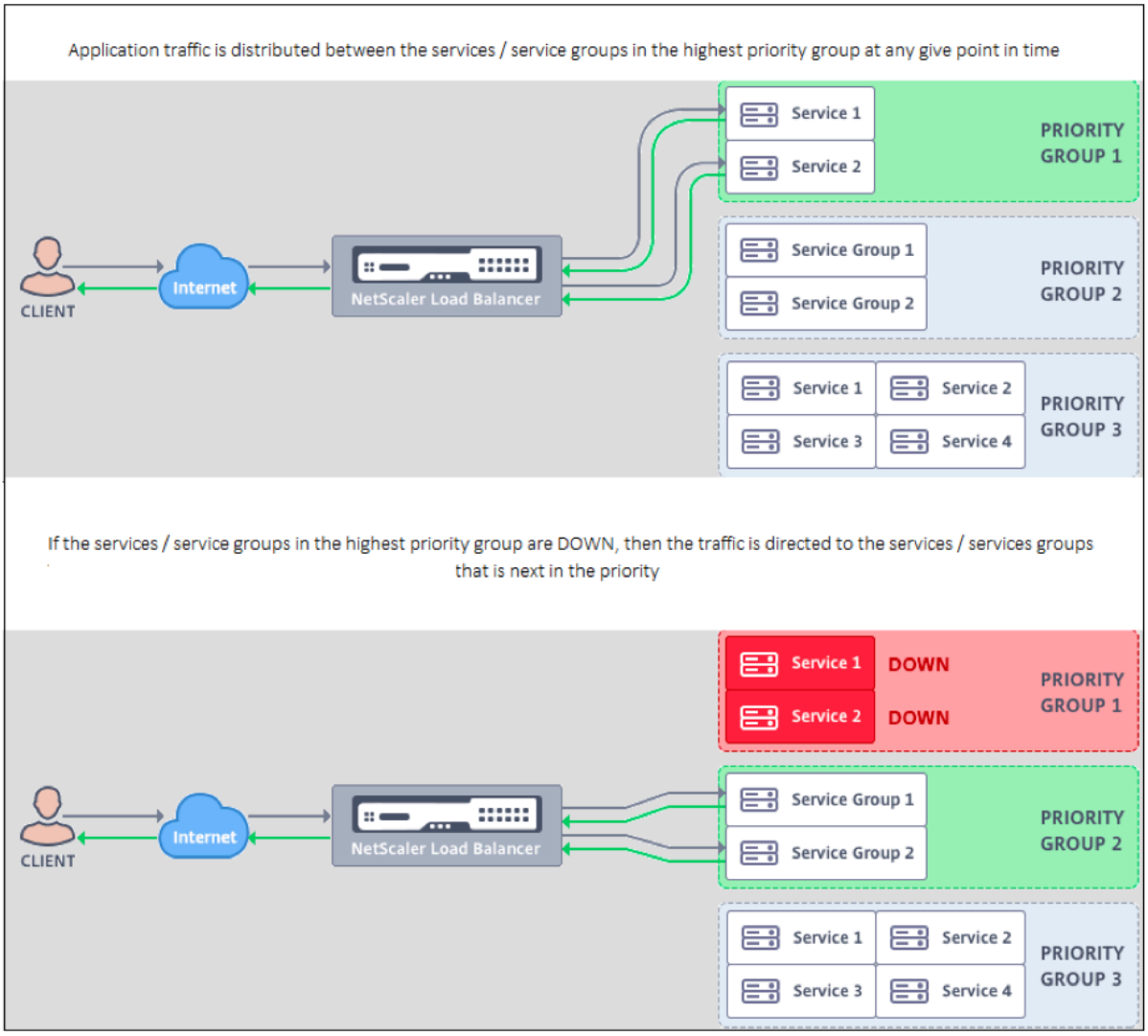
- SVG1 — priorité 1
- SVG2 — priorité 2
- SVG3 — priorité 3

Dans ce scénario, le trafic d'application est dirigé vers le groupe de services SVG1 car ce groupe reçoit le numéro de priorité le plus bas. Si tous les membres de SVG1 sont DOWN, le trafic est distribué au groupe de services SVG2 car ce groupe reçoit le numéro de priorité inférieur suivant. Si tous les membres de SVG2 sont également DOWN, le trafic est distribué à SVG3. Toutefois, lorsque l'un des membres de SVG1 est UP, le trafic est redirigé vers SVG1 car SVG1 est affecté au nombre le plus bas et a la priorité la plus élevée.

Vous pouvez attribuer une priorité à un service ou à un groupe de services pour mettre à niveau le service ou le groupe de services spécifique qui a la priorité la plus élevée, chaque fois que cela est nécessaire, avec un impact minimal ou nul sur le trafic de production.

En outre, si la mise à niveau échoue, vous pouvez basculer en toute sécurité vers le service ou le groupe de services qui est le suivant dans la priorité, avec un impact minimal ou nul sur le trafic de production.

La figure suivante illustre la fonction d'équilibrage de charge prioritaire.



Configurer l'équilibrage de charge prioritaire

> **Remarque**
>
> La configuration d'équilibrage de charge prioritaire Citrix ADC est prise en charge uniquement via l'interface graphique. Vous ne pouvez pas configurer l'équilibrage de la charge de priorité à l'aide de l'interface de ligne de commande.

1. Accédez à **Gestion du trafic** > **Équilibrage de charge prioritaire**> **Serveurs virtuels** et spécifiez le protocole du serveur virtuel, l'adresse IP et le numéro de port du serveur virtuel.
2. Dans la zone **Groupes de priorité maximale**, entrez le nombre de services prioritaires ou de groupes de services pouvant être liés à ce serveur virtuel. La valeur par défaut est 2 et la priorité maximale pouvant être définie est 10. Ce paramètre n'est pas modifiable une fois qu'il est configuré.

Remarque :

Après avoir spécifié le nombre maximal de groupes de priorité et cliqué sur **OK**, un serveur virtuel de commutation de contenu et un nombre « n » de serveurs virtuels d'équilibrage de charge de sauvegarde sont créés. L'alphabet « n » représente le nombre maximal de groupes prioritaires.

Par exemple, si vous avez entré le nom du serveur virtuel en tant que vs1 et que vous avez défini le groupe de priorité maximale sur 5, un serveur virtuel de commutation de contenu avec le nom `_Pri.LB##vs1##MaxPri=5` et les 5 serveurs virtuels d'équilibrage de charge suivants sont créés.

- `_Pri.LB##vs1##MaxPri=5_LB1`
- `_Pri.LB##vs1##MaxPri=5_LB2`
- `_Pri.LB##vs1##MaxPri=5_LB3`
- `_Pri.LB##vs1##MaxPri=5_LB4`
- `_Pri.LB##vs1##MaxPri=5_LB5`

3. Après avoir spécifié le nombre maximal de groupes de priorité et cliqué sur **OK**, vous êtes invité à choisir les services ou groupes de services qui doivent être liés à ce serveur virtuel de commutation de contenu.

   - Pour lier des services au serveur virtuel, cliquez sur **Insérer** dans la section Services. Ensuite, sélectionnez un service existant ou créez un service et définissez la priorité pour ce service. Définissez également le numéro de priorité auquel ce service doit être lié.
   - Pour lier des groupes de services au serveur virtuel, cliquez sur **Insérer** dans la section Groupes de services. Ensuite, sélectionnez un groupe de services existant ou créez un groupe de services et définissez la priorité pour ce groupe de services. Définissez également le numéro de priorité auquel ce groupe de services doit être lié.

   Répétez l'étape 3 en fonction du nombre maximal de groupes de priorités que vous avez saisis.

   Remarque :

   - Le service ou le groupe de services ayant la priorité la plus élevée est lié au serveur virtuel d'équilibrage de charge qui représente la priorité la plus élevée.

   Par exemple, si vous avez attribué `SG_App1 and SG_App2` respectivement la priorité 1 et 2 aux groupes de services, `SG_App1` est lié à `virtual server _Pri.LB##vs1##MaxPri=5_LB1` `and SG_App2` est lié à `virtual server _Pri.LB##vs1##MaxPri=5_LB2` créé à l'étape 2.

   - Pour modifier la priorité du groupe de services ou du service, cliquez sur l'icône Modifier dans la page Priority Load Balancing Virtual Server et modifiez la priorité si nécessaire.
   - Vous ne pouvez pas définir explicitement les méthodes d'équilibrage de charge et la persistance pour chaque serveur virtuel, car la configuration de tous les serveurs virtuels d'équilibrage de charge est identique.

4. Dans les sections Paramètres avancés, complétez l'autre configuration qui répond à vos besoins.

> **Important :**
>
> Les entités créées lors de la configuration d'équilibrage de charge prioritaire ne doivent pas être modifiées à partir d'autres onglets de l'interface graphique ni de l'interface de ligne de commande. Il est recommandé de modifier les entités d'équilibrage de charge prioritaires à partir de l'onglet Équilibrage de charge prioritaire uniquement.

Extensions Citrix ADC

January 21, 2021

Les extensions Citrix ADC peuvent être utilisées pour personnaliser une appliance Citrix ADC en écrivant un code d'extension. Actuellement, les extensions de stratégie et les extensions de protocole sont prises en charge. Les extensions de stratégie peuvent être utilisées pour étendre le langage de stratégie. Les extensions de protocole peuvent être utilisées pour ajouter la prise en charge des protocoles personnalisés sur une appliance Citrix ADC.

Les extensions Citrix ADC sont également prises en charge sur Citrix ADC CPX.

Ce document contient les renseignements suivants :

- Extensions Citrix ADC - Présentation de la langue
- Extensions Citrix ADC - Référence de la bibliothèque
- Référence de l'API Citrix ADC Extensions
- Extensions de protocole
- Extensions de stratégie

Extensions Citrix ADC - Présentation du language

January 21, 2021

Le langage d'extension est basé sur le langage de programmation Lua 5.2. Lua fournit un moteur d'exécution compact avec de bonnes performances conçu pour l'intégration dans des programmes C, comme le logiciel Citrix ADC.

Le langage d'extension est typé dynamiquement, ce qui signifie que chaque objet possède ses propres informations de type. Toute variable peut contenir n'importe quel type à tout moment pendant l'exécution, de sorte que les types variables ne sont pas déclarés.

La langue est également sous forme libre, où l'espace blanc entre les jetons est ignoré. Les instructions peuvent être séparées par des points-virgules, mais ce n'est pas obligatoire et généralement pas fait. Les blocs d'instructions sont généralement terminés par la fin. Il n'y a pas de crochets autour des blocs comme le {and} en C ou Java.

Les identificateurs sont des séquences de lettres (a à z et A à Z), de chiffres (0 à 9) et de traits de soulignement (_), qui ne commencent pas par un chiffre. Les identificateurs sont sensibles à la casse, donc var, VAR et Var sont tous des identificateurs différents.

Les commentaires sont commencés par —. Tout après — est ignoré jusqu'à la fin de la ligne. Exemple :

```
-- This is a comment.
```

Types simples

August 20, 2021

Le langage permet des valeurs des types simples suivants :

- Chiffres
- Chaînes
- Booléen
- Nil
- Autres types

Chiffres

Tous les nombres (entiers pairs) sont représentés par des valeurs à virgule flottante IEEE 754. Les entiers jusqu'à 2^54 ont des représentations exactes. Les valeurs numériques peuvent être représentées par :

- Nombres entiers décimaux signés et non signés (exemples : 10, -5)
- Nombre réel avec des points décimaux (10.5, 3.14159)
- Nombre réel avec exposants (1.0e+10)
- Hexadécimales (0xffff0000)

Les expressions de stratégie Citrix ADC ont trois types numériques :

- Nombre entier 32 bits (num_at)
- Nombre entier 64 bits (unsigned_long_at)
- virgule flottante 64 bits (double_at)

Tous ces éléments sont convertis dans le type de nombre lorsqu'ils sont transmis dans une fonction d'extension, et les nombres sont convertis au type numérique de stratégie attendu lorsqu'ils sont renvoyés.

Chaînes

Les chaînes sont des séquences d'octets de n'importe quelle longueur. Ils correspondent au type **text_at** de la stratégie. Les chaînes peuvent contenir des octets nuls (0x00). Les données binaires arbitraires peuvent être conservées dans des chaînes, y compris toute représentation de code de caractères (par exemple UTF-8 et Unicode complet). Cependant, les fonctions de chaîne **likestring.upper()** supposent ASCII 8 bits.

Les chaînes sont automatiquement allouées lorsqu'elles sont utilisées. Il n'y a pas besoin (ou même moyen) d'allouer explicitement des tampons pour les chaînes. Les chaînes sont également automatiquement désallouées par nettoyage de la mémoire lorsqu'elles ne sont plus utilisées. Il n'y a pas besoin (ou même moyen) de libérer explicitement des chaînes. Cette allocation et désaffectation automatiques évite certains problèmes courants dans des langages comme C, tels que les fuites de mémoire et les pointeurs pendants.

Les littéraux de chaîne sont des chaînes de caractères entre guillemets doubles ou simples. Il n'y a pas de différence entre les deux types de guillemets : « un littéral de chaîne » est le même que « une chaîne littérale ». La barre oblique inverse habituelle est disponible : \s (bell), \b (backspace), \f (feed de formulaire), \n (saut de ligne), \t (onglet horizontal), \\ (barre oblique inverse), \" (guillemet double) et \' (guillemet simple). Les valeurs décimales d'octets peuvent être saisies par une barre oblique inverse et un à trois chiffres (d, dd, ddd). Les valeurs d'octets hexadécimaux peuvent être saisies par une barre oblique inverse, un x et deux chiffres hexadécimaux (xhh)

Un appel de syntaxe spécial, la notation de crochets longs peut être utilisé pour de longs littéraux de chaînes multilignes. Cette notation enferme la chaîne entre crochets doubles avec zéro ou plus de signes égaux entre les parenthèses — l'idée est de trouver une combinaison de crochets et d'égaux qui ne se trouve pas dans la chaîne. Aucune séquence d'échappement n'est respectée dans la chaîne. Exemples :

[[This is a multi-line string using long bracket notation.]]

[= [Il s'agit d'une chaîne multiligne utilisant une notation longue avec [et]] et une chaîne inexploitée.] =]

La notation de crochets longs peut être utilisée pour faire un commentaire multi-ligne. Exemple :

—[[
Il s'agit d'un commentaire multiligne.
–]]

Booléen

Les valeurs booléennes vraies et fausses habituelles sont fournies. Notez que les valeurs booléennes sont différentes des valeurs numériques, contrairement à C où zéro est supposé être faux et toute valeur non nulle est vraie.

Nil

nil est une valeur spéciale qui signifie « aucune valeur ». Il est son propre type et n'est équivalent à aucune autre valeur, contrairement à C où NULL est défini comme zéro.

Autres types

Il existe deux autres types, userdata et threads. Ce sont des sujets avancés qui ne sont pas abordés ici.

Variables

January 21, 2021

Les variables contiennent des valeurs qui peuvent changer lors de l'exécution de l'extension. En raison du typage dynamique, toute variable peut contenir des valeurs de n'importe quel type. Il n'y a pas de déclaration de type pour les variables. Au lieu de cela, le type d'une variable est déterminé au moment de l'exécution. En fait, le type de valeur d'une variable peut changer pendant l'exécution, bien que ce ne soit pas une pratique recommandée. Une variable a initialement la valeur nil.

Les noms de variables sont des identificateurs, de même que les chaînes de lettres, de chiffres et de traits de soulignement qui ne commencent pas par un chiffre. Exemples : en-têtes, en-têtes combined_headers.

Variables globales

Dans Lua, les variables qui ne sont pas déclarées autrement sont globales au sein du programme. Cependant, les variables globales ne sont pas autorisées dans les fonctions d'extension de stratégie, car il existe plusieurs moteurs de paquets dans lesquels une fonction peut être exécutée, et chaque moteur de paquets a sa propre mémoire.

Si vous utilisez une variable globale dans votre extension, vous obtiendrez une erreur d'exécution : essayez de mettre à jour ou de créer un rapport global dans **/var/log/ns.log**.

Les fautes de frappe dans les noms de variables sont un problème potentiel, car la variable avec la faute de frappe sera interprétée comme une autre variable globale et ne provoquera pas d'erreur de

syntaxe comme dans un langage comme C ou Java. Comme indiqué ci-dessus, vous obtiendrez une erreur d'exécution à la place.

Variables locales

Une variable peut être déclarée locale à un bloc d'instructions, comme une fonction. Ceci est fait par nom variable local. La variable sera portée au bloc, c'est-à-dire qu'elle n'existera que dans le bloc. La déclaration locale peut éventuellement affecter une valeur à la variable.

Exemples :

```
local headers = {}
local combined_headers = {}
```

Expressions

January 21, 2021

Les expressions calculent les valeurs à partir de valeurs variables et littérales.

- Opérations arithmétiques
- Opérations relationnelles
- Opérations logiques
- Concaténation
- Longueur
- Priorité

Opérations arithmétiques

Les opérations arithmétiques sont effectuées sur les valeurs numériques. Si une valeur de chaîne est utilisée dans une opération arithmétique, elle est convertie en nombre — si cela échoue, une erreur est renvoyée.

a + b	ajouter a et b
a - b	soustraire b de a
a * b	multiplier a et b
a/b	diviser a par b
a% b	modulo = a - math.floor(a/b)*b

a ^ b	élever a à la puissance b ; b peut être n'importe quel nombre
-a	annule a

Opérations relationnelles

Les opérations relationnelles comparent deux valeurs et retournent true si la relation est satisfaite et false si ce n'est pas le cas. Des opérations relationnelles peuvent être effectuées entre des valeurs de n'importe quel type. Si les valeurs ne sont pas du même type, false est renvoyé. Les nombres sont comparés de la manière habituelle. Les chaînes sont comparées à l'aide de la séquence de classement pour les paramètres régionaux actuels.

a == b	a est égal à b
a ~= b	a n'est pas égal à b
a < b	a est inférieur à b
a > b	a est supérieur à b
a <= b	a est inférieur ou égal à b
a >= b	a est supérieur ou égal à b

Opérations logiques

Les opérations logiques sont traditionnellement effectuées sur des valeurs booléennes, mais dans ce langage, elles peuvent être effectuées sur deux valeurs. nil et false est considéré comme faux et toute autre valeur est considérée comme vrai. Les opérations logiques utilisent l'évaluation raccourci, où si la première valeur détermine le résultat de l'opération, la deuxième valeur n'est pas évaluée.

a and b	si a est faux ou nul alors retournez un autre retour b
a or b	si a n'est pas faux et pas nul alors retournez un autre retour b

not a	si un n'est pas faux ou nul retourne faux sinon retourne vrai

Les opérations et et ou peuvent être utilisées pour l'évaluation conditionnelle dans une expression :

a or b	peut être utilisé pour fournir une valeur par défaut b si a est non initialisé (nil). Ceci est utile pour les paramètres optionnels dans les fonctions.
a and b or c	peut être utilisé pour choisir non néant b ou c en fonction de la condition a. Si a est vrai, alors a et b renvoie b, et b ou c renvoie b. Si a est faux, alors a et b renvoie false et false ou c renvoie c. Cela équivaut à a ? b: c dans le langage de programmation C.

Concaténation

La concaténation de chaîne est s1.. s2. Cela crée une nouvelle chaîne assez grande pour contenir le contenu de s1 et s2 et copie le contenu dans la nouvelle chaîne. Une erreur se produit si s1 ou s2 ne sont pas des chaînes. Notez que la concaténation répétée peut avoir des frais de copie considérables. Si vous construisez une chaîne de n octets en concaténant un octet à la fois, cela copiera n* (n+1) /2 octets. Pour de meilleures performances, vous pouvez mettre des morceaux d'une chaîne à concaténer dans une table (discuté plus loin), puis utiliser la fonction table.concat (). Un exemple de ceci est illustré dans l'exemple COMBINE_HEADERS ().

Longueur

La longueur d'une chaîne s est renvoyée par #s. L'opérateur # est également utilisé avec les tables de tableau, comme discuté plus loin.

Priorité

La priorité de l'opérateur détermine l'ordre dans lequel les opérations sont exécutées dans une expression, avec des opérations de priorité supérieure effectuées avant celles de priorité inférieure. L'ordre

de priorité peut, comme d'habitude, être remplacé par des parenthèses. Par exemple, dans`a + b \* c`, * a une priorité supérieure à +, de sorte que l'expression est évaluée comme`a + (b \* c)`.

highest	^
-	not # - (unary)
-	* / %
-	..
-	= ~= < > <= >=
-	and
lowest	ou

Les opérations avec la même priorité sont exécutées de gauche à droite (associative gauche), sauf ^ et.. qui sont exécutées de droite à gauche (associative droite). Donc a^b^c est évalué comme a^(b^c).

Attribution

January 21, 2021

L'instruction affectation évalue une expression et affecte la valeur résultante à une variable.

```
variable = expression
```

Comme indiqué précédemment, les valeurs de n'importe quel type peuvent être affectées à n'importe quelle variable, de sorte que ce qui suit est autorisé :

```
local v1 = "a string literal"
v1 = 10
```

Une instruction d'affectation peut réellement définir plusieurs variables, en utilisant le formulaire

variable1, variable2, … = expression1, expression2, …

S'il y a plus de variables que d'expressions, les variables supplémentaires sont affectées à zéro. S'il y a plus d'expressions que de variables, les valeurs d'expression supplémentaires sont ignorées. Les expressions sont toutes évaluées avant les affectations, de sorte que cela peut être utilisé pour échanger succinctement les valeurs de deux variables :

v1, v2 = v2, v1

équivaut à

tmp = v1
v2 = v1
v1 = tmp

Tables

August 20, 2021

Les tables sont des collections d'entrées avec des clés et des valeurs. Il s'agit de la seule structure de données agrégées fournie. Toutes les autres structures de données (tableaux, listes, ensembles, etc.) sont construites à partir de tables. Les clés et les valeurs de table peuvent être n'importe quel type, y compris d'autres tables. Les clés et les valeurs d'une même table peuvent mélanger les types.

- Constructeurs de table
- Utilisation de la table
- Tables en tant que tableaux
- Tables en tant qu'enregistrements

Constructeurs de table

Les constructeurs de table vous permettent de spécifier une table avec des clés et des valeurs associées. La syntaxe est :

{[key1] = value1, [key2] = value2, …}

où les clés et les valeurs sont des expressions. Si les clés sont des chaînes qui ne sont pas des mots réservés, les crochets et les guillemets autour des clés peuvent être omis. Exemple :

{key1 = "value1", key2 = "value2", key3 = "value3"}

Une table vide est spécifiée simplement par {}.

Un constructeur de table peut être utilisé dans une affectation pour définir une variable pour faire référence à une table. Exemples :

local t1 = {} – set t1 to an empty table
local t2 = {key1 = "value1", key2 = "value2", key3 = "value3"}

Notez que les tables elles-mêmes sont anonymes. Plusieurs variables peuvent faire référence à la même table. Poursuivant l'exemple ci-dessus :

t3 local = t2 - t2 et t3 se réfèrent à la même table

Utilisation de la table

Comme vous vous y attendiez, vous pouvez utiliser des clés pour trouver des valeurs dans une table. La syntaxe est la[clé]de table, où table est une référence de table (généralement une variable assignée à une table), et key est une expression fournissant la clé. Si cela est utilisé dans une expression et que la clé existe dans la table, cela renvoie la valeur associée à la clé. Si la clé n'est pas dans la table, cela renvoie nil. Si elle est utilisée comme variable dans une affectation et que la clé n'existe pas dans la table, elle crée une nouvelle entrée pour la clé et la valeur. Si la clé existe déjà dans la table, elle remplace la valeur de la clé par la nouvelle valeur. Exemples :

local t = {} — définit t sur une table vide
t[« k1"] = « v1" — crée une entrée pour la clé « k1" et la valeur « v1"
v1 = t[« k1"] — définit v1 à la valeur de la clé « k1" = « v1"
t[« k1"] = « nouveau_v1" — définit la valeur de la clé « k1 » sur « new_v1"

Tableau en tant que tableaux

Le tableau traditionnel peut être implémenté en utilisant une table avec des clés entières comme indices. Un tableau peut avoir des indices, y compris négatifs, mais la convention est de démarrer des tableaux à l'index 1 (pas 0 comme c'est le cas avec des langages comme C et Java). Il existe un constructeur de table à usage spécial pour de tels tableaux :

{value1, value2, value3, … }

Les références de tableaux sont alors des[index de]tableaux.

L'opérateur de longueur # renvoie le nombre d'éléments dans un tableau avec des indices consécutifs commençant à 1. Exemple :

local a = {"value1", "value2", "value3"}
local length = #a – sets length to the length of array a = 3

Les tableaux peuvent être clairsemés, où seuls les éléments définis sont alloués. Mais # ne peut pas être utilisé sur un tableau clairsemé avec des indices non consécutifs. Exemple :

local sparse_array = {} — configurer un tableau vide
sparse_array[1] = « value1" — ajouter un élément à l'index 1
sparse_array[99] = « value99 » — ajouter un élément à l'index 99

Les tableaux multidimensionnels peuvent être configurés en tant que tables de tables. Par exemple, une matrice 3x3 peut être configurée par :

local m = {{1, 2, 3}, {4, 5, 6}, {7, 8, 9}}
local v22 = m[2][2] — définit v22 à 5

Tables en tant qu'enregistrements

Les enregistrements avec des champs peuvent être implémentés sous forme de tables avec des clés de nom de champ. Le formulaire de référence table.field peut être utilisé pour la table[« field »]. Exemples :

local person = {name = "John Smith", phone = "777-777-7777"}
local name = person.name – sets name to "John Smith"

Un tableau de tables peut être utilisé pour une séquence d'enregistrements. Exemple :

local people = {
{name = "John Smith", phone = "777-777-7777"},
{name = "Jane Doe", phone = "888-888-8888"}
…
}

name = people[2].name — définit le nom sur « Jane Doe »

Structures de contrôle

August 20, 2021

Le langage de la fonction d'extension fournit les instructions habituelles pour contrôler l'exécution du programme.

- If Then Else
- While Do and Repeat Until
- Numeric For
- Break
- Goto

If Then Else

Si les instructions sélectionnent des blocs d'instructions à exécuter en fonction d'une ou plusieurs conditions. Il existe trois formes :

If then Form

```
if expression then
     statements to execute if expression is not false or nil
end
<!--NeedCopy-->
```


If then else Form

```
if expression then
     statements to execute if expression is not false or nil
else
     statements to execute if expression is false or nil
end
<!--NeedCopy-->
```

If then elseif else Form

```
if expression1 then
     statements to execute if expression1 is not false or nil
     elseif expression2 then
          statements to execute if expression2 is not false or nil
. . .
else
     statements to execute if all expressions are false or nil
end
<!--NeedCopy-->
```

Exemple :

```
if headers[name] then

     local next_value_index = #(headers[name]) + 1
     headers[name][next_value_index] = value

else

     headers[name] = {
 name .. ":" .. value }


end
<!--NeedCopy-->
```

Remarque :

- L'expression n'est pas comprise entre parenthèses comme c'est le cas en C et Java.
- Il n'y a pas d'équivalent à l'instruction de commutateur C/Java. Vous devez utiliser une série d'instructions if elseif pour faire l'équivalent.

While Do and Repeat Until

Les instructions **while** et **repeat** fournissent des boucles contrôlées par une expression.

```
while expression do
     statements to execute while expression is not false or nil
end

repeat

     statements to execute until expression is not false or nil

until expression
<!--NeedCopy-->
```

Exemple pour tout :

```
local a = {
 1, 2, 3, 4 }

local sum, i = 0, 1 -- multiple assignment initializing sum and i
while i <= #a do -- check if at the end of the array
     sum = sum + a[i] -- add array element with index i to sum
     i = i + 1 -- move to the next element
end
<!--NeedCopy-->
```

Exemple de répétition :

```
sum, i = 0, 1 -- multiple assignment initializing sum and i
repeat
     sum = sum + a[i] -- add array element with index i to sum
     i = i + 1 -- move to the next element
until i > #a -- check if past the end of the array
<!--NeedCopy-->
```

Bien sûr, il est possible d'écrire une boucle qui ne se termine pas, par exemple, si vous omettez l'instruction i = i + 1 dans l'un de ces exemples. Lorsqu'une telle fonction est exécutée, Citrix ADC détectera que la fonction ne s'est pas terminée dans un délai raisonnable et la tuera avec une erreur d'exécution :

```
Cpu limit reached. Terminating extension execution in [[string "function
extension function..."]]: line line-number.
```

sera signalé dans /var/log/ns.log.

Numeric For

Il existe deux types de boucles pour. Le premier est le numérique for, qui est similaire à l'utilisation habituelle de l'instruction for en C et Java. L'instruction numérique pour initialise une variable, teste si la variable a passé une valeur finale, et sinon exécute un bloc d'instructions, incrémente la variable et se répète. La syntaxe de la boucle numérique for est :

```
for variable = initial, final, increment do

     statements in the loop body

end
<!--NeedCopy-->
```

où initial, final et incrément sont toutes les expressions qui génèrent (ou peuvent être converties en) des nombres. variable est considérée comme locale au bloc d'instruction de boucle for ; elle ne peut pas être utilisée en dehors de la boucle. incrément peut être omis ; la valeur par défaut est 1. Les expressions sont évaluées une fois au début de la boucle. La condition de fin est variable > final si l'incrément est positif et variable < final si l'incrément est négatif. La boucle se termine immédiatement si l'incrément est 0.

Exemple (équivalent aux boucles while et repeat dans la section précédente) :

```
sum = 0
for i = 1, #a do -- increment defaults to 1
     sum = sum + a[i]
end
<!--NeedCopy-->
```

Le deuxième type de boucle for est le générique pour, qui peut être utilisé pour les types de boucles plus flexibles. Il implique l'utilisation de fonctions, donc sera discuté plus tard après l'introduction des fonctions.

Break

L'instruction break est utilisée dans une boucle while, repeat ou for. Il mettra fin à la boucle et reprendra l'exécution à la première instruction après la boucle. Exemple (également équivalent à la précédente while, repeat, et pour les boucles) :

```
sum, i = 0, 1
while true do
     if i > #a then
          break
     end
```



```
6       sum = sum + a[i]
7       i = i + 1
8   end
9   <!--NeedCopy-->
```

Goto

L'instruction goto peut être utilisée pour sauter en avant ou en arrière vers une étiquette. L'étiquette est un identifiant et sa syntaxe est ::label::. L'instruction goto est l'étiquette goto. Exemple (une fois de plus équivalent aux boucles précédentes) :

```
1   sum, i = 0, 1
2   ::start_loop::
3       if i > #a then
4           goto end_loop -- forward jump
5       end
6       sum = sum + a[i]
7       i = i + 1
8       goto start_loop -- backwards jump
9   ::end_loop::
10  . . .
11  <!--NeedCopy-->
```

Il y a eu une controverse depuis longtemps sur l'utilisation de gotos dans la programmation. En général, vous devriez essayer d'utiliser les autres structures de contrôle pour rendre vos fonctions plus lisibles et fiables. Mais l'utilisation judicieuse occasionnelle des gotos peut conduire à de meilleurs programmes. En particulier, les gotos peuvent être utiles pour gérer les erreurs.

Fonctions

October 5, 2021

Les fonctions sont un élément de base de la programmation. Elles constituent un moyen pratique et puissant de regrouper des instructions exécutant une tâche. Il s'agit de l'interface entre l'appliance Citrix ADC et le code d'extension. Pour les stratégies, vous définissez des fonctions d'extension de stratégie. Pour les protocoles, vous implémentez des fonctions de rappel pour les comportements de protocole. Les fonctions sont constituées de définitions de fonctions qui spécifient quelles valeurs sont passées dans et hors de la fonction et quelles instructions sont exécutées pour la fonction, et d'appels de fonction, qui exécutent des fonctions avec des données d'entrée spécifiques et obtiennent des résultats de la fonction.

Fonctions de rappel du comportement du protocole

Le comportement du client TCP consiste en une fonction de rappel (on_data) qui traite les événements de flux de données du client TCP. Pour implémenter l'équilibrage de charge basé sur les messages (MBLB) pour un protocole TCP, vous pouvez ajouter du code pour cette fonction de rappel afin de traiter le flux de données TCP provenant du client et d'analyser le flux d'octets en messages de protocole.

Les fonctions de rappel d'un comportement sont appelées avec un contexte, qui correspond à l'état du module de traitement. Le contexte est l'instance du module de traitement. Par exemple, les rappels du comportement du client TCP sont appelés avec différents contextes pour différentes connexions TCP clientes.

En plus du contexte, les fonctions de rappel de comportement peuvent comporter d'autres arguments. Habituellement, le reste des arguments est passé en tant que charge utile, qui est la collection de tous les arguments. Ainsi, les instances du module de traitement programmable peuvent être considérées comme une combinaison de fonctions d'état d'instance et de rappel d'événement, c'est-à-dire le contexte et le comportement. Et le trafic circule à travers le pipeline comme charge utile d'événement.

Prototype de la fonction de rappel client TCP :

```
1             Function                client on_data (ctxt, payload)
2
3                                             //.code
4
5             end
```

Où,

- ctxt - Contexte de traitement du client TCP
- payload — charge utile d'événement
  - payload.data : données TCP reçues, disponibles sous forme de flux d'octets

Fonctions d'extension de stratégie

Étant donné que le langage d'expression de stratégie NetScaler est tapé, la définition d'une fonction d'extension doit spécifier les types de ses entrées et sa valeur de retour. La définition **de la fonction Lua** a été étendue pour inclure ces types :

,

function self-type: function-name(parameter1: parameter1-type, and so on): return-type
statements
end

Où,

Les types sont NSTEXT, NSNUM, NSBOOL ou NSDOUBLE.
‘

Self-type est le type de l’auto-paramètre implicite qui est passé à la fonction. Lorsque la fonction d’extension est utilisée dans une expression de stratégie Citrix ADC, il s’agit de la valeur générée par l’expression située à gauche de la fonction. Une autre façon de voir cela est que la fonction étend ce type dans le langage de stratégie Citrix ADC.

Les types de paramètres sont les types de chaque paramètre spécifié dans l’appel de fonction d’extension dans l’expression de stratégie. Une fonction d’extension peut avoir zéro paramètre ou plus.

Type de retour est le type de la valeur renvoyée par l’appel de la fonction d’extension. Il s’agit de l’entrée de la partie de l’expression de stratégie, le cas échéant, à droite de la fonction, ou bien de la valeur du résultat de l’expression.

Exemple :

```
function NSTEXT:COMBINE_HEADERS(): NSTEXT
```

Utilisation de la fonction d’extension dans une expression de stratégie :

```
HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1\r\n").COMBINE_HEADERS()
```

Ici, l’auto-paramètre est le résultat de `HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1\r\n")`, qui est une valeur de texte. Le résultat de l’appel COMBINE_HEADERS () est du texte, et comme il n’y a rien à droite de cet appel, le résultat de l’expression entière est du texte.

Définition de la fonction locale

Outre les fonctions d’extension, aucune fonction globale ne peut être définie dans un fichier d’extension. Mais les fonctions locales peuvent être définies dans les fonctions d’extension à l’aide de l’instruction normale de la fonction Lua. Cela déclare le nom de la fonction et les noms de ses paramètres (également appelés arguments), et comme toutes les déclarations de Lua, ne spécifie aucun type. La syntaxe est la suivante :

’

local function function-name(parameter1-name, parameter2-name, and so on)
statements
end
‘

Les noms des fonctions et des paramètres sont tous des identificateurs. (Le nom de la fonction est en fait une variable et l’instruction de fonction est un raccourci pour nom-fonction locale = fonction

(paramètre1, etc.), mais vous n'avez pas besoin de comprendre cette subtilité pour utiliser des fonctions.)

Notez que, et ainsi de suite, est utilisé ici pour la continuation du modèle des noms de paramètres au lieu de l'habituel…. C'est parce que… lui-même signifie en fait une liste de paramètres variables, qui ne sera pas discutée ici.

Corps de fonction et retour

Le bloc d'instructions entre la fonction et les instructions de fin est le corps de la fonction. Dans le corps de la fonction, les paramètres de la fonction agissent comme des variables locales, avec des valeurs fournies par les appels de fonction, comme décrit précédemment.

L'instruction return fournit les valeurs à renvoyer à l'appelant de la fonction. Il doit apparaître à la fin d'un bloc (dans une fonction, si alors, for loop, etc. ; Il peut être dans son propre bloc do return… end). Il peut spécifier aucune valeur de retour, une ou plusieurs valeurs de retour :

’

return — renvoie une expression de
retour nulle — une valeur
renvoyée renvoie expression1, expression2,… — plusieurs valeurs renvoyées
‘

Exemples :

‘fonction
locale fsum (a) somme
locale = 0
pour i = 1, #a do
sum = sum + a[i]
end
return sum
end

Fonction locale fsum_and_average (a) somme
locale = 0
pour i = 1, #a do
sum = sum + une somme de
retour de[i]
fin, sum/ #a
fin
‘

Les appels de fonctions

Un appel de fonction exécute le corps d'une fonction, fournit des valeurs pour ses paramètres et reçoit des résultats. La syntaxe d'un appel de fonction est nom-fonction (expression1, expression2, etc.), où les paramètres de la fonction sont définis sur les expressions correspondantes. Le nombre d'expressions et de paramètres ne doit pas nécessairement être le même. S'il y a moins d'expressions que de paramètres, les paramètres restants sont définis sur zéro. Vous pouvez donc rendre un ou plusieurs paramètres facultatifs à la fin de l'appel, et votre fonction peut vérifier s'ils sont spécifiés en vérifiant s'ils ne sont pas nuls. Une façon courante de procéder consiste à utiliser l'opération ou :

```
fonction f (p1, p2) — p2 est optionnel
p2 = p2 ou 0 — si p2 est nul, la valeur par défaut est 0
.
fin
```

S'il y a plus d'expressions que de paramètres, les valeurs d'expression restantes sont ignorées.

Comme indiqué précédemment, les fonctions peuvent renvoyer plusieurs valeurs. Ces retours peuvent être utilisés dans une instruction d'affectation multiple. Exemple :

```
local my_array = {1, 2, 3, 4} my_sum
local, my_ave = sum_and_average (my_array)
```

Fonctions d'itérateur et boucles génériques for

Maintenant que nous avons introduit des fonctions, nous pouvons parler de boucles for génériques. La syntaxe de la boucle for générique (avec une variable) est la suivante :

```
for variable in iterator (parameter1, parameter2, etc.) do
instructions dans la
fin du corps de la boucle for
```

Où iterator () est une fonction avec zéro ou plus de paramètres qui fournissent une valeur pour la variable à chaque itération du corps de la boucle. La fonction itérateur garde une trace de son emplacement dans l'itération à l'aide d'une technique appelée closure, dont vous n'avez pas à vous soucier ici. Il signale la fin de l'itération en renvoyant zéro. Les fonctions d'itérateur peuvent renvoyer plus d'une valeur, à utiliser dans plusieurs affectations.

L'écriture d'une fonction itérateur dépasse le cadre de cet article, mais il existe peu d'itérateurs intégrés utiles qui illustrent le concept. L'un est l'itérateur pairs (), qui parcourt les entrées d'une table et renvoie deux valeurs, la clé et la valeur de l'entrée suivante.

Exemple :

'

local t = {k1 = « v1", k2 = « v2", k3 = « v3"}
local a = {} — tableau pour accumuler des paires clé-valeur
local n = 0 — nombre de paires clé-valeur
pour la clé, valeur en paires (t) do
n = n + 1
a[n] = key. « = «.. Value — ajoute une paire clé-valeur à la
fin du tableau
local s = table.concat (a, « ; ») — concatène toutes les paires clé-valeur en une seule chaîne
‘

Un autre itérateur utile est la fonction string.gmatch (), qui sera utilisée dans l'exemple COMBINE_HEADERS () suivant.

Extensions Citrix ADC - Référence de bibliothèque

August 20, 2021

Liste des bibliothèques prises en charge dans les extensions de stratégie.

- Bibliothèque de base
- Bibliothèque de chaînes
- Modèles d'expression régulière - Classes de caractères
- Modèles d'expression régulière - Éléments de motif
- Bibliothèque de tables
- Bibliothèque mathématique
- Bibliothèque binaire
- Bibliothèque du système d'exploitation
- Bibliothèque Citrix ADC

Bibliothèque de base

affirmer (v[, message])	Emet une erreur, avec un message facultatif, lorsque v est faux.
error(message)	Termine une fonction et signale le message d'erreur.
ipairs(a)	Iterateur pour un tableau a. Renvoie un index et une valeur pour chaque itération.
pairs(t)	Iterateur pour une table t. Renvoie une clé et une valeur pour chaque itération.
numéro de tonne (e[, base])	Convertit e en nombre, avec une base facultative.
tostring(v)	Convertit v en une chaîne
type(v)	Retourne le type de v : nombre, chaîne, booléen, table, etc.
getmetatable (objet)	Renvoie nil si l'objet n'a pas de métatable. Sinon, si la métatable de l'objet a un champ « __metatable », renvoie la valeur associée. Sinon, retourne le métatable de l'objet donné.
setmetatable (table, metatable)	Définit la métatable de la table donnée. (Vous ne pouvez pas modifier la métatable d'autres types de Lua, seulement de C.) Si metatable est nul, supprime le metatable de la table donnée. Si le métatable d'origine a un champ « __metatable », déclenche une erreur.
sélectionner (index, ···)	Retourne tous les arguments après l'index du numéro d'argument. Si index est chaîne "#", alors il retourne le nombre total d'arguments supplémentaires qu'il a reçus.
pcall (f [, arg1, ··])	Appelle la fonction f avec les arguments donnés en mode protégé. Il renvoie le code d'état comme premier résultat qui indique si l'appel a réussi ou non. Si l'appel a réussi, puis avec le code d'état, il renvoie également tous les résultats de l'appel, sinon renvoie un message d'erreur.

xpcall (f, msgh [, arg1, ··])	Cette fonction est similaire à pcall, sauf qu'elle prend également un argument pour la gestion des erreurs.
_VERSION	Renvoie la version actuelle de l'interpréteur.

Bibliothèque de chaînes

string.byte (s[, i [, j]])	Renvoie les valeurs d'octets de s[i] à s[j]. Par défaut i = 1 et j = i
string.char (…)	Renvoie une chaîne construite à partir des paramètres entiers.
string.find (s, pattern[, init [, plain])	Recherche la première correspondance d'un motif d'expression régulière dans s. Retourne le premier et le dernier index de match ou nil. init is index to start, default 1. plain = true signifie que le modèle n'est pas une expression régulière.
string.format(form,…)	Renvoie une version formatée des paramètres.
string.gmatch(s,pattern)	Iterateur pour la recherche s avec le modèle regex. Renvoie les valeurs correspondantes.
string.gsub (s, pattern, repl[, n])	Renvoie une copie de s dans laquelle toutes (ou n) occurrences du modèle ont été remplacées par repl.
string.len(s)	Renvoie la longueur de la chaîne.
string.lower(s)	Renvoie une copie de la chaîne convertie en minuscules.
string.match (s, motif[, init])	Recherche la première correspondance du motif regex dans s et renvoie les captures ou le motif entier. init est l'index à démarrer, par défaut 1.
string.rep (s, n[, sep])	Retourne une chaîne qui est n copies de s, avec le séparateur sep, par défaut aucun séparateur
string.reverse(s)	Renvoie une chaîne qui est s inversée.

string.sub (s, i[, j])	Retourne la sous-chaîne de s de s[i] à s[j], par défaut j est la fin de la chaîne.
string.upper(s)	Renvoie une copie de la chaîne convertie en majuscules.
string.dump (function)	Renvoie une chaîne contenant une représentation binaire de la fonction donnée.

Modèles d'expression régulière - classes de caractères

x	le caractère x, à l'exception des caractères magiques ^$ () %.[]*+- ?)
.	n'importe quel caractère
%a	toute lettre
%c	tout caractère de contrôle
%d	n'importe quel chiffre
%g	tout caractère imprimable à l'exception de l'espace
%l	toute lettre minuscule
%p	tout caractère de ponctuation
%s	tout caractère d'espace blanc
%u	toute lettre majuscule
%w	toute lettre alphanumérique
%x	un caractère magique échappé x (par exemple%%)
[lot]	un ensemble de caractères : séquence de caractères individuels, plages x-y et% classes
[^set]	caractères ne figurant pas dans l'ensemble.

Motifs d'expression régulière - éléments de motif

X	une classe de caractères
X*	0 ou plus de répétitions de caractères les plus longues dans X
X+	1 ou plusieurs répétitions de caractères dans X
X-	0 ou plusieurs répétitions les plus courtes de caractères dans X
X?	0 ou 1 caractère dans X
%n	n=1 à 9 ; correspond à la nième chaîne capturée
%bxy	correspond à une sous-chaîne entre deux caractères équilibrés x et y. L'exemple %b() correspond à une sous-chaîne entre deux parenthèses équilibrées.
%f[lot]	correspond à une chaîne vide à n'importe quelle position de telle sorte que le caractère suivant appartient à set et que le caractère précédent n'appartient pas à set.

Une répétition est une séquence d'éléments de répétition. ^pattern correspond au début d'une chaîne et pattern$ correspond à la fin de la chaîne.

Les sous-chaînes appariées peuvent être capturées à l'aide de (motif). Les parenthèses sans pattern () capturent la position actuelle de la chaîne (un nombre).

Bibliothèque de tables

table.concat (liste[, sep [, i [, j]]])	Renvoie une liste de chaînes[i].. sep.. list[i+1].. sep… list[j]. Par défaut, sep est la chaîne vide. Par défaut i est 1, j est #list.
table.insert (liste,[pos,]valeur)	Insère une valeur dans la liste à l'index pos. La valeur par défaut pour pos est #list (fin de la liste).

table.pack (…)	Retourne un tableau contenant les paramètres commençant à l'index 1, et une clé n avec le nombre total de paramètres.
table.remove (liste[, pos])	Supprime de la liste l'élément à la position pos, déplaçant les éléments pour remplir la position. Renvoie l'élément supprimé. Par défaut pour posis #list (fin de la liste.)
table.sort (liste[, comp])	Trier les éléments de la liste en place. comp est la fonction de comparaison à utiliser. La valeur par défaut pour comp est <.
table.unpack(list[, i [, j]])	Retourne la liste[i] à travers la liste[j] . La valeur par défaut pour i est 1 et j est #list <c/ode>.

Bibliothèque mathématique

Diverses fonctions trigonométriques et logarithmiques ne sont pas montrées.

math.abs(x)	Renvoie la valeur absolue de x.
math.ceil(x)	Retourne le plus petit entier >= x.
math.floor(x)	Retourne le plus grand nombre entier <= x.
math.fmod(x,y)	Renvoie le reste de x/y arrondissant le quotient vers zéro.
math.énorme	Une valeur >= tout autre nombre.
math.max(x,…)	Renvoie l'argument maximum.
math.min(x,…)	Renvoie l'argument minimum.
math.modf(x)	Retourne les parties intégrales et fractionnelles de x.
math.random()	Renvoie un nombre pseudo-aléatoire compris entre 0 et 1.
math.random(m)	Retourne un entier pseudo-aléatoire compris entre 1 et m.
math.random(m, n)	Retourne un entier pseudo-aléatoire entre m et n.

math.randomseed(x)	Définit le générateur de nombres pseudo-aléatoires défini sur x.
math.sqrt(x)	Retourne la racine carrée de x (x^0.5)
math.acos(x)	Renvoie l'arc cosinus de x (en radians).
math.asin(x)	Renvoie le sinus arc de x (en radians).
math.atan(x)	Renvoie la tangente de l'arc de x (en radians).
math.atan2(y, x)	Renvoie la tangente d'arc de y/x (en radians).
math.cos(x)	Renvoie le cosinus de x.
math.cosh(x)	Renvoie le cosinus hyperbolique de x.
math.sin(x)	Retourne le sinus de x.
math.sinh(x)	Retourne le sinus hyperbolique de x.
math.tan(x)	Retourne la tangente de x.
math.tanh(x)	Renvoie la tangente hyperbolique de x.
math.deg(x)	Renvoie l'angle x (donné en radians) en degrés.
math.exp(x)	Renvoie la valeur e^x.
math.frexp (x)	Renvoie m et e de telle sorte que x = m2e, e est un entier et la valeur absolue de m est dans la plage [0.5, 1).
math.ldexp (m, e)	Retourne m2e (e devrait être un entier).
math.log (x [, base])	Renvoie le logarithme de x dans la base donnée. La valeur par défaut pour la base est e.
math.pow (x, y)	Renvoie x^y.
math.rad (x)	Renvoie l'angle x (donné en degrés) en radians.
math.pi	La valeur de π.

Bibliothèque binaire

Sauf indication contraire :

- Toutes les fonctions acceptent des arguments numériques dans la plage (-2^51, +2^51).
- Chaque argument est normalisé au reste de sa division par 2^32 et tronqué en entier (d'une manière non spécifiée), de sorte que sa valeur finale se situe dans la plage [0,2^32 - 1].

- Tous les résultats sont dans la plage[0,2^32 - 1].

bit32.arshift(x,disp)	Retourne x bits de cession décalés arithmétiquement vers la droite (+cession) ou la gauche (-cession).
bit32.band (…)	Renvoie le bit et les arguments.
bit32.bnot(x)	Retourne la négation binaire de x.
bit32.bor (…)	Renvoie le bit ou des arguments.
bit32.btest(…)	Renvoie true si le bit et les arguments ne sont pas nuls.
bit32.bxor (…)	Renvoie le bit exclusif ou des arguments.
bit32.extract(n,field[,width])	Retourne les bits en n du champ au champ + largeur - 1 (nombre de bits du plus au moins significatif). La valeur par défaut pour la largeur est 1.
bit32.replace(n,v,field[,width])	Renvoie une copie de n avec des bits du champ au champ + largeur -1 remplacée par v. La largeur par défaut est 1.
bit32.lrotate(x,disp)	Retourne x bits de disp pivotés vers la gauche (+disp) ou vers la droite (-disp).
bit32.lshift(x,disp)	Retourne x bits de cession décalés vers la gauche (+cession) ou vers la droite (-cession).
bit32.rrotate(x,disp)	Retourne x bits de cession pivotés vers la droite (+cession) ou vers la gauche (-cession).
bit32.rshift(x,disp)	Retourne x bits de cession décalés vers la droite (+cession) ou vers la gauche (-cession).

Bibliothèque du système d'exploitation

os.clock ()	Renvoie une approximation de la quantité en secondes de temps CPU.

os.date ([format [, heure]])	Renvoie une chaîne ou un tableau contenant la date et l'heure, formaté selon le format de chaîne donné.
os.time ([tableau])	Renvoie l'heure actuelle lorsqu'elle est appelée sans arguments, ou une heure représentant la date et l'heure spécifiées par la table donnée.
os.difftime (t2, t1)	Renvoie le nombre de secondes entre le temps t1 et le temps t2.

Bibliothèque Citrix ADC

ns.logger:level(message)	Pour consigner les messages dont le niveau est d'urgence, alerte, critique, erreur, avertissement, notification, informations ou débogage. Les paramètres sont les mêmes que la fonction C printf() : une chaîne de format et un nombre variable d'arguments pour fournir des valeurs pour les spécificateurs % dans la chaîne de format.

Référence de l'API des extensions Citrix ADC

August 20, 2021

Les comportements sont une formalisation des modèles programmables courants disponibles sur une appliance Citrix ADC. Par exemple, un serveur virtuel TCP prend en charge un comportement de client TCP et un comportement de serveur TCP. Un comportement est un ensemble prédéfini de fonctions de rappel. Vous pouvez implémenter des comportements en fournissant des fonctions de rappel. Par exemple, un comportement client TCP peut consister en la fonction on_data, qui traite le flux de données TCP.

Comportement du client TCP

on_data - fonction de rappel pour les événements de données du client TCP. Le rappel prend deux arguments :

- **ctxt** - Contexte de traitement client TCP
- **charge utile** : charge utile de l'événement
  - **payload.data - Données** TCP reçues, disponibles sous forme de flux d'octets

Comportement du serveur TCP

on_data - fonction callback pour les événements de données du serveur TCP, le callback prend deux arguments :

- **ctxt** - Contexte de traitement du serveur TCP
- **charge utile** : charge utile de l'événement
  - **payload.data - données** tcp reçues, disponibles sous forme d'un flux d'octets

Contexte client TCP

Le contexte qui est passé aux rappels d'événement client TCP :

- **ctxt.output** - Le contexte de traitement suivant dans le pipeline. Les gestionnaires de rappel d'extension peuvent envoyer des données de type ns.tcp.stream à ctxt.output en utilisant les événements DATA, ce qui signifie un message partiel ou EOM (fin du message) qui signifie la fin du message de protocole. L'événement EOM (fin du message) peut avoir ou non des données TCP avec elle. Un événement EOM (fin du message) avec des données TCP peut être envoyé sans un événement DATA précédent pour envoyer un message de protocole entier et marquer la fin du message. La décision d'équilibrage de charge est prise, en aval par le serveur virtuel d'équilibrage de charge, sur les premières données reçues. Une nouvelle décision d'équilibrage de charge est prise après la réception du message EOM (fin du message). Ainsi, pour diffuser des données de message de protocole, envoyez plusieurs événements DATA avec le dernier événement comme EOM (fin du message). Tous les événements DATA contigus et les événements EOM (fin du message) suivants sont envoyés à la même connexion serveur sélectionnée par la décision d'équilibrage de charge sur le premier événement DATA de la séquence.
- **ctxt.input** - Le contexte de traitement précédent dans le pipeline d'où proviennent les données du flux TCP.
- **ctxt:hold (data)** - Fonction pour stocker les données pour un traitement ultérieur. En appelant hold avec des données, les données sont stockées dans le contexte. Plus tard, lorsque d'autres données sont reçues dans le même contexte, les données nouvellement reçues sont ajoutées aux données précédemment stockées et le flux de données combiné est ensuite transmis à la

fonction de rappel on_data. Après avoir appelé un blocage, la référence de données n'est plus utilisable et donne une erreur sur toute utilisation.

- **ctxt.vserver** - Le contexte du serveur virtuel.
- **ctxt.client** — Contexte de traitement de la connexion client. Ce contexte de traitement peut être utilisé pour envoyer des données au client, et pour récupérer des informations liées à la connexion comme l'adresse IP, les ports source et de destination.
- **ctxt:close ()** — Ferme la connexion client en envoyant FIN au client. Après avoir appelé cette API, le contexte de traitement du client n'est plus utilisable et donne une erreur sur toute utilisation.

Contexte du serveur TCP

Le contexte qui est passé aux rappels d'événement du serveur TCP :

- **ctxt.output** — Le contexte de traitement suivant dans le pipeline. Les gestionnaires de rappel d'extension peuvent envoyer des données de type ns.tcp.stream à ctxt.output en utilisant les événements DATA, ce qui signifie un message partiel ou EOM (fin du message) qui signifie la fin du message de protocole.
- **ctxt.input** - Le contexte de traitement précédent dans le pipeline d'où proviennent les données du flux TCP.
- **ctxt:hold (data)** - Fonction pour stocker les données pour un traitement ultérieur. En appelant hold avec des données, les données sont stockées dans le contexte. Plus tard, lorsque d'autres données sont reçues dans le même contexte, les données nouvellement reçues sont ajoutées aux données précédemment stockées et le flux de données combiné est ensuite transmis à la fonction de rappel on_data. Après avoir appelé un blocage, la référence de données n'est plus utilisable et donne une erreur sur toute utilisation.
- **ctxt.vserver** - Le contexte du serveur virtuel.
- **ctxt.server** - Contexte de traitement de la connexion au serveur. Ce contexte de traitement peut être utilisé pour envoyer des données au serveur, et pour récupérer des informations liées à la connexion comme l'adresse IP, les ports source et de destination.
- **ctxt:reuse_server_connection ()** - Cette API est utilisée pour permettre la réutilisation de la connexion serveur pour d'autres connexions client dans le contexte serveur uniquement. Cette API ne peut être utilisée que si un événement EOM (fin du message) est utilisé (dans l'API ns.send ()) pour envoyer les données dans le contexte client. Sinon, l'appliance ADC génère une erreur.

  Pour permettre la réutilisation d'une connexion serveur par d'autres clients, cette API doit être appelée à la fin de chaque message de réponse. Après avoir appelé cette API, si plus de données sont reçues sur cette connexion serveur, ceci est traité comme une erreur et la connexion

serveur est fermée. Si cette API n'est pas utilisée, la connexion au serveur ne peut être utilisée que pour le client pour lequel elle a été ouverte. En outre, si le même serveur est sélectionné pour une autre décision d'équilibrage de charge pour ce client, la même connexion serveur est utilisée pour envoyer les données du client. Après avoir utilisé cette API, la connexion au serveur cesse d'être liée à la connexion client pour laquelle elle a été ouverte et peut être réutilisée pour une nouvelle décision d'équilibrage de charge pour toute autre connexion client. Après avoir appelé cette API, le contexte du serveur n'est plus utilisable et génère une erreur sur toute utilisation.

Remarque : Cette API est disponible dans Citrix ADC 12.1 build 49.xx et versions ultérieures.

- **ctxt:close ()** — Ferme la connexion au serveur en envoyant FIN au serveur. Après avoir appelé cette API, le contexte de traitement du client n'est plus utilisable et affiche une erreur sur toute utilisation.

  Remarque : Cette API est disponible dans Citrix ADC 12.1 build 50.xx et versions ultérieures.

Contexte Vserver

Le contexte du serveur virtuel utilisateur disponible via les contextes transmis aux rappels :

- **vserver:counter_increment (counter_name)** - Incrémente la valeur d'un compteur de serveur virtuel passé en argument. Actuellement, les compteurs intégrés suivants sont pris en charge.
  - **- invalid_messages** — Nombre de demandes/réponses non valides sur ce serveur virtuel.
  - **- invalid_messages_chuté** — Nombre de demandes/réponses non valides abandonnées par ce serveur virtuel.
- **vserver.params** - Paramètres configurés pour le serveur virtuel utilisateur. Les paramètres fournissent la configurabilité des extensions. Le code d'extension peut accéder aux paramètres spécifiés dans l'interface de ligne de commande pour ajouter un serveur virtuel utilisateur.

Contexte de connexion client

Contexte de traitement de la connexion client pour obtenir des informations relatives à la connexion.

- **client.ssl** — Contexte SSL
- **client.tcp** — Contexte TCP
- **client.is_ssl** — True si la connexion client est basée sur SSL

Contexte de connexion au serveur

Contexte de traitement de la connexion au serveur pour obtenir des informations relatives à la connexion.

- **server.ssl** — Contexte SSL
- **server.tcp** — Contexte TCP
- **server.is_ssl** — True si la connexion au serveur est basée sur SSL

Contexte TCP

Le contexte TCP fonctionne sur le protocole TCP.

- **tcp.srcport — Port** source sous forme de nombre
- **tcp.dstport - Port** de destination en tant que nombre

Contexte IP

Le contexte IP fonctionne sur les données de protocole IP ou IPv6.

- **ip.src** - Contexte d'adresse IP source.
- **ip.dst** - Contexte d'adresse IP de destination.

Remarque : Cette API est disponible dans Citrix ADC 12.1 build 51.xx et versions ultérieures.

Contexte d'adresse IP

Le contexte d'adresse IP fonctionne sur les données d'adresse IP ou IPv6.

- **<address>.to_s** - Chaîne d'adresse dans la notation ASCII appropriée.
- **<address>.to_n** - La valeur numérique des adresses sous forme de chaîne d'octets dans l'ordre du réseau (4 octets pour IPv4 et 16 octets pour IPv6).
- **<address>.version** - Retourne 4 pour IPv4 et 6 pour IPv6.
- **<address>:subnet(<prefix value>)** - Retourne la chaîne d'adresse de sous-réseau après avoir appliqué le numéro de préfixe.
  - Pour l'adresse IPv4, la valeur doit être comprise entre 0 et 32
  - Pour l'adresse IPv6, la valeur doit être comprise entre 0 et 128.
- **<address>:apply_mask(<mask string>)** - Retourne la chaîne d'adresse après l'application de la chaîne de masque. API valide la version de l'argument et effectue la vérification des erreurs appropriée.
- **address>:eq(<address string>)** - Retourne true ou false selon que l'argument est équivalent à l'objet address. L'API valide la version des arguments.

Remarque : Cette API est disponible dans Citrix ADC 12.1 build 51.xx et versions ultérieures.

Contexte SSL

Le contexte SSL fournit des informations relatives à la connexion SSL frontend.

- **ssl.cert** — Contexte de certificat SSL. Pour la connexion client, il fournit le contexte de certificat client et pour la connexion serveur, il fournit le contexte de certificat serveur.
- **ssl.version** - Un nombre qui représente la version du protocole SSL de la transaction actuelle, comme suit :
  - - 0: The transaction is not SSL-based
  - - 0x002: The transaction is SSLv2
  - - 0x300: The transaction is SSLv3
  - - 0x301: The transaction is TLSv1
  - - 0x302: The transaction is TLSv1.1
  - - 0x303: The transaction is TLSv1.2
- **ssl.cipher_name - Nom** de chiffrement SSL sous forme de chaîne s'il est invoqué à partir d'une connexion SSL, sinon donne une chaîne NULL.
- **ssl.cipher_bits** — Nombre de bits dans la clé cryptographique.

Contexte de certificat SSL

- **Cert.version** — Numéro de version du certificat. Si la connexion n'est pas basée sur SSL, renvoie 0.
- **CERT.VALID_NOT_Before** — Date au format chaîne avant laquelle le certificat n'est pas valide.
- **CERT.VALID_NOT_After** — Date au format chaîne après laquelle le certificat n'est plus valide.
- **Cert.days_to_expire** — Nombre de jours avant lesquels le certificat est valide. Renvoie -1 pour le certificat expiré.
- **Cert.to_PEM** — Certificat au format binaire.
- **cert.issuer** - Nom distinctif (DN) de l'émetteur dans le certificat en tant que liste nom-valeur. Un signe égal (« = ») est le délimiteur du nom et de la valeur, et la barre oblique (« / ») est le délimiteur qui sépare les paires nom-valeur.

  Voici un exemple du nom distinctif renvoyé :
  /C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@n
- **cert.auth_keyid** — Extension de l'identificateur de clé d'autorité du certificat X.509 V3.
  - **auth_keyid.exists** - TRUE si le certificat contient une extension d'identificateur de clé d'autorité.
  - **auth_keyid.issuer_name - Nom** unique de l'émetteur dans le certificat en tant que liste nom-valeur.
    Un signe égal (« = ») est le délimiteur du nom et de la valeur, et la barre oblique (« / ») est le délimiteur qui sépare les paires nom-valeur.

Voici un exemple :
/C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@n

  - **auth_keyid.keyid** - Champ keyIdentifier de l'Authority Key Identifier en tant que blob
  - **auth_keyid.cert_serialnumber** - Champ SerialNumber de l'identificateur de clé d'autorité en tant que blob.

- **cert.pk_algorithm** - Nom de l'algorithme de clé publique utilisé par le certificat.
- **cert.pk_size** - Taille de la clé publique utilisée dans le certificat.
- **cert.serialnumber** - Numéro de série du certificat client. S'il s'agit d'une transaction non-SSL ou s'il y a une erreur dans le certificat, cela donne une chaîne vide.
- **cert.signature_algorithm** - Nom de l'algorithme cryptographique utilisé par l'autorité de certification pour signer ce certificat.
- **cert.subject_keyid** - Sujet keyID du certificat client. S'il n'y a pas d'ID de clé d'objet, cela donne un objet texte de longueur nulle.
- **cert.subject** - Nom unique du sujet en tant que nom-valeur. Un signe égal (« = ») sépare les noms et les valeurs et une barre oblique (« / ») délimite les paires nom-valeur.

Voici un exemple :
/C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycom

Bibliothèques Citrix ADC

- **ns.tcp.stream** - bibliothèque de type chaîne pour gérer les données TCP comme un flux d'octets. La taille maximale des données de flux TCP sur lesquelles ces API peuvent fonctionner est de 128 Ko. Les fonctions de bibliothèque ns.tcp.stream peuvent également être appelées dans le style habituel d'appel orienté objet d'extension. Par exemple, data:len () est identique à ns.tcp.stream.len (data)
  - **ns.tcp.stream.len (data)** - Retourne la longueur des données en octets, similaire à String.len de Lua
  - **ns.tcp.stream.find (data, pattern,[init])**- Fonction similaire à string.find de Lua. En outre, il effectue également une correspondance partielle à la fin des données. En cas de correspondance partielle, l'index de début est renvoyé et l'index de fin devient nul.
  - **ns.tcp.stream.split (data, length)** - Fractionne les données en deux morceaux, le premier morceau est de la longueur spécifiée. Après un fractionnement réussi, les données d'origine ne sont plus utilisables en tant que flux de données TCP. Toute tentative de l'utiliser de cette façon provoque une erreur.
  - **ns.tcp.stream.byte (data[, i [, j]])**- Fonction similaire à string.byte de Lua. Renvoie les codes numériques internes des caractères data[i], data[i+1],…, data[j.]

  - n**s.tcp.stream.sub (data, i,[j])**- Fonction similaire à string.sub de Lua. Retourne la sous-chaîne de s qui commence à i et continue jusqu'à j.
  - **ns.tcp.stream.match (data, pattern,[init])**- Fonction similaire à String.match de Lua. Recherche la première *correspondance* de motif dans la chaîne s.

- **ns.send (processing_ctxt, event_name, event_data)** - Fonction générique pour envoyer des événements dans un contexte de traitement. Les données d'événement sont une table Lua qui peut avoir n'importe quel contenu. Le contenu dépend de l'événement. Une fois l'API ns.send () appelée, la référence de données n'est plus utilisable. Toute tentative de l'utiliser provoque une erreur.
- **ns.pipe (src_ctxt, « ctxt »)** - En utilisant une API d'appel à pipe (), le code d'extension peut connecter le contexte source à un contexte de destination. Après un appel au canal, tous les événements qui sont envoyés du contexte source au module suivant du pipeline vont directement dans le contexte de destination. Cette API est généralement utilisée par le module qui fait l'appel pipe (), pour se retirer du pipeline.
- **ns.inet** — Bibliothèque d'adresses Internet.
  - **ns.inet.apply_mask (address_str, mask_str)** - renvoie la chaîne d'adresse après l'application de la chaîne de masque.
  - **ns.inet.aton (address_str)** - Retourne la valeur numérique des adresses sous forme de chaîne d'octets dans l'ordre du réseau (4 octets pour IPv4 et 16 pour IPv6).
  - **ns.inet.ntoa (byte_str)** - Convertit la valeur d'octet numérique en tant que chaîne d'octets en chaîne d'adresse.
  - **ns.inet.ntohs (number)** - Convertit l'ordre d'octets réseau donné en ordre d'octets hôte. Si l'entrée est supérieure à 2^16 - 1, génère une erreur.
  - **ns.inet.htons (number)** - Convertit l'ordre des octets hôte donné en ordre des octets réseau. Si l'entrée est supérieure à 2^16 - 1, génère une erreur.
  - **ns.inet.ntohl (number)** - Convertit l'ordre d'octets réseau donné en ordre d'octets hôte. Si l'entrée est supérieure à 2^32 - 1, lance une erreur.
  - **ns.inet.htonl (number)** - Convertit l'ordre des octets hôte donné en ordre des octets réseau. Si l'entrée est supérieure à 2^32 - 1, lance une erreur.
  - **ns.inet.subnet (address_str, subnet_value)** — Retourne la chaîne d'adresse de sous-réseau après avoir appliqué un sous-réseau donné.

Extensions de protocole

August 20, 2021

Les appliances Citrix ADC bénéficient d'une prise en charge native des protocoles tels que HTTP. En

plus de cela, vous pouvez utiliser des extensions de protocole pour ajouter la prise en charge des protocoles personnalisés. Actuellement, seuls les protocoles personnalisés basés sur TCP sont pris en charge, par exemple le protocole Message Queuing Telemetry Transport (MQTT). Pour les transactions sécurisées, TCP sur SSL est également pris en charge.

Les extensions de protocole sur l'appliance Citrix ADC font partie de l'infrastructure de script de haut niveau disponible sur l'appliance Citrix ADC. Le langage de script est basé sur le langage de programmation Lua 5.2. Pour ajouter un protocole personnalisé à une appliance Citrix ADC, l'utilisateur doit écrire du code d'extension pour implémenter les comportements applicables. Par exemple, les comportements ns.tcp.client et ns.tcp.server sont applicables aux protocoles basés sur TCP. Pour implémenter un comportement, implémentez uniquement les rappels que vous souhaitez personnaliser. Si le rappel n'est pas implémenté, sa valeur par défaut prend effet. Pour plus d'informations sur le langage de script, consultez Citrix ADC Extensions - Language Overview. Pour plus d'informations sur les comportements, consultez Citrix ADC Extensions API Reference.

Les extensions de protocole Citrix ADC peuvent être utilisées pour les éléments suivants :

- Ajoutez une nouvelle prise en charge de protocole sur l'appliance Citrix ADC par programme, à l'aide d'extensions.
- Analyse le trafic de protocole et effectuez un équilibrage de charge basé sur des messages spécifiques au protocole (MBLB).
- Configurer la persistance d'équilibrage de charge définie par l'utilisateur.

Extensions de protocole - architecture

August 20, 2021

Pour obtenir une extensibilité au niveau du trafic, le traitement du trafic sur une appliance Citrix ADC est exposé sous la forme d'un pipeline de modules de traitement distincts. Le trafic circule à travers eux pendant qu'il le traite de l'entrée à la sortie. Ces modules du pipeline suivent un modèle de rien partagé. Le passage de message est utilisé pour envoyer les données de trafic d'un module du pipeline au module suivant.

Certains points du pipeline de traitement du trafic sont extensibles, de sorte que vous pouvez ajouter du code pour personnaliser le comportement de Citrix ADC.

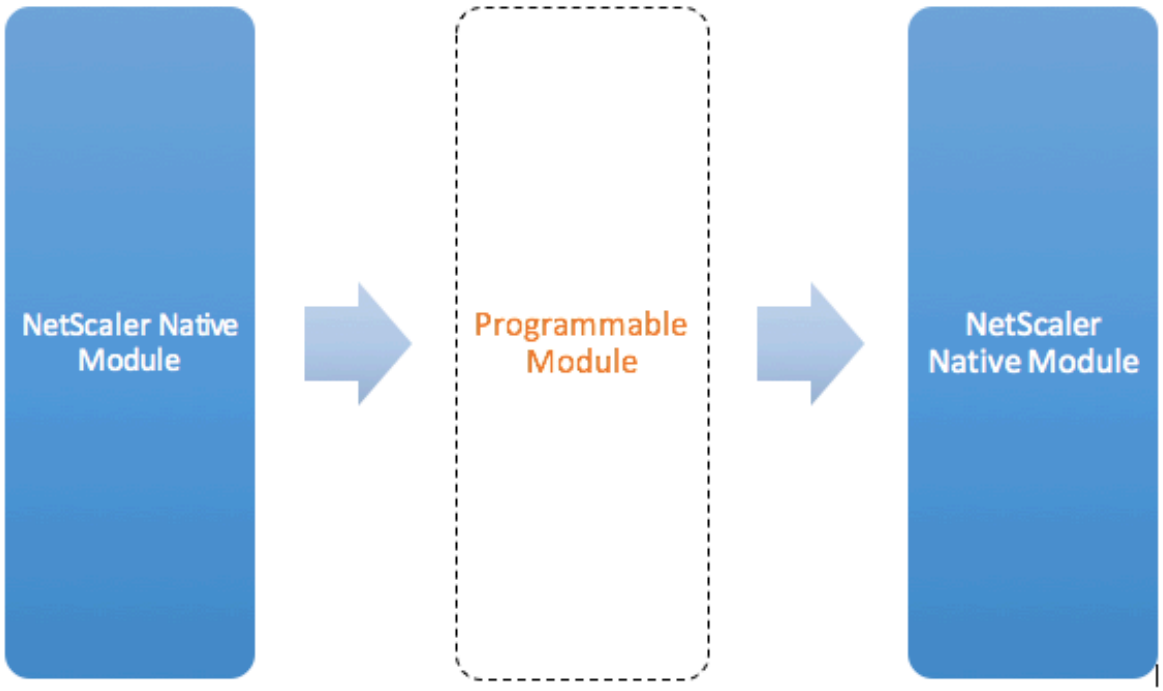


Figure: A Programmable Module In the Traffic Pipeline

Par défaut, le trafic contourne un module programmable auquel vous n'ajoutez aucun code.

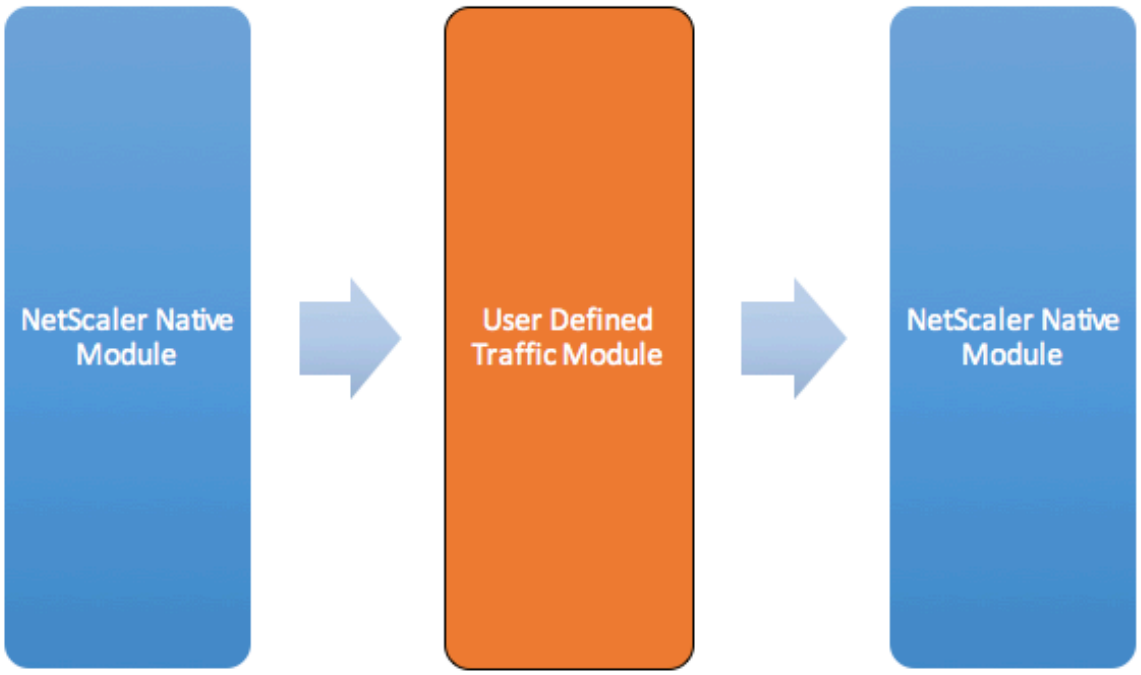


Figure: User Defined Traffic Module

Comportements

Les interfaces programmables pour personnaliser la gestion du trafic sont appelées comportements. Les comportements sont essentiellement une formalisation des modèles programmables courants disponibles sur une appliance Citrix ADC. Les comportements sont constitués d'un ensemble prédéfini de fonctions de rappel d'événement. Vous pouvez implémenter un comportement en fournissant des fonctions de rappel conformes au comportement.

Par exemple, le comportement du client TCP consiste en une fonction de rappel (on_data) qui traite les événements de flux de données client TCP. Pour implémenter l'équilibrage de charge basé sur le message (MBLB) pour un protocole basé sur TCP, vous pouvez ajouter du code pour cette fonction de rappel afin de traiter le flux de données TCP à partir du client et d'analyser le flux d'octets dans des messages de protocole.

Contexte :

Les fonctions de rappel dans un comportement sont appelées avec un contexte, qui est l'état du module de traitement. Le contexte est l'instance du module de traitement. Par exemple, les rappels de comportement du client TCP sont appelés avec différents contextes pour différentes connexions TCP client.

Charge utile :

En plus du contexte, les rappels de comportement peuvent avoir d'autres arguments. Habituellement, le reste des arguments sont passés en tant que charge utile, qui est la collection de tous les arguments.

Ainsi, les instances du module de traitement programmable peuvent être considérées comme une combinaison d'état d'instance et de fonctions de rappel d'événement, c'est-à-dire le contexte et le comportement. Et le trafic circule à travers le pipeline comme charge utile d'événement.

Pour les extensions d'API Citrix ADC, reportez-vous à la section Référence de l'API d'extension Citrix ADC.

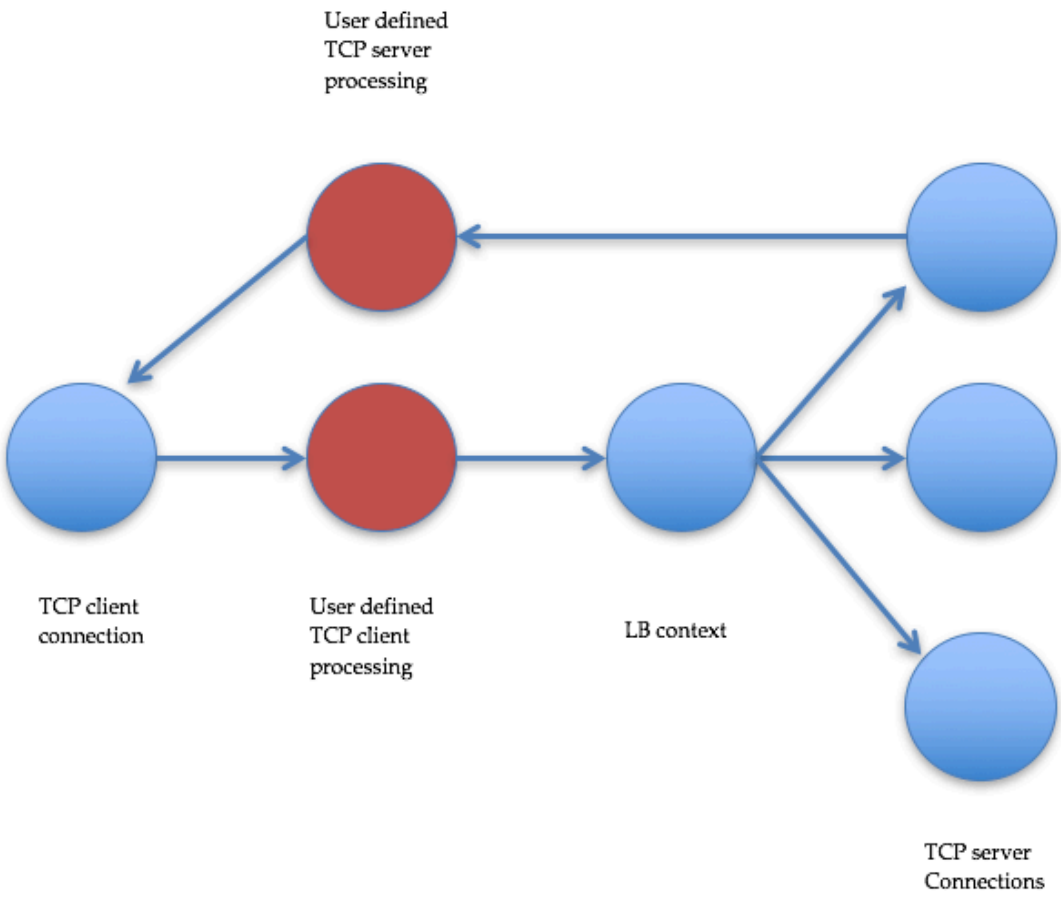
L'extrait de code suivant montre une fonction définie par l'utilisateur pour gérer les événements de flux de données client TCP. Le contexte et la charge utile sont transmis à la fonction par le code Citrix ADC. Ce code transfère simplement les données TCP reçues dans chaque appel au contexte du module de traitement suivant dans le pipeline. Dans ce cas, le module suivant est le contexte d'équilibrage de charge (LB), qui est un module natif Citrix ADC.

```
function client.on_data(ctxt, payload)
    ns.send(ctxt.output, "DATA", {
 data = payload.data }
 )
end
<!--NeedCopy-->
```


Extensions de protocole - pipeline de trafic pour les comportements de client et de serveur TCP définis par l'utilisateur

January 21, 2021

La figure suivante illustre l'exemple d'extension de protocole - pipeline de trafic pour les comportements du client et du serveur TCP définis par l'utilisateur



Traffic Pipeline For User Defined TCP Client And Server Behaviors

Ajouter un protocole personnalisé à l'aide d'extensions de protocole

Les commandes de l'interface de ligne de commande (CLI) pour le protocole personnalisé utilisent le mot-clé « user » pour indiquer la nature définie par l'utilisateur des entités de configuration sous-jacentes. Avec l'aide du code d'extension, vous pouvez ajouter un nouveau protocole utilisateur au système et ajouter des serveurs virtuels utilisateur pour les protocoles définis par l'utilisateur. Les

serveurs virtuels utilisateur sont à leur tour configurables en définissant des paramètres. Les valeurs configurées pour les paramètres de serveur virtuel sont disponibles dans le code d'extension.

L'exemple suivant illustre le flux utilisateur permettant d'ajouter la prise en charge d'un nouveau protocole. L'exemple ajoute la prise en charge du protocole MQTT au système. MQTT est un protocole de connectivité « Internet des objets » machine à machine. Il s'agit d'un transport léger de messagerie/abonnement. Utile pour les connexions avec des emplacements distants, ce protocole utilise des outils client et courtier pour publier des messages aux abonnés.

1. Importez le fichier d'implémentation de l'extension de protocole MQTT dans le système Citrix ADC. La liste des codes pour mqtt.lua est donnée ci-dessous. L'exemple ci-dessous importe le fichier d'extension MQTT hébergé sur un serveur Web.

   ```
   import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
   ```

2. Ajoutez un nouveau protocole TCP utilisateur au système à l'aide de l'extension.

   ```
   add user protocol MQTT -transport TCP -extension mqtt_code
   ```

3. Ajoutez un serveur d'équilibrage de charge utilisateur et liez des services backend à celui-ci.

   ```
   1 add service mqtt_svr1 10.217.24.48 USER_TCP 1501
   2 add service mqtt_svr2 10.217.24.48 USER_TCP 1502
   3 add lb vserver mqtt_lb USER_TCP  - lbmethod USER_TOKEN
   4 bind lb vserver mqtt_lb mqtt_svr1
   5 bind lb vserver mqtt_lb mqtt_svr2
   6 <!--NeedCopy-->
   ```

4. Ajoutez un utilisateur vserver pour le protocole nouvellement ajouté. Définissez defaultlb sur le serveur LB configuré ci-dessus.

   ```
   add user vserver mqtt_vs MQTT 10.217.24.28 8765 -defaultLb mqtt_lb
   ```

5. Le cas échéant, activez la persistance de session MQTT en fonction de l'ID client, définissez le type de persistance sur USERSESSION.

   ```
   set lb vserver mqtt_lb -persistenceType USERSESSION
   ```

Extensions de protocole - cas d'utilisation

August 20, 2021

Les extensions de protocole peuvent être utilisées dans les cas d'utilisation suivants.

- Équilibrage de charge basé sur les messages (MBLB)
- Diffusion en continu

- Équilibrage de charge basé sur des jetons
- Persistance de l'équilibrage de charge
- Équilibrage de charge basé sur la connexion TCP
- Équilibrage de charge basé sur le contenu
- SSL
- Modifier le trafic
- Trafic d'origine vers le client ou le serveur
- Traitement des données sur l'établissement de connexion

Équilibrage de charge basé sur les messages

Les extensions de protocole prennent en charge l'équilibrage de charge basé sur les messages (MBLB), qui peut analyser n'importe quel protocole sur une appliance Citrix ADC et équilibrer la charge les messages de protocole arrivant sur une connexion client, c'est-à-dire distribuer les messages sur plusieurs connexions serveur. MBLB est réalisé par le code utilisateur qui analyse le flux de données TCP client.

Le flux de données TCP est transmis aux callbacks on_data pour les comportements client et serveur. Le flux de données TCP est disponible pour les fonctions d'extension via une interface de type chaîne Lua. Vous pouvez utiliser une API similaire à l'API de chaîne Lua pour analyser le flux de données TCP.

Les API utiles comprennent :

```
data:len()
```

```
data:find()
```

```
data:byte()
```

```
data:sub()
```

```
data:split()
```

Une fois que le flux de données TCP a été analysé dans un message de protocole, le code utilisateur obtient l'équilibrage de charge en envoyant simplement le message de protocole au contexte suivant disponible à partir du contexte passé au rappel on_data pour le client.

L'API ns.send () est utilisée pour envoyer des messages à d'autres modules de traitement. En plus du contexte de destination, l'API send prend le nom de l'événement et la charge utile facultative comme arguments. Il existe une correspondance un-à-un entre le nom de l'événement et les noms de fonction de rappel pour les comportements. Les rappels pour les événements sont appelés on_<event_name>. Les noms de rappel utilisent uniquement des minuscules.

Par exemple, le client TCP et le serveur on_data callbacks sont des gestionnaires définis par l'utilisateur pour les événements nommés « DATA ». Pour envoyer le message de protocole entier dans un appel d'envoi, l'événement EOM (fin du message) est utilisé. EOM (fin du message), qui signifie la fin du message, signifie la fin du message de protocole vers le flux en aval du contexte LB,

de sorte qu'une nouvelle décision d'équilibrage de charge est prise pour les données qui suivent ce message.

Le code d'extension peut parfois ne pas recevoir l'intégralité du message de protocole dans l'événement on_data. Dans ce cas, les données peuvent être conservées à l'aide de l'API ctxt:hold (). L'API Hold est disponible pour les contextes client TCP-et serveur-callback. Lorsque « hold with data » est appelé, les données sont stockées dans le contexte. Lorsque d'autres données sont reçues dans le même contexte, les données nouvellement reçues sont ajoutées aux données précédemment stockées et la fonction de rappel on_data est appelée à nouveau avec les données combinées.

Remarque : La méthode d'équilibrage de charge utilisée dépend de la configuration du serveur virtuel d'équilibrage de charge correspondant au contexte d'équilibrage de charge.

L'extrait de code suivant montre l'utilisation de l'API send pour envoyer le message de protocole analysé.

Exemple :

```
    function client.on_data(ctxt, payload)
        --
        -- code to parse payload.data into protocol message comes here
        --
        -- sending the message to lb
        ns.send(ctxt.output, "EOM", {
 data = message }
 )
    end -- client.on_data

    function server.on_data(ctxt, payload)
        --
        -- code to parse payload.data into protocol message comes here
        --
        -- sending the message to client
        ns.send(ctxt.output, "EOM", {
 data = message }
 )

    end -- server.on_data
<!--NeedCopy-->
```

Diffusion en continu

Dans certains scénarios, maintenir le flux de données TCP jusqu'à ce que l'ensemble du message de protocole soit collecté peut ne pas être nécessaire. En fait, il n'est pas conseillé à moins qu'il ne soit nécessaire. La conservation des données augmente l'utilisation de la mémoire sur l'appliance Citrix

ADC et peut la rendre vulnérable aux attaques DDoS en épuisant la mémoire sur l'appliance Citrix ADC avec des messages de protocole incomplets sur de nombreuses connexions.

Les utilisateurs peuvent obtenir le streaming des données TCP dans les gestionnaires de rappel d'extension à l'aide de l'API send. Au lieu de conserver les données jusqu'à ce que l'ensemble du message soit collecté, les données peuvent être envoyées en morceaux. L'envoi de données à ctxt.output à l'aide de l'événement DATA envoie un message de protocole partiel. Il peut être suivi par d'autres événements DATA. Un événement EOM (fin du message) doit être envoyé pour marquer la fin du message de protocole. Le contexte d'équilibrage de charge en aval prend la décision d'équilibrage de charge sur les premières données reçues. Une nouvelle décision d'équilibrage de charge est prise après la réception du message EOM (fin du message).

Pour diffuser des données de message de protocole, envoyez plusieurs événements DATA suivis d'un événement EOM (fin du message). Les événements DATA contigus et l'événement EOM (fin du message) suivant sont envoyés à la même connexion serveur sélectionnée par décision d'équilibrage de charge pour le premier événement DATA de la séquence.

Pour un contexte d'envoi au client, les événements EOM (fin du message) et DATA sont effectivement les mêmes, car il n'y a pas de traitement spécial par le contexte client en aval pour les événements EOM (fin du message).

Équilibrage de charge basé sur des jetons

Pour les protocoles pris en charge en mode natif, une appliance Citrix ADC prend en charge une méthode d'équilibrage de charge basée sur un jeton qui utilise des expressions PI pour créer le jeton. Pour les extensions, le protocole n'est pas connu à l'avance, de sorte que les expressions PI ne peuvent pas être utilisées. Pour l'équilibrage de charge basé sur un jeton, vous devez définir le serveur virtuel d'équilibrage de charge par défaut pour utiliser la méthode d'équilibrage de charge USER_TOKEN et fournir la valeur de jeton à partir du code d'extension en appelant l'API send avec un champ user_token. Si la valeur du jeton est envoyée à partir de l'API send et que la méthode d'équilibrage de charge USER_TOKEN est configurée sur le serveur virtuel d'équilibrage de charge par défaut, la décision d'équilibrage de charge est prise en calculant un hachage basé sur la valeur du jeton. La longueur maximale de la valeur du jeton est de 64 octets.

```
add lb vserver v\\_mqttlb USER\\_TCP -lbMethod USER\\_TOKEN
```

L'extrait de code de l'exemple suivant utilise une API send pour envoyer une valeur de jeton LB.

Exemple :

```
1          -- send the message to lb
2
3
4
5
```



```
6          -- user_token is set to do LB based on clientID
7
8
9
10
11         ns.send(ctxt.output, "EOM", {
12  data = message,
13
14                                  user_token = token_info }
15  )
16 <!--NeedCopy-->
```

Persistance de l'équilibrage de charge

La persistance de l'équilibrage de charge est étroitement liée à l'équilibrage de charge basé sur un jeton. Les utilisateurs doivent pouvoir calculer par programmation la valeur de session de persistance et l'utiliser pour la persistance d'équilibrage de charge. L'API send est utilisée pour envoyer des paramètres de persistance. Pour utiliser la persistance de l'équilibrage de charge, vous devez définir le type de persistance USERSESSION sur le serveur virtuel d'équilibrage de charge par défaut et fournir un paramètre de persistance à partir du code d'extension en appelant l'API send avec un champ user_session. La longueur maximale de la valeur du paramètre de persistance est de 64 octets.

Si vous avez besoin de plusieurs types de persistance pour un protocole personnalisé, vous devez définir des types de persistance utilisateur et les configurer. Les noms des paramètres utilisés pour configurer les serveurs virtuels sont déterminés par l'implémenteur du protocole. La valeur configurée d'un paramètre est également disponible pour le code d'extension.

L'interface de ligne de commande et l'extrait de code suivants montrent l'utilisation d'une API d'envoi pour prendre en charge la persistance de l'équilibrage de charge. La liste de codes dans la section Liste de codes pour mqtt.lua illustre également l'utilisation du champ user_session.

Pour la persistance, vous devez spécifier le type de persistance USERSESSION sur le serveur virtuel d'équilibrage de charge et transmettre la valeur user_session à partir de l'API ns.send.

```
add lb vserver v\\_mqttlb USER\\_TCP -persistencetype USERSESSION
```

Envoyez le message MQTT à l'équilibreur de charge, avec le champ user_session défini sur ClientID dans la charge utile.

Exemple :

```
1 -- send the data so far to lb
2
3 -- user_session is set to clientID as well (it will be used to persist
     session)
```



```
4
5 ns.send(ctxt.output,  “DATA” , {
6  data = data, user_session = clientID }
7  )
8 <!--NeedCopy-->
```

Équilibrage de charge basé sur la connexion TCP

Pour certains protocoles, MBLB peut ne pas être nécessaire. Au lieu de cela, vous pouvez avoir besoin d'équilibrage de charge basé sur la connexion TCP. Par exemple, le protocole MQTT doit analyser la partie initiale du flux TCP pour déterminer le jeton d'équilibrage de charge. Et, tous les messages MQTT sur la même connexion TCP doivent être envoyés à la même connexion serveur.

L'équilibrage de charge basé sur la connexion TCP peut être réalisé en utilisant l'API send avec uniquement des événements DATA et en n'envoyant aucune EOM (fin du message). Ainsi, le contexte d'équilibrage de charge en aval basera la décision d'équilibrage de charge sur les données reçues en premier et envoie toutes les données suivantes à la même connexion serveur sélectionnée par la décision d'équilibrage de charge.

En outre, certains cas d'utilisation peuvent nécessiter la possibilité de contourner la gestion des extensions après que la décision d'équilibrage de charge a été prise. Le contournement des appels d'extension se traduit par de meilleures performances, car le trafic est traité uniquement par du code natif. Le contournement peut être fait en utilisant l'API ns.pipe(). Un appel au code d'extension de l'API pipe() peut connecter le contexte d'entrée à un contexte de sortie. Après l'appel à pipe(), tous les événements provenant du contexte d'entrée vont directement dans le contexte de sortie. Effectivement, le module à partir duquel l'appel pipe() est effectué est retiré du pipeline.

L'extrait de code suivant montre la diffusion en continu et l'utilisation de l'API pipe() pour contourner un module. La liste de codes de la section Liste de codes pour mqtt.lua illustre également comment effectuer le streaming et l'utilisation de l'API pipe () pour contourner le module pour le reste du trafic sur la connexion.

Exemple :

```
1         -- send the data so far to lb
2         ns.send(ctxt.output, "DATA", {
3  data = data,
4                                      user_token = clientID }
5  )
6         -- pipe the subsequent traffic to the lb - to bypass the client
              on_data handler
7         ns.pipe(ctxt.input, ctxt.output)
8 <!--NeedCopy-->
```


Équilibrage de charge basé sur le contenu

Pour les protocoles natifs, la fonctionnalité de commutation de contenu comme pour les extensions de protocole est prise en charge. Avec cette fonctionnalité, au lieu d'envoyer les données à l'équilibrage de charge par défaut, vous pouvez envoyer les données à l'équilibreur de charge sélectionné.

La fonction de commutation de contenu pour les extensions de protocole est obtenue à l'aide de l'API ctxt:lb_connect (<lbname>). Cette API est disponible pour le contexte client TCP. À l'aide de cette API, le code d'extension peut obtenir un contexte d'équilibrage de charge correspondant à un serveur virtuel d'équilibrage de charge déjà configuré. Vous pouvez ensuite utiliser l'API send avec le contexte d'équilibrage de charge ainsi obtenu.

Le contexte lb peut être NULL parfois :

- Le serveur virtuel n'existe pas
- Le serveur virtuel n'est pas du type de protocole utilisateur
- L'état du serveur virtuel n'est pas UP
- Le serveur virtuel est un serveur virtuel utilisateur, pas un serveur virtuel d'équilibrage de charge

Si vous supprimez le serveur virtuel d'équilibrage de charge cible lorsqu'il est en cours d'utilisation, toutes les connexions associées à ce serveur virtuel d'équilibrage de charge sont réinitialisées.

L'extrait de code suivant montre l'utilisation de l'API lb_connect (). Le code mappe l'ID client aux noms de serveurs virtuels d'équilibrage de charge (lbname) à l'aide de la table Lua lb_map, puis obtient le contexte LB pour lbname à l'aide de lb_connect (). Et enfin envoie au contexte LB en utilisant l'API send.

```
1     local lb_map = {
2
3        ["client1*"] = "lb_1",
4        ["client2*"] = "lb_2",
5        ["client3*"] = "lb_3",
6        ["client4*"] = "lb_4"
7      }
8
9
10    -- map the clientID to the corresponding LB vserver and connect to
         it
11    for client_pattern, lbname in pairs(lb_map) do
12       local match_idx = string.find(clientID, client_pattern)
13       if (match_idx == 1) then
14      lb_ctxt = ctxt:lb_connect(lbname)
15      if (lb_ctxt == nil) then
16         error("Failed to connect to LB vserver: " .. lbname)
17      end
```



```
18        break
19         end
20      end
21      if (lb_ctxt == nil) then
22      -- If lb context is NULL, the user can raise an error or send data
           to default LB
23         error("Failed to map LB vserver for client: " .. clientID)
24      end
25  -- send the data so far to lb
26  ns.send(lb_ctxt, "DATA", {
27   data = data }
28
29  <!--NeedCopy-->
```

SSL

SSL pour les protocoles utilisant des extensions est pris en charge de la manière dont SSL pour les protocoles natifs est pris en charge. En utilisant le même code d'analyse pour créer des protocoles personnalisés, vous pouvez créer une instance de protocole sur TCP ou sur SSL qui peut ensuite être utilisée pour configurer les serveurs virtuels. De même, vous pouvez ajouter des services utilisateur via TCP ou SSL.

Pour plus d'informations, consultez Configuration du déchargement SSL pour MQTT et Configuration du déchargement SSL pour MQTT avec chiffrement de bout en bout.

Multiplexage de connexion serveur

Parfois, le client envoie une requête à la fois et envoie la demande suivante uniquement après réception de la réponse de la première requête du serveur. Dans ce cas, la connexion au serveur peut être réutilisée pour d'autres connexions clientes et pour le message suivant sur la même connexion, après l'envoi de la réponse au client. Pour permettre la réutilisation de la connexion serveur par d'autres connexions client, vous devez utiliser l'API ctxt : reuse_server_connection() sur le contexte côté serveur.

Remarque : Cette API est disponible dans Citrix ADC 12.1 build 49.xx et versions ultérieures.

Modifier le trafic

Pour modifier les données de la demande ou de la réponse, vous devez utiliser la fonction de réécriture native qui utilise une expression PI de stratégie avancée. Étant donné que vous ne pouvez pas utiliser d'expressions PI dans les extensions, vous pouvez utiliser les API suivantes pour modifier les données d'un flux TCP.


```
data:replace(offset, length, new_string)
data:insert(offset, new_string)
data:delete(offset, length)
data:gsub(pattern, replace [,n]))
```

L'extrait de code suivant montre l'utilisation de l'API replace().

```
-- Get the offset of the pattern, we want to replace
   local old_pattern =  "pattern to repalace"
local old_pattern_length = old_pattern:len()
   local pat_off, pat_end = data:find(old_pattern)
   -- pattern is not present
if (not pat_off) then
    goto send_data
   end
  -- If the data we want to modify is not completely present, then
  -- wait for more data
  if (not pat_end) then
        ctxt:hold(data)
        data = nil
     goto done
  end
data:replace(pat_off, old_pattern_length,  "new pattern" )
::send_data::
ns.send(ctxt.output,  "EOM" , {
 data = data }
 )
::done::
```

L'extrait de code suivant montre l'utilisation de l'API insert().

```
data:insert(5,  "pattern to insert" )
```

L'extrait de code suivant montre l'utilisation de l'API insert (), lorsque nous voulons insérer après ou avant un motif :

```
-- Get the offset of the pattern, after or before which we want to
    insert
   local pattern =  "pattern after/before which we need to insert"
local pattern_length = pattern:len()
   local pat_off, pat_end = data:find(pattern)
-- pattern is not present
   if (not pat_off) then
    goto send_data
```



```
 8     end
 9    -- If the pattern after which we want to insert is not
10    -- completely present, then wait for more data
11    if (not pat_end) then
12          ctxt:hold(data)
13          data = nil
14       goto done
15    end
16 -- Insert after the pattern
17 data:insert(pat_end + 1,  “pattern to insert” )
18     -- Insert before the pattern
19 data:insert(pat_off,  “pattern to insert” )
20 ::send_data::
21     ns.send(ctxt.output,  “EOM” , {
22  data = data }
23  )
24 ::done::
```

L’extrait de code suivant montre l’utilisation de l’API delete ().

```
1  -- Get the offset of the pattern, we want to delete
2     local delete_pattern =  “pattern to delete”
3  local delete_pattern_length = delete_pattern:len()
4     local pat_off, pat_end = data:find(old_pattern)
5     -- pattern is not present
6  if (not pat_off) then
7             goto send_data
8     end
9    -- If the data we want to delete is not completely present,
10   -- then wait for more data
11   if (not pat_end) then
12         ctxt:hold(data)
13         data = nil
14      goto done
15   end
16 data:delete(pat_off, delete_pattern_length)
17 ::send_data::
18 ns.send(ctxt.output,  “EOM” , {
19  data = data }
20  )
21 ::done::
```

L’extrait de code suivant montre l’utilisation de l’API gsub().

```
1      -- Replace all the instances of the pattern with the new string
```



```
data:gsub( “old pattern” , “new string” )
-- Replace only 2 instances of “old pattern”
data:gsub( “old pattern” , “new string” , 2)
-- Insert new_string before all instances of “http”
data:gsub( “input data” , “(http)” , “new_string%1” )
-- Insert new_string after all instances of “http”
data:gsub( “input data” , “(http)” , “%1new_string” )
-- Insert new_string before only 2 instances of “http”
data:gsub( “input data” , “(http)” , “new_string%1” , 2)
```

Remarque : Cette API est disponible dans Citrix ADC 12.1 build 50.xx et versions ultérieures.

Trafic d’origine vers le client ou le serveur

Vous pouvez utiliser l’API ns.send () pour envoyer des données provenant du code d’extension à un client et à un serveur principal. Pour envoyer ou recevoir une réponse directement avec un client, à partir du contexte client, vous devez utiliser ctxt.client comme cible. Pour envoyer ou recevoir une réponse directement avec un serveur back-end à partir d’un contexte de serveur, vous devez utiliser ctxt.server comme cible. Les données de la charge utile peuvent être des données de flux TCP ou une chaîne Lua.

Pour arrêter le traitement du trafic sur une connexion, vous pouvez utiliser l’API ctxt:close () à partir du client ou du contexte du serveur. Cette API ferme la connexion côté client ou toute connexion serveur qui lui est liée.

Lorsque vous appelez l’API ctxt:close (), le code d’extension envoie le paquet TCP FIN aux connexions client et serveur et si plus de données sont reçues du client ou du serveur sur cette connexion, l’appliance réinitialise la connexion.

L’extrait de code suivant montre l’utilisation des API ctxt.client et ctxt:close().

```
    -- If the input packet is not MQTT CONNECT type, then
-- send some error response to the client.
function client.on_data(ctxt, payload)
    local data = payload.data
    local offset = 1
    local msg_type = 0
    local error_response = “Missing MQTT Connect packet.”
    byte = data:byte(offset)
msg_type = bit32.rshift(byte, 4)
if (msg_type ~= 1) then
-- Send the error response
   ns.send(ctxt.client, “DATA” , {
 data = error_response }
 )
```



```
-- Since error response has been sent, so now close the connection
    ctxt:close()
end
```

L'extrait de code suivant montre l'exemple lorsque l'utilisateur peut injecter les données dans le flux de trafic normal.

```
-- After sending request, send some log message to the server.
function client.on_data(ctxt, payload)
local data = payload.data
local log_message = "client id : "..data:sub(3, 7).." user name : "
    data:sub(9, 15)
-- Send the request we get from the client to backend server
ns.send(ctxt.output, "DATA" , {
 data = data }
 )
After sending the request, also send the log message
ns.send(ctxt.output, "DATA" , {
 data = log_message" }
 )
end
```

L'extrait de code suivant montre l'utilisation de l'API ctxt.to_server.

```
-- If the HTTP response status message is "Not Found" ,
-- then send another request to the server.
function server.on_data(ctxt, payload)
    local data = payload.data
    local request "GET /default.html HTTP/1.1\r\n\r\n" ss
    local start, end = data:find( "Not Found" )
    if (start) then
    -- Send the another request to server
        ns.send(ctxt.server, "DATA" , {
 data = request }
 )
end
```

Remarque : Cette API est disponible dans Citrix ADC 12.1 build 50.xx et versions ultérieures.

Traitement des données sur l'établissement de connexion

Il peut y avoir un cas d'utilisation où vous souhaitez envoyer des données à l'établissement de connexion (lorsque le ACK final est reçu). Par exemple, dans le protocole proxy, vous pouvez souhaiter envoyer les adresses IP source et de destination du client et les ports au serveur principal de

l'établissement de connexion. Dans ce cas, vous pouvez utiliser le gestionnaire de rappel client.init() pour envoyer les données sur l'établissement de la connexion.

L'extrait de code suivant montre l'utilisation du callback client.init() :

```
-- Send a request to the next processing context
-- on the connection establishment.
function client.init(ctxt)
   local request  "PROXY TCP4"  + ctxt.client.ip.src.to_s +  "  " +
      ctxt.client.ip.dst.to_s +  "  " + ctxt.client.tcp.srcport +  "  "
       +     ctxt.client.tcp.dstport
-- Send the another request to server
   ns.send(ctxt.output,  "DATA" , {
 data = request }
 )
  end
```

Remarque : Cette API est disponible dans Citrix ADC 13.0 build xx.xx et versions ultérieures.

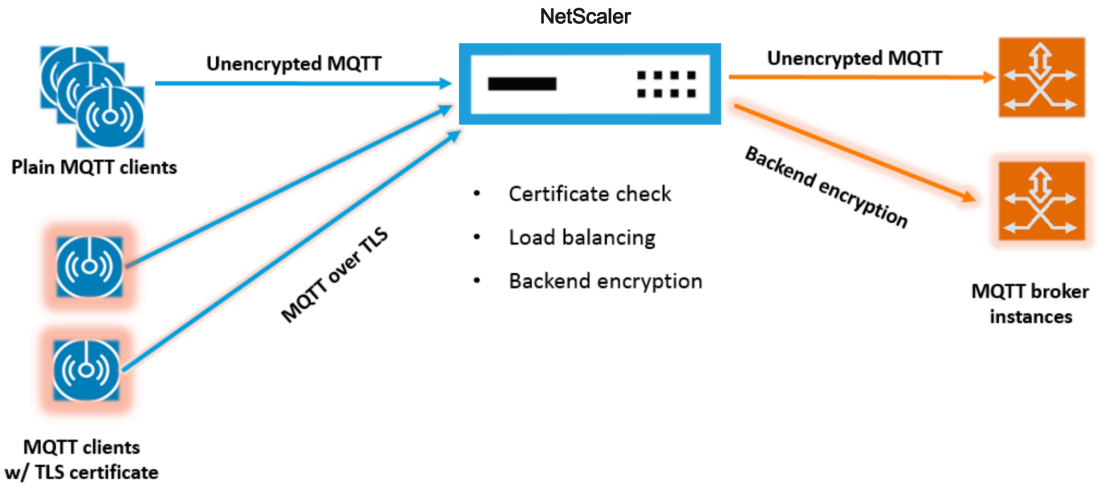
Didacticiel — Ajouter le protocole MQTT à l'appliance Citrix ADC à l'aide d'extensions de protocole

January 21, 2021

Les commandes de l'interface de ligne de commande (CLI) pour le protocole personnalisé utilisent le mot-clé « user » pour indiquer la nature définie par l'utilisateur des entités de configuration sous-jacentes. Avec l'aide du code d'extension, vous pouvez ajouter un nouveau protocole utilisateur au système et ajouter des serveurs virtuels utilisateur pour les protocoles définis par l'utilisateur. Les serveurs virtuels utilisateur sont à leur tour configurables en définissant des paramètres. Les valeurs configurées pour les paramètres de serveur virtuel sont disponibles dans le code d'extension.

Le protocole MQTT est utilisé à des fins d'illustration.

Le diagramme suivant illustre une appliance Citrix ADC et des outils client et courtier MQTT.



Liste de codes pour mqtt.lua

January 21, 2021

La liste de code ci-dessous, mqtt.lua, donne le code pour implémenter le protocole MQTT sur Citrix ADC à l'aide d'extensions de protocole. Le code a uniquement la fonction de rappel des données du client TCP définie - client.on_data(). Pour les données du serveur, il n'ajoute pas de fonction de rappel et le serveur au client prend le chemin natif rapide. Pour les données client, le code analyse le message de protocole CONNECT MQTT et extrait l'ID client. Il utilise ensuite l'ID client pour la valeur user_token, qui est utilisé pour équilibrer la charge tout le trafic client pour la connexion en fonction de l'ID client en définissant la méthode LB pour le serveur LB comme USER_TOKEN. Il utilise également l'ID client pour la valeur user_session, qui peut être utilisée pour la persistance LB en définissant le type de persistance pour le serveur LB comme USERSESSION. Le code utilise le ns.send () pour faire LB et envoyer les données initiales. Il utilise l'API ns.pipe () pour envoyer le reste du trafic client directement à la connexion au serveur, en contournant les appels au gestionnaire de rappel d'extension.

```
1  --[[
2
3    MQTT event handler for TCP client data
4
5      ctxt - TCP client side App processing context.
6
7      data - TCP Data stream received.
8
9      - parse the client ID from the connect message - the first message
           should be connect
10
```



```
11      - send the data to LB with ClientID as user token and session
12
13      - pipe the subsequent data to LB directly. This way the subsequent
            MQTT traffic will
14
15        bypass the tcp client on_data handler
16
17      - if a parse error is seen, throw an error so the connection is
            reset
18
19  --]]
20
21  function client.on_data(ctxt, payload)
22
23      local data = payload.data
24
25      local data_len = data:len()
26
27      local offset = 1
28
29      local byte = nil
30
31      local utf8_str_len = 0
32
33      local msg_type = 0
34
35      local multiplier = 1
36
37      local max_multiplier = 128 * 128 * 128
38
39      local rem_length = 0
40
41      local clientID = nil
42
43      -- check if MQTT fixed header is present (fixed header length is
            atleast 2 bytes)
44
45      if (data_len < 2) then
46
47          goto need_more_data
48
49      end
50
51      byte = data:byte(offset)
52
```



```
53      offset = offset + 1
54
55         -- check for connect packet - type value 1
56
57      msg_type = bit32.rshift(byte, 4)
58
59      if (msg_type ~= 1) then
60
61          error("Missing MQTT Connect packet.")
62
63      end
64
65      -- parse the remaining length
66
67      repeat
68
69          if (multiplier > max_multiplier) then
70
71             error("MQTT CONNECT packet parse error - invalid Remaining
                   Length.")
72
73         end
74
75         if (data_len < offset) then
76
77            goto need_more_data
78
79         end
80
81         byte = data:byte(offset)
82
83         offset = offset + 1
84
85         rem_length = rem_length + (bit32.band(byte, 0x7F) * multiplier)
86
87         multiplier = multiplier * 128
88
89      until (bit32.band(byte, 0x80) == 0)
90
91      -- protocol name
92
93      -- check if protocol name length is present
94
95      if (data_len < offset + 1) then
96
```



```
97          goto need_more_data
98
99       end
100
101      -- protocol name length MSB
102
103      byte = data:byte(offset)
104
105      offset = offset + 1
106
107      utf8_str_len = byte * 256
108
109      -- length LSB
110
111      byte = data:byte(offset)
112
113      offset = offset + 1
114
115      utf8_str_len = utf8_str_len + byte
116
117         -- skip the variable header for connect message
118
119      -- the four required fields (protocol name, protocol level, connect
             flags, keep alive)
120
121      offset = offset + utf8_str_len + 4
122
123      -- parse the client ID
124
125      --
126
127      -- check if client ID len is present
128
129      if (data_len < offset + 1) then
130
131         goto need_more_data
132
133      end
134
135         -- client ID length MSB
136
137      byte = data:byte(offset)
138
139      offset = offset + 1
140
```



```
141     utf8_str_len = byte * 256
142
143     -- length LSB
144
145     byte = data:byte(offset)
146
147     offset = offset + 1
148
149     utf8_str_len = utf8_str_len + byte
150
151     if (data_len < (offset + utf8_str_len - 1)) then
152
153         goto need_more_data
154
155     end
156
157     clientID = data:sub(offset, offset + utf8_str_len - 1)
158
159     -- send the data so far to lb, user_token is set to do LB based on
           clientID
160
161     -- user_session is set to clientID as well (it will be used to
           persist session)
162
163     ns.send(ctxt.output, "DATA", {
164 data = data,
165
166                                 user_token = clientID,
167
168                                 user_session = clientID }
169 )
170
171        -- pipe the subsequent traffic to the lb - to bypass the
              extension handler
172
173     ns.pipe(ctxt.input, ctxt.output)
174
175     goto parse_done
176
177     ::need_more_data::
178
179     ctxt:hold(data)
180
181     ::parse_done::
182
```



```
183     return
184
185 end
186 <!--NeedCopy-->
```

Configurer MQTT à l'aide d'extensions de protocole

August 20, 2021

Les étapes suivantes ajoutent un protocole MQTT à l'appliance Citrix ADC.

Importez le fichier d'extension vers l'appliance Citrix ADC, à partir d'un serveur Web (en utilisant HTTP) ou de votre station de travail locale. Pour plus d'informations sur l'importation du fichier d'extension, voir Importer des extensions.

```
import ns extension local:mqtt_generic_fs.lua mqtt_code
```

Ajoutez un nouveau protocole TCP utilisateur au système à l'aide de l'extension.

```
add user protocol MQTT -transport TCP -extension mqtt_code
```

Ajoutez un service de type USER_TCP pour indiquer qu'il s'agit d'un protocole défini par l'utilisateur.

```
add service s1 10.102.90.112 USER_TCP 80
```

Ajoutez un serveur d'équilibrage de charge utilisateur et liez des services backend à celui-ci.

```
add lb vs mysv USER_TCP
```

```
bind lb vs mysv s1
```

Ajoutez un serveur virtuel utilisateur pour le protocole nouvellement ajouté et faites du serveur virtuel d'équilibrage de charge configuré à l'étape précédente l'équilibreur de charge par défaut.

```
add user vs v_mqtt MQTT 10.217.24.28 80 -defaultlb mysv
```

Le cas échéant, activez la persistance de session MQTT en fonction de l'ID client, définissez le type de persistance sur USERSESSION.

```
set lb vserver mqtt_lb -persistenceType USERSESSION
```

Configuration du déchargement SSL pour MQTT

August 20, 2021

Vous pouvez implémenter le déchargement SSL pour les protocoles utilisateur en ajoutant une instance SSL pour le protocole. L'exemple ci-dessous montre comment effectuer le déchargement SSL pour un protocole utilisateur. Le trafic vers les services backend n'est pas chiffré avec cette configuration.

Remarque : Cet exemple ne fournit pas de détails relatifs à l'ajout ou à la mise à jour d'une paire de clés certificat-clé et à la lier à un serveur virtuel. Pour plus de détails, voir Certificats SSL.

Les commandes suivantes ajoutent le protocole MQTT_SSL en incluant mqtt.lua avec la valeur de transport « SSL ».

```
import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
add user protocol MQTT_SSL -transport SSL -extension mqtt_code
<!--NeedCopy-->
```

Les commandes suivantes ajoutent un serveur virtuel d'équilibrage de charge utilisateur et lui lient des services backend.

```
add service mqtt_svr1 10.217.24.48 USER_TCP 1501
add service mqtt_svr2 10.217.24.48 USER_TCP 1502
add lb vserver mqtt_lb USER_TCP  - lbMethod ROUNDROBIN
bind lb vserver mqtt_lb mqtt_svr1
bind lb vserver mqtt_lb mqtt_svr2
<!--NeedCopy-->
```

La commande suivante ajoute un serveur virtuel utilisateur pour le nouveau protocole MQTT_SSL. L'utilisation de MQTT_SSL signifie que l'appliance Citrix ADC effectuera le déchargement SSL, car MQTT_SSL a été configuré avec le transport SSL. La commande définit également defaultlb sur le serveur virtuel d'équilibrage de charge configuré à l'étape précédente.

```
add user vserver mqtt_vs MQTT_SSL 10.217.24.28 8765 -defaultLb mqtt_lb
```

Pour le déchargement SSL, vous devez également activer la fonctionnalité SSL et lier une clé de certificat au serveur virtuel utilisateur. Pour plus d'informations, consultez les rubriques suivantes :

Ajouter ou mettre à jour une paire de clés de certificat

Lier la paire de clés de certificat au serveur virtuel SSL

Exemple :

```
enable ns feature SSL

add SSL certKey mqtt_svr_cert_key -cert server1.cert -key server1.key

bind ssl vserver mqtt_vs  -certkeyName mqtt_svr_cert_key
<!--NeedCopy-->
```


Configuration du déchargement SSL avec chiffrement de bout en bout pour MQTT

August 20, 2021

L'exemple suivant montre comment effectuer le déchargement SSL pour MQTT avec chiffrement de bout en bout.

Remarque : Cet exemple ne fournit pas de détails relatifs à l'ajout ou à la mise à jour d'une paire de clés certificat-clé et à la lier à un serveur virtuel. Pour plus de détails, voir Certificats SSL.

Les commandes suivantes importent le fichier d'extension et ajoutent le protocole MQTT_SSL avec le transport SSL.

```
import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
add user protocol MQTT_SSL -transport SSL -extension mqtt_code
<!--NeedCopy-->
```

Les commandes suivantes ajoutent un serveur virtuel d'équilibrage de charge utilisateur et lui lient des services backend. Le serveur virtuel d'équilibrage de charge et les services sont tous deux configurés pour le type de service USER_SSL_TCP.

```
add service mqtt_svr1 10.217.24.48 USER_SSL_TCP 1501
add service mqtt_svr2 10.217.24.48 USER_SSL_TCP 1502
add lb vserver mqtt_lb USER_SSL_TCP  - lbmethod RR
bind lb vserver mqtt_lb mqtt_svr1
bind lb vserver mqtt_lb mqtt_svr2
<!--NeedCopy-->
```

La commande suivante ajoute un serveur virtuel utilisateur pour le nouveau protocole MQTT_SSL. L'utilisation de MQTT_SSL signifie que l'appliance Citrix ADC effectuera le déchargement SSL, car MQTT_SSL a été configuré avec le transport SSL. La commande fait également le serveur virtuel d'équilibrage de charge, configuré à l'étape précédente, l'équilibreur de charge par défaut.

```
add user vserver mqtt_vs MQTT_SSL 10.217.24.28 8765 -defaultLb mqtt_lb
```

Pour le chiffrement de bout en bout, vous devez également activer la fonctionnalité SSL et lier une clé de certificat à l'utilisateur et aux serveurs virtuels d'équilibrage de charge par défaut. Pour plus d'informations, consultez les rubriques suivantes :

Ajouter ou mettre à jour une paire de clés de certificat

Lier la paire de clés de certificat au serveur virtuel SSL

```
enable ns feature SSL

```



```
add SSL certKey mqtt_svr_cert_key -cert server1.cert -key server1.key

bind ssl vserver mqtt_lb  -certkeyName mqtt_svr_cert_key

bind ssl vserver mqtt_vs  -certkeyName mqtt_svr_cert_key
<!--NeedCopy-->
```

Tutoriel - équilibrage de charge des messages syslog à l'aide d'extensions de protocole

January 21, 2021

Le protocole Syslog disponible sur l'appliance Citrix ADC fonctionne uniquement pour les messages générés sur l'appliance Citrix ADC. Il n'équilibre pas la charge des messages provenant de nœuds externes. Pour équilibrer la charge de ces messages, vous devez utiliser la fonction d'extensions de protocole et écrire la logique d'analyse des messages syslog en utilisant le langage de programmation Lua 5.2.

Code pour l'analyse du message syslog

Le code a uniquement la fonction de rappel des données du client TCP définie - client.on_data(). Pour les données du serveur, il n'ajoute pas de fonction de rappel et le serveur au client prend le chemin natif rapide. Le code identifie la limite du message en fonction du caractère de fin. Si le paquet TCP contient plus d'un message syslog, nous divisons le paquet en fonction du caractère de fin et de l'équilibre de charge de chaque message.

```
--[[

  Syslog event handler for TCP client data

    ctxt - TCP client side App processing context.

    data - TCP Data stream received.

--]]

function client.on_data(ctxt, payload)

                  local message = nil

                  local data_len
```



```
16
17                  local data = payload.data
18
19                  local trailing_character = "\n"
20
21                  ::split_message::
22
23                                  -- Get the offset of trailing
                                       character
24
25                                  local new_line_character_offset =
                                       data:find(trailing_character)
26
27                                  -- If trailing character is not
                                       found, then wait for more data.
28
29                                  if (not new_line_character_offset)
                                       then
30
31                                                  goto
                                                       need_more_data
32
33                                  end
34
35                                  -- Get the length of the current
                                       message
36
37                                  data_len = data:len()
38
39                                  -- Check whether we have more than
                                       one message
40
41                                  -- by comparing trailing character
                                       offset and
42
43                                  -- current data length
44
45                                  if (data_len >
                                       new_line_character_offset) then
46
47                                                  -- If we have
                                                       more than one
                                                       message, then
                                                       split
48
```



```
49                                                      -- the data into
                                                           two parts such
                                                            that first
                                                           part
50
51                                                      -- will contain
                                                           message upto
                                                           trailing
                                                           character
52
53                                                      -- offset and
                                                           second part
                                                           will contain
54
55                                                      -- remaining
                                                           message.
56
57                                                      message, data =
                                                           data:split(
                                                           new_line_character_offse
                                                           )
58
59                                      else
60
61                                                      message = data
62
63                                                      data = nil
64
65                                      end
66
67  -- Send the data to the backend server.
68
69                                      ns.send(ctxt.output, "EOM", {
70   data = message }
71   )
72
73                                      goto done
74
75                                      ::need_more_data::
76
77                                                      -- Wait for more
                                                           data
78
79                                                      ctxt:hold(data)
80
```



```
81                                                      data = nil
82
83                                                      goto done
84
85                                      ::done::
86
87                                                      -- If we have
                                                           more data to
                                                           parse,
88
89                                                      -- then do
                                                           parsing again.
90
91                                                      if (data) then
92
93                                                                      goto
                                                                          split_
94
95                                                      end
96
97  end
98  <!--NeedCopy-->
```

Configuration du protocole syslog à l'aide d'extensions de protocole

January 21, 2021

Les étapes suivantes ajoutent un protocole SYSLOG utilisateur à l'appliance Citrix ADC.

Importez le fichier d'extension vers l'appliance Citrix ADC, à partir d'un serveur Web (en utilisant HTTP) ou de votre station de travail locale. Pour plus d'informations sur l'importation du fichier d'extension, reportez-vous à la section Importation d'extensions.

```
import ns extension local:syslog_parser.lua syslog_parser_code
```

Ajoutez un nouveau protocole TCP utilisateur au système à l'aide de l'extension.

```
add user protocol USER_SYSLOG -transport TCP -extension syslog_parser_code
```

Ajoutez un service de type USER_TCP pour indiquer qu'il s'agit d'un protocole défini par l'utilisateur.

```
add service s1 10.102.90.112 USER_TCP 80
```

Ajoutez un serveur d'équilibrage de charge utilisateur et liez des services backend à celui-ci.


```
add lb vs mysv USER_TCP

bind lb vs mysv s1
<!--NeedCopy-->
```

Ajoutez un serveur virtuel utilisateur pour le protocole nouvellement ajouté et faites du serveur virtuel d'équilibrage de charge configuré à l'étape précédente l'équilibreur de charge par défaut.

```
add user vs v_syslog USER_SYSLOG 10.217.24.28 80 -defaultlb mysv
```

Référence de commande des extensions de protocole

January 21, 2021

Le tableau suivant répertorie toutes les nouvelles commandes ajoutées pour les protocoles personnalisés et les commandes existantes qui ont été modifiées pour les protocoles personnalisés.

```
show lb persistentSessions [<vserv-name>]
```

- **Commande CLI :**

  ```
  add user protocol <name> -transport ( TCP | SSL )-extension <string> -comment <string>]>
  ```

- **Description :**

  Ajoute un nouveau protocole utilisateur à l'appliance Citrix ADC à l'aide d'extensions. Actuellement, seuls les protocoles utilisateur avec valeur de transport TCP ou SSL sont pris en charge.

  > **Exemple :**
  >
  > add user protocol MQTT -transport TCP -extension mqtt_code

- **Commande CLI :**

  ```
  rm user protocol <name>
  ```

- **Description :**

  Supprime un protocole utilisateur précédemment ajouté à l'appliance Citrix ADC.

  > **Exemple :**
  >
  > rm user protocol mqtt

- **Commande CLI :**

  ```
  set user protocol <name> -comment <string>
  ```


- **Description :**

  Modifie les paramètres d'un protocole utilisateur précédemment ajouté à l'appliance Citrix ADC.

  > **Exemple :**
  >
  > set user protocol mqtt -comment "MQTT protocol implementation"

- **Commande CLI :**

```
unset user protocol <name> -comment
```

- **Description :**

  Supprime les paramètres d'un protocole utilisateur précédemment ajouté à l'appliance Citrix ADC.

  > **Exemple :**
  >
  > unset user protocol mqtt -comment "MQTT protocol implementation"

- **Commande CLI :**

```
update ns extension <extension name>
```

- **Description :**

  Met à jour l'implémentation d'un protocole utilisateur précédemment ajouté à l'aide d'extensions.

  Vous pouvez mettre à jour l'implémentation du protocole uniquement si le protocole n'est pas utilisé par un serveur virtuel utilisateur.

  > **Exemple :**
  >
  > update ns extension my-extension

- **Commande CLI :**

```
add lb vserver <name> [USER_TCP | USER_SSL_TCP] [-lbmethod USER_TOKEN]
[-persistencetype USERSESSION] [-timeout <value>]
```

- **Description :**

  Ajoute un serveur virtuel d'équilibrage de charge à l'appliance Citrix ADC. Il s'agit d'une commande CLI existante.

  Pour les serveurs virtuels utilisateur d'équilibrage de charge, le type de service à utiliser est USER_TCP ou USER_SSL_TCP. L'adresse IP et le port ne sont pas autorisés avec les serveurs virtuels d'équilibrage de charge de l'utilisateur.

  Pour les serveurs virtuels d'équilibrage de charge utilisateur, seule la méthode d'équilibrage de charge ROUNDROBIN est autorisée et la valeur du jeton est fournie par le code d'extension.

De même, seule la persistance USERSESSION est autorisée, et le paramètre de persistance est fourni par le code d'extension.

> **Exemple :**
>
> add lb vserver mysv USER_TCP –lbmethod ROUNDROBIN

- **Commande CLI :**

```
add user vserver <name> <userProtocol> <IPAddress> <port> -defaultLB <
string> [-params <string>] [-comment <string>]
```

- **Description :**

Ajoute un serveur virtuel pour un protocole utilisateur à l'aide d'extensions. Le serveur virtuel d'équilibrage de charge utilisateur configuré par défaut est disponible pour le gestionnaire d'extension de données du client TCP en tant que ctxt.output. Pour un serveur virtuel, les paramètres d'extension peuvent être définis à l'aide de l'option -params avec un nom et une paire de valeurs. La valeur de paramètre correspondante est disponible pour les gestionnaires d'extension en tant que ctxt.vserver.params.<paramName>.

> **Exemple :**
>
> add user vs v_mqtt MQTT 10.217.24.28 80 -defaultlb mysv

- **Commande CLI :**

```
rm user vserver <name>
```

- **Description :**

Supprime un serveur virtuel utilisateur précédemment ajouté à l'appliance Citrix ADC.

> **Exemple :**
>
> rm user vserver v_mqtt

- **Commande CLI :**

```
set user vserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-defaultLB
<string>] [-params <string>] [-comment <string>]
```

- **Description :**

Modifie les paramètres d'un serveur virtuel utilisateur précédemment ajouté à l'appliance Citrix ADC. Lorsqu'une nouvelle valeur est affectée à un paramètre d'extension par l'option -params, l'ancienne valeur est remplacée.

> **Exemple :**

> set user vs v_mqtt MQTT 10.217.24.28 -defaultlb mysv -comment “MQTT protocol implementation”

- **Commande CLI :**

```
unset user vserver <name> [-params] [-comment]
```

- **Description :**

  Supprime les paramètres d’un serveur virtuel utilisateur précédemment ajouté à l’appliance Citrix ADC. Si vous utilisez l’option —params pour annuler la définition d’un paramètre d’extension, la valeur de paramètre correspondante disponible pour les gestionnaires d’extension est remplacée par zéro.

  > **Exemple :**
  >
  > unset user vs v_mqtt MQTT 10.217.24.28 -defaultlb mysv -comment “MQTT protocol implementation”

- **Commande CLI :**

```
show user protocol [<name>]
```

- **Description :**

  Affiche des informations sur un protocole utilisateur, telles que l’extension et les rappels.

  > **Exemple :**
  >
  > show user protocol mqtt

- **Commande CLI :**

```
show user vserver [<name>]
```

- **Description :**

  Affiche des informations sur un serveur virtuel utilisateur.

  > **Exemple :**
  >
  > show user vserver vs_mqtt

- **Commande CLI :**

```
stat user vserver [<name>]
```

- **Description :**

  Affiche des statistiques sur un serveur virtuel utilisateur.

  > **Exemple :**
  >
  > stat user vserver vs_mqtt

- **Commande CLI :**

  ```
  show lb persistentSessions [<vserv-name>]
  ```

- **Description :**

  Affiche des informations sur les sessions persistantes. Il s'agit d'une interface de ligne de commande existante. Pour les protocoles utilisateur, le type de persistance est affiché sous la forme USERSESSION.

- **Commande CLI :**

  ```
  rm lb vserver <name>
  ```

- **Description :**

  Supprime un serveur LB utilisateur précédemment ajouté à l'appliance Citrix ADC.

  > **Exemple :**
  >
  > rm lb vserver mysv

- **Commande CLI :**

  ```
  add service <name> <IPAddr> (USER_TCP | USER_SSL_TCP)<Port>
  ```

- **Description :**

  Ajoute un service backend à utiliser pour un protocole utilisateur. Il s'agit d'une commande CLI existante avec les nouveaux types de service USER_TCP et USER_SSL_TCP.

  > **Exemple :**
  >
  > add service mqtt_svr1 10.217.24.48 USER_TCP 1501
  >
  > **Remarque** : les commandes existantes « set service and unset service » peuvent être utilisées pour supprimer ou modifier les paramètres d'un service précédemment ajouté pour un protocole utilisateur.

- **Commande CLI :**

  ```
  bind lb vserver <name> <serviceName>
  ```

- **Description :**

  Lie un service à un serveur LB utilisateur. Le type de service doit être USER_TCP/USER_SSL_TCP pour la liaison à un serveur LB avec le type USER_TCP/USER_SSL_TCP.

  > **Exemple :**
  >
  > bind lb vserver mysv mqtt_svr1

- **Commande CLI :**

  ```
  unbind lb vserver <name> <serviceName>
  ```


- **Description :**

  Dissocie un service précédemment lié à un serveur LB utilisateur.

  > **Exemple :**
  >
  > unbind lb vserver mysv mqtt_svr1

- **Commande CLI :**

  ```
  rm service <name>
  ```

- **Description :**

  Supprime un service précédemment ajouté pour un protocole utilisateur.

  > **Exemple :**
  >
  > rm service mqtt_svr1

Dépannage des extensions de protocole

January 21, 2021

Si votre fonction d'extension ne se comporte pas comme prévu, vous pouvez utiliser la fonctionnalité de suivi d'extension pour vérifier le comportement de votre fonction d'extension. Vous pouvez également ajouter la journalisation à votre fonction d'extension à l'aide de la fonctionnalité de journalisation personnalisée, dans laquelle vous pouvez définir le niveau de journalisation à capturer sur l'appliance Citrix ADC.

Journalisation personnalisée

Vous pouvez également ajouter votre propre journalisation à votre fonction d'extension. Pour ce faire, utilisez la fonction ns.logger:level () intégrée, où level est urgence, alert, critique, error, warning, notice, info ou debug. Les paramètres sont les mêmes que la fonction C printf() : une chaîne de format et un nombre variable d'arguments pour fournir les valeurs pour le % spécifié dans la chaîne de format. Par exemple, vous pouvez ajouter ce qui suit à la fonction COMBINE_HEADERS pour consigner le résultat d'un appel :

```
local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"

ns.logger:info("Result: %s", result_str)

return result_str
<!--NeedCopy-->
```


La fonction ci-dessus enregistrerait le message suivant vers/var/log/ns.log pour l'exemple d'entrée illustré dans les exemples de messages de journal abrégés dans la section Suivi des extensions ci-dessus.

```
... : default NSEXTENSION Message 143 0 : "Result: Host: 10.217.24.7:2000^M
 H1: abcd, 1234^M User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4)libcurl
/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Accept: \*/\*^M H2: h2val1, h2val2,
h2val3^M ^M"
```

Extensions de stratégie

January 21, 2021

La fonctionnalité d'extension de stratégie vous permet d'écrire des fonctions d'extension pour les types de stratégie intégrés. Les extensions peuvent être utilisées dans les expressions de stratégie, tout comme les fonctions intégrées. Ils sont exécutés lorsque les expressions de stratégie correspondantes sont évaluées. Cette fonctionnalité est utile pour :

- Ajout de fonctions personnalisées aux stratégies existantes.
- Mise en œuvre de constructions logiques pour les besoins complexes des clients.

La fonctionnalité d'extension de stratégie corrige ces limitations en permettant aux utilisateurs d'écrire des fonctions d'extension pour les types de stratégie intégrés. Les extensions peuvent ensuite être utilisées dans les expressions de stratégie, tout comme les fonctions intégrées. Ils sont exécutés lorsque les expressions de stratégie correspondantes sont évaluées.

Le tableau suivant répertorie les types de stratégie qui peuvent être utilisés lors de l'écriture d'une extension, ainsi que les mappages associés.

Type de stratégie	Type de stratégie mappée	Résultat
TEXT_T	NSTEXT	Chaîne
BOOL_AT	NSBOOL	Booléen
NUM_AT	NSNUM	Nombre (virgule flottante double précision)
DOUBLE_AT	NSDOUBLE	Nombre (virgule flottante double précision)

Conditions préalables à l'utilisation des extensions de stratégie

Les fonctions importées doivent être conformes aux normes de stratégie existantes. Par conséquent :

- Le nom de la fonction doit commencer par une lettre et peut contenir des nombres ou des traits de soulignement.
- Le nom de la fonction est traité comme insensible à la casse par les stratégies Citrix ADC.
- La fonction doit renvoyer une valeur unique même si le langage d'extension renvoie plusieurs valeurs.
- Les fonctions avec un nombre variable d'arguments ne sont pas prises en charge.

Comment fonctionnent les extensions de stratégie ?

Les stratégies existantes sur une appliance Citrix ADC utilisent un interpréteur pour évaluer les fonctions importées dans un fichier d'extension de stratégie. Lorsqu'un utilisateur importe une nouvelle fonction dans un fichier d'extension de stratégie :

1. Le fichier d'extension est validé pour la syntaxe et d'autres conditions.
2. Si la validation échoue, l'erreur est signalée à l'utilisateur.
3. Si la validation réussit, le fichier d'extension est importé dans l'appliance Citrix ADC et son contenu peut être utilisé dans les expressions de stratégie, comme n'importe quelle fonction de stratégie intégrée
    a) Si l'évaluation de l'expression de stratégie renvoie une erreur pendant l'exécution, elle est signalée comme un événement undef et le compteur d'erreur associé est incrémenté.
    Remarque : Si un événement undef de stratégie se produit et que la règle de stratégie contient une ou plusieurs fonctions d'extension de stratégie, la `show ns extension <name>` commande affiche les succès undef lorsqu'ils sont appliqués à ces extensions de stratégie. Si la fonction d'extension est abandonnée, la valeur du compteur d'abandon est incrémentée.
    b) Si l'évaluation de l'expression de stratégie réussit, l'évaluation de l'expression reprend jusqu'à ce que l'expression entière soit évaluée ou jusqu'à ce qu'elle soit abandonnée en raison d'une erreur.

Si la fonction d'extension prend trop de temps à s'exécuter, elle est annulée et le compteur d'erreur relatif à cette fonction d'extension est incrémenté. La fonction d'extension est en bac à sable, ce qui empêche :

- Utilisation excessive du processeur sur l'appliance Citrix ADC.
- Utilisation excessive de la mémoire sur l'appliance Citrix ADC.
- Utilisation de bibliothèques intégrées nuisibles ou de bibliothèques ou de binaires tiers.
- Scripts de longue durée pouvant entraîner le redémarrage de l'appliance Citrix ADC.

Configuration des extensions de stratégie

August 20, 2021

Lorsque votre fichier d'extension de stratégie est prêt, importez-le dans l'appliance Citrix ADC. Le processus d'importation copie le fichier d'extension dans un répertoire de l'appliance Citrix ADC et vérifie les erreurs de syntaxe.

Après l'importation, vous devez rendre le fichier d'extension disponible pour une utilisation dans les expressions de stratégie.

Remarque : La commande import permet de télécharger le contenu du fichier à partir d'une source \<src\>externe ou d'une source interne sur le système de fichiers Citrix ADC. Pour charger ce contenu de fichier dans un ou plusieurs moteurs de paquets pour la première fois, utilisez la commande add. S'il y a une mise à jour du contenu du fichier, le contenu mis à jour peut être téléchargé sur le système de fichiers Citrix ADC en émettant la commande import avec l'argument écraser. La commande met à jour le contenu du système de fichiers. Pour charger le contenu mis à jour sur un ou plusieurs moteurs de paquets, utilisez la commande update.

Configurer les extensions de stratégie à l'aide de la CLI

1. Importez le fichier d'extension de stratégie dans l'appliance Citrix ADC, à partir d'un serveur Web (à l'aide de HTTP) ou de votre station de travail locale.

   a) Importation HTTP

   Si vous disposez d'un serveur Web, vous pouvez stocker le fichier d'extension dans le répertoire du serveur Web et l'importer dans l'appliance Citrix ADC.

   ```
   1 import ns extension <src> <name> [-comment<string>] [-
       overwrite]
   2 <!--NeedCopy-->
   ```

   Exemple :

   ```
   1 import ns extension http://myhost/path/to/extension
       myextension -comment  “Custom crc calculation
   2 <!--NeedCopy-->
   ```

   b) Importation locale

   Vous pouvez utiliser le client SSH pour copier le fichier d'extension de votre poste de travail vers le répertoire /var/tmp de l'appliance Citrix ADC.

   ```
   1 scp extension-file-name <ns-userid@ns-ip-addr>:/var/tmp
   ```



```
<!--NeedCopy-->
```

où,

- `extension-file-name` est le nom du fichier d'extension sur votre machine cliente.
- `ns-userid` est l'utilisateur de l'appliance Citrix ADC ayant l'autorisation d'écrire dans /var/tmp.
- `ns-ip-addr` est l'adresse IP Citrix ADC.

Après avoir copié le fichier sur l'appliance Citrix ADC, exécutez la commande import sur l'appliance Citrix ADC.

```
import ns extension local:<extension-file-name extension-name>
<!--NeedCopy-->
```

Remarque : L'interface de ligne de commande doit être utilisée pour importer un fichier d'extension local, en exécutant la commande
import .

2. Ajoutez l'extension de stratégie au moteur de paquets pour évaluation.

```
add ns extension <name> [-comment <string>]
<!--NeedCopy-->
```

Exemple :

```
add ns extension myextension
<!--NeedCopy-->
```

Après l'importation d'un fichier d'extension, vous pouvez le mettre à jour, si vous avez inclus le paramètre -overwrite dans la commande import, ou le supprimer. Vous pouvez également afficher les détails d'un fichier d'extension importé.

Mettre à jour un fichier d'extension sur l'appliance Citrix ADC à partir de la source

À l'invite de commandes, tapez :

```
update ns extension <name>
<!--NeedCopy-->
```

Remarque : vous ne pouvez mettre à jour le fichier d'extension qu'après avoir importé le fichier d'extension spécifié dans l'appliance Citrix ADC avec le paramètre -overwrite.

Exemple :


```
update ns extension myextension
<!--NeedCopy-->
```

Supprimer un fichier d'extension de l'appliance Citrix ADC

À l'invite de commandes, tapez :

```
rm ns extension <name>
<!--NeedCopy-->
```

Exemple :

```
rm ns extension myextension
<!--NeedCopy-->
```

Afficher les détails de la fonction d'extension spécifiée sur l'appliance Citrix ADC

À l'invite de commandes, tapez :

```
show ns extension <name>
<!--NeedCopy-->
```

Exemple :

```
show ns extension myextension
<!--NeedCopy-->
```

Configurer les extensions de stratégie à l'aide de l'interface graphique

1. Importez le fichier d'extension de stratégie dans l'appliance Citrix ADC, à partir d'un serveur Web (à l'aide de HTTP) ou de votre station de travail locale.

   a) Accédez à **AppExpert** > **Extensions** de **stratégie, cliquez sur Extensionde stratégie, dans la liste déroulante Importer** de, sélectionnez l'URL correspondant à l'emplacement du fichier d'extension à importer.

   b) Accédez à **AppExpert** > **Extensions de stratégie**, **Extension de stratégie** et importez le fichier d'extension en sélectionnant Fichier dans la liste déroulante **Importer** depuis.

2. Ajoutez l'extension de stratégie au moteur de paquets pour évaluation.

   Accédez à **AppExpert** > **Extensions de stratégie** et, sous l'ongletExtensions de stratégie, ajoutez le fichier d'extension.

Mettre à jour un fichier d'extension sur l'appliance Citrix ADC à partir de la source

Accédez à **AppExpert** > **Extensions de stratégie** et, sous l'onglet **Extensions de stratégie**, mettez à jour le fichier d'extension.

Supprimer un fichier d'extension de l'appliance Citrix ADC

Accédez à **AppExpert** > **Extensions de stratégie** et, onglet **Extensions de stratégie**, supprimez le fichier d'extension.

Afficher les détails de la fonction d'extension spécifiée sur l'appliance Citrix ADC

Accédez à **AppExpert** > **Extensions de stratégie** et, sous l'onglet **Fonctions des extensions de stratégie**, cliquez sur la flèche de liste déroulante de la fonction d'extension dont vous souhaitez voir les détails.

Extensions de stratégie - cas d'utilisation

August 20, 2021

Certaines applications client ont des exigences qui ne peuvent pas être prises en compte avec les stratégies et expressions existantes. La fonction d'extension de stratégie permet aux clients d'ajouter des fonctions personnalisées à leurs applications afin de répondre à leurs besoins.

Les cas d'utilisation suivants illustrent l'ajout de nouvelles fonctions à l'aide de la fonctionnalité d'extension de stratégie sur l'appliance Citrix ADC.

- Cas 1 : hachage personnalisé
- Cas 2 : Réduire les doubles barres obliques dans les URL
- Cas 3 : Combiner des en-têtes

Cas 1 : hachage personnalisé

La fonction CUSTOM_HASH fournit un mécanisme pour insérer n'importe quel type de valeur de hachage dans les réponses envoyées au client. Dans ce cas d'utilisation, la fonction de hachage est utilisée pour calculer le hachage de la chaîne de requête pour une requête HTTP de réécriture et insérer un en-tête HTTP nommé CUSTOM_HASH avec la valeur calculée. La fonction CUSTOM_HASH implémente l'algorithme de hachage DJB2.

Exemple d'utilisation de CUSTOM_HASH :


```
> add rewrite action test_custom_hash insert_http_header "CUSTOM_HASH"
   "HTTP.REQ.URL.QUERY.CUSTOM_HASH"
<!--NeedCopy-->
```

Exemple de définition de CUSTOM_HASH() :

```
    -- Extension function to compute custom hash on the text

    -- Uses the djb2 string hash algorithm
    function NSTEXT:CUSTOM_HASH() : NSTEXT

        local hash = 5381

        local len = string.len(self)

        for i = 1, len do

             hash = bit32.bxor((hash * 33), string.byte(self, i))

        end

        return tostring(hash)

    end
<!--NeedCopy-->
```

Description ligne par ligne de l'échantillon ci-dessus :

```
function NSTEXT:CUSTOM_HASH() : NSTEXT

Defines the CUSTOM_HASH() function, with text input and a text return
   value.

local hash = 5381
local len = string.len(self)

Declares two local variables:

 - hash. Accumulates the compute hash value and is seeded with the
    number 5381

 - len. Sets to the length of the self input text string, using the
    built-in string.len() function.

```



```
for i = 1, len do
      hash = bit32.bxor((hash * 33), string.byte(self, i))
end

Iterates through each byte of the input string and adds the byte to the
     hash. It uses the built-in string.byte() function to get the byte
    and the built-in bit32.bxor() function to compute the XOR of the
    existing hash value (multiplied by 33) and the byte.

return tostring(hash)

Calls the built-in tostring() function to convert the numeric hash
    value to a string and returns the string as the value of the
    function.
<!--NeedCopy-->
```

Cas 2 : Réduire les doubles barres obliques dans les URL

La réduction des doubles barres obliques dans les URL améliore le temps de rendu du site Web, car les navigateurs analysent les URL de barre oblique unique plus efficacement. Les URL de barre oblique unique également pour maintenir la compatibilité avec les applications qui n'acceptent pas les barres obliques doubles. La fonction d'extension de stratégie permet aux clients d'ajouter une fonction qui remplace les barres obliques doubles par des barres obliques simples dans les URL. L'exemple suivant illustre l'ajout d'une fonction d'extension de stratégie qui réduit les doubles barres obliques dans les URL.

Exemple de définition de COLLAPSE_DOUBLE_SLASHES() :

```
    -- Collapse double slashes in URL to a single slash and return the
       result
    function NSTEXT:COLLAPSE_DOUBLE_SLASHES() : NSTEXT

        local result = string.gsub(self, "//", "/")

        return result

    end
<!--NeedCopy-->
```

Description ligne par ligne de l'échantillon ci-dessus :

```
function NSTEXT:COLLAPSE_DOUBLE_SLASHES() : NSTEXT

```



```
3 Declares the COLLAPSE_DOUBLE_SLASHES() function with text input and
     return.
4
5 local result = string.gsub(self, "//", "/")
6
7 Declares a local variable named result and uses the built-in string.
     gsub() function to replace all double slashes with single slashes in
      the self input text.
8
9 The second parameter of string.gsub() is actually a regular expression
     pattern, although here a simple string is used for the pattern.
10
11 return result
12
13 Returns the resulting string.
14 <!--NeedCopy-->
```

Cas 3 : Combiner des en-têtes

Certaines applications client ne peuvent pas gérer plusieurs en-têtes dans une demande. En outre, l'analyse des en-têtes en double avec les mêmes valeurs d'en-tête, ou de plusieurs en-têtes avec le même nom mais des valeurs différentes dans une requête, consomme du temps et des ressources réseau. La fonction d'extension de stratégie permet aux clients d'ajouter une fonction pour combiner ces en-têtes en en-têtes simples avec une valeur combinant les valeurs d'origine. Par exemple, en combinant les valeurs des en-têtes H1 et H2.

Demande originale :

```
1 GET /combine_headers HTTP/1.1
2 User-Agent: amigo unit test
3 Host: myhost
4 H2: h2val1
5 H1: abcd
6 Accept: \*/\*
7 H2: h2val2
8 Content-Length: 0
9 H2: h2val3
10 H1: 1234
11 <!--NeedCopy-->
```

Demande modifiée :

```
1 GET /combine_headers HTTP/1.1
2 User-Agent: amigo unit test
```



```
Host: myhost
H2: h2val1, h2val2, h2val3
H1: abcd, 1234
Accept: \*/\*
Content-Length: 0
<!--NeedCopy-->
```

En général, ce type de modification de demande est effectué à l'aide de la fonction Réécriture, à l'aide d'expressions de stratégie pour délimiter la partie de la demande à modifier (la cible) et la modification à effectuer (l'expression du générateur de chaîne). Cependant, les expressions de stratégie n'ont pas la possibilité d'itérer sur un nombre arbitraire d'en-têtes.

La solution à ce problème nécessite une extension de la fonction de stratégie. Pour ce faire, nous allons définir une fonction d'extension, appelée COMBINE_HEADERS. Avec cette fonction, nous pouvons configurer l'action de réécriture suivante :

```
> add rewrite action combine_headers_act replace 'HTTP.REQ.FULL_HEADER
.AFTER_STR("HTTP/1.1rn")''HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1rn").
COMBINE_HEADERS'
```

Ici, la cible de réécriture est HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1rn"). AFTER_STR("HTTP/1.1rn") est requis car FULL_HEADER inclut la première ligne de la requête HTTP (par exemple GET /combine_headers HTTP/1.1).

L'expression du générateur de chaîne est HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1rn").COMBINE_HEADERS où les en-têtes (moins la première ligne) sont introduits dans la fonction d'extension COMBINE_HEADERS, qui combine et renvoie les valeurs des en-têtes.

Exemple de définition de COMBINE_HEADERS() :

```
    -- Extension function to combine multiple headers of the same name
       into one header.



    function NSTEXT:COMBINE_HEADERS(): NSTEXT

        local headers = {
}
-- headers

        local combined_headers = {
}
-- headers with final combined values
        -- Iterate over each header (format "name:valuer\r\n")

```



```
16          -- and build a list of values for each unique header name.
17
18          for name, value in string.gmatch(self, "([^:]+):([^\r\n]*)\r\n"
                ) do
19
20              if headers[name] then
21
22                  local next_value_index = #(headers[name]) + 1
23
24                  headers[name][next_value_index] = value
25
26              else
27
28                  headers[name] = {
29  name .. ":" .. value }
30
31
32              end
33
34          end
35
36
37
38          -- iterate over the headers and concat the values with
                separator ","
39
40          for name, values in pairs(headers) do
41
42              local next_header_index = #combined_headers + 1
43
44              combined_headers[next_header_index] = table.concat(values,
                    ",")
45
46          end
47
48
49
50          -- Construct the result headers using table.concat()
51
52          local result_str = table.concat(combined_headers, "\r\n") .. "\
                r\n\r\n"
53
54          return result_str
55
56      end
```



```
<!--NeedCopy-->
```

Description ligne par ligne de l'échantillon ci-dessus :

```
function NSTEXT:COMBINE_HEADERS(): NSTEXT

Defines the COMBINE_HEADERS extension function, with the text input
    into the function from the policy expression and a text return type
    to the policy expression.

local headers = {
  }
  -- headers
local combined_headers = {
  }
  -- headers with final combined values

Declares local variables headers and combined_headers and initialize
    these variables to empty tables. headers will be a table of arrays
    of strings, where each array holds one or more values for a header.
    combined_headers will be an array of strings, where each array
    element is a header with its combined values.

for name, value in string.gmatch(self, "([^:]+):([^\r\n]*)\r\n") do
. . .
end
<!--NeedCopy-->
```

Cette boucle générique pour analyse chaque en-tête dans l'entrée. L'itérateur est la fonction string.gmatch() intégrée. Cette fonction prend deux paramètres : une chaîne à rechercher et un modèle à utiliser pour faire correspondre des morceaux de la chaîne. La chaîne à rechercher est fournie par le paramètre self implicite, qui est le texte des en-têtes entrés dans la fonction.

Le motif est exprimé en utilisant une expression régulière (regex pour abrégé). Cette regex correspond au nom et à la valeur d'en-tête de chaque en-tête, que la norme HTTP définit comme *nom* :*valeur*\r\n. Les parenthèses dans la regex spécifient les parties correspondantes à extraire, de sorte que le schéma regex est (*match-name*) : (*match-value*)\r\n. Le modèle de *nom de correspondance* doit correspondre à tous les caractères sauf les deux-points. Ceci est écrit [^ :]+ ([^ :] n'importe quel caractère sauf : et + est une ou plusieurs répétitions). De même, le modèle *de valeur de correspondance* doit correspondre à tous les caractères sauf le \ r \ n, donc il est écrit [^ \ r \ n]*([^ \ r \ n] correspond à n'importe quel caractère sauf \ r et \ n et* correspond à zéro ou plus de répétitions). Cela rend la regex complète ([^ :]+):([^ \ r \ n]*)\r\n.

L'instruction for utilise une affectation multiple pour définir le nom et la valeur des deux correspon-

dances renvoyées par l'itérateur string.gmatch (). Ceux-ci sont implicitement déclarés comme variables locales dans le corps de la boucle for.

```
if headers[name] then
     local next_value_index = #(headers[name]) + 1
     headers[name][next_value_index] = value
else
     headers[name] = {
 name .. ":" .. value }

end
<!--NeedCopy-->
```

Ces instructions dans la boucle for placent les noms et les valeurs d'en-tête dans la table des en-têtes. La première fois qu'un nom d'en-tête est analysé (par exemple H2 : h2val1 dans l'exemple d'entrée), il n'y a pas d'entrée d'en-tête pour le nom et le[nom] des en-têtes est nul.

Puisque nil est traité comme false, la clause else est exécutée. Cela définit l'entrée des en-têtes pour name à un tableau avec une valeur de chaîne *name* :*value.*

Remarque : Le constructeur de tableau dans la boucle else est équivalent à {[1] = name.. « : ».. value}, qui définit le premier élément du tableau.) Pour le premier en-tête H2, il définit les en-têtes[« H2"] = {" H2:H2Val1"}.

Sur les instances suivantes d'un en-tête, (disons, H2: h2val2 dans l'exemple d'entrée). en-têtes n'[nom] est pas nul, donc la clause then est exécutée. Cela détermine l'index disponible suivant dans la valeur du tableau pour les en-têtes[nom]et place la valeur d'en-tête dans cet index. Pour le deuxième en-tête H2, il définit les en-têtes[« H2"] = {"H2:h2val1", "h2val2"}.

```
for name, values in pairs(headers) do
    local next_header_index = #combined_headers + 1
    combined_headers[next_header_index] = table.concat(values, ",")
end
<!--NeedCopy-->
```

Une fois les en-têtes d'origine analysés et la table d'en-têtes remplie, cette boucle construit le tableau combined_headers. Il utilise la fonction pairs() comme itérateur de boucle.

Chaque appel à pairs() renvoie le nom et la valeur de l'entrée suivante dans la table des en-têtes.

La ligne suivante détermine l'index disponible suivant dans le tableau combined_headers, et la ligne suivante définit cet élément de tableau à l'en-tête combiné. Il utilise la fonction table.concat() intégrée, qui prend comme arguments un tableau de chaînes et une chaîne à utiliser comme séparateur, et renvoie une chaîne qui est la concaténation des chaînes de tableau, séparées par le séparateur.

Par exemple, pour les valeurs = {"H2:h2val1", "h2val2"}, cela produit "H2:h2val1, h2val2"


```
local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"
<!--NeedCopy-->
```

Après la construction du tableau combined_headers, il concatène les éléments en une chaîne et ajoute un double rn qui termine les en-têtes HTTP.

```
return result_str
<!--NeedCopy-->
```

Renvoie une chaîne comme résultat de la fonction d'extension COMBINE_HEADERS.

Dépannage des extensions de stratégie

August 20, 2021

Si votre fonction d'extension ne se comporte pas comme prévu, vous pouvez utiliser la fonctionnalité de suivi d'extension pour vérifier le comportement de votre fonction d'extension. Vous pouvez également ajouter la journalisation à votre fonction d'extension à l'aide de la fonctionnalité de journalisation personnalisée, dans laquelle vous pouvez définir le niveau de journalisation à capturer sur l'appliance Citrix ADC.

Cette rubrique fournit des informations sur :

- Suivi des extensions
- Journalisation personnalisée

Suivi des extensions

Pour montrer ce que fait votre fonction d'extension, la fonctionnalité de suivi des extensions enregistre l'exécution de la fonction dans le journal système de Citrix ADC (/var/log/ns.log). La journalisation du suivi utilise le niveau de journalisation DEBUG, qui n'est normalement pas activé. Par conséquent, vous devez activer TOUS les niveaux de journalisation. Vous pouvez ensuite activer le traçage en définissant l'option -trace de la commande set ns extension. Les paramètres disponibles sont les suivants :

- désactive le traçage (équivalent à unset ns extension -trace).
- appelle trace les appels de fonction avec des arguments et fonction retourne avec la première valeur de retour.
- tracent les numéros de ligne ci-dessus plus pour les lignes exécutées.
- tous les tracent ci-dessus plus les variables locales modifiées par les lignes exécutées.

Exemple :


```
set audit syslogParams -loglevel ALL

set ns extension combine_headers -trace all
<!--NeedCopy-->
```

Chaque message de trace a le format

```
log-header : default NSEXTENSION Message message-number 0 : "TRACE function
-name CALL call-number: event"
```

Où,

- fournit des horodatages, l'adresse IP Citrix ADC et l'ID du moteur de paquets.
- message-number est un numéro séquentiel identifiant le message de journal.
- fonction-name est le nom de la fonction d'extension.
- call-number est un numéro séquentiel pour chaque appel de fonction d'extension. Il peut être utilisé pour regrouper tous les messages de trace pour un appel de fonction d'extension.
- est l'un des événements suivants :
  - CALL fonction-name ; parameter-values indique que la fonction a été appelée avec les paramètres spécifiés.
  - RETURN From fonction-name ; return = valeur indique qu'une fonction a renvoyé la (première) valeur spécifiée. (Les valeurs de retour supplémentaires ne sont pas signalées.)
  - LINE line-number ; variable values indique qu'une ligne a été exécutée et répertorie toutes les variables dont les valeurs ont été modifiées.

Où,

- valeur ou valeurs est
  - un nombre, avec ou sans point décimal ;
  - une chaîne, entre guillemets doubles et avec des caractères échappés comme décrit plus tôt,
  - un booléen vrai ou fausse,
  - néant
  - un constructeur de table, au format {[key1]=valeur1,[key2]=valeur2,…}.
- parameter-values est parameter1 = value1 ; parameter2 = value2 , …
- variable-values est variable1 = value1 ; variable2 = value2 , …

Exemple de messages de journal abrégés :

```
>shell tail -f /var/log/ns.log | grep TRACE | more

... NSEXTENSION Message 3035 0 : "TRACE combine_headers CALL 30 : CALL
    COMBINE_HEADERS; self = "User-Agent: curl/7.24.0 (amd64-portbld-
    freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nHost:
```



```
      10.217.24.7\r\nAccept: \*/\*\r\nH2: h2val1\r\nH1: abcd\r\nH2: h2val2
      \r\nH2: h2val3\r\n\r\n""
4
5  ... NSEXTENSION Message 3036 0 : "TRACE combine_headers CALL 30 : LINE
      4; headers = {
6    }
7   "
8
9  ... NSEXTENSION Message 3037 0 : "TRACE combine_headers CALL 30 : LINE
      5; combined_headers = {
10   }
11  "
12
13 ... NSEXTENSION Message 3038 0 : "TRACE combine_headers CALL 30 : CALL
      gmatch"
14
15 ... NSEXTENSION Message 3039 0 : "TRACE combine_headers CALL 30 :
      RETURN FROM gmatch; return = function 0x2bee5a80"
16
17 ... NSEXTENSION Message 3040 0 : "TRACE combine_headers CALL 30 : CALL
      for iterator"
18
19 ... NSEXTENSION Message 3041 0 : "TRACE combine_headers CALL 30 :
      RETURN FROM for iterator; return = " curl/7.24.0 (amd64-portbld-
      freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3""
20
21 ... NSEXTENSION Message 3042 0 : "TRACE combine_headers CALL 30 : LINE
      9; name = "User-Agent"; value = " curl/7.24.0 (amd64-portbld-
      freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3""
22
23 ... NSEXTENSION Message 3043 0 : "TRACE combine_headers CALL 30 : LINE
      10"
24
25 ... NSEXTENSION Message 3044 0 : "TRACE combine_headers CALL 30 : LINE
      14; headers = {
26  ["User-Agent"]={
27  [1]="User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0
        OpenSSL/0.9.8y zlib/1.2.3" }
28   }
29  "
30
31 . . .
32
33 ... NSEXTENSION Message 3117 0 : "TRACE combine_headers CALL 30 : CALL
      for iterator"
```



```
34
35 ... NSEXTENSION Message 3118 0 : "TRACE combine_headers CALL 30 :
   RETURN FROM for iterator; return = nil"
36
37 ... NSEXTENSION Message 3119 0 : "TRACE combine_headers CALL 30 : LINE
   19"
38
39 ... NSEXTENSION Message 3120 0 : "TRACE combine_headers CALL 30 : CALL
   concat"
40
41 ... NSEXTENSION Message 3121 0 : "TRACE combine_headers CALL 30 :
   RETURN FROM concat; return = "User-Agent: curl/7.24.0 (amd64-portbld
   -freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nH1: abcd\r\
   nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1, h2val2, h2val3""
   ... NSEXTENSION Message 3122 0 : "TRACE combine_headers CALL 30 :
   LINE 25; result_str = "User-Agent: curl/7.24.0 (amd64-portbld-
   freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nH1: abcd\r\
   nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1, h2val2, h2val3\r\
   n\r\n""
42
43 ... NSEXTENSION Message 3123 0 : "TRACE combine_headers CALL 30 :
   RETURN FROM COMBINE_HEADERS; return = "User-Agent: curl/7.24.0 (
   amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r
   \nH1: abcd\r\nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1,
   h2val2, h2val3\r\n\r\n""
44 <!--NeedCopy-->
```

Journalisation personnalisée

Vous pouvez également ajouter votre propre journalisation à votre fonction d'extension. Pour ce faire, utilisez la fonction ns.logger:*level*() intégrée, où *level*est urgence, alert, critique, error, warning, notice, info ou debug. Les paramètres sont les mêmes que la fonction C printf() : une chaîne de format et un nombre variable d'arguments pour fournir les valeurs pour le % spécifié dans la chaîne de format. Par exemple, vous pouvez ajouter ce qui suit à la fonction COMBINE_HEADERS pour consigner le résultat d'un appel :

```
1 local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"
2
3 ns.logger:info("Result: %s", result_str)
4
5 return result_str
6 <!--NeedCopy-->
```


La fonction ci-dessus enregistrerait le message suivant vers/var/log/ns.log pour l'exemple d'entrée illustré dans les exemples de messages de journal abrégés dans la section Suivi des extensions ci-dessus.

```
... : default NSEXTENSION Message 143 0 : "Result: Host: 10.217.24.7:2000^M
 H1: abcd, 1234^M User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4)libcurl
/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Accept: */*^M H2: h2val1, h2val2,
h2val3^M ^M"
```

Optimisation

October 5, 2021

Les fonctionnalités d'optimisation Citrix ADC réduisent les temps de transaction entre les clients et les serveurs, et réduisent la consommation de bande passante. Ils améliorent également les performances du serveur en déchargeant certaines tâches et en rendant d'autres plus efficaces.

Fonctionnalité	Description
Keep-Alive du client	Gère plusieurs demandes sur une seule connexion client. Le client n'a pas besoin de négocier une nouvelle connexion pour chaque demande envoyée au serveur.
Compression HTTP	Compresse les réponses HTTP envoyées depuis les serveurs vers des navigateurs compatibles avec la compression. Les réponses plus petites réduisent le temps de téléchargement et économisent de la bande passante.
Mise en cache intégrée	Stocke les réponses aux demandes des clients. Les demandes suivantes pour le même contenu sont traitées à partir du cache Citrix ADC au lieu d'être transférées vers le serveur d'origine.
Optimisation frontale	Réduit le temps de chargement et de rendu des pages Web en simplifiant et en optimisant le contenu diffusé dans le navigateur client. **Remarque** : prise en charge à partir de NetScaler 10.5.

Fonctionnalité	Description
Accélérateur de contenu	Stocke les réponses du serveur sur une appliance Citrix ByteMobile T2100. **Remarque** : prise en charge à partir de NetScaler 10.1.

Keep-alive du client

August 20, 2021

La fonction de keep-alive du client permet d'envoyer plusieurs demandes de clients sur une seule connexion. Cette fonctionnalité bénéficie de la gestion des transactions. Lorsque le mode Keep-Alive du client est activé sur une appliance et que la réponse du serveur à la demande du client contient la connexion : fermez l'en-tête HTTP et exécute les tâches suivantes :

- Renomme le nom d'en-tête Connection existant en mélangeant les caractères du nom de l'en-tête.
- Ajoute un nouvel en-tête Connection : avec Keep-Alive comme valeur de l'en-tête.

Le mode Keep-Alive du client permet à l'appliance Citrix ADC de traiter plusieurs demandes et réponses à l'aide de la même connexion socket. La fonctionnalité maintient la connexion entre le client et l'appliance (connexion côté client) ouverte même après la fermeture de la connexion avec l'appliance par le serveur. Cela permet à plusieurs clients de demander à l'aide d'une seule connexion et enregistre les allers-retours associés à l'ouverture et à la fermeture d'une connexion. Le client Keep-alive est le plus bénéfique dans les sessions SSL.

Le keep-alive du client est utile pour les scénarios suivants :

- Si le serveur ne prend pas en charge le client keep-alive.
- Si le serveur prend en charge mais qu'une application sur le serveur ne prend pas en charge le client keep-alive.

> **Remarque :**
> La keep-alive du client est applicable pour le trafic HTTP et SSL. Client-Keep alive peut être configuré globalement pour gérer tout le trafic. En outre, vous pouvez l'activer sur des services spécifiques.

Dans l'environnement de keep-alive du client, les services configurés interceptent le trafic client et la demande du client est dirigée vers le serveur d'origine. Le serveur envoie la réponse et ferme la connexion entre le serveur et l'appliance. Si un en-tête "Connection: Close" est présent dans la réponse du serveur, l'appliance corrompt cet en-tête dans la réponse côté client et la connexion côté client est

maintenue ouverte. Par conséquent, le client n'a pas besoin d'ouvrir une nouvelle connexion pour la demande suivante. Au lieu de cela, la connexion au serveur est rouverte.

> **Remarque :**
> Si un serveur renvoie deux en-têtes « Connexion : Fermer », un seul est modifié. Cela entraîne des retards importants sur le rendu client de l'objet car un client ne suppose pas que l'objet a été livré complètement jusqu'à ce que la connexion soit fermée.

Configurer le client Keep-alive

Le client Keep-alive, par défaut, est désactivé sur Citrix ADC, à la fois globalement et au niveau du service. Par conséquent, vous devez activer la fonction à l'étendue requise.

> **Remarque :**
> si vous activez le client de manière globale, il est activé pour tous les services, que vous l'activez ou non au niveau du service. En outre, vous devez configurer certains paramètres HTTP pour spécifier les éléments suivants :
>
> - le nombre maximal de connexions HTTP conservées dans le pool de réutilisation des connexions.
> - activer le multiplexage des connexions et activer la persistance `Etag`.
>
> **Remarque :**
> Lorsque Persistant `ETag` est activé, l' `ETag` en-tête inclut des informations sur le serveur qui a servi le contenu. Cela garantit que les demandes conditionnelles de validation du cache ou les demandes de navigateur, pour ce contenu, atteignent toujours le même serveur.

Configurer la keep-alive du client à l'aide de l'interface de commande Citrix ADC

À l'invite de commandes, procédez comme suit :

1. Activez le client Keep-alive sur Citrix ADC.
   - Au niveau mondial - `enable ns mode cka`
   - Au niveau des services - `set service <name> -CKA YES`

   > **Remarque :**
   >
   > Le client keep-alive ne peut être activé que pour les services HTTP et SSL.

2. Configurez les paramètres HTTP sur le profil HTTP lié à un ou plusieurs services.

```
set ns httpProfile <name> -maxReusePool <value> -conMultiplex
    ENABLED -persistentETag ENABLED
<!--NeedCopy-->
```

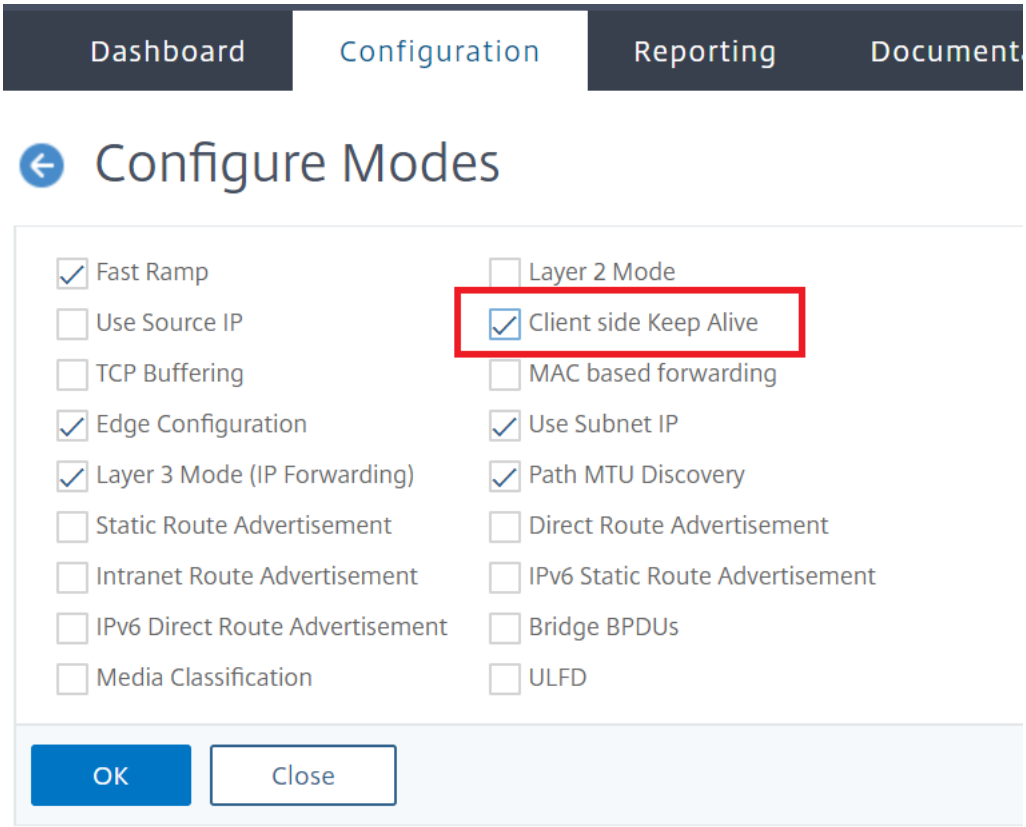

> **Remarque :**
>
> Configurez ces paramètres sur le profil `nshttp_default _profile HTTP` pour les rendre disponibles globalement.

Configurer la keep-alive du client à l'aide de Citrix ADC GUI

1. Activez le client Keep-alive sur Citrix ADC.

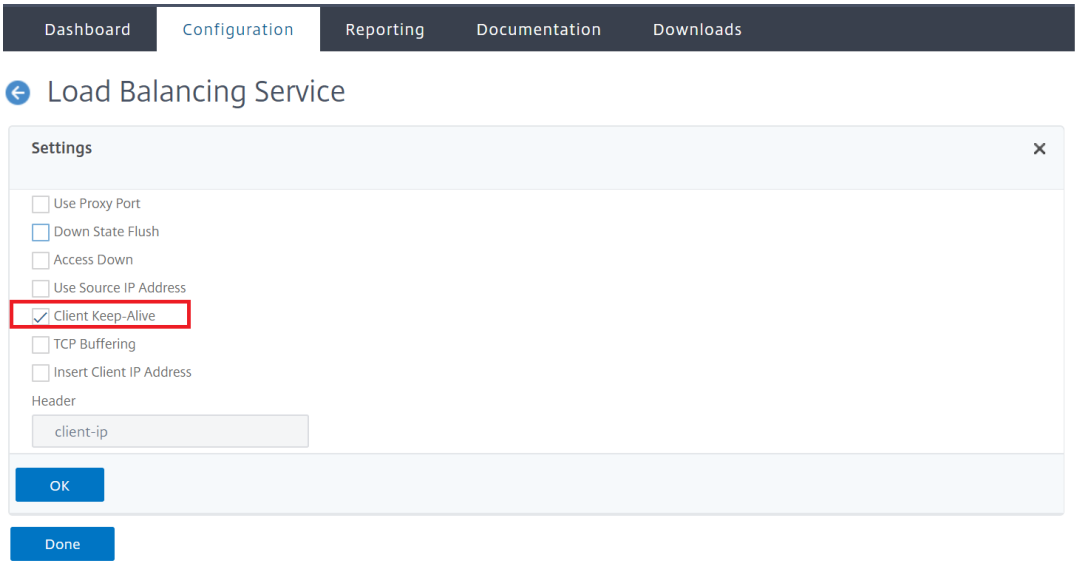
   - Au niveau global

     Accédez à **Système** > **Paramètres**, cliquez sur **Configurer les modes** et sélectionnez **Keep Alive côté client**.



   - Au niveau du service

     Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis sélectionnez le service requis. Dans la section **Paramètres**, activez la case à cocher **Keep-Alive du client**.



2. Configurez les paramètres HTTP requis sur le profil HTTP lié à un ou plusieurs services.
3. Accédez à **Système** > **Profils**, puis sous l'onglet **Profils HTTP**, sélectionnez le profil requis et mettez à jour les paramètres HTTP requis.

Compression HTTP

October 5, 2021

Pour les sites Web dont le contenu est compressible, la fonctionnalité de compression HTTP implémente une compression sans perte pour réduire la latence, les longs temps de téléchargement et d'autres problèmes de performances réseau en compressant les réponses HTTP envoyées depuis les serveurs vers les navigateurs sensibles à la compression. Vous pouvez améliorer les performances du serveur en déchargeant la tâche de compression gourmande en calcul de vos serveurs vers l'appliance Citrix ADC.

Le tableau suivant décrit les fonctionnalités de la fonction de compression HTTP :

Fonctionnalité	Description
Taux de compression	Le taux de compression dépend des types de fichiers contenus dans les réponses, mais il est toujours important, ce qui réduit sensiblement la quantité de données transmises sur le réseau.

Fonctionnalité	Description
Connaissance du navigateur	Citrix ADC sert les données compressées uniquement aux navigateurs compatibles avec la compression, ce qui réduit le temps de transaction entre le client et le serveur. La plupart des navigateurs Web modernes prennent en charge la compression HTTP.
blocage de la compression	Vous pouvez définir des filtres de contenu pour bloquer sélectivement la compression en appliquant des actions intégrées.
Mise en cache de compression	Lorsque la fonction de mise en cache intégrée est activée, les demandes suivantes pour le même contenu sont envoyées à partir du cache local, ce qui réduit le nombre d'allers-retours vers le serveur et améliore les temps de transaction.
Prise en charge HTTPS	La compression est utile sur les connexions SSL, car elle réduit la quantité de contenu qui doit être chiffré, sur le serveur ou par l'appliance Citrix ADC, et déchiffré par le client.
Filtrage intelligent des réponses	Le moteur de compression Citrix ADC filtre intelligemment les réponses du serveur en fonction des paramètres de compression définis. Par exemple, le moteur de compression détecte les réponses de longueur nulle et les réponses compressées et ne les compresse pas. La détection des réponses compressées permet aux sites d'origine d'utiliser la compression basée sur le serveur avec la fonctionnalité de compression Citrix ADC.

Fonctionnalité	Description
Commutation des	L'appliance Citrix ADC dirige de manière transparente les demandes des clients sensibles à la compression vers des serveurs compatibles avec la compression, afin que les réponses à ces clients soient compressées et que les réponses aux autres clients ne soient pas retardées par le traitement de compression.

Fonctionnement de la compression HTTP

Un Citrix ADC peut compresser des données statiques et générées dynamiquement. Il applique l'algorithme de compression GZIP ou DEFLATE pour supprimer les informations superflues et répétitives des réponses du serveur et représenter les informations d'origine dans un format plus compact et efficace. Ces données compressées sont envoyées au navigateur du client et décompressées selon les algorithmes pris en charge par le navigateur (GZIP ou DEFLATE).

La compression Citrix ADC traite différemment les contenus statiques et dynamiques.

- Les fichiers statiques ne sont compressés qu'une seule fois et une copie compressée est stockée dans la mémoire locale. Les demandes ultérieures des clients concernant les fichiers mis en cache sont traitées à partir de cette mémoire.
- Les pages dynamiques sont créées dynamiquement chaque fois qu'un client en fait la demande.

Lorsqu'un client envoie une demande au serveur :

1. La demande du client arrive au Citrix ADC. L'ADC examine les en-têtes et stocke des informations sur le type de compression, le cas échéant, pris en charge par le navigateur.
2. L'ADC transmet la demande au serveur et reçoit la réponse.
3. Le moteur de compression Citrix ADC examine la compressibilité de la réponse du serveur en la comparant aux stratégies.
4. Si la réponse correspond à une stratégie associée à une action de compression et que le navigateur client prend en charge un algorithme de compression spécifié par l'action, Citrix ADC applique l'algorithme et envoie la réponse compressée au navigateur client.
5. Le client applique l'algorithme de compression pris en charge pour décompresser la réponse.

Configurer la compression HTTP

Par défaut, la compression est désactivée sur Citrix ADC. Vous devez activer la fonctionnalité avant de la configurer. Si la fonctionnalité est activée, l'ADC compresse les demandes de serveur spécifiées par

les stratégies de compression.

Pour activer la compression HTTP à l'aide de l'interface de ligne de commande

La compression ne peut être activée que pour les services HTTP et SSL. Vous pouvez l'activer globalement, de sorte qu'il s'applique à tous les services HTTP et SSL, ou vous pouvez l'activer uniquement pour des services spécifiques.

À l'invite de commandes, saisissez l'une des commandes suivantes pour activer la compression globalement ou pour un service spécifique :

- `enable ns feature cmp`
  OU
- `set service \<name\> -CMP YES`

Pour configurer la compression à l'aide de l'interface graphique

Procédez comme suit :

Pour activer la compression globalement, accédez à Système > Paramètres, cliquez sur **Configurer les fonctionnalités de base**, puis sélectionnez Compression HTTP.

Pour activer la compression pour un service spécifique, accédez à **Gestion du trafic > Équilibrage de charge > Services**, sélectionnez le service, puis cliquez sur Modifier. Dans le groupe Paramètres, cliquez sur l'icône en forme de crayon et activez Compression.

Configuration d'une action de compression

Une action de compression spécifie l'action à effectuer lorsqu'une demande ou une réponse correspond à la règle (expression) de la stratégie à laquelle l'action est associée. Par exemple, vous pouvez configurer une stratégie de compression qui identifie les demandes qui seront envoyées à un serveur particulier et associer la stratégie à une action qui compresse la réponse du serveur.

Il existe quatre actions de compression intégrées :

- COMPRESSER : utilise l'algorithme GZIP pour compresser les données des navigateurs qui prennent en charge GZIP ou GZIP et DEFLATE. Utilise l'algorithme DEFLATE pour compresser les données des navigateurs qui prennent uniquement en charge l'algorithme DEFLATE. Si le navigateur ne prend pas en charge l'un ou l'autre algorithme, la réponse du navigateur n'est pas compressée.
- NOCOMPRESS : ne compresse pas les données.
- GZIP : utilise l'algorithme GZIP pour compresser les données des navigateurs qui prennent en charge la compression GZIP. Si le navigateur ne prend pas en charge l'algorithme GZIP, la réponse du navigateur n'est pas compressée.
- DEFLATE : utilise l'algorithme DEFLATE pour compresser les données des navigateurs qui prennent en charge l'algorithme DEFLATE. Si le navigateur ne prend pas en charge l'algorithme

DEFLATE, la réponse du navigateur n'est pas compressée. Après avoir créé une action, vous l'associez à une ou plusieurs stratégies de compression.

À l'invite de commandes, saisissez la commande suivante pour créer une action de compression :

```
add cmp action <name> <cmpType> [-addVaryHeader <addVaryHeader> -varyHeaderValue
<string>]
```

Pour configurer une stratégie de compression à l'aide de l'interface de ligne de commande

Une stratégie de compression contient une règle, qui est une expression logique qui permet à l'appliance Citrix ADC d'identifier le trafic à compresser.

Lorsque Citrix ADC reçoit une réponse HTTP d'un serveur, il évalue les stratégies de compression intégrées et les stratégies de compression personnalisées pour déterminer s'il faut compresser la réponse et, le cas échéant, le type de compression à appliquer. Les priorités attribuées aux stratégies déterminent l'ordre dans lequel les stratégies sont mises en correspondance avec les demandes.

À l'invite de commandes, saisissez la commande suivante pour créer une stratégie de compression :

```
add cmp policy <name> -rule <expression> -resAction <string>
```

Pour créer une action de compression à l'aide de l'interface graphique

Accédez à **Optimisation** > **Compression HTTP** > **Actions**, cliquez sur **Ajouter** et créez une action de compression pour spécifier le type de compression à effectuer sur la réponse HTTP.

Configuration d'une stratégie de compression

Une stratégie de compression contient une règle, qui est une expression logique qui permet à l'appliance Citrix ADC d'identifier le trafic à compresser.

Lorsque Citrix ADC reçoit une réponse HTTP d'un serveur, il évalue les stratégies de compression intégrées et les stratégies de compression personnalisées pour déterminer s'il faut compresser la réponse et, le cas échéant, le type de compression à appliquer. Les priorités attribuées aux stratégies déterminent l'ordre dans lequel les stratégies sont mises en correspondance avec les demandes.

Le tableau suivant répertorie les stratégies de compression HTTP intégrées. Ces stratégies sont activées globalement lorsque vous activez la compression.

Stratégie classique ou avancée intégrée	Description
ns_nocmp_mozilla_47, ns_adv_nocmp_mozilla_	Empêche la compression des fichiers CSS lorsqu'une requête est envoyée depuis un navigateur Mozilla 4.7.
ns_cmp_mscss, ns_adv_cmp_mscss	Compresse les fichiers CSS lorsque la demande est envoyée depuis un navigateur Microsoft Internet Explorer.

Stratégie classique ou avancée intégrée	Description
ns_cmp_msapp, ns_adv_cmp_msapp	Compresse les fichiers générés par les applications suivantes : Microsoft Office Word, Microsoft Office Excel, Microsoft Office PowerPoint.
ns_cmp_content_type, ns_adv_cmp_content_type	Compresse les données lorsque la réponse contient un en-tête Content-type et contient du texte.
ns_nocmp_xml_ie, ns_adv_nocmp_xml_ie	Empêche la compression lorsqu'une demande est envoyée à partir d'un navigateur Microsoft Internet Explorer et que la réponse contient un en-tête Content-Type et contient du texte ou du XML.

Liaison d'une stratégie de compression

Pour mettre en œuvre une stratégie de compression, vous devez la lier soit globalement, afin qu'elle s'applique à tout le trafic qui passe par Citrix ADC, ou à un serveur virtuel spécifique, de sorte que la stratégie s'applique uniquement aux demandes dont la destination est l'adresse VIP de ce serveur virtuel.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel nombre entier positif.

Pour lier une stratégie de compression à l'aide de l'interface de ligne de commande

À l'invite de commandes, saisissez l'une des commandes suivantes pour lier une stratégie de compression globalement ou à un serveur virtuel spécifique :

- `bind cmp global <policyName> [-priority <positive_integer>] [-state ( ENABLED|DISABLED)]...`
- `bind lb vserver <vserverName> -policyName <policyName> -priority < positive_integer>.`

Répétez cette commande pour chaque serveur virtuel auquel vous souhaitez lier la stratégie de compression.

Pour lier une stratégie de compression à l'aide de l'interface graphique

Procédez comme suit :

Au niveau global, accédez à **Optimisation** > **Compression HTTP** > **Stratégies**, cliquez sur **Gestionnaire de stratégies** et liez les stratégies requises en spécifiant le point de liaison et le type de connexion appropriés (demande/réponse).

Au niveau du serveur virtuel

Pour le serveur virtuel d'équilibrage de charge, accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez le serveur virtuel requis, cliquez sur **Stratégies**et liez la stratégie correspondante.

Pour le serveur virtuel de commutation de contenu, accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez le serveur virtuel requis, cliquez sur **Stratégies**et liez la stratégie correspondante.

Définissez les paramètres de compression globaux pour des performances optimales

De nombreux utilisateurs acceptent les valeurs par défaut des paramètres de compression globaux, mais vous pouvez peut-être fournir une compression plus efficace en personnalisant ces paramètres.

> **Remarque**
> Après avoir configuré les paramètres de compression globaux, il n'est pas nécessaire de redémarrer votre solution matérielle-logicielle. Ils sont immédiatement appliqués aux nouveaux flux.

Le tableau suivant décrit les paramètres de compression que vous pouvez définir sur Citrix ADC.

Paramètres de compression	Description
Taille Quantum	Taille, en Ko, de la mémoire tampon conservée pour l'accumulation des réponses du serveur. Les réponses sont compressées lorsque la taille de la mémoire tampon dépasse cette valeur. Par exemple, si vous définissez la taille quantique sur 50 Ko, Citrix ADC compresse le contenu du tampon lorsque sa taille dépasse 50 Ko. Valeur minimale : 1. Valeur maximale : 63488. Par défaut : 57344.
Niveau de compression	Niveau de compression à appliquer aux réponses du serveur. Valeurs possibles : meilleure vitesse, meilleure compression, optimale.
Taille de réponse HTTP minimale	Taille minimale, en octets, d'une réponse HTTP compressée. Les réponses inférieures à la valeur spécifiée par ce paramètre sont envoyées sans être compressées.

Paramètres de compression	Description
Contournement de la compression sur l'utilisation du processeur	Utilisation du processeur Citrix ADC, en pourcentage, égal ou supérieur à celui auquel aucune compression n'est effectuée. Par défaut : 100.
Type de politique*	Type de stratégies utilisées pour la compression. Valeurs possibles : stratégie classique, avancée. Par défaut : Classic.
Autoriser la compression côté serveur	Autorisez les serveurs à envoyer des données compressées vers Citrix ADC.
Compresser le paquet push	À la réception d'un paquet avec un drapeau TCP PUSH, compressez immédiatement les paquets accumulés, sans attendre que le tampon quantique soit rempli.
Cache externe	Émettez une directive de réponse privée indiquant que le message de réponse est destiné à un seul utilisateur et ne doit pas être mis en cache par un cache partagé ou proxy.

Pour configurer la compression HTTP à l'aide de l'interface graphique

Procédez comme suit :

- Pour activer la compression globalement, accédez à**Système**>**Paramètres**, cliquez sur**Configurer les fonctionnalités de base**, puis sélectionnez**Compression HTTP**.
- Pour activer la compression pour un service spécifique, accédez à**Gestion du trafic**>**Équilibrage de charge**>**Services**, sélectionnez le service, puis cliquez sur**Modifier**.
- Dans le groupe**Paramètres**, cliquez sur l'icône en forme de crayon et activez**Compression**.

Pour créer une action de compression à l'aide de l'interface graphique

Accédez à**Optimisation**>**Compression HTTP**>**Actions**, cliquez sur**Ajouter**et créez une action de compression pour spécifier le type de compression à effectuer sur la réponse HTTP.

Pour créer une stratégie de compression à l'aide de l'interface graphique

Accédez à**Optimisation**>**Compression HTTP**>**Stratégies**, cliquez sur**Ajouter**, puis créez une stratégie de compression en spécifiant la condition et l'action correspondante à exécuter.

Évaluation de la configuration de compression

Vous pouvez afficher les statistiques de compression dans l'utilitaire de tableau de bord ou dans un moniteur SNMP. L'utilitaire de tableau de bord affiche des statistiques récapitulatives et détaillées sous forme de tableau et de graphique.

Vous pouvez également afficher les statistiques d'une stratégie de compression, y compris le nombre de demandes incrémentées par le compteur de stratégie pendant la compression basée sur la stratégie.

> **Remarque**
>
> - Pour plus d'informations sur les statistiques et les graphiques, consultez l'aide du Tableau de bord sur l'appliance Citrix ADC.
> - Pour plus d'informations sur SNMP, consultez la rubriqueSNMP .

Pour afficher les statistiques de compression à l'aide de l'interface de ligne de commande

À l'invite de commandes, saisissez les commandes suivantes pour afficher les statistiques de compression :

1. Pour afficher le résumé des statistiques de compression.

```
stat cmp
```

> **Remarque**
> La commande stat cmp policy affiche les statistiques pour les stratégies de compression de stratégie avancée uniquement.

2. Pour afficher les résultats et les détails de la stratégie de compression

```
show cmp policy \<name\>
```

3. Pour afficher des statistiques de compression détaillées

```
stat cmp -detail
```

Pour afficher les statistiques de compression à l'aide du tableau de bord :

Dans l'utilitaire Tableau de bord, vous pouvez afficher les types de statistiques de compression suivants :

- Sélectionnez Compression pour afficher un résumé des statistiques de compression.
- Pour afficher des statistiques de compression détaillées par type de protocole, cliquez sur le bouton Détails
- Pour afficher le taux de demandes traitées par la fonction de compression, cliquez sur l'onglet Affichage graphique.

Pour afficher les statistiques de compression à l'aide du protocole SNMP

Vous pouvez afficher les statistiques de compression suivantes à l'aide de l'application de gestion de réseau SNMP.

- Nombre de demandes de compression (OID : 1.3.6.1.4.1.5951.4.1.1.50.1)
- Nombre d'octets compressés transmis (OID : 1.3.6.1.4.1.5951.4.1.1.50.2)
- Nombre d'octets compressibles reçus (OID : 1.3.6.1.4.1.5951.4.1.1.50.3)
- Nombre de paquets compressibles transmis (OID : 1.3.6.1.4.1.5951.4.1.1.50.4)
- Nombre de paquets compressibles reçus (OID : 1.3.6.1.4.1.5951.4.1.1.50.5)
- Rapport des données compressibles reçues et des données compressées transmises (OID : 1.3.6.1.4.1.5951.4.1.1.50.6)
- Rapport entre le total des données reçues et le total des données transmises (OID : 1.3.6.1.4.1.5951.4.1.1.50.7)

Pour afficher plus de statistiques de compression à l'aide de l'interface graphique

1. Pour afficher les statistiques de compression HTTP :

Accédez à **Optimisation** >**Compression HTTP**, puis cliquez sur**Statistiques**.

1. Pour afficher les statistiques d'une stratégie de compression.

Accédez à**Optimisation** >**Compression HTTP** >**Stratégies**, sélectionnez la stratégie, puis cliquez sur **Statistiques**.

1. Pour afficher les statistiques d'une étiquette de stratégie de compression
2. Accédez à**Optimisation** >**Compression HTTP** >**Stratégies**, sélectionnez une étiquette de stratégie, puis cliquez sur **Statistiques**.

Déchargement de la compression HTTP

La compression sur un serveur peut affecter les performances du serveur. Un Citrix ADC placé devant vos serveurs Web et configuré pour la compression HTTP supporte la compression du contenu statique et dynamique, ce qui permet d'économiser les cycles de processeur et les ressources du serveur.

Vous pouvez décharger la compression des serveurs Web de l'une des deux manières suivantes :

Désactivez la compression sur les serveurs Web, activez la fonctionnalité de compression Citrix ADC au niveau global et configurez les services pour la compression.

Laissez la fonction de compression activée sur les serveurs Web et configurez l'appliance Citrix ADC pour supprimer l'en-tête « Accept Encoding » de toutes les demandes des clients HTTP. Les serveurs envoient ensuite des réponses non compressées. Citrix ADC compresse les réponses du serveur avant de les envoyer aux clients.

> **Remarque**
> La deuxième option ne fonctionne pas si les serveurs compressent automatiquement toutes les réponses. Citrix ADC n'essaie pas de compresser une réponse déjà compressée.

Le paramètre Servercmp permet à l'appliance Citrix ADC de gérer la compression HTTP de déchargement. Par défaut, ce paramètre est défini sur ON pour que le serveur envoie des données compressées

à l'appliance Citrix ADC. Pour décharger la compression HTTP, vous devez définir le paramètre servercmp sur OFF. À l'invite de commandes, saisissez les commandes suivantes :

```
set service <service name> -CMP YES
```

Répétez cette commande pour chaque service pour lequel vous souhaitez activer la compression.

```
show service <service name>
```

Répétez cette commande pour chaque service afin de vérifier que la compression est activée.

```
Save config
```

```
set cmp parameter -serverCmp OFF
```

> **Remarque :**
>
> Lorsque le `Servercmp` paramètre est activé et que la solution matérielle-logicielle reçoit une réponse compressée du serveur, la solution matérielle-logicielle ne compresse plus les données. Au lieu de cela, il transmet la réponse compressée au client.

Mise en cache intégrée

August 20, 2021

Le cache intégré fournit un stockage en mémoire sur l'appliance Citrix ADC et fournit du contenu Web aux utilisateurs sans nécessiter un aller-retour vers un serveur d'origine. Pour le contenu statique, le cache intégré nécessite peu de configuration initiale. Après avoir activé la fonctionnalité de cache intégrée et effectué une configuration de base (par exemple, la détermination de la quantité de mémoire de l'appliance Citrix ADC que le cache est autorisée à utiliser), le cache intégré utilise des stratégies intégrées pour stocker et diffuser des types spécifiques de contenu statique, y compris des pages Web simples et des fichiers image. Vous pouvez également configurer le cache intégré pour stocker et diffuser du contenu dynamique marqué comme non mis en cache par les serveurs Web et d'applications (par exemple, les enregistrements de base de données et les cotations boursières).

> **Remarque :**
>
> Le terme Cache intégré peut être utilisé de façon interchangeable avec AppCache ; notez que d'un point de vue fonctionnel, les deux termes signifient la même chose.

Lorsqu'une demande ou une réponse correspond à la règle (expression logique) spécifiée dans une stratégie intégrée ou une stratégie que vous avez créée. L'appliance Citrix ADC exécute l'action associée à la stratégie. Par défaut, toutes les stratégies stockent les objets mis en cache dans et les récupèrent à partir du groupe de contenu par défaut. Vous pouvez créer vos propres groupes de contenu pour différents types de contenu.

Pour permettre à l'appliance de rechercher des objets mis en cache dans un groupe de contenu, vous pouvez configurer des sélecteurs. Les sélecteurs correspondent aux objets mis en cache et aux expressions, ou vous pouvez spécifier des paramètres pour rechercher des objets dans le groupe de contenu. Si vous utilisez des sélecteurs comme recommandé par Citrix, configurez-les d'abord, afin que vous puissiez spécifier des sélecteurs lorsque vous configurez des groupes de contenu. Ensuite, configurez les groupes de contenu que vous souhaitez ajouter afin qu'ils soient disponibles lorsque vous configurez les stratégies. Pour terminer la configuration initiale, créez des banques de stratégies en liant chaque stratégie à un point de liaison global ou à un serveur virtuel. Ou bien, vous pouvez lier une étiquette qui peut être appelée à partir d'autres banques de stratégies.

La mise en cache intégrée peut être améliorée en utilisant la méthode d'objet mis en cache de préchargement avant qu'ils ne soient planifiés pour expirer. Pour gérer la gestion des données mises en cache, vous pouvez configurer des en-têtes liés à la mise en cache insérés dans les réponses. Le cache intégré peut également servir de proxy de transfert pour d'autres serveurs de cache.

> **Remarque :**
>
> La mise en cache intégrée nécessite une certaine familiarité avec les demandes et réponses HTTP. Pour plus d'informations sur la structure des données HTTP, consultez *En-têtes HTTP en direct* à l'adresse"<http://livehttpheaders.mozdev.org/>."

Fonctionnement du cache d'intégration

Le cache intégré surveille les demandes HTTP et SQL qui circulent via l'appliance Citrix ADC et compare les demandes avec les stratégies stockées. Selon le résultat, la fonction de cache intégrée recherche la réponse dans le cache ou transmet la demande au serveur d'origine. Pour les requêtes HTTP, la mise en cache intégrée sert de contenu partiel à partir du cache en réponse à des demandes de plage d'octets unique et de plage d'octets multi-parties.

Les données mises en cache sont compressées si le client accepte le contenu compressé. Vous pouvez configurer les durées d'expiration d'un groupe de contenus et expirer sélectivement les entrées d'un groupe de contenus.

Les données qui sont servies à partir du cache intégré sont une requête, et les données transmises à partir de l'origine sont une manquer de cache, comme décrit dans le tableau suivant.

Type de mouvement	Spécifications
Cache touché	Réponses que l'appliance Citrix ADC sert à partir du cache, y compris : objets statiques, par exemple, fichiers image et pages Web statiques, 200 pages OK, 203 pages de réponse non faisant autorité, 300 pages à choix multiples, 301 pages déplacées définitivement, 302 pages trouvées, 304 pages non modifiées, Ces réponses sont appelées des réponses positives. L'appliance Citrix ADC met également en cache les réponses négatives suivantes : 307 pages de redirection temporaire, 403 pages interdites, 404 pages introuvables, 410 pages disparues. Pour améliorer encore les performances, vous pouvez configurer l'appliance Citrix ADC pour mettre en cache davantage de types de contenu.
Miss cache stockable	Pour une absence de cache stockable, l'appliance Citrix ADC récupère la réponse du serveur d'origine et stocke la réponse dans le cache avant de la servir au client.
Miss de cache non stockable	Un défaut de cache non stockable est inapproprié pour la mise en cache. Par défaut, toute réponse contenant les codes d'état suivants est une erreur de cache non stockable : 201, 202, 204, 205, 206 codes d'état, Tous les codes 4xx, sauf 403, 404 et 410, 5xx codes d'état

> **Remarque :**
> Pour intégrer la mise en cache dynamique à votre infrastructure applicative, utilisez l'API NITRO pour émettre des commandes de cache à distance. Par exemple, vous pouvez configurer des déclencheurs qui expirent les réponses mises en cache lorsqu'une table de base de données est mise à jour.

Pour assurer la synchronisation des réponses mises en cache avec les données sur le serveur d'origine, vous configurez les méthodes d'expiration. Lorsque l'appliance Citrix ADC reçoit une demande corre-

spondant à une réponse expirée, elle actualise la réponse du serveur d'origine.

> **Remarque :**
> Citrix vous recommande de synchroniser les heures sur l'appliance Citrix ADC et un ou plusieurs serveurs principaux.

Fonctionnement du cache dynamique

La mise en cache dynamique évalue les requêtes HTTP et les réponses basées sur des paires paramètre-valeur, des chaînes, des modèles de chaîne ou d'autres données. Par exemple, supposons qu'un utilisateur recherche le bogue 31231 dans une application de rapport de bogue. Le navigateur envoie la demande suivante au nom de l'utilisateur :

```
1     GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&
          Template=view&TableId=1000
2
3     Host: mycompany.net
4
5     User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9)
          Gecko/2008052906 Firefox/3.0
6
7     Accept: text/html,application/xhtml+xml,application/xml;q
          =0.9,\*/\*;q=0.8
8
9     Accept-Language: en-us,en;q=0.5
10 <!--NeedCopy-->
```

Dans cet exemple, les requêtes GET pour cette application de rapport de bogue contiennent toujours les paramètres suivants :

- IssuePage
- RecordID
- Modèle
- TableId

Les requêtes GET ne mettent pas à jour ou ne modifient pas les données. Vous pouvez donc configurer ces paramètres dans les stratégies de mise en cache et les sélecteurs, comme suit :

- Vous configurez une stratégie de mise en cache qui recherche la chaîne mybugreportingsystem et la méthode GET dans les requêtes HTTP. Cette stratégie dirige les demandes de correspondance vers un groupe de contenu pour les bogues.
- Dans le groupe de contenu pour les bogues, vous configurez un `hit` sélecteur qui correspond à différentes paires paramètres-valeur, y compris IssuePage, RecordiD, etc.

> **Remarque**
>
> Un navigateur peut envoyer plusieurs requêtes GET en fonction d'une action utilisateur. Voici une série de trois requêtes GET distinctes qu'un navigateur émet lorsqu'un utilisateur recherche un bogue basé sur un identifiant de bogue.

```
1     GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&
          Template=view&TableId=1000
2
3     GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=
          viewbtns&RecordId=31231&TableId=1000
4
5     GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=
          viewbody&RecordId=31231&tableid=1000
6 <!--NeedCopy-->
```

Pour répondre à ces demandes, plusieurs réponses sont envoyées au navigateur de l'utilisateur, et la page Web que l'utilisateur voit est un ensemble de réponses.

Si un utilisateur met à jour un rapport de bogue, les réponses correspondantes dans le cache doivent être actualisées avec les données du serveur d'origine. L'application de rapport de bogue émet des requêtes HTTP POST lorsqu'un utilisateur met à jour un rapport de bogue. Dans cet exemple, vous configurez les éléments suivants pour vous assurer que les demandes POST déclenchent l'invalidation dans le cache :

- Stratégie d'invalidation au moment de la requête qui recherche la chaîne mybugreportingsystem et la méthode de requête POST HTTP, et dirige les requêtes correspondantes vers le groupe de contenu pour les rapports de bogue.
- Sélecteur d'invalidation pour le groupe de contenu pour les rapports de bogue qui expire le contenu mis en cache en fonction du paramètre RecordID. Ce paramètre apparaît dans toutes les réponses, de sorte que le sélecteur d'invalidation peut expirer tous les éléments pertinents du cache.

L'extrait suivant montre une demande POST qui met à jour l'exemple de rapport de bogue.

```
1     POST /mybugreportingsystem/mybugreport.dll?TransitionForm HTTP/1.1\
          r\n
2
3     User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
          Opera 7.23 [en]\r\n
4
5     Host: mybugreportingsystem\r\n
6
7     Cookie:ttSearch.134=%23options%3Afalse%23active%23owner%3Afalse%23
          unowned%3Afalse%23submitter%3Afalse%23incsub%3Atrue;
```



```
8
9       Cookie2: $Version=1\r\n
10
11      . . .
12
13      \r\n
14
15      ProjectId=2&RecordId=31231&TableId=1000&TransitionId=1&Action=
           Update&CopyProjectId=0&ReloadForm=0&State=&RecordLockId=49873+
           issues+in+HTTP&F43. . .
16  <!--NeedCopy-->
```

Lorsque l'appliance Citrix ADC reçoit cette demande, il effectue les opérations suivantes :

- Correspond à la demande avec une stratégie d'invalidation.
- Recherche le groupe de contenu nommé dans la stratégie.
- Applique le sélecteur d'invalidation pour ce groupe de contenus et expire toutes les réponses correspondant à RecorDid=31231.

Lorsqu'un utilisateur émet une nouvelle demande pour ce rapport de bogue, l'appliance Citrix ADC accède au serveur d'origine pour obtenir des copies mises à jour de toutes les réponses associées à l'instance de rapport. Il stocke les réponses dans le groupe de contenu et les sert au navigateur de l'utilisateur, qui réassemble le rapport et l'affiche.

Configurer le cache intégré

Pour utiliser le cache intégré, vous devez installer la licence et activer la fonctionnalité. Après avoir activé le cache intégré, l'appliance Citrix ADC® met automatiquement en cache les objets statiques tels que spécifiés par les stratégies intégrées et génère des statistiques sur le comportement du cache. (Les stratégies intégrées ont un trait de soulignement dans la position initiale du nom de la stratégie.)

Même si les stratégies intégrées conviennent à votre situation, vous pouvez modifier les attributs globaux. Par exemple, vous pouvez modifier la quantité de mémoire de l'appliance Citrix ADC allouée au cache intégré.

Si vous souhaitez observer le fonctionnement du cache avant de modifier les paramètres, reportez-vous à la section « Affichage des objets mis en cache et des statistiques de cache ». «

> **Remarque :**
>
> Le cache Citrix ADC est un magasin en mémoire qui est purgé lorsque vous redémarrez l'appliance.

Pour installer la licence de cache intégrée

- Une licence de cache intégrée est requise.

- Obtenez un code de licence auprès de Citrix, accédez à l'interface de ligne de commande et connectez-vous.

Sur l'interface de ligne de commande, copiez le fichier de licence `/nsconfig/license` dans le dossier.

- Redémarrez l'appliance Citrix ADC à l'aide de la commande suivante :

```
reboot
```

Pour activer la mise en cache intégrée :
lorsque vous activez la mise en cache intégrée, l'appliance Citrix ADC commence à mettre en cache les réponses du serveur. Si vous n'avez configuré aucune stratégie ou groupe de contenu, les stratégies intégrées stockent les objets mis en cache dans le groupe de contenu par défaut.

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver la mise en cache intégrée :

```
enable ns feature IC
```

Configurer les attributs globaux pour la mise en cache

Les attributs globaux s'appliquent à toutes les données mises en cache. Vous pouvez spécifier la quantité de mémoire Citrix ADC allouée au cache intégré, Via l'insertion d'en-tête. Critère permettant de vérifier qu'un objet mis en cache doit être servi. Longueur maximale d'un corps POST autorisé dans le cache, s'il faut contourner l'évaluation de stratégie pour les requêtes HTTP GET et action à entreprendre lorsqu'une stratégie ne peut pas être évaluée.

La capacité de mémoire cache est limitée uniquement par la mémoire de l'appliance matérielle. En outre, tout moteur de paquets (concentrateur de distribution central de toutes les requêtes TCP entrantes) dans l'appliance NCore Citrix ADC est conscient des objets mis en cache par d'autres moteurs de paquets dans l'appliance NCore Citrix ADC.

> **Remarque :**
>
> Lorsque la limite de mémoire globale par défaut est définie sur 0 et que la fonctionnalité de mise en cache intégrée (IC) est activée, l'appliance ne met en cache aucun objet. Pour la mise en cache, vous devez configurer explicitement la limite de mémoire globale. Toutefois, si vous activez l'option « définir l'authentification, l'autorisation et le paramètre d'audit EnableStaticPageCaching », il y aura une certaine mémoire configurée par défaut dans l'appliance. Cette mémoire est insuffisante pour mettre en cache des objets volumineux et il est donc nécessaire d'attribuer une limite de mémoire plus élevée à IC. Vous pouvez effectuer cette opération en configurant la commande « set cache parameter —memLimit ». Le nouveau paramètre n'est appliqué qu'après avoir enregistré la configuration et redémarré l'appliance.

Vous pouvez modifier la limite de mémoire globale configurée pour les objets de mise en cache. Toutefois, lorsque vous mettez à jour la limite de mémoire globale à une valeur inférieure à la valeur existante (par exemple, de 10 Go à 4 Go), l'appliance continue d'utiliser la limite de mémoire.

Cela signifie que même si la limite de mise en cache intégrée est configurée à une certaine valeur, la limite réelle utilisée peut être plus élevée. Cette mémoire excessive est cependant libérée lorsque les objets sont supprimés du cache.

La sortie de la commande show cache parameter indique la valeur configurée (limite d'utilisation de la mémoire) et la valeur réelle utilisée (limite d'utilisation de la mémoire (valeur active)).

À l'invite de commandes, tapez :

```
1     set cache parameter [-memLimit <MBytes>] [-via <string>] [-
         verifyUsing <criterion>] [-maxPostLen <positiveInteger>] [-
         prefetchMaxPending <positiveInteger>] [-enableBypass(YES|NO)] [-
         undefAction (NOCACHE|RESET)]
2 <!--NeedCopy-->
```

Activer la mise en cache intégrée par l'interface graphique Citrix ADC

Accédez à **Système** > **Paramètres**, cliquez sur **Configurer les fonctionnalités de base**, puis sélectionnez **Mise en cache intégrée**.

Configurer les paramètres globaux pour la mise en cache à l'aide de l'interface graphique Citrix ADC

Accédez à **Optimisation** > **Mise en cache intégrée**, cliquez sur **Modifier les paramètres du cache** et configurez les paramètres globaux pour la mise en cache.

Configurer un groupe de contenu intégré, un jeu de modèles et des stratégies pour le cache intégré

L'appliance Citrix ADC comprend une configuration intégrée de mise en cache que vous pouvez utiliser pour mettre en cache du contenu. La configuration se compose d'un groupe de contenu appelé ctx_cg_poc, d'un jeu de motifs appelé ctx_file_extensions et d'un ensemble de stratégies de cache intégrées. Dans le groupe de contenu ctx_cg_poc, seuls les objets d'une taille inférieure ou inférieure à 500 Ko sont mis en cache. Le contenu est mis en cache pendant 86000 secondes et la limite de mémoire pour le groupe de contenus est de 512 Mo. Le jeu de motifs est un tableau indexé d'extensions communes pour la correspondance de type de fichier.

Le tableau suivant répertorie les stratégies intégrées de mise en cache. Par défaut, les stratégies ne sont liées à aucun point de liaison. Vous devez lier les stratégies à un point de liaison si vous souhaitez

que l'appliance Citrix ADC évalue le trafic par rapport aux stratégies. Les stratégies mettent en cache les objets du groupe de contenu ctx_cg_poc.

Nom de la stratégie de mise en cache intégrée	Règle de stratégie
_cacheVPNStaticObjects	HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS_IN
_cacheTCPVPNStaticObjects	HTTP.REQ.URL.ENDSWITH(".css")
_cacheOCVPNStaticObjects	HTTP.REQ.URL.ENDSWITH(".pdf")
_cacheWFStaticObjects	HTTP.REQ.URL.ENDSWITH(".js")
_mayNoCacheReq	HTTP.RES.HEADER("Content-Type").CONTAINS("application/x-javascript")
_noCacheRest	VRAI

Configuration du cache de vidage

Vous pouvez vider un groupe de cache, des groupes de cache ou un localisateur d'objets de cache. Voici les commandes pour vider les objets de cache.

À l'invite de commandes, tapez :

```
flush cache contentgroup all
```

Exemple

```
1          0x00000089bae000000004 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hello
2          0x00000089bae000000005 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hi
3
4          Flush cache contentGroup all
5          done
6
7  `flush cache contentgroup <content group name>`
8  <!--NeedCopy-->
```

Exemple :

```
1          0x00000089bae000000004 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hello
2          0x00000089bae000000005 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hi
```



```
3
4         Flush cache ob -| 0x00000089bae000000004
5         done
6
7 `flush cache object (-locator <positive_integer> | (-url <URL> (-host <
     string> [-port <port>] [-groupName <string>] [-httpMethod ( GET |
     POST )]))))`
8 <!--NeedCopy-->
```

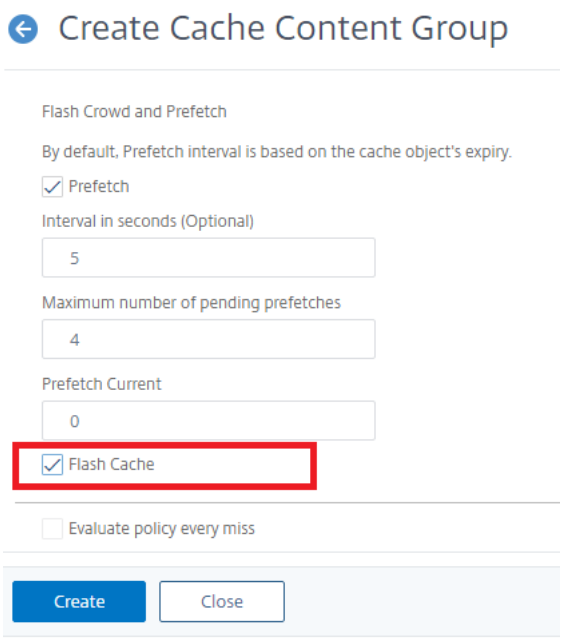
Exemple :

```
1         0x00000089bae000000006 DEFAULT GET //1.1.1.1:80/html/index.html
2
3         flush cache ob -URL /html/index.html -host 1.1.1.1 -groupName
             DEFAULT
4         done
5 <!--NeedCopy-->
```

Vider la configuration du cache à l'aide de l'interface graphique Citrix ADC

Suivez les étapes pour configurer le vidage du cache à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Optimisation** > **Groupes de contenu**.
2. Dans le volet détaillé **Groupes de contenu**, cliquez sur **Ajouter**.
3. Dans la page **Créer des groupes de contenu de cache**, définissez le paramètre suivant sous l'onglet **Autres** :
   a) Vider le cache. Activez la case à cocher pour vider l'objet cache.
4. Cliquez sur **Créer** et **Fermer**.



Configurer la mise en cache intégrée pour différents scénarios

La section suivante décrit la configuration de la mise en cache intégrée sur l'appliance NetScaler pour différents scénarios.

À partir de la version NetScaler 9.2, la mise en cache intégrée a plus de mémoire pour la mise en cache. La mémoire de mise en cache intégrée n'est limitée que par la mémoire disponible sur l'appliance matérielle. Vous pouvez allouer jusqu'à 50 % de la mémoire disponible à la fonction de mise en cache intégrée.

Pour définir l'allocation de mémoire pour le cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cache parameter -memlimit <value>
```

> **Remarque :**
>
> La limite de mémoire globale par défaut pour la mise en cache intégrée est nulle. Par conséquent, même si vous activez la fonctionnalité de mise en cache intégrée, l'appliance NetScaler ne met en cache aucun objet tant que la limite de mémoire globale n'est pas explicitement définie.

La section suivante vous indique de configurer la mise en cache intégrée sur différents scénarios.

> **Remarque :**
>
> La limite de mémoire de l'appliance NetScaler est identifiée au démarrage de l'appliance. Par

> conséquent, toute modification de la limite de mémoire nécessite le redémarrage de l'appliance pour que les modifications soient applicables à tous les moteurs de paquets.

La mise en cache intégrée est activée et la limite de mémoire cache est définie sur une valeur non nulle

Considérons un scénario selon lequel vous démarrez l'appliance, la fonctionnalité de mise en cache intégrée est activée et la limite de mémoire globale est définie sur un nombre positif. La mémoire que vous aviez définie précédemment est allouée à la fonction de mise en cache intégrée pendant le processus de démarrage. Vous pouvez modifier la limite de mémoire en fonction de la mémoire disponible sur l'appliance.

Configuration à l'aide de l'interface de ligne de commande

1. Afficher le paramètre cache

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 MBytes
4                  Memory usage limit (active value): 500 MBytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

1. Définir une limite de mémoire non nulle

```
set cache parameter -memlimit 600
```

> **Remarque :**
>
> La commande précédente affiche le message d'avertissement suivant : **Avertissement : Pour utiliser une nouvelle limite de mémoire cache intégrée, enregistrez la configuration et redémarrez l'appliance NetScaler.**

1. Enregistrer la configuration

```
save config
```

1. À partir de l'invite shell, exécutez la commande suivante pour vérifier dans le fichier de configuration.


```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 600 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 0 -enableBypass YES -undefAction NOCACHE
```

1. Redémarrer l'appliance

```
root@ns## reboot
```

1. Vérifier la nouvelle valeur de la limite de mémoire

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 600 MBytes
4                  Memory usage limit (active value): 600 MBytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

Une fois tous les moteurs de paquets démarrés avec succès, la fonction de mise en cache intégrée négocie la mémoire que vous aviez configurée. Si l'appliance ne peut pas utiliser la mémoire configurée, la mémoire est allouée en conséquence. Si la mémoire disponible est inférieure à celle que vous avez allouée, l'appliance recommande un nombre inférieur. La fonction de mise en cache intégrée utilise la même chose que la valeur active.

La mise en cache intégrée est désactivée et la limite de mémoire cache est définie sur une valeur non nulle

Dans ce scénario, lorsque vous démarrez l'appliance, la fonctionnalité de mise en cache intégrée est désactivée et la limite de mémoire globale est définie sur un nombre positif. Par conséquent, aucune mémoire n'est allouée à la mise en cache intégrée pendant le processus de démarrage.

Configuration à l'aide de l'interface de ligne de commande

1. Afficher le paramètre cache

```
1          > show cache parameter
2                  Integrated cache global configuration:
```



```
3                   Memory usage limit: 600 MBytes
4                   Maximum value for Memory usage limit: 843 MBytes
5                   Via header: NS-CACHE-9.3: 18
6                   Verify cached object using: HOSTNAME_AND_IP
7                   Max POST body size to accumulate: 0 bytes
8                   Current outstanding prefetches: 0
9                   Max outstanding prefetches: 4294967295
10                  Treat NOCACHE policies as BYPASS policies: YES
11                  Global Undef Action: NOCACHE
12  <!--NeedCopy-->
```

1. Définir une nouvelle limite de mémoire

```
set cache parameter -memlimit 500
```

> **Remarque :**
>
> La commande précédente affiche le message d'avertissement suivant : **Avertissement : Fonctionnalité non activée [IC]**.

1. Enregistrer la configuration

```
save config
```

1. À partir de l'invite shell, exécutez la commande suivante pour vérifier dans le fichier de configuration

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 500 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 0 -enableBypass YES -undefAction NOCACHE
```

1. Vérifier la nouvelle valeur de la limite de mémoire

```
1           > show cache parameter
2                   Integrated cache global configuration:
3                   Memory usage limit: 500 MBytes
4                   Maximum value for Memory usage limit: 843 MBytes
5                   Via header: NS-CACHE-9.3: 18
6                   Verify cached object using: HOSTNAME_AND_IP
7                   Max POST body size to accumulate: 0 bytes
8                   Current outstanding prefetches: 0
9                   Max outstanding prefetches: 4294967295
10                  Treat NOCACHE policies as BYPASS policies: YES
11                  Global Undef Action: NOCACHE
12  <!--NeedCopy-->
```


1. Activer la fonctionnalité de mise en cache intégrée

```
enable ns feature IC
```

1. Vérifier la nouvelle valeur de la limite de mémoire

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 Mbytes
4                  Memory usage limit (active value): 500 Mbytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

> **Remarque :**
>
> 500 Mo de mémoire sont alloués à la fonction de mise en cache intégrée.

1. Enregistrez la configuration pour vous assurer que la mémoire est automatiquement allouée à la fonction au redémarrage de l'appliance.

La mise en cache intégrée est activée et la mémoire cache est définie sur zéro

Dans ce scénario, lorsque vous démarrez l'appliance, la fonctionnalité de mise en cache intégrée est activée et la limite de mémoire globale est définie sur zéro. Par conséquent, aucune mémoire n'est allouée à la mise en cache intégrée pendant le processus de démarrage.

Configuration à l'aide de l'interface de ligne de commande

1. Vérifiez les limites de mémoire définies dans le fichier ns.conf à partir de l'invite shell

```
root@ns## cat ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 0 -via NS-CACHE-9.3: 18 -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

1. Vérifier la valeur de la limite de mémoire

```
1          > show cache parameter
```



```
2                   Integrated cache global configuration:
3                   Memory usage limit: 0 Mbytes
4                   Maximum value for Memory usage limit: 843 MBytes
5                   Via header: NS-CACHE-9.3: 18
6                   Verify cached object using: HOSTNAME_AND_IP
7                   Max POST body size to accumulate: 0 bytes
8                   Current outstanding prefetches: 0
9                   Max outstanding prefetches: 4294967295
10                  Treat NOCACHE policies as BYPASS policies: YES
11                  Global Undef Action: NOCACHE
12 <!--NeedCopy-->
```

> **Remarque :**
>
> La limite de mémoire est définie sur 0 Mo et aucune mémoire n'est allouée à la fonction de mise en cache intégrée.

1. Définissez les limites de mémoire pour garantir que la fonction de mise en cache intégrée met en cache les objets

```
set cache parameter -memLimit 600
```

Une fois la commande précédente exécutée, l'appliance négocie la mémoire pour la fonction de mise en cache intégrée et la mémoire disponible est affectée à la fonction. L'appliance met en cache les objets sans redémarrer l'appliance.

1. Vérifier la valeur de la limite de mémoire

```
1          > show cache parameter
2                   Integrated cache global configuration:
3                   Memory usage limit: 600 Mbytes
4                   Memory usage limit (active value): 600 Mbytes
5                   Maximum value for Memory usage limit: 843 MBytes
6                   Via header: NS-CACHE-9.3:
7                   Verify cached object using: HOSTNAME_AND_IP
8                   Max POST body size to accumulate: 0 bytes
9                   Current outstanding prefetches: 0
10                  Max outstanding prefetches: 4294967295
11                  Treat NOCACHE policies as BYPASS policies: YES
12                  Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

> **Remarque :**
>
> 600 Mo de mémoire sont alloués à la fonction de mise en cache intégrée.

1. Enregistrez la configuration. Assurez-vous que la mémoire est automatiquement allouée à la fonction lorsque l'appliance est redémarrée.
2. Vérifiez les limites de mémoire définies dans le fichier ns.conf à partir de l'invite shell

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 600 -via NS-CACHE-9.3: -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

La mise en cache intégrée est désactivée et la mémoire cache est définie sur zéro

Dans ce scénario, lorsque vous démarrez l'appliance, la fonctionnalité de mise en cache intégrée est désactivée et la limite de mémoire globale est définie sur zéro. Par conséquent, aucune mémoire n'est allouée à la mise en cache intégrée pendant le processus de démarrage.

Configuration à l'aide de l'interface de ligne de commande

1. Vérifiez les limites de mémoire définies dans le fichier ns.conf à partir de l'invite shell

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 0 -via NS-CACHE-9.3: 18 -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

1. Vérifier la valeur de la limite de mémoire

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 0 Mbytes
4                  Maximum value for Memory usage limit: 843 MBytes
5                  Via header: NS-CACHE-9.3: 18
6                  Verify cached object using: HOSTNAME_AND_IP
7                  Max POST body size to accumulate: 0 bytes
8                  Current outstanding prefetches: 0
9                  Max outstanding prefetches: 4294967295
10                 Treat NOCACHE policies as BYPASS policies: YES
11                 Global Undef Action: NOCACHE
12 <!--NeedCopy-->
```

> **Remarque :**
>
> La limite de mémoire est définie sur 0 Mo et aucune mémoire n'est allouée à la fonction de mise

> en cache intégrée. En outre, lorsque vous exécutez une commande de configuration du cache, le message d'avertissement suivant s'affiche : **Avertissement : Fonction non activée [IC]**.

1. Activer la fonctionnalité de mise en cache intégrée

```
enable ns feature IC
```

> **Remarque :**
>
> À ce stade, lorsque vous activez la fonctionnalité de mise en cache intégrée, l'appliance n'alloue pas de mémoire à la fonction. Par conséquent, aucun objet n'est mis en cache dans la mémoire. En outre, lorsque vous exécutez une commande de configuration du cache, le message d'avertissement suivant s'affiche : **Aucune mémoire n'est configurée pour IC. Utilisez la commande set cache paramètre pour définir la limite de mémoire.**

1. Définissez les limites de mémoire pour garantir que la fonction de mise en cache intégrée met en cache les objets

```
set cache parameter -memLimit 500
```

Une fois la commande précédente exécutée, l'appliance négocie la mémoire pour la fonction de mise en cache intégrée et la mémoire disponible est affectée à la fonction. L'appliance met en cache les objets sans redémarrer l'appliance.

> **Remarque :**
>
> L'ordre dans lequel vous activez la fonction et définissez les limites de mémoire est important. Si vous définissez les limites de mémoire avant d'activer la fonction, le message d'avertissement suivant s'affiche : **Avertissement : Fonction non activée [IC]**.

1. Vérifier la valeur de la limite de mémoire

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 Mbytes
4                  Memory usage limit (active value): 500 Mbytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3:
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```


> **Remarque :**
>
> 500 Mo de mémoire sont alloués à la fonction de mise en cache intégrée.

1. Enregistrer la configuration

```
save config
```

1. Vérifiez les limites de mémoire définies dans le fichier ns.conf à partir de l'invite shell

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 500 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

Configurer les sélecteurs et les groupes de contenu de base

August 20, 2021

Vous pouvez configurer des sélecteurs et les appliquer à des groupes de contenu. Lorsque vous ajoutez un sélecteur à un ou plusieurs groupes de contenu, vous spécifiez si le sélecteur doit être utilisé pour identifier les demandes de cache ou identifier les objets mis en cache à invalider (expiré). Les sélecteurs sont facultatifs. Vous pouvez également configurer des groupes de contenu pour qu'ils utilisent des `hit` paramètres et des paramètres d'invalidation. Toutefois, Citrix vous recommande de configurer les sélecteurs.

Après avoir configuré les sélecteurs ou décidé d'utiliser des paramètres à la place, vous êtes prêt à configurer un groupe de contenus de base. Après avoir créé le groupe de contenu de base, vous devez décider comment les objets doivent expirer du cache et configurer l'expiration du cache. Vous pouvez modifier davantage le cache comme décrit dans Amélioration des performances du cache et Configuration des cookies, des en-têtes et des interrogations, mais vous pouvez tout d'abord configurer des stratégies de mise en cache.

> **Remarque**
>
> Les paramètres et sélecteurs du groupe de contenu sont utilisés uniquement au moment de la demande et vous les associez généralement à des stratégies qui utilisent des actions MAY_CACHE ou MAY_NOCACHE.

Avantages des sélecteurs

Un sélecteur est un filtre qui localise des objets particuliers dans un groupe de contenu. Si vous ne configurez pas de sélecteur, l'appliance Citrix® ADC recherche une correspondance exacte dans

le groupe de contenus. Cela peut conduire à plusieurs copies du même objet résidant dans un groupe de contenus. Par exemple, un groupe de contenu qui n'a pas de sélecteur peut avoir besoin de stocker des URL pour host1.domain.commypage.htm, host2.domain.commypage.htm et host3.domain.commypage.htm. En revanche, un sélecteur peut correspondre uniquement à l'URL (mypage.html, en utilisant l'expression http.req.url) et au domaine (.com, en utilisant l'expression http.req.hostname.domain), permettant aux requêtes d'être satisfaites par la même URL.

Les expressions de sélecteur peuvent effectuer une correspondance simple des paramètres (par exemple, pour trouver des objets qui correspondent à quelques paramètres de chaîne de requête et à leurs valeurs). Une expression sélecteur peut utiliser une logique booléenne, des opérations arithmétiques et des combinaisons d'attributs pour identifier des objets (par exemple, des segments d'une tige d'URL, une chaîne de requête, une chaîne dans un corps de requête POST, une chaîne dans un en-tête HTTP, un cookie). Les sélecteurs peuvent également exécuter des fonctions programmatiques pour analyser les informations dans une demande. Par exemple, un sélecteur peut extraire du texte dans un corps POST, convertir le texte en liste et extraire un élément spécifique de la liste.

Pour plus d'informations sur les expressions et sur ce que vous pouvez spécifier dans une expression, voir Stratégies et expressions.

Utiliser les paramètres au lieu de sélecteurs

Bien que Citrix recommande l'utilisation de sélecteurs avec un groupe de contenu, vous pouvez configurer des `hit` paramètres et des paramètres d'invalidation. Par exemple, supposons que vous configurez trois paramètres `hit` dans un groupe de contenu pour les rapports de bogues : BugID, Issuer et Assignee. Si une requête contient BugID = 456, avec issuer=RohitV et Assignee=Robert, l'appliance Citrix ADC peut fournir des réponses correspondant à ces paires paramètre-valeur.

Les paramètres d'invalidation dans un groupe de contenu expirent les entrées mises en cache. Par exemple, supposons que BugID soit un paramètre d'invalidation et qu'un utilisateur émet une requête POST pour mettre à jour un rapport de bogue. Une stratégie d'invalidation dirige la demande vers ce groupe de contenu et le paramètre d'invalidation du groupe de contenu expire toutes les réponses mises en cache qui correspondent à la valeur BugID. (La prochaine fois qu'un utilisateur émet une requête GET pour ce rapport, une stratégie de mise en cache peut permettre à l'appliance Citrix ADC d'actualiser l'entrée mise en cache du rapport à partir du serveur d'origine.)

Notez que le même paramètre peut être utilisé comme `hit` paramètre ou paramètre d'invalidation.

Les groupes de contenu extraient les paramètres de demande dans l'ordre suivant :

- Requête URL
- Corps POST
- En-tête de cookie

Après la première occurrence d'un paramètre, quel que soit l'endroit où il s'est produit dans la requête,

toutes ses occurrences suivantes sont ignorées. Par exemple, si un paramètre existe à la fois dans la requête URL et dans le corps POST, seul celui de la requête URL est pris en compte.

Si vous décidez d'utiliser les paramètres d'accès et d'invalidation pour un groupe de contenus, configurez les paramètres lorsque vous configurez le groupe de contenus.

Remarque : Citrix vous recommande d'utiliser des sélecteurs plutôt que des groupes de contenu paramétrés, car les sélecteurs sont plus flexibles et peuvent être adaptés à un plus grand nombre de types de données.

Configurer un sélecteur

Un groupe de contenu peut utiliser un sélecteur d'accès pour récupérer les accès au cache ou utiliser un sélecteur d'invalidation pour les objets mis en cache expirés et en extraire de nouveaux depuis le serveur d'origine.

Un sélecteur contient un nom et une expression logique, appelée *expression avancée*.

Pour plus d'informations sur les expressions avancées, voir Stratégies et expressions.

Pour configurer un sélecteur, vous lui attribuez un nom et entrez une ou plusieurs expressions. Une expression de sélecteur devrait inclure le tronc d'URL et l'hôte, à moins qu'il n'y ait une raison valable de les omettre.

Pour configurer un sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add cache selector \<selectorName\> ( \<rule\> ... )
```

Pour plus d'informations sur la configuration de l'expression ou des expressions, reportez-vous à la section Pour configurer une expression de sélecteur à l'aide de l'interface de ligne de commande.

```
1 >add cache selector product_selector "http.req.url.query.value("
     ProductId")" "http.req.url.query.value("BatchNum")" "http.req.url.
     query.value("depotLocation")"
2
3 > add cache selector batch_selector "http.req.url.query.value("
     ProductId")" "http.req.url.query.value("BatchId")" "http.req.url.
     query.value("depotLocation")"
4
5 > add cache selector product_id_selector "http.req.url.query.value("
     ProductId")"
6
7 > add cache selector batchnum_selector "http.req.url.query.value("
     BatchNum")" "http.req.url.query.value("depotLocation")"
8
```



```
> add cache selector batchid_selector "http.req.url.query.value("
    depotLocation")" "http.req.url.query.value("BatchId")"

<!--NeedCopy-->
```

Pour configurer un sélecteur à l'aide de l'interface graphique

Accédez à **Optimisation > Mise en cache intégrée > Sélecteurs**de cache et ajoutez le sélecteur de cache.

Groupes de contenu

Un groupe de contenu est un conteneur pour les objets mis en cache qui peuvent être servis dans une réponse. Lorsque vous activez le cache intégré pour la première fois, les objets pouvant être mis en cache sont stockés dans un groupe de contenu nommé Par défaut. Vous pouvez créer des groupes de contenu possédant des propriétés uniques. Par exemple, vous pouvez définir des groupes de contenu distincts pour les données d'image, les rapports de bogue et les cotations boursières, et vous pouvez configurer le groupe de contenu de cotation de stock pour qu'il soit actualisé plus souvent que les autres groupes.

Vous pouvez configurer l'expiration d'un groupe de contenu entier ou d'entrées sélectionnées dans un groupe de contenu.

Les données d'un groupe de contenu peuvent être statiques ou dynamiques, comme suit :

- **Groupes de contenu statiques**. Trouve une correspondance exacte entre la tige d'URL et le nom d'hôte sur la demande et la tige d'URL et le nom d'hôte de la réponse.
- **Groupes de contenu dynamiques**. recherche les objets qui contiennent des paires paramètre-valeur, des chaînes arbitraires ou des modèles de chaîne spécifiques. Les groupes de contenus dynamiques sont utiles lors de la mise en cache de données fréquemment mises à jour (par exemple, un rapport de bogue ou un devis boursier).

Servir une requête d'un groupe de contenu

1. Un utilisateur saisit des critères de recherche pour un élément, tel qu'un rapport de bogue, et clique sur le bouton Rechercher dans un formulaire HTML.
2. Le navigateur émet une ou plusieurs requêtes HTTP GET. Ces requêtes contiennent des paramètres (par exemple, le propriétaire du bogue, l'ID du bogue, etc.).
3. Lorsque l'appliance Citrix ADC reçoit les demandes, il recherche une stratégie correspondante et, s'il trouve une stratégie de mise en cache qui correspond à ces demandes, il dirige les demandes vers un groupe de contenus.
4. Le groupe de contenu recherche les objets appropriés dans le groupe de contenu, en fonction des critères que vous configurez dans un sélecteur.

Par exemple, le groupe de contenu peut récupérer des réponses qui correspondent `NameField=username and BugID=ID`.

1. S'il trouve des objets correspondants, l'appliance Citrix ADC peut les servir dans le navigateur de l'utilisateur, où ils sont assemblés en réponse complète (par exemple, un rapport de bogue).

Invalidation d'un objet dans un groupe de contenus

1. Un utilisateur modifie les données (par exemple, l'utilisateur modifie le rapport de bogue et clique sur le bouton Soumettre).
2. Le navigateur envoie ces données sous la forme d'une ou plusieurs requêtes HTTP. Par exemple, il peut envoyer un rapport de bogue sous la forme de plusieurs requêtes HTTP POST qui contiennent des informations sur le propriétaire et l'ID de bogue.
3. L'appliance Citrix ADC correspond aux demandes par rapport aux stratégies d'invalidation. Généralement, ces stratégies sont configurées pour détecter la méthode HTTP POST.
4. Si la demande correspond à une stratégie d'invalidation, l'appliance Citrix ADC recherche le groupe de contenus associé à cette stratégie et expire les réponses qui correspondent aux critères configurés pour l'invalidation.

Par exemple, un sélecteur d'invalidation peut trouver des réponses qui correspondent `NameField=username and BugID=ID`.

1. La prochaine fois que l'appliance Citrix ADC reçoit une requête GET pour ces réponses, elle récupère les versions actualisées du serveur d'origine, met en cache les réponses actualisées et envoie ces réponses au navigateur de l'utilisateur, où elles sont assemblées dans un rapport de bogue complet.

Configurer un groupe de contenus de base

Par défaut, toutes les données mises en cache sont stockées dans le groupe de contenus par défaut. Vous pouvez configurer plus de groupes de contenu et spécifier ces groupes de contenu dans une ou plusieurs stratégies.

Vous pouvez configurer des groupes de contenu pour le contenu statique et vous devez configurer des groupes de contenu pour le contenu dynamique. Vous pouvez modifier la configuration de n'importe quel groupe de contenu, y compris le groupe par défaut.

Pour configurer un groupe de contenus de base à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add cache contentgroup <name> (-hitSelector <hitSelectorName> -invalSelector
 <invalidationSelectorName> | -hitParams <hitParamName> -invalParams<
invalidationParamName>)-type <type> [-relExpiry <sec> | -relExpiryMilliSec
<msec>] [-heurExpiryParam <positiveInteger>]
```



```
add cache contentgroup Products_Details -hitSelector product_selector -
invalSelector id_selector

add cache contentgroup bugrep -hitParams IssuePage RecordID Template
TableId -invalParams RecordID -relExpiry 864000
```

Pour configurer un groupe de contenus de base à l'aide de l'interface graphique

Accédez à **Optimisation > Mise en cache intégrée > Groupes de contenu**et créez le groupe de contenu.

Expiration ou vidage des objets mis en cache

Si une réponse n'a pas d'en-tête Expires ou d'en-tête Cache-Control avec un délai d'expiration (Max-Age ou Smax-Age), vous devez expirer les objets d'un groupe de contenu à l'aide de l'une des méthodes suivantes :

- Configurez les paramètres d'expiration du groupe de contenu pour déterminer si l'objet doit être conservé et combien de temps.
- Configurez une stratégie d'invalidation et une action pour le groupe de contenus. Pour plus d'informations, voir Configuration des stratégies pour la mise en cache et l'invalidation.
- Expire manuellement le groupe de contenu ou les objets qu'il contient.

Après l'expiration d'une réponse mise en cache, l'appliance Citrix ADC l'actualise la prochaine fois que le client émet une demande de réponse. Par défaut, lorsque le cache est plein, l'appliance Citrix ADC remplace en premier la réponse la moins récente utilisée.

La liste suivante décrit les méthodes d'expiration des réponses mises en cache à l'aide des paramètres d'un groupe de contenus. Généralement, ces méthodes sont spécifiées sous forme de pourcentage ou en secondes :

- **Manuel**. Invalidez manuellement toutes les réponses d'un groupe de contenu ou toutes les réponses du cache.
- **Basé sur la réponse**. Intervalles d'expiration spécifiques pour les réponses positives et négatives. L'expiration basée sur la réponse n'est prise en compte que si l'en-tête Last Modified est manquant dans la réponse.
- **Expiration heuristique**. Pour les réponses qui ont un en-tête Dernière modification, l'expiration heuristique spécifie le montage du temps pris à partir du moment où la réponse a été modifiée (calculée comme l'heure actuelle moins l'heure de dernière modification, multipliée par la valeur d'expiration heuristique). Par exemple, si un en-tête Last Modified indique qu'une réponse a été mise à jour il y a 2 heures et que le paramètre d'expiration heuristique est de 10%, les objets mis en cache expirent après 0,2 heure. Cette méthode suppose que les réponses fréquemment mises à jour doivent expirer plus souvent.

- **Absolu ou relatif**. Spécifiez une heure exacte (absolue) à laquelle la réponse expire tous les jours, au format HH:MM, heure locale ou GMT. L'heure locale peut ne pas fonctionner dans tous les fuseaux horaires.

L'expiration relative spécifie quelques secondes ou millisecondes entre le moment où un échec du cache provoque un déplacement vers le serveur d'origine jusqu'à l'expiration de la réponse. Si vous spécifiez l'expiration relative en millisecondes, entrez un multiple de 10. Cette forme d'expiration fonctionne pour toutes les réponses positives. Les en-têtes Last Modified, Expires et Cache-Control de la réponse sont ignorés.

L'expiration absolue et relative remplace toute information d'expiration dans la réponse elle-même.

- **En téléchargement**. L'option Expirer après avoir terminé la réponse reçue expire une réponse lorsqu'elle est téléchargée. Ceci est utile pour les réponses fréquemment mises à jour, par exemple les cotations boursières. Par défaut, cette option est désactivée.

L'activation du cache Flash et de l'expiration après réception de la réponse complète accélère les performances des applications dynamiques. Lorsque vous activez les deux options, l'appliance Citrix ADC récupère une seule réponse pour un bloc de requêtes simultanées.

- **Épinglé**. Par défaut, lorsque le cache est plein, l'appliance Citrix ADC remplace en premier la réponse la moins récente utilisée. L'appliance Citrix ADC n'applique pas ce comportement aux groupes de contenu marqués comme épinglés.

Si vous ne configurez pas les paramètres d'expiration pour un groupe de contenu, les options suivantes sont supplémentaires pour les objets expirant dans le groupe :

- Configurez une stratégie avec une action INVAL qui s'applique au groupe de contenus.
- Entrez les noms des groupes de contenu lors de la configuration d'une stratégie qui utilise une action INVAL.

Comment les méthodes d'expiration sont appliquées

L'expiration fonctionne différemment pour les réponses positives et négatives. Les réponses positives et négatives sont décrites dans le tableau *Expiration des réponses positives et négatives* mentionné ci-dessous.

Voici des règles générales permettant de comprendre la méthode d'expiration appliquée à un groupe de contenus :

- Vous pouvez contrôler si l'appliance Citrix ADC évalue les en-têtes de réponse lorsque vous décidez d'expirer un objet.
- L'expiration absolue et relative entraîne l'application Citrix ADC à ignorer les en-têtes de réponse (ils remplacent toutes les informations d'expiration de la réponse).

- Les paramètres d'expiration heuristiques et l'expiration « faible positif » et « faible négatif » (libellés comme valeurs **par défaut** dans l'utilitaire de configuration) entraînent l'examen des en-têtes de réponse par l'appliance Citrix ADC. Ces paramètres fonctionnent ensemble comme suit :
  - La valeur d'un en-tête Expires ou Cache-Control remplace ces paramètres de groupe de contenu.
  - Pour les réponses positives qui n'ont pas d'en-tête Expires ou Cache-Control mais qui ont un en-tête Last Modified, l'appliance Citrix ADC compare les paramètres d'expiration heuristiques avec la valeur d'en-tête.
  - Pour les réponses positives qui n'ont pas d'en-tête Expire, Cache-Control ou Last Modified, l'appliance Citrix ADC utilise la valeur « faible positif ».
  - Pour les réponses négatives qui n'ont pas d'en-tête Expire ou Cache-Control, l'appliance Citrix ADC utilise la valeur « faible négatif ».

Le tableau suivant décrit comment ces méthodes sont appliquées.

Type de réponse	Type d'en-tête d'expiration	Paramètre du groupe de contenus	Période où l'objet reste dans le cache
Positif	N'importe quel en-tête	Expiration du contenu après (relExpiry) sans autres paramètres	Utilisez la valeur du paramètre **Expirer le contenu après**.
Positif	N'importe quel en-tête	Expirer le contenu à (absExpiry) sans autre paramètre	Soustrayez la date actuelle de la valeur du paramètre **Expirer le contenu à**.
Positif	N'importe quel en-tête	Expiration du contenu après (relExpiry) et expiration du contenu à (absExpiry)	Utilisez la plus petite des deux valeurs pour les paramètres du groupe de contenu. Voir les lignes précédentes de ce tableau.

Type de réponse	Type d'en-tête d'expiration	Paramètre du groupe de contenus	Période où l'objet reste dans le cache
Positif	Last-Modified (avec d'autres en-têtes)	Heuristique (heurExpiry Param) avec n'importe quel autre paramètre	Soustrayez la date de dernière modification de la date actuelle, multipliez le résultat par la valeur du paramètre d'expiration heuristique, puis divisez par 100.
Positif	Last-Modified (avec d'autres en-têtes)	Par défaut (positif) (Expiration Weakposrel) et aucun autre paramètre	Utilisez la valeur du paramètre d'expiration par défaut (positif).
Positif	Expire ou Cache-Control : l'en-tête Max-Age est présent	L'en-tête Dernière modification est absent, Heuristique (HeurexPiry Param), Default (positif) (WeakPoSrel Expiration), ou les deux	Soustrayez la date actuelle de la date d'expiration ou de la `Cache-Control: Max-Age` date.
Positif	aucun en-tête de mise en cache	Par défaut (positif) (Weakposrel Expiration) et tout autre paramètre d'expiration	Utilisez la valeur du paramètre Par défaut (positif).

Type de réponse	Type d'en-tête d'expiration	Paramètre du groupe de contenus	Période où l'objet reste dans le cache
Positif	aucun en-tête de mise en cache	Heuristique (HeurexPiry Param) est présent, le paramètre Par défaut (positif) (WeakPoSrel Expiration) est absent.	Si l'en-tête Last Modified est absent, la réponse n'est pas mise en cache ou elle est mise en cache avec l'état Déjà expiré. Si l'en-tête Last Modified est présent, utilisez la valeur d'expiration heuristique.
Négatif	Expire ou `Cache-Control:Max-Age`	Expiration du contenu après (relExpiry), Expiration du contenu à (absExpiry) ou les deux paramètres	Soustrayez la date actuelle de la valeur de l'en-tête Expires ou utilisez la valeur de l'en-tête Cache-Control:Max-Age.
Négatif	Expire ou les en-têtes Cache-Control sont absents	Expiration du contenu après (relExpiry), Expiration du contenu à (absExpiry) ou les deux paramètres	La réponse n'est pas mise en cache ou est mise en cache avec l'état Déjà expiré.
Négatif	Expire ou `Cache-Control:Max-Age`	N'importe quel paramètre	Soustrayez la date actuelle de la date d'expiration ou de `Cache-Control:Max-Age` la date.
Négatif	Expire et Cache-Control:Les en-têtes Max-Age sont absents	Par défaut (négatif) (Expiration weakNegRel)	Utilisez la valeur du paramètre Par défaut (négatif).
Négatif	Expire et Cache-Control:Les en-têtes Max-Age sont absents	Tout paramètre autre que Default (négatif) (weakNegRel Expiration)	L'objet n'est pas mis en cache ou est mis en cache avec l'état Déjà expiré.

Expirer un groupe de contenus par méthode manuelle

Vous pouvez expirer manuellement toutes les entrées d'un groupe de contenu.

Pour expirer manuellement toutes les réponses d'un groupe de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
expire cache contentGroup <name>
```

Pour expirer manuellement toutes les réponses d'un groupe de contenu à l'aide de l'interface graphique

Accédez à **Optimisation > Mise en cache intégrée > Groupes**de contenu, sélectionnez le groupe de contenu, puis cliquez sur Invalider pour expirer toutes les réponses d'un groupe de contenu.

Pour expirer manuellement toutes les réponses dans le cache à l'aide de l'interface graphique

Accédez à **Optimisation > Mise en cache intégrée > Groupes de contenu**, puis cliquez sur Invalider tout pour expirer toutes les réponses dans le cache.

Configurer l'expiration périodique d'un groupe de contenus

Vous pouvez configurer un groupe de contenus de sorte qu'il effectue une expiration sélective ou complète de ses entrées. L'intervalle d'expiration peut être fixe ou relatif.

Pour configurer l'expiration du groupe de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cache contentgroup \<name> (-relExpiry|-relExpiryMilliSec|-absExpiry
|-absExpiryGMT| -heurExpiryParam|-weakPosRelExpiry|-weakNegRelExpiry| -
expireAtLastBye)\<expirationValue>
```

Pour configurer l'expiration du groupe de contenu à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu**, sélectionnez le groupe de contenu et spécifiez la méthode d'expiration.

Expiration des réponses individuelles

L'expiration d'une réponse oblige l'appliance Citrix ADC à récupérer une copie actualisée à partir du serveur d'origine. Les réponses qui n'ont pas de validateurs, par exemple, `ETag` ou d'en-têtes Dernière modification, ne peuvent pas être revalidées. Par conséquent, le rinçage de ces réponses a le même effet que leur expiration.

Pour expirer une réponse mise en cache dans un groupe de contenu pour les données statiques, vous pouvez spécifier une URL qui doit correspondre à l'URL stockée. Si la réponse mise en cache fait partie

d'un groupe de contenu paramétré, vous devez spécifier le nom du groupe et la tige d'URL exacte. Le nom d'hôte et le numéro de port doivent être les mêmes que dans l'en-tête de requête HTTP hôte de la réponse mise en cache. Si le port n'est pas spécifié, le port 80 est supposé.

Pour expirer des réponses individuelles dans un groupe de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
expire cache object -url <URL> -host <hostName> [-port <port>] [-groupName<
contentGroupName>] [-httpMethod GET|POST]
```

Pour expirer des réponses individuelles dans un groupe de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
expire cache object -locator <positiveInteger>
```

Pour expirer une réponse mise en cache à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Objets mis en cache**, sélectionnez la réponse mise en cache et expirez.

Pour expirer une réponse à l'aide de l'interface graphique

Accédez à **Optimisation** > Mise en **cache intégrée** > **Objets mis en cache**, cliquez sur **Rechercher** et définissez les critères de recherche pour rechercher la réponse mise en cache requise et expirer.

Vidage des réponses dans un groupe de contenus

Vous pouvez supprimer ou vider toutes les réponses d'un groupe de contenu, certaines réponses d'un groupe ou toutes les réponses du cache. Le vidange d'une réponse mise en cache libère de la mémoire pour les nouvelles réponses mises en cache.

> **Remarque :**
>
> Pour vider les réponses pour plusieurs objets à la fois, utilisez la méthode de l'utilitaire de configuration. L'interface de ligne de commande n'offre pas cette option.

Pour vider les réponses d'un groupe de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
flush cache contentGroup <name> [-query <queryString> | [-selectorValue <
selectorExpressionIDList> -host <hostName>]]
```

Pour vider les réponses d'un groupe de contenu à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu**.

2. Dans le volet d'informations, videz les réponses comme suit :
    - Pour vider toutes les réponses de tous les groupes de contenu, cliquez sur Invalider tout, puis vider toutes les réponses.
    - Pour vider les réponses d'un groupe de contenu particulier, sélectionnez le groupe de contenu, cliquez sur **Invalider**, puis vider toutes les réponses.

> **Remarque** :
> Si ce groupe de contenu utilise un sélecteur, vous pouvez vider sélectivement les réponses en entrant une chaîne dans la zone de texte Valeur du sélecteur, en entrant un nom d'hôte dans la zone de texte Hôte. Cliquez ensuite sur **Vider et OK**. La valeur Selector peut être une chaîne de requête pouvant contenir jusqu'à 2319 caractères utilisée pour l'invalidation paramétrée.

Si le groupe de contenus utilise un paramètre d'invalidation, vous pouvez vider les réponses de manière sélective en saisissant une chaîne dans le champ **Requête**.

Si le groupe de contenu utilise un paramètre d'invalidation et que Invalidate objets appartenant à l'hôte cible est configuré, entrez des chaînes dans les champs **Requête et Hôte**.

Pour vider une réponse mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
flush cache object -locator <positiveInteger> | -url <URL> -host <hostName>
 [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET|POST]
```

Pour vider une réponse mise en cache à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Objets mis en cache**, sélectionnez l'objet mis en cache et vider.

Suppression d'un groupe de contenus

Vous pouvez supprimer un groupe de contenus s'il n'est pas utilisé par une stratégie qui stocke les réponses dans le cache. Si le groupe de contenus est lié à une stratégie, vous devez d'abord la supprimer. La suppression du groupe de contenus supprime toutes les réponses stockées dans ce groupe.

Vous ne pouvez pas supprimer le groupe Default, BASEFILE ou Deltas. Le groupe par défaut stocke les réponses mises en cache qui n'appartiennent à aucun autre groupe de contenu.

Pour supprimer un groupe de contenus à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm cache contentgroup <name>
```

Pour supprimer un groupe de contenus à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu,** sélectionnez le groupe de contenu et supprimez.

Configurer les stratégies de mise en cache et d'invalidation

August 20, 2021

Les stratégies permettent au cache intégré de déterminer s'il faut essayer de servir une réponse à partir du cache ou de l'origine. L'appliance NetScaler fournit des stratégies intégrées pour la mise en cache intégrée et vous pouvez configurer d'autres stratégies. Lorsque vous configurez une stratégie, vous l'associez à une action. Une action met en cache les objets auxquels la stratégie s'applique ou invalide (expire) les objets. Généralement, vous basez les stratégies de mise en cache sur les informations dans les requêtes GET et POST. Vous basez généralement les stratégies d'invalidation sur la présence de la méthode POST dans les requêtes, ainsi que sur d'autres informations. Vous pouvez utiliser toutes les informations d'une requête GET ou POST dans une stratégie de mise en cache ou d'invalidation.

Vous pouvez afficher certaines des stratégies intégrées dans le nœud Stratégies du cache intégré dans l'utilitaire de configuration. Les noms de stratégie intégrés commencent par un trait de soulignement (_).

Les actions déterminent ce que fait l'appliance NetScaler lorsque le trafic correspond à une stratégie. Les actions suivantes sont disponibles :

- **Actions de mise en cache**. Les stratégies que vous associez à l'action CACHE stockent les réponses dans le cache et les servent à partir du cache.
- **Actions d'invalidation**. Les stratégies que vous associez à l'action INVAL expirent immédiatement les réponses mises en cache et les actualisent à partir du serveur d'origine. Pour les applications Web, les stratégies d'invalidation évaluent souvent les requêtes POST.
- **Actions « Ne pas mettre en cache »**. Les stratégies que vous associez à une action NOCACHE ne stockent jamais d'objets dans le cache.
- **Actions de mise en cache provisoire**. Les stratégies que vous associez à une action MAYCACHE ou MAYNOCACHE dépendent du résultat de plusieurs évaluations de stratégies.

Bien que le cache intégré ne stocke pas les objets spécifiés par la méthode LOCK, vous pouvez invalider les objets mis en cache à la réception d'une `LOCK` demande. Pour les stratégies d'invalidation uniquement, vous pouvez spécifier `LOCK` en tant que méthode à l'aide de l'expression `http.req.method.eq( "lock" )`. Contrairement aux stratégies `GET` et aux `POST` requêtes, vous devez mettre la méthode LOCK entre guillemets car l'appliance NetScaler reconnaît ce nom de méthode comme une chaîne uniquement.

Après avoir créé une stratégie, vous la liez à un point particulier dans le traitement global des demandes et des réponses. Bien que vous créez une stratégie avant de la lier, vous devez comprendre comment les points de liaison affectent l'ordre de traitement avant de créer vos stratégies.

Les polices liées à un point de liaison particulier constituent une banque de polices. Vous pouvez

utiliser des expressions goto pour modifier l'ordre d'exécution dans une banque de stratégies. Vous pouvez également invoquer des stratégies dans d'autres banques de stratégies. En outre, vous pouvez créer des étiquettes et y lier des stratégies. Une telle étiquette n'est pas associée à un point de traitement, mais les stratégies qui y sont liées peuvent être invoquées à partir d'autres banques de polices.

Actions à associer aux stratégies de mise en cache intégrées

Le tableau suivant décrit les actions pour les stratégies de mise en cache intégrées.

Action	Spécifications
CACHE	Sert une réponse du cache si la réponse n'a pas expiré. Si la réponse doit être récupérée à partir du serveur d'origine, l'appliance NetScaler met en cache la réponse avant de la servir. Même les données mises à jour et consultées fréquemment peuvent être mises en cache. Par exemple, les cotations boursières sont mises à jour fréquemment, mais elles peuvent être mises en cache afin qu'elles puissent être utilisées rapidement à plusieurs utilisateurs. Si nécessaire, les données mises en cache peuvent être actualisées immédiatement après leur téléchargement. Une action CACHE peut être remplacée par des stratégies intégrées.
NOCACHE	Récupère toujours la réponse du serveur d'origine et marque la réponse comme non stockable. Vous configurez généralement les stratégies NOCACHE pour les données sensibles ou personnalisées.

Action	Spécifications
MAY_CACHE	Utilisé dans une stratégie de temps de demande, ce paramètre permet provisoirement de stocker une réponse dans un groupe de contenus, en attendant l'évaluation des stratégies de temps de réponse. Les éléments suivants sont possibles : 1. Si une stratégie de temps de réponse correspondante comporte une action CACHE mais ne spécifie pas de groupe de contenu, la réponse est stockée dans le groupe Par défaut, sauf si les stratégies intégrées remplacent cette stratégie. 2. Si une stratégie de temps de réponse correspondante comporte une action CACHE et spécifie le même groupe de contenu que celui de la stratégie de temps de requête, la réponse est stockée dans le groupe de contenu nommé, sauf si les stratégies intégrées remplacent cette stratégie. 3. Si une stratégie de temps de réponse correspondante comporte une action CACHE mais spécifie un groupe de contenu différent de celui de la stratégie de temps de requête, une action NOCACHE est appliquée. 4. Si une stratégie de temps de réponse correspondante comporte une action NOCACHE, exécutez une action NOCACHE. 5. S'il n'y a pas de stratégie de temps de réponse correspondante, une action CACHE est appliquée, sauf si une stratégie intégrée remplace cette stratégie.

Action	Spécifications
MAY_NOCACHE	Pour une stratégie de temps de requête, ce paramètre empêche provisoirement la mise en cache de la réponse. Au moment de la réponse, l'une des actions suivantes est prise Si aucune stratégie de temps de réponse ne correspond à la demande, l'action finale est NOCACHE. - Si une stratégie de temps de réponse correspondante contient une action CACHE, l'action finale est CACHE, sauf si les stratégies intégrées remplacent cette stratégie. - Si une stratégie de temps de réponse correspondante contient une action NOCACHE, l'action finale est NOCACHE. - Si une stratégie de temps de réponse correspondante comporte une action CACHE mais ne spécifie pas de groupe de contenu, l'action finale consiste à mettre en cache la réponse dans le groupe de contenu par défaut, sauf si les stratégies intégrées remplacent cette stratégie.
INVAL	Expire les réponses mises en cache. Selon la configuration de la stratégie et du groupe de contenu, toutes les réponses d'un ou de plusieurs groupes de contenu ont expiré ou les objets sélectionnés dans le groupe de contenu ont expiré. Remarque : Vous ne pouvez spécifier des actions INVAL que dans les stratégies de temps de demande.

Liez des points pour une stratégie

Vous pouvez lier la stratégie à l'un des points de liaison suivants :

- **Une banque de politiques mondiales**. Il s'agit des banques de stratégies par défaut, de remplacement de l'heure de demande, de temps de réponse par défaut et de remplacement du temps de réponse, comme décrit dans « Ordre d'évaluation des stratégies ». «
- **Un serveur virtuel**. Les stratégies que vous liez à un serveur virtuel sont traitées après les stratégies globales de remplacement et avant les stratégies globales par défaut, comme décrit dans

« Ordre d'évaluation des stratégies ». « Lorsque vous liez une stratégie à un serveur virtuel, vous la liez au traitement de la demande ou du temps de réponse.

- **Une étiquette de stratégie ad hoc**. Une étiquette de stratégie est un nom attribué à une banque de stratégies. Outre les étiquettes globales, le cache intégré comporte deux étiquettes de stratégie personnalisées intégrées :
  - _reqBuiltinDefaults. Cette étiquette de stratégie, par défaut, est appelée à partir de la banque de stratégies par défaut au moment de la requête.
  - _resBuiltinDefaults. Cette étiquette de stratégie, par défaut, est appelée à partir de la banque de stratégies par défaut de temps de réponse.

Vous pouvez également définir de nouvelles étiquettes de stratégie. Les stratégies liées à une étiquette de stratégie définie par l'utilisateur doivent être appelées à partir d'une banque de stratégies pour l'un des points de liaison intégrés.

> **Important :**
> Vous devez lier une stratégie avec une action INVAL à un point de liaison de remplacement au moment de la demande ou à un point de liaison de remplacement de temps de réponse. Pour supprimer une stratégie, vous devez d'abord la dissocier.

Ordre d'évaluation des stratégies

Pour qu'une stratégie avancée prenne effet, vous devez vous assurer qu'elle est appelée à un moment donné pendant le traitement du trafic par l'appliance NetScaler. Pour spécifier l'heure d'invocation, vous associez la stratégie à un point de liaison. Voici les points de liaison, énumérés par ordre d'évaluation :

- **Remplacer l'heure de la demande**. Si une demande correspond à une stratégie de remplacement au moment de la demande, l'évaluation de la stratégie de demande se termine par défaut et l'appliance NetScaler stocke l'action associée à la stratégie correspondante.
- **Serveur virtuel d'équilibrage de charge au moment de la demande**. Si l'évaluation des stratégies ne peut pas être effectuée après l'évaluation de toutes les stratégies de remplacement au moment de la demande, l'appliance NetScaler traite les stratégies au moment de la demande qui sont liées à l'équilibrage de la charge des serveurs virtuels. Si la demande correspond à l'une de ces stratégies, l'évaluation se termine et l'appliance NetScaler stocke l'action associée à la stratégie correspondante.
- **Serveur virtuel de commutation de contenu au moment de la demande**. Les stratégies liées à ce point de liaison sont évaluées après les stratégies de demande liées à l'équilibrage de charge des serveurs virtuels.
- **Heure de demande par défaut**. Si l'évaluation de la stratégie ne peut pas être effectuée après l'évaluation de toutes les stratégies spécifiques au serveur virtuel à l'heure de la demande, l'appliance NetScaler traite les stratégies par défaut au moment de la demande. Si la demande

correspond à une stratégie par défaut au moment de la demande, l'évaluation de la stratégie de délai de demande se termine par défaut et l'appliance NetScaler stocke l'action associée à la stratégie correspondante.

- **Remplacer le temps de réponse**. Similaire à l'évaluation de la stratégie de remplacement au moment de la demande.
- **Serveur virtuel d'équilibrage de charge en temps de réponse**. Similaire à l'évaluation de stratégie de serveur virtuel au moment de la demande.
- **Serveur virtuel de commutation de contenu en temps de réponse**. Similaire à l'évaluation de stratégie de serveur virtuel au moment de la demande.
- **Temps de réponse par défaut**. Similaire à l'évaluation de stratégie par défaut au moment de la requête.

Vous pouvez associer plusieurs stratégies à chaque point de liaison. Pour contrôler l'ordre d'évaluation des stratégies associées au point de liaison, configurez un niveau de priorité. En l'absence de toute autre information sur le contrôle des flux, les stratégies sont évaluées en fonction du niveau de priorité, en commençant par la valeur de priorité numérique la plus faible.

> **Remarque :**
> les politiques de temps de demande pour les données POST ou les en-têtes de cookie doivent être invoquées lors de l'évaluation du remplacement du moment de la demande, car les stratégies de temps de demande intégrées dans le cache intégré renvoient une `NOCACHE` action pour les demandes POST et une `MAY_NOCACHE` action pour les demandes contenant des cookies. Vous devez associer `MAY_CACHE` ou `MAY_NOCACHE` effectuer des actions à une stratégie de temps de demande pointant vers un groupe de contenu paramétré. La stratégie de temps de réponse détermine si la transaction est stockée dans le cache.

Configurer une stratégie de mise en cache intégrée

Vous configurez de nouvelles stratégies pour gérer les données que les stratégies intégrées ne peuvent pas traiter. Vous configurez des stratégies distinctes pour la mise en cache, la prévention de la mise en cache et l'invalidation des données mises en cache. Voici les principaux composants d'une stratégie pour la mise en cache intégrée :

- Règle : expression logique qui évalue une requête ou une réponse HTTP.
- Action : Vous associez une stratégie à une action pour déterminer ce qu'il faut faire avec une demande ou une réponse correspondant à la règle de stratégie.

Groupes de contenu : vous associez la stratégie à un ou plusieurs groupes de contenu pour identifier où l'action doit être effectuée.

Pour configurer une stratégie de mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
add cache policy <policyName> -rule <expression> -actionCACHE|MAY_CACHE
|NOCACHE|MAY_NOCACHE [-storeInGroup <contentGroupName>] [-undefAction
NOCACHE|RESET]
> add cache policy image_cache -rule "http.req.url.contains(\"jpg\")|| http
.req.url.contains(\"jpeg\")"-action CACHE -storeingroup myImages_group -
undefaction NOCACHE

> add cache policy bugReportPolicy -rule "http.req.url.query.contains(\"
IssuePage\")"-action CACHE -storeInGroup bugReportGroup

> add cache policy my_form_policy -rule "http.req.header(\"Host\")contains
(\"my.company.com\")&& http.req.method.eq(\"GET\")&& http.req.url.query.
contains(\"v=7\")"-action CACHE -storeInGroup my_form_event

> add cache policy viewproducts_policy -rule "http.req.url.contains(\"
viewproducts.aspx\")"-action CACHE -storeInGroup Product_Details
```

Pour configurer une stratégie pour invalidation à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add cache policy <policyName> -rule <expression> -action INVAL [-
    invalObjects "<contentGroupName1>[,<selectorName1>"]. . .]] | [-
    invalGroup <contentGroupName1>[, <contentGroupName2>. . .]] [-
    undefAction NOCACHE|RESET]
<!--NeedCopy-->
```

```
> add cache policy invalidation_events_policy -rule "http.req.header("
    Host")contains("my.company.com") && http.req.method.eq("GET") &&
    http.req.url.query.contains("v=8") -action INVAL -invalObjects
    my_form_event -undefaction NOCACHE
<!--NeedCopy-->
```

```
> add cache policy inval_all -rule "http.req.method.eq("POST") && http.
    req.url.contains("jpeg")" -action INVAL -invalGroups myImages_group
    myApps_group PDF_group
<!--NeedCopy-->
```

```
> add cache policy bugReportInvalidationPolicy -rule "http.req.url.
    query.contains("TransitionForm")" -action INVAL -invalObjects
    bugReport`
`> add cache policy editproducts_policy  - rule "http.req.url.contains("
    editproducts.aspx")"  - action INVAL -invalObjects "Product_Details,
    batchnum_sel" "Products_In_Depots,batchid_sel"
<!--NeedCopy-->
```


Pour configurer une stratégie de mise en cache ou d'invalidation à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Stratégies**, puis créez la nouvelle stratégie.

Liaison globale d'une stratégie de mise en cache intégrée

Lorsque vous liez globalement une stratégie, elle est disponible pour tous les serveurs virtuels de l'appliance NetScaler.

Pour lier une stratégie de mise en cache intégrée globalement à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
bind cache global <policy> -priority <positiveInteger> [-
    typeREQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT] [-
    gotoPriorityExpression <expression>] [-invoke <labelType> <labelName
    >]
<!--NeedCopy-->
```

```
> bind cache global myCachePolicy -priority 100 -type req_default
<!--NeedCopy-->
```

> **Remarque :**
>
> L'argument type est facultatif pour les stratégies liées globalement, afin de maintenir une compatibilité descendante avec les stratégies que vous avez définies à l'aide de versions antérieures de l'appliance NetScaler. Si vous omettez le type, la stratégie est liée à REQ_DEFAULT ou RES_DEFAULT, selon que la règle de stratégie est une expression de temps de réponse ou de temps de demande. Si la règle contient à la fois des paramètres de temps de requête et de temps de réponse, elle est liée à RES_DEFAULT. Voici un exemple d'une liaison qui omet le type

Voici un exemple d'une liaison qui omet le type.

```
> bind cache global myCache Policy 200
```

Pour lier globalement une stratégie de mise en cache intégrée à l'aide de l'utilitaire de configuration

Accédez à **Optimisation** > **Mise en cache intégrée, cliquez sur Gestionnaire de stratégies** de cache et liez les stratégies en spécifiant le point de liaison et le type de connexion appropriés (Request/Réponse).

Liez une stratégie de mise en cache intégrée à un serveur virtuel

Lorsque vous liez une stratégie à un serveur virtuel, elle est disponible uniquement pour les demandes et réponses qui correspondent à la stratégie et qui passent par le serveur virtuel concerné.

Lorsque vous utilisez l'interface graphique, vous pouvez lier la stratégie à l'aide de la boîte de dialogue de configuration du serveur virtuel. Cela vous permet d'afficher toutes les stratégies de tous les modules Citrix ADC liés à ce serveur virtuel. Vous pouvez également utiliser la boîte de dialogue de **configuration de Policy Manager** pour le cache intégré. Cela vous permet d'afficher uniquement les stratégies de mise en cache intégrées qui sont liées au serveur virtuel.

Pour lier une stratégie de mise en cache intégrée à un serveur virtuel à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
bind lb vserver <name>@ -policyName <policyName> -priority <
    positiveInteger> -type(REQUEST|RESPONSE)
<!--NeedCopy-->
```

```
bind cs vserver <name>@ -policyName <policyName> -priority <
    positiveInteger> -type(REQUEST|RESPONSE)
<!--NeedCopy-->
```

Pour lier une stratégie de mise en cache intégrée à un serveur virtuel à l'aide de l'utilitaire de configuration (méthode du serveur virtuel)

- CS Virtual Server - Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez le serveur virtuel et liez les stratégies de cache pertinentes.
- LB Virtual Server - Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, sélectionnez le serveur virtuel et liez les stratégies de cache pertinentes.

Pour lier une stratégie de mise en cache intégrée à un serveur virtuel à l'aide de l'interface graphique (méthode Policy Manager).

Accédez à **Optimisation** > **Mise en cache intégrée, cliquez sur Gestionnaire de stratégies** de cache et liez les stratégies de cache en spécifiant le point de liaison et le type de connexion appropriés.

> **Remarque :**
> Vous pouvez lier des stratégies de cache à la fois au serveur virtuel d'équilibrage de charge et au serveur virtuel de commutation de contenu en sélectionnant le point de liaison approprié.

Comment mettre en cache les versions compressées et non compressées d'un fichier

Par défaut, un client capable de gérer la compression peut recevoir des réponses non compressées ou compressées au format gzip, deflate, compress et pack200-gzip. Si le client gère la compression, un en-tête de `Accept-Encoding:compression` format est envoyé dans la requête. Le type de compression accepté par le client doit correspondre au type de compression de l'objet mis en cache. Par exemple, un `cached.gzip` fichier ne peut pas être servi en réponse à une requête avec un `Accept-Encoding:deflate` en-tête.

Un client qui ne peut pas gérer la compression est servi une manque de cache si la réponse mise en cache est compressée.

Pour la mise en cache dynamique, vous devez configurer deux groupes de contenu, l'un pour les données compressées et l'autre pour les versions non compressées des mêmes données. Voici un exemple de configuration des sélecteurs, des groupes de contenu et des stratégies pour la distribution de fichiers non compressés du cache à des clients qui ne peuvent pas gérer la compression et de servir des versions compressées des mêmes fichiers au client capable de gérer la compression.

```
add cache selector uncompressed_response_selector http.req.url "http.req.
header(\"Host\")"

add cache contentGroup uncompressed_group -hitSelector uncompressed_responst_selector
 -invalSelector uncomp_resp_sel

add cache policy cache_uncompressed -rule "HTTP.REQ.URL.CONTAINS(\"xyz\")&&
 !HTTP.REQ.HEADER(\"Accept-Encoding\").EXISTS"-action CACHE -storeInGroup
uncompressed_group

bind cache global cache_uncompressed -priority 100 -gotoPriorityExpression
END -type REQ_OVERRIDE

add cache selector compressed_response_selector HTTP.REQ.URL "HTTP.REQ.
HEADER(\"Host\")""HTTP.REQ.HEADER(\"Accept-Encoding\")"

add cache contentGroup compressed_group -hitSelector compressed_response_selector


add cache policy cache_compressed -rule "HTTP.REQ.URL.CONTAINS(\"xyz\")&&
 HTTP.REQ.HEADER(\"Accept-Encoding\").EXISTS"-action CACHE -storeInGroup
compressed_group

bind cache global cache_compressed -priority 200 -gotoPriorityExpression
END -type REQ_OVERRIDE
```

Configurer une banque de stratégies pour la mise en cache

Toutes les stratégies associées à un point de liaison particulier sont collectivement appelées banque de polices. En plus de configurer les niveaux de priorité pour les stratégies d'une banque, vous pouvez modifier l'ordre d'évaluation dans une banque en configurant les expressions Goto. Vous pouvez modifier davantage l'ordre d'évaluation en appelant une banque de stratégies externe à partir de la banque de stratégies en cours. Vous pouvez également configurer de nouvelles banques de stratégies auxquelles vous affectez vos propres étiquettes. Étant donné que ces banques de stratégies ne sont liées à aucun point du cycle de traitement, elles ne peuvent être invoquées qu'à partir d'autres banques de stratégies. Pour plus de commodité, les banques de stratégies dont les étiquettes ne correspondent pas à un point de liaison intégré sont appelées étiquettes de stratégie.

En plus de contrôler l'ordre d'évaluation des stratégies en liant la stratégie et en attribuant un niveau de priorité, comme décrit dans « Politiques de liaison », vous pouvez établir le flux au sein d'une banque de stratégies en configurant une expression Goto. Une expression Goto remplace le flux déterminé par les niveaux de priorité. Vous pouvez également contrôler le flux d'évaluation en appelant une banque de stratégies externe après avoir évalué une entrée dans la banque en cours. L'évaluation revient toujours à la banque actuelle une fois l'évaluation terminée.

Le tableau suivant récapitule les entrées pour contrôler l'évaluation dans une banque de stratégies.

Attribut	Spécifie
Nom	Nom d'une stratégie ou, pour invoquer une autre banque de stratégies sans évaluer la stratégie, le mot clé NOPOLICY. Vous pouvez spécifier NOPOLICY plusieurs fois dans une banque de stratégies, mais vous ne pouvez spécifier une stratégie nommée qu'une seule fois.
Priority	Un entier. Plus l'entier est bas, plus la priorité est élevée.
Goto Expression	Détermine la prochaine stratégie ou banque de stratégies à évaluer. Vous pouvez fournir l'une des valeurs suivantes : 1. NEXT : Aller à la stratégie avec la priorité supérieure suivante. 2. END : Arrêter l'évaluation. 3. USE_INVOCATION_RESULT : Applicable si cette entrée appelle une autre banque de stratégies. Si le Goto final dans la banque invoquée a une valeur de END, l'évaluation s'arrête. Si le Goto final est autre chose que END, la banque de polices actuelle effectue un NEXT. 4. Nombre positif : Numéro de priorité de la prochaine stratégie à évaluer. 5. Expression numérique : expression qui produit le numéro de priorité de la stratégie suivante à évaluer. Le Goto ne peut aller de l'avant que dans une banque de polices. L'omission de l'expression Goto équivaut à la spécification END.

Attribut	Spécifie
Type d'invocation	Désigne un type de banque de stratégies. La valeur peut être l'une des valeurs suivantes - 1. Demander un serveur virtuel : Invoque des stratégies de demande associées à un serveur virtuel. 2. Serveur virtuel de réponse : Invoque des stratégies de temps de réponse associées à un serveur virtuel. 3. Étiquette de stratégie : invoque une autre banque de stratégies, telle qu'elle est identifiée par l'étiquette de stratégie de la banque.
Nom d'appel	Nom d'un serveur virtuel ou d'une étiquette de stratégie, en fonction de la valeur que vous avez spécifiée pour le type d'appel.

Le cache intégré comporte deux étiquettes de stratégie intégrées et vous pouvez configurer d'autres étiquettes de stratégie :

`_reqBuiltInDefaults`: cette étiquette de stratégie est appelée à partir du point de liaison par défaut de l'heure de la demande.
`_resBuiltInDefaults`: cette étiquette de stratégie est appelée à partir du point de liaison par défaut du temps de réponse.

Pour appeler une étiquette de stratégie dans une banque de stratégies de mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 bind cache policylabel <labelName> -policname<policyName> -priority<
     priority> [-gotoPriorityExpression <gotoprioritыExpression>] [-
     invoke <labelType> <labelName>]
2 <!--NeedCopy-->
```

Pour appeler une étiquette de stratégie dans une banque de stratégies de mise en cache à l'aide de l'interface graphique :

1. Accédez à **Optimisation** > **Mise en cache intégrée, cliquez sur Gestionnaire de stratégies** de cache, puis spécifiez le point de liaison approprié (Remplacer Global ou Global par défaut) et le type de connexion pour afficher la liste des stratégies liées à ce point de liaison.
2. Si vous souhaitez appeler une étiquette de stratégie sans évaluer de stratégie, cliquez sur **NOPOLICY**.

> **Remarque :**
>
> Pour appeler une banque de stratégies externe, cliquez sur le champ de la colonne Type d'appel et sélectionnez le type de banque de stratégies que vous souhaitez appeler à ce stade dans la banque de stratégies. Il peut s'agir d'une étiquette globale ou d'une banque de serveurs virtuels. Dans le champ Nom d'appel, entrez l'étiquette ou le nom du serveur virtuel.

Pour appeler une étiquette de stratégie de mise en cache dans une banque de stratégies de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb vserver <name>@ -policyName <policyName>|<NOPOLICY-CACHE> -
    priority<positiveInteger> -gotoPriorityExpression <expression> -type
     REQUEST|RESPONSE -invoke<labelType> <labelName>
<!--NeedCopy-->
```

```
bind cs vserver <name> -policyName <policyName>|<NOPOLICY-CACHE> -
    priority<positiveInteger> -gotoPriorityExpression <expression> -type
     REQUEST|RESPONSE -invoke<labelType> <labelName>
<!--NeedCopy-->
```

Pour appeler une étiquette de stratégie de mise en cache dans une banque de stratégies de serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge/Commutation de contenu** > **Serveurs virtuels**, sélectionnez le serveur virtuel et cliquez sur **Stratégies**.
2. Si vous configurez une entrée existante dans cette banque, ignorez cette étape. Si vous ajoutez une nouvelle stratégie à cette banque de stratégies ou si vous souhaitez utiliser l'entrée NOPOLICY « factice », cliquez sur **Ajouter** et effectuez l'une des opérations suivantes :
   - Pour configurer une nouvelle stratégie, cliquez sur Cache et configurez la nouvelle stratégie comme décrit dans Configuration d'une stratégie dans le cache intégré.
   - Pour appeler une banque de stratégies sans traiter de règle de stratégie, sélectionnez l'`NOPOLICY-CACHE` option.

> **Remarque :**
>
> Pour appeler une banque de stratégies externe, cliquez sur le champ de la colonne Type d'appel et sélectionnez le type de banque de stratégies que vous souhaitez appeler à ce stade dans la banque de stratégies. Il peut s'agir d'une étiquette globale ou d'une banque de serveurs virtuels. Dans le champ Nom d'appel, entrez l'étiquette ou le nom du serveur virtuel.

Configurer une étiquette de stratégie dans un cache intégré

Outre la configuration des stratégies dans une banque de stratégies pour l'un des points de liaison intégrés ou un serveur virtuel, vous pouvez créer des étiquettes de stratégie de mise en cache et configurer des banques de stratégies pour ces nouvelles étiquettes.

Une étiquette de stratégie pour le cache intégré ne peut être appelée qu'à partir de l'un des points de liaison que vous pouvez afficher dans le Gestionnaire de stratégies dans le volet de détails de la mise en **cache intégrée** (remplacement de la requête, requête par défaut, remplacement de réponse ou par défaut) ou les étiquettes de stratégie intégrées `\\_reqBuiltinDefaults` et `\\_resBuiltinDefaults`. Vous pouvez appeler une étiquette de stratégie n'importe quel nombre de fois, contrairement à une stratégie, qui ne peut être invoquée qu'une seule fois.

L'interface graphique Citrix ADC offre une option permettant de renommer une étiquette de stratégie. Le changement de nom d'une étiquette de stratégie n'affecte pas le processus d'évaluation des stratégies liées à l'étiquette.

> **Remarque** :
>
> Vous pouvez utiliser la stratégie `NOPOLICY` « factice » pour invoquer n'importe quelle étiquette de stratégie provenant d'une autre banque de stratégies. L' `NOPOLICY` entrée est un espace réservé qui ne traite pas de règle.

Pour configurer une étiquette de stratégie pour la mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour créer une étiquette de stratégie et vérifier la configuration :

- `add cache policylabel <labelName> -evaluates (REQ|RES)`
- `show cache policylabel <labelName>`

Invoquez cette étiquette de stratégie à partir d'une banque de stratégies.

Pour configurer une étiquette de stratégie pour la mise en cache à l'aide de l'interface graphique :

Accédez à **Optimisation** > **Mise en cache intégrée** > **Étiquettes** de stratégie, ajoutez une étiquette de stratégie et liez les stratégies mises en cache.

> **Remarque :**
> Pour s'assurer que Citrix ADC traite l'étiquette de stratégie au bon moment, configurez un appel de cette étiquette dans l'une des banques de stratégies associées aux points de liaison intégrés.

Pour renommer une étiquette de stratégie à l'aide de l'interface graphique :

Accédez à **Optimisation** > **Mise en cache intégrée** > **Étiquettes** de stratégie, sélectionnez l'étiquette de stratégie et renommez.

Dissocier et supprimer une stratégie de mise en cache intégrée et une étiquette de stratégie

Vous pouvez dissocier une stratégie d'une banque de stratégies et la supprimer. Pour supprimer la stratégie, vous devez d'abord la dissocier. Vous pouvez également supprimer une invocation d'étiquette de stratégie et supprimer une étiquette de stratégie. Pour supprimer l'étiquette de stratégie, vous devez d'abord supprimer toutes les invocations que vous avez configurées pour l'étiquette.

Vous ne pouvez pas dissocier ou supprimer les étiquettes des points de liaison intégrés (demande par défaut, remplacement de la demande, réponse par défaut et remplacement de la réponse).

Pour dissocier une stratégie de mise en cache globale à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind cache global <policy>
```

Pour dissocier une stratégie de mise en cache spécifique au serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
(unbind lb vserver|unbind cs vserver)<vserverName> -policyName <policyName>
 -type(REQUEST|RESPONSE)
```

Pour supprimer une stratégie de mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm cache policy <policyName>
```

Pour dissocier une stratégie de mise en cache à l'aide de l'interface graphique :

Accédez à **Optimisation** > **Mise en cache intégrée, cliquez sur Gestionnaire de stratégies** de cache et dissociez les stratégies en spécifiant le point de liaison et le type de connexion appropriés (Request/Response).

Pour supprimer un appel d'étiquette de stratégie à l'aide de l'interface graphique :

1. Accédez à **Optimisation** > Mise en **cache intégrée**, cliquez sur **Gestionnaire de stratégies de cache**et spécifiez le point de liaison approprié (serveur virtuel d'équilibrage de charge ou serveur virtuel de commutation de contenu) et le type de connexion pour afficher la liste des stratégies de cache liées à ce serveur virtuel.
2. Dans la colonne Invoke de stratégie, désactivez l'entrée.

Prise en charge du cache pour les protocoles de base de données

August 20, 2021

La fonction de cache intégrée surveille et met en cache la demande de base de données tel que déterminé par les stratégies de cache. Les utilisateurs doivent configurer les stratégies de cache pour les protocoles MYSQL et MSSQL car l'appliance Citrix ADC ne fournit aucune stratégie par défaut. Lors de la configuration des protocoles par défaut, rappelez-vous que les stratégies basées sur les demandes ne prennent en charge que les actions CACHE et INVAL, tandis que les stratégies basées sur les réponses ne prennent en charge que l'action « NOCACHE ». Après avoir configuré les stratégies, vous devez les lier aux serveurs virtuels. Les stratégies MYSQL et MSSQL, à la fois requête et réponse, sont liées uniquement aux serveurs virtuels.

Avant de créer une stratégie de cache, vous devez créer un groupe de contenu de cache de type MYSQL ou MSSQL. Lorsque vous créez un groupe de contenu de cache, associez au moins un sélecteur de sélection à celui-ci. Reportez-vous à la section Configuration d'un groupe de contenu de base pour configurer un groupe de contenu de cache.

L'exemple suivant explique comment configurer et vérifier la prise en charge du cache pour les protocoles SQL.

```
1  > enable feature IC
2  > set cache parameter -memlimit 100
3  > add cache selector sel1 mssql.req.query.text
4
5  > add cache contentgroup cg1  -type "MSSQL" -hitselector "sel1" -
       invalselector "inval_sel" -relExpiry "500" -maxResSize
6   "100"
7  > add cache policy cp1  -rule "mssql.req.query.command.contains("select
       ")" -action "CACHE" -storeInGroup "cg1"
8  > add cache policy cp2  -invalObjects "cg1" -rule "mssql.req.query.text
       .contains("insert")" -action "INVAL"
9  > add db user user1  -password "Pass1"
10 > add service svc_sql_1 10.102.147.70 mssql 64834 -healthMonitor "NO" -
       downstateflush "ENABLED"
11 > add lb vserver lb_mssql1 mssql 10.102.147.77 1433  -lbmethod "
       roundrobin"
12 > bind lb vserver lb_mssql1 svc_sql_1
13 > bind lb vserver lb_mssql1 -policyName cp1  -type "REQUEST" -priority
       "2"
14 > bind lb vserver lb_mssql1 -policyName cp2  -type "REQUEST" -priority
       "1"
15
16 > show cache selector sel1
```



```
      Name:sel1
                    Expressions:
                    1)mssql.req.query.text
> show cache policy cp1
                    Name:cp1
      Rule:mssql.req.query.command.contains("select")
                    CacheAction:CACHE
                    Stored in group: cg1
                    UndefAction:Use Global
                Hits:2
                    Undef Hits:0
                    Policy is bound to following entities
                    1) Bound to:
                                REQ VSERVER lb_mssql1
                                Priority:2
                                GotoPriorityExpression: END
<!--NeedCopy-->
```

> **Remarque :**
>
> Les méthodes de réduction des foules flash, comme expliqué dans Réduction des foules Flash, ne sont pas prises en charge pour les protocoles MYSQL et MSSQL.

Configuration des expressions pour la mise en cache des stratégies et des sélecteurs

October 5, 2021

Une expression de temps de demande examine les données de la transaction de temps de demande, et une expression de temps de réponse examine les données d'une transaction de temps de réponse. Dans une stratégie de mise en cache, si une expression correspond aux données d'une demande ou d'une réponse, l'appliance Citrix ADC effectue l'action associée à la stratégie. Dans un sélecteur, les expressions de temps de demande sont utilisées pour trouver des réponses correspondantes qui sont stockées dans un groupe de contenus.

Avant de configurer des stratégies et des sélecteurs pour le cache intégré, vous devez connaître, au minimum, les noms d'hôte, les chemins et les adresses IP qui apparaissent dans les URL de requête et de réponse HTTP. Et vous devez probablement connaître le format des requêtes et réponses HTTP entières. Des programmes tels que les en-têtes HTTP en direct `http://livehttpheaders.mozdev.org/)or HTTPFox https://addons.mozilla.org/en-US/firefox/addon/6647` peuvent vous aider à étudier la structure des données HTTP avec lesquelles votre organisation travaille.

Voici un exemple de demande HTTP GET pour un programme de cotation boursière :

```
GET /quote.dll?page=dynamic&mode=data&mode=stock&symbol=CTXS&page=multi
    &selected=CTXS&random=0.00792039478975548 HTTP/1.1

Host: quotes.mystockquotes.com

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9)
    Gecko/2008052906 Firefox/3.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q
    =0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate,compress,pack200-gzip

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive

Referer: http://quotes.mystockquotes.com/quote.dll?mode=stock&symbol=
    CTXS&page=multi&selected=CTXS

Cookie: __qca=1210021679-72161677-10297606
<!--NeedCopy-->
```

Lorsque vous configurez une expression, notez les limitations suivantes :

Type d'expression	Restrictions
Demander	Ne configurez pas les expressions de temps de demande dans une stratégie avec une action CACHE ou NOCACHE. Utilisez plutôt MAY_CACHE ou MAY_NOCACHE.

Type d'expression	Restrictions
Réponse	Configurez les expressions de temps de réponse dans les stratégies de mise en cache uniquement. Les sélecteurs peuvent utiliser uniquement des expressions de temps de demande. Ne configurez pas les expressions de temps de réponse dans une stratégie avec une action INVAL. Remarque : Ne configurez pas les expressions de temps de réponse dans une stratégie avec une action CACHE et un groupe de contenus paramétré. Utilisez l'action MAY_CACHE.

> **Remarque :**
> Pour obtenir une présentation complète des expressions avancées, reportez-vous à la section Stratégies et expressions.

Syntaxe d'expression

Voici les composants de base de la syntaxe :

- Séparez les mots-clés par des points (.), comme suit :

```
http.req.url
```

- Enclenchez les valeurs de chaîne entre parenthèses et guillemets, comme suit :

```
http.req.url.query.contains("this")
```

- Lorsque vous configurez une expression à partir de la ligne de commande, vous devez échapper les guillemets internes (les guillemets qui délimitent les valeurs de l'expression, par opposition aux guillemets qui délimitent l'expression). Une méthode consiste à utiliser une barre oblique, comme suit :

```
\"abc\"
```

Les expressions de sélecteur sont évaluées par ordre d'apparition, et plusieurs expressions d'une définition de sélecteur sont jointes par un AND logique. Contrairement aux expressions de sélection, vous pouvez spécifier des opérateurs booléens et modifier la priorité d'une expression avancée pour une règle de stratégie.

Configurer une expression dans une stratégie de mise en cache ou un sélecteur

> **Remarque :**
> La syntaxe d'une expression de stratégie est différente de celle d'une expression de sélection. Pour obtenir une présentation complète des expressions avancées, reportez-vous à la section « Stratégies et expressions. «

Pour configurer une expression de stratégie à l'aide de l'interface de ligne de commande

1. Commencez la définition de stratégie comme décrit dans la section « Liaison globale d'une stratégie de mise en cache intégrée ». «
2. Pour configurer la règle de stratégie, délimiter la règle entière entre guillemets et délimiter les valeurs de chaîne au sein de la règle par des guillemets d'échappement.

Voici un exemple :

« http.req.url.contains (« jpg ») »

1. Pour ajouter des valeurs booléennes, insérez &&, || ou ! opérateurs.

Voici quelques exemples :

```
"http.req.url.contains(\"jpg\")|| http.req.url.contains(\"jpeg\")"
```

```
"http.req.url.query.contains(\"IssuePage\")"
```

```
"http.req.header(\"Host\")contains(\"my.company.com\")&& http.req.method.eq
(\"GET\")&& http.req.url.query.contains(\"v=7\")"
```

1. Pour configurer un ordre d'évaluation pour les parties constitutives d'un composé

```
"http.req.url.contains(\"jpg\")|| (http.req.url.contains(\"jpeg\")&& http.
req.method.eq(\"GET\"))"
```

Pour configurer une expression de sélecteur à l'aide de l'interface de ligne de commande :

1. Démarrez la définition du sélecteur comme décrit dans « A propos des groupes de contenu ».
2. Pour configurer l'expression du sélecteur, délimiter la règle entière entre guillemets et délimiter les valeurs de chaîne dans la règle par des guillemets d'échappement.

Voici un exemple :

```
"http.req.url.contains(\"jpg\")"
```

1. Vous ne pouvez pas ajouter de valeurs booléennes, insérer &&, || ou ! opérateurs. Entrez chaque élément d'expression délimité entre guillemets. Les expressions multiples de la définition sont traitées comme une expression composée jointe par des ANDs logiques.

Voici quelques exemples :

```
1 "http.req.url.query.value("ProductId")" "http.req.url.query.value("
     BatchNum")" "http.req.url.query.value("depotLocation")"
2 <!--NeedCopy-->
```


Pour configurer une stratégie ou une expression de sélecteur à l'aide de l'interface graphique

1. Démarrez la définition de la stratégie ou du sélecteur comme décrit dans « Pour configurer une stratégie pour la mise en cache ou l'invalidation à l'aide de l'utilitaire de configuration » ou « Pour configurer un sélecteur à l'aide de l'utilitaire de configuration. «
2. Dans le champ **Expression**, vous pouvez soit taper manuellement la stratégie avancée en cliquant sur Basculer vers la syntaxe classique, soit créer une expression à l'aide de l' **éditeur d'expression**.
3. Pour insérer un opérateur entre deux parties d'une expression composée, cliquez sur le bouton Opérateurs et sélectionnez le type d'opérateur. Voici un exemple d'expression configurée avec un OR booléen (signalé par des barres verticales doubles, ||) :
4. Cliquez sur la liste déroulante **Expressions fréquemment utilisées** pour insérer les expressions couramment utilisées.
5. Pour tester l'expression, cliquez sur le bouton **Evaluer**. Dans la boîte de dialogue **Expression Evaluator**, sélectionnez le type de flux correspondant à l'expression. Dans le champ de données, collez la demande ou la réponse HTTP que vous souhaitez analyser à l'aide de l'expression, puis cliquez sur **Evaluer**.

Afficher les objets mis en cache et les statistiques de cache

Vous pouvez afficher des objets mis en cache particuliers et afficher des statistiques récapitulatives sur les demandes de cache, les échecs et l'utilisation de la mémoire. Les statistiques fournissent des informations sur la quantité de données qui sont servies à partir du cache, les éléments responsables du plus grand avantage de performances et les éléments que vous pouvez régler pour améliorer les performances du cache.

Cette section comprend les détails suivants :

- Affichage des objets mis en cache
- Recherche de réponses mises en cache particulières
- Affichage des statistiques de cache

Afficher les objets mis en cache

Après avoir activé la mise en cache, vous pouvez afficher les détails des objets mis en cache. Par exemple, vous pouvez afficher les éléments suivants :

- Tailles de réponse et tailles d'en-tête
- Codes d'état
- Groupes de contenus
- ETagen-têtes, Last-Modified et Cache-Control
- URL de demande

- Paramètres de l'accès
- Adresses IP de destination
- Délais de demande et de réponse

Pour afficher la liste des objets mis en cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show cache object
```

Propriétés	Description
Taille de la réponse (octets)	Taille de l'en-tête et du corps de la réponse.
Taille de l'en-tête de réponse (octets)	Taille de la partie en-tête de la réponse.
Code d'état de la réponse	Le code d'état envoyé avec la réponse.
ETag	En-tête ETag inséré dans la réponse. En général, cet en-tête indique si la réponse a récemment été modifiée.
Dernière modification	L'en-tête Last-Modified inséré dans la réponse. Cet en-tête indique la date à laquelle la réponse a été modifiée pour la dernière fois.
Contrôle du cache	L'en-tête Cache-Control inséré dans la réponse.
Date	En-tête Date qui indique quand la réponse a été envoyée.
Groupe de contenu	Le groupe de contenus dans lequel la réponse est stockée.
Match complexe	Si cet objet a été mis en cache en fonction de valeurs paramétrées, la valeur de ce champ est OUI.
Hôte	L'hôte spécifié dans l'URL qui a demandé cette réponse.
Port hôte	Port d'écoute de l'hôte spécifié dans l'URL qui a demandé cette réponse
URL	URL émise pour la réponse stockée.
IP destination	Adresse IP du serveur à partir duquel cette réponse a été récupérée.
Port de destination	Port d'écoute du serveur de destination.

Propriétés	Description
Paramètres de l'accès	Si le groupe de contenu qui stocke la réponse utilise des paramètres d'accès, ils sont répertoriés dans ce champ.
Sélecteur de succès	Si ce groupe de contenus utilise un sélecteur d'accès, il est répertorié dans ce champ.
Sélecteur Inval	Si ce groupe de contenus utilise un sélecteur d'invalidation, il est répertorié dans ce champ.
Expressions du sélecteur	Si ce groupe de contenus utilise un sélecteur, ce champ affiche l'expression qui définit la règle de sélection.
Request time	Durée en millisecondes écoulée depuis l'émission de la demande.
Temps de réponse	Durée en millisecondes écoulée depuis que le cache a commencé à recevoir la réponse.
Âge	Durée pendant laquelle l'objet est resté dans le cache.
Expiration	Durée après laquelle l'objet est marqué comme expiré.
Rinçage	Indique si la réponse a été vigée après son expiration.
Prefetch	Si Prefetch a été configuré pour ce groupe de contenus, délai avant expiration pendant lequel l'objet est récupéré depuis l'origine. La prélecture ne s'applique pas aux objets négatifs (par exemple, réponses 404 « objet introuvable »).

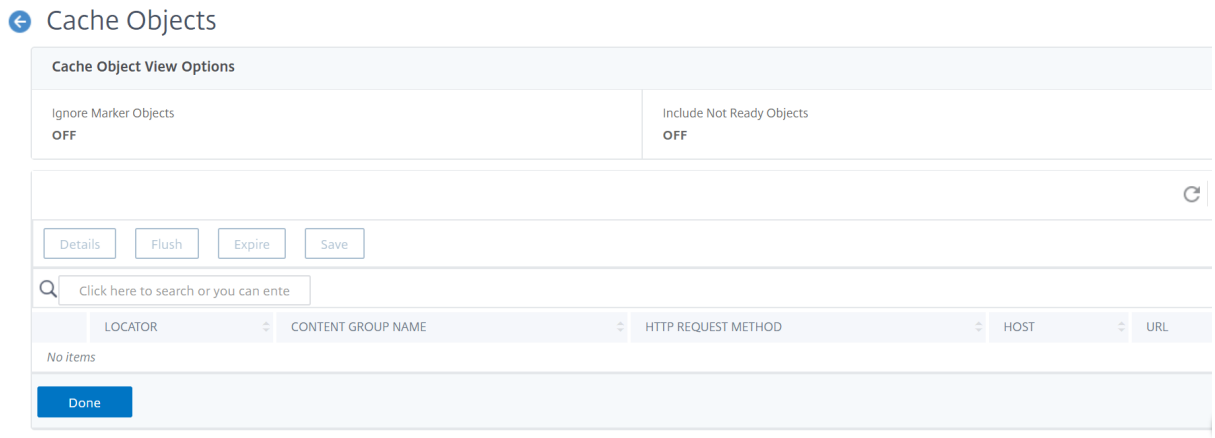
Propriétés	Description
Lecteurs actuels	Approximativement le nombre actuel de demandes traitées. Lorsqu'une réponse avec un objet d'en-tête Content-Length est en cours de téléchargement, les valeurs manques actuelles et les valeurs des lecteurs actuels sont généralement égales à 1. Lorsqu'un objet de réponse en morceaux est téléchargé, la valeur actuelle des échecs est généralement de 1, mais la valeur des lecteurs actuels est généralement égale à 0, car la réponse en morceaux qui est fournie au client ne provient pas des tampons de mise en cache intégrés.
Les manques actuelles	Nombre actuel de requêtes ayant entraîné une absence de cache et une récupération à partir du serveur d'origine. Cette valeur est généralement égale à 0 ou 1. Si Poll Every Time est activé pour un groupe de contenus, le nombre peut être supérieur à 1.
Accès	Nombre d'accès au cache pour cet objet.
Misses	Le nombre de mises en cache manquant pour cet objet
Format de compression	Type de compression appliqué à cet objet. Les formats de compression incluent gzip, deflate, compress et pack200-gzip.
Version HTTP en réponse	Version du protocole HTTP utilisée pour envoyer la réponse.
Etag faible présent en réponse	Les en-têtes d'étiquette forts changent si les bits d'une entité changent. Les en-têtes forts sont basés sur les valeurs d'octet d'un objet. Les en-têtes d'étiquette faibles changent si la signification d'une entité change. Les valeurs etag faibles sont basées sur l'identité sémantique. Les valeurs d'etags faibles commencent par un « W ».

Propriétés	Description
Cellule marqueur négative	Un objet marqueur peut être mis en cache, mais il ne répond pas encore à tous les critères de mise en cache. Par exemple, l'objet peut dépasser la taille de réponse maximale pour le groupe de contenus. Une cellule de marqueur est créée pour les objets de ce type. La prochaine fois qu'un utilisateur envoie une demande pour cet objet, un échec de cache est envoyé.
Marqueur Reason créé	La raison pour laquelle une cellule de marqueur a été créée (par exemple, « En attente de minhit », « Les données de réponse de longueur de contenu ne sont pas dans la limite de taille du groupe »).
Sondage automatique à chaque fois	Si le cache intégré reçoit une réponse 200 OK déjà expirée avec des validateurs (en-têtes de réponse Last-Modified ou ETag), il stocke la réponse et la marque comme auto-PET (interrogation automatique à chaque fois).
Citrix ADC Etag inséré en réponse	Variante de l'en-tête ETag généré par l'appliance Citrix ADC. La valeur YES s'affiche si Citrix ADC insère un Etag dans la réponse.
Réponse complète présente dans le cache	Indique s'il s'agit d'une réponse complète.
IP de destination vérifiée par DNS	Indique si la résolution DNS a été effectuée lors du stockage de l'objet.
Objet stocké via un proxy de transfert de cache	Indique si cette réponse a été stockée en raison d'un proxy de transfert configuré dans le cache intégré.
Object est un fichier de base Delta	Réponse compressée en delta.
En attente de minhits	Indique si ce groupe de contenus nécessite un nombre minimum de serveurs d'origine avant de mettre en cache une réponse.

Propriétés	Description
Comptage de Minhit	Si ce groupe de contenus nécessite un nombre minimum de demandes de serveur d'origine avant de mettre en cache un objet, ce champ affiche le nombre de demandes reçues jusqu'à présent.
Méthode de requête HTTP	La méthode, GET ou POST, utilisée dans la requête qui a obtenu cet objet.
Stocké par stratégie	Nom de la stratégie de mise en cache qui a provoqué le stockage de cet objet. La valeur NOT AVAILABLE indique que la stratégie a été désactivée ou supprimée. La valeur NONE indique que l'objet ne correspond pas à une stratégie visible, mais qu'il a été stocké selon des critères internes de mise en cache.
Les métadonnées du pare-feu d'application existent	Ce paramètre est utilisé lorsque le pare-feu d'application et le cache intégré sont tous deux activés. Le pare-feu d'application analyse le contenu d'une page de réponse, stocke ses métadonnées (par exemple, les URL et les formulaires contenus dans la page) et exporte les métadonnées avec la réponse vers le cache. Le cache stocke la page et les métadonnées, et lorsque le cache sert la page, il renvoie les métadonnées à la session de la demande.
objet de légende HTTP, nom, type, réponse	Ces cellules indiquent si ces données ont été stockées à la suite d'une expression de légende HTTP et fournissent des informations sur divers aspects de la légende et de la réponse correspondante. Pour plus d'informations sur les légendes HTTP, consultez « Légendes HTTP ».

Pour afficher les objets mis en cache à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Objets de cache**. Vous pouvez afficher tous les objets mis en cache et les trier en conséquence selon vos besoins.



Rechercher des réponses en cache particulières

Vous pouvez trouver des éléments individuels dans le cache en fonction de critères de recherche. Il existe différentes méthodes pour rechercher des éléments mis en cache, selon que le groupe de contenus contenant les données utilise des sélecteurs d'accès et d'invalidation, comme suit :

- Si le groupe de contenus utilise des sélecteurs, vous ne pouvez effectuer la recherche qu'à l'aide de l'ID de localisateur de l'élément mis en cache.
- Si le groupe de contenus n'utilise pas de sélecteurs, vous effectuez la recherche à l'aide de critères tels que l'URL, l'hôte et le nom du groupe de contenus.

Lorsque vous recherchez une réponse mise en cache, vous pouvez localiser certains éléments par URL et par hôte. Si la réponse se trouve dans un groupe de contenus qui utilise un sélecteur, vous ne pouvez la trouver qu'en utilisant un numéro de localisateur (par exemple, 0x00000000ad7af00000050). Pour enregistrer un numéro de localisateur en vue d'une utilisation ultérieure, cliquez avec le bouton droit de la souris sur l'entrée et sélectionnez **Copier**. Pour plus d'informations sur les sélecteurs, voir « Configuration des sélecteurs et des groupes de contenu de base ». «

Pour afficher les réponses mises en cache dans des groupes de contenu ne disposant pas d'un sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show cache object [-locator <positiveInteger>] | [(-url <URL> (-host <
hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET
 | POST ]))| [-httpStatus <positive integer>] | -group <contentGroupName> |
 -ignoreMarkerObjects (ON | OFF)| -includeNotReadyObjects (ON | OFF)]
```

Pour afficher les réponses mises en cache dans des groupes de contenus dotés d'un sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
show cache object -locator <locatorString> MarkerObjects ( ON | OFF )| -
includeNotReadyObjects ( ON | OFF )| [-httpStatus<positive integer>]
```

Pour afficher les réponses mises en cache dans des groupes de contenus qui ne possèdent pas de sélecteur à l'aide de l'utilitaire de configuration

Accédez à **Optimisation > Mise en cache intégrée > Objets de cache**, cliquez sur Rechercher et définissez les critères de recherche pour afficher la réponse mise en cache requise.

Si vous n'avez pas encore configuré de groupe de contenu, tous les objets se trouvent dans le groupe Par défaut.

Afficher les statistiques du cache

Le tableau suivant récapitule les statistiques de cache détaillées que vous pouvez consulter.

Comptoir	Description
—	—
Accès	Réponses trouvées et servies à partir du cache intégré. Inclut des objets statiques tels que des fichiers image, des pages avec des codes d'état 200, 203, 300, 301, 302, 304, 307, 403, 404, 410, et des réponses qui correspondent à une stratégie définie par l'utilisateur avec une action CACHE.
Misses	Demandes HTTP interceptées pour lesquelles la réponse a finalement été récupérée depuis le serveur d'origine.
Demandes	Nombre total de demandes de cache plus le nombre total d'échecs de cache.
Hits non-304	Si l'utilisateur demande un élément plusieurs fois et que l'élément du cache est inchangé depuis la dernière fois que l'appliance Citrix ADC l'a servi, l'appliance Citrix ADC fournit une réponse 304 au lieu de l'objet mis en cache.
Cette statistique indique le nombre d'éléments que l'appliance Citrix ADC a servis à partir du cache, à l'exclusion de 304 réponses.
304 Hits	Nombre de 304 réponses (objet non modifié) que l'appliance Citrix ADC a servies à partir du cache.
304 taux d'accès (%)	Pourcentage de 304 réponses fournies par l'appliance Citrix ADC, par rapport aux autres réponses.
Taux d'accès (%)	Pourcentage de réponses que l'appliance Citrix ADC a servies à partir du cache (demandes de cache) par rapport aux réponses qui n'ont pas pu être servies à partir du cache.
Bande passante d'origine enregistrée (%)	Une estimation de la capacité de traitement que l'appliance Citrix ADC a enregistrée sur le serveur d'origine en raison de la diffusion des réponses à partir du cache.
Octets desservis par Citrix ADC	Nombre total d'octets que l'appliance Citrix ADC a servis à partir du serveur d'origine et du cache.
Octets servis par le cache	Nombre total d'octets que l'appliance Citrix ADC a servis à partir du cache.

Taux d'accès aux octets (%)	Pourcentage de données que l'appliance Citrix ADC a servi à partir du cache, par rapport à toutes les données de toutes les réponses servies.
Octets compressés depuis le cache	Quantité de données, en octets, que l'appliance Citrix ADC a servie sous forme compressée.
Storable Misses	Si l'appliance Citrix ADC ne trouve pas un objet demandé dans le cache, elle récupère l'objet depuis le serveur d'origine. Ceci connu sous le nom de « cache miss » (échec d'accès au cache). Une mémoire cache manquante peut être stockée dans le cache.
Non stockables manquant	Un cache non stockable ne peut pas être stocké dans le cache.
Misses	Tous les fichiers cache manquaient.
Revalidations	Le paramètre Max-Age dans un en-tête Cache-Control détermine, en quelques secondes, quand un cache intermédiaire doit revalider le contenu avec le cache intégré avant de le diffuser à l'utilisateur.
Pour plus d'informations, reportez-vous à la section « Insertion d'un en-tête Cache-Control ». «
Revalidations réussies	Nombre de revalidations qui ont été effectuées.
Pour plus d'informations, reportez-vous à la section « Insertion d'un en-tête Cache-Control ». «
Conversions en requêtes conditionnelles	Une demande d'agent utilisateur pour un objet PET mis en cache est toujours convertie en demande conditionnelle et envoyée au serveur d'origine.
Pour plus d'informations, reportez-vous à la section « Interrogation du serveur Origin chaque fois qu'une demande est reçue. «
Taux d'échec stockable (%)	Le cache stockable manque en pourcentage des échecs de cache non stockables.
Taux de réévaluation réussie (%)	Les revalidations réussies en pourcentage de toutes les tentatives de revalidation.
Pour plus d'informations, reportez-vous à la section « Insertion d'un en-tête Cache-Control ». «
Expire au dernier octet	Nombre de fois que le contenu du cache a expiré immédiatement après avoir reçu le dernier octet du corps. S'applique uniquement aux réponses positives, comme décrit dans le tableau « Cache Hits and Misses ». «
Pour plus d'informations, reportez-vous à la section « Exemple d'optimisation des performances. «
`Flashcache` Misses	Si vous activez Flash Cache, le cache n'autorise qu'une seule requête à atteindre le serveur, ce qui élimine les foules Flash. Cette statistique indique le nombre de demandes Flash Cache qui ont été manquantes dans le cache.
Pour plus d'informations, consultez la section « Mise en file d'attente des demandes dans le cache. «
Accès Flashcache	Nombre de demandes Flash Cache qui ont été des accès au cache.
Pour plus d'informations, reportez-vous à la section « Mise en file d'attente des demandes dans le cache ». «
Demandes inval paramétrées	Demandes qui correspondent à une stratégie avec une action d'invalidation (INVAL) et à un groupe de contenus qui utilise un sélecteur d'invalidation ou des paramètres pour faire expirer sélectivement les objets mis en cache dans le groupe.
Demandes d'annulation complètes	Demandes qui correspondent à une stratégie d'invalidation dans

laquelle le paramètre InvalGroups est configuré et expire un ou plusieurs groupes de contenu. |
Demandes invalies	Demandes qui correspondent à une stratégie d'invalidation et entraînent l'expiration de réponses mises en cache spécifiques ou de groupes de contenu entiers.
Demandes paramétrées	Nombre de demandes de cache traitées à l'aide d'une stratégie avec un groupe de contenu paramétré.
Hits non 304 paramétrés	Nombre de demandes de cache qui ont été traitées à l'aide d'une stratégie avec un groupe de contenus paramétré, où une réponse en cache complète a été trouvée et la réponse n'était pas une réponse 304 (objet non mis à jour).
304 accès paramétrés	Nombre de demandes de cache traitées à l'aide d'une stratégie avec un groupe de contenus paramétré, où l'objet mis en cache a été trouvé et l'objet était une réponse 304 (objet non mis à jour).
Nombre total d'accès paramétrés	Nombre de demandes de cache traitées à l'aide d'une stratégie avec un groupe de contenus paramétré, où l'objet mis en cache a été trouvé.
Taux de succès 304 paramétré (%)	Pourcentage de 304 réponses (objet non mis à jour) qui ont été trouvées à l'aide d'une stratégie paramétrée, par rapport à tous les accès au cache.
Interroger à chaque requête	Si Poll Every Time est activé, l'appliance Citrix ADC consulte toujours le serveur d'origine avant de servir un objet stocké.
Pour plus d'informations, reportez-vous à la section « Interrogation du serveur Origin chaque fois qu'une demande est reçue. «
Interrogez chaque fois qu'un accès au cache a été trouvé à l'aide de la méthode Poll Every Time.
Pour plus d'informations, reportez-vous à la section « Interrogation du serveur Origin chaque fois qu'une demande est reçue. «
Poll every time hit ratio (%)	Pourcentage d'accès au cache à l'aide de la méthode Poll Every Time, par rapport à toutes les recherches d'objets mis en cache à l'aide de Poll Every Time. Pour plus d'informations, reportez-vous à la section « Interrogation du serveur Origin chaque fois qu'une demande est reçue. «
Mémoire maximale (Ko)	Quantité maximale de mémoire dans l'appliance Citrix ADC allouée au cache. Pour plus d'informations, reportez-vous à la section « Configuration des attributs globaux pour la mise en cache ». «
Valeur maximale de la mémoire active (Ko)	Quantité maximale de mémoire (valeur active) qui sera définie une fois la mémoire allouée au cache. Pour plus d'informations, reportez-vous à la section « Comment configurer la fonctionnalité de mise en cache intégrée d'un dispositif Citrix ADC pour différents scénarios. «
Mémoire utilisée (Ko)	Quantité de mémoire réellement utilisée.
Échecs d'allocation de mémoire	Nombre de tentatives infructueuses d'utilisation de la mémoire dans le but de stocker une réponse dans le cache.
La réponse la plus importante à ce jour	La plus grande réponse en octets trouvée dans le cache ou le serveur d'origine et envoyée au client.
Objets mis en cache	Nombre d'objets dans le cache, y compris les réponses qui n'ont pas encore été

entièrement téléchargées et les réponses qui ont expiré mais qui n'ont pas encore été vidées. |
Objets Marqueur	Les objets de marqueur sont créés lorsqu'une réponse dépasse la taille de réponse maximale ou minimale pour le groupe de contenus, ou n'a pas encore reçu le nombre minimum d'accès pour le groupe de contenus.
Hits servis	Nombre d'accès qui ont été diffusés à partir du cache.
Manque d'être gérée	Réponses récupérées depuis le serveur d'origine, stockées dans le cache, puis servies. Devrait se rapprocher du nombre d'erreurs pouvant être stockées. N'inclut pas les erreurs non stockables.

Pour afficher les statistiques du cache récapitulatif à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
stat cache
```

Pour afficher des statistiques de cache spécifiques à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
stat cache -detail
```

```
> stat cache -detail

Integrated Cache Statistics - Detail
Integrated Cache Statistics - Summary
                                          Rate (/s)
                                             Total


Hits                                             0
                        0

Misses                                           0
                        0

Requests                                         0
                        0

Hit ratio(%)                                    --
                        0

Origin bandwidth saved(%)                       --
                        0
Cached objects                                  --
                        0

```



```
19 Marker objects                                        --
                        0
20                                                 Rate (/s)
                                                      Total
21
22 Requests                                               0
                        0
23
24
25 Hit Statistics
26
27                                                 Rate (/s)
                                                      Total
28
29
30 Non-304 hits                                           0
                        0
31
32 304 hits                                               0
                        0
33
34
35 Sql hits                                               0
                        0
36
37
38 Hits                                                   0
                        0
39
40 304 hit ratio(%)                                      --
                        0
41
42 Hit ratio(%)                                          --
                        0
43
44 Origin bandwidth saved(%)                             --
                        0
45 Byte Statistics
46                                                 Rate (/s)
                                                      Total
47
48
49 Bytes served by Citrix ADC                           648
    55379204
50
```



```
51 Bytes served by cache                                  0
                         0
52 Byte hit ratio(%)                                     --
                         0
53 Compressed bytes from cache                            0
                         0
54
55 Miss Statistics
56
57                                                 Rate (/s)
                                                      Total
58
59
60 Storable misses                                        0
                         0
61
62 Non-storable misses                                    0
                         0
63
64 Misses                                                 0
                         0
65
66 Revalidations                                          0
                         0
67
68 Successful revalidations                               0
                         0
69
70 Conversions to conditional req                         0
                         0
71
72
73 Storable miss ratio(%)                                --
                         0
74 Successful reval ratio(%)                             --
                         0
75
76 Flashcache Statistics
77                                                 Rate (/s)
                                                      Total
78
79
80 Expire at last byte                                    0
                         0
81
```



```
Flashcache misses                                    0
                        0
Flashcache hits                                      0
                        0

Invalidation Statistics

                                                Rate (/s)
                                                   Total

Parameterized inval requests                         0
                        0


Full inval requests                                  0
                        0


Inval requests                                       0
                        0

Parameterized Caching Statistics

                                                Rate (/s)
                                                   Total


Parameterized requests                               0
                        0

Parameterized non-304 hits                           0
                        0

Parameterized 304 hits                               0
                        0


Total parameterized hits                             0
                        0

Parameterized 304 hit ratio(%)                      --
                        0

Poll Every Time (PET) Statistics
```



```
115
116                                                Rate (/s)
                                                      Total
117
118
119  Poll every time requests                                0
                           0
120
121  Poll every time hits                                    0
                           0
122
123  Poll every time hit ratio(%)                           --
                           0
124
125  Memory Usage Statistics
126                                                    Total
127
128  Maximum memory(KB)                                      0
129
130  Maximum memory active value(KB)                         0
131
132  Utilized memory(KB)                                     0
133
134  Memory allocation failures                              0
135
136  Largest response so far(B)                              0
137
138  Cached objects                                          0
139
140  Marker objects                                          0
141
142  Hits being served                                       0
143  Misses being handled                                    0
144   Done
145  <!--NeedCopy-->
```

Pour afficher les statistiques du cache récapitulatif à l'aide de l'interface graphique

1. Cliquez sur l'onglet Tableau de **bord** en haut de la page.
2. Faites défiler l'écran jusqu'à la section **Mise en cache intégrée** de la fenêtre.
3. Pour afficher des statistiques détaillées, cliquez sur le lien Plus… en bas du tableau.

Pour afficher des statistiques de cache spécifiques à l'aide de l'interface graphique

1. Cliquez sur l'onglet **Rapports** en haut de la page.

2. Sous Rapports **intégrés, développez le cache intégré**, puis cliquez sur le rapport contenant les statistiques que vous souhaitez afficher.
3. Pour enregistrer le rapport en tant que modèle, cliquez sur **Enregistrer sous** et nommez le rapport. Le rapport enregistré apparaît sous Rapports **personnalisés** .

Affichage des objets mis en cache et des statistiques de cache

August 20, 2021

Vous pouvez afficher des objets mis en cache particuliers et afficher des statistiques récapitulatives sur les accès au cache, les échecs et l'utilisation de la mémoire. Les statistiques fournissent un aperçu de la quantité de données qui est servi à partir du cache, des éléments qui apportent le plus de gain en matière de performance et des éléments que vous pouvez régler pour améliorer les performances du cache.

Cette section comprend les détails suivants :

- Affichage des objets mis en cache
- Recherche de réponses mises en cache particulières
- Affichage des statistiques du cache

Afficher les objets mis en cache

Après avoir activé la mise en cache, vous pouvez afficher les détails des objets mis en cache. Par exemple, vous pouvez afficher les éléments suivants :

- Tailles de réponse et tailles d'en-tête
- Codes d'état
- Groupes de contenu
- ETag, Dernier modifié et en-têtes Cache-Control
- URL de demande
- Paramètres d'accès
- Adresses IP de destination
- Délais de demande et de réponse

Pour afficher une liste d'objets mis en cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show cache object
```


Propriétés	Spécifications
Taille de la réponse (octets)	Taille de l'en-tête et du corps de la réponse.
Taille de l'en-tête de réponse (octets)	Taille de la partie d'en-tête de la réponse.
Code d'état de la réponse	Code d'état envoyé avec la réponse.
ETag	ETag En-tête inséré dans la réponse. En règle générale, cet en-tête indique si la réponse a changé récemment.
Last-Modified	En-tête Last-Modified inséré dans la réponse. Cet en-tête indique la date à laquelle la réponse a été modifiée pour la dernière fois.
Cache-Control	En-tête Cache-Control inséré dans la réponse.
Date	En-tête Date qui indique quand la réponse a été envoyée.
Contentgroup	Groupe de contenu dans lequel la réponse est stockée.
Correspondance complexe	Si cet objet a été mis en cache en fonction de valeurs paramétrées, cette valeur de champ est YES.
Hôte	Hôte spécifié dans l'URL qui a demandé cette réponse.
Port hôte	Port d'écoute de l'hôte spécifié dans l'URL qui a demandé cette réponse
URL	URL émise pour la réponse stockée.
IP destination	Adresse IP du serveur à partir duquel cette réponse a été récupérée.
Port de destination	Port d'écoute du serveur de destination.
Paramètres d'accès	Si le groupe de contenu qui stocke la réponse utilise des paramètres d'accès, ils sont répertoriés dans ce champ.
Sélecteur d'accès	Si ce groupe de contenu utilise un sélecteur d'accès, il est répertorié dans ce champ.
Sélecteur inval	Si ce groupe de contenu utilise un sélecteur d'invalidation, il est répertorié dans ce champ.

Propriétés	Spécifications
Expressions de sélecteur	Si ce groupe de contenu utilise un sélecteur, ce champ affiche l'expression qui définit la règle de sélection.
Request time	Durée en millisecondes depuis que la demande a été émise.
Temps de réponse	Temps en millisecondes depuis que le cache a commencé à recevoir la réponse.
Âge	Durée pendant laquelle l'objet a été dans le cache.
Expiration	Durée après laquelle l'objet est marqué comme expiré.
Vidé	Si la réponse a été vidé après expiration.
Prérécupération	Si la fonction Prefetch a été configurée pour ce groupe de contenu, la durée avant l'expiration pendant laquelle l'objet est récupéré à partir de l'origine. Prefetch ne s'applique pas aux objets négatifs (par exemple, 404 réponses « objet introuvable »).
Lecteurs actuels	Nombre actuel approximatif d'accès servis. Lorsqu'une réponse avec un objet d'en-tête Content-Length est en cours de téléchargement, les échecs actuels et les valeurs des lecteurs actuels sont généralement 1. Lorsqu'un objet de réponse fragmentée est téléchargé, la valeur d'erreur actuelle est généralement 1, mais la valeur des lecteurs actuels est généralement 0, car la réponse fragmentée qui est fournie au client ne provient pas des tampons de mise en cache intégrés.
Échecs actuels	Nombre actuel de requêtes qui ont entraîné une absence de cache et une extraction à partir du serveur d'origine. Cette valeur est généralement 0 ou 1. Si l'option Interroger chaque fois est activée pour un groupe de contenus, le nombre peut être supérieur à 1.

Propriétés	Spécifications
Accès	Nombre d'accès au cache pour cet objet.
Absences	Nombre d'échecs de cache pour cet objet.
Format de compression	Type de compression appliqué à cet objet. Les formats de compression incluent gzip, deflate, compress et pack200-gzip.
Version HTTP en réponse	Version de HTTP utilisée pour envoyer la réponse.
Faible `etag` présent en réponse	`etag` Les en-têtes forts changent si les bits d'une entité changent. Les en-têtes forts sont basés sur les valeurs d'octet d'un objet. `etag` Les en-têtes faibles changent si la signification d'une entité change. Les `etag` valeurs faibles sont basées sur l'identité sémantique. `etags` Les valeurs faibles commencent par un « W ».
Cellule marqueur négatif	Un objet marqueur peut être mis en cache, mais il ne répond pas encore à tous les critères pour être mis en cache. Par exemple, l'objet peut dépasser la taille de réponse maximale pour le groupe de contenus. Une cellule de marqueur est créée pour les objets de ce type. La prochaine fois qu'un utilisateur envoie une requête pour cet objet, une absence de cache est servie.
Marqueur de motif créé	La raison pour laquelle une cellule de marqueur a été créée (par exemple, « En attente de minhit », « Les données de réponse Content-length ne sont pas dans la limite de taille du groupe »).
Sondage automatique à chaque fois	Si le cache intégré reçoit une réponse OK 200 déjà expirée avec des validateurs (soit les en-têtes Last Modified ou les en-têtes de `ETag` réponse), il stocke la réponse et la marque comme auto-PET (interrogation automatique à chaque fois).

Propriétés	Spécifications
Citrix ADC Etag inséré dans la réponse	Variante de l' `ETag` en-tête généré par l'appliance Citrix ADC. La valeur YES apparaît si Citrix ADC insère un `Etag` dans la réponse.
Réponse complète présente dans le cache	Indique s'il s'agit d'une réponse complète.
IP de destination vérifiée par DNS	Indique si la résolution DNS a été effectuée lors du stockage de l'objet.
Objet stocké via un proxy de transfert de cache	Indique si cette réponse a été stockée en raison d'un proxy de transfert configuré dans le cache intégré.
L'objet est un fichier de base Delta	Une réponse qui est compressée en delta.
En attente de minhits	Indique si ce groupe de contenu requiert un nombre minimal de serveurs d'origine touchés avant la mise en cache d'une réponse.
Nombre de minhit	Si ce groupe de contenu nécessite un nombre minimal de serveurs d'origine touchés avant de mettre en cache un objet, ce champ affiche le nombre d'accès reçus jusqu'à présent.
Méthode de requête HTTP	Méthode, GET ou POST, utilisée dans la requête qui a obtenu cet objet.
Stocké par stratégie	Nom de la stratégie de mise en cache qui a provoqué le stockage de cet objet. La valeur NOT AVAILABLE indique que la stratégie a été désactivée ou supprimée. La valeur NONE indique que l'objet ne correspond pas à une stratégie visible, mais qu'il a été stocké selon des critères internes de mise en cache.

Propriétés	Spécifications
Des métadonnées de pare-feu d'application existent	Ce paramètre est utilisé lorsque le pare-feu de l'application et le cache intégré sont tous les deux activés. Le pare-feu de l'application analyse le contenu d'une page de réponse, stocke ses métadonnées (par exemple, les URL et les formulaires contenus dans la page) et exporte les métadonnées avec la réponse dans le cache. Le cache stocke la page et les métadonnées, et lorsque le cache sert la page, il renvoie les métadonnées à la session de la requête.
Objet de légende HTTP, nom, type, réponse	Ces cellules indiquent si ces données ont été stockées à la suite d'une expression de légende HTTP et fournissent des informations sur divers aspects de la légende et la réponse correspondante. Pour plus d'informations sur les légendes HTTP, voir « Légendes HTTP ».

Rechercher des réponses mises en cache particulières

Vous pouvez trouver des éléments individuels dans le cache en fonction de critères de recherche. Il existe différentes méthodes pour trouver les éléments mis en cache, selon que le groupe de contenu contenant les données utilise des sélecteurs d'accès et d'invalidation, comme suit :

Si le groupe de contenu utilise des sélecteurs, vous ne pouvez effectuer la recherche qu'à l'aide de l'ID de localisateur de l'élément mis en cache.

Si le groupe de contenu n'utilise pas de sélecteurs, vous effectuez la recherche en utilisant des critères tels que l'URL, l'hôte, le nom du groupe de contenu.

Lorsque vous recherchez une réponse mise en cache, vous pouvez localiser certains éléments par URL et hôte. Si la réponse se trouve dans un groupe de contenu qui utilise un sélecteur, vous ne pouvez la trouver qu'à l'aide d'un numéro de localisateur (par exemple, 0x00000000ad7af00000050). Pour enregistrer un numéro de localisateur en vue d'une utilisation ultérieure, cliquez avec le bouton droit sur l'entrée et sélectionnez Copier. Pour plus d'informations sur les sélecteurs, consultez “Configuration des sélecteurs et des groupes de contenu de base.”

Pour afficher les réponses mises en cache dans des groupes de contenu qui n'ont pas de sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show cache object [-locator <positiveInteger>] | [(-url <URL> (-host <
hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET
 | POST ]))| [-httpStatus<positive integer>] | -group <contentGroupName> |
-ignoreMarkerObjects (ON | OFF)| -includeNotReadyObjects (ON | OFF)]
```

Pour afficher les réponses mises en cache dans des groupes de contenu dotés d'un sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show cache object -locator <locatorString> MarkerObjects ( ON | OFF )| -
includeNotReadyObjects ( ON | OFF )| [-httpStatus<positive integer>]
```

Pour afficher les réponses mises en cache dans des groupes de contenu qui n'ont pas de sélecteur à l'aide de l'interface graphique graphique

Accédez à **Optimisation** > **Mise en cache intégrée> Objets**de cache, cliquez sur**Rechercher**et définissez les critères de recherche pour afficher la réponse requise mise en cache.

Si vous n'avez pas encore configuré de groupes de contenu, tous les objets se trouvent dans le groupe Par défaut.

Pour afficher les réponses mises en cache dans des groupes de contenu dotés d'un sélecteur à l'aide de l'interface graphique graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Objets de cache**, cliquez sur **Rechercher** et définissez les critères de recherche du sélecteur pour afficher la réponse mise en cache requise.

Afficher les statistiques du cache

Le tableau suivant récapitule les statistiques du cache.

Compteur

Spécifications

Affichage des statistiques du cache

Mis à jour : 2013-10-28

Le tableau suivant récapitule les statistiques détaillées du cache que vous pouvez consulter.

Compteur	Spécifie
Accès	Réponses trouvées dans et servies à partir du cache intégré. Inclut des objets statiques tels que des fichiers image, des pages avec des codes d'état 200, 203, 300, 301, 302, 304, 307, 403, 404, 410 et des réponses qui correspondent à une stratégie définie par l'utilisateur avec une action CACHE.
Absences	Requêtes HTTP interceptées où la réponse a finalement été récupérée à partir du serveur d'origine.
Demandes	Nombre total d'accès au cache et nombre total d'échecs de cache.
Accès non-304	Si l'utilisateur demande un élément plusieurs fois et que l'élément du cache est inchangé depuis la dernière fois que l'appliance Citrix ADC l'a servi, l'appliance Citrix ADC fournit une réponse 304 au lieu de l'objet mis en cache. Cette statistique indique le nombre d'éléments que l'appliance Citrix ADC a servis à partir du cache, à l'exclusion des réponses 304.
304 accès	Nombre de 304 réponses (objet non modifié) fournies par l'appliance Citrix ADC à partir du cache.
Taux de succès 304 (%)	Pourcentage de 304 réponses fournies par l'appliance Citrix ADC, par rapport aux autres réponses.
Taux de succès (%)	Pourcentage de réponses fournies par l'appliance Citrix ADC à partir du cache (accès au cache) par rapport aux réponses qui n'ont pas pu être fournies à partir du cache.
Bande passante d'origine enregistrée (%)	Estimation de la capacité de traitement enregistrée par l'appliance Citrix ADC sur le serveur d'origine en raison du service de réponses provenant du cache.

Compteur	Spécifie
Octets servis par Citrix ADC	Nombre total d'octets que l'appliance Citrix ADC a servis à partir du serveur d'origine et du cache.
Octets servis par le cache	Nombre total d'octets que l'appliance Citrix ADC a servis à partir du cache.
Taux d'octets de succès (%)	Pourcentage de données fournies par l'appliance Citrix ADC à partir du cache, par rapport à toutes les données de toutes les réponses envoyées.
Octets compressés à partir du cache	Quantité de données, en octets, que l'appliance Citrix ADC a servi sous forme compressée.
Ravages de stockage	Si l'appliance Citrix ADC ne trouve pas d'objet demandé dans le cache, il récupère l'objet à partir du serveur d'origine. Ceci connu sous le nom de « cache miss » (échec d'accès au cache). Une absence de cache stockable peut être stockée dans le cache.
Échecs non stockables	Un défaut de mémoire cache non stockable ne peut pas être stocké dans le cache.
Absences	Toutes les absences du cache.
Revalidations	Le paramètre Max-Age dans un en-tête Cache-Control détermine, en nombre de secondes, lorsqu'un cache intermédiaire doit revalider le contenu avec le cache intégré avant de le diffuser à l'utilisateur. Pour plus d'informations, voir "Insertion d'un en-tête de contrôle de cache".
Revalidations réussies	Nombre de revalidations effectuées. Pour plus d'informations, voir "Insertion d'un en-tête de contrôle de cache".

Compteur	Spécifie
Conversions en demande conditionnelle	Une demande d'agent utilisateur pour un objet PET mis en cache est toujours convertie en requête conditionnelle et envoyée au serveur d'origine. Pour plus d'informations, reportez-vous à la section "Interroger le serveur d'origine chaque fois qu'une demande est reçue."
Tau d'échec de cache stockables (%)	Nombre d'échecs de cache stockable en pourcentage des échecs de cache non stockable.
Taux de reprise réussi (%)	Revalidations réussies en pourcentage de toutes les tentatives de revalidation. Pour plus d'informations, voir "Insertion d'un en-tête de contrôle de cache".
Expire au dernier octet	Nombre de fois où le cache a expiré le contenu immédiatement après avoir reçu le dernier octet corporel. Ne s'applique qu'aux réponses positives, comme décrit dans le tableau « Accès au cache et échecs. « Pour plus d'informations, consultez « Exemple d'optimisation des performances. »
Écarte du cache flash	Si vous activez Flash Cache, le cache n'autorise qu'une seule requête pour atteindre le serveur, éliminant ainsi les foules flash. Cette statistique indique le nombre de requêtes Flash Cache qui se sont soldées par des échecs d'accès au cache. Pour plus d'informations, « Queuing Requests to the Cache ».
`Flashcache` hits	Nombre de requêtes Flash Cache qui ont été des accès au cache. Pour plus d'informations, voir « Queuing Requests to the Cache ».

Compteur	Spécifie
Demandes inval paramétrées	Demandes qui correspondent à une stratégie avec une action d'invalidation (INVAL) et un groupe de contenu qui utilise un sélecteur d'invalidation ou des paramètres pour expirer sélectivement les objets mis en cache dans le groupe.
Demandes d'inval complètes	Demandes qui correspondent à une stratégie d'invalidation dans laquelle le paramètre InvalGroups est configuré et expire un ou plusieurs groupes de contenu.
Demandes inval	Demandes qui correspondent à une stratégie d'invalidation et entraînent l'expiration de réponses mises en cache spécifiques ou de groupes de contenu entiers.
Demandes paramétrées	Nombre de demandes de cache traitées à l'aide d'une stratégie avec un groupe de contenu paramétré.
Résultats paramétrés non 304	Nombre de demandes de cache traitées à l'aide d'une stratégie avec un groupe de contenu paramétré, où une réponse mise en cache complète a été trouvée et où la réponse n'était pas une réponse 304 (objet non mis à jour).
304 résultats paramétrés	Nombre de demandes de cache traitées à l'aide d'une stratégie avec un groupe de contenu paramétré, où l'objet mis en cache a été trouvé et où l'objet était une réponse 304 (objet non mis à jour).
Nombre total de résultats paramétrés	Nombre de requêtes de cache traitées à l'aide d'une stratégie avec un groupe de contenu paramétré, où l'objet mis en cache a été trouvé.
Taux de succès paramétré 304 (%)	Pourcentage de 304 réponses (objet non mis à jour) trouvées à l'aide d'une stratégie paramétrée, par rapport à tous les accès au cache.

Compteur	Spécifie
Sondage à chaque demande	Si l'option Poll chaque fois est activée, l'appliance Citrix ADC consulte toujours le serveur d'origine avant de servir un objet stocké. Pour plus d'informations, reportez-vous à la section "Interroger le serveur d'origine chaque fois qu'une demande est reçue."
Sondage à chaque fois que des visites	Nombre de fois qu'un accès au cache a été trouvé à l'aide de la méthode Poll Every Time. Pour plus d'informations, reportez-vous à la section "Interroger le serveur d'origine chaque fois qu'une demande est reçue."
Sondage à chaque fois que le taux de succès (%)	Pourcentage d'accès au cache à l'aide de la méthode Poll Every Time, par rapport à toutes les recherches d'objets mis en cache à l'aide de l'option Poll Every Time. Pour plus d'informations, reportez-vous à la section "Interroger le serveur d'origine chaque fois qu'une demande est reçue."
Mémoire maximale (Ko)	Quantité maximale de mémoire allouée au cache dans l'appliance Citrix ADC. Pour plus d'informations, reportez-vous à "Configuration des attributs globaux pour la mise en cache."
Valeur maximale de la mémoire active (Ko)	Quantité maximale de mémoire (valeur active) qui sera définie après que la mémoire est réellement allouée au cache. Pour plus d'informations, reportez-vous à "Procédure de configuration de la fonctionnalité de mise en cache intégrée d'une appliance Citrix ADC pour différents scénarios."
Mémoire utilisée (Ko)	Quantité de mémoire réellement utilisée.
Échecs d'allocation de mémoire	Nombre de tentatives d'utilisation de la mémoire dans le but de stocker une réponse dans le cache.

Compteur	Spécifie
Réponse la plus importante à ce jour	Réponse la plus importante en octets trouvés dans le cache ou le serveur d'origine et envoyée au client.
Objets mis en cache	Nombre d'objets dans le cache, y compris les réponses qui n'ont pas encore été entièrement téléchargées et les réponses qui ont expiré mais qui n'ont pas encore été virées.
Objets marqueurs	Les objets marqueurs sont créés lorsqu'une réponse dépasse la taille de réponse maximale ou minimale du groupe de contenus ou n'a pas encore reçu le nombre minimum de résultats pour le groupe de contenus.
Succès en cours de service	Nombre d'accès qui ont été servis à partir du cache.
Manque en cours de traitement	Réponses récupérées à partir du serveur d'origine, stockées dans le cache, puis servies. Devrait évaluer le nombre approximatif d'échecs stockables. N'inclut pas les échecs non stockables.

Pour afficher les statistiques du cache récapitulatif à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat cache
```

Pour afficher des statistiques de cache spécifiques à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 stat cache -detail
2
3     > stat cache -detail
4     Integrated Cache Statistics - Detail
5     Integrated Cache Statistics - Summary
6                                                 Rate (/s)
                                                     Total
7     Hits                                              0
                            0
8     Misses                                            0
                            0
```



```
 9      Requests                                                 0
                            0
10      Hit ratio(%)                                            --
                            0
11      Origin bandwidth saved(%)                               --
                            0
12      Cached objects                                          --
                            0
13      Marker objects                                          --
                            0
14                                                  Rate (/s)
                                                       Total
15      Requests                                                 0
                            0
16      Hit Statistics
17                                                  Rate (/s)
                                                       Total
18      Non-304 hits                                             0
                            0
19      304 hits                                                 0
                            0
20      Sql hits                                                 0
                            0
21      Hits                                                     0
                            0
22      304 hit ratio(%)                                        --
                            0
23      Hit ratio(%)                                            --
                            0
24      Origin bandwidth saved(%)                               --
                            0
25
26      Byte Statistics
27                                                  Rate (/s)
                                                       Total
28      Bytes served by Citrix ADC                             648
           55379204
29      Bytes served by cache                                    0
                            0
30      Byte hit ratio(%)                                       --
                            0
31      Compressed bytes from cache                              0
                            0
32      Miss Statistics
33                                                  Rate (/s)
```



```
                                                    Total
34      Storable misses                                 0
                            0
35      Non-storable misses                             0
                            0
36      Misses                                          0
                            0
37      Revalidations                                   0
                            0
38      Successful revalidations                        0
                            0
39      Conversions to conditional req                  0
                            0
40      Storable miss ratio(%)                         --
                            0
41      Successful reval ratio(%)                      --
                            0
42      Flashcache Statistics
43                                              Rate (/s)
                                                    Total
44      Expire at last byte                             0
                            0
45      Flashcache misses                               0
                            0
46      Flashcache hits                                 0
                            0
47
48      Invalidation Statistics
49                                              Rate (/s)
                                                    Total
50      Parameterized inval requests                    0
                            0
51      Full inval requests                             0
                            0
52      Inval requests                                  0
                            0
53
54      Parameterized Caching Statistics
55                                              Rate (/s)
                                                    Total
56      Parameterized requests                          0
                            0
57      Parameterized non-304 hits                      0
                            0
58      Parameterized 304 hits                          0
```



```
                              0
59      Total parameterized hits                              0
                              0
60      Parameterized 304 hit ratio(%)                       --
                              0
61
62      Poll Every Time (PET) Statistics
63                                                  Rate (/s)
                                                       Total
64      Poll every time requests                              0
                              0
65      Poll every time hits                                  0
                              0
66      Poll every time hit ratio(%)                         --
                              0
67      Memory Usage Statistics
68                                                      Total
69      Maximum memory(KB)                                    0
70      Maximum memory active value(KB)                       0
71      Utilized memory(KB)                                   0
72      Memory allocation failures                            0
73      Largest response so far(B)                            0
74      Cached objects                                        0
75      Marker objects                                        0
76      Hits being served                                     0
77      Misses being handled                                  0
78       Done
79  <!--NeedCopy-->
```

Pour afficher les statistiques de cache récapitulatif à l'aide de l'interface graphique

1. Cliquez sur l'onglet **Tableau de bord** en haut de la page.
2. Faites défiler la page jusqu'à la section Mise en cache intégrée de la fenêtre.
3. Pour afficher des statistiques détaillées, cliquez sur le lien Plus… au bas du tableau.

Pour afficher des statistiques de cache spécifiques à l'aide de l'interface graphique

1. Cliquez sur l'onglet Rapports en haut de la page.
2. Sous Rapports intégrés, développez Cache intégré, puis cliquez sur le rapport contenant les statistiques que vous souhaitez afficher.
3. Pour enregistrer le rapport en tant que modèle, cliquez sur Enregistrer sous et nommez le rapport. Le rapport enregistré apparaît sous Rapports personnalisés.

Améliorer les performances du cache

January 21, 2021

Vous pouvez améliorer les performances du cache intégré, notamment en gérant les demandes simultanées pour les mêmes données mises en cache, en évitant les retards associés à l'actualisation des réponses mises en cache depuis le serveur d'origine et en veillant à ce qu'une réponse soit demandée suffisamment souvent pour mériter la mise en cache.

Réduire les foules flash

Les foules Flash se produisent lorsque de nombreux utilisateurs demandent simultanément les mêmes données. Les requêtes d'une foule flash peuvent devenir des échecs de cache si vous avez configuré le cache pour diffuser des appels uniquement après le téléchargement de l'objet entier.

Les techniques suivantes peuvent réduire ou éliminer les foules flash :

- **PREFETCH** : Actualise une réponse positive avant qu'elle n'expire pour s'assurer qu'elle ne devienne jamais périmée ou inactive. Pour plus d'informations, consultez la section « Actualisation d'une réponse avant l'expiration ».
- Mise en**mémoire tampon du cache** : Commence à fournir une réponse à plusieurs clients lorsqu'il reçoit l'en-tête de réponse du serveur d'origine, plutôt que d'attendre que la réponse entière soit téléchargée. La seule limite du nombre de clients pouvant télécharger une réponse simultanément est les ressources système disponibles. L'appliance Citrix ADC télécharge et envoie des réponses même si le client qui a initié le téléchargement s'arrête avant la fin du téléchargement. Si la réponse dépasse la taille du cache ou si la réponse est tronquée, le cache cesse de stocker la réponse, mais le service aux clients n'est pas interrompu.
- **Flash Cache :** Flash Cache met en file d'attente les demandes vers le cache et n'autorise qu'une seule requête à atteindre le serveur à la fois.

Pour plus d'informations, consultez la section « Demandes de mise en file d'attente vers le cache ».

Actualiser une réponse avant l'expiration

Pour s'assurer qu'une réponse mise en cache est fraîche chaque fois qu'elle est nécessaire, l'option PREFETCH actualise une réponse avant son délai d'expiration calculé. L'intervalle de préextraction est calculé après réception de la première demande client. À partir de ce moment, l'appliance Citrix ADC actualise la réponse mise en cache à un intervalle de temps que vous configurez dans le paramètre PREFETCH.

Ce paramètre est utile pour les données fréquemment mises à jour entre les demandes. Il ne s'applique pas aux réponses négatives (par exemple, 404 messages).

Pour configurer la préextraction d'un groupe de contenus à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cache contentgroup <name> -prefetch YES [-prefetchPeriod <seconds> | -
prefetchPeriodMilliSec <milliseconds>] [-prefetchMaxPending <positiveInteger
>]
```

*Pour configurer la préextraction d'un groupe de contenus à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu**, puis sélectionnez le **groupe de contenu**.

Sous l'onglet **Autres**, dans le groupe Flash Foule et Pré-extraction, sélectionnez l'option **Pré-extraction**, puis spécifiez les valeurs dans les zones de texte Intervalle et Nombre maximal de préextraction en attente.

Demandes de file d'attente vers le cache

L'option Flash Cache met en file d'attente les demandes qui arrivent simultanément (une foule flash), récupère la réponse et la distribue à tous les clients dont les demandes sont dans la file d'attente. Si, au cours de ce processus, la réponse devient non mise en cache, l'appliance Citrix ADC cesse de fournir la réponse à partir du cache et sert à la place la réponse du serveur d'origine aux clients mis en file d'attente. Si la réponse n'est pas disponible, les clients reçoivent un message d'erreur.

Flash Cache est désactivé par défaut. Vous ne pouvez pas activer Poll Every Time (PET) et Flash Cache sur le même groupe de contenu.

Un inconvénient de Flash Cache est que si le serveur répond avec une erreur (par exemple, un 404 qui est rapidement corrigé), l'erreur est vendue aux clients en attente.

> **Remarque** :
> si Flash Cache est activé, dans certains cas, l'appliance Citrix ADC ne parvient pas à faire correspondre correctement l'en-tête Accept-Encoding dans la demande client avec l'en-tête Content-Encoding dans la réponse. L'appliance Citrix ADC peut supposer que ces en-têtes correspondent et servent par erreur un appel. Pour contourner le problème, vous pouvez configurer des stratégies de mise en cache intégrée pour interdire le service d'accès aux clients qui n'ont pas d'en-tête Accept-Encoding approprié.

Pour activer Flash Cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cache contentgroup <contentGroupName> -flashcache yes
```

Pour activer Flash Cache à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu**, puis sélectionnez le groupe de contenu.

Sous l'onglet **Autres**, dans le groupe Flash Crowd et Prefetch, sélectionnez l'option **Prefetch**.

Mettre en cache une réponse après qu'un client arrête un téléchargement

Vous pouvez définir le paramètre Quick Abort pour continuer à mettre en cache une réponse, même si le client arrête une demande avant que la réponse ne soit dans le cache.

Si la taille de la réponse téléchargée est inférieure ou égale à la taille d'Abort rapide, l'appliance Citrix ADC cesse de télécharger la réponse. Si vous définissez le paramètre Quick Abort sur 0, tous les téléchargements sont interrompus.

Pour configurer la taille d'abandon rapide à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cache contentgroup <name> -quickAbortSize <integerInKBytes>
```

Pour configurer la taille d'abandon rapide à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu**, puis sélectionnez le groupe de contenu.
2. Sous l'onglet **Mémoire**, définissez la valeur appropriée dans Quick Abort : Continuer la mise en cache si plus de zone de texte.

Exiger un nombre minimum d'accès au serveur avant la mise en cache

Vous pouvez configurer le nombre minimum de fois qu'une réponse doit être trouvée sur le serveur d'origine avant qu'elle ne puisse être mise en cache. Vous devez envisager d'augmenter le nombre minimum d'accès si la mémoire cache se remplit rapidement et a un taux d'accès inférieur à ce qui était prévu.

La valeur par défaut du nombre minimum d'accès est 0. Cette valeur met en cache la réponse après la première requête.

Pour configurer le nombre minimum d'accès requis avant la mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cache contentgroup <name> -minhits <positiveInteger>
```

Pour configurer le nombre minimum d'accès requis avant la mise en cache à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu**, puis sélectionnez le groupe de contenu.
2. Sous l'onglet **Mémoire**, définissez la valeur appropriée dans Ne pas mettre en cache, si les accès sont inférieurs à la zone de texte.

Exemple d'optimisation des performances

Dans cet exemple, un client accède à un devis boursier. Les cotations boursières sont très dynamiques. Vous configurez le cache intégré pour qu'il serve le même devis de stock aux clients simultanés sans envoyer plusieurs demandes au serveur d'origine. Le devis de stock expire après avoir été téléchargé sur les clients, et la demande suivante est récupérée à partir du serveur d'origine. Cela garantit que le devis est toujours à jour.

La présentation des tâches suivante décrit les étapes de configuration du cache pour l'application de cotation de stock.

Configurer la mise en cache pour une application de cotation d'actions

Créer un groupe de contenus pour les cotations boursières

Pour plus d'informations, reportez-vous à "A propos des groupes de contenu."

Configurez les éléments suivants pour ce groupe de contenu :

1. Sous l'onglet **Méthode d'expiration**, activez la case à cocher Expirer après réception de la réponse complète.
2. Sous l'onglet **Autres**, activez la case à cocher **Flash Cache**, puis cliquez sur **Créer**.
3. Ajoutez une stratégie de cache pour mettre en cache les cotations boursières.

Pour plus d'informations, consultez "Configuration d'une stratégie dans le cache intégré."

Configurez les éléments suivants pour la stratégie

1. Dans les **listes Action et Stocker dans le groupe**, sélectionnez **CACHE**et sélectionnez le groupe que vous avez défini à l'étape précédente.
2. Cliquez sur **Ajouter**et, dans la boîte de dialogue **Ajouter**une expression, configurez une expression qui identifie les demandes de devis, par exemple : http.req.url.contains (« cgi-bin/stockquote.pl »)
3. Activez la stratégie.

Pour plus d'informations, consultez « Liaison globale d'une stratégie de mise en cache intégrée ». Dans cet exemple, vous liez cette stratégie au traitement de remplacement au moment de la requête et définissez la priorité sur une valeur faible.

Configurer les cookies, les en-têtes et l'interrogation

August 20, 2021

Cette rubrique explique comment configurer le cache gère les cookies, les en-têtes HTTP et l'interrogation du serveur d'origine. Cela inclut la modification du comportement par défaut qui provoque la divergence du cache des normes documentées, le remplacement des en-têtes HTTP susceptibles de provoquer l'absence de stockage du contenu mis en cache dans le cache et la configuration du cache pour toujours interroger l'origine pour le contenu mis à jour.

Divergence du comportement du cache par rapport aux normes

Par défaut, le cache intégré respecte les normes RFC suivantes :

- RFC 2616, « HTTP HTTP/1.1 »
- Les comportements de mise en cache décrits dans RFC 2617, « HTTP Authentication : Basic and Digest Access Authentication »
- Le comportement de mise en cache décrit dans RFC 2965, « HTTP State Management Mechanism »

Les stratégies intégrées et les attributs du groupe de contenu par défaut garantissent la conformité avec la plupart de ces normes.

Le comportement du cache intégré par défaut diffère de la spécification comme suit :

- La prise en charge de l'en-tête Vary est limitée. Par défaut, toute réponse contenant un en-tête Vary est considérée comme non mise en cache à moins qu'elle ne soit compressée. Une réponse compressée contient l'encodage de contenu : gzip, content-encoding : deflate, ou content-encoding : pack200-gzip et peut être mis en cache même si elle contient l'en-tête Vary : Accept-encoding.
- Le cache intégré ignore les valeurs des en-têtes cache-control : no-cache et cache-control : private. Par exemple, une réponse contenant cache-control : no-cache=”set-cookie » est traitée comme si la réponse contenait Cache-Control : no-cache. Par défaut, la réponse n'est pas mise en cache.
- Une image (content-type = image/*) est toujours considérée comme pouvant être mise en cache, même si une réponse d'image contient des en-têtes set-cookie ou set-cookie2, ou si une requête d'image contient un en-tête de cookie. Le cache intégré supprime les en-têtes set-cookie et set-cookie2 d'une réponse avant de la mettre en cache. Cela diffère de la RFC 2965. Vous pouvez configurer un comportement compatible RFC comme suit :

```
1 add cache policy rfc_compliant_images_policy -rule "http.res.header.set
    -cookie2.exists || http.res.header.set-cookie.exists" -action
    NOCACHE
```



```
2
3
4 bind cache global rfc_compliant_images_policy -priority 100 -type
     REQ_OVERRIDE
5 <!--NeedCopy-->
```

- Les en-têtes de contrôle de cache suivants dans une requête forçent un cache compatible RFC à recharger une réponse mise en cache à partir du serveur d'origine :

```
Cache-control: max-age=0
```

```
Cache-control: no-cache
```

Pour se protéger contre les attaques par déni de service, ce comportement n'est pas le comportement par défaut.

- Par défaut, le module de mise en cache considère une réponse comme pouvant être mise en cache à moins qu'un état d'en-tête de réponse n'en soit autrement. Pour rendre ce comportement conforme à la RFC 2616, définissez `-weakPosRelExpiry` et `-weakNegResExpiry` sur 0 pour tous les groupes de contenu.

Supprimer les cookies d'une réponse

Les cookies sont souvent personnalisés pour un utilisateur et ne doivent généralement pas être mis en cache. Le `Remove Response Cookies` paramètre supprime `Set-Cookie and Set-Cookie2` les en-têtes avant la mise en cache d'une réponse. Par défaut, l'option `Remove Response Cookies` d'un groupe de contenu empêche la mise en cache des réponses avec les en-têtes `Set-Cookie` ou `Set-Cookie2`.

> **Remarque :**
> lorsque les images sont mises en cache, le comportement intégré consiste à supprimer `Set-Cookie2` les en-têtes `Set-Cookie` et avant la mise en cache, quelle que soit la façon dont le groupe de contenu est configuré.
>
> Citrix vous recommande d'accepter la valeur par défaut `Remove Response Cookies` pour chaque groupe de contenu qui stocke des réponses intégrées, par exemple les images.

`Remove Response Cookies` Pour configurer un groupe de contenu à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
set cache contentgroup <name> -removeCookies YES
```


Configurer Supprimer les cookies de réponse pour un groupe de contenu à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu**, puis sélectionnez le groupe de contenu.
2. Sous l'onglet **Autres**, dans le groupe **Paramètres**, sélectionnez l'option Supprimer les cookies de réponse.

Insertion d'en-têtes HTTP au temps de réponse

Le cache intégré peut insérer des en-têtes HTTP dans les réponses résultant de requêtes de cache. L'appliance Citrix ADC ne modifie pas les en-têtes dans les réponses résultant d'erreurs de cache.

Le tableau suivant décrit les en-têtes que vous pouvez insérer dans une réponse.

En-tête	Spécifications
Âge	Fournit l'âge de la réponse en secondes, calculé à partir du moment où la réponse a été générée sur le serveur d'origine. Par défaut, le cache insère un en-tête Age pour chaque réponse fournie à partir du cache.
via	Répertorie les protocoles et les destinataires entre les points de départ et de fin d'une demande ou d'une réponse. L'appliance Citrix ADC insère un en-tête Via dans chaque réponse qu'elle sert à partir du cache. La valeur par défaut de l'en-tête inséré est "NS-CACHE-9.2: last octet of the Citrix ADC IP address." Pour plus d'informations, reportez-vous à "Configuration des attributs globaux pour la mise en cache."

En-tête	Spécifications
Tag	Le cache prend en charge la validation des réponses en utilisant Last Modified et Tag les en-têtes pour déterminer si une réponse est obsolète. Le cache insère un Tag dans une réponse uniquement s'il met en cache la réponse et que le serveur d'origine n'a pas inséré son propre Tag en-tête. La Tag valeur est un nombre unique arbitraire. La Tag valeur d'une réponse change si elle est actualisée à partir du serveur d'origine, mais elle reste la même si le serveur envoie une réponse 304 (objet non mis à jour). Les serveurs Origin ne génèrent généralement pas de validateurs pour le contenu dynamique car le contenu dynamique est considéré comme non mis en cache. Vous pouvez remplacer ce comportement. Avec l'insertion d' Tag en-tête, le cache est autorisé à ne pas fournir de réponses complètes. Au lieu de cela, l'agent utilisateur est requis pour mettre en cache la réponse dynamique envoyée par le cache intégré la première fois. Pour forcer un agent utilisateur à mettre en cache une réponse, vous configurez le cache intégré pour insérer un Tag en-tête et remplacer l'en-tête Cache-Control fourni par l'origine.

En-tête	Spécifications
Cache-Control	En règle générale, l'appliance Citrix ADC ne modifie pas les en-têtes de mise en cache dans les réponses fournies par le serveur d'origine. Si le serveur d'origine envoie une réponse étiquetée comme non mise en cache, le client traite la réponse comme non mise en cache, même si l'appliance Citrix ADC met en cache la réponse. Pour mettre en cache les réponses dynamiques dans un agent utilisateur, vous pouvez remplacer les en-têtes Cache-Control à partir du serveur d'origine. Cela s'applique uniquement aux agents utilisateur et aux autres caches intermédiaires. Ils n'affectent pas le cache intégré.

En-tête	Spécifications
Âge	Fournit l'âge de la réponse en secondes, calculé à partir du moment où la réponse a été générée sur le serveur d'origine. Par défaut, le cache insère un en-tête Age pour chaque réponse fournie à partir du cache.
via	Répertorie les protocoles et les destinataires entre les points de départ et de fin d'une demande ou d'une réponse. L'appliance Citrix ADC insère un en-tête Via dans chaque réponse qu'elle sert à partir du cache. La valeur par défaut de l'en-tête inséré est "NS-CACHE-9.2: last octet of the Citrix ADC IP address." Pour plus d'informations, reportez-vous à "Configuration des attributs globaux pour la mise en cache."

En-tête	Spécifications
Tag	Le cache prend en charge la validation des réponses à l'aide des en-têtes Last Modified et Tag pour déterminer si une réponse est obsolète. Le cache insère un Tag dans une réponse uniquement s'il met en cache la réponse et que le serveur d'origine n'a pas inséré son propre Tag en-tête. La Tag valeur est un nombre unique arbitraire. La Tag valeur d'une réponse change si elle est actualisée à partir du serveur d'origine, mais elle reste la même si le serveur envoie une réponse 304 (objet non mis à jour). Les serveurs Origin ne génèrent généralement pas de validateurs pour le contenu dynamique car le contenu dynamique est considéré comme non mis en cache. Vous pouvez remplacer ce comportement. Avec l'insertion d' Tag en-tête, le cache est autorisé à ne pas fournir de réponses complètes. Au lieu de cela, l'agent utilisateur est requis pour mettre en cache la réponse dynamique envoyée par le cache intégré la première fois. Pour forcer un agent utilisateur à mettre en cache une réponse, vous configurez le cache intégré pour insérer un Tag en-tête et remplacer l'en-tête Cache-Control fourni par l'origine.

En-tête	Spécifications
Cache-Control	En règle générale, l'appliance Citrix ADC ne modifie pas les en-têtes de mise en cache dans les réponses fournies par le serveur d'origine. Si le serveur d'origine envoie une réponse étiquetée comme non mise en cache, le client traite la réponse comme non mise en cache, même si l'appliance Citrix ADC met en cache la réponse. Pour mettre en cache les réponses dynamiques dans un agent utilisateur, vous pouvez remplacer les en-têtes Cache-Control à partir du serveur d'origine. Cela s'applique uniquement aux agents utilisateur et aux autres caches intermédiaires. Ils n'affectent pas le cache intégré.

Insérer un âge, via, ou un en-tête de balise

Les procédures suivantes décrivent comment insérer des en-têtes Age, Via et ETag.

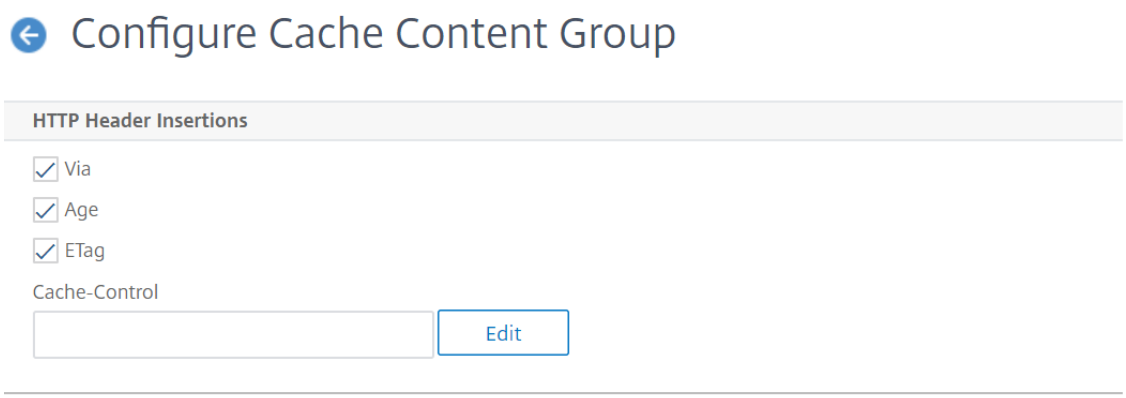
Insérez un en-tête Age, Via ou Etag à l'aide de l'interface de commande Citrix ADC :

À l'invite de commandes, tapez :

```
set cache contentgroup <name> -insertVia YES -insertAge YES -insertETag YES
```

Configurer l'en-tête Age, Via ou Etag à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu,** puis sélectionnez le **groupe de contenu**.
2. Sous l'onglet **Autres**, dans le groupe Insertions d'en-tête HTTP, sélectionnez les options **Via**, **Age** ou **ETag**, selon le cas.
3. Les valeurs des autres types d'en-tête sont calculées automatiquement. Vous configurez la valeur Via dans les paramètres principaux du cache.



Insérer un en-tête de contrôle de cache

Lorsque le cache intégré remplace un en-tête Cache-Control inséré par le serveur d'origine, il remplace également l'en-tête Expires. Le nouvel en-tête Expires contient un délai d'expiration dans le passé. Cela garantit que les clients HTTP/1.0 et les caches (qui ne comprennent pas l'en-tête Cache-Control) ne mettent pas en cache le contenu.

Insérer un en-tête de contrôle cache à l'aide de l'interface de commande Citrix ADC

À l'invite de commandes, tapez :

```
set cache contentgroup <name> -cacheControl <value>
```

Insérer un en-tête de contrôle de cache à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu** et
   a) Cliquez sur **l'onglet Méthode d'expiration**, désactivez les paramètres heuristiques et d'expiration par défaut et définissez la valeur correspondante dans la zone de texte Expirer le contenu après.
   b) Cliquez sur l'onglet **Autres** et tapez l'en-tête à insérer dans la zone de texte Contrôle du cache. Vous pouvez également cliquer sur Configurer pour définir les directives Cache-Control dans les réponses mises en cache.

Ignorer les en-têtes de contrôle de cache et de pragma dans les requêtes

Par défaut, le module de mise en cache traite les en-têtes Cache-Control et Pragma. Les jetons suivants dans les en-têtes Cache-Control sont traités comme décrit dans la RFC 2616.

- âge max-âge
- max-vicié
- mise en cache seulement-if-cache

- sans cache

Un en-tête Pragma : no-cache dans une requête est traité de la même manière qu'un en-tête Cache-Control : no-cache.

Si vous configurez le module de mise en cache pour ignorer les en-têtes Cache-Control et Pragma, une demande qui contient un en-tête Cache-Control : No-Cache entraîne la récupération de la réponse du serveur d'origine par l'appliance Citrix ADC, mais la réponse mise en cache n'est pas mise à jour. Si le module de mise en cache traite les en-têtes Cache-Control et Pragma, la réponse mise en cache est actualisée.

Le tableau suivant résume les implications de différents paramètres pour ces en-têtes et le paramètre Ignorer la demande de rechargement du navigateur.

Définition des en-têtes Ignorer le contrôle du cache et Pragma	**Paramétrage pour Ignorer la demande de rechargement du navigateur**	**Résultat**
Oui	Oui ou Non	Ignorer les en-têtes Cache-Control et Pragma du client, y compris la directive Cache-Control : no-cache.
Non	Oui	L'en-tête Cache-Control : no-cache produit un défaut de cache, mais une réponse déjà dans le cache n'est pas actualisée.
Non	Non	Une requête qui contient un en-tête Cache-Control : no-cache provoque un échec du cache et la réponse stockée est actualisée.

Pour ignorer les en-têtes Cache-Control et Pragma dans une requête à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cache contentgroup <name> -ignoreReqCachingHdrs YES
```

Pour ignorer les demandes de rechargement du navigateur à l'aide de l'interface de ligne de commande

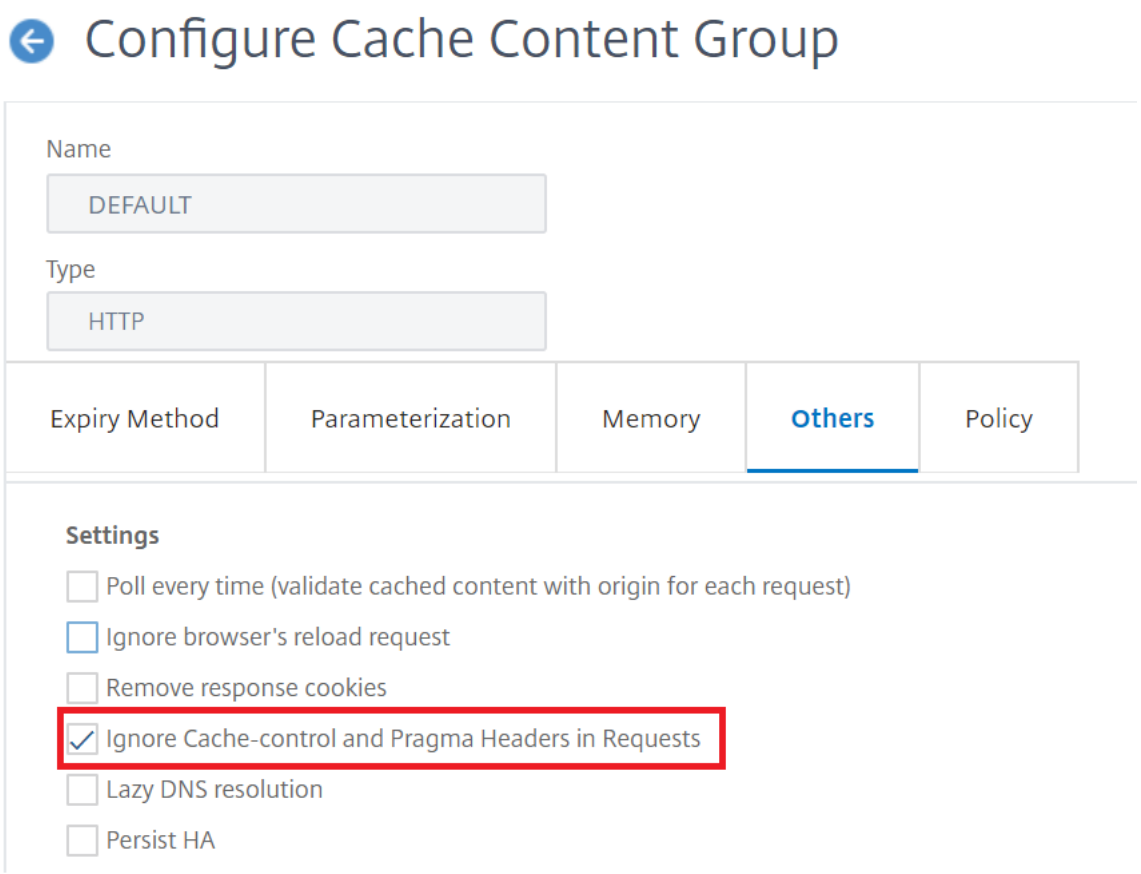
À l'invite de commandes, tapez :


```
set cache contentgroup <name> -ignoreReloadReq NO
```

> **Remarque :**
> Par défaut, le paramètre -IgnoreLoadReq est défini sur YES.

Ignorer les en-têtes Cache-Control et Pragma dans une requête à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu**, puis sélectionnez le groupe de contenu.
2. Sous l'onglet **Autres**, dans le groupe **Paramètres**, sélectionnez **Ignorer le contrôle du cache et En-têtes Pragma dans lesrequêtes** option.



Exemple de stratégie pour ignorer les en-têtes Cache-Control :

Dans l'exemple suivant, vous configurez une stratégie de remplacement au moment de la requête pour mettre en cache les réponses contenant Content-type : image/* quel que soit l'en-tête Cache-Control de la réponse.

Pour configurer une stratégie de remplacement au moment de la requête afin de mettre en cache toutes les réponses avec image/*

Vider le cache à l'aide de l'option Tout invalider.

Configurez une nouvelle stratégie de cache et dirigez la stratégie vers un groupe de contenu particulier. Pour plus d'informations, consultez "Configuration d'une stratégie dans le cache intégré."

Assurez-vous que le groupe de contenu utilisé par la stratégie est configuré pour ignorer les en-têtes Cache-Control, comme décrit dans « Ignorer les en-têtes Cache-Control et Pragma dans les requêtes ».

Liez la stratégie à la banque de stratégies de remplacement au moment de la requête.

Pour plus d'informations, consultez la rubrique Liaison globale d'une stratégie de mise en cache intégrée .

Serveur d'origine du sondage chaque fois qu'une demande est reçue

Vous pouvez configurer l'appliance Citrix ADC pour qu'elle consulte toujours le serveur d'origine avant de servir une réponse stockée. Ceci est connu sous le nom de Poll Every Time (PET). Lorsque l'appliance Citrix ADC consulte le serveur d'origine et que la réponse PET n'a pas expiré, une réponse complète du serveur d'origine n'écrase pas le contenu mis en cache. Cette propriété est utile lors de la diffusion d'un contenu spécifique au client.

Après l'expiration d'une réponse PET, l'appliance Citrix ADC l'actualise lorsque la première réponse complète arrive du serveur d'origine.

La fonction Poll Every Time (PET) fonctionne comme suit :

Pour une réponse mise en cache qui a des validateurs sous la forme d'une balise ou d'un en-tête Dernière modification, si la réponse expire, elle est automatiquement marquée PET et mise en cache.

Vous pouvez configurer PET pour un groupe de contenus.

Si vous configurez un groupe de contenus comme PET, chaque réponse du groupe de contenus est marquée PET. Le groupe de contenu PET peut stocker des réponses qui n'ont pas de validateurs. Les réponses qui sont automatiquement marquées PET sont toujours expirées. Les réponses appartenant à un groupe de contenus PET peuvent expirer après un délai, en fonction de la façon dont vous configurez le groupe de contenus.

Deux types de demandes sont touchés par l'interrogation :

- Demandes conditionnelles : Un client émet une demande conditionnelle pour s'assurer que la réponse qu'il contient est la copie la plus récente. Une demande d'agent utilisateur pour une réponse PET mise en cache est toujours convertie en demande conditionnelle et envoyée au serveur d'origine. Une demande conditionnelle a des validateurs dans les en-têtes If-Modified-Since ou If-NoneMatch. L'en-tête If-Modified-Since contient l'heure de l'en-tête Last Modified. Un en-tête If-Non-Match contient la valeur d'en-tête Tag de la réponse. Si la copie de la réponse du client est fraîche, le serveur d'origine répond avec 304 Not Modified. Si la copie est obsolète, une réponse conditionnelle génère un OK 200 qui contient l'intégralité de la réponse.

- Demandes non conditionnelles : une demande non conditionnelle ne peut générer qu'un 200 OK contenant la réponse entière.

Réponse du serveur Origin	Action
Envoyer la réponse complète	Le serveur d'origine envoie la réponse telle quelle au client. Si la réponse mise en cache a expiré, elle est actualisée.
304 Non modifié	Les valeurs d'en-tête suivantes dans la réponse 304 sont fusionnées avec la réponse mise en cache et la réponse mise en cache est fournie au client : Date, Expire, Age, en-tête Cache-Control Max-Age et jetons S-Maxage
401 Non autorisé ; 400 Demande incorrecte ; 405 Méthode non autorisée ; 406 Non acceptable ; 407 Authentification par proxy requise	La réponse de l'origine est fournie telle quelle au client. La réponse mise en cache n'est pas modifiée.
Toute autre réponse d'erreur, par exemple, 404 Introuvable	La réponse de l'origine est fournie telle quelle au client. La réponse mise en cache est supprimée.

> **Remarque :**
> Le paramètre Sondage à chaque fois traite les réponses affectées comme non stockables.

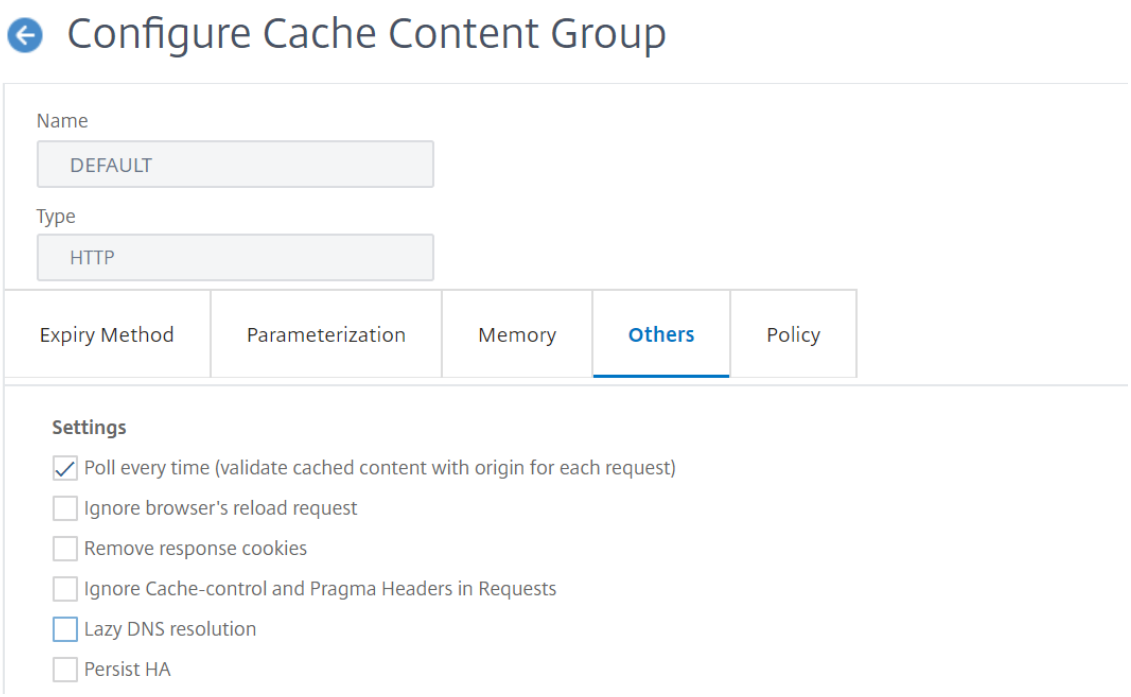
Pour configurer le sondage à chaque fois à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add cache contentgroup <contentGroupName> -pollEveryTime YES
```

Sondage à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu**, puis sélectionnez le groupe de contenu.
2. Sous l'onglet **Autres**, dans le groupe Paramètres, sélectionnez l'option Poll à chaque fois (valider le contenu mis en cache avec l'origine pour chaque requête).



PET et contenu spécifique au client

La fonction PET permet de s'assurer que le contenu est personnalisé pour un client. Par exemple, un site Web qui sert du contenu dans plusieurs langues examine l'en-tête de requête Accept-Language pour sélectionner la langue du contenu qu'il sert. Pour un site Web multilingue où l'anglais est la langue dominante, tout le contenu en anglais peut être mis en cache dans un groupe de contenu PET. Cela garantit que chaque requête va au serveur d'origine pour déterminer la langue de la réponse. Si la réponse est en anglais et que le contenu n'a pas changé, le serveur d'origine peut servir un 304 Not Modified dans le cache.

L'exemple suivant montre des commandes permettant de mettre en cache les réponses anglaises dans un groupe de contenu PET, de configurer une expression nommée qui identifie les réponses anglaises dans le cache et de configurer une stratégie qui utilise ce groupe de contenu et cette expression nommée. En gras est utilisé pour mettre l'accent :

```
1 add cache contentgroup EnglishLanguageGroup -pollEveryTime YES
2 add expression containsENExpression  - rule "http.res.header(\\"Content-
     Language\\").contains(\\"en\\")"
3 add cache policy englishPolicy -rule containsENExpression -action CACHE
      -storeInGroup englishLanguageGroup
4 bind cache policy englishPolicy -priority 100 -precedeDefRules NO
5 <!--NeedCopy-->
```


PET et authentification, autorisation et audit

Outlook Web Access (OWA) est un bon exemple de contenu généré dynamiquement qui bénéficie de PET. Toutes les réponses de courrier (objets *.EML) ont un `ETag` validateur qui leur permet d'être stockées en tant que réponses PET.

Chaque demande de réponse de messagerie se dirige vers le serveur d'origine, même si la réponse est mise en cache. Le serveur d'origine détermine si le demandeur est authentifié et autorisé. Il vérifie également que la réponse existe dans le serveur d'origine. Si tous les résultats sont positifs, le serveur d'origine envoie une réponse 304 Non modifié.

Configurer le cache intégré en tant que proxy de transfert

January 21, 2021

Le cache intégré peut servir de périphérique proxy de transfert qui transmet des demandes à d'autres appliances Citrix ADC ou à d'autres types de serveurs de cache. Vous configurez le cache intégré en tant que proxy de transfert en identifiant les adresses IP du ou des serveurs de cache. Après avoir configuré le proxy de transfert, l'appliance Citrix ADC envoie des demandes contenant l'adresse IP configurée sur au serveur de cache au lieu d'impliquer le cache intégré.

Pour configurer Citrix ADC en tant que proxy de cache de transfert à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add cache forwardProxy <IPAddress> <port>
```

Pour configurer Citrix ADC en tant que proxy de cache de transfert à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Proxy** de transfert et ajoutez un proxy de transfert en spécifiant l'adresse IP et le numéro de port.

Paramètres par défaut pour le cache intégré

August 20, 2021

La fonctionnalité de cache intégré Citrix ADC fournit des stratégies intégrées avec les paramètres par défaut et les paramètres initiaux pour le groupe de contenu par défaut. Les informations de cette section définissent les paramètres des stratégies intégrées et du groupe de contenu par défaut.

Stratégies de mise en cache par défaut

Le cache intégré a des stratégies intégrées. L'appliance Citrix ADC évalue les stratégies dans un ordre particulier, comme indiqué dans les sections suivantes.

Vous pouvez remplacer ces stratégies intégrées par une stratégie définie par l'utilisateur qui est liée à une banque de stratégies de remplacement au moment de la demande ou de remplacement au moment de la réponse.

> **Remarque**
> Si vous avez configuré des stratégies avant la version 9.0 et que vous avez spécifié le paramètre -precedeDefRules lors de la liaison des stratégies, elles sont automatiquement affectées aux points de liaison de dépassement pendant la migration.

Afficher les stratégies par défaut

Les noms de stratégie intégrés commencent par un trait de soulignement (_). Vous pouvez afficher les stratégies intégrées à partir de la ligne de commande et de la console d'administration à l'aide de la commande show cache policy.

Stratégies de demande par défaut

Vous pouvez remplacer les stratégies de temps de demande intégrées suivantes en configurant de nouvelles stratégies et en les liant au point de traitement de remplacement de l'heure de la demande. Dans les stratégies suivantes, notez que l'action MAY_NOCACHE stipule que la transaction est mise en cache uniquement lorsqu'il existe une directive CACHE configurée par l'utilisateur ou intégrée au moment de la réponse.

Les stratégies suivantes sont liées à l'étiquette de stratégie _reqBuiltinDefaults. Ils sont répertoriés par ordre de priorité.

Ne mettez pas en cache une réponse pour une requête qui utilise une méthode autre que GET.

Le nom de la stratégie est _nonGetReq. Ce qui suit est la règle de stratégie :

```
!HTTP.REQ.METHOD.eq(GET)
```

Définissez une action NOCACHE pour une requête dont la valeur d'en-tête contient If-Match ou If-Unmodified-Since.

Le nom de la stratégie est _advancedConditionalReq. Ce qui suit est la règle de stratégie :

```
HTTP.REQ.HEADER("If-Match").EXISTS || HTTP.REQ.HEADER("If-Unmodified-Since"
).EXISTS
```

Définissez une action MAY_NOCACHE pour une requête avec les valeurs d'en-tête suivantes : Cookie, Authorization, Proxy-Authorization ou une requête contenant l'en-tête NTLM ou Negotiate.

Le nom de la stratégie est _personalizedReq. Ce qui suit est la règle de stratégie :

```
HTTP.REQ.HEADER("Cookie").EXISTS || HTTP.REQ.HEADER("Authorization").EXISTS
 || HTTP.REQ.HEADER("Proxy-Authorization").EXISTS || HTTP.REQ.IS_NTLM_OR_NEGOTIATE
```

Stratégies de réponse par défaut

Vous pouvez remplacer les stratégies de temps de réponse par défaut suivantes en configurant de nouvelles stratégies et en les liant au point de traitement de remplacement de temps de réponse.

Les stratégies suivantes sont liées à l'étiquette de stratégie **_resBuiltinDefaults** et sont évaluées dans l'ordre dans lequel elles sont répertoriées :

1. Ne mettez pas en cache les réponses HTTP sauf si elles sont de type 200, 304, 307, 203 ou si les types sont compris entre 400 et 499 ou entre 300 et 302.

   Le nom de la stratégie est **_uncacheableStatusRes**. Ce qui suit est la règle de stratégie :

   ```
   !((HTTP.RES.STATUS.EQ(200))|| (HTTP.RES.STATUS.EQ(304))|| (HTTP.RES.
   STATUS.BETWEEN(400,499))|| (HTTP.RES.STATUS.BETWEEN(300, 302))|| (HTTP.
   RES.STATUS.EQ(307))|| (HTTP.RES.STATUS.EQ(203)))
   ```

2. Ne mettez pas en cache une réponse HTTP si elle a un en-tête Vary avec une valeur autre que Accept-Encoding.

   Le module de compression insère l'en-tête Vary : Accept_Encoding. Le nom de cette expression est **_uncacheableVaryRes**. Ce qui suit est la règle de stratégie :

   ```
   ((HTTP.RES.HEADER("Vary").EXISTS)&& ((HTTP.RES.HEADER("Vary").INSTANCE
   (1).LENGTH > 0)|| (!HTTP.RES.HEADER("Vary").STRIP_END\\_WS.SET_TEXT_MODE
   (IGNORECASE).eq("Accept-Encoding"))))
   ```

3. Ne mettez pas en cache une réponse si sa valeur d'en-tête Cache-Control est No-Cache, No-Store ou Private, ou si l'en-tête Cache-Control n'est pas valide.

   Le nom de la stratégie est **_uncacheableCacheControlRes**. Ce qui suit est la règle de stratégie :

   ```
   ((HTTP.RES.CACHE\\_CONTROL.IS\\_PRIVATE)|| (HTTP.RES.CACHE\\_CONTROL.IS
   \\_NO\\_CACHE)|| (HTTP.RES.CACHE\\_CONTROL.IS\\_NO\\_STORE)|| (HTTP.RES
   .CACHE\\_CONTROL.IS\\_INVALID))
   ```

4. Réponses du cache si l'en-tête Cache-Control a l'une des valeurs suivantes : Public, Must-Revalidate, Proxy-Revalidate, Max-Age, S-Maxage.

   Le nom de la stratégie est **_cacheableCacheControlRes**. Ce qui suit est la règle de stratégie :


```
((HTTP.RES.CACHE_CONTROL.IS_PUBLIC)|| (HTTP.RES.CACHE_CONTROL.IS_MAX_AGE
)|| (HTTP.RES.CACHE_CONTROL.IS_MUST_REVALIDATE)|| (HTTP.RES.CACHE_CONTROL
.IS_PROXY_REVALIDATE)|| (HTTP.RES.CACHE_CONTROL.IS_S_MAXAGE))
```

5. Ne mettez pas en cache les réponses contenant un en-tête Pragma.

   Le nom de la stratégie est **_uncacheablePragmaRes**. Ce qui suit est la règle de stratégie :

   ```
   HTTP.RES.HEADER("Pragma").EXISTS
   ```

6. Réponses de cache contenant un en-tête Expires.

   Le nom de la stratégie est **_cacheableExpiryRes**. Ce qui suit est la règle de stratégie :

   ```
   HTTP.RES.HEADER("Expires").EXISTS
   ```

7. Si la réponse contient un en-tête Content-Type avec la valeur Image, supprimez tous les cookies dans l'en-tête et mettez en cache.

   Le nom de la stratégie est **_imageRes**. Ce qui suit est la règle de stratégie :

   ```
   HTTP.RES.HEADER("Content-Type").SET_TEXT_MODE(IGNORECASE).STARTSWITH("
   image/")
   ```

   Vous pouvez configurer le groupe de contenu suivant pour qu'il fonctionne avec cette stratégie :

   ```
   add cache contentgroup nocookie -group -removeCookies YES
   ```

8. Ne mettez pas en cache une réponse contenant un en-tête Set-Cookie.

   Le nom de la stratégie est **_personalizedRes**. Ce qui suit est la règle de stratégie :

HTTP.RES.HEADER("Set-Cookie").EXISTS	HTTP.RES.HEADER("Set-Cookie2").EXISTS

Restrictions sur les stratégies par défaut

Vous ne pouvez pas remplacer les stratégies de temps de demande intégrées suivantes par des stratégies définies par l'utilisateur.

Ces stratégies sont répertoriées par ordre de priorité.

1. Ne mettez pas en cache les réponses si la requête HTTP correspondante manque une méthode GET ou POST.
2. Ne mettez pas en cache les réponses pour une requête si la longueur de l'URL de la requête HTTP plus le nom d'hôte dépasse 1744 octets.
3. Ne mettez pas en cache une réponse pour une requête contenant un en-tête If-Match.
4. Ne mettez pas en cache une requête contenant un en-tête If-Unmodified-Since.

> **Remarque**
> Ceci est différent de l'en-tête If-Modified-Since.

1. Ne mettez pas en cache une réponse si le serveur ne définit pas d'en-tête d'expiration.

Vous ne pouvez pas remplacer les stratégies de temps de réponse intégrées suivantes. Ces stratégies sont évaluées dans l'ordre dans lequel elles sont répertoriées :

1. Ne mettez pas en cache les réponses dont le code d'état de réponse HTTP est 201, 202, 204, 205 ou 206.
2. Ne mettez pas en cache les réponses qui ont un code d'état de réponse HTTP 4xx, à l'exception des codes d'état 403, 404 et 410.
3. Ne mettez pas en cache les réponses si le type de réponse est FIN terminé ou si la réponse ne possède pas l'un des attributs suivants : Content-Length ou Transfer-Encoding: Chunked.
4. Ne mettez pas en cache la réponse si le module de mise en cache ne peut pas analyser son en-tête Cache-Control.

Paramètres initiaux pour le groupe de contenus par défaut

Lorsque vous activez la mise en cache intégrée pour la première fois, l'appliance Citrix ADC fournit un groupe de contenu prédéfini nommé Groupe de contenu par défaut. Pour plus d'informations, consultez le tableau des paramètres par défaut du groupe de contenu .

Résolution des problèmes

August 20, 2021

Si la fonctionnalité de cache intégrée ne fonctionne pas comme prévu une fois que vous l'avez configurée, vous pouvez utiliser certains outils courants pour accéder aux ressources Citrix ADC et diagnostiquer le problème.

Ressources pour le dépannage

Pour plus d'informations sur les ressources disponibles pour le dépannage et les exemples de configurations, voir le fichier PDF Resource for troubleshooting.

Optimisation frontale

August 20, 2021

> **Remarque :** L'optimisation frontale est disponible si vous disposez d'une licence Citrix ADC Advanced ou Premium et que vous exécutez Citrix ADC version 10.5 ou ultérieure.

Les protocoles HTTP qui sous-tendent les applications Web ont été développés à l'origine pour prendre en charge la transmission et le rendu de pages Web simples. Les nouvelles technologies telles que JavaScript et les feuilles de style en cascade (CSS), ainsi que les nouveaux types de médias tels que les vidéos Flash et les images riches en graphiques, imposent de lourdes exigences sur les performances front-end, c'est-à-dire sur les performances au niveau du navigateur.

La fonctionnalité d'optimisation frontale (FEO) Citrix ADC résout ces problèmes et réduit le temps de chargement et le temps de rendu des pages Web en :

- Réduction du nombre de demandes.
- Requis pour le rendu de chaque page.
- Réduction du nombre d'octets dans les réponses de page.

Simplifier et optimiser le contenu servi au navigateur client.

Vous pouvez personnaliser votre configuration FEO pour fournir les meilleurs résultats pour vos utilisateurs. Les Citrix ADC prennent en charge de nombreuses optimisations de contenu Web pour les utilisateurs de bureau et mobiles. Les tableaux suivants décrivent les optimisations frontales fournies par la fonction FEO et les opérations effectuées sur différents types de fichiers.

Optimisations effectuées par la fonction FEO

Optimisation Web	Problème	Que fait la fonctionnalité Citrix ADC FEO	Avantages
En ligne	Les navigateurs clients envoient souvent plusieurs demandes aux serveurs pour charger des CSS externes, des images et du JavaScript associés à la page Web.	CSS en ligne, JavaScript en ligne, CSS combiner	Le chargement du CSS externe, des images et du JavaScript en ligne avec les fichiers HTML améliore le temps de rendu des pages. Cette optimisation est bénéfique pour le contenu qui n'est affiché qu'une seule fois et pour les appareils mobiles dont la taille du cache est limitée.
Minimisation	Les données extraites des serveurs comprennent des caractères inessentiels tels que des espaces blancs, des commentaires et des caractères de nouvelle ligne. Le temps que les navigateurs passent dans le traitement de ces données crée une latence du site Web.	minimisation CSS, minimisation JavaScript, suppression des commentaires HTML	Les fichiers miniaturisés consomment moins de bande passante et évitent la latence causée par un traitement spécial.

Optimisation Web	Problème	Que fait la fonctionnalité Citrix ADC FEO	Avantages
Optimisation des images	Les navigateurs mobiles ont souvent des vitesses de connexion lentes et une mémoire cache limitée. Le téléchargement des images sur des clients mobiles consomme plus de bande passante, de temps de traitement et d'espace cache, ce qui entraîne une latence du site Web.	Optimisation JPEG, insertion d'image CSS, Attributs de **réduction d'image**, conversion GIF en PNG, Insertion d'image HTML, conversion d'image WebP, JPEG, GIF, conversion d'image PNG en JPEG-XR	Réduit l'image à la taille indiquée dans la balise image par Citrix ADC, ce qui permet aux navigateurs clients de charger les images plus rapidement.
Repositionnement	Le traitement inefficace de CSS, d'images et de JavaScript externes augmente le temps de chargement des pages.	Chargement paresseux de l'image, déplacement CSS vers la tête, déplacement JavaScript vers la fin	Repositionne les éléments HTML pour réduire le temps de rendu des pages Web et permettre aux navigateurs clients de charger les objets plus rapidement.

Optimisation Web	Problème	Que fait la fonctionnalité Citrix ADC FEO	Avantages
Gestion des connexions	De nombreux navigateurs fixent des limites sur le nombre de connexions simultanées pouvant être établies à un seul domaine. Cela peut amener les navigateurs à télécharger les ressources de page Web une à la fois, ce qui augmente le temps des navigateurs.	Partage de domaine	Surmonte la limite de connexion, ce qui améliore le temps de rendu des pages en permettant aux navigateurs clients de télécharger davantage de ressources en parallèle.

Optimisations Web sur différents types de fichiers :

Citrix ADC peut effectuer des optimisations Web sur CSS, images, Javascript et HTML. Pour plus d'informations, reportez-vous à la section Web Optimisations PDF.

> **Remarque :**
> La fonction d'optimisation frontale prend uniquement en charge les caractères ASCII. Il ne prend pas en charge le jeu de caractères Unicode.

Fonctionnement de l'optimisation frontale

Une fois que Citrix ADC reçoit la réponse du serveur :

1. Analyse le contenu de la page, crée une entrée dans le cache (le cas échéant) et applique la stratégie FEO.

   Par exemple, un Citrix ADC peut appliquer les règles d'optimisation suivantes :

   - Supprimez les espaces blancs ou les commentaires présents dans un CSS ou JavaScript.
   - Combinez un ou plusieurs fichiers CSS en un seul fichier.
   - Convertir le format d'image GIF au format PNG.

2. Réécrit les objets incorporés et enregistre le contenu optimisé dans le cache, avec une signature différente de celle utilisée pour l'entrée de cache initiale.

3. Pour les requêtes suivantes, récupère les objets optimisés du cache, et non du serveur, et transfère les réponses au client.

**

Supprimez les informations superflues telles que les espaces blancs et les commentaires.

Période pendant laquelle le navigateur peut utiliser la ressource mise en cache sans vérifier si du contenu frais est disponible sur le serveur.

Configurer l'optimisation frontale

Vous pouvez éventuellement modifier les valeurs des paramètres globaux d'optimisation frontale. Sinon, commencez par créer des actions qui spécifient les règles d'optimisation à appliquer aux objets incorporés.

Après avoir configuré les actions, créez des stratégies, chacune avec une règle spécifiant un type de demande pour lequel optimiser la réponse, et associez les actions aux stratégies.

> **Remarque :** Citrix ADC évalue les stratégies d'optimisation frontales uniquement au moment de la demande, et non au moment de la réponse.

Pour mettre les stratégies en vigueur, liez-les pour lier des points. Vous pouvez lier une stratégie globalement, de sorte qu'elle s'applique à tout le trafic qui circule via Citrix ADC, ou vous pouvez lier la stratégie à un serveur virtuel d'équilibrage de charge ou de commutation de contenu de type HTTP ou SSL. Lorsque vous liez une stratégie, affectez-lui une priorité. Un numéro de priorité inférieur indique une valeur plus élevée. Citrix ADC applique les stratégies dans l'ordre de leurs priorités.

Conditions préalables

L'optimisation frontale nécessite l'activation de la fonctionnalité de mise en cache intégrée Citrix ADC. En outre, vous devez effectuer les configurations de mise en cache intégrées suivantes :

- Allouer de la mémoire cache.
- Définissez la taille maximale de réponse et la limite de mémoire pour un groupe de contenu de cache par défaut.

Pour plus d'informations sur la configuration de la mise en cache intégrée, consultez la section Mise en cache intégrée.

Remarque : Le terme Cache intégré peut être utilisé de façon interchangeable avec AppCache ; notez que d'un point de vue fonctionnel, les deux termes signifient la même chose.

Configurer l'optimisation frontale à l'aide de l'interface de commande Citrix ADC

À l'invite de commandes, procédez comme suit :

1. Activez la fonction d'optimisation frontale.

```
enable ns feature FEO
```

1. Créez une ou plusieurs actions d'optimisation frontale.

```
add feo action <name> [-imgShrinkToAttrib] [-imgGifToPng] ...
```

Exemple : Pour ajouter une action d'optimisation frontale pour convertir des images au format GIF au format PNG et prolonger la période d'expiration du cache :

```
add feo action allact -imgGifToPng -pageExtendCache
```

1. [Facultatif] Spécifiez des valeurs autres que par défaut pour les paramètres globaux d'optimisation frontale.

```
set feo parameter [-cacheMaxage <integer>] [-JpegQualityPercent <integer>]
[-cssInlineThresSize <integer>] [-inlineJsThresSize <integer> [-inlineImgThresSize
 <integer>]
```

Exemple : Pour spécifier la période d'expiration maximale du cache :

```
set feo parameter -cacheMaxage 10
```

1. Créez une ou plusieurs stratégies d'optimisation frontale.

```
add feo policy <name> <rule> <action>
```

Exemple : Pour ajouter une stratégie d'optimisation frontale et l'associer à l'action allact spécifiée ci-dessus :

```
1 >add feo policy pol1 TRUE all act
2 >add feo policy pol1 "(HTTP.REQ.URL.CONTAINS("testsite"))" allact1
3 <!--NeedCopy-->
```

1. Liez la stratégie à un serveur virtuel d'équilibrage de charge ou de commutation de contenu, ou liez-la globalement.

```
bind lb vserver <name> -policyName <string> -priority <num>
```

```
bind cs vserver <name> -policyName <string> -priority <num>
```

```
bind feo global <policyName> <priority> -type <type> <gotoPriorityExpression
>
```

Exemple : Pour appliquer la stratégie d'optimisation frontale à un serveur virtuel nommé « abc » :

```
> bind lb vserver abc -policyName pol1 -priority 1 -type NONE
```

Exemple : Pour appliquer la stratégie d'optimisation frontale pour tout le trafic atteignant ADC :

```
> bind feo global pol1 100 -type REQ_DEFAULT
```

1. Enregistrer la configuration. save ns config

Configurer l'optimisation frontale à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Optimisation frontale** > **Actions**, puis cliquez sur **Ajouter** et créez une action d'optimisation frontale en spécifiant les détails pertinents.
2. [Facultatif] Spécifiez les paramètres globaux d'optimisation frontale.
3. Accédez à **Optimization** > **Front End Optimization** et, dans le volet droit, sous Paramètres, cliquez sur **Change Front End Optimization** et spécifiez les paramètres globaux d'optimisation frontale.
4. Créez une stratégie d'optimisation frontale.
5. Accédez à **Optimization** > **Front End Optimization** > **Policies**, cliquez sur **Add** et créez une stratégie d'optimisation frontale en spécifiant les détails pertinents.
6. Liez la stratégie à un serveur virtuel d'équilibrage de charge ou de commutation de contenu.
   a) Accédez à **Optimisation** > **Optimisation frontale** > **Stratégies**.
   b) Sélectionnez une stratégie d'optimisation frontale et cliquez sur **Gestionnaire de stratégies**.
   c) Sous **Front End Optimization Policy Manager**, liez la stratégie d'optimisation frontale à un serveur virtuel d'équilibrage de charge ou de commutation de contenu.

Vérifier la configuration de l'optimisation frontale

L'utilitaire de tableau de bord affiche des statistiques récapitulatives et détaillées sous forme de tableaux et de graphiques. Vous pouvez afficher les statistiques FEO pour évaluer votre configuration FEO.

Vous pouvez également afficher des statistiques pour une stratégie FEO, y compris le nombre de sélection que le compteur de stratégie incrémente pendant l'opération FEO basée sur la stratégie.

> **Remarque :**
> Pour plus d'informations sur les statistiques et les graphiques, consultez l'aide du tableau de bord sur l'appliance Citrix ADC.

Afficher les statistiques FEO à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour afficher un résumé des statistiques FEO, la sélection et les détails de la stratégie FEO, ainsi que les statistiques FEO détaillées, respectivement :

- `stat feo` Remarque : La commande stat feo policy affiche des statistiques uniquement pour les stratégies FEO avancées.
- `show feo policy name`
- `stat feo -detail`

Afficher les statistiques FEO sur le tableau de bord Citrix ADC

Dans l'interface graphique du tableau de bord, vous pouvez :

- Sélectionnez Optimisation frontale pour afficher un résumé des FEO statistiques.
- Cliquez sur l'onglet **Affichage graphique** pour afficher le taux de demandes traitées par la fonction FEO.

Optimisation des échantillons :

Reportez-vous à l' exemple de PDF pour obtenir des exemples d'actions d'optimisation du contenu appliquées au contenu HTML et aux objets incorporés dans le contenu HTML.

Accélérateur de contenu

August 20, 2021

> **Important :**
>
> La fonctionnalité d'accélérateur de contenu n'est plus prise en charge sur l'appliance Citrix ADC.

L'accélérateur de contenu est une fonctionnalité Citrix ADC que vous pouvez utiliser dans un déploiement Citrix ByteMobile T1100, pour stocker des données sur une appliance Citrix ByteMobile T2100.

Le stockage des données sur une appliance T2100 permet d'économiser de la bande passante et d'obtenir des temps de réponse plus rapides, car le Citrix ADC n'a pas à se connecter au serveur pour les demandes répétées des mêmes données.

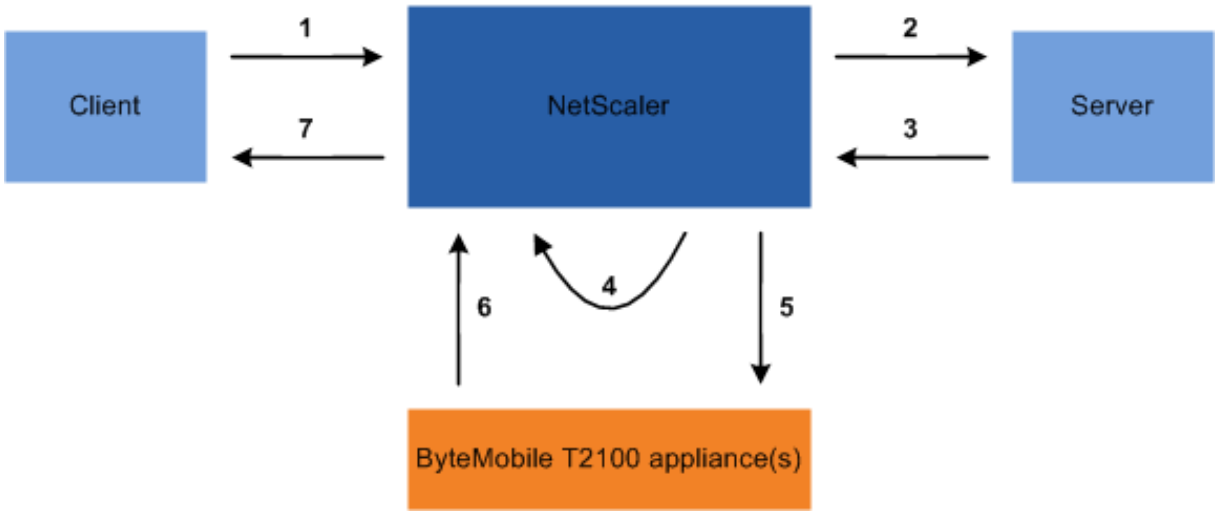
> **Remarque :** L'accélérateur de contenu fonctionne avec une licence Citrix ByteMobile Premium. Contactez le support client pour plus d'informations et pour obtenir la licence.

Fonctionnement de l'accélérateur de contenu

Lorsqu'un serveur virtuel d'équilibrage de charge ou de commutation de contenu reçoit une demande client, l'appliance Citrix ADC évalue une stratégie d'accélérateur de contenu que vous avez liée au serveur virtuel. La stratégie filtre les demandes pour identifier celles auxquelles appliquer la fonctionnalité d'accélérateur de contenu.

> **Remarque :**
>
> Pour les requêtes HTTP, la fonctionnalité d'accélérateur de contenu peut servir du contenu partiel en réponse à des demandes de plage d'octets unique.

La figure suivante illustre les opérations effectuées par l'appliance lorsqu'une demande client arrive sur un serveur virtuel configuré pour utiliser la fonction d'accélérateur de contenu :



Le flux de processus est le suivant :

1. Le client envoie la demande.
2. Citrix ADC transmet la demande au serveur.
3. Le serveur répond avec la taille prédéfinie de la réponse (spécifiée par le paramètre AccumResSize de la commande add ca action).
4. Citrix ADC calcule un hachage de la réponse envoyée par le serveur.
5. Citrix ADC recherche le hachage sur l'appliance T2100.
6. Une recherche réussie indique que les données sont disponibles et que l'appliance T2100 envoie les données au Citrix ADC.

   > **Remarque :**
   > lorsque la recherche de base de données échoue, l'appliance récupère les données demandées du serveur, les envoie au client et les met à jour sur l'appliance T2100.
   > L'appliance T2100 peut être configurée pour spécifier le nombre de demandes pour lesquelles des données doivent être mises en cache.

7. Citrix ADC envoie la réponse au client.

Configurer l'accélérateur de contenu

Avant de configurer la fonctionnalité d'accélérateur de contenu, vous devez l'activer sur l'appliance Citrix ADC.

Vous devez configurer la fonctionnalité d'accélérateur de contenu pour utiliser un ou plusieurs appliances T2100. Vous devez ajouter chaque appliance T2100 en tant que service et lier ces services à un

serveur virtuel d'équilibrage de charge dédié à la répartition de la charge entre les appliances T2100 configurées.

Vous devez configurer une action d'accélérateur de contenu pour rechercher les données sur l'appliance T2100. L'action doit spécifier le serveur virtuel d'équilibrage de charge T2100 et la taille des données (en Ko) à extraire du serveur pour calculer le hachage.

L'action doit être liée à une stratégie d'accélérateur de contenu qui définit le trafic sur lequel effectuer l'accélération de contenu. La stratégie d'accélérateur de contenu doit être liée à un serveur virtuel de commutation de contenu ou d'équilibrage de charge qui reçoit du trafic client. Vous pouvez également lier la stratégie globalement à tous les serveurs virtuels applicables.

Pour configurer l'accélérateur de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

1. Activez la fonction d'accélérateur de contenu.

   ```
   enable ns feature ca
   ```

2. Identifiez les appliances T2100 et ajoutez-les en tant que service sur l'appliance Citrix ADC.

   ```
   add service <name> <IPAddress> <serviceType> <port>
   ```

   Exemple :

   ```
   1 > add service T2100-A 10.102.29.61 HTTP 30
   2 > add service T2100-B 10.102.29.62 HTTP 40
   3 > add service T2100-C 10.102.29.63 HTTP 50
   4 <!--NeedCopy-->
   ```

   > **Remarque :**
   > Les services doivent être de type HTTP uniquement.

3. Créez un serveur virtuel d'équilibrage de charge pour les appliances T2100. Spécifiez la méthode d'équilibrage de charge de jeton et la règle indiquée dans la syntaxe suivante.

   ```
   1 add lb vserver <name> <serviceType> <IPAddress> <port> -lbMethod
       TOKEN -rule "http.req.url.after_str("/lookup/") alt http.req.
       url.path.SKIP(1).PREFIX(64)"
   2 <!--NeedCopy-->
   ```

   Exemple :

   ```
   1 add lb vserver T2100-lbvserver HTTP 10.102.29.64 99 -lbMethod
       TOKEN -rule "http.req.url.after_str("/lookup/") alt http.req.
       url.path.SKIP(1).PREFIX(64)"
   2 <!--NeedCopy-->
   ```


4. Liez les services T2100 au serveur virtuel d'équilibrage de charge que vous avez créé pour eux.

   ```
   bind lb vserver <name> <serviceName>
   ```

   Exemple :

   ```
   1 > bind lb vserver T2100-lbvserver T2100-A
   2 > bind lb vserver T2100-lbvserver T2100-B
   3 > bind lb vserver T2100-lbvserver T2100-C
   4 <!--NeedCopy-->
   ```

5. Définissez une action d'accélérateur de contenu.

   ```
   add ca action <name> accumResSize <KBytes> -lbvserver <string> -type
   lookup
   ```

   Exemple :

   ```
   > add ca action ca_action1 -type lookup -lbvserver T2100-lbvserver -
   accumResSize 60
   ```

6. Définissez une stratégie d'accélérateur de contenu.

   ```
   add ca policy <name> -rule <expression> -action <name>
   ```

   Exemple :

   Pour créer une stratégie d'accélérateur de contenu qui met en cache tous les formats vidéo.

   ```
   > add ca policy ca_mp4_pol -rule ns_video -action ca_action1
   ```

   où ns_video est une expression intégrée.

7. Liez la stratégie d'accélérateur de contenu à un serveur virtuel qui reçoit du trafic ou globalement au système Citrix ADC.

   ```
   bind lb vserver <name> -policyName <string>
   ```

   ```
   bind cs vserver <name> -policyName <string>
   ```

   ```
   bind ca global -policyName <string> -priority <num> -type <type>
   ```

   Exemple : Pour appliquer la stratégie d'accélérateur de contenu à un serveur virtuel nommé « traf_rec »

   ```
   bind lb vserver traf_rec -policyName ca_mp4_pol
   ```

   Exemple : pour appliquer la stratégie d'accélérateur de contenu à tout le trafic atteignant le Citrix ADC.

   ```
   bind ca global -policyName ca_mp4_pol -priority 100 -type RES_DEFAULT
   ```

8. Enregistrez la configuration.

   ```
   save ns config
   ```


Configuration de l'accélérateur de contenu à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres** > **Configurer les fonctionnalités avancées** et sélectionnez **Content Accelerator**.
2. Créez un service pour chacune des appliances T2100.
   a) Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
   b) Cliquez sur **Ajouter** et spécifiez les détails pertinents. Dans le champ **Serveur**, assurez-vous de spécifier l'adresse IP de l'appliance T2100. Dans le champ **Protocole**, sélectionnez HTTP.
3. Créez un serveur virtuel et liez les services T2100 à celui-ci.
   a) Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
   b) Cliquez sur **Ajouter** et spécifiez les détails pertinents.
   c) Dans l'onglet **Méthode et persistance**, spécifiez la méthode comme **jeton**.
   d) Dans l'onglet **Stratégies**, spécifiez la règle comme http.req.url.after_str("/lookup/") alt http.req.url.path.SKIP(1).PREFIX(64).
   e) Dans l'onglet **Services**, sélectionnez les services T2100 que vous souhaitez lier au serveur virtuel.
4. Créez une action d'accélérateur de contenu.
   a) Accédez à **Optimisation** > **Accélérateur de contenu** > **Actions**.
   b) Spécifiez les détails pertinents.
5. Créez une stratégie d'accélérateur de contenu.
   a) Accédez à **Optimisation** > **Accélérateur de contenu** > **Stratégies**.
   b) Cliquez sur **Ajouter**, spécifiez la règle de stratégie et associez l'action d'accélérateur de contenu.
6. Liez la stratégie d'accélérateur de contenu globalement ou à un serveur virtuel.
   a) Accédez à **Optimisation** > **Accélérateur de contenu**.
   b) Dans les sections **Content Accelerator Policy Manager** [REQUEST] ou Content Accelerator Policy Manager [RESPONSE], liez la stratégie d'accélérateur de contenu globalement ou à un serveur virtuel.

Classification des médias

January 21, 2021

La compréhension du type de trafic dans le réseau aide les administrateurs réseau à gérer la consommation de bande passante pour des performances réseau optimales. Le mode de classification des supports surveille et affiche les statistiques du trafic multimédia passant par l'appliance Citrix ADC.

Lorsque ce mode est activé, un administrateur réseau peut collecter des statistiques indiquant la quantité de données consultées et les types de périphériques à partir desquels les fichiers multimé-

dias ont été consultés. L'appliance Citrix ADC prend également en charge les demandes de plage d'octets dans ce mode.

Actuellement, l'appliance Citrix ADC peut surveiller et afficher des statistiques pour les types de fichiers multimédias suivants :

Média	Type de fichier
Microsoft Smooth Streaming	Vidéo
Apple Live Streaming	Vidéo
Flux de transport de données audio (ADTS)	Audio
Codage audio avancé (AAC)	Audio
Vidéo Flash (FLV)	Audio et Vidéo
3GP	Audio et Vidéo

L'appliance peut afficher des statistiques pour les périphériques suivants :

Plate-forme de l'appareil	Type d'appareil
iOS	iPad et iPod
Android	Mobiles et tablettes
Ordinateur portable ou ordinateur de bureau	Ordinateurs portables et de bureau Windows
Autres	Autres appareils mobiles (mobiles et tablettes)

Les administrateurs réseau peuvent vérifier les compteurs de statistiques suivants pour connaître la quantité de données accessibles via l'appliance Citrix ADC pour différents types de trafic multimédia.

Nom du fichier multimédia	Compteur de statistiques
Microsoft Smooth Streaming	mcmssmthstrmvid: ce compteur enregistre le nombre total de vidéos Microsoft Smooth Streaming diffusées par l'appliance Citrix ADC ;Mcmssmthstrvidpl—Ce compteur enregistre le nombre total de listes de lecture vidéo Microsoft Smooth Streaming diffusées par l'appliance Citrix ADC ;Mcmssmthstrmvidbytes—Ce compteur enregistre le nombre total de octets de données servis pour le trafic multimédia Microsoft Smooth Streaming sur l'appliance Citrix ADC ;Mcmssmthstrmplvidbytespl—Ce compteur enregistre le nombre total d'octets de lecture Microsoft Smooth Streaming servis par l'appliance Citrix ADC.
Apple Live Streaming	mccaplelivestrmngvid : ce compteur enregistre le nombre total de vidéos Apple Live Streaming diffusées par l'appliance Citrix ADC.Mccapplelivestrmngvidpll : ce compteur enregistre le nombre total de listes de lecture vidéo Apple Live Streaming diffusées par l'appliance Citrix ADC.Mcapplelivestreamingvidbytes: ce compteur enregistre le nombre total d'octets de données servis pour le trafic multimédia Apple Live Streaming sur l'appliance Citrix ADC.Mcapplelivestreamingplaylistvidbytespl : ce compteur enregistre le nombre total d'octets Apple Live Playlist servis par l'appliance Citrix ADC.
Flux de transport de données audio (ADTS)	mcadtsaudio: ce compteur enregistre le nombre total de clips audio ADTS servis par l'appliance Citrix ADC.Mcadtsaudiobytes: ce compteur enregistre le nombre total d'octets de données servis pour le trafic multimédia ADTS sur l'appliance Citrix ADC.

Nom du fichier multimédia	Compteur de statistiques
Codage audio avancé (AAC)	`Mcaacaudio`: ce compteur enregistre le nombre total de clips audio AAC servis par l'appliance Citrix ADC.`Mcaacaudiobytes`: ce compteur enregistre le nombre total d'octets de données servis pour le trafic multimédia AAC sur l'appliance Citrix ADC.
Vidéo Flash (FLV)	`Mcflvvid`: ce compteur enregistre le nombre total de vidéos flash diffusées par l'appliance Citrix ADC.`Mcflvvidbytes`: ce compteur enregistre le nombre total d'octets de données servis pour les vidéos flash sur l'appliance Citrix ADC.
3GP	`mc3gpvidbytes` : ce compteur enregistre le nombre total d'octets de données servis pour le trafic média 3GP sur l'appliance Citrix ADC.

L'appliance Citrix ADC détecte les types de fichiers multimédias par leurs signatures dans *les octets initiaux* des réponses. Par exemple, les octets de corps initiaux d'un fichier mp4 ont la signature suivante dans la réponse :

```
**....ftypmp42** ....isommp42....moov...lmvhd.....c.\!.c.\!..
```

L'appliance Citrix ADC détecte le type de périphérique client par la *chaîne de l'agent utilisateur* que la machine client inclut dans la requête HTTP GET. Par exemple, un téléphone Windows utilisant un navigateur UC a la chaîne de l'agent utilisateur suivante dans la requête HTTP GET :

```
User-Agent: **UCWEB**/2.0 (**Windows**; U; wds 8.10; en-US; HTC; 8X by HTC)
U2/1.0.0
```

Activer la classification des médias

Par défaut, la classification des supports est désactivée sur l'appliance Citrix ADC. Vous devez activer le mode avant de l'utiliser.

Pour activer la classification des médias à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
enable ns mode Mediaclassification
```

Pour activer la classification des médias à l'aide de l'interface graphique

Activer la classification des médias sur l'appliance Citrix ADC

Accédez à **Système** > **Paramètres** > **Configurer les modes** et sélectionnez **Classification des médias**.

Pour afficher les statistiques de trafic multimédia sur l'appliance Citrix ADC

Accédez à **Optimisation** et cliquez sur **Classification des médias** pour afficher les statistiques du trafic des médias.

Vérifier les statistiques de classification des médias

Vous pouvez afficher les statistiques du trafic multimédia dans l'utilitaire de tableau de bord ou à l'aide de l'interface de ligne de commande. L'utilitaire de tableau de bord affiche des statistiques récapitulatives et détaillées sous forme de tableaux et de graphiques.

> **Remarque**
> Pour plus d'informations sur les statistiques et les graphiques, consultez l'aide du Tableau de bord sur votre appliance Citrix ADC.

Pour afficher les statistiques de classification des médias à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour afficher un résumé des statistiques de classification des médias, afficher des statistiques détaillées ou effacer l'affichage :

```
stat Mediaclassification
```

```
stat Mediaclassification -detail
```

```
stat Mediaclassification -clearstats
```

Pour afficher les statistiques de classification des médias dans le tableau de bord

Dans l'utilitaire **Tableau de bord**, vous pouvez afficher les types de statistiques de classification des médias suivants :

1. Sélectionnez **Classification des médias** pour afficher un résumé des statistiques du trafic des médias.
2. Pour afficher des statistiques détaillées sur le trafic des médias, cliquez sur **Détails**.
3. Pour effacer les statistiques du trafic multimédia, cliquez sur **Effacer**.

Réputation

August 20, 2021

Citrix offre une sécurité basée sur la réputation. En utilisant l'évaluation de la réputation pour déterminer le risque de traitement des demandes, vous pouvez prendre des mesures telles que le blocage ou la suppression de certaines demandes pour améliorer les performances de votre application.

La fonctionnalité de réputation IP Citrix ADC utilise des vérifications de réputation IP pour empêcher les attaques Zero day et fournir une protection contre les sources malveillantes associées aux attaques Web, aux activités de phishing ou à l'analyse Web.

Pour plus de détails, voir Réputation IP.

Réputation IP

October 5, 2021

La réputation IP est un outil qui identifie les adresses IP qui envoient des demandes indésirables. À l'aide de la liste de réputation IP, vous pouvez rejeter les demandes provenant d'une adresse IP de mauvaise réputation. Optimisez les performances du pare-feu des applications Web en filtrant les demandes que vous ne souhaitez pas traiter. Réinitialisez, abandonnez une demande ou même configurez une stratégie de répondeur pour qu'elle entreprenne une action de répondeur spécifique.

Voici quelques attaques que vous pouvez prévenir en utilisant la réputation IP :

- **Ordinateurs personnels infectés par un virus**. (PC personnels) sont la principale source de spam sur Internet. La réputation IP peut identifier l'adresse IP qui envoie des demandes indésirables. La réputation IP peut être particulièrement utile pour bloquer les attaques DDoS, DoS ou inondation SYN anormale à grande échelle provenant de sources infectées connues.
- **Botnet géré et automatisé de manière centralisée**. Les attaquants ont gagné en popularité pour avoir volé des mots de passe, car il ne faut pas longtemps lorsque des centaines d'ordinateurs travaillent ensemble pour déchiffrer votre mot de passe. Il est facile de lancer des attaques de botnets pour trouver des mots de passe qui utilisent des mots de passe couramment utilisés dans le dictionnaire.
- **Serveur Web compromis**. Les attaques ne sont pas aussi fréquentes car la sensibilisation et la sécurité des serveurs ont augmenté, de sorte que les pirates et les spammeurs recherchent des cibles plus faciles. Il existe encore des serveurs Web et des formulaires en ligne que les pirates informatiques peuvent compromettre et utiliser pour envoyer des spams (tels que des virus et de la pornographie). Une telle activité est plus facile à détecter et à arrêter rapidement, ou à bloquer avec une liste de réputation telle que SpamRATS.
- **Exploits Windows**. (telles que les adresses IP actives proposant ou distribuant des logiciels malveillants, du code shell, des rootkits, des vers ou des virus).
- **Spammeurs et hackers connus**.
- **Campagnes de marketing par e-mail de masse**
- **Proxys d'hameçonnage** (adresses IP hébergeant des sites d'hameçonnage et autres fraudes telles que la fraude par clic publicitaire ou la fraude aux jeux).
- **Proxys anonymes** (IP fournissant des services de proxy et d'anonymisation, y compris The Onion Router alias TOR).

Une appliance Citrix ADC utilise **Webroot** en tant que fournisseur de services pour une base de données IP malveillante générée dynamiquement et les métadonnées de ces adresses IP. Les métadonnées peuvent inclure des détails de géolocalisation, une catégorie de menace, un nombre de menaces, etc. Le moteur Webroot Threat Intelligence reçoit des données en temps réel de millions de capteurs. Il capture, analyse, analyse et note automatiquement et en continu les données, à l'aide d'un apprentissage automatique avancé et d'une analyse comportementale. Les renseignements concernant une menace sont continuellement mis à jour.

Lorsqu'une menace est détectée n'importe où sur le réseau, l'adresse IP est signalée comme malveillante et toutes les appliances connectées au réseau sont immédiatement protégées. Les modifications dynamiques des adresses IP sont traitées avec une vitesse et une précision élevées grâce à l'apprentissage automatique avancé.

Comme indiqué dans la fiche technique de Webroot, le réseau de capteurs de Webroot identifie de nombreux types de menaces IP clés, notamment les sources de spam, les exploits Windows, les réseaux de zombies, les scanners et autres. (Voir le diagramme de flux sur la fiche technique.)

L'appliance Citrix ADC utilise un processus `iprep` client pour obtenir la base de données de Webroot. Le `iprep` client utilise la méthode HTTP GET pour obtenir la liste des adresses IP absolues de Webroot pour la première fois. Plus tard, il vérifie les changements de delta une fois toutes les 5 minutes.

> **Important :**
>
> - Assurez-vous que l'appliance Citrix ADC dispose d'un accès Internet et que le DNS est configuré avant d'utiliser la fonctionnalité de réputation d'IP.
> - Pour accéder à la base de données Webroot, l'appliance Citrix ADC doit pouvoir se connecter à **api.bcti.brightcloud.com** sur le **port 443**. Chaque nœud du déploiement HA ou de cluster obtient la base de données de Webroot et doit pouvoir accéder à ce nom de domaine complet (FQDN).
> - Webroot héberge actuellement sa base de données de réputation dans AWS. Par conséquent, Citrix ADC doit être en mesure de résoudre les domaines AWS pour télécharger la base de données de réputation. En outre, le pare-feu doit être ouvert pour les domaines AWS.
>
> **Remarque :**
>
> Chaque moteur de paquets nécessite au moins 4 Go pour fonctionner correctement lorsque la fonctionnalité de réputation IP est activée.

Expressions de stratégie avancées. Configurez la fonctionnalité de réputation IP à l'aide d'expressions de stratégie avancées (expressions de stratégie avancées) dans les stratégies liées aux modules pris en charge, tels que le pare-feu d'application Web et le répondeur. Voici deux exemples d'expressions qui peuvent être utilisées pour détecter si l'adresse IP du client est malveillante.

1. **CLIENT.IP.SRC.IPREP_IS_MALICIOUS** : Cette expression renvoie la valeur TRUE si le client est

inclus dans la liste des adresses IP malveillantes.

2. **CLIENT.IP.SRC.IPREP_THREAT_CATEGORY (CATEGORY)** : Cette expression renvoie la valeur TRUE si l'adresse IP du client est une adresse IP malveillante et se trouve dans la catégorie de menace spécifiée.

Voici les valeurs possibles pour la catégorie de menace :

SPAM_SOURCES, WINDOWS_EXPLOITS, WEB_ATTACKS, BOTNETS, SCANNERS, DOS, REPUTATION, PHISHING, PROXY, NETWORK, CLOUD_PROVIDERS, MOBILE_THREATS, TOR_PROXY.

> **Remarque :**
>
> La fonctionnalité de réputation IP vérifie les adresses IP source et de destination. Il détecte les adresses IP malveillantes dans l'en-tête. Si l'expression PI d'une stratégie peut identifier l'adresse IP, la vérification de réputation IP détermine si elle est malveillante.

Message du journal iPrep. Le `/var/log/iprep.log` fichier contient des messages utiles qui capturent des informations sur la communication avec la base de données Webroot. Les informations peuvent porter sur les informations d'identification utilisées lors de la communication Webroot, l'échec de la connexion à Webroot, les informations incluses dans une mise à jour (telles que le nombre d'adresses IP dans la base de données).

Création d'une liste de blocage ou d'une liste d'adresses IP autorisées à l'aide d'un ensemble de données de stratégie. Vous pouvez maintenir une liste d'autorisation pour autoriser l'accès à des adresses IP spécifiques qui sont bloquées dans la base de données Webroot. Vous pouvez également créer une liste de blocage personnalisée d'adresses IP pour compléter le contrôle de réputation Webroot. Ces listes peuvent être créées à l'aide d'un **jeu de données de**stratégie. Un ensemble de données est une forme spécialisée de jeu de motifs qui convient parfaitement à la mise en correspondance d'adresses IPv4. Pour utiliser des jeux de données, commencez par créer le jeu de données et liez-y des adresses IPv4. Lorsque vous configurez une stratégie de comparaison d'une chaîne dans un paquet, utilisez un opérateur approprié et transmettez le nom du jeu de motifs ou du jeu de données en tant qu'argument.

Pour créer une liste d'adresses autorisées à traiter comme des exceptions lors de l'évaluation de la réputation IP, procédez comme suit :

- Configurez la stratégie de sorte que l'expression PI donne la valeur False même si une adresse de la liste d'autorisation est répertoriée comme malveillante par Webroot (ou tout autre fournisseur de services).

Activation ou désactivation de la réputation IP. La réputation IP fait partie de la fonctionnalité de réputation générale, qui est basée sur la licence. Lorsque vous activez ou désactivez la fonctionnalité de réputation, elle active ou désactive la réputation IP.

Procédure générale. Le déploiement de la réputation IP implique les tâches suivantes :

- Vérifiez que la licence installée sur l'appliance Citrix ADC prend en charge la réputation IP. Les licences de pare-feu d'application Premium et autonome prennent en charge la fonctionnalité de réputation IP.
- Activez les fonctionnalités de réputation IP et de pare-feu d'application.
- Ajoutez un profil de pare-feu d'application.
- Ajoutez une stratégie de pare-feu d'application à l'aide des expressions PI pour identifier les adresses IP malveillantes dans la base de données de réputation IP.
- Liez la stratégie de pare-feu d'application à un point de liaison approprié.
- Vérifiez que toute demande reçue d'une adresse malveillante est consignée dans le `ns.log` fichier pour montrer que la demande a été traitée comme indiqué dans le profil.

Configurez la fonctionnalité de réputation IP à l'aide de la CLI

À l'invite de commandes, tapez :

- `enable feature reputation`
- `disable feature reputation`

Les exemples suivants montrent comment ajouter une stratégie de pare-feu d'application à l'aide de l'expression PI pour identifier les adresses malveillantes. Vous pouvez utiliser les profils intégrés, ajouter un profil ou configurer un profil existant pour appeler l'action souhaitée lorsqu'une demande correspond à une correspondance de stratégie.

Les exemples 3 et 4 montrent comment créer un jeu de données de stratégie pour générer une liste de blocage ou une liste d'adresses IP autorisées.

Exemple 1 :

La commande suivante crée une stratégie qui identifie les adresses IP malveillantes et bloque la demande en cas de déclenchement d'une correspondance :

```
add appfw policy pol1 CLIENT.IP.SRC.IPREP_IS_MALICIOUS APPFW_BLOCK
```

Exemple 2 :

La commande suivante crée une stratégie qui utilise le service de réputation pour vérifier l'adresse IP du client dans l' `X-Forwarded-For` en-tête et réinitialiser la connexion si une correspondance est déclenchée.

```
> add appfw policy pol1 "HTTP.REQ.HEADER(\"X-Forwarded-For\").TYPECAST_IP_ADDRESS_AT
.IPREP_IS_MALICIOUS"APPFW_RESET**
```

Exemple 3 :

L'exemple suivant montre comment ajouter une liste pour ajouter des exceptions autorisant des adresses IP spécifiées :


```
> add policy dataset Allow_list1 ipv4
> bind policy dataset Allow_list1 10.217.25.17 -index 1
> bind policy dataset Allow_list1 10.217.25.18 -index 2
```

Exemple 4 :

L'exemple suivant montre comment ajouter la liste personnalisée pour signaler les adresses IP spécifiées comme malveillantes :

```
> add policy dataset Block_list1 ipv4
> bind policy dataset Block_list1 10.217.31.48 -index 1
> bind policy dataset Block_list1 10.217.25.19 -index 2
```

Exemple 5 :

L'exemple suivant illustre une expression de stratégie pour bloquer l'adresse IP du client dans les conditions suivantes :

- Il correspond à une adresse IP configurée dans le block_list1 personnalisé (exemple 4)
- Il correspond à une adresse IP répertoriée dans la base de données Webroot, sauf si elle est assouplie par inclusion dans la liste Allow_List1 (exemple 3).

```
1 > add appfw policy "Ip_Rep_Policy" "((CLIENT.IP.SRC.IPREP_IS_MALICIOUS
     || CLIENT.IP.SRC.TYPECAST_TEXT_T.CONTAINS_ANY("Block_list1")) && ! (
     CLIENT.IP.SRC.TYPECAST_TEXT_T.CONTAINS_ANY("Allow_list1")))"
     APPFW_BLOCK
2 <!--NeedCopy-->
```

Utilisation du serveur proxy :

Si l'appliance Citrix ADC n'a pas d'accès direct à Internet et est connectée à un proxy, configurez le client de réputation IP pour qu'il envoie des demandes au proxy.

À l'invite de commandes, tapez :

```
set reputation settings -proxyServer <proxy server ip> -proxyPort <proxy
server port>
```

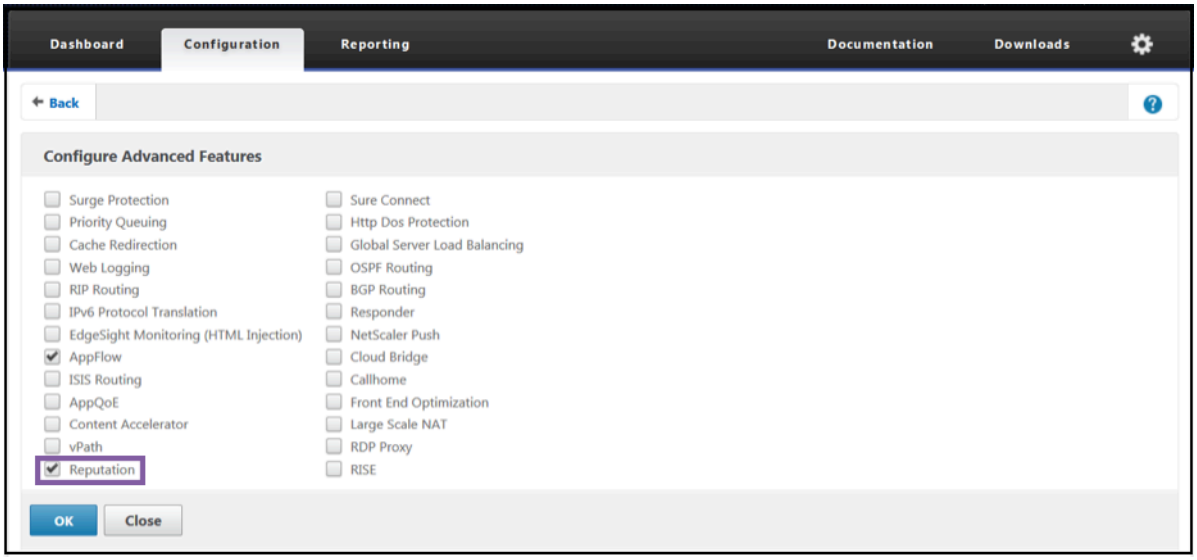
Exemple :

```
> set reputation settings proxyServer 10.102.30.112 proxyPort 3128
> set reputation settings -proxyServer testproxy.citrite.net -proxyPort 3128
> unset reputation settings -proxyserver -proxyport
> sh reputation settings
```


> **Remarque :**
>
> L'adresse IP du serveur proxy peut être une adresse IP ou un nom de domaine complet (FQDN).

Configuration de la réputation IP à l'aide de l'interface graphique Citrix ADC

1. Accédez au **système > aux paramètres**. Dans la section **Modes et fonctionnalités**, cliquez sur le lien pour accéder au volet **Configurer les fonctionnalités avancées** et activez la case à cocher **Réputation** .
2. Cliquez sur **OK**.

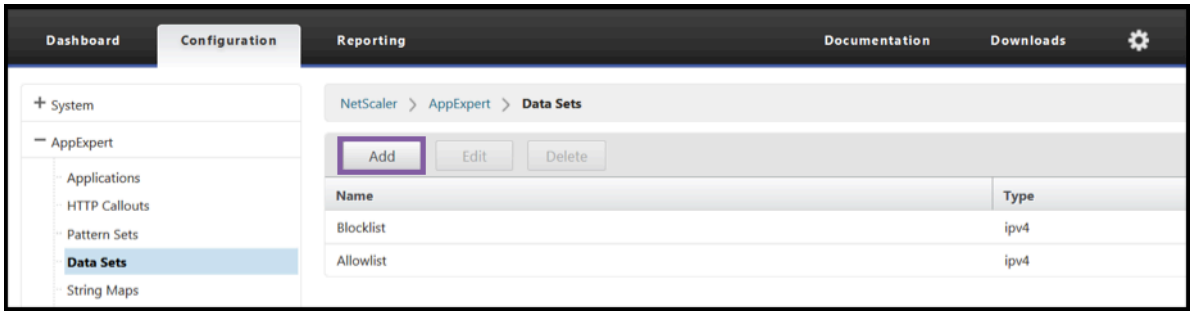


Pour configurer un serveur proxy à l'aide de l'interface graphique Citrix ADC

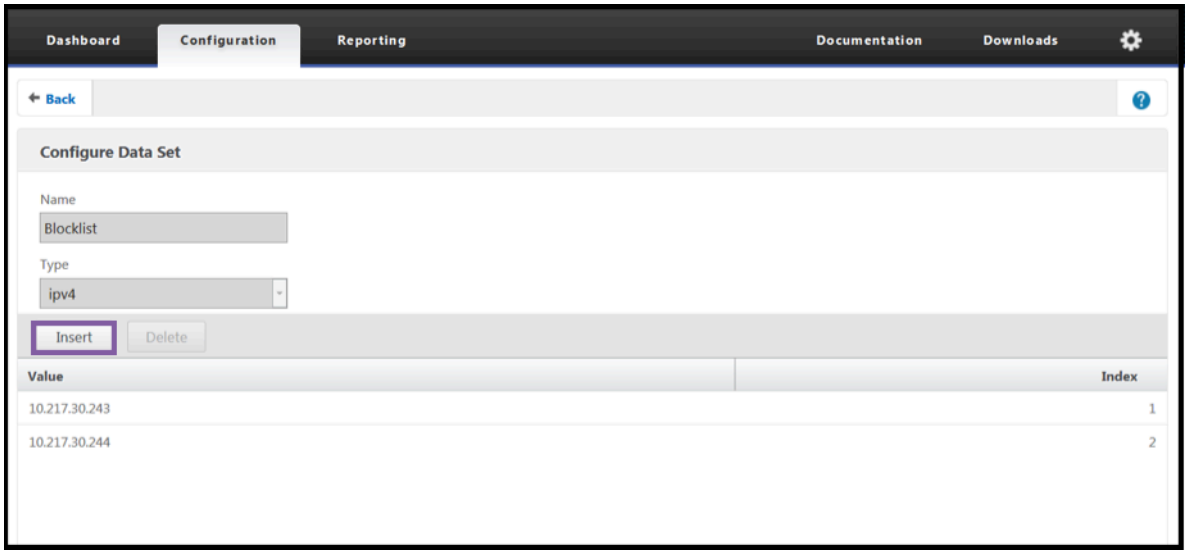
1. Dans l'onglet de configuration, accédez à **Sécurité > Réputation**. Sous **Paramètres**, cliquez sur **Modifier les paramètres de réputation** pour configurer un serveur proxy. Vous pouvez également activer ou désactiver la fonctionnalité de réputation. Le**serveur proxy** peut être une adresse IP ou un nom de domaine complet (FQDN). **Le port proxy** accepte des valeurs comprises entre [1 et 65535].

Créer une liste d'autorisation et une liste de blocage des adresses IP des clients à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, accédez à **AppExpert > Jeux de données**.
2. Cliquez sur **Ajouter**.



- Dans le volet **Créer un ensemble de données** (ou **Configurer un ensemble de données**), indiquez un nom significatif pour la liste des adresses IP. Le nom doit refléter l'objectif de la liste.
- Sélectionnez **Type** as **IPv4**.
- Cliquez sur **Insérer** pour ajouter une entrée.



- Dans le volet **Configurer la liaison du jeu de données de stratégie**, ajoutez une adresse IP au format IPv4 dans la zone de saisie Valeur.
- Fournissez un index.
- Ajoutez un commentaire qui explique l'objectif de la liste. Cette étape est facultative, mais elle est recommandée car un commentaire descriptif est utile pour gérer la liste.

De même, vous pouvez créer une liste de blocage et ajouter les adresses IP qui doivent être considérées comme malveillantes.

Reportez-vous également à la section Jeux de modèles et jeux de données pour plus de détails sur l'utilisation des jeux de données et la configuration des expressions de stratégie avancées.

Configurer une stratégie de pare-feu d'application à l'aide de l'interface graphique Citrix ADC

1. Dans l'onglet **Configuration**, accédez à **Sécurité > Pare-feu d'application > Stratégies > Pare-feu**. Cliquez sur **Ajouter** pour ajouter une stratégie à l'aide des expressions PI afin d'utiliser la réputation IP.

Vous pouvez également utiliser l'éditeur d'expressions pour créer votre propre expression de stratégie. La liste présente les options préconfigurées qui sont utiles pour configurer une expression à l'aide des catégories de menaces.

Résumé

- Arrêtez rapidement et précisément le mauvais trafic à la périphérie du réseau provenant d'adresses IP malveillantes connues posant différents types de menaces. Vous pouvez bloquer la demande sans analyser le corps.
- Configurez dynamiquement la fonctionnalité de réputation IP pour plusieurs applications.
- Sécurisez votre réseau contre les violations de données sans nuire aux performances, et consolidez les protections sur une structure de services unique grâce à des déploiements rapides et faciles.
- Vous pouvez effectuer des vérifications de réputation IP sur les adresses IP source et de destination.
- Vous pouvez également inspecter les en-têtes pour détecter les adresses IP malveillantes.
- La vérification de la réputation IP est prise en charge dans les déploiements de proxy direct et de proxy inverse.
- Le processus de réputation IP se connecte à Webroot et met à jour la base de données toutes les 5 minutes.
- Chaque nœud du déploiement High Availability (HA) ou Cluster obtient la base de données de Webroot.
- Les données de réputation IP sont partagées entre toutes les partitions des déploiements de partition d'admin-partition.
- Vous pouvez utiliser un ensemble de données AppExpert pour créer des listes d'adresses IP afin d'ajouter des exceptions pour les adresses IP bloquées dans la base de données Webroot. Vous pouvez également créer votre propre liste de blocage personnalisée pour désigner des adresses IP spécifiques comme malveillantes.
- Le fichier iprep.db est créé dans le `/var/nslog/iprep` dossier. Une fois créé, il n'est pas supprimé même si la fonctionnalité est désactivée.
- Lorsque la fonctionnalité de réputation est activée, la base de données Citrix ADC Webroot est téléchargée. Après cela, il est mis à jour toutes les 5 minutes.
- La version majeure de la base de données Webroot est la version : 1.
- La version mineure est mise à jour tous les jours. La version de mise à jour est incrémentée toutes les 5 minutes et est réinitialisée à 1 lorsque la version mineure est incrémentée.

- Les expressions PI vous permettent d'utiliser la réputation IP avec d'autres fonctionnalités, telles que le répondeur et la réécriture.
- Les adresses IP de la base de données sont en notation décimale.

Conseils de débogage

- Si vous ne pouvez pas voir la fonctionnalité de réputation dans l'interface graphique, vérifiez que vous disposez de la bonne licence.
- Surveillez les messages entrants `var/log/iprep.log` pour le débogage.
- **Connectivité Webroot** : si le `ns iprep: Not able to connect/resolve WebRoot` message s'affiche, assurez-vous que la solution matérielle-logicielle dispose d'un accès Internet et que le DNS est configuré.
- **Serveur proxy** : si le `ns iprep: iprep_curl_download: 88 curl_easy_perform failed. Error code: 5 Err msg:couldnt resolve proxy name` message s'affiche, assurez-vous que la configuration du serveur proxy est correcte.
- La**fonctionnalité de réputation IP ne fonctionne pas** : le processus de réputation IP prend environ cinq minutes pour démarrer une fois que vous avez activé la fonctionnalité de réputation. La fonctionnalité de réputation IP risque de ne pas fonctionner pendant cette durée.
- **Téléchargement de la base**de données : si le téléchargement des données de la base de données IP échoue après l'activation de la fonctionnalité de réputation IP, l'erreur suivante apparaît dans les journaux.

```
iprep: iprep_curl_download:86 curl_easy_perform failed. Error code:7 Err
msg:Couldn't connect to server
```

Solution : autorisez le trafic sortant vers les URL suivantes ou configurez un proxy pour résoudre le problème.

```
1 localdb-ip-daily.brightcloud.com:443
2 localdb-ip-rtu.brightcloud.com:443
3 api.bcti.brightcloud.com:443
4 <!--NeedCopy-->
```

Déchargement et accélération SSL

January 21, 2021

Une appliance Citrix ADC configurée pour l'accélération SSL accélère de manière transparente les transactions SSL en déchargeant le traitement SSL du serveur. Pour configurer le déchargement SSL, vous configurez un serveur virtuel pour intercepter et traiter les transactions SSL et envoyer le trafic

déchiffré au serveur (sauf si vous configurez le chiffrement de bout en bout, auquel cas le trafic est rechiffré). Dès réception de la réponse du serveur, l'appliance effectue la transaction sécurisée avec le client. Du point de vue du client, la transaction semble être directement avec le serveur. Un Citrix ADC configuré pour l'accélération SSL exécute également d'autres fonctions configurées, telles que l'équilibrage de charge.

La configuration du déchargement SSL nécessite un certificat SSL et une paire de clés, que vous devez obtenir si vous n'avez pas déjà de certificat SSL. D'autres tâches liées à SSL que vous devrez peut-être effectuer incluent la gestion des certificats, la gestion des listes de révocation de certificats, la configuration de l'authentification client et la gestion des actions et des stratégies SSL.

Une appliance Citrix ADC non FIPS stocke la clé privée du serveur sur le disque dur. Sur une appliance FIPS, la clé est stockée dans un module cryptographique connu sous le nom de module de sécurité matérielle (HSM).

Toutes les appliances Citrix ADC qui ne prennent pas en charge une carte FIPS (y compris les appliances virtuelles) prennent en charge les HSM externes Thales NShield® Connect et SafeNet. (Les appliances MPX 9700/10500/12500/15500 ne prennent pas en charge un HSM externe.)

Remarque : les options liées à FIPS pour certaines procédures de configuration SSL décrites dans ce document sont spécifiques à une appliance Citrix ADC compatible FIPS.

Configuration de déchargement SSL

August 20, 2021

Pour configurer le déchargement SSL, vous devez activer le traitement SSL sur l'appliance Citrix ADC et configurer un serveur virtuel SSL. Le serveur virtuel intercepte le trafic SSL, décrypte le trafic et le transmet à un service lié au serveur virtuel. Pour sécuriser le trafic temporel, tel que la diffusion multimédia, vous pouvez configurer un serveur virtuel DTLS. Pour activer le déchargement SSL, vous devez importer un certificat et une clé valides et lier la paire au serveur virtuel.

Activer SSL

Pour traiter le trafic SSL, vous devez activer le traitement SSL. Vous pouvez configurer des entités SSL, telles que des serveurs virtuels et des services, sans activer le traitement SSL. Cependant, ils ne fonctionnent pas tant que le traitement SSL n'est pas activé.

Activer le traitement SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
enable ns feature ssl

show ns feature
<!--NeedCopy-->
```

Exemple :

```
enable ns feature SSL
 Done
show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 9)     SSL Offloading                  SSL                 ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```

Activer le traitement SSL à l'aide de l'interface graphique

Accédez à **Système > Paramètres** et, dans le groupe **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités de base**, puis sur **Déchargement SSL**.

Configurer les services

Sur l'appliance Citrix ADC, un service représente un serveur physique ou une application sur un serveur physique. Une fois configurés, les services sont désactivés jusqu'à ce que l'appliance puisse atteindre le serveur physique du réseau et surveiller son état.

Ajouter un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un service et vérifier la configuration :


```
add service <name> (<IP> | <serverName>) <serviceType> <port>
show service <serviceName>
<!--NeedCopy-->
```

Exemple :

```
add service sslsvc 198.51.100.225 SSL 443

Done

sh ssl service sslsvc

            Advanced SSL configuration for Back-end SSL Service sslsvc:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Server Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
            Send Close-Notify: YES
            Strict Sig-Digest Check: DISABLED
            Zero RTT Early Data: ???
            DHE Key Exchange With PSK: ???
            Tickets Per Authentication Context: ???

            ECC Curve: P_256, P_384, P_224, P_521

    1)      Cipher Name: DEFAULT_BACKEND
            Description: Default cipher list for Backend SSL session
     Done
<!--NeedCopy-->
```


Modifier ou supprimer un service à l'aide de l'interface de ligne de commande

Pour modifier un service, utilisez la commande set service, qui ressemble à la commande add service, sauf que vous entrez le nom d'un service existant.

Pour supprimer un service, utilisez la commande rm service, qui accepte uniquement l'argument <name>.

```
rm service <servicename>
<!--NeedCopy-->
```

Exemple :

```
rm service sslsvc
<!--NeedCopy-->
```

Pour modifier un service, utilisez la commande set service, sélectionnez n'importe quel paramètre et modifiez son paramètre.

```
set service <name> (<IP> | <serverName>) <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
set service sslsvc 198.51.100.225 SSL 443
<!--NeedCopy-->
```

Configurer un service à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Services**, créez un service et spécifiez le protocole en tant que protocole SSL.

Configuration du serveur virtuel SSL

Les sessions sécurisées nécessitent l'établissement d'une connexion entre le client et un serveur virtuel SSL sur l'appliance Citrix ADC. Le serveur virtuel SSL intercepte le trafic SSL, le déchiffre et le traite avant de l'envoyer aux services liés au serveur virtuel.

Remarque : le serveur virtuel SSL est marqué comme étant hors tension sur l'appliance Citrix ADC jusqu'à ce qu'une paire de certificat/clé valide et au moins un service y soient liés. Un serveur virtuel basé sur SSL est un serveur virtuel d'équilibrage de charge de type protocole SSL ou SSL_TCP. La fonction d'équilibrage de charge doit être activée sur l'appliance Citrix ADC.

Ajouter un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel SSL et vérifier la configuration :

```
add lb vserver <name> (serviceType) <IPAddress> <port>
show ssl vserver <name>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver sslvs SSL 192.0.2.240 443
Done

sh ssl vserver sslvs

            Advanced SSL configuration for VServer sslvs:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: ENABLED          Refresh Count: 0
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
            HSTS IncludeSubDomains: NO
            HSTS Max-Age: 0
            SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
            Push Encryption Trigger: Always
            Send Close-Notify: YES
            Strict Sig-Digest Check: DISABLED
            Zero RTT Early Data: DISABLED
            DHE Key Exchange With PSK: NO
            Tickets Per Authentication Context: 1
            ECC Curve: P_256, P_384, P_224, P_521

    1)      Cipher Name: DEFAULT
            Description: Default cipher list with encryption strength
                >= 128bit
```



```
32       Done
33 <!--NeedCopy-->
```

Modifier ou supprimer un serveur virtuel SSL à l'aide de l'interface de ligne de commande

Pour modifier les propriétés d'équilibrage de charge d'un serveur virtuel SSL, utilisez la commande `set lb vserver`. La commande set est similaire à la commande `add lb vserver`, sauf que vous entrez le nom d'un serveur virtuel existant. Pour modifier les propriétés **SSL** d'un serveur virtuel SSL, utilisez la commande `set ssl vserver`. Pour plus d'informations, consultez la section « Paramètres du serveur virtuel SSL » plus loin dans cette page.

Pour supprimer un serveur virtuel SSL, utilisez la commande `rm lb vserver`, qui accepte uniquement l'argument `<name>`.

Configurer un serveur virtuel SSL à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, créez un serveur virtuel et spécifiez le protocole en tant que protocole SSL.

Lier des services au serveur virtuel SSL

L'appliance ADC transfère les données SSL déchiffrées aux serveurs du réseau. Pour transférer des données, les services représentant ces serveurs physiques doivent être liés au serveur virtuel qui reçoit les données SSL.

En règle générale, la liaison entre l'appliance ADC et le serveur physique est sécurisée. Par conséquent, le transfert de données entre l'appliance et le serveur physique n'a pas besoin d'être chiffré. Toutefois, vous pouvez fournir un chiffrement de bout en bout en chiffrant le transfert de données entre l'appliance et le serveur. Pour plus de détails, voir Configurer le déchargement SSL avec un chiffrement de bout en bout.

Remarque : Activez la fonctionnalité d'équilibrage de charge sur l'appliance ADC avant de lier les services au serveur virtuel SSL.

Lier un service à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier le service au serveur virtuel et vérifier la configuration :

```
1 bind lb vserver <name> <serviceName>
2 show lb vserver <name>
3 <!--NeedCopy-->
```


Exemple :

```
bind lb vserver sslvs sslsvc
     Done

sh lb vserver sslvs

            sslvs (192.0.2.240:443) - SSL       Type: ADDRESS
            State: DOWN[Certkey not bound]
            Last state change was at Wed May  2 11:43:04 2018
            Time since last state change: 0 days, 00:13:21.150
            Effective State: DOWN
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Appflow logging: ENABLED
            No. of Bound Services :  1 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION      BackupMethod:
               ROUNDROBIN
            Mode: IP
            Persistence: NONE
            Vserver IP and Port insertion: OFF
            Push: DISABLED  Push VServer:
            Push Multi Clients: NO
            Push Label Rule: none
            L2Conn: OFF
            Skip Persistency: None
            Listen Policy: NONE
            IcmpResponse: PASSIVE
            RHIstate: PASSIVE
            New Service Startup Request Rate: 0 PER_SECOND, Increment
               Interval: 0
            Mac mode Retain Vlan: DISABLED
            DBS_LB: DISABLED
            Process Local: DISABLE
            Traffic Domain: 0
            TROFS Persistence honored: ENABLED
            Retain Connections on Cluster: NO
    1) sslsvc (198.51.100.225: 443) - SSL State: DOWN       Weight: 1
     Done
<!--NeedCopy-->
```


Dissocier un service d'un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
unbind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
unbind lb vserver sslvs sslsvc
     Done
<!--NeedCopy-->
```

Lier un service à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel et cliquez sur la vignette **Liaisons de service Serveur virtuel d'équilibrage de charge** sous la section **Services et groupes de services**.
3. Dans la page **Liaison de service Serveur virtuel d'équilibrage de charge**, cliquez sur l'onglet **Ajouter des liaisons**, **cliquez sur Cliquez pour sélectionnersous Sélectionner un service**, puis activez la case à cocher en regard du service à lier.
4. Cliquez sur **Sélectionner** et cliquez sur **Lier**.

Configurer un serveur virtuel d'indication de nom de serveur (SNI) pour l'hébergement sécurisé de plusieurs sites

L'hébergement virtuel est utilisé par les serveurs Web pour héberger plus d'un nom de domaine avec la même adresse IP. L'appliance prend en charge l'hébergement de plusieurs domaines sécurisés en déchargeant le traitement SSL des serveurs Web à l'aide de services SSL transparents ou de déchargement SSL basé sur un serveur virtuel. Toutefois, lorsque plusieurs sites Web sont hébergés sur le même serveur virtuel, la liaison SSL est terminée avant que le nom d'hôte attendu soit envoyé au serveur virtuel. Par conséquent, l'appliance ne peut pas déterminer le certificat à présenter au client après l'établissement d'une connexion. Ce problème est résolu en activant SNI sur le serveur virtuel. SNI est une extension TLS (Transport Layer Security) utilisée par le client pour fournir le nom d'hôte lors de l'initiation de la poignée de main. L'appliance ADC compare ce nom d'hôte au nom commun et, s'il ne correspond pas, le compare au nom alternatif du sujet (SAN). Si le nom correspond, l'appliance présente le certificat correspondant au client.

Un certificat SSL générique permet d'activer le chiffrement SSL sur plusieurs sous-domaines si la même organisation contrôle ces domaines et que le nom de domaine de deuxième niveau est le même. Par exemple, un certificat générique émis à un réseau sportif sous le nom commun

« *.sports.net » peut être utilisé pour sécuriser des domaines, tels que « login.sports.net » et « help.sports.net ». Il ne peut pas sécuriser le domaine « login.ftp.sports.net ».

Remarque :
sur une appliance ADC, seules les entrées DNS de nom de domaine, d'URL et d'ID de messagerie dans le champ **SAN**sont comparées.

Vous pouvez lier plusieurs certificats de serveur à un seul serveur virtuel SSL ou un service transparent à l'aide de l'option -snicert. Le serveur virtuel ou le service émet ces certificats si SNI est activé sur le serveur ou le service virtuel. Vous pouvez activer SNI à tout moment.

Liez plusieurs certificats de serveur à un seul serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer SNI et vérifier la configuration :

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )]

bind ssl vserver <vServerName>@ -certkeyName <string> -SNICert

show ssl vserver <vServerName>
<!--NeedCopy-->
```

Pour lier plusieurs certificats de serveur à un service transparent à l'aide de l'interface de ligne de commande, remplacez `vserver` par le service et `vservername` par le nom de service dans les commandes précédentes.

Remarque : Créez le service SSL avec l'option `-clearTextPort 80`.

Liez plusieurs certificats de serveur à un serveur virtuel SSL unique à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel SSL et, dans **Certificats**, sélectionnez **Certificat de serveur**.
3. Ajoutez un certificat ou sélectionnez un certificat dans la liste, puis cliquez sur **Certificat de serveur pour SNI**.
4. Dans **Paramètres avancés**, sélectionnez **Paramètres SSL**.
5. Cliquez sur **Activation SNI**.

Prise en charge de SNI sur le service back-end

> **Remarque** : SNI n'est pas pris en charge sur un service dorsal DTLS.

L'appliance Citrix ADC prend en charge l'indication de nom de serveur (SNI) au niveau du back-end. Autrement dit, le nom commun est envoyé comme nom de serveur dans le client bonjour au serveur principal pour la réussite de la poignée de main. Ce support permet de répondre aux exigences de sécurité des clients de l'intégrateur de systèmes fédéral. En outre, SNI offre l'avantage d'utiliser un seul port au lieu d'ouvrir des centaines d'adresses IP et de ports différents sur un pare-feu.

Les exigences de sécurité des clients de l'intégrateur de système fédéral incluent la prise en charge des services ADFS (Active Directory Federation Services) 3.0 dans 2012R2 et les serveurs WAP. Pour répondre à cette exigence, la prise en charge de SNI au back-end d'une appliance Citrix ADC est requise.

> **Remarque :**
>
> Pour que SNI fonctionne, le nom du serveur dans le client Hello doit correspondre au nom d'hôte configuré sur le service principal lié à un serveur virtuel SSL. Par exemple, si le nom d'hôte du serveur principal est www.mail.example.com, le service principal compatible SNI doit être configuré avec le nom du serveur comme https://www.mail.example.com. Et ce nom d'hôte doit correspondre au nom du serveur dans le client hello.

Prise en charge de SNI dynamique sur le service back-end

L'appliance Citrix ADC prend en charge les connexions SNI dynamiques sur les connexions TLS dorsales. En d'autres termes, l'appliance apprend le SNI dans la connexion client et l'utilise dans la connexion côté serveur. Vous n'avez plus besoin de spécifier un nom commun dans le service, le groupe de services ou le profil SSL. Le nom commun reçu dans l'extension SNI du message Client Hello est transmis à la connexion SSL back-end.

Auparavant, vous deviez configurer des SNI statiques sur les services SSL, les groupes de services et les profils SSL. Par conséquent, seule l'extension SNI statique configurée a été envoyée au serveur. Si un client avait besoin d'accéder à plusieurs domaines simultanément, l'appliance ADC n'était pas en mesure d'envoyer le SNI reçu du client au service back-end. Au lieu de cela, il a envoyé le nom commun statique qui a été configuré. Désormais, si le serveur principal est configuré pour plusieurs domaines, le serveur peut répondre avec le certificat correct basé sur le SNI reçu dans le message Client Hello de l'appliance.

Pointez à la note :

- SNI doit être activé sur le front end et le certificat SNI correct lié au serveur virtuel SSL. Si vous n'activez pas SNI sur le front end, les informations SNI ne sont pas transmises au back-end.
- Lorsque l'authentification du serveur est activée, le certificat de serveur est vérifié par le certificat de l'autorité de certification et les entrées de nom commun/SAN dans le certificat de serveur

sont mises en correspondance avec le SNI. Par conséquent, le certificat de l'autorité de certification doit être lié au service.

- La réutilisation de la connexion back-end et de la session SSL est basée sur SNI lorsque SNI dynamique est activé.

Les moniteurs SSL n'envoient pas de SNI lorsque SNI dynamique est activé. Pour une sonde basée sur SNI, attachez un profil back-end sur lequel SNI statique est configuré aux moniteurs SSL. Le moniteur doit être configuré avec le même en-tête personnalisé que SNI.

Configurer SNI sur le service principal à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add service <name>  <IP>  <serviceType>  <port>

add lb vserver <name>  <IPAddress> <serviceType>  <port>

bind lb vserver <name> <serviceName>

set ssl service <serviceName> -SNIEnable ENABLED -commonName <string>

set ssl profile <name> -SNIEnable ENABLED
<!--NeedCopy-->
```

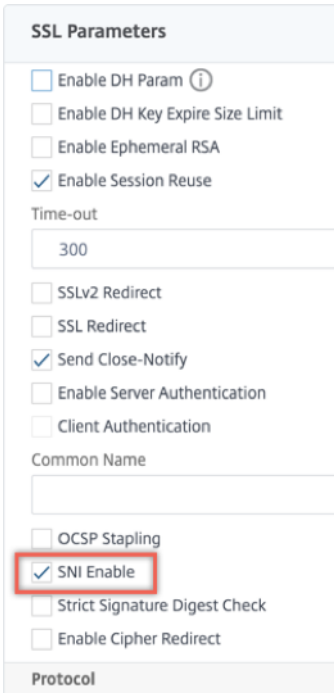
Exemple :

```
    add service service_ssl 198.51.100.100 SSL 443

    add lb vserver ssl-vs 203.0.113.200 SSL 443

    bind lb vserver ssl-vs service_ssl

    set ssl service service_ssl -SNIEnable ENABLED  - commonName www.
       example.com

    set ssl profile sslprof -SNIEnable ENABLED
<!--NeedCopy-->
```

Configurer SNI sur le service principal à l'aide de l'interface graphique

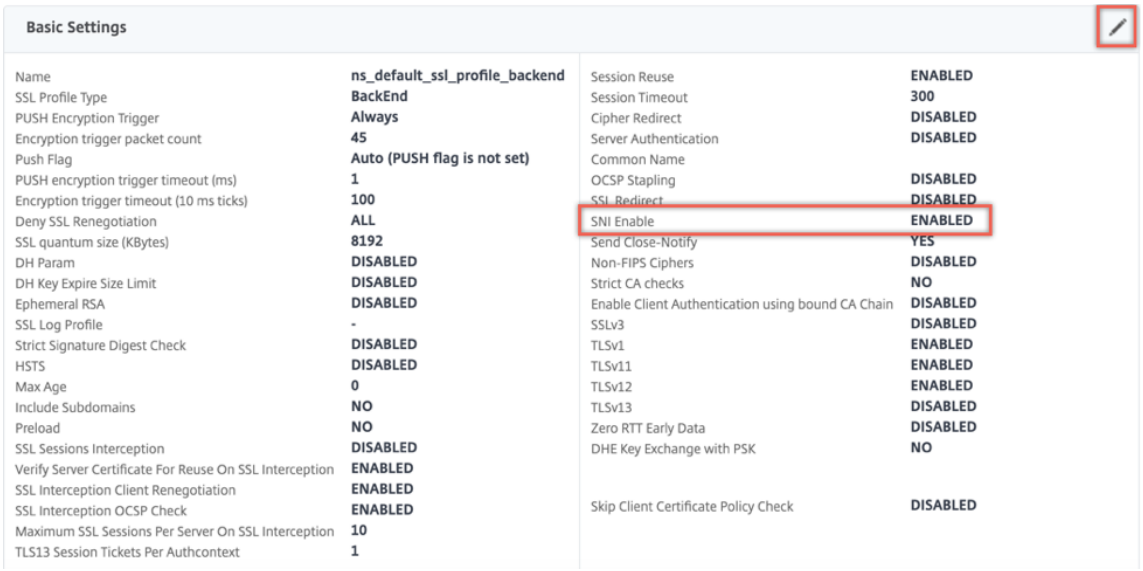
1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Sélectionnez un service SSL et, dans **Paramètres avancés**, cliquez sur **Paramètres SSL**.

3. Cliquez sur **Activation SNI**.



Configurer SNI sur le profil SSL à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profil SSL**.
2. Cliquez sur **Ajouter**.
3. Dans **Paramètres de base**, sélectionnez **Activation SNI**.



4. Cliquez sur **OK**.

Liez un moniteur sécurisé à un service back-end compatible SNI

Vous pouvez lier des moniteurs sécurisés de type HTTP, HTTP-ECV, TCP ou TCP-ECV aux services back-end et aux groupes de services qui prennent en charge SNI. Toutefois, les sondes du moniteur n'envoient pas l'extension SNI si SNI dynamique est activé. Pour envoyer des sondes SNI, activez SNI statique dans le profil SSL back-end et liez le profil au moniteur. Définissez l'en-tête personnalisé dans le moniteur sur le nom du serveur qui est envoyé en tant qu'extension SNI dans le Hello client de la sonde moniteur.

Configurer et lier un moniteur sécurisé à un service back-end compatible SNI à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

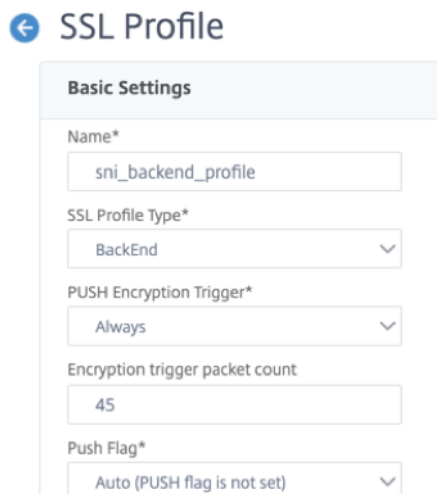
```
add lb monitor <monitorName> <type> -secure YES
add ssl profile <name> -sslProfileType BackEnd
set lb monitor <monitorName> <type> -customHeaders <string> -sslprofile
    <backend ssl profile>
set ssl profile <name> -sniEnable ENABLED -commonName <string>
bind service <name> -monitorName <string>
<!--NeedCopy-->
```

Exemple :

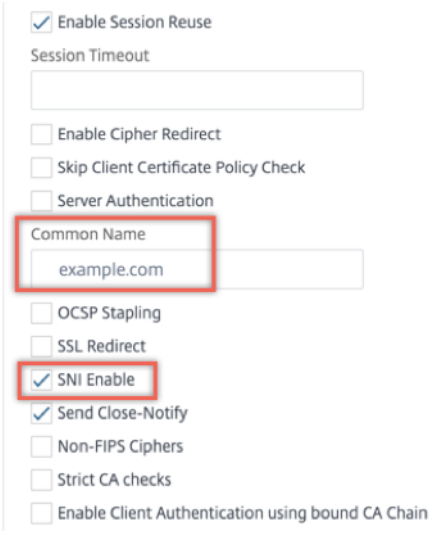
```
add ssl profile sni_backend_profile -sslProfileType BackEnd
set ssl profile sni_backend_profile -sniEnable ENABLED -commonName
   example.com
add lb monitor http-ecv-mon HTTP-ECV -secure YES
set monitor http-ecv-mon HTTP-ECV -customHeaders "Host: example.com\r\n
   " -sslprofile sni_backend_profile
bind service ssl_service  - monitorName http-ecv-mon
<!--NeedCopy-->
```

Configurer et lier un moniteur sécurisé à un service back-end compatible SNI à l'aide de l'interface graphique

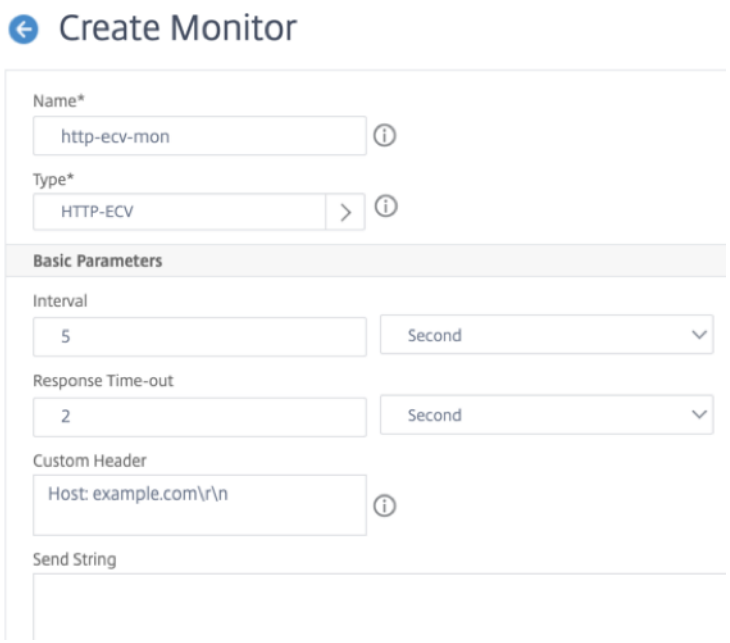
1. Accédez à **Système > Profils > Profils SSL**.
2. Cliquez sur **Ajouter**.
3. Spécifiez un nom pour le profil et dans **Type de profil SSL**, sélectionnez **Backend**.



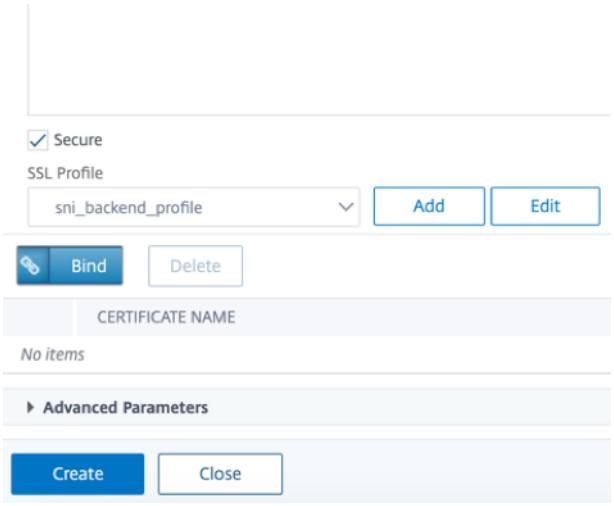
4. Spécifiez le nom commun (identique à l'en-tête d'hôte) et sélectionnez **SNI Enable**.



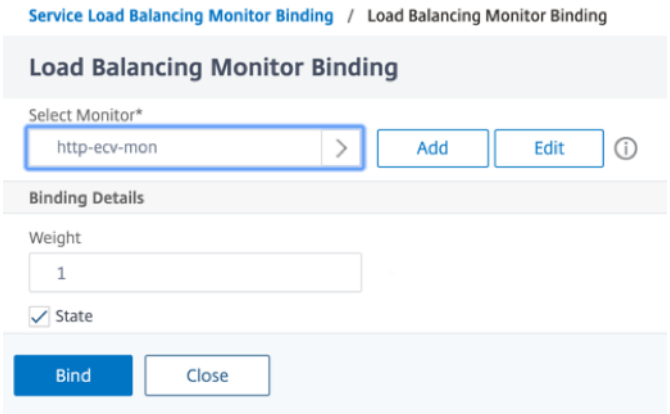
5. Cliquez sur **OK**.
6. Accédez à **Gestion du trafic > Équilibrage de charge > Surveiller**.
7. Cliquez sur **Ajouter**.
8. Spécifiez un nom pour le moniteur. Dans **Type**, sélectionnez HTTP, HTTP-ECV, TCP ou TCP-ECV.
9. Spécifiez un **en-tête personnalisé**.



10. Sélectionnez **Sécurisé**.
11. Dans **Profile SSL**, sélectionnez le profil SSL back-end créé dans les étapes précédentes.
12. Cliquez sur **Créer**.



13. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
14. Sélectionnez un service SSL et cliquez sur **Modifier**.
15. Dans **Moniteurs**, cliquez sur **Ajouter une liaison**, sélectionnez le moniteur créé dans les étapes précédentes, puis cliquez sur **Lier**.



Configurer et lier un moniteur sécurisé à un service back-end compatible SNI à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteur**.
2. Ajoutez un moniteur de type **HTTP-ECV** ou **TCP-ECV** et spécifiez un **en-tête personnalisé**.
3. Sélectionnez **Créer**.
4. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
5. Sélectionnez un service SSL et cliquez sur **Modifier**.
6. Dans **Moniteurs**, cliquez sur **Ajouter une liaison**, sélectionnez le moniteur créé à l'étape 3, puis cliquez sur **Lier**.

Ajouter ou mettre à jour une paire de clés de certificat

> **Remarques :**
>
> Si vous ne possédez pas de certificat ni de clé existants, reportez-vous à la section Créer un certificat.
>
> Pour créer une paire de clés de certificat ECDSA, cliquez sur Créer une paire de clés de certificat ECDSA.
>
> À partir de la version 41.x, les noms de certificats pouvant contenir jusqu'à 63 caractères sont pris en charge.
>
> Depuis la version 13.0 build 79.x, les paires de clés de certificat protégées par mot de passe sont toujours ajoutées avec succès. Auparavant, si l'option de mot de passe fort était activée sur une appliance Citrix ADC, les paires de clés de certificat protégées par mot de passe n'étaient parfois pas ajoutées. Toutefois, la configuration de la clé de certificat est perdue si vous rétrogradez vers une version antérieure. De plus, dans la réponse de l'API NITRO pour les paires de clés de certificat, la `passplain` variable est envoyée à la place de la `passcrypt` variable.

Pour toute transaction SSL, le serveur a besoin d'un certificat valide et de la paire de clés privées et

publiques correspondante. Les données SSL sont chiffrées avec la clé publique du serveur, qui est disponible via le certificat du serveur. Le décryptage nécessite la clé privée correspondante. Le mot de passe de la clé privée utilisée lors de l'ajout d'une paire de clés de certificat SSL est enregistré à l'aide d'une clé de chiffrement unique pour chaque appliance Citrix ADC.

L'appliance ADC décharge les transactions SSL du serveur. Par conséquent, le certificat et la clé privée du serveur doivent être présents sur l'appliance, et le certificat doit être jumelé à sa clé privée correspondante. Cette paire de clés de certificat doit être liée au serveur virtuel qui traite les transactions SSL.

Remarque : Le certificat par défaut sur une appliance Citrix ADC est de 2048 bits. Dans les versions précédentes, le certificat par défaut était 512 bits ou 1024 bits. Après la mise à niveau vers la version 11.0, vous devez supprimer toutes vos anciennes paires de clés de certificat en commençant par`"ns-"`, puis redémarrer l'appliance pour générer automatiquement un certificat par défaut de 2048 bits.

Le certificat et la clé doivent tous deux se trouver dans le stockage local de l'appliance Citrix ADC avant de pouvoir être ajoutés à l'appliance. Si votre certificat ou fichier de clé ne se trouve pas sur l'appliance, téléchargez-le sur l'appliance avant de créer la paire.

Important : les certificats et les clés sont stockés dans le répertoire /nsconfig/ssl par défaut. Si vos certificats ou clés sont stockés dans un autre emplacement, vous devez fournir le chemin d'accès absolu aux fichiers de l'appliance Citrix ADC. Les appliances Citrix ADC FIPS ne prennent pas en charge les clés externes (clés non FIPS). Sur une appliance FIPS, vous ne pouvez pas charger de clés à partir d'un périphérique de stockage local tel qu'un disque dur ou une mémoire flash. Les clés FIPS doivent être présentes dans le Hardware Security Module (HSM) de l'appliance.

Seules les clés RSA sont prises en charge sur les appliances Citrix ADC.

Définissez la période de notification et activez le moniteur d'expiration pour émettre une invite avant l'expiration du certificat.

L'appliance Citrix ADC prend en charge les formats d'entrée suivants du certificat et des fichiers de clé privée :

- PEM - Courrier amélioré en matière de confidentialité
- DER - Règle de codage distinguée
- PFX - Échange de renseignements personnels

Le logiciel détecte automatiquement le format. Par conséquent, vous n'êtes plus obligé de spécifier le format dans le paramètre inform. Si vous spécifiez le format (correct ou incorrect), le logiciel l'ignore. Le format du certificat et du fichier de clé doivent être identiques.

Remarque : Un certificat doit être signé à l'aide de l'un des algorithmes de hachage suivants :

- MD5
- SHA-1
- SHA-224

- SHA-256
- SHA-384 (pris en charge uniquement sur l'extrémité frontale)
- SHA-512 (pris en charge uniquement sur l'extrémité frontale)

Une appliance MPX prend en charge les certificats de 512 bits ou plus, jusqu'aux tailles suivantes :

- Certificat de serveur 4096 bits sur le serveur virtuel
- Certificat client 4096 bits sur le service
- Certificat d'autorité de certification 4096 bits (inclut les certificats intermédiaires et racine)
- Certificat 4096 bits sur le serveur principal
- Certificat client 4096 bits (si l'authentification client est activée sur le serveur virtuel)

Un dispositif virtuel VPX prend en charge les certificats de 512 bits ou plus, jusqu'aux tailles suivantes :

- Certificat de serveur 4096 bits sur le serveur virtuel
- Certificat client 4096 bits sur le service
- Certificat d'autorité de certification 4096 bits (inclut les certificats intermédiaires et racine)
- Certificat 4096 bits sur le serveur principal
- Certificat client 4096 bits (si l'authentification client est activée sur le serveur virtuel)

> **Remarque**
>
> Une appliance Citrix ADC SDX prend en charge les certificats de 512 bits ou plus. Chaque instance Citrix ADC VPX hébergée sur l'appliance prend en charge les tailles de certificat précédentes pour une appliance virtuelle VPX. Toutefois, si une puce SSL est affectée à une instance, cette instance prend en charge les tailles de certificat prises en charge par une appliance MPX.

Ajouter une paire de clés de certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter une paire de clés de certificat et vérifier la configuration :

```
add ssl certKey <certkeyName> -cert <string>[(-key <string> [-password
    ]) | -fipsKey <string>] [-inform ( DER | PEM )] [<passplain>] [-
    expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
    positive_integer>]]

show ssl certKey [<certkeyName>]
<!--NeedCopy-->
```

Exemple :

```
add ssl certKey sslckey -cert server_cert.pem -key server_key.pem -
    password ssl -expiryMonitor ENABLED -notificationPeriod 30
 Done
Note: For FIPS appliances, replace -key with -fipskey
```



```
4
5  show ssl certKey sslckey
6          Name: sslckey           Status: Valid,   Days to expiration
               :8418
7          Version: 3
8          Serial Number: 01
9          Signature Algorithm: md5WithRSAEncryption
10         Issuer:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.root.com
11         Validity
12                 Not Before: Jul 15 02:25:01 2005 GMT
13                 Not After : Nov 30 02:25:01 2032 GMT
14         Subject:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.server.com
15         Public Key Algorithm: rsaEncryption
16         Public Key size: 2048
17  Done
18 <!--NeedCopy-->
```

Mettre à jour ou supprimer une paire de clés de certificat à l'aide de l'interface de ligne de commande

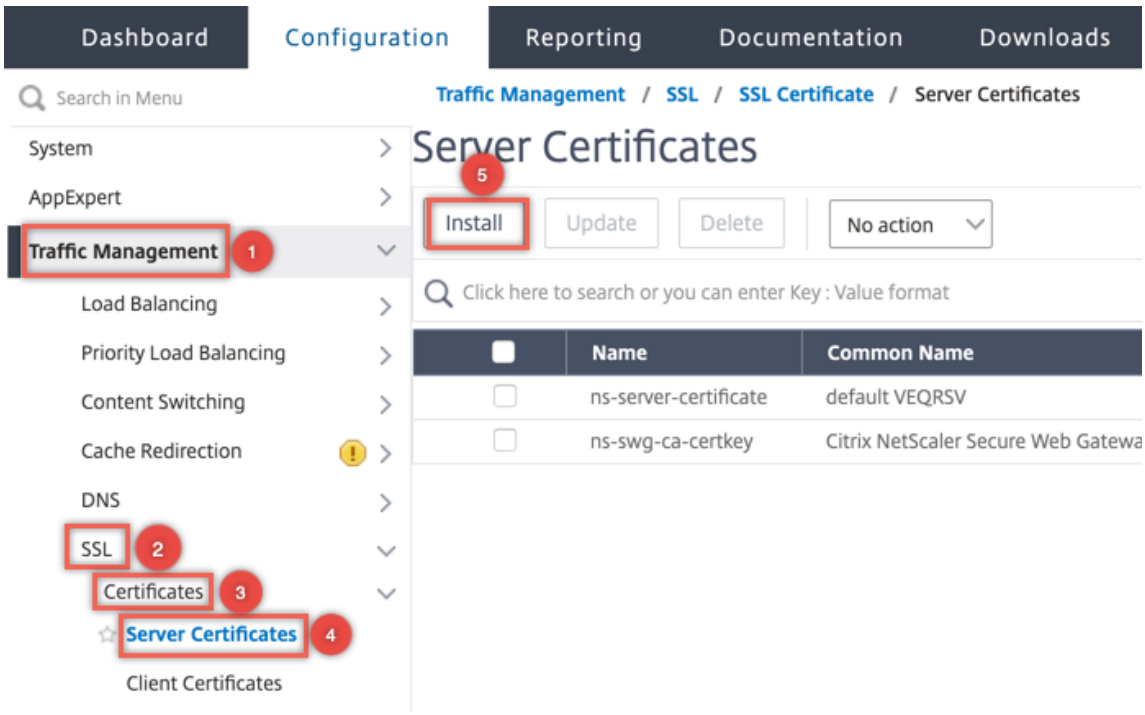
Pour modifier le moniteur d'expiration ou la période de notification dans une paire de clés de certificat, utilisez la commande `set ssl certkey`. Pour remplacer le certificat ou la clé dans une paire de clés de certificat, utilisez la commande `update ssl certkey`. La commande `update ssl certkey` a un paramètre supplémentaire pour remplacer la vérification du domaine. Pour les deux commandes, entrez le nom d'une paire de clés de certificat existante. Pour supprimer une paire de clés de certificat SSL, utilisez la commande `rm ssl certkey`, qui accepte uniquement l'argument `<certkeyName>`.

Exemple :

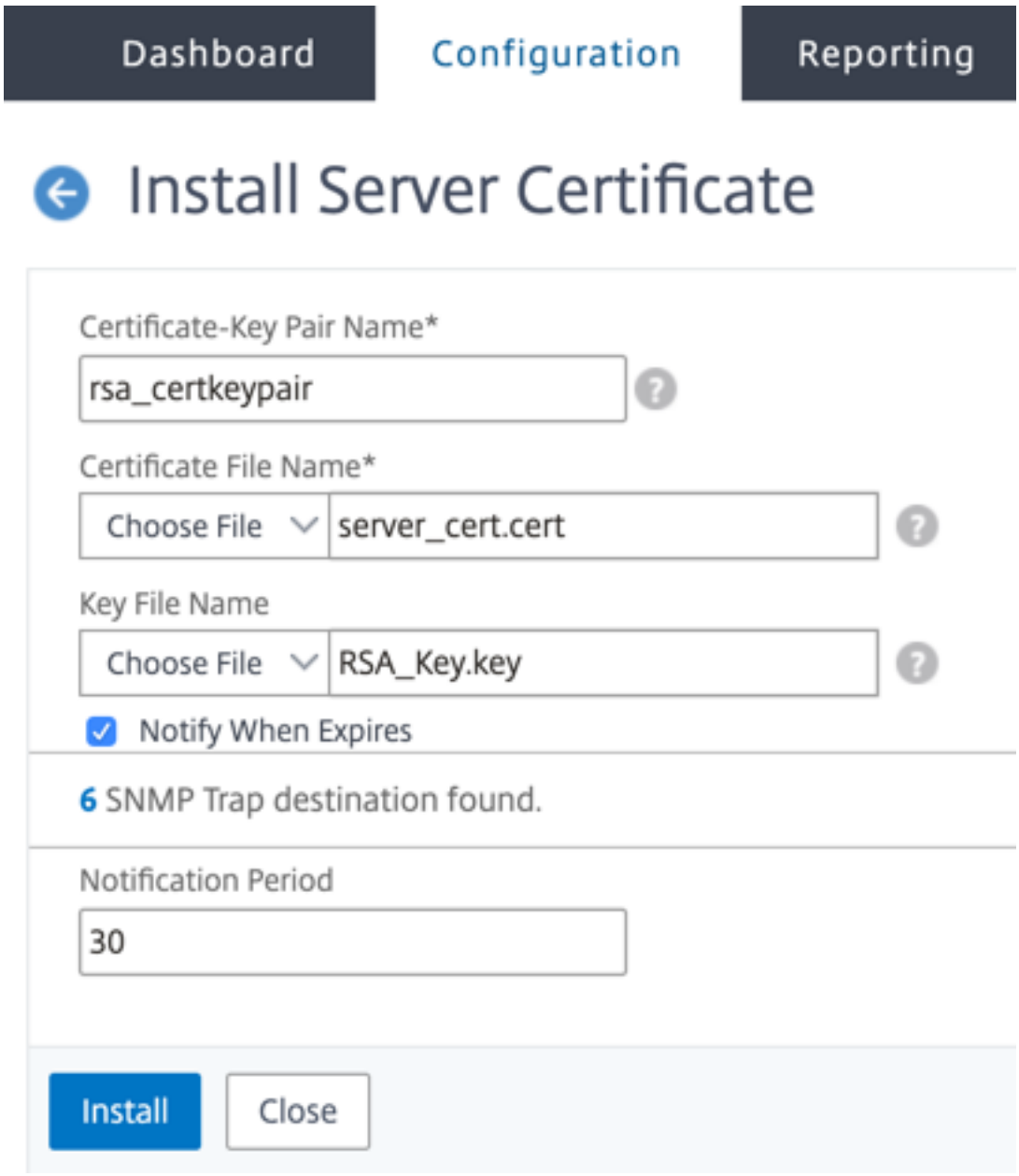
```
1 set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED | DISABLED )
2        [-notificationPeriod <positive_integer>]]
3
4 update ssl certKey <certkeyName> [-cert <string> [-password]] [-key
5        <string> | -fipsKey <string>] [-inform <inform>] [-noDomainCheck
            ]
6 <!--NeedCopy-->
```

Ajouter ou mettre à jour une paire de clés de certificat à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Certificats > Serveur**.



2. Entrez les valeurs des paramètres suivants et cliquez sur **Installer**.
   - Nom de la paire de clés de certificat - Nom du certificat et de la paire de clés privées.
   - Nom du fichier du certificat - Certificat signé reçu de l'autorité de certification.
   - Nom du fichier de clé - Nom du fichier de clé privée et éventuellement chemin d'accès au fichier de clé privée utilisé pour former la paire de clés de certificat.



Lier la paire de clés de certificat au serveur virtuel SSL

Important : associez tous les certificats intermédiaires à ce certificat avant de lier le certificat à un serveur virtuel SSL. Pour plus d'informations sur la liaison des certificats, voir Créer une chaîne de certificats.

Le certificat utilisé pour le traitement des transactions SSL doit être lié au serveur virtuel qui reçoit les données SSL. Si plusieurs serveurs virtuels reçoivent des données SSL, une paire de clés de certificat valide doit être liée à chacun d'eux.

Utilisez un certificat SSL existant valide que vous avez chargé sur l'appliance Citrix ADC. Comme alter-

native à des fins de test, créez votre propre certificat SSL sur l'appliance. Les certificats intermédiaires créés à l'aide d'une clé FIPS sur l'appliance ne peuvent pas être liés à un serveur virtuel SSL.

Lors de la prise de contact SSL, dans le message de demande de certificat lors de l'authentification client, le serveur répertorie les noms distincts (DN) de toutes les autorités de certification (CA) liées au serveur. Le serveur accepte un certificat client uniquement à partir de cette liste. Si vous ne souhaitez pas que le nom DN d'un certificat d'autorité de certification spécifique soit envoyé au client SSL, définissez l'indicateur `skipCA`. Ce paramètre indique que le nom unique du certificat d'autorité de certification particulière ne doit pas être envoyé au client SSL.

Pour plus d'informations sur la création de votre propre certificat, consultez Gestion des certificats.

Remarque : Citrix vous recommande d'utiliser uniquement des certificats SSL valides émis par une autorité de certification approuvée.

Lier une paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une paire de clés de certificat SSL à un serveur virtuel et vérifier la configuration :

```
1 - bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName
    > -CA -skipCAName
2 - show ssl vserver <vServerName>
3 <!--NeedCopy-->
```

Exemple :

```
1 bind ssl vs vs1 -certkeyName cert2 -CA -skipCAName
2  Done
3 sh ssl vs vs1
4
5  Advanced SSL configuration for VServer vs1:
6
7  DH: DISABLED
8
9  Ephemeral RSA: ENABLED Refresh Count: 0
10
11  Session Reuse: ENABLED Timeout: 120 seconds
12
13  Cipher Redirect: DISABLED
14
15  SSLv2 Redirect: DISABLED
16
17  ClearText Port: 0
```



```
18
19   Client Auth: DISABLED
20
21   SSL Redirect: DISABLED
22
23   Non FIPS Ciphers: DISABLED
24
25   SNI: DISABLED
26
27   OCSP Stapling: DISABLED
28
29   HSTS: DISABLED
30
31   IncludeSubDomains: NO
32
33   HSTS Max-Age: 0
34
35   SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: DISABLED
        TLSv1.2: DISABLED
36
37   Push Encryption Trigger: Always
38
39   Send Close-Notify: YES
40
41   Strict Sig-Digest Check: DISABLED
42
43 ECC Curve: P_256, P_384, P_224, P_521
44
45   1) CertKey Name: cert1 CA Certificate OCSPCheck: Optional CA_Name Sent
46   2) CertKey Name: cert2 CA Certificate OCSPCheck: Optional CA_Name
        Skipped
47   1) Cipher Name: DEFAULT
48
49 Description: Default cipher list with encryption strength >= 128bit
50 Done
51 <!--NeedCopy-->
```

Dissocier une paire de clés de certificat SSL d'un serveur virtuel à l'aide de l'interface de ligne de commande

Si vous essayez de dissocier une paire de clés de certificat d'un serveur virtuel à l'aide de la commande `unbind ssl certKey <certkeyName>`, un message d'erreur s'affiche. L'erreur apparaît car la syntaxe de la commande a changé. À l'invite de commandes, tapez la commande suivante :

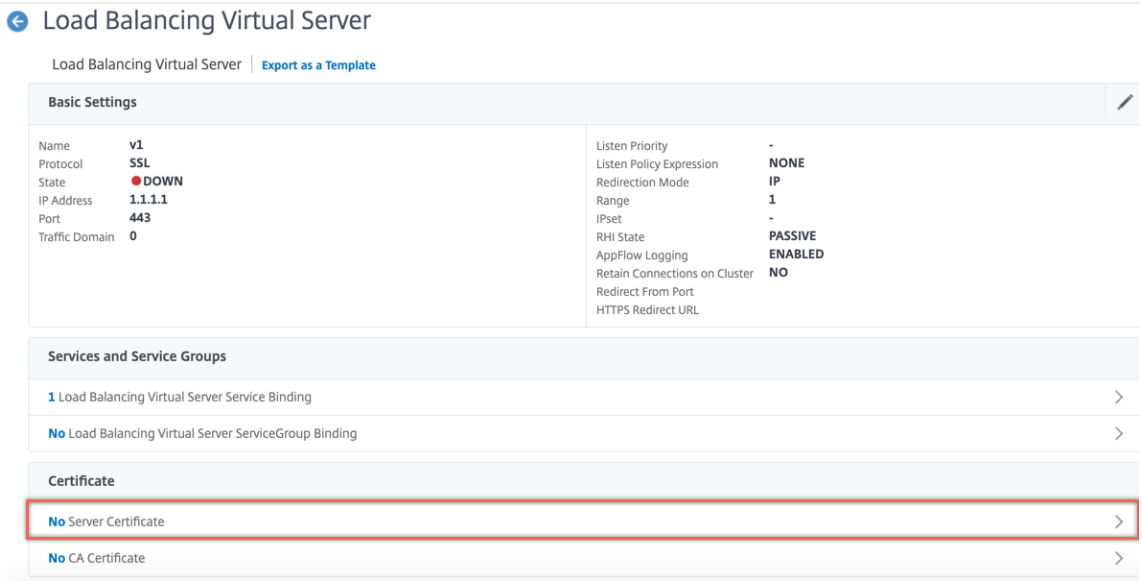

```
unbind ssl vserver <vServerName> -certkeyName <string>
<!--NeedCopy-->
```

Exemple :

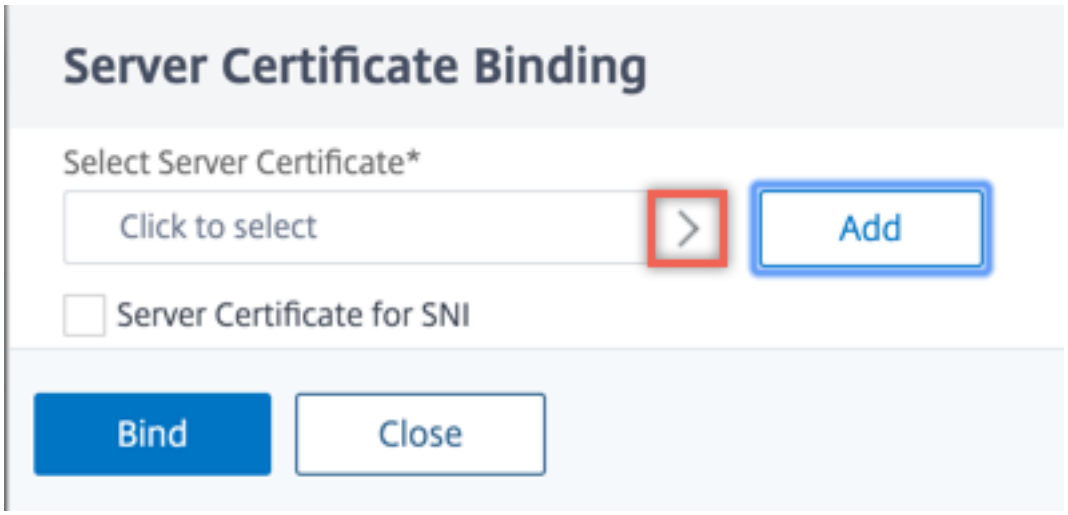
```
unbind ssl vserver vssl -certkeyName sslckey
<!--NeedCopy-->
```

Lier une paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface graphique

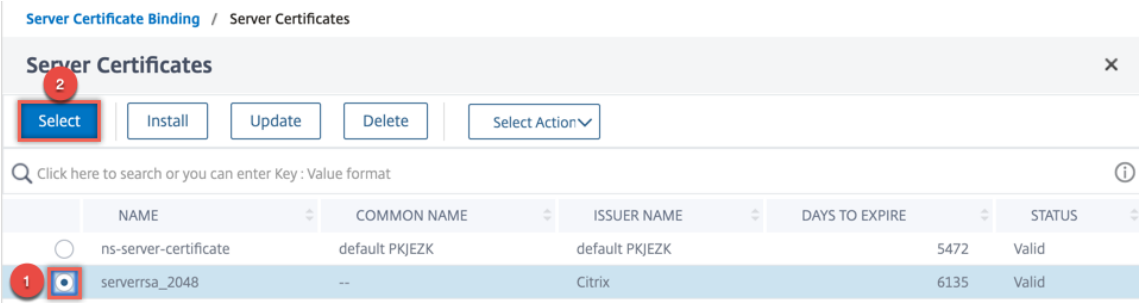
1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et ouvrez un serveur virtuel SSL. Cliquez dans la section **Certificat**.



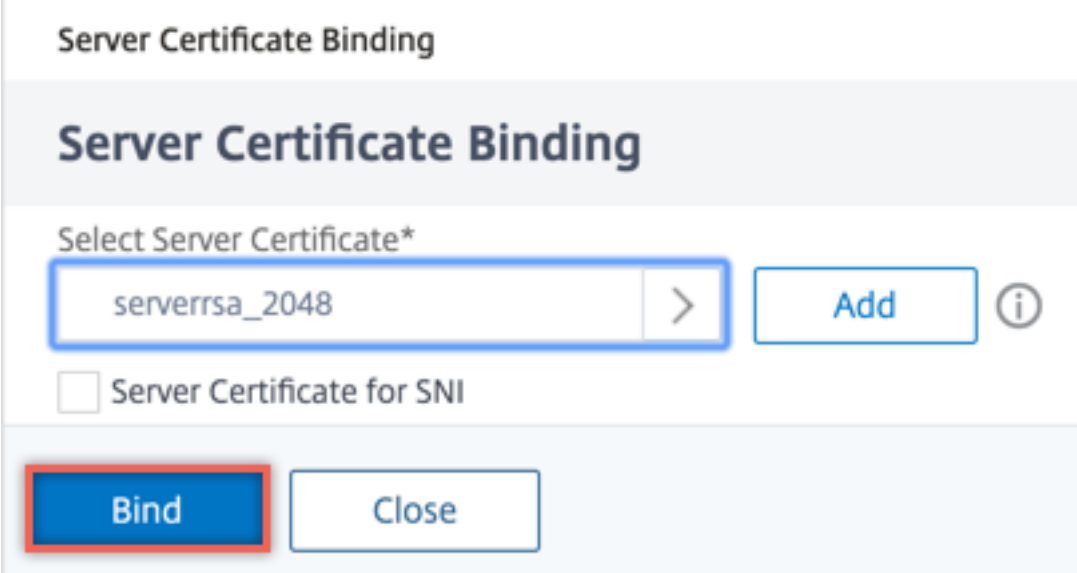
2. Cliquez sur la flèche pour sélectionner la paire de clés de certificat.



3. Sélectionnez la paire de clés de certificat dans la liste.



4. Liez la paire de clés de certificat au serveur virtuel. Pour ajouter un certificat de serveur en tant que certificat SNI, sélectionnez **Certificat de serveur pour SNI**.



Paramètres du serveur virtuel SSL

Définissez la configuration SSL avancée pour un serveur virtuel SSL. Vous pouvez également définir plusieurs de ces paramètres dans un profil SSL. Pour plus d'informations sur les paramètres pouvant être définis dans un profil SSL, consultez Paramètres de profil SSL.

Définir les paramètres du serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl vserver <vServerName>@ [-clearTextPort <port>] [-dh ( ENABLED |
    DISABLED ) -dhFile <string>] [-dhCount <positive_integer>][-
    dhKeyExpSizeLimit ( ENABLED | DISABLED )] [-eRSA ( ENABLED |
    DISABLED) [-eRSACount <positive_integer>]] [-sessReuse ( ENABLED |
    DISABLED )[-sessTimeout <positive_integer>]] [-cipherRedirect (
```



```
      ENABLED | DISABLED ) [-cipherURL <URL>]] [-sslv2Redirect ( ENABLED |
       DISABLED )[-sslv2URL <URL>]] [-clientAuth ( ENABLED | DISABLED ) [-
      clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED |
      DISABLED )][-redirectPortRewrite ( ENABLED | DISABLED )] [-ssl2 (
      ENABLED | DISABLED )] [-ssl3 ( ENABLED | DISABLED )] [-tls1 (
      ENABLED | DISABLED )] [-tls11 ( ENABLED | DISABLED )] [-tls12 (
      ENABLED | DISABLED )][-tls13 ( ENABLED | DISABLED )] [-SNIEnable (
      ENABLED | DISABLED )][-ocspStapling ( ENABLED | DISABLED )] [-
      pushEncTrigger <pushEncTrigger>] [-sendCloseNotify ( YES | NO )] [-
      dtlsProfileName <string>] [-sslProfile <string>] [-HSTS ( ENABLED |
      DISABLED )][-maxage <positive_integer>] [-IncludeSubdomains ( YES |
      NO )][-strictSigDigestCheck ( ENABLED | DISABLED )] [-
      zeroRttEarlyData (ENABLED | DISABLED )] [-
      tls13SessionTicketsPerAuthContext <positive_integer>] [-
      dheKeyExchangeWithPsk ( YES | NO )]
<!--NeedCopy-->
```

Paramètres Diffie-Hellman (DH)

Pour utiliser des chiffrements sur l'appliance qui nécessitent un échange de clés DH pour configurer la transaction SSL, activez l'échange de clés DH sur l'appliance. Configurez d'autres paramètres en fonction de votre réseau.

Pour répertorier les chiffrements pour lesquels les paramètres DH doivent être définis à l'aide de l'interface de ligne de commande, tapez : sh cipher DH.

Pour répertorier les chiffrements pour lesquels les paramètres DH doivent être définis à l'aide de l'utilitaire de configuration, accédez à **Gestion du trafic > SSL > Groupes de chiffrement**, puis double-cliquez sur **DH**.

Pour plus d'informations sur la façon d'activer l'échange de clés DH, voir Générer une clé Diffie-Hellman (DH).

Configurer les paramètres DH à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer les paramètres DH et vérifier la configuration :

```
- `set ssl vserver <vserverName> -dh <Option> -dhCount <
   RefreshCountValue> -filepath <string>
- show ssl vserver <vServerName>`
<!--NeedCopy-->
```

Exemple :


```
set ssl vserver vs-server -dh ENABLED  -dhFile /nsconfig/ssl/ns-server.cert -dhCount 1000
Done

show ssl vserver vs-server

            Advanced SSL configuration for VServer vs-server:
            DH: ENABLED
            Ephemeral RSA: ENABLED          Refresh Count: 1000
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
            HSTS IncludeSubDomains: NO
            HSTS Max-Age: 0
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2: ENABLED  TLSv1.2: ENABLED

    1)      Cipher Name: DEFAULT
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Configurer les paramètres DH à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Activer le param DH**, puis spécifiez un nombre d'actualisation et un chemin d'accès au fichier.

RSA éphémère

Ephemeral RSA permet aux clients d'exportation de communiquer avec le serveur sécurisé même si le certificat de serveur ne prend pas en charge les clients d'exportation (certificat 1024 bits). Si vous souhaitez empêcher les clients d'exportation d'accéder à l'objet Web sécurisé ou à la ressource, vous devez désactiver l'échange de clés RSA éphémères.

Par défaut, cette fonctionnalité est activée sur l'appliance Citrix ADC, le nombre d'actualisation étant défini sur zéro (utilisation infinie).

Remarque :

La clé RSA éphémère est automatiquement générée lorsque vous liez un chiffrement d'exportation à un serveur ou service virtuel SSL SSL ou TCP. Lorsque vous supprimez le chiffrement d'exportation, la clé ERSA n'est pas supprimée. Il est réutilisé ultérieurement lorsqu'un autre chiffrement d'exportation est lié à un serveur ou service virtuel SSL SSL ou TCP. La clé ERSA est supprimée lorsque le système redémarre.

Configurer RSA éphémère à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer RSA éphémère et vérifier la configuration :

```
set ssl vserver <vServerName> -eRSA (enabled | disabled) -eRSACount <
   positive_integer>
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver vs-server -eRSA ENABLED -eRSACount 1000
 Done

show ssl vserver vs-server

        Advanced SSL configuration for VServer vs-server:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 1000
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        OCSP Stapling: DISABLED
        HSTS: DISABLED
        HSTS IncludeSubDomains: NO
        HSTS Max-Age: 0
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
           ENABLED  TLSv1.2: ENABLED
```



```
22
23 1)      Cipher Name: DEFAULT
24         Description: Predefined Cipher Alias
25  Done
26 <!--NeedCopy-->
```

Configurer RSA éphémère à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Activer le RSA éphémère**et spécifiez un nombre d'actualisations.

Réutilisation des sessions

Pour les transactions SSL, l'établissement de la liaison SSL initiale nécessite des opérations de chiffrement de clé publique à forte intensité de CPU. La plupart des opérations de poignée de main sont associées à l'échange de la clé de session SSL (message d'échange de clé client). Lorsqu'une session client est inactive pendant un certain temps et est ensuite reprise, la poignée de main SSL est généralement réexécutée. Lorsque la réutilisation de session est activée, l'échange de clés de session est évité pour les demandes de reprise de session reçues du client.

La réutilisation de session est activée sur l'appliance Citrix ADC par défaut. L'activation de cette fonctionnalité réduit la charge du serveur, améliore le temps de réponse et augmente le nombre de transactions SSL par seconde (TPS) que le serveur peut prendre en charge.

Configurer la réutilisation de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la réutilisation de session et vérifier la configuration :

```
1 set ssl vserver <vServerName> -sessReuse ( ENABLED | DISABLED ) -
     sessTimeout <positive_integer>
2 show ssl vserver <vServerName>
3 <!--NeedCopy-->
```

Exemple :

```
1 set ssl vserver vs-ssl -sessreuse enabled -sesstimeout 600
2  Done
3
4 show ssl vserver vs-ssl
5
```



```
6           Advanced SSL configuration for VServer vs-ssl:
7           DH: DISABLED
8           Ephemeral RSA: ENABLED          Refresh Count: 1000
9           Session Reuse: ENABLED          Timeout: 600 seconds
10          Cipher Redirect: DISABLED
11          SSLv2 Redirect: DISABLED
12          ClearText Port: 0
13          Client Auth: DISABLED
14          SSL Redirect: DISABLED
15          Non FIPS Ciphers: DISABLED
16          SNI: DISABLED
17          OCSP Stapling: DISABLED
18          HSTS: DISABLED
19          HSTS IncludeSubDomains: NO
20          HSTS Max-Age: 0
21          SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
                ENABLED  TLSv1.2: ENABLED
22
23  1)      CertKey Name: Auth-Cert-1       Server Certificate
24
25  1)      Cipher Name: DEFAULT
26          Description: Predefined Cipher Alias
27   Done
28  <!--NeedCopy-->
```

Configurer la réutilisation de session à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Activer la réutilisation de la session** et spécifiez la durée pendant laquelle la session est active.

Paramètres du protocole SSL

L'appliance Citrix ADC prend en charge les protocoles SSLv3, TLSv1, TLSv1.1 et TLSv1.2. Chacun de ces protocoles peut être défini sur l'appliance en fonction de votre déploiement et du type de clients qui se connectent à l'appliance.

Les versions 1.0, 1.1 et 1.2 du protocole TLS sont plus sécurisées que les anciennes versions du protocole TLS/SSL. Toutefois, pour prendre en charge les systèmes hérités, de nombreuses implémentations TLS conservent une compatibilité descendante avec le protocole SSLv3. Dans une poignée de main SSL, la version de protocole la plus élevée commune au client et au serveur virtuel SSL configuré sur l'appliance Citrix ADC est utilisée.

Lors de la première tentative de poignée de main, un client TLS offre la version de protocole la plus élevée qu'il prend en charge. Si la poignée de main échoue, le client propose une version de protocole inférieure. Par exemple, si une poignée de main avec TLS version 1.1 échoue, le client tente de renégocier en proposant le protocole TLSv1.0. Si cette tentative échoue, le client tente de nouveau avec le protocole SSLv3. Un attaquant « homme au milieu » (MITM) peut rompre la poignée de main initiale et déclencher une renégociation avec le protocole SSLv3, puis exploiter une vulnérabilité dans SSLv3. Pour atténuer ces attaques, vous pouvez désactiver SSLv3 ou ne pas autoriser la renégociation à l'aide d'un protocole rétrogradé. Toutefois, cette approche peut ne pas être pratique si votre déploiement inclut des systèmes hérités. Une alternative consiste à reconnaître une valeur de suite de chiffrement de signalisation (TLS_FALLBACK_SCSV) dans la requête client.

Une valeur TLS_FALLBACK_SCSV dans un message de bonjour client indique au serveur virtuel que le client a précédemment tenté de se connecter avec une version de protocole supérieure et que la demande actuelle est une solution de secours. Si le serveur virtuel détecte cette valeur et prend en charge une version supérieure à celle indiquée par le client, il rejette la connexion avec une alerte fatale. La poignée de main réussit si l'une des conditions suivantes est remplie :

- La valeur TLS_FALLBACK_SCSV n'est pas incluse dans le message client Hello.
- La version de protocole dans le client hello est la version de protocole la plus élevée prise en charge par le serveur virtuel.

Configurer la prise en charge du protocole SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la prise en charge du protocole SSL et vérifier la configuration :

```
set ssl vserver <vServerName> -ssl2 ( ENABLED | DISABLED ) -ssl3 (
    ENABLED | DISABLED ) -tls1 ( ENABLED | DISABLED ) -tls11 ( ENABLED |
     DISABLED ) -tls12 ( ENABLED | DISABLED )

show ssl vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver vs-ssl -tls11 ENABLED -tls12 ENABLED
Done

sh ssl vs vs-ssl

        Advanced SSL configuration for VServer vs-ssl:
            DH: DISABLED
            Ephemeral RSA: ENABLED                          Refresh
               Count: 0
```



```
9               Session Reuse: ENABLED                                  Timeout
                    : 120 seconds
10              Cipher Redirect: DISABLED
11              SSLv2 Redirect: DISABLED
12              ClearText Port: 0
13              Client Auth: DISABLED
14              SSL Redirect: DISABLED
15              Non FIPS Ciphers: DISABLED
16              SNI: DISABLED
17              SSLv2: DISABLED        SSLv3: ENABLED    TLSv1.0: ENABLED
                    TLSv1.1: ENABLED  TLSv1.2: ENABLED
18              Push Encryption Trigger: Always
19              Send Close-Notify: YES
20              1 bound certificate:
21
22      1)      CertKey Name: mycert  Server Certificate
23              1 configured cipher:
24
25      1)      Cipher Name: DEFAULT
26              Description: Predefined Cipher Alias
27
28  Done
29  <!--NeedCopy-->
```

Configurer la prise en charge du protocole SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez un protocole à activer.

Ferme notifier

Une notification de fermeture est un message sécurisé qui indique la fin de la transmission de données SSL. Un paramètre de notification de fermeture est requis au niveau global. Ce paramètre s'applique à tous les serveurs virtuels, services et groupes de services. Pour plus d'informations sur le paramètre global, consultez la section « Paramètres SSL globaux » plus loin dans cette page.

Outre le paramètre global, vous pouvez définir le paramètre de notification rapprochée au niveau du serveur virtuel, du service ou du groupe de services. Vous avez donc la flexibilité de définir le paramètre pour une entité et de le désinstaller pour une autre entité. Cependant, assurez-vous que vous définissez ce paramètre au niveau global. Sinon, le paramètre au niveau de l'entité ne s'applique pas.

Configurer la notification de fermeture au niveau de l'entité à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour configurer la fonctionnalité de notification rapprochée et vérifier la configuration :

1. Pour configurer au niveau du serveur virtuel, tapez :

```
set ssl vserver <vServerName> -sendCloseNotify ( YES | NO )
show ssl vserver <vServerName>
<!--NeedCopy-->
```

1. Pour configurer au niveau du service, tapez :

```
set ssl service <serviceName> -sendCloseNotify ( YES | NO )
show ssl service <serviceName>
<!--NeedCopy-->
```

1. Pour configurer au niveau du groupe de services, tapez :

```
set ssl serviceGroup <serviceGroupName> -sendCloseNotify ( YES | NO )
show ssl serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver sslvsvr -sendCloseNotify YES

Done
<!--NeedCopy-->
```

Configurez la fonctionnalité de notification rapprochée au niveau de l'entité à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans la section **SSL Parameters**, sélectionnez **Send Close-Notify**.

Paramètres SSL globaux

La personnalisation avancée de votre configuration SSL répond à des problèmes spécifiques. Vous pouvez utiliser la `set ssl parameter` commande ou l'utilitaire de configuration pour spécifier les éléments suivants :

- Taille quantique à utiliser pour les transactions SSL.

- Taille de la mémoire CRL.
- Taille du cache OCSP.
- Refuser la renégociation SSL.
- Définissez l'indicateur PUSH pour les enregistrements déchiffrés, chiffrés ou tous les enregistrements.
- Supprimer les requêtes si le client initie la poignée de main pour un domaine et envoie une requête HTTP pour un autre domaine.
- Définissez l'heure après laquelle le chiffrement est déclenché.
  Remarque : l'heure que vous spécifiez s'applique uniquement si vous utilisez la commande `set ssl vserver` ou l'utilitaire de configuration pour définir le chiffrement basé sur la minuterie.
- Vérification du certificat de conformité NDCPP : s'applique lorsque l'appliance agit sur un client (connexion principale). Pendant la vérification du certificat, ignorez le nom commun si SAN est présent dans le certificat SSL.
- Activez un cluster hétérogène d'appliances basées sur des puces Cavium, telles que MPX 14000, et des appliances basées sur des puces Intel Coleto, telles que les appliances MPX 15000 avec un nombre différent de moteurs de paquets. (Prise en charge ajoutée dans la version 13.0 build 47.x).
- Activer la renégociation sécurisée au back-end (Support ajouté à partir de la version 1.0 build 58.x).
- Contrôle du trafic SSL adaptatif (prise en charge ajoutée dans la version 13.0 build 58.x).

Configurer les paramètres SSL globaux à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer les paramètres SSL avancés et vérifier la configuration :

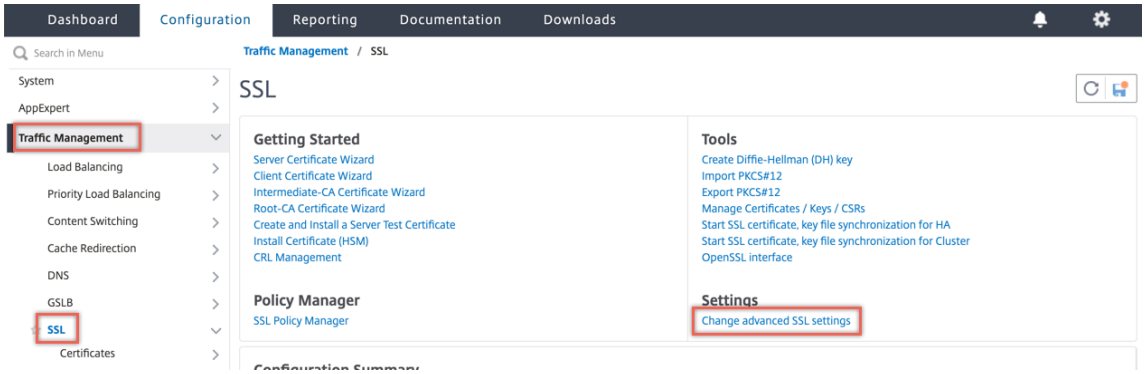
```
1 set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB <
    positive_integer>] [-strictCAChecks (YES | NO)] [-sslTriggerTimeout
    <positive_integer>] [-sendCloseNotify (YES | NO)] [-
    encryptTriggerPktCount <positive_integer>] [-denySSLReneg <
    denySSLReneg>] [-insertionEncoding (Unicode|UTF-8)] [-ocspCacheSize
    <positive_integer>][- pushFlag <positive_integer>] [-
    dropReqWithNoHostHeader (YES | NO)] [-pushEncTriggerTimeout <
    positive_integer>] [-ndcppComplianceCertCheck ( YES | NO)] [-
    heterogeneousSSLHW (ENABLED | DISABLED )]
2 show ssl parameter
3 <!--NeedCopy-->
```

Exemple :

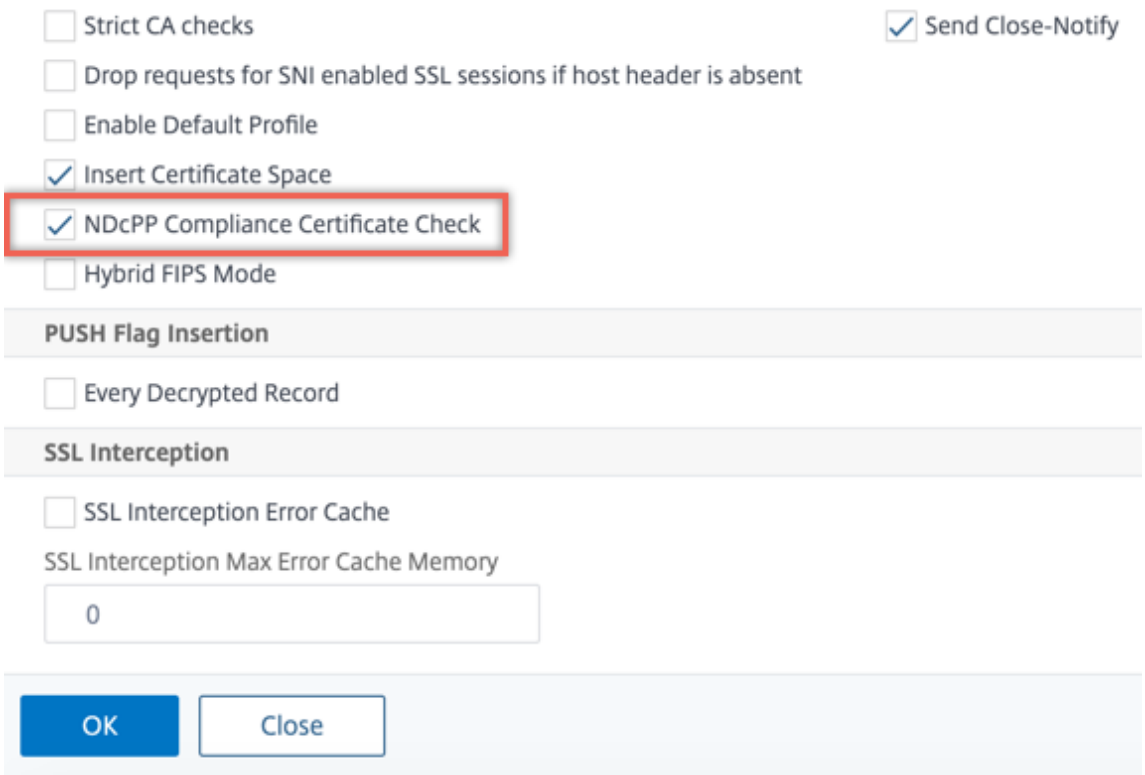

```
set ssl parameter -quantumSize 8 -crlMemorySizeMB 256 -strictCAChecks
    no -ssltriggerTimeout 100 -sendClosenotify no -
    encryptTriggerPktCount 45 -denySSLReneg NONSECURE -insertionEncoding
     unicode -ocspCacheSize 10 -pushFlag 3 -dropReqWithNoHostHeader YES
     -pushEncTriggerTimeout 100 ms -ndcppComplianceCertCheck YES
Done

show ssl parameter
Advanced SSL Parameters
-----------------------
    SSL quantum size                                    : 8 KB
    Max CRL memory size                                 : 256 MB
    Strict CA checks                                    : NO
    Encryption trigger timeout                          : 100 ms
    Send Close-Notify                                   : NO
    Encryption trigger packet count                     : 45
    Deny SSL Renegotiation                              : NONSECURE
    Subject/Issuer Name Insertion Format                : Unicode
    OCSP cache size                                     : 10 MB
    Push flag                                           : 0x3 (On
       every decrypted and encrypted record)
    Strict Host Header check for SNI enabled SSL sessions : YES
    PUSH encryption trigger timeout                     : 100 ms
    Crypto Device Disable Limit                         : 0
    Global undef action for control policies            : CLIENTAUTH
    Global undef action for data policies               : NOOP
    Default profile                                     : DISABLED
    SSL Insert Space in Certificate Header              : YES
    Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors  : NO
    Disable TLS 1.1/1.2 for dynamic and VPN services    : NO
    Software Crypto acceleration CPU Threshold          : 0
    Hybrid FIPS Mode                                    : DISABLED
    Signature and Hash Algorithms supported by TLS1.2   : ALL
    SSL Interception Error Learning and Caching         : DISABLED
    SSL Interception Maximum Error Cache Memory         : 0 Bytes
    NDCPP Compliance Certificate Check                  : YES
    Heterogeneous SSL HW (Cavium and Intel Based)       : ENABLED
 Done
<!--NeedCopy-->
```

Configurer la vérification du certificat de conformité NDCPP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL** et, dans le groupe **Paramètres**, sélectionnez **Modifier les paramètres SSL avancés**.



2. Sélectionnez **Vérification du certificat de conformité du NDCPP**. Cliquez sur **OK**.



Prise en charge de la renégociation sécurisée au niveau du back-end d'une appliance Citrix ADC

Remarque : Cette fonctionnalité est prise en charge dans la version 13.0 build 58.x et ultérieure. Dans les versions et versions antérieures, seule la renégociation non sécurisée était prise en charge sur le back-end.

La fonctionnalité est prise en charge sur les plates-formes suivantes :

• VPX
• Plateformes MPX contenant des puces N2 ou N3
• Plates-formes à puce SSL Intel Coleto

La fonctionnalité n'est pas encore prise en charge sur la plate-forme FIPS.

La renégociation sécurisée est refusée par défaut sur le back-end d'une appliance ADC. C'est-à-dire que le denySSLReneg paramètre est défini sur ALL (par défaut).

Pour autoriser la renégociation sécurisée sur le back-end, sélectionnez l'un des paramètres suivants pour le paramètre denySSLReneg :

- NON
- FRONTEND_CLIENT
- FRONTEND_CLIENTSERVER
- NONSECURE

Activer la renégociation sécurisée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl parameter -denySSLReneg <denySSLReneg>
```

Exemple :

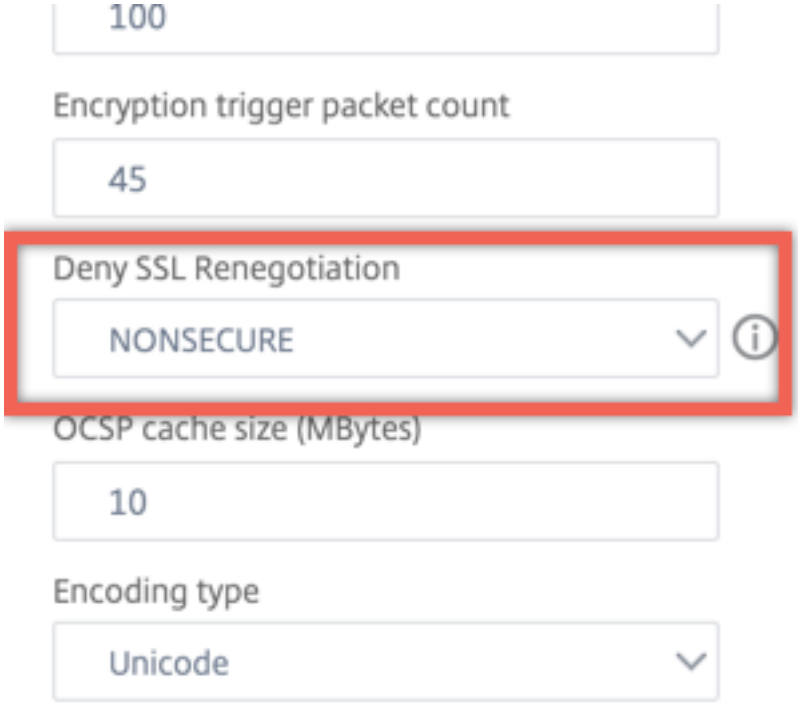
```
set ssl parameter -denySSLReneg NONSECURE
 Done

sh ssl parameter
Advanced SSL Parameters
-----------------------
    SSL quantum size                                    : 8 KB
    Max CRL memory size                                 : 256 MB
    Strict CA checks                                    : NO
    Encryption trigger timeout                          : 100 ms
    Send Close-Notify                                   : YES
    Encryption trigger packet count                     : 45
    Deny SSL Renegotiation                              : NONSECURE
    Subject/Issuer Name Insertion Format                : Unicode
    OCSP cache size                                     : 10 MB
    Push flag                                           : 0x0 (Auto)
    Strict Host Header check for SNI enabled SSL sessions : NO
    Match HTTP Host header with SNI                     : CERT
    PUSH encryption trigger timeout                     : 1 ms
    Crypto Device Disable Limit                         : 0
    Global undef action for control policies            : CLIENTAUTH
    Global undef action for data policies               : NOOP
    Default profile                                     : ENABLED
    SSL Insert Space in Certificate Header              : YES
    Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors  : NO
    Disable TLS 1.1/1.2 for dynamic and VPN services    : NO
```



```
    Software Crypto acceleration CPU Threshold            : 0
    Hybrid FIPS Mode                                      : DISABLED
    Signature and Hash Algorithms supported by TLS1.2     : ALL
    SSL Interception Error Learning and Caching           : DISABLED
    SSL Interception Maximum Error Cache Memory           : 0 Bytes
    NDCPP Compliance Certificate Check                    : NO
    Heterogeneous SSL HW (Cavium and Intel Based)         : DISABLED
    Crypto Operation Queue Limit                          : 150%
 Done
<!--NeedCopy-->
```

Activer la renégociation sécurisée à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Modifier les paramètres SSL avancés**.
2. Définissez **Refuser la renégociation SSL** sur toute valeur autre que ALL.



Contrôle du trafic SSL adaptatif

Remarque : Cette fonctionnalité est prise en charge dans la version 13.0 build 58.x et ultérieure.

Lorsque le trafic est élevé sur l'appliance et que la capacité d'accélération de crypto est pleine, l'appliance commence à mettre en file d'attente les connexions à traiter ultérieurement. Actuellement, la taille de cette file d'attente est fixée à 64 Ko et l'appliance commence à abandonner les connexions si cette valeur est dépassée.

À partir de la version 13.0 build 58.x, l'utilisateur peut configurer une valeur qui correspond à un pourcentage de la capacité réelle. Avec cette amélioration, l'appliance supprime les nouvelles connexions si le nombre d'éléments dans la file d'attente est supérieur à la limite calculée de manière adaptative et dynamique. Cette approche contrôle les connexions SSL entrantes et empêche la consommation excessive de ressources et d'autres pannes, telles que les défaillances de surveillance de l'équilibrage de charge ou les réponses lentes aux applications sécurisées, sur l'appliance.

Si la file d'attente est vide, l'appliance peut continuer à accepter les connexions. Si la file d'attente n'est pas vide, le système crypto a atteint sa capacité et l'appliance démarre la mise en file d'attente des connexions.

La limite est calculée en fonction des éléments suivants :

- Capacité réelle de l'appliance.
- Valeur configurée par l'utilisateur en pourcentage de la capacité réelle. La valeur par défaut est définie sur 150 %.

Par exemple, si la capacité réelle d'une appliance est de 1000 opérations/seconde à un moment donné et que le pourcentage par défaut est configuré, la limite après laquelle l'appliance supprime les connexions est de 1500 (150 % de 1 000).

Pour configurer la limite de la file d'attente d'opérations à l'aide de la CLI

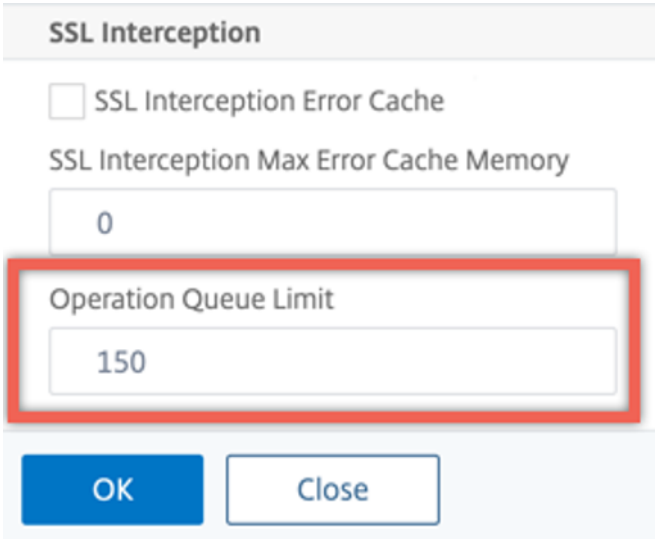
À l'invite de commandes, tapez :

```
set ssl parameter -operationQueueLimit <positive_integer>
```

Limite de file d'attente d'opération - Limite du pourcentage de capacité de la file d'attente des opérations de chiffrement au-delà de laquelle les nouvelles connexions SSL ne sont pas acceptées tant que la file d'attente n'est pas réduite. Valeur par défaut : 150. Valeur minimale : 0. Valeur maximale : 10000.

Pour configurer la limite de la file d'attente d'opérations à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL**.
2. Dans **Paramètres**, cliquez sur **Modifier les paramètres SSL avancés**.
3. Saisissez une valeur dans **Limite de file d'attente d'opération**. La valeur par défaut est 150.
4. Cliquez sur **OK**.



Déploiements de cluster hétérogènes

À partir de la version 13.0 build 47.x, vous pouvez former un déploiement de cluster hétérogène d'appliances Citrix ADC MPX avec un nombre différent de moteurs de paquets en définissant le paramètre SSL « HW SSL hétérogène » sur ENABLED. Par exemple, pour former un cluster d'appliances basées sur des puces Cavium (MPX 14000 ou similaire) et d'appliances basées sur puce Intel Coleto (MPX 15000 ou similaire), activez le paramètre SSL « HW SSL hétérogène. « Pour former un cluster de plates-formes utilisant la même puce, conservez la valeur par défaut (DISABLED) pour ce paramètre.

> **Remarques :**
>
> Les fonctionnalités suivantes ne sont pas prises en charge dans un cluster hétérogène :
>
> - Instances VPX hébergées sur des appliances Citrix ADC SDX.
> - Protocole SSLv3 sur les entités SSL, telles que le serveur virtuel, les services, le groupe de services et les services internes.
> - Seuil du processeur d'accélération crypto logicielle (utilisant du matériel et des logiciels pour améliorer les performances de chiffrement ECDSA et ECDHE).

Pour plus d'informations sur les plates-formes prises en charge dans un cluster hétérogène, reportez-vous à la section https://docs.citrix.com/fr-fr/citrix-adc/current-release/clustering/support-for-heterogeneous-cluster.html.

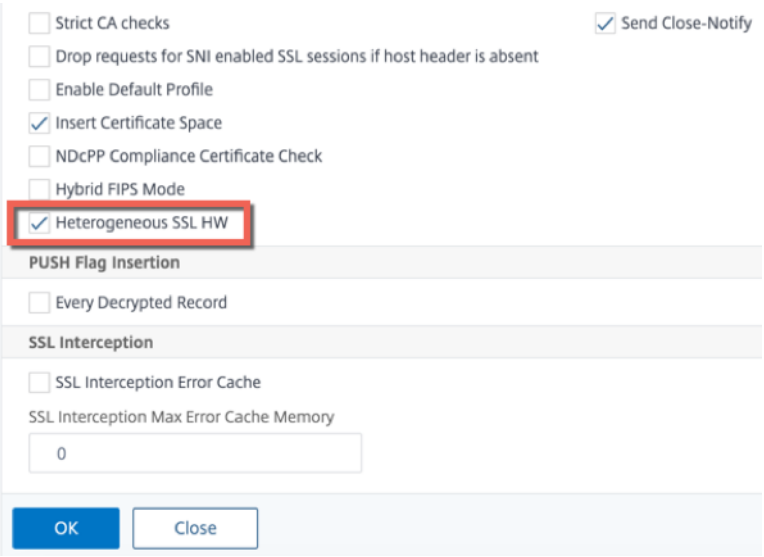
Activer un cluster hétérogène à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl parameter -heterogeneousSSLHW ENABLED
```


Activer un cluster hétérogène à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL** et, dans le groupe **Paramètres**, sélectionnez **Modifier les paramètres SSL avancés**.
2. Sélectionnez **HW SSL hétérogène**. Cliquez sur **OK**.



Mécanisme de déclenchement de chiffrement basé sur l'indicateur PUSH

Le mécanisme de déclenchement de chiffrement basé sur l'indicateur PSH TCP vous permet désormais d'effectuer les opérations suivantes :

- Fusionnez les paquets consécutifs dans lesquels l'indicateur PSH est défini dans un seul enregistrement SSL, ou ignorez l'indicateur PSH.
- Effectuez un chiffrement basé sur la minuterie, dans lequel la valeur de délai d'attente est définie globalement à l'aide de la commande `set ssl parameter -pushEncTriggerTimeout <positive_integer>`.

Configurer le chiffrement basé sur les indicateurs PUSH à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le chiffrement basé sur les indicateurs PUSH et vérifier la configuration :

```
set ssl vserver <vServerName> [-pushEncTrigger <pushEncTrigger>]

show ssl vserver
<!--NeedCopy-->
```

Exemple :


```
set ssl vserver vserver1 -pushEncTrigger always

Done

sh ssl vserver vserver1

            Advanced SSL configuration for VServer vserver1:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
               RSA: ENABLED

               Refresh Count: 0
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
            HSTS IncludeSubDomains: NO
            HSTS Max-Age: 0
            SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
            Push Encryption Trigger: Always
            Send Close-Notify: YES
            Strict Sig-Digest Check: DISABLED
            Zero RTT Early Data: DISABLED
            DHE Key Exchange With PSK: NO
            Tickets Per Authentication Context: 1
            ECC Curve: P_256, P_384, P_224, P_521

    1)      Cipher Name: DEFAULT
            Description: Default cipher list with encryption strength
               >= 128bit
Done
<!--NeedCopy-->
```

Configurer le chiffrement basé sur les indicateurs PUSH à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et ouvrez un serveur

virtuel SSL.

2. Dans la section **Paramètres SSL**, dans la liste **Trigger de chiffrement PUSH**, sélectionnez une valeur.

Prise en charge de l'algorithme de hachage de signature TLS1.2

L'appliance Citrix ADC est entièrement compatible avec l'extension de hachage de signature TLS1.2.

Dans une poignée de main SSL, un client envoie une liste des algorithmes de hachage de signature pris en charge. Le client indique au serveur quelles paires d'algorithmes de hachage de signature peuvent être utilisées dans les messages SSL (SKE et CCV) à l'aide de l'extension « signature_algorithms ». Le champ « extension_data » de cette extension contient une valeur « supported_signature_algorithms » dans le message Client Hello. La poignée de main SSL se poursuit si le serveur prend en charge l'un de ces algorithmes de hachage de signature. Si le serveur ne prend pas en charge l'un de ces algorithmes, la connexion est interrompue.

De même, si le serveur demande un certificat client pour l'authentification client, le message Demande de certificat contient une valeur « supported_signature_algorithms ». Le certificat client est sélectionné en fonction de cet algorithme de hachage de signature.

> **Remarque :**
>
> L'appliance Citrix ADC agit en tant que serveur pour un client et client pour le serveur principal.

L'appliance prend uniquement en charge les RSA-SHA1 et RSA-SHA256 sur l'avant, et RSA-MD5, RSA-SHA1 et RSA-SHA256 sur le back-end.

L'appliance MPX/SDX/VPX prend en charge les combinaisons de hachage de signature suivantes. Sur une appliance SDX, si une puce SSL est affectée à une instance VPX, la prise en charge du chiffrement d'une appliance MPX s'applique. Sinon, le support de chiffrement normal d'une instance VPX s'applique.

- Sur une instance VPX et sur une appliance MPX/SDX sans puces N3 :
  - RSA-MD5
  - RSA-SHA1
  - RSA-SHA224
  - RSA-SHA256
  - RSA-SHA384
  - RSA-SHA512
- Sur un appareil MPX/SDX doté de puces N3 :
  - RSA-MD5
  - RSA-SHA1
  - RSA-SHA224
  - RSA-SHA256

- RSA-SHA384
- RSA-SHA512
- ECDSA-SHA1
- ECDSA-SHA224
- ECDSA-SHA256
- ECDSA-SHA384
- ECDSA-SHA512

Par défaut, tous les algorithmes de hachage de signature sont activés. Toutefois, vous ne pouvez activer que quelques algorithmes de hachage de signature à l'aide de la commande suivante :

```
set ssl parameter -sigDigestType <sigDigestType>

Parameters

sigDigestType

Signature digest algorithms supported by the appliance. The platform
   determines the list of algorithms supported by default.

             On VPX: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384
                  RSA-

             SHA512

             On MPX with N3 cards: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-

             SHA256 RSA-SHA384 RSA-SHA512 ECDSA-SHA1 ECDSA-SHA224
                ECDSA-

             SHA256 ECDSA-SHA384 ECDSA-SHA512

             Other MPX Platforms: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-
                SHA256 RSA-SHA384 RSA-

             SHA512.

    set ssl parameter -sigDigestType RSA-SHA224 RSA-SHA256 RSA-SHA384
       RSA-SHA512
<!--NeedCopy-->
```

Valider le certificat homologue

Selon la RFC 5246, le certificat homologue doit être signé à l'aide de l'un des algorithmes de

hachage de signature inclus dans l'extension Client Hello. Vous pouvez utiliser le paramètre `strictSigDigestCheck`. Selon la liste de hachage de signature envoyée par le client, si vous l'activez`strictSigDigestCheck`, l'appliance renvoie un certificat signé par l'un des algorithmes de hachage de signature mentionnés dans l'extension Client Hello. Si l'homologue n'a pas de certificat approprié, la connexion est interrompue. Si ce paramètre est désactivé, le hachage de signature n'est pas vérifié dans le certificat homologue.

Vous pouvez configurer une vérification stricte du résumé de signature sur un serveur virtuel SSL et un service. Si vous activez ce paramètre sur un serveur virtuel SSL, le certificat de serveur envoyé par le serveur doit être signé par l'un des algorithmes de hachage de signature répertoriés dans l'extension Client Hello. Si l'authentification du client est activée, le certificat client reçu par le serveur doit être signé à l'aide de l'un des algorithmes de hachage de signature répertoriés dans la demande de certificat envoyée par le serveur.

Si vous activez ce paramètre sur un service SSL, le certificat de serveur reçu par le client doit être signé par l'un des algorithmes de hachage de signature répertoriés dans l'extension Client Hello. Le certificat client doit être signé à l'aide de l'un des algorithmes de hachage de signature répertoriés dans le message de demande de certificat.

Si le profil par défaut est activé, vous pouvez l'utiliser pour configurer une vérification stricte du résumé de signature sur un serveur virtuel SSL, un service SSL et un profil SSL.

Configurez la vérification stricte du résumé de signature sur un serveur virtuel SSL, un service ou un profil à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl vserver <vServerName> -strictSigDigestCheck ( ENABLED |
    DISABLED )

set ssl service <serviceName> -strictSigDigestCheck ( ENABLED |
    DISABLED )

set ssl profile <name>-strictSigDigestCheck ( ENABLED | DISABLED )

Parameters

strictSigDigestCheck

              Check whether peer entity certificate is signed using one
                  of the signature-hash algorithms supported by the
                 Citrix ADC appliance.

              Possible values: ENABLED, DISABLED
```



```
14
15                Default: DISABLED
16 <!--NeedCopy-->
```

Exemple :

```
1 set ssl vserver v1 -strictSigDigestCheck Enabled
2 set ssl service s1 -strictSigDigestCheck Enabled
3 set ssl profile p1 -strictSigDigestCheck Enabled
4 <!--NeedCopy-->
```

> **Important :**
>
> Si des chiffrements DH, ECDHE ou ECDSA sont configurés sur l'appliance, le message SKE doit être signé à l'aide de l'un des hachages de signature communs à la liste des clients et à la liste configurée sur l'appliance. S'il n'y a pas de hachage de signature commun, la connexion est supprimée.

Prise en charge du protocole TLSv1.3 tel que défini dans la RFC 8446

August 20, 2021

Les appliances Citrix ADC VPX et Citrix ADC MPX prennent désormais en charge le protocole TLSv1.3, spécifié dans la RFC 8446.

> **Remarques :**
>
> - Depuis la version 13.0 build 71.x et les versions ultérieures, l'accélération matérielle TLS1.3 est prise en charge sur les plates-formes suivantes :
>   - MPX 5900
>   - MPX/SDX 8900
>   - MPX/SDX 15000
>   - MPX/SDX 15000-50G
>   - MPX/SDX 26000
>   - MPX/SDX 26000-50S
>   - MPX/SDX 26000-100G
>
> - La prise en charge logicielle du protocole TLSv1.3 est disponible sur tous les autres appliances Citrix ADC MPX et SDX, à l'exception des appliances Citrix ADC FIPS.
>
> - TLSv1.3 n'est pris en charge qu'avec le profil amélioré. Pour activer le profil amélioré, voir Activer le profil amélioré.

> • Pour utiliser TLS1.3, vous devez utiliser un client conforme à la spécification RFC 8446.

Fonctionnalités Citrix ADC prises en charge

Les fonctionnalités SSL suivantes sont prises en charge :

1. Suites de chiffrement TLSv1.3 :
   - TLS1.3-AES256-GCM-SHA384 (0x1302)
   - TLS1.3_CHACHA20_POLY1305_SHA256 (0x1303)
   - TLS1.3-AES128_GCM-SHA256 (0x1301)
2. Courbes ECC pour l'échange éphémère de clés Diffie-Hellman :
   - P_256
   - P_384
   - P_521
3. Poignées de main abrégées lorsque la reprise de session basée sur un ticket est activée
4. Données d'application anticipée 0-RTT
5. Authentification client optionnelle ou obligatoire basée sur des certificats, avec prise en charge de la validation OCSP et CRL des certificats clients
6. Extension de nom de serveur : sélection de certificat de serveur à l'aide de SNI
7. Négociation du protocole d'application (ALPN) à l'aide de l'extension application_level_protocol_negotiation
8. Association d'OCSP
9. Les messages de journal et les enregistrements AppFlow sont produits pour les poignées de main TLSv1.3.
10. Journalisation facultative des secrets de trafic TLS 1.3 par l'utilitaire de capture de`nstrace` paquets.
11. Interopérabilité avec les clients TLS implémentant la RFC 8446. Par exemple, Mozilla Firefox, Google Chrome et OpenSSL.

Navigateurs pris en charge

Les versions de navigateur suivantes sont prises en charge et compatibles avec l'implémentation Citrix ADC du protocole TLS 1.3 :

- Google Chrome - Version 72.0.3626.121 (version officielle) (64 bits)
- Mozilla Firefox - 65.0.2 (64 bits)
- Opéra - Version:58.0.3135.79

Configuration

TLSv1.3 est désactivé par défaut sur un profil SSL.

Ajouter un profil SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ssl profile <tls13-profile-name>
<!--NeedCopy-->
```

Exemple :

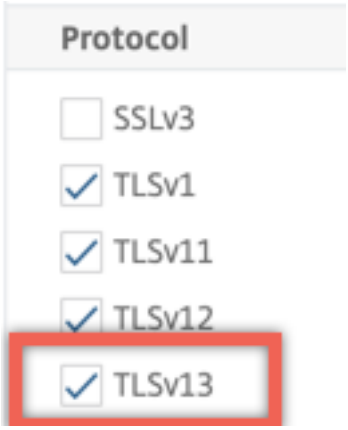
```
add ssl profile tls13profile

sh ssl profile tls13profile
1)  Name: tls13profile           (Front-End)
    SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1.1: ENABLED
       TLSv1.2: ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:   NO
    Session Reuse: ENABLED                      Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED   Ephemeral RSA:
       ENABLED                             Refresh Count: 0
    Deny SSL Renegotiation                                 ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:             1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions: NO
    Push flag:            0x0 (Auto)
    SSL quantum size:                            8 kB
    Encryption trigger timeout           100 mS
    Encryption trigger packet count:               45
    Subject/Issuer Name Insertion Format: Unicode
```



```
31
32      SSL Interception: DISABLED
33      SSL Interception OCSP Check: ENABLED
34      SSL Interception End to End Renegotiation: ENABLED
35      SSL Interception Maximum Reuse Sessions per Server:  10
36      Session Ticket: DISABLED
37      HSTS: DISABLED
38      HSTS IncludeSubDomains: NO
39      HSTS Max-Age: 0
40
41      ECC Curve: P_256, P_384, P_224, P_521
42
43  1)  Cipher Name: DEFAULT Priority :1
44      Description: Predefined Cipher Alias
45  Done
46  <!--NeedCopy-->
```

Ajouter un profil SSL à l'aide de l'interface graphique

1. Accédez à **Système > Profils**. Sélectionnez **Profils SSL**.
2. Cliquez sur **Ajouter** et spécifiez un nom pour le profil.
3. Dans **Protocole**, sélectionnez **TLSv13**.



4. Cliquez sur **OK**.

Liez un profil SSL à un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1  set ssl vserver <vServerName> -sslProfile <tls13-profile-name>
2  <!--NeedCopy-->
```


Exemple :

```
set ssl vserver ssl-vs -sslProfile tls13profile
```

Liez un profil SSL à un serveur virtuel SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis sélectionnez un serveur virtuel SSL.
2. Dans **Paramètres avancés**, cliquez sur **Profil SSL**.
3. Sélectionnez le profil TLSv1.3 créé précédemment.
4. Cliquez sur **OK**.
5. Cliquez sur **Terminé**.

Paramètres de profil SSL pour le protocole TLSv1.3

1. Activez ou désactivez les paramètres TLS1.3 dans un profil SSL.

   tls13 : état de la prise en charge du protocole TLSv1.3 pour le profil SSL.

   Valeurs possibles : ENABLED, DISABLED

   Valeur par défaut : DISABLED

   ```
   1 set ssl profile tls13profile -tls13 enable
   2 <!--NeedCopy-->
   ```

   ```
   1 set ssl profile tls13profile -tls13 disable
   2 <!--NeedCopy-->
   ```

2. Définir le nombre de tickets de session émis.

   TLS13SessionTicketsPerAuthContext : nombre de tickets que le serveur virtuel SSL émet lorsque TLS1.3 est négocié, la reprise basée sur les tickets est activée et (1) une poignée de main est terminée ou (2) l'authentification du client se termine après la poignée de main.

   Cette valeur peut être augmentée pour permettre aux clients d'ouvrir plusieurs connexions parallèles à l'aide d'un nouveau ticket pour chaque connexion.

   Aucun ticket n'est envoyé si la reprise est désactivée.

   Valeur par défaut : 1

   Valeur minimale : 1

   Valeur maximale : 10


```
set ssl profile tls13profile -tls13sessionTicketsPerAuthContext 1

set ssl profile tls13profile -tls13sessionTicketsPerAuthContext 10
<!--NeedCopy-->
```

3. Définir l'échange de clés DH

   dheKeyExchangeWithPsk: spécifie si un serveur virtuel SSL nécessite un échange de clés DHE lorsqu'une clé pré-partagée est acceptée lors d'une poignée de main de reprise de session TLS 1.3. Un échange de clés DHE garantit le secret avant, même si les clés de ticket sont compromises, au détriment des ressources supplémentaires nécessaires à l'échange de clés **DHE**.

   Les paramètres disponibles fonctionnent comme suit, si le ticket de session est activé :

   YES : L'échange de clés DHE est requis lorsqu'une clé pré-partagée est acceptée, que le client prenne ou non en charge l'échange de clés. La poignée de main est interrompue avec une alerte fatale, si le client ne prend pas en charge l'échange de clés DHE lors de l'offre d'une clé pré-partagée.

   NO : L'échange de clés DHE est effectué lorsqu'une clé pré-partagée est acceptée, uniquement si le client le demande.

   Valeurs possibles : YES, NO

   Valeur par défaut : NO

```
set ssl profile tls13profile dheKeyExchangeWithPsk yes

set ssl profile tls13profile dheKeyExchangeWithPsk no
<!--NeedCopy-->
```

4. Activer ou désactiver l'acceptation anticipée des données 0-RTT

   zeroRttEarlyData: état des données d'application précoces de TLS 1.3. Les paramètres applicables fonctionnent comme suit :

   ENABLED : Les données d'application anticipées peuvent être traitées avant la fin de la poignée de main.
   DISABLED : les données d'application précoces sont ignorées.

   Valeurs possibles : ENABLED, DISABLED

   Valeur par défaut : DISABLED

```
set ssl profile tls13profile -zeroRttEarlyData ENABLED

set ssl profile tls13profile -zeroRttEarlyData DISABLED
<!--NeedCopy-->
```


Groupe de chiffrement par défaut

Le groupe de chiffrement par défaut inclut les chiffrements TLS1.3.

```
sh cipher DEFAULT
1) Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035

2)  Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
...
...
27) Cipher Name: TLS1.3-AES256-GCM-SHA384         Priority : 27
    Description: TLSv1.3 Kx=any      Au=any  Enc=AES-GCM(256) Mac=AEAD
         HexCode=0x1302

28) Cipher Name: TLS1.3_CHACHA20_POLY1305_SHA256     Priority : 28
    Description: TLSv1.3 Kx=any      Au=any  Enc=CHACHA20/POLY1305(256)
        Mac=AEAD   HexCode=0x1303

29) Cipher Name: TLS1.3-AES128_GCM-SHA256        Priority : 29
    Description: TLSv1.3 Kx=any      Au=any  Enc=AES-GCM(128) Mac=AEAD
         HexCode=0x1301
Done
<!--NeedCopy-->
```

Limitations

- Sur la plate-forme Citrix ADC MPX, le traitement TLSv1.3 n'est pas déchargé vers du matériel crypto.
- TLSv1.3 n'est pas pris en charge sur le back-end.
- TLSv1.3 n'est pas pris en charge sur une appliance Citrix Secure Web Gateway et sur une appliance Citrix ADC FIPS.

Considérations opérationnelles

Note de compatibilité de la version provisoire de TLS 1.3 : Une appliance Citrix ADC implémente la variante RFC 8446 du protocole TLS 1.3 (par opposition aux versions provisoires antérieures du protocole). Utilisez un client TLS 1.3 prenant en charge la RFC 8446 (ou un brouillon interopérable # 26, 27 ou 28) pour terminer une prise de contact TLS 1.3 avec une appliance Citrix ADC. Les clients et serveurs

qui implémentent différentes versions provisoires du protocole TLS 1.3 peuvent ne pas interagir entre eux.

Restrictions de sécurité

Les opérateurs de serveur TLSv1.3 doivent garder à l'esprit les restrictions de sécurité suivantes pour la compatibilité descendante décrites dans la RFC 8446. La configuration par défaut d'une appliance NetScaler est conforme à ces restrictions. Toutefois, une appliance NetScaler n'applique pas le respect de ces règles.

- La sécurité des suites de chiffrement RC4 est jugée insuffisante comme décrit dans la RFC7465. Les implémentations ne doivent pas proposer ou négocier des suites de chiffrement RC4 pour aucune version de TLS.
- Les anciennes versions de TLS ont permis l'utilisation de chiffrements à faible résistance. Les chiffrements dont la force est inférieure à 112 bits ne doivent pas être proposés ou négociés pour aucune version de TLS.
- La sécurité de SSL 3.0 [SSLv3] est considérée comme insuffisante comme décrit dans la RFC7568 et ne doit pas être négociée. Désactivez SSLv3 lorsque TLSv1.3 est activé (SSLv3 est désactivé par défaut).
- La sécurité de SSL 2.0 [SSLv2] est considérée comme insuffisante comme décrit dans la RFC6176 et ne doit pas être négociée. Désactivez SSLv2 lorsque TLS 1.3 est activé (SSLv2 est désactivé par défaut).

> **Remarque :**
>
> Pour plus d'informations sur le dépannage des protocoles exécutés sur TLS1.3, consultez Déchiffrement du trafic TLS1.3 du suivi des paquets.

Articles pratiques

August 20, 2021

Les articles pratiques sont simples et faciles à utiliser avec des étapes de configuration pour les déploiements courants. Cliquez sur un lien pour afficher l'article.

Créer une demande de signature de certificat et utiliser des certificats SSL sur une appliance Citrix ADC

Configurer l'action SSL pour transférer le trafic client

Configurer l'action SSL pour transférer le trafic client si un chiffrement n'est pas pris en charge sur ADC

Certificats SSL

October 5, 2021

Un certificat SSL, qui fait partie de toute transaction SSL, est un formulaire de données numérique (X509) qui identifie une entreprise (domaine) ou un individu. Le certificat possède un composant de clé publique visible par tout client qui souhaite lancer une transaction sécurisée avec le serveur. La clé privée correspondante, qui réside en toute sécurité sur l'appliance Citrix ADC, est utilisée pour effectuer le chiffrement et le déchiffrement par clé asymétrique (ou clé publique).

Vous pouvez obtenir un certificat SSL et une clé de l'une des manières suivantes :

- À partir d'une autorité de certification (CA) autorisée, telle que Verisign
- En générant un nouveau certificat SSL et une nouvelle clé sur l'appliance Citrix ADC

Vous pouvez également utiliser un certificat SSL existant sur l'appliance.

Les certificats sont classés en quatre types par l'appliance Citrix ADC :

- **Certificats de serveur :** un certificat de serveur authentifie l'identité du serveur auprès du client. Sur le front-end, l'appliance ADC joue le rôle de serveur. Vous liez un certificat de serveur et une clé privée à un serveur virtuel SSL sur l'appliance ADC.
- **Certificats clients :** Un certificat client authentifie l'identité du client auprès du serveur. Sur le back-end, l'appliance ADC agit en tant que client. Vous liez un certificat client et une clé privée au service SSL ou au groupe de services sur l'appliance ADC.
- **Certificats d'autorité de certification :** les certificats d'autorité de certification délivrent les certificats d'utilisateur final (certificats client et serveur). Un certificat d'autorité de certification peut être une autorité de certification racine approuvée (auto-signée par l'autorité de certification) ou une autorité de certification intermédiaire (signée par une autorité de certification racine approuvée). En règle générale, les certificats d'autorité de certification n'ont pas besoin de clés privées.
- **Certificats inconnus :** Tous les autres certificats entrent dans cette catégorie.

Important : Citrix vous recommande d'utiliser des certificats obtenus auprès d'autorités de certification autorisées, telles que Verisign, pour toutes vos transactions SSL. Utilisez les certificats générés sur l'appliance Citrix ADC à des fins de test uniquement, et non dans un déploiement en direct.

- Si, lors de l'ajout d'une paire de clés de certificat, vous ajoutez un fichier de certificat portant le même nom qu'un fichier de certificat existant, le fichier de certificat d'origine est écrasé sans avertissement. Cette action peut entraîner des problèmes après le redémarrage de la solution matérielle-logicielle, car le fichier de certificat d'origine n'est plus disponible dans le `/nsconfig/ssl` répertoire.
- La suppression de tout certificat ou fichier clé dans un environnement de cluster limite la configuration de l'appliance ADC. Rajoutez les fichiers au même emplacement pour apporter des modifications de configuration.

Remarque : vous pouvez utiliser le tableau de bord SSL ADM pour faciliter la gestion des certificats SSL et définir des notifications pour les certificats qui ne sont pas utilisés ou qui expirent bientôt. Pour plus d'informations, voir Gestion des certificats SSL.

Créer un certificat

August 20, 2021

Une autorité de certification (CA) est une entité qui émet des certificats numériques à utiliser dans la cryptographie à clé publique. Applications, telles que les navigateurs Web, qui effectuent des transactions SSL certificats d'approbation émis ou signés par une autorité de certification. Ces applications tiennent à jour une liste des autorités de certification qu'elles ont confiance. Si l'une des autorités de certification de confiance signent le certificat utilisé pour la transaction sécurisée, l'application

procède à la transaction.

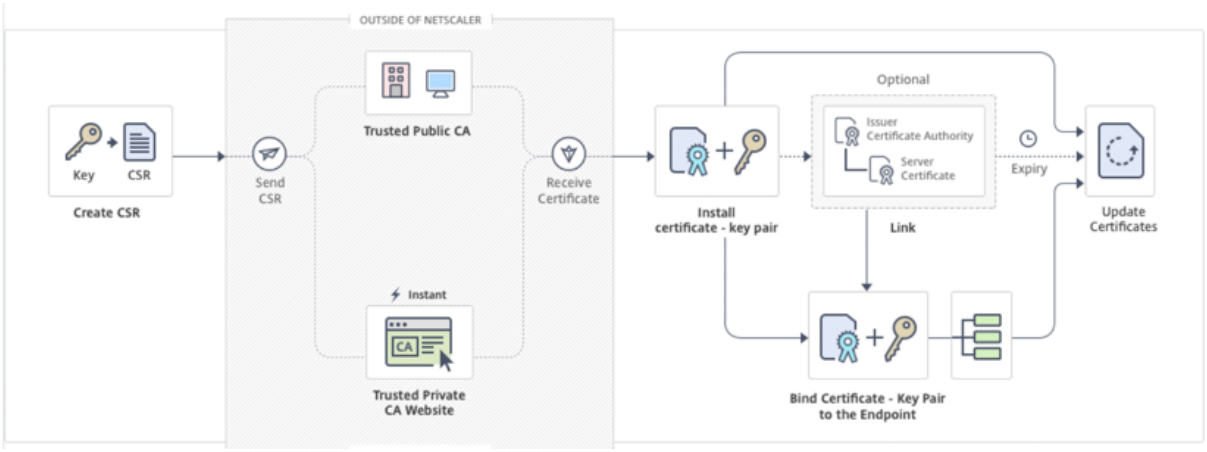
Attention : Citrix vous recommande d'utiliser des certificats obtenus auprès d'autorités de certification autorisées, telles que Verisign, pour toutes vos transactions SSL. Utilisez les certificats générés sur l'appliance Citrix ADC à des fins de test uniquement, et non dans un déploiement en direct.

Pour importer un certificat et une clé existants, reportez-vous à la section Importer un certificat.

Procédez comme suit pour créer un certificat et le lier à un serveur virtuel SSL. Les seuls caractères spéciaux autorisés dans les noms de fichiers sont le trait de soulignement et le point.

- Créez une clé privée.
- Créez une demande de signature de certificat (CSR).
- Soumettre le CSR à une autorité de certification.
- Créez une paire de clés de certificat.
- Lier la paire de clés de certificat à un serveur virtuel SSL

Le diagramme suivant illustre le flux de travail.



Lien vidéo vers Comment créer et installer un nouveau certificat.

Créer une clé privée

> **Remarques :**
>
> - À partir de la version 12.1 build 49.x, vous pouvez utiliser l'algorithme AES256 avec le format de clé PEM pour chiffrer une clé privée sur l'appliance. AES avec clé 256 bits est mathématiquement plus efficace et plus sûr que la clé 56 bits du Data Encryption Standard (DES).
> - À partir de la version 12.1 build 50.x, vous pouvez créer une clé RSA au format PKCS #8.

La clé privée est la partie la plus importante d'un certificat numérique. Par définition, cette clé ne doit être partagée avec personne et doit être conservée en toute sécurité sur l'appliance Citrix ADC. Toutes les données chiffrées avec la clé publique ne peuvent être déchiffrées qu'à l'aide de la clé privée.

Le certificat que vous recevez de l'autorité de certification est valide uniquement avec la clé privée utilisée pour créer le CSR. La clé est requise pour ajouter le certificat à l'appliance Citrix ADC.

L'appliance prend uniquement en charge les algorithmes de chiffrement RSA pour la création de clés privées. Vous pouvez soumettre l'un ou l'autre type de clé privée à l'autorité de certification (CA). Le certificat que vous recevez de l'autorité de certification est valide uniquement avec la clé privée utilisée pour créer le CSR. La clé est requise pour ajouter le certificat à l'appliance Citrix ADC.

Important :

> - Veillez à limiter l'accès à votre clé privée. Toute personne ayant accès à votre clé privée peut déchiffrer vos données SSL.
> - La longueur du nom de clé SSL autorisée inclut la longueur du nom de chemin absolu si le chemin est inclus dans le nom de la clé.

Tous les certificats et clés SSL sont stockés dans le `/nsconfig/ssl` dossier de l'appliance. Pour plus de sécurité, vous pouvez utiliser l'algorithme DES ou triple DES (3DES) pour chiffrer la clé privée stockée sur l'appliance.

Créer une clé privée RSA à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

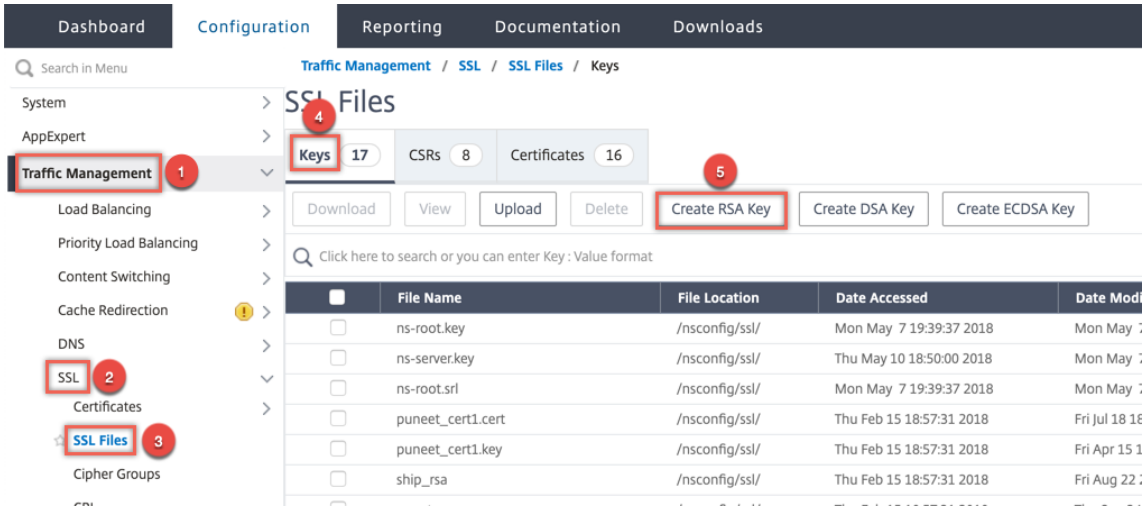
```
create ssl rsakey <keyFile> <bits> [-exponent ( 3 | F4 )] [-keyform (
    DER | PEM )] [-des | -des3 | -aes256] {
 -password  }
  [-pkcs8]
<!--NeedCopy-->
```

Exemple :

```
create rsakey testkey 2048 -aes256 -password 123456 -pkcs8
<!--NeedCopy-->
```

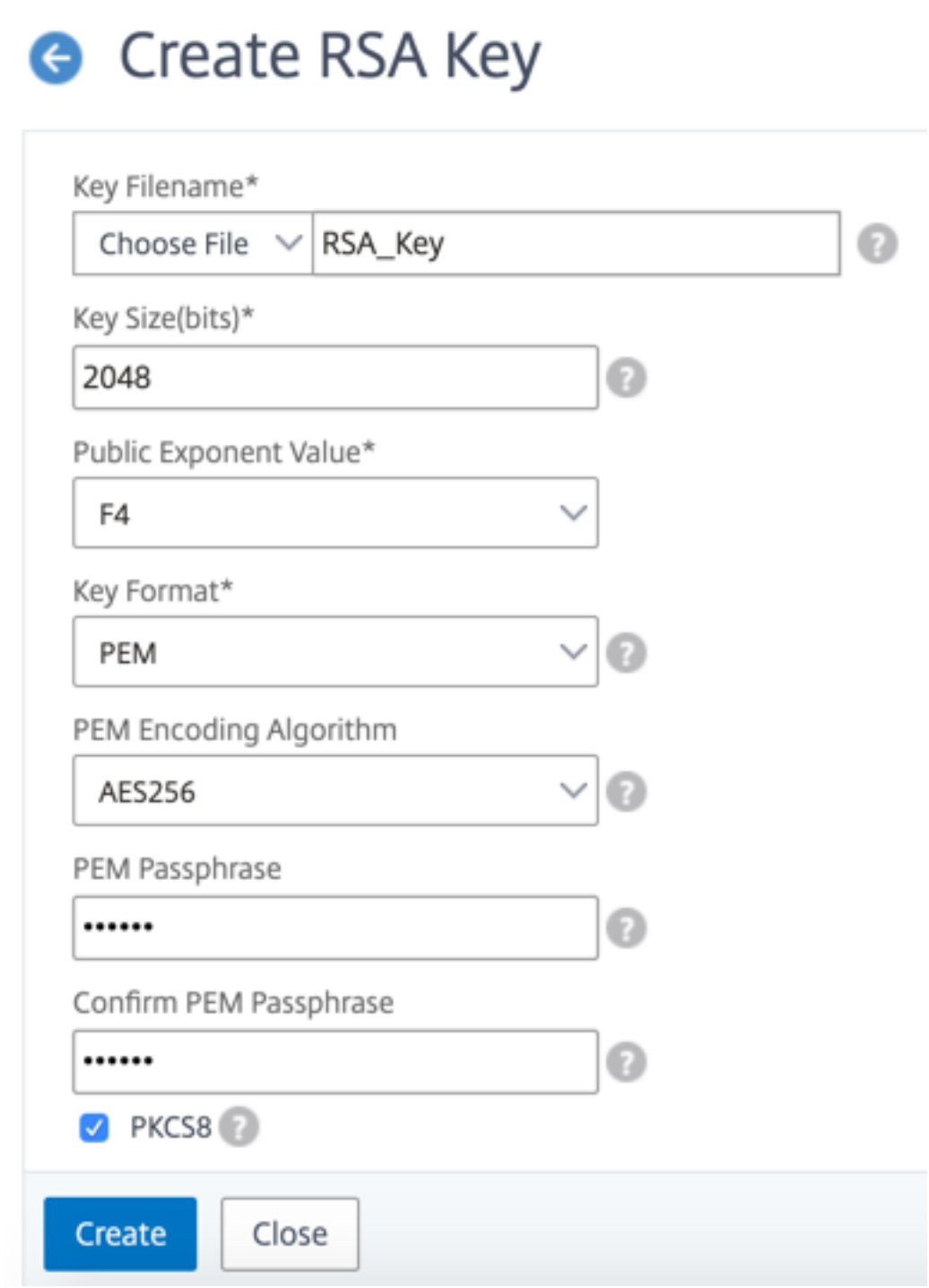
Créer une clé privée RSA à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Fichiers SSL**.
2. Dans l'onglet **Clés**, sélectionnez **Créer une clé RSA**.



3. Entrez des valeurs pour les paramètres suivants et cliquez sur **Créer**.

   - **Key Filename** - Nom du fichier de clé RSA et, éventuellement, chemin d'accès au fichier de clé RSA. /nsconfig/ssl/ est le chemin par défaut.
   - **Taille de la clé** - Taille, en bits, de la clé RSA. Peut varier de 512 bits à 4096 bits.
   - **Valeur de l'exposant** public - Exposant public pour la clé RSA. L'exposant fait partie de l'algorithme de chiffrement et est requis pour créer la clé RSA.
   - **Format de clé** : format dans lequel le fichier de clé RSA est stocké sur l'appliance.
   - **Algorithme d'encodage PEM** - Chiffrez la clé RSA générée à l'aide de l'algorithme AES 256, DES ou Triple-DES (DES3). Par défaut, les clés privées ne sont pas chiffrées.
   - **Phrase de passe PEM** - Si la clé privée est chiffrée, entrez une phrase de passe pour la clé.



Sélectionner un algorithme de codage AES256 dans une clé RSA à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Fichiers SSL > Créer une clé RSA**.

2. Dans **Format de clé**, sélectionnez **PEM**.
3. Dans **PEM Encoding Algorithm**, sélectionnez **AES256**.
4. Sélectionnez **PKCS8**.

Créer une demande de signature de certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

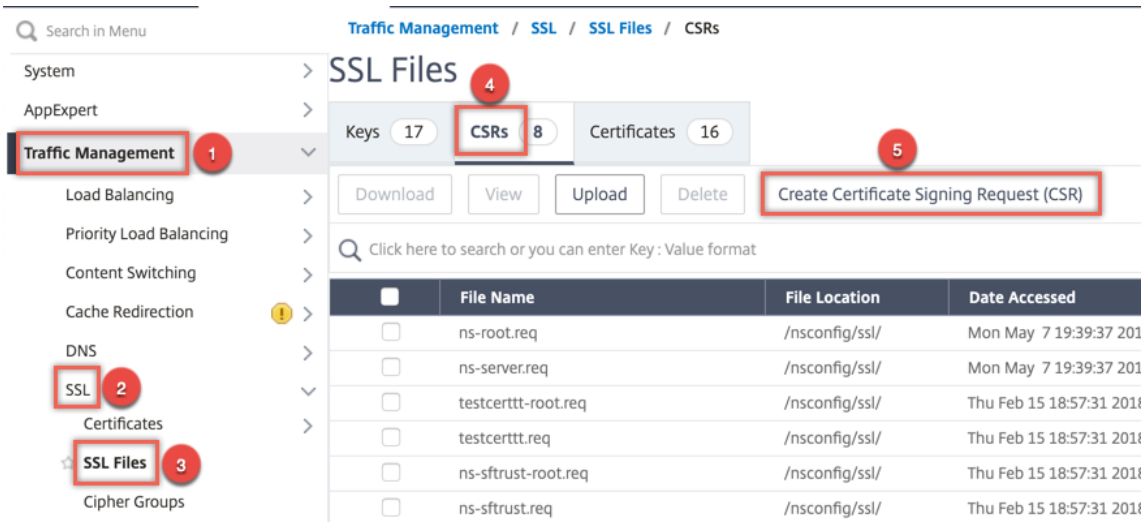
```
create ssl certreq <reqFile> -keyFile <input_filename> | -fipsKeyName <
   string>) [-keyForm (DER | PEM) {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName <string>
     -organizationUnitName <string> -localityName <string> -commonName
    <string> -emailAddress <string> {
 -challengePassword  }
  -companyName <string> -digestMethod ( SHA1 | SHA256 )
<!--NeedCopy-->
```

Exemple :

```
create ssl certreq priv_csr_sha256 -keyfile priv_2048_2 -keyform PEM -
   countryName IN -stateName Karnataka -localityName Bangalore -
   organizationName Citrix -organizationUnitName NS -digestMethod
   SHA256
<!--NeedCopy-->
```

Créer une demande de signature de certificat à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL**.
2. Dans Certificat **SSL**, cliquez sur **Créer une demande de signature de certificat (CSR)**.



3. Dans Méthode **de synthèse**, sélectionnez **SHA256**.

Pour plus d'informations, reportez-vous à la section Créer une CSR .

Prise en charge du nom alternatif du sujet dans une demande de signature de certificat

Le champ de nom alternatif de sujet (SAN) d'un certificat vous permet d'associer plusieurs valeurs, telles que des noms de domaine et des adresses IP, à un seul certificat. En d'autres termes, vous pouvez sécuriser plusieurs domaines, tels que www.example.com, www.example1.com, www.example2.com, avec un seul certificat.

Certains navigateurs, tels que Google Chrome, ne prennent plus en charge un nom commun dans une demande de signature de certificat (CSR). Ils appliquent le SAN dans tous les certificats de confiance publique.

L'appliance Citrix ADC prend en charge l'ajout de valeurs SAN lors de la création d'un CSR. Vous pouvez envoyer un CSR avec une entrée SAN à une autorité de certification pour obtenir un certificat signé avec cette entrée SAN. Lorsque l'appliance reçoit une demande, elle recherche un nom de domaine correspondant dans les entrées SAN du certificat de serveur. Si une correspondance est trouvée, il envoie le certificat au client et termine la poignée de main SSL. Vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique pour créer un CSR avec des valeurs SAN.

> **Remarque :** L'appliance Citrix ADC traite uniquement les valeurs SAN basées sur DNS.

Créez un CSR avec le nom alternatif de l'objet à l'aide de l'interface de ligne de commande

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
    <string>) [-subjectAltName <string>] [-keyform ( DER | PEM )  {
 -PEMPassPhrase  }
```



```
3   ] -countryName <string> -stateName <string> -organizationName <string>
        [-organizationUnitName <string>] [-localityName <string>] [-
       commonName <string>] [-emailAddress <string>] {
4   -challengePassword  }
5    [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
6   <!--NeedCopy-->
```

Paramètres :

SubjectAltName : Le nom alternatif du sujet (SAN) est une extension de X.509 qui permet d'associer diverses valeurs à un certificat de sécurité à l'aide d'un champ SubjectAltName. Ces valeurs sont appelées « Subject Alternative Names » (SAN). Les noms comprennent :

1. Adresses IP (préfixe avec « IP : » Exemple : IP:198.51.10.5 IP:192.0.2.100)
2. Noms DNS (Préfixe avec « DNS : » Exemple : DNS : www.example.com DNS : www.example.org DNS : www.example.net)

Sur la ligne de commande, entrez des valeurs entre guillemets. Séparer deux valeurs par un espace. Les guillemets ne sont pas obligatoires dans l'interface graphique.
Longueur maximale : 127

Exemple :

```
1  create certReq test1.csr -keyFile test1.ky -countryName IN -stateName
       Kar -organizationName citrix -commonName ctx.com -subjectAltName "
       DNS:*.example.com DNS:www.example.org DNS:www.example.net"
2  <!--NeedCopy-->
```

> **Remarque :**
>
> Sur une appliance FIPS, vous devez remplacer le nom du fichier de clé par le nom de clé FIPS si vous créez la clé FIPS directement sur l'appliance.
>
> ```
> 1  create certReq <csrname> -fipsKeyName fipskey.ky -countryName IN -
>        stateName Kar -organizationName citrix -commonName ctx.com -
>        subjectAltName "DNS:www.example.com DNS:www.example.org DNS:www.
>        example.net"
> 2  <!--NeedCopy-->
> ```

Créer un CSR à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Fichiers SSL**.
2. Dans l'onglet **CSR**, cliquez sur **Créer une demande de signature de certificat (CSR)**.
3. Entrez les valeurs et cliquez sur **Créer**.

Limitations

Pour utiliser SAN lors de la création d'un certificat SSL, vous devez spécifier explicitement les valeurs SAN. Les valeurs ne sont pas lues automatiquement à partir du fichier CSR.

Soumettre le CSR à l'autorité de certification

La plupart des autorités de certification acceptent les envois de certificats par courriel. L'autorité de certification renvoie un certificat valide à l'adresse e-mail à partir de laquelle vous soumettez le CSR.

Le CSR est stocké dans le `/nsconfig/ssl` dossier.

Générer un certificat de test

> **Remarque :**
>
> Pour générer un certificat de test de serveur, reportez-vous à la section Génération d'un certificat de test de serveur.

L'appliance Citrix ADC dispose d'une suite d'outils CA intégrée que vous pouvez utiliser pour créer des certificats auto-signés à des fins de test.

Attention : Étant donné que l'appliance Citrix ADC signe ces certificats, et non une autorité de certification réelle, vous ne devez pas les utiliser dans un environnement de production. Si vous tentez d'utiliser un certificat auto-signé dans un environnement de production, les utilisateurs reçoivent un avertissement « certificat non valide » chaque fois que le serveur virtuel est accédé.

L'appliance prend en charge la création des types de certificats suivants

- Certificats de CA racine
- Certificats de CA intermédiaire
- Certificats d'utilisateur final
  - certificats de serveur
  - certificats clients

Avant de générer un certificat, créez une clé privée et utilisez-la pour créer une demande de signature de certificat (CSR) sur l'appliance. Ensuite, au lieu d'envoyer le CSR à une autorité de certification, utilisez Citrix ADC CA Tools pour générer un certificat.

Créer un certificat à l'aide d'un assistant

1. Accédez à **Gestion du trafic > SSL**.
2. Dans le volet d'informations, sous **Mise en route**, sélectionnez l'Assistant pour le type de certificat que vous souhaitez créer.
3. Suivez les instructions à l'écran.

Créer un certificat racine CA à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days <positive_integer>]
<!--NeedCopy-->
```

Dans l'exemple suivant, csreq1 est le CSR et rsa1 est la clé privée créée précédemment.

Exemple :

```
create ssl cert cert1 csreq1 ROOT_CERT -keyFile rsa1 -keyForm PEM -days
     365

  Done
<!--NeedCopy-->
```

Créer un certificat CA intermédiaire à l'aide de l'interface de ligne de commande

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days <positive_integer>]
     [-certForm ( DER | PEM )] [-CAcert <input_filename>] [-CAcertForm (
     DER | PEM )] [-CAkey <input_filename>] [-CAkeyForm ( DER | PEM )]
    [-CAserial <output_filename>]
<!--NeedCopy-->
```

Dans l'exemple suivant, csr1 est le CSR créé précédemment. Cert1 et rsakey1 sont le certificat et la clé correspondante du certificat auto-signé (Root-CA), et pvtkey1 est la clé privée du certificat CA intermédiaire.

Exemple :

```
create ssl cert certsy csr1 INTM_CERT -CAcert cert1 -CAkey rsakey1 -
    CAserial 23
Done

create ssl rsakey pvtkey1 2048 -exponent F4 -keyform PEM
Done
<!--NeedCopy-->
```


Créer un certificat racine CA à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL** et, dans le groupe Mise en route, sélectionnez **Assistant Certificat Root CA**et configurez un certificat d'autorité de certification racine.

Créer un certificat CA intermédiaire à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL** et, dans le groupe Mise en route, sélectionnez **Assistant Certificat d'autorité de certification intermédiaire**et configurez un certificat d'autorité de certification intermédiaire.

Créer un certificat d'utilisateur final

Un certificat d'utilisateur final peut être un certificat client ou un certificat de serveur. Pour créer un certificat d'utilisateur final de test, spécifiez le certificat d'autorité de certification intermédiaire ou le certificat d'autorité de certification racine auto-signé.

> **Remarque :** Pour créer un certificat d'utilisateur final pour une utilisation en production, spécifiez un certificat d'autorité de certification approuvée et envoyez le CSR à une autorité de certification (CA).

Créer un certificat d'utilisateur final de test à l'aide de l'interface de ligne de commande

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days<positive_integer>]
    [-certForm ( DER | PEM )] [-CAcert <input_filename>] [-CAcertForm (
    DER | PEM )] [-CAkey<input_filename>] [-CAkeyForm ( DER | PEM )] [-
    CAserial <output_filename>]
<!--NeedCopy-->
```

S'il n'y a pas de certificat intermédiaire, utilisez les valeurs de certificat (cert1) et de clé privée (rsakey1) du certificat Root-CA dans `CAcert` et `CAkey`.

Exemple :

```
create ssl cert cert12 csr1 SRVR_CERT -CAcert cert1 -CAkey rsakey1 -
    CAserial 23

Done
<!--NeedCopy-->
```

S'il existe un certificat intermédiaire, utilisez les valeurs certificate (`certsy`) et clé privée (pvtkey1) du certificat intermédiaire dans `CAcert` et `CAkey`.

Exemple :

```
create ssl cert cert12 csr1 SRVR_CERT -CAcert certsy -CAkey pvtkey1 -
    CAserial 23

Done
<!--NeedCopy-->
```

Créer un certificat SAN auto-signé à l'aide d'OpenSSL

Pour créer un certificat SAN auto-signé avec plusieurs noms alternatifs d'objet, effectuez les opérations suivantes :

1. Créez un fichier de configuration OpenSSL sur votre ordinateur local en modifiant les champs liés selon les exigences de l'entreprise.

   Remarque : Dans l'exemple suivant, le fichier de configuration est « req.conf ».

   ```
   [req]
   distinguished_name = req_distinguished_name
   x509_extensions = v3_req
   prompt = no
   [req_distinguished_name]
   C = US
   ST = VA
   L = SomeCity
   O = MyCompany
   OU = MyDivision
   CN = www.company.com
   [v3_req]
   keyUsage = keyEncipherment, dataEncipherment
   extendedKeyUsage = serverAuth
   subjectAltName = @alt_names
   [alt_names]
   DNS.1 = www.company.net
   DNS.2 = company.com
   DNS.3 = company.net
   <!--NeedCopy-->
   ```

2. Chargez le fichier dans le répertoire /nsconfig/ssl de l'appliance Citrix ADC.
3. Connectez-vous à Citrix ADC CLI en tant qu'utilisateur `nsroot` et passez à l'invite de l'interpréteur de commandes.
4. Exécutez la commande suivante pour créer le certificat :


```
cd /nsconfig/ssl
openssl req -x509 -nodes -days 730 -newkey rsa:2048 -keyout cert.
   pem -out cert.pem -config req.conf -extensions 'v3_req'
<!--NeedCopy-->
```

5. Exécutez la commande suivante pour vérifier le certificat :

```
openssl x509 -in cert.pem -noout  - text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
ed:90:c5:f0:61:78:25:ab
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=VA, L=SomeCity, O=MyCompany, OU=MyDivision, CN=
   www.company.com
Validity
Not Before: Nov 6 22:21:38 2012 GMT
Not After : Nov 6 22:21:38 2014 GMT
Subject: C=US, ST=VA, L=SomeCity, O=MyCompany, OU=MyDivision, CN=
   www.company.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
…
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage:
Key Encipherment, Data Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 Subject Alternative Name:
DNS:www.company.net, DNS:company.com, DNS:company.net
Signature Algorithm: md5WithRSAEncryption …
<!--NeedCopy-->
```

Installer, lier et mettre à jour des certificats

August 20, 2021

Pour installer un certificat, reportez-vous à la section Ajouter ou mettre à jour une paire de clés de certificat.

Certificats de liaison

De nombreux certificats de serveur sont signés par plusieurs autorités de certification (CA) hiérarchiques, ce qui signifie que les certificats forment une chaîne comme suit :

```
Root CA
|
+---------- Intermediate CA
|
+---------------------- End-Entity (Server) Certificate
```

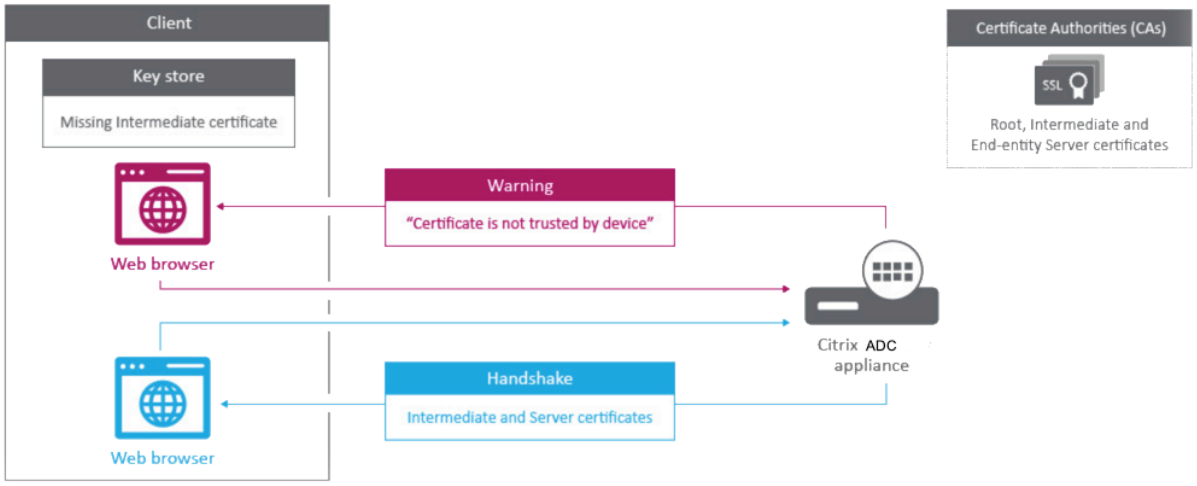
Parfois, l'autorité de certification intermédiaire est divisée en un certificat d'autorité de certification intermédiaire primaire et secondaire. Ensuite, les certificats forment une chaîne comme suit :

```
Root CA
|
+------ Primary Intermediate CA
|+-------------- Secondary Intermediate CA
|
+---------------------- End-Entity (Server) Certificate
```

Les machines clientes contiennent généralement le certificat d'autorité de certification racine dans leur magasin de certificats local, mais pas un ou plusieurs certificats d'autorité de certification intermédiaire. L'appliance ADC doit envoyer un ou plusieurs certificats d'autorité de certification intermédiaire aux clients.

Remarque : l'appliance ne doit pas envoyer le certificat d'autorité de certification racine au client. Le modèle de relation d'approbation PKI (Public Key Infrastructure) nécessite l'installation de certificats d'autorité de certification racine sur les clients via une méthode out-of-band. Par exemple, les certificats sont inclus avec le système d'exploitation ou le navigateur Web. Le client ignore un certificat d'autorité de certification racine envoyé par l'appliance.

Parfois, une autorité de certification intermédiaire que les navigateurs Web standard ne reconnaissent pas comme une autorité de certification approuvée émet le certificat du serveur. Dans ce cas, un ou plusieurs certificats d'autorité de certification doivent être envoyés au client avec le certificat du serveur. Sinon, le navigateur met fin à la session SSL car il ne parvient pas à authentifier le certificat du serveur.



Lien vidéo vers Comment associer un certificat d'autorité intermédiaire ?

Reportez-vous aux sections suivantes pour ajouter le serveur et les certificats intermédiaires :

- Liaison manuelle de certificats
- Liaison automatique de certificats
- Créer une chaîne de certificats

Liaison manuelle de certificats

Remarque : cette fonctionnalité n'est pas prise en charge sur la plate-forme Citrix ADC FIPS et dans une configuration de cluster.

Au lieu d'ajouter et de lier des certificats individuels, vous pouvez désormais regrouper un certificat de serveur et jusqu'à neuf certificats intermédiaires dans un seul fichier. Vous pouvez spécifier le nom du fichier lors de l'ajout d'une paire de clés de certificat. Avant de le faire, assurez-vous que les conditions préalables suivantes sont remplies.

- Les certificats dans le fichier sont dans l'ordre suivant :
  - Certificat de serveur (doit être le premier certificat du fichier)
  - Facultativement, une clé de serveur
  - Certificat intermédiaire 1 (ic1)
  - Certificat intermédiaire 2 (ic2)
  - Certificat intermédiaire 3 (ic3), etc.
    Remarque : Les fichiers de certificat intermédiaire sont créés pour chaque certificat intermédiaire avec le nom "<certificatebundlename>.pem_ic<
    n>" où n est compris entre 1 et 9. Par exemple, bundle.pem_ic1, où **bundle** est le nom du jeu de certificats et ic1 est le premier certificat intermédiaire du jeu.
- L'option Bundle est sélectionnée.
- Pas plus de neuf certificats intermédiaires sont présents dans le fichier.

Le fichier est analysé et le certificat du serveur, les certificats intermédiaires et la clé du serveur (le cas échéant) sont identifiés. Tout d'abord, le certificat du serveur et la clé sont ajoutés. Ensuite, les certificats intermédiaires sont ajoutés, dans l'ordre dans lequel ils ont été ajoutés au fichier, et liés en conséquence.

Une erreur est signalée si l'une des conditions suivantes existe :

- Un fichier de certificat pour l'un des certificats intermédiaires existe sur l'appliance.
- La clé est placée avant le certificat du serveur dans le fichier.
- Un certificat intermédiaire est placé avant le certificat du serveur.
- Les certificats intermédiaires ne sont pas placés dans le fichier dans le même ordre qu'ils ont été créés.
- Aucun certificat n'est présent dans le fichier.
- Un certificat n'est pas au format PEM approprié.
- Le nombre de certificats intermédiaires dans le fichier dépasse neuf.

Ajouter un jeu de certificats à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un jeu de certificats et vérifier la configuration :

```
add ssl certKey <certkeyName> -cert <string> -key <string> -bundle (YES
    | NO)

show ssl

show ssl certlink
<!--NeedCopy-->
```

Dans l'exemple suivant, le jeu de certificats (bundle.pem) contient les fichiers suivants :

Certificat de serveur (bundle) lié à bundle_ic1

Premier certificat intermédiaire (bundle_ic1) lié à bundle_ic2

Deuxième certificat intermédiaire (bundle_ic2) lié à bundle_ic3

Troisième certificat intermédiaire (bundle_ic3)

```
add ssl certKey bundletest -cert bundle9.pem -key bundle9.pem -bundle
   yes

sh ssl certkey

1)      Name: ns-server-certificate
        Cert Path: ns-server.cert
```



```
        Key Path: ns-server.key
        Format: PEM
        Status: Valid,   Days to expiration:5733
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS
           Internal,CN=default OULLFT
        Validity
                Not Before: Apr 21 15:56:16 2016 GMT
                Not After : Mar  3 06:30:56 2032 GMT
        Subject:  C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS
           Internal,CN=default OULLFT
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

2)      Name: servercert
        Cert Path: complete/server/server_rsa_1024.pem
        Key Path: complete/server/server_rsa_1024.ky
        Format: PEM
        Status: Valid,   Days to expiration:7150
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 1F
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:  C=IN,ST=KAR,O=Citrix R&D Pvt Ltd,CN=Citrix
        Validity
                Not Before: Sep  2 09:54:07 2008 GMT
                Not After : Jan 19 09:54:07 2036 GMT
        Subject:  C=IN,ST=KAR,O=Citrix Pvt Ltd,CN=Citrix
        Public Key Algorithm: rsaEncryption
        Public Key size: 1024

3)      Name: bundletest
        Cert Path: bundle9.pem
        Key Path: bundle9.pem
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
```



```
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA9
        Validity
                Not Before: Nov 28 06:43:11 2014 GMT
                Not After : Nov 25 06:43:11 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=Server9
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

4)      Name: bundletest_ic1
        Cert Path: bundle9.pem_ic1
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA8
        Validity
                Not Before: Nov 28 06:42:56 2014 GMT
                Not After : Nov 25 06:42:56 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA9
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

5)      Name: bundletest_ic2
        Cert Path: bundle9.pem_ic2
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA7
        Validity
                Not Before: Nov 28 06:42:55 2014 GMT
                Not After : Nov 25 06:42:55 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA8
```



```
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

6)      Name: bundletest_ic3
        Cert Path: bundle9.pem_ic3
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA6
        Validity
                Not Before: Nov 28 06:42:53 2014 GMT
                Not After : Nov 25 06:42:53 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA7
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

7)      Name: bundletest_ic4
        Cert Path: bundle9.pem_ic4
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA5
        Validity
                Not Before: Nov 28 06:42:51 2014 GMT
                Not After : Nov 25 06:42:51 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA6
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

8)      Name: bundletest_ic5
        Cert Path: bundle9.pem_ic5
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
```



```
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA4
        Validity
                Not Before: Nov 28 06:42:50 2014 GMT
                Not After : Nov 25 06:42:50 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA5
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

9)      Name: bundletest_ic6
        Cert Path: bundle9.pem_ic6
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA3
        Validity
                Not Before: Nov 28 06:42:48 2014 GMT
                Not After : Nov 25 06:42:48 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA4
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

10)     Name: bundletest_ic7
        Cert Path: bundle9.pem_ic7
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA2
        Validity
                Not Before: Nov 28 06:42:46 2014 GMT
                Not After : Nov 25 06:42:46 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA3
```



```
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

11)     Name: bundletest_ic8
        Cert Path: bundle9.pem_ic8
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA1
        Validity
                Not Before: Nov 28 06:42:45 2014 GMT
                Not After : Nov 25 06:42:45 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA2
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

12)     Name: bundletest_ic9
        Cert Path: bundle9.pem_ic9
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=RootCA4096
        Validity
                Not Before: Nov 28 06:42:43 2014 GMT
                Not After : Nov 25 06:42:43 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA1
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048
Done

sh ssl certlink

1)      Cert Name: bundletest    CA Cert Name: bundletest_ic1
2)      Cert Name: bundletest_ic1        CA Cert Name: bundletest_ic2
3)      Cert Name: bundletest_ic2        CA Cert Name: bundletest_ic3
```



```
4)      Cert Name: bundletest_ic3        CA Cert Name: bundletest_ic4
5)      Cert Name: bundletest_ic4        CA Cert Name: bundletest_ic5
6)      Cert Name: bundletest_ic5        CA Cert Name: bundletest_ic6
7)      Cert Name: bundletest_ic6        CA Cert Name: bundletest_ic7
8)      Cert Name: bundletest_ic7        CA Cert Name: bundletest_ic8
9)      Cert Name: bundletest_ic8        CA Cert Name: bundletest_ic9
Done
<!--NeedCopy-->
```

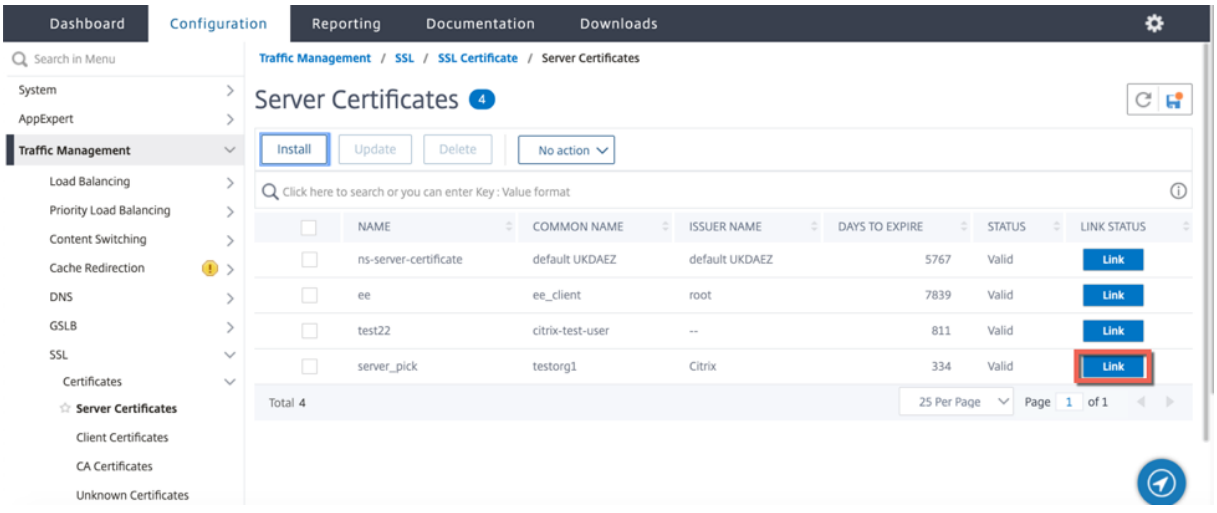
Ajouter un jeu de certificats à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Certificats > Certificats** de l'autorité de **certification**.
2. Dans le volet d'informations, cliquez sur **Installer**.
3. Dans la boîte de dialogue **Installer le certificat**, tapez les détails, tels que le nom du fichier de certificat et de clé, puis sélectionnez **Ensemble de certificats**.
4. Cliquez sur **Installer**, puis cliquez sur **Fermer**.

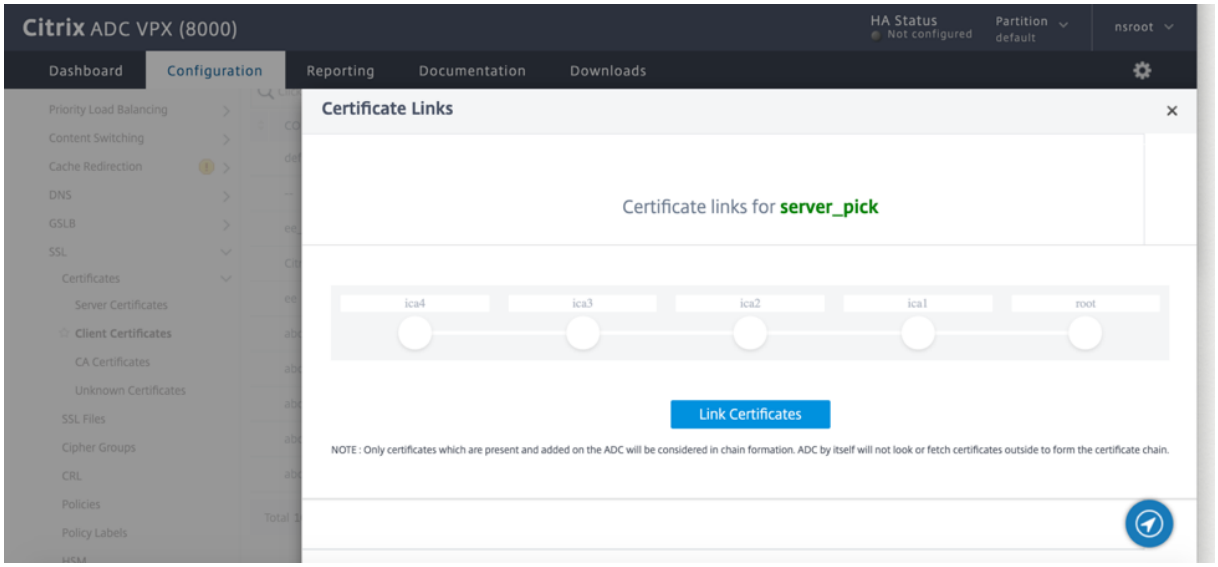
Liaison automatique de certificats

Remarque : Cette fonctionnalité est disponible à partir de la version 13.0 build 47.x.

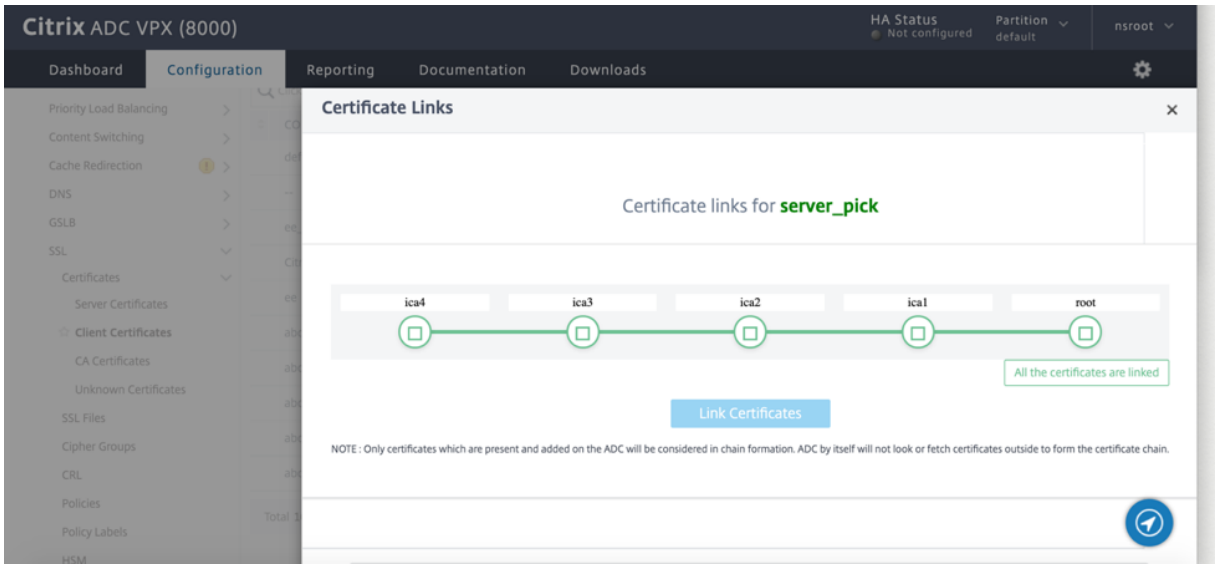
Vous n'avez plus à lier manuellement un certificat à son émetteur jusqu'au certificat racine. Si les certificats d'autorité de certification intermédiaire et le certificat racine sont présents sur l'appliance, vous pouvez cliquer sur le bouton **Lien** dans le certificat d'utilisateur final.



La chaîne potentielle apparaît.



Cliquez sur **Lien certificat** pour lier tous les certificats.



Créer une chaîne de certificats

Au lieu d'utiliser un ensemble de certificats (un seul fichier), vous pouvez créer une chaîne de certificats. La chaîne lie le certificat du serveur à son émetteur (l'autorité de certification intermédiaire). Cette approche nécessite que le fichier de certificat d'autorité de certification intermédiaire soit installé sur l'appliance ADC et que l'application cliente doit approuver l'un des certificats de la chaîne. Par exemple, liez Cert-Intermediate-A à Cert-Intermediate-B, où Cert-Intermediate-B est lié à Cert-Intermediate-C, qui est un certificat approuvé par l'application cliente.

Remarque : l'appliance prend en charge l'envoi d'un maximum de 10 certificats dans la chaîne de certificats envoyés au client (un certificat de serveur et neuf certificats d'autorité de certification).

Créer une chaîne de certificats à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une chaîne de certificats et vérifier la configuration. (Répétez la première commande pour chaque nouveau maillon de la chaîne.)

```
link ssl certkey <certKeyName> <linkCertKeyName>
show ssl certlink
<!--NeedCopy-->
```

Exemple :

```
link ssl certkey siteAcertkey CAcertkey
Done

show ssl certlink

linked certificate:
       1) Cert Name: siteAcertkey CA Cert Name: CAcertkey
Done
<!--NeedCopy-->
```

Créer une chaîne de certificats à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Certificats**.
2. Sélectionnez un certificat de serveur et, dans la liste **Action**, sélectionnez **Lien**, puis spécifiez un nom de certificat d'autorité de certification.

Mettre à jour un certificat de serveur existant

Pour modifier manuellement un certificat de serveur existant, vous devez effectuer les opérations suivantes :

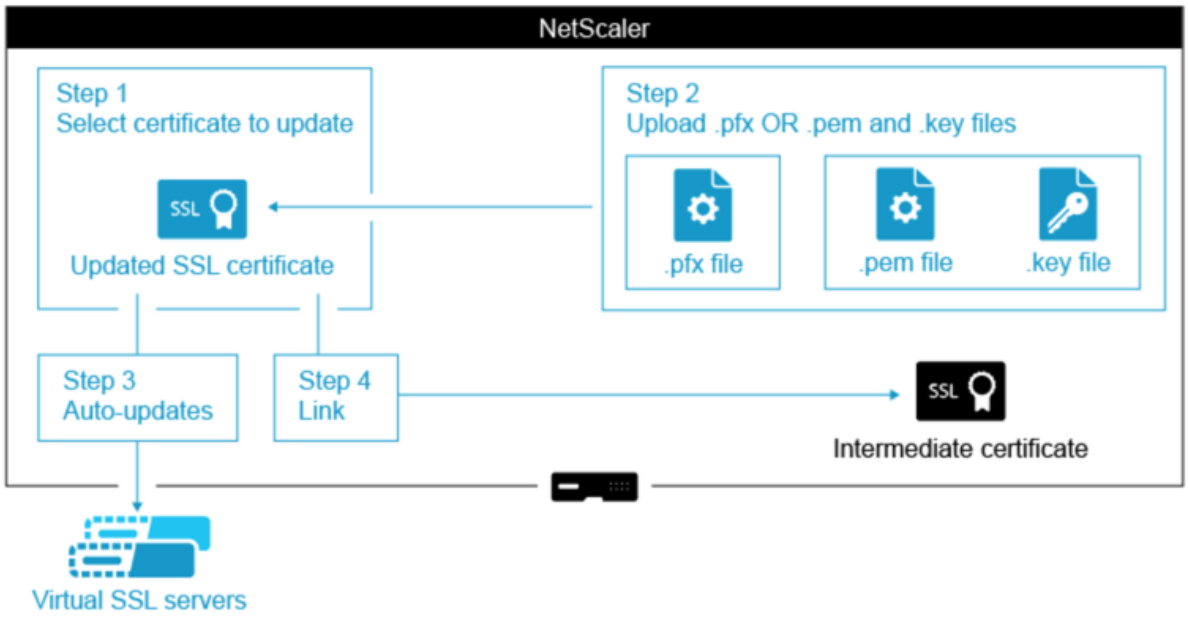
1. Délier l'ancien certificat du serveur virtuel.
2. Supprimez le certificat de l'appliance.
3. Ajoutez le nouveau certificat à l'appliance.
4. Liez le nouveau certificat au serveur virtuel.

Pour réduire les temps d'inactivité lors du remplacement d'une paire de clés de certificat-clé, vous pouvez mettre à jour un certificat existant. Si vous souhaitez remplacer un certificat par un certificat émis à un autre domaine, vous devez désactiver les vérifications de domaine avant de mettre à jour le certificat.

Pour recevoir des notifications sur les certificats qui expirent, vous pouvez activer le moniteur d'expiration.

Lorsque vous supprimez ou dissociez la liaison d'un certificat d'un serveur virtuel SSL configuré ou d'un service, le serveur virtuel ou le service devient inactif. Ils sont actifs après qu'un nouveau certificat valide leur est lié. Pour réduire les temps d'inactivité, vous pouvez utiliser la fonctionnalité de mise à jour pour remplacer une paire de clés de certificat liée à un serveur virtuel SSL ou à un service SSL.

Schéma d'ensemble de la mise à jour d'un certificat SSL sur l'appliance Citrix ADC.



Lien vidéo vers Comment mettre à jour un certificat existant ?

Mettre à jour une paire de clés de certificat existante à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour mettre à jour une paire de clés de certificat existante et vérifier la configuration :

```
update ssl certkey <certkeyName> -cert <string> -key <string>

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Exemple :

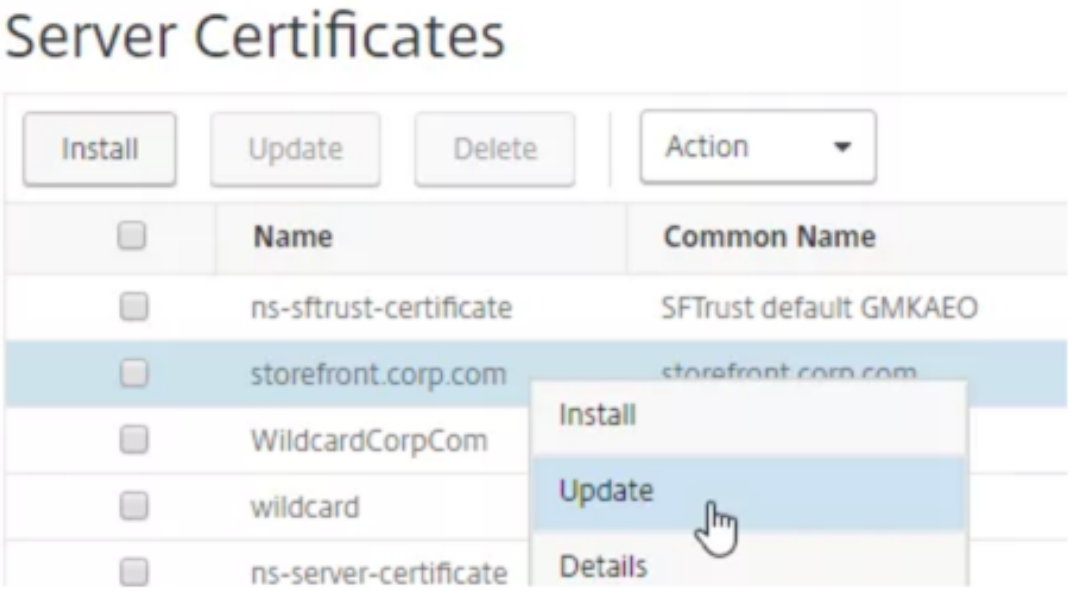
```
update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /
   nsconfig/ssl/pkey.pem

Done

```



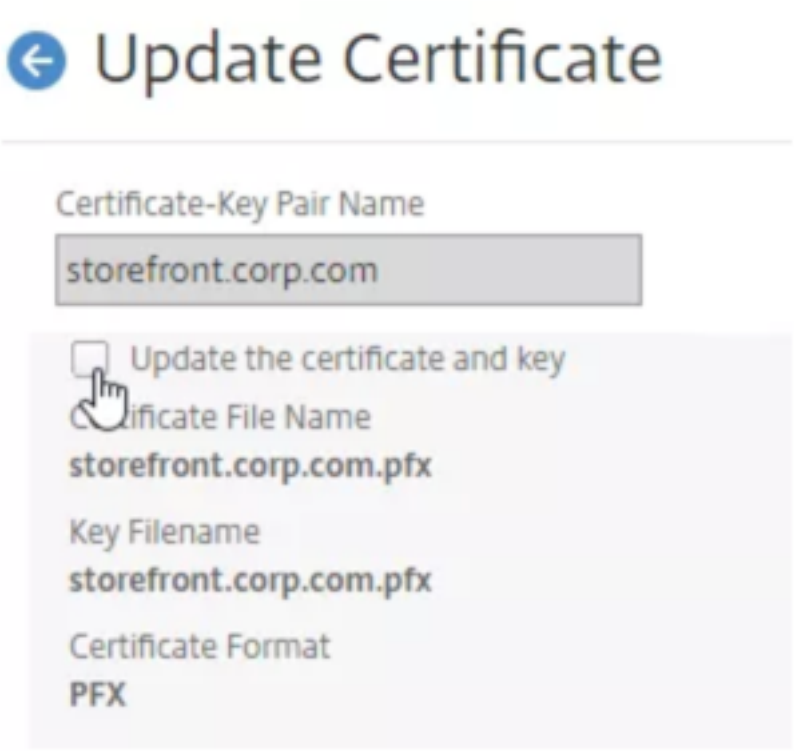
```
show ssl certkey siteAcertkey

Name: siteAcertkey       Status: Valid
           Version: 3
           Serial Number: 02
           Signature Algorithm: md5WithRSAEncryption
           Issuer: /C=US/ST=CA/L=Santa Clara/O=siteA/OU=Tech
           Validity
                Not Before: Nov 11 14:58:18 2001 GMT
                Not After: Aug 7 14:58:18 2004 GMT
           Subject: /C=US/ST-CA/L=San Jose/O=CA/OU=Security
           Public Key Algorithm: rsaEncryption
           Public Key size: 2048
Done
<!--NeedCopy-->
```

Mettre à jour une paire de clés de certificat existante à l'aide de l'interface graphique

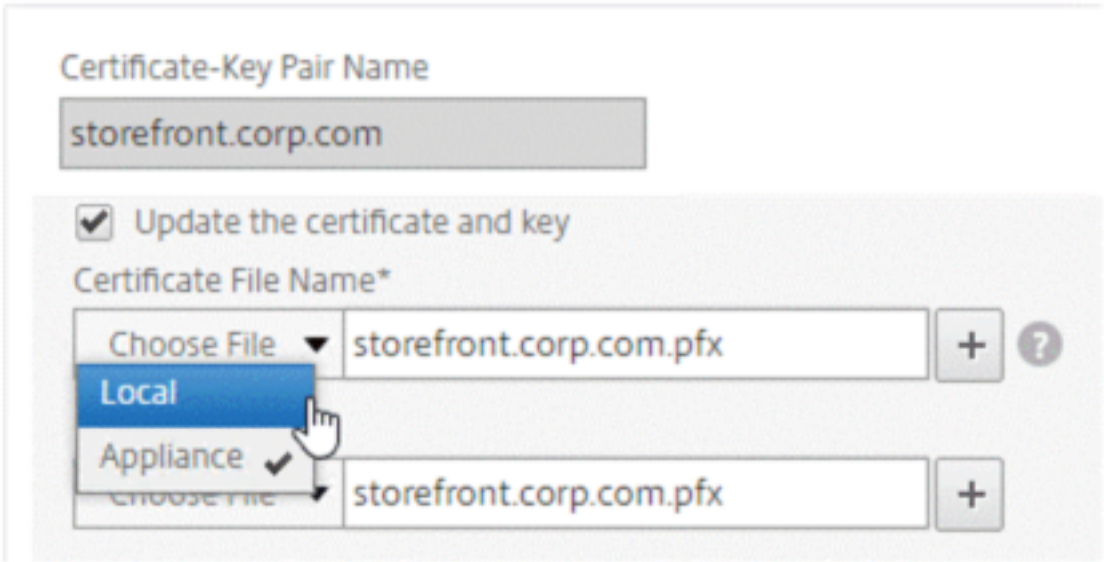
1. Accédez à **Gestion du trafic** > **SSL** > **Certificats > Certificatsde serveur**.
2. Sélectionnez le certificat à mettre à jour, puis cliquez sur **Mettre à jour**.



3. Sélectionnez **Mettre à jour le certificat et la clé**.



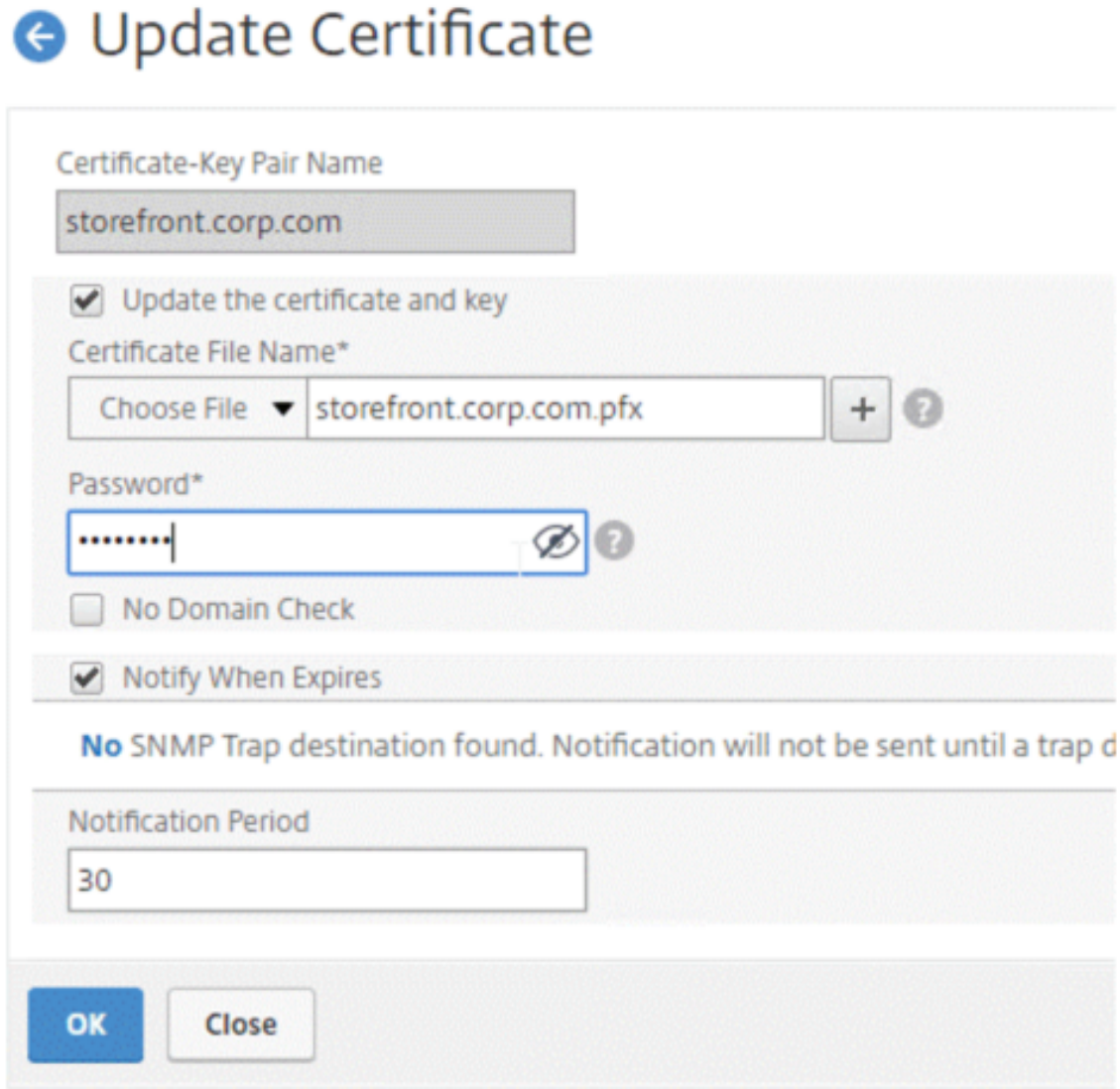
4. Dans **Nom du fichier de certificat**, cliquez sur **Choisir Fichier**> **Local** et accédez au fichier .pfx mis à jour ou au fichier PEM de certificat.



- Si vous téléchargez un fichier .pfx, vous êtes invité à spécifier le mot de passe du fichier .pfx.
- Si vous téléchargez un fichier pem de certificat, vous devez également télécharger un fichier de clé de certificat. Si la clé est chiffrée, vous devez spécifier le mot de passe de

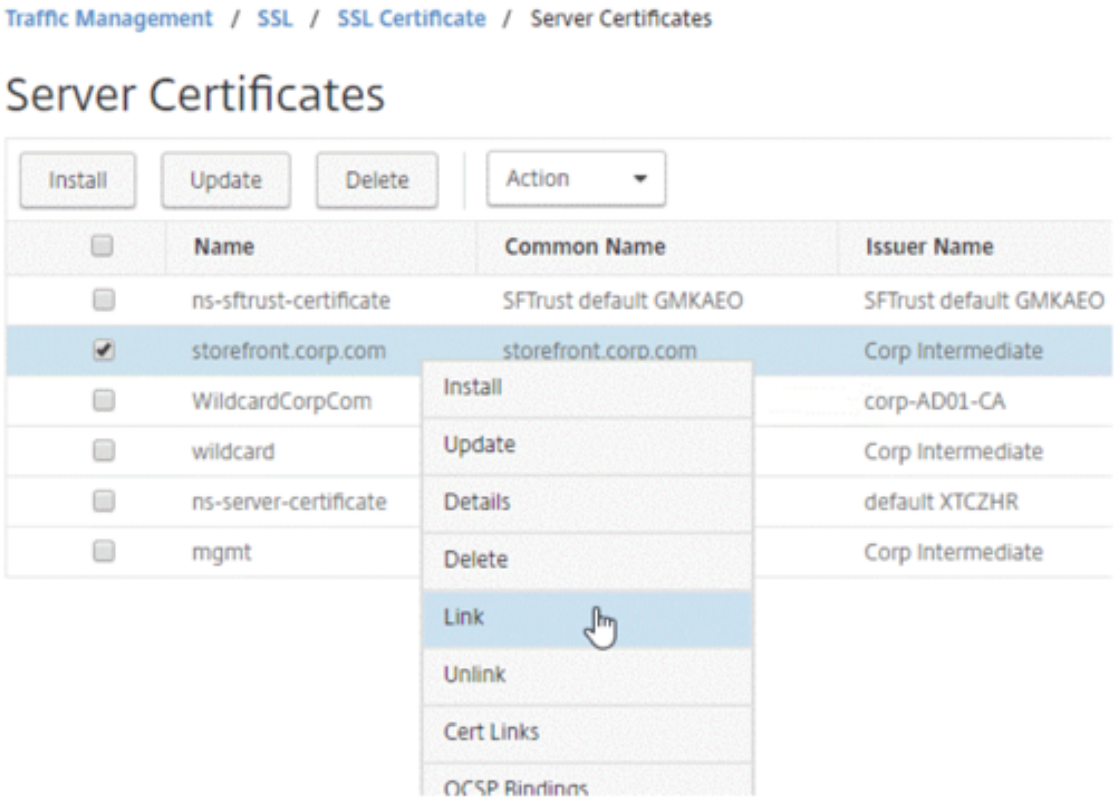
chiffrement.

5. Si le nom commun du nouveau certificat ne correspond pas à l'ancien certificat, sélectionnez **Aucune vérification de domaine**.
6. Cliquez sur **OK**. Tous les serveurs virtuels SSL auxquels ce certificat est lié sont automatiquement mis à jour.



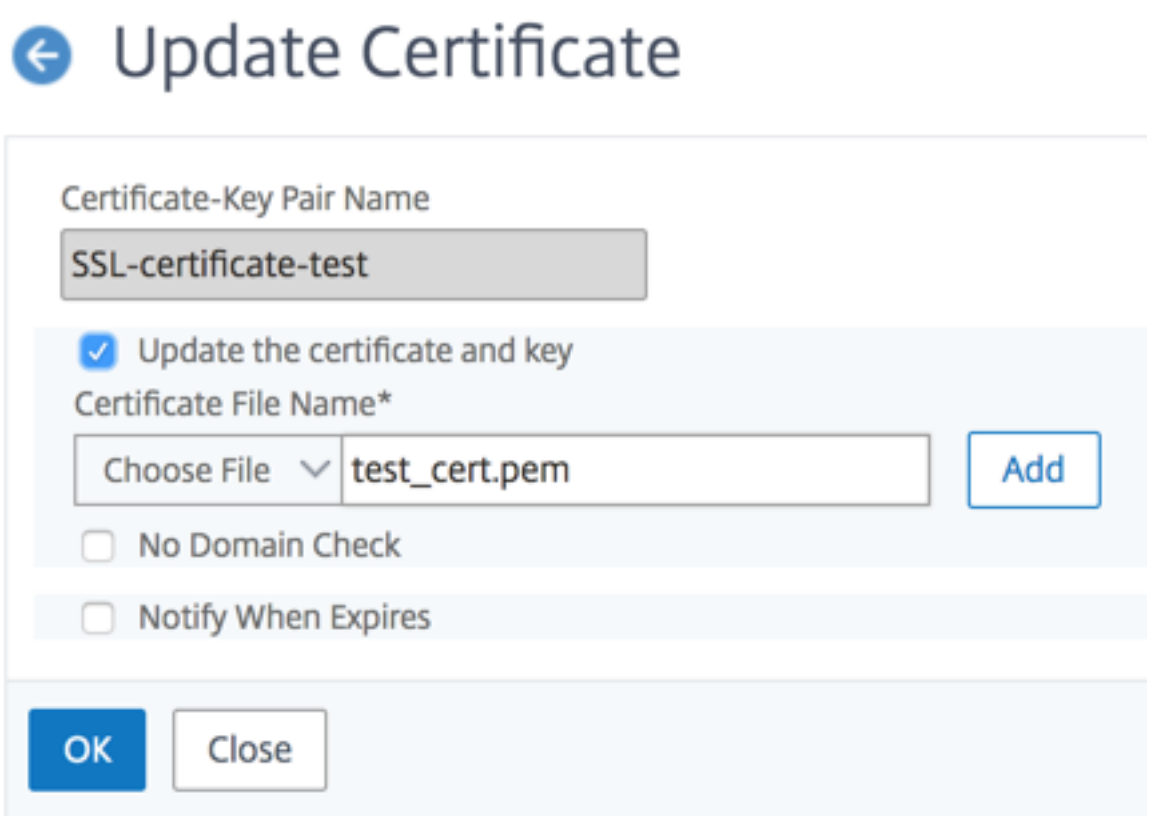
7. Après avoir remplacé le certificat, vous devrez peut-être mettre à jour le lien de certificat vers un nouveau certificat intermédiaire. Pour plus d'informations sur la mise à jour d'un certificat intermédiaire sans rompre les liens, voir Mettre à jour un certificat intermédiaire sans rompre les liens.
   - Cliquez avec le bouton droit sur le certificat mis à jour, puis cliquez sur **Liaisons**de certificats, pour voir s'il est lié à un certificat intermédiaire.
   - **Si le certificat n'est pas lié, cliquez avec le bouton droit sur le certificat mis à jour, puis**

cliquez sur Lier pour le lier à un certificat intermédiaire. Si aucune option de liaison ne s'affiche, vous devez d'abord installer un nouveau certificat intermédiaire sur l'appliance sous le nœud **Certificats de l'autorité de certification**.



Mettre à jour un certificat d'autorité de certification existant

Les étapes de mise à jour d'un certificat d'autorité de certification existant sont les mêmes que la mise à jour d'un certificat de serveur existant. La seule différence est que vous n'avez pas besoin d'une clé dans le cas des certificats d'autorité de certification.



Désactiver les vérifications de domaine

Lorsqu'un certificat SSL est remplacé sur l'appliance, le nom de domaine mentionné sur le nouveau certificat doit correspondre au nom de domaine du certificat en cours de remplacement. Par exemple, si vous avez un certificat émis sur abc.com et que vous le mettez à jour avec un certificat émis sur def.com, la mise à jour du certificat échoue.

Toutefois, si vous souhaitez que le serveur qui héberge un domaine particulier héberge un nouveau domaine, désactivez la vérification du domaine avant de mettre à jour son certificat.

Désactiver la vérification du domaine pour un certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour désactiver la vérification du domaine et vérifier la configuration :

```
update ssl certKey <certkeyName> -noDomainCheck

show ssl certKey <certkeyName>
<!--NeedCopy-->
```


Exemple :

```
update ssl certKey sv -noDomainCheck

Done

show ssl certkey sv

Name: sv
Cert Path: /nsconfig/ssl/complete/server/server_rsa_512.pem
Key Path: /nsconfig/ssl/complete/server/server_rsa_512.ky
Format: PEM
Status: Valid,   Days to expiration:9349
Certificate Expiry Monitor: DISABLED
Done
<!--NeedCopy-->
```

Désactiver la vérification du domaine pour un certificat à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Certificats**, sélectionnez un certificat et cliquez sur **Mettre à jour**.
2. Sélectionnez **Aucune vérification de domaine**.

Remplacez le certificat par défaut d'une appliance ADC par un certificat d'autorité de certification approuvé qui correspond au nom d'hôte de l'appliance

La procédure suivante suppose que le certificat par défaut (`ns-server-certificate`) est lié aux services internes.

1. Accédez à **Gestion du trafic > SSL > Certificats SSL > Créer une demande de certificat**.
2. Dans le nom commun, tapez `test.citrixadc.com`.
3. Soumettez le CSR à une autorité de certification approuvée.
4. Après avoir reçu le certificat de l'autorité de certification approuvée, copiez le fichier dans le `/nsconfig/ssl` répertoire.
5. Accédez à **Gestion du trafic > SSL > Certificats > Certificats de serveur**.
6. Sélectionnez le certificat de serveur par défaut (`ns-server-certificate`) et cliquez sur **Mettre à jour**.
7. Dans la boîte de dialogue **Mettre à jour** le **certificat, dans Nom du fichier du**certificat, accédez au certificat reçu de l'autorité de certification après la signature.
8. Dans le champ **Nom du fichier clé**, spécifiez le nom de fichier de clé privée par défaut (`ns-server.key`).
9. Sélectionnez **Aucune vérification de domaine**.

10. Cliquez sur **OK**.

Activer le moniteur d'expiration

Un certificat SSL est valide pour une période spécifique. Un déploiement standard inclut plusieurs serveurs virtuels qui traitent les transactions SSL, et les certificats qui leur sont liés peuvent expirer à des moments différents. Un moniteur d'expiration configuré sur l'appliance crée des entrées dans les journaux d'audit syslog et ns de l'appliance lorsqu'un certificat configuré doit expirer.

Si vous souhaitez créer des alertes SNMP pour l'expiration du certificat, vous devez les configurer séparément.

Activer un moniteur d'expiration pour un certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer un moniteur d'expiration pour un certificat et vérifier la configuration :

```
set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED | DISABLED ) [-
    notificationPeriod <positive_integer>]]

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Exemple :

```
set ssl certKey sv -expiryMonitor ENABLED  - notificationPeriod 60
Done
<!--NeedCopy-->
```

Activer un moniteur d'expiration pour un certificat à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Certificats**, sélectionnez un certificat et cliquez sur **Mettre à jour**.
2. Sélectionnez **Notifier quand expire**et spécifiez éventuellement une période de notification.

Mettre à jour un certificat intermédiaire sans rompre les liens

Vous pouvez maintenant mettre à jour un certificat intermédiaire sans rompre les liens existants. L'extension « AuthorityKeyIdentifier », dans le certificat lié émis par le certificat à remplacer, ne doit pas contenir de champ numéro de série du certificat d'autorité (« AuthorityCertSerialNumber »). Si l'extension 'AuthorityKeyIdentifier' contient un champ de numéro de série, les numéros de série du certificat de l'ancien et du nouveau certificat doivent être identiques. Vous pouvez mettre à jour

n'importe quel nombre de certificats dans le lien, un par un, si la condition précédente est remplie. Auparavant, les liens étaient cassés si un certificat intermédiaire était mis à jour.

Par exemple, il existe quatre certificats : CertACertB, CertC, et CertD. Certificat CertA est l'émetteur pour CertB, CertB est l'émetteur pour CertC, et ainsi de suite. Si vous souhaitez remplacer un certificat intermédiaire par CertB_new, CertB sans rompre le lien, la condition suivante doit être remplie :

Le numéro de série du certificat CertB doit correspondre au numéro de série du certificat CertB_new si les deux conditions suivantes sont remplies :

- L'extension AuthorityKeyIdentifier est présente dans CertC.
- Cette extension contient un champ de numéro de série.

Si le nom commun d'un certificat change, lors de la mise à jour du certificat spécifiez nodomaincheck.

Dans l'exemple précédent, pour remplacer "www.example.com" dans CertD par "*.example.com", sélectionnez le paramètre "No Domain Check".

Mettre à jour le certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
update ssl certKey <certkeyName> -cert <string> [-password] -key <
   string>  [-noDomainCheck]
<!--NeedCopy-->
```

Exemple :

```
update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /
   nsconfig/ssl/pkey.pem -noDomainCheck
<!--NeedCopy-->
```

Afficher une chaîne de certificats

Un certificat contient le nom de l'autorité émettrice et le sujet auquel le certificat est délivré. Pour valider un certificat, vous devez consulter l'émetteur de ce certificat et confirmer si vous lui faites confiance. Si vous ne faites pas confiance à l'émetteur, vous devez voir qui a émis le certificat d'émetteur. Accédez à la chaîne jusqu'à ce que vous atteigniez le certificat d'autorité de certification racine ou un émetteur en qui vous avez confiance.

Dans le cadre de la connexion SSL, lorsqu'un client demande un certificat, l'appliance présente un certificat et la chaîne de certificats émetteurs présents sur l'appliance. Un administrateur peut afficher la chaîne de certificats des certificats présents sur l'appliance et installer les certificats manquants.

Afficher la chaîne de certificats des certificats présents sur l'appliance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show ssl certchain <cert_name>
<!--NeedCopy-->
```

Exemples

Il y a 3 certificats : c1, c2 et c3. Certificat c3 est le certificat d'autorité de certification racine et signe c2, et c2 signes c1. Les exemples suivants illustrent la sortie de la commande `show ssl certchain c1` dans différents scénarios.

Scénario 1 :

Le certificat c2 est lié à c1 et c3 est lié à c2.

Le certificat c3 est un certificat d'autorité de certification racine.

Si vous exécutez la commande suivante, les liens de certificat vers le certificat d'autorité de certification racine s'affichent.

```
show ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate name: c2              linked; not a root
       certificate
    2) Certificate name: c3              linked; root certificate
Done
<!--NeedCopy-->
```

Scénario 2 :

Le certificat c2 est lié à c1.

Le certificat c2 n'est pas un certificat d'autorité de certification racine.

Si vous exécutez la commande suivante, les informations selon lesquelles le certificat c3 est un certificat d'autorité de certification racine mais n'est pas lié à c2 s'affichent.

```
show ssl certchain c1

Certificate chain  details of certificate name c1 are:
    1) Certificate Name: c2              linked; not a root
       certificate
    2) Certificate Name: c3              not linked; root certificate
```



```
6      Done
7  <!--NeedCopy-->
```

Scénario 3 :

Les certificats c1, c2 et c3 ne sont pas liés mais sont présents sur l'appliance.

Si vous exécutez la commande suivante, des informations sur tous les certificats commençant par l'émetteur du certificat c1 s'affichent. Il est également spécifié que les certificats ne sont pas liés.

```
1  show ssl certchain c1
2
3  Certificate chain details of certificate name c1 are:
4      1) Certificate Name: c2                not linked; not a root
          certificate
5      2) Certificate Name: c3                not linked; root certificate
6      Done
7  <!--NeedCopy-->
```

Scénario 4 :

Le certificat c2 est lié à c1.

Le certificat c3 n'est pas présent sur l'appliance.

Si vous exécutez la commande suivante, les informations sur le certificat lié à c1 s'affichent. Vous êtes invité à ajouter un certificat avec le nom d'objet spécifié dans c2. Dans ce cas, l'utilisateur est invité à ajouter le certificat d'autorité de certification racine c3.

```
1  show ssl certchain c1
2
3  Certificate chain details of certificate name c1 are:
4      1) Certificate Name: c2                linked; not a root
          certificate
5      2) Certificate Name: /C=IN/ST=ka/O=netscaler/CN=test
6         Action: Add a certificate with this subject name.
7  Done
8  <!--NeedCopy-->
```

Scénario 5 :

Un certificat n'est pas lié au certificat c1 et le certificat émetteur de c1 n'est pas présent sur l'appliance.

Si vous exécutez la commande suivante, vous êtes invité à ajouter un certificat portant le nom du sujet dans le certificat c1.

```
1  sh ssl certchain c1
2
```



```
Certificate chain details of certificate name c1 are:
    1) Certificate Name: /ST=KA/C=IN
       Action: Add a certificate with this subject name.
<!--NeedCopy-->
```

Générer un certificat de test de serveur

January 21, 2021

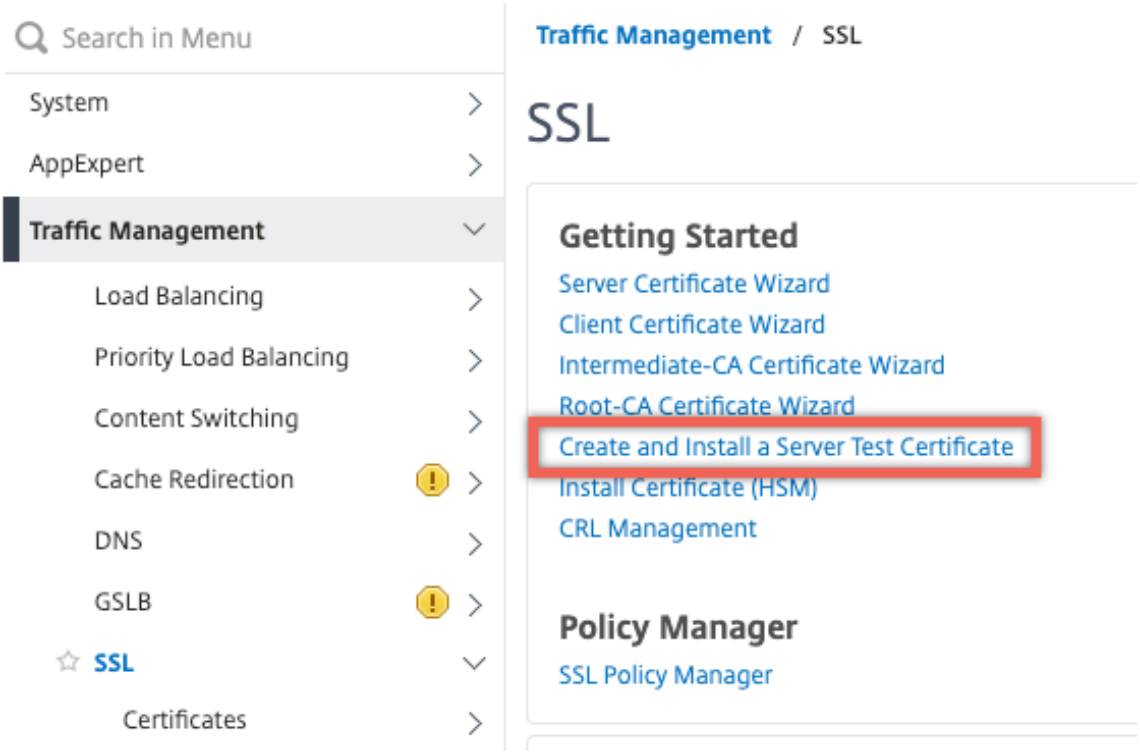
L'appliance Citrix ADC vous permet de créer un certificat de test pour l'authentification du serveur à l'aide d'un assistant GUI dans l'utilitaire de configuration. Un certificat de serveur est utilisé pour authentifier et identifier un serveur dans une poignée de main SSL. En règle générale, une autorité de certification approuvée émet un certificat de serveur. Le serveur envoie le certificat à un client qui l'utilise pour authentifier le serveur.

Pour l'émission d'un certificat de test de serveur, l'appliance fonctionne en tant qu'autorité de certification. Ce certificat peut être lié à un serveur virtuel SSL pour l'authentification dans une poignée de main SSL avec un client. Ce certificat est uniquement à des fins de test. Ne pas utiliser dans un environnement de production.

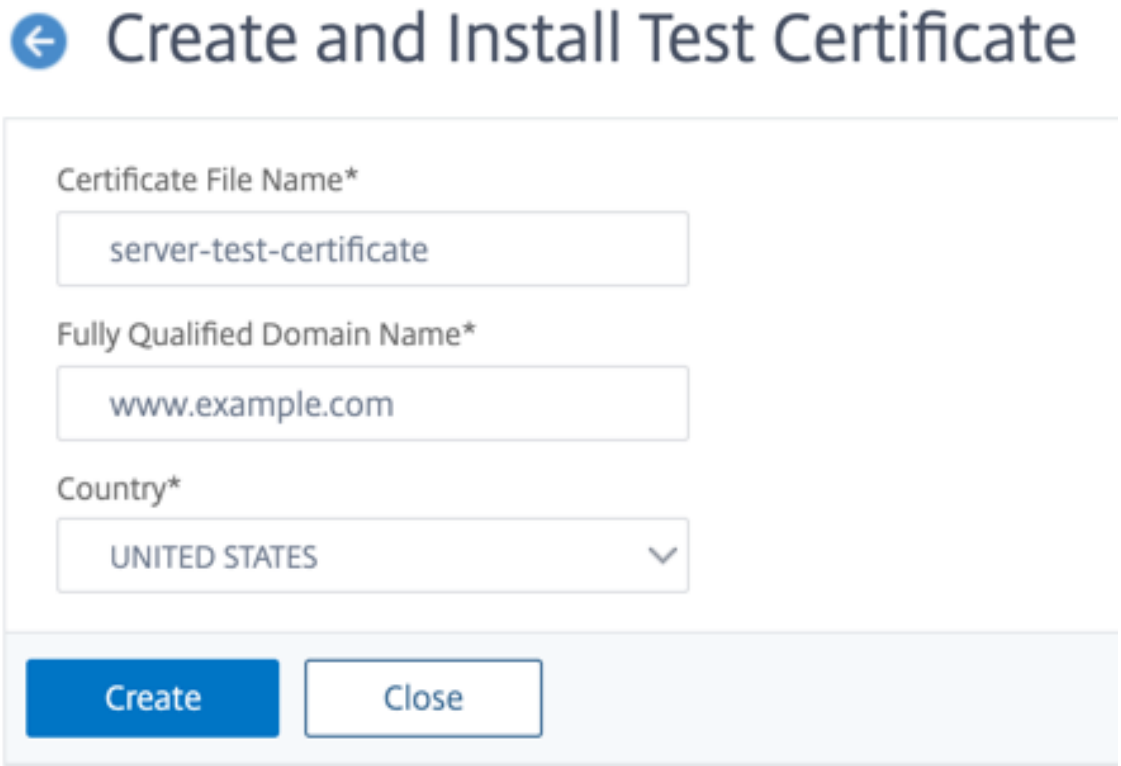
Vous pouvez installer le certificat de test de serveur sur n'importe quel serveur virtuel qui utilise le protocole SSL ou SSL_TCP.

Générer un certificat de test de serveur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL** et, dans le **groupe Certificats SSL**, sélectionnez **Créer et installer un certificat de test de serveur**.



2. Entrez les détails des paramètres et cliquez sur **Créer**.



Importer et convertir des fichiers SSL

August 20, 2021

Vous pouvez désormais importer des ressources SSL, telles que des certificats, des clés privées, des CRL et des clés DH, à partir d'hôtes distants, même si l'accès FTP à ces hôtes n'est pas disponible. Cette fonctionnalité est particulièrement utile dans les environnements où l'accès shell à l'hôte distant est restreint. Les dossiers par défaut sont créés dans /nsconfig/ssl comme suit :

- Pour les fichiers de certificat : /nsconfig/ssl/certfile
- Pour les clés privées : le fichier /nsconfig/ssl/keyfile
- Pour les listes de révocation des droits de révocation : /var/netscaler/ssl/crlfile
- Pour les clés DH : /nsconfig/ssl/dhfile

Les importations à partir de serveurs HTTP et HTTPS sont prises en charge. Toutefois, l'importation échoue si le fichier se trouve sur un serveur HTTPS qui nécessite l'authentification de certificat client pour l'accès.

> **Remarque :**
>
> La commande import n'est pas stockée dans le fichier de configuration (ns.conf), car le réimportation du fichier après un redémarrage peut provoquer une erreur.

Importer un fichier de certificat

Vous pouvez utiliser l'interface de ligne de commande et l'interface graphique pour importer un fichier (ressource) à partir d'un hôte distant.

Importer un fichier de certificat à partir d'un hôte distant à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
import ssl certFile [<name>] [<src>]
<!--NeedCopy-->
```

Exemple :

```
import ssl certfile my-certfile http://www.example.com/file_1
<!--NeedCopy-->
```

```
show ssl certfile
     Name : my-certfile
     URL : http://www.example.com/file_1
```



```
<!--NeedCopy-->
```

Pour supprimer un fichier de certificat, utilisez la commande `rm ssl certFile`, qui accepte uniquement l'argument 'name'.

Importer un fichier de clé à partir d'un hôte distant à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
import ssl keyFile [<name>] [<src>]
<!--NeedCopy-->
```

Exemple :

```
import ssl keyfile my-keyfile http://www.example.com/key_file
<!--NeedCopy-->
```

```
show ssl keyfile
     Name : my-keyfile
     URL : http://www.example.com/key_file
<!--NeedCopy-->
```

Pour supprimer un fichier clé, utilisez la commande `rm ssl keyFile`, qui accepte uniquement l'argument 'name'.

Importer un fichier CRL à partir d'un hôte distant à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
import ssl crlFile [<name>] [<src>]
<!--NeedCopy-->
```

Pour supprimer un fichier CRL, utilisez la commande `rm ssl crlFile` qui accepte uniquement l'argument <name>.

Exemple :

```
import ssl crlfile my-crlfile http://www.example.com/crl_file

show ssl crlfile

    Name : my-crlfile
    URL : http://www.example.com/crl_file
```



```
<!--NeedCopy-->
```

Importer un fichier DH à partir d'un hôte distant à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
import ssl dhFile [<name>] [<src>]
<!--NeedCopy-->
```

Exemple :

```
import ssl dhfile my-dhfile http://www.example.com/dh_file
show ssl dhfile
     Name : my-dhfile
     URL : http://www.example.com/dh_file
<!--NeedCopy-->
```

Pour supprimer un fichier DH, utilisez la commande `rm ssl dhFile`, qui accepte uniquement l'argument <name>.

Importer une ressource SSL à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > Importations**, puis sélectionnez l'onglet approprié.

Importer les certificats PKCS #8 et PKCS #12

Si vous souhaitez utiliser des certificats et des clés que vous possédez déjà sur d'autres serveurs ou applications sécurisés de votre réseau, vous pouvez les exporter, puis les importer dans l'appliance Citrix ADC. Vous devrez peut-être convertir les certificats et les clés exportés avant de pouvoir les importer dans l'appliance Citrix ADC.

Pour plus d'informations sur l'exportation de certificats à partir de serveurs ou d'applications sécurisés de votre réseau, consultez la documentation du serveur ou de l'application à partir duquel vous souhaitez exporter.

> **Remarque :**
>
> Pour l'installation sur l'appliance Citrix ADC, les noms de clé et de certificat ne peuvent pas contenir d'espaces ou de caractères spéciaux autres que ceux pris en charge par le système de fichiers UNIX. Suivez la convention de dénomination appropriée lorsque vous enregistrez la clé et le certificat exportés.

Un certificat et une paire de clés privées sont généralement envoyés au format PKCS #12. L'appliance prend en charge les formats PEM et DER pour les certificats et les clés. Pour convertir PKCS #12 en PEM ou DER, ou PEM ou DER en PKCS #12, consultez la section « Convertir les certificats SSL pour l'importation ou l'exportation » plus loin dans cette page.

L'appliance Citrix ADC ne prend pas en charge les clés PEM au format PKCS #8. Toutefois, vous pouvez convertir ces clés dans un format pris en charge à l'aide de l'interface OpenSSL, à laquelle vous pouvez accéder depuis l'interface CLI ou l'utilitaire de configuration. Avant de convertir la clé, vous devez vérifier que la clé privée est au format PKCS #8. Les clés au format PKCS #8 commencent généralement par le texte suivant :

```
-----BEGIN ENCRYPTED PRIVATE KEY-----



leuSSZQZKgrgUQ==



-----END ENCRYPTED PRIVATE KEY-----
<!--NeedCopy-->
```

Ouvrez l'interface OpenSSL à partir de l'interface CLI

1. Ouvrez une connexion SSH à l'appliance à l'aide d'un client SSH, tel que PuTTY.
2. Connectez-vous à l'appliance à l'aide des informations d'identification de l'administrateur.
3. À l'invite de commandes, tapez shell.
4. À l'invite shell, tapez `openssl`.

Ouvrez l'interface OpenSSL à partir de l'interface graphique

Accédez à **Gestion du trafic > SSL** et, dans le groupe Outils, sélectionnez **Interface OpenSSL**.

Convertir un format de clé PKCS #8 non pris en charge en un format de clé pris en charge chiffré à l'aide de l'interface OpenSSL

À l'invite OpenSSL, tapez l'une des commandes suivantes, selon que le format de clé non pris en charge est de type RSA ou ECDSA :

```
OpenSSL>rsa- in <PKCS#8 Key Filename> -des3 -out <encrypted Key
    Filename>

```



```
OpenSSL>ec -in <PKCS#8 Key Filename> -des3 -out <encrypted Key Filename
    >
<!--NeedCopy-->
```

Paramètres pour convertir un format de clé non pris en charge en format de clé pris en charge

- **PKCS #8 Key Filename :** nom de fichier d'entrée de la clé privée PKCS #8 incompatible.
- Nom de**fichier de clé chiffrée : nom** de fichier de sortie de la clé privée cryptée compatible au format PEM.
- Nom de**fichier de clé non chiffrée : nom** de fichier de sortie de la clé privée non chiffrée compatible au format PEM.

Convertir des certificats SSL pour l'importation ou l'exportation

Une appliance Citrix ADC prend en charge les formats PEM et DER pour les certificats SSL. D'autres applications, telles que les navigateurs clients et certains serveurs sécurisés externes, nécessitent divers formats PKCS (Public Key Cryptography Standard). L'appliance peut convertir le format PKCS #12 au format PEM ou DER pour l'importation d'un certificat dans l'appliance, et peut convertir PEM ou DER en PKCS #12 pour l'exportation d'un certificat. Pour plus de sécurité, la conversion d'un fichier pour importation peut inclure le chiffrement de la clé privée avec l'algorithme DES ou DES3.

> **Remarque :**
>
> Si vous utilisez l'interface graphique pour importer un certificat PKCS #12 et que le mot de passe contient un signe dollar ($), une citation arrière (‘) ou un caractère escape (), l'importation peut échouer. Si c'est le cas, le message ERREUR : mot de passe non valide s'affiche. Si vous devez utiliser un caractère spécial dans le mot de passe, veillez à le préfixer avec un caractère d'échappement (), sauf si toutes les importations sont effectuées à l'aide de l'interface de ligne de commande.

Convertir le format d'un certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
convert ssl pkcs12 <outfile> [-import [-pkcs12File <inputFilename>] [-
    des | -des3] [-export [-certFile <inputFilename>] [-keyFile <
    inputFilename>]]
<!--NeedCopy-->
```

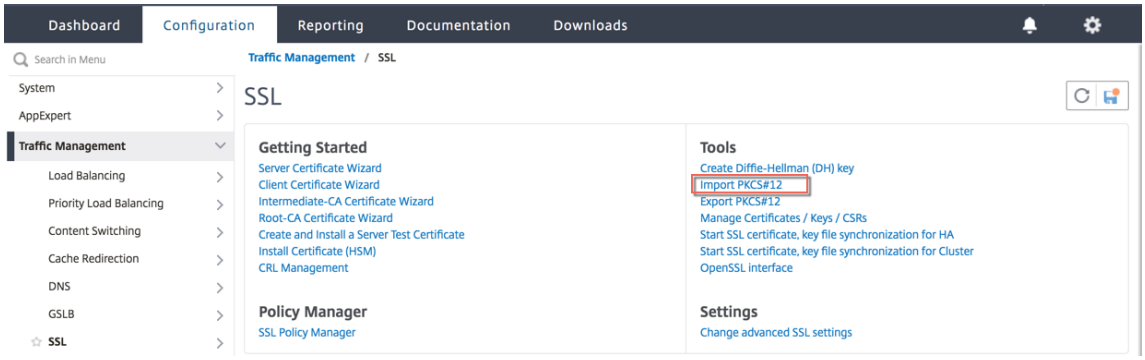
Au cours de l'opération, vous êtes invité à entrer un mot de passe d'importation ou un mot de passe d'exportation. Pour un fichier chiffré, vous êtes également invité à entrer une phrase secrète.

Exemple :

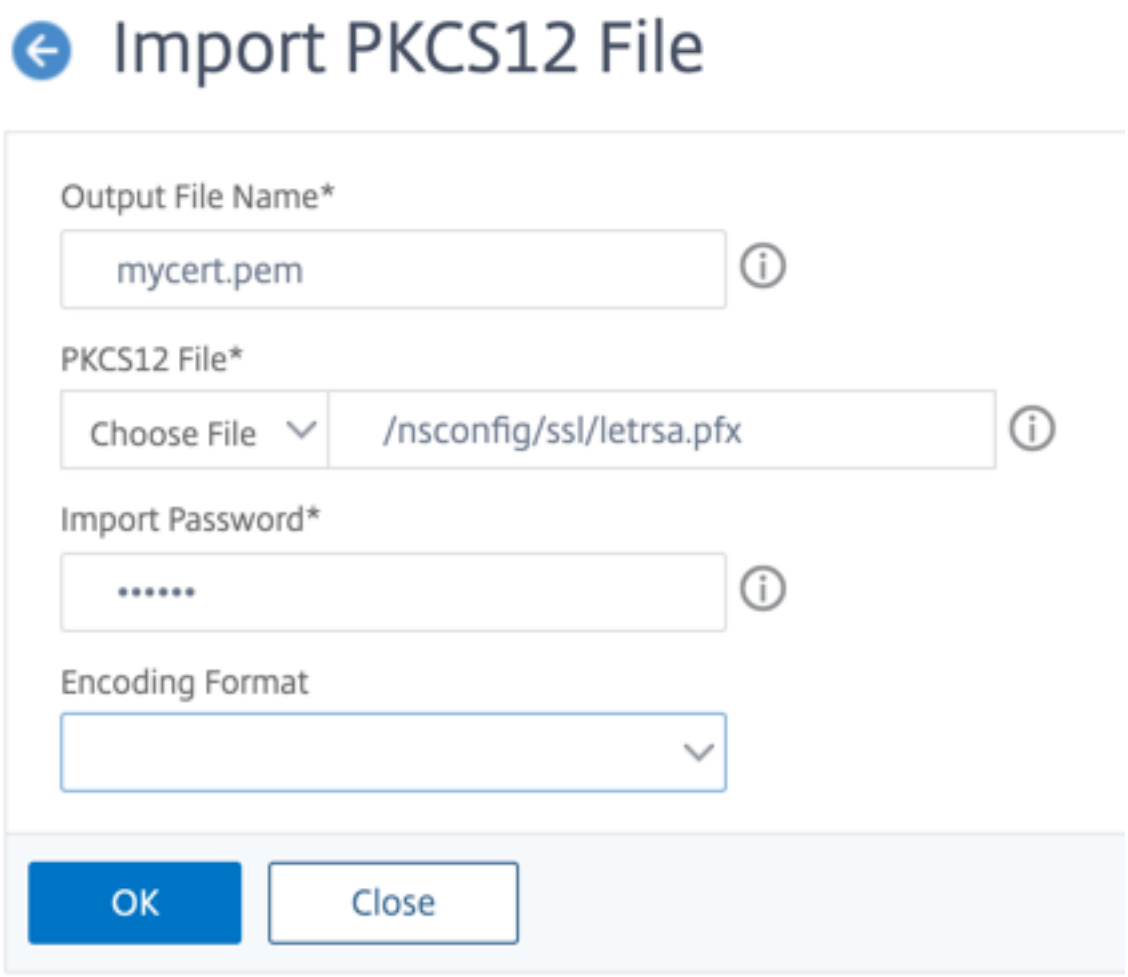

```
convert ssl pkcs12 Cert-Import-1.pem -import -pkcs12File Cert-Import-1.pfx -des

convert ssl pkcs12 Cert-Client-1.pfx -export -certFile Cert-Client-1 -keyFile Key-Client-1
<!--NeedCopy-->
```

Convertir le format d'un certificat à l'aide de l'interface graphique

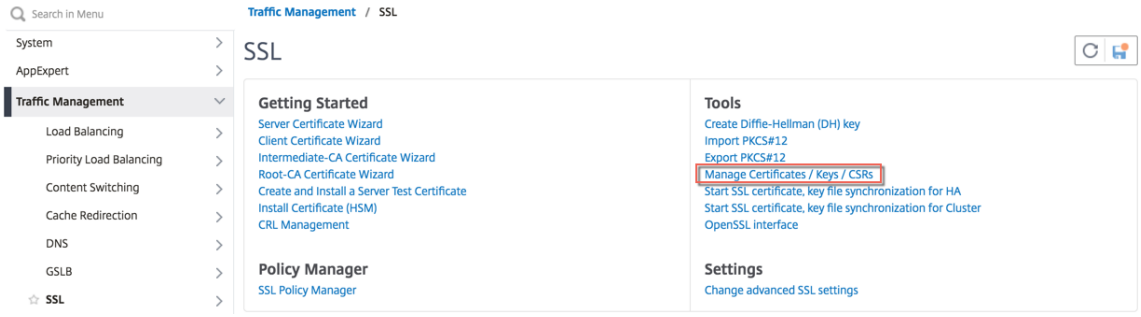
1. Accédez à **Gestion du trafic > SSL** et, dans le groupe **Outils**, sélectionnez **Importer PKCS #12**.



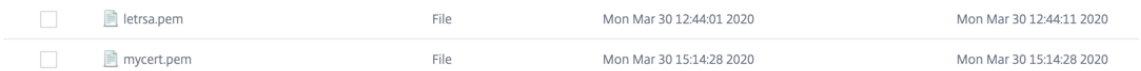
2. Spécifiez le nom du certificat PEM dans le champ **Nom du fichier de sortie**.
3. Accédez à l'emplacement du certificat PFX sur votre ordinateur local ou sur l'appliance.



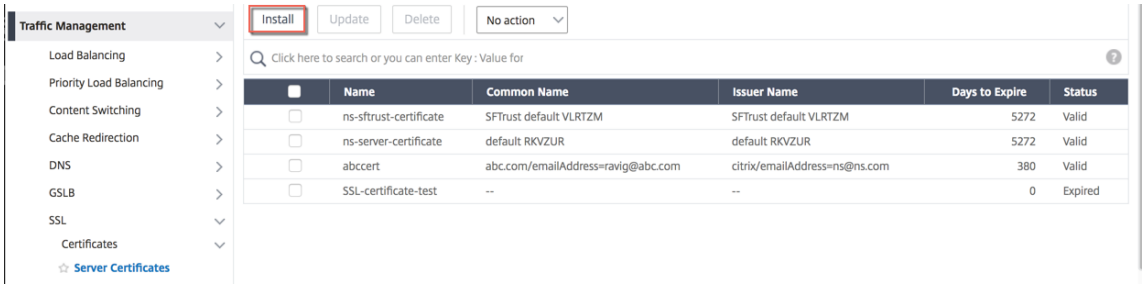
4. Cliquez sur **OK**.
5. Cliquez sur **Gérer les certificats/Clés/CSR** pour afficher le fichier PEM converti.



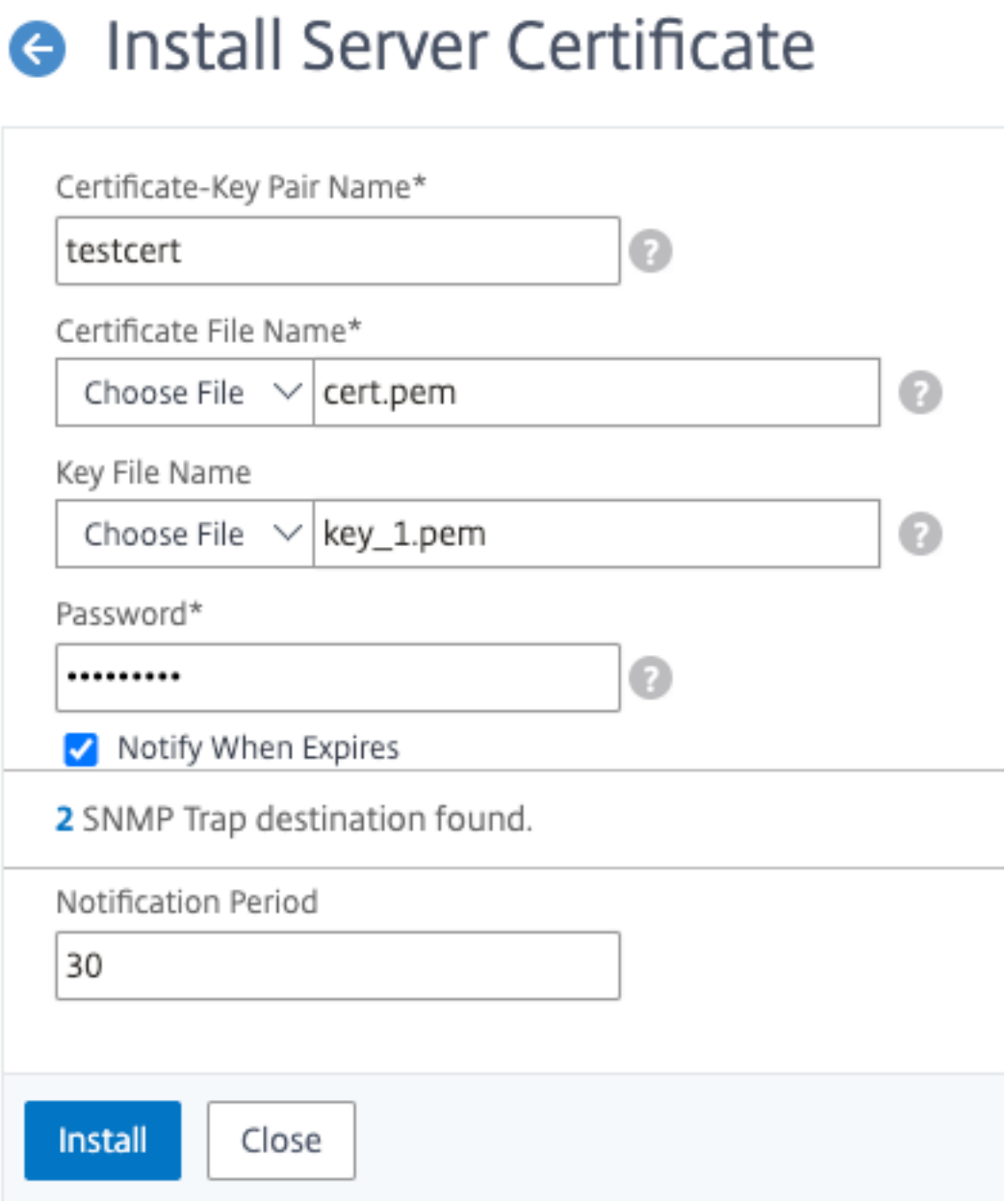
6. Vous pouvez afficher le fichier PFX téléchargé et le fichier PEM converti.



7. Accédez à **SSL** > **Certificats > Certificats** de **serveur** et cliquez sur **Installer**.



8. Spécifiez un **nom de paire de clés de certificat**.
9. Accédez à l'emplacement du fichier PEM.
10. Spécifiez le mot de passe lorsque vous y êtes invité.
11. Cliquez sur **Installer**.



12. Liez la paire de clés de certificat à un serveur virtuel SSL.

Liaison d'un certificat SSL à un serveur virtuel sur l'appliance Citrix ADC

October 5, 2021

Un certificat SSL est un élément essentiel des processus de cryptage et de déchiffrement SSL. Le certificat est utilisé lors d'une connexion SSL pour établir l'identité du serveur SSL, qui est l'appliance Citrix ADC car il agit en tant que point de terminaison SSL pour les clients.

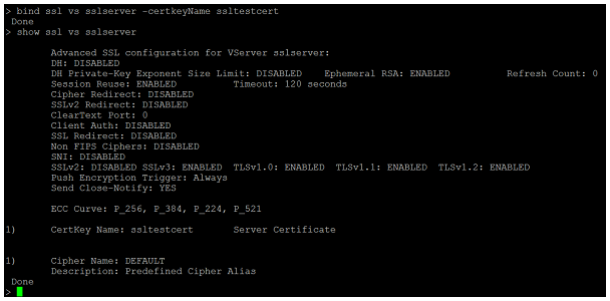
Le certificat utilisé pour traiter les transactions SSL doit être lié au serveur virtuel (SSL) qui reçoit les données SSL.

Pour lier un certificat SSL à un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

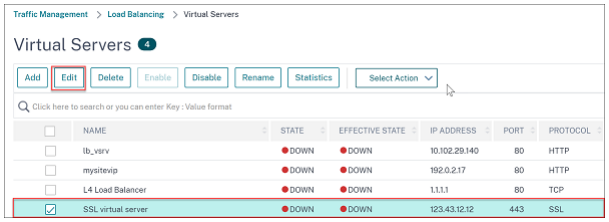
```
bind ssl vs <vServerName> -certkeyName <certificate-KeyPairName>
show ssl vs <vServerName>
<!--NeedCopy-->
```

Exemple :



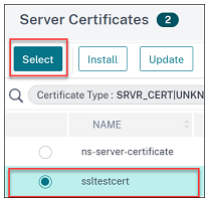
Pour lier un certificat SSL à un serveur virtuel SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel de type SSL, puis cliquez sur **Modifier**.



3. Dans la page **Serveur virtuel d'équilibrage de charge**, sous la section **Certificats**, cliquez sur **Aucun certificat de serveur**.

4. Dans la page **Liaison de certificat du serveur**, cliquez **sur Cliquez pour sélectionner**.
5. Sélectionnez le certificat SSL, puis cliquez sur **Sélectionner**.



6. Cliquez sur **Liaison pour lier** le certificat SSL au serveur virtuel.
7. Cliquez sur **Terminé**.

   Vous avez terminé de lier le certificat SSL au serveur virtuel.

Profils SSL

January 21, 2021

Un profil SSL est un ensemble de paramètres pour les entités SSL. Il offre une facilité de configuration et de flexibilité. Au lieu de configurer les paramètres sur chaque entité, vous pouvez les configurer dans un profil et lier le profil à toutes les entités auxquelles les paramètres s'appliquent.

L'infrastructure de profil SSL a été améliorée pour utiliser les derniers chiffrements et protocoles. Les différences entre le profil hérité (ancien profil) et le profil SSL amélioré (nouveau profil) sont mises en évidence.

Différences entre l'ancienne et la nouvelle infrastructure de profil SSL

Différences	Ancien profil	Nouveau profil
Chiffrements et courbes ECC inclus dans le profil	Non	Oui
Insertion d'un groupe de chiffrement ou de chiffrement au milieu d'une liste existante	Dissociez tous les chiffrements et liez à nouveau dans l'ordre de priorité requis.	Ajoutez un chiffrement et affectez-lui une priorité. Si aucune priorité n'est spécifiée, le chiffrement se voit attribuer la priorité la plus basse dans la liste.

Différences	Ancien profil	Nouveau profil
Dissociation de tous les chiffrements	`unbind ssl vserver \< name\> ciphername -ALL`	`unbind ssl profile -cipherName FlushAllCiphers` (La version 11.0 build 64.x ou ultérieure inclut le paramètre FlusHallCiphers pour délier tous les chiffrements ou groupes de chiffrement d'un profil, car ALL est traité comme un groupe de chiffrement.)
État de SSLv3	s/o	Désactivé sur le profil frontal par défaut (ns_default_ssl_profile_frontend). Remarque : Avant d'activer ce profil, SSLv3 est activé globalement. Après avoir activé le profil, SSLv3 est désactivé sur le profil par défaut frontal.

Infrastructure de profil SSL

August 20, 2021

Des vulnérabilités dans l'implémentation SSLv3 et RC4 ont souligné la nécessité d'utiliser les derniers chiffrements et protocoles pour négocier les paramètres de sécurité d'une connexion réseau. La mise en œuvre de toute modification de la configuration, telle que la désactivation de SSLv3 sur des milliers de points de terminaux SSL, est un processus fastidieux. Par conséquent, les paramètres qui faisaient partie de la configuration des points de fin SSL ont été déplacés vers les profils SSL, ainsi que les chiffrements par défaut. Pour implémenter des modifications dans la configuration, y compris la prise en charge du chiffrement, vous devez uniquement modifier le profil lié aux entités.

Les profils SSL frontal et back-end par défaut contiennent tous les chiffrements et courbes ECC par défaut, en plus des paramètres qui faisaient partie des anciens profils. Des exemples de résultats pour les profils par défaut sont fournis en annexe. L'opération Activer le profil par défaut lie automatiquement le profil frontal par défaut à toutes les entités frontales, et le profil principal par défaut à toutes

les entités back-end. Vous pouvez modifier un profil par défaut en fonction de votre déploiement. Vous pouvez également créer des profils personnalisés et les lier aux entités SSL.

Le profil frontal contient des paramètres applicables à une entité frontale. Autrement dit, ils s'appliquent à l'entité qui reçoit des demandes d'un client. Généralement, cette entité est un serveur virtuel SSL ou un service SSL transparent sur l'appliance Citrix ADC. Le profil back-end contient des paramètres applicables à une entité back-end. C'est-à-dire qu'ils s'appliquent à l'entité sur l'appliance ADC qui envoie des demandes client à un serveur principal. Généralement, cette entité est un service SSL sur l'appliance Citrix ADC. Si vous essayez de configurer un paramètre non pris en charge, l'erreur `ERROR: Specified parameters are not applicable for this type of SSL profile` apparaît.

> **Important :**
>
> - Un profil SSL a priorité sur les paramètres SSL. C'est-à-dire que si vous configurez les paramètres SSL à l'aide de la `set ssl parameter` commande, puis liez un profil à une entité SSL, les paramètres du profil ont priorité.
> - Après la mise à niveau, si vous activez les profils par défaut, vous ne pouvez pas annuler les modifications. Autrement dit, les profils ne peuvent pas être désactivés. Enregistrez la configuration et créez une copie du fichier de configuration (ns.conf) avant d'activer les profils. Toutefois, si vous ne souhaitez pas utiliser les fonctionnalités du profil par défaut, vous pouvez continuer à utiliser les anciens profils SSL. Pour plus d'informations sur ces profils, voir Profil SSL hérité.
> - À partir de la version 11.1 51.x, dans l'interface graphique et CLI, une invite de confirmation est ajoutée lorsque vous activez le profil par défaut pour empêcher l'activation par erreur.

Commande :

```
set ssl parameter -defaultProfile ENABLED
    Save your configuration before enabling the Default profile. You
       cannot undo the changes. Are you sure you want to enable the
       Default profile? [Y/N]Y
Done
<!--NeedCopy-->
```

Par défaut, certains paramètres SSL, appelés *paramètres globaux*, s'appliquent à tous les points de fin SSL. Toutefois, si un profil est lié à un point de terminaison SSL, les paramètres globaux ne s'appliquent pas. Les paramètres spécifiés dans le profil s'appliquent à la place.

Points à noter

1. Un profil peut être lié à plusieurs serveurs virtuels, mais un serveur virtuel ne peut avoir qu'un seul profil lié à lui.

2. Pour supprimer un profil lié à un serveur virtuel, dissociez d'abord le profil.
3. Un groupe de chiffrement ou de chiffrement peut être lié à plusieurs profils à des priorités différentes.
4. Un profil peut avoir plusieurs chiffrements et groupes de chiffrement liés à différentes priorités.
5. Les modifications apportées à un groupe de chiffrement sont immédiatement répercutées dans tous les profils et dans tous les serveurs virtuels auxquels l'un des profils est lié.
6. Si une suite de chiffrement fait partie d'un groupe de chiffrement, modifiez le groupe de chiffrement pour supprimer cette suite de chiffrement avant de supprimer la suite de chiffrement du profil.
7. Si vous n'affectez pas de priorité à une suite de chiffrements ou à un groupe de chiffrements attachés à un profil, la priorité la plus basse lui est attribuée.
8. Vous pouvez créer un groupe de chiffrement personnalisé (également appelé groupe de chiffrement défini par l'utilisateur) à partir de groupes de chiffrement et de suites de chiffrement existants. Si vous créez un groupe de chiffrement A et y ajoutez des groupes de chiffrement X et Y existants, dans cet ordre, Y est assigné à une priorité inférieure à X. Autrement dit, le groupe ajouté a une priorité supérieure.
9. Si une suite de chiffrement fait partie de deux groupes de chiffrement attachés au même profil, la suite de chiffrement n'est pas ajoutée dans le deuxième groupe de chiffrement. La suite de chiffrement à la priorité la plus élevée est en vigueur lorsque le trafic est traité.
10. Les groupes de chiffrement ne sont pas développés dans le profil. Par conséquent, le nombre de lignes dans le fichier de configuration (ns.conf) est considérablement réduit. Par exemple, si deux groupes de chiffrement contenant 15 chiffrements chacun sont liés à un millier de serveurs virtuels SSL, l'extension ajoute 30*1000 entrées liées au chiffrement dans le fichier de configuration. Avec le nouveau profil, il n'aurait que deux entrées : une pour chaque groupe de chiffrement lié à un profil.
11. La création d'un groupe de chiffrement défini par l'utilisateur à partir de chiffrements et de groupes de chiffrement existants est une opération de copier-coller. Les modifications apportées au groupe d'origine ne sont pas reflétées dans le nouveau groupe.
12. Un groupe de chiffrement défini par l'utilisateur répertorie tous les profils dont il fait partie.
13. Un profil répertorie tous les serveurs virtuels SSL, services et groupes de services auxquels il est lié.
14. Si la fonctionnalité de profil SSL par défaut est activée, utilisez le profil pour définir ou modifier l'un des attributs d'une entité SSL. Par exemple, un serveur virtuel, un service, un groupe de services ou un service interne.

Enregistrer la configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 save config
```



```
2
3 shell
4
5 root@ns# cd /nsconfig
6
7 root@ns# cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber
     >
8 <!--NeedCopy-->
```

Exemple :

```
1 save config
2 shell
3 root@ns# cd /nsconfig
4 root@ns# cp ns.conf ns.conf.NS.11.0.jun.16
5 <!--NeedCopy-->
```

Activer le profil par défaut

> **Important :**
>
> Enregistrez votre configuration avant de mettre à niveau le logiciel et d'activer les profils par défaut.
>
> À partir de la version 11.1 build 51.x, dans l'interface graphique et l'interface de ligne de commande, une invite de confirmation apparaît lorsque vous activez le profil par défaut pour éviter de l'activer par erreur.

Commande : La commande suivante active le profil par défaut et lie ce profil aux entités SSL auxquelles un profil est déjà lié. C'est-à-dire que si un profil (par exemple P1) est déjà lié à une entité SSL, le profil frontal par défaut ou le profil back-end par défaut remplace P1. L'ancien profil (P1) n'est pas supprimé. Il s'agit maintenant d'un profil SSL amélioré et contient les paramètres précédents, ainsi que les chiffrements et courbes ECC. Si vous ne voulez pas le profil par défaut, vous pouvez lier explicitement P1 à l'entité SSL.

```
1 set ssl parameter -defaultProfile ENABLED
2     Save your configuration before enabling the Default profile. You
        cannot undo the changes. Are you sure you want to enable the
        Default profile? [Y/N]Y
3 Done
4 <!--NeedCopy-->
```

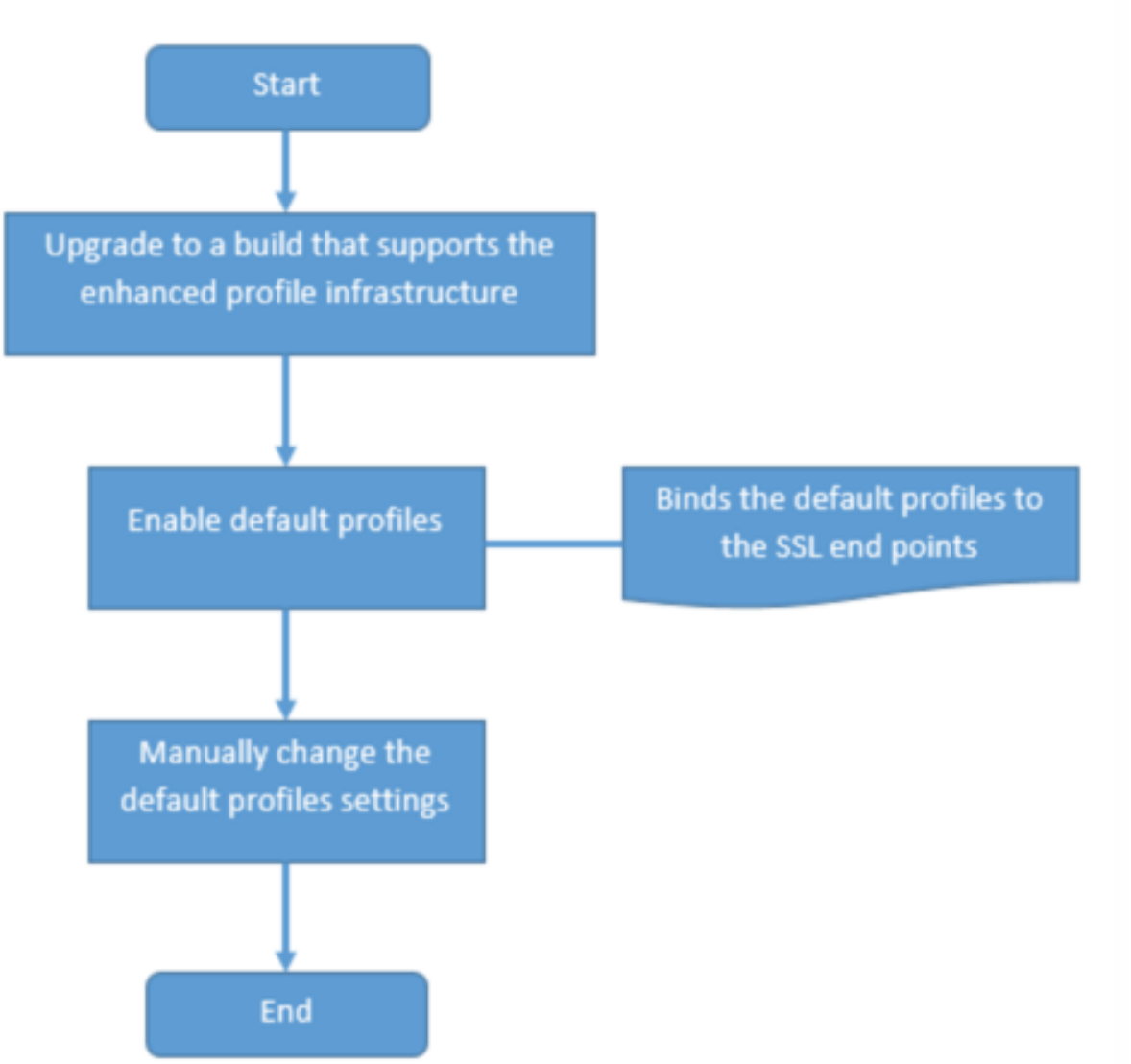
Mettez à niveau le logiciel vers une version prenant en charge l'infrastructure de profil améliorée, puis activez les profils par défaut.

> **Remarques :**
>
> - Si un profil hérité (P1) est déjà lié à une entité SSL et que vous activez le profil par défaut, le profil par défaut remplace la liaison précédente. Autrement dit, le profil par défaut est lié aux entités SSL. Si vous ne souhaitez pas que le profil par défaut soit lié, vous devez à nouveau lier P1 à l'entité SSL.
> - Une seule opération (Activer le profil par défaut ou`set ssl parameter -defaultProfile ENABLED`) active (lie) le profil frontal par défaut et le profil principal par défaut.

Cas d'utilisation

Après avoir activé les profils par défaut, ils sont liés à tous les points d'extrémité SSL. Les profils par défaut sont modifiables. Si votre déploiement utilise la plupart des paramètres par défaut et ne modifie que quelques paramètres, vous pouvez modifier les profils par défaut. Les changements sont immédiatement répercutés sur tous les points de fin. Vous pouvez également créer des profils SSL personnalisés avec des paramètres personnalisés et par défaut et les lier aux entités SSL.

L'organigramme suivant explique les étapes que vous devez effectuer :



1. Pour plus d'informations sur la mise à niveau du logiciel, reportez-vous à la section Mise à niveau du logiciel système.
2. Activez les profils par défaut à l'aide de l'interface de ligne de commande ou de l'interface graphique.

- Sur la ligne de commande, tapez : `set ssl parameter -defaultProfile ENABLED`
- Si vous préférez utiliser l'interface graphique, accédez à **Gestion du trafic** > **SSL** > **Modifier les paramètres SSL avancés**, faites défiler la page vers le bas et sélectionnez **Activer le profil par défaut**.

Si un profil n'était pas lié à un point de fin avant la mise à niveau, un profil par défaut est lié au point de fin SSL. Si un profil était lié à un point final avant la mise à niveau, le même profil est lié après la mise à niveau et les chiffrements par défaut sont ajoutés au profil.

1. (Facultatif) Modifiez manuellement les paramètres du profil par défaut.

- Sur la ligne de commande, tapez : `set ssl profile <name>` suivi des paramètres à modifier.
- Si vous préférez utiliser l'interface graphique, accédez à **Système** > **Profils**. Dans **Profils SSL**, sélectionnez un profil et cliquez sur **Modifier**.

Paramètres du profil SSL

Vous pouvez définir les paramètres SSL suivants dans un profil SSL. Vous pouvez définir certains de ces paramètres dans un serveur virtuel SSL. Pour plus d'informations sur les paramètres du serveur virtuel SSL, consultez Paramètres du serveur virtuel SSL.

Prise en charge de la renégociation sécurisée au niveau du back-end d'une appliance Citrix ADC

Remarque : Ce paramètre est introduit dans la version 13.0 build 58.x et ultérieure. Dans les versions et versions antérieures, seule la renégociation non sécurisée était prise en charge sur le back-end.

La fonctionnalité est prise en charge sur les plates-formes suivantes :

- VPX
- Plateformes MPX contenant des puces N2 ou N3
- Plates-formes à puce SSL Intel Coleto

La fonctionnalité n'est pas encore prise en charge sur la plate-forme FIPS.

La renégociation sécurisée est refusée par défaut sur le back-end d'une appliance ADC. C'est-à-dire que le `denySSLReneg` paramètre est défini sur ALL (par défaut).

Pour autoriser la renégociation sécurisée sur le back-end, sélectionnez l'un des paramètres suivants pour le paramètre `denySSLReneg` :

- NON
- FRONTEND_CLIENT
- FRONTEND_CLIENTSERVER
- NONSECURE

Activer la renégociation sécurisée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl profile <name> -denySSLReneg <denySSLReneg>
```

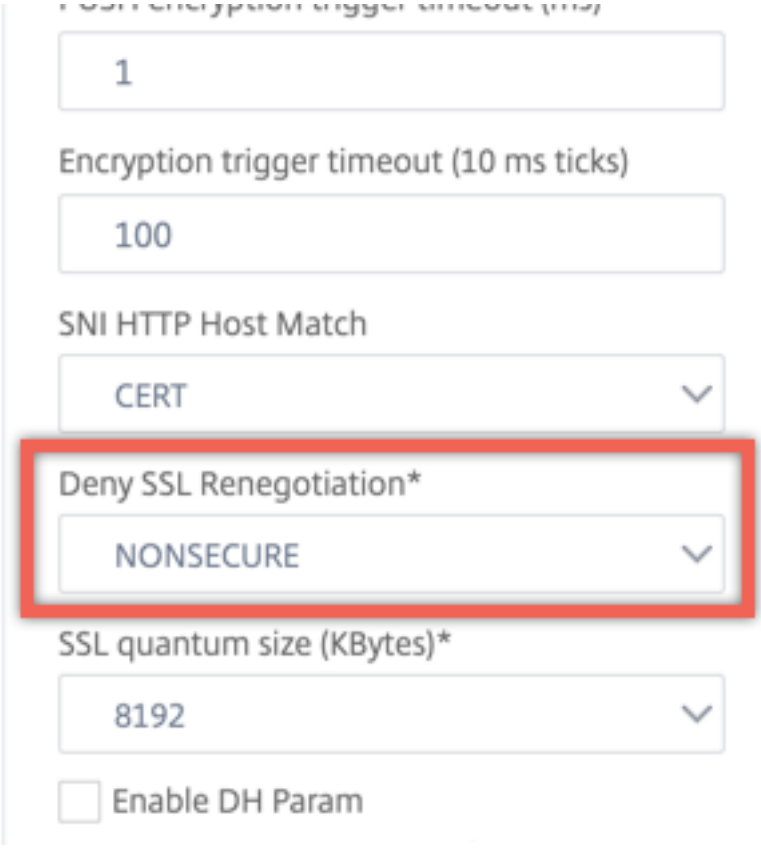
Exemple :


```
set ssl profile ns_default_ssl_profile_backend -denySSLReneg NONSECURE
 Done

sh ssl profile ns_default_ssl_profile_backend
1)  Name: ns_default_ssl_profile_backend    (Back-End)
    SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Server Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:       NO
    Session Reuse: ENABLED      Timeout: 300 seconds
    DH: DISABLED
    Ephemeral RSA: DISABLED
    Deny SSL Renegotiation      NONSECURE
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:    1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:      NO
    Push flag:  0x0 (Auto)
    SSL quantum size:       8 kB
    Encryption trigger timeout  100 mS
    Encryption trigger packet count:    45

    ECC Curve: P_256, P_384, P_224, P_521

1)  Cipher Name: DEFAULT_BACKEND        Priority :2
    Description: Predefined Cipher Alias

1)  Service Name: s187
 Done
<!--NeedCopy-->
```

Activer la renégociation sécurisée à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profil SSL**.
2. Ajouter ou modifier un profil.

3. Définissez **Refuser la renégociation SSL** sur toute valeur autre que ALL.



Validation en-tête hôte

Remarque : Ce paramètre est introduit dans la version 13.0 build 52.x.

Avec HTTP/1.1, les clients devaient utiliser plusieurs connexions pour traiter plusieurs requêtes. Avec HTTP/2, les clients peuvent réutiliser les connexions entre des domaines couverts par le même certificat. Pour une session activée SNI, l'appliance ADC doit être en mesure de contrôler la façon dont l'en-tête d'hôte HTTP est validé pour tenir compte de cette modification. Dans les versions antérieures, la demande a été supprimée si le paramètre était activé (défini sur « Oui ») et si la requête ne contenait pas l'en-tête hôte d'une session activée SNI. Si le paramètre était désactivé (défini sur « Non »), l'appliance n'a pas effectué la validation. Un nouveau paramètre `SNIHTTPHostMatch` est ajouté à un profil SSL et aux paramètres globaux SSL pour avoir un meilleur contrôle sur cette validation. Ce paramètre peut prendre trois valeurs : CERT, STRICT et NONE. Ces valeurs fonctionnent comme suit uniquement pour les sessions activées SNI. SNI doit être activé sur le serveur virtuel SSL ou sur le profil lié au serveur virtuel, et la requête HTTP doit contenir l'en-tête de l'hôte.

- CERT - La connexion est transférée si la valeur d'en-tête de l'hôte dans la demande est couverte par le certificat utilisé pour établir cette session SSL.
- STRICT - La connexion est transférée uniquement si la valeur d'en-tête d'hôte dans la requête

correspond à la valeur du nom du serveur passée dans le message Client Hello de la connexion SSL.

- NO - La valeur de l'en-tête de l'hôte n'est pas validée.

Valeurs possibles : NO, CERT, STRICT Valeur
par défaut : CERT

Avec l'introduction du nouveau paramètre, `SNIHTTPHostMatch` il y a un changement dans le comportement du `dropReqWithNoHostHeader` paramètre. Le `dropReqWithNoHostHeader` paramètre n'affecte plus la façon dont l'en-tête d'hôte est validé par rapport au certificat SNI.

Définir les paramètres de profil SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl profile <name> [-ssllogProfile <string>] [-dh ( ENABLED |
    DISABLED ) -dhFile <string>] [-dhCount <positive_integer>][-
    dhKeyExpSizeLimit ( ENABLED | DISABLED )] [-eRSA ( ENABLED |
    DISABLED) [-eRSACount <positive_integer>]] [-sessReuse ( ENABLED |
    DISABLED )
[-sessTimeout <positive_integer>]] [-cipherRedirect ( ENABLED |
    DISABLED ) [-cipherURL <URL>]] [-clientAuth ( ENABLED | DISABLED )[-
    clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED |
DISABLED )] [-redirectPortRewrite ( ENABLED | DISABLED )] [-ssl3 (
    ENABLED | DISABLED )] [-tls1 ( ENABLED | DISABLED )] [-tls11 (
    ENABLED| DISABLED )] [-tls12 ( ENABLED | DISABLED )] [-tls13 (
    ENABLED |DISABLED )] [-SNIEnable ( ENABLED | DISABLED )] [-
    ocspStapling (ENABLED | DISABLED )] [-serverAuth ( ENABLED |
    DISABLED )] [-commonName <string>] [-pushEncTrigger <pushEncTrigger
    >] [-sendCloseNotify ( YES |
NO )] [-clearTextPort <port|*>] [-insertionEncoding ( Unicode | UTF-8)]
     [-denySSLReneg <denySSLReneg>] [-quantumSize <quantumSize>]
[-strictCAChecks ( YES | NO )] [-encryptTriggerPktCount <
    positive_integer>] [-pushFlag <positive_integer>][-
    dropReqWithNoHostHeader ( YES | NO )] [-SNIHTTPHostMatch <
    SNIHTTPHostMatch>] [-pushEncTriggerTimeout <positive_integer>]
[-sslTriggerTimeout <positive_integer>] [-clientAuthUseBoundCAChain (
    ENABLED | DISABLED )] [-sslInterception ( ENABLED | DISABLED )][-
    ssliReneg ( ENABLED | DISABLED )] [-ssliOCSPCheck ( ENABLED |
    DISABLED )] [-ssliMaxSessPerServer <positive_integer>] [-HSTS (
    ENABLED| DISABLED )] [-maxage <positive_integer>] [-
    IncludeSubdomains ( YES | NO )] [-preload ( YES | NO )] [-
    sessionTicket ( ENABLED | DISABLED )][-sessionTicketLifeTime <
    positive_integer>] [-sessionTicketKeyRefresh (ENABLED | DISABLED )]
    {
```

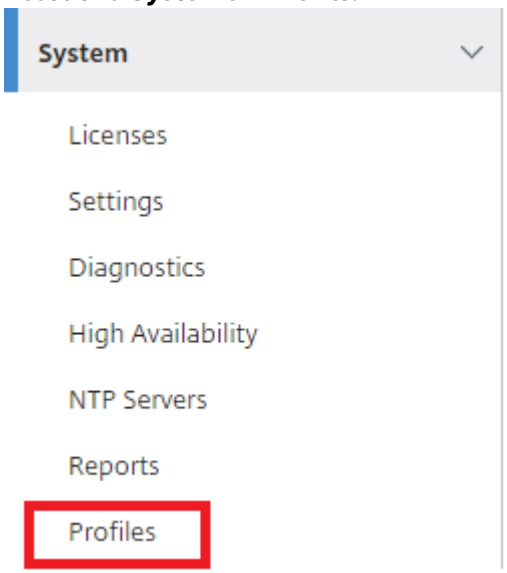


```
 -sessionTicketKeyData  }
  [-sessionKeyLifeTime <positive_integer>] [-prevSessionKeyLifeTime <
     positive_integer>]
[-cipherName <string> -cipherPriority <positive_integer>][-
   strictSigDigestCheck ( ENABLED | DISABLED )]
[-skipClientCertPolicyCheck ( ENABLED | DISABLED )] [-zeroRttEarlyData
   ( ENABLED | DISABLED )] [-tls13SessionTicketsPerAuthContext
<positive_integer>] [-dheKeyExchangeWithPsk ( YES | NO )]
<!--NeedCopy-->
```

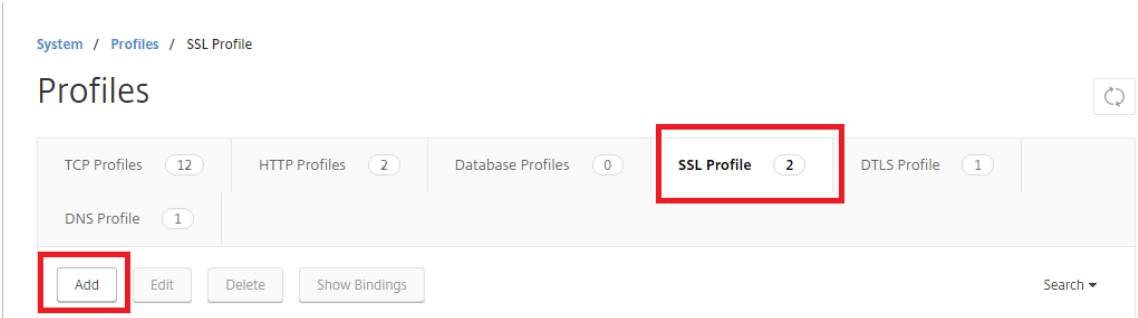
Définir les paramètres de profil SSL à l'aide de l'interface graphique

Pour ajouter un profil :

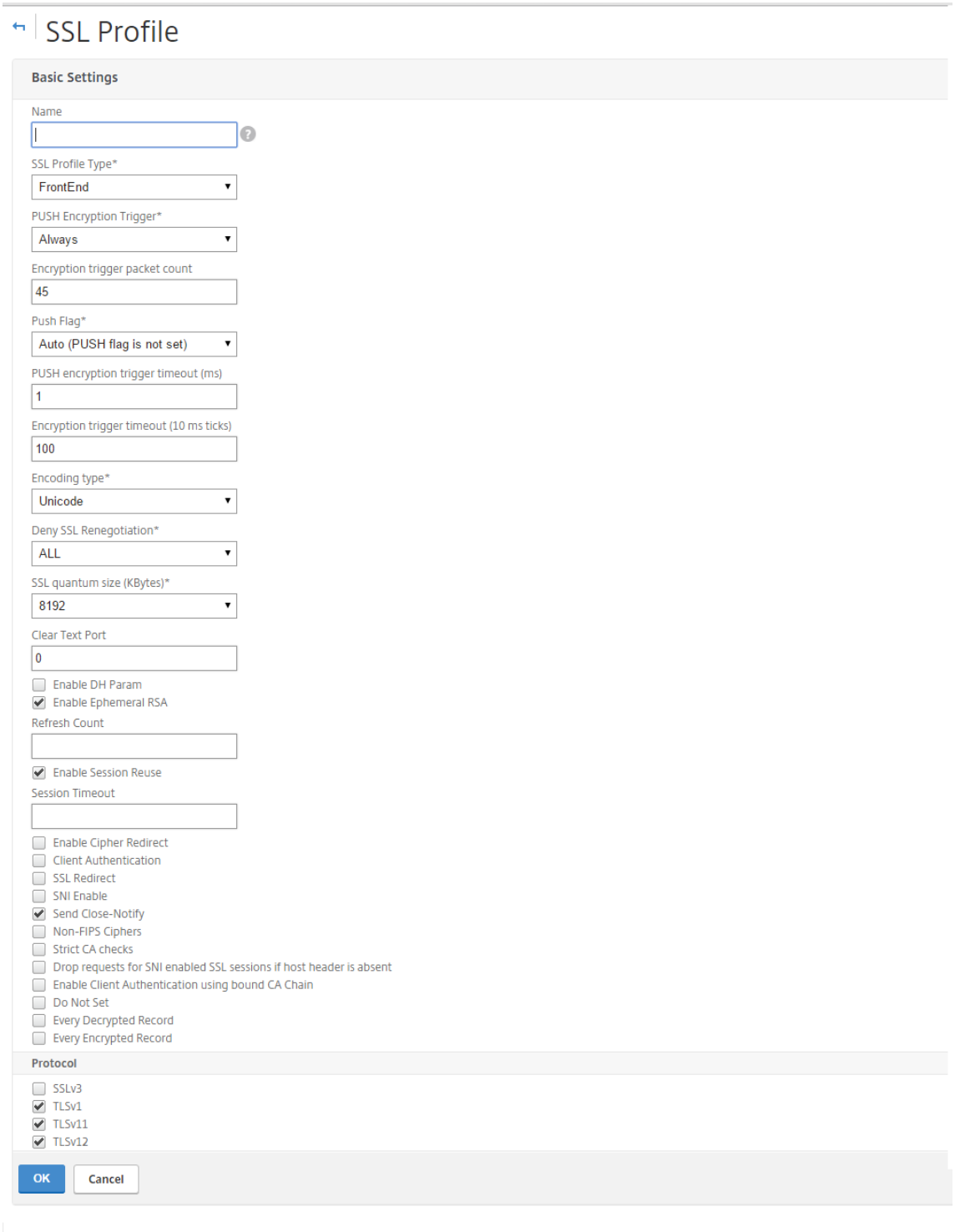
1. Accédez à **Système > Profils**.



2. Sélectionnez **Profils SSL**. Cliquez sur **Ajouter**.



3. Spécifiez les valeurs pour les différents paramètres.



4. Cliquez sur **OK**.
5. Cliquez sur **Terminé**.

Pour réutiliser un profil SSL existant :

1. Accédez à **Système > Profils**.
2. Sélectionnez un profil existant et cliquez sur **Ajouter**.

3. Spécifiez un nom différent, modifiez les paramètres, puis cliquez sur **OK**.
4. Cliquez sur **Terminé**.

Extension de ticket de session TLS

Une poignée de main SSL est une opération intensive en CPU. Si la réutilisation de session est activée, l'opération d'échange de clés serveur/client est ignorée pour les clients existants. Ils sont autorisés à reprendre leurs sessions. Cette action améliore le temps de réponse et augmente le nombre de transactions SSL par seconde qu'un serveur peut prendre en charge. Toutefois, le serveur doit stocker les détails de chaque état de session, ce qui consomme de la mémoire et est difficile à partager entre plusieurs serveurs si les demandes sont équilibrées entre les serveurs.

Les appliances Citrix ADC prennent en charge l'extension SessionTicket TLS. L'utilisation de cette extension indique que les détails de session sont stockés sur le client plutôt que sur le serveur. Le client doit indiquer qu'il prend en charge ce mécanisme en incluant l'extension TLS du ticket de session dans le message Hello client. Pour les nouveaux clients, cette extension est vide. Le serveur envoie un nouveau ticket de session dans le message de poignée de main NewsessionTicket. Le ticket de session est chiffré à l'aide d'une paire de clés connue uniquement du serveur. Si un serveur ne peut pas émettre de nouveau ticket maintenant, il termine une poignée de main normale.

Cette fonctionnalité n'est disponible que dans les profils SSL frontaux et uniquement dans le cadre de la communication dans laquelle l'appliance agit en tant que serveur et génère des tickets de session.

Limitations

- Cette fonctionnalité n'est pas prise en charge sur une plate-forme FIPS.
- Cette fonctionnalité est prise en charge uniquement avec les versions 1.1 et 1.2 de TLS.
- La persistance des ID de session SSL n'est pas prise en charge avec les tickets de session.

Activer l'extension de ticket de session TLS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl profile <name> -sessionTicket (ENABLED | DISABLED ) [-
    sessionTicketLifeTime <positive_integer>
<!--NeedCopy-->
```

Arguments :

SessionTicket : État de l'extension de ticket de session TLS. L'utilisation de cette extension indique que les détails de session sont stockés sur le client plutôt que sur le serveur, tel que défini dans la RFC 5077.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

SessionTicketLifetime : spécifiez une heure, en secondes, après laquelle le ticket de session expire et une nouvelle poignée de main SSL doit être lancée.

Valeur par défaut : 300

Valeur minimale : 0

Valeur maximale : 172800

Exemple :

```
1 add ssl profile profile1 -sessionTicket ENABLED -sessionTicketlifeTime
     300
2 Done
3 <!--NeedCopy-->
```

Activer l'extension de ticket de session TLS à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils**. Sélectionnez **Profils SSL**.
2. Cliquez sur **Ajouter** et spécifiez un nom pour le profil.
3. Sélectionnez le **ticket de session**.
4. Le cas échéant, spécifiez Durée de **vie du ticket de session (secondes)**.

Mise en œuvre sécurisée des tickets de session

En utilisant des tickets de session TLS, les clients peuvent utiliser des poignées de main abrégées pour une reconnexion plus rapide aux serveurs. Toutefois, si les tickets de session ne sont pas chiffrés ou modifiés pendant de longues périodes, ils peuvent poser un risque de sécurité. Vous pouvez sécuriser les tickets de session en les chiffrant avec une clé symétrique. Pour obtenir le secret de transfert, vous pouvez spécifier un intervalle de temps auquel la clé de ticket de session est actualisée.

L'appliance génère les clés de ticket de session par défaut. Toutefois, si plusieurs appliances d'un déploiement doivent déchiffrer les tickets de session de l'autre, elles doivent toutes utiliser la même clé de ticket de session. Par conséquent, vous devez définir (ajouter ou charger) les mêmes données de clé de session manuellement sur toutes les appliances. Les données de la clé de ticket de session comprennent les informations suivantes :

- Nom du ticket de session.
- Clé AES de session utilisée pour chiffrer ou déchiffrer le ticket.
- Clé HMAC de session utilisée pour calculer le résumé du ticket.

Vous pouvez maintenant configurer les données de clé de ticket de session d'une longueur de 64 octets pour prendre en charge les clés HMAC 256 bits, comme recommandé dans la RFC 5077. Des longueurs de clés de 48 octets sont également prises en charge pour une compatibilité descendante.

> **Remarque :**
>
> Lors de la saisie manuelle des données de clé de ticket de session, assurez-vous que la configuration de toutes les appliances Citrix ADC dans une configuration HA ou dans une configuration de cluster est identique.

Le paramètre `sessionTicketKeyLifeTime` spécifie la fréquence à laquelle une clé de ticket de session est actualisée. Vous pouvez définir le paramètre `prevSessionTicketKeyLifeTime` pour spécifier combien de temps la clé de session précédente sera conservée pour le décryptage des tickets à l'aide de cette clé, après la génération d'une nouvelle clé. Le paramètre `prevSessionTicketKeyLifeTime` prolonge la durée pendant laquelle un client peut utiliser une poignée de main abrégée pour se reconnecter. Par exemple, si elle`sessionTicketKeyLifeTime` est définie sur 10 minutes et`prevSessionTicketKeyLifeTime` sur 5 minutes, une nouvelle clé est générée après 10 minutes et utilisée pour toutes les nouvelles sessions. Cependant, les clients précédemment connectés disposent de 5 minutes supplémentaires pour lesquelles les tickets émis précédemment sont honorés pour une poignée de main abrégée.

Configurer les données de ticket de session SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl profile <name> -sessionTicket ENABLED -sessionTicketLifeTime <
    positive_integer> -sessionTicketKeyRefresh ( ENABLED | DISABLED )] -
    sessionTicketKeyLifeTime <positive_integer> [-
    prevSessionTicketKeyLifeTime <positive_integer>]
<!--NeedCopy-->
```

Arguments :

SessionTicket : utilisez les tickets de session comme décrit par RFC 5077. L'établissement de la prise de contact initiale nécessite des opérations de chiffrement à clé publique à forte intensité de processeur. Avec le paramètre **ENABLED**, un serveur émet un ticket de session à un client, que le client peut utiliser pour effectuer une poignée de main abrégée.

Valeurs possibles : ENABLED, DISABLED. Par défaut : DISABLED

SessionTicketLifetime : Durée de vie, en secondes, du ticket de session. Après l'expiration de ce délai, les clients ne peuvent pas utiliser ce ticket pour reprendre leurs sessions.

Valeur maximale : 172800. Valeur minimale : 0. Par défaut : 300.

SessionTicketKeyRefresh : Lorsque le temps spécifié par le paramètre de durée de vie de la clé de session expire, régénérez la clé de session utilisée pour chiffrer ou déchiffrer les tickets de session. Activé automatiquement si SessionTicket est activé. Désactivé si un administrateur saisit les données du ticket de session.

Valeurs possibles : ENABLED, DISABLED. Par défaut : ENABLED

SessionKeyLifetime : Durée de vie, en secondes, d'une clé symétrique utilisée pour chiffrer les tickets de session émis par une appliance Citrix ADC.

Valeur maximale : 86400. Valeur minimale : 600. Par défaut : 3000

PrevSessionKeyLifetime : Durée, en secondes, pendant laquelle la clé symétrique précédente utilisée pour chiffrer les tickets de session reste valide pour les clients existants après l'expiration de la durée de vie de la clé de session. Dans ce délai, les clients existants peuvent reprendre leurs sessions à l'aide de la clé de ticket de session précédente. Les tickets de session pour les nouveaux clients sont cryptés à l'aide de la nouvelle clé.

Valeur maximale : 172800. Valeur minimale : 0. Par défaut : 0

Exemple :

```
set ssl profile ns_default_ssl_profile_frontend -sessionTicket ENABLED
    -sessionTicketlifeTime 120 -sessionTicketKeyRefresh ENABLED -
    sessionTicketKeyLifeTime 100 -prevSessionTicketKeyLifeTime 60

Done

show ssl profile ns_default_ssl_profile_frontend

     Session Ticket: ENABLED
     Session Ticket Lifetime: 120 (secs)
     Session Key Auto Refresh: ENABLED
     Session Key Lifetime: 100 (secs)
     Previous Session Key Lifetime: 60 (secs)
<!--NeedCopy-->
```

Configurer les données de ticket de session SSL à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils**, puis sélectionnez **Profil SSL**.
2. Sélectionnez **ns_default_ssl_profile_frontend** et cliquez sur **Modifier**.
3. Dans la section **Paramètres de base**, cliquez sur l'icône en forme de crayon et définissez les paramètres suivants :
    - Ticket de session

- Durée de vie du ticket de session (secondes)
- Actualisation automatique de la clé de ticket de session
- Durée de vie de la clé de ticket de session (secondes)
- Durée de vie de la clé de ticket de session précédente (secondes)

4. Cliquez sur **OK**.

Tapez manuellement les données de ticket de session SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl profile <name> -sessionTicket ENABLED

set ssl profile <name> -sessionTicketKeyData

show ssl profile ns_default_ssl_profile_frontend
<!--NeedCopy-->
```

Arguments :

SessionTicket : utilisation des tickets de session comme décrit par la RFC 5077. L'établissement de la prise de contact initiale nécessite des opérations de chiffrement à clé publique à forte intensité de processeur. Avec le paramètre **ENABLED**, un serveur émet un ticket de session à un client, que le client peut utiliser pour effectuer une poignée de main abrégée.

Valeurs possibles : ENABLED, DISABLED. Par défaut : DISABLED

SessionTicketKeyData : Contains the session ticket name (0-15 bytes), the session AES key used to encrypt or decrypt the session ticket (16-31 bytes), and the session HMAC key used to compute the digest of the ticket (32-63 bytes). Externally generated by an administrator and added to a Citrix ADC appliance.

Longueur maximale : 64 octets

Exemple :

```
set ssl profile ns_default_ssl_profile_frontend -sessionTicket ENABLED

Done

set ssl profile ns_default_ssl_profile_frontend -sessionTicketKeyData
    1111111111111111111111111111111111111111111111111

Done
```



```
8
9  show ssl profile ns_default_ssl_profile_frontend
10
11     1) Name: ns_default_ssl_profile_frontend (Front-End)
12     SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.1: ENABLED TLSv1.2: ENABLED
13     Client Auth: DISABLED
14     Use only bound CA certificates: DISABLED
15     Strict CA checks: NO
16     Session Reuse: ENABLED Timeout: 120 seconds
17     DH: DISABLED
18     DH Private-Key Exponent Size Limit: DISABLED Ephemeral RSA: ENABLED
           Refresh Count: 0
19     Deny SSL Renegotiation ALL
20     Non FIPS Ciphers: DISABLED
21     Cipher Redirect: DISABLED
22     SSL Redirect: DISABLED
23     Send Close-Notify: YES
24     Push Encryption Trigger: Always
25     PUSH encryption trigger timeout: 1 ms
26     SNI: DISABLED
27     OCSP Stapling: DISABLED
28     Strict Host Header check for SNI enabled SSL sessions: NO
29     Push flag: 0x0 (Auto)
30     SSL quantum size: 8 kB
31     Encryption trigger timeout 100 mS
32     Encryption trigger packet count: 45
33     Subject/Issuer Name Insertion Format: Unicode
34     Session Ticket: ENABLED
35     Session Ticket Lifetime: 300 (secs)
36     Session Key Auto Refresh: DISABLED
37     Session Key Lifetime: 3000 (secs)
38     Previous Session Key Lifetime: 0 (secs)
39     Session Key Data: 84
          dad1afc6d56b0deeb0a7fd7f299a207e8d8c15cdd087a5684a11a329fd732e87a0535d908
40     47
          e8c181ba266f5c8838ae472cb3ab9255b683bf922fad32cee816c329989ef7cdeb278e93a
41
42     ECC Curve: P_256, P_384, P_224, P_521
43
44     1) Cipher Name: DEFAULT Priority :4
45     Description: Predefined Cipher Alias
46
47     1) Internal Service Name (Front-End): nsrnatsip-127.0.0.1-5061
```



```
48      2) Internal Service Name (Front-End): nskrpcs-127.0.0.1-3009
49      3) Internal Service Name (Front-End): nshttps-::1l-443
50      4) Internal Service Name (Front-End): nsrpcs-::1l-3008
51      5) Internal Service Name (Front-End): nshttps-127.0.0.1-443
52      6) Internal Service Name (Front-End): nsrpcs-127.0.0.1-3008
53      7) Vserver Name: v1
54
55  Done
56  <!--NeedCopy-->
```

Tapez manuellement les données de ticket de session SSL à l'aide de l'interface graphique

1. Accédez à **Système > Profils**, puis sélectionnez **Profil SSL**.
2. Sélectionnez **ns_default_ssl_profile_frontend** et cliquez sur **Modifier**.
3. Dans la section **Paramètres de base**, cliquez sur l'icône en forme de crayon et définissez les paramètres suivants :
   - Ticket de session
   - Données de clé de ticket de session
   - Confirmer les données de clé de ticket de session
4. Cliquez sur **OK**.

Prise en charge de Extended Master Secret dans la poignée de main SSL sur les plates-formes Citrix ADC non-FIPS

Remarque : Ce paramètre est introduit dans la version 13.0 build 61.x.

Extended Master Secret (EMS) est une extension facultative du protocole TLS (Transport Layer Security). Un nouveau paramètre s'applique aux profils SSL frontal et back-end pour prendre en charge EMS sur l'appliance Citrix ADC. Si le paramètre est activé et que l'homologue prend en charge EMS, l'appliance ADC utilise le calcul EMS. Si l'homologue ne prend pas en charge EMS, le calcul EMS n'est pas utilisé pour la connexion, même si le paramètre est activé sur l'appliance. Pour plus d'informations sur EMS, reportez-vous à la RFC 7627.

Remarque : EMS s'applique uniquement aux handshakes qui utilisent le protocole TLS version 1.0, 1.1 ou 1.2.

Prise en charge des plateformes EMS

- Plates-formes MPX et SDX contenant soit des puces Cavium N3 soit des cartes crypto Intel Coleto Creek. Les plates-formes suivantes sont livrés avec des puces Intel Coleto :

- MPX 5900
- MPX/SDX 8900
- MPX/SDX 26000
- MPX/SDX 26000-50S
- MPS/SDX 26000-100G
- MPX/SDX 15000-50G

Vous pouvez également utiliser la commande « show hardware » pour déterminer si votre appliance possède des puces Coleto (COL) ou N3.

- Plates-formes MPX et SDX sans carte crypto (logiciel uniquement).
- Plates-formes logicielles uniquement : VPX, CPX et BLX.

EMS ne peut pas être activé sur les plates-formes suivantes :

- MPX 9700 FIPS et MPX 14000 plates-formes FIPS.
- Plateformes MPX et SDX contenant des puces crypto Cavium N2.

Si le paramètre est activé, l'appliance ADC tente d'utiliser EMS dans les connexions TLS 1.2, TLS 1.1 et TLS 1.0. Le paramètre n'affecte pas les connexions TLS 1.3 ou SSLv3.

Pour permettre à EMS d'être négocié avec l'homologue, activez le paramètre sur le profil SSL lié au serveur virtuel (frontal) ou au service (backend).

Activer EMS à l'aide de la CLI

À l'invite de commandes, tapez :

```
set ssl profile <profile name> [-allowExtendedMasterSecret (YES | NO)]
```

Exemples

```
1 set ssl profile ns_default_ssl_profile_frontend  -
     allowExtendedMasterSecret YES
2
3 set ssl profile ns_default_ssl_profile_backend  -
     allowExtendedMasterSecret YES
4 <!--NeedCopy-->
```

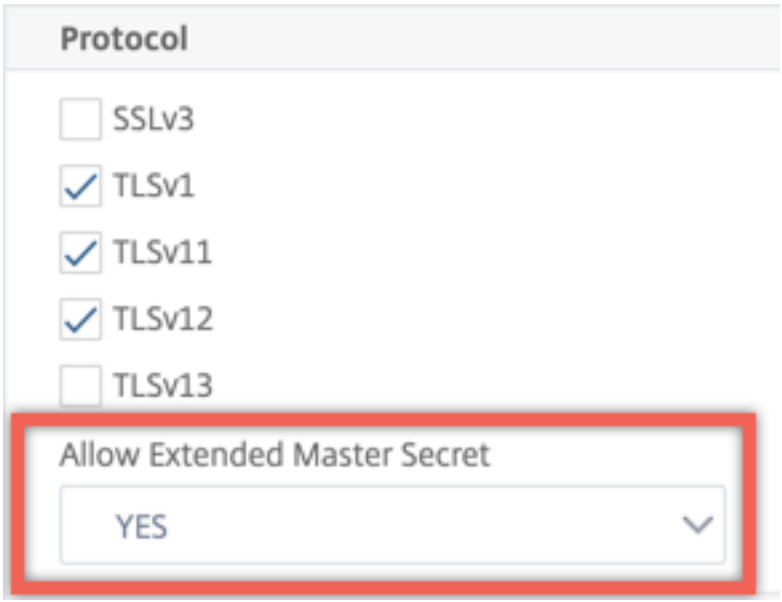
Le tableau suivant présente la valeur par défaut du `allowExtendedMasterSecret` paramètre sur différents profils par défaut et définis par l'utilisateur.

Profile	Paramètre par défaut
Profil frontal par défaut	NON

Profile	Paramètre par défaut
Profil sécurisé frontal par défaut	OUI
Profil back-end par défaut	NON
Profil défini par l'utilisateur	NON

Activer EMS à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profil SSL**.
2. Ajoutez un profil ou modifiez un profil.
3. Définissez **Autoriser le secret maître étendu** sur YES.



Prise en charge du traitement de l'extension ALPN dans le message de bonjour du client

Remarque : Cette fonctionnalité est prise en charge dans la version 13.0 build 61.x et ultérieure.

Un paramètre `alpnProtocol` est ajouté aux profils SSL frontaux pour négocier le protocole d'application dans l'extension ALPN pour les connexions gérées par le serveur virtuel SSL_TCP. Seul le protocole spécifié dans le profil SSL est négocié, si le même protocole est reçu dans l'extension ALPN du message bonjour client.

Remarque : Le `alpnProtocol` paramètre est pris en charge uniquement sur les profils SSL frontaux et est applicable aux connexions SSL gérées par les serveurs virtuels de type SSL_TCP.

Définir le protocole dans le profil SSL frontal à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl profile ns_default_ssl_profile_frontend -alpnProtocol <protocol_name
>
```

Le `alpnProtocol` paramètre peut prendre trois valeurs. Longueur maximale : 4096 octets.

- **AUCUN :** La négociation du protocole d'application n'a pas lieu. il s'agit du réglage par défaut.
- **HTTP1 :** HTTP1 peut être négocié comme protocole d'application.
- **HTTP2 :** HTTP2 peut être négocié en tant que protocole d'application.

Exemple :

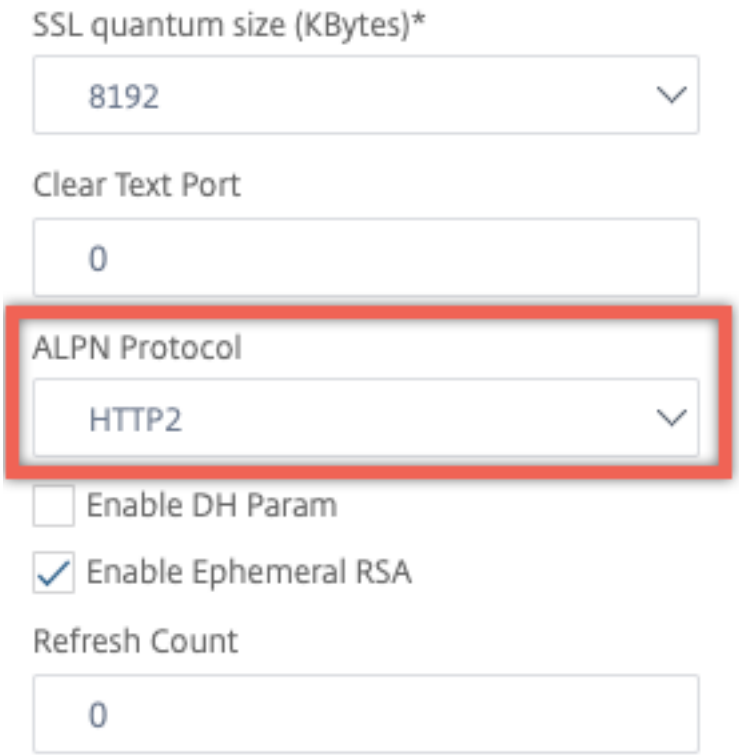
```
set ssl profile ns_default_ssl_profile_frontend -ALPNProtocol HTTP2
> sh ssl profile ns_default_ssl_profile_frontend
1)  Name: ns_default_ssl_profile_frontend   (Front-End)
    SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:   NO
    Session Reuse: ENABLED  Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED  Refresh Count: 0
    Deny SSL Renegotiation  ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:    1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:  NO
    Match HTTP Host header with SNI:    CERT
    Push flag:  0x0 (Auto)
    SSL quantum size:   8 kB
    Encryption trigger timeout  100 mS
    Encryption trigger packet count:    45
    Subject/Issuer Name Insertion Format:   Unicode
```



```
31
32      SSL Interception: DISABLED
33      SSL Interception OCSP Check: ENABLED
34      SSL Interception End to End Renegotiation: ENABLED
35      SSL Interception Maximum Reuse Sessions per Server: 10
36      Session Ticket: DISABLED
37      HSTS: DISABLED
38      HSTS IncludeSubDomains: NO
39      HSTS Max-Age: 0
40      HSTS Preload: NO
41      Allow Extended Master Secret: NO
42      Send ALPN Protocol: HTTP2
43
44   Done
45   <!--NeedCopy-->
```

Définir le protocole dans le profil SSL frontal à l'aide de l'interface graphique

1. Accédez à **Système > Profils**, puis sélectionnez **Profil SSL**.
2. Sélectionnez **ns_default_ssl_profile_frontend** et cliquez sur **Modifier**.
3. Dans la liste **Protocole ALPN**, sélectionnez **HTTP2**.



Charger une ancienne configuration

L'activation des profils par défaut n'est pas réversible. Toutefois, si vous décidez que votre déploiement ne nécessite pas les profils par défaut, vous pouvez charger une configuration plus ancienne que vous avez enregistrée avant d'activer les profils par défaut. Les modifications sont effectives après le redémarrage de l'appliance.

Charger une ancienne configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
shell

root@ns# clear config

root@ns# cd /nsconfig

root@ns# cp ns.conf.NS.11.0.jun.16 ns.conf

root@ns# reboot
<!--NeedCopy-->
```

Profil frontal sécurisé

August 20, 2021

En plus d'un frontal par défaut et d'un profil principal par défaut, un nouveau profil frontal sécurisé par défaut est disponible à partir de la version 12.1. Les paramètres requis pour une note A+ (à partir de mai 2018) de Qualys SSL Labs sont préchargés dans ce profil. Auparavant, vous deviez définir explicitement chacun des paramètres requis pour une évaluation A+ sur un profil frontal SSL ou un serveur virtuel SSL. Vous pouvez maintenant lier le profil ns_default_ssl_profile_secure_frontend à votre serveur virtuel SSL et les paramètres requis sont automatiquement définis sur votre serveur virtuel SSL.

> **Remarque :**
>
> Le profil frontal sécurisé n'est pas modifiable.

Lorsque vous activez le profil par défaut, le profil frontal par défaut est automatiquement lié à tous les serveurs virtuels SSL. Pour obtenir une note A+, vous devez lier explicitement le profil ns_default_ssl_profile_secure_frontend et lier également un certificat de serveur SHA2/SHA256 à votre serveur virtuel SSL.

Paramètres sécurisés du profil frontal

Les paramètres avec leurs paramètres par défaut sont listés ici :

```
SSLv3: DISABLED  TLSv1.0: DISABLED  TLSv1.1: DISABLED  TLSv1.2: ENABLED
      TLSv1.3: DISABLED

Deny SSL Renegotiation: NONSECURE

HSTS: ENABLED

HSTS IncludeSubDomains: YES

HSTS Max-Age: 15552000

Cipher Name: SECURE    Priority :1
<!--NeedCopy-->
```

Secure cipher alias

Un nouvel alias de chiffrement sécurisé est ajouté et lié au profil frontal sécurisé. Pour répertorier les chiffrements qui font partie de cet alias, à l'invite de commandes, tapez : show cipher SECURE

```
show cipher SECURE

    1) Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 1
           Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256)
              Mac=AEAD   HexCode=0xc030
    2) Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 2
           Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128)
              Mac=AEAD   HexCode=0xc02f
    3) Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
       Priority : 3
           Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256)
              Mac=AEAD   HexCode=0xc02c
    4) Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
       Priority : 4
           Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128)
              Mac=AEAD   HexCode=0xc02b
Done
<!--NeedCopy-->
```


Configuration

Procédez comme suit :

1. Ajoutez un serveur virtuel d'équilibrage de charge de type SSL.
2. Liez un certificat SHA2/SHA256.
3. Activez le profil par défaut.
4. Liez le profil frontal sécurisé au serveur virtuel SSL.

Obtenez une note A+ pour un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb vserver <name> <serviceType> <IPAddress> <port>
bind ssl vserver <vServerName> -certkeyName <string>
set ssl parameter -defaultProfile ENABLED
set ssl vserver <vServerName> -sslProfile
   ns_default_ssl_profile_secure_frontend
show ssl vserver [<vServerName>]
<!--NeedCopy-->
```

Exemple :

```
add lb vserver ssl-vsvr SSL 192.0.2.240 443

bind ssl vserver ssl-vsvr -certkeyName letrsa

set ssl parameter -defaultProfile ENABLED

Save your configuration before enabling the Default profile. You cannot
    undo the changes. Are you sure you want to enable the Default
   profile? [Y/N]y

set ssl vserver ssl-vsvr -sslProfile
   ns_default_ssl_profile_secure_frontend
<!--NeedCopy-->
```

```
sh ssl vserver ssl-vsvr

    Advanced SSL configuration for VServer ssl-vsvr:
    Profile Name :ns_default_ssl_profile_secure_frontend
    1) CertKey Name: letrsa     Server Certificate
Done
<!--NeedCopy-->
```



```
sh ssl profile ns_default_ssl_profile_secure_frontend

    1) Name: ns_default_ssl_profile_secure_frontend (Front-End)
    SSLv3: DISABLED  TLSv1.0: DISABLED  TLSv1.1: DISABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:                  NO
    Session Reuse: ENABLED   Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED     Refresh Count: 0
    Deny SSL Renegotiation                NONSECURE
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:  1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:
                           NO
    Push flag:              0x0 (Auto)
    SSL quantum size:                8 kB
    Encryption trigger timeout       100 mS
    Encryption trigger packet count: 45
    Subject/Issuer Name Insertion Format:  Unicode
    SSL Interception: DISABLED
    SSL Interception OCSP Check: ENABLED
    SSL Interception End to End Renegotiation: ENABLED
    SSL Interception Maximum Reuse Sessions per Server:   10
    Session Ticket: DISABLED
    HSTS: ENABLED
    HSTS IncludeSubDomains: YES
    HSTS Max-Age: 15552000
    ECC Curve: P_256, P_384, P_224, P_521
    1) Cipher Name: SECURE    Priority :1
    Description: Predefined Cipher Alias
    1) Vserver Name: v2
```



```
42 Done
43 <!--NeedCopy-->
```

Obtenez une note A+ pour un serveur virtuel SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis sélectionnez un serveur virtuel SSL.
2. Dans Paramètres avancés, cliquez sur Profil SSL.
3. Sélectionnez ns_default_ssl_profile_secure_frontend.
4. Cliquez sur OK.
5. Cliquez sur Terminé.

Annexe A : exemple de migration de la configuration SSL après la mise à niveau

January 21, 2021

Remarque : Ce contenu a été supprimé car le script de migration SSL pour le nouveau profil par défaut n'est plus pris en charge.

Annexe B : paramètres de profil SSL front-end et back-end par défaut

January 21, 2021

Un profil frontal par défaut possède les paramètres suivants :

```
1  sh ssl profile ns_default_ssl_profile_frontend
2
3  1)Name: ns_default_ssl_profile_frontend
4
5       Configuration for Front-End SSL profile
6       DH: DISABLED
7       Ephemeral RSA: ENABLED          Refresh Count: 0
8       Session Reuse: ENABLED          Timeout: 120 seconds
9       Non FIPS Ciphers: DISABLED
10      Cipher Redirect: ENABLED   Redirect URL: http://10.102.28.212/
            redirect.html
11      Client Auth: DISABLED
12      SSL Redirect: DISABLED
```



```
13       SNI: DISABLED
14       SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
             ENABLED
15       Push Encryption Trigger: Always
16       PUSH encryption trigger timeout:     1 ms
17       Send Close-Notify: YES
18       Push flag: 0x0 (Auto)
19       Deny SSL Renegotiation          NO
20       SSL quantum size:          8 kB
21       Strict CA checks:          NO
22       Encryption trigger timeout 100 mS
23       Encryption trigger packet count:     45
24       Use only bound CA certificates: DISABLED
25       Subject/Issuer Name Insertion Format: Unicode
26       Strict Host Header check for SNI enabled SSL sessions:          NO
27
28       ECC Curve: P_256, P_384, P_521
29
30  1)   Cipher Name: AES     Priority :2
31       Description: Predefined Cipher Alias
32
33  1)   Vserver Name: v1
34  2)   Vserver Name: nshttps-::1l-443
35  3)   Vserver Name: nsrpcs-::1l-3008
36  4)   Vserver Name: nskrpcs-127.0.0.1-3009
37  5)   Vserver Name: nshttps-127.0.0.1-443
38  6)   Vserver Name: nsrpcs-127.0.0.1-3008
39  Done
40  <!--NeedCopy-->
```

Un profil principal par défaut possède les paramètres suivants :

```
1  sh ssl profile ns_default_ssl_profile_backend
2
3  1)Name: ns_default_ssl_profile_backend
4
5       Configuration for Back-End SSL profile
6       Session Reuse: ENABLED          Timeout: 300 seconds
7       Non FIPS Ciphers: DISABLED
8       Server Auth: DISABLED
9       SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: DISABLED  TLSv1.2:
            DISABLED
10      Push Encryption Trigger: Always
11      PUSH encryption trigger timeout:     1 ms
12      Send Close-Notify: YES
```



```
13      Push flag: 0x0 (Auto)
14      Deny SSL Renegotiation          ALL
15      SSL quantum size:          8 kB
16      Strict CA checks:          NO
17      Encryption trigger timeout 100 mS
18      Encryption trigger packet count:     45
19      Use only bound CA certificates: DISABLED
20
21      ECC Curve: P_256, P_224, P_521
22
23  1)  Cipher Name: AES     Priority :1
24      Description: Predefined Cipher Alias
25
26  2)  Cipher Name: RC4     Priority :2
27      Description: Predefined Cipher Alias
28
29  1)  Service Name: s2
30  2)  Service Name: s1
31  Done
32  <!--NeedCopy-->
```

Profil SSL hérité

August 20, 2021

> **Remarque :**
>
> Citrix recommande d'utiliser les profils améliorés au lieu des profils hérités. Pour plus d'informations sur l'infrastructure de profils améliorée, voir Infrastructure de profils SSL.

Important :

> Liez un profil SSL à un serveur virtuel SSL. Ne liez pas un profil DTLS à un serveur virtuel SSL. Pour plus d'informations sur les profils DTLS, consultez Profils DTLS.

Vous pouvez utiliser un profil SSL pour spécifier comment un Citrix ADC traite le trafic SSL. Le profil est un ensemble de paramètres SSL pour les entités SSL, telles que les serveurs virtuels, les services et les groupes de services, et offre une configuration facile et une flexibilité. Vous n'êtes pas limité à la configuration d'un seul ensemble de paramètres globaux. Vous pouvez créer plusieurs ensembles (profils) de paramètres globaux et affecter différents ensembles à différentes entités SSL. Les profils SSL sont classés en deux catégories :

- Profils frontaux, contenant les paramètres applicables à l'entité frontale. Autrement dit, ils

s'appliquent à l'entité qui reçoit des demandes d'un client.
- Profils principaux contenant les paramètres applicables à l'entité principale. Autrement dit, ils s'appliquent à l'entité qui envoie des demandes client à un serveur.

Contrairement à un profil TCP ou HTTP, un profil SSL est facultatif. Par conséquent, il n'y a pas de profil SSL par défaut. Le même profil peut être réutilisé sur plusieurs entités. Si aucun profil n'est attaché à une entité, les valeurs définies au niveau global s'appliquent. Pour les services apprises de manière dynamique, les valeurs globales actuelles s'appliquent.

Le tableau suivant répertorie les paramètres qui font partie de chaque profil.

Profil d'extrémité avant	Profil back-end
cipherRedirect, cipherURL	denySSLReneg
clearTextPort*	encryptTriggerPktCount
clientAuth, clientCert	nonFipsCiphers
denySSLReneg	pushEncTrigger
dh, dhFile, dhCount	pushEncTriggerTimeout
dropReqWithNoHostHeader	pushFlag
encryptTriggerPktCount	quantumSize
eRSA, eRSACount	serverAuth
insertionEncoding	commonName
nonFipsCiphers	sessReuse, sessTimeout
pushEncTrigger	`SNIEnable`
pushEncTriggerTimeout	ssl3
pushFlag	sslTriggerTimeout
quantumSize	strictCAChecks
redirectPortRewrite	tls1
sendCloseNotify	-
sessReuse, sessTimeout	-
`SNIEnable`	-
ssl3	-
sslRedirect	-
sslTriggerTimeout	-
strictCAChecks	-

Profil d'extrémité avant	Profil back-end
tls1, tls11, tls12	-

* Le paramètre ClearTextPort s'applique uniquement à un serveur virtuel SSL.

Un message d'erreur s'affiche si vous essayez de définir un paramètre qui ne fait pas partie du profil. Par exemple, si vous essayez de définir le paramètre ClientAuth dans un profil back-end.

Certains paramètres SSL, tels que la taille de la mémoire CRL, la taille du cache OCSP, le contrôle UnDefaction Control et UnDefaction Data, ne font partie d'aucun des profils précédents, car ces paramètres sont indépendants des entités.

Un profil SSL prend en charge les opérations suivantes :

- Add : crée un profil SSL sur Citrix ADC. Spécifiez si le profil est frontal ou principal. Front end est la valeur par défaut.
- Set : modifie les paramètres d'un profil existant.
- Unset : définit les paramètres spécifiés sur leurs valeurs par défaut. Si vous ne spécifiez aucun paramètre, un message d'erreur s'affiche. Si vous désactivez un profil sur une entité, le profil est indépendant de l'entité.
- Remove : supprime un profil. Un profil utilisé par une entité ne peut pas être supprimé. La suppression de la configuration supprime toutes les entités. Par conséquent, les profils sont également supprimés.
- Afficher : affiche tous les profils disponibles sur Citrix ADC. Si un nom de profil est spécifié, les détails de ce profil sont affichés. Si une entité est spécifiée, les profils associés à cette entité sont affichés.

Créer un profil SSL à l'aide de l'interface de ligne de commande

- Pour ajouter un profil SSL, tapez :

```
add ssl profile <name> [-sslProfileType ( BackEnd | FrontEnd )]
<!--NeedCopy-->
```

- Pour modifier un profil existant, tapez :

```
set ssl profile <name>
<!--NeedCopy-->
```

- Pour annuler la définition d'un profil existant, tapez :

```
unset ssl profile <name> [-dh] [-dhFile] [-dhCount] [-eRSA] ...
<!--NeedCopy-->
```


- Pour annuler la définition d'un profil existant d'une entité, tapez :

```
unset ssl vserver <vServerName>  - sslProfile
<!--NeedCopy-->
```

- Pour supprimer un profil existant, tapez :

```
rm ssl profile <name>
<!--NeedCopy-->
```

- Pour afficher un profil existant, tapez :

```
sh ssl profile <name>
<!--NeedCopy-->
```

Créer un profil SSL à l'aide de l'interface graphique

Accédez à **Système** > **Profils**, sélectionnez l'onglet Profils SSL et créez un profil SSL.

Activer un contrôle plus strict sur la validation du certificat client

L'appliance Citrix ADC accepte les certificats d'autorité de certification intermédiaire valides si une seule autorité de certification Root-CA les a délivrés. C'est-à-dire que si seul le certificat Root-CA est lié au serveur virtuel et que Root-CA valide l'un des certificats intermédiaires envoyés avec le certificat client, l'appliance approuve la chaîne de certificats et la connexion réussit.

Toutefois, si un client envoie une chaîne de certificats dans la connexion, les certificats intermédiaires peuvent être validés à l'aide d'un répondeur CRL ou OCSP uniquement si ce certificat est lié au serveur virtuel SSL. Par conséquent, même si l'un des certificats intermédiaires est révoqué, la négociation est réussie. Dans le cadre de la poignée de main, le serveur virtuel SSL envoie la liste des certificats d'autorité de certification qui lui sont liés. Pour un contrôle plus strict, vous pouvez configurer le serveur virtuel SSL pour qu'il accepte uniquement un certificat signé par l'un des certificats d'autorité de certification liés à ce serveur virtuel. Pour ce faire, vous devez activer le paramètre `ClientAuthUseBoundCAChain` dans le profil SSL lié au serveur virtuel. La connexion échoue si l'un des certificats d'autorité de certification liés au serveur virtuel n'a pas signé le certificat client.

Par exemple, deux certificats clients, clientcert1 et clientcert2, sont signés respectivement par les certificats intermédiaires Int-CA-A et Int-CA-B. Les certificats intermédiaires sont signés par le certificat racine Root-CA. Int-CA-A et Root-CA sont liés au serveur virtuel SSL. Dans le cas par défaut (ClientAuthUseBoundCAChain désactivé), clientcert1 et clientcert2 sont acceptés. Toutefois, si ClientAuthUseBoundCachain est activé, l'appliance Citrix ADC accepte uniquement clientcert1.

Activer un contrôle plus strict sur la validation des certificats client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez : `set ssl profile <name> -ClientAuthUseBoundCAChain Enabled`

Activer un contrôle plus strict sur la validation du certificat client à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils**, sélectionnez l'onglet **Profils SSL** et créez un profil SSL ou sélectionnez un profil existant.
2. Sélectionnez **Activer l'authentification client à l'aide de la chaîne de certification liée**.

Listes de révocation de certificats

August 20, 2021

Un certificat émis par une autorité de certification reste généralement valide jusqu'à sa date d'expiration. Toutefois, dans certaines circonstances, l'AC peut révoquer le certificat délivré avant la date d'expiration. Par exemple, lorsque la clé privée d'un propriétaire est compromise, le nom d'une société ou d'un particulier change, ou l'association entre le sujet et l'autorité de certification change.

Une liste de révocation de certificats (CRL) identifie les certificats non valides par numéro de série et émetteur.

Les autorités de certification délivrent régulièrement des CRL. Vous pouvez configurer l'appliance Citrix ADC pour qu'elle utilise une liste de révocation de certificats pour bloquer les demandes client qui présentent des certificats non valides.

Si vous disposez déjà d'un fichier CRL provenant d'une autorité de certification, ajoutez-le à l'appliance Citrix ADC. Vous pouvez configurer les options d'actualisation. Vous pouvez également configurer Citrix ADC pour qu'il synchronise automatiquement le fichier CRL à un intervalle spécifié, à partir d'un emplacement Web ou d'un emplacement LDAP. L'appliance prend en charge les listes de révocation des droits de révocation au format PEM ou DER. Veillez à spécifier le format de fichier du fichier CRL ajouté à l'appliance Citrix ADC.

Si vous avez utilisé ADC en tant qu'autorité de certification pour créer des certificats utilisés dans les déploiements SSL, vous pouvez également créer une liste de révocation de certificats pour révoquer un certificat particulier. Cette fonctionnalité peut être utilisée, par exemple, pour s'assurer que les certificats auto-signés créés sur Citrix ADC ne sont pas utilisés dans un environnement de production ou au-delà d'une date particulière.

Remarque :

Par défaut, les listes de révocation de révocation des droits de révocation sont stockées dans le répertoire /var/netscaler/ssl de l'appliance Citrix ADC.

Créer une liste de rérérequis sur l'appliance ADC

Étant donné que vous pouvez utiliser l'appliance ADC pour agir en tant qu'autorité de certification et créer des certificats auto-signés, vous pouvez également révoquer les certificats suivants :

- Certificats que vous avez créés.
- Certificats dont vous possédez le certificat CA.

L'appliance doit révoquer les certificats non valides avant de créer une liste de révocation de certificats pour ces certificats. L'appliance stocke les numéros de série des certificats révoqués dans un fichier d'index et met à jour le fichier chaque fois qu'elle révoque un certificat. Le fichier d'index est automatiquement créé la première fois qu'un certificat est révoqué.

Révoquer un certificat ou créer une liste de révocation de certificats à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
create ssl crl <CAcertFile> <CAkeyFile> <indexFile> (-revoke <
    input_filename> | -genCRL <output_filename>)
<!--NeedCopy-->
```

Exemple :

```
create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -revoke Invalid-1

create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -genCRL CRL-1
<!--NeedCopy-->
```

Révoquer un certificat ou créer une liste de révocation de certificats à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL** et, dans le groupe Mise en route, sélectionnez Gestion des CRL.
2. Entrez les détails du certificat et, dans la liste **Choisir une opération**, sélectionnez **Révoquer le certificat**ou **Générer une liste de révocation de certificats**.

Ajouter une liste de révocation de révocation existante à ADC

Avant de configurer la liste de révocation des droits de révocation sur l'appliance Citrix ADC, assurez-vous que le fichier de révocation de révocation des droits de révocation est stocké localement sur l'appliance Citrix ADC. Dans une configuration HA, le fichier CRL doit être présent sur les deux appliances ADC, et le chemin d'accès au répertoire du fichier doit être le même sur les deux appliances.

Ajouter une liste de révocation de révocation de révocation sur Citrix ADC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter une liste de révocation de révocation de révocation sur Citrix ADC et vérifiez la configuration :

```
add ssl crl <crlName> <crlPath> [-inform (DER | PEM)]

show ssl crl [<crlName>]
<!--NeedCopy-->
```

Exemple :

```
> add ssl crl crl-one /var/netscaler/ssl/CRL-one -inform PEM

Done

> show ssl crl crl-one

            Name: crl-one   Status: Valid,  Days to expiration: 29
            CRL Path: /var/netscaler/ssl/CRL-one
            Format: PEM     CAcert: samplecertkey
            Refresh: DISABLED
            Version: 1
            Signature Algorithm: sha1WithRSAEncryption
            Issuer:  C=US,ST=California,L=Santa Clara,O=NetScaler Inc.,
               OU=SSL Acceleration,CN=www.ns.com/emailAddress=
               support@Citrix ADC appliance.com
            Last_update:Jun 15 10:53:53 2010 GMT
            Next_update:Jul 15 10:53:53 2010 GMT

    1)      Serial Number: 00
            Revocation Date:Jun 15 10:51:16 2010 GMT
     Done
<!--NeedCopy-->
```


Ajouter une liste de révocation de révocation de révocation sur le Citrix ADC à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **SSL** > **CRL**, puis ajoutez une CRL.

Configurer les paramètres d'actualisation de la liste de révocation des droits de révocation

Une CRL est générée et publiée par une autorité de certification périodiquement ou, parfois, immédiatement après la révocation d'un certificat particulier. Citrix vous recommande de mettre régulièrement à jour les listes de révocation de certificats sur l'appliance Citrix ADC afin de vous protéger contre les clients qui tentent de se connecter à des certificats non valides.

L'appliance Citrix ADC peut actualiser les listes de révocation des droits de révocation à partir d'un emplacement Web ou d'un répertoire LDAP. Lorsque vous spécifiez des paramètres d'actualisation et un emplacement Web ou un serveur LDAP, la CRL n'a pas besoin d'être présente sur le disque dur local au moment de l'exécution de la commande. La première actualisation stocke une copie sur le disque dur local, dans le chemin spécifié par le paramètre Fichier CRL. Le chemin d'accès par défaut pour stocker la liste de révocation des droits de révocation est /var/netscaler/ssl.

Remarque : Dans les versions 10.0 et ultérieures, la méthode d'actualisation d'une liste de révocation de révocation de révocation n'est pas incluse par défaut. Spécifiez une méthode HTTP ou LDAP. Si vous effectuez une mise à niveau à partir d'une version antérieure vers la version 10.0 ou ultérieure, vous devez ajouter une méthode et exécuter à nouveau la commande.

Configurer l'actualisation automatique des CRL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer l'actualisation automatique de la CRL et vérifier la configuration :

```
set ssl crl <crlName> [-refresh ( ENABLED | DISABLED )] [-CAcert <
    string>] [-server <ip_addr|ipv6_addr|*> | -url <URL>] [-method (
    HTTP | LDAP )] [-port <port>] [-baseDN <string>] [-scope ( Base |
    One )] [-interval <interval>] [-day <positive_integer>] [-time <HH:
    MM>][-bindDN <string>] {
 -password  }
  [-binary ( YES | NO )]

show ssl crl [<crlName>]
<!--NeedCopy-->
```

Exemple :


```
1     set CRL crl1  -refresh enabled -method ldap -inform DER -CAcert ca1
          -server 10.102.192.192 -port 389 -scope base -baseDN "cn=
         clnt_rsa4_multicert_der,ou=eng,o=ns,c=in" -time 00:01
2
3     set ssl crl crl1 -refresh enabled -method http -cacert ca1 -port 80
          -time 00:10 -url http://10.102.192.192/crl/ca1.crl
4
5
6     > sh crl
7
8     1)         Name: crl1        Status: Valid,     Days to expiration:
          355
9                  CRL Path: /var/netscaler/ssl/crl1
10                 Format: PEM      CAcert: ca1
11                 Refresh: ENABLED          Method: HTTP
12                 URL: http://10.102.192.192/crl/ca1.crl
                      Port:80
13                 Refresh Time: 00:10
14                 Last Update: Successful, Date:Tue Jul  6 14:38:13 2010
15    Done
16 <!--NeedCopy-->
```

Configurer l'actualisation automatique des CRL à l'aide de LDAP ou HTTP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > CRL**.
2. Ouvrez une liste de révocation de révocation de révocation de révocation **de révocation de révocation de révocation de révocation**.

> **Remarque**
>
> Si la nouvelle CRL a été actualisée dans le référentiel externe avant son heure de mise à jour réelle, tel que spécifié par le champ **Heure de dernière mise à jour** de la liste de rétention, vous devez effectuer les opérations suivantes : Actualisez
>
> immédiatement la CRL sur le dispositif Citrix ADC.

Pour afficher l'heure de la dernière mise à jour, sélectionnez la liste de révocation des droits de révocation, puis cliquez sur **Détails**.

Synchroniser les listes de révocation

L'appliance Citrix ADC utilise la liste de révocation de certificats distribuée la plus récente pour empêcher les clients ayant des certificats révoqués d'accéder à des ressources sécurisées.

Si les listes de révocation de révocation de révocation de révocation Citrix ADC révocation de révocation de révocation de révocation de révocation de révocation de révocation de révocation de révocation de révocation de ré Vous pouvez configurer l'appliance pour qu'elle mette à jour automatiquement les listes de régénération à un intervalle d'actualisation spécifié.

L'appliance tient à jour une liste interne des listes de révocation des droits de révocation qui doivent être mises à jour à intervalles réguliers. À ces intervalles spécifiés, l'appliance analyse la liste des listes de révocation de révocation qui doivent être mises à jour. Il se connecte ensuite au serveur LDAP distant ou au serveur HTTP, récupère les LCR les plus récentes, puis met à jour la liste des listes de CRL locale avec les nouvelles LCR.

> **Remarque :**
>
> Si la vérification de la liste de révocation de certificats est définie sur obligatoire lorsque le certificat de l'autorité de certification est lié au serveur virtuel et que l'actualisation initiale échoue, l'action suivante est entreprise pour les connexions :
>
> Toutes les connexions d'authentification client avec le même émetteur que la liste de révocation de certificats sont rejetées comme REVOKED jusqu'à ce que la liste de révocation de certificats est actualisé avec succès.

Vous pouvez spécifier l'intervalle auquel l'actualisation de la liste de révocation de révocation doit être effectuée. Vous pouvez également spécifier l'heure exacte.

Synchroniser l'actualisation automatique de CRL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
1 set ssl crl <crlName> [-interval <interval>] [-day <integer>] [-time <
     HH:MM>]
2 <!--NeedCopy-->
```

Exemple :

```
1 set ssl crl CRL-1 -refresh ENABLE -interval MONTHLY -days 10 -time
     12:00
2 <!--NeedCopy-->
```

Synchroniser l'actualisation des listes de révocation des droits de révocation à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > CRL**.
2. Ouvrez une liste de révocation de révocation de révocation **de révocation de révocation de révocation de révocation**de révocation de révocation de révocation de

Effectuer l'authentification du client à l'aide d'une liste de révocation de certificats

Si une liste de révocation de certificats est présente sur une appliance Citrix ADC, une vérification de révocation de certificats est effectuée, que la vérification de révocation de certificats soit définie sur obligatoire ou facultative.

Le succès ou l'échec d'une poignée de main dépend d'une combinaison des facteurs suivants :

- Règle pour la vérification des CRL
- Règle de vérification du certificat client
- État de la liste de révocation de certificats configurée pour le certificat de l'autorité de certification

Le tableau suivant répertorie les résultats des combinaisons possibles pour une poignée de main impliquant un certificat révoqué.

Tableau 1. Résultat d'une poignée de main avec un client à l'aide d'un certificat révoqué

Règle pour la vérification des CRL	Règle de vérification du certificat client	État de la liste de révocation de certificats configurée pour le certificat de l'autorité de certification	Résultat d'une poignée de main avec un certificat révoqué
Facultatif	Facultatif	Manquant	Succès
Facultatif	Obligatoire	Manquant	Succès
Facultatif	Obligatoire	Présent	Échec
Obligatoire	Facultatif	Manquant	Succès
Obligatoire	Obligatoire	Manquant	Échec
Obligatoire	Facultatif	Présent	Succès
Obligatoire	Obligatoire	Présent	Échec
Optionnel/Obligatoire	Facultatif	Expiré	Succès
Optionnel/Obligatoire	Obligatoire	Expiré	Échec

> **Remarque :**
>
> - La vérification des CRL est facultative par défaut. Pour passer de facultatif à obligatoire ou inversement, vous devez d'abord délier le certificat du serveur virtuel SSL, puis le lier à nouveau après avoir modifié l'option.

> - Dans la sortie de la commande `sh ssl vserver`, OCSP check : optional implique qu'une vérification CRL est également facultative. Les paramètres de vérification des CRL sont affichés dans la sortie de la `sh ssl vserver` commande uniquement si la vérification CRL est définie sur obligatoire. Si la vérification des CRL est définie sur facultative, les détails de la vérification des LCR n'apparaissent pas.

Pour configurer la vérification des CRL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
bind ssl vserver <vServerName> -certkeyName <string> [(-CA -crlCheck (
    Mandatory | Optional ))]
sh ssl vserver
<!--NeedCopy-->
```

Exemple :

```
bind ssl vs v1 -certkeyName ca -CA -crlCheck mandatory
> sh ssl vs v1

Advanced SSL configuration for VServer v1:

DH: DISABLED
DH Private-Key Exponent Size Limit: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: ENABLED Client Cert Required: Mandatory
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
HSTS Max-Age: 0
SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.1: ENABLED TLSv1
    .2: ENABLED
Push Encryption Trigger: Always
Send Close-Notify: YES

ECC Curve: P_256, P_384, P_224, P_521

```



```
1) CertKey Name: ca CA Certificate CRLCheck: Mandatory CA_Name Sent

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Configurer la vérification des CRL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel SSL.
2. Cliquez dans la section **Certificats**.
3. Sélectionnez un certificat et, dans la liste **OCSP et CRL Check**, sélectionnez **CRL Obligatoire**.

Résultat d'une poignée de main avec un certificat révoqué ou valide

Règle pour la vérification des CRL	Règle de vérification du certificat client	État de la liste de révocation de certificats configurée pour le certificat de l'autorité de certification	Résultat d'une poignée de main avec un certificat révoqué	Résultat d'une poignée de main avec un certificat valide
Obligatoire	Obligatoire	Présent	Échec	Succès
Obligatoire	Obligatoire	Expiré	Échec	Échec
Obligatoire	Obligatoire	Manquant	Échec	Échec
Obligatoire	Obligatoire	Indéfini	Échec	Échec
Facultatif	Obligatoire	Présent	Échec	Succès
Facultatif	Obligatoire	Expiré	Succès	Succès
Facultatif	Obligatoire	Manquant	Succès	Succès
Facultatif	Obligatoire	Indéfini	Succès	Succès
Obligatoire	Facultatif	Présent	Succès	Succès
Obligatoire	Facultatif	Expiré	Succès	Succès
Obligatoire	Facultatif	Manquant	Succès	Succès
Obligatoire	Facultatif	Indéfini	Succès	Succès

Règle pour la vérification des CRL	Règle de vérification du certificat client	État de la liste de révocation de certificats configurée pour le certificat de l'autorité de certification	Résultat d'une poignée de main avec un certificat révoqué	Résultat d'une poignée de main avec un certificat valide
Facultatif	Facultatif	Présent	Succès	Succès
Facultatif	Facultatif	Expiré	Succès	Succès
Facultatif	Facultatif	Manquant	Succès	Succès
Facultatif	Facultatif	Indéfini	Succès	Succès

Surveiller l'état du certificat avec OCSP

August 20, 2021

Le protocole OCSP (Online Certificate Status Protocol) est un protocole Internet qui est utilisé pour déterminer l'état d'un certificat SSL client. Les appliances Citrix ADC prennent en charge OCSP tel que défini dans la RFC 2560. L'OCSP offre des avantages importants par rapport aux listes de révocation de certificats (CRL) en termes d'information opportune. Le statut actuel de révocation d'un certificat de client est particulièrement utile dans les transactions impliquant des sommes importantes et des opérations boursières de grande valeur. Il utilise également moins de ressources système et réseau. L'implémentation Citrix ADC d'OCSP inclut le traitement par lots de requêtes et la mise en cache des réponses.

Mise en œuvre de l'OCSP

La validation OCSP sur une appliance Citrix ADC commence lorsque celle-ci reçoit un certificat client lors d'une liaison SSL. Pour valider le certificat, l'appliance crée une demande OCSP et la transmet au répondeur OCSP. Pour ce faire, l'appliance utilise une URL configurée localement. La transaction est suspendue jusqu'à ce que l'appliance évalue la réponse du serveur et détermine s'il faut autoriser la transaction ou la rejeter. Si la réponse du serveur est retardée au-delà de l'heure configurée et qu'aucun autre répondeur n'est configuré, l'appliance autorise la transaction ou affiche une erreur, selon que la vérification OCSP a été définie sur facultative ou obligatoire, respectivement.

L'appliance prend en charge le traitement par lots de requêtes OCSP et la mise en cache des réponses OCSP afin de réduire la charge sur le répondeur OCSP et de fournir des réponses plus rapides.

Lots de demandes OCSP

Chaque fois que l'appliance reçoit un certificat client, elle envoie une demande au répondeur OCSP. Pour éviter de surcharger le répondeur OCSP, l'appliance peut interroger l'état de plusieurs certificats client dans la même demande. Pour que cette fonctionnalité fonctionne efficacement, un délai d'attente doit être défini afin que le traitement d'un seul certificat ne soit pas excessivement retardé en attendant de former un lot.

Mise en cache des réponses OCSP

La mise en cache des réponses reçues du répondeur OCSP permet des réponses plus rapides aux clients et réduit la charge sur le répondeur OCSP. Dès réception de l'état de révocation d'un certificat client du répondeur OCSP, l'appliance met en cache la réponse localement pendant une durée prédéfinie. Lorsqu'un certificat client est reçu lors d'une connexion SSL, l'appliance vérifie d'abord dans son cache local une entrée pour ce certificat. Si une entrée est trouvée qui est toujours valide (dans la limite du délai d'expiration du cache), elle est évaluée et le certificat client est accepté ou rejeté. Si aucun certificat n'est trouvé, l'appliance envoie une demande au répondeur OCSP et stocke la réponse dans son cache local pendant une durée configurée.

> **Remarque** : à partir de la version 12.1 build 49.x, la limite de délai d'expiration du cache est désormais augmentée à un maximum de 43200 minutes (30 jours). Auparavant, la limite était de 1440 minutes (un jour). La limite accrue permet de réduire les recherches sur le serveur OCSP et d'éviter les échecs de connexion SSL/TLS au cas où le serveur OCSP n'est pas accessible en raison de problèmes de réseau ou d'autres.

Configuration du répondeur OCSP

La configuration d'OCSP implique l'ajout d'un répondeur OCSP, la liaison du répondeur OCSP à un certificat d'autorité de certification (CA) et la liaison du certificat à un serveur virtuel SSL. Si vous devez lier un certificat différent à un répondeur OCSP déjà configuré, vous devez d'abord dissocier le répondeur, puis lier le répondeur à un autre certificat.

Ajouter un répondeur OCSP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer OCSP et vérifier la configuration :

```
add ssl ocspResponder <name> -url <URL> [-cache ( ENABLED | DISABLED )
    [-cacheTimeout <positive_integer>]] [ -batchingDepth <
    positive_integer>][-batchingDelay <positive_integer>] [-resptimeout
    <positive_integer>] [-responderCert <string> | -trustResponder] [-
```



```
    producedAtTimeSkew <positive_integer>][-signingCert <string>][-
    useNonce ( YES | NO )][ -insertClientCert( YES | NO )]
<!--NeedCopy-->
```

```
bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]
<!--NeedCopy-->
```

```
bind ssl vserver <vServerName>@ (-certkeyName <string> ( CA [-ocspCheck
     ( Mandatory | Optional )]))
<!--NeedCopy-->
```

```
show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Exemple :

```
add ssl ocspResponder ocsp_responder1 -url "http:// www.myCA.org:80/
    ocsp/" -cache ENABLED -cacheTimeout 30 -batchingDepth 8 -
    batchingDelay 100 -resptimeout 100 -responderCert responder_cert -
    producedAtTimeSkew 300 -signingCert sign_cert  -insertClientCert YES
<!--NeedCopy-->
```

```
bind ssl certKey ca_cert -ocspResponder ocsp_responder1 -priority 1
<!--NeedCopy-->
```

```
bind ssl vserver vs1 -certkeyName ca_cert -CA -ocspCheck Mandatory
<!--NeedCopy-->
```

```
sh ocspResponder ocsp_responder1

    1)Name: ocsp_responder1
    URL: http://www.myCA.org:80/ocsp/, IP: 192.128.22.22
    Caching: Enabled        Timeout: 30 minutes
    Batching: 8 Timeout: 100 mS
    HTTP Request Timeout: 100mS
    Request Signing Certificate: sign_cert
    Response Verification: Full, Certificate: responder_cert
    ProducedAt Time Skew: 300 s
    Nonce Extension: Enabled
     Client Cert Insertion: Enabled
    Done
<!--NeedCopy-->
```



```
show certkey ca_cert

    Name: ca_cert     Status: Valid,   Days to expiration:8907
    Version: 3
    …

    1)  VServer name: vs1      CA Certificate
    1)  OCSP Responder name: ocsp_responder1     Priority: 1
Done
<!--NeedCopy-->
```

```
sh ssl vs vs1

    Advanced SSL configuration for VServer vs1:
    DH: DISABLED
    …

    1) CertKey Name: ca_cert CA Certificate OCSPCheck: Mandatory
    1) Cipher Name: DEFAULT
      Description: Predefined Cipher Alias
    Done
<!--NeedCopy-->
```

Modifier un répondeur OCSP à l'aide de l'interface de ligne de commande

Vous ne pouvez pas modifier le nom du répondeur. Tous les autres paramètres peuvent être modifiés à l'aide de la `set ssl ocspResponder` commande.

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
set ssl ocspResponder <name> [-url <URL>] [-cache ( ENABLED | DISABLED)
    ] [-cacheTimeout <positive_integer>] [-batchingDepth <
    positive_integer>] [-batchingDelay <positive_integer>] [-resptimeout
     <positive_integer>] [ -responderCert <string> | -trustResponder][-
    producedAtTimeSkew <positive_integer>][-signingCert <string>] [-
    useNonce ( YES | NO )]

unbind ssl certKey [<certkeyName>] [-ocspResponder <string>]

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]

```



```
show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Configurer un répondeur OCSP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Répondeur OCSP** et configurez un répondeur OCSP.
2. Accédez à **Gestion du trafic** > **SSL** > **Certificats**, sélectionnez un certificat et, dans la liste **Action**, sélectionnez **Liaisons OCSP**. Liez un répondeur OCSP.
3. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, ouvrez un serveur virtuel et cliquez dans la section Certificats pour lier un certificat d'autorité de certification.
4. Le cas échéant, **sélectionnez OCSP Obligatoire**.

Association d'OCSP

August 20, 2021

L'implémentation Citrix ADC de CRL et OCSP signale l'état de révocation des certificats clients uniquement. Pour vérifier l'état de révocation d'un certificat de serveur reçu lors d'une connexion SSL, un client doit envoyer une demande à une autorité de certification.

Pour les sites Web où le trafic est important, de nombreux clients reçoivent le même certificat de serveur. Si chaque client envoyait une requête pour l'état de révocation du certificat serveur, l'autorité de certification serait inondée de requêtes OCSP pour vérifier la validité du certificat.

Solution d'agrafage OCSP

Pour éviter une congestion inutile, l'appliance Citrix ADC prend désormais en charge l'agrafage OCSP. Autrement dit, l'appliance peut désormais envoyer l'état de révocation d'un certificat de serveur à un client, au moment de la connexion SSL, après avoir validé l'état du certificat à partir d'un répondeur OCSP. L'état de révocation d'un certificat de serveur est « agrafé » à la réponse que l'appliance envoie au client dans le cadre de la poignée de main SSL. Pour utiliser la fonctionnalité d'agrafage OCSP, vous devez l'activer sur un serveur virtuel SSL et ajouter un répondeur OCSP sur l'appliance.

Remarque :

- Les appliances Citrix ADC prennent en charge l'agrafage OCSP tel que défini dans la RFC 6066.
- L'agrafage OCSP n'est pris en charge que sur le front-end des appliances Citrix ADC.

> **Important :**
>
> La prise en charge de Citrix ADC pour l'agrafage OCSP est limitée aux poignées de main utilisant

> le protocole TLS version 1.0 ou supérieure.

Mise en cache des réponses OCSP des certificats de serveur

Au cours de la poignée de main SSL, lorsqu'un client demande l'état de révocation du certificat de serveur, l'appliance vérifie d'abord dans son cache local une entrée pour ce certificat. Si une entrée valide est trouvée, elle est évaluée et le certificat du serveur et son état sont présentés au client. Si aucune entrée d'état de révocation n'est trouvée, l'appliance envoie une demande d'état de révocation du certificat de serveur au répondeur OCSP. S'il reçoit une réponse, il envoie le certificat et l'état de révocation au client. Si le champ de mise à jour suivant est présent dans la réponse OCSP, la réponse est mise en cache pendant la durée configurée (valeur spécifiée dans le champ Délai d'expiration).

> **Remarque** : à partir de la version 12.1 build 49.x, vous pouvez effacer la réponse mise en cache, du certificat serveur, du répondeur OCSP même avant l'expiration du délai d'expiration. Auparavant, il n'était pas possible d'ignorer l'état mis en cache dans la paire de clés certificat-clé tant que le délai d'attente configuré n'était pas terminé.

Pour effacer l'état mis en cache à l'aide de l'interface de ligne de commande, tapez :

```
clear ssl certKey <certkey name> -ocspstaplingCache
<!--NeedCopy-->
```

Exemple :

```
clear ssl certKey s1 -ocspstaplingCache
<!--NeedCopy-->
```

Pour effacer l'état mis en cache à l'aide de l'interface graphique

1. Dans l'interface graphique, accédez à **Gestion du trafic** > **SSL** > **Certificats > Certificats** d'autorité de **certification**.
2. Dans le volet d'informations, sélectionnez un certificat.
3. Dans la liste **Sélectionner une action**, sélectionnez **Effacer**. Lorsque vous êtes invité à confirmer, cliquez sur **Oui**.

Configuration de l'agrafage OCSP

La configuration de l'agrafage OCSP implique l'activation de la fonction et la configuration d'OCSP. Pour configurer OCSP, vous devez ajouter un répondeur OCSP, lier le répondeur OCSP à un certificat d'autorité de certification et lier le certificat à un serveur virtuel SSL.

> **Remarque :**
>
> Les répondeurs OCSP avec une URL basée uniquement sur HTTP sont pris en charge.

Activer l'agrafage OCSP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl vserver <name> -ocspstapling [ENABLED | DISABLED]
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver vip1 -ocspStapling ENABLED
Done

sh ssl vserver vip1

     Advanced SSL configuration for VServer vip1:
     DH: DISABLED
     DH Private-Key Exponent Size Limit: DISABLED Ephemeral RSA:
        ENABLED Refresh Count: 0
     Session Reuse: ENABLED Timeout: 120 seconds
     Cipher Redirect: DISABLED
     SSLv2 Redirect: DISABLED
     ClearText Port: 0
     Client Auth: DISABLED
     SSL Redirect: DISABLED
     Non FIPS Ciphers: DISABLED
     SNI: ENABLED
     OCSP Stapling: ENABLED
     SSLv2: DISABLED SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED
          TLSv1.2: ENABLED
     Push Encryption Trigger: Always
     Send Close-Notify: YES

     ECC Curve: P_256, P_384, P_224, P_521

    1) CertKey Name: server_certificate1 Server Certificate

    1) Cipher Name: DEFAULT
     Description: Default cipher list with encryption strength >= 128
        bit
Done
<!--NeedCopy-->
```


Remarque : Si le profil (amélioré) par défaut est activé, utilisez la `set ssl profile <profile name> -ocspStapling [ENABLED | DISABLED]` commande pour activer ou désactiver OCSP.

Activer l'agrafage OCSP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Serveur virtuel**.
2. Ouvrez un serveur virtuel et, dans **Paramètres SSL**, sélectionnez **Agrafage OCSP**.

Configuration OCSP

Un répondeur OCSP est ajouté dynamiquement ou manuellement pour envoyer des demandes d'agrafage OCSP. Un répondeur interne est ajouté dynamiquement lorsque vous ajoutez un certificat de serveur et son certificat d'émetteur basé sur l'URL OCSP dans le certificat de serveur. Un répondeur OCSP manuel est ajouté à partir de l'interface de ligne de commande ou de l'interface graphique. Pour envoyer une demande OCSP pour un certificat de serveur, l'appliance Citrix ADC sélectionne un répondeur OCSP en fonction de la priorité qui lui est attribuée lors de la liaison avec un certificat d'émetteur. Si un répondeur ne parvient pas à envoyer une demande d'agrafage OCSP, celui qui a la priorité la plus élevée est sélectionné pour l'envoi de la demande. Par exemple, si un seul répondeur est configuré manuellement et qu'il échoue et qu'un répondeur lié dynamiquement existe, il est sélectionné pour envoyer la demande OCSP.

Si l'URL OCSP est autre que HTTP, aucun répondeur OCSP interne n'est créé.

> **Remarque**
>
> Un répondeur OCSP ajouté manuellement a priorité sur un répondeur ajouté dynamiquement.

Différence entre un répondeur OCSP créé manuellement et un répondeur OCSP créé en interne

Répondeur OCSP créé manuellement	Répondeur OCSP créé en interne (dynamiquement)
Créé manuellement et explicitement lié au certificat de l'émetteur avec une priorité.	Créé et lié par défaut, lors de l'ajout d'un certificat de serveur et de son certificat d'émetteur (certificat d'autorité de certification). Le nom commence par « ns_internal_ ».
La priorité comprise entre 1 et 127 est réservée à un répondeur configuré.	La priorité est automatiquement attribuée à partir de 128.

L'URL et la profondeur du lot peuvent être modifiées.	L'URL et la profondeur du lot ne peuvent pas être modifiées.
Supprimé directement.	Supprimé uniquement lorsque vous supprimez le certificat de serveur ou le certificat d'autorité de certification.
Peut être lié à n'importe quel certificat d'autorité de certification.	Lié par défaut à un certificat d'autorité de certification. Impossible d'être lié à un autre certificat d'autorité de certification.
Enregistré dans la configuration (ns.conf).	Les commandes Ajouter ne sont pas enregistrées dans la configuration. Seules les commandes set sont enregistrées.
Si vous liez trois répondeurs OCSP au même certificat d'émetteur avec les priorités 1, 2 et 3 respectivement, puis que vous dissociez la priorité 2 plus tard, les autres priorités ne sont pas affectées.	Trois répondeurs OCSP sont automatiquement liés à un certificat d'émetteur avec les priorités 128, 129 et 130 respectivement. Si vous supprimez le certificat de serveur utilisé pour créer un répondeur lié à la priorité 129, ce répondeur est supprimé. En outre, la priorité du répondeur suivant (priorité 130) est automatiquement modifiée à 129.

Exemple de traitement des demandes :

1. Ajouter un serveur virtuel (VIP1).
2. Ajouter un certificat émetteur (CA1) et le lier à VIP1.
3. Ajoutez trois certificats S1, S2 et S3. Les répondeurs internes resp1, resp2 et resp3 respectivement sont créés par défaut.
4. Liez S3 à VIP1.
5. Une demande vient à VIP1. Le répondeur resp3 est sélectionné.

Pour créer dynamiquement un répondeur OCSP interne, l'appliance a besoin des éléments suivants :

- Certificat de l'émetteur du certificat du serveur (généralement le certificat de l'autorité de certification).
- Paire de clé de certificat du serveur. Ce certificat doit contenir l'URL OCSP fournie par l'autorité de certification. L'URL est utilisée comme nom du répondeur interne ajouté dynamiquement.

Un répondeur OCSP interne a les mêmes valeurs par défaut qu'un répondeur configuré manuellement.

> **Remarque :**
>
> La mise en cache est désactivée par défaut sur un répondeur interne. Utilisez la `set ssl ocspResponder` commande pour activer la mise en cache.

Configurer OCSP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer OCSP et vérifier la configuration :

```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
    string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>]
    [-expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
    positive_integer>]] [-bundle ( YES | NO )]

add ssl ocspResponder <name> -url <URL> [-cache ( ENABLED | DISABLED )
    [-cacheTimeout <positive_integer>]] [-resptimeout <positive_integer
    >] [-responderCert <string> | -trustResponder] [-producedAtTimeSkew
    <positive_integer>][-signingCert <string>][-useNonce ( YES | NO )][
    -insertClientCert ( YES | NO )]

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]

show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Paramètres :

httpMethod:

Méthode HTTP utilisée pour envoyer des requêtes OCSP. Pour les requêtes de moins de 255 octets, vous pouvez configurer la méthode HTTP GET pour les requêtes vers un serveur OCSP. Si vous spécifiez la méthode GET mais que la longueur est supérieure à 255 octets, l'appliance utilise la méthode par défaut (POST).

Valeurs possibles : GET, POST

Valeur par défaut : POST

ocspUrlResolveTimeout:

Temps d'attente, en millisecondes, pour une résolution d'URL OCSP. Une fois ce temps écoulé, le répondeur avec la priorité supérieure suivante est sélectionné. Si tous les répondeurs échouent, un message d'erreur s'affiche ou la connexion est interrompue, en fonction des paramètres du serveur virtuel.

Valeur minimale : 100

Valeur maximale : 2000

Exemple :

```
add ssl certkey root_ca1  - cert root_cacert.pem
add ssl ocspResponder ocsp_responder1 -url "http:// www.myCA.org:80/
    ocsp/" -cache ENABLED -cacheTimeout 30  -resptimeout 100 -
    responderCert responder_cert -producedAtTimeSkew 300 -signingCert
    sign_cert  -insertClientCert YES
bind ssl certKey root_ca1 -ocspResponder ocsp_responder1 -priority 1
sh ocspResponder ocsp_responder1
    1)Name: ocsp_responder1
    URL: http://www.myCA.org:80/ocsp/, IP: 192.128.22.22
    Caching: Enabled        Timeout: 30 minutes
    Batching: 8 Timeout: 100 mS
    HTTP Request Timeout: 100mS
    Request Signing Certificate: sign_cert
    Response Verification: Full, Certificate: responder_cert
    ProducedAt Time Skew: 300 s
    Nonce Extension: Enabled
     Client Cert Insertion: Enabled
    Done

show certkey root_ca1
    Name: root_ca1     Status: Valid,   Days to expiration:8907
    Version: 3
    …
    1)  OCSP Responder name: ocsp_responder1     Priority: 1
    Done
<!--NeedCopy-->
```

Modifier OCSP à l'aide de l'interface de ligne de commande

Vous ne pouvez pas modifier le nom d'un répondeur OCSP, mais vous pouvez utiliser la `set ssl ocspResponder` commande pour modifier l'un des autres paramètres.

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
set ssl ocspResponder <name> [-url <URL>] [-cache ( ENABLED | DISABLED)
    ] [-cacheTimeout <positive_integer>]  [-resptimeout <
    positive_integer>] [ -responderCert <string> | -trustResponder][-
    producedAtTimeSkew <positive_integer>][-signingCert <string>] [-
    useNonce ( YES | NO )]
```



```
2
3 unbind ssl certKey [<certkeyName>] [-ocspResponder <string>]
4
5 bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
     positive_integer>]
6
7 show ssl ocspResponder [<name>]
8 <!--NeedCopy-->
```

Configurer OCSP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Répondeur OCSP** et configurez un répondeur OCSP.
2. Accédez à **Gestion du trafic** > **SSL** > **Certificats**, sélectionnez un certificat et, dans la liste **Action**, sélectionnez **Liaisons OCSP**. **Liez un répondeur OCSP**.
3. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, ouvrez un serveur virtuel et cliquez dans la section Certificats pour lier un certificat d'autorité de certification.
4. Le cas échéant, sélectionnez **OCSP Obligatoire**.

> **Remarque :**
>
> Le paramètre de certificat client d'insertion dans le `add ssl ocspResponder` et `set ssl ocspResponder` les commandes n'est plus valide. Autrement dit, le paramètre est ignoré lors de la configuration.

Suites de chiffrement disponibles sur les appliances Citrix ADC

August 20, 2021

Votre appliance Citrix ADC est livrée avec un ensemble prédéfini de groupes de chiffrement. Pour utiliser des chiffrements qui ne font pas partie du groupe de chiffrement DEFAULT, vous devez les lier explicitement à un serveur virtuel SSL. Vous pouvez également créer un groupe de chiffrement défini par l'utilisateur pour lier au serveur virtuel SSL. Pour plus d'informations sur la création d'un groupe de chiffrement défini par l'utilisateur, voir Configurer des groupes de chiffrement définis par l'utilisateur sur l'appliance ADC.

> **Remarques**
>
> Le chiffrement RC4 n'est pas inclus dans le groupe de chiffrement par défaut sur l'appliance Citrix ADC. Cependant, il est pris en charge dans le logiciel sur les appliances basées sur N3. Le chiffrement RC4, y compris la poignée de main, se fait dans le logiciel.
>
> Citrix vous recommande de ne pas utiliser ce chiffrement car il est considéré comme non sécurisé

> et obsolète par la RFC 7465.
>
> Utilisez la commande ‘show hardware ‘pour déterminer si votre appliance possède des puces N3.

```
sh hardware

Platform: NSMPX-22000 16\*CPU+24\*IX+12\*E1K+2\*E1K+4*CVM N3 2200100

Manufactured on: 8/19/2013

CPU: 2900MHZ

Host Id: 1006665862

Serial no: ENUK6298FT

Encoded serial no: ENUK6298FT
<!--NeedCopy-->
```

- Pour afficher des informations sur les suites de chiffrement liées par défaut à l'extrémité frontale (à un serveur virtuel), tapez : `sh cipher DEFAULT`
- Pour afficher des informations sur les suites de chiffrement liées par défaut au back-end (à un service), tapez : `sh cipher DEFAULT_BACKEND`
- Pour afficher des informations sur tous les groupes de chiffrement (alias) définis sur l'appliance, tapez :`sh cipher`
- Pour afficher des informations sur toutes les suites de chiffrement faisant partie d'un groupe de chiffrement spécifique, tapez : `sh cipher <alias name>`. Par exemple, le chiffrement sh ECDHE.

Les liens suivants répertorient les suites de chiffrement prises en charge sur différentes plates-formes Citrix ADC et sur des modules de sécurité matérielle externes (HSM) :

- Appliance**Citrix ADC MPX/SDX (N3) : prise en charge du chiffrement sur une appliance**Citrix ADC MPX/SDX (N3)
- Appliance**Intel Coleto Citrix ADC MPX/SDX : prise en charge du chiffrement sur une appliance**basée sur puce SSL Intel Coleto Citrix ADC MPX/SDX
- **Appliance Citrix ADC VPX** : prise en charge du chiffrement sur une appliance Citrix ADC VPX
- Appliance**FIPS Citrix ADC MPX/SDX 14000 : prise en charge du chiffrement sur une appliance**FIPS Citrix ADC MPX/SDX 14000
- **HSM externe (Thales/Safenet)** : chiffrement pris en charge sur un HSM externe (Thales/Safenet)
- Appliance**Citrix ADC MPX/SDX (N2) : prise en charge du chiffrement sur une appliance**Citrix ADC MPX/SDX (N2)
- **Appliance FIPS Citrix ADC MPX 9700** : prise en charge du chiffrement sur une Citrix ADC MPX

9700 FIPS avec microprogramme 2.2

- Appliances**CITRIX ADC VPX FIPS et MPX FIPS : prise en charge du chiffrement sur les appliances**certifiées Citrix ADC VPX FIPS et MPX FIPS

> **Remarque :**
>
> Pour connaître la prise en charge du chiffrement DTLS, reportez-vous à la section Prise en charge du chiffrement DTLS sur les appliances Citrix ADC VPX, MPX et SDX.

Tableau1 - Prise en charge du serveur virtuel/service frontend interne :

Protocole/Plateforme	MPX/SDX (f2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
TLS 1.3	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	Non pris en charge	Non pris en charge	13.0 toutes les versions
	12.1–50.x	12.1–50.x	12.1–50.x	Non pris en charge	Non pris en charge	12.1–50.x
TLS 1.1/1.2	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12.0-57.x pour MPX 15000-50G, 12.0-60.x pour MPX 26000-100G
	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11.1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11.1-60.x pour MPX 26000-100G
	11.0 toutes les versions	11.0 toutes les versions	11.0 toutes les versions	11.0 toutes les versions	11.0 toutes les versions	11.0—70.x (uniquement sur MPX 5900/8900)
	10.5 toutes les versions	10.5 toutes les versions	10.5–57.x	10.5 58.1108.e	10.5–59.1359.e	10.5—67.x, 10.5-63,47 (uniquement sur MPX 5900/8900)

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
ECDHE/DHE (Exemple TLS1-ECDHE-RSA-AES128-SHA)	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12.0-57.x pour MPX 15000-50G, 12.0-60.x pour MPX 26000-100G

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11.1–51.x	11.1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11.1-60.x pour MPX 26000-100G
	11.0 toutes les versions	11.0 toutes les versions	11.0 toutes les versions			11.0—70.114 (uniquement sur MPX 5900/8900)
	10.5–53.x	10.5–53.x	10.5 toutes les versions	10.5–59.1306.e		10.5—67.x, 10.5-63,47 (uniquement sur MPX 5900/8900)
AES-GCM (Exemple TLS1.2-AES128-GCM-SHA256)	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12.0-57.x pour MPX 15000-50G, 12.0-60.x pour MPX 26000-100G
	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11.1—51.x (Voir note)	11.1—51.x (Voir note)	11.1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11.1-60.x pour MPX 26000-100G

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	11.0 toutes les versions	11.0 toutes les versions	11.0–66.x			11.0—70.114 (uniquement sur MPX 5900/8900)
	10.5–53.x	10.5–53.x				10.5—67.x, 10.5-63,47 (uniquement sur MPX 5900/8900)
Ciphers SHA-2 (Exemple TLS1.2-AES-128-SHA256)	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12.0-57.x pour MPX 15000-50G, 12.0-60.x pour MPX 26000-100G
	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11.1–52.x	11.1–52.x	11.1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11.1-60.x pour MPX 26000-100G
	11.0 toutes les versions	11.0 toutes les versions	11.0–66.x			11.0—72.x, 11.0-70.114 (uniquement sur MPX 5900/8900)
	10.5–53.x	10.5–53.x				10.5—67.x, 10.5-63,47 (uniquement sur MPX 5900/8900)

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
ECDSA (Exemple TLS1-ECDHE-ECDSA-AES256-SHA)	Non pris en charge	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions
	Non pris en charge	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	Non pris en charge	12.0 toutes les versions	12.0—57.x	Sans objet	Non pris en charge	12.0 toutes les versions pour MPX 5900/8900, 12.0-57.x pour MPX 15000-50G, 12.0-60.x pour MPX 26000-100G

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
		11.1 toutes les versions				11.1—56.x, 11.1-54.126 (Seules les courbes ECC P_256 et P_384 sont prises en charge.)
CHACHA20	Non pris en charge	13.0 toutes les versions	13.0 toutes les versions	Non pris en charge	Non pris en charge	13.0 toutes les versions
	Non pris en charge	Non pris en charge	12.1 toutes les versions	Non pris en charge	Non pris en charge	12.1—49.x (uniquement sur MPX 5900/8900)
	Non pris en charge	Non pris en charge	12.0–56.x	Non pris en charge	Non pris en charge	Non pris en charge

Tableau 2 - Prise en charge des services back-end :

TLS 1.3 n’est pas pris en charge sur le back-end.

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
TLS 1.1/1.2	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12.0-57.x pour MPX 15000-50G, 12.0-60.x pour MPX 26000-100G
	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11.1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11.1-60.x pour MPX 26000-100G

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	11.0–50.x	11.0–50.x	11.0–66.x	11.0 toutes les versions		11.0—70.119 (uniquement sur MPX 5900/8900)
	10.5–59.x	10.5–59.x		10.5–58.1108.e	10.5–59.1359.e	10.5—67.x, 10.5-63,47 (uniquement sur MPX 5900/8900)
ECDHE/DHE (Exemple TLS1-ECDHE-RSA-AES128-SHA)	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.0 toutes les versions	12.0 toutes les versions	12.0–56.x	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12.0-57.x pour MPX 15000-50G, 12.0-60.x pour MPX 26000-100G
	11.1 toutes les versions	11.1 toutes les versions		11.1 toutes les versions	11.1–51.x	11.1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11.1-60.x pour MPX 26000-100G
	11.0–50.x	11.0–50.x				11.0—70.119 (uniquement sur MPX 5900/8900)
	10.5–58.x	10.5–58.x		10.5–59.1306.e		10.5—67.x, 10.5-63,47 (uniquement sur MPX 5900/8900)

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
AES-GCM (Exemple TLS1.2-AES128-GCM-SHA256)	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	12.0 toutes les versions	12.0 toutes les versions	Non pris en charge	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12.0-57.x pour MPX 15000-50G, 12.0-60.x pour MPX 26000-100G

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	11.1 toutes les versions	11.1 toutes les versions		11.1–51.x	11.1–51.x	11.1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11.1-60.x pour MPX 26000-100G
Ciphers SHA-2 (Exemple TLS1.2-AES-128-SHA256)	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G

Protocole/Plate-forme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.0 toutes les versions	12.0 toutes les versions	Non pris en charge	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12.0-57.x pour MPX 15000-50G, 12.0-60.x pour MPX 26000-100G
	11.1 toutes les versions	11.1 toutes les versions		11.1–52.x	11.1–52.x	11.1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11.1-60.x pour MPX 26000-100G
ECDSA (Exemple TLS1-ECDHE-ECDSA-AES256-SHA)	Non pris en charge	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	Non pris en charge	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	Non pris en charge	12.0 toutes les versions	12.0–57.x	Sans objet	Non pris en charge	12.0 toutes les versions pour MPX 5900/8900, 12.0-57.x pour MPX 15000-50G, 12.0-60.x pour MPX 26000-100G

Protocole/Plateforme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS avec firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
		11.1–51.x		Sans objet		11.1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11.1-60.x pour MPX 26000-100G (Seules les courbes ECC P_256 et P_384 sont prises en charge).
CHACHA20	Non pris en charge	13.0 toutes les versions	13.0 toutes les versions	Non pris en charge	Non pris en charge	13.0 toutes les versions
	Non pris en charge	Non pris en charge	12.1 toutes les versions	Non pris en charge	Non pris en charge	12.1—49.x pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	Non pris en charge	Non pris en charge	12.0–56.x	Non pris en charge	Non pris en charge	Non pris en charge

Pour obtenir la liste détaillée des chiffrements ECDSA pris en charge, voir Prise en charge des suites de chiffrement ECDSA.

> Remarque

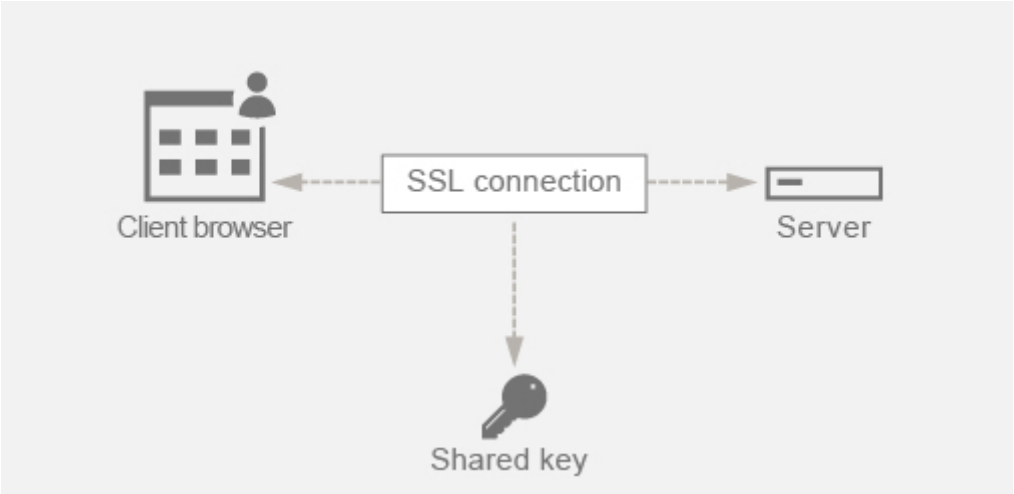
- La suite de chiffrement TLS-Fallback_scsv est prise en charge sur toutes les appliances de la version 10.5 build 57.x
- La prise en charge de HTTP Strict Transport Security (HSTS) est basée sur des stratégies.
- Tous les certificats signés SHA-2 (SHA256, SHA384, SHA512) sont pris en charge sur le front de toutes les appliances. Dans la version 11.1, version 54.x et ultérieure, ces certificats sont également pris en charge sur le back-end de toutes les appliances. Dans les versions 11.0 et antérieures, seuls les certificats signés SHA256 sont pris en charge sur le back-end de toutes les appliances.
- Dans la version 11.1 build 52.x et antérieure, les chiffrements suivants ne sont pris en charge que sur l'avant des appliances MPX 9700 et MPX/SDX 14000 FIPS :
  - TLS1.2-ECDHE-RSA-AES-256-SHA384
  - TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 From release 11.1 build 53.x, and in release 12.0, these ciphers are also supported on the back end.
- Tous les chiffrements Chacha20-Poly1035 utilisent une fonction pseudo-aléatoire (PSF) TLS avec la fonction de hachage SHA-256.

Secret Perfect Forward (PFS)

Perfect Forward Secrecy garantit la protection des communications SSL actuelles même si la clé de session d'un serveur Web est compromise ultérieurement.

Pourquoi avez-vous besoin de Perfect Forward Secrecy (PFS) ?

Une connexion SSL est utilisée pour sécuriser les données transmises entre un client et un serveur. Cette connexion commence par la prise de contact SSL entre le navigateur d'un client et le serveur Web contacté. C'est au cours de cette poignée de contact que le navigateur et le serveur échangent certaines informations pour parvenir à une clé de session qui sert de moyen de chiffrer les données tout au long de la communication.

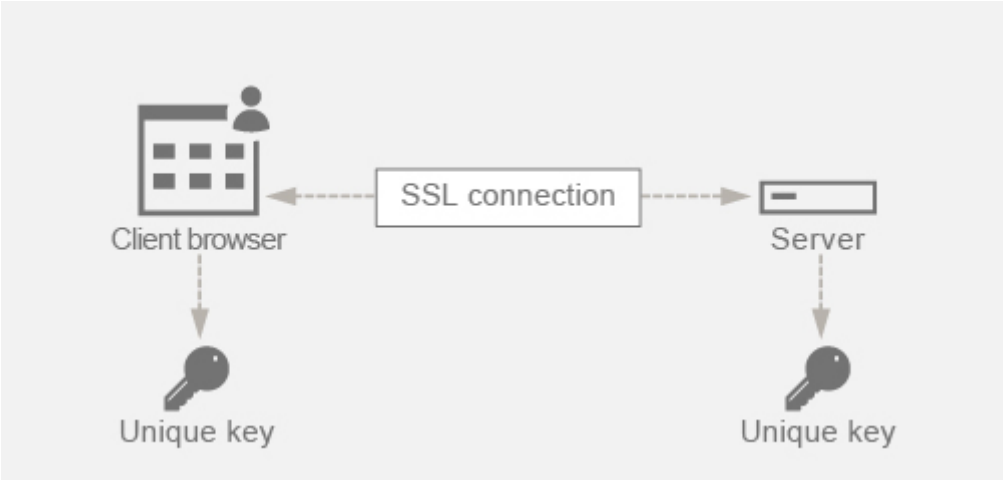


Le RSA est l'algorithme le plus couramment utilisé pour l'échange de clés. Le navigateur utilise la clé publique du serveur pour chiffrer et envoyer le secret pré-maître à un serveur. Ce secret pré-maître est utilisé pour arriver à la clé de session. Le problème dans l'approche d'échange de clés RSA est que si un attaquant parvient à saisir la clé privée du serveur à n'importe quel moment dans le futur, l'attaquant obtient le secret pré-maître à l'aide duquel la clé de session peut être obtenue. Cette clé de session peut désormais être utilisée par l'attaquant pour déchiffrer toutes les conversations SSL. Cela signifie que vos communications SSL historiques étaient sécurisées auparavant, mais elles ne sont plus sécurisées, car la clé privée volée du serveur peut être utilisée pour arriver à la clé de session et ainsi déchiffrer toute conversation historique enregistrée.

Le besoin est de pouvoir protéger les communications SSL passées même si la clé privée du serveur a été compromise. C'est là que la configuration de Perfect Forward Secrecy (PFS) vient à la rescousse.

Comment PFS aide-t-il ?

Perfect Forward Secrecy (PFS) protège les communications SSL passées en demandant au client et au serveur d'accepter une nouvelle clé pour chaque session et en gardant le calcul de cette clé de session secret. Il fonctionne sur la base que la compromission d'une clé de serveur ne doit pas entraîner de compromis sur la clé de session. La clé de session est dérivée séparément aux deux extrémités et n'est jamais transférée sur le fil. Les clés de session sont également détruites une fois la communication terminée. Ces faits garantissent que même si quelqu'un a accès à la clé privée du serveur, il ne sera pas en mesure d'arriver à la clé de session et ne serait donc pas en mesure de déchiffrer les données passées.



Explication avec exemple

Supposons que nous utilisons DHE pour atteindre le PFS. L'algorithme DH garantit que même si un pirate met en main la clé privée du serveur, le pirate ne pourra pas arriver à la clé de session car la clé de session et les numéros aléatoires (utilisés pour arriver à la clé de session) sont gardés secrets aux deux extrémités et ne sont jamais échangés par fil.
PFS peut être atteint en utilisant l'échange de clés Diffie-Hellman éphémère qui crée de nouvelles clés temporaires pour chaque session SSL.

L'inverse de la création d'une clé pour chaque session est qu'elle nécessite des calculs supplémentaires, mais cela peut être surmonté en utilisant la courbe elliptique qui a des tailles de clés plus petites.

Configurer PFS sur l'appliance Citrix ADC

PFS peut être configuré sur un Citrix ADC en configurant des chiffrements DHE ou ECDHE. Ces chiffrements garantissent que la clé de session secrète créée n'est pas partagée sur le fil (algorithme DH) et que la clé de session ne reste vivante que pendant une courte période (éphémère). Les deux configurations sont expliquées dans les sections suivantes.

Remarque : L'utilisation de chiffrements ECDHE au lieu de DHE permet de sécuriser la communication avec des tailles de clés plus petites.

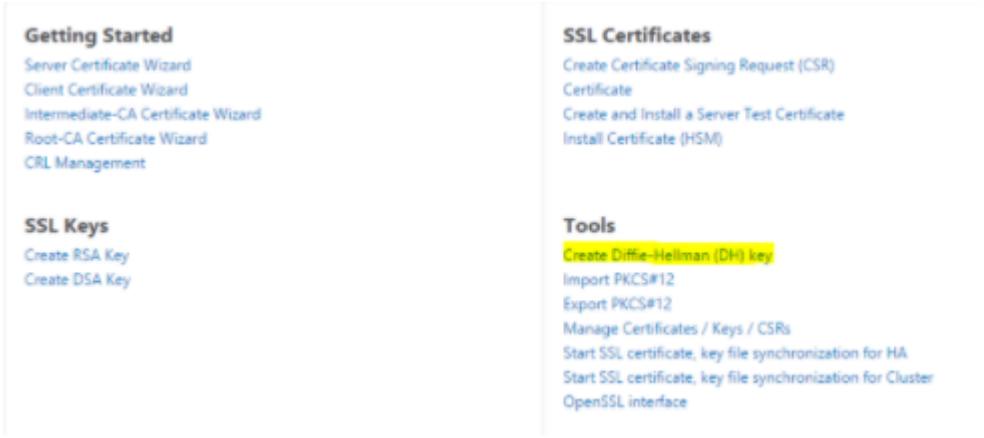
Configurer DHE à l'aide de l'interface graphique

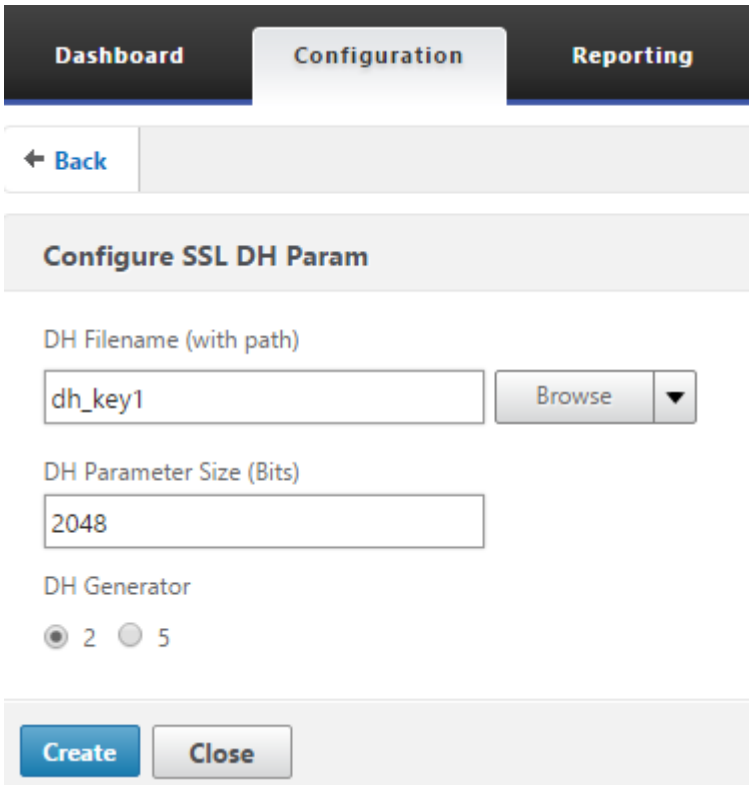
1. Générez une clé DH.

   a. Accédez à **Gestion du trafic > SSL > Outils**.

   b. Cliquez sur **Créer une clé DH (Diffice Helman)**.

Remarque : La génération d'une clé DH de 2 048 bits peut prendre jusqu'à 30 minutes.



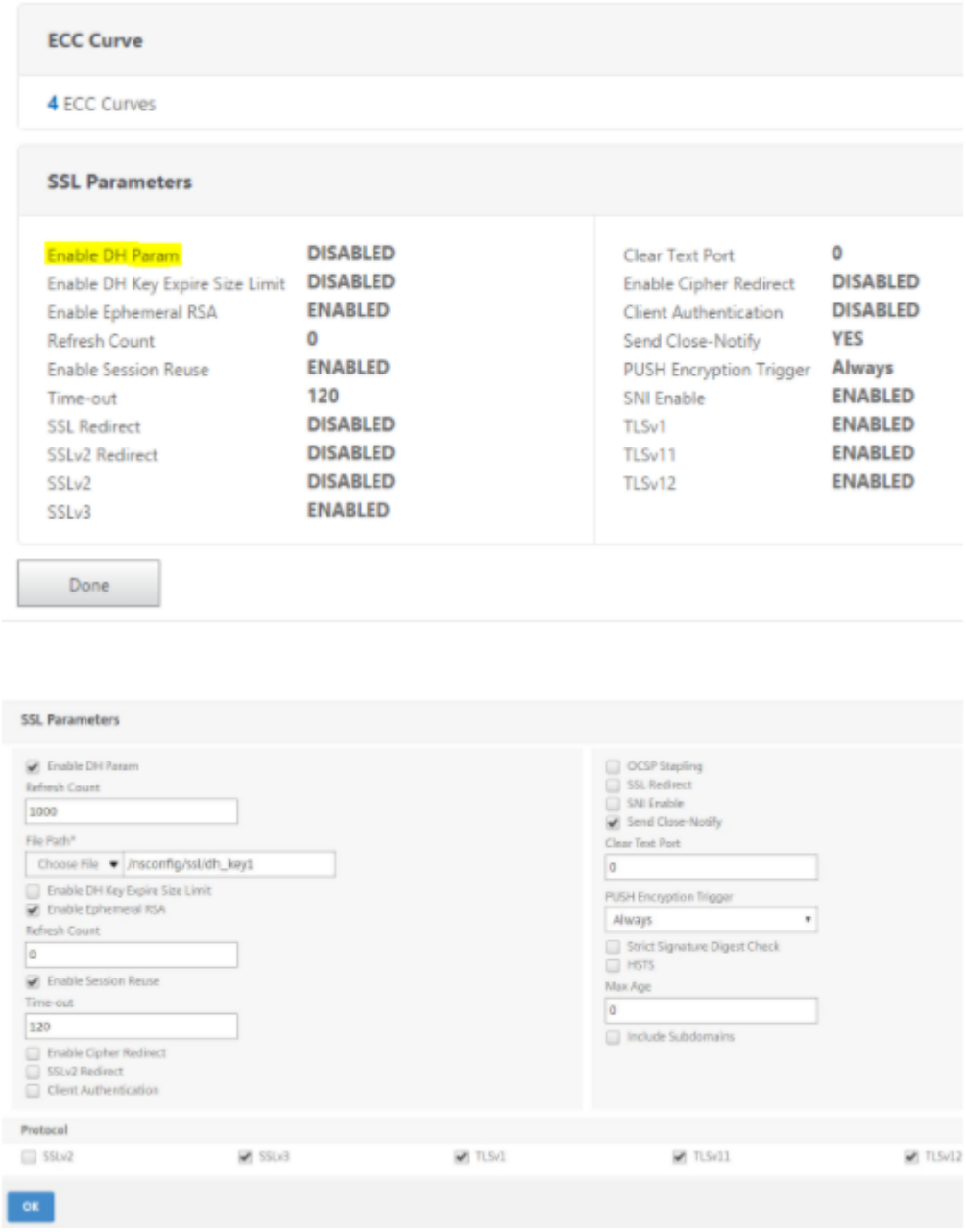


2. Activez DH Param pour le serveur virtuel SSL et attachez la clé DH au serveur virtuel SSL.

   a. Accédez à **Configuration > Gestion du trafic > Serveurs virtuels**.

   b. Sélectionnez le serveur virtuel sur lequel vous souhaitez activer DH.

   c. Cliquez sur **Modifier**, cliquez sur **Paramètres SSL**, puis sur **Activer le paramètre DH**.



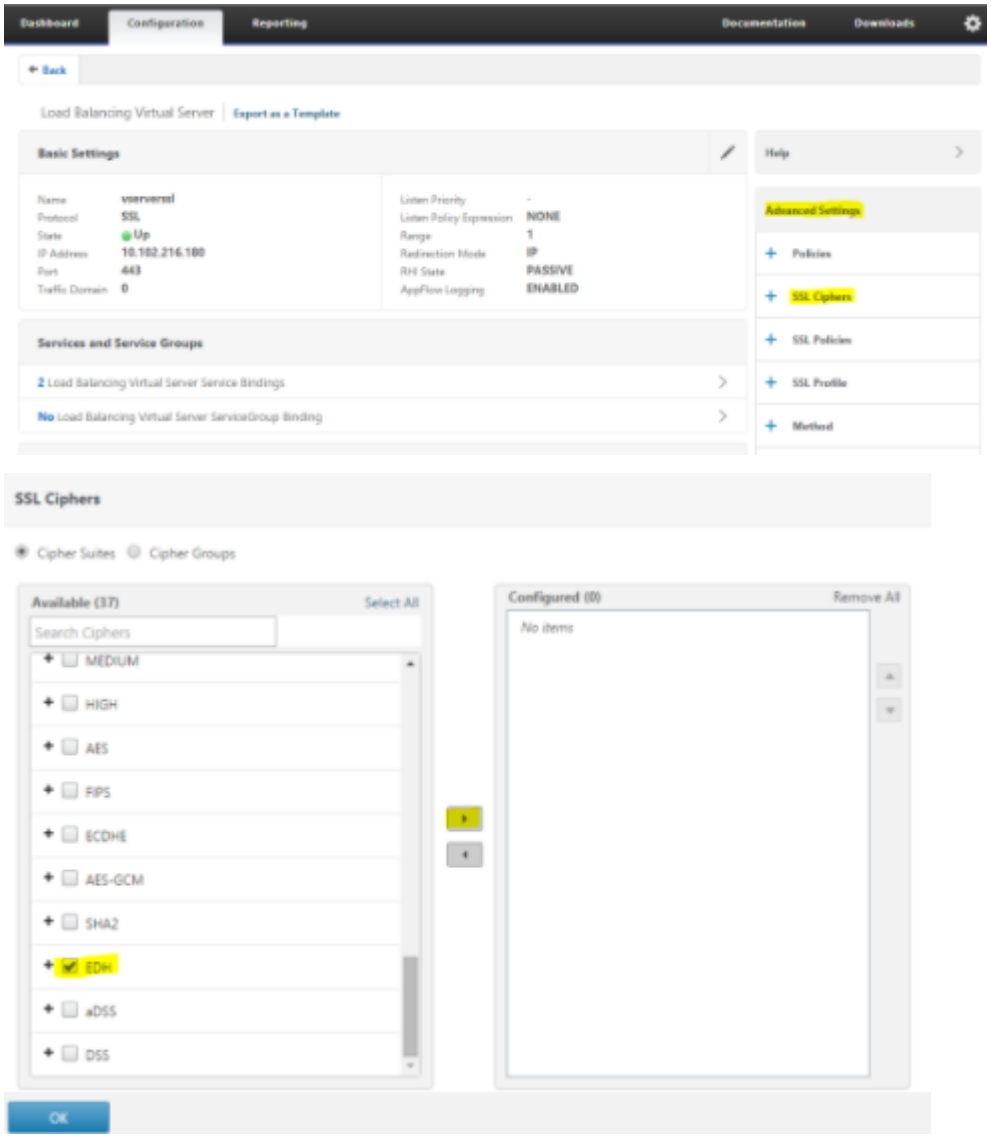
3. Liez les chiffrements DHE au serveur virtuel.

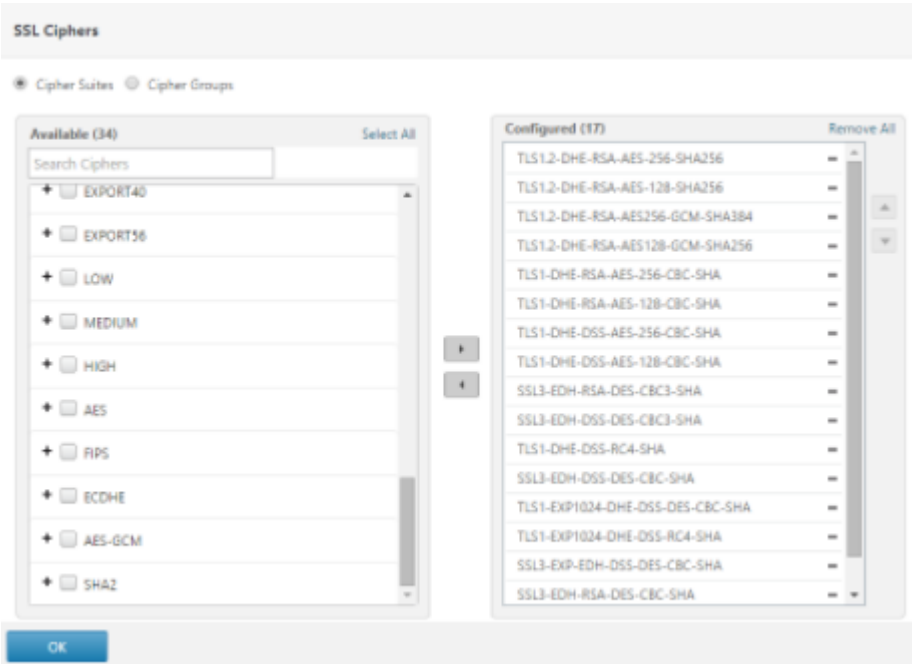
   a. Accédez à **Configuration > Gestion du trafic > Serveurs virtuels**.

   b. Sélectionnez le serveur virtuel sur lequel vous souhaitez activer DH et cliquez sur l'icône crayon pour le modifier.

   c. Sous **Paramètres avancés**, cliquez sur l'icône Plus en regard de **Chiphers SSL**, sélectionnez les groupes de chiffrement DHE, puis cliquez sur **OK** pour lier.

   Remarque : Assurez-vous que les chiffrements DHE se trouvent en haut de la liste des chiffrements liés au serveur virtuel.





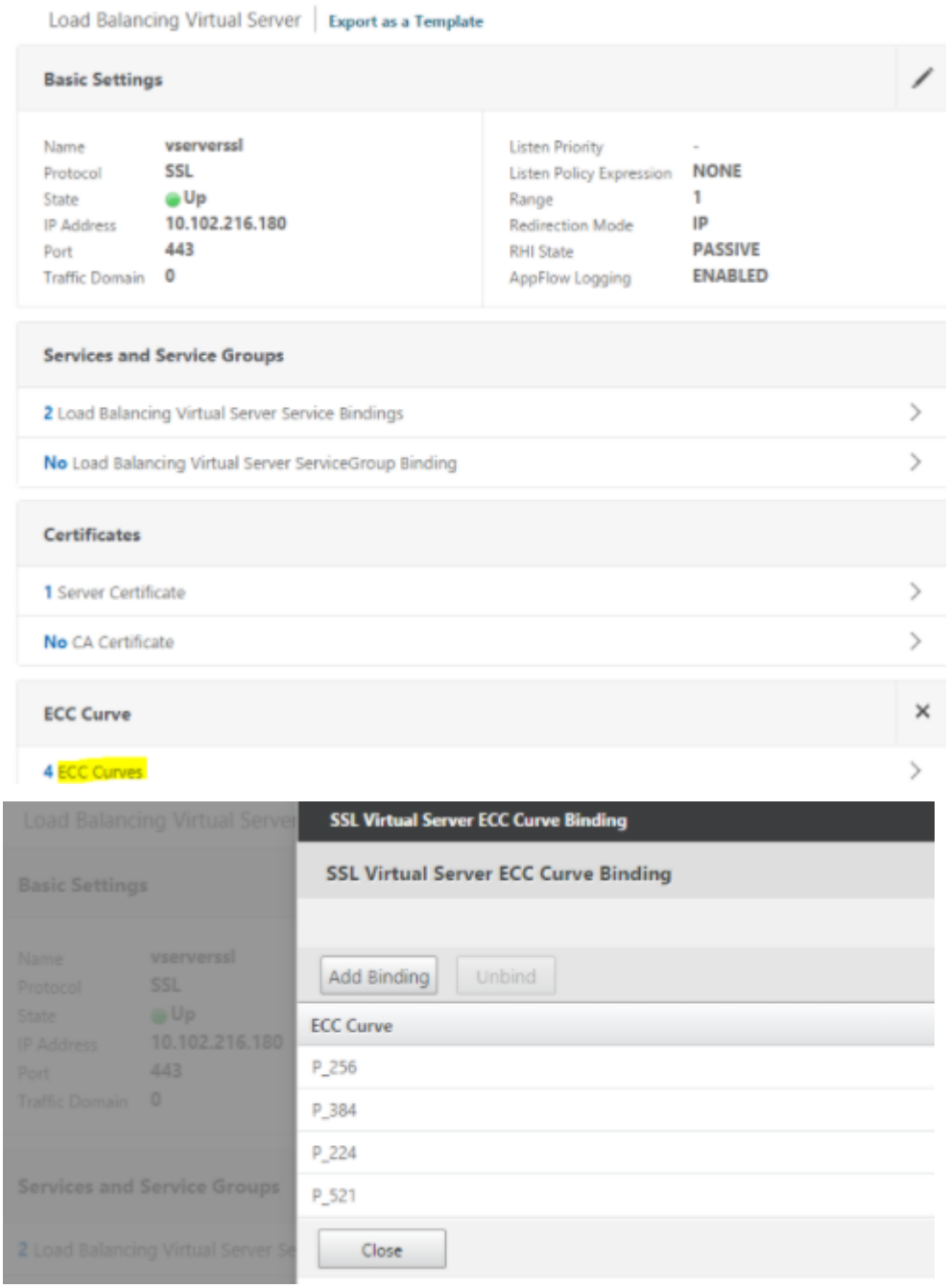
Configurer ECDHE à l'aide de l'interface graphique

1. Liez les courbes ECC au serveur virtuel SSL.

   a. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

   b. Sélectionnez le serveur virtuel SSL que vous souhaitez modifier, cliquez sur **Courbe ECC**, puis sur **Ajouter une liaison**.

   c. Liez la courbe ECC requise au serveur virtuel.

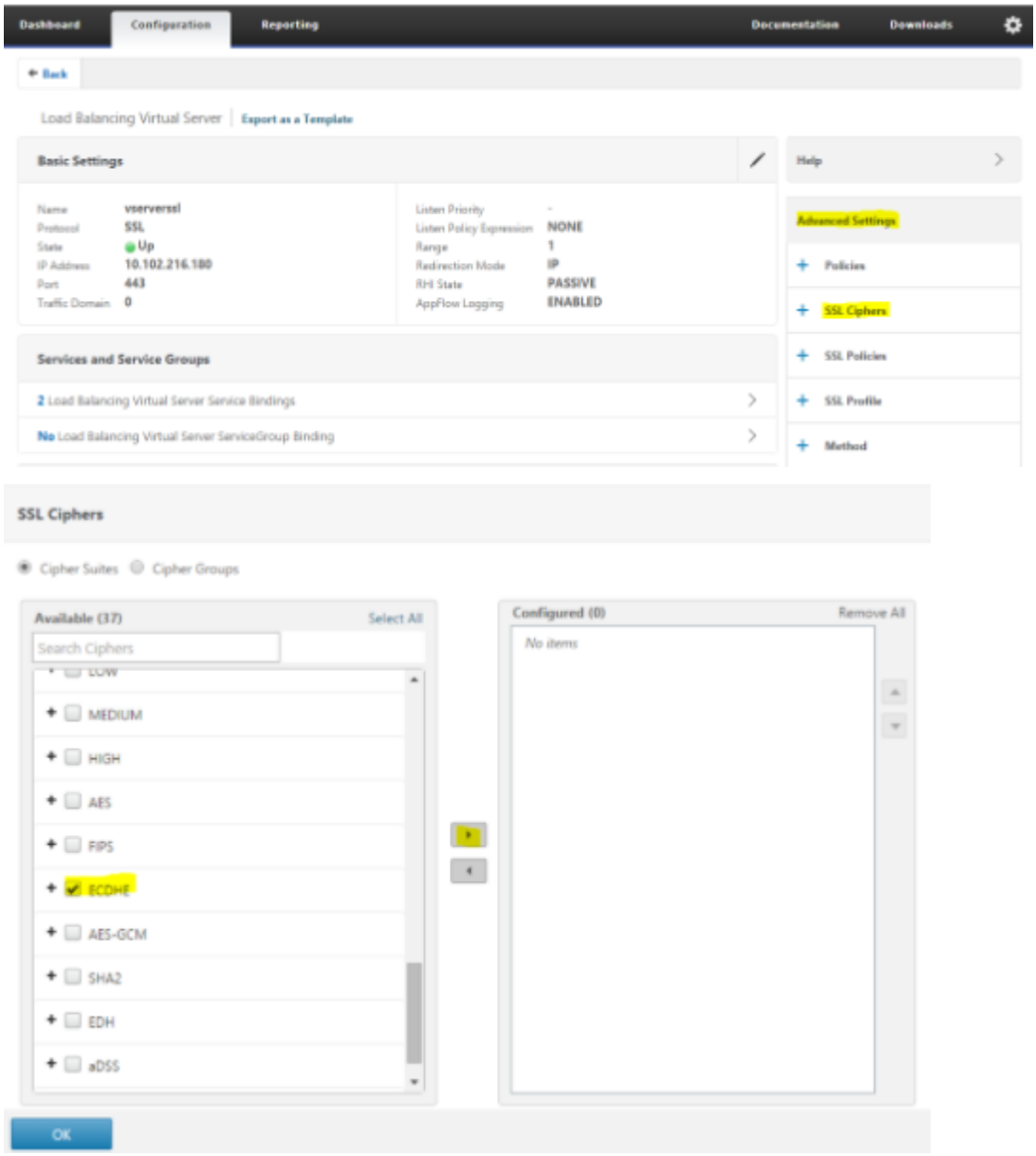


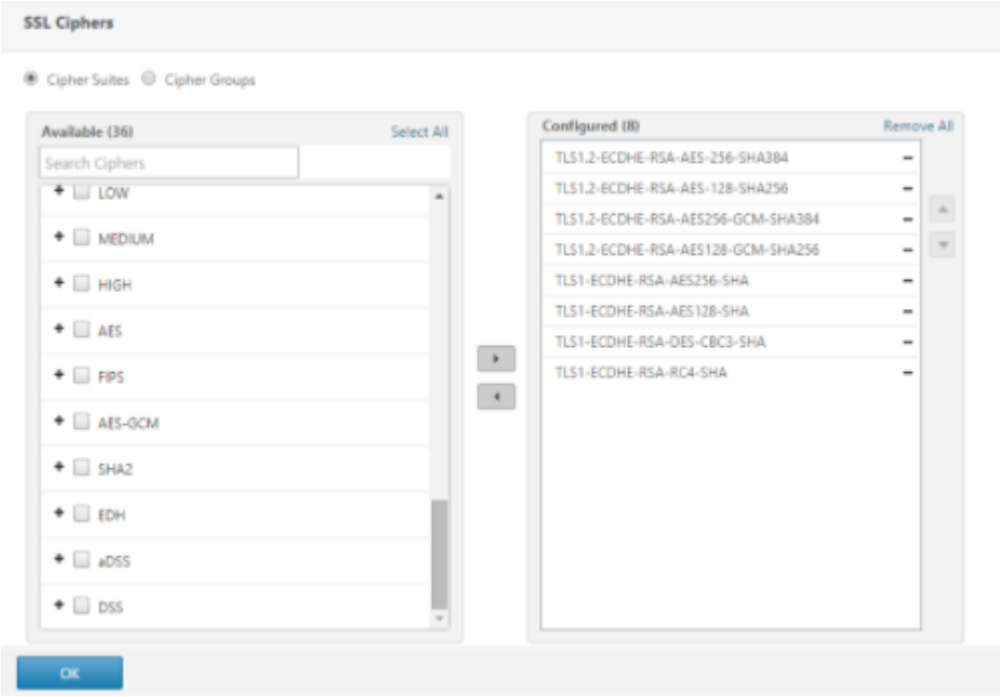
2. Liez les chiffrements ECDHE au serveur virtuel.

   a. Navigate to **Configuration > Traffic Management > Virtual Servers** and select the virtual server on which you want to enable DH.

   b. Click **Edit > SSL Ciphers** and select the ECDHE cipher groups and click **Bind**.

   Note: Ensure that the ECDHE ciphers are at the top of the cipher list bound to the virtual server.





Remarque : Dans chaque cas, vérifiez que l'appliance Citrix ADC prend en charge les chiffrements que vous souhaitez utiliser pour la communication.

Configurer PFS à l'aide d'un profil SSL

Remarque : L'option permettant de configurer PFS (chiffrement ou ECC) à l'aide d'un profil SSL est introduite à partir de la version 11.0 64.x. Ignorez la section suivante si vous utilisez des versions antérieures.

Pour activer PFS à l'aide d'un profil SSL, une configuration similaire (comme expliqué dans les sections de configuration précédentes) doit être effectuée mais sur le profil SSL au lieu de la configurer directement sur un serveur virtuel.

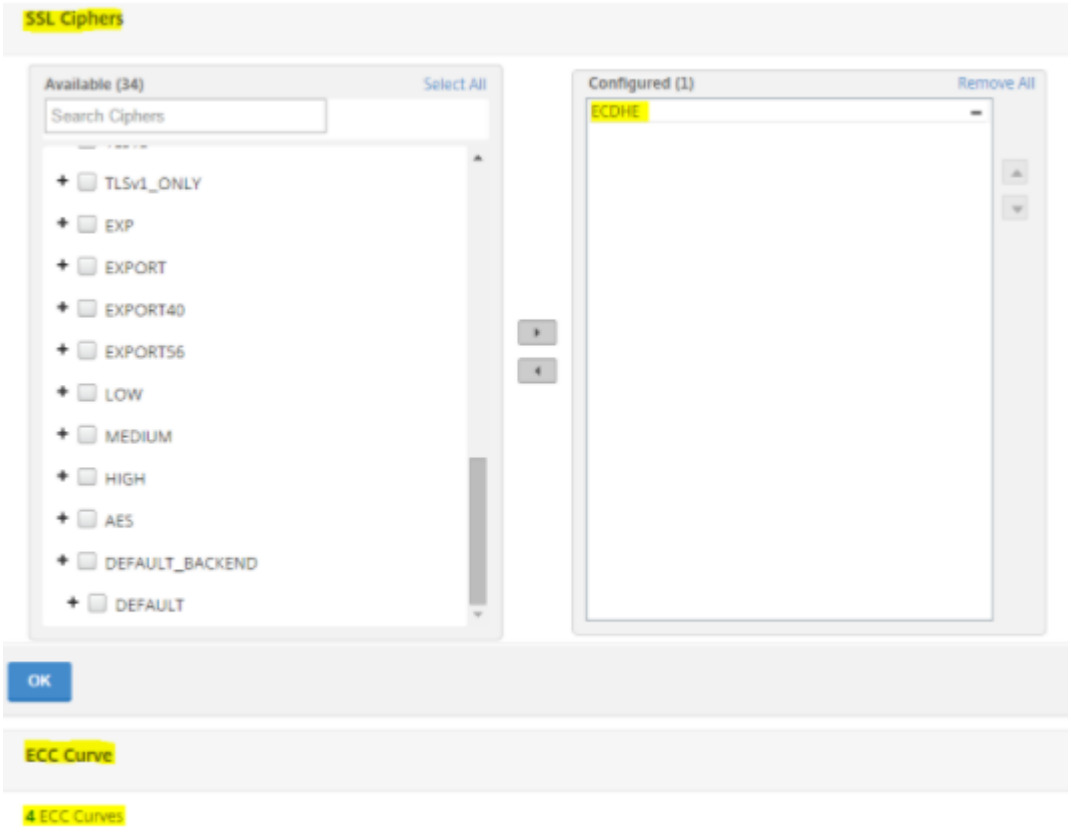
Configurer PFS à l'aide d'un profil SSL à l'aide de l'interface graphique

1. Liez les courbes ECC et les chiffrements ECDHE sur le profil SSL.

   Remarque : les courbes ECC sont déjà liées par défaut à tous les profils SSL.

   a. Accédez à **Système > Profils > Profils SSL** et choisissez le profil sur lequel vous souhaitez activer PFS.

   b. Liez les chiffrements ECDHE.



2. Liez le profil SSL au serveur virtuel.

   a. Accédez à **Configuration > Gestion du trafic > Serveurs virtuels** et sélectionnez le serveur virtuel.

   b. Cliquez sur l'icône crayon pour modifier le profil SSL.

   c. Cliquez sur **OK**, puis sur **Terminé**.

Configurer PFS avec SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

1. Liez les courbes ECC au profil SSL.

```
bind sslprofile <SSLProfileName> -eccCurveName <Name_of_curve>
<!--NeedCopy-->
```


2. Liez le groupe de chiffrement ECDHE.

```
bind sslprofile <SSLProfileName> cipherName <ciphergroupName>
<!--NeedCopy-->
```

3. Définissez la priorité du chiffrement ECDHE sur 1.

```
set sslprofile <SSLProfileName> cipherName <ciphergroupName>
   cipherPriority <positive_integer>
<!--NeedCopy-->
```

4. Liez le profil SSL au serveur virtuel.

```
set SSL vserver <vservername> sslProfile <SSLProfileName>
<!--NeedCopy-->
```

Chiffrements ECDHE

August 20, 2021

Toutes les appliances Citrix ADC prennent en charge le groupe de chiffrement ECDHE sur le front end et le back-end. Sur une appliance SDX, si une puce SSL est affectée à une instance VPX, la prise en charge du chiffrement d'une appliance MPX s'applique. Sinon, le support de chiffrement normal d'une instance VPX s'applique.

Pour plus d'informations sur les versions et les plates-formes qui prennent en charge ces chiffrements, consultez la section Chiphers disponibles sur les appliances Citrix ADC.

Les suites de chiffrement ECDHE utilisent la cryptographie à courbe elliptique (ECC). En raison de sa taille de clé plus petite, ECC est particulièrement utile dans un environnement mobile (sans fil) ou un environnement de réponse vocale interactive, où chaque milliseconde est importante. Des tailles de clés plus petites permettent d'économiser de l'énergie, de la mémoire, de la bande passante et des coûts de calcul.

Une appliance Citrix ADC prend en charge les courbes ECC suivantes :

- P_256
- P_384
- P_224
- P_521

Remarque : Si vous effectuez une mise à niveau à partir d'une version antérieure à la version 10.1 build 121.10, vous devez lier explicitement les courbes ECC à vos serveurs et services virtuels SSL

existants. Les courbes sont liées par défaut à tous les serveurs virtuels et services que vous créez après la mise à niveau.

Vous pouvez lier une courbe ECC à des entités frontales et back-end SSL. Par défaut, les quatre courbes sont liées, dans l'ordre suivant : P_256, P_384, P_224, P_521. Pour changer l'ordre, vous devez d'abord délier toutes les courbes, puis les lier dans l'ordre désiré.

Lier des courbes ECC à un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind ssl vserver <vServerName > -eccCurveName <eccCurveName >
```

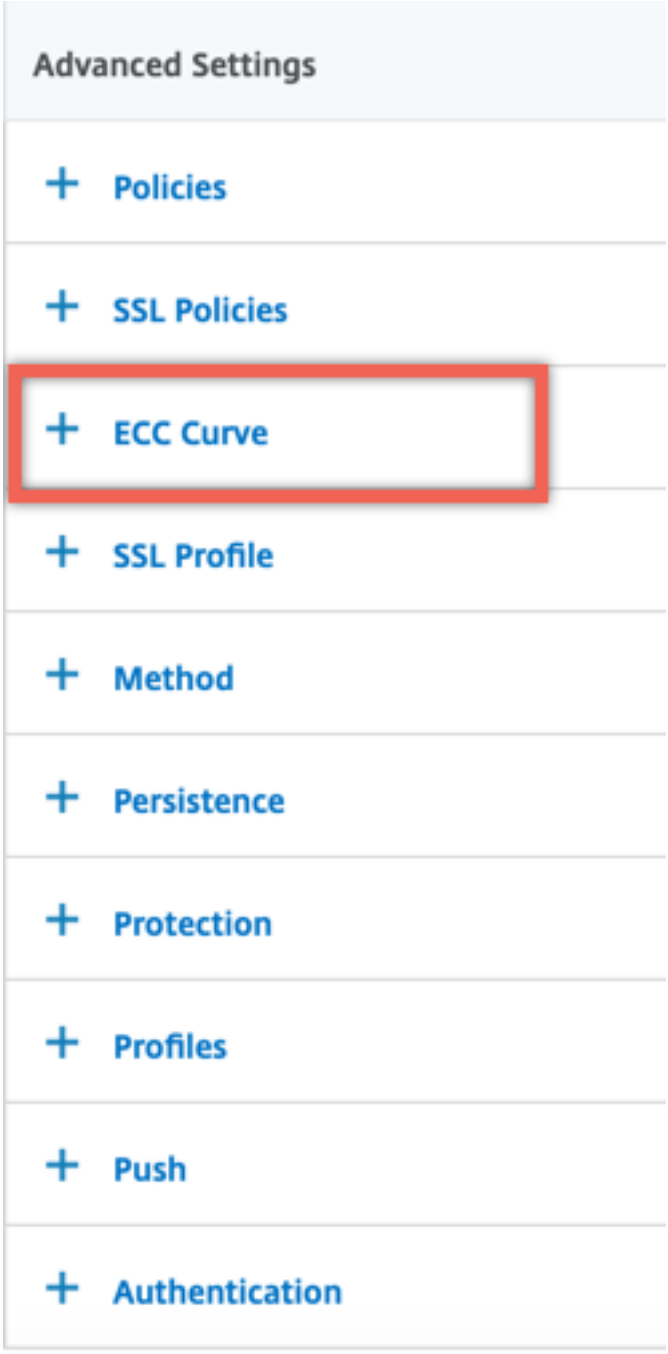
Exemple :

```
1  bind ssl vserver  v1 -eccCurveName P_224
2
3  sh ssl vserver v1
4
5  Advanced SSL configuration for VServer v1:
6  DH: DISABLED
7  Ephemeral RSA: ENABLED Refresh Count: 0
8  Session Reuse: ENABLED Timeout: 120 seconds
9  Cipher Redirect: DISABLED
10 SSLv2 Redirect: DISABLED
11 ClearText Port: 0
12 Client Auth: DISABLED
13 SSL Redirect: DISABLED
14 Non FIPS Ciphers: DISABLED
15 SNI: DISABLED
16 SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED  TLSv1.1: DISABLED
      TLSv1.2: DISABLED
17 Push Encryption Trigger: Always
18 Send Close-Notify: YES
19 ECC Curve: P_224
20
21 1) Cipher Name: DEFAULT
22 Description: Predefined Cipher Alias
23 Done
24 <!--NeedCopy-->
```

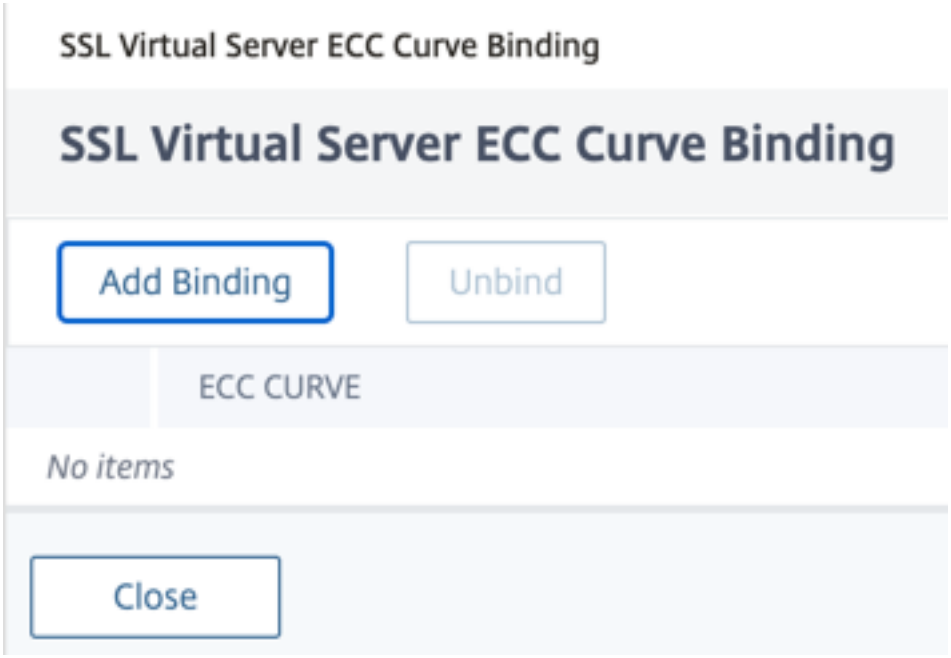
Liez des courbes ECC à un serveur virtuel SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

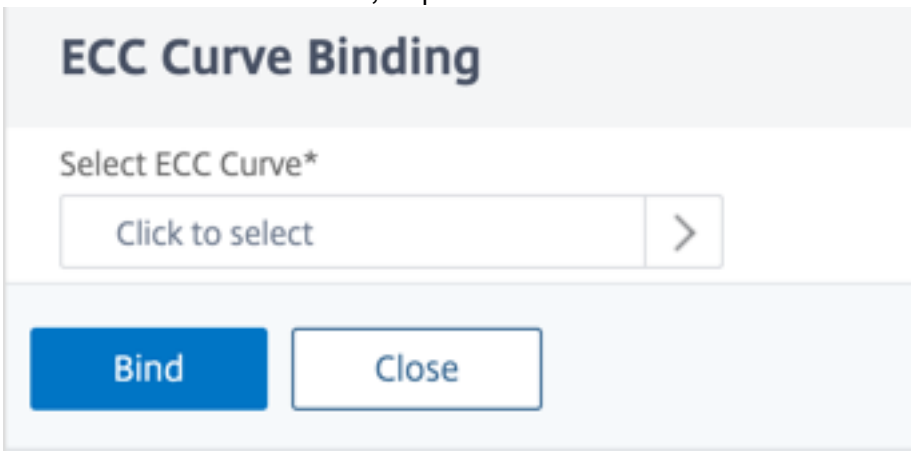
2. Sélectionnez un serveur virtuel SSL et cliquez sur **Modifier**.
3. Dans **Paramètres avancés**, cliquez sur **Courbe ECC**.



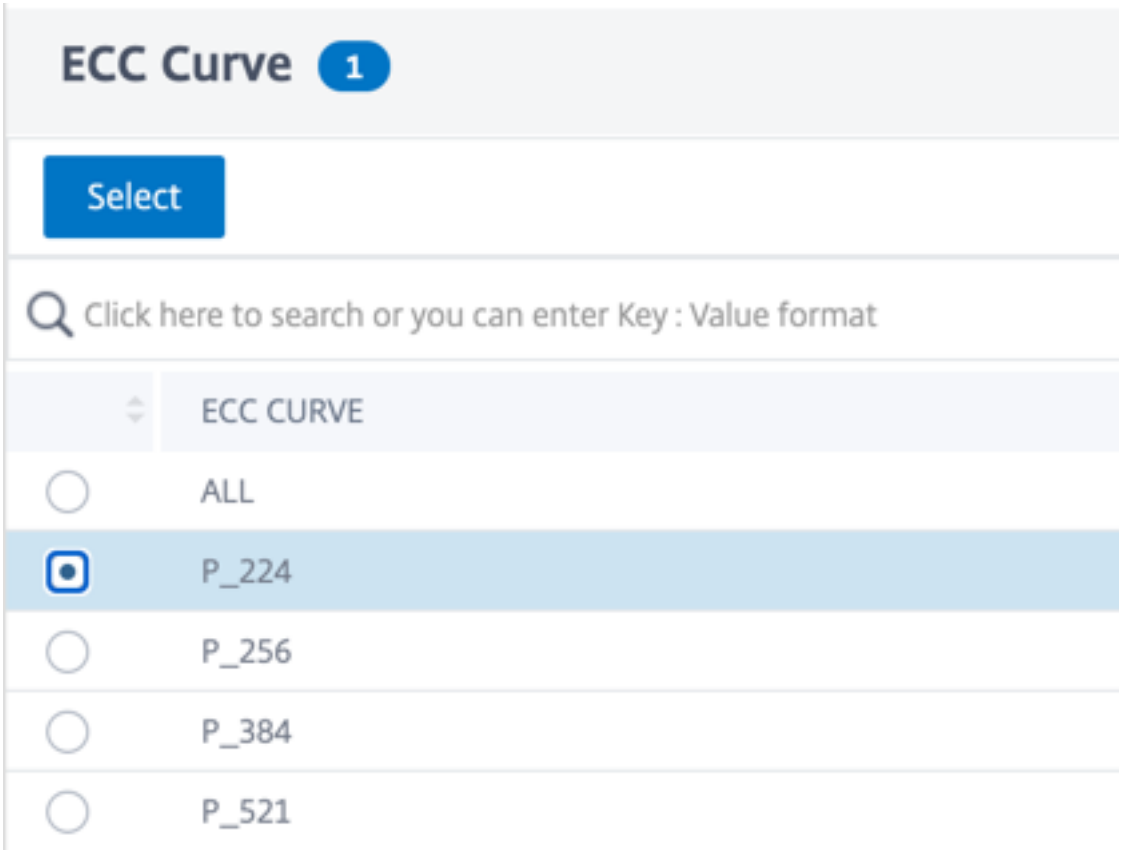
4. Cliquez à l'intérieur de la section courbe ECC.
5. Dans la page **Liaison de courbe ECC du serveur virtuel SSL**, cliquez sur **Ajouter une liaison**.



6. Dans la **liaison de courbe ECC**, cliquez sur **Sélectionner une courbe ECC**.



7. Sélectionnez une valeur, puis cliquez sur **Sélectionner**.



8. Cliquez sur **Bind**.
9. Cliquez sur **Fermer**.
10. Cliquez sur **Terminé**.

Liez des courbes ECC à un service SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind ssl service <vServerName > -eccCurveName <eccCurveName >
```

Exemple :

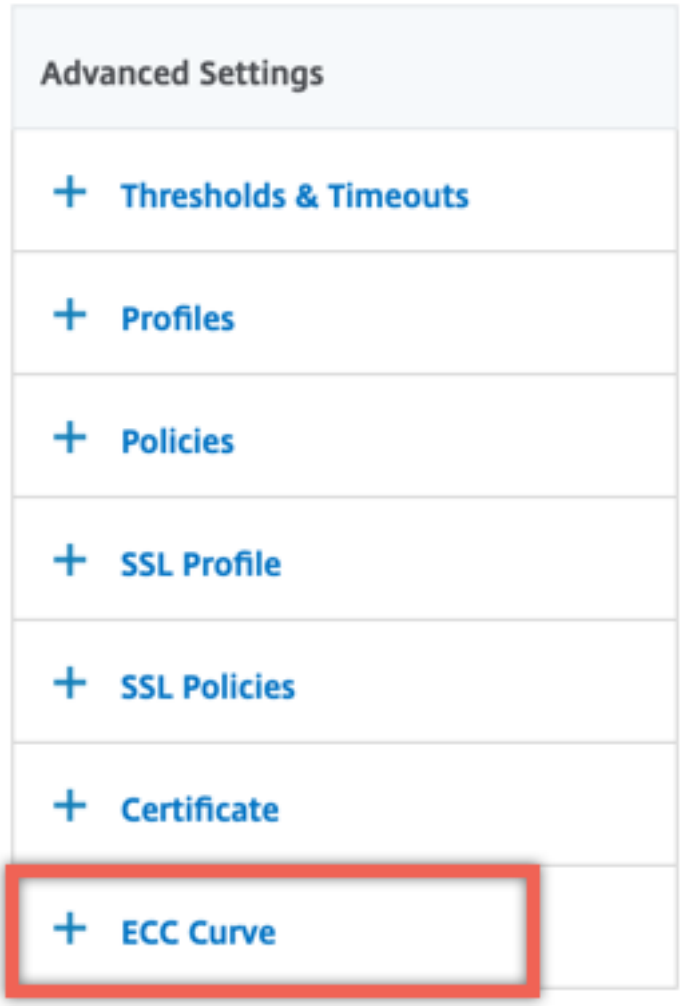
```
1  > bind ssl service sslsvc -eccCurveName P_224
2   Done
3  > sh ssl service sslsvc
4
5      Advanced SSL configuration for Back-end SSL Service sslsvc:
6      DH: DISABLED
7      DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
           DISABLED
8      Session Reuse: ENABLED      Timeout: 300 seconds
9      Cipher Redirect: DISABLED
10     ClearText Port: 0
```



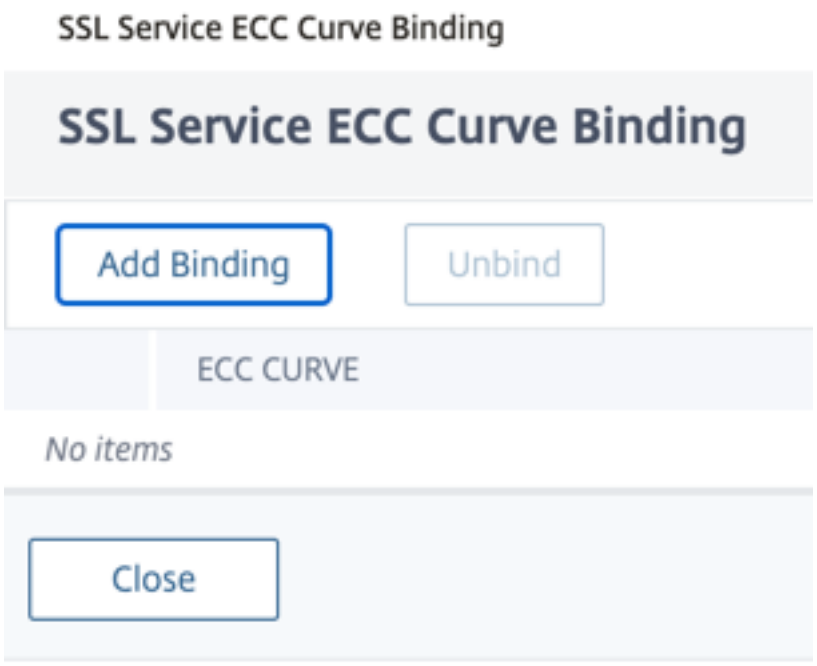
```
11      Server Auth: DISABLED
12      SSL Redirect: DISABLED
13      Non FIPS Ciphers: DISABLED
14      SNI: DISABLED
15      OCSP Stapling: DISABLED
16      SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
            ENABLED  TLSv1.3: DISABLED
17      Send Close-Notify: YES
18      Strict Sig-Digest Check: DISABLED
19      Zero RTT Early Data: ???
20      DHE Key Exchange With PSK: ???
21      Tickets Per Authentication Context: ???
22
23      ECC Curve: P_224
24
25
26  1)  Cipher Name: DEFAULT_BACKEND
27      Description: Default cipher list for Backend SSL session
28   Done
29  <!--NeedCopy-->
```

Liez des courbes ECC à un service SSL à l'aide de l'interface graphique

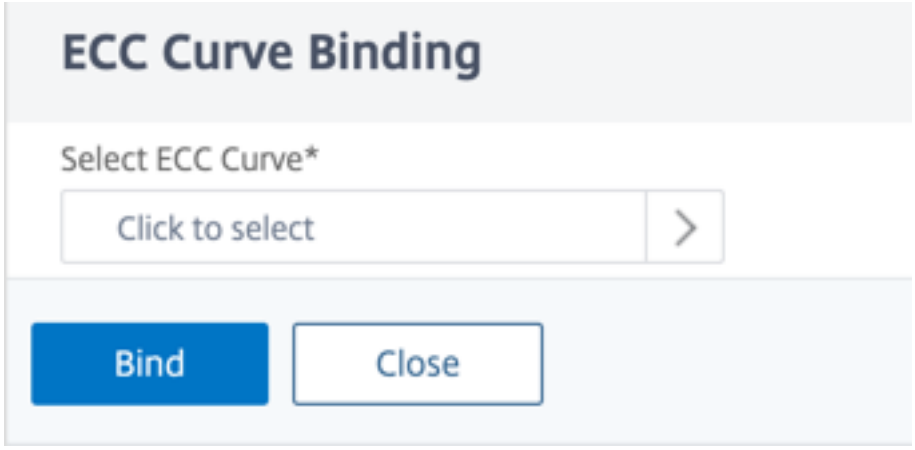
1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Sélectionnez un service SSL et cliquez sur **Modifier**.
3. Dans **Paramètres avancés**, cliquez sur **Courbe ECC**.



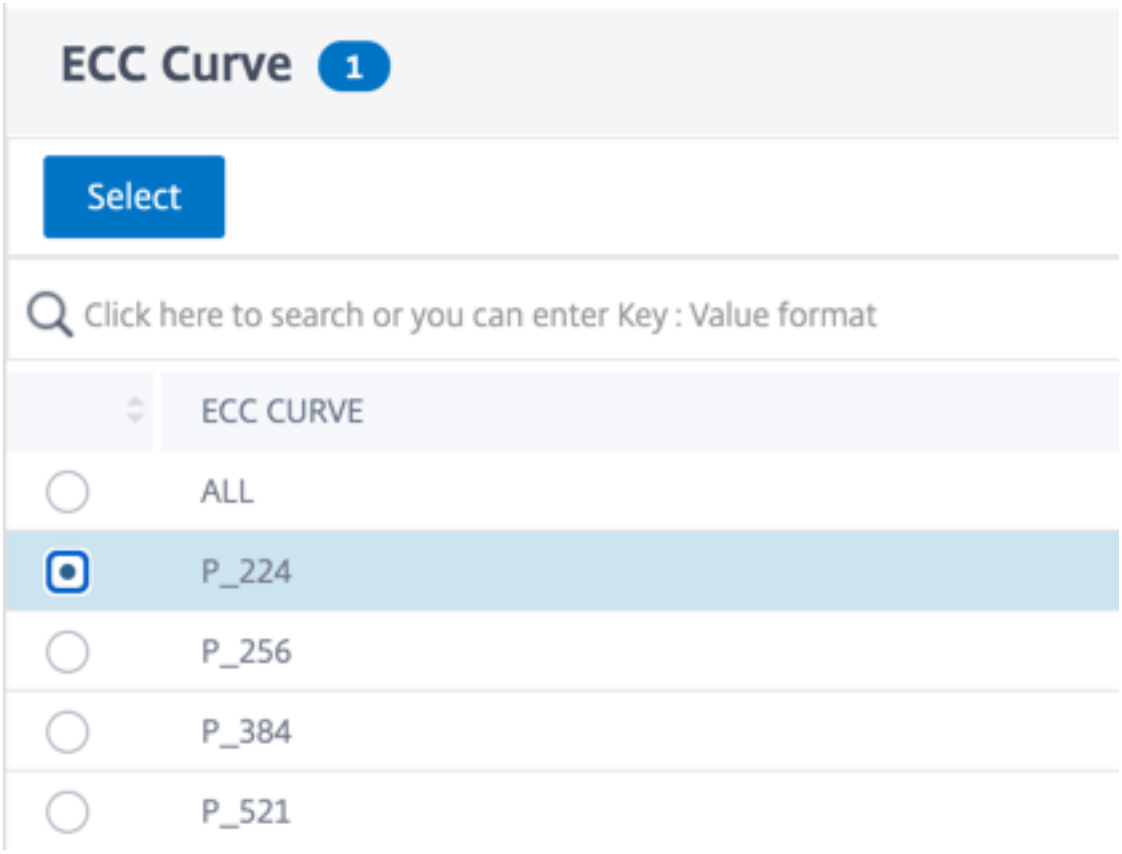
4. Cliquez à l'intérieur de la section courbe ECC.
5. Dans la page **Liaison de courbe ECC Service SSL**, cliquez sur **Ajouter une liaison**.



6. Dans la **liaison de courbe ECC**, cliquez sur **Sélectionner une courbe ECC**.



7. Sélectionnez une valeur, puis cliquez sur **Sélectionner**.



8. Cliquez sur **Bind**.
9. Cliquez sur **Fermer**.
10. Cliquez sur **Terminé**.

Génération de paramètres Diffie-Hellman et réalisation de PFS avec DHE

August 20, 2021

L'échange de clés Diffie-Hellman (DH) est un moyen pour deux parties impliquées dans une transaction SSL de s'entendre sur un secret partagé sur un canal non sécurisé. Ces parties n'ont aucune connaissance préalable les unes des autres. Ce secret peut être converti en matériau de clé cryptographique pour les algorithmes de chiffrement de clé symétrique qui nécessitent un tel échange de clés.

Cette fonction est désactivée par défaut. Configurez la fonctionnalité pour prendre en charge les chiffrements qui utilisent DH comme algorithme d'échange de clés.

> **Remarque** :
>
> La génération de paramètres DH 2048 bits peut prendre beaucoup de temps (jusqu'à 30 minutes).

Générer des paramètres DH à l'aide de la CLI

À l'invite de commandes, tapez la commande suivante :

```
create ssl dhparam <dhFile> [<bits>] [-gen (2 | 5)]
<!--NeedCopy-->
```

Exemple :

```
create ssl dhparam Key-DH-1 512 -gen 2
<!--NeedCopy-->
```

Générer des paramètres DH à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **SSL** et, dans le groupe **Outils**, sélectionnez **Créer une clé Diffie-Hellman (DH)** et **Configurer le param SSL DH**.

> **Remarque :**
>
> Pour plus d'informations sur les paramètres DH, voir Paramètres Diffie-Hellman.

Obtenir un secret avant parfait avec DHE

La génération de paramètres DH est une opération intensive en CPU. Dans les versions antérieures, la génération de paramètres, sur une appliance VPX, prenait beaucoup de temps car elle était effectuée dans le logiciel. La génération de paramètres est optimisée en définissant le `dhKeyExpSizeLimit` paramètre. Vous pouvez définir ce paramètre pour un serveur virtuel SSL ou un profil SSL, puis lier le profil à un serveur virtuel.

Vous pouvez maintenir un secret avancé parfait (PFS) sur les appliances Citrix ADC MPX en définissant le nombre de DH égal à zéro. Par conséquent, les paramètres DH sont générés pour chaque transaction (minimum `DHcount` 0) sur les appliances Citrix ADC MPX. Les paramètres sont générés sans baisse significative des performances, car l'opération est optimisée. Auparavant, le nombre minimum de DH autorisé était de 500. C'est-à-dire que vous ne pouvez pas régénérer la clé pour un maximum de 500 transactions.

Sur une appliance Citrix ADC VPX, vous pouvez générer des paramètres DH pour chaque transaction 500 au minimum (`DHcount` = 500). Si `DHcount` est égal à 0, les paramètres DH ne sont pas régénérés.

> **Limitation :**
>
> Vous ne pouvez pas atteindre PFS dans VPX aujourd'hui avec les chiffrements DH.

Optimiser la génération des paramètres DH à l'aide de la CLI

À l'invite de commandes, tapez les commandes 1 et 2, ou tapez commande 3 :

```
1. add ssl profile <name> [-sslProfileType ( BackEnd | FrontEnd )] [-dhCount <positive_integer>] [-dh ( ENABLED | DISABLED) -dhFile <string>] [-dhKeyExpSizeLimit ( ENABLED | DISABLED)]
2. set ssl vserver <vServerName> [-sslProfile <string>]
<!--NeedCopy-->
```

```
3. set ssl vserver <vServerName> [-dh ( ENABLED | DISABLED) -dhFile <string>] [-dhCount <positive_integer>] [-dhKeyExpSizeLimit ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Optimiser la génération des paramètres DH à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Activer la limite de taille d'expiration de la clé DH**.

Redirection de chiffrement

August 20, 2021

Pendant la poignée de main SSL, le client SSL (généralement un navigateur Web) annonce la suite de chiffrements qu'il prend en charge, dans l'ordre de préférence de chiffrement configuré. À partir de cette liste, le serveur SSL sélectionne ensuite un chiffrement correspondant à sa propre liste de chiffrements configurés.

Si les chiffrements annoncés par le client ne correspondent pas aux chiffrements configurés sur le serveur SSL, la connexion SSL échoue. L'échec est annoncé par un message d'erreur cryptique affiché dans le navigateur. Ces messages mentionnent rarement la cause exacte de l'erreur.

Avec la redirection de chiffrement, vous pouvez configurer un serveur virtuel SSL pour fournir des messages d'erreur précis et significatifs en cas d'échec d'une connexion SSL. En cas d'échec d'une connexion SSL, l'appliance ADC redirige l'utilisateur vers une URL configurée précédemment ou, si aucune URL n'est configurée, affiche une page d'erreur générée en interne.

Configurer la redirection de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la redirection de chiffrement et vérifier la configuration :

```
1 -  set ssl vserver <vServerName> -cipherRedirect < ENABLED | DISABLED>
     -cipherURL < URL>
2 -  show ssl vserver <vServerName>
3 <!--NeedCopy-->
```

Exemple :

```
1  set ssl vserver vs-ssl -cipherRedirect ENABLED -cipherURL http://
       redirectURl
2
3  Done
4
5  show ssl vserver vs-ssl
6
7  Advanced SSL configuration for VServer vs-ssl:
8  DH: DISABLED
9  Ephemeral RSA: ENABLED          Refresh Count: 1000
10 Session Reuse: ENABLED          Timeout: 600 seconds
11 Cipher Redirect: ENABLED        Redirect URL: http://redirectURl
12 SSLv2 Redirect: DISABLED
13 ClearText Port: 0
14 Client Auth: DISABLED
15 SSL Redirect: DISABLED
16 Non FIPS Ciphers: DISABLED
17 SNI: DISABLED
18 OCSP Stapling: DISABLED
19 HSTS: DISABLED
20 HSTS IncludeSubDomains: NO
21 HSTS Max-Age: 0
22 SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2: ENABLED
       TLSv1.2: ENABLED
23     1)      CertKey Name: Auth-Cert-1       Server Certificate
24     1)      Cipher Name: DEFAULT
25             Description: Predefined Cipher Alias
26 Done
27 <!--NeedCopy-->
```


Configurer la redirection de chiffrement à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Activer la redirection de chiffrement** et spécifiez une URL de redirection.

Utiliser le matériel et les logiciels pour améliorer les performances de chiffrement ECDHE et ECDSA

August 20, 2021

> **Remarque :**
>
> Cette amélioration s'applique uniquement aux plates-formes suivantes :
>
> - MPX/SDX 11000
> - MPX/SDX 14000
> - MPX 22000, MPX 24000 et MPX 25000
> - MPX/SDX 14000 FIPS

Auparavant, le calcul ECDHE et ECDSA sur une appliance Citrix ADC était effectué uniquement sur le matériel (puces Cavium), ce qui limitait le nombre de sessions SSL à un moment donné. Avec cette amélioration, certaines opérations sont également effectuées dans le logiciel. Autrement dit, le traitement se fait à la fois sur les puces Cavium et sur les cœurs CPU pour améliorer les performances de chiffrement ECDHE et ECDSA.

Le traitement est d'abord effectué dans le logiciel, jusqu'au seuil de crypto logiciel configuré. Une fois ce seuil atteint, les opérations sont déchargées vers le matériel. Par conséquent, ce modèle hybride utilise à la fois du matériel et des logiciels pour améliorer les performances SSL. Vous pouvez activer le modèle hybride en définissant le paramètre « SoftwareCryptoThreshold » selon vos besoins. Pour désactiver le modèle hybride, définissez ce paramètre sur 0.

Les avantages sont les plus importants si l'utilisation actuelle du processeur n'est pas trop élevée, car le seuil du processeur n'est pas exclusif au calcul ECDHE et ECDSA. Par exemple, si la charge de travail actuelle de l'appliance consomme 50% des cycles du processeur et que le seuil est défini sur 80%, le calcul ECDHE et ECDSA ne peuvent utiliser que 30%. Une fois que le seuil de crypto logiciel configuré de 80% est atteint, d'autres calculs ECDHE et ECDSA sont déchargés sur le matériel. Dans ce cas, l'utilisation réelle du processeur peut dépasser 80 %, car effectuer des calculs ECDHE et ECDSA dans le matériel consomme certains cycles CPU.

Activer le modèle hybride à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl parameter -softwareCryptoThreshold <positive_integer>

Synopsis:

softwareCryptoThreshold:

Citrix ADC CPU utilization threshold (as a percentage) beyond which
    crypto operations are not done in software. A value of zero implies
    that CPU is not utilized for doing crypto in software.

Default = 0

Min = 0

Max = 100
<!--NeedCopy-->
```

Exemple :

```
set ssl parameter - softwareCryptoThreshold 80
Done

show ssl parameter
Advanced SSL Parameters

SSL quantum size                  : 8 KB
Max CRL memory size               : 256 MB
Strict CA checks                  : NO
Encryption trigger timeout        : 100 ms
Send Close-Notify                 : YES
Encryption trigger packet c       : 45
Deny SSL Renegotiation            : ALL
Subject/Issuer Name Insertion Format : Unicode
OCSP cache size                   : 10 MB
Push flag                         : 0x0 (Auto)
Strict Host Header check for SNI enabled SSL sessions : NO
PUSH encryption trigger timeout   : 1 ms
Crypto Device Disable Limit       : 0
Global undef action for control policies : CLIENTAUTH
Global undef action for data policies : NOOP
Default profile                   : DISABLED
Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors    : NO
```



```
Disable TLS 1.1/1.2 for dynamic and VPN services : NO
Software Crypto acceleration CPU Threshold : 80
Signature and Hash Algorithms supported by TLS1.2 : ALL
<!--NeedCopy-->
```

Activer le modèle hybride à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Modifier les paramètres SSL avancés**.
2. Entrez une valeur pour le **seuil de chiffrement logiciel (%)**.

Réglez une alarme SNMP pour le taux de change ECDHE

L'échange de clés basé sur ECDHE peut entraîner la suppression des transactions par seconde sur l'appliance. À partir de la version 13.0 build 52.x, vous pouvez configurer une alarme SNMP pour les transactions basées sur ECDHE. Dans cette alarme, vous pouvez définir le seuil et les limites normales pour le taux de change ECDHE. Un nouveau compteur `nsssl_tot_sslInfo_ECDHE_Tx` est ajouté. Ce compteur est la somme de tous les compteurs de transactions ECDHE sur le front-end et le back-end de l'appliance. Lorsque l'échange de clés ECDHE franchit les limites configurées, une interruption SNMP est envoyée. Une autre interruption est envoyée lorsque la valeur est de retour à la valeur normale configurée.

Définir une alarme SNMP pour le taux de change ECDHE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set snmp alarm ECDHE-EXCHANGE-RATE -logging ( ENABLED | DISABLED ) -
    severity <severity>
 -state ( ENABLED | DISABLED ) -thresholdValue <positive_integer>  [-
     normalValue <positive_integer>] -time <secs>
<!--NeedCopy-->
```

Exemple :

```
set snmp alarm ECDHE-EXCHANGE-RATE -logging eNABLED -severity critical
    -state eNABLED -thresholdValue 100 -normalValue 50
<!--NeedCopy-->
```


ECDSA cipher suites support

August 20, 2021

Les suites de chiffrement ECDSA utilisent la cryptographie à courbe elliptique (ECC). En raison de sa taille réduite, il est utile dans les environnements où la puissance de traitement, l'espace de stockage, la bande passante et la consommation d'énergie sont limitées.

Lorsque le groupe de chiffrement ECDHE_ECDSA est utilisé, le certificat du serveur doit contenir une clé publique compatible ECDSA.

Le tableau suivant répertorie les chiffrements ECDSA pris en charge sur les appliances Citrix ADC MPX et SDX avec des puces N3, des appliances Citrix ADC VPX, MPX 5900/26000 et MPX/SDX 8900/15000.

Nom de chiffrement	Priority	Description	Algorithme d'échange de clés	Algorithme d'authentification	Algorithme de chiffrement (taille de clé)	Algorithme de code d'authentification des messages (MAC)	HexCode
TLS1-ECDHE-ECDSA-AES128-SHA	1	SSLv3	ECC-DHE	ECDSA	AES(128)	SHA1	0xc009
TLS1-ECDHE-ECDSA-AES256-SHA	2	SSLv3	ECC-DHE	ECDSA	AES(256)	SHA1	0xc00a
TLS1.2-ECDHE-ECDSA-AES128-SHA256	3	TLSv1.2	ECC-DHE	ECDSA	AES(128)	SHA-256	0xc023
TLS1.2-ECDHE-ECDSA-AES256-SHA384	4	TLSv1.2	ECC-DHE	ECDSA	AES(256)	SHA-384	0xc024

Nom de chiffrement	Priority	Description	Algorithme d'échange de clés	Algorithme d'authentification	Algorithme de chiffrement (taille de clé)	Algorithme de code d'authentification des messages (MAC)	HexCode
TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256	5	TLSv1.2	ECC-DHE	ECDSA	AES-GCM(128)	SHA-256	0xc02b
TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384	6	TLSv1.2	ECC-DHE	ECDSA	AES-GCM(256)	SHA-384	0xc02c
TLS1-ECDHE-ECDSA-RC4-SHA	7	SSLv3	ECC-DHE	ECDSA	RC4(128)	SHA1	0xc007
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	8	SSLv3	ECC-DHE	ECDSA	3DES(168)	SHA1	0xc008
TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305	9	TLSv1.2	ECC-DHE	ECDSA	CHACHA20/	AEAD	0xcca9

Sélection de certificat et chiffrement ECDSA/RSA

Vous pouvez lier simultanément les certificats de serveur ECDSA et RSA à un serveur virtuel SSL. Lorsque les certificats ECDSA et RSA sont liés au serveur virtuel, il sélectionne automatiquement

le certificat de serveur approprié à présenter au client. Si la liste de chiffrement client inclut des chiffrements RSA, mais n'inclut pas les chiffrements ECDSA, le serveur virtuel présente le certificat du serveur RSA. Si les deux chiffrements sont présents dans la liste du client, le certificat de serveur présenté dépend de la priorité de chiffrement définie sur le serveur virtuel. C'est-à-dire que si RSA a une priorité plus élevée, le certificat RSA est présenté. Si ECDSA a une priorité supérieure, le certificat ECDSA est présenté au client.

Authentification client à l'aide d'un certificat ECDSA ou RSA

Pour l'authentification client, le certificat d'autorité de certification lié au serveur virtuel peut être signé ECDSA ou RSA. L'appliance prend en charge une chaîne de certificats mixte. Par exemple, la chaîne de certificats suivante est prise en charge.

Certificat client (ECDSA) <-> Certificat CA (RSA) <-> Certificat intermédiaire (RSA) <-> Certificat racine (RSA)

Le tableau suivant présente les courbes elliptiques prises en charge sur les différentes appliances Citrix ADC avec des groupes de chiffrement ECDSA et des certificats ECDSA :

Courbes elliptiques	Plates-formes prises en charge
prime256v1	Toutes les plateformes, y compris FIPS.
secp384r1	Toutes les plateformes, y compris FIPS.
secp521r1	MPX 5900, MPX/SDX 8900, MPX/SDX 15000, MPX/SDX 26000, VPX
secp224r1	MPX 5900, MPX/SDX 8900. MPX/SDX 15000, MPX/SDX 26000, VPX

Créer une paire de clés de certificat ECDSA

Vous pouvez créer une paire de clés de certificat ECDSA directement sur une appliance Citrix ADC à l'aide de l'interface de ligne de commande ou de l'interface graphique. Auparavant, vous étiez en mesure d'installer et de lier une paire de clés de certificat ECC sur l'appliance, mais vous avez dû utiliser OpenSSL pour créer une paire de clés de certificat-clé.

Seules les courbes P_256 et P_384 sont prises en charge.

> **Remarque**
>
> Ce support est disponible sur toutes les plates-formes sauf MPX 9700/1050/12500/15500.

Pour créer une paire de clés de certificat-clé ECDSA à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
create ssl ecdsaKey <keyFile> -curve ( P_256 | P_384 ) [-keyform ( DER
    | PEM )] [-des | -des3] {
 -password  }
  [-pkcs8]
<!--NeedCopy-->
```

Exemple :

```
create ecdsaKey ec_p256.ky -curve P_256 -pkcs8
Done
create ecdsaKey ec_p384.ky -curve P_384
Done
<!--NeedCopy-->
```

Pour créer une paire de clés de certificat ECDSA à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic > SSL > Fichiers SSL > Clés**, puis cliquez sur **Créer une clé ECDSA**.
2. Pour créer une clé au format PKCS #8, sélectionnez **PKCS8**.

Configurer des groupes de chiffrement définis par l'utilisateur sur l'appliance ADC

August 20, 2021

Un groupe de chiffrement est un ensemble de suites de chiffrement que vous liez à un serveur virtuel, service ou groupe de services SSL sur l'appliance Citrix ADC. Une suite de chiffrement comprend un protocole, un algorithme d'échange de clés (Kx), un algorithme d'authentification (Au), un algorithme de cryptage (Enc) et un algorithme de code d'authentification de message (Mac). Votre appliance est livré avec un ensemble prédéfini de groupes de chiffrement. Lorsque vous créez un service SSL ou un groupe de services SSL, le groupe de chiffrement ALL y est automatiquement lié. Toutefois, lorsque vous créez un serveur virtuel SSL ou un service SSL transparent, le groupe de chiffrement DEFAULT y est automatiquement lié. En outre, vous pouvez créer un groupe de chiffrement défini par l'utilisateur et le lier à un serveur virtuel, service ou groupe de services SSL.

Remarque : si votre appliance MPX ne possède aucune licence, seul le chiffrement EXPORT est lié à votre serveur virtuel, service ou groupe de services SSL.

Pour créer un groupe de chiffrement défini par l'utilisateur, créez d'abord un groupe de chiffrement, puis vous liez des chiffrements ou des groupes de chiffrement à ce groupe. Si vous spécifiez un alias de chiffrement ou un groupe de chiffrement, tous les chiffrements de l'alias ou du groupe de chiffrement sont ajoutés au groupe de chiffrement défini par l'utilisateur. Vous pouvez également ajouter

des chiffrements individuels (suites de chiffrement) à un groupe défini par l'utilisateur. Toutefois, vous ne pouvez pas modifier un groupe de chiffrement prédéfini. Avant de supprimer un groupe de chiffrement, délier toutes les suites de chiffrement du groupe.

La liaison d'un groupe de chiffrement à un serveur virtuel, service ou groupe de services SSL ajoute les chiffrements aux chiffrements existants qui sont liés à l'entité. Pour lier un groupe de chiffrement spécifique à l'entité, vous devez d'abord délier les chiffrements ou le groupe de chiffrement lié à l'entité. Ensuite, liez le groupe de chiffrement spécifique à l'entité. Par exemple, pour lier uniquement le groupe de chiffrement AES à un service SSL, effectuez les opérations suivantes :

1. Dissociez le groupe de chiffrement par défaut ALL qui est lié par défaut au service lors de la création du service.

```
unbind ssl service <service name> -cipherName ALL
<!--NeedCopy-->
```

2. Lier le groupe de chiffrement AES au service

```
bind ssl service <Service name> -cipherName AE
<!--NeedCopy-->
```

   Si vous souhaitez lier le groupe de chiffrement DES en plus d'AES, à l'invite de commandes, tapez :

```
bind ssl service <service name> -cipherName DES
<!--NeedCopy-->
```

Remarque : Le dispositif virtuel Citrix ADC gratuit prend en charge uniquement le groupe de chiffrement DH.

Configurer un groupe de chiffrement défini par l'utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un groupe de chiffrement ou ajouter des chiffrements à un groupe précédemment créé, et vérifiez les paramètres :

```
add ssl cipher <cipherGroupName>
bind ssl cipher <cipherGroupName> -cipherName <cipherGroup/cipherName>
show ssl cipher <cipherGroupName>
<!--NeedCopy-->
```

Exemple :

```
add ssl cipher test
```



```
2
3  Done
4
5  bind ssl cipher test -cipherName ECDHE
6
7  Done
8
9  sh ssl cipher test
10
11 1)      Cipher Name: TLS1-ECDHE-RSA-AES256-SHA  Priority : 1
12 Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1   HexCode
      =0xc014
13 2)      Cipher Name: TLS1-ECDHE-RSA-AES128-SHA  Priority : 2
14 Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1   HexCode
      =0xc013
15 3)      Cipher Name: TLS1.2-ECDHE-RSA-AES-256-SHA384    Priority : 3
16 Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA-384
      HexCode=0xc028
17 4)      Cipher Name: TLS1.2-ECDHE-RSA-AES-128-SHA256    Priority : 4
18 Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA-256
      HexCode=0xc027
19 5)      Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 5
20 Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256) Mac=AEAD
      HexCode=0xc030
21 6)      Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 6
22 Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128) Mac=AEAD
      HexCode=0xc02f
23 7)      Cipher Name: TLS1-ECDHE-ECDSA-AES256-SHA        Priority : 7
24 Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=AES(256)  Mac=SHA1
      HexCode=0xc00a
25 8)      Cipher Name: TLS1-ECDHE-ECDSA-AES128-SHA        Priority : 8
26 Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=AES(128)  Mac=SHA1
      HexCode=0xc009
27 9)      Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-SHA384   Priority : 9
28 Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES(256)  Mac=SHA-384
      HexCode=0xc024
29 10)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-SHA256   Priority : 10
30 Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES(128)  Mac=SHA-256
      HexCode=0xc023
31 11)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
      Priority : 11
32 Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256) Mac=AEAD
      HexCode=0xc02c
33 12)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
      Priority : 12
```



```
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128) Mac=AEAD
   HexCode=0xc02b
13)     Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA        Priority : 13
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1   HexCode
   =0xc012
14)     Cipher Name: TLS1-ECDHE-ECDSA-DES-CBC3-SHA      Priority : 14
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=3DES(168) Mac=SHA1
   HexCode=0xc008
15)     Cipher Name: TLS1-ECDHE-RSA-RC4-SHA     Priority : 15
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=RC4(128)  Mac=SHA1   HexCode
   =0xc011
16)     Cipher Name: TLS1-ECDHE-ECDSA-RC4-SHA   Priority : 16
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=RC4(128)  Mac=SHA1
   HexCode=0xc007
17)     Cipher Name: TLS1.2-ECDHE-RSA-CHACHA20-POLY1305 Priority : 17
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=CHACHA20/POLY1305(256) Mac
   =AEAD   HexCode=0xcca8
18)     Cipher Name: TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305
   Priority : 18
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=CHACHA20/POLY1305(256)
   Mac=AEAD   HexCode=0xcca9
Done

bind ssl cipher test -cipherName TLS1-ECDHE-RSA-DES-CBC3-SHA
<!--NeedCopy-->
```

Dissocier les chiffrements d'un groupe de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier les chiffrements d'un groupe de chiffrement défini par l'utilisateur et vérifier les paramètres :

```
show ssl cipher <cipherGroupName>

unbind ssl cipher <cipherGroupName> -cipherName <string>

show ssl cipher <cipherGroupName>
<!--NeedCopy-->
```

Supprimer un groupe de chiffrement à l'aide de l'interface de ligne de commande

Remarque : Vous ne pouvez pas supprimer un groupe de chiffrement intégré. Avant de supprimer un groupe de chiffrement défini par l'utilisateur, assurez-vous que le groupe de chiffrement est vide.

À l'invite de commandes, tapez les commandes suivantes pour supprimer un groupe de chiffrement défini par l'utilisateur et vérifiez la configuration :

```
rm ssl cipher <userDefCipherGroupName> [<cipherName> ...]
show ssl cipher <cipherGroupName>

<!--NeedCopy-->
```

Exemple :

```
rm ssl cipher test Done

sh ssl cipher test ERROR: No such resource [cipherGroupName, test]
<!--NeedCopy-->
```

Configurer un groupe de chiffrement défini par l'utilisateur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Groupes de chiffrement**.
2. Cliquez sur **Ajouter**.
3. Spécifiez un nom pour le groupe de chiffrement.
4. Cliquez sur **Ajouter** pour afficher les chiffrements et groupes de chiffrement disponibles.
5. Sélectionnez un groupe de chiffrement ou de chiffrement, puis cliquez sur le bouton fléché pour les ajouter.
6. Cliquez sur **Créer**.
7. Cliquez sur **Fermer**.

Pour lier un groupe de chiffrement à un serveur virtuel, un service ou un groupe de services SSL à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des options suivantes :

```
bind ssl vserver <vServerName> -cipherName <string>

bind ssl service <serviceName> -cipherName <string>

bind ssl serviceGroup <serviceGroupName> -cipherName <string>

<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver ssl_vserver_test -cipherName test
Done
```



```
3
4 bind ssl service  nshttps -cipherName test
5 Done
6
7 bind ssl servicegroup  ssl_svc  -cipherName test
8 Done
9 <!--NeedCopy-->
```

Pour lier un groupe de chiffrement à un serveur virtuel, service ou groupe de services SSL à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

   Pour le service, remplacez les serveurs virtuels par des services. Pour les groupes de services, remplacez les serveurs virtuels par des groupes de services.

   Ouvrez le serveur virtuel, le service ou le groupe de services.

2. Dans **Advanced Settings**, sélectionnez **SSL Ciphers**.
3. Liez un groupe de chiffrement au serveur virtuel, au service ou au groupe de services.

Liaison de chiffrements individuels à un serveur virtuel SSL ou à un service

Vous pouvez également lier des chiffrements individuels, au lieu d'un groupe de chiffrement, à un serveur virtuel ou à un service.

Pour lier un chiffrement à l'aide de l'interface de ligne de commande :
à l'invite de commandes, tapez :

```
1 bind ssl vserver <vServerName> -cipherName <string>
2 bind ssl service <serviceName> -cipherName <string>
3 <!--NeedCopy-->
```

Exemple :

```
1 bind ssl vserver v1 -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
2 Done
3
4 bind ssl service sslsvc -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
5 Done
6 <!--NeedCopy-->
```

Pour lier un chiffrement à un serveur virtuel SSL à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel SSL et cliquez sur **Modifier**.

3. Dans **Advanced Settings**, sélectionnez **SSL Ciphers**.
4. Dans **Cipher Suites**, sélectionnez **Ajouter**.
5. Recherchez le chiffrement dans la liste disponible et cliquez sur la flèche pour l'ajouter à la liste configurée.
6. Cliquez sur **OK**.
7. Cliquez sur **Terminé**.

Pour lier un chiffrement à un service SSL, répétez les étapes précédentes après le remplacement du serveur virtuel par le service.

Matrice de prise en charge des certificats de serveur sur l'appliance ADC

August 20, 2021

À partir de la version 13.0 build 41.x, l'appliance Citrix ADC prend en charge les messages de certificat de serveur qui sont fragmentés en plusieurs enregistrements tant que la taille totale est inférieure à 32 Ko. Auparavant, la taille maximale prise en charge était de 16 Ko et la fragmentation n'était pas prise en charge.

L'appliance Citrix ADC prend en charge les certificats de serveur suivants.

Tableau 1 : Prise en charge des services front-end (FE) et back-end (BE)

Certificat/Plate-forme serveur	MPX/SDX (N2 CHIPS) FE	MPX/SDX (N2 CHIPS) BE	MPX/SDX (N3 CHIPS) FE	MPX/SDX (N3 CHIPS) BE	VPX FE	VPX BE
MD5	O	O	O	O	O	O
SHA1	O	O	O	O	O	O
SHA224	O	O	O	O	O	O
SHA256	O	O	O	O	O	O
SHA384	O	O	O	O	O	O
SHA512	O	O	O	O	O	O
Clé RSA	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits
Clé DH	1024 bits et 2048 bits	1024 bits et 2048 bits	1024 bits et 2048 bits	1024 bits et 2048 bits	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits

Certificat/Plateforme serveur	MPX 9700/10500/12500/15500/ FIPS avec FW 2.2 FE	MPX 9700/10500/12500/15500/ FIPS avec FW 2.2 BE	MPX/SDX 14030/14060/14080 FIPS FE	MPX/SDX 14030/14060/14080 FIPS BE
MD5	O	O	O	O
SHA1	O	O	O	O
SHA224	O	O	O	O
SHA256	O	O	O	O
SHA384	O	O	O	O
SHA512	O	O	O	O
Clé RSA	2048 bits	2048 bits	2048 bits et 3072 bits	2048 bits et 3072 bits
Clé DH	N	N	N	N

Remarque :

- Dans les versions 11.1 et antérieures, une appliance Citrix ADC prend en charge les extensions « algorithmes de signature » suivantes dans le message Hello client back-end : RSA-MD5, RSA-SHA1 et RSA-SHA256.
  Étant donné que l'appliance Citrix ADC ne prend pas en charge les extensions d'algorithmes de signature SHA 384 et SHA 512, certains serveurs, tels que les serveurs Windows IIS, réinitialisent la connexion.
- À partir de la version 12.0, une appliance Citrix ADC prend en charge toutes les extensions signature_algorithms.

Authentification client

August 20, 2021

Dans une transaction SSL typique, le client qui se connecte à un serveur via une connexion sécurisée vérifie la validité du serveur. Pour ce faire, il vérifie le certificat du serveur avant d'initier la transaction SSL. Cependant, vous pouvez parfois vouloir configurer le serveur pour authentifier le client qui se connecte à lui.

Remarque : à partir de la version 13.0 build 41.x, l'appliance Citrix ADC prend en charge les messages de demande de certificat qui sont fragmentés en plusieurs enregistrements à condition que la taille

totale soit inférieure à 32 Ko. Auparavant, la taille maximale prise en charge était de 16 Ko et la fragmentation n'était pas prise en charge.

Lorsque l'authentification client est activée sur un serveur virtuel SSL, l'appliance Citrix ADC demande le certificat client pendant la poignée de main SSL. L'appliance vérifie que le certificat présenté par le client ne présente pas de contraintes normales, telles que la signature de l'émetteur et la date d'expiration.

Remarque : pour que l'appliance vérifie les signatures de l'émetteur, le certificat de l'autorité de certification qui a émis le certificat client doit être installé sur l'appliance et lié au serveur virtuel avec lequel le client effectue des transactions.

Si le certificat est valide, l'appliance autorise le client à accéder à toutes les ressources sécurisées. Toutefois, si le certificat n'est pas valide, l'appliance supprime la demande client pendant la poignée de main SSL.

L'appliance vérifie le certificat client en formant d'abord une chaîne de certificats, en commençant par le certificat client et en se terminant par le certificat d'autorité de certification racine du client (par exemple, Verisign). Le certificat d'autorité de certification racine peut contenir un ou plusieurs certificats d'autorité de certification intermédiaire (si l'autorité de certification racine n'émet pas directement le certificat client).

Avant d'activer l'authentification client sur l'appliance Citrix ADC, assurez-vous qu'un certificat client valide est installé sur le client. Ensuite, activez l'authentification client pour le serveur virtuel qui gère les transactions. Enfin, liez le certificat de l'autorité de certification qui a émis le certificat client au serveur virtuel de l'appliance.

Remarque : Une appliance Citrix ADC MPX prend en charge une paire de clés de certificat de 512 bits à 4096 bits. Le certificat doit être signé à l'aide de l'un des algorithmes de hachage suivants :

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Sur une appliance SDX, si une puce SSL est affectée à une instance VPX, la prise en charge de la taille de paire de clés de certificat d'une appliance MPX s'applique. Sinon, la prise en charge normale de la taille de paire de clés de certificat d'une instance VPX s'applique.

Une appliance virtuelle Citrix ADC (instance VPX) prend en charge les certificats d'au moins 512 bits, jusqu'aux tailles suivantes :

- Certificat de serveur 4096 bits sur le serveur virtuel
- Certificat client 4096 bits sur le service

- Certificat d'autorité de certification 4096 bits
- Certificat 4096 bits sur le serveur physique

Remarque : à partir de la version 13.0 build 79.x, l'authentification client avec certificat client RSA 4096 bits est prise en charge lors d'une liaison SSL sur la plate-forme VPX.

Remarques :

- Pour connaître les limitations MPX FIPS, consultez Limitations MPX FIPS.
- Pour connaître les limitations SDX FIPS, reportez-vous à la section Limitations FIPS SDX.

Fournir le certificat client

Avant de configurer l'authentification client, un certificat client valide doit être installé sur le client. Un certificat client inclut des détails sur le système client spécifique qui crée des sessions sécurisées avec l'appliance Citrix ADC. Chaque certificat client est unique et doit être utilisé par un seul système client.

Que vous obteniez le certificat client d'une autorité de certification, utilisiez un certificat client existant ou génériez un certificat client sur l'appliance Citrix ADC, vous devez convertir le certificat au format correct. Sur l'appliance Citrix ADC, les certificats sont stockés au format PEM ou DER et doivent être convertis au format PKCS #12 avant d'être installés sur le système client. Après avoir converti le certificat et le transférer sur le système client, assurez-vous qu'il est installé sur ce système et configuré pour l'application cliente. L'application, telle qu'un navigateur Web, doit faire partie des transactions SSL.

Pour obtenir des instructions sur la façon de convertir un certificat du format PEM ou DER au format PKCS #12, voir Importer et convertir des fichiers SSL.

Pour obtenir des instructions sur la façon de générer un certificat client, reportez-vous à la section Créer un certificat.

Activer l'authentification basée sur le certificat client

Par défaut, l'authentification du client est désactivée sur l'appliance Citrix ADC, et toutes les transactions SSL se déroulent sans authentifier le client. Vous pouvez configurer l'authentification client pour qu'elle soit facultative ou obligatoire dans le cadre de la poignée de main SSL.

Si l'authentification du client est facultative, l'appliance demande le certificat client mais procède à la transaction SSL même si le client présente un certificat non valide. Si l'authentification du client est obligatoire, l'appliance met fin à la liaison SSL si le client SSL ne fournit pas de certificat valide.

Attention : Citrix vous recommande de définir des stratégies de contrôle d'accès appropriées avant de modifier la vérification d'authentification basée sur le certificat client en option.

Remarque : l'authentification client est configurée pour les serveurs virtuels SSL individuels, et non globalement.

Activer l'authentification basée sur le certificat client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer l'authentification basée sur le certificat client et vérifier la configuration :

```
set ssl vserver <vServerName> [-clientAuth (ENABLED | DISABLED)] [-
    clientCert (MANDATORY | OPTIONAL)]
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver vssl -clientAuth ENABLED -clientCert Mandatory
Done
show ssl vserver vssl

Advanced SSL configuration for VServer vssl:
DH: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: ENABLED Client Cert Required: Mandatory
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        OCSP Stapling: DISABLED
        HSTS: DISABLED
        HSTS IncludeSubDomains: NO
        HSTS Max-Age: 0
SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.2: ENABLED TLSv1
    .2: ENABLED

1) CertKey Name: sslckey Server Certificate

1) Policy Name: client_cert_policy Priority: 0

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
```



```
28 Done
29 <!--NeedCopy-->
```

Activer l'authentification basée sur le certificat client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans la section Paramètres SSL, sélectionnez Authentification client et, dans la liste Certificat client, sélectionnez Obligatoire.

> **Remarque :**
>
> Si l'authentification du client est définie sur obligatoire et si le certificat client contient des extensions de stratégie, la validation du certificat échoue. À partir de la version 12.0-56.x, vous pouvez définir un paramètre dans le profil SSL frontal pour ignorer cette vérification. Le paramètre est désactivé par défaut. Autrement dit, la vérification est effectuée par défaut.

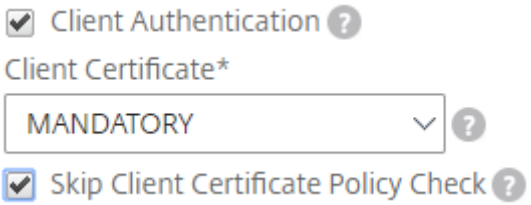
Ignorer la vérification de l'extension de stratégie lors de l'authentification du client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1  set ssl profile ns_default_ssl_profile_frontend -clientauth ENABLED -
       skipClientCertPolicyCheck ENABLED
2
3  Parameter
4
5  skipClientCertPolicyCheck
6
7                Control policy extension check, if present inside the
                     X509 certificate chain. Applicable only if client
                     authentication is enabled and client certificate is
                     set to mandatory. Possible values functions as follows
                     :
8
9  - ENABLED: Skip the policy check during client authentication.
10
11 - DISABLED: Perform policy check during client authentication.
12
13 Possible values: ENABLED, DISABLED
14
15 Default: DISABLED
16 <!--NeedCopy-->
```


Ignorer la vérification de l'extension de stratégie lors de l'authentification du client à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils > ProfilsSSL**.
2. Créez un nouveau profil frontal ou modifiez un profil frontal existant.
3. Vérifiez que l'authentification client est activée et que le certificat client est défini sur obligatoire.
4. Sélectionnez **Ignorer la vérification de stratégie de certificat client**.



Liez les certificats d'autorité de certification au serveur virtuel

Une autorité de certification dont le certificat est présent sur l'appliance Citrix ADC doit émettre le certificat client utilisé pour l'authentification client. Liez ce certificat au serveur virtuel Citrix ADC qui effectue l'authentification du client.

Liez le certificat de l'autorité de certification au serveur virtuel SSL de manière à ce que l'appliance puisse former une chaîne de certificats complète lorsqu'elle vérifie le certificat client. Sinon, la formation de la chaîne de certificats échoue et le client se voit refuser l'accès même si son certificat est valide.

Vous pouvez lier des certificats d'autorité de certification au serveur virtuel SSL dans n'importe quel ordre. L'appliance effectue l'ordre approprié lors de la vérification du certificat client.

Par exemple, si le client présente un certificat émis par **CA_A**, où **CA_A est une**autorité de certification intermédiaire dont le certificat est émis par **CA_B**, dont le certificat est à son tour émis par une autorité de certification racine approuvée, **Root_CA**, une chaîne de certificats contenant ces trois certificats doivent être liés au serveur virtuel sur l'appliance Citrix ADC.

Pour obtenir des instructions sur la liaison d'un ou de plusieurs certificats au serveur virtuel, voir Lier la paire de clés de certificat au serveur virtuel SSL.

Pour obtenir des instructions sur la création d'une chaîne de certificats, voir Créer une chaîne de certificats.

Contrôle plus strict de la validation des certificats clients

L'appliance Citrix ADC accepte les certificats d'autorité de certification intermédiaire valides si une autorité de certification racine unique les émet. C'est-à-dire que si seul le certificat Root-CA est lié au

serveur virtuel et que Root-CA valide n'importe quel certificat intermédiaire envoyé avec le certificat client, l'appliance fait confiance à la chaîne de certificats et l'établissement de liaison réussit.

Toutefois, si un client envoie une chaîne de certificats dans la négociation, aucun des certificats intermédiaires ne peut être validé à l'aide d'un répondeur CRL ou OCSP, sauf si ce certificat est lié au serveur virtuel SSL. Par conséquent, même si l'un des certificats intermédiaires est révoqué, la négociation est réussie. Dans le cadre de la poignée de main, le serveur virtuel SSL envoie la liste des certificats d'autorité de certification qui lui sont liés. Pour un contrôle plus strict, vous pouvez configurer le serveur virtuel SSL pour qu'il accepte uniquement un certificat signé par l'un des certificats d'autorité de certification liés à ce serveur virtuel. Pour ce faire, vous devez activer le paramètre **ClientAuthUseBoundCachain** dans le profil SSL lié au serveur virtuel. La connexion échoue si l'un des certificats d'autorité de certification liés au serveur virtuel n'a pas signé le certificat client.

Par exemple, deux certificats clients, clientcert1 et clientcert2, sont signés respectivement par les certificats intermédiaires Int-CA-A et Int-CA-B. Les certificats intermédiaires sont signés par le certificat racine Root-CA. Int-CA-A et Root-CA sont liés au serveur virtuel SSL. Dans le cas par défaut (ClientAuthUseBoundCAChain désactivé), clientcert1 et clientcert2 sont acceptés. Toutefois, si ClientAuthUseBoundCachain est activé, l'appliance Citrix ADC accepte uniquement clientcert1.

Activer un contrôle plus strict sur la validation des certificats client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl profile <name> -ClientAuthUseBoundCAChain Enabled
<!--NeedCopy-->
```

Activer un contrôle plus strict sur la validation du certificat client à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils**, sélectionnez l'onglet **Profils SSL** et créez un profil SSL ou sélectionnez un profil existant.
2. Sélectionnez **Activer l'authentification client à l'aide de la chaîne de certification liée**.

Authentification du serveur

August 20, 2021

Étant donné que l'appliance Citrix ADC effectue le déchargement et l'accélération SSL pour le compte d'un serveur Web, l'appliance n'authentifie généralement pas le certificat du serveur Web. Toutefois,

vous pouvez authentifier le serveur dans les déploiements nécessitant un chiffrement SSL de bout en bout.

Dans ce cas, l'appliance devient le client SSL et effectue une transaction sécurisée avec le serveur SSL. Il vérifie qu'une autorité de certification dont le certificat est lié au service SSL a signé le certificat de serveur et vérifie la validité du certificat de serveur.

Pour authentifier le serveur, activez l'authentification du serveur et liez le certificat de l'autorité de certification qui a signé le certificat du serveur au service SSL sur l'appliance ADC. Lors de la liaison du certificat, vous devez spécifier la liaison en tant qu'option d'autorité de certification.

Activer (ou désactiver) l'authentification de certificat du serveur

Vous pouvez utiliser l'interface de ligne de commande et l'interface graphique pour activer et désactiver l'authentification par certificat de serveur.

Activer (ou désactiver) l'authentification de certificat de serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer l'authentification par certificat de serveur et vérifier la configuration :

```
set ssl service <serviceName> -serverAuth ( ENABLED | DISABLED )
show ssl service <serviceName>
<!--NeedCopy-->
```

Exemple :

```
set ssl service ssl-service-1 -serverAuth ENABLED
<!--NeedCopy-->
```

```
show ssl service ssl-service-1

            Advanced SSL configuration for Back-end SSL Service ssl-
               service-1:`
            DH: DISABLED
            Ephemeral RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            Server Auth: ENABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
```



```
13     1)      Cipher Name: ALL
14             Description: Predefined Cipher Alias
15 Done
16 <!--NeedCopy-->
```

Activer (ou désactiver) l'authentification de certificat de serveur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service SSL.
2. Dans la section Paramètres SSL, sélectionnez Activer l'authentification du serveur et spécifiez un nom commun.
3. Dans Paramètres avancés, sélectionnez Certificats et liez un certificat d'autorité de certification au service.

Liez le certificat de l'autorité de certification au service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier le certificat d'autorité de certification au service et vérifier la configuration :

```
1 bind ssl service <serviceName> -certkeyName <string> -CA
2
3 show ssl service <serviceName>
4 <!--NeedCopy-->
```

Exemple :

```
1 bind ssl service ssl-service-1 -certkeyName samplecertkey -CA
2 <!--NeedCopy-->
```

```
1 show ssl service ssl-service-1
2
3             Advanced SSL configuration for Back-end SSL Service ssl-
                 service-1:
4             DH: DISABLED
5             Ephemeral RSA: DISABLED
6             Session Reuse: ENABLED          Timeout: 300 seconds
7             Cipher Redirect: DISABLED
8             SSLv2 Redirect: DISABLED
9             Server Auth: ENABLED
10            SSL Redirect: DISABLED
11            Non FIPS Ciphers: DISABLED
```



```
12              SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
13      1)      CertKey Name: samplecertkey     CA Certificate
           CRLCheck: Optional
14      1)      Cipher Name: ALL
15              Description: Predefined Cipher Alias
16  Done
17  <!--NeedCopy-->
```

Configurer un nom commun pour l'authentification de certificat de serveur

Dans le cryptage de bout en bout avec l'authentification du serveur activée, vous pouvez inclure un nom commun dans la configuration d'un service ou d'un groupe de services SSL. Le nom que vous spécifiez est comparé au nom commun dans le certificat de serveur lors d'une poignée de main SSL. Si les deux noms correspondent, la poignée de main réussit.
Si les noms communs ne correspondent pas, le nom commun spécifié pour le service ou le groupe de services est comparé aux valeurs du champ Nom alternatif de l'objet (SAN) du certificat. Si elle correspond à l'une de ces valeurs, la poignée de main réussit. Cette configuration est particulièrement utile s'il y a, par exemple, deux serveurs derrière un pare-feu et l'un des serveurs usurpent l'identité de l'autre. Si le nom commun n'est pas coché, un certificat présenté par l'un ou l'autre serveur est accepté si l'adresse IP correspond.

Remarque : seules les entrées DNS de nom de domaine, d'URL et d'ID de messagerie dans le champ SAN sont comparées.

Configurer la vérification de nom commun pour un service ou un groupe de services SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour spécifier l'authentification du serveur avec la vérification du nom commun et vérifier la configuration :

1. Pour configurer un nom commun dans un service, tapez :

```
1  set ssl service <serviceName> -commonName <string> -serverAuth
       ENABLED
2  show ssl service <serviceName>
3  <!--NeedCopy-->
```

2. Pour configurer un nom commun dans un groupe de services, tapez :

```
1  set ssl serviceGroup <serviceGroupName> -commonName <string> -
       serverAuth ENABLED
2  show ssl serviceGroup <serviceGroupName>
3  <!--NeedCopy-->
```


Exemple :

```
> set ssl service svc1 -commonName xyz.com -serverAuth ENABLED
<!--NeedCopy-->
```

```
show ssl service svc

     Advanced SSL configuration for Back-end SSL Service svc1:
     DH: DISABLED
     Ephemeral RSA: DISABLED
     Session Reuse: ENABLED Timeout: 300 seconds
     Cipher Redirect: DISABLED
     SSLv2 Redirect: DISABLED
     Server Auth: ENABLED Common Name: www.xyz.com
     SSL Redirect: DISABLED
     Non FIPS Ciphers: DISABLED
     SNI: DISABLED
     SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
    1) CertKey Name: cacert CA Certificate OCSPCheck: Optional
    1) Cipher Name: ALL
     Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Configurer la vérification de nom commun pour un service ou un groupe de services SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services** ou accédez à **Gestion du trafic > Équilibrage de charge > Groupes de services**, puis ouvrez un service ou un groupe de services.
2. Dans la section Paramètres SSL, sélectionnez Activer l'authentification du serveur et spécifiez un nom commun.

Actions et stratégies SSL

October 5, 2021

Une stratégie SSL évalue le trafic entrant et applique une action prédéfinie aux demandes qui correspondent à une règle (expression). Configurez les actions avant de créer les stratégies, afin de pouvoir spécifier une action lorsque vous créez une stratégie. Pour mettre une stratégie en vigueur, effectuez l'une des opérations suivantes :

- Liez la stratégie à un serveur virtuel sur l'appliance, afin qu'elle s'applique uniquement au trafic circulant via ce serveur virtuel.
- Liez la stratégie globalement, afin qu'elle s'applique à tout le trafic passant par l'appliance.

Les actions SSL définissent les paramètres SSL que vous pouvez appliquer aux demandes sélectionnées. Vous associez une action à une ou plusieurs stratégies. Les données des demandes ou réponses de connexion client sont comparées à une règle spécifiée dans la stratégie, et l'action est appliquée aux connexions qui correspondent à la règle (expression).

Vous pouvez configurer des stratégies classiques avec des expressions classiques et des stratégies de stratégie avancées avec des expressions de stratégie avancées pour SSL.

Remarque : Les utilisateurs qui ne sont pas expérimentés dans la configuration des stratégies au niveau de l'interface de ligne de commande trouvent généralement l'utilisation de l'utilitaire de configuration beaucoup plus facile.

Vous pouvez associer une action définie par l'utilisateur ou une action intégrée à une stratégie avancée. Les stratégies classiques autorisent uniquement les actions définies par l'utilisateur. Dans la stratégie avancée, vous pouvez également regrouper les stratégies sous une étiquette de stratégie, auquel cas elles ne sont appliquées que lorsqu'elles sont appelées à partir d'une autre stratégie.

Les actions et stratégies SSL sont couramment utilisées, notamment l'authentification client par répertoire, la prise en charge de l'accès Web Outlook et les insertions d'en-têtes SSL. Les insertions d'en-tête SSL contiennent les paramètres SSL requis par un serveur dont le traitement SSL a été déchargé vers l'appliance Citrix ADC.

Stratégies SSL

October 5, 2021

Les stratégies sur l'appliance Citrix ADC permettent d'identifier les connexions spécifiques que vous souhaitez traiter. Le traitement est basé sur les actions configurées pour cette stratégie particulière. Une fois que vous avez créé la stratégie et configuré une action pour celle-ci, vous devez effectuer l'une des opérations suivantes :

- Liez la stratégie à un serveur virtuel sur l'appliance, afin qu'elle s'applique uniquement au trafic circulant via ce serveur virtuel.
- Liez la stratégie globalement, afin qu'elle s'applique à tout le trafic passant par n'importe quel serveur virtuel configuré sur l'appliance Citrix ADC.

La fonctionnalité SSL de l'appliance Citrix ADC prend en charge les stratégies de stratégie avancée (avancées). Pour obtenir une description complète des expressions de stratégie avancées, de leur fonctionnement et de leur configuration manuelle, consultez Stratégies et expressions.

> **Remarque :**
>
> Les utilisateurs qui ne sont pas expérimentés dans la configuration des stratégies dans l'interface de ligne de commande trouvent généralement l'utilisation de l'utilitaire de configuration beaucoup plus facile.

Les stratégies SSL exigent que vous créiez une action avant de créer une stratégie, afin de pouvoir spécifier les actions lors de la création des stratégies.
Dans les stratégies de stratégie SSL Advanced, vous pouvez également utiliser les actions intégrées. Pour plus d'informations sur les actions intégrées, consultez Actions intégrées SSL et actions définies parl'utilisateur.

Stratégies de stratégie SSL Advanced

Une stratégie SSL Advanced, également connue sous le nom de stratégie avancée, définit un contrôle ou une action de données à exécuter sur les demandes. Les stratégies SSL peuvent donc être classées en tant que stratégies de contrôle et stratégies de données :

- **Politique de contrôle**. Une stratégie de contrôle utilise une action de contrôle, telle que forcer l'authentification du client.
  Remarque : Dans la version 10.5 ou ultérieure, le paramètre Refuser la renégociation SSL (DenySSLReneg) est défini, par défaut, sur ALL. Toutefois, les stratégies de contrôle, telles que CLIENTAUTH, déclenchent une négociation de renégociation. Si vous utilisez de telles stratégies, vous devez définir DenySSLReneg sur NO.
- **Politique de données**. Une stratégie de données utilise une action de données, telle que l'insertion de certaines données dans la demande.

Les éléments essentiels d'une politique sont une expression et une action. L'expression identifie les demandes sur lesquelles l'action doit être exécutée.

Vous pouvez configurer une stratégie avancée avec une action intégrée ou une action définie par l'utilisateur. Vous pouvez configurer une stratégie avec une action intégrée sans créer d'action distincte. Toutefois, pour configurer une stratégie avec une action définie par l'utilisateur, configurez d'abord l'action, puis configurez la stratégie.

Vous pouvez spécifier une action supplémentaire, appelée action UNDEF, à effectuer lorsque l'application de l'expression à une demande a un résultat non défini.

Configuration de la stratégie SSL

Vous pouvez configurer une stratégie SSL Advanced à l'aide de l'interface de ligne de commande et de l'interface graphique.

Configurer une stratégie SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ssl policy <name> -rule <expression> -Action <string> [-undefAction
    <string>] [-comment <string>]
<!--NeedCopy-->
```

Configurer une stratégie SSL à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > Stratégies** et, sous l'onglet **Stratégies**, cliquez sur *Ajouter*.

Prise en charge des stratégies SSL avec le protocole TLS1.3

À partir de la version 13.0 build 71.x et ultérieure, la prise en charge des stratégies SSL avec le protocole TLS1.3 est ajoutée. Lorsque le protocole TLSv1.3 est négocié pour une connexion, les règles de stratégie qui inspectent les données TLS reçues du client déclenchent désormais l'action configurée.

Par exemple, si la règle de stratégie suivante renvoie true, le trafic est transféré vers le serveur virtuel défini dans l'action.

```
add ssl action action1 -forward vserver2
add ssl policy pol1 -rule client.ssl.client_hello.sni.contains( "xyz" )
    -action action1
<!--NeedCopy-->
```

Limitations

- Les stratégies de contrôle ne sont pas prises en charge.
- Les actions suivantes ne sont pas prises en charge :
  - DOCLIENTAUTH
  - NOCLIENTAUTH
  - caCertGrpName
  - Vérification du certificat client
  - ssllogProfile

Actions intégrées SSL et actions définies par l'utilisateur

August 20, 2021

À moins que vous n'ayez besoin que des actions intégrées dans vos stratégies, vous devez créer les actions avant de créer les stratégies. Ensuite, vous pouvez spécifier les actions lorsque vous créez les stratégies. Les actions intégrées sont de deux types, les actions de contrôle et les actions de données. Vous utilisez des actions de contrôle dans les stratégies de contrôle et des actions de données dans les stratégies de données.

Les actions de contrôle intégrées sont les suivantes :

- DOCLIENTAUTH : effectue l'authentification du certificat client. (Non pris en charge pour TLS1.3)
- NOCLIENTAUTH : n'effectuez pas d'authentification de certificat client. (Non pris en charge pour TLS1.3)

Les actions de données intégrées sont les suivantes :

- Réinitialiser : fermez la connexion en envoyant un paquet RST au client.
- DROP : dépose tous les paquets du client. La connexion reste ouverte jusqu'à ce que le client la ferme.
- NOOP : transmet le paquet sans effectuer aucune opération sur celui-ci.

Remarque : Toutes les actions dépendantes de l'authentification client, telles que ClientCertVerification et SSLLogProfile, ne sont pas prises en charge par le protocole TLS 1.3.

Vous pouvez créer des actions de données définies par l'utilisateur. Si vous activez l'authentification client, vous pouvez créer une action SSL pour insérer des données de certificat client dans l'en-tête de la demande avant de transférer la demande au serveur Web.

Si une évaluation de stratégie donne lieu à un état non défini, une action du Fonds des Nations Unies pour le développement (UNDEF) est exécutée. Pour une stratégie de données ou une stratégie de contrôle, vous pouvez spécifier RESET, DROP ou NOOP comme action UNDEF. Pour une stratégie de contrôle, vous avez également la possibilité de spécifier DOCLIENTAUTH ou NOCLIENTAUTH.

Exemples d'actions intégrées dans une stratégie

Dans l'exemple suivant, si le client envoie un chiffrement autre qu'un chiffrement de catégorie EXPORT, l'appliance Citrix ADC demande l'authentification du client. Le client doit fournir un certificat valide pour une transaction réussie.

```
1 add ssl policy pol1 -rule CLIENT.SSL.CIPHER_EXPORTABLE.NOT -reqAction
     DOCLIENTAUTH
2 <!--NeedCopy-->
```

Les exemples suivants supposent que l'authentification client est activée.

Si la version du certificat fourni par l'utilisateur correspond à la version de la stratégie, aucune action n'est effectuée et le paquet est transféré :


```
1 add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
     reqAction NOOP
2 <!--NeedCopy-->
```

Si la version du certificat fourni par l'utilisateur correspond à la version de la stratégie, la connexion est supprimée :

```
1 add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
     reqAction DROP
2 <!--NeedCopy-->
```

Si la version du certificat fourni par l'utilisateur correspond à la version de la stratégie, la connexion est réinitialisée :

```
1 add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
     reqAction RESET
2 <!--NeedCopy-->
```

Vérification du certificat client avec authentification client basée sur des stratégies

Vous pouvez définir la vérification du certificat client sur obligatoire ou option lorsque vous avez configuré l'authentification client basée sur une stratégie. La valeur par défaut est obligatoire.

Définir la vérification du certificat client sur facultative à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add ssl action <name> ((-clientAuth ( DOCLIENTAUTH | NOCLIENTAUTH ) [-
     clientCertVerification ( Mandatory | Optional )]
2 <!--NeedCopy-->
```

Exemple :

```
1 add ssl action sslact -clientauth DOCLIENTAUTH -clientcertverification
     OPTIONAL
2 <!--NeedCopy-->
```

Définir la vérification du certificat client sur facultative à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Stratégies**.

2. Sous l'onglet **Actions SSL**, cliquez sur **Ajouter** .
3. Spécifiez un nom et dans la liste **Vérification du certificat client**, sélectionnez **Facultatif**.

Actions SSL définies par l'utilisateur

En plus des actions intégrées, vous pouvez également configurer d'autres actions SSL en fonction de votre déploiement. Ces actions sont appelées actions définies par l'utilisateur.

Configurer une action SSL définie par l'utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une action et vérifier la configuration :

```
add SSL action <name> -clientAuth(DOCLIENTAUTH | NOCLIENTAUTH) -
    clientCert (ENABLED | DISABLED) certHeader <string> -clientHeader <
    string> -clientCertSerialNumber (ENABLED | DISABLED) -
    certSerialHeader <string> -clientCertSubject (ENABLED | DISABLED) -
    certSubjectHeader <string> -clientCertHash (ENABLED | DISABLED) -
    certHashHeader <string> -clientCertIssuer (ENABLED | DISABLED) -
    certIssuerHeader <string> -sessionID (ENABLED | DISABLED) -
    sessionIDheader <string> -cipher (ENABLED | DISABLED) -cipherHeader
    <string> -clientCertNotBefore (ENABLED | DISABLED) -
    certNotBeforeHeader <string> -clientCertNotAfter (ENABLED | DISABLED
    ) -certNotAfterHeader <string> -OWASupport (ENABLED | DISABLED)
<!--NeedCopy-->
```

```
show ssl action [<name>]
<!--NeedCopy-->
```

Exemple :

```
add ssl action Action-SSL-ClientCert -clientCert ENABLED -certHeader "X
    -Client-Cert"
<!--NeedCopy-->
```

```
show ssl action Action-SSL-ClientCert

1)      Name: Action-SSL-ClientCert
        Data Insertion Action:
        Cert Header: ENABLED            Cert Tag: X-Client-Cert
Done
<!--NeedCopy-->
```


Configurer une action SSL définie par l'utilisateur à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > Stratégies** et, sous l'onglet **Actions**, cliquez sur **Ajouter**.

Configurer une action SSL pour transférer le trafic client vers un autre serveur virtuel

Les administrateurs peuvent configurer une action SSL pour transférer le trafic client reçu sur un serveur virtuel SSL vers un autre serveur virtuel afin d'éviter le déchargement SSL. Ou pour mettre fin à la connexion sur l'appliance ADC. Ce serveur virtuel peut être du type : SSL, TCP ou SSL_BRIDGE. Par exemple, les administrateurs peuvent choisir de transférer la demande à un autre serveur virtuel pour une action supplémentaire au lieu de mettre fin à la connexion dans l'un des cas suivants :

- L'appliance ne possède pas de certificat.
- L'appliance ne prend pas en charge un chiffrement spécifique.

Pour atteindre ce qui précède, un nouveau point de liaison 'CLIENTHELLO_REQ' est ajouté pour évaluer le trafic client lorsqu'un client Hello est reçu. Si la stratégie liée au serveur virtuel recevant le trafic client est évaluée à true après avoir analysé le client hello, le trafic est transféré à un autre serveur virtuel. Si ce serveur virtuel est de type SSL, il effectue la poignée de main. Si ce serveur virtuel est de type TCP ou SSL_BRIDGE, le serveur principal effectue la liaison.

Dans la version 12.1-49.x, seules les actions de transfert et de réinitialisation sont prises en charge pour le point de liaison CLIENTHELLO_REQ. Les préfixes d'expression suivants sont disponibles :

- CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXCODE
- CLIENT.SSL.CLIENT_HELLO.CLIENT_VERSION
- CLIENT.SSL.CLIENT_HELLO.IS_RENEGOTIATE
- CLIENT.SSL.CLIENT_HELLO.IS_REUSE
- CLIENT.SSL.CLIENT_HELLO.IS_SCSV
- CLIENT.SSL.CLIENT_HELLO.IS_SESSION_TICKET
- CLIENT.SSL.CLIENT_HELLO.LENGTH
- CLIENT.SSL.CLIENT_HELLO.SNI
- CLIENT.SSL.CLIENT_HELLO.ALPN.HAS_NEXTPROTOCOL (à partir de la version 13.0 build 61.x)

Pour obtenir une description de ces préfixes, voir Expressions de stratégie avancées : analyse SSL.

Un paramètre `forward` est ajouté à la commande `add SSL action` et un nouveau point de liaison `CLIENTHELLO_REQ` est ajouté à la commande `bind ssl vserver`.

Configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add ssl action <name> -forward <virtual server name>
2
```



```
3 add ssl policy <name> -rule <expression> -action <string>
4
5 bind ssl vserver <vServerName> -policyName <string> -priority <
     positive_integer> -type <type>
6 <!--NeedCopy-->
```

EXEMPLE :

```
1 add ssl action act1 -forward v2
2
3 add ssl policy pol1 -rule client.ssl.client_hello.ciphers.has_hexcode(0
     x002f) -action act1
4
5 bind ssl vserver v1 -policyName pol1 -priority 1 -type CLIENTHELLO_REQ
6 <!--NeedCopy-->
```

Configuration à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > Stratégies**.

Créer une action SSL :

1. Dans **Actions SSL**, cliquez sur **Ajouter**.
2. Dans **Créer une action SSL**, spécifiez un nom pour l'action.
3. Dans **Serveur virtuel Action de transfert**, sélectionnez un serveur virtuel existant ou ajoutez un nouveau serveur virtuel vers lequel transférer le trafic.
4. Vous pouvez également définir d'autres paramètres.
5. Cliquez sur **Créer**.

Créer une stratégie SSL :

1. Dans **Stratégies SSL**, cliquez sur **Ajouter**.
2. Dans **Créer une stratégie SSL**, spécifiez un nom pour la stratégie.
3. Dans **Action**, sélectionnez l'action que vous avez créée précédemment.
4. Dans **Expression Editor**, entrez la règle à évaluer.
5. Cliquez sur **Créer**.

Créez ou ajoutez un serveur virtuel et une stratégie de liaison :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Ajoutez ou sélectionnez un serveur virtuel.
3. Dans **Paramètres avancés**, cliquez sur **Stratégies SSL**.
4. Cliquez dans la section Stratégie SSL.
5. Dans **Sélectionner une stratégie**, sélectionnez la stratégie que vous avez créée précédemment.

6. Dans **Liaison de stratégie**, spécifiez une priorité pour la stratégie.
7. Dans **Type**, sélectionnez **CLIENTHELLO_REQ**.
8. Cliquez sur **Bind**.
9. Cliquez sur **Terminé**.

Pour connaître la configuration de bout en bout pour les cas d'utilisation les plus courants, consultez les rubriques suivantes :

- Configurez l'action SSL pour transférer le trafic client si l'appliance ne possède pas de certificat SNI (spécifique au domaine).
- Configurez une action SSL pour transférer le trafic client en fonction du protocole dans l'extension ALPN du message Hello du client.
- Configurez l'action SSL pour transférer le trafic client si un chiffrement n'est pas pris en charge sur ADC.

Action SSL pour sélectionner sélectivement des autorités de certification basées sur SNI pour l'authentification du client

Vous pouvez envoyer uniquement la liste des autorités de certification basées sur SNI (domaine) dans la demande de certificat client plutôt que la liste de toutes les autorités de certification liées à un serveur virtuel SSL. Par exemple, lorsqu'un client Hello est reçu, seuls les certificats d'autorité de certification basés sur l'expression de stratégie SSL (par exemple, SNI) sont envoyés. Pour envoyer un ensemble spécifique de certificats, vous devez créer un groupe de certificats d'autorité de certification. Ensuite, lier ce groupe à une action SSL et lier l'action à une stratégie SSL. Si la stratégie liée au serveur virtuel recevant le trafic client est évaluée à true après avoir analysé le client Hello, seul un groupe de certificats d'autorité de certification spécifique est envoyé dans le certificat de demande client.

Auparavant, vous deviez lier des certificats d'autorité de certification à un serveur virtuel SSL. Avec cette amélioration, vous pouvez simplement ajouter des groupes de certificats CA et les associer à une action SSL.

Remarque : activez l'authentification client et SNI sur le serveur virtuel SSL. Liez les certificats SNI corrects au serveur virtuel.

Procédez comme suit :

1. Ajoutez un groupe de certificats d'autorité de certification.
2. Ajoutez des paires de clés de certificat.
3. Liez les paires de clés de certificat à ce groupe.
4. Ajoutez une action SSL.

5. Ajoutez une stratégie SSL. Spécifiez l'action dans la stratégie.
6. Liez la stratégie à un serveur virtuel SSL. Spécifiez le point de liaison comme CLIENTHELLO_REQ.

Configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes dans une séquence :

```
add ssl caCertGroup <caCertGroupName>
add ssl certkey <certkey_name> -cert <cert> -key <key>
bind ssl caCertGroup <caCertGroupName> <certkey_name>
add ssl action <name> -caCertGrpName <string>
add ssl policy <name> -rule <expression> -action <string>
bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type CLIENTHELLO_REQ
<!--NeedCopy-->
```

Exemple :

```
add ssl cacertGroup ca_cert_group

add ssl certkey ca_certkey1 -cert cacert1 -key cakey1
add ssl certkey ca_certkey2 -cert cacert2 -key cakey2
add ssl certkey snicert -cert snicert -key snikey

bind ssl cacertGroup ca_cert_group ca_certkey1
bind ssl caCertGroup ca_cert_group ca_certkey2
<!--NeedCopy-->
```

```
sh ssl caCertGroup ca_cert_group

CA GROUP NAME:     ca_cert_group
ACTIONS REFERRING: 1

1) CertKey Name: ca_certkey1   CA Certificate   CRLCheck: Optional
   CA_Name Sent
2) CertKey Name: ca_certkey2   CA Certificate   CRLCheck: Optional
   CA_Name Sent
<!--NeedCopy-->
```

```
add ssl action pick_ca_group -cacertGrpName ca_cert_group
<!--NeedCopy-->
```



```
sh ssl action pick_ca_group
1) Name: pick_ca_group
   Type: Data Insertion
   PickCaCertGroup: ca_cert_group
   Hits: 0
   Undef Hits: 0
   Action Reference Count: 1
<!--NeedCopy-->
```

```
add ssl policy snipolicy -rule client.ssl.client_hello.sni.contains("
    abc") -action pick_ca_group
bind ssl vserver v_SSL -policyName snipolicy -type CLIENTHELLO_REQ -
    priority 10
<!--NeedCopy-->
```

```
sh ssl policy snipolicy
    Name: snipolicy
    Rule: client.ssl.client_hello.sni.contains("abc")
    Action: pick_ca_group
    UndefAction: Use Global
    Hits: 0
    Undef Hits: 0


    Policy is bound to following entities
1)  Bound to: CLIENTHELLO_REQ VSERVER v_SSL
    Priority: 10
<!--NeedCopy-->
```

```
set ssl vserver v_SSL -clientauth ENABLED -SNIEnable ENABLED
bind ssl vserver v_SSL -certkeyName snicert -sniCert
<!--NeedCopy-->
```

```
sh ssl vserver v_SSL

    Advanced SSL configuration for VServer v_SSL:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED   Ephemeral RSA:
       ENABLED   Refresh Count: 0
    Session Reuse: ENABLED   Timeout: 120 seconds
    Cipher Redirect: DISABLED
    SSLv2 Redirect: DISABLED
    ClearText Port: 0
```



```
10      Client Auth: ENABLED   Client Cert Required: Mandatory
11      SSL Redirect: DISABLED
12      Non FIPS Ciphers: DISABLED
13      SNI: ENABLED
14      OCSP Stapling: DISABLED
15      HSTS: DISABLED
16      HSTS IncludeSubDomains: NO
17      HSTS Max-Age: 0
18      SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED
             TLSv1.2: ENABLED  TLSv1.3: DISABLED
19      Push Encryption Trigger: Always
20      Send Close-Notify: YES
21      Strict Sig-Digest Check: DISABLED
22      Zero RTT Early Data: DISABLED
23      DHE Key Exchange With PSK: NO
24      Tickets Per Authentication Context: 1
25
26      ECC Curve: P_256, P_384, P_224, P_521
27
28  1)  CertKey Name: snicert   Server Certificate for SNI
29
30
31      Data policy
32  1)  Policy Name: snipolicy  Priority: 10
33
34
35
36  1)  Cipher Name: DEFAULT
37      Description: Default cipher list with encryption strength >= 128bit
38  <!--NeedCopy-->
```

Configuration à l'aide de l'interface graphique

Créez un groupe de certificats d'autorité de certification et liez des certificats au groupe :

1. Accédez à **Gestion du trafic > SSL > Groupe de certificats CA**.
2. Cliquez sur **Ajouter** et spécifiez un nom pour le groupe.
3. Cliquez sur **Créer**.
4. Sélectionnez le **groupe de certificats de l'autorité** de certification, puis cliquez sur **Afficher les liaisons**.
5. Cliquez sur **Bind**.
6. Dans la page **Liaison de certificat de l'autorité** de certification, sélectionnez un certificat existant ou cliquez sur Ajouter pour ajouter un nouveau certificat.

7. Cliquez sur **Sélectionner**, puis sur **Lier**.
8. Pour lier un autre certificat, répétez les étapes 5 à 7.
9. Cliquez sur **Fermer**.

Accédez à **Gestion du trafic > SSL > Stratégies**.

Créer une action SSL :

1. Dans **Actions SSL**, cliquez sur **Ajouter**.
2. Dans **Créer une action SSL**, spécifiez un nom pour l'action.
3. Dans **Serveur virtuel Action de transfert**, sélectionnez un serveur virtuel existant ou ajoutez un serveur virtuel vers lequel transférer le trafic.
4. Vous pouvez également définir d'autres paramètres.
5. Cliquez sur **Créer**.

Créer une stratégie SSL :

1. Dans **Stratégies SSL**, cliquez sur **Ajouter**.
2. Dans **Créer une stratégie SSL**, spécifiez un nom pour la stratégie.
3. Dans **Action**, sélectionnez l'action créée précédemment.
4. Dans **Expression Editor**, entrez la règle à évaluer.
5. Cliquez sur **Créer**.

Créez ou ajoutez un serveur virtuel et une stratégie de liaison :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Ajoutez ou sélectionnez un serveur virtuel.
3. Dans **Paramètres avancés**, cliquez sur **Stratégies SSL**.
4. Cliquez dans la section Stratégie SSL.
5. Dans **Sélectionner une stratégie**, sélectionnez la stratégie que vous avez créée précédemment.
6. Dans **Liaison de stratégie**, spécifiez une priorité pour la stratégie.
7. Dans **Type**, sélectionnez **CLIENTHELLO_REQ**.
8. Cliquez sur **Bind**.
9. Cliquez sur **Terminé**.

Dissocier un groupe de certificats d'autorité de certification à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Groupe de certificats CA**.
2. Sélectionnez un groupe de certificats et cliquez sur **Afficher les liaisons**.
3. Sélectionnez le certificat à supprimer du groupe et cliquez sur **Dissocier**.
4. Si vous êtes invité à confirmer, cliquez sur **Oui••.
5. Cliquez sur **Fermer**.

Supprimer un groupe de certificats d'autorité de certification à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Groupe de certificats CA**.
2. Sélectionnez un groupe de certificats et cliquez sur **Supprimer**.
3. Si vous y êtes invité, cliquez sur **Oui**.

Liaison de stratégie SSL

August 20, 2021

Vous pouvez lier des stratégies SSL globalement ou à un serveur virtuel de type SSL uniquement. Les stratégies liées globalement sont évaluées après l'évaluation de toutes les stratégies liées aux services, aux serveurs virtuels ou à d'autres points de liaison Citrix ADC. Si les données entrantes correspondent à l'une des règles configurées dans la stratégie SSL, la stratégie est déclenchée et l'action qui y est associée est exécutée.

Lorsque vous liez une stratégie SSL à un serveur virtuel, vous devez sélectionner l'un des points de liaison suivants :

- REQUEST (point de liaison par défaut. L'évaluation de la stratégie est effectuée dans la couche HTTP une fois la poignée de main SSL terminée.)
- INTERCEPT_REQ (Cette option s'applique à une configuration de Citrix Secure Web Gateway. Pour plus d'informations, voir Infrastructure de stratégies SSL pour l'interceptionSSL).
- CLIENTHELLO_REQ

De même, lorsque vous dissociez une stratégie d'un serveur virtuel, vous devez spécifier le point de liaison.

Si vous spécifiez CLIENTHELLO_REQ comme point de liaison, la stratégie est évaluée lorsqu'un message de bonjour client est reçu. Les actions autorisées sont RESET, FORWARD et `caCertGrpName`. L'action de réinitialisation met fin à la connexion. L'action de transfert transfère la demande à un serveur virtuel d'équilibrage de charge pour traitement. L'action `caCertGrpName` sélectionne les autorités de certification basées sur SNI pour l'authentification du client. Pour plus d'informations sur les actions SSL, consultez Actions intégrées SSL et actions définies parl'utilisateur.

Remarque : L'action cacertgrpName n'est pas prise en charge avec le protocole TLS 1.3.

Liez une stratégie SSL globalement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour lier une stratégie SSL globale et vérifier la configuration :


```
bind ssl global - policyName <string> [- priority <positive_integer>]
show ssl global
<!--NeedCopy-->
```

Exemple :

```
bind ssl global -policyName Policy-SSL-2 -priority 90
Done

sh ssl global

     1) Name: Policy-SSL-2 Priority: 90
     2) Name: Policy-SSL-1 Priority: 100
     Done
<!--NeedCopy-->
```

Liez une stratégie SSL globalement à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Stratégies**.
2. Dans le volet d'informations, cliquez sur **Liaisons globales**.
3. Dans la boîte de dialogue **Bind/Unbind SSL Policies to Global**, cliquez sur **Insert Policy**.
4. Dans la liste **Nom de la stratégie**, sélectionnez une stratégie.
5. Le cas échéant, faites glisser l'entrée vers un nouveau poste dans la banque de stratégies pour mettre à jour automatiquement le niveau de priorité.
6. Cliquez sur **OK**. Un message apparaît dans la barre d'état indiquant que la stratégie a été liée avec succès.

Liez ou dissociez une stratégie SSL à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour lier une stratégie SSL à un serveur virtuel et vérifier la configuration :

```
bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type <type>

unbind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type <type>

<!--NeedCopy-->
```

Exemple :


```
bind ssl vserver v1 -policyName pol1 -priority 1 -type CLIENTHELLO_REQ
<!--NeedCopy-->
```

```
unbind ssl vserver v1 -policyName pol1 -priority 1 -type
   CLIENTHELLO_REQ
<!--NeedCopy-->
```

```
show ssl vserver vs-server

Advanced SSL configuration for VServer vs-server:

DH: DISABLED

Ephemeral RSA: ENABLED          Refresh Count: 1000

Session Reuse: ENABLED          Timeout: 120 seconds

Cipher Redirect: DISABLED

SSLv2 Redirect: DISABLED

ClearText Port: 80

Client Auth: DISABLED

SSL Redirect: ENABLED

SSL-REDIRECT Port Rewrite: ENABLED

Non FIPS Ciphers: DISABLED

SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      Policy Name: ssl-policy-1        Priority: 10

1)      Cipher Name: DEFAULT

            Description: Predefined Cipher Alias

Done
<!--NeedCopy-->
```


Liez une stratégie SSL à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel SSL.
2. Dans **Paramètres avancés**, sélectionnez **Stratégie SSL**. Cliquez dans la section **Stratégie SSL** pour lier une stratégie au serveur virtuel.
3. Dans la page **Liaison de stratégie**, sélectionnez une stratégie existante ou ajoutez une nouvelle stratégie.
4. Spécifiez la priorité et le type (point de liaison) de la stratégie.
5. Sélectionnez **Lier**.
6. Sélectionnez **Terminé**.

Étiquettes de stratégie SSL

August 20, 2021

Les étiquettes de stratégie sont des détenteurs de stratégies. Une étiquette de stratégie aide à gérer un groupe de stratégies, appelé banque de stratégies, qui peut être invoquée à partir d'une autre stratégie. Les étiquettes de stratégie SSL peuvent être des étiquettes de contrôle ou des étiquettes de données, selon le type de stratégies incluses dans l'étiquette de stratégie. Vous pouvez ajouter uniquement des stratégies de données dans une étiquette de stratégie de données et uniquement des stratégies de contrôle dans une étiquette de stratégie de contrôle. Pour créer la banque de stratégies, liez les stratégies à l'étiquette et spécifiez l'ordre d'évaluation de chaque stratégie par rapport aux autres dans la banque de stratégies pour l'étiquette de stratégie. Dans l'interface de ligne de commande, vous entrez deux commandes pour créer une étiquette de stratégie et lier des stratégies à l'étiquette de stratégie. Dans l'utilitaire de configuration, vous sélectionnez des options dans une boîte de dialogue.

Remarque : les étiquettes de stratégie du contrôle de type ne sont pas prises en charge avec le protocole TLS 1.3.

Créez une étiquette de stratégie SSL et liez des stratégies à l'étiquette à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ssl policylabel <labelName> -type ( CONTROL | DATA )

bind ssl policylabel <labelName> <policyName> <priority> [<
    gotoPriorityExpression>] [-invoke (<labelType> <labelName>) ]
<!--NeedCopy-->
```


Exemple :

```
add ssl policylabel cpl1 -type CONTROL

add ssl policylabel dpl1 -type DATA

bind ssl policylabel cpl1 -policyName ctrlpol -priority 1

bind ssl policylabel dpl1 -policyName datapol -priority 1
<!--NeedCopy-->
```

Configurer une étiquette de stratégie SSL et lier des stratégies à l'étiquette à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > Étiquettes de stratégie**et configurez une étiquette de stratégie SSL.

Journalisation SSL sélective

August 20, 2021

Dans un déploiement important comprenant des milliers de serveurs virtuels, toutes les informations relatives au SSL sont enregistrées. Auparavant, il n'était pas facile de filtrer l'authentification client et les succès et échecs de la poignée de main SSL pour quelques serveurs virtuels critiques. Parcourez tout le journal pour obtenir cette information a été une tâche fastidieuse et fastidieuse car l'infrastructure n'offrait pas le contrôle de filtrer les journaux. Vous pouvez désormais consigner des informations relatives à SSL dans`ns.log`, pour un serveur virtuel spécifique ou pour un groupe de serveurs virtuels. Ces informations sont particulièrement utiles pour les échecs de débogage. Pour consigner ces informations, vous devez ajouter un profil de journal SSL.

Voir l'exemple de sortie ns.log pour une authentification client réussie à la fin de cette page.

Important : définissez le niveau du journal syslog sur DEBUG. À l'invite de commandes, tapez :

```
set audit syslogParams -logLevel DEBUG
```

Profil du journal SSL

Un profil de journal SSL permet de contrôler la journalisation des événements suivants pour un serveur virtuel ou un groupe de serveurs virtuels :

- Succès et échecs de l'authentification du client, ou seulement échecs.

- SSL succès et échecs de la poignée de main, ou seulement les échecs.

Par défaut, tous les paramètres sont désactivés.

Un profil de journal SSL peut être défini sur un profil SSL ou sur une action SSL. Si défini sur un profil SSL, vous pouvez consigner à la fois l'authentification client et les informations de réussite et d'échec de la poignée de main SSL. Si elle est définie sur une action SSL, vous ne pouvez consigner que les informations de réussite et d'échec de l'authentification du client, car la poignée de main est terminée avant l'évaluation de la stratégie.

L'authentification du client et la réussite et les échecs de la poignée de main SSL sont consignés même si vous ne configurez pas un profil de journal SSL. Toutefois, la journalisation sélective n'est possible que si un profil de journal SSL est utilisé.

> **Remarque :**
>
> Le profil de journal SSL est pris en charge dans les configurations de haute disponibilité et de cluster.

Ajouter un profil de journal SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add ssl logprofile <name> [-sslLogClAuth ( ENABLED | DISABLED )] [-
     ssllogClAuthFailures ( ENABLED | DISABLED )] [-sslLogHS ( ENABLED |
     DISABLED )] [-sslLogHSfailures ( ENABLED | DISABLED )]
2 <!--NeedCopy-->
```

Paramètres :

Nom :

Nom du profil de journal SSL. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier le profil après la création du profil.

Le nom est un argument obligatoire. Longueur maximale : 127

`sslLogClAuth` :

Enregistrez tous les événements d'authentification du client. Comprend les événements de réussite et d'échec.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

`ssllogClAuthFailures` :

Enregistrez tous les événements d'échec d'authentification client.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

sslLogHS :

Enregistrez tous les événements liés à la poignée de main SSL. Comprend les événements de réussite et d'échec.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

sslLogHSfailures :

Enregistrez tous les événements d'échec liés à la poignée de main SSL.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

Exemple :

```
> add ssl logprofile ssllog10 -sslLogClAuth ENABLED -sslLogHS ENABLED

 Done

sh ssllogprofile ssllog10

1)      Name: ssllog10

        SSL log ClientAuth [Success/Failures] : ENABLED

        SSL log ClientAuth [Failures] : DISABLED

        SSL log Handshake [Success/Failures] : ENABLED

        SSL log Handshake [Failures] : DISABLED

 Done
<!--NeedCopy-->
```

Ajouter un profil de journal SSL à l'aide de l'interface graphique

Accédez à **Système > Profils > Profil de journal SSL** et ajoutez un profil.

Modifier un profil de journal SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl logprofile <name> [-sslLogClAuth ( ENABLED | DISABLED )][-
    ssllogClAuthFailures ( ENABLED | DISABLED )] [-sslLogHS ( ENABLED |
    DISABLED )] [-sslLogHSfailures ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Exemple :

```
set ssllogprofile ssllog10 -ssllogClAuth en -ssllogClAuthFailures en -
    ssllogHS en -ssllogHSfailures en

Done

sh ssllogprofile ssllog10

    1)            Name: ssllog10

                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : ENABLED
                    SSL log Handshake [Failures] : ENABLED
     Done
<!--NeedCopy-->
```

Modifier un profil de journal SSL à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profil du journal SSL**, sélectionnez un profil et cliquez sur **Modifier**.
2. Effectuez des modifications et cliquez sur **OK**.

Afficher tous les profils de journaux SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
sh ssl logprofile
<!--NeedCopy-->
```

Exemple :

```
sh ssl logprofile

```



```
    1)              Name: ssllogp1
                      SSL log ClientAuth [Success/Failures] : ENABLED
                      SSL log ClientAuth [Failures] : ENABLED
                      SSL log Handshake [Success/Failures] : DISABLED
                      SSL log Handshake [Failures] : ENABLED

    2)              Name: ssllogp2
                      SSL log ClientAuth [Success/Failures] : DISABLED
                      SSL log ClientAuth [Failures] : DISABLED
                      SSL log Handshake [Success/Failures] : DISABLED
                      SSL log Handshake [Failures] : DISABLED

    3)              Name: ssllogp3
                      SSL log ClientAuth [Success/Failures] : DISABLED
                      SSL log ClientAuth [Failures] : DISABLED
                      SSL log Handshake [Success/Failures] : DISABLED
                      SSL log Handshake [Failures] : DISABLED

    4)              Name: ssllog10
                      SSL log ClientAuth [Success/Failures] : ENABLED
                      SSL log ClientAuth [Failures] : ENABLED
                      SSL log Handshake [Success/Failures] : ENABLED
                      SSL log Handshake [Failures] : ENABLED
Done
<!--NeedCopy-->
```

Afficher tous les profils de journaux SSL à l'aide de l'interface graphique

Accédez à **Système > Profils > Profil du journal SSL**. Tous les profils sont répertoriés.

Attacher un profil de journal SSL à un profil SSL

Vous pouvez attacher (définir) un profil de journal SSL sur un profil SSL lorsque vous créez un profil SSL, ou ultérieurement en modifiant le profil SSL. Vous pouvez consigner à la fois l'authentification du client et les succès et échecs de la poignée de main.

> **Important :**
>
> Le profil SSL par défaut doit être activé avant de pouvoir joindre un profil de journal SSL.

Joindre un profil de journal SSL sur un profil SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set ssl profile <name> [-ssllogProfile <string>]
<!--NeedCopy-->
```

Exemple :

```
set ssl profile fron_1 -ssllogProfile ssllog10
<!--NeedCopy-->
```

Attacher un profil de journal SSL à un profil SSL à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profil SSL**.
2. Cliquez sur **Modifier** et dans **Profil du journal SSL**, spécifiez un profil.

Attacher un profil de journal SSL à une action SSL

Vous pouvez définir un profil de journal SSL uniquement lors de la création d'une action SSL. Vous ne pouvez pas modifier une action SSL pour définir le profil du journal. Associer l'action à une stratégie. Vous ne pouvez consigner que les succès et les échecs d'authentification du client.

Attacher un profil de journal SSL à une action SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ssl action <name> -clientAuth ( DOCLIENTAUTH | NOCLIENTAUTH ) -
   ssllogProfile <string>
<!--NeedCopy-->
```

Exemple :

```
> add ssl action act1 -clientAuth DoCLIENTAUTH -ssllogProfile ssllog10

Done

> sh ssl action act1

    1)            Name: act1
                    Type: Client Authentication (DOCLIENTAUTH)
                    Hits: 0
                    Undef Hits: 0
                    Action Reference Count: 0
                    SSLlogProfile: ssllog10
Done
```



```
<!--NeedCopy-->
```

Attacher un profil de journal SSL à une action SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Stratégies** et cliquez sur **Actions SSL**.
2. Cliquez sur **Ajouter**.
3. Dans Authentification du client, sélectionnez **Activé**.
4. Dans SSL Log Profile, sélectionnez un profil dans la liste ou cliquez sur « + » pour créer un profil.
5. Cliquez sur **Créer**.

Exemple de sortie du fichier journal

Voici un exemple de sortie de journal`ns.log` pour une authentification client réussie.

```
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 158 0 :  SPCBId 671 - ClientIP 10.102.1.98 - ClientPort 49451 - VserverServiceIP 10.102.57.82 - VserverServicePort 443 - ClientVersion TLSv1.2 - CipherSuite "AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit" - Session New - CLIENT_AUTHENTICATED -SerialNumber "2A" - SignatureAlgorithm "sha1WithRSAEncryption" - ValidFrom "Sep 22 09:15:20 2008 GMT" - ValidTo "Feb  8 09:15:20 2036 GMT" - HandshakeTime 10 ms
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 159 0 :  SPCBId 671 - IssuerName " C=IN,ST=KAR,O=Citrix R&D Pvt Ltd,CN=Citrix"
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 160 0 :  SPCBId 671 - SubjectName " C=IN,ST=KAR,O=Citrix Pvt Ltd,OU=A,CN=B"
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 161 0 :  Backend SPCBId 674 - ServerIP 10.102.57.85 - ServerPort 443 - ProtocolVersion TLSv1.2 - CipherSuite "AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit" - Session Reuse - SERVER_AUTHENTICATED -SerialNumber "3E" - SignatureAlgorithm "sha1WithRSAEncryption" - ValidFrom "Sep 24 06:40:37 2008 GMT" - ValidTo "Feb 10 06:40:37 2036 GMT" - HandshakeTime 1 ms
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 162 0 :  SPCBId 674 - IssuerName " C=IN,ST=KAR,O=Citrix Pvt Ltd"
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 163 0 :  SPCBId 674 - SubjectName " C=IN,ST=P,L=Q,O=R"
<!--NeedCopy-->
```


Prise en charge du protocole DTLS

October 5, 2021

Remarques :

- Le protocole DTLSv1.0 est pris en charge sur les appliances FIPS Citrix ADC MPX/SDX (N2 et N3), VPX et MPX 14000. Il n'est pas pris en charge sur les HSM externes.
- Le protocole DTLS 1.0 est pris en charge sur les appliances Citrix ADC contenant des puces SSL Intel Coleto (à partir de la version 12.1 build 50.x).
- Le protocole DTLSv1.2 est pris en charge sur le front-end des appliances Citrix ADC VPX (à partir de la version 13.0 build 47.x).
- Le protocole DTLS 1.2 est pris en charge sur le frontal des appliances Citrix ADC contenant des puces SSL Intel Coleto (version 13.0 build 52.x). Pour plus d'informations sur les plates-formes contenant des puces SSL Intel Coleto, voir Prise en charge des plates-formes à puce SSL Intel Coleto.
- Les groupes de services de type DTLS ne sont pas pris en charge.
- Le protocole DTLSv1.2 est pris en charge sur le frontal des appliances Citrix ADC MPX (basé sur N3) (à partir de la version 13.0 build 58.x).
- Pour plus d'informations sur la prise en charge de Enlightened Data Transport (EDT) pour Citrix Gateway, reportez-vous à la section Prise en charge du transport de données éclairé HDX.
- Des modifications ont été apportées au profil DTLS depuis la version 13.0 build 79.x. Pour plus d'informations, voir Profil DTLS.
- Depuis la version 13.0 build 82.x, un nouveau paramètre « MaxBadMacIgnoreCount « est introduit dans le profil DTLS pour ignorer les enregistrements MAC erronés reçus dans une session DTLS. Pour plus d'informations, voir Profil DTLS.

Les protocoles SSL et TLS ont traditionnellement été utilisés pour sécuriser le trafic en continu. Ces deux protocoles sont basés sur le protocole TCP, qui est lent. De plus, TLS ne peut pas gérer les paquets perdus ou réordonnés.

UDP est le protocole préféré pour les applications audio et vidéo, telles que Lync, Skype, iTunes, YouTube, les vidéos de formation et Flash. Toutefois, UDP n'est ni sécurisé ni fiable. Le protocole DTLS est conçu pour sécuriser les données via UDP et est utilisé pour des applications telles que le streaming multimédia, la VOIP et les jeux en ligne pour la communication. Dans DTLS, chaque message de prise de main se voit attribuer un numéro de séquence spécifique au sein de cette prise de liaison. Lorsqu'un homologue reçoit un message de prise de main, il peut rapidement déterminer si ce message est le prochain message attendu. Si c'est le cas, l'homologue traite le message. Si ce n'est pas le cas, le message est mis en file d'attente pour être traité une fois que tous les messages précédents ont été reçus.

Créez un serveur virtuel DTLS et un service de type UDP. Par défaut, un profil DTLS (nsdtls_default_profile) est lié au serveur virtuel. Vous pouvez éventuellement créer et lier un profil DTLS défini par l'utilisateur au serveur virtuel.

Remarque : Les chiffrements RC4 ne sont pas pris en charge sur un serveur virtuel DTLS.

Configuration DTLS

Vous pouvez utiliser la ligne de commande (CLI) ou l'utilitaire de configuration (GUI) pour configurer DTLS sur votre appliance ADC.

Remarque : à partir de la version 13.0 build 47.x, le protocole DTLS 1.2 est pris en charge sur le frontal d'un dispositif Citrix ADC VPX. Lors de la configuration d'un serveur virtuel DTLSv1.2, spécifiez DTLS12. La valeur par défaut est DTLS1.

À l'invite de commandes, tapez :

```
set ssl vserver DTLS [-dtls1 ( ENABLED | DISABLED )] [-dtls12 ( ENABLED |
DISABLED )]
```

Créer une configuration DTLS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add lb vserver <vserver_name> DTLS <IPAddress>  <port>
2 add service  <service_name>  <IPAddress> UDP 443
3 bind lb vserver  <vserver_name>  <udp_service_name>
4 <!--NeedCopy-->
```

Les étapes suivantes sont facultatives :

```
1 add dtlsProfile dtls-profile -maxretryTime <positive_integer>
2 set ssl vserver <vserver_name> -dtlsProfileName <dtls_profile_name>
3 <!--NeedCopy-->
```

Créer une configuration DTLS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Créez un serveur virtuel de type DTLS et liez un service UDP au serveur virtuel.
3. Un profil DTLS par défaut est lié au serveur virtuel DTLS. Pour lier un profil différent, dans Paramètres SSL, sélectionnez un autre profil DTLS. Pour créer un profil, cliquez sur le signe plus (+) en regard de Profil DTLS.

Prise en charge de SNI sur un serveur virtuel DTLS

Pour plus d'informations sur SNI, voir Configurer un serveur virtuel SNI pour l'hébergement sécurisé de plusieurs sites.

Configurer SNI sur un serveur virtuel DTLS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl vserver <vServerName> -SNIEnable ENABLED
bind ssl vserver <vServerName> -certkeyName <string> -SNICert
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver v1 -sniEnable ENABLED
bind ssl vserver  v1 -certkeyName san2 -sniCert
bind ssl vserver  v1 -certkeyName san13  - sniCert
bind ssl vserver  v1 -certkeyName san17  - sniCert
<!--NeedCopy-->
```

```
sh ssl vserver v1

Advanced SSL configuration for VServer v1:
DH: DISABLED
DH Private-Key Exponent Size Limit: DISABLED
Ephemeral RSA: ENABLED
Refresh Count: 0
Session Reuse: ENABLED
Timeout: 1800 seconds
Cipher Redirect: DISABLED

ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: ENABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
HSTS Max-Age: 0
DTLSv1: ENABLED
Send Close-Notify: YES
Strict Sig-Digest Check: DISABLED
```



```
Zero RTT Early Data: DISABLED
DHE Key Exchange With PSK: NO
Tickets Per Authentication Context: 1

DTLS profile name: nsdtls_default_profile

ECC Curve: P_256, P_384, P_224, P_521

1) CertKey Name: ca
CA Certificate  OCSPCheck: OptionalCA_Name Sent
2) CertKey Name: san2 Server Certificate for SNI
3) CertKey Name: san17 Server Certificate for SNI
4) CertKey Name: san13 Server Certificate for SNI


1) Cipher Name: DEFAULT
Description: Default cipher list with encryption strength >= 128bit
Done
<!--NeedCopy-->
```

Configurez SNI sur un serveur virtuel DTLS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel DTLS et, dans Certificats, cliquez sur **Certificat de serveur**.
3. Ajoutez un certificat ou sélectionnez un certificat dans la liste, puis sélectionnez **Certificat de serveur pour SNI**.
4. Dans **Paramètres avancés**, cliquez sur **Paramètres SSL**.
5. Sélectionnez **Activer SNI**.

Fonctionnalités non prises en charge par un serveur virtuel DTLS

Les options suivantes ne peuvent pas être activées sur un serveur virtuel DTLS :

- SSLv2
- SSLv3
- TLSv1
- TLSv1.1
- TLSv1.2
- Déclencheur de cryptage push
- SSLv2Redirect
- SSLv2URL

Paramètres non utilisés par un serveur virtuel DTLS

Un serveur virtuel DTLS ignore les paramètres SSL suivants, même s'ils sont définis :

- Nombre de paquets de déclencheurs de chiffrement
- Délai de déclenchement du chiffrement
- Taille quantique SSL
- Délai d'expiration du déclencheur
- Format d'insertion du nom du sujet/émetteur

Configuration de la renégociation sur un service DTLS

La renégociation non sécurisée est prise en charge sur un service DTLS. Vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique pour configurer ce paramètre.

Configurer la renégociation sur un service DTLS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl parameter -denysslreneg NONSECURE
<!--NeedCopy-->
```

Exemple :

```
set ssl parameter -denysslreneg NONSECURE


sh ssl parameter
Advanced SSL Parameters
-----------------------
SSL quantum size                                  : 8 KB
Max CRL memory size                               : 256 MB
Strict CA checks                                  : NO
Encryption trigger timeout                        : 100 ms
Send Close-Notify                                 : YES
Encryption trigger packet count                   : 45
Deny SSL Renegotiation                            : NONSECURE
Subject/Issuer Name Insertion Format              : Unicode
OCSP cache size                                   : 10 MB
Push flag                                         : 0x0 (Auto)
Strict Host Header check for SNI enabled SSL sessions : NO
PUSH encryption trigger timeout                   : 1 ms
Crypto Device Disable Limit                       : 0
Global undef action for control policies          : CLIENTAUTH
```



```
Global undef action for data policies                : NOOP
Default profile                                      : DISABLED
SSL Insert Space in Certificate Header               : YES
Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors   : NO
Disable TLS 1.1/1.2 for dynamic and VPN services     : NO
Software Crypto acceleration CPU Threshold           : 0
Hybrid FIPS Mode                                     : DISABLED
Signature and Hash Algorithms supported by TLS1.2    : ALL
SSL Interception Error Learning and Caching          : DISABLED
SSL Interception Maximum Error Cache Memory          : 0 Bytes
Done
<!--NeedCopy-->
```

Configurer la renégociation sur un service DTLS à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Sélectionnez un service DTLS et cliquez sur **Modifier**.
3. Accédez à **SSL** > **Paramètres avancés**.
4. Sélectionnez **Refuser la renégociation SSL**.

Fonctionnalités non prises en charge par un service DTLS

Les options suivantes ne peuvent pas être activées sur un service DTLS :

- SSLv2
- SSLv3
- TLSv1
- TLSv1.1
- TLSv1.2
- Déclencheur de cryptage push
- SSLv2Redirect
- SSLv2URL
- SNI
- Renégociation sécurisée

Paramètres non utilisés par un service DTLS

Un service DTLS ignore les paramètres SSL suivants, même s'ils sont définis :

- Nombre de paquets de déclencheurs de chiffrement
- Délai de déclenchement du chiffrement
- Taille quantique SSL

- Délai d'expiration du déclencheur
- Format d'insertion du nom du sujet/émetteur

> **Remarque :**
>
> La connexion de réutilisation de session SSL échoue sur un service DTLS car la réutilisation de session n'est actuellement pas prise en charge sur les services DTLS.
>
> **Solution :** désactivez manuellement la réutilisation de session sur un service DTLS. À l'interface de ligne de commande, tapez :
>
> ```
> set ssl service <dtls-service-name> -sessReuse DISABLED
> ```

Profil DTLS

Un profil DTLS avec les paramètres par défaut est automatiquement lié à un serveur virtuel DTLS. Toutefois, vous pouvez créer un profil DTLS avec des paramètres spécifiques en fonction de vos besoins.

Utilisez un profil DTLS avec un serveur virtuel DTLS ou un serveur virtuel DTLS VPN. Vous ne pouvez pas utiliser de profil SSL avec un serveur virtuel DTLS.

> **Remarque :**
>
> Modifiez le paramètre de taille d'enregistrement maximale dans le profil DTLS en fonction des modifications apportées au MTU et à la taille des paquets. Par exemple, la taille d'enregistrement maximale par défaut de 1459 octets est calculée en fonction de la taille d'un en-tête d'adresse IPv4. Avec les enregistrements IPv6, la taille de l'en-tête est plus grande et, par conséquent, la taille d'enregistrement maximale doit être réduite pour répondre aux critères suivants.

```
max record size + UDP header(8bytes)+ IP header size < MTU
```

Exemple :

```
Default DTLS profile
    1) Name: nsdtls_default_profile
    PMTU Discovery: DISABLED
    Max Record Size: 1459 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: ENABLED
    Terminate Session: DISABLED
    Max Packet Count: 120 bytes

Custom DTLS profile
    1) Name: ns_dtls_profile_ipv6_1
    PMTU Discovery: DISABLED
    Max Record Size: 1450 bytes
```



```
14      Max Retry Time: 3 sec
15      Hello Verify Request: ENABLED
16      Terminate Session: DISABLED
17      Max Packet Count: 120 bytes
18  <!--NeedCopy-->
```

Créer un profil DTLS à l'aide de l'interface de ligne de commande

Remarques :

À partir de la version 13.0 build 79.x, les modifications apportées au profil DTLS sont les suivantes :

- Le paramètre `helloverifyrequest` est activé par défaut. L'activation de ce paramètre permet d'atténuer le risque qu'un attaquant ou des robots subisse le débit réseau, entraînant potentiellement un épuisement de la bande passante sortante. C'est-à-dire qu'il aide à atténuer l'attaque d'amplification DDoS DTLS.
- Le paramètre `maxHoldQlen` est ajouté. Ce paramètre définit le nombre de datagrammes pouvant être mis en file d'attente à la couche DTLS pour traitement. Une valeur élevée du paramètre `maxHoldQlen` peut entraîner une accumulation de mémoire au niveau de la couche DTLS si le multiplexage UDP transmet un trafic UDP élevé. Par conséquent, il est recommandé de configurer une valeur inférieure. La valeur minimale est 32, la valeur maximale est 65535 et la valeur par défaut est 32.

Depuis la version 13.0 build 82.x, un nouveau paramètre `maxBadmacIgnorecount` est introduit dans le profil DTLS pour ignorer les enregistrements MAC erronés reçus dans une session DTLS. À l'aide de ce paramètre, les enregistrements erronés jusqu'à la valeur définie dans le paramètre sont ignorés. L'appliance met fin à la session uniquement après que la limite est atteinte et envoie une alerte.

Ce paramètre n'est effectif que lorsque le paramètre « TerminateSession » est activé.

```
1  ssl dtlsProfile <name> -maxRetryTime <positive_integer> -
       helloVerifyRequest ( ENABLED | DISABLED ) -terminateSession (ENABLED
        | DISABLED ) -maxHoldQLen <positive_integer> -maxBadmacIgnorecount
       <positive_integer>
2
3  helloVerifyRequest
4                 Send a Hello Verify request to validate the client.
5                 Possible values: ENABLED, DISABLED
6                 Default value: ENABLED
7
8  terminateSession
9                 Terminate the session if the message authentication code
                      (MAC)
```



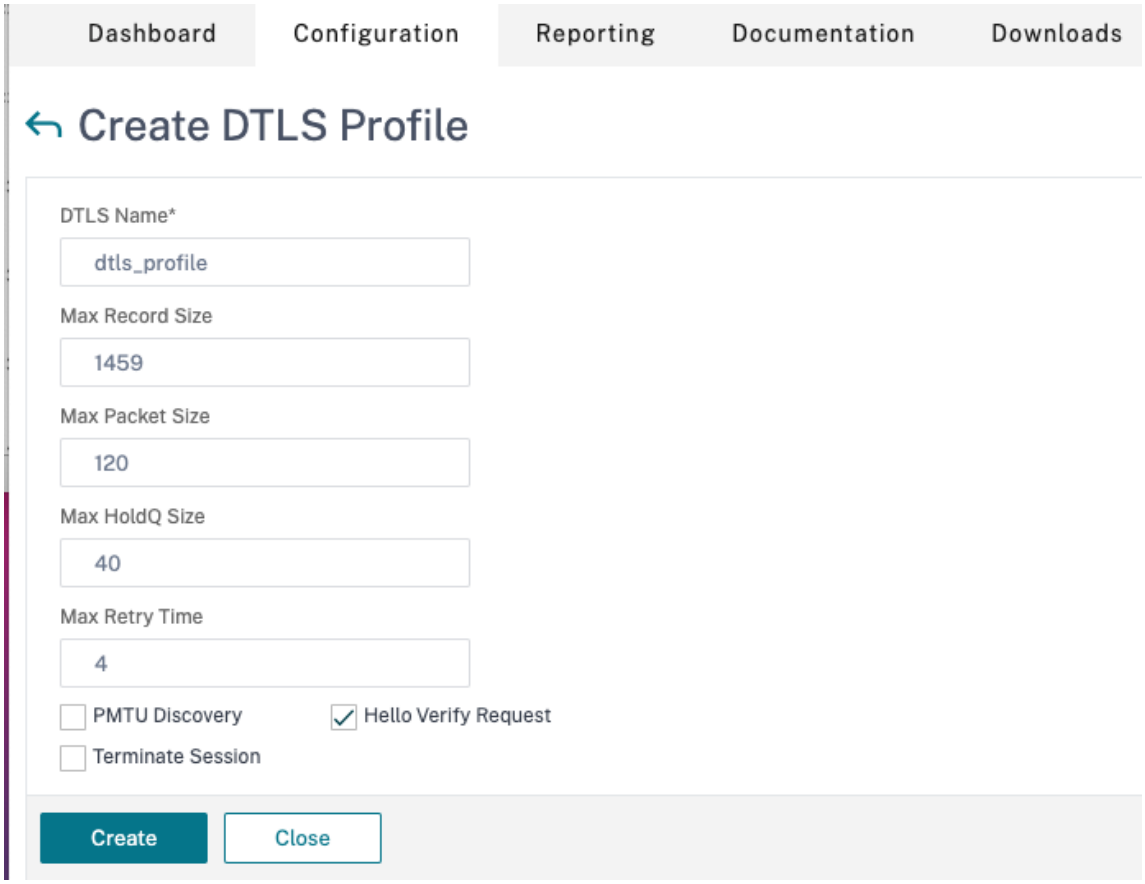
```
                of the client and server do not match.
                Possible values: ENABLED, DISABLED
                Default value: DISABLED

maxHoldQLen
                Maximum number of datagrams that can be queued at DTLS
                    layer for
                processing
                Default value: 32
                Minimum value: 32
                Maximum value: 65535

maxBadmacIgnorecount
                Maximum number of bad MAC errors to ignore for a
                    connection prior disconnect. Disabling parameter
                    terminateSession
terminates session immediately when bad MAC is detected in the
    connection.
                Default value: 100
                Minimum value: 1
                Maximum value: 65535
<!--NeedCopy-->
```

Exemple :

```
> add ssl dtlsprofile dtls_profile -maxRetryTime 4 -helloVerifyRequest
    ENABLED -terminateSession ENABLED -maxHoldQLen 40 -
    maxBadmacIgnorecount 150
 Done
> sh dtlsprofile dtls_profile
1)  Name: dtls_profile
    PMTU Discovery: DISABLED
    Max Record Size: 1459 bytes
    Max Retry Time: 4 sec
    Hello Verify Request: ENABLED
    Terminate Session: ENABLED
    Max Packet Count: 120 bytes
    Max HoldQ Size: 40 datagrams
    Max bad-MAC Ignore Count: 150

 Done
<!--NeedCopy-->
```


Créer un profil DTLS à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profils DTLS**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un profil DTLS**, saisissez les valeurs des différents paramètres.



3. Cliquez sur **Create**.

Exemple de configuration DTLS de bout en bout

```
enable ns feature SSL LB

add server s1 198.51.100.2

en ns mode usnip

add service svc_dtls s1 DTLS 443

add lb vserver v1 DTLS 10.102.59.244 443

bind ssl vserver v1 -ciphername ALL

```



```
13 add ssl certkey servercert -cert servercert_aia_valid.pem -key
      serverkey_aia.pem
14
15 bind ssl vserver v1 -certkeyname servercert
16
17 bind lb vserver lb1 svc_dtls
18
19 sh lb vserver v1
20
21                     v1 (10.102.59.244:4433) - DTLS     Type: ADDRESS
22                     State: UP
23                     Last state change was at Fri Apr 27 07:00:27 2018
24                     Time since last state change: 0 days, 00:00:04.810
25                     Effective State: UP
26                     Client Idle Timeout: 120 sec
27                     Down state flush: ENABLED
28                     Disable Primary Vserver On Down : DISABLED
29                     Appflow logging: ENABLED
30                     No. of Bound Services :  1 (Total) 0 (Active)
31                     Configured Method: LEASTCONNECTION
32                     Current Method: Round Robin, Reason: A new service
                          is bound         BackupMethod: ROUNDROBIN
33                     Mode: IP
34                     Persistence: NONE
35                     L2Conn: OFF
36                     Skip Persistency: None
37                     Listen Policy: NONE
38                     IcmpResponse: PASSIVE
39                     RHIstate: PASSIVE
40                     New Service Startup Request Rate: 0 PER_SECOND,
                          Increment Interval: 0
41                     Mac mode Retain Vlan: DISABLED
42                     DBS_LB: DISABLED
43                     Process Local: DISABLED
44                     Traffic Domain: 0
45                     TROFS Persistence honored: ENABLED
46                     Retain Connections on Cluster: NO
47
48     1) svc_dtls (10.102.59.190: 4433) - DTLS State: UP  Weight: 1
49 Done
50
51
52 sh ssl vserver v1
53
54                     Advanced SSL configuration for VServer v1:
```



```
55                      DH: DISABLED
56                      DH Private-Key Exponent Size Limit: DISABLED
                                  Ephemeral RSA: ENABLED
                                                        Refresh Count: 0
57                      Session Reuse: ENABLED                Timeout:
                           1800 seconds
58                      Cipher Redirect: DISABLED
59                      ClearText Port: 0
60                      Client Auth: DISABLED
61                      SSL Redirect: DISABLED
62                      Non FIPS Ciphers: DISABLED
63                      SNI: DISABLED
64                      OCSP Stapling: DISABLED
65                      HSTS: DISABLED
66                      HSTS IncludeSubDomains: NO
67                      HSTS Max-Age: 0
68                      DTLSv1: ENABLED
69                      Send Close-Notify: YES
70                      Strict Sig-Digest Check: DISABLED
71                      Zero RTT Early Data: DISABLED
72                      DHE Key Exchange With PSK: NO
73                      Tickets Per Authentication Context: 1
74                      DTLS profile name: nsdtls_default_profile
75
76                      ECC Curve: P_256, P_384, P_224, P_521
77
78      1)            CertKey Name: servercert               Server
           Certificate
79
80      1)            Cipher Name: DEFAULT
81                      Description: Default cipher list with encryption
                           strength >= 128bit
82
83      2)            Cipher Name: ALL
84                      Description: All ciphers supported by NetScaler,
                           excluding NULL ciphers
85       Done
86
87  sh service svc_dtls
88
89                      svc_dtls (10.102.59.190:4433) - DTLS
90                      State: UP
91                      Last state change was at Fri Apr 27 07:00:26 2018
92                      Time since last state change: 0 days, 00:00:22.790
93                      Server Name: s1
```



```
94                      Server ID : None                  Monitor Threshold
                            : 0
95                      Max Conn: 0        Max Req: 0           Max
                            Bandwidth: 0 kbits
96                      Use Source IP: NO
97                      Client Keepalive(CKA): NO
98                      Access Down Service: NO
99                      TCP Buffering(TCPB): NO
100                     HTTP Compression(CMP): NO
101                     Idle timeout: Client: 120 sec           Server: 120
                             sec
102                     Client IP: DISABLED
103                     Cacheable: NO
104                     SC: OFF
105                     SP: OFF
106                     Down state flush: ENABLED
107                     Monitor Connection Close : NONE
108                     Appflow logging: ENABLED
109                     Process Local: DISABLED
110                     Traffic Domain: 0
111
112     1)            Monitor Name: ping-default
113                                    State: UP               Weight: 1
                                                    Passive: 0
114                                  Probes: 5              Failed [Total
                                        : 0 Current: 0]
115                                  Last response: Success - ICMP echo
                                        reply received.
116                        Response Time: 2.77 millisec
117      Done
118
119 sh ssl service svc_dtls
120
121                     Advanced SSL configuration for Back-end SSL Service
                             svc_dtls:
122                     DH: DISABLED
123                     DH Private-Key Exponent Size Limit: DISABLED
                                  Ephemeral RSA: DISABLED
124                     Session Reuse: ENABLED                 Timeout:
                            1800 seconds
125                     Cipher Redirect: DISABLED
126                     ClearText Port: 0
127                     Server Auth: DISABLED
128                     SSL Redirect: DISABLED
129                     Non FIPS Ciphers: DISABLED
```



```
130                     SNI: DISABLED
131                     OCSP Stapling: DISABLED
132                     DTLSv1: ENABLED
133                     Send Close-Notify: YES
134                     Strict Sig-Digest Check: DISABLED
135                     Zero RTT Early Data: ???
136                     DHE Key Exchange With PSK: ???
137                     Tickets Per Authentication Context: ???
138                     DTLS profile name: nsdtls_default_profile
139                     ECC Curve: P_256, P_384, P_224, P_521
140     1)            Cipher Name: DEFAULT_BACKEND
141                     Description: Default cipher list for Backend SSL
                           session
142      Done
143
144
145  > sh dtlsProfile nsdtls_default_profile
146  1)  Name: nsdtls_default_profile
147      PMTU Discovery: DISABLED
148      Max Record Size: 1459 bytes
149      Max Retry Time: 3 sec
150      Hello Verify Request: DISABLED
151      Terminate Session: ENABLED
152      Max Packet Count: 120 bytes
153      Max HoldQ Size: 32 datagrams
154      Max bad-MAC Ignore Count: 10
155
156   Done
157  <!--NeedCopy-->
```

Prise en charge DTLS de l'adresse IPv6

DTLS est également pris en charge avec les adresses IPv6. Toutefois, pour utiliser DTLS avec des adresses IPv6, la taille d'enregistrement maximale doit être ajustée dans le profil DTLS.

Si la valeur par défaut est utilisée pour la taille d'enregistrement maximale, la connexion DTLS initiale peut échouer. Ajustez la taille d'enregistrement maximale à l'aide d'un profil DTLS.

Prise en charge du chiffrement DTLS

Par défaut, un groupe de chiffrement DTLS est lié lorsque vous créez un serveur ou un service virtuel DTLS. DEFAULT_DTLS contient les chiffrements pris en charge par une entité DTLS frontale. Ce groupe est lié par défaut lorsque vous créez un serveur virtuel DTLS. DEFAULT_DTLS_BACKEND contient les

chiffrements pris en charge par une entité DTLS dorsale. Ce groupe est lié par défaut à un service principal DTLS. DTLS_FIPS contient les chiffrements pris en charge sur la plate-forme FIPS Citrix ADC. Ce groupe est lié par défaut à un serveur virtuel DTLS ou à un service créé sur une plate-forme FIPS.

Prise en charge du chiffrement DTLS sur les appliances Citrix ADC VPX, MPX/SDX (N2 et N3)

Comment lire les tableaux :

À moins qu'un numéro de version ne soit spécifié, une suite de chiffrement est prise en charge pour toutes les versions d'une version.

Exemple :

- **10.5, 11.0, 11.1, 12.0, 12.1, 13.0** : toutes les versions des versions 10.5, 11.0, 11.1, 12.0, 12.1, 13.0.
- **-NA-** : non applicable.

Prise en charge du chiffrement DTLS sur les appliances Citrix ADC VPX, MPX/SDX (N2 et N3)

Nom de la suite de chiffrement	Code Hex	Nom de la suite de chiffrement Wireshark	Builds pris en charge (frontal)	Builds prises en charge (back-end)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AI	11.0, 11.1, 12.0, 12.1, 13.0	12.0, 12.1, 13.0
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CBC_SHA	11.0, 11.1, 12.0, 12.1, 13.0	12.0, 12.1, 13.0
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_D	11.0, 11.1, 12.0, 12.1, 13.0	-SO-
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA	11.0, 11.1, 12.0, 12.1, 13.0	12.0, 12.1, 13.0
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WI	11.0, 11.1, 12.0, 12.1, 13.0	-SO-
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	11.0, 11.1, 12.0, 12.1, 13.0	-SO-
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_	12.1, 13.0	12.1, 13.0

Nom de la suite de chiffrement	Code Hex	Nom de la suite de chiffrement Wireshark	Builds pris en charge (frontal)	Builds prises en charge (back-end)
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	12.1, 13.0	12.1, 13.0
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_	12.1, 13.0	-SO-
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	12.1, 13.0	12.1, 13.0
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WI	12.1, 13.0	12.1, 13.0

Pour afficher la liste des chiffrements par défaut pris en charge sur le frontal, à l'invite de commandes, tapez :

```
show ssl cipher DEFAULT_DTLS
1)    Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA    Priority : 5
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0039
6)    Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA    Priority : 6
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x0033
7)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA Priority : 7
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
```



```
16 8)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 8
17     Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
          HexCode=0x000a
18 <!--NeedCopy-->
```

Pour afficher la liste des chiffrements par défaut pris en charge sur le back-end, à l'invite de commandes, tapez :

```
1  show ssl cipher DEFAULT_DTLS_BACKEND
2  1)  Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
3      Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
          HexCode=0x0035
4  2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
5      Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
          HexCode=0x002f
6  3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
7      Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
          HexCode=0xc014
8  4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
9      Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
          HexCode=0xc013
10 5)    Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA    Priority : 5
11     Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
          HexCode=0x0039
12 6)    Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA    Priority : 6
13     Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
          HexCode=0x0033
14 7)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA Priority : 7
15     Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
          HexCode=0xc012
16 8)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 8
17     Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
          HexCode=0x000a
18 <!--NeedCopy-->
```

Prise en charge du chiffrement DTLS sur la plate-forme FIPS Citrix ADC MPX 14000

Remarque : EDT est pris en charge sur la plateforme FIPS si les conditions suivantes sont remplies :

- La valeur MSS UDT définie sur StoreFront est 900.
- La version du client Windows est 4.12 ou ultérieure.
- La version du VDA compatible DTLS est 7.17 ou ultérieure.
- La version VDA non-DTLS est 7.15 LTSR CU3 ou ultérieure.

Comment lire les tableaux :

À moins qu'un numéro de version ne soit spécifié, une suite de chiffrement est prise en charge pour toutes les versions d'une version.

Exemple :

- **10.5, 11.0, 11.1, 12.0, 12.1, 13.0** : toutes les versions des versions 10.5, 11.0, 11.1, 12.0, 12.1, 13.0.
- **-NA-** : non applicable.

Nom de la suite de chiffrement	Code Hex	Nom de la suite de chiffrement Wireshark	Builds pris en charge (frontal)	Builds prises en charge (back-end)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AI	11.0, 11.1, 12.0, 12.1–49.x, 13.0	12.0, 12.1–49.x, 13.0
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CBC_SHA	11.0, 11.1, 12.0, 12.1–49.x, 13.0	12.0, 12.1–49.x, 13.0
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_D	11.0, 11.1, 12.0, 12.1–49.x, 13.0	-SO-
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA	11.0, 11.1, 12.0, 12.1–49.x, 13.0	12.0, 12.1–49.x, 13.0
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WI	11.0, 11.1, 12.0, 12.1–49.x, 13.0	-SO-
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	11.0, 11.1, 12.0, 12.1–49.x, 13.0	-SO-
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_	12.1–49.x, 13.0	12.1–49.x, 13.0
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	12.1–49.x, 13.0	12.1–49.x, 13.0
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_	12.1–49.x, 13.0	-SO-
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	12.1–49.x, 13.0	12.1–49.x, 13.0

Nom de la suite de chiffrement	Code Hex	Nom de la suite de chiffrement Wireshark	Builds pris en charge (frontal)	Builds prises en charge (back-end)
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WI	12.1–49.x, 13.0	12.1–49.x, 13.0

Pour afficher la liste des chiffrements par défaut pris en charge sur une appliance FIPS Citrix ADC, à l'invite de commandes, tapez :

```
show ssl cipher DTLS_FIPS
1)    Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA  Priority : 5
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
6)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 6
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0x000a
<!--NeedCopy-->
```

Prise en charge du chiffrement DTLSv1.2 sur les appliances VPX frontales, les appliances MPX/SDX (basées sur Coleto et N3)

Le tableau suivant répertorie les chiffrements supplémentaires pris en charge par le protocole DTLSv1.2.

Nom de la suite de chiffrement	Code Hex	Nom de la suite de chiffrement Wireshark	Builds prises en charge (frontal VPX)	Builds prises en charge (basé sur Coleto)	Builds prises en charge (basé sur N3)
TLS1.2-AES256-GCM-SHA384	0x009d	TLS_RSA_WITH	13.0–47.x	13.0–52.x	13.0–58.x
TLS1.2-AES128-GCM-SHA256	0x009c	TLS_RSA_WITH_AES_128_GCM_SHA256	13.0–47.x	13.0–52.x	13.0–58.x
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	0xc030	TLS_ECDHE_RS	13.0–47.x	13.0–52.x	13.0–58.x
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	0xc02f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	13.0–47.x	13.0–52.x	13.0–58.x
TLS1.2-DHE-RSA-AES256-GCM-SHA384	0x009f	TLS_DHE_RSA_	13.0–47.x	13.0–52.x	13.0–58.x
TLS1.2-DHE-RSA-AES128-GCM-SHA256	0x009e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	13.0–47.x	13.0–52.x	13.0–58.x
TLS1.2-AES-256-SHA256	0x003d	TLS_RSA_WITH	13.0–47.x	13.0–52.x	13.0–58.x
TLS1.2-AES-128-SHA256	0x003c	TLS_RSA_WITH_AES_128_CBC_SHA256	13.0–47.x	13.0–52.x	13.0–58.x
TLS1.2-ECDHE-RSA-AES-256-SHA384	0xc028	TLS_ECDHE_RS	13.0–47.x	13.0–52.x	13.0–58.x
TLS1.2-ECDHE-RSA-AES-128-SHA256	0xc027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	13.0–47.x	13.0–52.x	13.0–58.x

Nom de la suite de chiffrement	Code Hex	Nom de la suite de chiffrement Wireshark	Builds prises en charge (frontal VPX)	Builds prises en charge (basé sur Coleto)	Builds prises en charge (basé sur N3)
TLS1.2-DHE-RSA-AES-256-SHA256	0x006b	TLS_DHE_RSA_	13.0–47.x	13.0–52.x	13.0–58.x
TLS1.2-DHE-RSA-AES-128-SHA256	0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	13.0–47.x	13.0–52.x	13.0–58.x

Prise en charge des plates-formes à puce Intel Coleto SSL

January 21, 2021

Les appareils suivants sont livrés avec des puces Intel Coleto :

- MPX 5900
- MPX/SDX 8900
- MPX/SDX 15000
- MPX/SDX 15000-50G
- MPX/SDX 26000
- MPX/SDX 26000-50S
- MPX/SDX 26000-100G

Utilisez la commande ‘show hardware ‘pour déterminer si votre appliance possède des puces Coleto (COL).

```
> sh hardware

    Platform: NSMPX-8900 8\*CPU+4\*F1X+6\*E1K+1\*E1K+1*COL 8955 30010
    Manufactured on: 10/18/2016
    CPU: 2100MHZ
    Host Id: 0
    Serial no: CRAC5CR8UA
    Encoded serial no: CRAC5CR8UA
 Done
<!--NeedCopy-->
```

Remarque : la renégociation sécurisée est prise en charge sur le back-end pour ces plates-formes.

Limitations :

- Le chiffrement DH 512 n'est pas pris en charge.
- Le protocole SSLv3 n'est pas pris en charge.
- Le module de sécurité matérielle (HSM) n'est pas pris en charge.
- GnuTLS n'est pas pris en charge.
- Les certificats ECDSA avec les courbes ECC P_224 et P521 ne sont pas pris en charge (non pris en charge sur les plates-formes avec des puces Cavium également.)
- Le déchargement DNSSEC n'est pas pris en charge. (DNSSEC est pris en charge dans le logiciel, mais le déchargement vers le matériel n'est pas pris en charge.)

Afficher l'utilisation de la puce SSL sur les plates-formes Citrix ADC MPX

À partir de la version 13.0 build 47.x, vous pouvez visualiser l'utilisation des puces SSL sur les plates-formes MPX livrés avec les puces Intel Coleto. Cette fonctionnalité n'est pas prise en charge sur la plate-forme SDX et sur un cluster MPX.

À l'invite de commandes, tapez :

```
> stat ssl


SSL Summary


# SSL cards present                                4

# SSL cards UP                                     4

SSL engine status                                  1

SSL sessions (Rate)                              0

SSL Crypto Utilization Asym (%)                    67

SSL Crypto Utilization Symm (%)                    19
<!--NeedCopy-->
```

Appareils FIPS MPX 9700/10500/12500/15500

August 20, 2021

Important La plate-forme FIPS MPX 9700/10500/12500/15500 est en fin de vie.

Le Federal Information Processing Standard (FIPS), publié par le National Institute of Standards and Technologies des États-Unis, précise les exigences de sécurité d'un module cryptographique utilisé dans un système de sécurité. L'appliance Citrix ADC FIPS est conforme à la deuxième version de cette norme, FIPS-140-2.

Note : Désormais, toutes les références à FIPS impliquent FIPS-140-2.

L'appareil FIPS est équipé d'un module cryptographique inviolable (inviolable) et d'un Cavium CN1620-NFBE3-2.0-G sur les appareils FIPS MPX 9700/10500/12500/15500, conçus pour répondre aux spécifications FIPS 140-2 de niveau 2. Les paramètres de sécurité critiques (CSP), principalement la clé privée du serveur, sont stockés et générés en toute sécurité à l'intérieur du module cryptographique, également appelé Hardware Security Module (HSM). Les CSP ne sont jamais accessibles à l'extérieur des limites du HSM. Seul le superutilisateur peut effectuer des opérations sur les clés stockées dans le HSM.

Le tableau suivant résume les différences entre les appliances Citrix ADC standard et Citrix ADC FIPS.

Paramètre	Appliance Citrix ADC	Appliance Citrix ADC FIPS
Stockage des clés	Sur le disque dur	Sur la carte FIPS
Prise en charge du chiffrement	Tous les chiffrements	Ciphers approuvés par FIPS
Accès aux clés	A partir du disque dur	Non accessible

La configuration d'une appliance FIPS implique la configuration du HSM immédiatement après la fin du processus de configuration générique. Vous créez ou importez ensuite une clé FIPS. Après avoir créé une clé FIPS, vous devez l'exporter pour la sauvegarde. Vous devrez peut-être également exporter une clé FIPS afin de pouvoir l'importer dans un autre dispositif. Par exemple, la configuration des appliances FIPS dans une configuration haute disponibilité nécessite le transfert de la clé FIPS du nœud principal vers le nœud secondaire immédiatement après avoir terminé la configuration standard de haute disponibilité.

Vous pouvez mettre à niveau la version du firmware sur la carte FIPS de la version 4.6.0 vers 4.6.1. Vous pouvez également réinitialiser un HSM qui a été verrouillé pour empêcher l'ouverture de session non autorisée. Seuls les chiffrements approuvés par FIPS sont pris en charge sur une appliance Citrix ADC FIPS.

Configuration HSM

Avant de pouvoir configurer le HSM de votre appliance Citrix ADC FIPS, vous devez terminer la configuration matérielle initiale. Pour plus d'informations sur les appliances MPX, voir Configuration initiale. Pour plus d'informations sur les appliances SDX, cliquez ici.

La configuration du HSM de votre appliance Citrix ADC FIPS efface toutes les données existantes sur le HSM. Pour configurer le HSM, vous devez être connecté à l'appliance en tant que superutilisateur. Le HSM est préconfiguré avec des valeurs par défaut pour le mot de passe Security Officer (SO) et le mot de passe utilisateur, que vous utilisez pour configurer le HSM ou réinitialiser un HSM verrouillé. La longueur maximale autorisée pour le mot de passe est de 14 caractères alphanumériques. Les symboles ne sont pas autorisés.

Important : exécutez la `set ssl fips` commande uniquement après la réinitialisation de la carte FIPS et le redémarrage de l'appliance MPX FIPS.

Bien que l'appliance FIPS puisse être utilisée avec les valeurs de mot de passe par défaut, vous devez les modifier avant de l'utiliser. Le HSM ne peut être configuré que lorsque vous ouvrez une session sur l'appliance en tant que superutilisateur et spécifiez les mots de passe SO et utilisateur.

Important : en raison de contraintes de sécurité, l'appliance ne permet pas de récupérer le mot de passe SO. Stockez une copie du mot de passe en toute sécurité. Si vous devez réinitialiser le HSM, vous devez spécifier ce mot de passe comme ancien mot de passe SO.

Avant d'initialiser le HSM, vous pouvez effectuer une mise à niveau vers la dernière version du logiciel. Pour effectuer une mise à niveau vers la dernière version, reportez-vous à la section Mise à niveau ou rétrogradation du logiciel système.

Après la mise à niveau, vérifiez que le `/nsconfig/fips` répertoire a été créé avec succès sur l'appliance.

Configurez le HSM sur la plate-forme FIPS MPX 9700/10500/12500/15500 à l'aide de l'interface de ligne de commande

Après avoir ouvert une session sur l'appliance en tant que superutilisateur et terminé la configuration initiale, à l'invite de commandes, tapez les commandes suivantes pour configurer le HSM et vérifier la configuration :

```
1 show ssl fips
2
3 reset ssl fips
4
5 reboot
6
```



```
set ssl fips -initHSM Level-2 <newSOpassword> <oldSOpassword> <
   userPassword> [-hsmLabel <string>]

save ns config

reboot

show ssl fips
<!--NeedCopy-->
```

Exemple :

```
show fips

    FIPS Card is not configured
    Done
    reset fips
    reboot
    Are you sure you want to restart NetScaler (Y/N)? [N]:y

    set ssl fips -initHSM Level-2 sopin12345 so12345 user123 -hsmLabel
       cavium

    This command will erase all data on the FIPS card. You must save
       the configuration

    (saveconfig) after executing this command.


    Do you want to continue?(Y/N)y
    Done

    save ns config

    reboot

    Are you sure you want to restart NetScaler (Y/N)? [N]:y

    show fips

            FIPS HSM Info:
    HSM Label              : Citrix ADC FIPS
    Initialization         : FIPS-140-2 Level-2
    HSM Serial Number      : 2.1G1008-IC000021
    HSM State              : 2
```



```
32      HSM Model               : NITROX XL CN1620-NFBE
33      Firmware Version        : 1.1
34      Firmware Release Date   : Jun04,2010
35      Max FIPS Key Memory     : 3996
36      Free FIPS Key Memory    : 3994
37      Total SRAM Memory       : 467348
38      Free SRAM Memory        : 62564
39      Total Crypto Cores       : 3
40      Enabled Crypto Cores     : 1
41      Done
42
43      Note: If you upgrade the firmware to version 2.2, the firmware
           release date is replaced with the firmware build.
44
45
46
47      > show fips
48
49      FIPS HSM Info:
50
51      HSM Label                 : Citrix ADC FIPS
52      Initialization               : FIPS-140-2 Level-2
53      HSM Serial Number    : 3.0G1235-ICM000264
54      HSM State                 : 2
55      HSM Model                : NITROX XL CN1620-NFBE
56      Hardware Version       : 2.0-G
57      Firmware Version        : 2.2
58      Firmware Build           : NFBE-FW-2.2-130009
59      Max FIPS Key Memory : 3996
60      Free FIPS Key Memory : 3958
61      Total SRAM Memory    : 467348
62      Free SRAM Memory     : 50524
63      Total Crypto Cores       : 3
64      Enabled Crypto Cores  : 3
65      Done
66  <!--NeedCopy-->
```

Configurez le HSM sur la plate-forme FIPS MPX 9700/10500/12500/15500 à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l' **onglet InfoFIPS**, cliquez sur **Réinitialiser FIPS**.
3. Dans le volet de navigation, cliquez sur **Système**.

4. Dans le volet d'informations, cliquez sur **Redémarrer**.
5. Dans le volet d'informations, sous l'onglet Infos FIPS, cliquez sur **Initialiser HSM**.
6. Dans la boîte de dialogue Initialiser HSM, spécifiez les valeurs des paramètres suivants :
   - Mot de passe de l'agent de sécurité (SO) *—Nouveau mot de passe de l'agent de sécurité
   - Ancien mot de passe SO *—ancien mot de passe SO
   - Mot de passe utilisateur* : mot de passe utilisateur
   - level : inithSM (actuellement défini sur Level2 et ne peut pas être modifié)
   - Étiquette HSM—HSMLabel

   *Paramètre obligatoire
7. Cliquez sur **OK**.
8. Dans le volet d'informations, cliquez sur **Enregistrer**.
9. Dans le volet de navigation, cliquez sur **Système**.
10. Dans le volet d'informations, cliquez sur **Redémarrer**.
11. Sous FIPS HSM Info, vérifiez que les informations affichées sont correctes pour le HSM FIPS que vous avez configuré.

Créer et transférer des clés FIPS

Après avoir configuré le HSM de votre appliance FIPS, vous êtes prêt à créer une clé FIPS. La clé FIPS est créée dans le HSM de l'appliance. Vous pouvez ensuite exporter la clé FIPS vers la carte CompactFlash de l'appliance en tant que sauvegarde sécurisée. L'exportation de la clé vous permet également de la transférer en la copiant vers /flash d'une autre appliance, puis en l'important dans le HSM de cette appliance. Activez la carte SIM entre deux nœuds autonomes avant d'exporter et de transférer les clés. Dans une configuration haute disponibilité, si l'un des nœuds est remplacé par un nouveau, vous devez effectuer les opérations suivantes :

1. Activez la carte SIM entre cette nouvelle appliance et l'appliance existante de la configuration haute disponibilité.
2. Exportez ou importez des clés FIPS.

Au lieu de créer une clé FIPS, vous pouvez importer une clé FIPS existante ou importer une clé externe en tant que clé FIPS. Si vous ajoutez une paire de clés de certificat de 2048 bits sur les appliances FIPS MPX 9700/10500/12500/15500, assurez-vous d'avoir le bon certificat et la bonne paire de clés.

Remarque : Si vous prévoyez une configuration haute disponibilité, assurez-vous que les appliances FIPS sont configurées dans une configuration haute disponibilité avant de créer une clé FIPS.

Créer des clés FIPS

Avant de créer une clé FIPS, assurez-vous que le HSM est configuré.

Spécifiez le type de clé (RSA ou ECDSA) et spécifiez la courbe pour les clés ECDSA.

Créer une clé FIPS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Touches FIPS, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Créer une clé FIPS, spécifiez les valeurs des paramètres suivants :
   - Nom de la clé FIPS*—fipsKeyName
   - Module*—modulus
   - Exposant*—exponent

   *Paramètre obligatoire
4. Cliquez sur **Créer**, puis sur **Fermer**.
5. Sous l'onglet Touches FIPS, vérifiez que les paramètres affichés pour la clé FIPS que vous avez créée sont corrects.

Créer une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une clé FIPS et vérifier les paramètres :

```
create ssl fipsKey <fipsKeyName> -modulus <positive_integer> [-exponent
    ( 3 | F4 )]

show ssl fipsKey [<fipsKeyName>]
<!--NeedCopy-->
```

Exemple :

```
    create fipskey Key-FIPS-1 -keytype RSA -modulus 2048 -exponent 3

    show ssl fipsKey Key-FIPS-1

                FIPS Key Name: Key-FIPS-1 Key Type: RSA Modulus: 2048
                     Public Exponent: F4 (Hex: 0x10001)
<!--NeedCopy-->
```


Exporter les clés FIPS

Citrix vous recommande de créer une sauvegarde de toute clé créée dans le HSM FIPS. Si une clé dans le HSM est supprimée, il n'y a aucun moyen de créer à nouveau la même clé, et tous les certificats qui y sont associés sont rendus inutiles.

Outre l'exportation d'une clé en tant que sauvegarde, vous devrez peut-être exporter une clé pour le transfert vers une autre appliance.

La procédure suivante fournit des instructions sur l'exportation d'une clé FIPS vers le `/nsconfig/ssl` dossier du CompactFlash de l'appliance et la sécurisation de la clé exportée à l'aide d'une méthode de chiffrement de clé asymétrique forte.

Exporter une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
export ssl fipsKey <fipsKeyName> -key <string>
<!--NeedCopy-->
```

Exemple :

```
export fipskey Key-FIPS-1 -key Key-FIPS-1.key
<!--NeedCopy-->
```

Exporter une clé FIPS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Clés FIPS, cliquez sur **Exporter**.
3. Dans la boîte de dialogue Exporter FIPS dans un fichier, spécifiez les valeurs des paramètres suivants :
   - Nom de la clé FIPS*—fipsKeyName
   - Nom du fichier* : touche (Pour placer le fichier dans un emplacement autre que celui par défaut, vous pouvez spécifier le chemin d'accès complet ou cliquer sur le bouton Parcourir et accéder à un emplacement.)

   *Paramètre obligatoire
4. Cliquez sur **Exporter**, puis sur **Fermer**.

Importer une clé FIPS existante

Pour utiliser une clé FIPS existante avec votre appliance FIPS, vous devez transférer la clé FIPS du disque dur de l'appliance vers son HSM.

Remarque : Pour éviter les erreurs lors de l'importation d'une clé FIPS, assurez-vous que le nom de la clé importée est le même que le nom de la clé d'origine lors de sa création.

Importer une clé FIPS sur les appliances FIPS MPX 9700/10500/12500/15500 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour importer une clé FIPS et vérifier les paramètres :

```
1 - import ssl fipsKey <fipsKeyName> -key <string> -inform SIM -exponent
     (F4 | 3)
2 - show ssl fipskey <fipsKeyName>
3 <!--NeedCopy-->
```

Exemple :

```
1 import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4
2 show ssl fipskey key-FIPS-2
3 FIPS Key Name: Key-FIPS-2 Modulus: 2048   Public Exponent: F4 (Hex
     value 0x10001)
4 <!--NeedCopy-->
```

Importer une clé FIPS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Touches FIPS, cliquez sur **Importer**.
3. Dans la boîte de dialogue Importer en tant que clé FIPS, sélectionnez le fichier de clé FIPS et définissez les valeurs pour les paramètres suivants :
   - Nom de la clé FIPS*
   - Nom du fichier clé* : pour placer le fichier dans un emplacement autre que celui par défaut, vous pouvez spécifier le chemin d'accès complet ou cliquer sur Parcourir et accéder à un emplacement.
   - Exposant*

   *Paramètre obligatoire
4. Cliquez sur **Importer**, puis sur **Fermer**.
5. Sous l'onglet Touches FIPS, vérifiez que les paramètres affichés pour la clé FIPS que vous avez importée sont corrects.

Importer une clé externe

Vous pouvez transférer des clés FIPS créées dans le HSM de l'appliance Citrix ADC. Vous pouvez également transférer des clés privées externes (telles que des clés créées sur un Citrix ADC, Apache ou IIS standard) vers une appliance Citrix ADC FIPS. Les clés externes sont créées en dehors du HSM, à l'aide d'un outil tel que OpenSSL. Avant d'importer une clé externe dans le HSM, copiez-la sur le lecteur flash de l'appliance sous `/nsconfig/ssl`.

Sur les appliances MPX 9700/10500/12500/15500 FIPS, le paramètre -exponent de la `import ssl fipskey` commande n'est pas requis lors de l'importation d'une clé externe. L'exposant public correct est détecté automatiquement lorsque la clé est importée et la valeur du paramètre -exponent est ignorée.

L'appliance Citrix ADC FIPS ne prend pas en charge les clés externes avec un exposant public autre que 3 ou F4.

Vous n'avez pas besoin d'une clé d'enroulement sur les appareils FIPS MPX 9700/10500/12500/15500.

Vous ne pouvez pas importer une clé FIPS externe cryptée directement vers une appliance FIPS MPX 9700/10500/12500/15500. Pour importer la clé, vous devez d'abord la déchiffrer, puis l'importer. Pour déchiffrer la clé, à l'invite du shell, tapez :

```
openssl rsa -in <EncryptedKey.key> > <DecryptedKey.out>
<!--NeedCopy-->
```

Remarque : Si vous importez une clé RSA en tant que clé FIPS, Citrix vous recommande de supprimer la clé RSA de l'appliance à des fins de sécurité.

Importer une clé externe en tant que clé FIPS vers une appliance FIPS MPX 9700/10500/12500/15500 à l'aide de l'interface de ligne de commande

1. Copiez la clé externe sur le lecteur flash de l'appliance.
2. Si la clé est au format .pfx, vous devez d'abord la convertir au format PEM. À l'invite de commandes, tapez :

   ```
   convert ssl pkcs12 <output file> -import -pkcs12File <input .pfx
       file name> -password <password>
   <!--NeedCopy-->
   ```

3. À l'invite de commandes, tapez les commandes suivantes pour importer la clé externe en tant que clé FIPS et vérifiez les paramètres :

   ```
   import ssl fipsKey <fipsKeyName> -key <string> -informPEM
   show ssl fipskey<fipsKeyName>
   <!--NeedCopy-->
   ```


Exemple :

```
convert ssl pkcs12 iis.pem -password 123456 -import -pkcs12File iis.pfx

import fipskey Key-FIPS-2 -key iis.pem -inform PEM

show ssl fipskey key-FIPS-2

FIPS Key Name: Key-FIPS-2 Modulus: 0   Public Exponent: F4 (Hex value 0
   x10001)
<!--NeedCopy-->
```

Importer une clé externe en tant que clé FIPS vers une appliance FIPS MPX 9700/10500/12500/15500 à l'aide de l'interface graphique

1. Si la clé est au format .pfx, vous devez d'abord la convertir au format PEM.
   a) Accédez à **Gestion du trafic > SSL**.
   b) Dans le volet d'informations, sous Outils, cliquez sur **Importer PKCS #12**.
   c) Dans la boîte de dialogue Importer un fichier PKCS12, définissez les paramètres suivants :
      - Nom du fichier de sortie*
      - Nom du fichier PKCS12 *: spécifiez le nom du fichier .pfx.
      - Importer le mot de passe *
      - Format de codage

      *Paramètre obligatoire
2. Accédez à **Gestion du trafic > SSL > FIPS**.
3. Dans le volet d'informations, sous l'onglet Touches FIPS, cliquez sur **Importer**.
4. Dans la boîte de dialogue Importer en tant que clé FIPS, sélectionnez fichier PEM et définissez les valeurs pour les paramètres suivants :
   - Nom de la clé FIPS*
   - Nom du fichier clé* : pour placer le fichier dans un emplacement autre que celui par défaut, vous pouvez spécifier le chemin d'accès complet ou cliquer sur Parcourir et accéder à un emplacement.

   *Paramètre obligatoire
5. Cliquez sur **Importer**, puis sur **Fermer**.
6. Sous l'onglet Touches FIPS, vérifiez que les paramètres affichés pour la clé FIPS que vous avez importée sont corrects.

Configurer FIPS sur les appliances dans une configuration haute disponibilité

August 20, 2021

Important La plate-forme FIPS MPX 9700/10500/12500/15500 est en fin de vie.

Vous pouvez configurer deux appliances dans une paire haute disponibilité (HA) en tant que appliances FIPS.

Conditions préalables

- Le module de sécurité matérielle (HSM) doit être configuré sur les deux appliances. Pour plus d'informations, voir Configurer le HSM.
- Lorsque vous utilisez l'interface graphique, vérifiez que les appliances sont déjà dans une configuration HA. Pour plus d'informations sur la configuration d'une configuration HA, voir Haute disponibilité.

Remarque : Citrix vous recommande d'utiliser l'utilitaire de configuration (GUI) pour cette procédure. Si vous utilisez la ligne de commande (CLI), assurez-vous de suivre attentivement les étapes indiquées dans la procédure. La modification de l'ordre des étapes ou la spécification d'un fichier d'entrée incorrect peut entraîner une incohérence nécessitant un redémarrage de l'appliance. En outre, si vous utilisez l'interface de ligne de commande, la commande `create ssl fipskey` n'est pas propagée vers le nœud secondaire. Lorsque vous exécutez la commande avec les mêmes valeurs d'entrée pour la taille du module et l'exposant sur deux appliances FIPS différentes, les clés générées ne sont pas les mêmes. Créez la clé FIPS sur l'un des nœuds, puis transférez-la vers l'autre nœud. Mais si vous utilisez l'utilitaire de configuration pour configurer les appliances FIPS dans une configuration HA, la clé FIPS que vous créez est automatiquement transférée vers le nœud secondaire. Le processus de gestion et de transfert des clés FIPS est connu sous le nom de gestion sécurisée de l'information (SIM).

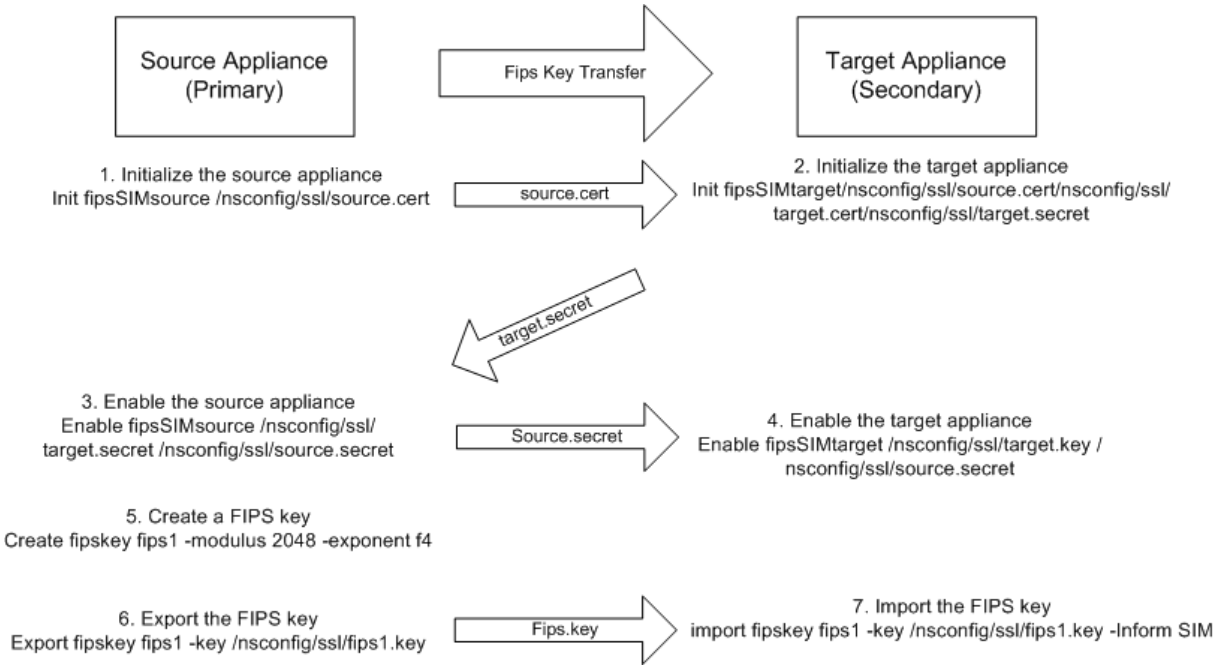
> **Important :** La configuration HA doit être terminée dans les six minutes. Si la procédure échoue à n'importe quelle étape, procédez comme suit :
>
> 1. Redémarrez l'appliance ou attendez 10 minutes.
> 2. Supprimez tous les fichiers créés par la procédure.
> 3. Répétez la procédure de configuration HA.
>
> Ne réutilisez pas les noms de fichiers existants.

Dans la procédure suivante, l'appliance A est le nœud principal et l'appliance B est le nœud secondaire.

Configurer FIPS sur les appliances dans une configuration haute disponibilité à l'aide de l'interface de ligne de commande

Le diagramme suivant résume le processus de transfert sur l'interface de ligne de commande.

Figure 1. Transférer le résumé des clés FIPS



1. **Sur l'appliance A**, ouvrez une connexion SSH à l'appliance à l'aide d'un client SSH, tel que PuTTY.
2. Ouvrez une session sur l'appliance à l'aide des informations d'identification de l'administrateur.
3. Initialisez l'appliance A en tant que appliance source. À l'invite de commandes, tapez :

   ```
   1 init ssl fipsSIMsource <certFile>
   2 <!--NeedCopy-->
   ```

   Exemple :

   ```
   init fipsSIMsource /nsconfig/ssl/nodeA.cert
   ```

4. Copiez ce fichier <certFile> dans l'appliance B, dans le dossier /nconfig/ssl.

   Exemple :

   ```
   scp /nsconfig/ssl/nodeA.cert nsroot@198.51.100.10:/nsconfig/ssl
   ```

5. **Sur l'appliance B**, ouvrez une connexion SSH à l'appliance à l'aide d'un client SSH, tel que PuTTY.
6. Ouvrez une session sur l'appliance à l'aide des informations d'identification de l'administrateur.

7. Initialisez l'appliance B en tant qu'appliance cible. À l'invite de commandes, tapez :

```
1 init ssl fipsSIMtarget <certFile> <keyVector> <targetSecret>
2 <!--NeedCopy-->
```

Exemple :

```
init fipsSIMtarget /nsconfig/ssl/nodeA.cert /nsconfig/ssl/nodeB.key /
nsconfig/ssl/nodeB.secret
```

8. Copiez ce fichier <targetSecret> dans l'appliance A.

Exemple :

```
scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.20:/nsconfig/
ssl
```

9. **Sur l'appliance A**, activez l'appliance A comme appliance source. À l'invite de commandes, tapez :

```
1 enable ssl fipsSIMSource <targetSecret> <sourceSecret>
2 <!--NeedCopy-->
```

Exemple :

```
enable fipsSIMsource /nsconfig/ssl/nodeB.secret /nsconfig/ssl/nodeA.
secret
```

10. Copiez ce fichier <sourceSecret> dans l'appliance B.

Exemple :

```
scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.10:/nsconfig/
ssl
```

11. **Sur l'appliance B**, activez l'appliance B en tant que solution cible. À l'invite de commandes, tapez :

```
1 enable ssl fipsSIMtarget <keyVector> <sourceSecret>
2 <!--NeedCopy-->
```

Exemple :

```
enable fipsSIMtarget /nsconfig/ssl/nodeB.key /nsconfig/ssl/nodeA.secret
```

12. **Sur l'appliance A**, créez une clé FIPS, comme décrit dans Créer une clé FIPS.
13. Exportez la clé FIPS vers le disque dur de l'appliance, comme décrit dans Exporter une clé FIPS.
14. Copiez la clé FIPS sur le disque dur de l'appliance secondaire à l'aide d'un utilitaire de transfert de fichiers sécurisé, tel que SCP.

15. **Sur l'appliance B**, importez la clé FIPS du disque dur dans le HSM de l'appliance, comme décrit dans Importer une clé FIPS existante.

Configurer FIPS sur les appliances dans une configuration haute disponibilité à l'aide de l'interface graphique

1. Sur l'appliance à configurer en tant qu'appliance source (principale), accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Infos FIPS, cliquez sur **Activer la carte SIM**.
3. Dans la boîte de dialogue **Activer la paire SIM pour la paire HA**, dans la zone de texte **Nom de fichier du certificat**, tapez le nom du fichier. Le nom de fichier doit contenir le chemin d'accès à l'emplacement où le certificat FIPS doit être stocké sur l'appliance source.
4. Dans la zone de texte **Nom de fichier du vecteur clé**, tapez le nom du fichier. Le nom de fichier doit contenir le chemin d'accès à l'emplacement où le vecteur de clé FIPS doit être stocké sur l'appliance source.
5. Dans la zone de texte **Nom de fichier secret cible**, tapez l'emplacement de stockage des données secrètes sur l'appliance cible.
6. Dans la zone de texte **Nom du fichier secret source**, tapez l'emplacement de stockage des données secrètes sur l'appliance source.
7. Sous **Informations d'identification de connexion système secondaire**, entrez les valeurs **Nom d'utilisateur** et **Mot de passe**.
8. Cliquez sur **OK**. Les appliances FIPS sont maintenant configurées en mode HA.

Remarque : Après avoir configuré les appliances dans HA, créez une clé FIPS, comme décrit dans Créer une clé FIPS. La clé FIPS est automatiquement transférée de l'appliance principale à l'appliance secondaire.

Mettre à jour le firmware vers la version 2.2 sur une carte FIPS

August 20, 2021

Important La plate-forme FIPS MPX 9700/10500/12500/15500 est en fin de vie.

La version 2.2 du firmware FIPS prend en charge les versions 1.1 et 1.2 du protocole TLS. À partir de la ligne de commande, vous pouvez mettre à jour la version du firmware de la carte FIPS d'une appliance FIPS Citrix ADC MPX 9700/10500/12500/15500 de la version 1.1 à la version 2.2.

Pour une propagation réussie de la clé SIM du primaire au secondaire dans une paire haute disponibilité (HA), la version du firmware Cavium sur chaque appliance doit être identique. Effectuez d'abord la mise à jour du microprogramme sur l'appliance secondaire. S'il est effectué en premier sur l'appliance principale, le processus de mise à jour de longue durée entraîne un basculement sur incident.

Limitations

- La renégociation sécurisée est prise en charge uniquement sur les serveurs virtuels SSL et les services SSL frontaux.
- La création d'une demande de signature de certificat à l'aide d'une clé créée sur la version 1.1 du firmware et mise à jour vers la version 2.2 du firmware échoue.
- Vous ne pouvez pas créer une clé RSA 1024 bits sur la version 2.2 du firmware. Toutefois, si vous avez importé ou créé une clé FIPS 1024 bits sur la version 1.1 du firmware et que vous mettez ensuite à jour vers la version 2.2 du firmware, vous pouvez utiliser cette clé FIPS sur la version 2.2 du firmware.
- Seules les clés RSA 2048 bits sont prises en charge.
- Le certificat client 4096 bits n'est pas pris en charge (si l'authentification client est activée sur le serveur principal).
- La renégociation sécurisée à l'aide du protocole SSLv3 n'est pas prise en charge.
- Après la mise à niveau du microprogramme, TLSv1.1 et TLSv1.2 sont désactivés par défaut sur le serveur virtuel, les services internes, frontaux et back-end existants. Pour utiliser TLS 1.1/1.2, vous devez activer explicitement ces protocoles, sur les entités SSL, après la mise à niveau.
- Les clés FIPS créées dans la version 2.2 du firmware ne sont pas disponibles si vous rétrogradez le firmware vers la version 1.1.

Conditions préalables

Téléchargez les fichiers suivants à partir de la page de téléchargement sur www.citrix.com. Les fichiers doivent être stockés dans le répertoire /var/nsinstall de l'appliance.

- FW 2.2 Fichier : FW-2.2-130013
- Fichier de signature FW 2.2 : FW-2.2-130013.Sign

FW-2.2-130013 est la version recommandée du firmware. Il inclut des correctifs pour améliorer DRBG.

Mettre à jour le firmware FIPS vers la version 2.2 sur une appliance autonome

1. Connectez-vous à l'appliance à l'aide des informations d'identification de l'administrateur.
2. À l'invite, tapez la commande suivante pour confirmer que la carte FIPS est initialisée.

```
1 show fips
2
3 FIPS HSM Info:
4 HSM Label       : Citrix ADC FIPS
5 Initialization      : FIPS-140-2 Level-2
```



```
HSM Serial Number   : 3.0G1235-ICM000264
HSM State       : 2
HSM Model       : NITROX XL CN1620-NFBE

Hardware Version    : 2.0-G
Firmware Version    : 1.1
Firmware Release Date   : Jun04,2010

Max FIPS Key Memory : 3996
Free FIPS Key Memory    : 3992
Total SRAM Memory   : 467348
Free SRAM Memory    : 62512
Total Crypto Cores  : 3
Enabled Crypto Cores    : 1
Done
<!--NeedCopy-->
```

3. Enregistrez la configuration. À l'invite, tapez :

```
save config
<!--NeedCopy-->
```

4. Effectuez la mise à jour. À l'invite, tapez :

```
update ssl fips -fipsFW <path to the extracted contents>/CN16XX-
   NFBE-FW-2.2-1300013
<!--NeedCopy-->
```

Appuyez sur Y lorsque l'invite suivante s'affiche :

```
This command will update compatible version of the FIPS firmware.
     You must save the current configuration (saveconfig) before
   executing this command. You must reboot the system after
   execution of this command, for the firmware update to take
   effect. Do you want to continue?(Y/N)Y

Done
<!--NeedCopy-->
```

Remarque : Il suffit de spécifier le fichier du microprogramme, car le fichier de signature du microprogramme est placé au même emplacement.

La mise à jour prend jusqu'à 10 secondes. La commande update est bloquée, ce qui signifie qu'aucune autre action n'est effectuée tant que la commande n'est pas terminée. L'invite de commande réapparaît lorsque l'exécution de la commande est terminée.

1. Redémarrez l'appliance. À l'invite, tapez :

```
reboot

Are you sure you want to restart NetScaler (Y/N)? [N]:Y
<!--NeedCopy-->
```

2. Vérifiez que la mise à jour est réussie. À l'invite, tapez :

```
show fips
<!--NeedCopy-->
```

   La version du firmware affichée dans la sortie doit être 2.2. Par exemple :

```
sh fips
    FIPS HSM Info:
        HSM Label       : Citrix ADC FIPS
        Initialization      : FIPS-140-2 Level-2
        HSM Serial Number   : 2.1G1207-IC002429
        HSM State       : 2
        HSM Model       : NITROX XL CN1620-NFBE

        Hardware Version    : 2.0-G
        Firmware Version    : 2.2
        Firmware Build          : NFBE-FW-2.2-130013
        Max FIPS Key Memory : 3996
        Free FIPS Key Memory    : 3982
        Total SRAM Memory   : 467348
        Free SRAM Memory    : 50472
        Total Crypto Cores  : 3
        Enabled Crypto Cores    : 1
Done
<!--NeedCopy-->
```

Mettre à jour le firmware FIPS vers la version 2.2 sur les appliances d'une paire haute disponibilité

1. Ouvrez une session sur le nœud secondaire et effectuez la mise à jour comme décrit dans « Mettre à jour le firmware FIPS vers la version 2.2 sur une appliance autonome ».

   Forcer le nœud secondaire à devenir principal. À l'invite, tapez :

```
force failover
<!--NeedCopy-->
```


Appuyez sur **Y** à l'invite de confirmation.

2. Connectez-vous au nouveau nœud secondaire (ancien nœud principal) et effectuez la mise à jour comme décrit dans « Mettre à jour le firmware FIPS vers la version 2.2 sur une appliance autonome ».
3. Forcer le nouveau nœud secondaire à redevenir primaire. À l'invite, tapez :

```
1 force failover
2 <!--NeedCopy-->
```

Appuyez sur **Y** à l'invite de confirmation.

Mettre à jour le firmware FIPS vers la version 1.1 sur une appliance autonome

1. Téléchargez les fichiers nfb_firmware-r1235_100604 et nfb_firmware-r1235_100604.sign dans le même répertoire de l'appliance, à partir de la page de téléchargement sur www.citrix.com.
2. Connectez-vous à l'appliance à l'aide des informations d'identification de l'administrateur.
3. À l'invite, tapez :

```
1 update ssl fips -fipsFW /<full path to the file>/nfb_firmware-
     r1235_100604
2 <!--NeedCopy-->
```

Réinitialiser un HSM verrouillé

August 20, 2021

Important La plate-forme FIPS MPX 9700/10500/12500/15500 est en fin de vie.

Le HSM devient verrouillé (plus opérationnel) si vous modifiez le mot de passe SO, redémarrez l'appliance sans enregistrer la configuration et effectuez trois tentatives infructueuses de modification du mot de passe. Le verrouillage est une mesure de sécurité pour empêcher les tentatives d'accès non autorisées et les modifications apportées aux paramètres HSM.

Important : Pour éviter cette situation, enregistrez la configuration après l'initialisation du HSM.
Si le HSM est verrouillé, vous devez réinitialiser le HSM et redémarrer l'appliance pour restaurer les mots de passe par défaut. Vous pouvez ensuite utiliser les mots de passe par défaut pour accéder au HSM et le configurer avec de nouveaux mots de passe. Lorsque vous avez terminé, vous devez enregistrer la configuration et redémarrer l'appliance.

Attention : Réinitialisez le HSM uniquement s'il est verrouillé.

Réinitialiser un HSM verrouillé à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour réinitialiser et réinitialiser un HSM verrouillé :

```
reset ssl fips
reboot -warm
set ssl fips -initHSM Level-2 <new SO password> <old SO password> <user
    password> [-hsmLabel <string>]
save ns config
reboot -warm
<!--NeedCopy-->
```

Exemple :

```
reset fips

reboot -warm

set fips -initHSM Level-2 newsopin123 sopin123 userpin123 -hsmLabel
   NSFIPS

saveconfig

reboot -warm

Note: By default the HSM passwords are preconfigured. The <
   Old_SO_Password> = so12345, <User_Password> = user123, <
   New_SO_Password> = sopin12345, <New_User_Password> = userpin123.
<!--NeedCopy-->
```

Réinitialiser un HSM verrouillé à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > FIPS**
2. Dans le volet d'informations, sous l'onglet Informations FIPS, cliquez sur Réinitialiser FIPS.
3. Configurez le HSM, comme décrit dans Configuration du HSM.
4. Dans le volet d'informations, cliquez sur Enregistrer.

Appareils FIPS MPX 14000

October 5, 2021

> **Important :**
>
> - La plate-forme FIPS MPX 9700/10500/12500/15500 est en fin de vie.
> - Les étapes de configuration des appliances FIPS NetScaler MPX 14000 et NetScaler MPX 9700/10500/12500/15500 FIPS sont différentes. Les appareils MPX 14000 FIPS n'utilisent pas le firmware v2.2. Une clé FIPS créée sur le module de sécurité matérielle (HSM) de la plate-forme MPX 9700 ne peut pas être transférée vers le HSM de la plate-forme MPX 14000. L'inverse n'est pas non plus pris en charge. Toutefois, si vous avez importé une clé RSA en tant que clé FIPS, vous pouvez copier la clé RSA sur la plate-forme MPX 14000. Importez-le ensuite en tant que clé FIPS. Seules les clés 2048 bits et 3072 bits sont prises en charge.

Un appareil FIPS est équipé d'un module cryptographique inviolable (inviolable) — un Cavium CNN3560-NFBE-G — conçu pour répondre aux spécifications FIPS 140-2 Niveau 3 (de la version 12.0 build 56.x). Les paramètres de sécurité critiques (CSP), principalement la clé privée du serveur, sont stockés et générés en toute sécurité dans le module cryptographique, également appelé HSM. Les CSP ne sont jamais accessibles à l'extérieur des limites du HSM. Seul le superutilisateur (`nsroot`) peut effectuer des opérations sur les clés stockées dans le HSM.

Avant de configurer un dispositif FIPS, vous devez vérifier l'état de la carte FIPS, puis initialiser la carte. Créez une clé FIPS et un certificat de serveur, et ajoutez toute configuration SSL supplémentaire.

Pour plus d'informations sur les chiffrements FIPS pris en charge, consultez Algorithmes et chiffrements approuvés FIPS.

Pour plus d'informations sur la configuration des appliances FIPS dans une configuration HA, voir Configurer FIPS sur les appliances dans une configuration HA.

Limitations

1. La renégociation SSL à l'aide du protocole SSLv3 n'est pas prise en charge sur le back-end d'une appliance MPX FIPS.
2. Les clés 1024 bits et 4096 bits et la valeur de l'exposant 3 ne sont pas prises en charge.
3. Le certificat serveur 4096 bits n'est pas pris en charge.
4. Le certificat client 4096 bits n'est pas pris en charge (si l'authentification client est activée sur le serveur principal).

Configurer le HSM

Avant de configurer le HSM sur une appliance FIPS MPX 14000, vérifiez l'état de votre carte FIPS pour vérifier que le pilote s'est correctement chargé. Initialisez ensuite la carte.

À l'invite de commandes, tapez :


```
show fips

FIPS Card is not configured
<!--NeedCopy-->
```

Le message « ERREUR : opération non autorisée - aucune carte FIPS présente dans le système » s'affiche si le pilote n'est pas correctement chargé.

Initialiser la carte FIPS

La solution matérielle-logicielle doit être redémarrée trois fois pour que la carte FIPS soit correctement initialisée.

> **Important**
>
> - Vérifiez que le `/nsconfig/fips` répertoire a bien été créé sur l'appliance.
> - N'enregistrez pas la configuration avant de redémarrer l'appliance pour la troisième fois.

Pour initialiser la carte FIPS, effectuez les opérations suivantes :

1. Réinitialisez la carte FIPS.
2. Redémarrez l'appliance.
3. Définissez le mot de passe du responsable de la sécurité pour les partitions 0 et 1, et le mot de passe utilisateur pour la partition

   Remarque : L'exécution de la commande set ou reset prend plus de 60 secondes.
4. Enregistrez la configuration.
5. Vérifiez que la clé chiffrée par mot de passe de la partition principale (master_pek.key) a été créée dans le `/nsconfig/fips/` répertoire.
6. Redémarrez l'appliance.
7. Vérifiez que la clé chiffrée par mot de passe de la partition par défaut (default_pek.key) a été créée dans le `/nsconfig/fips/` répertoire.
8. Redémarrez l'appliance.
9. Vérifiez que la carte FIPS est en état de fonctionnement.

Initialisez la carte FIPS à l'aide de l'interface de ligne de commande

La `set fips` commande initialise le module de sécurité matérielle (HSM) sur la carte FIPS et définit un nouveau mot de passe du responsable de la sécurité et un nouveau mot de passe utilisateur.

Attention : Cette commande efface toutes les données de la carte FIPS. Vous y êtes invité avant de poursuivre l'exécution de la commande. Un redémarrage est nécessaire avant et après l'exécution de cette commande pour que les modifications s'appliquent. Enregistrez la configuration après avoir exécuté cette commande et avant de redémarrer la solution matérielle-logicielle.

À l'invite de commandes, tapez les commandes suivantes :

```
reset fips

reboot

set fips -initHSM Level-2 so12345 so12345 user123 -hsmLabel NSFIPS

This command will erase all data on the FIPS card. You must save the
   configuration (saveconfig) after executing this command. Do you want
    to continue?(Y/N)y

<!--NeedCopy-->
```

Remarque : Le message suivant s'affiche lorsque vous exécutez la `set fips` commande :

```
This command will erase all data on the FIPS card. You must save the
   configuration (saveconfig) after executing this command. [Note: On
   MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
   default, and the -initHSM Level-2 option is internally converted to
   Level-3]  Do you want to continue?(Y/N)y

saveconfig

reboot

reboot

show fips

        FIPS HSM Info:
                HSM Label               : NetScaler FIPS
                Initialization          : FIPS-140-2 Level-3
                HSM Serial Number       : 3.1G1836-ICM000136
                HSM State               : 2
                HSM Model               : NITROX-III CNN35XX-NFBE
                Hardware Version        : 0.0-G
                Firmware Version        : 1.0
                Firmware Build          : NFBE-FW-1.0-48
                Max FIPS Key Memory     : 102235
```



```
21                  Free FIPS Key Memory    : 102231
22                  Total SRAM Memory       : 557396
23                  Free SRAM Memory        : 262780
24                  Total Crypto Cores      : 63
25                  Enabled Crypto Cores    : 63
26
27 <!--NeedCopy-->
```

Créer une clé FIPS

Vous pouvez créer une clé FIPS sur votre appliance FIPS MPX 14000 ou importer une clé FIPS existante dans l'appliance. L'appliance FIPS MPX 14000 ne prend en charge que les clés 2048 bits et 3072 bits et une valeur d'exposant F4 (dont la valeur est 65537). Pour les clés PEM, aucun exposant n'est requis. Vérifiez que la clé FIPS a été créée correctement. Créez une demande de signature de certificat et un certificat de serveur. Enfin, ajoutez la paire de clés de certificat à votre solution matérielle-logicielle.

Spécifiez le type de clé (RSA ou ECDSA). Pour les clés ECDSA, spécifiez uniquement la courbe. La création de clés ECDSA avec les courbes P_256 et P_384 est prise en charge.

> **Remarque :**
>
> Les clés 1024 bits et 4096 bits et une valeur d'exposant de 3 ne sont pas prises en charge.

Créer une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 create ssl fipsKey <fipsKeyName> -keytype ( RSA | ECDSA ) [-exponent (
     3 | F4 )] [-modulus <positive_integer>] [-curve ( P_256 | P_384 )]
2 <!--NeedCopy-->
```

Example1:

```
1 create fipsKey f1 -keytype RSA -modulus 2048 -exponent F4
2
3
4 show ssl fipskey f1
5
6 FIPS Key Name: f1  Key Type: RSA Modulus: 2048   Public Exponent: F4 (
     Hex: 0x10001)
7
8 <!--NeedCopy-->
```

Example2:


```
> create fipskey f2 -keytype ECDSA -curve P_256


> sh fipskey f2
    FIPS Key Name: f2   Key Type: ECDSA Curve: P_256

<!--NeedCopy-->
```

Créer une clé FIPS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Clés FIPS, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Créer une clé FIPS, spécifiez les valeurs des paramètres suivants :
   - Nom de clé FIPS* : nom de clé FIPSKey
   - Module* : module
   - Exposant* : exposant

   *Paramètre obligatoire
4. Cliquez sur **Créer**, puis cliquez sur **Fermer**.
5. Sous l'onglet Touches FIPS, vérifiez que les paramètres affichés pour la clé FIPS que vous avez créée sont corrects.

Importer une clé FIPS

Pour utiliser une clé FIPS existante avec votre appliance FIPS, vous devez transférer la clé FIPS du disque dur de l'appliance vers son HSM.

Remarque : Pour éviter les erreurs lors de l'importation d'une clé FIPS, assurez-vous que le nom de la clé importée est identique au nom de clé d'origine lors de sa création.

Importer une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-
    wrapKeyName <string>] [-iv<string>] -exponent  F4 ]
<!--NeedCopy-->
```

Exemple :


```
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4


import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform PEM

<!--NeedCopy-->
```

Vérifiez que la clé FIPS est créée ou importée correctement en exécutant la commande `show fipskey`.

```
show fipskey
1)      FIPS Key Name: Key-FIPS-2

<!--NeedCopy-->
```

Importer une clé FIPS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Clés FIPS, cliquez sur **Importer**.
3. Dans la boîte de dialogue Importer en tant que clé FIPS, sélectionnez le fichier de clé FIPS et définissez les valeurs des paramètres suivants :
   - Nom de la clé FIPS*
   - Nom du fichier clé* : pour placer le fichier dans un emplacement autre que celui par défaut, spécifiez le chemin complet ou cliquez sur **Parcourir** et accédez à un emplacement.
   - Exposant*

   *Paramètre obligatoire
4. Cliquez sur **Importer**, puis cliquez sur **Fermer**.
5. Sous l'onglet Touches FIPS, vérifiez que les paramètres affichés pour la clé FIPS que vous avez importée sont corrects.

Exporter une clé FIPS

Citrix vous recommande de créer une sauvegarde de toute clé créée dans le HSM FIPS. Si une clé du HSM est supprimée, vous ne pouvez plus créer la même clé et tous les certificats associés sont rendus inutiles.

Outre l'exportation d'une clé en tant que sauvegarde, vous devrez peut-être exporter une clé pour le transfert vers une autre appliance.

La procédure suivante fournit des instructions sur l'exportation d'une clé FIPS vers le /nsconfig/ssl dossier du CompactFlash de la solution matérielle-logicielle et sur la sécurisation de la clé exportée à l'aide d'une méthode de chiffrement à clé asymétrique forte.

Exportation d'une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
export ssl fipsKey <fipsKeyName> -key <string>
<!--NeedCopy-->
```

Exemple :

```
export fipskey Key-FIPS-1 -key Key-FIPS-1.key
<!--NeedCopy-->
```

Exporter une clé FIPS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Clés FIPS, cliquez sur **Exporter**.
3. Dans la boîte de dialogue Exporter la clé FIPS vers un fichier, spécifiez les valeurs des paramètres suivants :
   - Nom de clé FIPS* : nom de clé FIPSKey
   - Nom du fichier* : touche (Pour placer le fichier à un emplacement autre que celui par défaut, vous pouvez spécifier le chemin d'accès complet ou cliquer sur le bouton Parcourir et accéder à un emplacement.)

   *Paramètre obligatoire
4. Cliquez sur **Exporter**, puis sur **Fermer**.

Importer une clé externe

Vous pouvez transférer des clés FIPS créées dans le HSM de l'appliance Citrix ADC. Vous pouvez également transférer des clés privées externes (telles que des clés créées sur un Citrix ADC, Apache ou IIS standard) vers une appliance Citrix ADC FIPS. Les clés externes sont créées en dehors du HSM, à l'aide d'un outil tel qu'OpenSSL. Avant d'importer une clé externe dans le HSM, copiez-la sur le lecteur flash de l'appliance sous /nsconfig/ssl.

Sur les appliances FIPS MPX 14000, le paramètre -exponent de la **import** ssl fipskey commande n'est pas requis lors de l'importation d'une clé externe. L'exposant public correct est détecté automatiquement lorsque la clé est importée et la valeur du paramètre -exponent est ignorée.

L'appliance Citrix ADC FIPS ne prend pas en charge les clés externes avec un exposant public autre que 3 ou F4.

Vous n'avez pas besoin d'une clé d'enroulement sur les appliances FIPS MPX 14000.

Vous ne pouvez pas importer de clé FIPS externe chiffrée directement sur une appliance FIPS MPX 14000. Pour importer la clé, vous devez d'abord la déchiffrer, puis l'importer. Pour déchiffrer la clé, à l'invite du shell, tapez :

```
openssl rsa -in <EncryptedKey.key> > <DecryptedKey.out>
<!--NeedCopy-->
```

Remarque : Si vous importez une clé RSA en tant que clé FIPS, Citrix vous recommande de supprimer la clé RSA de l'appliance à des fins de sécurité.

Importer une clé externe en tant que clé FIPS à l'aide de l'interface de ligne de commande

1. Copiez la clé externe sur le lecteur flash de l'appliance.
2. Si la clé est au format .pfx, vous devez d'abord la convertir au format PEM. À l'invite de commandes, tapez :

   ```
   convert ssl pkcs12 <output file> -import -pkcs12File <input .pfx
       file name> -password <password>
   <!--NeedCopy-->
   ```

3. À l'invite de commandes, tapez les commandes suivantes pour importer la clé externe en tant que clé FIPS et vérifier les paramètres :

   ```
   import ssl fipsKey <fipsKeyName> -key <string> -informPEM
   show ssl fipskey<fipsKeyName>
   <!--NeedCopy-->
   ```

Exemple :

```
convert ssl pkcs12 iis.pem -password 123456 -import -pkcs12File iis.pfx

import fipskey Key-FIPS-2 -key iis.pem -inform PEM

show ssl fipskey key-FIPS-2

FIPS Key Name: Key-FIPS-2 Modulus: 0   Public Exponent: F4 (Hex value 0
    x10001)
<!--NeedCopy-->
```


Importer une clé externe en tant que clé FIPS à l'aide de l'interface graphique

1. Si la clé est au format .pfx, vous devez d'abord la convertir au format PEM.

   a) Accédez à **Gestion du trafic > SSL**.
   b) Dans le volet d'informations, sous Outils, cliquez sur **Importer PKCS #12**.
   c) Dans la boîte de dialogue Importer un fichier PKCS12, définissez les paramètres suivants :
      - Nom du fichier de sortie*
      - Nom du fichier PKCS12* : spécifiez le nom du fichier .pfx.
      - Mot de passe d'importation*
      - Format d'encodage

      *Un paramètre obligatoire
2. Accédez à **Gestion du trafic > SSL > FIPS**.
3. Dans le volet d'informations, sous l'onglet Clés FIPS, cliquez sur **Importer**.
4. Dans la boîte de dialogue Importer en tant que clé FIPS, sélectionnez le fichier PEM et définissez les valeurs des paramètres suivants :

   - Nom de la clé FIPS*
   - Nom du fichier clé* : pour placer le fichier dans un emplacement autre que celui par défaut, vous pouvez spécifier le chemin d'accès complet ou cliquer sur Parcourir et accéder à un emplacement.

   *Paramètre obligatoire
5. Cliquez sur **Importer**, puis cliquez sur **Fermer**.
6. Sous l'onglet Touches FIPS, vérifiez que les paramètres affichés pour la clé FIPS que vous avez importée sont corrects.

Configurer FIPS sur des appliances dans une configuration HA

Vous pouvez configurer deux appliances dans une paire HA en tant qu'appliances FIPS.

Conditions préalables

- Le module de sécurité matérielle (HSM) doit être configuré sur les deux appliances. Pour plus d'informations, voir Configurer le HSM.
- Lorsque vous utilisez l'interface graphique, vérifiez que les appliances sont déjà dans une configuration HA. Pour plus d'informations sur la configuration d'une configuration HA, voir Haute disponibilité.

> **Remarque :**
>
> Citrix recommande d'utiliser l'utilitaire de configuration (GUI) pour cette procédure. Si vous utilisez la ligne de commande (CLI), assurez-vous de suivre attentivement les étapes indiquées dans la procédure. La modification de l'ordre des étapes ou la spécification d'un fichier d'entrée incorrect peut entraîner une incohérence nécessitant un redémarrage de la solution matérielle-logicielle. En outre, si vous utilisez l'interface de ligne de commande, la `create ssl fipskey` commande n'est pas propagée au nœud secondaire. Lorsque vous exécutez la commande avec les mêmes valeurs d'entrée pour la taille du module et l'exposant sur deux dispositifs FIPS différents, les clés générées ne sont pas les mêmes. Créez la clé FIPS sur l'un des nœuds, puis transférez-la vers l'autre nœud. Toutefois, si vous utilisez l'utilitaire de configuration pour configurer des dispositifs FIPS dans une configuration HA, la clé FIPS que vous créez est automatiquement transférée vers le nœud secondaire. Le processus de gestion et de transfert des clés FIPS est connu sous le nom de gestion sécurisée des informations (SIM).

Important : La configuration de la haute disponibilité doit être terminée dans un délai de six minutes. Si la procédure échoue à une étape quelconque, procédez comme suit :

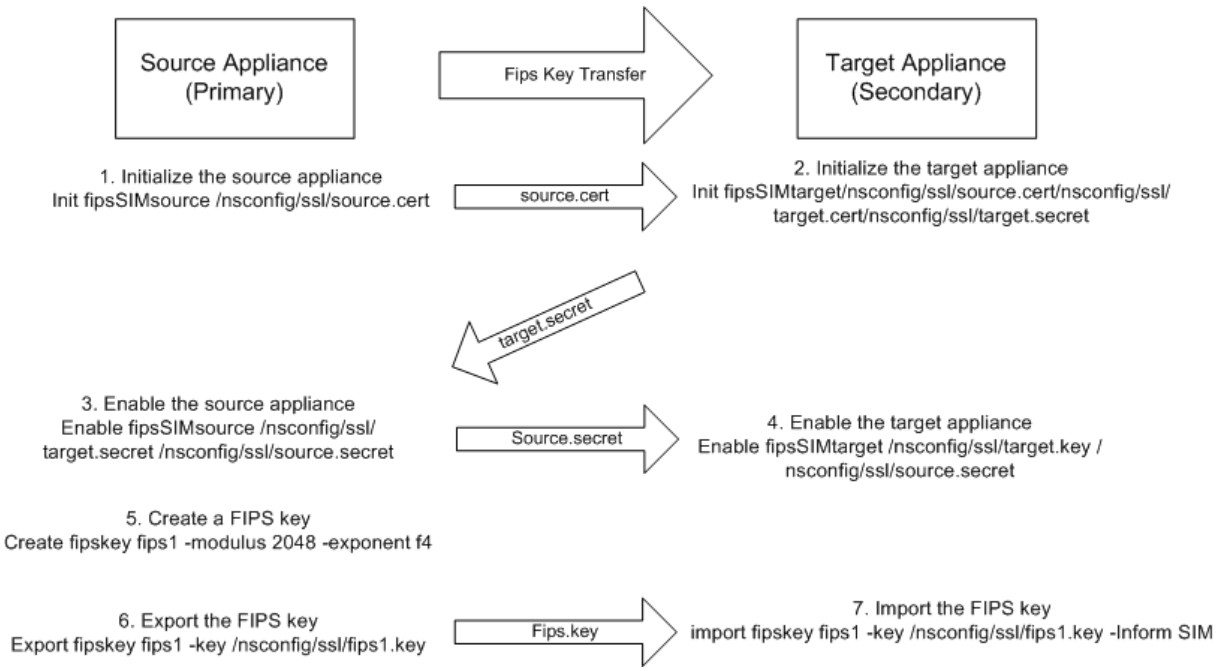
> 1. Redémarrez la solution matérielle-logicielle ou attendez 10 minutes.
> 2. Supprimez tous les fichiers créés par la procédure.
> 3. Répétez la procédure de configuration HA.
>
> Ne réutilisez pas les noms de fichiers existants.

Dans la procédure suivante, l'appliance A est le nœud principal et l'appliance B est le nœud secondaire.

Configurer FIPS sur des appliances dans une configuration HA à l'aide de l'interface de ligne de commande

Le diagramme suivant résume le processus de transfert sur l'interface de ligne de commande.

Figure 1. Transférer le récapitulatif des clés FIPS



1. **Sur l'appliance A**, ouvrez une connexion SSH à l'appliance à l'aide d'un client SSH, tel que PuTTY.
2. Ouvrez une session sur la solution matérielle-logicielle à l'aide des informations d'identification de l'administrateur.
3. Initialisez l'appliance A en tant que solution matérielle-logicielle source. À l'invite de commandes, tapez :

```
1 init ssl fipsSIMsource <certFile>
2 <!--NeedCopy-->
```

Exemple :

```
init fipsSIMsource /nsconfig/ssl/nodeA.cert
```

4. Copiez ce <certFile> fichier sur l'appliance B, dans le dossier /nconfig/ssl.

Exemple :

```
scp /nsconfig/ssl/nodeA.cert nsroot@198.51.100.10:/nsconfig/ssl
```

5. **Sur l'appliance B**, ouvrez une connexion SSH à l'appliance à l'aide d'un client SSH, tel que PuTTY.
6. Ouvrez une session sur la solution matérielle-logicielle à l'aide des informations d'identification de l'administrateur.
7. Initialisez l'appliance B en tant qu'appliance cible. À l'invite de commandes, tapez :

```
1 init ssl fipsSIMtarget <certFile> <keyVector> <targetSecret>
```



```
2 <!--NeedCopy-->
```

Exemple :

```
init fipsSIMtarget /nsconfig/ssl/nodeA.cert /nsconfig/ssl/nodeB.key /
nsconfig/ssl/nodeB.secret
```

8. Copiez ce <targetSecret> fichier sur l'appliance A.

   Exemple :

   ```
   scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.20:/nsconfig/
   ssl
   ```

9. **Sur l'appliance A**, activez l'appliance A en tant que solution matérielle-logicielle source. À l'invite de commandes, tapez :

   ```
   1 enable ssl fipsSIMSource <targetSecret> <sourceSecret>
   2 <!--NeedCopy-->
   ```

   Exemple :

   ```
   enable fipsSIMsource /nsconfig/ssl/nodeB.secret /nsconfig/ssl/nodeA.
   secret
   ```

10. Copiez ce <sourceSecret> fichier sur l'appliance B.

    Exemple :

    ```
    scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.10:/nsconfig/
    ssl
    ```

11. **Sur l'appliance B**, activez l'appliance B en tant qu'appliance cible. À l'invite de commandes, tapez :

    ```
    1 enable ssl fipsSIMtarget <keyVector> <sourceSecret>
    2 <!--NeedCopy-->
    ```

    Exemple :

    ```
    enable fipsSIMtarget /nsconfig/ssl/nodeB.key /nsconfig/ssl/nodeA.secret
    ```

12. **Sur l'appliance A**, créez une clé FIPS, comme décrit dans Créer une clé FIPS.
13. Exportez la clé FIPS vers le disque dur de l'appliance, comme décrit dans Exporter une clé FIPS.
14. Copiez la clé FIPS sur le disque dur de l'appliance secondaire à l'aide d'un utilitaire de transfert de fichiers sécurisé, tel que SCP.
15. **Sur l'appliance B**, importez la clé FIPS du disque dur dans le HSM de l'appliance, comme décrit dans Importer une clé FIPS.

Configurer FIPS sur des appliances dans une configuration HA à l'aide de l'interface graphique

1. Sur l'appliance à configurer en tant qu'appliance source (principale), accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Informations FIPS, cliquez sur **Activer la carte SIM**.
3. Dans la boîte de dialogue **Activer la carte SIM pour la paire HA**, dans la zone de texte **Nom du fichier de certificat**, tapez le nom du fichier. Le nom du fichier doit contenir le chemin d'accès à l'emplacement où le certificat FIPS doit être stocké sur l'appliance source.
4. Dans la zone de texte **Nom du fichier vectoriel clé**, tapez le nom du fichier. Le nom du fichier doit contenir le chemin d'accès à l'emplacement où le vecteur de clé FIPS doit être stocké sur l'appliance source.
5. Dans la zone de texte **Nom du fichier secret cible**, tapez l'emplacement de stockage des données secrètes sur le dispositif cible.
6. Dans la zone de texte **Nom du fichier secret source**, tapez l'emplacement de stockage des données secrètes sur le dispositif source.
7. Sous **Secondary System Login Credential**, entrez les valeurs du **nom d'utilisateur et dumot de passe**.
8. Cliquez sur **OK**. Les appliances FIPS sont maintenant configurées en mode HA.

Remarque : Après avoir configuré les appliances dans HA, créez une clé FIPS, comme décrit dans Créer une clé FIPS. La clé FIPS est automatiquement transférée de l'appliance principale à l'appliance secondaire.

Créer une demande de signature de certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
    <string>) [-keyform ( DER | PEM )  {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName<string>
    [-organizationUnitName <string>] [-localityName <string>] [-
    commonName <string>] [-emailAddress <string>] {
 -challengePassword  }
  [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
<!--NeedCopy-->
```

Exemple :

```
>create certreq f1.req  - fipsKeyName  f1 -countryName US  -stateName CA
     -organizationName Citrix -companyName Citrix -commonName ctx -
    emailAddress test@example.com
```



```
2 Done
3 <!--NeedCopy-->
```

Créer un certificat de serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 create ssl cert <certFile> <reqFile> <certType> [-keyFile <
     input_filename>] [-keyform ( DER | PEM ) {
2  -PEMPassPhrase  }
3  ] [-days <positive_integer>] [-certForm ( DER | PEM )] [-CAcert <
      input_filename>] [-CAcertForm ( DER | PEM )] [-CAkey <
      input_filename>][-CAkeyForm ( DER | PEM )] [-CAserial <
      output_filename>]
4 <!--NeedCopy-->
```

Exemple :

```
1 create cert f1.cert f1.req SRVR_CERT -CAcert ns-root.cert -CAkey ns-
     root.key -CAserial ns-root.srl -days 1000
2 Done
3 <!--NeedCopy-->
```

L'exemple précédent crée un certificat de serveur à l'aide d'une autorité de certification racine locale sur l'appliance.

Ajouter une paire de clés de certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
     string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>][-
     expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
     positive_integer>]] [-bundle ( YES | NO )]
2 <!--NeedCopy-->
```

Exemple :

```
1 add certkey cert1 -cert f1.cert -fipsKey f1
2
3 <!--NeedCopy-->
```

Après avoir créé la clé FIPS et le certificat de serveur, vous pouvez ajouter la configuration SSL générique. Activez les fonctionnalités requises pour votre déploiement. Ajoutez des serveurs, des

services et des serveurs virtuels SSL. Liez la paire de clés de certificat et le service au serveur virtuel SSL. Enregistrez la configuration.

```
enable ns feature SSL LB

add server s1 10.217.2.5

add service sr1 s1 HTTP 80

add lb vserver v1 SSL 10.217.2.172 443

bind ssl vserver v1  -certkeyName cert1

bind lb vserver v1 sr1

saveconfig

<!--NeedCopy-->
```

La configuration de base de votre appliance MPX 14000 FIPS est maintenant terminée.

Pour plus d'informations sur la configuration de HTTPS sécurisé, cliquez sur Configurer FIPS.

Pour plus d'informations sur la configuration du RPC sécurisé, cliquez sur Configurer FIPS pour la première fois.

Mettre à jour la licence sur un dispositif FIPS MPX 14000

Toute mise à jour de la licence sur cette plate-forme nécessite deux redémarrages.

1. Mettez à jour la licence dans le `/nsconfig/license` dossier.
2. Redémarrez l'appliance.
3. Ouvrez une session sur la solution matérielle-logicielle.
4. Redémarrez l'appliance à nouveau.
   Remarque : N'ajoutez pas de nouvelles commandes, n'enregistrez pas la configuration et ne vérifiez pas l'état du système avant le deuxième redémarrage.
5. Ouvrez une session sur la solution matérielle-logicielle et vérifiez que FIPS est initialisé en exécutant la `show ssl fips` commande.

Prise en charge du mode FIPS hybride sur les plates-formes FIPS MPX 14000 et SDX 14000 FIPS

> **Remarque :**
>
> Cette fonctionnalité n'est prise en charge que sur la nouvelle plate-forme FIPS MPX/SDX 14000 contenant une carte FIPS principale et une ou plusieurs cartes secondaires. Il n'est pas pris en charge sur une plate-forme VPX ou une plate-forme contenant un seul type de carte matérielle.

Sur une plateforme FIPS, le chiffrement et le déchiffrement asymétriques et symétriques sont effectués sur la carte FIPS pour des raisons de sécurité. Toutefois, vous pouvez effectuer une partie de cette activité (asymétrique) sur une carte FIPS et décharger le chiffrement et le déchiffrement en masse (symétrique) sur une autre carte sans compromettre la sécurité de vos clés.

La nouvelle plateforme FIPS MPX/SDX 14000 contient une carte principale et une ou plusieurs cartes secondaires. Si vous activez le mode FIPS hybride, les commandes de déchiffrement secret prémaître sont exécutées sur la carte principale car la clé privée est stockée sur cette carte. Toutefois, le chiffrement et le déchiffrement en masse sont déchargés sur la carte secondaire. Ce déchargement augmente considérablement le débit de chiffrement en masse sur une plate-forme FIPS MPX/SDX 14000 par rapport au mode FIPS non hybride et à la plate-forme FIPS MPX 9700/10500/12500/15000 existante. L'activation du mode FIPS hybride améliore également la transaction SSL par seconde sur cette plate-forme.

> **Remarques :**
>
> - Le mode FIPS hybride est désactivé par défaut pour répondre aux exigences de certification strictes, où tous les calculs cryptographiques doivent être effectués dans un module certifié FIPS. Activez le mode hybride pour décharger le chiffrement et le déchiffrement en masse sur la carte secondaire.
> - Sur une plate-forme FIPS SDX 14000, vous devez d'abord attribuer une puce SSL à l'instance VPX avant d'activer le mode hybride.

Activer le mode FIPS hybride à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set SSL parameter -hybridFIPSMode {
 ENABLED|DISABLED }


Arguments

hybridFIPSMode

When this mode is enabled, system will use additional crypto hardware
    to accelerate symmetric crypto operations.

```



```
Possible values: ENABLED, DISABLED

Default value: DISABLED
<!--NeedCopy-->
```

Exemple :

```
    set SSL parameter -hybridFIPSMode ENABLED
    show SSL parameter
    Advanced SSL Parameters
    ----------------------
    . . . . . .
    Hybrid FIPS Mode    : ENABLED
    . . . . . .

<!--NeedCopy-->
```

Activer le mode FIPS hybride à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres SSL avancés**.
3. Dans la boîte de dialogue **Modifier les paramètres SSL avancés**, sélectionnez **Mode FIPS hybride**.

Limitations :

1. La renégociation n'est pas prise en charge.
2. La `stat ssl parameter` commande sur une plate-forme SDX 14000 n'affiche pas le pourcentage d'utilisation de la carte secondaire correct. Il affiche toujours 0,00% d'utilisation.

```
stat ssl

SSL Summary
# SSL cards present 1
# SSL cards UP  1
# Secondary SSL cards present   4
# Secondary SSL cards UP    4
SSL engine status      1
SSL sessions (Rate)     963
Secondary card utilization (%)     0.00
<!--NeedCopy-->
```


Appliances SDX 14000 FIPS

August 20, 2021

Une appliance Citrix ADC SDX est une plate-forme multilocataire sur laquelle vous pouvez provisionner et gérer plusieurs instances Citrix ADC virtuelles. L'appliance SDX répond aux exigences de cloud computing et de multilocation en permettant à un administrateur unique de configurer et de gérer l'appliance et de déléguer l'administration de chaque instance hébergée aux locataires.

Une appliance Citrix ADC SDX 14030/14060/14080 FIPS fournit les fonctionnalités d'une appliance SDX dotée de fonctionnalités FIPS. Il est équipé d'un module cryptographique inviolable (inviolable) — un Cavium CNN3560-NFBE-G — conçu pour répondre aux spécifications FIPS 140-2 Niveau 3 (de la version 12.0 build 56.x). Les paramètres de sécurité critiques (CSP), principalement la clé privée du serveur, sont stockés en toute sécurité et générés à l'intérieur du module cryptographique. Ce module est également appelé Hardware Security Module (HSM). Les CSP ne sont jamais accessibles à l'extérieur des limites du HSM. Seul le superutilisateur (`nsroot`) peut effectuer des opérations sur les clés stockées dans le HSM.

Une appliance Citrix ADC SDX 14030/14060/14080 FIPS contient un module FIPS HSM avec 63 cœurs. Le module FIPS HSM peut être partitionné jusqu'à un maximum de 32 partitions. L'administrateur SDX peut affecter un stockage de clés dédié, des ressources cryptographiques et le nombre de cœurs FIPS SSL crypto à chaque partition. Les clés et les ressources allouées à une partition sont dédiées et sécurisées et toute autre partition ne peut pas y accéder ni les partager.

La partition HSM FIPS que vous créez peut être affectée ou attachée à une instance VPX au moment du Provisioning de l'instance, ou ultérieurement en modifiant l'instance. La partition FIPS créée et attachée à une instance agit comme un module HSM virtuel pour cette instance.

Les instances VPX sur un dispositif FIPS SDX 14030/14060/14080 se voient attribuer une partition FIPS Virtual Function (VF), qui est traitée comme une carte virtuelle FIPS isolée ou HSM. Par conséquent, les étapes de configuration d'une partition FIPS à l'intérieur d'une instance VPX sont similaires à celles de configuration d'une appliance MPX FIPS. Pour plus de détails sur la conformité, consultez les détails de la politique de sécurité sur le site Web du National Institute of Standards and Technology (NIST) des États-Unis.

Pour plus d'informations sur la configuration des appliances FIPS dans une configuration haute disponibilité, consultez Appliances FIPS dans une configuration haute disponibilité.

> **Important**
>
> Chaque clé comprend une clé privée et une clé publique. En conséquence, il occupe deux espaces clés. Par conséquent, le nombre maximal de clés est limité à moins de la moitié de la taille du magasin de clés.

La plate-forme FIPS SDX 14000 prend en charge un mode FIPS hybride. Ce mode vous permet de décharger une partie de l'activité de chiffrement et de déchiffrement sur une carte non-FIPS. Pour plus d'informations, voir Mode FIPS hybride.

Limitations

January 21, 2021

1. La renégociation SSL à l'aide du protocole SSLv3 n'est pas prise en charge sur le back-end d'une appliance SDX FIPS.
2. Les clés 1024 bits et 4096 bits et une valeur exposant de 3 ne sont pas prises en charge.
3. La sauvegarde et la restauration ne sont pas prises en charge.
4. Les domaines de cluster et d'administration ne sont pas pris en charge.
5. Vous ne pouvez attacher qu'une seule partition FIPS à une instance.
6. Une instance avec une partition FIPS ne peut être affectée qu'à un seul cœur de CPU.
7. Vous pouvez attribuer une partition FIPS ou un cœur SSL à une instance, mais pas les deux.
8. Le certificat de serveur 4096 bits n'est pas pris en charge.
9. Le certificat client 4096 bits n'est pas pris en charge (si l'authentification client est activée sur le serveur principal).

Terminologie

February 12, 2021

Zeroize : réinitialise le HSM. Toutes les données du HSM sont supprimées. Cette étape est obligatoire avant l'initialisation du HSM.

Initialize : définit les capacités HSM. L'appliance Citrix ADC SDX FIPS est conforme à la norme FIPS-140-2 niveau 2. Vous pouvez créer des partitions après avoir initialisé la puce.

Taille du magasin de clés : Nombre de clés pouvant être stockées sur une partition. Un maximum de 102235 clés peut être spécifié. Le nombre maximal de clés pouvant être stockées est inférieur à la moitié du nombre spécifié. Par exemple, si vous spécifiez 100, vous ne pouvez créer que 49 clés, car l'une des clés est la paire de clés RSA qui consomme 2 magasins de clés.

Capacité de base de crypto : Nombre de cœurs de crypto affectés à une partition. Un maximum de 63 cœurs sont disponibles.

Contexte SSL : nombre de connexions SSL simultanées pouvant être créées sur une partition.

Initialiser le HSM

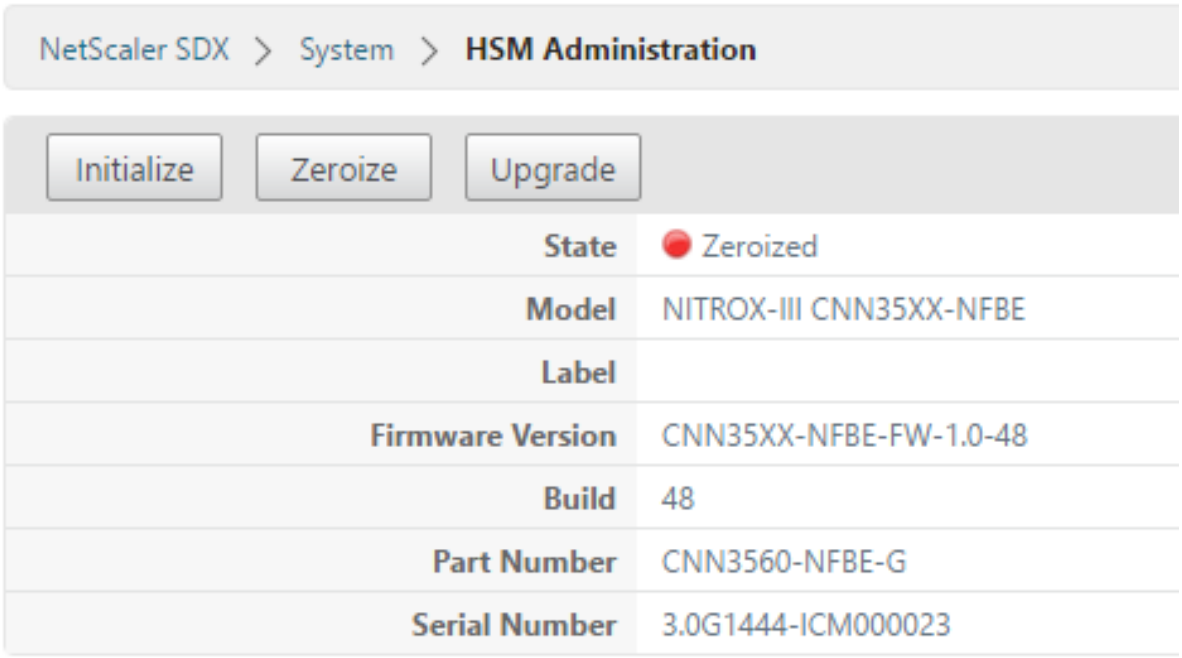
January 21, 2021

Avant d'initialiser le HSM, vous devez d'abord le mettre à zéro.

Mettre à zéro le HSM à l'aide du service de gestion

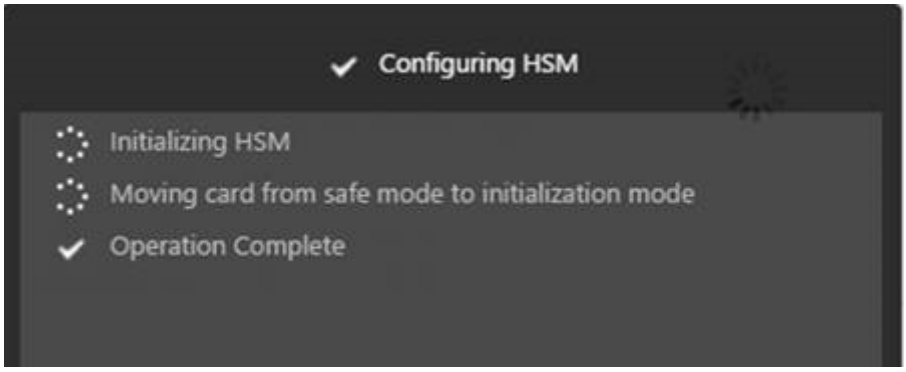
1. Ouvrez un navigateur et connectez-vous à l'appliance.
2. Sous l'onglet **Configuration**, accédez à **Système > Administration HSM**et, dans le plan de détails, cliquez sur **Mise à zéro**.

Toutes les données sont effacées de la puce FIPS, et l'état apparaît comme « mis à zéro ». Toutes les partitions HSM créées précédemment sont supprimées.

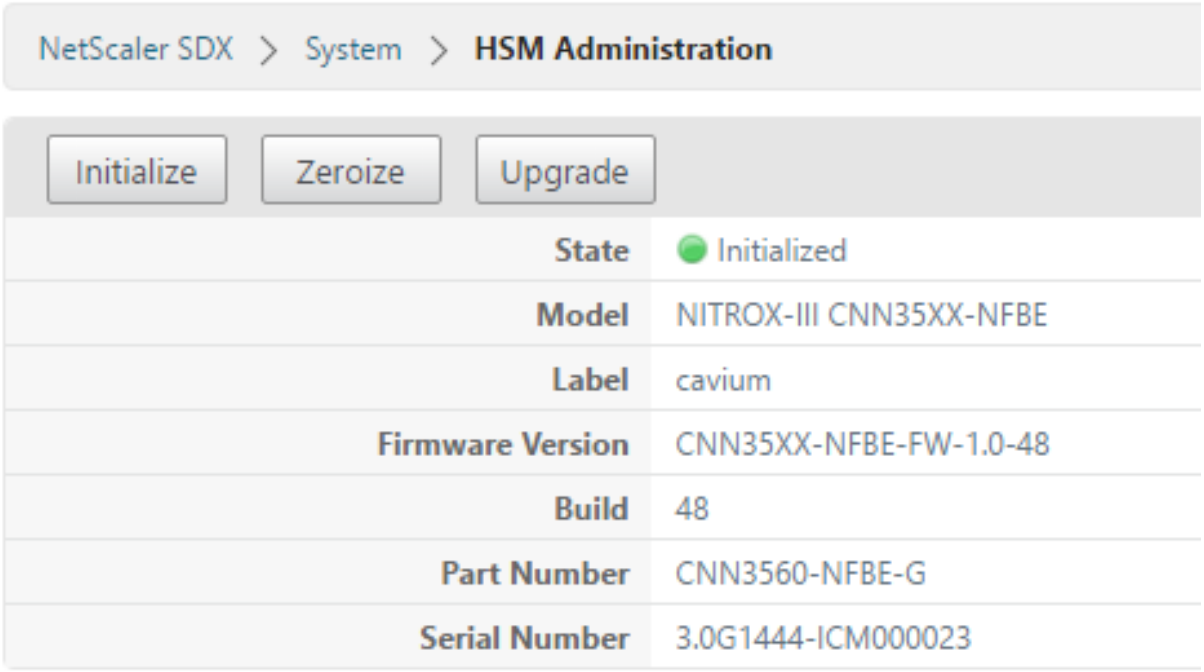


Initialiser le HSM à l'aide du service de gestion

1. Sous l'onglet **Configuration**, accédez à **Système > Administration HSM**et, dans le plan de détails, cliquez sur **Initialiser**.
2. Tapez un nouveau nom d'utilisateur, spécifiez un mot de passe, puis cliquez sur **OK**.



L'état de la carte apparaît comme « Initialisé ».



Créer des partitions

January 21, 2021

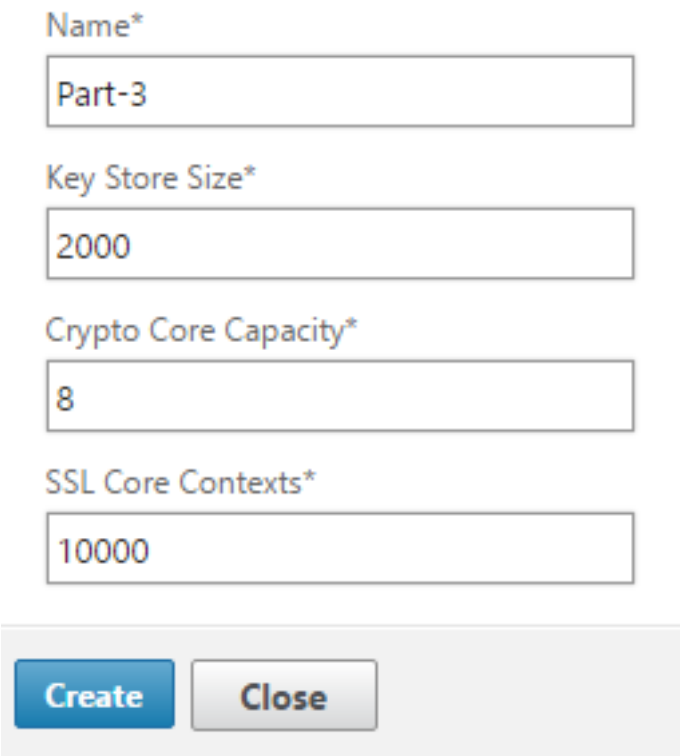
Créez des partitions pour différents locataires et spécifiez les ressources cryptographiques pour chaque partition. Chaque instance est affectée à une partition, et une partition ne peut être affectée qu'à une seule instance. La suppression d'une instance supprime la partition affectée à l'instance. Par conséquent, les données de partition sont également supprimées et ne sont pas laissées non

sécurisées ou accessibles ultérieurement. Le nombre de clés et l'attribution de contexte SSL dépendent de votre application. Pour plus d'informations sur le nombre de cœurs à affecter, consultez la fiche technique Citrix ADC.

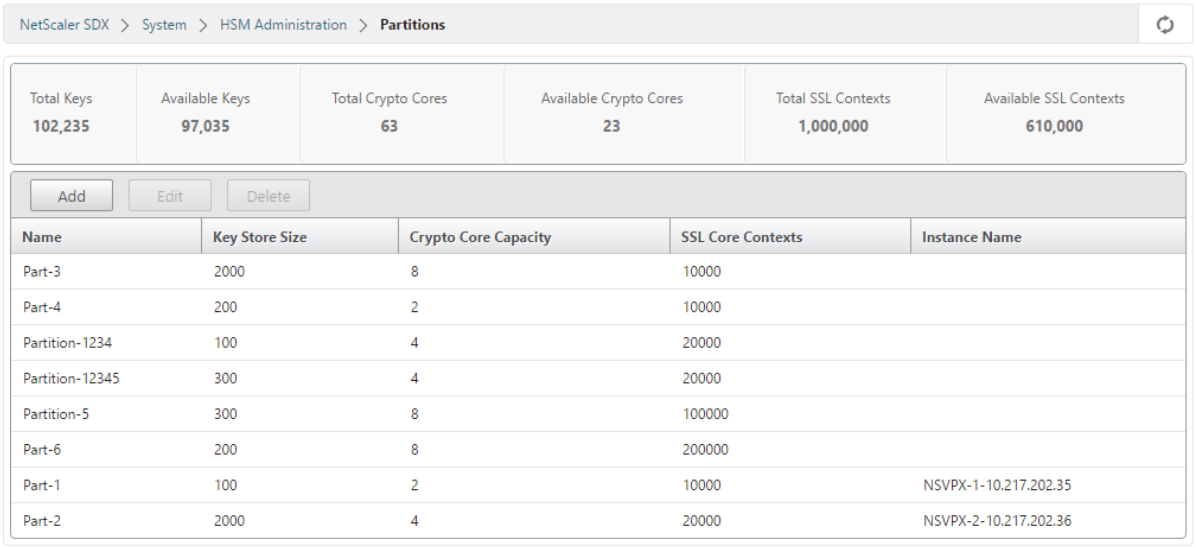
> **Important**
>
> Après avoir assigné une taille de magasin de clés et des cœurs à une partition HSM, vous ne pouvez pas les modifier au moment de l'exécution. Détachez d'abord la partition de l'instance.

Créer une partition à l'aide du service de gestion

1. Sous l'onglet Configuration, accédez à **Système** > **Administration HSM** > **Partitions**, puis dans le plan de détails, cliquez sur **Ajouter**.
2. Spécifiez un nom pour la partition et les ressources à affecter à cette partition.
3. Cliquez sur **OK**.



La page récapitulative affiche toutes les partitions créées. Certaines partitions se voient attribuer une instance tandis que d'autres sont des partitions libres.



Provisionner une nouvelle instance ou modifier une instance existante et affecter une partition

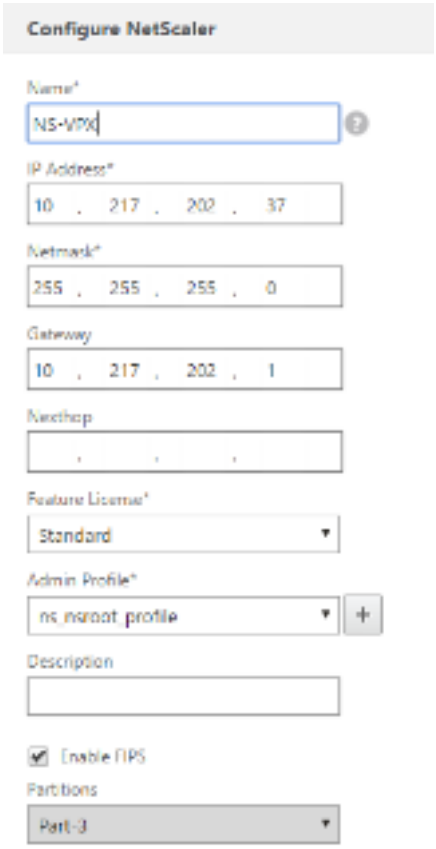
August 20, 2021

Après avoir créé les partitions, vous devez les affecter à des instances.

> **Important :**
>
> - Vous ne pouvez attacher qu'une seule partition FIPS à une instance.
> - Une instance avec une partition FIPS ne peut être affectée qu'à un seul cœur de CPU.

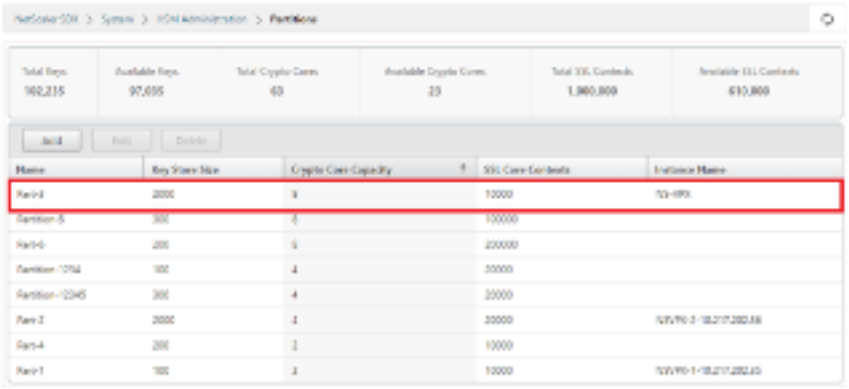
Provisionner une nouvelle instance ou modifier une instance existante

1. Sous l'onglet Configuration, accédez à **NetScaler** > **Instances** et ajoutez ou modifiez une instance.
2. Sélectionnez **Activer FIPS**et, dans la liste **Partitions**, sélectionnez une partition à attacher à cette instance.



Vous pouvez vérifier que la partition est attachée à une instance à l'aide de l'interface graphique ou de l'interface de ligne de commande.

Dans l'interface graphique, accédez à **Système** > **Administration HSM** > **Partitions**. Le nom de l'instance attachée à la partition s'affiche.



Pour annuler l'affectation d'une partition FIPS¸ accédez à **NetScaler** > **Instances**. Modifiez l'instance et désactivez la case à cocher **Activer FIPS**.

Dans l'interface de ligne de commande, à l'invite de commandes, tapez les commandes suivantes :

```
1 show fips
```



```
2
3 FIPS Card is not configured
4  Done
5 <!--NeedCopy-->
```

Si vous voyez la sortie suivante, consultez la section de dépannage pour le débogage.

ERREUR : Opération non autorisée - aucune carte FIPS présente dans le système

Configurer le HSM pour une instance sur une appliance FIPS SDX 14030/14060/14080

August 20, 2021

Vérifiez d'abord l'état de votre carte FIPS pour vérifier que le pilote est correctement chargé, puis initialisez la carte.

À l'invite de commandes, tapez :

```
1 show fips
2
3 FIPS Card is not configured
4
5 Done
6 <!--NeedCopy-->
```

Si le pilote n'est pas chargé correctement, le message « ERREUR : Opération non autorisée - aucune carte FIPS présente dans le système » apparaît.

Initialiser la carte FIPS

> **Important :**
>
> Vérifiez que le répertoire `/nsconfig/fips` a bien été créé sur l'appliance.

N'enregistrez pas la configuration avant de redémarrer l'appliance pour la troisième fois.

Effectuez les étapes suivantes pour initialiser la carte FIPS :

1. Réinitialisez la carte FIPS.
2. Redémarrez l'appliance.
3. Définissez le mot de passe de l'agent de sécurité pour les partitions 0 et 1, et le mot de passe utilisateur pour la partition

   Remarque : L'exécution de la commande set ou reset prend plus de 60 secondes.

4. Enregistrez la configuration.
5. Vérifiez que la clé cryptée par mot de passe pour la partition principale (master_pek.key) a été créée dans le répertoire /nsconfig/fips/.
6. Redémarrez l'appliance.
7. Vérifiez que la carte FIPS est UP.

Initialisez la carte FIPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
reset fips

reboot

set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -
    hsmLabel <string>
<!--NeedCopy-->
```

> **Remarque** : Le message suivant s'affiche lorsque vous exécutez la commande **set fips** :

```
This command will erase all data on the FIPS card. You must save the
    configuration (saveconfig) after executing this command. [Note: On
    MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
    default, and the -initHSM Level-2 option is internally converted to
    Level-3]  Do you want to continue?(Y/N)y

saveconfig

reboot

show fips
<!--NeedCopy-->
```

Exemple :

```
reset fips

Done

reboot

set fips -initHSM Level-2 so12345 so12345 user123 -hsmLabel NSFIPS

```



```
This command will erase all data on the FIPS card. You must save the
    configuration (saveconfig) after executing this command. [Note: On
    MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
    default, and the -initHSM Level-2 option is internally converted to
    Level-3]  Do you want to continue?(Y/N)y

Done

saveconfig

Done

reboot

show fips

    FIPS HSM Info:
    HSM Label : NSFIPS
    Initialization : FIPS-140-2 Level-2
    HSM Serial Number : 3.0G1532-ICM000228
    HSM State : 2
    HSM Model : NITROX-III CNN35XX-NFBE
    Hardware Version : 0.0-G
    Firmware Version : 1.0
    Firmware Build : NFBE-FW-1.0-48
    Max FIPS Key Memory : 1000
    Free FIPS Key Memory : 1000
    Total SRAM Memory : 557396
    Free SRAM Memory : 238088
    Total Crypto Cores : 4
    Enabled Crypto Cores : 4
Done
<!--NeedCopy-->
```

Créer une clé FIPS pour une instance sur une appliance FIPS SDX 14030/14060/14080

August 20, 2021

Vous pouvez créer une clé FIPS sur votre instance ou importer une clé FIPS existante dans l'instance. Une appliance FIPS SDX 14030/14060/14080 ne prend en charge que les clés 2048 bits et 3072 bits et une valeur exposant F4. Pour les clés PEM, un exposant n'est pas requis. Vérifiez que la clé FIPS est

créée correctement. Créez une demande de signature de certificat et un certificat de serveur. Enfin, ajoutez la paire de clés de certificat à votre instance.

> **Remarque :**
>
> Les clés 1024 bits et 4096 bits et une valeur exposant de 3 ne sont pas prises en charge.

Créer une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
create ssl fipsKey <fipsKeyName> -keytype ( RSA | ECDSA ) [-exponent (3
    | F4 )] [-modulus <positive_integer>] [-curve ( P_256 | P_384 )]
<!--NeedCopy-->
```

Exemple :

```
create fipsKey f1 -keytype RSA -modulus 2048 -exponent F4

Done

show ssl fipskey ddvws

FIPS Key Name: f1  Key Type: RSA Modulus: 2048   Public Exponent: F4 (
   Hex: 0x10001)

Done
<!--NeedCopy-->
```

Importer une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-
   wrapKeyName <string>] [-iv<string>] [-exponent F4 ]
<!--NeedCopy-->
```

Exemple :

```
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4
Done
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform PEM
Done
<!--NeedCopy-->
```


Vérifiez que la clé FIPS est créée ou importée correctement en exécutant la commande **show fipskey**.

```
show fipskey
1)      FIPS Key Name: Key-FIPS-2
Done
<!--NeedCopy-->
```

Créer une demande de signature de certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
    <string>) [-keyform ( DER | PEM )  {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName<string>
     [-organizationUnitName <string>] [-localityName <string>] [-
     commonName <string>] [-emailAddress <string>] {
 -challengePassword  }
  [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
<!--NeedCopy-->
```

Exemple :

```
create certreq f1.req  - fipsKeyName f1 -countryName US -stateName CA -
    organizationName Citrix -companyName Citrix -commonName ctx -
    emailAddress test@example.com`
`Done
<!--NeedCopy-->
```

Créer un certificat de serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM ) {
 -PEMPassPhrase  }
 ] [-days <positive_integer>] [-certForm ( DER | PEM )] [-CAcert <
     input_filename>] [-CAcertForm ( DER | PEM )] [-CAkey <
     input_filename>] [-CAkeyForm ( DER | PEM )] [-CAserial <
     output_filename>]
<!--NeedCopy-->
```

Exemple :


```
create cert f1.cert f1.req SRVR_CERT -CAcert ns-root.cert -CAkey ns-
    root.key -CAserial ns-root.srl -days 1000
Done
<!--NeedCopy-->
```

L'exemple précédent crée un certificat de serveur à l'aide d'une autorité de certification racine locale sur l'appliance.

Ajouter une paire de clés de certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
    string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>]
    [-expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod   <
    positive_integer>]] [-bundle ( YES | NO )]
<!--NeedCopy-->
```

Exemple :

```
add certkey cert1 -cert f1.cert -fipsKey f1
Done
<!--NeedCopy-->
```

Après avoir créé la clé FIPS et le certificat de serveur, vous pouvez ajouter la configuration SSL générique. Activez les fonctionnalités requises pour votre déploiement. Ajoutez des serveurs, des services et des serveurs virtuels SSL. Liez la paire de clés de certificat et le service au serveur virtuel SSL et enregistrez la configuration.

```
enable ns feature SSL LB
Done
add server s1 10.217.2.5
Done
add service sr1 s1 HTTP 80
Done
add lb vserver v1 SSL 10.217.2.172 443
Done
bind ssl vserver v1  - certkeyName cert1
Done
bind lb vserver v1 sr1
Done
saveconfig
Done
```



```
<!--NeedCopy-->
```

Pour plus d'informations sur la configuration du protocole HTTPS sécurisé et du RPC sécurisé, cliquez ici.

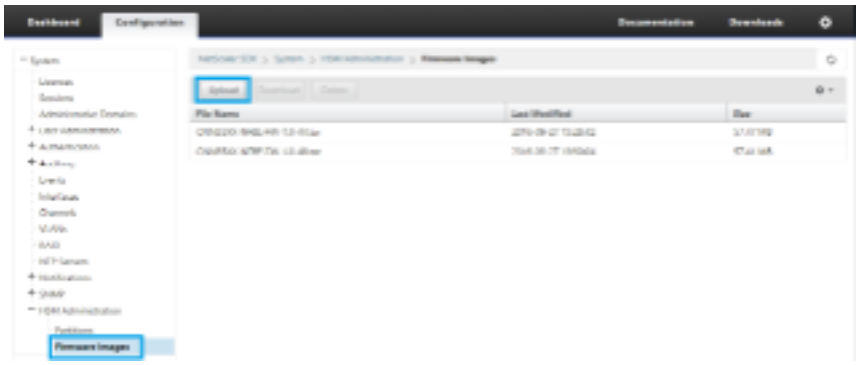
Mettre à niveau le firmware FIPS sur une instance VPX

January 21, 2021

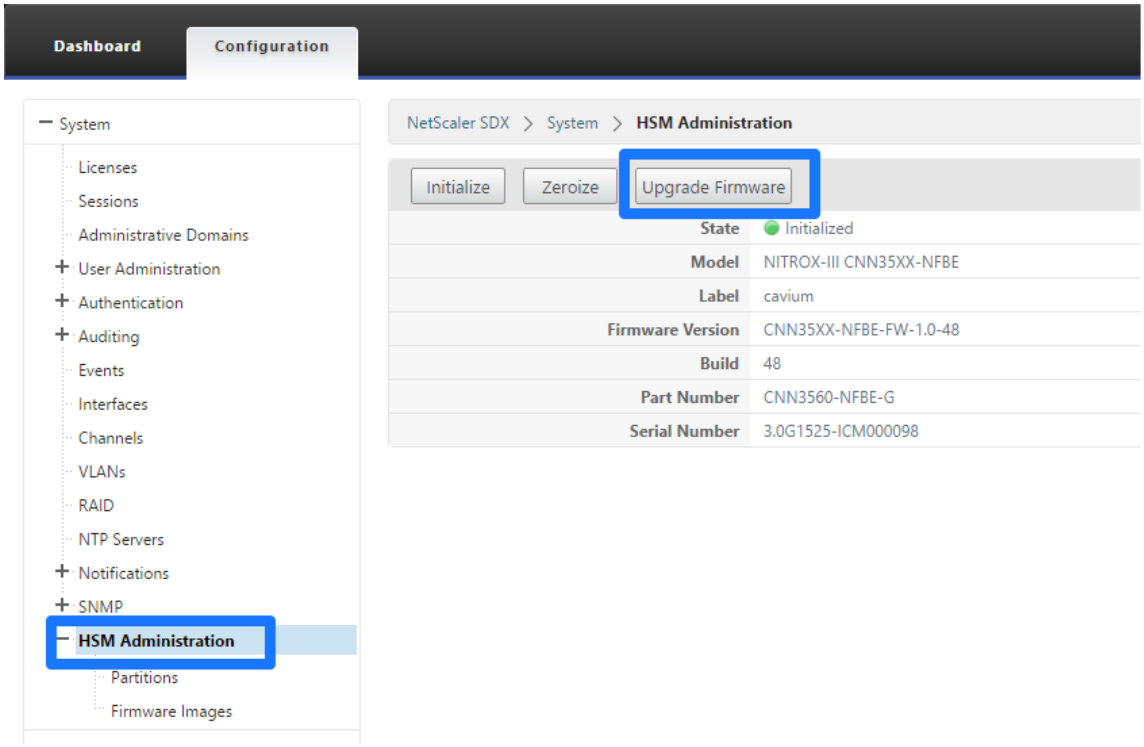
Les mises à jour du firmware FIPS sont publiées de temps en temps. Téléchargez le dernier firmware à partir de la page de téléchargement Citrix et téléchargez-le sur l'appliance. Le processus de mise à niveau peut prendre jusqu'à 10 minutes. L'instance est redémarrée après la mise à niveau.

Mettre à niveau le firmware FIPS

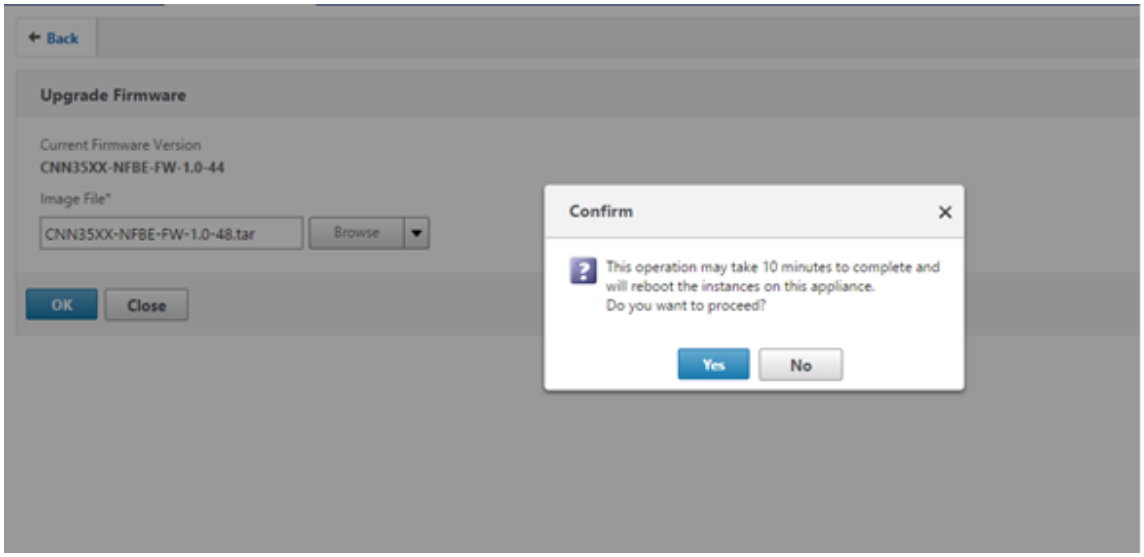
1. Accédez à **Système > Administration HSM > Images du microprogramme**.
2. Sélectionnez **Charger**.

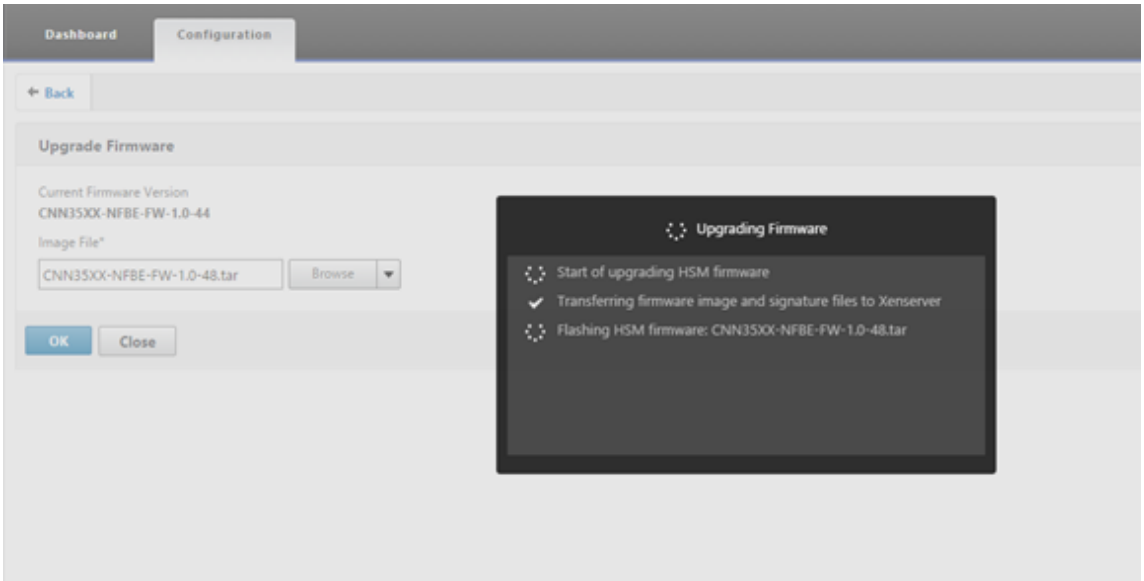


3. Accédez au dossier contenant l'image du microprogramme et sélectionnez le fichier.
4. Accédez à **Système > Administration HSM**, puis sélectionnez **Mettre à niveau le firmware**.



5. Sélectionnez l'image du firmware vers laquelle effectuer la mise à niveau, puis cliquez sur **OK**.





Prise en charge du module de sécurité matérielle (HSM) NShield Connect

August 20, 2021

Une appliance Citrix ADC non FIPS stocke la clé privée du serveur sur le disque dur. Sur une appliance FIPS, la clé est stockée dans un module cryptographique appelé HSM. Le stockage d'une clé dans le HSM la protège contre les attaques physiques et logicielles. En outre, les clés sont chiffrées à l'aide de chiffrements spéciaux approuvés par FIPS.

Seuls les appliances FIPS Citrix ADC MPX 9700/10500/12500/15500 prennent en charge une carte FIPS. La prise en charge FIPS n'est pas disponible sur les autres appliances MPX, ni sur les appliances SDX et VPX. Cette limitation est résolue en prenant en charge un HSM externe NShield Connect sur toutes les appliances Citrix ADC MPX, SDX et VPX, à l'exception des appliances FIPS MPX 9700/10500/12500/15500.

NShield® Connect est un HSM connecté au réseau certifié FIPS externe. Avec un HSM NShield, les clés sont stockées en toute sécurité en tant que jetons de clé d'application sur un serveur de fichiers distant (RFS) et peuvent être reconstituées uniquement dans le HSM NShield.

Si vous utilisez déjà un HSM NShield, vous pouvez désormais utiliser un Citrix ADC pour optimiser, sécuriser et contrôler la fourniture de tous les services d'entreprise et de cloud.

Remarque :

- Les HSM NShield sont conformes aux spécifications FIPS 140-2 Niveau 3, tandis que les appliances MPX FIPS sont conformes aux spécifications de niveau 2.

- Vous ne pouvez pas déchiffrer la trace lorsque vous utilisez le HSM NShield. Seul le `hardserver` peut lire la réponse du HSM à l'appliance Citrix ADC, car elle est chiffrée.

Matrice des versions prises en charge

Version de Citrix ADC	Version client NShield	`Hardserver` Version	Version du firmware de NShield
10.5e, 11.0, 11.1, 12.0, 12.1	11.70, 11.72	2.71.2	2.50.16, 2.51.10

Aperçu de l'architecture

August 20, 2021

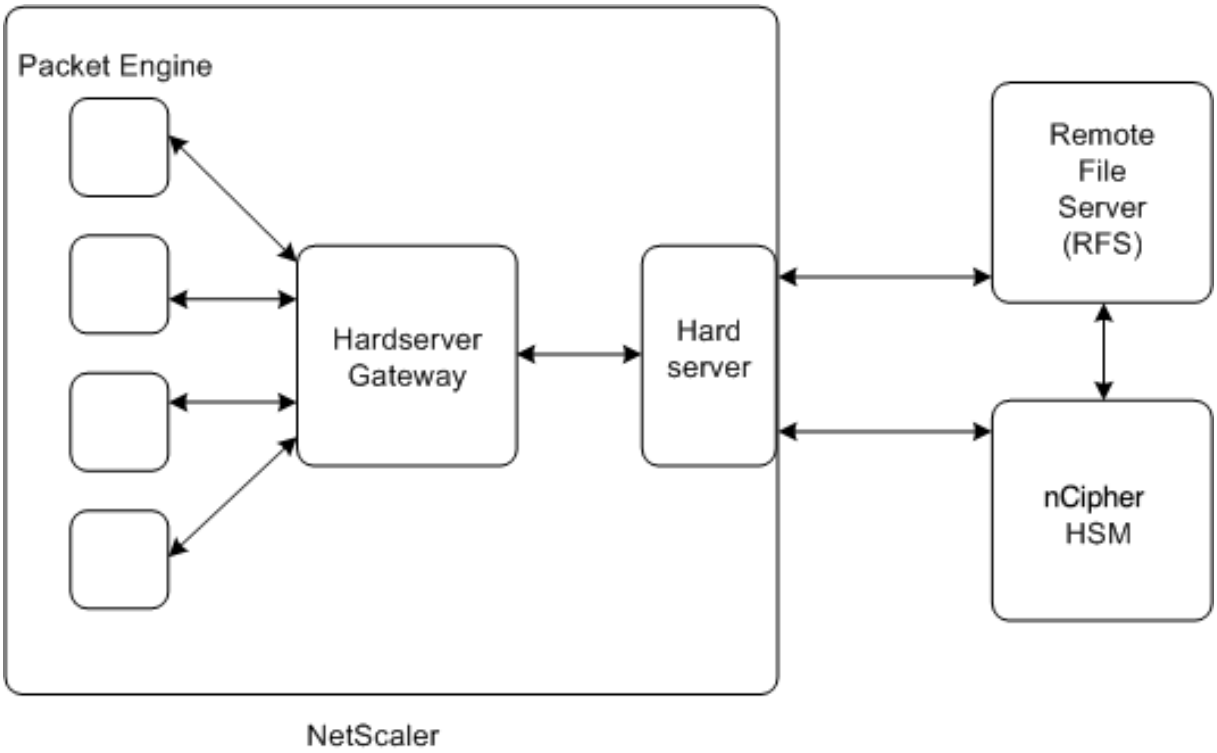
Les trois entités qui font partie d'un déploiement Citrix ADC-Entrust sont un module Entrust NShield Connect, un serveur de fichiers distant (RFS) et un Citrix ADC.

L'Entrust NShield Connect est un module de sécurité matériel connecté au réseau. Le RFS permet de configurer le HSM et de stocker les fichiers de clés chiffrées.

`Hardserver`, un démon propriétaire fourni par Entrust, est utilisé pour la communication entre le client (ADC), le HSM Entrust et le RFS. Il utilise le protocole de communication sécurisé IMPATH. Un démon de passerelle, appelé `Hardserver Gateway`, est utilisé pour communiquer entre le moteur de paquets Citrix ADC et le `Hardserver`.

Remarque : Les termes Entrust NShield Connect, Entrust HSM et HSM sont utilisés de manière interchangeable dans cette documentation.

La figure suivante illustre l'interaction entre les différents composants.

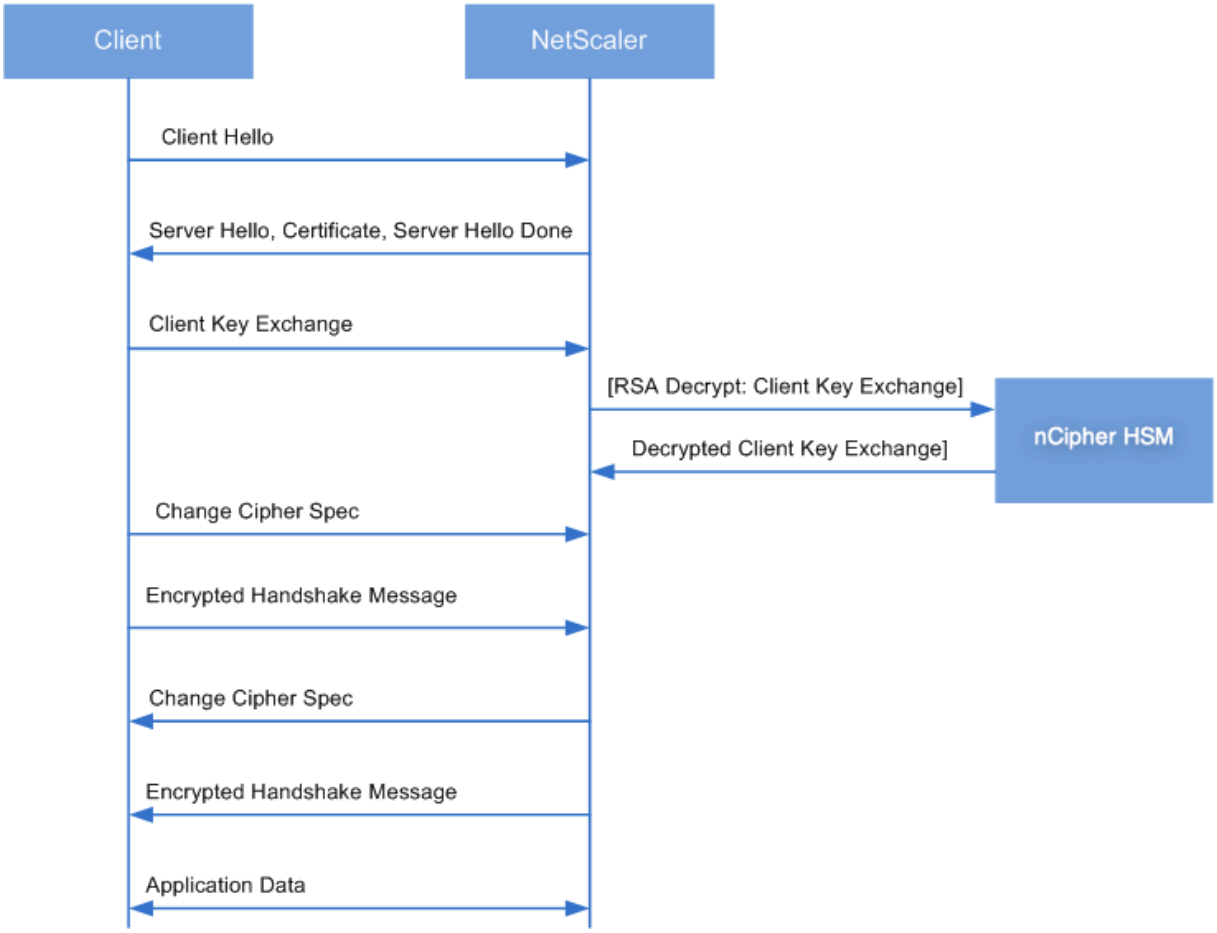


Dans un déploiement standard, le RFS est utilisé pour stocker en toute sécurité les clés générées par le HSM. Une fois les clés générées, vous pouvez les transférer en toute sécurité vers ADC, puis utiliser l'interface graphique ou la ligne de commande pour charger les clés dans le HSM. Un serveur virtuel sur ADC utilise Entrust pour déchiffrer l'échange de clés client afin de terminer la liaison SSL. Par la suite, toutes les opérations SSL sont effectuées sur ADC.

Remarque : Les termes clés et jetons de clé d'application sont utilisés de manière interchangeable dans cette documentation.

La figure suivante illustre le flux de paquets dans la poignée de contact SSL avec Entrust HSM.

Figure 1. Diagramme de flux de paquets SSL avec Citrix ADC à l'aide d'Entrust HSM



Remarque : La communication entre l'ADC et le HSM utilise un protocole de communication propriétaire Entrust, appelé IMPATH.

Conditions préalables

August 20, 2021

Avant de pouvoir utiliser un Entrust NShield Connect avec un Citrix ADC, assurez-vous que les conditions préalables suivantes sont remplies :

- Un appareil Entrust NShield Connect est installé sur le réseau, prêt à l'emploi et accessible à Citrix ADC. Autrement dit, l'adresse du NSIP est ajoutée en tant que client autorisé sur le HSM.
- Un monde de sécurité utilisable existe. Security World est une architecture de gestion des clés unique utilisée par la gamme de HSM Entrust NShield. Il protège et gère les clés en tant que jetons de clé d'application, permettant une capacité de clé illimitée, ainsi que la sauvegarde et la récupération automatiques des clés. Pour plus d'informations sur la création d'un monde de sécurité, consultez le Guide de démarrage rapide de NShield Connect d'Entrust. Vous

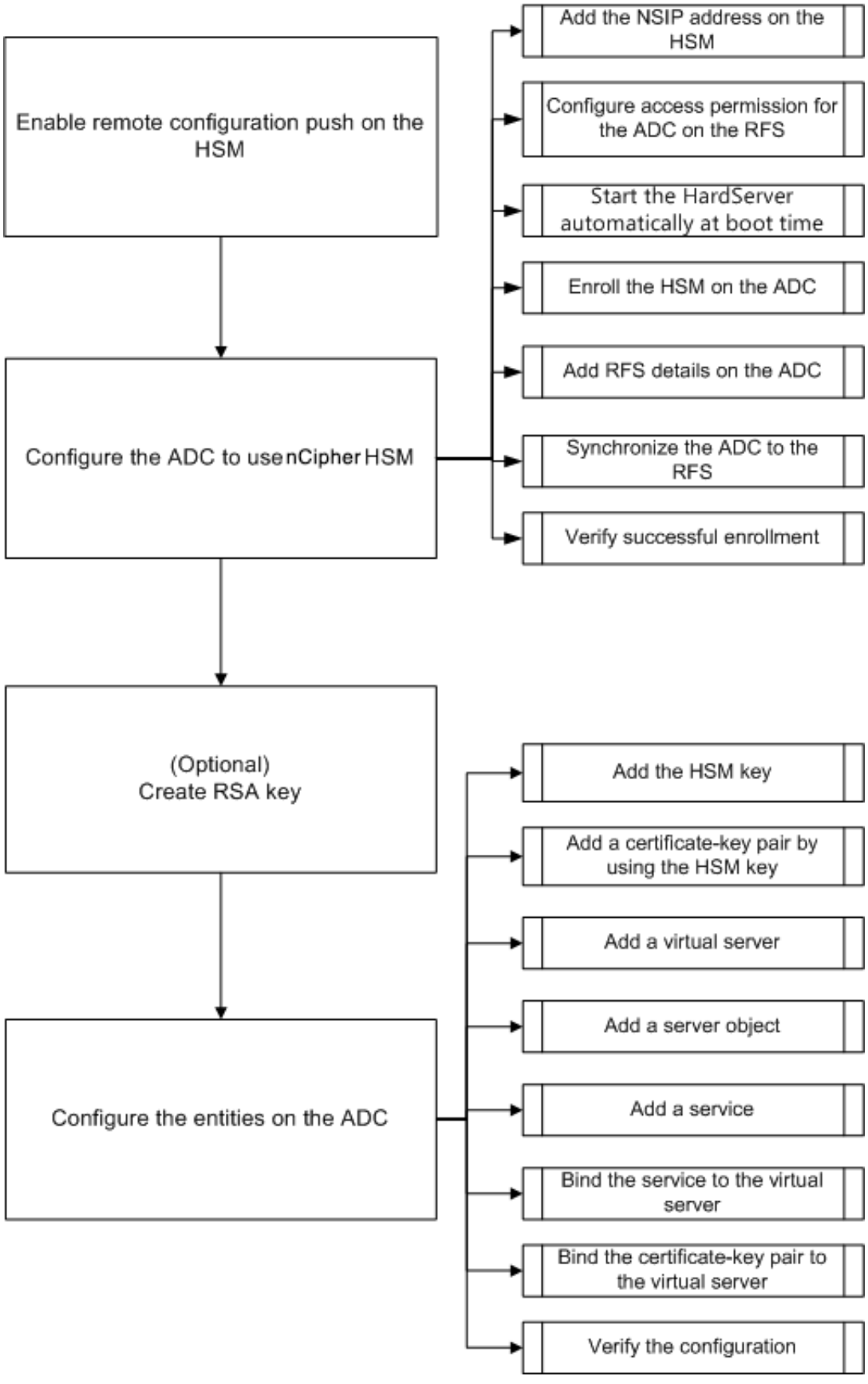
pouvez également trouver le guide dans le CD fourni avec le module Entrust HSM à l'adresse CipherTools-Linux-Dev-XX.xx.xx/Document/NShield_Connect_Quick_Start_Guide.pdf.
Remarque : `Softcard` ou les clés protégées Token/OCS ne sont actuellement pas prises en charge sur Citrix ADC.

- Des licences sont disponibles pour prendre en charge le nombre de clients connectés au HSM Entrust. L'ADC et le serveur de fichiers distant (RFS) sont des clients du HSM.
- Un RFS est installé sur le réseau et est accessible à Citrix ADC.
- Le périphérique Entrust NShield Connect, le RFS et Citrix ADC peuvent initier des connexions entre eux via le port 9004.
- Vous utilisez NetScaler version 10.5 build 52.1115.e ou version ultérieure.
- L'appliance Citrix ADC ne contient pas de carte FIPS Cavium.
  Important : Entrust HSM n'est pas pris en charge sur les appliances FIPS MPX 9700/10500/12500/15500.

Configurer l'intégration ADC-Entrust

August 20, 2021

L'organigramme suivant illustre les tâches que vous devez effectuer pour utiliser Entrust HSM avec un Citrix ADC :



Comme indiqué dans l'organigramme précédent, vous effectuez les tâches suivantes :

1. Activez la poussée de configuration à distance, sur le HSM.
2. Configurez l'ADC pour qu'il utilise le HSM Entrust.
    - Ajoutez l'adresse NSIP sur le HSM.
    - Configurez l'autorisation d'accès pour ADC sur le RFS.
    - Configurez le démarrage automatique de l' `Hardserver` au démarrage.
    - Inscrire le HSM sur ADC.
    - Ajoutez des détails RFS sur ADC.
    - Synchronisez ADC avec le RFS.
    - Vérifiez que Entrust HSM est correctement inscrit sur ADC.
3. (Facultatif) Créez une clé HSM RSA.
4. Configurez les entités sur Citrix ADC.
    - Ajoutez la clé HSM.
    - Ajoutez une paire de clés de certificat à l'aide de la clé HSM.
    - Ajoutez un serveur virtuel.
    - Ajoutez un objet serveur.
    - Ajoutez un service.
    - Liez le service au serveur virtuel.
    - Liez la paire de clés de certificat au serveur virtuel.
    - Vérifiez la configuration.

Configurer le HSM Entrust

Spécifiez l'adresse IP du RFS sur le HSM Entrust afin qu'il accepte la configuration que le RFS y envoie. Utilisez le panneau avant de NShield Connect sur l'Entrust HSM pour effectuer la procédure suivante.

Spécifiez l'adresse IP d'un ordinateur distant sur le HSM Entrust

1. Accédez à **Configuration système > Options du fichier de configuration > Autoriser la poussée automatique**.
2. Sélectionnez **ON**et spécifiez l'adresse IP de l'ordinateur (RFS) à partir duquel accepter la configuration.

Activer la poussée de la configuration distante sur le HSM

Spécifiez l'adresse IP du RFS sur le HSM Entrust afin qu'il accepte la configuration que le RFS y envoie. Utilisez le panneau avant de NShield Connect sur l'Entrust HSM pour effectuer la procédure suivante.

Spécifiez l'adresse IP d'un ordinateur distant sur le HSM Entrust

1. Accédez à **Configuration système > Options du fichier de configuration > Autoriser la poussée automatique**.
2. Sélectionnez **ON**et spécifiez l'adresse IP de l'ordinateur (RFS) à partir duquel accepter la configuration.

Configurer l'ADC pour utiliser le HSM Entrust

Exemples de valeurs utilisées dans cette documentation :

Adresse NSIP=10.217.2.43

Adresse IP Entrust HSM = 10.217.2.112

Adresse IP RFS = 10.217.2.6

Ajouter l'adresse NSIP sur le HSM

Généralement, vous utilisez le panneau avant de nShield Connect pour ajouter des clients au HSM. Pour plus d'informations, consultez le Guide de démarrage rapide de nShield Connect.

Vous pouvez également utiliser le RFS pour ajouter ADC en tant que client au HSM. Pour ajouter ADC, vous devez ajouter l'adresse NSIP dans la configuration HSM sur le RFS, puis pousser la configuration vers le HSM. Avant de pouvoir pousser la configuration, vous devez connaître le numéro de série électronique (ESN) du HSM.

Pour obtenir le numéro ESN de votre HSM, exécutez la commande suivante sur le RFS :

```
root@ns# /opt/nfast/bin/anonkneti <Entrust HSM IP address>
<!--NeedCopy-->
```

Exemple :

```
root@ns# /opt/nfast/bin/anonkneti 10.217.2.112
BD17-C807-58D9 5e30a698f7bab3b2068ca90a9488dc4e6c78d822
<!--NeedCopy-->
```

Le numéro ESN est BD17-C807-58D9.

Une fois que vous avez le numéro ESN, utilisez un éditeur, tel que vi, pour modifier le fichier de configuration HSM sur le RFS.

```
vi /opt/nfast/kmdata/hsm-BD17-C807-58D9/config/config
<!--NeedCopy-->
```


Dans la hs_clients section, ajoutez les entrées suivantes :

```
# Amount of data in bytes to encrypt with a session key before session key# renegotiation, or 0 for unlimitied. (default=1024\*1024\*8b=8Mb).
#  datalimit=INT
addr=10.217.2.43
clientperm=unpriv
keyhash=0000000000000000000000000000000000000000
esn=
timelimit=86400
datalimit=8388608
-----
<!--NeedCopy-->
```

Remarque : Incluez un ou plusieurs traits d'union comme délimiteurs pour ajouter plusieurs entrées dans la même section.

Pour pousser la configuration vers le HSM, exécutez la commande suivante sur le RFS :

```
/opt/nfast/bin/cfg-pushnethsm --address=<Entrust HSM IP address> --force /opt/nfast/kmdata/hsm-BD17-C807-58D9/config/config
<!--NeedCopy-->
```

Exemple :

```
/opt/nfast/bin/cfg-pushnethsm --address=10.217.2.112 --force
                /opt/nfast/kmdata/hsm-BD17-C807-58D9/config/config
<!--NeedCopy-->
```

Configurer l'autorisation d'accès pour ADC sur le RFS

Pour configurer l'autorisation d'accès pour ADC sur le RFS, exécutez la commande suivante sur le RFS :

```
/opt/nfast/bin/rfs-setup --force -g --write-noauth <NetScaler IP address>
<!--NeedCopy-->
```

Exemple :

```
[root@localhost bin]# /opt/nfast/bin/rfs-setup --force -g --write-noauth 10.217.2.43
Adding read-only remote_file_system entries
Ensuring the directory /opt/nfast/kmdata/local exists
Adding new writable remote_file_system entries
```



```
Ensuring the directory /opt/nfast/kmdata/local/sync-store exists
Saving the new config file and configuring the hardserver
Done
<!--NeedCopy-->
```

Vérifiez que l'ADC peut atteindre à la fois le RFS et le HSM Entrust à l'aide du port 9004.

Configurer le démarrage automatique `hardserver` de l'

Créez un fichier, puis redémarrez l'appliance. Désormais, chaque fois que vous redémarrez l'appliance et si ce fichier est trouvé, le `Hardserver` est automatiquement démarré.

À l'invite shell, tapez :

```
touch /var/opt/nfast/bin/thales_hsm_is_enrolled
<!--NeedCopy-->
```

À l'invite de commandes, tapez :

```
reboot
<!--NeedCopy-->
```

Inscrire le HSM sur ADC

Changer le répertoire en /var/opt/nfast/bin.

Pour ajouter des détails HSM dans la configuration ADC, exécutez la commande suivante sur ADC :

`nethsmenroll --force <Thales_nShield_Connect_ip_address> $(anonkneti <Thales_nShield_Connect_ip_address>)`

Exemple :

```
root@ns# ./nethsmenroll --force 10.217.2.112 $(anonkneti 10.217.2.112)
OK configuring hardserver's nethsm imports
<!--NeedCopy-->
```

Cette étape ajoute les entrées suivantes après la ligne # NToken_ESn=ESN dans la `nethsm_imports` section du fichier /var/opt/nfast/kmdata/config.

```
…
local_module=0
remote_ip=10.217.2.112
remote_port=9004
remote_esn=BD17-C807-58D9
```



```
keyhash=5e30a698f7bab3b2068ca90a9488dc4e6c78d822
timelimit=86400
datalimit=8388608
privileged=0
privileged_use_high_port=0
ntoken_esn=
<!--NeedCopy-->
```

Changez le répertoire en /var/opt/nfast/bin et exécutez la commande suivante sur ADC :

```
touch "thales_hsm_is_enrolled"
<!--NeedCopy-->
```

Remarque : Pour supprimer un HSM inscrit sur ADC, tapez :

```
./nethsmenroll - -remove <NETHSM-IP>
<!--NeedCopy-->
```

Ajouter des détails RFS sur ADC

Pour ajouter des détails RFS, changez le répertoire par /var/opt/nfast/bin/, puis exécutez la commande suivante :

```
./rfs-sync --no-authenticate --setup <rfs_ip_address>
<!--NeedCopy-->
```

Exemple :

```
./rfs-sync --no-authenticate --setup 10.217.2.6
No current RFS synchronization configuration.
Configuration successfully written; new config details:
Using RFS at 10.217.2.6:9004: not authenticating.
<!--NeedCopy-->
```

Cette étape ajoute les entrées suivantes après la ligne # local_esn=ESN dans la `rfs_sync_client` section du fichier /var/opt/nfast/kmdata/config/config.

```
... ...
remote_ip=10.217.2.6
remote_port=9004
use_kneti=no
local_esn=
<!--NeedCopy-->
```


Remarque : Pour supprimer un RFS inscrit sur ADC, tapez :

```
./rfs_sync - remove
<!--NeedCopy-->
```

Synchroniser ADC avec le RFS

Pour synchroniser tous les fichiers, changez le répertoire en /var/opt/nfast/bin, puis exécutez la commande suivante sur le ADC :

```
./rfs-sync - -update
<!--NeedCopy-->
```

Cette commande récupère tous les fichiers World, les fichiers modules et les fichiers clés du répertoire /opt/nfast/kmdata/local du RFS et les place dans le répertoire /var/opt/nfast/kmdata/local de ADC. Citrix vous recommande de copier manuellement les fichiers World, les fichiers Module_xxxx_xxxx, où XXXX_XXXX correspond à l'ESN du HSM inscrit, et uniquement les fichiers de clé et de certificat RSA requis.

Vérifiez que le HSM Entrust est correctement inscrit sur ADC

Après avoir synchronisé ADC avec le RFS, procédez comme suit :

- Vérifiez que le local `Hardserver` est actif et en cours d'exécution. (Entrust server en cours d'exécution).
- Obtenez l'état des HSM configurés et vérifiez que les valeurs du champ n_modules (nombre de modules) et des champs d'informations km ne sont pas nulles.
- Vérifiez que le HSM est correctement inscrit et qu'il est utilisable (état 0 x 2 utilisable) par ADC.
- Charger les tests en utilisant `sigtest` exécuter correctement.

Modifiez le répertoire en /var/opt/nfast/bin, et à l'invite shell, exécutez les commandes suivantes :

```
root@ns# ./chkserv root@ns# ./nfkminfo root@ns# ./sigtest
<!--NeedCopy-->
```

Voir l'annexe pour un exemple.

Créer une clé HSM RSA

Seules les clés RSA sont prises en charge en tant que clés HSM.

Remarque : Ignorez cette étape si des clés sont déjà présentes dans le `/opt/nfast/kmdata/local` dossier sur le RFS.

Créez une clé RSA, un certificat auto-signé et une demande de signature de certificat (CSR). Envoyez le CSR à une autorité de certification pour obtenir un certificat de serveur.

Les fichiers suivants sont créés dans l'exemple suivant :

- Incorporer la clé RSA : key_embed_2ed5428aaeae1e159bdbd63f25292c7113ec2c78
- Certificat auto-signé : example_selfcert
- Demande de signature de certificat : example_req

Remarque : la `generatekey` commande est prise en charge dans le strict FIPS 140-2 Niveau 3 Security World. Un jeu de cartes d'administrateur (ACS) ou un jeu de cartes d'opérateur (OCS) est nécessaire pour contrôler de nombreuses opérations, y compris la création de clés et d'OCS. Lorsque vous exécutez la `generatekey` commande, vous êtes invité à insérer une carte ACS ou OCS. Pour plus d'informations sur FIPS 140-2 Niveau 3 Security World, consultez le Guide de l'utilisateur de nShield Connect.

L'exemple suivant utilise Level-2 Security World. Dans l'exemple, les commandes sont en caractères gras.

Exemple :

```
[root@localhost bin]# ./generatekey embed
size: Key size? (bits, minimum 1024) [1024] > 2048
OPTIONAL: pubexp: Public exponent for RSA key (hex)? []
>
embedsavefile: Filename to write key to? []
> example
plainname: Key name? [] > example
x509country: Country code? [] > US
x509province: State or province? [] > CA
x509locality: City or locality? [] > Santa Clara
x509org: Organisation? [] > Citrix
x509orgunit: Organisation unit? [] > NS
x509dnscommon: Domain name? [] > www.citrix.com
x509email: Email address? [] > example@citrix.com
nvram: Blob in NVRAM (needs ACS)? (yes/no) [no] >
digest: Digest to sign cert req with? (md5, sha1, sha256, sha384,
    sha512)
  [default sha1] > sha512
key generation parameters:
 operation      Operation to perform              generate
 application    Application                       embed
 verify         Verify security of key            yes
 type           Key type                          RSA
 size           Key size                          2048
 pubexp         Public exponent for RSA key (hex)
```



```
 embedsavefile  Filename to write key to          example
 plainname      Key name                          example
 x509country    Country code                      US
 x509province   State or province                 CA
 x509locality   City or locality                  Santa Clara
 x509org        Organisation                      Citrix
 x509orgunit    Organisation unit                 NS
 x509dnscommon  Domain name                       www.citrix.com
 x509email      Email address                     example@citrix.com
 nvram          Blob in NVRAM (needs ACS)         no
 digest         Digest to sign cert req with      sha512
Key successfully generated.
Path to key: /opt/nfast/kmdata/local/
   key_embed_2ed5428aaeae1e159bdbd63f25292c7113ec2c78
You have new mail in /var/spool/mail/root
<!--NeedCopy-->
```

Résultats :

Vous avez créé un CSR (example_req), un certificat auto-signé (example_selfcert) et un fichier de jeton de clé d'application au format intégré (/opt/nfast/kmdata/local/key_embed_2ed5428aae1e159bdbd63f25292c711

Étant donné que ADC ne prend en charge que les clés au format simple, vous devez convertir la clé intégrée en une clé simple.

Pour convertir la clé intégrée en une clé simple, exécutez la commande suivante sur le RFS :

```
[root@localhost bin]# ./generatekey -r simple
from-application: Source application? (embed, simple) [embed] > embed
from-ident: Source key identifier? (
   c6410ca00af7e394157518cb53b2db46ff18ce29,
                                    2
                                       ed5428aaeae1e159bdbd63f25292c7113ec2c78
                                       )
  [default c6410ca00af7e394157518cb53b2db46ff18ce29]
> 2ed5428aaeae1e159bdbd63f25292c7113ec2c78
ident: Key identifier? [] > examplersa2048key
plainname: Key name? [] > examplersa2048key
key generation parameters:
 operation         Operation to perform    retarget
 application       Application             simple
 verify            Verify security of key  yes
 from-application  Source application      embed
 from-ident        Source key identifier   2
    ed5428aaeae1e159bdbd63f25292c7113ec2c78
 ident             Key identifier          examplersa2048key
```



```
 plainname         Key name                examplersa2048key
Key successfully retargetted.
Path to key: /opt/nfast/kmdata/local/key_simple_examplersa2048key
<!--NeedCopy-->
```

> **Important :**
>
> Lorsque vous y êtes invité, entrez **2ed5428aaeae1e159bdbd63f25292c7113ec2c78** comme clé d'intégration.

Résultats :

Une clé avec le préfixe key_simple (par exemple key_simple_examplersa2048key) est créée.

Remarque : examplersa2048key est l'identificateur de clé (ident) et est appelé nom de clé HSM sur ADC. Un identificateur de clé est unique. Tous les fichiers simples ont le préfixe key_simple.

Configurer les entités sur ADC

Avant que ADC puisse traiter le trafic, vous devez effectuer les opérations suivantes :

1. Activer les fonctionnalités.
2. Ajoutez une adresse IP de sous-réseau (SNIP).
3. Ajoutez la clé HSM à ADC.
4. Ajoutez une paire de clés de certificat à l'aide de la clé HSM.
5. Ajoutez un serveur virtuel.
6. Ajoutez un objet serveur.
7. Ajoutez un service.
8. Liez le service au serveur virtuel.
9. Liez la paire de clés de certificat au serveur virtuel.
10. Vérifiez la configuration.

Activer les fonctionnalités sur ADC

Les licences doivent être présentes sur ADC avant de pouvoir activer une fonctionnalité.

Activer une fonctionnalité à l'aide de l'interface de ligne de commande

À l'invite de commandes, exécutez les commandes suivantes :

```
enable feature lb
enable feature ssl
<!--NeedCopy-->
```


Activer une fonctionnalité à l'aide de l'interface graphique

Accédez à **Système** > **Paramètres** et, dans le groupe **Modes et fonctionnalités**, sélectionnez **Configurer les fonctionnalités de base**, puis sélectionnez **Déchargement SSL**.

Ajouter une adresse IP de sous-réseau

Pour plus d'informations sur les adresses IP des sous-réseaux, voir Configuration des adresses IP de sous-réseau.

Ajoutez une adresse SNIP et vérifiez la configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, exécutez les commandes suivantes :

```
add ns ip <IPAddress> <netmask> -type SNIP
show ns ip
<!--NeedCopy-->
```

Exemple :

```
add ns ip 192.168.17.253 255.255.248.0 -type SNIP
Done
show ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp
                 Icmp     Vserver  State
        ---------        --------------  ----             ----     ---
                 ----     -------  ------
1)      192.168.17.251   0               NetScaler IP     Active
   Enabled  Enabled  NA       Enabled
2)      192.168.17.252   0               VIP              Active
   Enabled  Enabled  Enabled  Enabled
3)      192.168.17.253   0               SNIP              Active
   Enabled  Enabled  NA       Enabled
 Done
<!--NeedCopy-->
```

Ajouter une adresse SNIP et vérifier la configuration à l'aide de l'interface graphique

Accédez à **Système > Réseau > IP**, ajoutez une adresse IP et sélectionnez le **Type IP comme IP de sous-réseau**.

Copiez la clé HSM et le certificat dans ADC

Utilisez un utilitaire de transfert de fichiers sécurisé pour copier en toute sécurité la clé (key_simple_examplersa204
dans le dossier `/var/opt/nfast/kmdata/local` et le certificat (exemple_selfcert) dans le dossier `/nsconfig/ssl` de ADC.

Ajouter la clé sur ADC

Toutes les clés ont un préfixe clé-simple. Lorsque vous ajoutez la clé à ADC, utilisez l'ident comme nom de clé HSM. Par exemple, si la clé que vous avez ajoutée est KEY_Simple_XXXX, le nom de la clé HSM est XXXX.

Important :

- Le nom de la clé HSM doit être le même que l'ident que vous avez spécifié lorsque vous avez converti une clé intégrée dans un format de clé simple.
- Les clés doivent être présentes dans le `/var/opt/nfast/kmdata/local/` répertoire de ADC.

Ajouter une clé HSM à l'aide de l'interface de ligne de commande

À l'invite du shell, exécutez la commande suivante :

```
1 add ssl hsmKey <hsmKeyName> -key <string>
2 <!--NeedCopy-->
```

Exemple :

```
1 add ssl hsmKey examplersa2048key  - key key_simple_examplersa2048key
2 Done
3 <!--NeedCopy-->
```

Ajouter une clé HSM à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > HSM**, puis ajoutez une clé HSM.

Ajouter une paire de clés de certificat sur ADC

Pour plus d'informations sur les paires de clés de certificat, voir Ajouter ou mettre à jour une paire de clés de certificat.

Ajouter une paire de clés de certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, exécutez la commande suivante :


```
add ssl certKey <certkeyName> -cert <string> -hsmKey <string>
<!--NeedCopy-->
```

Exemple :

```
add ssl certKey key22 -cert example_selfcert -hsmKey examplersa2048key
Done
<!--NeedCopy-->
```

Ajouter une paire de clés de certificat à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > Certificats**et ajoutez une paire certificat-clé.

Ajouter un serveur virtuel

Pour plus d'informations sur un serveur virtuel, reportez-vous à la section Configuration du serveur virtuel SSL.

Configurer un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, exécutez la commande suivante :

```
add lb vserver <name> <serviceType> <IPAddress> <port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver v1 SSL 192.168.17.252 443
<!--NeedCopy-->
```

Configurer un serveur virtuel SSL à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, créez un serveur virtuel et spécifiez le protocole en tant que protocole SSL.

Ajouter un objet serveur

Avant de pouvoir ajouter un objet serveur sur ADC, assurez-vous que vous avez créé un serveur principal. L'exemple suivant utilise le module Python HTTP Server intégré sur un système Linux.

Exemple :


```
%python -m SimpleHTTPServer 80
<!--NeedCopy-->
```

Ajouter un objet serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, exécutez la commande suivante :

```
add server <name> <IPAddress>
<!--NeedCopy-->
```

Exemple :

```
add server s1 192.168.17.246
<!--NeedCopy-->
```

Ajouter un objet serveur à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs**et ajoutez un serveur.

Ajouter un service

Pour plus d'informations, voir Configuration des services.

Configurer un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, exécutez la commande suivante :

```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
add service sr1 s1 HTTP 80
<!--NeedCopy-->
```

Configurer un service à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis créez un service.

Liez le service au serveur virtuel

Pour plus d'informations, voir Lier les services au serveur virtuel SSL.

Lier un service à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, exécutez la commande suivante :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver v1 sr1
<!--NeedCopy-->
```

Lier un service à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel, puis cliquez dans le volet Services pour lier un service au serveur virtuel.

Liez la paire de clés de certificat au serveur virtuel sur ADC

Pour plus d'informations, voir Lier la paire de clés de certificat au serveur virtuel SSL.

Liez une paire de clés de certificat à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, exécutez la commande suivante :

```
bind ssl vserver <vServerName> -certkeyName <string>
<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver v1 -certkeyName key22
Warning: Current certificate replaces the previous binding
<!--NeedCopy-->
```

Liez une paire de clés de certificat à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel SSL et, dans **Paramètres avancés**, cliquez sur **Certificat SSL**.
3. Liez un certificat de serveur au serveur virtuel.

Vérifier la configuration

Pour afficher la configuration à l'aide de l'interface de ligne de commande :

À l'invite de commandes, exécutez les commandes suivantes :

```
show lb vserver <name>
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
show lb vserver v1
        v1 (192.168.17.252:443) - SSL   Type: ADDRESS
        State: UP
        Last state change was at Wed Oct 29 03:11:11 2014
        Time since last state change: 0 days, 00:01:25.220
        Effective State: UP
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow logging: ENABLED
        No. of Bound Services :  1 (Total)       1 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: Bound service's state
           changed to UP
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
        L2Conn: OFF
        Skip Persistency: None
        IcmpResponse: PASSIVE
        RHIstate: PASSIVE
        New Service Startup Request Rate: 0 PER_SECOND, Increment
           Interval: 0
        Mac mode Retain Vlan: DISABLED
        DBS_LB: DISABLED
        Process Local: DISABLED
        Traffic Domain: 0

1) sr1 (192.168.17.246: 80) - HTTP State: UP    Weight: 1
Done
<!--NeedCopy-->
```



```
sh ssl vserver v1
        Advanced SSL configuration for VServer v1:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 0
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        SSLv2: DISABLED  SSLv3: DISABLED  TLSv1.0: ENABLED  TLSv1.1:
           DISABLED  TLSv1.2: DISABLED
        Push Encryption Trigger: Always
        Send Close-Notify: YES

        ECC Curve: P_256, P_384, P_224, P_521

1)      CertKey Name: key22       Server Certificate

1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
 Done
<!--NeedCopy-->
```

Pour afficher la configuration à l'aide de l'interface graphique :

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis double-cliquez sur un serveur virtuel SSL pour l'ouvrir et afficher la configuration.

Limitations

August 20, 2021

- SSL version 3 (SSLv3) n'est pas pris en charge sur une appliance MPX, mais est pris en charge sur une appliance virtuelle VPX. Une instance VPX provisionnée sur une appliance SDX prend en charge SSLv3 uniquement si une puce SSL n'est pas affectée à l'instance.
- Les chiffrements d'exportation ne sont pas pris en charge.
- L'échange de clés de serveur SSL à l'aide de clés HSM n'est pas pris en charge.
- Si vous avez ajouté ou supprimé des clés après la dernière sauvegarde de la configuration, vous devez enregistrer la configuration avant d'effectuer un redémarrage à chaud. Si vous

n'enregistrez pas la configuration, il y a une incompatibilité de clé entre ADC et le HSM.

- Vous ne pouvez pas lier une clé HSM à un serveur virtuel DTLS.
- Vous ne pouvez pas lier une paire de clés de certificat créée à l'aide d'une clé HSM à un service SSL.
- Vous ne pouvez pas utiliser l'interface graphique pour inscrire ADC en tant que client du HSM ou vérifier l'état du HSM à partir de l'utilitaire de configuration.
- À partir de la version 11 build 62.x, la renégociation SSL est prise en charge.
- Vous ne pouvez pas signer des demandes OCSP à l'aide d'une paire de clés de certificat créée à l'aide d'une clé HSM.
- Un ensemble de certificats avec des clés HSM n'est pas pris en charge.
- Une erreur n'apparaît pas si la clé HSM et le certificat ne correspondent pas. Par conséquent, lors de l'ajout d'une paire certificat-clé, vous devez vous assurer que la clé HSM et le certificat correspondent.
- Les partitions de clustering et d'administration ne sont pas prises en charge.

Annexe

August 20, 2021

Exemple :

Remarque : Dans l'exemple suivant, les commandes sont en caractères gras.

```
root@ns# ./chkserv
nCipher server running
root@ns# ./nfkminfo
World
 generation  2
 state       0x17a70000 Initialised Usable Recovery PINRecovery !
    ExistingClient RTC NVRAM FTO !AlwaysUseStrongPrimes SEEDebug
 n_modules   1
 hknso       cbec8c0c56c6b5e76b73147ef02d34a661eaa044
 hkm     bbb8d4839da5782be4d092735a7535538834dc91 (type Rijndael)
 hkmwk       1d572201be533ebc89f30fdd8f3fac6ca3395bf0
 hkre        01f21ecf43933ffdd45e74c3883525176c5c439c
 hkra        ac8ec5ee6bce00991bd97adce2091d9739b9b452
 hkmc        cf1b509abaad91995ed202d8f36613fc99433155
 hkp         c20910b2ed1ca62d6a2b0db67052a05f7bbfeb43
 hkrtc       bd811020a7c2f8df435a481c3767a89c2e13bc4f
 hknv        278b8012e48910d518a9ee91cff57233fb0c9093
 hkdsee      12230b0e31e3cec66324c0815f782cfb9249edd5
 hkfto       89dd6250b3d6149bcd15606f4553085e2fd6271a
```



```
 hkmnull     0100000000000000000000000000000000000000
 ex.client   none
 k-out-of-n  1/2
 other quora m=1 r=1 p=1 nv=1 rtc=1 dsee=1 fto=1
 createtime  2014-02-28 21:05:32
 nso timeout 10 min
 ciphersuite DLf1024s160mRijndael

Module #1
 generation 2
 state      0x2 Usable
 flags      0x10000 ShareTarget
 n_slots    2
 esn        BD17-C807-58D9
 hkml       70289a6edba00ddc7e3f6d6f5a49edc963e822f2

Module #1 Slot #0 IC 0
 generation    1
 phystype      SmartCard
 slotlistflags 0x2 SupportsAuthentication
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
No Cardset

Module #1 Slot #1 IC 0
 generation    1
 phystype      SoftToken
 slotlistflags 0x0
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
No Cardset

No Pre-Loaded Objects

root@ns# ./sigtest
 Hardware module #1 speed index 5792 recommended minimum queue 19
Found 1 module; using 19 jobs
Making 1024-bit RSAPrivate key on module #1;
  using Mech_RSApPKCS1 and PlainTextType_Bignum.
```



```
Generated and exported key from module #1.
Imported keys on module #1
 1,       3059 1223.6, 3059 overall
 2,       8698 2989.76, 4349 overall
 3,      14396 4073.06, 4798.67 overall
 4,      20091 4721.83, 5022.75 overall
 5,      25799 5116.3, 5159.8 overall
 6,      31496 5348.58, 5249.33 overall
 7,      37192 5487.55, 5313.14 overall
 8,      42780 5527.73, 5347.5 overall
 9,      45777 4515.44, 5086.33 overall
 10,      51457 4981.26, 5145.7 overall
 11,      57151 5266.36, 5195.55 overall
 12,      62813 5424.61, 5234.42 overall
 13,      68496 5527.97, 5268.92 overall
 14,      74182 5591.18, 5298.71 overall
 15,      79832 5614.71, 5322.13 overall
 16,      85518 5643.23, 5344.88 overall
 17,      88412 4543.54, 5200.71 overall
 18,      94086 4995.72, 5227 overall
 19,      99778 5274.23, 5251.47 overall
 20,     105469 5440.94, 5273.45 overall
 21,     111133 5530.16, 5292.05 overall
 22,     116838 5600.1, 5310.82 overall
 23,     122522 5633.66, 5327.04 overall
 24,     128175 5641.4, 5340.62 overall
 25,     131072 4543.64, 5242.88 overall
 26,     136762 5002.18, 5260.08 overall
 27,     142415 5262.51, 5274.63 overall
 28,     148125 5441.51, 5290.18 overall
 29,     153816 5541.3, 5304 overall
 30,     159414 5563.98, 5313.8 overall
<!--NeedCopy-->
```

Prise en charge du module de sécurité matérielle Thales Luna Network

August 20, 2021

Une appliance Citrix ADC non FIPS stocke la clé privée du serveur sur le disque dur. Sur une appliance FIPS, la clé est stockée dans un module cryptographique connu sous le nom de module de sécurité matérielle (HSM). Le stockage d'une clé dans le HSM la protège contre les attaques physiques et logicielles. En outre, les clés sont cryptées avec des chiffrements spéciaux approuvés par FIPS.

Seules les appliances FIPS Citrix ADC MPX 9700/10500/12500/15500 et les appliances FIPS MPX/SDX 14000 prennent en charge une carte FIPS. La prise en charge FIPS n'est pas disponible sur les autres appliances MPX/SDX, ni sur les appliances Citrix ADC VPX. Cette limitation est résolue en prenant en charge un HSM réseau Thales Luna sur toutes les appliances Citrix ADC MPX, SDX et VPX, à l'exception des appliances FIPS MPX 9700/10500/12500/15500 et MPX/SDX 14000 FIPS.

Un réseau HSM Thales Luna est conçu pour protéger les clés cryptographiques critiques et accélérer les opérations cryptographiques sensibles dans un large éventail d'applications de sécurité.

Matrice des versions prises en charge

Version de Citrix ADC	Version de l'appliance logicielle	Version du micrologiciel	Version du client
11.1, 12.0, 12.1, 13.0	5.2.3-1	6.2.1	6.0.0
11.1, 12.0, 12.1, 13.0	6.2.2-5	6.10.9	6.2.2
13.0	7.2.0-220	7.0.3	7.2.2 (7.2.0-220)

Conditions préalables

August 20, 2021

Avant de pouvoir utiliser un HSM réseau Thales Luna avec un Citrix ADC, assurez-vous que les conditions préalables suivantes sont remplies :

- Un HSM réseau Thales Luna est installé sur le réseau, prêt à l'emploi et accessible à Citrix ADC. C'est-à-dire que l'adresse NSIP ou l'adresse SNIP est ajoutée en tant que client autorisé sur le HSM.
- Des licences sont disponibles pour prendre en charge le nombre requis de partitions sur le HSM.
- Le réseau HSM Thales Luna et Citrix ADC peuvent initier des connexions entre elles via le port 1792.
- Vous utilisez NetScaler version 11.1 ou ultérieure.
- L'appliance Citrix ADC ne contient pas de carte FIPS Cavium.

> **Important**
>
> Les HSM réseau Thales Luna ne sont pas pris en charge sur les appliances FIPS MPX 9700/10500/12500/15500.

Configurer un client Thales Luna sur ADC

August 20, 2021

Une fois que vous avez configuré le HSM Thales Luna et créé les partitions requises, vous devez créer des clients et les affecter à des partitions. Commencez par configurer les clients Thales Luna sur Citrix ADC et configurer les liens de confiance réseau (NTL) entre les clients Thales Luna et le HSM Thales Luna. Un exemple de configuration est fourni dans l' annexe.

1. Remplacez le répertoire par /var/safenet et installez le client Thales Luna. À l'invite shell, tapez :

   ```
   cd /var/safenet
   <!--NeedCopy-->
   ```

   Pour installer le client Thales Luna version 6.0.0, tapez :

   ```
   install_client.sh -v 600
   <!--NeedCopy-->
   ```

   Pour installer le client Thales Luna version 6.2.2, tapez :

   ```
   install_client.sh -v 622
   <!--NeedCopy-->
   ```

   Pour installer le client Thales Luna version 7.2.2, tapez :

   ```
   install_client.sh -v 722
   <!--NeedCopy-->
   ```

2. Configurez les NTL entre le client Thales Luna (ADC) et HSM.

   Une fois le répertoire '/var/safenet/' créé, effectuez les tâches suivantes sur ADC.

   a) Changez le répertoire en '/var/safenet/config/' et exécutez le script 'safenet_config'. À l'invite shell, tapez :

   ```
   cd /var/safenet/config

   sh safenet_config
   <!--NeedCopy-->
   ```

   Ce script copie le fichier « Chrystoki.conf » dans le répertoire /etc/. Il génère également un lien symbolique 'LibCryptoki2_64.so' dans le répertoire '/usr/lib/'.

   b) Créer et transférer un certificat et une clé entre l'ADC et le HSM Thales Luna.

Pour communiquer en toute sécurité, l'ADC et le HSM doivent échanger des certificats. Créez un certificat et une clé sur ADC, puis transférez-le au HSM. Copiez le certificat HSM dans ADC.

i) Changer le répertoire en /var/safenet/safenet/lunaclient/bin.

ii) Créer un certificat sur ADC. À l'invite shell, tapez :

```
./vtl createCert -n <ip address of Citrix ADC>
<!--NeedCopy-->
```

Cette commande ajoute également le chemin d'accès du certificat et de la clé au fichier « /etc/Chrystoki.conf ».

iii) Copier ce certificat au HSM. À l'invite shell, tapez :

```
scp /var/safenet/safenet/lunaclient/cert/client/<ip address of NS
   >.pem <LunaSA_HSM account>@<IP address of Luna SA>
<!--NeedCopy-->
```

iv) Copiez le certificat HSM dans Citrix ADC. À l'invite shell, tapez :

```
scp <HSM account>@<HSM IP>:server.pem  /var/safenet/safenet/
   lunaclient/server_<HSM ip>.pem
<!--NeedCopy-->
```

3. Enregistrez Citrix ADC en tant que client et attribuez-lui une partition sur le HSM Thales Luna.

   Connectez-vous au HSM et créez un client. Entrez le NSIP comme adresse IP du client. Cette adresse doit être l'adresse IP de l'ADC à partir duquel vous avez transféré le certificat au HSM. Une fois que le client est correctement enregistré, affectez-lui une partition. Exécutez les commandes suivantes sur le HSM.

   a) Utilisez SSH pour vous connecter au HSM Thales Luna et entrez le mot de passe.

   b) Enregistrez Citrix ADC sur le HSM Thales Luna. Le client est créé sur le HSM. L'adresse IP est l'adresse IP du client. Autrement dit, l'adresse du NSIP.

   À l'invite, tapez :

   ```
   client register  -client <client name> -ip <Citrix ADC ip>
   <!--NeedCopy-->
   ```

   c) Attribuez au client une partition à partir de la liste des partitions. Pour afficher les partitions disponibles, tapez :

   ```
   <luna_sh> partition list
   <!--NeedCopy-->
   ```


Attribuez une partition à partir de cette liste. Type :

```
<lunash:> client assignPartition -client <Client Name> -par <
   Partition Name>
<!--NeedCopy-->
```

4. Enregistrez le HSM avec son certificat sur le Citrix ADC.

   Dans l'ADC, changez le répertoire par « /var/safenet/safenet/lunaclient/bin » et, à l'invite du shell, tapez :

```
./vtl addserver -n <IP addr of HSM> -c /var/safenet/safenet/
   lunaclient/server_<HSM_IP>.pem
<!--NeedCopy-->
```

   Pour supprimer le HSM inscrit sur ADC, tapez :

```
./vtl deleteServer -n <HSM IP> -c <cert path>
<!--NeedCopy-->
```

   Pour répertorier les serveurs HSM configurés sur ADC, tapez :

```
./vtl listServer
<!--NeedCopy-->
```

   > **Remarque :**
   >
   > Avant de supprimer le HSM à l'aide `vtl`, assurez-vous que toutes les clés de ce HSM sont supprimées manuellement de l'appliance. Les clés HSM ne peuvent pas être supprimées après la suppression du serveur HSM.

5. Vérifiez la connectivité des liens d'approbation réseau (NTL) entre ADC et le HSM. À l'invite shell, tapez :

```
./vtl verify
<!--NeedCopy-->
```

   Si la vérification échoue, passez en revue toutes les étapes. Les erreurs sont dues à une adresse IP incorrecte dans les certificats clients.

6. Enregistrez la configuration.

   Les étapes précédentes mettent à jour le fichier de configuration « /etc/Chrystoki.conf ». Ce fichier est supprimé au démarrage de l'ADC. Copiez la configuration dans le fichier de configuration par défaut, qui est utilisé lors du redémarrage d'un ADC.

   À l'invite shell, tapez :


```
root@ns# cp /etc/Chrystoki.conf /var/safenet/config/
<!--NeedCopy-->
```

La pratique recommandée consiste à exécuter cette commande chaque fois qu'il y a une modification de la configuration associée à Thales Luna.

7. Démarrez le processus de passerelle Thales Luna.

   À l'invite shell, tapez :

```
sh /var/safenet/gateway/start_safenet_gw
<!--NeedCopy-->
```

8. Configurez le démarrage automatique du démon de Gateway au démarrage.

   Créez le fichier « safenet_is_enrolled », qui indique que Thales Luna HSM est configuré sur cet ADC. Chaque fois que ADC redémarre et que ce fichier est trouvé, la Gateway est automatiquement démarrée.

   À l'invite shell, tapez :

```
touch /var/safenet/safenet_is_enrolled
<!--NeedCopy-->
```

Configurer les HSM Thales Luna dans une configuration haute disponibilité sur ADC

August 20, 2021

La configuration des HSM Thales Luna en haute disponibilité (HA) garantit un service ininterrompu même si tous les appareils, sauf un, ne sont pas disponibles. Dans une configuration HA, chaque HSM rejoint un groupe HA en mode actif. Les HSM Thales Luna dans une configuration HA fournissent un équilibrage de charge de tous les membres du groupe afin d'augmenter les performances et le temps de réponse tout en garantissant un service haute disponibilité. Pour plus d'informations, contactez le service commercial et le support de Thales Luna.

Conditions préalables :

- Au moins deux appareils Thales Luna HSM. Tous les périphériques d'un groupe HA doivent avoir une authentification PED (chemin d'accès approuvé) ou une authentification par mot de passe. Une combinaison d'authentification de chemin d'accès approuvé et d'authentification de mot de passe dans un groupe HA n'est pas prise en charge.

- Les partitions de chaque périphérique HSM doivent avoir le même mot de passe même si l'étiquette (nom) est différente.
- Toutes les partitions de HA doivent être affectées au client (appliance Citrix ADC).

Après avoir configuré un client Thales Luna sur ADC, comme décrit dans Configurer un client Thales Luna sur ADC, effectuez les étapes suivantes pour configurer les HSM Thales Luna dans HA :

1. Sur l'invite Citrix ADC shell, lancez `lunacm` (/usr/safenet/lunaclient/bin)

   Exemple :

   ```
   root@ns# cd /var/safenet/safenet/lunaclient/bin/

   root@ns# ./lunacm
   <!--NeedCopy-->
   ```

2. Identifiez les ID de slot des partitions. Pour répertorier les emplacements (partitions) disponibles, tapez :

   ```
   lunacm:> slot list
   <!--NeedCopy-->
   ```

   Exemple :

   ```
       Slot Id ->              0
       HSM Label ->            trinity-p1
       HSM Serial Number ->    481681014
       HSM Model ->            LunaSA 6.2.1
       HSM Firmware Version -> 6.10.9
       HSM Configuration ->    Luna SA Slot (PED) Signing With
          Cloning Mode
       HSM Status ->           OK

       Slot Id ->              1
       HSM Label ->            trinity-p2
       HSM Serial Number ->    481681018
       HSM Model ->            LunaSA 6.2.1
       HSM Firmware Version -> 6.10.9
       HSM Configuration ->    Luna SA Slot (PED) Signing With
          Cloning Mode
       HSM Status ->           OK

        Slot Id ->              2
        HSM Label ->            neo-p1
        HSM Serial Number ->    487298014
        HSM Model ->            LunaSA 6.2.1
   ```



```
21       HSM Firmware Version -> 6.10.9
22       HSM Configuration ->    Luna SA Slot (PED) Signing With
             Cloning Mode
23      HSM Status ->           OK
24
25      Slot Id ->              3
26      HSM Label ->            neo-p2
27      HSM Serial Number ->    487298018
28      HSM Model ->            LunaSA 6.2.1
29      HSM Firmware Version -> 6.10.9
30      HSM Configuration ->    Luna SA Slot (PED) Signing With
            Cloning Mode
31      HSM Status ->           OK
32
33      Slot Id ->              7
34      HSM Label ->            hsmha
35      HSM Serial Number ->    1481681014
36      HSM Model ->            LunaVirtual
37      HSM Firmware Version -> 6.10.9
38      HSM Configuration ->    Luna Virtual HSM (PED) Signing With
            Cloning Mode
39      HSM Status ->           N/A - HA Group
40
41      Slot Id ->              8
42      HSM Label ->            newha
43      HSM Serial Number ->    1481681018
44      HSM Model ->            LunaVirtual
45      HSM Firmware Version -> 6.10.9
46      HSM Configuration ->    Luna Virtual HSM (PED) Signing With
            Cloning Mode
47      HSM Status ->           N/A - HA Group
48
49      Current Slot Id: 0
50  <!--NeedCopy-->
```

3. Créez le groupe HA. La première partition est appelée partition primaire. Vous pouvez ajouter plusieurs partitions secondaires.

```
1  lunacm:> hagroup createGroup -slot <slot number of primary
       partition> -label <group name> -password <partition password >
2
3  lunacm:> hagroup createGroup -slot 1 -label gp12 -password ******
4  <!--NeedCopy-->
```

4. Ajoutez les membres secondaires (partitions HSM). Répétez cette étape pour que toutes les par-

titions soient ajoutées au groupe HA.

```
lunacm:> hagroup addMember -slot <slot number of secondary
    partition to be added> -group <group name> -password <partition
     password>
<!--NeedCopy-->
```

Code :

```
lunacm:> hagroup addMember -slot 2 -group gp12 -password ******
<!--NeedCopy-->
```

5. Activer le mode HA uniquement.

```
lunacm:> hagroup HAOnly  - enable
<!--NeedCopy-->
```

6. Activer le mode de récupération actif.

```
lunacm:.>hagroup recoveryMode  - mode active
<!--NeedCopy-->
```

7. Définissez l'intervalle de récupération automatique (en secondes). Le délai par défaut est de 60 secondes.

```
lunacm:.>hagroup interval  - interval <value in seconds>
<!--NeedCopy-->
```

Exemple :

```
lunacm:.>hagroup interval  - interval 120
<!--NeedCopy-->
```

8. Définissez le nombre de tentatives de récupération. Une valeur de -1 permet un nombre infini de nouvelles tentatives.

```
lunacm:> hagroup retry -count <xxx>
<!--NeedCopy-->
```

Exemple :

```
lunacm:> hagroup retry -count 2
<!--NeedCopy-->
```

9. Copiez la configuration de `Chrystoki.conf` vers le répertoire de configuration SafeNet.


```
cp /etc/Chrystoki.conf /var/safenet/config/
<!--NeedCopy-->
```

10. Redémarrez l'appliance ADC.

```
reboot
<!--NeedCopy-->
```

Après avoir configuré Thales Luna HSM dans HA, reportez-vous à la section Autre configuration ADC pour plus de configuration sur ADC.

Autres configurations ADC

August 20, 2021

1. Générez une clé sur le HSM.

   Utilisez des outils tiers pour créer des clés sur le HSM.

2. Ajoutez une clé HSM sur ADC.

   Important Le caractère # n'est pas pris en charge dans un nom de clé. Si le nom de clé inclut ce caractère, l'opération de clé de chargement échoue.

   Pour ajouter une clé HSM Thales Luna à l'aide de l'interface de ligne de commande :

   À l'invite de commandes, tapez :

```
add ssl hsmkey <KeyName> -hsmType SAFENET -serialNum <serial #> -
   password
<!--NeedCopy-->
```

   où :

   -keyName est la clé créée sur le HSM à l'aide d'outils tiers.

   -SerialNum est le numéro de série de la partition sur le HSM sur lequel les clés sont générées.

   Remarque : Pour HSM dans une configuration haute disponibilité, utilisez le numéro de série du groupe haute disponibilité.

   -password est le mot de passe de la partition sur laquelle les clés sont présentes.

   Pour ajouter une clé HSM Thales Luna à l'aide de l'interface graphique :

   Accédez à **Gestion du trafic** > **SSL** > **HSM** et ajoutez une clé HSM. Vous devez spécifier le type HSM comme **SAFENET**.

3. Ajoutez une paire de clés de certificat sur ADC. Utilisez d'abord un outil tiers pour générer un certificat associé à la clé. Ensuite, copiez le certificat dans le répertoire /nsconfig/ssl/ de ADC.

   Remarque : La clé doit être une clé HSM.

   Pour ajouter une paire certkey sur ADC à l'aide de l'interface de ligne de commande :

   À l'invite de commandes, tapez :

   ```
   add ssl certkey <CertkeyName> -cert <cert name> -hsmkey <KeyName>
   <!--NeedCopy-->
   ```

   Pour ajouter une paire certkey sur ADC à l'aide de l'interface graphique :

   a) Accédez à **Gestion du trafic** > **SSL**.
   b) Dans **Mise en route**, sélectionnez **Installer le certificat (HSM)**et créez une paire de clés de certificat à l'aide d'une clé HSM.

4. Créez un serveur virtuel et liez la paire de clés de certificat à ce serveur virtuel.

Pour plus d'informations sur la création d'un serveur virtuel, cliquez sur Configuration du serveur virtuel SSL.

Pour plus d'informations sur l'ajout d'une paire de clés de certificat, cliquez sur Ajouter ou mettre à jour une paire de clés de certificat.

Pour plus d'informations sur la liaison d'une paire de clés de certificat à un serveur virtuel SSL, cliquez sur Lier la paire de clés de certificat au serveur virtuel SSL.

Appliances Citrix ADC dans une configuration haute disponibilité

August 20, 2021

Vous pouvez configurer une configuration haute disponibilité (HA) sur les appliances Citrix ADC avec une configuration Thales Luna HSM de l'une des deux manières suivantes :

- Tout d'abord, configurez un HSM Thales Luna sur les deux nœuds, en utilisant le même HSM et la même partition. Ensuite, créez une paire HA. Enfin, ajoutez la configuration de Citrix ADC, telle que les clés, les paires de clés de certificat et les serveurs virtuels, sur le nœud principal.
- Si un HSM Thales Luna est déjà configuré sur un nœud avec la configuration Citrix ADC, ajoutez une configuration similaire sur l'autre nœud. Copiez « /var/safenet/sfgw_ident_file » du premier nœud vers l'autre et redémarrez le binaire safenet_gw. Une fois que la Gateway est en cours d'exécution, ajoutez les nœuds dans une configuration HA.

Limitations

October 5, 2021

1. Pour toute modification de la configuration liée au HSM dans une configuration existante, telle que l'ajout ou la suppression d'un HSM, ou la création d'une configuration HA, copiez « /etc/Chrystoki.conf » dans « /var/safenet/config'.
2. Après avoir ajouté, supprimé ou redémarré un HSM, vous devez redémarrer le binaire « /var/safenet/gateway/safenet_gw ». Si vous ne redémarrez pas le binaire de la passerelle, le HSM ne servira aucun trafic après son ajout ou après son redémarrage.
3. Pour redémarrer ou arrêter le binaire « /var/safenet/gateway/safenet_gw » actuel, utilisez

   ```
   kill -SIGTERM <PID>
   kill -SIGINT <PID>
   <!--NeedCopy-->
   ```

   Important ! Ne pas utiliser `kill -9 <PID>` ou `kill -6 <PID>`
4. Avant de supprimer un HSM existant de ADC, supprimez de ADC, toutes les clés et paires de clés de certificat associées à ce HSM. Vous ne pouvez pas supprimer ces fichiers de l'ADC après avoir supprimé le HSM.
5. Sur une appliance Citrix ADC autonome, les HSM Thales Luna en HA sont pris en charge pour Luna version 6.2 et ultérieure.
6. Les chiffrements EXPORT ne sont pas pris en charge.
7. L'opération de mise à jour des paires de clés de certificat n'est pas prise en charge.
8. Lorsque vous générez une clé HSM sur un outil tiers, les noms des clés privée et publique doivent être identiques. Lorsque vous ajoutez la clé HSM sur la solution matérielle-logicielle, indiquez ce nom comme nom de clé.
9. Le ## caractère n'est pas pris en charge dans un nom de clé et un mot de passe de partition.
10. Les partitions de cluster et d'administration ne sont pas prises en charge.

Annexe

August 20, 2021

Exemples de commandes avec leurs sorties :

Exécuter le script

```
1      root@ns# pwd
2     /var/safenet/config
3     root@ns# sh safenet_config
4 <!--NeedCopy-->
```

Créer un certificat

```
1     root@ns# cd /var/safenet/safenet/lunaclient/bin
2     root@ns# ./vtl createcert -n 10.102.59.175
3     Private Key created and written to: /var/safenet/safenet/lunaclient
         /cert/client/10.102.59.175Key.pem
4     Certificate created and written to: /var/safenet/safenet/lunaclient
         /cert/client/10.102.59.175.pem
5 <!--NeedCopy-->
```

Copier le certificat dans le HSM

```
1     root@ns# scp /var/safenet/safenet/lunaclient/cert/client
         /10.102.59.175.pem admin@10.217.2.7:
2     admin@10.217.2.7's password:
3
4     10.102.59.175.pem          100%  818     0.8KB/s   00:00
5 <!--NeedCopy-->
```

Copiez le certificat et la clé du HSM vers l'appliance Citrix ADC

```
1     root@ns# scp admin@10.217.2.7:server.pem /var/Thales Luna/safenet/
         lunaclient/server.2.7.pem
2     admin@10.217.2.7's password:
3
4     server.pem            100% 1164     1.1KB/s   00:01
5 <!--NeedCopy-->
```

Utiliser SSH pour se connecter au Thales Luna HSM

```
1     ssh admin@10.217.2.7
2     Connecting to 10.217.2.7:22...
3     Connection established.
```



```
    To escape to local shell, press 'Ctrl+Alt+]'.

    Last login: Thu Jun 23 02:20:29 2016 from 10.252.243.11

    Luna SA 5.2.3-1 Command Line Shell - Copyright (c) 2001-2014
       SafeNet, Inc. All rights reserved.

    [Safenet1] lunash:>hsm login


      Please enter the HSM Administrators' password:
      > *******

    'hsm login' successful.


    Command Result : 0 (Success)
    [Safenet1] lunash:>
<!--NeedCopy-->
```

Enregistrez le Citrix ADC sur le HSM Thales Luna

```
    [Safenet1] lunash:>client register -client ns175 -ip 10.102.59.175

    'client register' successful.


    Command Result : 0 (Success)
    [Safenet1] lunash:>
<!--NeedCopy-->
```

Attribuer au client une partition à partir de la liste des partitions

```
    [Safenet1] lunash:>client assignPartition -client ns175 -partition
       p2

    'client assignPartition' successful.


    Command Result : 0 (Success)
    [Safenet1] lunash:>
<!--NeedCopy-->
```


Enregistrez le HSM avec son certificat sur le Citrix ADC

```
1     root@ns# ./vtl addserver -n 10.217.2.7 -c /var/safenet/safenet/
          lunaclient/server.2.7.pem
2
3     New server 10.217.2.7 successfully added to server list.
4 <!--NeedCopy-->
```

Vérifier la connectivité des liens d'approbation réseau (NTL) entre ADC et le HSM

```
1     root@ns# ./vtl verify
2
3     The following Luna SA Slots/Partitions were found:
4
5     Slot        Serial #                  Label
6     ====      ================          =====
7        0              477877010          p2
8 <!--NeedCopy-->
```

Enregistrer la configuration

```
1     root@ns# cp /etc/Chrystoki.conf /var/safenet/config/
2 <!--NeedCopy-->
```

Configurer le démarrage automatique du démon de Gateway au démarrage

```
1     touch /var/safenet/safenet_is_enrolled
2 <!--NeedCopy-->
```

Questions fréquentes

August 20, 2021

- **Comment puis-je vérifier que le processus Thales Luna est en cours d'exécution ?**

  À l'invite de shell Citrix ADC, tapez :

  ```
  1  ps - aux | grep safenet_gw
  2  <!--NeedCopy-->
  ```


- **Comment vérifier la connectivité des liens d'approbation réseau (NTL) entre ADC et le HSM ?**

  Après avoir configuré Thales Luna, remplacez le répertoire par « /var/safenet/safenet/lunaclient/bin » et tapez :

```
./vtl verify
<!--NeedCopy-->
```

Prise en charge de Azure Key Vault

August 20, 2021

L'appliance Citrix ADC s'intègre aux HSM externes (SafeNet et Thales) pour les déploiements locaux. Pour les déploiements dans le cloud, l'appliance ADC s'intègre à Azure Key Vault. L'appliance stocke ses clés privées dans Key Vault pour faciliter la gestion et la sécurité de la clé privée dans le domaine du cloud public. Vous n'avez plus à stocker et à gérer les clés dans différents emplacements pour les appliances ADC déployées sur plusieurs datacenters et fournisseurs de cloud.

L'utilisation d'ADC avec le niveau de tarification Azure Key Vault Premium, qui fournit des clés HSM, assure la conformité FIPS 140-2 niveau 2.

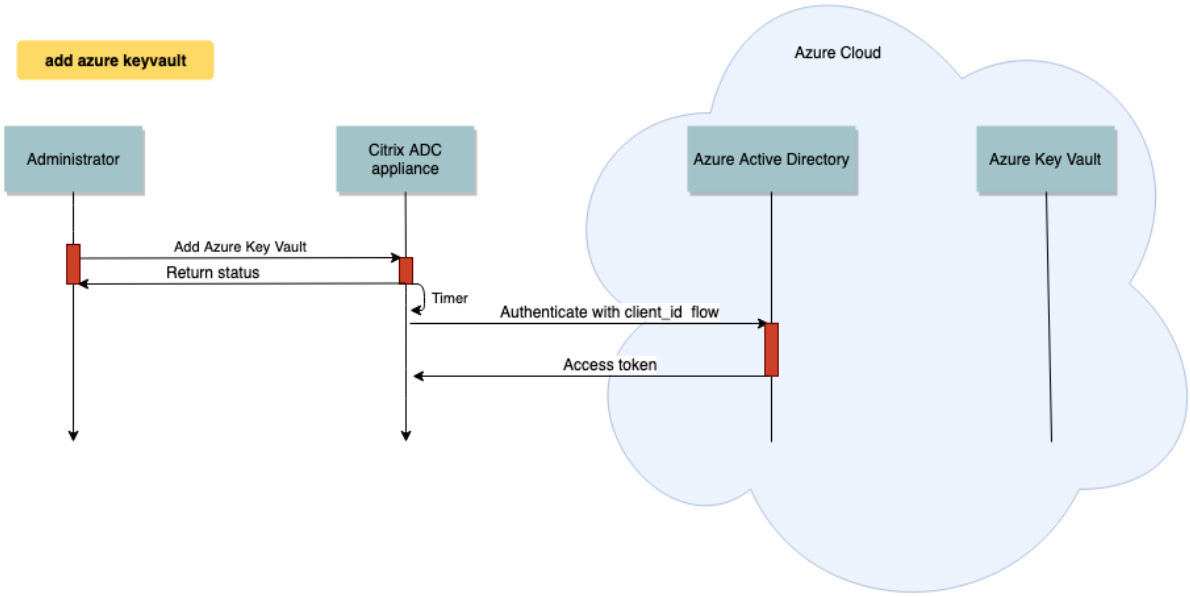
Azure Key Vault est une offre standard de Microsoft. Pour plus d'informations sur Azure Key Vault, consultez la documentation Microsoft Azure.

Remarque : L'intégration de Citrix ADC avec Azure Key Vault est prise en charge avec le protocole TLS 1.3.

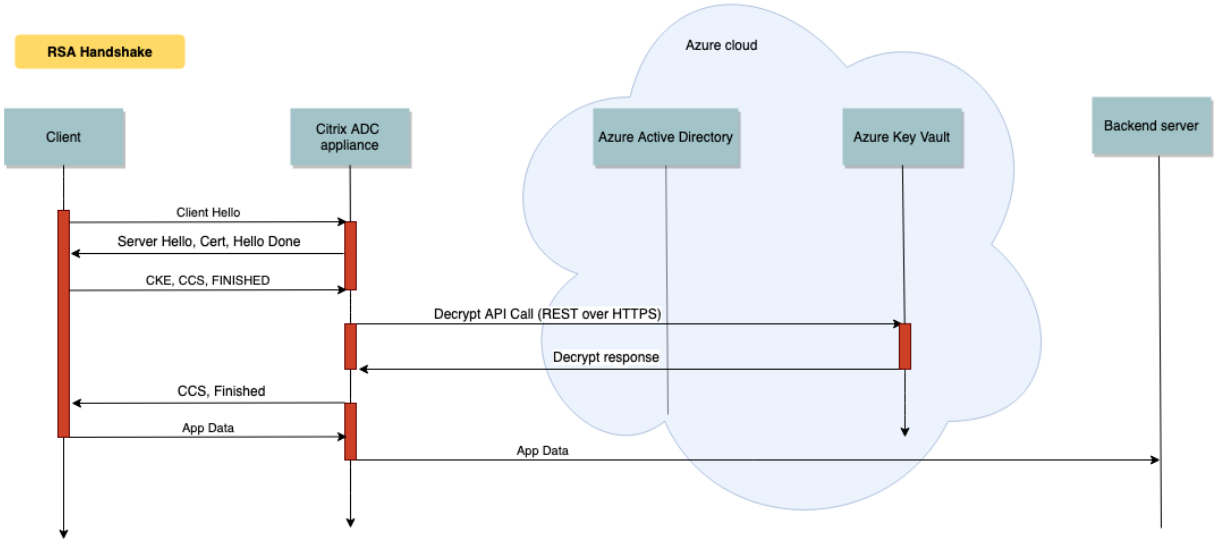
Aperçu de l'architecture

Azure Key Vault est un service permettant de stocker des secrets en toute sécurité dans le cloud Azure. En stockant vos clés dans Azure Key Vault, vous réduisez les risques de vol des clés. Une fois le coffre de clés configuré, vous pouvez y stocker vos clés. Configurez des serveurs virtuels sur l'appliance ADC pour effectuer des opérations de clé privée dans Key Vault. L'appliance ADC accède à la clé de chaque poignée de main SSL.

Le diagramme suivant illustre le processus d'obtenir un jeton d'accès à partir d'Azure Active Directory après l'authentification. Ce jeton est utilisé avec les appels d'API REST pour les opérations de crypto utilisant des clés privées.



Le diagramme suivant montre une poignée de main RSA typique. Le message d'échange de clés client (CKE) chiffré à l'aide de la clé publique est déchiffré à l'aide de la clé privée stockée dans le coffre de clés.



Dans une poignée de main ECDHE, le message d'échange de clés de serveur (SKE) envoyé par l'appliance Citrix ADC est signé à l'aide de la clé privée stockée dans Key Vault.

Conditions préalables

1. Vous devez disposer d'un abonnement Azure.

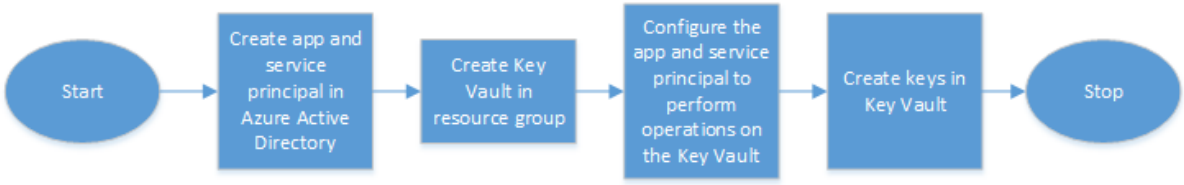
2. (Facultatif) Installez Azure CLI sur une machine Linux. Pour obtenir des instructions, reportez-vous à la documentation Azurehttps://docs.microsoft.com/en-us/cli/azure/install-azure-cli-apt?view=azure-cli-latest.
3. Terminez la configuration sur le portail Azure avant de configurer des entités sur l'appliance ADC.

Configurer l'intégration d'ADC Azure Key Vault

Effectuez d'abord la configuration sur le portail Azure suivie de la configuration sur l'appliance ADC.

Effectuez les étapes suivantes sur le portail Azure

L'organigramme suivant illustre le flux de haut niveau pour la configuration requise sur le portail Azure.

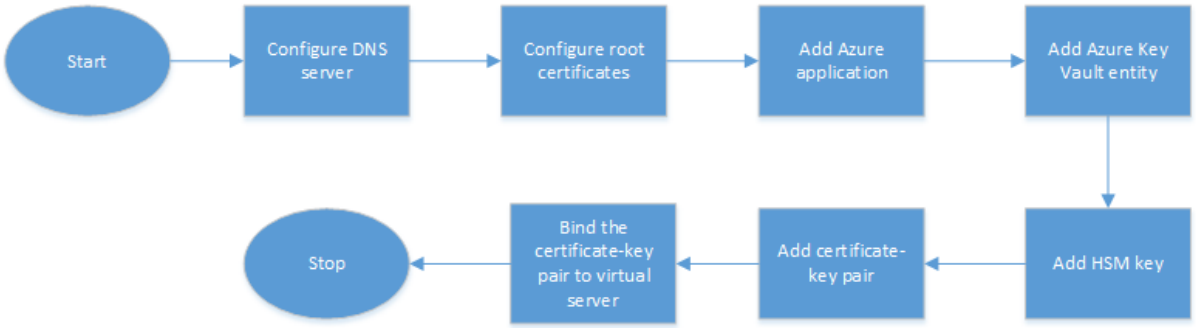


1. Créez l'application et le service principal dans Azure Active Directory.
2. Créez Key Vault dans un groupe de ressources.
3. Configurez l'application et le principal de service pour effectuer des opérations de signature et de décryptage sur Key Vault.
4. Créez des clés dans Key Vault en utilisant l'une des méthodes suivantes :
    a) En important un fichier clé.
    b) En générant un certificat.

Pour plus d'informations sur les commandes permettant de configurer les étapes précédentes, consultez la documentation Azure à l'adressehttps://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals.

Effectuez les étapes suivantes sur l'appliance ADC

L'organigramme suivant illustre le flux de haut niveau pour la configuration requise sur l'appliance ADC.



1. Configurez un serveur DNS.
2. Configurez les certificats racine pour vérifier les certificats présentés par Azure.
3. Créez une application Azure.
4. Créer une entité Azure Key Vault.
5. Créez une clé HSM.
6. Créez une paire de clés de certificat.
7. Liez la paire de clés de certificat à un serveur virtuel.

Configurer un serveur DNS

Un serveur DNS est requis pour la résolution de noms de l'hôte Key Vault et du point de terminaison Azure Active Directory.

Pour configurer un serveur DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

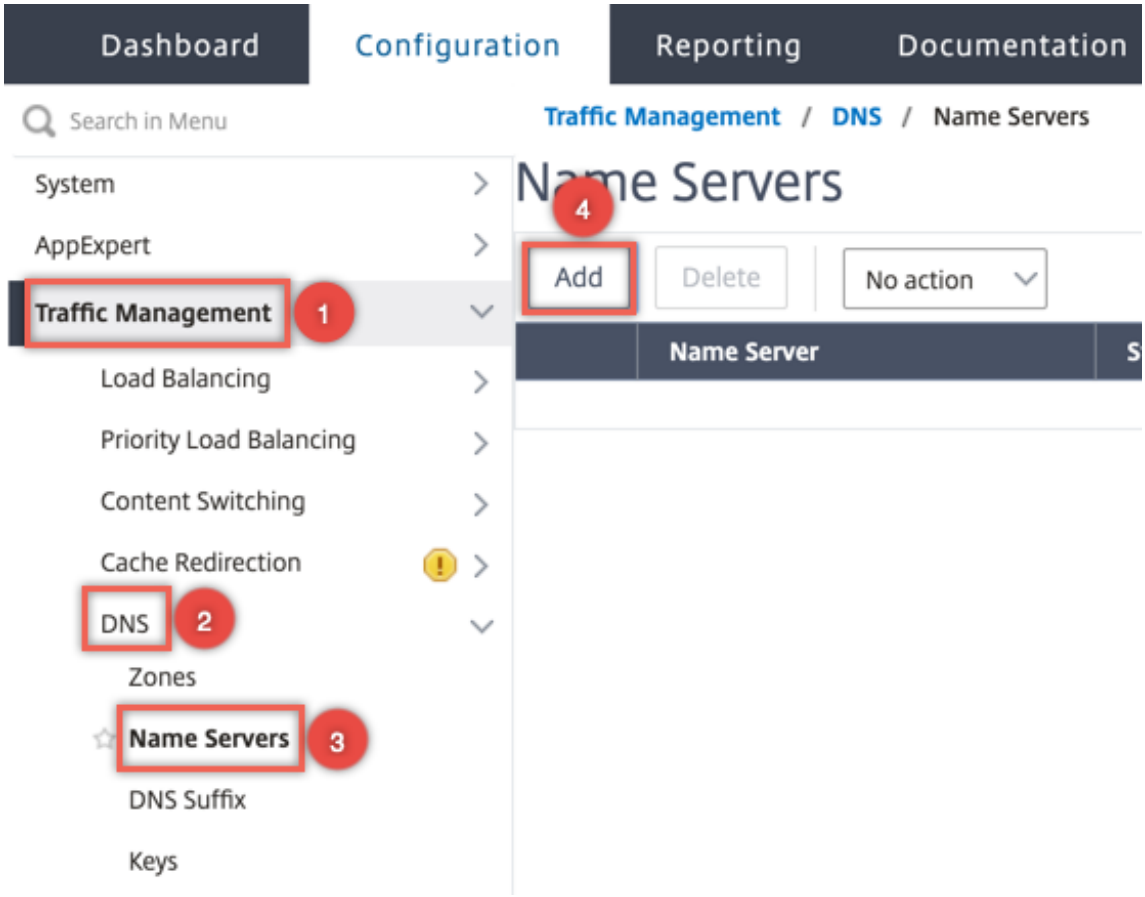
```
add dns nameserver <IP address>
<!--NeedCopy-->
```

Exemple :

```
add dns nameserver 192.0.2.150
<!--NeedCopy-->
```

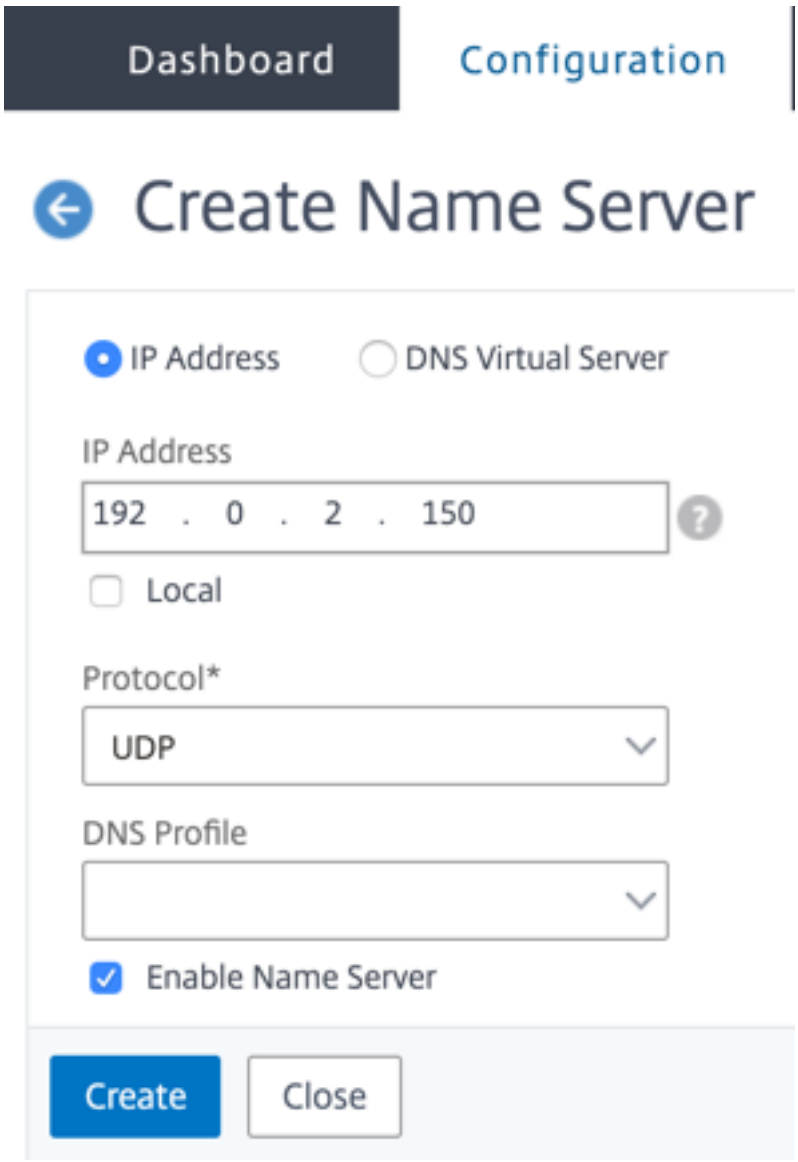
Pour configurer un serveur DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Serveurs de noms**. Cliquez sur **Ajouter**.



2. Entrez des valeurs pour les paramètres suivants :

   - Adresse IP : adresse IP d'un serveur de noms externe ou, si le paramètre Local est défini, adresse IP d'un serveur DNS local (LDNS).
   - Protocole - Protocole utilisé par le serveur de noms. UDP_TCP n'est pas valide si le serveur de noms est un serveur virtuel DNS configuré sur l'appliance.



3. Cliquez sur **Créer**.

Ajouter et lier un certificat racine

Téléchargez les certificats racine du certificat présenté par Azure Key Vault`https://<vault_name>.vault.azure.net` et Azure Active Directory (AAD)https://login.microsoftonline.com et chargez-le sur l'appliance ADC. Ces certificats sont requis pour valider le certificat présenté par Azure Key Vault et AAD. Liez un ou plusieurs certificats au groupe de certificats de l'autorité de certificationns_callout_certs.

Pour ajouter un certificat racine à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
add ssl certkey <certkeyname> -cert <certname>
bind ssl caCertGroup <caCertGroupName> <certkeyName>
<!--NeedCopy-->
```

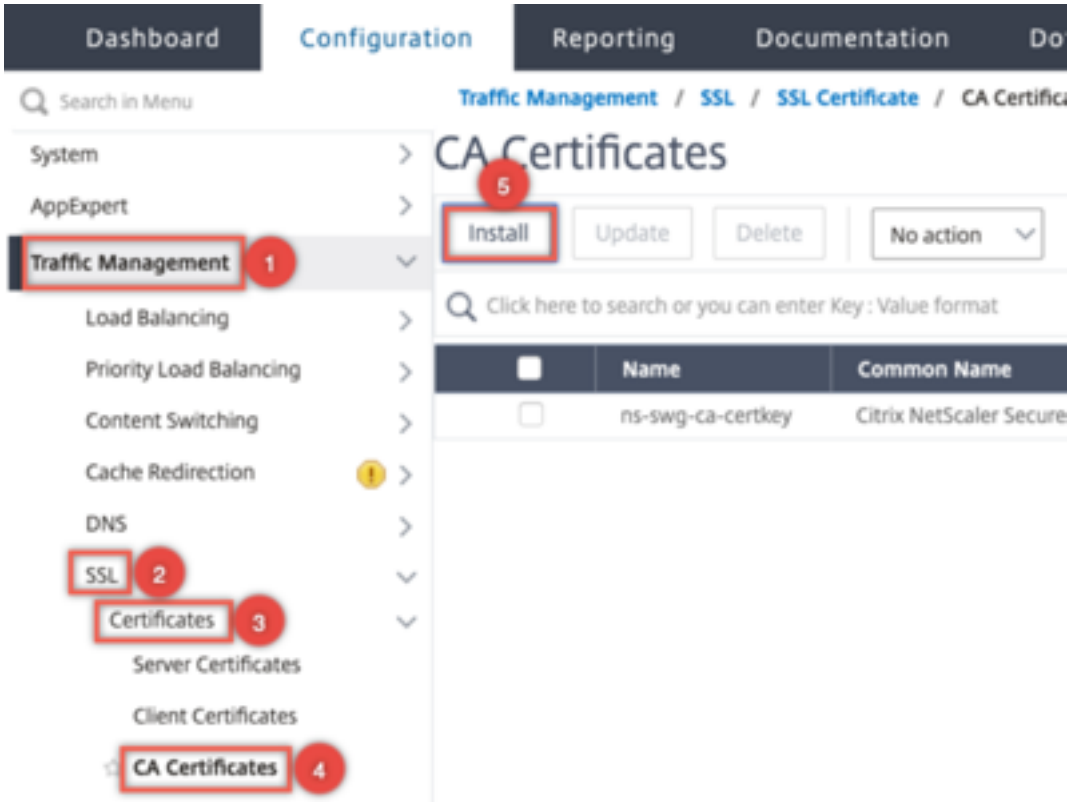
Exemple :

Dans l'exemple suivant, le certificat racine présenté par Azure Key Vault et AAD est le même.

```
add ssl certKey rootcert -cert RootCyberTrustRoot.crt
bind ssl cacertGroup ns_callout_certs  rootcert
<!--NeedCopy-->
```

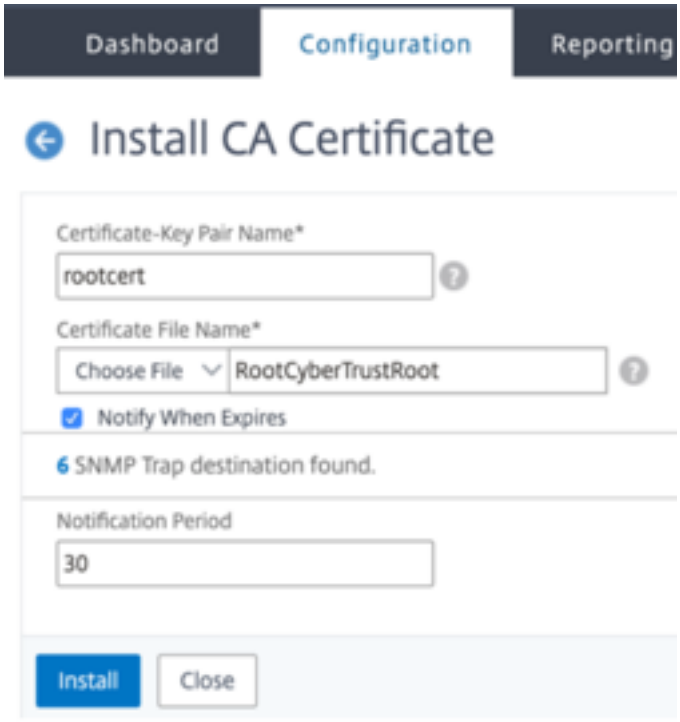
Pour ajouter un certificat racine à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Certificats > Certificats d'autorité de certification**.

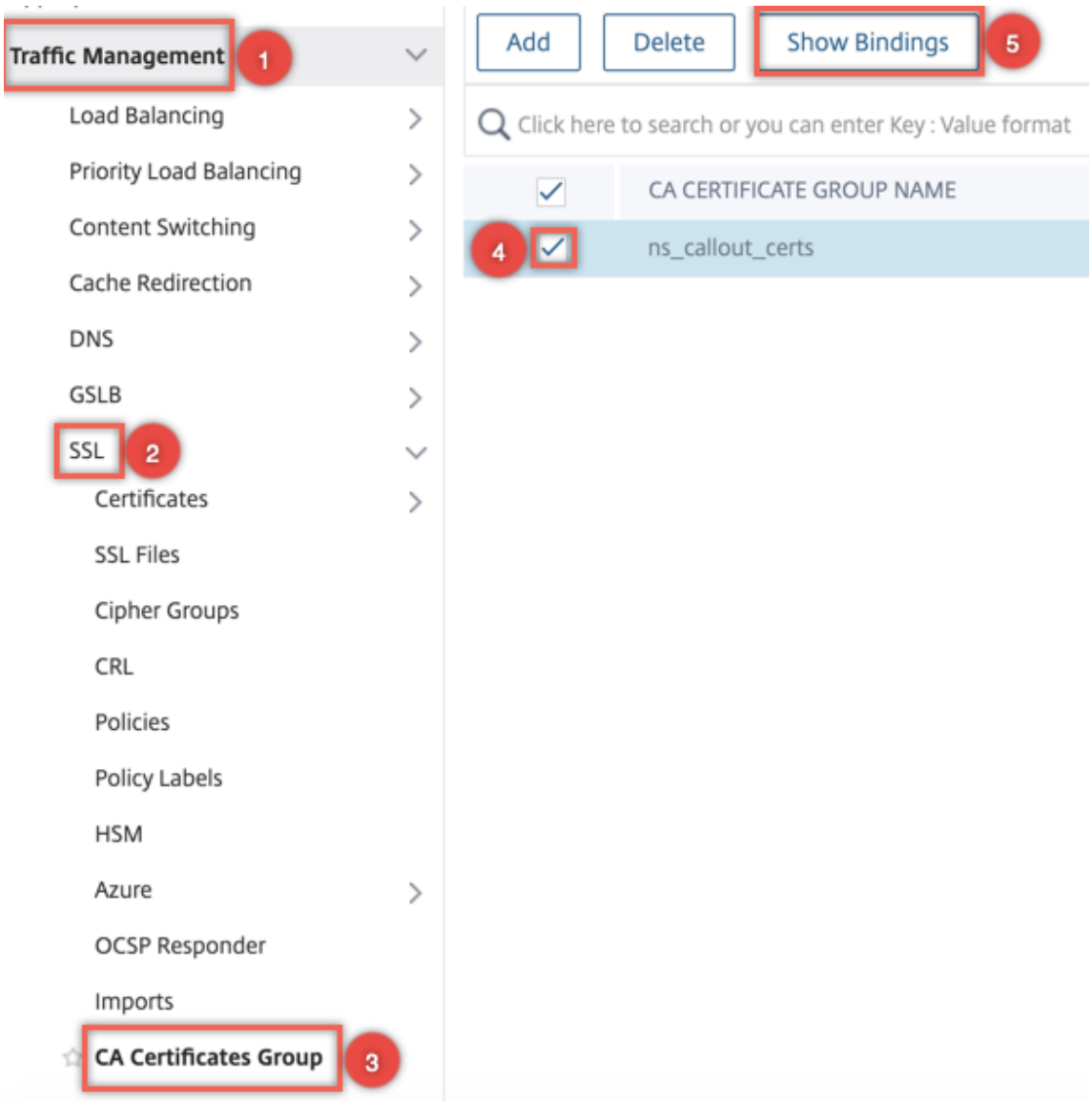


2. Entrez des valeurs pour les paramètres suivants :

   - Nom de la paire de clés de certificat
   - Nom du fichier de certificat



3. Cliquez sur **Installer**.
4. Accédez à **Gestion du trafic > SSL > Groupe de certificats CA**.
5. Sélectionnez **ns_callout_certs** et cliquez sur **Afficher les liaisons**.



6. Cliquez sur **Bind**.
7. Sélectionnez le certificat d'autorité de certification créé précédemment et cliquez sur **Sélectionner**.
8. Cliquez sur **Lier**, puis sur **Fermer**.

Configurer une application Azure

L'entité d'application Azure contient les informations d'identification requises pour s'authentifier auprès d'Azure Active Directory et obtenir le jeton d'accès. Autrement dit, pour obtenir l'accès d'autorisation aux ressources et aux API Key Vault, ajoutez l'ID d'application Azure, le mot de passe (mot de passe) et l'ID de locataire sur l'appliance ADC.
Lorsque vous configurez l'entité Application Azure à l'aide de l'interface de ligne de commande,

vous devez entrer le mot de passe. Si vous utilisez l'interface graphique, l'entité d'application Azure contient les informations d'identification requises pour s'authentifier auprès d'Azure Active Directory et obtenir le jeton d'accès.

Pour configurer une application Azure à l'aide de l'interface de ligne de commande

À partir de la version 13.0-61.x, un paramètre, VaultResource, est ajouté à la `add azure application` commande pour obtenir le domaine du groupe de ressources avant que le jeton d'accès ne soit accordé à l'application. Ce paramètre est ajouté car le nom de domaine peut être différent pour différentes régions. Par exemple, le domaine peut être `vault.azure.net` ou `vault.usgov.net`.

À l'invite de commandes, tapez :

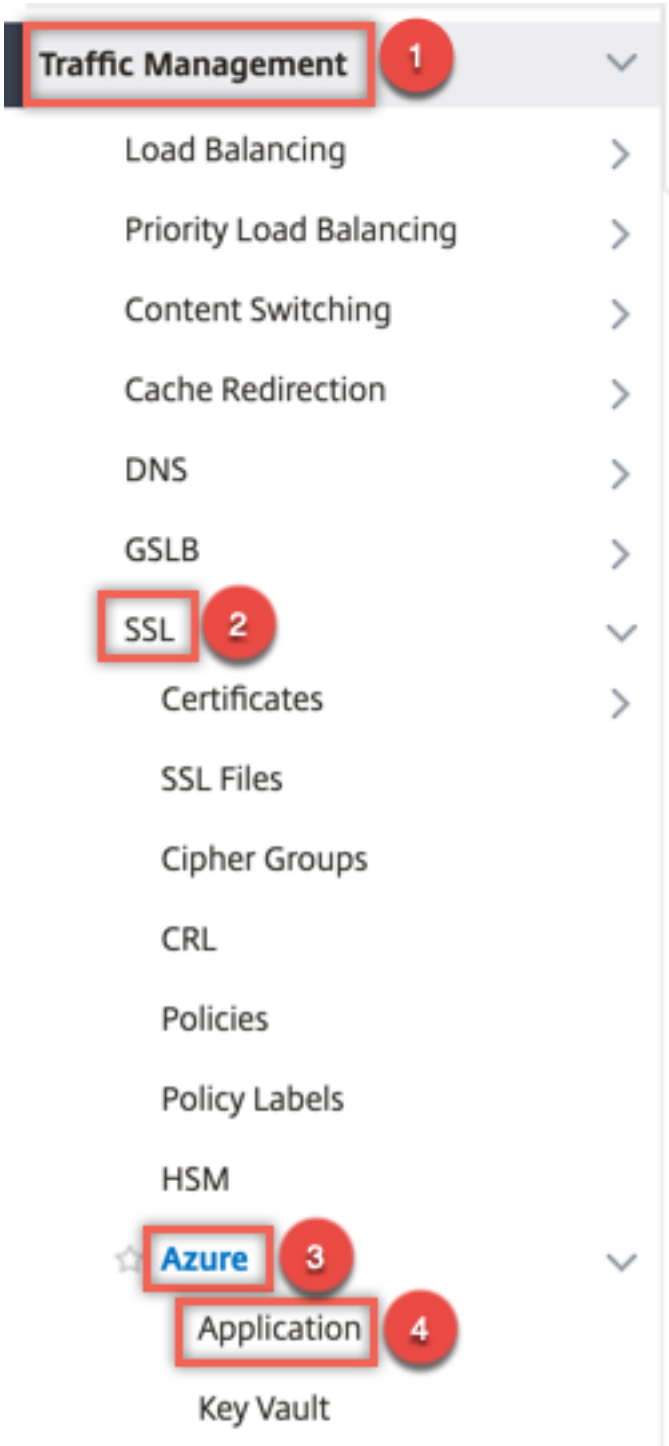
```
add azure application <name> -clientID <string> -clientSecret -tenantID
    <string> -vaultResource <string> [-tokenEndpoint <URL>]
show azure application
<!--NeedCopy-->
```

Exemple :

```
add azure application app10 -clientiD 12345t23aaa5 -clientsecret
   csHzOoEzmuY= -vaultResource example.vault.azure.net -tenantID 33583
   ee9ca5b
 Done
> sh azure application app10
1)  Name:  app10            ClientID:  12345t23aaa5
    TokenEndpoint:  "https://login.microsoftonline.com/33583ee9ca5b/"
    TenantID:  33583ee9ca5b  VaultResource:  example.vault.azure.net
 Done

<!--NeedCopy-->
```

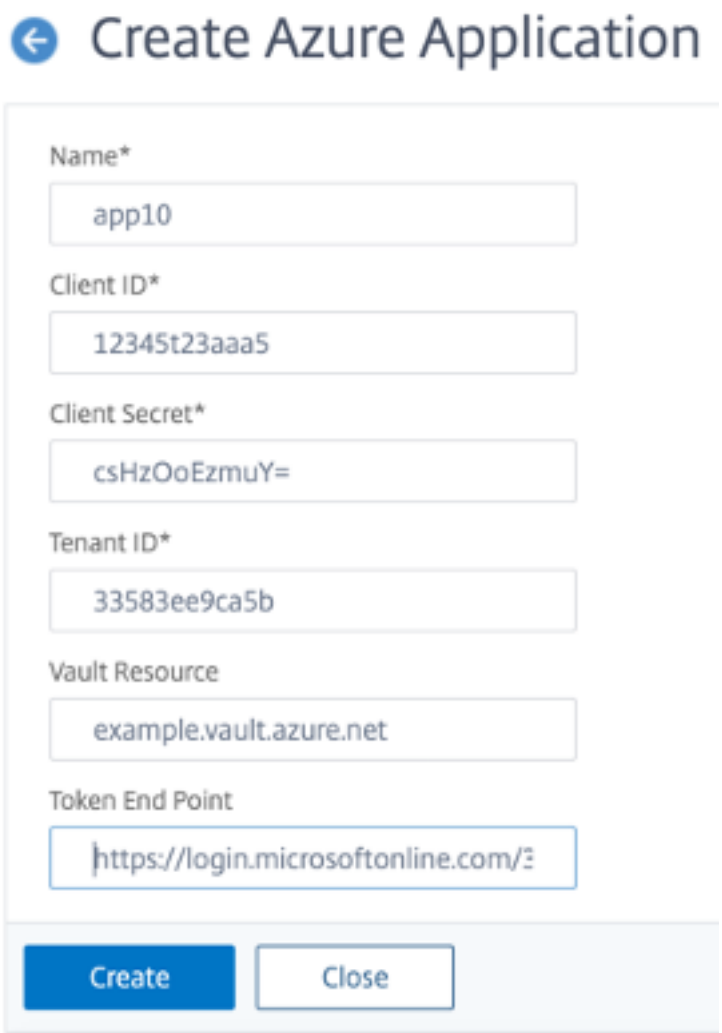
Pour configurer une application Azure à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Azure > Application**.



2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Entrez des valeurs pour les paramètres suivants :
   - Nom : nom de l'objet d'application sur l'appliance Citrix ADC.
   - ID client : ID d'application généré lorsqu'une application est créée dans Azure Active Directory à l'aide de l'interface de ligne de commande Azure ou du portail Azure (GUI).

- Client Secret : mot de passe de l'application configurée dans Azure Active Directory. Le mot de passe est spécifié dans l'interface de ligne de commande Azure ou généré dans le portail Azure (GUI).
- ID du locataire : ID du répertoire dans Azure Active Directory dans lequel l'application a été créée.
- Ressource Vault - Ressource de coffre-fort pour laquelle le jeton d'accès est accordé. Exemple `vault.azure.net`.
- Point de fin de jeton — URL à partir de laquelle le jeton d'accès peut être obtenu. Si le point d'extrémité du jeton n'est pas spécifié, la valeur par défaut est`https://login.microsoftonline.com/<tenant id>`.



Configurer Azure Key Vault

Créez un objet Azure Key Vault sur l'appliance ADC.

Pour configurer Azure Key Vault à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add azure keyVault <name> -azureVaultName <string> -azureApplication
       <string>
show azure keyvault
<!--NeedCopy-->
```

Exemple :

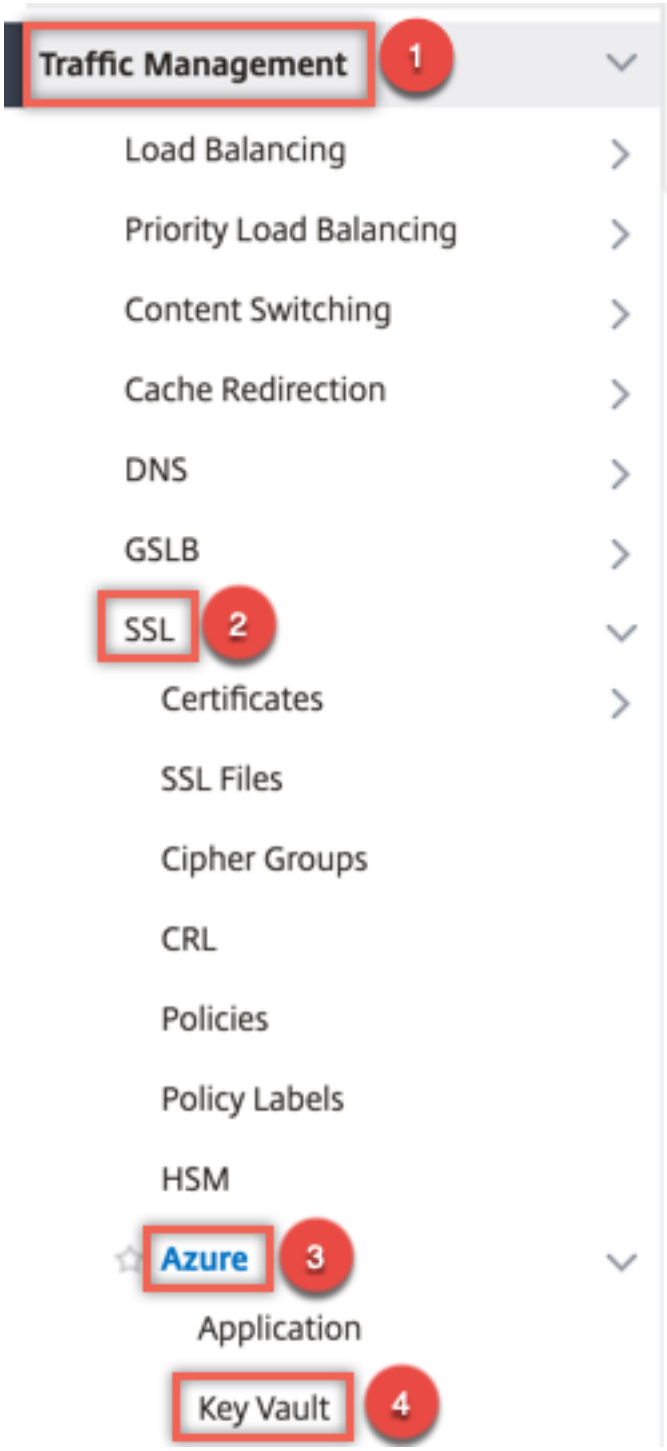
```
add azure keyvault kv1 -azureapplication app10 -azurevaultName pctest.
   vault.azure.net
> sh azure keyVault
1)  Name:  kv1               AzureVaultName:  pctest.vault.azure.net
  AzureApplication:  app10  State:  "Access token obtained"
 Done
<!--NeedCopy-->
```

Le tableau suivant répertorie les différentes valeurs que l'état d'Azure Key Vault peut prendre ainsi qu'une brève description de chaque état.

State	Description
`Created`	État initial de l'objet Key Vault. L'authentification n'a pas été tentée.
`Could not reach token end point`	Indique l'un des éléments suivants : serveur DNS non configuré, certificat émetteur non lié à un groupe de certificats d'autorité de certification ou problèmes de réseau.
`Authorization failed`	Informations d'identification de l'application incorrectes.
`Token parse error`	La réponse d'Azure Active Directory n'est pas dans le format attendu.
`Access token obtained`	Authentification réussie par Azure Active Directory.

Pour configurer Azure Key Vault à l'aide de l'interface graphique

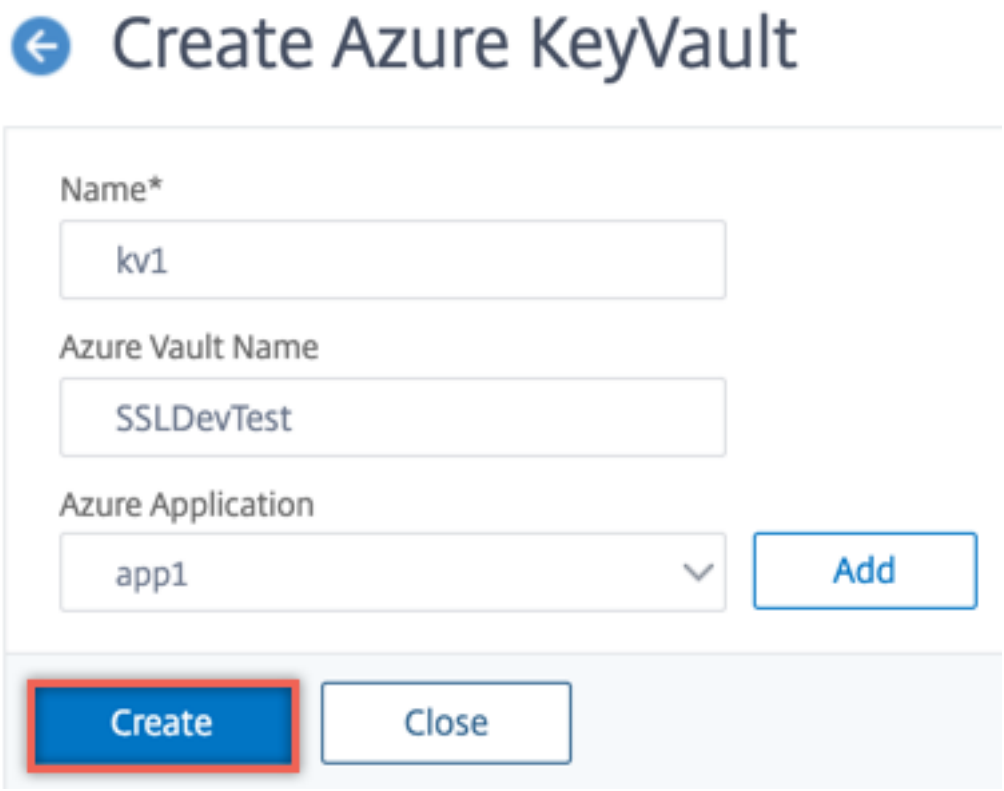
1. Accédez à **Gestion du trafic > SSL > Azure > Key Vault**.



2. Entrez des valeurs pour les paramètres suivants :

   - Nom - Nom du coffre à clés.
   - Azure Key Vault Name - Nom du coffre-fort de clés configuré dans le cloud Azure à l'aide de l'interface de ligne de commande Azure ou du portail Azure (GUI) avec un nom de domaine.
   - Nom de l'application Azure : nom de l'objet Application Azure créé sur l'appliance ADC.

L'objet Application Azure portant ce nom est utilisé pour l'authentification avec Azure Active Directory.



Ajouter une clé HSM

Le stockage de votre clé privée dans le HSM assure la conformité FIPS 140-2 niveau 2.

Pour ajouter une clé HSM à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ssl hsmKey <hsmKeyName> [-hsmType <hsmType>] [-key <string> |
       -serialNum <string>] {
 -password  }
  [-keystore <string>]
<!--NeedCopy-->
```

Exemple :

```
add ssl hsmKey h1 -keystore kv1 -key san15key -hsmType KEYVAULT


> sh ssl hsmKey h1
```



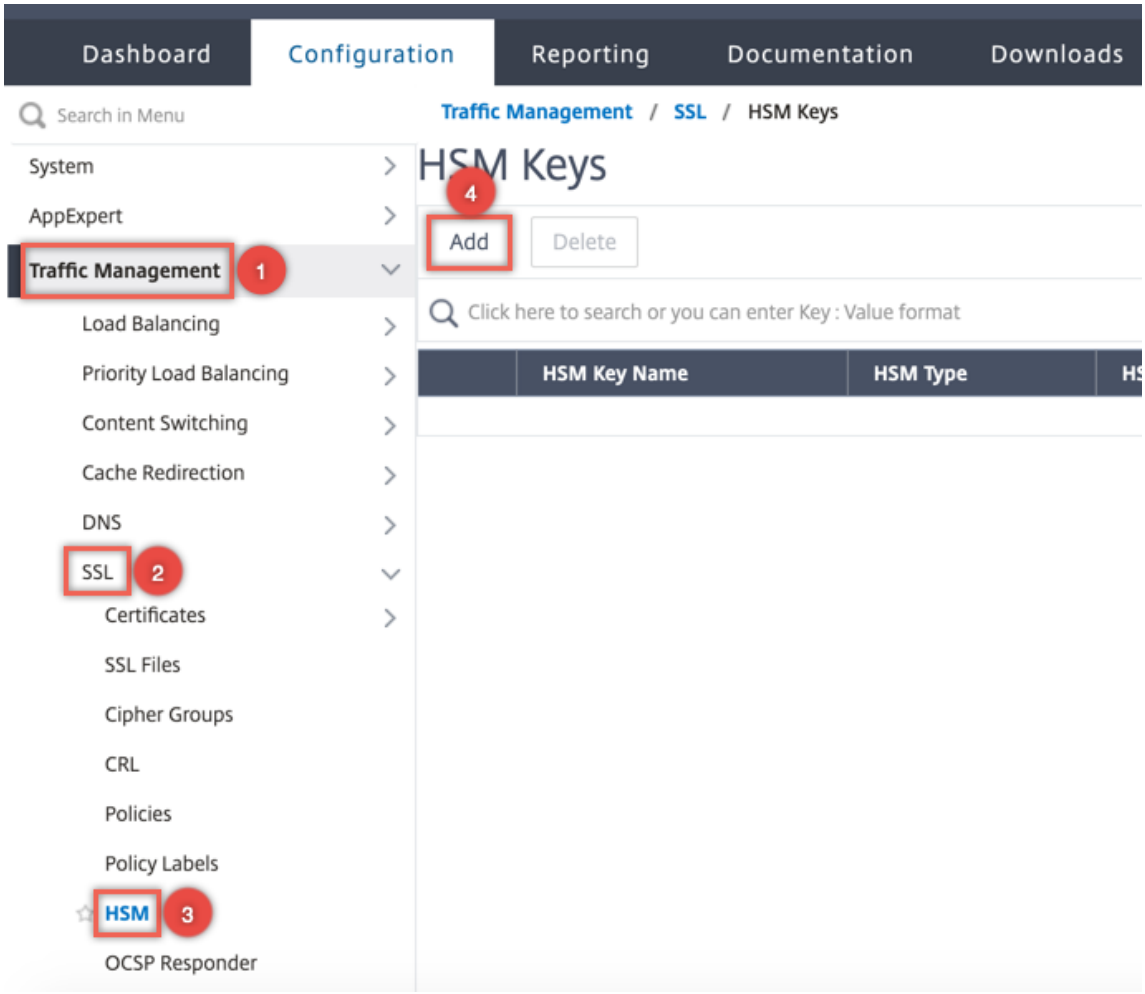
```
5      HSM Key Name: h1        Type: KEYVAULT
6      Key: san15key
7      Key store: kv1
8      State:  “Created”
9   Done
10 <!--NeedCopy-->
```

Le tableau suivant répertorie les différentes valeurs que l'état d'une clé HSM peut prendre avec une brève description de chaque état.

State	Description
Created	La clé HSM est ajoutée sur l'appliance ADC. Une opération clé n'est pas encore tentée.
Jeton d'accès non disponible	Le jeton d'accès n'est pas disponible lors de la tentative d'opération de clé.
Non autorisé	L'application Azure configurée n'a pas l'autorisation d'effectuer l'opération de clé.
N'existe pas	La clé n'existe pas dans Azure Key Vault.
Injoignable	L'hôte Key Vault n'est pas accessible sur le réseau.
Marqué down	La clé HSM est marquée comme DOWN sur l'appliance ADC en raison d'erreurs de seuil lors du fonctionnement de la clé.
Opérations clés réussies	Réponse réussie reçue du Key Vault pour l'opération des clés.
Échec des opérations de clé	Réponse en cas de défaillance reçue de Key Vault pour le fonctionnement de la clé.
Opération de clé étranglée	La demande d'opération de clé est étranglée par Key Vault.

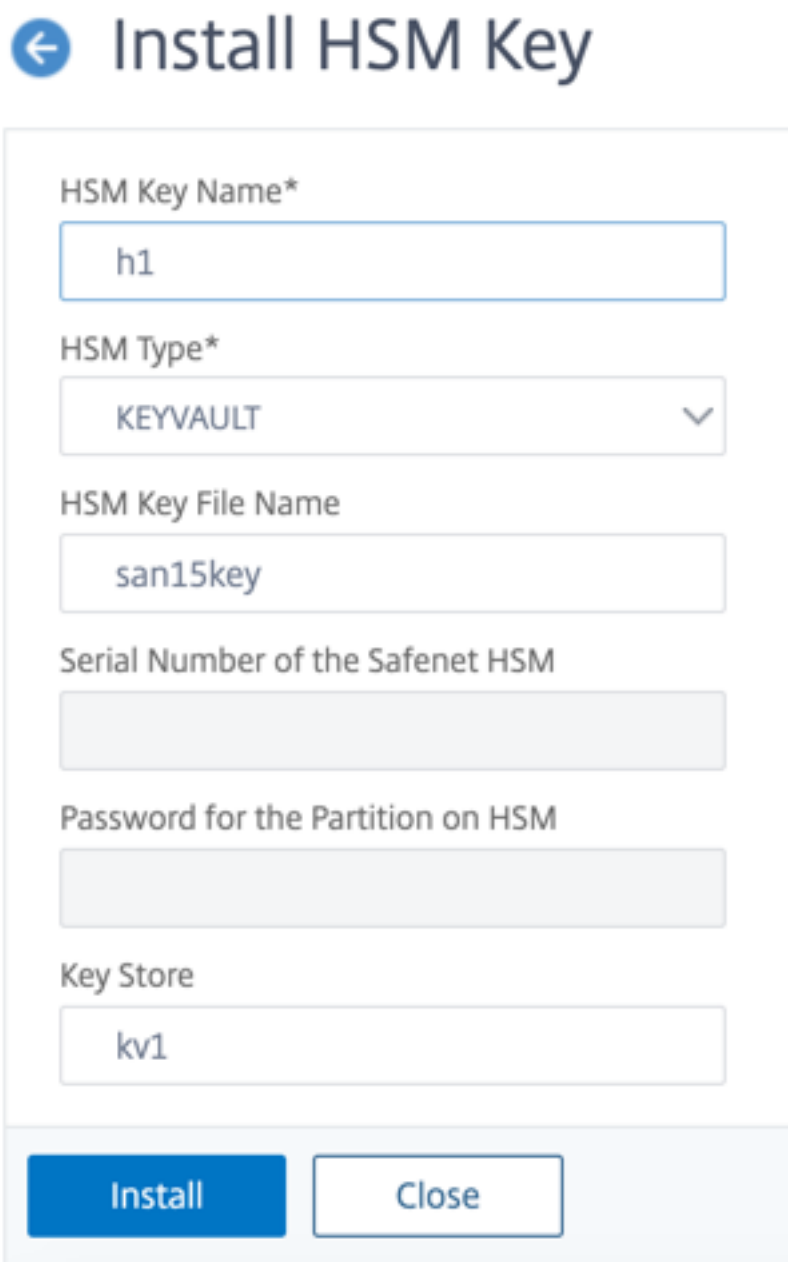
Pour ajouter une clé HSM à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > HSM**.



2. Entrez des valeurs pour les paramètres suivants.

   - Nom de la clé HSM - Nom de la clé.
   - Type HSM - Type de HSM.
   - Magasin de clés - Nom de l'objet de magasin de clés représentant HSM où la clé est stockée. Par exemple, nom de l'objet Key Vault ou de l'objet d'authentification Azure Key Vault. S'applique uniquement au`KEYVAULT` type HSM.



3. Cliquez sur **Ajouter**

Ajouter une paire de clés de certificat

Ajoutez une paire de clés de certificat à l'aide de la clé HSM créée précédemment.

Pour ajouter une paire de clés de certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

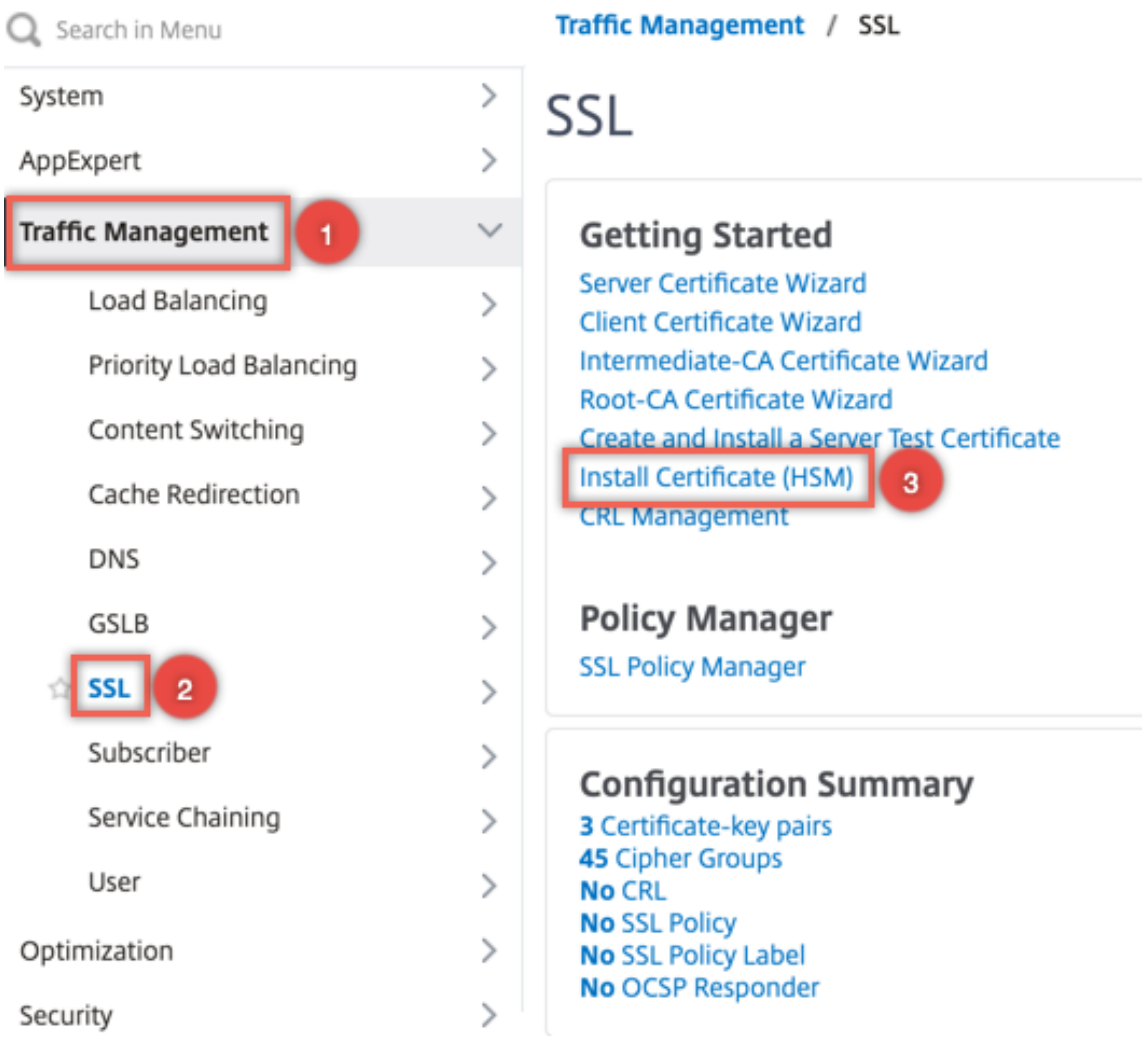

```
add ssl certKey <certkeyName> (-cert <string> [-password]) -hsmKey <
    string>]
show ssl certkey
<!--NeedCopy-->
```

Exemple :

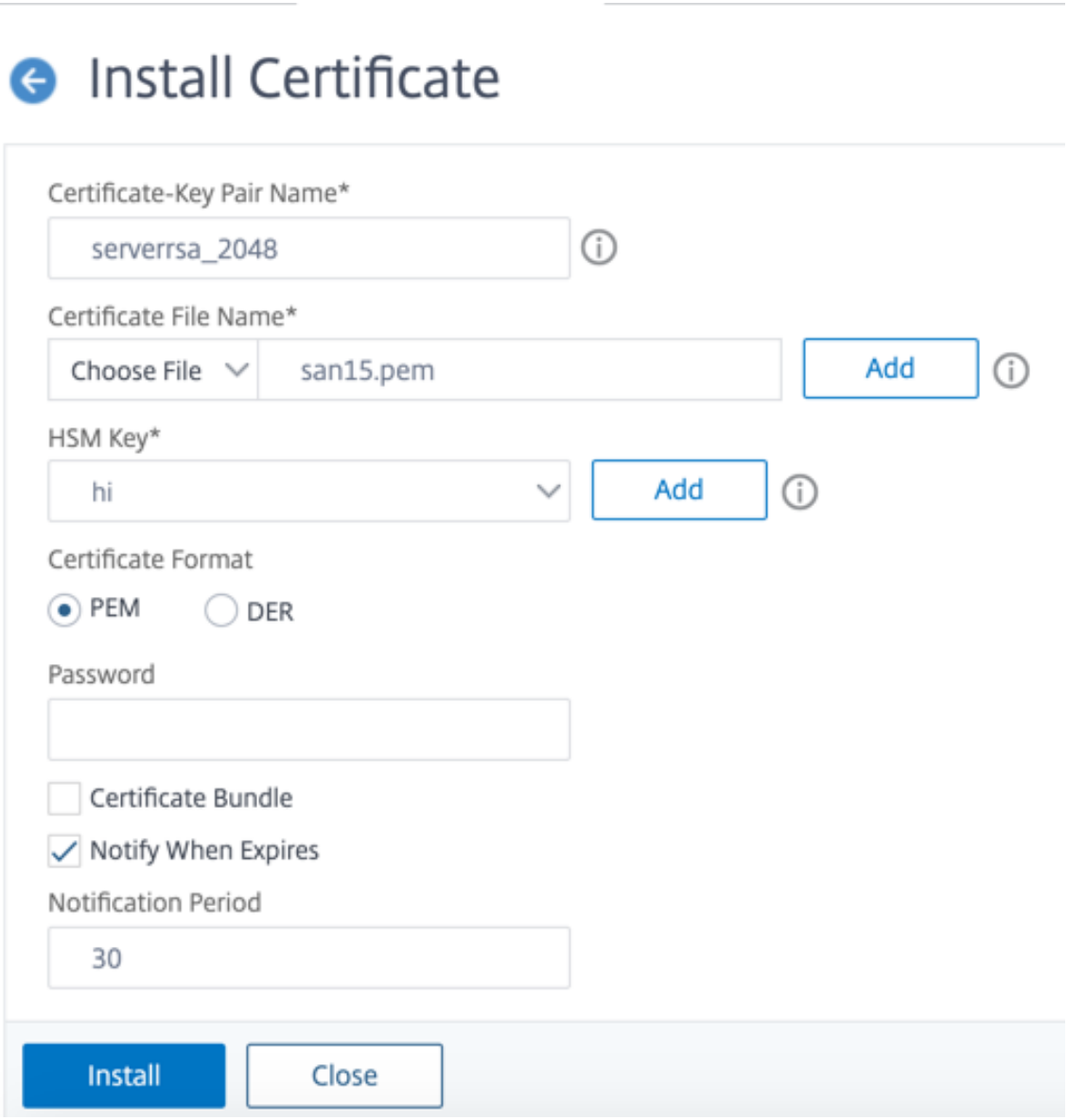
```
add ssl certKey serverrsa_2048 -cert /nsconfig/ssl/san_certs/san15.pem
    -hsmKey h1
> sh ssl certkey serverrsa_2048
    Name: serverrsa_2048        Status: Valid,   Days to expiration
        :9483
    Version: 3
    Serial Number: F5CFF9EF1E246022
    Signature Algorithm: sha256WithRSAEncryption
    Issuer:  C=in,O=citrix,CN=ca
    Validity
        Not Before: Mar 20 05:42:57 2015 GMT
        Not After : Mar 12 05:42:57 2045 GMT
    Certificate Type:   "Server Certificate"
    Subject:  C=in,O=citrix
    Public Key Algorithm: rsaEncryption
    Public Key size: 2048
    Ocsp Response Status: NONE
 Done
<!--NeedCopy-->
```

Pour ajouter une paire de clés de certificat à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Installer le certificat (HSM)**.



2. Entrez des valeurs pour les paramètres suivants :
   - Nom de la paire de clés de certificat
   - Nom du fichier de certificat
   - Clé HSM



3. Cliquez sur **Installer**.

Liez la paire de clés de certificat à un serveur virtuel

Le certificat utilisé pour le traitement des transactions SSL doit être lié au serveur virtuel qui reçoit les données SSL.

Pour lier la paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
show ssl vserver <vServerName>
```



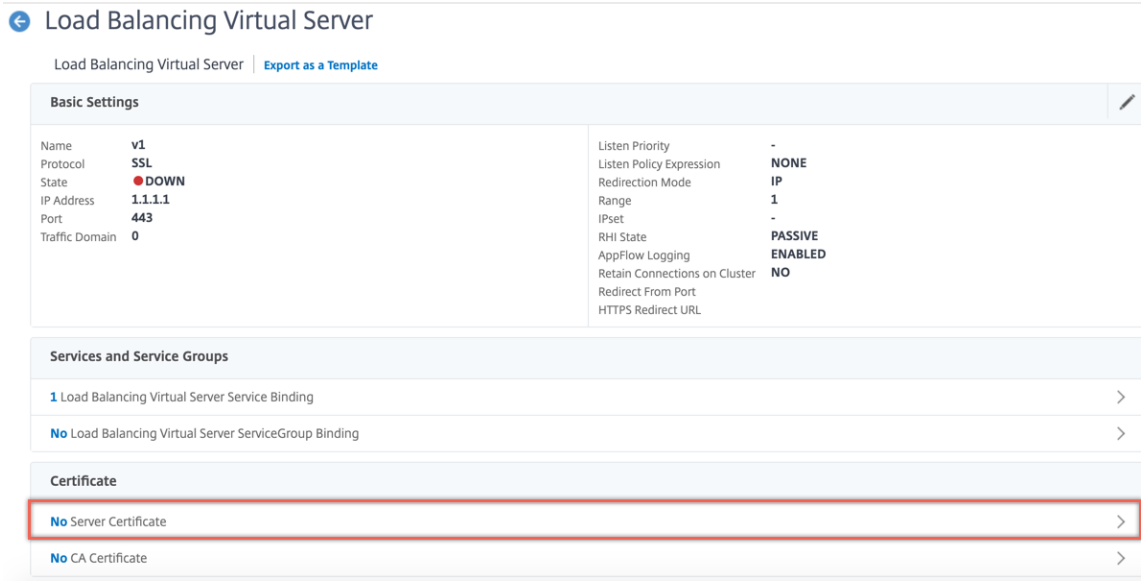
```
<!--NeedCopy-->
```

Exemple :

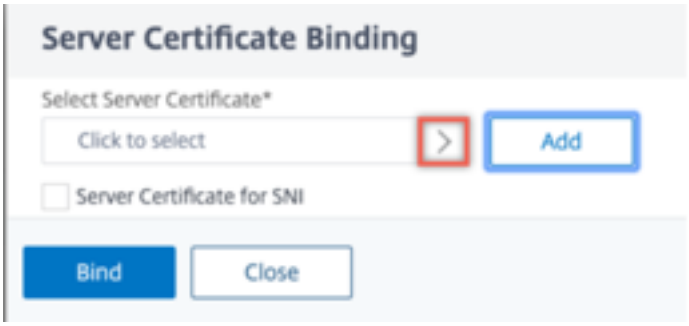
```
bind ssl vserver v1 -certkeyName serverrsa_2048

sh ssl vserver v1

    Advanced SSL configuration for VServer v1:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED      Refresh Count: 0
    Session Reuse: ENABLED      Timeout: 120 seconds
    Cipher Redirect: DISABLED
    ClearText Port: 0
    Client Auth: DISABLED
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: DISABLED
    OCSP Stapling: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    HSTS Preload: NO
    SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Push Encryption Trigger: Always
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1

    ECC Curve: P_256, P_384, P_224, P_521

1)  CertKey Name: serverrsa_2048    Server Certificate



1)  Cipher Name: DEFAULT
    Description: Default cipher list with encryption strength >= 128bit
 Done
<!--NeedCopy-->
```

Pour lier une paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface graphique

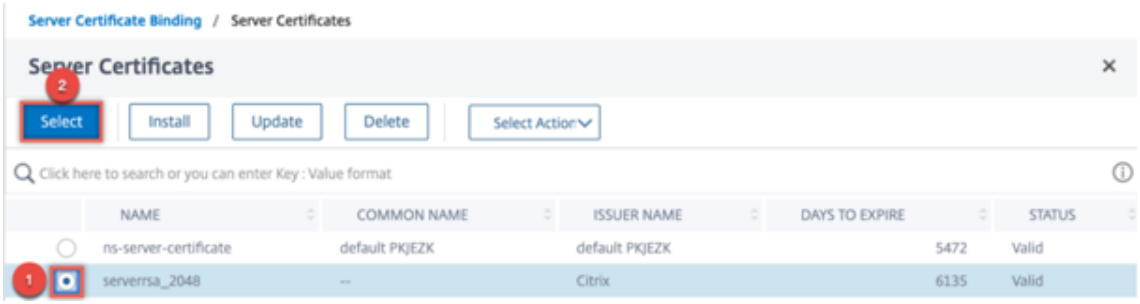
1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et ouvrez un serveur virtuel SSL. Cliquez dans la section Certificat.



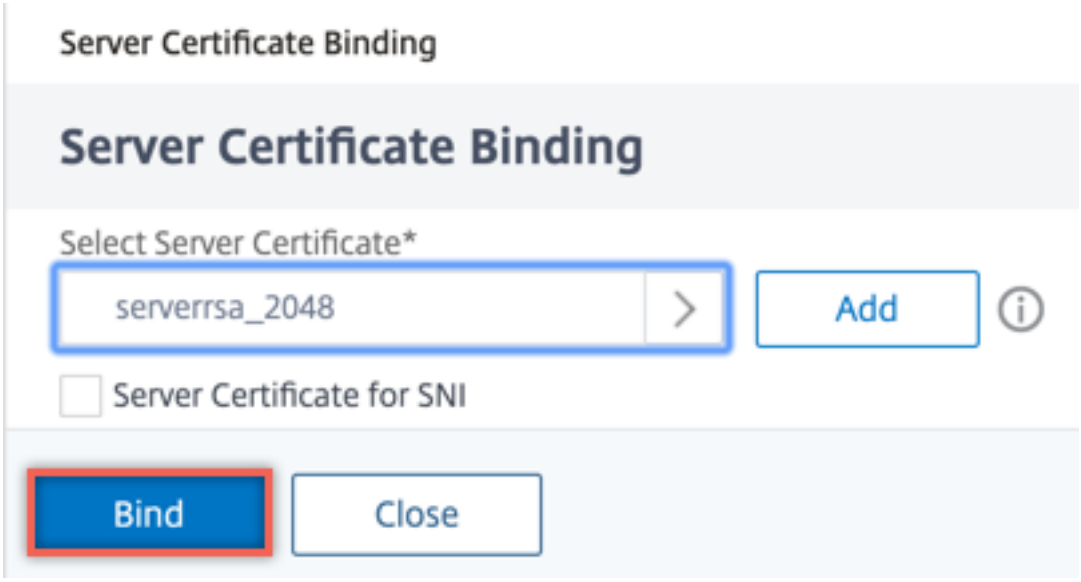
2. Cliquez sur la flèche pour sélectionner la paire de clés de certificat.



3. Sélectionnez la paire de clés de certificat dans la liste.



4. Liez la paire de clés de certificat au serveur virtuel.



Limitations

- Le nombre d'appels simultanés vers Azure Key Vault pour les opérations clés est limité. Les performances de l'appliance ADC dépendent des limites de Key Vault. Pour plus d'informations, reportez-vous à la documentation de Microsoft Azure Key Vault.
- Les clés EC ne sont pas prises en charge.
- Les protocoles EDT et DTLS ne sont pas pris en charge.
- Les appareils ADC dotés de puces Intel Coleto SSL ne sont pas pris en charge.
- Les partitions de clustering et d'administration ne sont pas prises en charge.
- Vous ne pouvez pas mettre à jour l'entité Application Azure, l'objet Azure Key Vault et la paire de clés de certificat HSM après les avoir ajoutés à l'appliance ADC.

Questions fréquentes

Lorsqu'elles sont intégrées à Azure Key Vault, les clés privées sont-elles stockées dans la mémoire de l'appliance ADC ?

Non, les clés privées ne sont pas stockées dans la mémoire de l'appliance ADC. Pour chaque transaction SSL, l'appliance envoie une demande à Key Vault.

L'intégration FIPS 140-2 niveau 2 est-elle conforme ?

Oui, la solution intégrée fournit la prise en charge FIPS 140-2 Niveau 2.

Quels types de clés sont pris en charge ?

Seuls les types de clés RSA sont pris en charge.

Quelles tailles de clés sont prises en charge ?

Les clés RSA 1024 bits, 2048 bits et 4096 bits sont prises en charge.

Quels chiffrements sont pris en charge ?

Tous les chiffrements pris en charge par l'appliance ADC, y compris les chiffrements TLSv1.3 avec ECDHE et SHA256, sont pris en charge.

Les transactions sont-elles enregistrées ?

L'appliance ADC enregistre chaque transaction qu'elle effectue avec Key Vault. Les détails tels que l'heure, l'adresse IP du coffre-fort, le port, le succès ou l'échec de la connexion et les erreurs sont consignés.
Voici un exemple de sortie de journal SSL.

```
Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
      0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 896 0 :
    Backend SPCBId 30894 - ServerIP 104.211.224.186 - ServerPort 443
     - ProtocolVersion TLSv1.2 - CipherSuite "ECDHE-RSA-AES256-GCM-
    SHA384 TLSv1.2 Non-Export 256-bit" - Session New -
    SERVER_AUTHENTICATED -SerialNumber "200005
    A75B04365827852D630000000005A75B" - SignatureAlgorithm "
    sha256WithRSAEncryption" - ValidFrom "Mar 17 03:28:42 2019 GMT"
    - ValidTo "Mar 17 03:28:42 2021 GMT" - HandshakeTime 40 ms
Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
      0-PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 897 0 :
    SPCBId 30894 - IssuerName " C=US,ST=Washington,L=Redmond,O=
    Microsoft Corporation,OU=Microsoft IT,CN=Microsoft IT TLS CA 2"
Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
      0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 898 0 :
    SPCBId 30894 - SubjectName " CN=vault.azure.net"
<!--NeedCopy-->
```

Résolution des problèmes

August 20, 2021

Si la fonctionnalité SSL ne fonctionne pas comme prévu après la configuration, vous pouvez utiliser certains outils courants pour accéder aux ressources Citrix ADC et diagnostiquer le problème.

Ressources pour le dépannage

Pour obtenir de meilleurs résultats, utilisez les ressources suivantes pour résoudre un problème SSL sur une appliance Citrix ADC :

- Le fichier ns.log correspondant
- Le dernier fichier ns.conf
- Le fichier de messages
- Le fichier `newnslog` pertinent
- Fichiers de suivi
- Une copie des fichiers de certificat, si possible
- Une copie du fichier clé, si possible
- Le message d'erreur, le cas échéant

En plus de ces ressources, vous pouvez utiliser l'application Wireshark personnalisée pour les fichiers de trace Citrix ADC pour accélérer le dépannage.

Résolution des problèmes SSL

Pour résoudre un problème SSL, procédez comme suit :

- Vérifiez que l'appliance Citrix ADC est sous licence pour le déchargement SSL et l'équilibrage de charge.
- Vérifiez que les fonctions de déchargement SSL et d'équilibrage de charge sont activées sur l'appliance.
- Vérifiez que l'état du serveur virtuel SSL n'est pas affiché comme DOWN.
- Vérifiez que l'état du service lié au serveur virtuel n'est pas affiché comme étant DOWN.
- Vérifiez qu'un certificat valide est lié au serveur virtuel.
- Vérifiez que le service utilise un port approprié, de préférence le port 443.

Décryptage du trafic TLS1.3 à partir de la trace de paquets

Pour dépanner les protocoles qui s'exécutent sur TLS1.3, vous devez d'abord déchiffrer le trafic TLS1.3. Pour décrypter TLS 1.3 dans Wireshark, les secrets doivent être exportés dans le format du journal des clés `NSS`. Pour plus d'informations sur le format du journal de clés, voir Format du journal de clés NSS.

Pour plus d'informations sur la façon de capturer une trace de paquets, voir Capture des clés de session SSL pendant un suivi.

Remarque : Citrix ADC enregistre automatiquement les secrets de chaque connexion dans le format approprié pour la version du protocole TLS/SSL utilisée.

L'actualisation de la liste de révocation de révocation de révocation ne se produit pas sur le nœud secondaire dans une configuration HA

L'actualisation ne se produit pas car le serveur CRL est accessible uniquement au nœud principal via un réseau privé.

Solution : ajoutez un service sur le nœud principal avec l'adresse IP du serveur CRL. Ce service agit comme un proxy pour le serveur CRL. Lorsque la configuration est synchronisée entre les nœuds, l'actualisation des listes de révocation des droits de révocation fonctionne pour les nœuds principaux et secondaires via le service configuré sur le nœud principal.

FAQ SSL

September 8, 2021

Questions de base

L'accès HTTPS à l'interface graphique échoue sur une instance VPX. Comment puis-je y accéder ?

Une paire de clés de certificat est nécessaire pour accéder au protocole HTTPS à l'interface graphique. Sur une appliance Citrix ADC, une paire de clés de certificat est automatiquement liée aux services internes. Sur une appliance MPX ou SDX, la taille de clé par défaut est de 1024 octets et sur une instance VPX, la taille de clé par défaut est de 512 octets. Cependant, la plupart des navigateurs n'acceptent pas aujourd'hui une clé inférieure à 1024 octets. Par conséquent, l'accès HTTPS à l'utilitaire de configuration VPX est bloqué.

Citrix recommande d'installer une paire de clés de certificat d'au moins 1024 octets et de la lier au service interne pour accéder HTTPS à l'utilitaire de configuration. Vous pouvez également mettre à jour le `ns-server-certificate` jusqu'à 1024 octets. Vous pouvez utiliser l'accès HTTP à l'utilitaire de configuration ou à l'interface de ligne de commande pour installer le certificat.

Si j'ajoute une licence à une appliance MPX, la liaison de la paire de clés de certificat est perdue. Comment puis-je résoudre ce problème ?

Si aucune licence n'est présente sur une appliance MPX au démarrage, et que vous ajoutez une licence plus tard et que vous redémarrez l'appliance, vous risquez de perdre la liaison du certificat. Réinstallez

le certificat et liez-le au service interne

Citrix recommande d'installer une licence appropriée avant de démarrer l'appliance.

Quelles sont les différentes étapes de la configuration d'un canal sécurisé pour une transaction SSL ?

La configuration d'un canal sécurisé pour une transaction SSL implique les étapes suivantes :

1. Le client envoie une demande HTTPS pour un canal sécurisé au serveur.
2. Après avoir sélectionné le protocole et le chiffrement, le serveur envoie son certificat au client.
3. Le client vérifie l'authenticité du certificat de serveur.
4. Si l'une des vérifications échoue, le client affiche les commentaires correspondants.
5. Si les vérifications réussissent ou que le client décide de continuer même en cas d'échec d'une vérification, le client crée une clé temporaire et jetable. Cette clé est appelée *secret pré-maître* et le client crypte cette clé à l'aide de la clé publique du certificat du serveur.
6. Le serveur, après avoir reçu le secret pré-maître, le déchiffre à l'aide de la clé privée du serveur et génère les clés de session. Le client génère également les clés de session à partir du secret pré-maître. Ainsi, le client et le serveur disposent désormais d'une clé de session commune, utilisée pour le chiffrement et le déchiffrement des données d'application.

Je comprends que SSL est un processus à forte intensité de processeur. Quel est le coût du processeur associé au processus SSL ?

Les deux étapes suivantes sont associées au processus SSL :

- La poignée de main initiale et la configuration sécurisée des canaux à l'aide de la technologie de clé publique et privée.
- Cryptage des données en masse à l'aide de la technologie de clé symétrique.

Les deux étapes précédentes peuvent affecter les performances du serveur, et elles nécessitent un traitement intensif du processeur pour les raisons suivantes :

1. La prise de contact initiale implique la cryptographie à clé public-privée, qui nécessite beaucoup d'UC en raison des grandes tailles de clés (1024 bits, 2048 bits, 4096 bits).
2. Le chiffrement/déchiffrement des données est également coûteux sur le plan informatique, en fonction de la quantité de données qui doivent être chiffrées ou déchiffrées.

Quelles sont les différentes entités d'une configuration SSL ?

Une configuration SSL comporte les entités suivantes :

- Écran Server certificate
- Certificat d'autorité de certification (CA)
- Suite de chiffrement qui spécifie les protocoles pour les tâches suivantes :
  - Échange de clés initial
  - Authentification des serveurs et des clients
  - Algorithme de chiffrement en masse
  - L'authentification des messages
- Authentification client
- CRL
- Outil de génération de clés de certificat SSL qui vous permet de créer les fichiers suivants :
  - Demande de certificat
  - Certificat auto-signé
  - Clés RSA
  - Paramètres DH

Je souhaite utiliser la fonction de déchargement SSL de l'appliance Citrix ADC. Quelles sont les différentes options de réception d'un certificat SSL ?

Vous devez recevoir un certificat SSL avant de pouvoir configurer la configuration SSL sur l'appliance Citrix ADC. Vous pouvez utiliser l'une des méthodes suivantes pour recevoir un certificat SSL :

- Demandez un certificat à une autorité de certification autorisée (CA).
- Utilisez le certificat de serveur existant.
- Créez une paire de clés de certificat sur l'appliance Citrix ADC.

Remarque : Ce certificat est un certificat de test signé par l'autorité de certification racine de test générée par l'appliance Citrix ADC. Les certificats de test signés par la Root-CA de test ne sont pas acceptés par les navigateurs. Le navigateur envoie un message d'avertissement indiquant que le certificat du serveur ne peut pas être authentifié.

- À des fins autres que des tests, vous devez fournir un certificat d'autorité de certification et une clé d'autorité de certification valides pour signer le certificat du serveur.

Quelle est la configuration minimale requise pour une configuration SSL ?

La configuration minimale requise pour configurer une configuration SSL est la suivante :

- Obtenez les certificats et les clés.
- Créez un serveur virtuel SSL d'équilibrage de charge.
- Liez les services HTTP ou SSL au serveur virtuel SSL.
- Liez une paire de clés de certificat au serveur virtuel SSL.

Quelles sont les limites des différents composants de SSL ?

Les composants SSL présentent les limites suivantes :

- Taille des bits des certificats SSL : 4096.
- Nombre de certificats SSL : dépend de la mémoire disponible sur l'appliance.
- Nombre maximal de certificats SSL CA intermédiaires liés : 9 par chaîne.
- Révocations de CRL : dépend de la mémoire disponible sur l'appliance.

Quelles sont les différentes étapes du chiffrement des données de bout en bout sur une appliance Citrix ADC ?

Les étapes impliquées dans le processus de chiffrement côté serveur sur une appliance Citrix ADC sont les suivantes :

1. Le client se connecte au VIP SSL configuré sur l'appliance Citrix ADC sur le site sécurisé.
2. Après avoir reçu la demande sécurisée, l'appliance déchiffre la demande et applique des techniques de commutation de contenu de couche 4 à 7 et des stratégies d'équilibrage de charge. Il sélectionne ensuite le meilleur serveur Web back-end disponible pour la demande.
3. L'appliance Citrix ADC crée une session SSL avec le serveur sélectionné.
4. Après avoir établi la session SSL, l'appliance chiffre la demande du client et l'envoie au serveur Web à l'aide de la session SSL sécurisée.
5. Lorsque la solution matérielle-logicielle reçoit la réponse chiffrée du serveur, elle déchiffre et rechiffre les données. Il envoie ensuite les données au client à l'aide de la session SSL côté client.

La technique de multiplexage de l'appliance Citrix ADC permet à l'appliance de réutiliser les sessions SSL établies avec les serveurs Web. Par conséquent, la solution matérielle-logicielle évite l'échange de clés intensif du processeur, connu sous le nom de *poignée de main complète*. Ce processus réduit le nombre global de sessions SSL sur le serveur et assure la sécurité de bout en bout.

Certificats et clés

Puis-je placer le certificat et les fichiers clés à n'importe quel endroit ? Existe-t-il un emplacement recommandé pour stocker ces fichiers ?

Vous pouvez stocker le certificat et les fichiers de clés sur l'appliance Citrix ADC ou sur un ordinateur local. Toutefois, Citrix recommande de stocker le certificat et les fichiers de clés dans le `/nsconfig/ssl` répertoire de l'appliance Citrix ADC. Le `/etc` répertoire existe dans la mémoire flash de l'appliance Citrix ADC. Cette action assure la portabilité et facilite la sauvegarde et la restauration des fichiers de certificats sur l'appliance.

Remarque : Assurez-vous que le certificat et les fichiers clés sont stockés dans le même répertoire.

Quelle est la taille maximale de la clé de certificat prise en charge sur l'appliance Citrix ADC ?

Une appliance Citrix ADC exécutant une version logicielle antérieure à la version 9.0 prend en charge une taille maximale de clé de certificat de 2048 bits. Les versions 9.0 et ultérieures prennent en charge une taille maximale de clé de certificat de 4096 bits. Cette limite s'applique aux certificats RSA.

Une appliance MPX prend en charge les certificats de 512 bits jusqu'aux tailles suivantes :

- Certificat de serveur 4096 bits sur le serveur virtuel
- Certificat client 4096 bits sur le service
- Certificat d'autorité de certification 4096 bits (inclut les certificats intermédiaires et racine)
- Certificat 4096 bits sur le serveur principal
- Certificat client 4096 bits (si l'authentification client est activée sur le serveur virtuel)

Une appliance virtuelle prend en charge les certificats de 512 bits jusqu'aux tailles suivantes :

- Certificat de serveur 4096 bits sur le serveur virtuel
- Certificat client 4096 bits sur le service
- Certificat d'autorité de certification 4096 bits (inclut les certificats intermédiaires et racine)
- Certificat 4096 bits sur le serveur principal de la version 12.0-56.x. Les anciennes versions prennent en charge les certificats 2048 bits.
- Certificat client 2048 bits (si l'authentification client est activée sur le serveur virtuel) de la version 12.0-56.x.

Quelle est la taille maximale du paramètre DH pris en charge sur l'appliance Citrix ADC ?

L'appliance Citrix ADC prend en charge un paramètre DH de 2048 bits maximum.

Quelle est la longueur maximale de la chaîne de certificats, c'est-à-dire le nombre maximal de certificats dans une chaîne, pris en charge sur une appliance Citrix ADC ?

Une appliance Citrix ADC peut envoyer un maximum de 10 certificats dans une chaîne lors de l'envoi d'un message de certificat de serveur. Une chaîne de longueur maximale comprend le certificat de serveur et neuf certificats d'autorité de certification intermédiaires.

Quels sont les différents formats de certificats et de clés pris en charge sur l'appliance Citrix ADC ?

L'appliance Citrix ADC prend en charge les formats de certificats et de clés suivants :

- Messagerie améliorée de confidentialité (PEM)
- Règle de codage distinguée (DER)

Le nombre de certificats et de clés que je peux installer sur l'appliance Citrix ADC est-il limité ?

Non. Le nombre de certificats et de clés pouvant être installés est limité uniquement par la mémoire disponible sur l'appliance Citrix ADC.

J'ai enregistré le certificat et les fichiers clés sur l'ordinateur local. Je souhaite transférer ces fichiers vers l'appliance Citrix ADC à l'aide du protocole FTP. Existe-t-il un mode privilégié pour transférer ces fichiers vers l'appliance Citrix ADC ?

Oui. Si vous utilisez le protocole FTP, vous devez utiliser le mode binaire pour transférer le certificat et les fichiers clés vers l'appliance Citrix ADC.

Remarque : Par défaut, FTP est désactivé. Citrix recommande d'utiliser le protocole SCP pour transférer des fichiers de certificats et de clés. L'utilitaire de configuration utilise implicitement SCP pour se connecter à l'appliance.

Quel est le chemin d'accès au répertoire par défaut du certificat et de la clé ?

Le chemin d'accès au répertoire par défaut du certificat et de la clé est '/nsconfig/ssl'.

Lorsque vous ajoutez un certificat et une paire de clés, que se passe-t-il si je ne spécifie pas de chemin absolu vers les fichiers de certificat et de clé ?

Lorsque vous ajoutez une paire de clés de certificat, spécifiez un chemin absolu vers le certificat et les fichiers de clés. Si vous ne le spécifiez pas, l'appliance ADC recherche ces fichiers dans le répertoire par défaut et tente de les charger dans le noyau. Le répertoire par défaut est `/nsconfig/ssl`. Par exemple, si les fichiers cert1024.pem et rsa1024.pem sont disponibles dans le `/nsconfig/ssl` répertoire de l'appliance, les deux commandes suivantes réussissent :

```
1 add ssl certKey cert1 -cert cert1204.pem -key rsa1024.pem
2 <!--NeedCopy-->
```

```
1 add ssl certKey cert1 -cert /nsconfig/ssl/cert1204.pem -key /nsconfig/
     ssl/rsa1024.pem
2 <!--NeedCopy-->
```


J'ai configuré une configuration haute disponibilité. Je souhaite implémenter la fonctionnalité SSL lors de la configuration. Comment dois-je gérer le certificat et les fichiers clés dans une configuration haute disponibilité ?

Dans une configuration haute disponibilité, vous devez stocker les fichiers de certificat et de clé sur l'appliance Citrix ADC principale et secondaire. Le chemin d'accès au répertoire du certificat et des fichiers de clé doit être le même sur les deux appliances avant d'ajouter une paire de clés de certificat SSL sur l'appliance principale.

Chipher NShield® HSM

Lors de l'intégration avec NCipher NShield® HSM, devons-nous garder à l'esprit une configuration spécifique lors de l'ajout de l'appliance Citrix ADC à HA ?

Configurez les mêmes périphériques NCipher sur les deux nœuds de HA. Les commandes de configuration NCipher ne sont pas synchronisées dans HA. Pour plus d'informations sur les conditions préalables à NCipher NShield® HSM, consultez Prérequis.

Doit-on intégrer individuellement les deux appliances avec NCipher NShield® HSM et RFS ? Doit-on effectuer cette action avant ou après la configuration HA ?

Vous pouvez terminer l'intégration avant ou après la configuration HA. Si l'intégration est effectuée après la configuration HA, les clés importées sur le nœud principal avant de configurer le nœud secondaire ne sont pas synchronisées avec le nœud secondaire. Par conséquent, Citrix recommande l'intégration de NCipher avant la configuration HA.

Doit-on importer la clé dans les appliances Citrix ADC principale et secondaire, ou les clés sont-elles synchronisées entre le nœud principal et le nœud secondaire ?

Si NCipher est intégré sur les deux appareils avant de former l'HA, les clés sont automatiquement synchronisées à partir de RFS en cours d'intégration.

Étant donné que le HSM ne se trouve pas sur l'appliance Citrix ADC, mais sur NCipher, qu'advient-il des clés et des certificats lorsqu'un nœud tombe en panne et est remplacé ?

Si un nœud échoue, vous pouvez synchroniser les clés et les certificats avec le nouveau nœud, en intégrant NCipher sur le nouveau nœud. Exécutez ensuite les commandes suivantes :

```
1 sync ha files ssl
2 force ha sync
3 <!--NeedCopy-->
```


Les certificats sont synchronisés et ajoutés si les clés sont synchronisées lors de l'intégration de NCipher.

Chiphers

Qu'est-ce qu'un chiffrement NULL ?

Les chiffrements sans chiffrement sont connus sous le nom de chiffrement NULL. Par exemple, NULL-MD5 est un chiffrement NULL.

Les chiffrements NULL sont-ils activés par défaut pour un service VIP SSL ou SSL ?

Non. Les chiffrements NULL ne sont pas activés par défaut pour un service VIP SSL ou SSL.

Quelle est la procédure pour supprimer les chiffrements NULL ?

Pour supprimer les chiffrements NULL d'une VIP SSL, exécutez la commande suivante :

```
bind ssl cipher <SSL_VIP> REM NULL
<!--NeedCopy-->
```

Pour supprimer les chiffrements NULL d'un service SSL, exécutez la commande suivante :

```
bind ssl cipher <SSL_Service> REM NULL -service
<!--NeedCopy-->
```

Quels sont les différents alias de chiffrement pris en charge sur l'appliance Citrix ADC ?

Pour répertorier les alias de chiffrement pris en charge sur l'appliance, à l'invite de commandes, tapez :

```
sh cipher
<!--NeedCopy-->
```

Quelle est la commande permettant d'afficher tous les chiffrements prédéfinis de l'appliance Citrix ADC ?

Pour afficher tous les chiffrements prédéfinis de l'appliance Citrix ADC, à l'interface de ligne de commande, tapez :

```
show ssl cipher
<!--NeedCopy-->
```


Quelle est la commande permettant d'afficher les détails d'un chiffrement individuel de l'appliance Citrix ADC ?

Pour afficher les détails d'un chiffrement individuel de l'appliance Citrix ADC, à l'interface de ligne de commande, tapez :

```
show ssl cipher <Cipher_Name/Cipher_Alias_Name/Cipher_Group_Name>
<!--NeedCopy-->
```

Exemple :

```
show cipher SSL3-RC4-SHA
     1) Cipher Name: SSL3-RC4-SHA
     Description: SSLv3 Kx=RSA Au=RSA Enc=RC4(128)
    Mac=SHA1
     Done
<!--NeedCopy-->
```

Quelle est l'importance de l'ajout des chiffrements prédéfinis de l'appliance Citrix ADC ?

L'ajout des chiffrements prédéfinis de l'appliance Citrix ADC entraîne l'ajout des chiffrements NULL à un service VIP SSL ou SSL.

Est-il possible de modifier l'ordre du chiffrement sans les délier d'un groupe de chiffrement sur une appliance Citrix ADC ?

Oui. Il est possible de modifier l'ordre du chiffrement sans délier les chiffrements d'un groupe de chiffrement personnalisé. Toutefois, vous ne pouvez pas modifier la priorité dans les groupes de chiffrement intégrés. Pour modifier la priorité d'un chiffrement lié à une entité SSL, commencez par dissocier le chiffrement du serveur virtuel, du service ou du groupe de services.

Remarque : Si le groupe de chiffrement lié à une entité SSL est vide, l'établissement de liaison SSL échoue car il n'y a pas de chiffrement négocié. Le groupe de chiffrement doit contenir au moins un chiffre.

ECDSA est-il pris en charge sur l'appliance Citrix ADC ?

ECDSA est pris en charge sur les plates-formes Citrix ADC suivantes. Pour plus d'informations sur les versions prises en charge, reportez-vous au tableau 1 et au tableau 2 des chiffrements disponibles sur les appliances Citrix ADC.

- Appliances Citrix ADC MPX et SDX avec puces N3
- Citrix ADC MPX 5900/8900/15000/26000

- Citrix ADC SDX 8900/15000
- Appliances Citrix ADC VPX

L'appliance Citrix ADC VPX prend-elle en charge les chiffrements AES-GCM/SHA2 sur le frontal ?

Oui, les chiffrements AES-GCM/SHA2 sont pris en charge sur l'appliance Citrix ADC VPX. Pour plus d'informations sur les versions prises en charge, reportez-vous à la section Chiphers disponibles sur les appliances Citrix ADC.

Certificats

Le nom unique d'un certificat client est-il disponible pendant toute la durée de la session utilisateur ?

Oui. Vous pouvez accéder au nom unique du certificat client lors des demandes suivantes pendant la durée de la session utilisateur. C'est-à-dire que même une fois la prise de main SSL terminée et que le certificat n'est plus envoyé par le navigateur. Utilisez une variable et une affectation comme détaillé dans l'exemple de configuration suivant :

Exemple :

```
add ns variable v2 -type "text(100)"

add ns assignment a1 -variable "$v2" -set       "CLIENT.SSL.CLIENT_CERT
    .SUBJECT.TYPECAST_NVLIST_T('=','/').VALUE("CN")"

add rewrite action act1 insert_http_header subject "$v2"  // example:
    to insert the distinguished name in the header

add rewrite policy pol1 true a1

add rewrite policy pol2 true act1

bind rewrite global pol1 1 next -type RES_DEFAULT

bind rewrite global pol2 2 next -type RES_DEFAULT

set rewrite param -undefAction RESET
<!--NeedCopy-->
```


Pourquoi dois-je lier le certificat de serveur ?

La liaison des certificats de serveur est l'exigence de base pour permettre à la configuration SSL de traiter les transactions SSL.

Pour lier le certificat de serveur à un VIP SSL, à l'interface de ligne de commande, tapez :

```
bind ssl vserver <vServerName> -certkeyName <cert_name>
<!--NeedCopy-->
```

Pour lier le certificat de serveur à un service SSL, à l'interface de ligne de commande, tapez :

```
bind ssl service <serviceName> -certkeyName <cert_name>
<!--NeedCopy-->
```

Combien de certificats puis-je lier à un VIP SSL ou à un service SSL ?

Sur une appliance CItrix ADC VPX, MPX/SDX (N3) et MPX/SDX 14000 FIPS, vous pouvez lier deux certificats à un serveur virtuel SSL ou à un service SSL si SNI est désactivé. Les certificats doivent être des certificats de type RSA et ECDSA. Si SNI est activé, vous pouvez lier plusieurs certificats de serveur de type RSA ou ECDSA. Sur une appliance CItrix ADC MPX (N2) ou MPX 9700 FIPS, si SNI est désactivé, vous ne pouvez lier qu'un seul certificat de type RSA. Si SNI est activé, vous pouvez lier plusieurs certificats de serveur de type RSA uniquement.

Que se passe-t-il si je dissocie ou que je remplace un certificat de serveur ?

Lorsque vous dissociez ou écrasez un certificat de serveur, toutes les connexions et sessions SSL créées à l'aide du certificat existant sont terminées. Lorsque vous écrasez un certificat existant, le message suivant s'affiche :

```
ERROR:

Warning: Current certificate replaces the previous binding.
<!--NeedCopy-->
```

Comment installer un certificat intermédiaire sur une appliance Citrix ADC et créer un lien vers un certificat de serveur ?

Consultez l'article à l'adresse http://support.citrix.com/article/ctx114146 pour plus d'informations sur l'installation d'un certificat intermédiaire.

Pourquoi est-ce que je reçois une erreur « La ressource existe déjà » lorsque j'essaie d'installer un certificat sur Citrix ADC ?

Consultez l'article à la page http://support.citrix.com/article/CTX117284 pour obtenir des instructions sur la résolution de l'erreur « La ressource existe déjà ».

Je souhaite créer un certificat de serveur sur une appliance Citrix ADC pour tester et évaluer le produit. Quelle est la procédure de création d'un certificat de serveur ?

Procédez comme suit pour créer un certificat de test.

Remarque : Un certificat créé avec cette procédure ne peut pas être utilisé pour authentifier tous les utilisateurs et navigateurs. Après avoir utilisé le certificat à des fins de test, vous devez obtenir un certificat de serveur signé par une autorité de certification racine autorisée.

Pour créer un certificat de serveur auto-signé, procédez comme suit :

1. Pour créer un certificat d'autorité de certification racine, à l'interface de ligne de commande, tapez :

```
create ssl rsakey /nsconfig/ssl/test-ca.key 1024

create ssl certreq /nsconfig/ssl/test-ca.csr -keyfile /nsconfig/
   ssl/test-ca.key

Enter the required information when prompted, and then type the
   following command:

create ssl cert /nsconfig/ssl/test-ca.cer /nsconfig/ssl/test-ca.
   csr ROOT_CERT -keyfile /nsconfig/ssl/test-ca.key
<!--NeedCopy-->
```

2. Effectuez la procédure suivante pour créer un certificat de serveur et le signer avec le certificat d'autorité de certification racine que vous venez de créer.

   a) Pour créer la demande et la clé, à l'interface de ligne de commande, tapez :

```
create ssl rsakey /nsconfig/ssl/test-server.key 1024

    create ssl certreq /nsconfig/ssl/test-server.csr -keyfile
       /nsconfig/ssl/test-server.key
<!--NeedCopy-->
```

   b) Entrez les informations requises lorsque vous y êtes invité.

   c) Pour créer un fichier de numéro de série, à l'interface de ligne de commande, tapez :


```
shell
 # echo '01' >
/nsconfig/ssl/serial.txt
 # exit
<!--NeedCopy-->
```

d) Pour créer un certificat de serveur signé par le certificat d'autorité de certification racine créé à l'étape 1, à l'interface de ligne de commande, tapez :

```
create ssl cert /nsconfig/ssl/test-server.cer /nsconfig/ssl/
   test-server.csr SRVR_CERT -CAcert /nsconfig/ssl/test-ca.cer
    -CAkey /nsconfig/ssl/test-ca.key -CAserial /nsconfig/ssl/
   serial.txt
<!--NeedCopy-->
```

e) Pour créer une paire de clés de certificat Citrix ADC, qui est l'objet en mémoire qui contient les informations de certificat de serveur pour les prises de main SSL et le chiffrement en bloc, à l'interface de ligne de commande, tapez :

```
add ssl certkey test-certkey -cert /nsconfig/ssl/test-server.
   cer -key /nsconfig/ssl/test-server.key
<!--NeedCopy-->
```

f) Pour lier la paire de clés de certificat au serveur virtuel SSL, à l'interface de ligne de commande, tapez :

```
bind ssl vserver <vServerName> -certkeyName <cert_name>
<!--NeedCopy-->
```

J'ai reçu une appliance Citrix ADC sur laquelle le logiciel NetScaler version 9.0 est installé. J'ai remarqué un fichier de licence supplémentaire sur l'appliance. Y a-t-il un changement dans la politique de licence à partir du logiciel NetScaler version 9.0 ?

Oui. À partir de la version 9.0 du logiciel Citrix NetScaler, l'appliance peut ne pas disposer d'un seul fichier de licence. Le nombre de fichiers de licences dépend de l'édition de la version du logiciel Citrix ADC. Par exemple, si vous avez installé l'édition Advanced, vous aurez peut-être besoin de fichiers de licence supplémentaires pour bénéficier de toutes les fonctionnalités des différentes fonctionnalités. Toutefois, si vous avez installé l'édition Premium, la solution matérielle-logicielle ne possède qu'un seul fichier de licence.

Comment exporter le certificat depuis Internet Information Service (IIS) ?

Il existe plusieurs façons, mais en utilisant la méthode suivante, le certificat et la clé privée appropriés pour le site Web sont exportés. Cette procédure doit être effectuée sur le serveur IIS réel.

1. Ouvrez l'outil d'administration du Gestionnaire des services Internet (IIS).
2. Développez le nœud des sites Web et localisez le site Web compatible SSL que vous souhaitez desservir via l'appliance Citrix ADC.
3. Cliquez avec le bouton droit sur ce site Web et cliquez sur Propriétés.
4. Cliquez sur l'onglet Sécurité de l'annuaire et, dans la section Communications sécurisées de la fenêtre, sélectionnez la zone Afficher le certificat.
5. Cliquez sur l'onglet Détails, puis cliquez sur Copier dans un fichier.
6. Sur la page Bienvenue dans l'Assistant Export de certificats, cliquez sur Suivant.
7. Sélectionnez Oui, exportez la clé privée, puis cliquez sur Suivant.

   Remarque : La clé privée DOIT être exportée pour que le déchargement SSL fonctionne sur Citrix ADC.
8. Assurez-vous que le bouton radio Échange d'informations personnelles -PKCS #12 est sélectionné et activez *uniquement* la case à cocher Inclure tous les certificats dans le chemin de certification si possible. Cliquez sur Suivant.
9. Entrez un mot de passe, puis cliquez sur Suivant.
10. Entrez un nom et un emplacement de fichier, puis cliquez sur Suivant. Donnez au fichier une extension de .PFX.
11. Cliquez sur Terminer.

Comment convertir le certificat PKCS #12 et l'installer sur Citrix ADC ?

1. Déplacez le fichier de certificat .PFX exporté vers un emplacement à partir duquel il peut être copié sur l'appliance Citrix ADC. C'est-à-dire à une machine qui autorise l'accès SSH à l'interface de gestion d'une appliance Citrix ADC. Copiez le certificat sur l'appliance à l'aide d'un utilitaire de copie sécurisée tel que SCP.
2. Accédez au shell BSD et convertissez le certificat (par exemple, Cert.PFX) au format .PEM :

```
root@ns# openssl pkcs12 -in cert.PFX -out cert.PEM
<!--NeedCopy-->
```

3. Pour vous assurer que le certificat converti est au format x509 correct, vérifiez que la commande suivante ne génère aucune erreur :


```
root@ns# openssl x509 -in cert.PEM -text
<!--NeedCopy-->
```

4. Vérifiez que le fichier de certificat contient une clé privée. Commencez par lancer la commande suivante :

```
root@ns# cat cert.PEM

Verify that the output file includes an RSA PRIVATE KEY section.

-----BEGIN RSA PRIVATE KEY-----
Mkm^s9KMs9023pz/s...
-----END RSA PRIVATE KEY-----
<!--NeedCopy-->
```

Voici un autre exemple de section CLÉ PRIVÉE RSA :

```
    Bag Attributes
    1.3.6.1.4.1.311.17.2: <No Values>
    localKeyID: 01 00 00 00
    Microsoft CSP Name: Microsoft RSA SChannel Cryptographic
    Provider
    friendlyName:
    4b9cef4cc8c9b849ff5c662fd3e0ef7e_76267e3e-6183-4d45-886e-6
       e067297b38f

    Key Attributes
    X509v3 Key Usage: 10
    -----BEGIN RSA PRIVATE KEY-----
    Proc-Type: 4,ENCRYPTED
    DEK-Info: DES-EDE3-CBC,43E7ACA5F4423968
    pZJ2SfsSVqMbRRf6ug37Clua5gY0Wld4frPIxFXyJquUHr31dilW5ta3hbIaQ+
       Rg

    ... (more random characters)
    v8dMugeRplkaH2Uwt/mWBk4t71Yv7GeHmcmjafK8H8iW80ooPO3D/ENV8X4U/
       tlh

    5eU6ky3WYZ1BTy6thxxLlwAullynVXZEflNLxq1oX+ZYl6djgjE3qg==
    -----END RSA PRIVATE KEY-----
<!--NeedCopy-->
```

Voici une section CERTIFICAT DE SERVEUR :


```
    Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: AG Certificate
    subject=/C=AU/ST=NSW/L=Wanniassa/O=Dave Mother
    Asiapacific/OU=Support/CN=davemother.food.lan
    issuer=/DC=lan/DC=food/CN=hotdog
    -----BEGIN CERTIFICATE-----
    MIIFiTCCBHGgAwIBAgIKCGryDgAAAAAHzANBgkqhkiG9w0BAQUFADA8MRMwEQYK


    ... (more random characters) 5
       pLDWYVHhLkA1pSxvFjNJHRSIydWHc5ltGyKqIUcBezVaXyel94pNSUYx07NpPV
       /

    MY2ovQyQZM8gGe3+lGFum0VHbv/y/gB9HhFesog=
    -----END CERTIFICATE-----
<!--NeedCopy-->
```

Voici une section CERTIFICAT D'AUTORITÉ DE CERTIFICATION INTERMÉDIAIRE :

```
    Bag Attributes: <Empty Attributes>
    subject=/DC=lan/DC=food/CN=hotdog
    issuer=/DC=lan/DC=food/CN=hotdog
    -----BEGIN CERTIFICATE-----
    MIIESDCCAzCgAwIBAgIQah20fCRYTY9LRXYMIRaKGjANBgkqhkiG9w0BAQUFADA8


    ... (more random characters)
       Nt0nksawDnbKo86rQcNnY5xUs7c7pj2zxj/IOsgNHUp5W6dDI9pQoqFFaDk
       =

    -----END CERTIFICATE-----
<!--NeedCopy-->
```

D'autres certificats d'autorité de certification intermédiaire peuvent suivre, en fonction du chemin de certification du certificat exporté.

5. Ouvrez le fichier .PEM dans un éditeur de texte
6. Localisez la première ligne du fichier .PEM et la première instance de la ligne suivante, puis copiez ces deux lignes et toutes les lignes entre elles :

```
-----END CERTIFICATE-----

Note: Make sure that last copied line is the first
-----END CERTIFICATE----- line in the .PEM file.
```



```
5
6 <!--NeedCopy-->
```

7. Collez les lignes copiées dans un nouveau fichier. Appelez le nouveau fichier quelque chose d'intuitif, tel que cert-key.pem. Cette paire de clés de certificat est destinée au serveur hébergeant le service HTTPS. Ce fichier doit contenir à la fois la section intitulée CLÉ PRIVÉE RSA et la section intitulée CERTIFICAT DE SERVEUR dans l'exemple précédent.

   Remarque : Le fichier de paires de clés de certificat contient la clé privée et doit être sécurisé.

8. Localisez toutes les sections suivantes commençant par —BEGIN CERTIFICATE— et se terminant par —END CERTIFICATE—, puis copiez chacune de ces sections dans un nouveau fichier distinct.

   Ces sections correspondent aux certificats des autorités de certification approuvées qui ont été inclus dans le chemin de certification. Ces sections doivent être copiées et collées dans de nouveaux fichiers individuels pour ces certificats. Par exemple, la section CERTIFICAT D'AUTORITÉ DE CERTIFICATION INTERMÉDIAIRE de l'exemple précédent doit être copiée et collée dans un nouveau fichier).

   Pour plusieurs certificats d'autorité de certification intermédiaires dans le fichier d'origine, créez des fichiers pour chaque certificat d'autorité de certification intermédiaire dans l'ordre dans lequel ils apparaissent dans le fichier. Gardez le suivi (en utilisant les noms de fichiers appropriés) de l'ordre dans lequel les certificats apparaissent, car ils doivent être liés entre eux dans le bon ordre dans une étape ultérieure.

9. Copiez le fichier de clé de certificat (cert-key.pem) et tout autre certificat d'autorité de certification supplémentaire dans le répertoire /nsconfig/ssl de l'appliance Citrix ADC.
10. Quittez le shell BSD et accédez à l'invite Citrix ADC.
11. Suivez les étapes de la section « Installer les fichiers de clés de certificat sur l'appliance » pour installer la clé/certificat une fois téléchargé sur le périphérique.

Comment convertir le certificat PKCS #7 et l'installer sur l'appliance Citrix ADC ?

Vous pouvez utiliser OpenSSL pour convertir un certificat PKCS #7 dans un format reconnaissable par l'appliance Citrix ADC. La procédure est identique à la procédure pour les certificats PKCS #12, sauf que vous appelez OpenSSL avec des paramètres différents. Les étapes de conversion des certificats PKCS #7 sont les suivantes :

1. Copiez le certificat sur l'appliance à l'aide d'un utilitaire de copie sécurisée, tel que SCP.
2. Convertissez le certificat (par exemple, Cert.P7B) au format PEM :

```
1 openssl pkcs7 -inform DER -in cert.p7b -print_certs -text -out
     cert.pem
2 <!--NeedCopy-->
```


3. Suivez les étapes 3 à 7 comme décrit dans la réponse aux certificats PKCS #12.
   Remarque : Avant de charger le certificat PKCS #7 converti sur l'appliance, vérifiez qu'il contient une clé privée, exactement comme décrit à l'étape 3 pour la procédure PKCS #12. Les certificats PKCS #7, en particulier les certificats exportés depuis IIS, ne contiennent généralement pas de clé privée.

Lorsque je lie un chiffrement à un serveur ou un service virtuel à l'aide de la commande bind cipher, le message d'erreur « Commande obsolète » s'affiche. « ?

La commande de liaison d'un chiffrement à un serveur ou service virtuel a été modifiée.

Utilisez la `bind ssl vserver <vsername> -ciphername <ciphername>` commande pour lier un chiffrement SSL à un serveur virtuel SSL.

Utilisez la `bind ssl service <serviceName> -ciphername <ciphername>` commande pour lier un chiffrement SSL à un service SSL.

Remarque : Les nouveaux chiffrements et groupes de chiffrement sont ajoutés à la liste existante et ne sont pas remplacés.

Pourquoi ne puis-je pas créer un groupe de chiffrement et y lier des chiffrements à l'aide de la commande add cipher ?

La fonctionnalité de commande add cipher a été modifiée dans la version 10. La commande crée uniquement un groupe de chiffrement. Pour ajouter des chiffrements au groupe, utilisez la commande de chiffrement de liaison.

OpenSSL

Comment utiliser OpenSSL pour convertir des certificats entre PEM et DER ?

Pour utiliser OpenSSL, vous devez disposer d'une installation fonctionnelle du logiciel OpenSSL et pouvoir exécuter OpenSSL à partir de la ligne de commande.

Les certificats x509 et les clés RSA peuvent être stockés dans différents formats.

Deux formats courants sont les suivants :

- DER (format binaire utilisé principalement par les plates-formes Java et Macintosh)
- PEM (représentation base64 de DER avec des informations d'en-tête et de pied de page, utilisée principalement par les plates-formes UNIX et Linux).

Une clé et le certificat correspondant, en plus du certificat racine et des certificats intermédiaires, peuvent également être stockés dans un seul fichier PKCS #12 (.P12, .PFX).

Procédure

Utilisez la commande **OpenSSL** pour convertir entre les formats comme suit :

1. Pour convertir un certificat PEM en DER :

```
x509 -in input.crt -inform PEM -out output.crt -outform DER
<!--NeedCopy-->
```

2. Pour convertir un certificat de DER en PEM :

```
x509 -in input.crt -inform DER -out output.crt -outform PEM
<!--NeedCopy-->
```

3. Pour convertir une clé de PEM en DER :

```
rsa -in input.key -inform PEM -out output.key -outform DER
<!--NeedCopy-->
```

4. Pour convertir une clé de DER en PEM :

```
rsa -in input.key -inform DER -out output.key -outform PEM
<!--NeedCopy-->
```

Remarque : Si la clé que vous importez est chiffrée avec un chiffrement symétrique pris en charge, vous êtes invité à entrer la phrase secrète.

Remarque : Pour convertir une clé vers ou depuis le format NET (serveur Netscape) obsolète, remplacez NET par PEM ou DER, selon le cas. La clé stockée est chiffrée dans un chiffrement symétrique RC4 faible non salé, donc une phrase secrète est demandée. Une phrase secrète vide est acceptable.

Limites système

Quels sont les chiffres importants à retenir ?

1. Créer une demande de certificat :
   - Nom du fichier de demande : 63 caractères maximum
   - Nom du fichier clé : 63 caractères maximum
   - Phrase secrète PEM (pour clé chiffrée) : 31 caractères maximum
   - Nom commun : 63 caractères maximum
   - Ville : 127 caractères maximum
   - Nom de l'organisation : 63 caractères maximum
   - Nom de l'État/de la province : 63 caractères maximum
   - Adresse e-mail : 39 caractères maximum
   - Unité d'organisation : 63 caractères maximum

- Mot de passe Challenge : 20 caractères maximum
- Nom de l'entreprise : 127 caractères maximum

2. Créer un certificat :

   - Nom du fichier de certificat : 63 caractères maximum
   - Nom du fichier de demande de certificat : 63 caractères maximum
   - Nom du fichier clé : 63 caractères maximum
   - Phrase secrète PEM : 31 caractères maximum
   - Période de validité : maximum 3650 jours
   - Nom du fichier du certificat CA : 63 caractères maximum
   - Nom de fichier de la clé CA : 63 caractères maximum
   - Phrase secrète PEM : 31 caractères maximum
   - Fichier de numéro de série CA : 63 caractères maximum

3. Créez et installez un certificat de test de serveur :

   - Nom du fichier de certificat : 31 caractères maximum
   - Nom de domaine complet : 63 caractères maximum

4. Créer une clé Diffie-Hellman (DH) :

   - Nom de fichier DH (avec chemin d'accès) : 63 caractères maximum
   - Taille des paramètres DH : maximum 2048 bits

5. Importer la clé PKCS12 :

   - Nom du fichier de sortie : 63 caractères maximum
   - Nom de fichier PKCS12 : 63 caractères maximum
   - Mot de passe d'importation : 31 caractères maximum
   - Phrase secrète PEM : 31 caractères maximum
   - Vérifier la phrase secrète PEM : 31 caractères maximum

6. Exporter PKCS12

   - Nom de fichier PKCS12 : 63 caractères maximum
   - Nom du fichier de certificat : 63 caractères maximum
   - Nom du fichier clé : 63 caractères maximum
   - Mot de passe d'exportation : 31 caractères maximum
   - Phrase secrète PEM : 31 caractères maximum

7. Gestion des CRL :

   - Nom du fichier du certificat CA : 63 caractères maximum
   - Nom de fichier de la clé CA : 63 caractères maximum
   - Mot de passe du fichier de clé CA : 31 caractères maximum
   - Nom du fichier d'index : 63 caractères maximum

- Nom du fichier de certificat : 63 caractères maximum

8. Créer une clé RSA :
   - Nom du fichier clé : 63 caractères maximum
   - Taille de la clé : 4096 bits maximum
   - Phrase secrète PEM : 31 caractères maximum
   - Vérifier la phrase secrète : 31 caractères maximum
9. Modifiez les paramètres SSL avancés :
   - Taille maximale de la mémoire CRL : 1024 Mo maximum
   - Délai d'expiration du déclencheur de chiffrement (10 mS) : maximum 200
   - Nombre de paquets de déclencheurs de chiffrement : 50 maximum
   - Taille du cache OCSP : 512 Mo maximum
10. Certificat d'installation :
    - Nom de la paire de clés de certificat : 31 caractères maximum
    - Nom du fichier de certificat : 63 caractères maximum
    - Nom du fichier de clé privée : 63 caractères maximum
    - Mot de passe : 31 caractères maximum
    - Période de notification : 100 maximum
11. Créer un groupe de chiffrement :
    - Nom du groupe de chiffrement : 39 caractères maximum
12. Créer une CRL :
    - Nom de la LCR : 31 caractères maximum
    - Fichier CRL : 63 caractères maximum
    - URL : 127 caractères maximum
    - DN de base : 127 caractères maximum
    - DN de liaison : 127 caractères maximum
    - Mot de passe : 31 caractères maximum
    - Jours : 31 maximum
13. Créer une stratégie SSL :
    - Nom : 127 caractères maximum
14. Créer une action SSL :
    - Nom : 127 caractères maximum
15. Créer un répondeur OCSP :
    - Nom : 32 caractères maximum
    - URL : 128 caractères maximum

- Profondeur de lot : 8 maximum
- Délai de traitement par lots : maximum 10000
- Fait produit à la fois : Maximum 86400
- Délai d'expiration de la demande : maximum 120000

16. Créer un serveur virtuel :
    - Nom : 127 caractères maximum
    - URL de redirection : 127 caractères maximum
    - Délai d'expiration du client : maximum 31536000 secondes
17. Créer un service :
    - Nom : 127 caractères maximum
    - Délai d'inactivité (s) :
      Client : maximum 31536000
      Serveur : maximum 31536000
18. Créer un groupe de services :
    - Nom du groupe de services : 127 caractères maximum
    - ID du serveur : maximum 4294967295
    - Délai d'attente d'inactivité (s) :
      Client : Valeur maximale 31536000
      Serveur : maximum 31536000
19. Créer un moniteur :
    - Nom : 31 caractères maximum
20. Créer un serveur :
    - Nom du serveur : 127 caractères maximum
    - Nom de domaine : 255 caractères maximum
    - Résoudre la nouvelle tentative : 20 939 secondes maximum

Inspection du contenu

January 21, 2021

Ces derniers temps, il y a une expansion des types de périphériques pour afficher divers contenus multimédias. Les types d'appareils peuvent être des combinés mobiles aux tablettes et aux ordinateurs de bureau. Les fournisseurs d'infrastructure intermédiaires doivent transformer le contenu original d'un serveur Web en un format adapté au périphérique qui demande le contenu. Les périphériques

externes inspectent le contenu qui transcode et le renvoyer au client. Le protocole couramment utilisé pour y parvenir est ICAP. ICAP permet à l'appliance Citrix ADC d'être mise en place dans divers déploiements. ICAP utilise la technique d'inspection du contenu qui inspecte les données à la recherche de logiciels malveillants et de problèmes de sécurité.

> **Remarque**
>
> HTTP/2 n'est pas compatible avec l'inspection du contenu. Les applications utilisant HTTP/2 peuvent ne pas fonctionner correctement si le trafic est envoyé via l'inspection du contenu.

ICAP pour l'inspection de contenu à distance

August 20, 2021

ICAP (Internet Content Adaptation Protocol) est un protocole léger simple pour exécuter le service de transformation à valeur ajoutée sur les messages HTTP. Dans un scénario typique, un client ICAP transmet les requêtes HTTP et les réponses à un ou plusieurs serveurs ICAP pour traitement. Les serveurs ICAP effectuent la transformation du contenu des demandes et renvoient les réponses avec les mesures appropriées à prendre sur la demande ou la réponse.

ICAP sur une appliance Citrix ADC

Dans une configuration Citrix ADC, l'appliance agit en tant que client ICAP qui interagit avec des serveurs ICAP tiers (tels que la protection contre les programmes malveillants et la protection contre la perte de données (DLP)). Lorsque l'appliance reçoit un trafic Web entrant, elle intercepte le trafic et utilise une stratégie d'inspection du contenu pour évaluer si la demande HTTP nécessite un traitement ICAP. Si oui, l'appliance déchiffre et envoie le message sous forme de texte brut aux serveurs ICAP. Les serveurs ICAP exécutent le service de transformation de contenu sur le message de demande et envoient une réponse à l'appliance. Les messages adaptés peuvent être une requête HTTP ou une réponse HTTP. Si l'appliance interagit avec plusieurs serveurs ICAP, elle effectue l'équilibrage de la charge des serveurs ICAP. Ce scénario se produit lorsqu'un serveur ICAP n'est pas suffisant pour gérer toute la charge de trafic. Une fois que les serveurs ICAP renvoient un message modifié, l'appliance transmet le message modifié au serveur d'origine principal.

L'appliance Citrix ADC fournit également un service ICAP sécurisé si le trafic entrant est de type HTTPS. L'appliance utilise un service TCP basé sur SSL pour établir une connexion sécurisée entre l'appliance et les serveurs ICAP.

Fonctionnement de la modification des demandes ICAP (REQMOD)

En mode Request modification (REQMOD), l'appliance Citrix ADC transfère la requête HTTP reçue du client au serveur ICAP. Le serveur ICAP effectue ensuite l'une des opérations suivantes :

1. Retourne une version modifiée de la demande et l'appliance envoie à son tour la demande modifiée au serveur d'origine principal ou achemine la demande modifiée vers un autre serveur ICAP.
2. Répond avec un message indiquant qu'aucune adaptation n'est requise.
3. Renvoie une erreur et l'appliance renvoie le message d'erreur à l'utilisateur.

Fonctionnement de la modification de la réponse ICAP (RESPMOD)

En mode de modification de réponse (RESPMOD), l'appliance Citrix ADC envoie une réponse HTTP au serveur ICAP (la réponse envoyée par l'appliance est généralement la réponse envoyée par le serveur d'origine). Le serveur ICAP effectue ensuite l'une des opérations suivantes :

1. Envoie une version modifiée de la réponse et l'appliance envoie la réponse à l'utilisateur ou achemine la réponse à un autre serveur ICAP.
2. Répond avec un message indiquant qu'aucune adaptation n'est requise.
3. Renvoie une erreur et l'appliance envoie le message d'erreur à l'utilisateur.

Licence ICAP

La fonctionnalité ICAP fonctionne sur une configuration autonome ou haute disponibilité Citrix ADC avec Citrix ADC Premium ou Advanced License Edition.

Configurer ICAP pour le service de transformation de contenu

Pour utiliser ICAP pour le service de transformation de contenu, vous devez commencer par activer les fonctions d'inspection du contenu et d'équilibrage de charge. Une fois les fonctionnalités activées, vous pouvez effectuer les tâches suivantes

Pour activer l'inspection du contenu

Si vous souhaitez que l'appliance Citrix ADC agisse en tant que client ICAP, vous devez d'abord activer les fonctionnalités d'inspection du contenu et d'équilibrage de charge.

À l'invite de commandes, tapez :

```
enable ns feature contentInspection LoadBalancing
<!--NeedCopy-->
```


Ajouter un profil ICAP

Les configurations ICAP pour une appliance Citrix ADC sont spécifiées dans une entité appelée profil ICAP. Le profil contient un ensemble de paramètres ICAP. Les paramètres incluent des paramètres permettant de générer dynamiquement une requête ICAP, de recevoir la réponse ICAP et de consigner les données d'inspection du contenu.

Pour générer dynamiquement une requête ICAP au serveur ICAP, un nouveau paramètre, « InserthTTpRequest » est ajouté au profil ICAP. Si ce paramètre est configuré, l'appliance prend la valeur configurée en tant qu'expression de stratégie et évalue l'expression et inclut le résultat sous la forme d'une requête ou d'une réponse HTTP encapsulée, puis l'a envoyée au serveur ICAP. En outre, un nouveau paramètre « InserticapHeaders » est configurable pour évaluer dynamiquement et inclure les en-têtes ICAP.

Lorsque l'appliance envoie une demande ICAP et ne reçoit pas de réponse au serveur ICAP, la connexion cesse de répondre. Cela se produit jusqu'à ce que le serveur ICAP envoie une réponse ou qu'une session soit libérée. Le comportement peut être géré en configurant l'option de délai d'attente de réponse ICAP. Vous pouvez définir un paramètre de délai d'attente de demande pour l'action en cas de réponse ICAP différée. Si l'appliance Citrix ADC ne reçoit pas de réponse dans le délai d'expiration de la demande configuré, l'action de délai d'expiration de la demande est effectuée.

ReqTimeoutAction : Les valeurs possibles sont BYPASS, RESET, DROP.
BYPASS : Ceci ignore la réponse du serveur ICAP distant et envoie la demande/réponse au client/serveur.
RESET (par défaut) : réinitialisez la connexion client en la fermant.
DROP : Supprimer la demande sans envoyer de réponse à l'utilisateur

Pour évaluer une réponse ICAP, une nouvelle expression de stratégie `ICAP.RES` est utilisée dans l'expression de retour de légende d'inspection du contenu. Cette expression évalue la réponse ICAP de la même manière que l'`HTTP.RES` expression dans un `HTTP_CALLOUT`.

Par exemple, lorsqu'une appliance Citrix ADC reçoit une requête HTTP pour un service hébergé derrière l'adresse IP virtuelle Citrix ADC, l'appliance peut devoir vérifier l'authentification du client auprès d'un serveur externe et effectuer une action.

À l'invite de commandes, tapez :

```
add ns icapProfile <name> [-preview ( ENABLED | DISABLED )][-previewLength
 <positive_integer>] -uri <string> [-hostHeader <string>] [-userAgent <
string>] -Mode ( REQMOD | RESPMOD )[-queryParams <string>] [-connectionKeepAlive
 ( ENABLED | DISABLED )][-allow204 ( ENABLED | DISABLED )] [-insertICAPHeaders
 <string>][-insertHTTPRequest <string>] [-reqTimeout <positive_integer>][-
reqTimeoutAction <reqTimeoutAction>] [-logAction <string>]
```

Exemple :


```
add icapprofile reqmod-profile -mode RESPMOD -uri “/req_scan” -hostHeader “Webroot.reqsca” -useragent “NS_SWG-Proxy”

add ns icapProfile icap_prof1 -uri "/example"-Mode REQMOD -reqtimeout 4 -reqtimeoutaction BYPASS

> add icapProfile reqmode-profile -uri '/example'-mode REQMOD -insertHTTPRequest q{ HTTP.REQ.METHOD + ""+ HTTP.REQ.URL + "HTTP/1.1\r\n"+ "Host: "+ HTTP.REQ.HOSTNAME + "\r\n\r\n"}
```

Consigner l’action d’inspection du contenu ICAP

Pour générer dynamiquement des enregistrements de flux de journaux d’inspection de contenu ou des journaux SYSLOG, vous pouvez utiliser l’expression de stratégie ICAP.RES sur la réponse ICAP. Ce paramètre est configurable dans le profil ICAP pour configurer l’expression de stratégie afin de générer les enregistrements de journal dynamiques.

À l’invite de commandes, tapez :

```
add audit messageaction icap_log_expr INFORMATIONAL icap.res.full_header

set icapProfile reqmode-profile -logAction messageaction
```

Ajouter un service ICAP en tant que service TCP ou SSL_TCP

Après avoir activé la fonctionnalité d’inspection du contenu, vous devez ajouter un service ICAP pour les serveurs ICAP qui feront partie de la configuration d’équilibrage de charge. Le service que vous ajoutez fournit la connexion ICAP entre l’appliance Citrix ADC et les serveurs virtuels d’équilibrage de charge.

Remarque : En tant qu’administrateur, vous pouvez ajouter un service ICAP et configurer directement l’adresse IP du serveur ICAP dans l’action Inspection du contenu.

À l’invite de commandes, tapez ce qui suit :

```
1 add service <name> <IP> <serviceType> <port>
2 <!--NeedCopy-->
```

Exemple :

```
add service icapsv1 10.10.10.10 SSL_TCP 1345

add service icapsv2 10.10.10.11 SSL_TCP 1345
```


Ajouter un serveur virtuel d'équilibrage de charge basé sur TCP ou SSL_TCP

Après avoir créé un service ICAP, vous devez créer un serveur virtuel pour accepter le trafic ICAP et équilibrer la charge des serveurs ICAP.

> **Remarque :**
>
> Vous pouvez également utiliser un service TCP basé sur SSL sur un canal sécurisé. Vous utilisez un service SSL_TCP et vous liez à l'action Inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name> <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver vicap TCP 0.0.0.0 - persistenceType NONE -cltTimeout
    9000

add lb vserver vicap SSL_TCP 0.0.0.0 0 - persistenceType NONE -
    cltTimeout 9000
<!--NeedCopy-->
```

Liez le service ICAP au serveur virtuel d'équilibrage de charge

Après avoir créé un service ICAP et un serveur virtuel, vous devez lier le service ICAP au serveur virtuel.

À l'invite de commandes, tapez ce qui suit :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver vicap icapsv1
<!--NeedCopy-->
```

Ajouter une action d'inspection du contenu

Après avoir activé la fonction d'inspection du contenu, vous devez ajouter une action ICAP pour gérer les informations de demande ICAP. Le profil ICAP et les services, ou le serveur virtuel d'équilibrage de charge créés sont liés à l'action ICAP. Si le serveur ICAP est en panne, vous pouvez configurer le `ifserverdown` paramètre pour que l'appliance exécute l'une des actions suivantes.

CONTINUER : Si l'utilisateur souhaite contourner l'inspection du contenu lorsque le serveur distant est en panne, vous pouvez choisir l'action « CONTINUER », par défaut.
RESET (par défaut) : Cette action répond au client en fermant la connexion avec RST.
DROP : Cette action supprime silencieusement les paquets sans envoyer de réponse à l'utilisateur.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection action <name> -type ICAP -serverName <string> -
    icapProfileName <string>

add ContentInspection action <name> -type ICAP -serverip <ip> -
    serverport <port> -icapProfileName <string>
<!--NeedCopy-->
```

> **Remarque :**
>
> Si vous pouvez configurer le service ICAP au lieu d'un serveur virtuel d'équilibrage de charge, vous pouvez mentionner le nom du service dans l' \<-serverip> option. Lors de l'ajout de l'action Inspection du contenu, le service TCP est automatiquement créé pour l'adresse IP donnée avec le port 1344 et il est utilisé pour la communication ICAP.

Exemple :

```
add ContentInspection action ci_act_lb -type ICAP -serverName vicap -
    icapProfileName icap_reqmod

add ContentInspection action ci_act_svc -type ICAP -serverName icapsv1
    -icapProfileName icap_reqmod

add ContentInspection action ci_act_svc -type ICAP -serverip 1.1.1.1 -
    serverport 1344 -icapProfileName icap_reqmod
<!--NeedCopy-->
```

Ajouter des stratégies d'inspection du contenu

Après avoir créé une action d'inspection de contenu, vous devez créer des stratégies d'inspection de contenu pour évaluer les demandes de traitement ICAP et de journalisation d'audit. La stratégie est basée sur une règle qui consiste en une ou plusieurs expressions. La règle est associée à l'action d'inspection du contenu associée si une demande correspond à la règle.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```


Exemple :

```
add ContentInspection policy ci_pol_basic -rule true -action
    ci_act_svc

add ContentInspection policy ci_pol_HTTP -rule HTTP.REQ.URL.CONTAINS(
    "html") -action ci_act_svc
<!--NeedCopy-->
```

Lier les stratégies d'inspection de contenu au serveur virtuel de commutation de contenu ou d'équilibrage de charge

Pour mettre en œuvre une stratégie ICAP, vous devez la lier globalement ou la lier à un serveur virtuel de commutation de contenu ou d'équilibrage de charge, qui frontent l'application. Lorsque vous liez la stratégie, vous devez lui attribuer une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées.

> **Remarque :**
>
> Le serveur virtuel d'application doit être de type HTTP/SSL/CS-PROXY.

Pour plus d'informations sur la configuration d'une configuration d'équilibrage de charge pour le transfert du trafic vers le serveur d'origine principal après la transformation du contenu, reportez-vous à la section Équilibrage de charge.

Configurer le service ICAP sécurisé

Pour établir une connexion sécurisée entre l'appliance Citrix ADC et les serveurs Web ICAP, l'appliance utilise un service TCP basé sur SSL ou un serveur virtuel d'équilibrage de charge lié à une action ICAP.

Pour établir une connexion ICAP sécurisée, effectuez les tâches suivantes :

1. Ajouter un service TCP basé sur SSL.
2. Liez le service TCP basé sur SSL à un serveur virtuel d'équilibrage de charge de type TCP ou SSL_TCP.
3. Liez un service TCP basé sur SSL ou un serveur virtuel d'équilibrage de charge à l'action d'inspection de contenu.

Ajouter un service TCP basé sur SSL au serveur virtuel d'équilibrage de charge

Pour établir une connexion sécurisée entre l'appliance Citrix ADC et les serveurs Web ICAP, l'appliance utilise un service TCP basé sur SSL ou un serveur virtuel d'équilibrage de charge lié à une action ICAP.

Pour établir une connexion ICAP sécurisée, effectuez les tâches suivantes :

1. Ajouter un service TCP basé sur SSL.
2. Liez le service TCP basé sur SSL à un serveur virtuel d'équilibrage de charge de type TCP ou SSL_TCP.

Liez un service TCP basé sur SSL ou un serveur virtuel d'équilibrage de charge à l'action d'inspection de contenu

Ajouter un service TCP basé sur SSL au serveur virtuel d'équilibrage de charge

Après avoir activé la fonction d'inspection du contenu, vous devez ajouter un service ICAP sécurisé qui fera partie de la configuration d'équilibrage de charge. Le service que vous ajoutez fournit une connexion ICAP sécurisée entre l'appliance Citrix ADC et les serveurs virtuels d'équilibrage de charge.

À l'invite de commandes, tapez ce qui suit :

```
add service <name> <IP> <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
add service icapsv2 10.102.29.200 SSL_TCP 1344 -gslb NONE -maxclient
    0 -maxReq 0 -cip DISABLED -usip NO -useproxport YES -sp ON -
    cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB NO -CMP NO
<!--NeedCopy-->
```

Liez un service TCP basé sur SSL au serveur virtuel d'équilibrage de charge SSL_TCP ou TCP

Après avoir créé un service ICAP sécurisé, vous devez lier le service au serveur virtuel d'équilibrage de charge. Il est obligatoire si vous utilisez un serveur virtuel d'équilibrage de charge pour équilibrer la charge des serveurs ICAP.

À l'invite de commandes, tapez ce qui suit :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver vicap icapsv2
<!--NeedCopy-->
```


Liez un service TCP basé sur SSL ou un serveur virtuel d'équilibrage de charge à l'action d'inspection du contenu

Vous ajoutez une action ICAP pour gérer les informations de demande ICAP et lier également le service TCP SSL à l'action.

À l'invite de commandes, tapez ce qui suit :

```
1 add contentInspection action <name> -type ICAP -serverName <string> -
     icapProfileName <string>
2 <!--NeedCopy-->
```

Exemple :

```
1 add ContentInspection action ci_act_svc -type ICAP -serverName icapsv2
     -icapProfileName icap_reqmod
2
3 add ContentInspection action ci_act_svc -type ICAP -serverName vicap -
     icapProfileName icap_reqmod
4 <!--NeedCopy-->
```

Configurer le protocole ICAP à l'aide de l'interface graphique

1. Accédez à **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
2. Dans la page **Services**, entrez les détails du service.
3. Accédez à **Équilibrage de charge** > **Serveurs virtuels**. Ajoutez un serveur virtuel d'équilibrage de charge de type HTTP/SSL. Vous pouvez également sélectionner un serveur virtuel et cliquer sur **Modifier**.
4. Après avoir entré les détails de base du serveur, cliquez sur **Continuer**.
5. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
6. Accédez à la section **Stratégies** et cliquez sur l'icône **Crayon** pour configurer la stratégie d'inspection du contenu.
7. Dans la page **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.
8. Dans la section **Liaison de stratégie**, cliquez sur **+** pour ajouter une stratégie d'inspection du contenu.
9. Dans la page **Créer une stratégie ICAP**, entrez un nom pour la stratégie.
10. Dans le champ **Action**, cliquez sur le signe « + » pour ajouter une action ICAP.
11. Dans la page **Créer une action ICAP**, entrez un nom pour l'action.
12. Entrez un nom pour l'action.
13. Dans le champ **Nom du serveur**, entrez le nom du service TCP déjà créé.
14. Dans le champ **Profil ICAP**, cliquez sur le signe « + » pour ajouter un profil ICAP.

15. Dans la page **Créer un profil ICAP**, entrez un nom de profil, un URI et un MODE.
16. Cliquez sur **Créer**.
17. Dans la page **Créer une action ICAP**, cliquez sur **Créer**.
18. Dans la page **Créer une stratégie ICAP**, entrez « true » dans l'**éditeur d'expressions**, puis cliquez sur **Créer** .
19. Cliquez sur **Bind**.
20. Lorsque vous êtes invité à activer la fonction d'inspection du contenu, cliquez sur **Oui**.
21. Cliquez sur **Terminé**.

Pour plus d'informations sur la configuration de l'interface graphique Citrix ADC pour l'équilibrage de charge et le transfert du trafic vers le serveur d'origine principal après la transformation du contenu, reportez-vous à la section Équilibrage de charge.

Configurer le protocole ICAP sécurisé à l'aide de l'interface graphique

1. Accédez à **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
2. Dans la page **Services**, entrez les détails du service.
3. Accédez à **Équilibrage de charge** > **Serveurs virtuels**. Ajoutez un serveur virtuel de type HTTP/SSL. Vous pouvez également sélectionner un serveur virtuel et cliquer sur **Modifier**.
4. Après avoir entré les détails de base du serveur, cliquez sur **Continuer**.
5. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
6. Accédez à la section **Stratégies** et cliquez sur l'icône **Crayon** pour configurer la stratégie d'inspection du contenu.
7. Dans la page **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.
8. Dans la section **Liaison de stratégie**, cliquez sur **+** pour ajouter une stratégie d'inspection du contenu.
9. Dans la page **Créer une stratégie ICAP**, entrez un nom pour la stratégie.
10. Dans le champ **Action**, cliquez sur le signe « + » pour ajouter une action ICAP.
11. Dans la page **Créer une action ICAP**, entrez un nom pour l'action.
12. Entrez un nom pour l'action.
13. Dans le champ **Nom du serveur**, entrez le nom du service TCP_SSL déjà créé.
14. Dans le champ **Profil ICAP**, cliquez sur le signe « + » pour ajouter un profil ICAP.
15. Dans la page **Créer un profil ICAP**, entrez un nom de profil, un URI et un MODE.
16. Cliquez sur **Créer**.
17. Dans la page **Créer une action ICAP**, cliquez sur **Créer**.
18. Dans la page **Créer une stratégie ICAP**, entrez « true » dans l'**éditeur d'expressions**, puis cliquez sur **Créer** .
19. Cliquez sur **Bind**.
20. Lorsque vous êtes invité à activer la fonction d'inspection du contenu, cliquez sur **Oui**.

21. Cliquez sur **Terminé**.

Prise en charge du journal d'audit pour l'inspection à distance de

Si une demande entrante ou une réponse sortante fait l'objet d'une inspection de contenu, l'appliance Citrix ADC consigne les détails ICAP. L'appliance stocke les détails sous forme de message de journal dans le fichier ns.log.

Chaque message de journal contient généralement les détails suivants :

```
<Source IP> <Destination IP> <Domain> <ICAP server IP><ICAP Mode> <
    Service URI> <ICAP response> <Policy action>
<!--NeedCopy-->
```

Exemple de message de journal de requête inspecté par le contenu :

```
Apr 18 14:45:41 <local0.info> 10.106.97.104 04/18/2018:14:45:41 GMT 0-
    PPE-0 : default CI ICAP_LOG 788 0 : Source 10.102.1.98:39048 -
    Destination 10.106.97.89:8011 - Domain 10.106.97.89 - Content-Type
    application/x-www-form-urlencoded - ICAP Server 10.106.97.99:1344 -
    Mode REQMOD - Service /example - Response 204 - Action FORWARD
<!--NeedCopy-->
```

Exemple de message du journal des réponses inspecté par le contenu :

```
Apr 18 12:34:08 <local0.info> 10.106.97.104 04/18/2018:12:34:08 GMT 0-
    PPE-0 : default CI ICAP_LOG 71 0 : Source 10.106.97.105:18552 -
    Destination 10.106.97.99:80 - Domain NA - Content-Type NA - ICAP
    Server 10.106.97.99:1344 - Mode RESPMOD - Service /example -
    Response 400 - Action Internal Error
<!--NeedCopy-->
```

Intégration de périphériques en ligne avec Citrix ADC

August 20, 2021

Les dispositifs de sécurité tels que le système de prévention des intrusions (IPS) et le pare-feu de nouvelle génération (NGFW) protègent les serveurs contre les attaques réseau. Ces périphériques sont déployés en mode Inline couche 2 et leur fonction principale est de protéger les serveurs contre les attaques réseau et de signaler les menaces de sécurité sur le réseau.

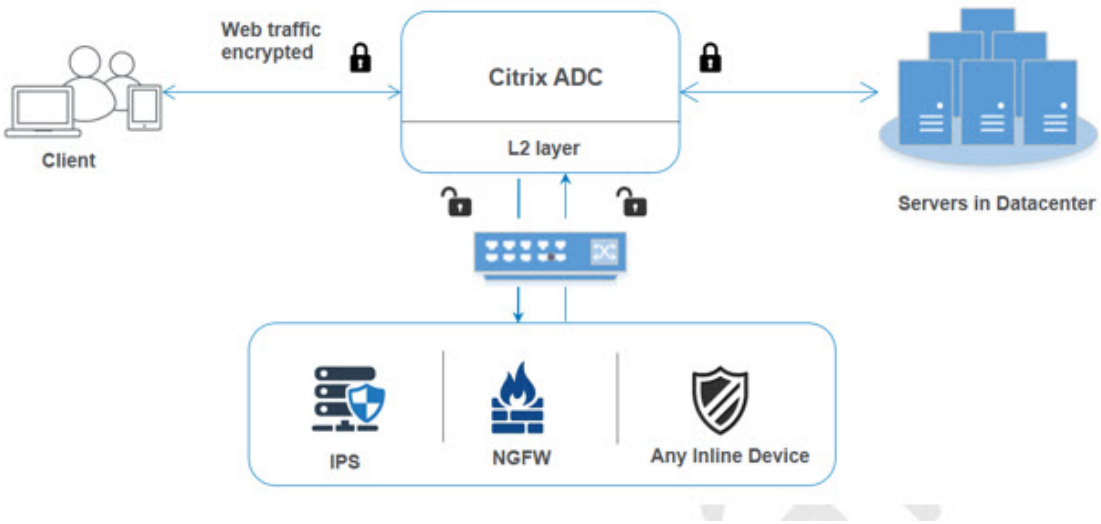
Pour prévenir les menaces vulnérables et offrir une protection de sécurité avancée, une appliance Citrix ADC est intégrée à un ou plusieurs périphériques en ligne. Les périphériques en ligne peuvent être n'importe quel périphérique de sécurité tel que IPS, NGFW.

Voici quelques-uns des cas d'utilisation qui bénéficient de l'intégration de périphérique en ligne avec l'appliance Citrix ADC :

- **Inspection du trafic chiffré**. La plupart des appliances IPS et NGFW contournent le trafic crypté, ce qui rend les serveurs vulnérables aux attaques. Une appliance Citrix ADC peut déchiffrer le trafic et l'envoyer à des périphériques en ligne pour inspection. Il améliore la sécurité du réseau du client.
- **Déchargement des périphériques en ligne du traitement TLS/SSL**. Le traitement TLS/SSL est coûteux et le problème peut entraîner un processeur système élevé dans les appliances IPS ou NGFW s'ils déchiffrent le trafic. Comme le trafic chiffré augmente rapidement, ces systèmes ne parviennent pas à décrypter et à inspecter le trafic chiffré. Citrix ADC aide à décharger les périphériques en ligne du traitement TLS/SSL. Il en résulte que l'appareil en ligne supportant un volume élevé d'inspection de la circulation.
- **Chargement des appareils en ligne d'équilibrage**. La charge de l'appliance Citrix ADC équilibre plusieurs périphériques en ligne lorsqu'il y a un volume élevé de trafic.
- **Sélection intelligente du trafic**. Chaque paquet entrant dans l'appliance peut faire l'objet d'un contrôle de contenu, par exemple le téléchargement de fichiers texte. L'utilisateur peut configurer l'appliance Citrix ADC pour sélectionner le trafic spécifique (par exemple les fichiers .exe) pour l'inspection et envoyer le trafic aux périphériques en ligne pour le traitement des données

Comment Citrix ADC est intégré aux périphériques en ligne

Le diagramme suivant montre comment un Citrix ADC est intégré aux périphériques de sécurité en ligne.



Lorsque vous intégrez des périphériques en ligne à l'appliance Citrix ADC, le composant interagit comme suit :

1. Un client envoie une demande à l'appliance Citrix ADC.
2. L'appliance reçoit la demande et l'envoie à un périphérique en ligne en fonction de l'évaluation de la stratégie.
   Remarque : s'il existe au moins deux périphériques en ligne, la charge de l'appliance équilibre les périphériques et envoie le trafic.
   Si le trafic entrant est chiffré, l'appliance déchiffre les données et les envoie sous forme de texte brut au périphérique en ligne pour inspection du contenu.
3. Le périphérique en ligne inspecte les données à la recherche de menaces et décide de supprimer, de réinitialiser ou de renvoyer les données à l'appliance.
4. S'il existe des menaces de sécurité, le périphérique modifie les données et les envoie à l'appliance.
5. Citrix ADC à son tour crypte à nouveau les données et transmet la demande au serveur principal.
6. Le serveur principal envoie la réponse à l'appliance Citrix ADC.
7. L'appliance déchiffre à nouveau les données et les envoie au périphérique en ligne pour inspection.
8. L'appliance crypte à nouveau les données et envoie la réponse au client

Licences logicielles

Pour déployer l'intégration de périphérique en ligne, votre appliance Citrix ADC doit être provisionné avec l'une des licences suivantes :

1. ADC Premium
2. ADC Avancé
3. Telco Advanced
4. Telco Premium
5. Licence SWG

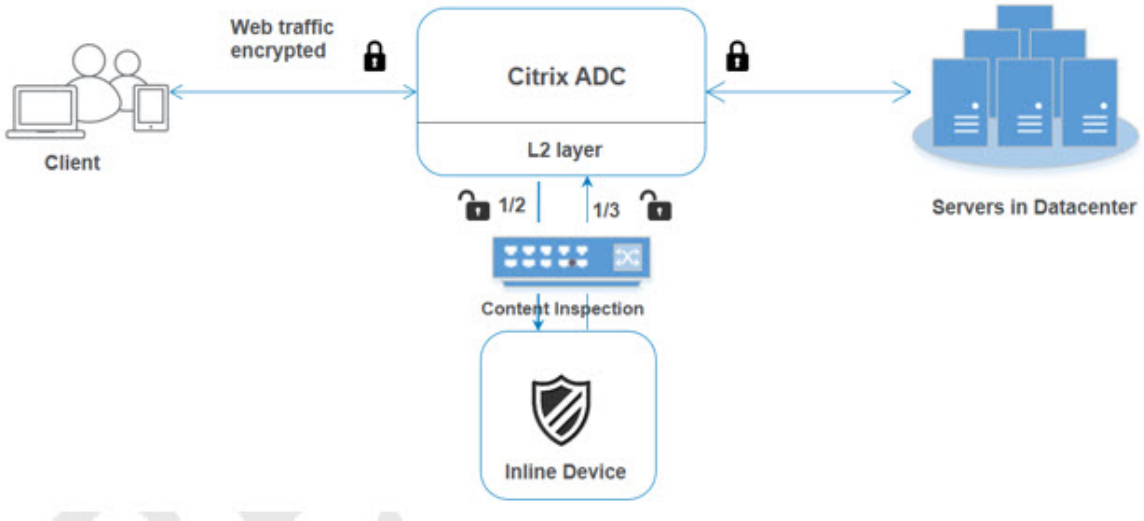
Configuration de l'intégration de périphériques en ligne

Vous pouvez configurer une appliance Citrix ADC avec un périphérique en ligne de trois manières différentes. Les scénarios de configuration sont les suivants.

Scénario 1 pour l'utilisation d'un seul périphérique en ligne

Si vous souhaitez intégrer un périphérique de sécurité (IPS ou NGFW) en mode intégré, vous devez commencer par activer la fonctionnalité d'inspection de contenu et activer Citrix ADC en MBF (transfert basé sur Mac) en mode global. Une fois que vous avez activé les fonctionnalités, vous devez

ajouter le profil Inspection du contenu, ajouter l'action Inspection du contenu pour les périphériques en ligne pour réinitialiser, bloquer ou supprimer le trafic en fonction de l'inspection. Ajoutez ensuite la stratégie d'inspection du contenu de l'appliance pour décider du sous-ensemble de trafic à envoyer aux périphériques en ligne. Ensuite, configurez le serveur virtuel d'équilibrage de charge avec la connexion de couche 2 activée sur le serveur. Enfin, liez la stratégie d'inspection de contenu au serveur virtuel d'équilibrage de charge.



Activer le mode MBF (transfert basé sur Mac)

Si vous souhaitez que l'appliance Citrix ADC soit intégrée à des périphériques en ligne tels que IPS ou pare-feu, vous devez activer ce mode. Pour plus d'informations sur MBF, consultez la rubrique Configurer le transfert basé sur Mac.

À l'invite de commandes, tapez :

```
enable ns mode mbf
```

Activer l'inspection du contenu

Si vous souhaitez que l'appliance Citrix ADC décrypte puis envoie le contenu pour inspection aux périphériques en ligne, vous devez activer les fonctionnalités d'inspection du contenu et d'équilibrage de charge.

```
enable ns feature contentInspection LoadBalancing
```

Méthode de connexion Add couche 2

Pour gérer la réponse générée par les périphériques en ligne, l'appliance utilise le canal VLAN comme méthode de couche 2 (L2ConnMethod) de communication avec les périphériques en ligne.

À l'invite de commandes, tapez :

```
set l4param -l2ConnMethod <l2ConnMethod>
```

Exemple

```
set l4param -l2ConnMethod VlanChannel
```

Ajouter un profil d'inspection de contenu pour le service

La configuration de périphérique en ligne pour une appliance Citrix ADC peut être spécifiée dans une entité appelée profil d'inspection de contenu. Le profil possède une collection de paramètres qui expliquent comment intégrer un périphérique en ligne.

À l'invite de commandes, tapez :

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface "1/2" -egressInterface "1/3"
```

Ajouter un moniteur IPS-TCP

Si vous souhaitez configurer des moniteurs, vous ajoutez un moniteur défini par l'utilisateur.
Remarque : Si vous souhaitez configurer des moniteurs, vous devez utiliser un moniteur personnalisé. Lorsque vous ajoutez un moniteur, vous devez activer le paramètre transparent.

À l'invite de commandes, tapez :

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr>] [-destPort
 <port>] [-transparent ( YES | NO )]
```

Exemple :

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

Ajouter un service

Ajoutez un service. Spécifiez une adresse IP fictive qui n'appartient à aucun des périphériques, y compris les périphériques en ligne. Définissez `use source IP address` (USIP) sur YES. Définissez `useproxyport` sur NO. Par défaut, la surveillance de l'intégrité est ACTIVÉE, lie le service à un moniteur d'intégrité et définit également l'option TRANSPARENT dans le moniteur ON. À l'invite de commandes, tapez :


```
add service <Service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor YES -usip ON -useproxyport OFF
```

Exemple :

```
add service ips_service 192.168.10.2 TCP * -healthMonitor YES -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof
```

Ajouter un moniteur de santé

Par défaut, le moniteur de santé est activé et vous avez également la possibilité de le désactiver, si nécessaire. À l'invite de commandes, tapez :

```
add lb monitor <name> TCP -destIP <ip address> -destPort 80 -transparent <
YES, NO>
```

Exemple :

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

Liez le service au moniteur de santé

Après avoir configuré le moniteur de santé, vous devez lier le service au moniteur de santé. À l'invite de commandes, tapez :

```
bind service <name> -monitorName <name>
```

Exemple :

```
bind service ips_svc -monitorName ips_tcp
```

Ajouter une action d'inspection de contenu pour le service

Après avoir activé la fonctionnalité Inspection du contenu, puis après avoir ajouté le profil et le service en ligne, vous devez ajouter l'action Inspection du contenu pour gérer la demande. En fonction de l'action d'inspection du contenu, le périphérique en ligne peut supprimer, réinitialiser ou bloquer l'action après avoir inspecté les données.

Si le serveur ou le service en ligne est en panne, vous pouvez configurer le `ifserverdown` paramètre de l'appliance pour effectuer l'une des actions suivantes.

CONTINUER : Si l'utilisateur souhaite contourner l'inspection du contenu lorsque le serveur distant est en panne, vous pouvez choisir l'action « CONTINUER », par défaut.
RESET (par défaut) : Cette action répond au client en fermant la connexion avec RST.
DROP : Cette action supprime silencieusement les paquets sans envoyer de réponse à l'utilisateur.

À l'invite de commandes, tapez :

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>] [-reqTimeout <positive_integer>] [-reqTimeoutAction
 <reqTimeoutAction>]
```

```
add ContentInspection action <action_name> -type InlineINSPECTION -serverName
 Service_name/Vserver_name>
```

Exemple :

```
add ContentInspection action <Inline_action> -type InlineSPECTION -serverName
 Inline_service1
```

Ajouter une stratégie d'inspection du contenu à des fins d'inspection

Après avoir créé une action d'inspection du contenu, vous devez ajouter des stratégies d'inspection du contenu pour évaluer les demandes d'inspection. La stratégie est basée sur une règle qui consiste en une ou plusieurs expressions. La stratégie évalue et sélectionne le trafic à inspecter en fonction de la règle.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Exemple

```
add contentInspection policy Inline_pol1 -rule true -action Inline_action
```

Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Pour recevoir le trafic Web, vous devez ajouter un serveur virtuel d'équilibrage de charge. Vous devez également activer la connexion layer2 sur le serveur virtuel.

À l'invite de commandes, tapez :

```
add lb vserver <name> <vserver name> -l2Conn ON
```

Exemple :

```
add lb vserver HTTP_vserver HTTP 10.102.29.200 8080 -l2Conn ON
```

Lier la stratégie d'inspection de contenu au serveur virtuel de commutation de contenu ou à un serveur virtuel d'équilibrage de charge de type HTTP/SSL

Vous liez le serveur virtuel d'équilibrage de charge ou le serveur virtuel de commutation de contenu de type HTTP/SSL à la stratégie d'inspection du contenu.
À l'invite de commandes, tapez ce qui suit :

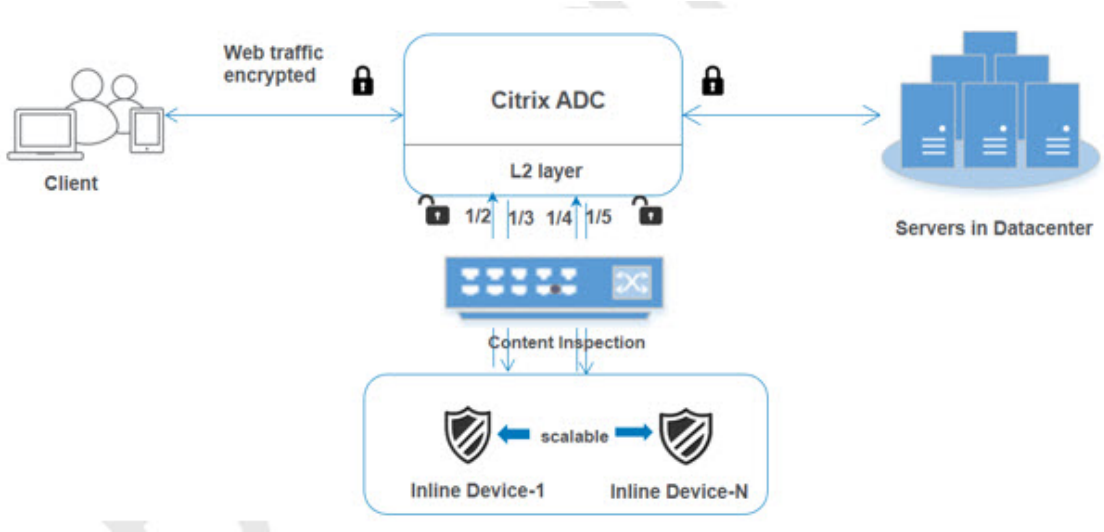
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Exemple :

```
bind lb vserver HTTP_vserver -policyName Inline_pol1 -priority 100 -type
REQUEST
```

Scénario 2 : équilibrage de charge de plusieurs périphériques en ligne à l'aide d'interfaces dédiées

Si vous utilisez au moins deux périphériques en ligne, vous devez équilibrer la charge des périphériques à l'aide de différents services d'inspection de contenu dans une configuration VLAN dédiée. Dans ce cas, la charge de l'appliance Citrix ADC équilibre les périphériques en plus de l'envoi d'un sous-ensemble de trafic à chaque périphérique via une interface dédiée.
Pour les étapes de configuration de base, reportez-vous au scénario 1.



Ajouter un profil d'inspection de contenu1 pour service1

Les configurations en ligne d'une appliance Citrix ADC peuvent être spécifiées dans une entité appelée profil d'inspection de contenu. Le profil possède une collection de paramètres de périphérique. Le profil Content Inspection 1 est créé pour le service 1 en ligne et la communication se fait par des interfaces dédiées 1/2 et 1/3.

À l'invite de commandes, tapez :


```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface "1/2" -egressInterface "1/3"
```

Ajouter un profil d'inspection de contenu2 pour service2

Le profil d'inspection du contenu2 est ajouté pour service2 et le périphérique en ligne communique avec l'appliance via 1/4 des interfaces 1/5 dédiées.
À l'invite de commandes, tapez :

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile Inline_profile2 -type InlineInspection -
ingressinterface "1/4" -egressInterface "1/5"
```

Ajouter le service 1 pour le périphérique en ligne 1

Après avoir activé la fonction d'inspection du contenu et ajouté le profil en ligne, vous devez ajouter un service en ligne 1 pour que le périphérique en ligne 1 fasse partie de la configuration d'équilibrage de charge. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commandes, tapez :

```
add service <Service_name_1> <Pvt_IP1> TCP * -contentInspectionProfileName
<Inline_Profile_1> -healthmonitor OFF -usip ON -useproxyport OFF
```

Exemple :

```
add service Inline_service1 10.102.29.200 TCP 80 -contentInspectionProfileName
 Inline_profile1 -healthmonitor OFF -usip ON -useproxyport OFF
```

Ajouter le service 2 pour le périphérique en ligne 2

Après avoir activé la fonction d'inspection du contenu et ajouté le profil en ligne, vous devez ajouter un service en ligne 2 pour le périphérique en ligne 2. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commandes, tapez :


```
add service <Service_name_1> <Pvt_IP1> TCP * -contentInspectionProfileName
<Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```

Exemple :

```
add service Inline_service1 10.29.20.205 TCP 80 -contentInspectionProfileName
 Inline_profile2 -healthmonitor OFF -usip ON -useproxyport OFF
```

Ajouter un serveur virtuel d'équilibrage de charge

Après avoir ajouté le profil en ligne et les services, vous devez ajouter un serveur virtuel d'équilibrage de charge pour l'équilibrage de charge des services.

À l'invite de commandes, tapez :

```
add lb vserver <vserver_name> TCP <Pvt_IP3> <port>
```

Exemple :

```
add lb vserver lb-Inline_vserver TCP *
```

Lier le service 1 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur virtuel d'équilibrage de charge au premier service.

À l'invite de commandes, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-Inline_vserver Inline_service1
```

Lier le service 2 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur au second service.

À l'invite de commandes, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-Inline_vserver Inline_service2
```


Ajouter une action d'inspection du contenu pour le service

Après avoir activé la fonction Inspection du contenu, vous devez ajouter l'action Inspection du contenu pour gérer les informations de demande en ligne. En fonction de l'action sélectionnée, le périphérique en ligne abandonne, réinitialise ou bloque après avoir examiné le sous-ensemble de trafic donné.

À l'invite de commandes, tapez :

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>] [-reqTimeout <positive_integer>] [-reqTimeoutAction
 <reqTimeoutAction>]
```

```
add ContentInspection action < action_name > -type InlineINSPECTION -
serverName Service_name/Vserver_name>
```

Exemple :

```
add ContentInspection action Inline_action -type InlineINSPECTION -serverName
 lb-Inline_vserver
```

Ajouter une stratégie d'inspection du contenu à des fins d'inspection

Après avoir créé une action Inspection du contenu, vous devez ajouter la stratégie d'inspection du contenu pour évaluer les demandes de service. La stratégie est basée sur une règle qui consiste en une ou plusieurs expressions. La règle est associée à l'action Inspection du contenu associée si une demande correspond à la règle.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Exemple :

```
add contentInspection policy Inline_pol1 -rule true -action Inline_action
```

Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Ajoutez un serveur virtuel de commutation de contenu ou d'équilibrage de charge pour accepter le trafic Web. Vous devez également activer la connexion layer2 sur le serveur virtuel.
Pour plus d'informations sur l'équilibrage de charge, consultez la rubrique Fonctionnement de l'équilibrage de charge.

À l'invite de commandes, tapez :

```
add lb vserver <name> <vserver name> -l2Conn ON
```


Exemple :

```
add lb vserver http_vserver HTTP 10.102.29.200 8080 -l2Conn ON
```

Lier la stratégie d'inspection de contenu pour équilibrer la charge serveur virtuel de type HTTP/SSL

Vous devez lier le serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL à la stratégie d'inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

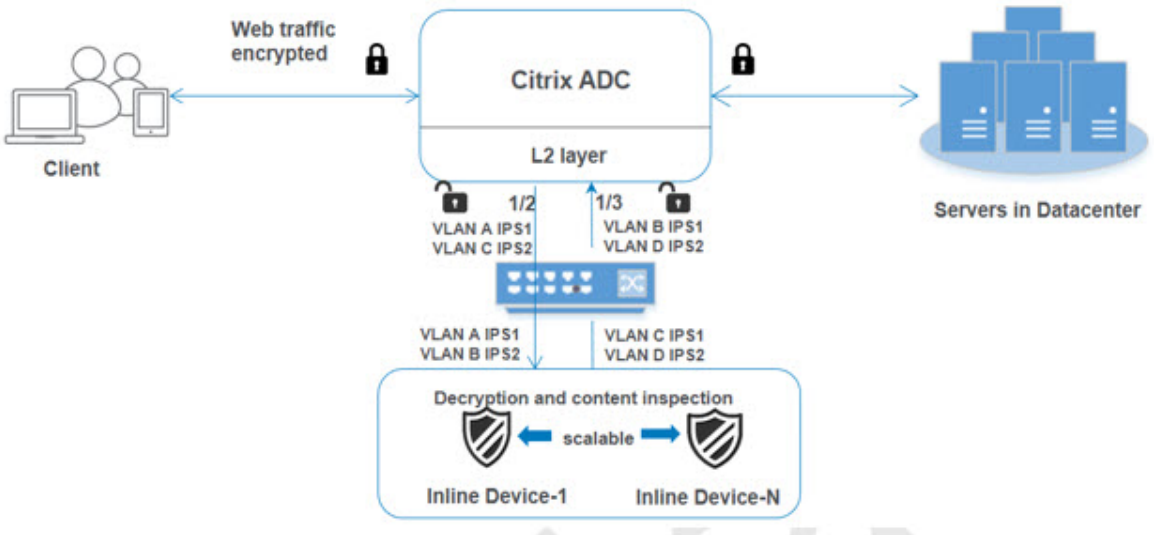
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <L7InlineREQUEST | L4Inline-REQUEST>
```

Exemple :

```
bind lb vserver http_vserver -policyName Inline_pol1 -priority 100 -type
REQUEST
```

Scénario 3 : équilibrage de charge de plusieurs périphériques en ligne à l'aide d'interfaces partagées

Vous pouvez vous référer à cette configuration si vous utilisez plusieurs périphériques en ligne et si vous souhaitez équilibrer la charge des périphériques à l'aide de différents services dans une interface VLAN partagée. Cette configuration utilisant des interfaces VLAN partagées est similaire au cas d'utilisation 2. Pour la configuration de base, reportez-vous au scénario 2.



Liaison du VLAN A avec l'option de partage activée

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> -ifnum <interface> -tagged
```

Exemple :

```
bind vlan 100 -ifnum 1/2 tagged
```

Liaison du VLAN B avec l'option de partage activée

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> -ifnum <interface> -tagged
```

Exemple :

```
bind vlan 200 -ifnum 1/3 tagged
```

Liaison VLAN C avec option de partage activée

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> -ifnum <interface> -tagged
```

Exemple :

```
bind vlan 300 -ifnum 1/2 tagged
```

Lier le VLAN D avec l'option de partage activée

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> -ifnum <interface> -tagged
```

Exemple :

```
bind vlan 400 -ifnum 1/3 tagged
```

Ajouter un profil d'inspection de contenu1 pour service1

Les configurations en ligne d'une appliance Citrix ADC peuvent être spécifiées dans une entité appelée profil d'inspection de contenu. Le profil possède une collection de paramètres de périphérique. Le profil d'inspection du contenu est créé pour le service en ligne 1 et la communication se fait via des interfaces dédiées 1/2 et 1/3.

À l'invite de commandes, tapez :

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```


Exemple :

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface “1/2” -egressInterface “1/3” -egressVlan 100 -ingressVlan
 300
```

Ajouter un profil d’inspection de contenu2 pour service2

Le profil d’inspection du contenu2 est ajouté pour service2 et le périphérique en ligne communique avec l’appliance via `1/2` des interfaces `1/3` dédiées.

À l’invite de commandes, tapez :

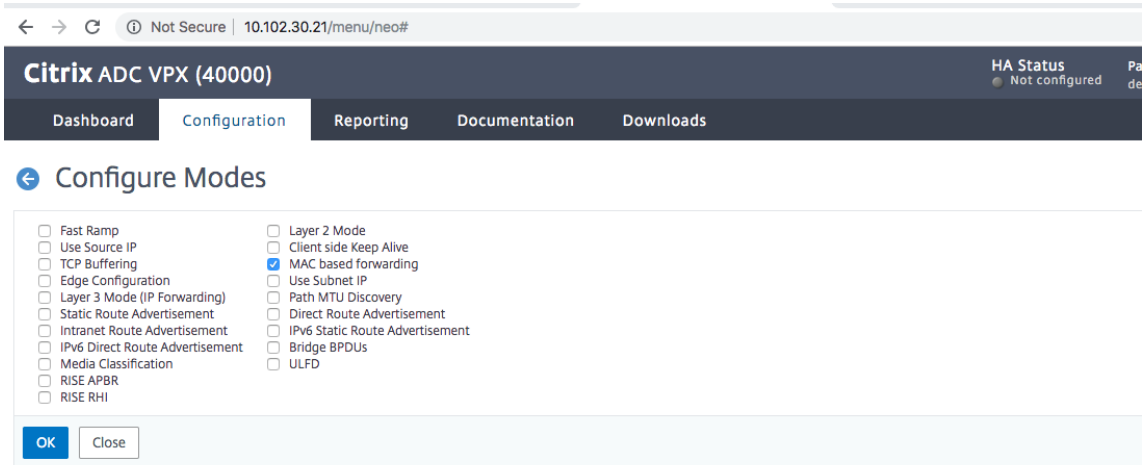
```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

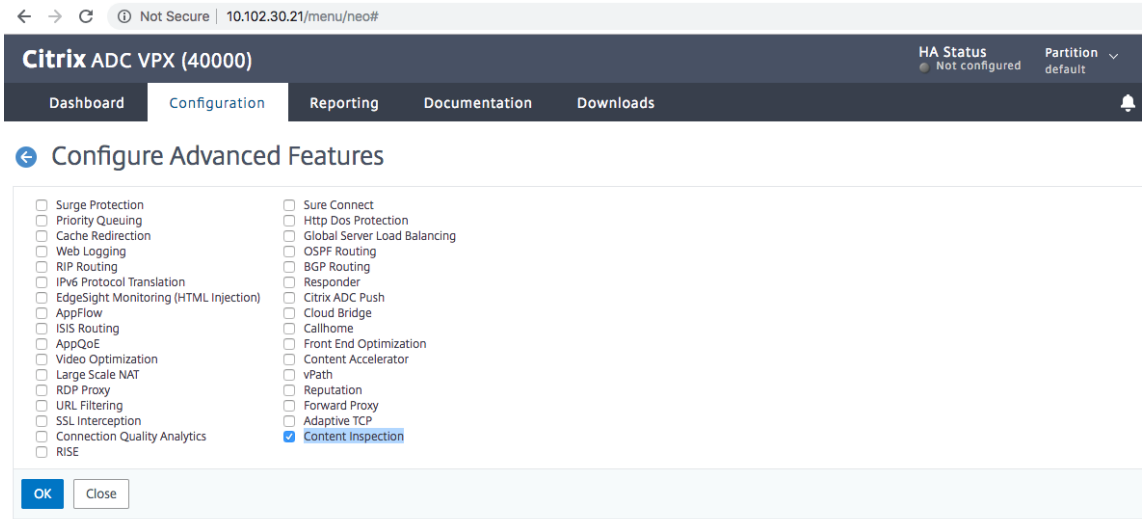
```
add contentInspection profile Inline_profile2 -type InlineInspection -
ingressinterface “1/2” -egressInterface “1/3” -egressVlan 200 -ingressVlan
 400
```

Configurer l’intégration de service en ligne à l’aide de l’interface graphique Citrix ADC

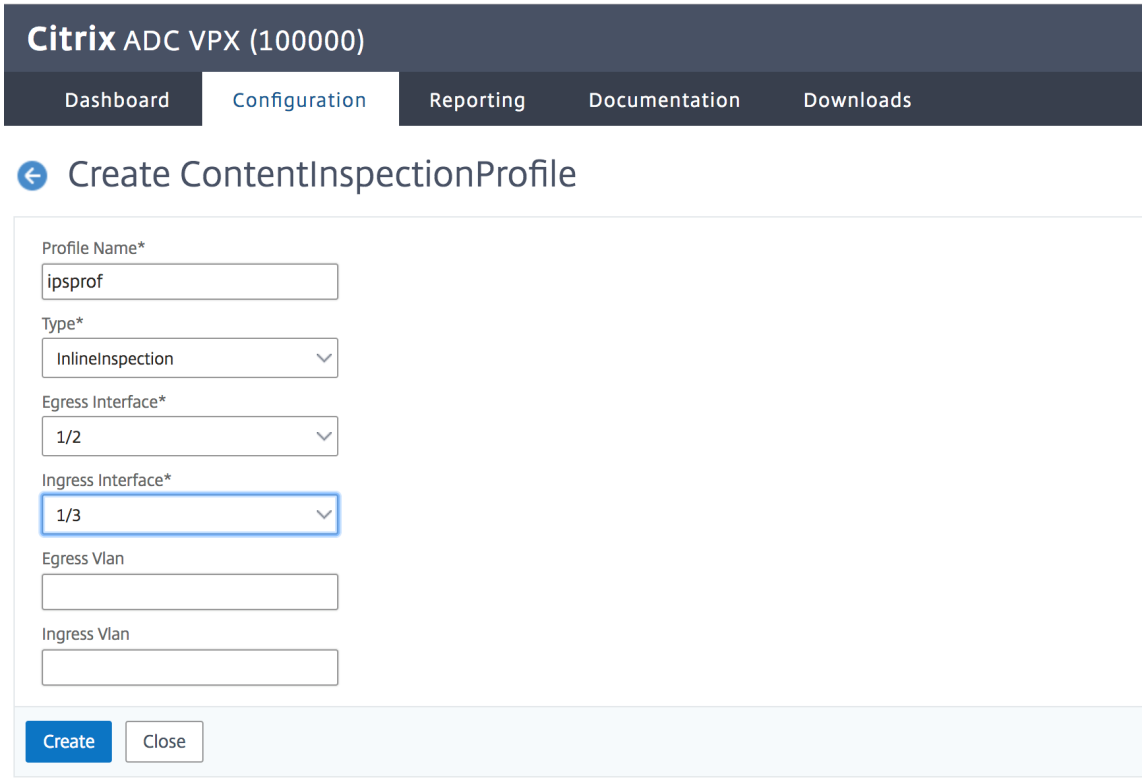
1. Ouvrez une session sur l’appliance Citrix ADC et accédez à la page **de l’onglet Configuration** .
2. Accédez à **Système** > **Paramètres** > **Configurer les modes** .
3. Dans la page **Configurer les modes**, sélectionnez **Transfert basé sur Mac** .
4. Cliquez sur **OK** et **Fermer**.



5. Accédez à **Système** > **Paramètres** > **Configurer les fonctionnalités avancées** .
6. Dans la page **Configurer la fonctionnalité avancée**, sélectionnez **Inspection du contenu** .
7. Cliquez sur **OK** et **Fermer**.

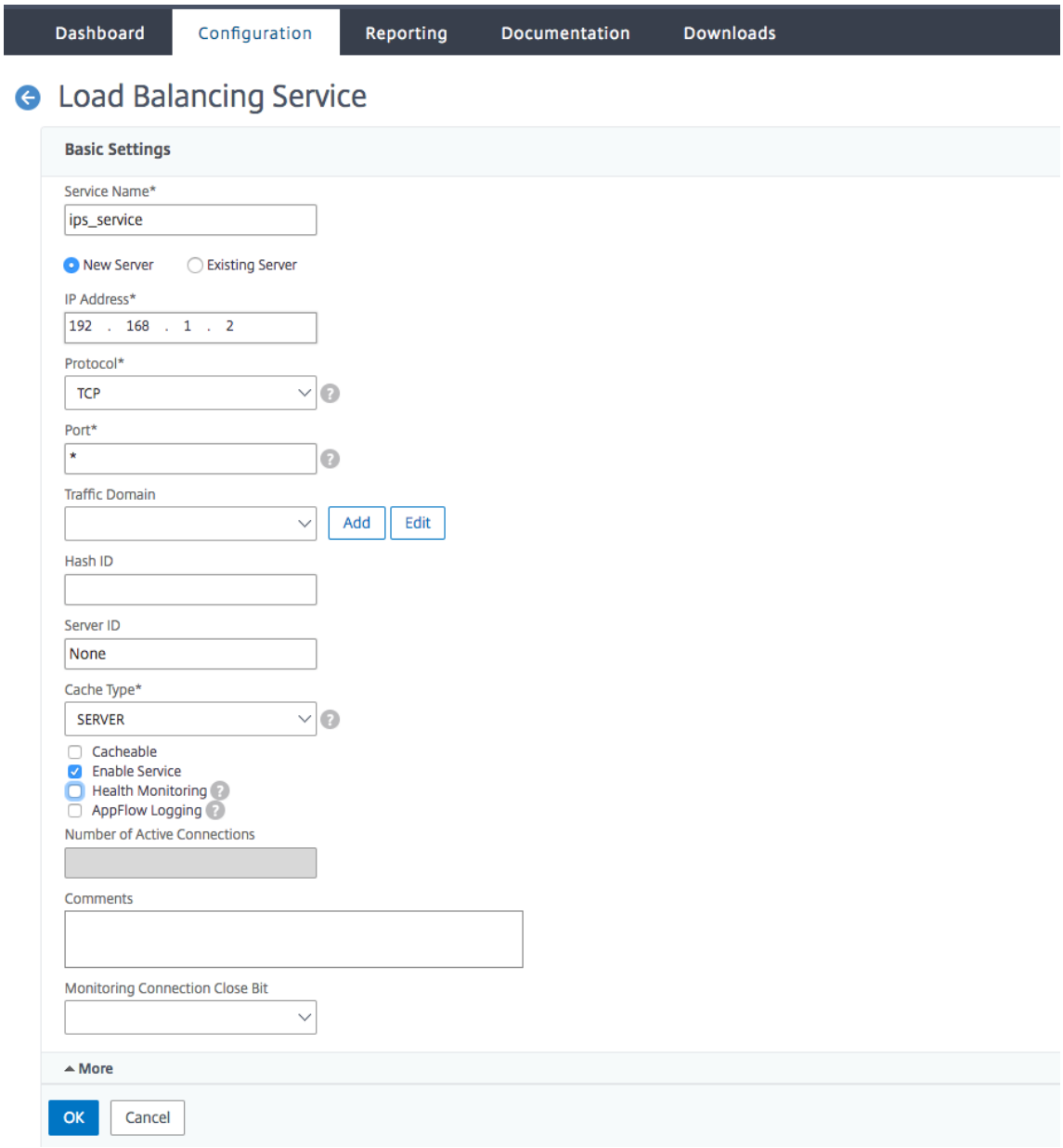


8. Accédez à **Sécurité** > **Inspection du contenu** > **Profils ContentInspection** .
9. Dans la page **Profils ContentInspection**, cliquez sur **Ajouter** .
10. Dans la page **Créer des profils ContentInspection**, définissez les paramètres suivants.
    a) Nom du profil. Nom du profil d'inspection du contenu.
    b) Type. Sélectionnez le type de profil en tant que InlineInspection.
    c) Interface de sortie. Interface par laquelle l'appliance envoie le trafic depuis Citrix ADC vers le périphérique en ligne.
    d) Interface d'entrée. Interface par laquelle l'appliance reçoit le trafic du périphérique en ligne vers Citrix ADC.
    e) VLAN de sortie. ID de VLAN d'interface via lequel le trafic est envoyé au périphérique Inline.
    f) Insertion du VLAN. ID de VLAN d'interface via lequel l'appliance reçoit du trafic d'Inline vers Citrix ADC (si elle est configurée).



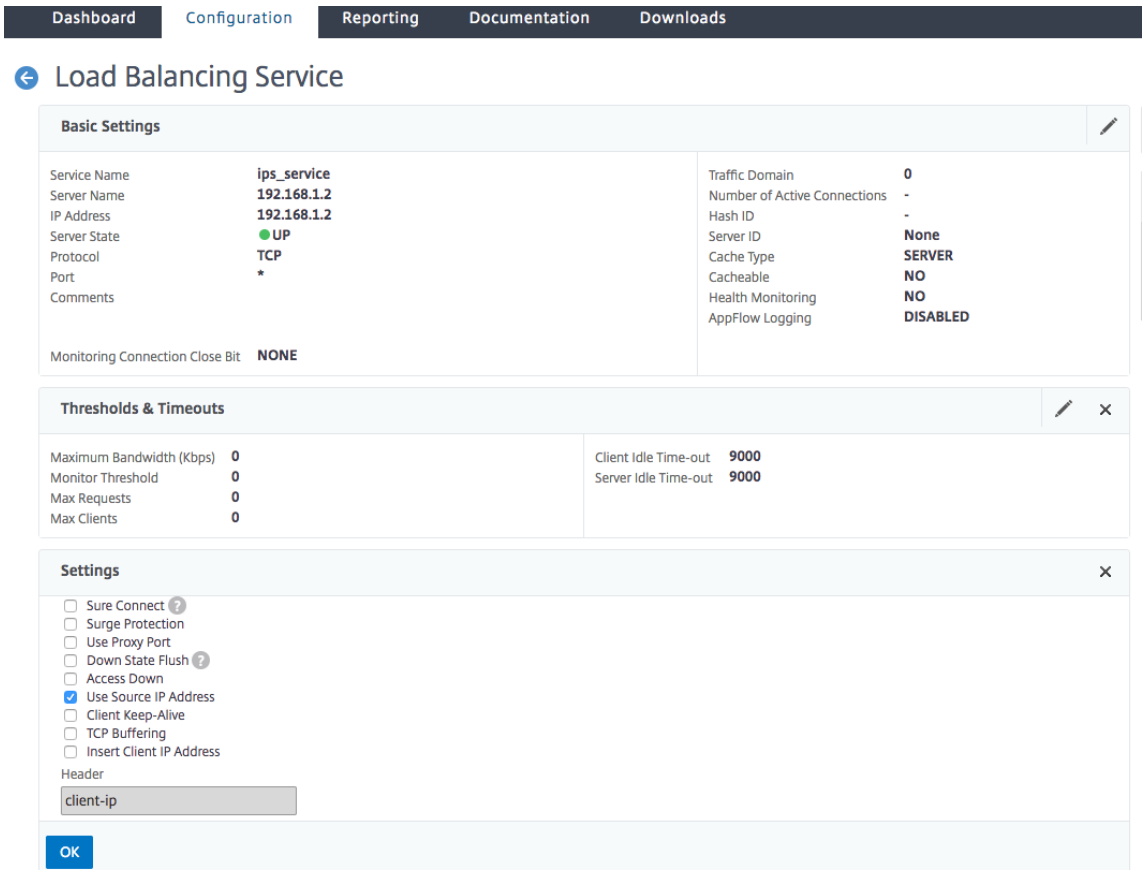
11. Cliquez sur **Créer** et **Fermer**.
12. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
13. Dans la page **Services**, définissez les paramètres suivants :
    a) Nom du service. Nom du service d'équilibrage de charge.
    b) Adresse IP. Utilisez une adresse IP factice. Remarque : Aucun périphérique ne doit posséder l'adresse IP.

c) Protocole. Sélectionnez le type de protocole comme TCP.
d) Port. Entrez *
e) Surveillance de la santé. Désactivez cette option et activez cette option uniquement si vous souhaitez lier le service au moniteur de type TCP. Si vous voulez lier un moniteur au service, l' TRANSPARENT option dans le moniteur doit être ACTIVÉE. Reportez-vous à l'étape 14 pour savoir comment ajouter un moniteur et comment le lier au service.
f) Cliquez sur **OK**.

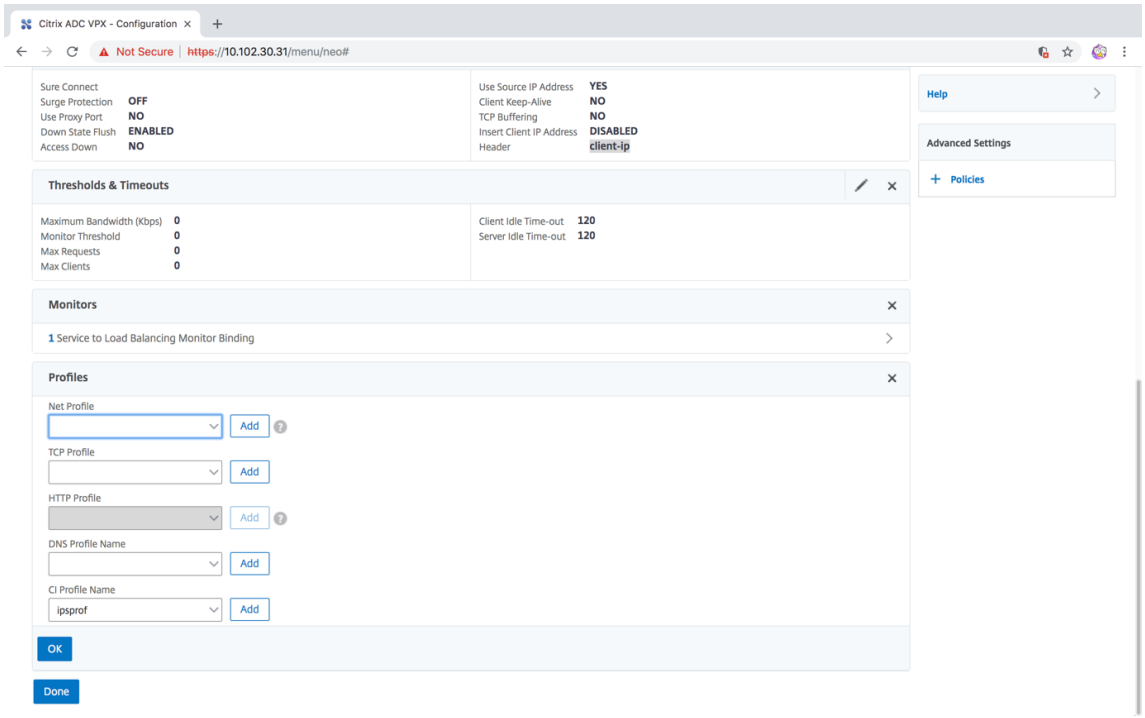


14. Dans la section **Paramètres**, modifiez les éléments suivants et cliquez sur **OK**.

a) Utiliser le port proxy : l'éteindre
b) Utiliser l'adresse IP source : Activer



15. Dans la section **Paramètres avancés**, cliquez sur **Profils**.
16. Accédez à la section **Profils**, ajoutez le profil d'inspection de contenu en ligne et cliquez sur **OK**.

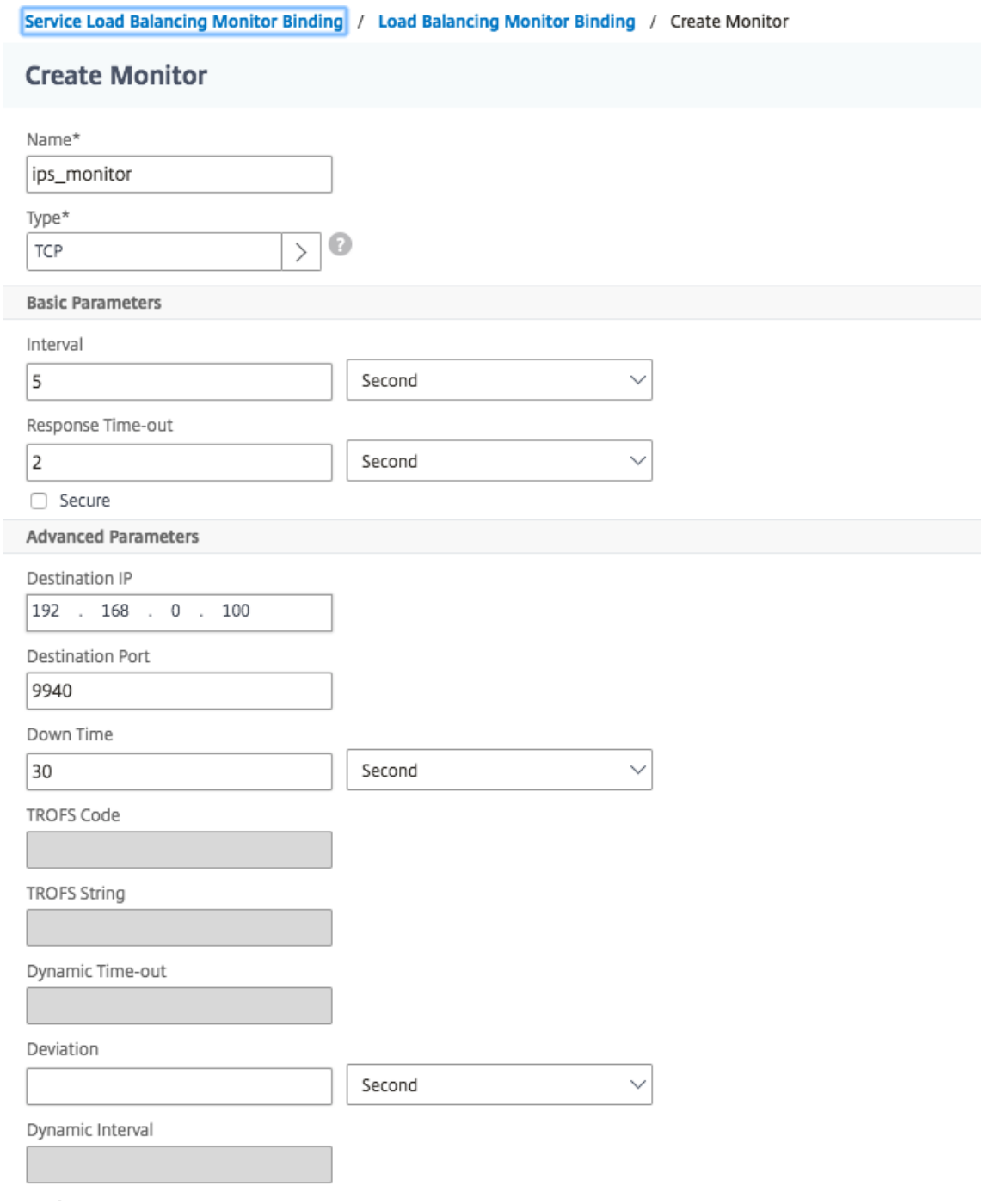


17. Accédez à la section **Moniteurs**, **Ajouter des liaisons** > **Sélectionnez Moniteur** > **Ajouter**.

    a) Nom : Nom du moniteur
    b) Type : Sélectionnez le type TCP
    c) IP de destination, PORT : adresse IP de destination et port.
    d) Transparent : Activer

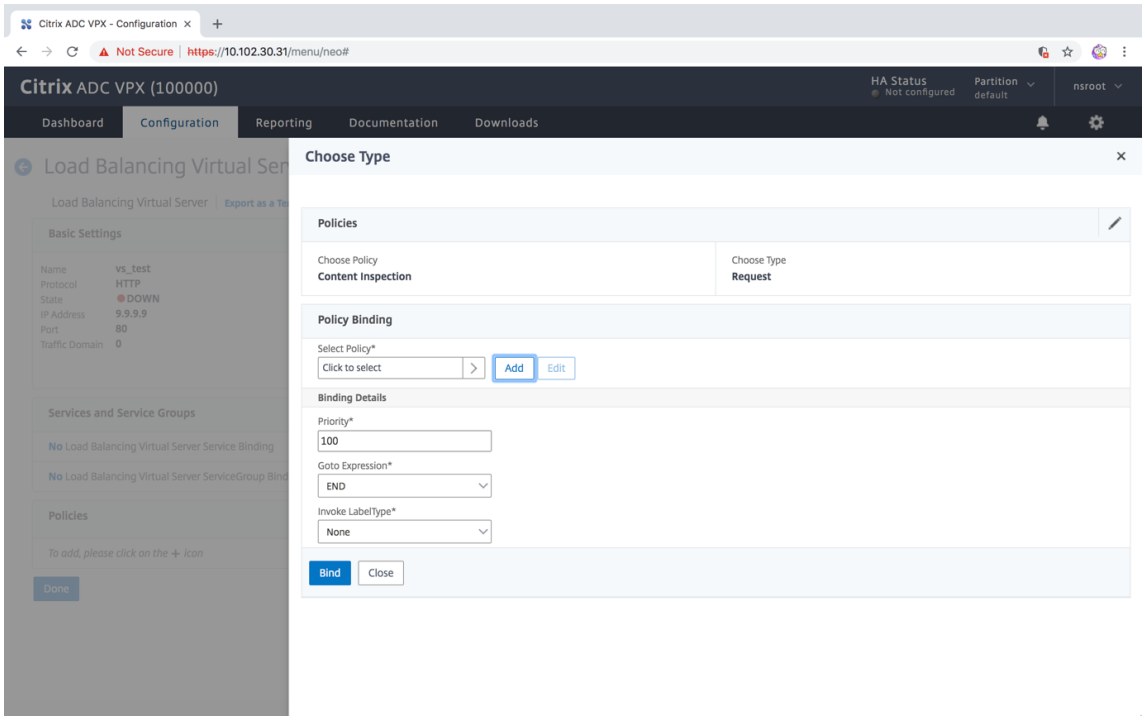
    Remarque : Les paquets de surveillance doivent circuler à travers le périphérique en ligne pour surveiller l'état du périphérique en ligne.

18. Cliquez sur **Créer**.

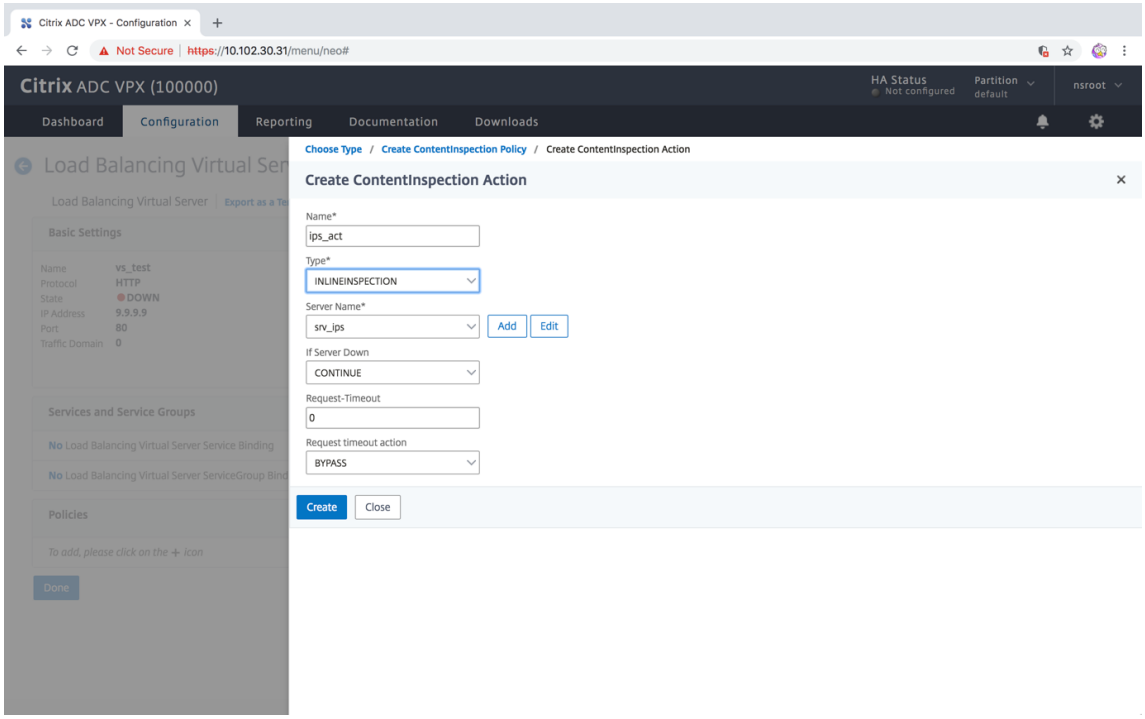


19. Cliquez sur **Terminé**.
20. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**. Ajoutez un serveur virtuel de type HTTP ou SSL.
21. Après avoir entré les détails du serveur, cliquez sur **OK** et à nouveau sur **OK**.
22. Dans la section **Paramètres de trafic** du serveur virtuel d'équilibrage de charge, activez les paramètres de couche 2.

23. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
24. Allez dans la section **Stratégies** et cliquez sur l'icône « + » pour configurer la stratégie d'inspection du contenu.
25. Sur la page **Choisir une stratégie**, sélectionnez Inspection du contenu. Cliquez sur **Continuer**.
26. Dans la section **Liaison de stratégie**, cliquez sur **Ajouter** pour ajouter une stratégie d'inspection du contenu.



27. Dans la page **Créer une stratégie ContentInspection**, entrez un nom pour la stratégie d'inspection du contenu en ligne.
28. Dans le champ **Action**, cliquez sur **Ajouter** pour créer une action d'inspection de contenu en ligne.
29. Dans la page **Créer une action CI**, définissez les paramètres suivants :
    a) Nom. Nom de la stratégie Inline d'inspection du contenu.
    b) Type. Sélectionnez le type en tant que InlineInspection.
    c) Serveur. Sélectionnez le serveur/service en tant que périphériques Inline.
    d) Si le serveur est hors service. Sélectionnez une opération si le serveur tombe en panne.
    e) Demander le délai d'expiration. Sélectionnez une valeur de délai d'expiration. Vous pouvez utiliser des valeurs par défaut.
    f) Demander une action de délai d'expiration. Sélectionnez une action de délai d'expiration. Vous pouvez utiliser des valeurs par défaut.
30. Cliquez sur **Créer**.



31. Cliquez sur **Créer**.
32. Dans la page **Créer une stratégie CI**, entrez d'autres détails :
33. Cliquez sur **OK** et **Fermer**.

Intégration avec IPS ou NGFW en tant que périphériques en ligne à l'aide du proxy de transfert SSL

August 20, 2021

Les dispositifs de sécurité tels que le système de prévention des intrusions (IPS) et le pare-feu de nouvelle génération (NGFW) protègent les serveurs contre les attaques réseau. Ces périphériques peuvent inspecter le trafic en direct et sont généralement déployés en mode Inline de couche 2. L'appliance proxy de transfert SSL assure la sécurité des utilisateurs et du réseau d'entreprise lors de l'accès aux ressources sur Internet.

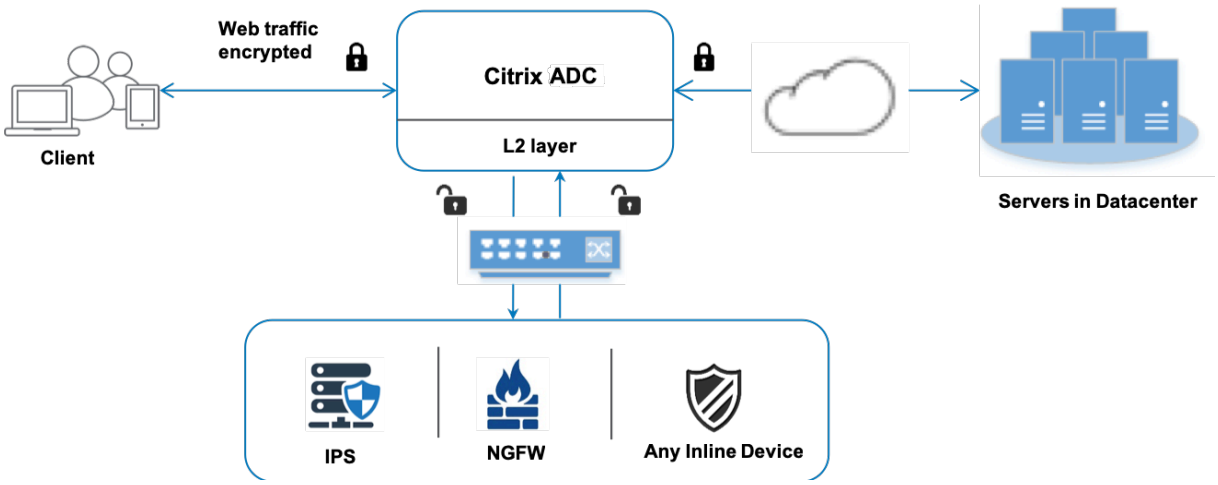
Une appliance proxy de transfert SSL peut être intégrée à un ou plusieurs périphériques en ligne pour prévenir les menaces et fournir une protection de sécurité avancée. Les périphériques en ligne peuvent être n'importe quel périphérique de sécurité, tel que IPS et NGFW.

Certains cas d'utilisation dans lesquels vous pouvez tirer parti de l'appliance proxy de transfert SSL et de l'intégration de périphériques en ligne sont les suivants :

- **Inspection du trafic chiffré :** la plupart des appliances IPS et NGFW contournent le trafic chiffré, ce qui peut rendre les serveurs vulnérables aux attaques. Une appliance proxy de transfert SSL peut déchiffrer le trafic et l'envoyer aux périphériques en ligne pour inspection. Cette intégration améliore la sécurité réseau du client.
- **Déchargement des périphériques en ligne du traitement TLS/SSL : le traitement** TLS/SSL est coûteux, ce qui peut entraîner une utilisation élevée du processeur dans les appliances IPS ou NGFW s'ils décryptent également le trafic. Une appliance proxy de transfert SSL aide à décharger le traitement TLS/SSL des périphériques en ligne. Par conséquent, les appareils en ligne peuvent inspecter un volume plus élevé de trafic.
- **Chargement des périphériques en ligne d'équilibrage :** si vous avez configuré plusieurs périphériques en ligne pour gérer le trafic lourd, un dispositif proxy de transfert SSL peut équilibrer la charge et répartir le trafic uniformément vers ces périphériques.
- **Sélection intelligente du trafic :** au lieu d'envoyer tout le trafic au périphérique en ligne pour inspection, l'appliance effectue une sélection intelligente du trafic. Par exemple, il ignore l'envoi de fichiers texte pour inspection aux périphériques en ligne.

Intégration par proxy SSL avec des périphériques en ligne

Le diagramme suivant montre comment un proxy de transfert SSL est intégré aux périphériques de sécurité en ligne.



Lorsque vous intégrez des périphériques en ligne à l'appliance proxy de transfert SSL, les composants interagissent comme suit :

1. Un client envoie une requête à un dispositif proxy de transfert SSL.
2. L'appliance envoie les données au périphérique en ligne pour inspection du contenu en fonction de l'évaluation de la stratégie. Pour le trafic HTTPS, l'appliance décrypte les données et les envoie en texte brut au périphérique en ligne pour inspection du contenu.

> **Remarque**
>
> S'il y a au moins deux périphériques en ligne, la charge de l'appliance équilibre les périphériques et envoie le trafic.

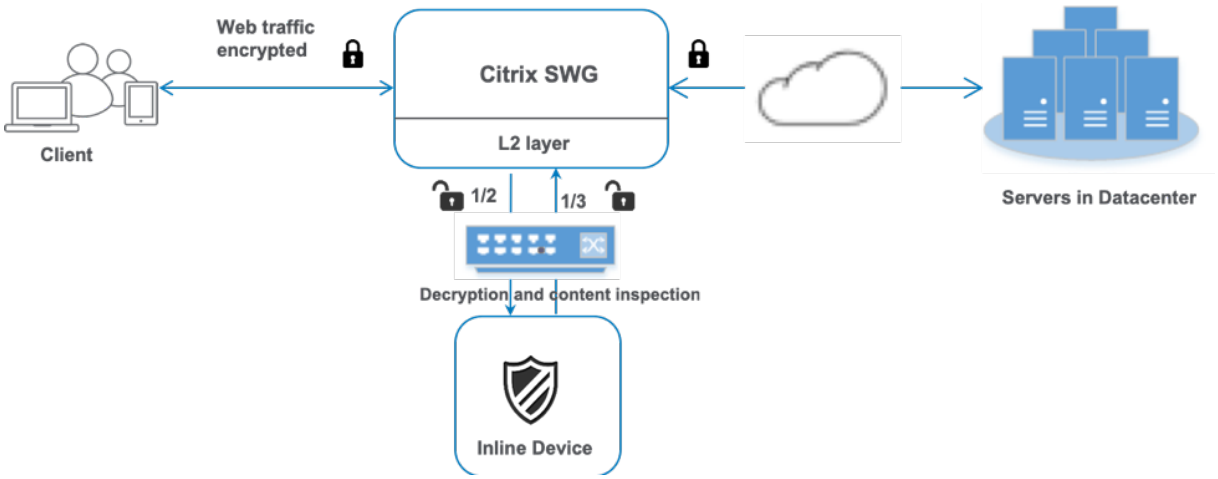
3. Ajoutez une commutation de contenu ou un serveur virtuel d'équilibrage de charge HTTP/HTTPS.
4. Le périphérique en ligne inspecte les données à la recherche de menaces et décide de supprimer, de réinitialiser ou de renvoyer les données à l'appliance.
5. S'il existe des menaces de sécurité, le périphérique modifie les données et les envoie à l'appliance.
6. Pour le trafic HTTPS, l'appliance chiffre à nouveau les données et transmet la demande au serveur principal.
7. Le serveur principal envoie la réponse à l'appliance.
8. L'appliance déchiffre à nouveau les données et les envoie au périphérique en ligne pour inspection.
9. Le périphérique en ligne inspecte les données. S'il existe des menaces de sécurité, le périphérique modifie les données et les envoie à l'appliance.
10. L'appliance recrypte les données et envoie la réponse au client.

Configuration de l'intégration de périphériques en ligne

Vous pouvez configurer une appliance proxy de transfert SSL avec un périphérique en ligne de trois manières différentes :

Scénario 1 : Utilisation d'un seul périphérique en ligne

Pour intégrer un périphérique de sécurité (IPS ou NGFW) en mode Inline, vous devez activer l'inspection du contenu et le transfert basé sur Mac (MBF) en mode global sur l'appliance proxy SSL. Ensuite, ajoutez un profil d'inspection de contenu, un service TCP, une action d'inspection de contenu pour les périphériques en ligne pour réinitialiser, bloquer ou supprimer le trafic basé sur l'inspection. Ajoutez également une stratégie d'inspection du contenu utilisée par l'appliance pour décider du sous-ensemble de trafic à envoyer aux périphériques en ligne. Enfin, configurez le serveur virtuel proxy avec la connexion de couche 2 activée sur le serveur et liez la stratégie d'inspection de contenu à ce serveur virtuel proxy.



Procédez comme suit :

1. Activer le mode de transfert basé sur Mac (MPF).
2. Activez la fonction d'inspection du contenu.
3. Ajoutez un profil d'inspection de contenu pour le service. Le profil d'inspection du contenu contient les paramètres de périphérique en ligne qui intègrent le dispositif proxy SSL à un périphérique en ligne.
4. (Facultatif) Ajoutez un moniteur TCP.

   > **Remarque :**
   >
   > Les périphériques transparents n'ont pas d'adresse IP. Par conséquent, pour effectuer des vérifications de l'état, vous devez lier explicitement un moniteur.

5. Ajoutez un service. Un service représente un périphérique en ligne.
6. (Facultatif) Liez le service au moniteur TCP.
7. Ajoutez une action d'inspection du contenu pour le service.
8. Ajoutez une stratégie d'inspection du contenu et spécifiez l'action.
9. Ajoutez un serveur virtuel proxy HTTP ou HTTPS (commutation de contenu).
10. Liez la stratégie d'inspection de contenu au serveur virtuel.

Configurer à l'aide de la CLI

Tapez les commandes suivantes à l'invite de commandes. Des exemples sont donnés après la plupart des commandes.

1. Activez MBF.

```
enable ns mode mbf
```


1. Activez la fonctionnalité.

```
enable ns feature contentInspection
```

1. Ajouter un profil d'inspection de contenu.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile ipsprof -type InlineInspection -ingressinterface
 "1/2" -egressInterface "1/3"
```

1. Ajoutez un service. Spécifiez une adresse IP fictive qui n'appartient à aucun des périphériques, y compris les périphériques en ligne. Définissez `use source IP address` (USIP) sur YES. Définissez `useproxyport` sur NO. Par défaut, la surveillance de l'intégrité est ACTIVÉE, lie le service à un moniteur d'intégrité et définit également l'option TRANSPARENT dans le moniteur ON.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor YES -usip YES -useproxyport NO
```

Exemple :

```
add service ips_service 198.51.100.2 TCP * -healthMonitor YES -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof
```

1. Ajoutez un moniteur de santé. Par défaut, le moniteur de santé est activé et vous avez également la possibilité de le désactiver, si nécessaire. À l'invite de commandes, tapez :

   ```
   add lb monitor <name> TCP -destIP <ip address> -destPort 80 -transparent
    <YES, NO>
   ```

Exemple :

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

1. Liez le service au moniteur de santé

Après avoir configuré le moniteur de santé, vous devez lier le service au moniteur de santé. À l'invite de commandes, tapez :

```
bind service <name> -monitorName <name>
```

Exemple :

```
bind service ips_svc -monitorName ips_tcp
```

1. Ajoutez une action d'inspection du contenu.


```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Exemple :

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
ips_service
```

1. Ajoutez une stratégie d'inspection du contenu.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Exemple :

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Ajoutez un serveur virtuel proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -cltTimeout <secs> -Listenpolicy
 <expression> -authn401 ( ON | OFF )-authnVsName <string> -l2Conn ON
```

> **Remarque :**
>
> Les serveurs virtuels d'équilibrage de charge de type HTTP/SSL sont également pris en charge.

Exemple :

```
add cs vserver transparentcs PROXY * * -cltTimeout 180 -Listenpolicy exp1 -
authn401 on -authnVsName swg-auth-vs-trans-http -l2Conn ON
```

1. Liez la stratégie au serveur virtuel.

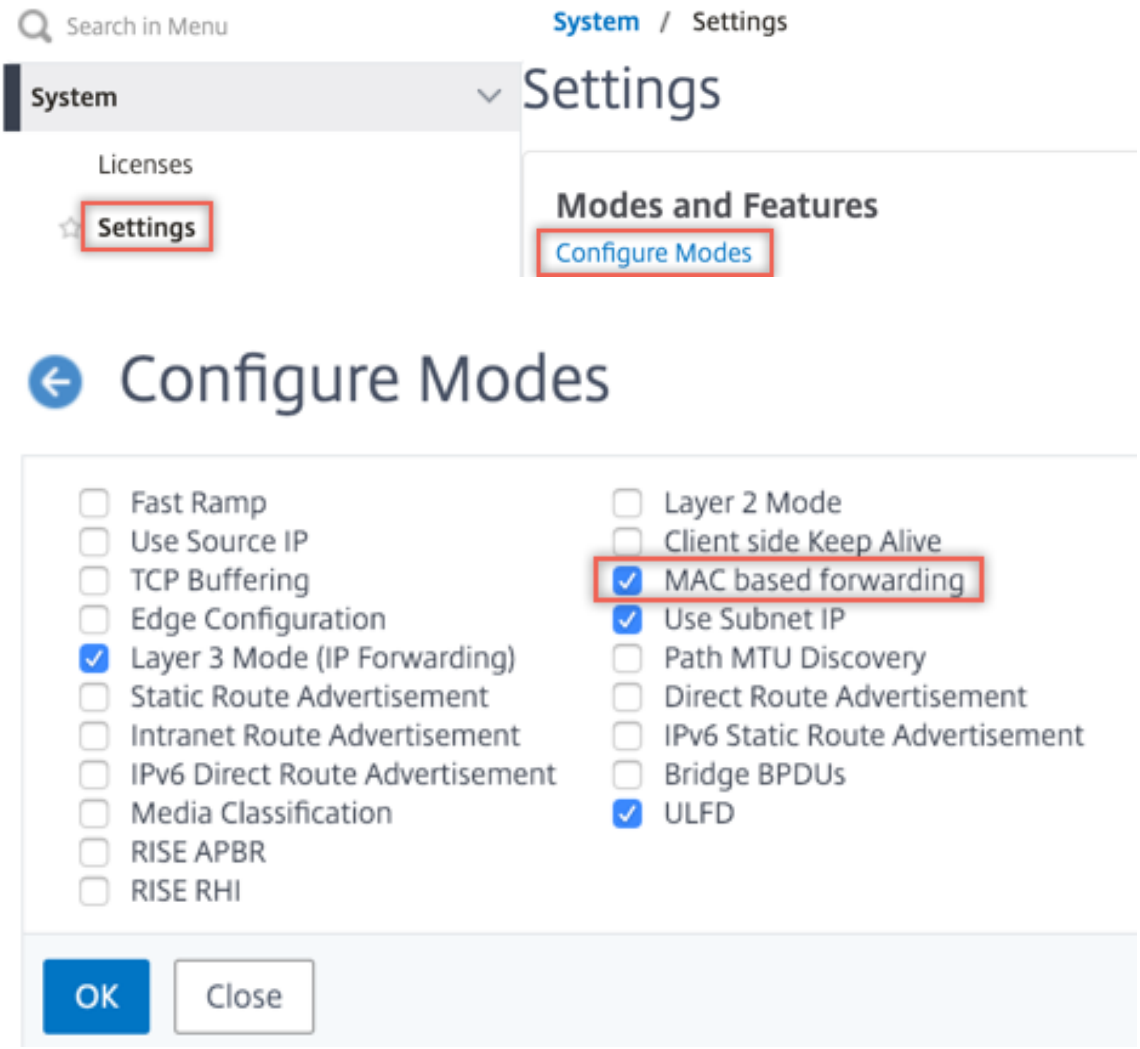
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Exemple :

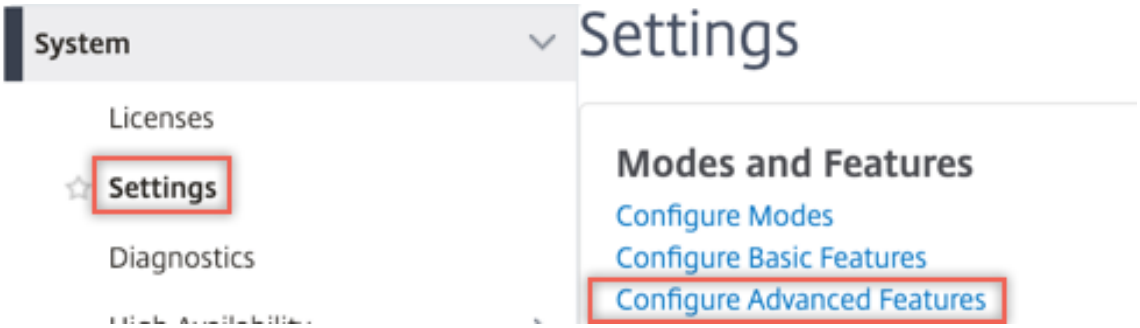
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

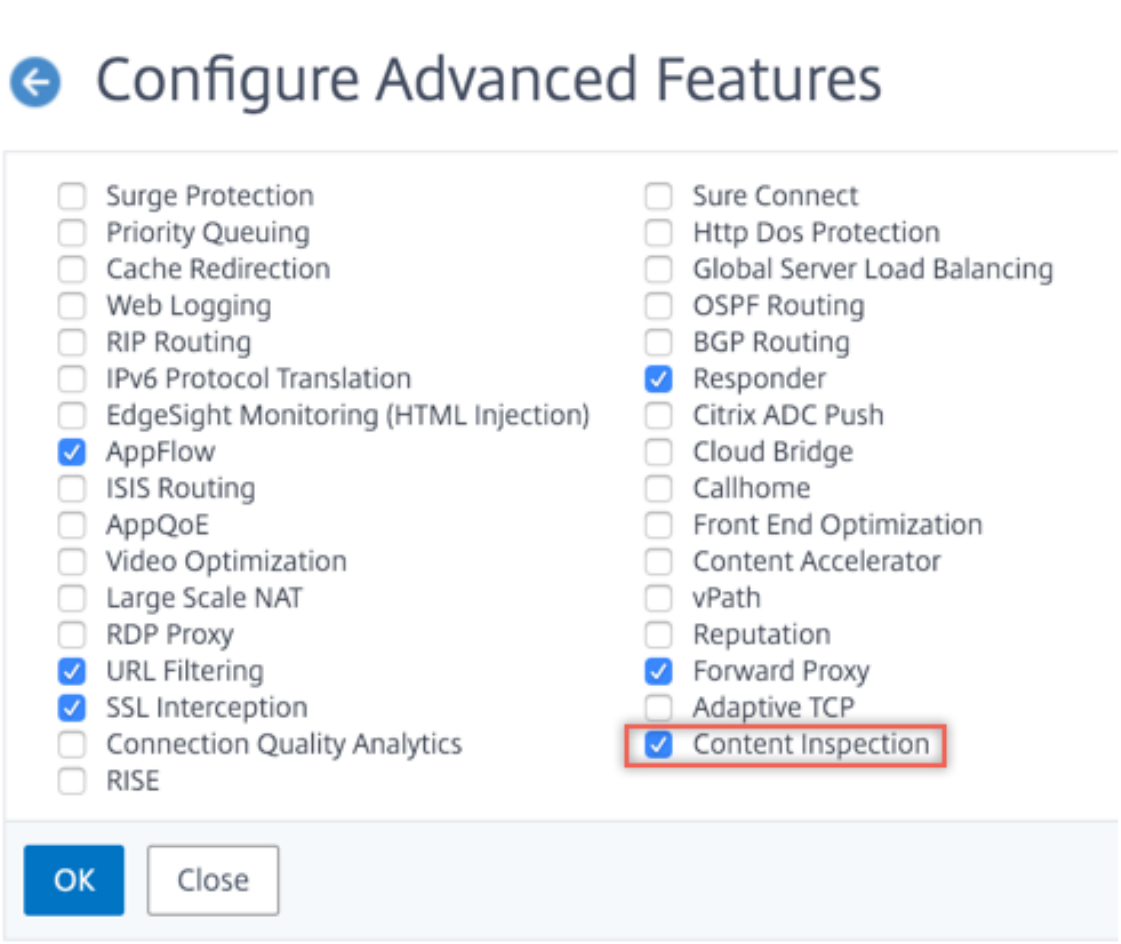
Configurer à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.

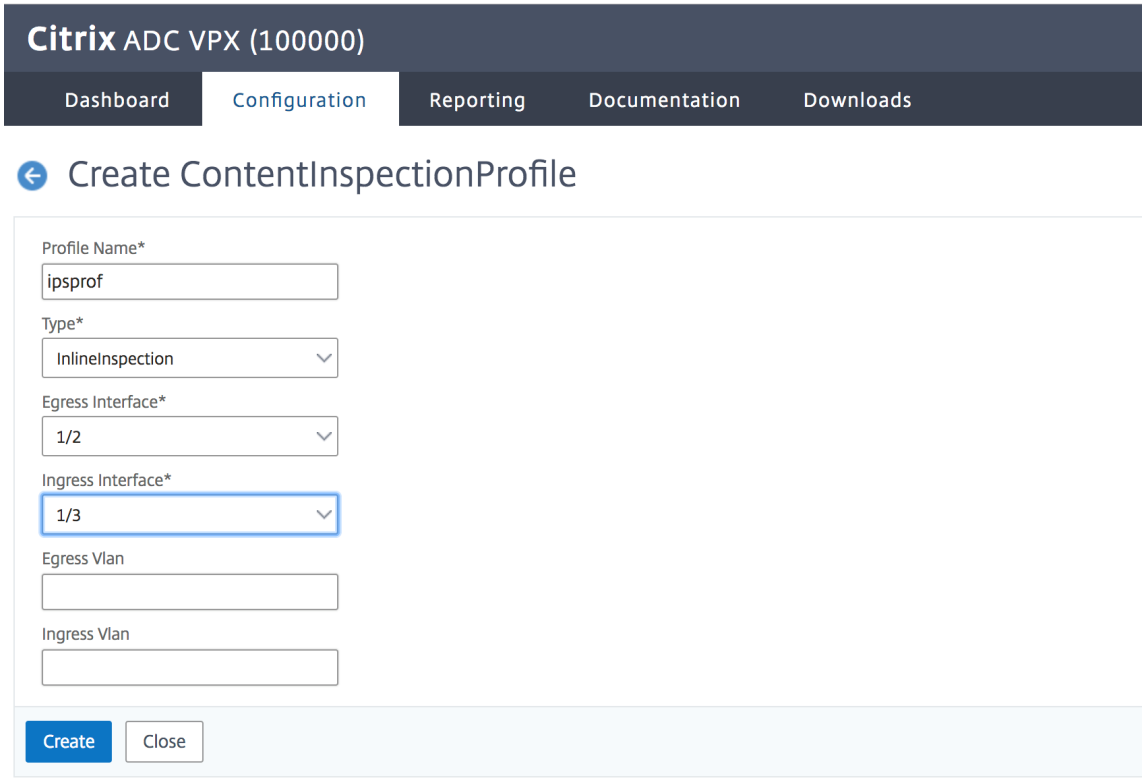


2. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.

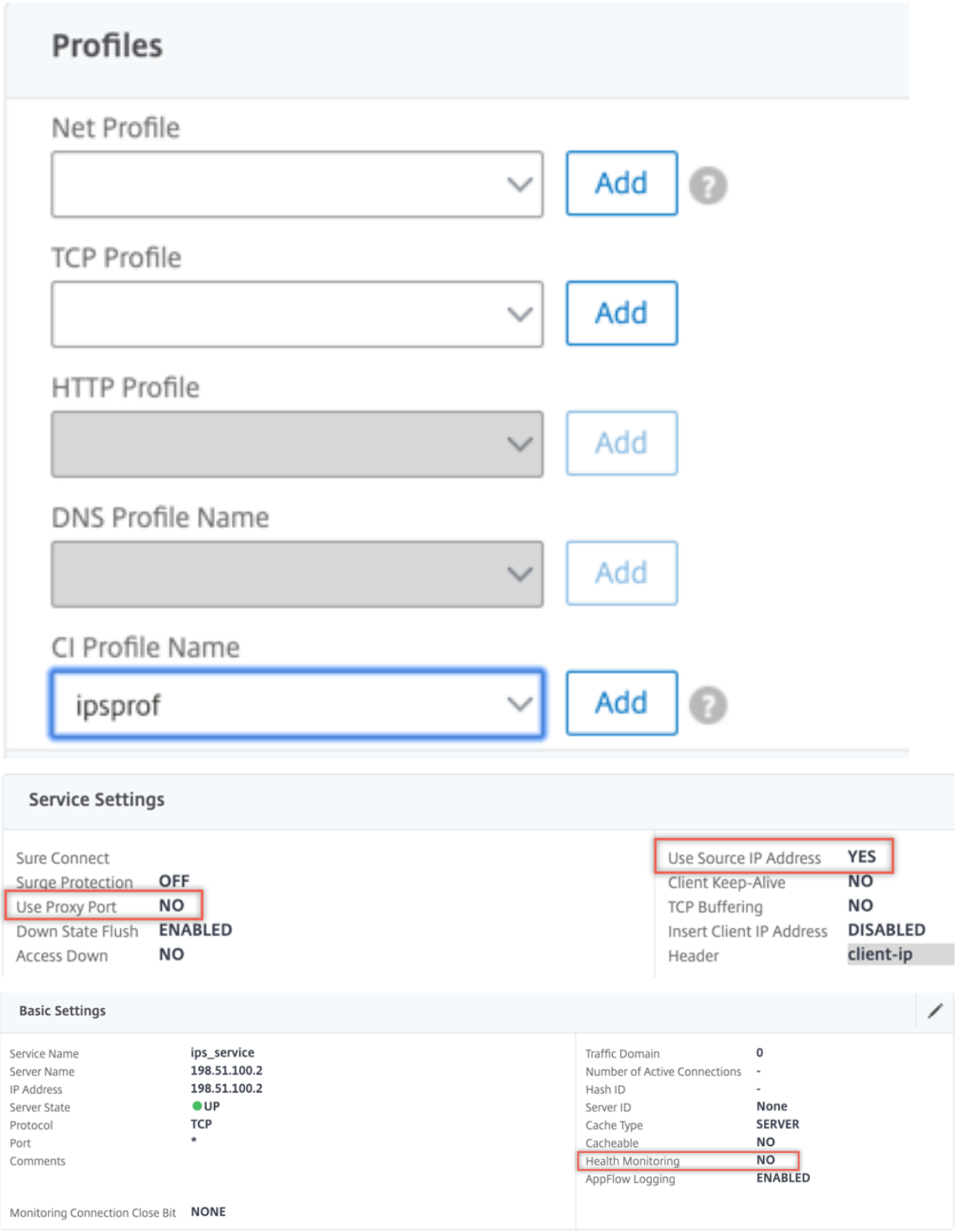




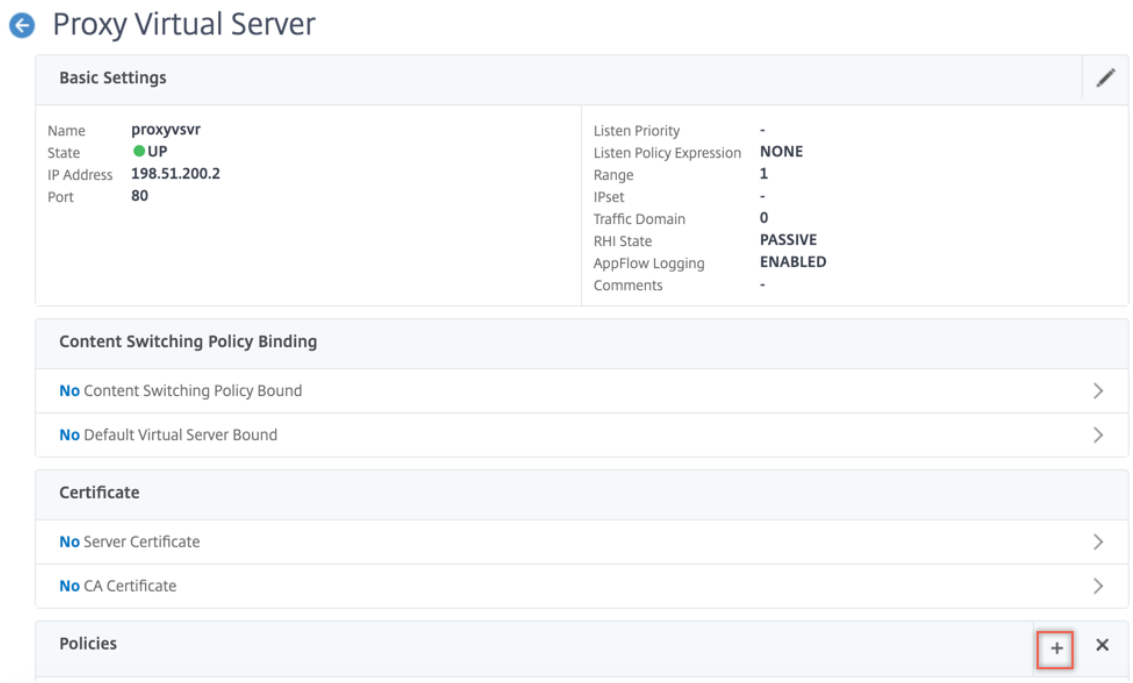
3. Accédez à **Secure Web Gateway > Inspection du contenu > Profils d'inspection du contenu**. Cliquez sur **Ajouter**.



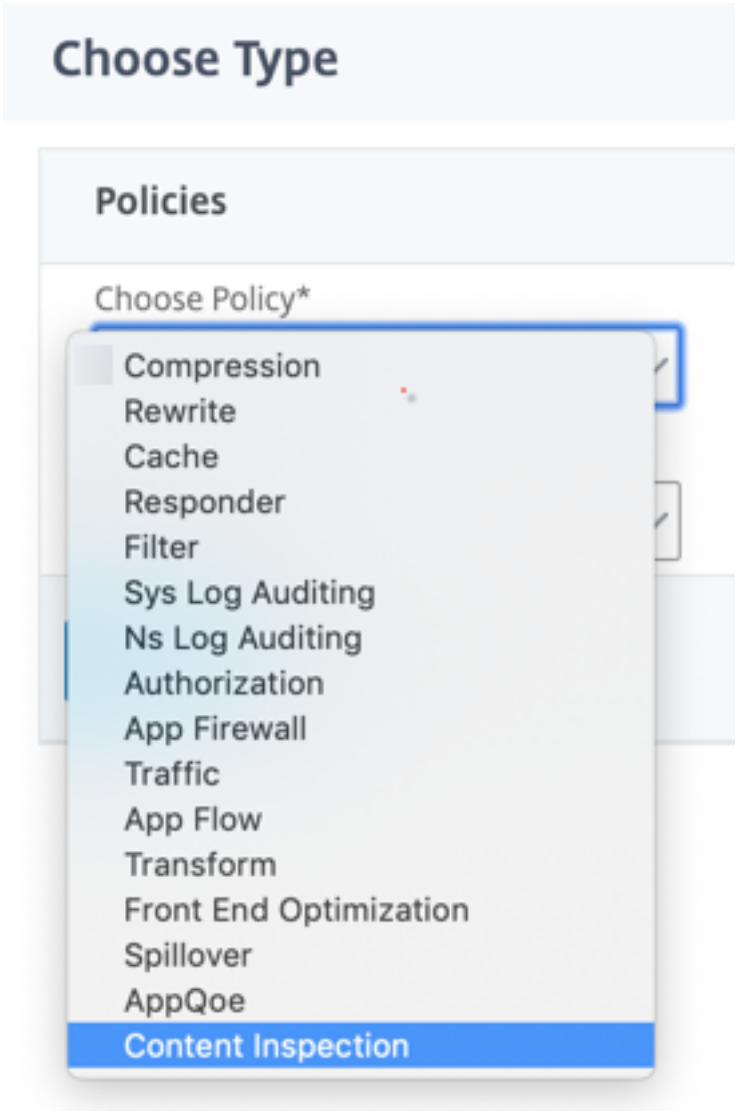
4. Accédez à **Équilibrage de charge > Services > Ajouter** et ajouter un service. Dans **Paramètres avancés**, cliquez sur **Profils**. Dans la liste **Nom du profil CI**, sélectionnez le profil d'inspection du contenu créé précédemment. Dans **Paramètres de service**, définissez **Utiliser l'adresse IP source**sur YES et **Utiliser le port proxy**sur Non. Dans **Paramètres de base**, définissez le **contrôle de l'intégrité** sur NO. Activez la surveillance de l'intégrité uniquement si vous liez ce service à un moniteur TCP. Si vous liez un moniteur à un service, définissez l'option TRANSPARENT du moniteur sur ON.



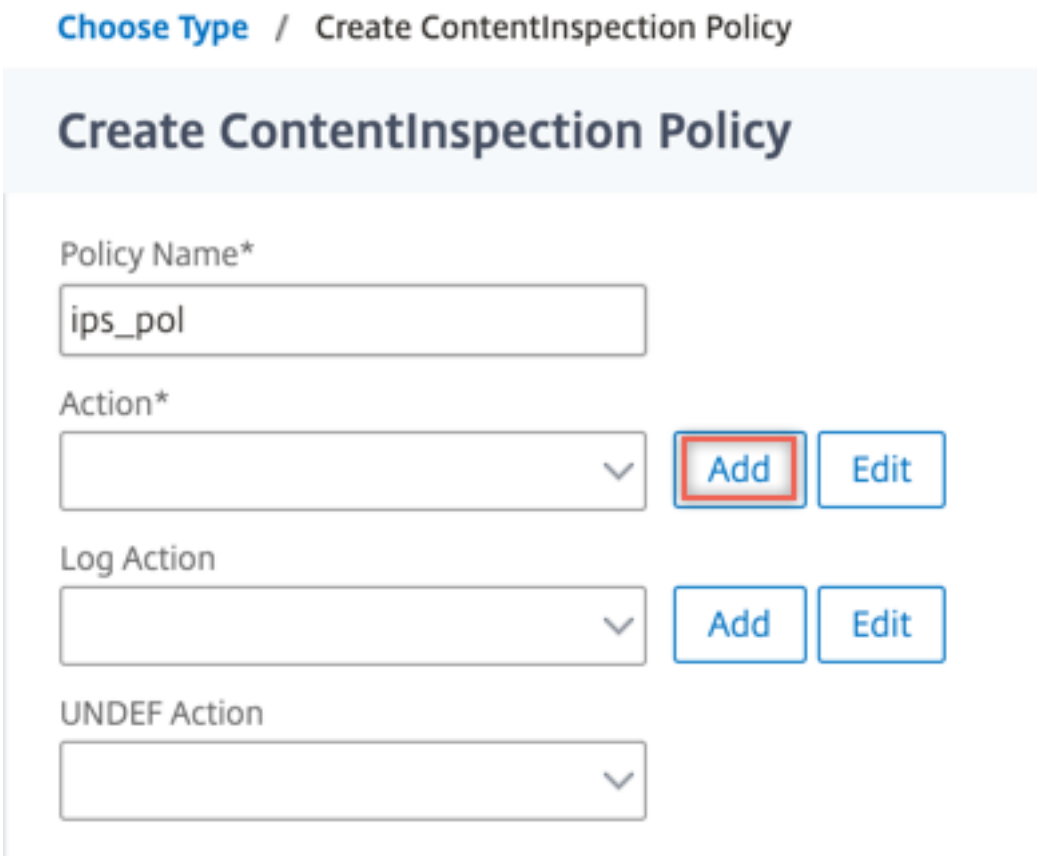
5. Accédez à **Secure Web Gateway > Servers virtuels Proxy > Ajouter**. Spécifiez un nom, une adresse IP et un port. Dans **Paramètres avancés**, sélectionnez **Stratégies**. Cliquez sur le signe « + ».



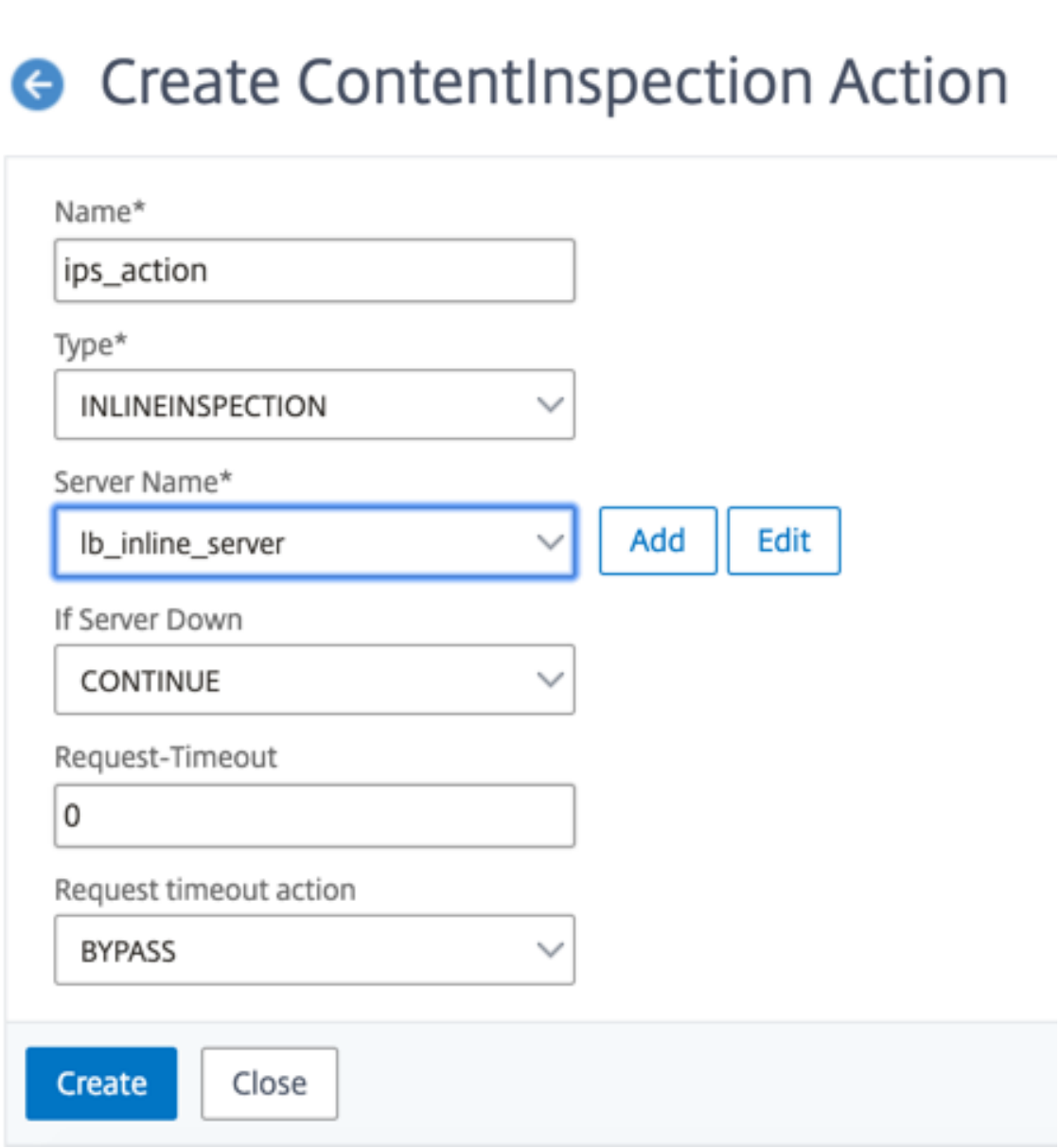
6. Dans **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.



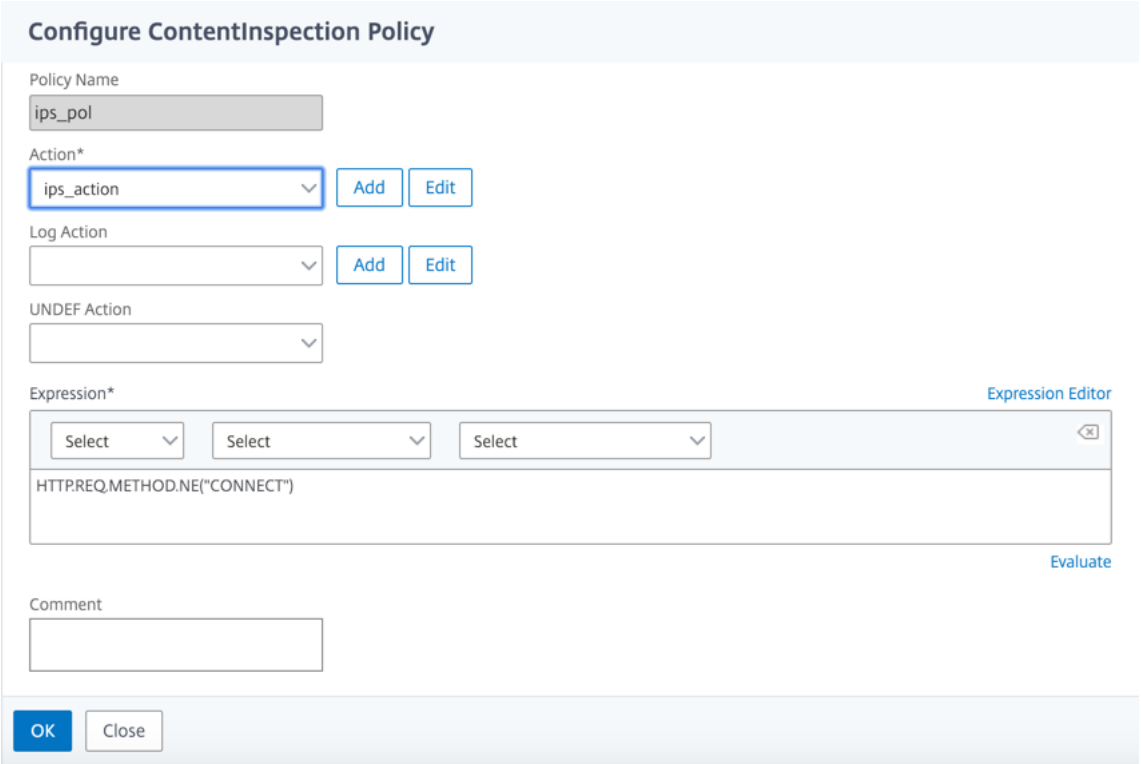
7. Cliquez sur **Ajouter**. Spécifiez un nom. Dans **Action**, cliquez sur **Ajouter**.



8. Spécifiez un nom. Dans **Type**, sélectionnez **INLINEINSPECTION**. Dans **Nom du serveur**, sélectionnez le service TCP créé précédemment.



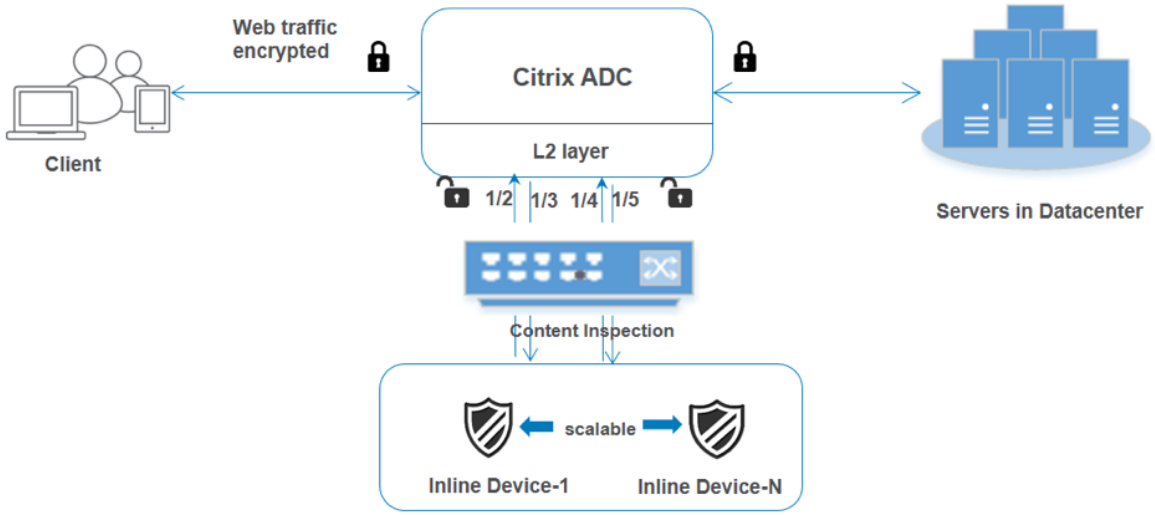
9. Cliquez sur **Créer**. Spécifiez la règle et cliquez sur **Créer**.



10. Cliquez sur **Bind**.
11. Cliquez sur **Terminé**.

Scénario 2 : équilibrage de la charge de plusieurs périphériques en ligne avec interfaces dédiées

Si vous utilisez au moins deux périphériques en ligne, vous pouvez équilibrer la charge des périphériques à l'aide de différents services d'inspection de contenu avec des interfaces dédiées. Dans ce cas, la charge de l'appliance proxy de transfert SSL équilibre le sous-ensemble du trafic envoyé à chaque périphérique via une interface dédiée. Le sous-ensemble est décidé en fonction des stratégies configurées. Par exemple, les fichiers TXT ou image peuvent ne pas être envoyés pour inspection aux périphériques en ligne.



La configuration de base reste la même que dans le scénario 1. Toutefois, vous devez créer un profil d'inspection de contenu pour chaque périphérique en ligne et spécifier l'interface d'entrée et de sortie dans chaque profil. Ajoutez un service pour chaque périphérique en ligne. Ajoutez un serveur virtuel d'équilibrage de charge et spécifiez-le dans l'action d'inspection du contenu. Effectuez les étapes supplémentaires suivantes :

1. Ajoutez des profils d'inspection de contenu pour chaque service.
2. Ajoutez un service pour chaque périphérique.
3. Ajoutez un serveur virtuel d'équilibrage de charge.
4. Spécifiez le serveur virtuel d'équilibrage de charge dans l'action d'inspection du contenu.

Configurer à l'aide de la CLI

Tapez les commandes suivantes à l'invite de commandes. Des exemples sont donnés après chaque commande.

1. Activez MBF.

```
enable ns mode mbf
```

1. Activez la fonctionnalité.

```
enable ns feature contentInspection
```

1. Ajouter le profil 1 pour le service 1.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :


```
add contentInspection profile ipsprof1 -type InlineInspection -ingressInterface
 "1/2"-egressInterface "1/3"
```

1. Ajouter le profil 2 pour le service 2.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile ipsprof2 -type InlineInspection -ingressInterface
 "1/4"-egressInterface "1/5"
```

1. Ajouter le service 1. Spécifiez une adresse IP fictive qui n'appartient à aucun des périphériques, y compris les périphériques en ligne. Définissez `use source IP address` (USIP) sur YES. Définissez `useproxyport` sur NO. Activez la surveillance de l'intégrité avec le moniteur TCP avec l'option TRANSPARENT activée.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Exemple :

```
add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof1
```

1. Ajouter le service 2. Spécifiez une adresse IP fictive qui n'appartient à aucun des périphériques, y compris les périphériques en ligne. Définissez `use source IP address` (USIP) sur YES. Définissez `useproxyport` sur NO. Activez la surveillance de l'état avec l'option TRANSPARENT activée.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Exemple :

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof2
```

1. Ajoutez un serveur virtuel d'équilibrage de charge.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Exemple :

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```

1. Liez les services au serveur virtuel d'équilibrage de charge.


```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Exemple :

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
```

1. Spécifiez le serveur virtuel d'équilibrage de charge dans l'action d'inspection du contenu.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Exemple :

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
lb_inline_vserver
```

1. Ajoutez une stratégie d'inspection du contenu. Spécifiez l'action d'inspection du contenu dans la stratégie.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Exemple :

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Ajoutez un serveur virtuel proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Exemple :

```
add cs vserver transparentcs PROXY * * -l2Conn ON
```

1. Liez la stratégie d'inspection de contenu au serveur virtuel.

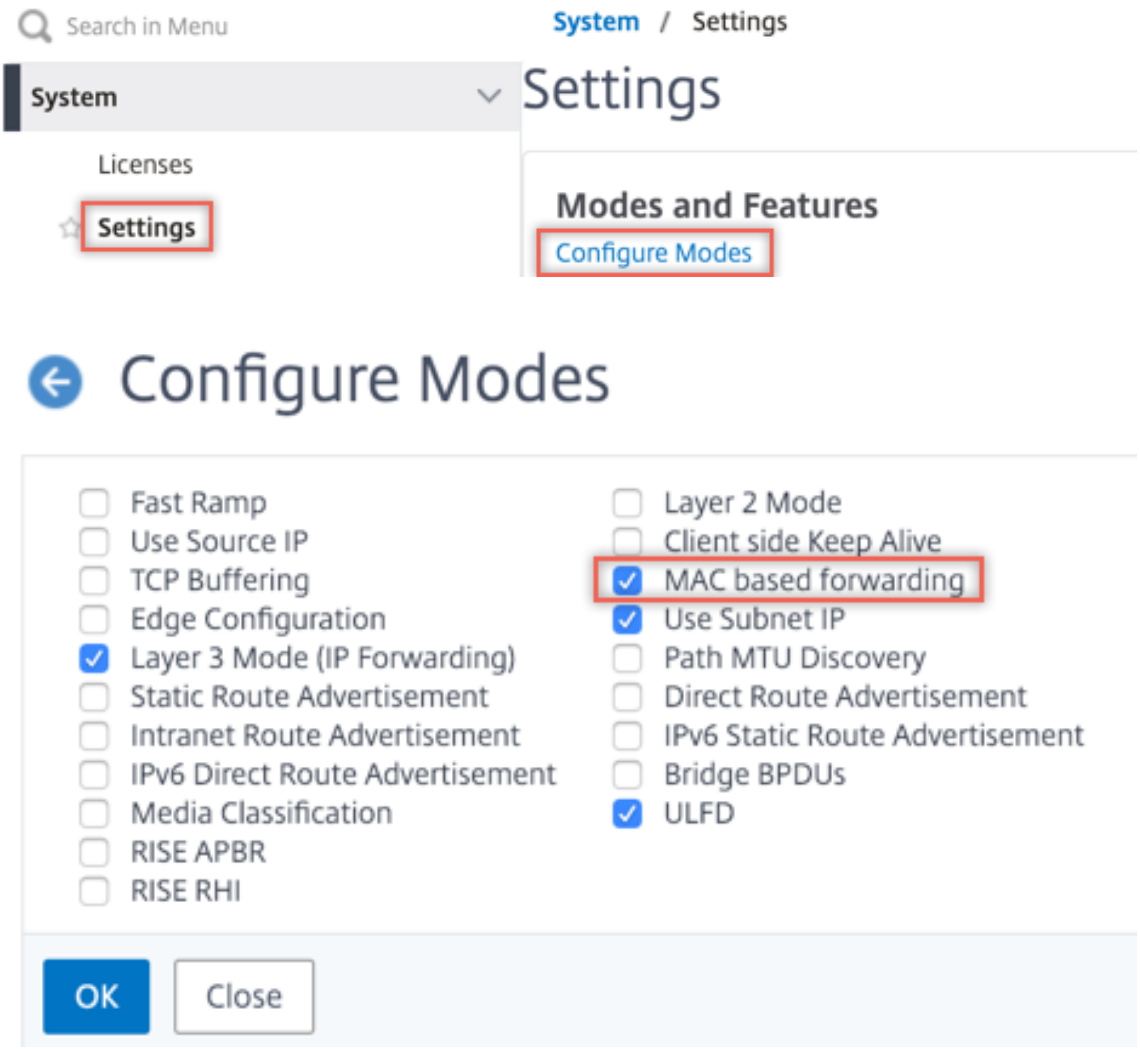
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Exemple :

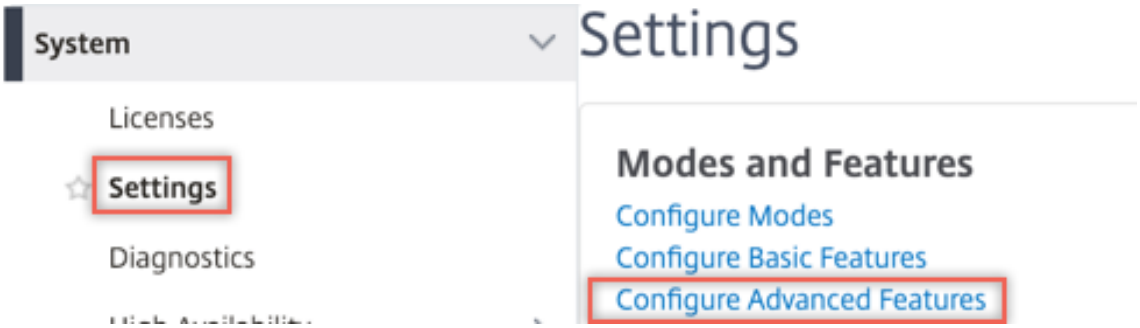
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

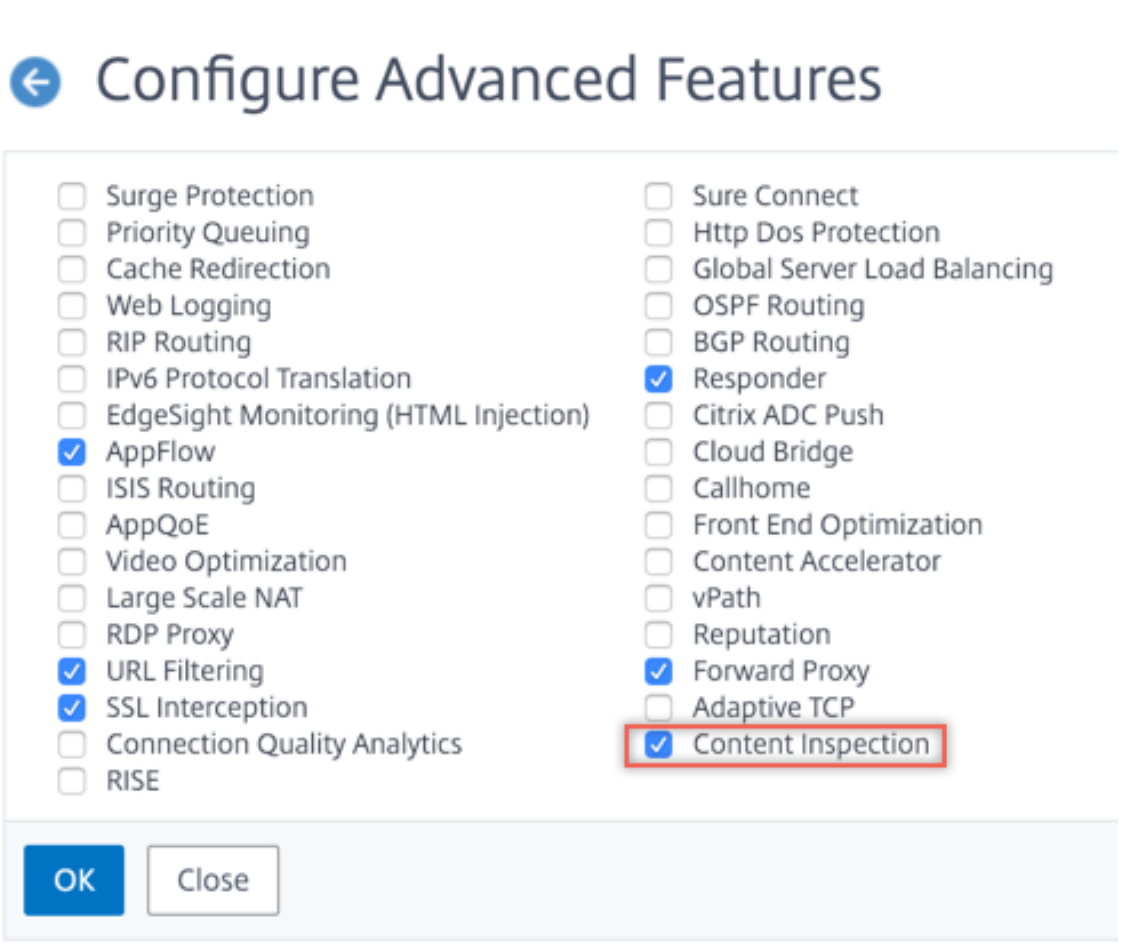
Configuration à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.

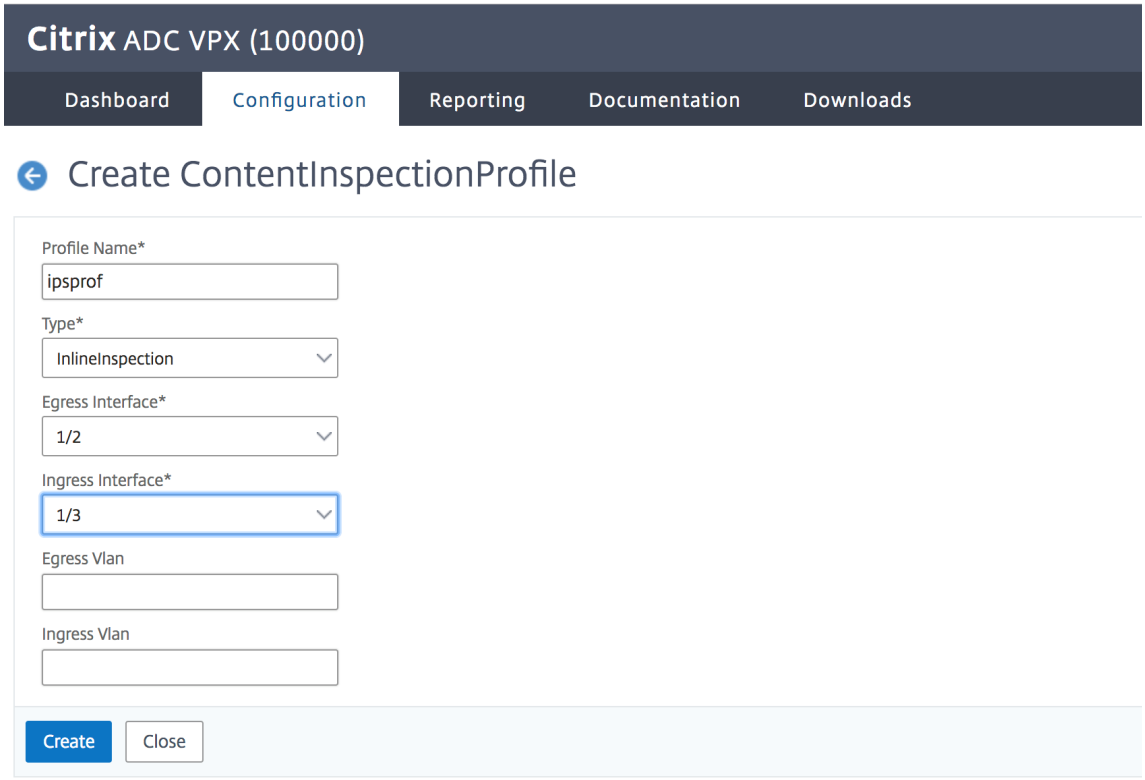


2. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.

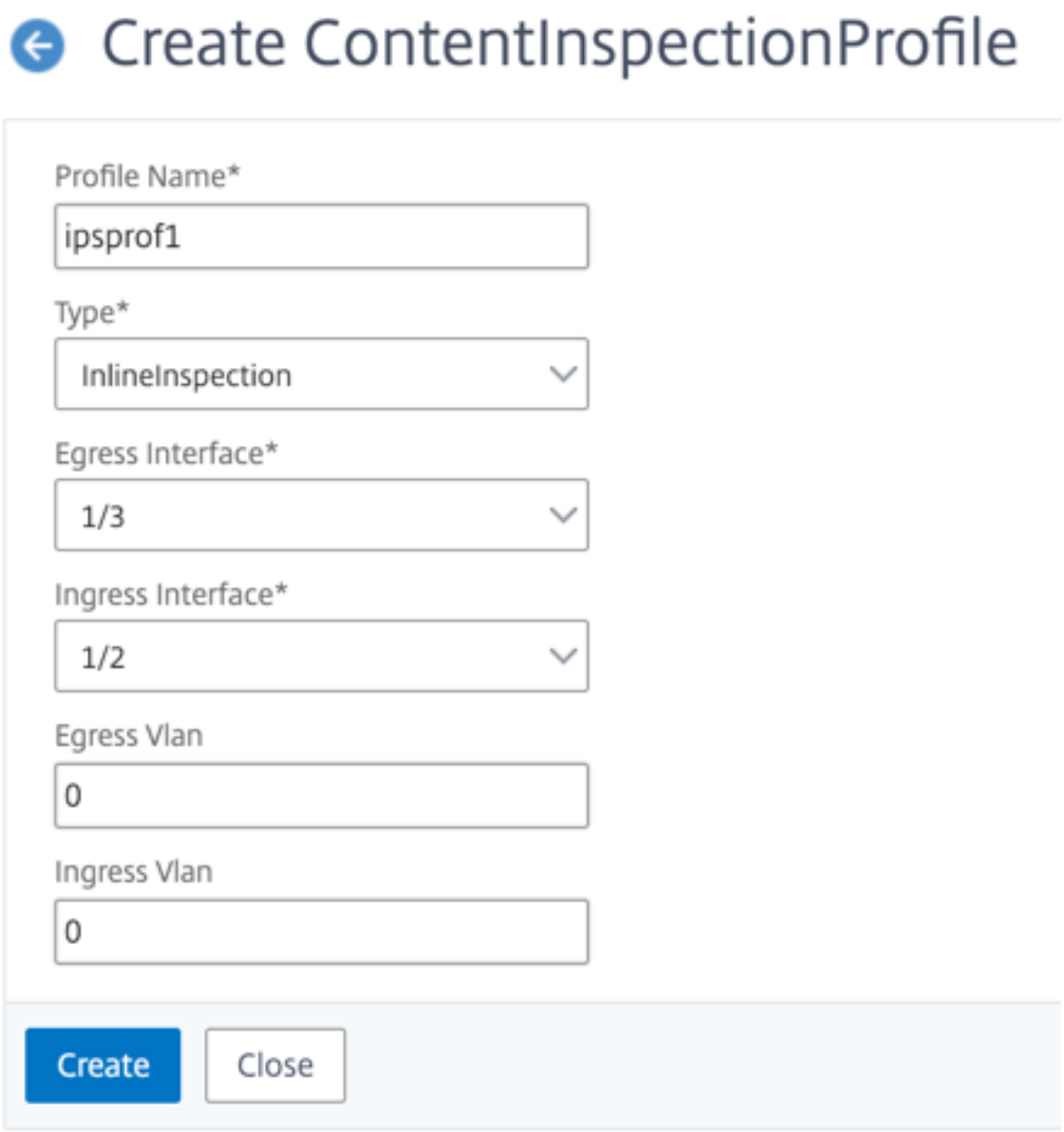




3. Accédez à **Secure Web Gateway > Inspection du contenu > Profils d'inspection du contenu**. Cliquez sur **Ajouter**.

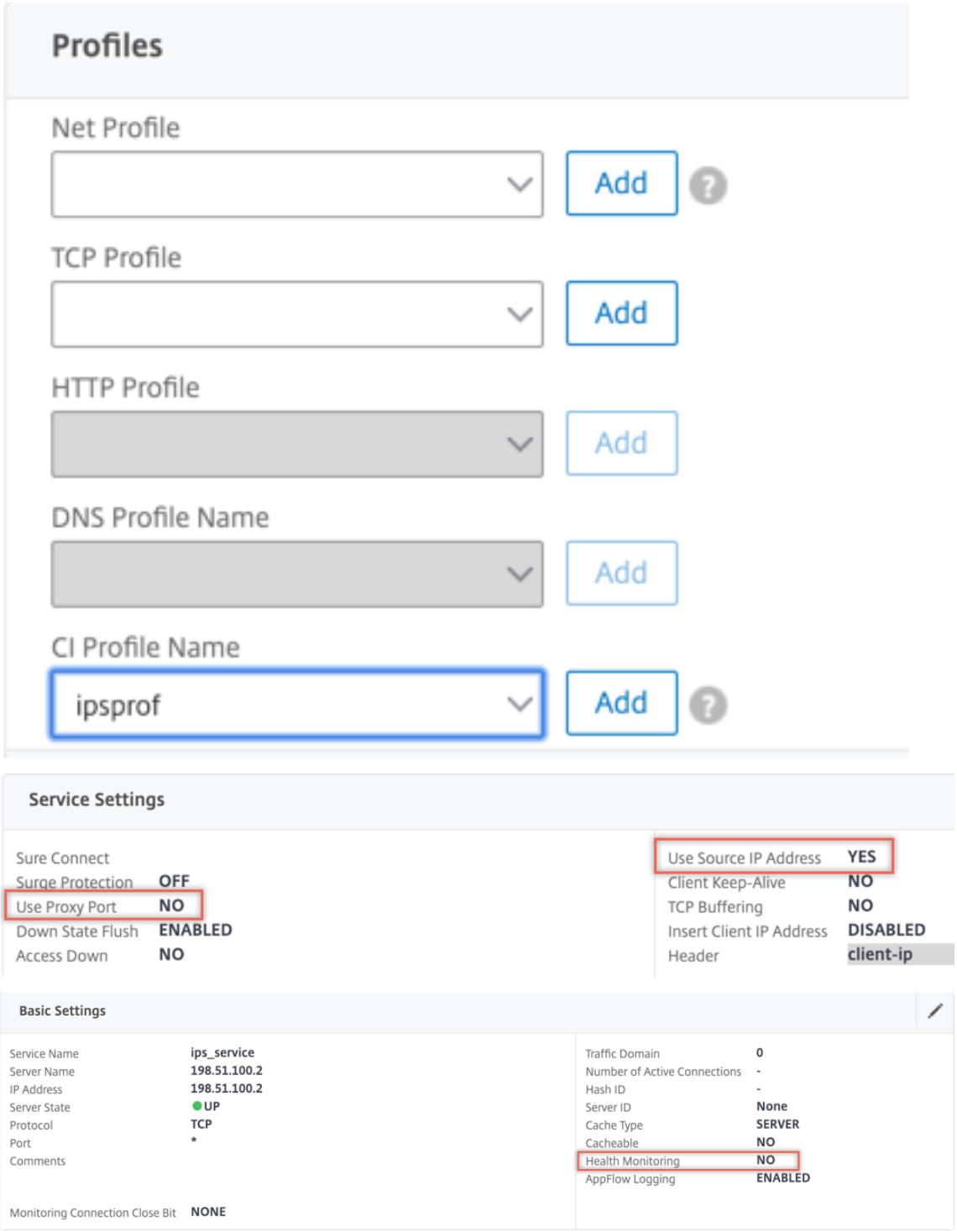


Spécifiez les interfaces d’entrée et de sortie.



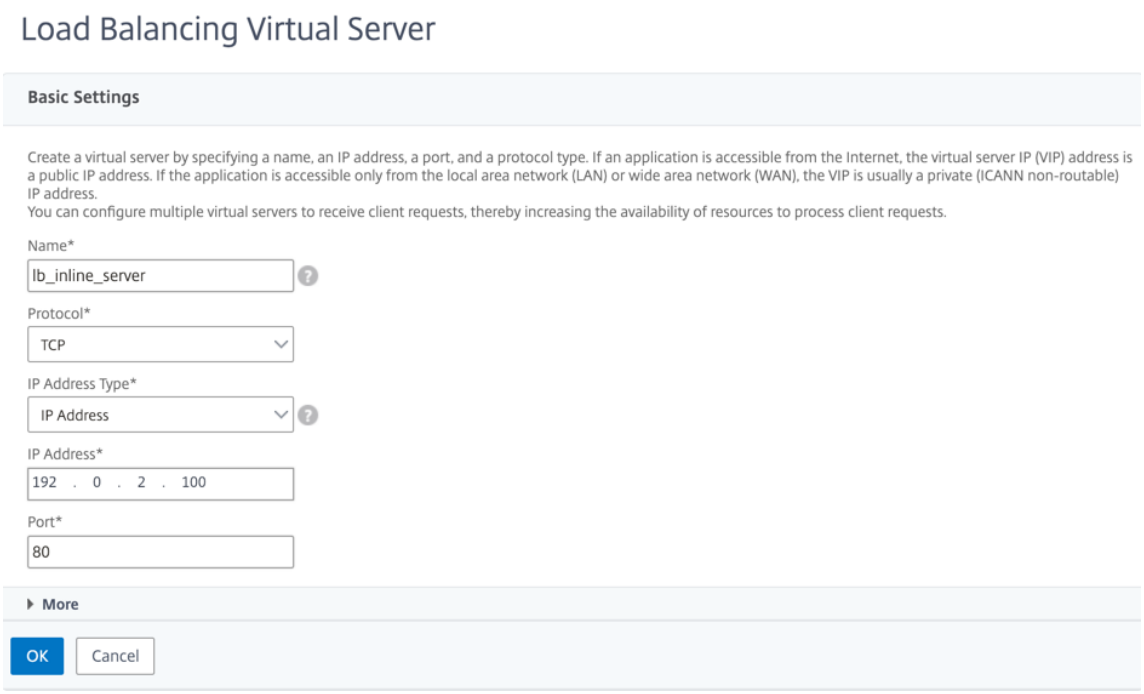
Créez deux profils. Spécifiez une interface d'entrée et de sortie différente dans le second profil.

4. Accédez à **Équilibrage de charge > Services > Ajouter** et ajouter un service. Dans **Paramètres avancés**, cliquez sur **Profils**. Dans la liste **Nom du profil CI**, sélectionnez le profil d'inspection du contenu créé précédemment. Dans **Paramètres de service**, définissez **Utiliser l'adresse IP source**sur YES et **Utiliser le port proxy**sur Non. Dans **Paramètres de base**, définissez le **contrôle de l'intégrité** sur NO. Activez la surveillance de l'intégrité uniquement si vous liez ce service à un moniteur TCP. Si vous liez un moniteur à un service, définissez l'option TRANSPARENT du moniteur sur ON.



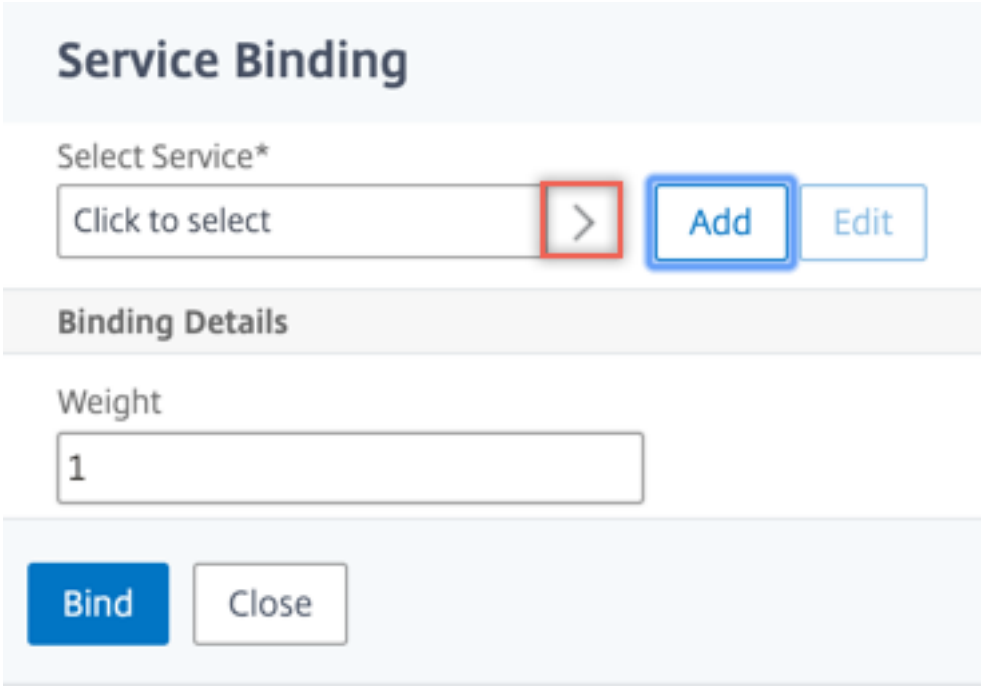
Créez deux services. Spécifiez les adresses IP factices qui ne sont la propriété d'aucun des périphériques, y compris les périphériques en ligne.

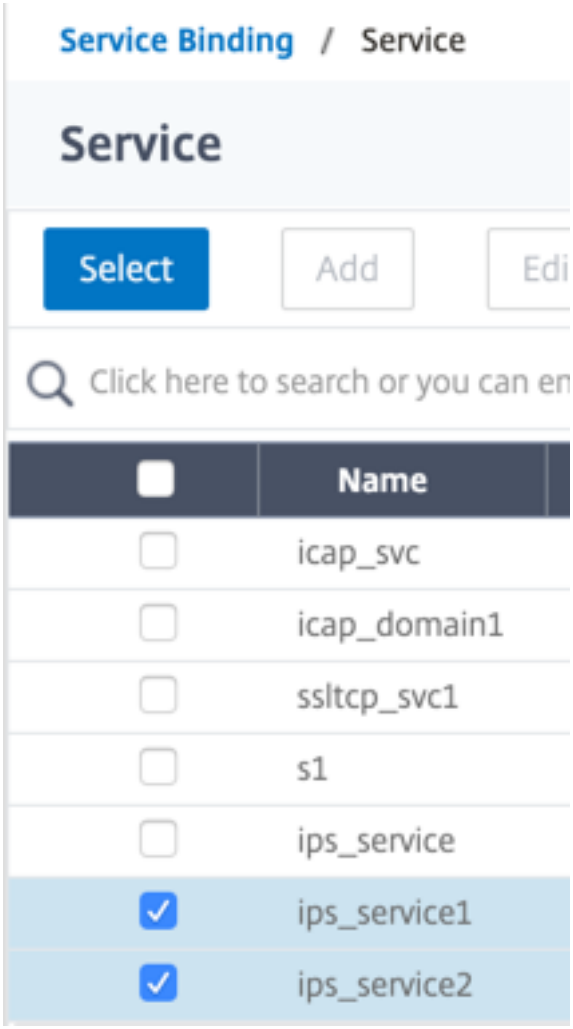
5. Accédez à **Équilibrage de charge > Serveurs virtuels > Ajouter**. Créez un serveur virtuel d'équilibrage de charge TCP.

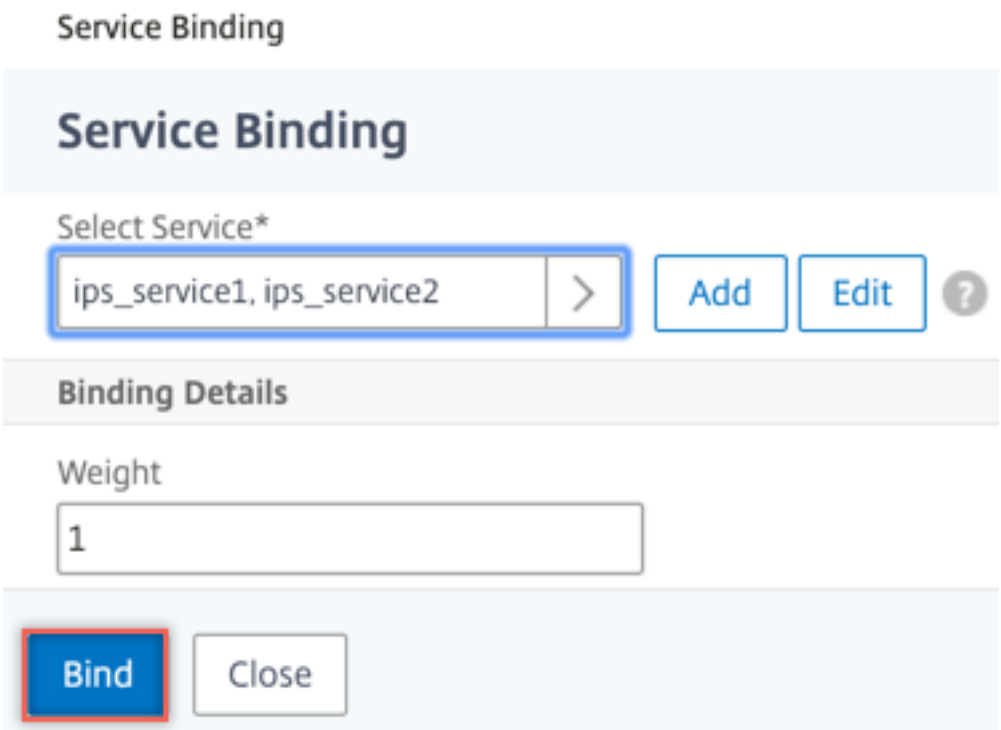


Cliquez sur **OK**.

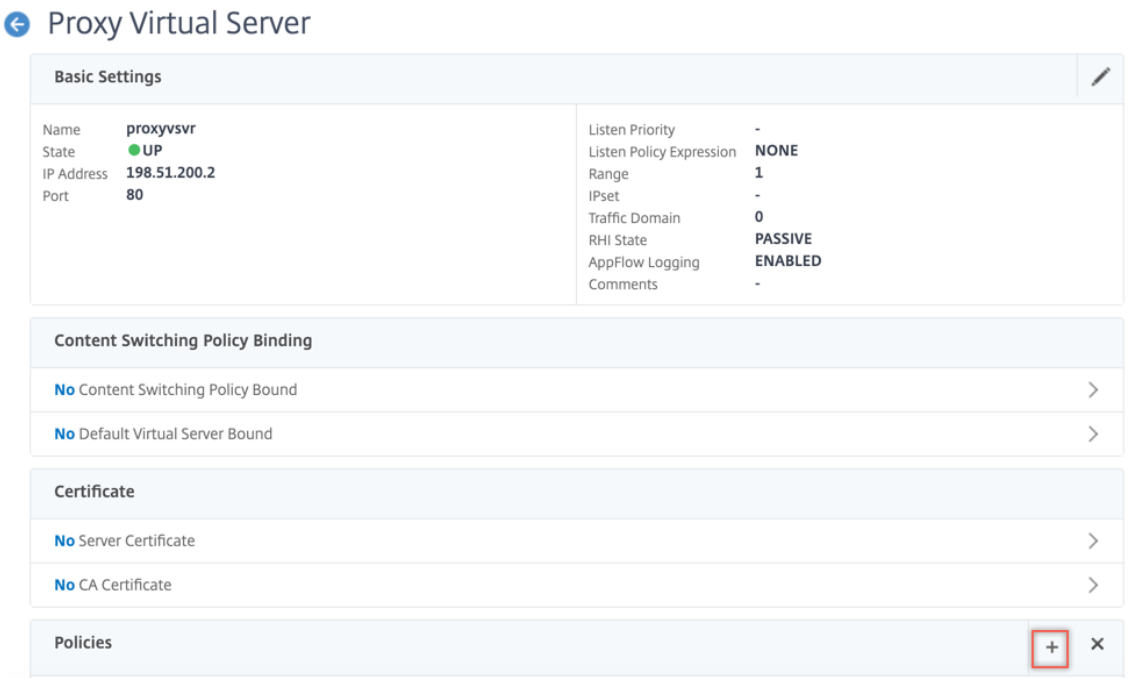
6. Cliquez dans la section **Load Balancing Virtual Server Service Liaison**. Dans **Liaison de service**, cliquez sur la flèche dans **Sélectionner un service**. Sélectionnez les deux services créés précédemment, puis cliquez sur **Sélectionner**. Cliquez sur **Bind**.



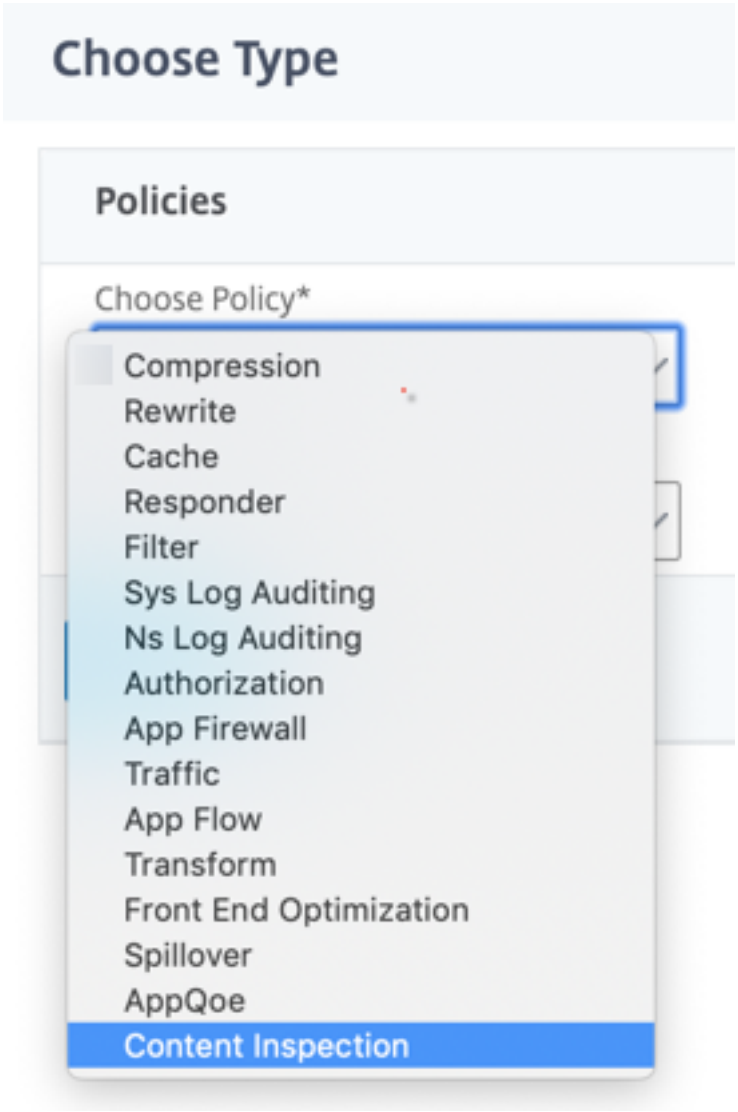




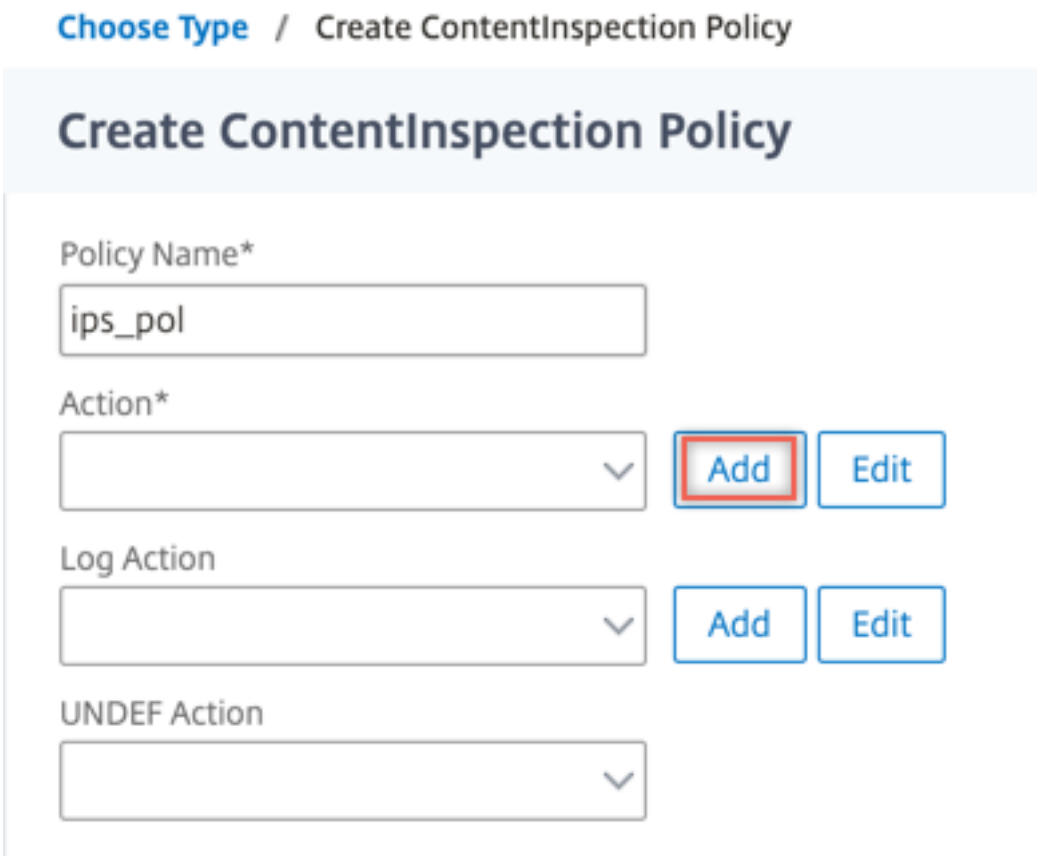
7. Accédez à **Secure Web Gateway > Servers virtuels Proxy > Ajouter**. Spécifiez un nom, une adresse IP et un port. Dans **Paramètres avancés**, sélectionnez **Stratégies**. Cliquez sur le signe « + ».



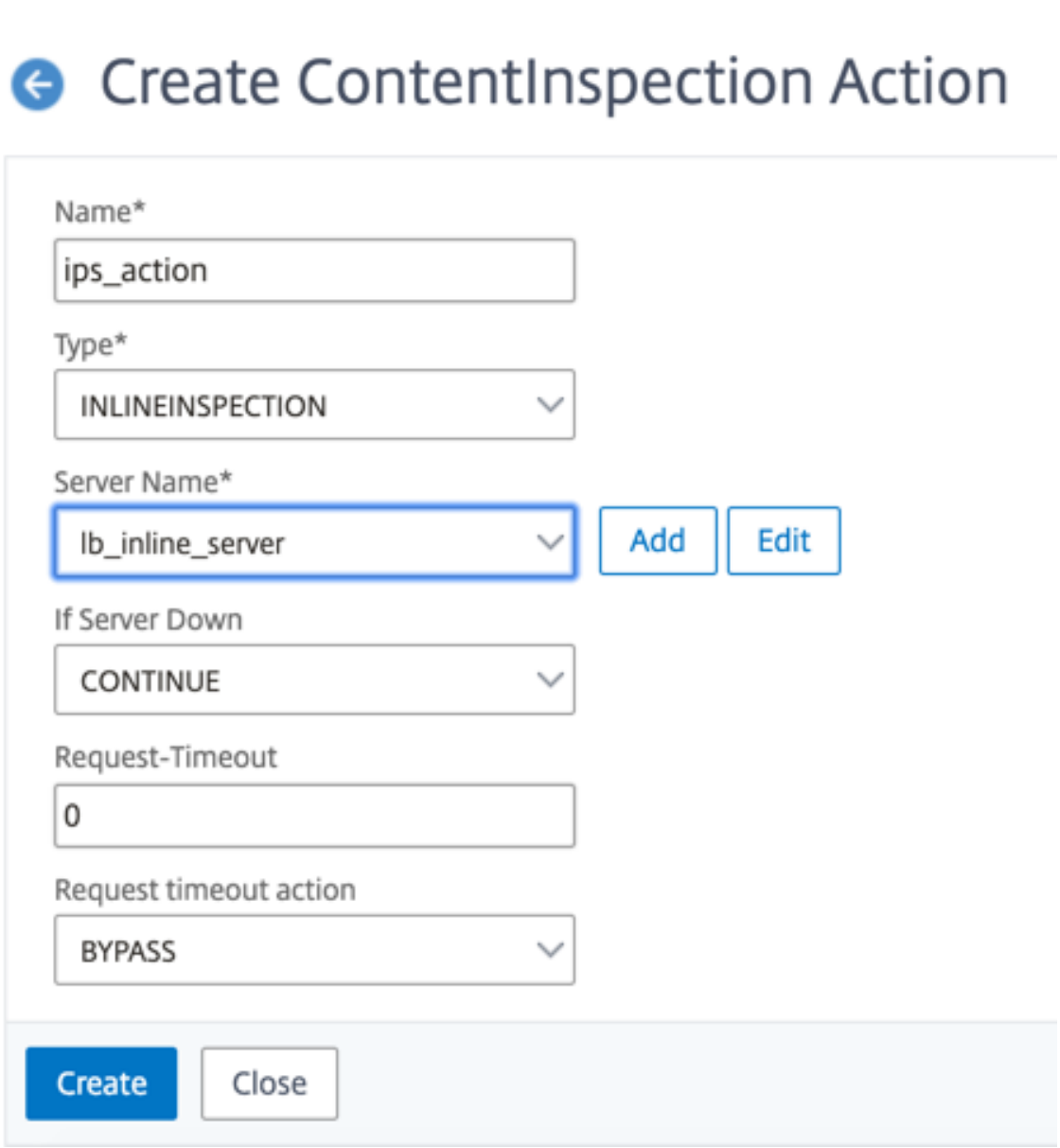
8. Dans **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.



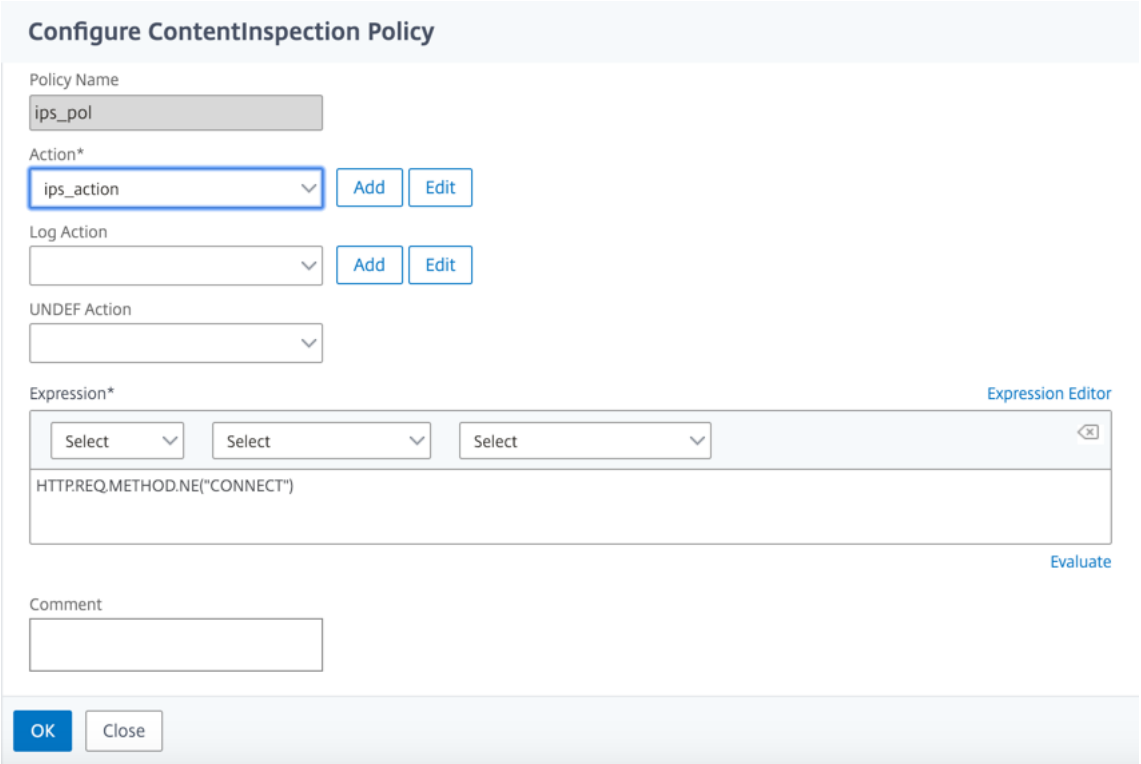
9. Cliquez sur **Ajouter**. Spécifiez un nom. Dans **Action**, cliquez sur **Ajouter**.



10. Spécifiez un nom. Dans **Type**, sélectionnez **INLINEINSPECTION**. Dans **Nom du serveur**, sélectionnez le serveur virtuel d'équilibrage de charge créé précédemment.



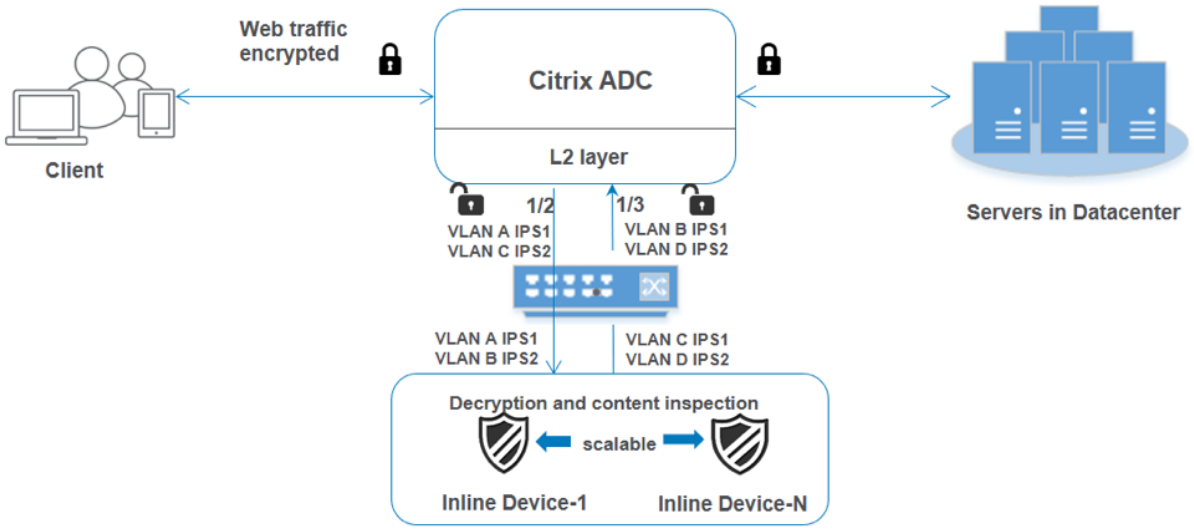
11. Cliquez sur **Créer**. Spécifiez la règle et cliquez sur **Créer**.



12. Cliquez sur **Bind**.
13. Cliquez sur **Terminé**.

Scénario 3 : équilibrage de la charge de plusieurs périphériques en ligne avec des interfaces partagées

Si vous utilisez au moins deux périphériques en ligne, vous pouvez équilibrer la charge des périphériques à l'aide de différents services d'inspection de contenu avec des interfaces partagées. Dans ce cas, la charge de l'appliance proxy de transfert SSL équilibre le sous-ensemble du trafic envoyé à chaque périphérique via une interface partagée. Le sous-ensemble est décidé en fonction des stratégies configurées. Par exemple, les fichiers TXT ou image peuvent ne pas être envoyés pour inspection aux périphériques en ligne.



La configuration de base reste la même que dans le scénario 2. Pour ce scénario, liez les interfaces à différents VLAN pour séparer le trafic de chaque périphérique en ligne. Spécifiez les VLAN dans les profils d'inspection de contenu. Effectuez les étapes supplémentaires suivantes :

1. Liez les interfaces partagées à différents VLAN.
2. Spécifiez les VLAN d'entrée et de sortie dans les profils d'inspection de contenu.

Configuration à l'aide de l'interface de ligne de commande

Tapez les commandes suivantes à l'invite de commandes. Des exemples sont donnés après chaque commande.

1. Activez MBF.

```
enable ns mode mbf
```

1. Activez la fonctionnalité.

```
enable ns feature contentInspection
```

1. Liez les interfaces partagées à différents VLAN.

```
bind vlan <id> -ifnum <interface> -tagged
```

Exemple :

```
bind vlan 100  - ifnum 1/2 tagged
bind vlan 200  - ifnum 1/3 tagged
bind vlan 300  - ifnum 1/2 tagged
bind vlan 400  - ifnum 1/3 tagged
<!--NeedCopy-->
```


1. Ajouter le profil 1 pour le service 1. Spécifiez les VLAN d'entrée et de sortie dans le profil.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile ipsprof1 -type InlineInspection -egressInterface
 "1/3" -ingressinterface "1/2" -egressVlan 100 -ingressVlan 300
```

1. Ajouter le profil 2 pour le service 2. Spécifiez les VLAN d'entrée et de sortie dans le profil.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile ipsprof2 -type InlineInspection -egressInterface
 "1/3" -ingressinterface "1/2" -egressVlan 200 -ingressVlan 400
```

1. Ajouter le service 1.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Exemple :

```
add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof1
```

1. Ajouter le service 2.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Exemple :

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof2
```

1. Ajoutez un serveur virtuel d'équilibrage de charge.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Exemple :

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```

1. Liez les services au serveur virtuel d'équilibrage de charge.


```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Exemple :

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
```

1. Spécifiez le serveur virtuel d'équilibrage de charge dans l'action d'inspection du contenu.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Exemple :

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
lb_inline_vserver
```

1. Ajoutez une stratégie d'inspection du contenu. Spécifiez l'action d'inspection du contenu dans la stratégie.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Exemple :

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Ajoutez un serveur virtuel proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Exemple :

```
add cs vserver transparentcs PROXY * * -l2Conn ON
```

1. Liez la stratégie d'inspection de contenu au serveur virtuel.

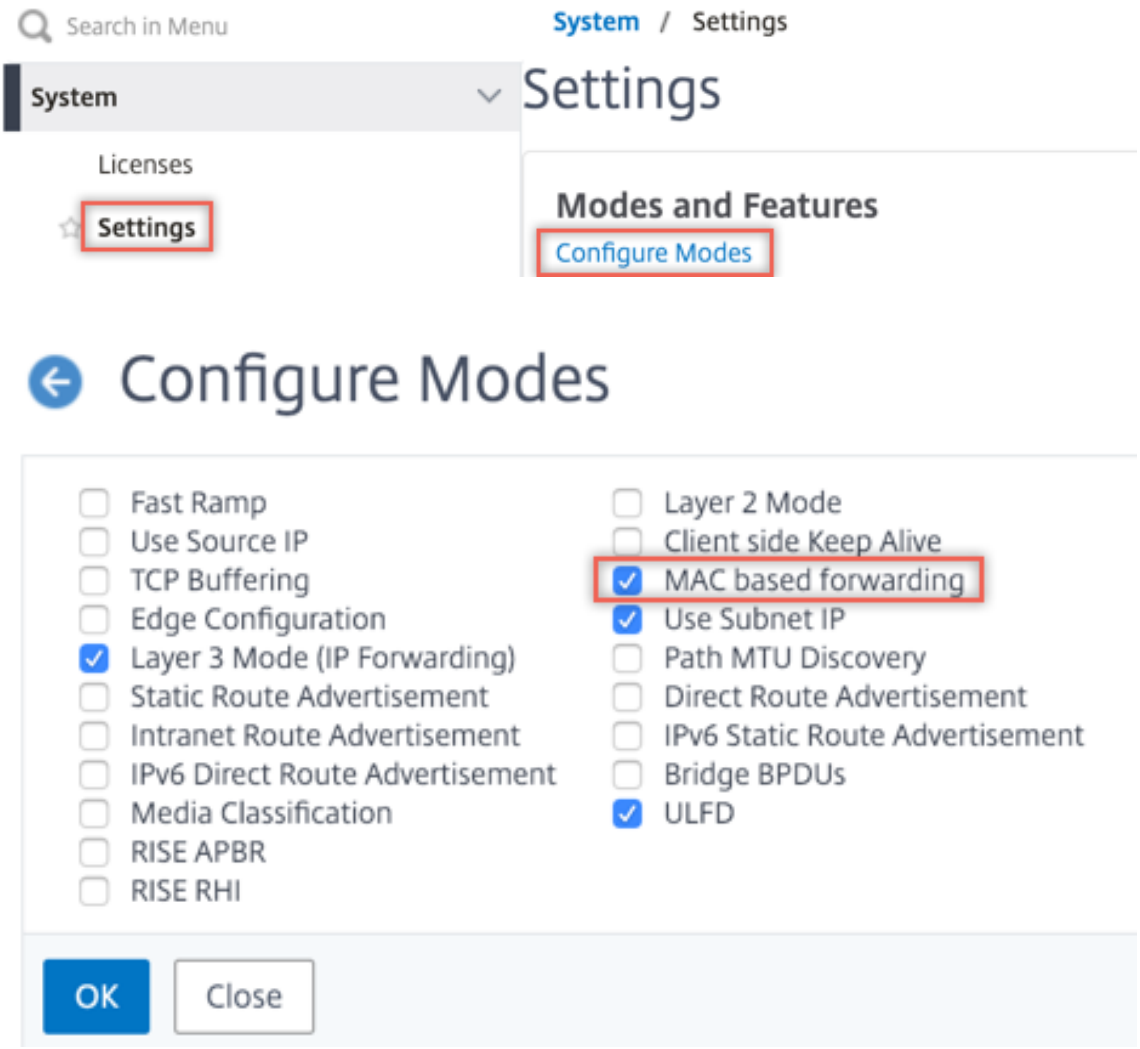
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Exemple :

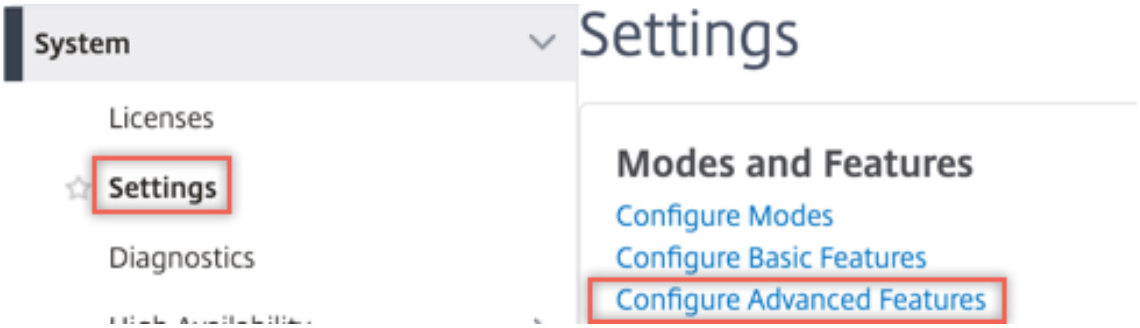
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

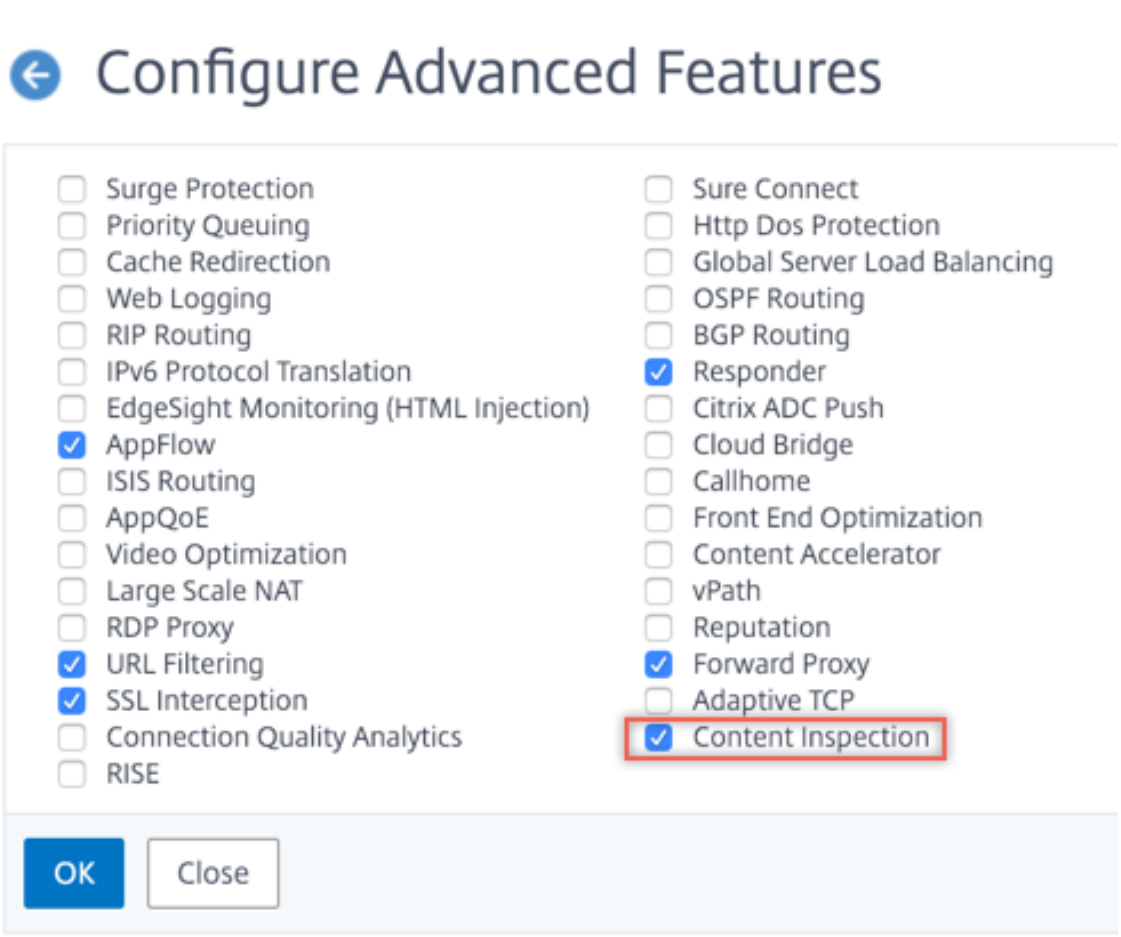
Configuration à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.

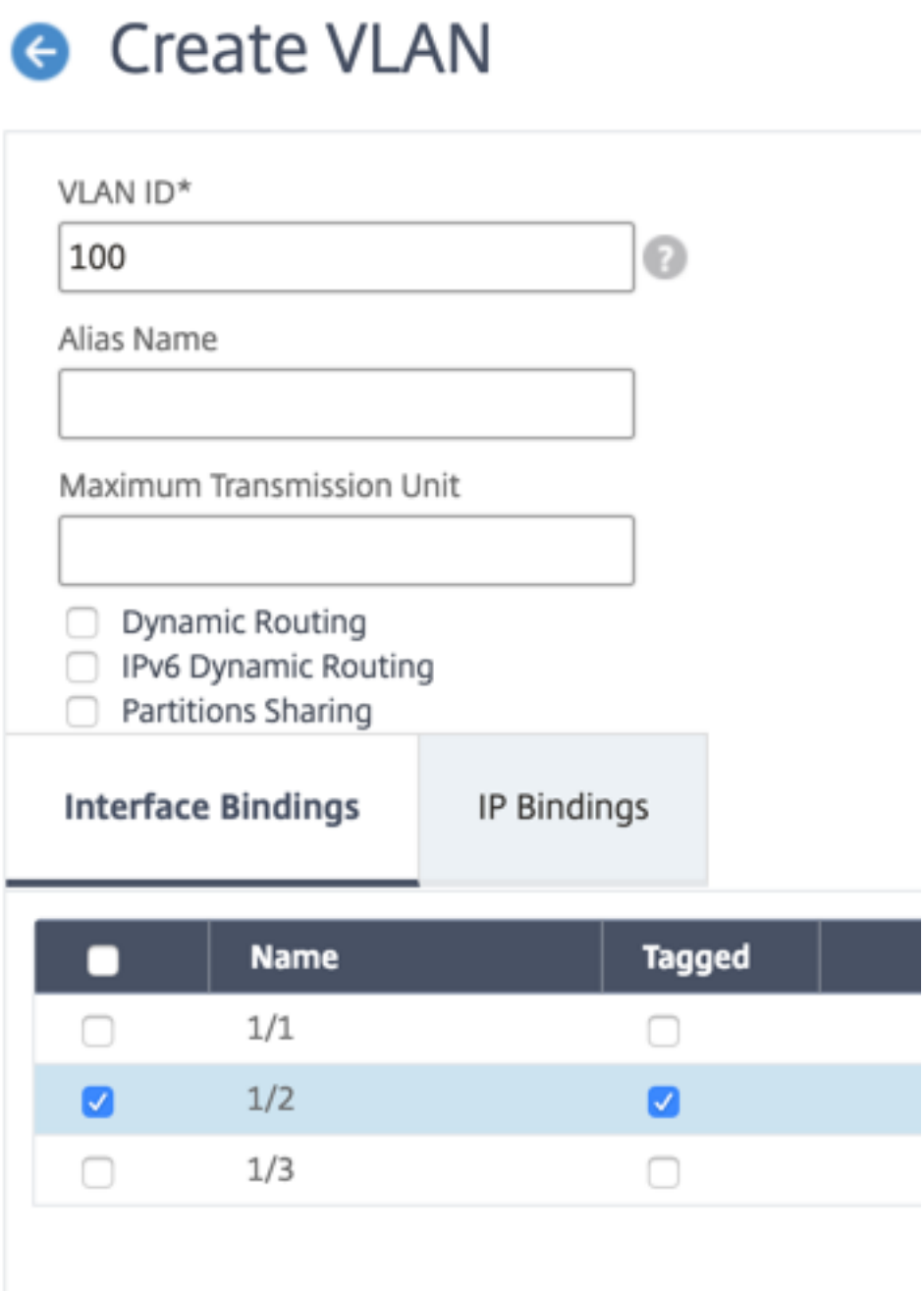


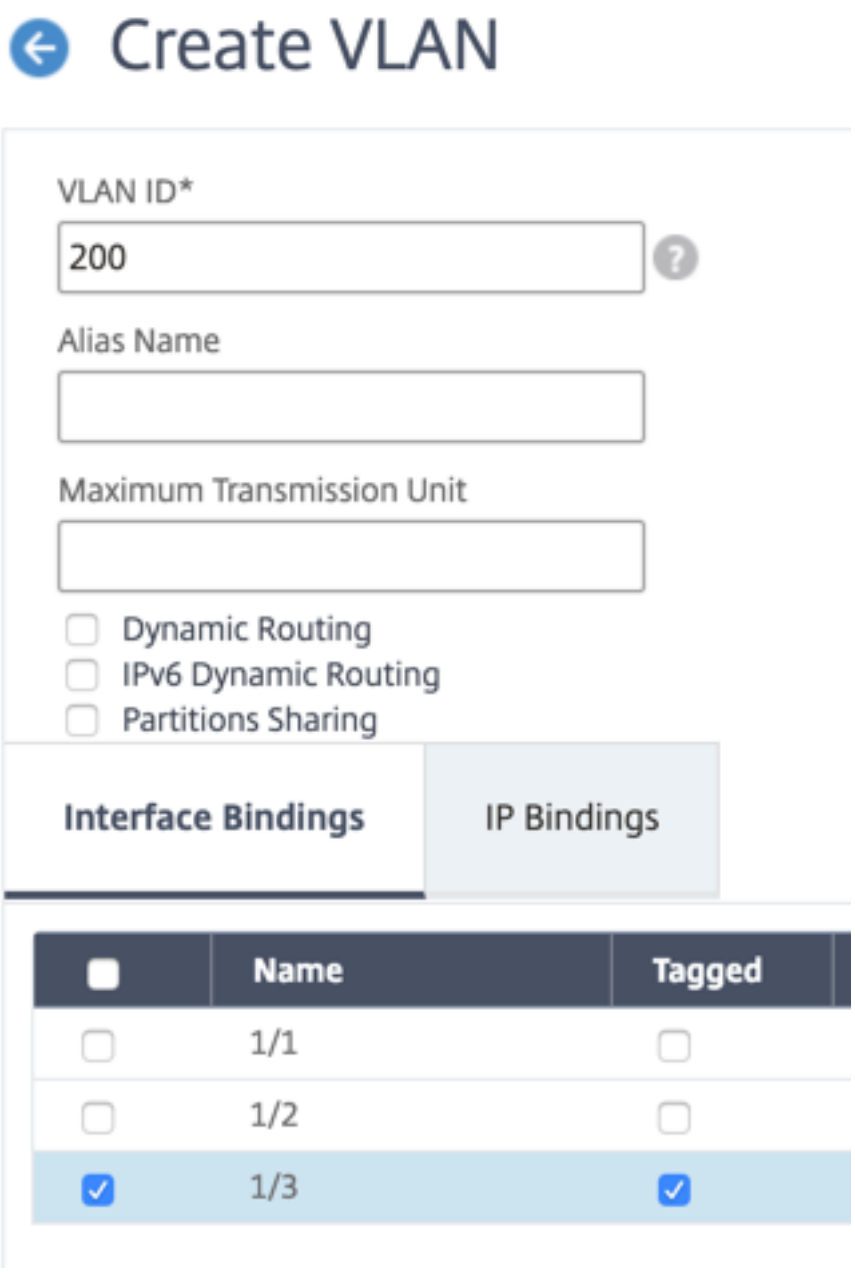
2. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.

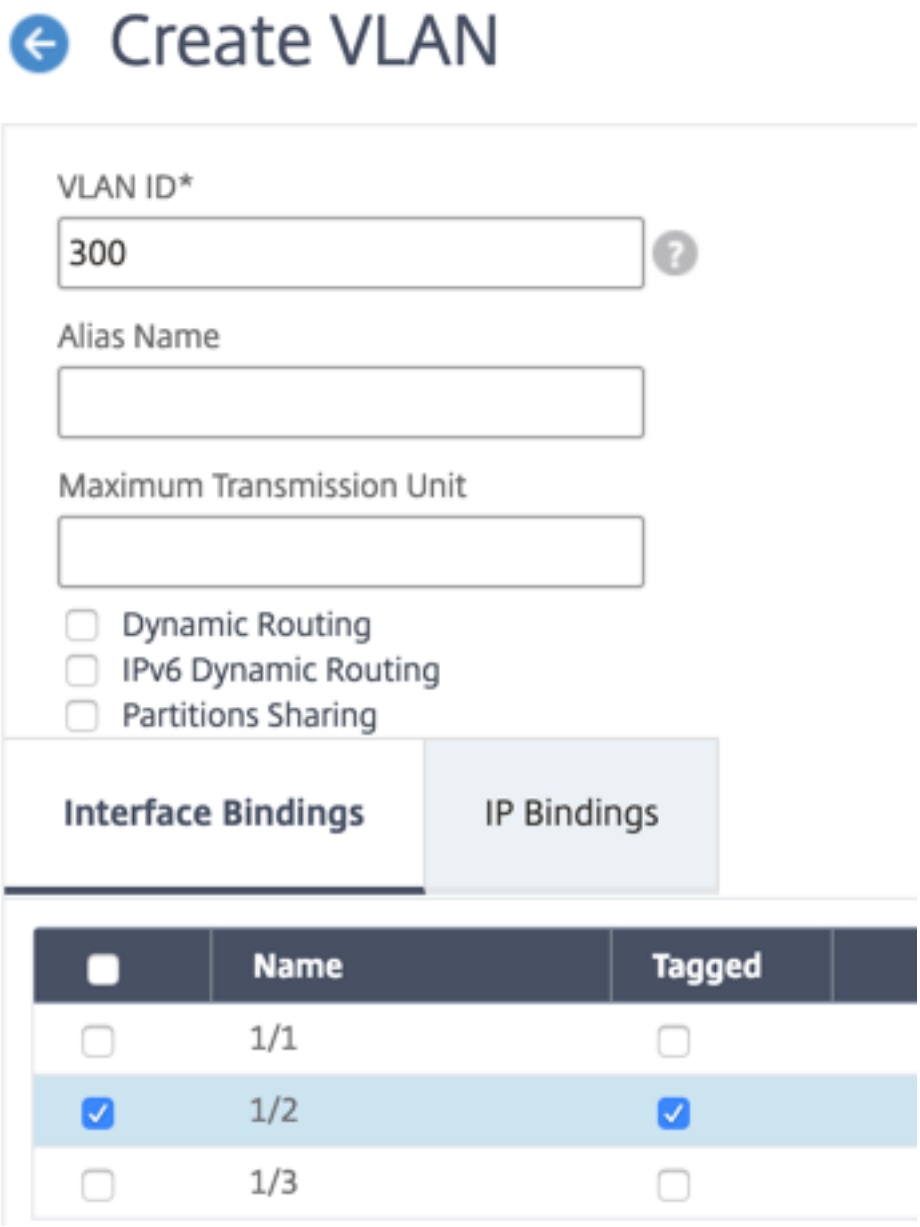


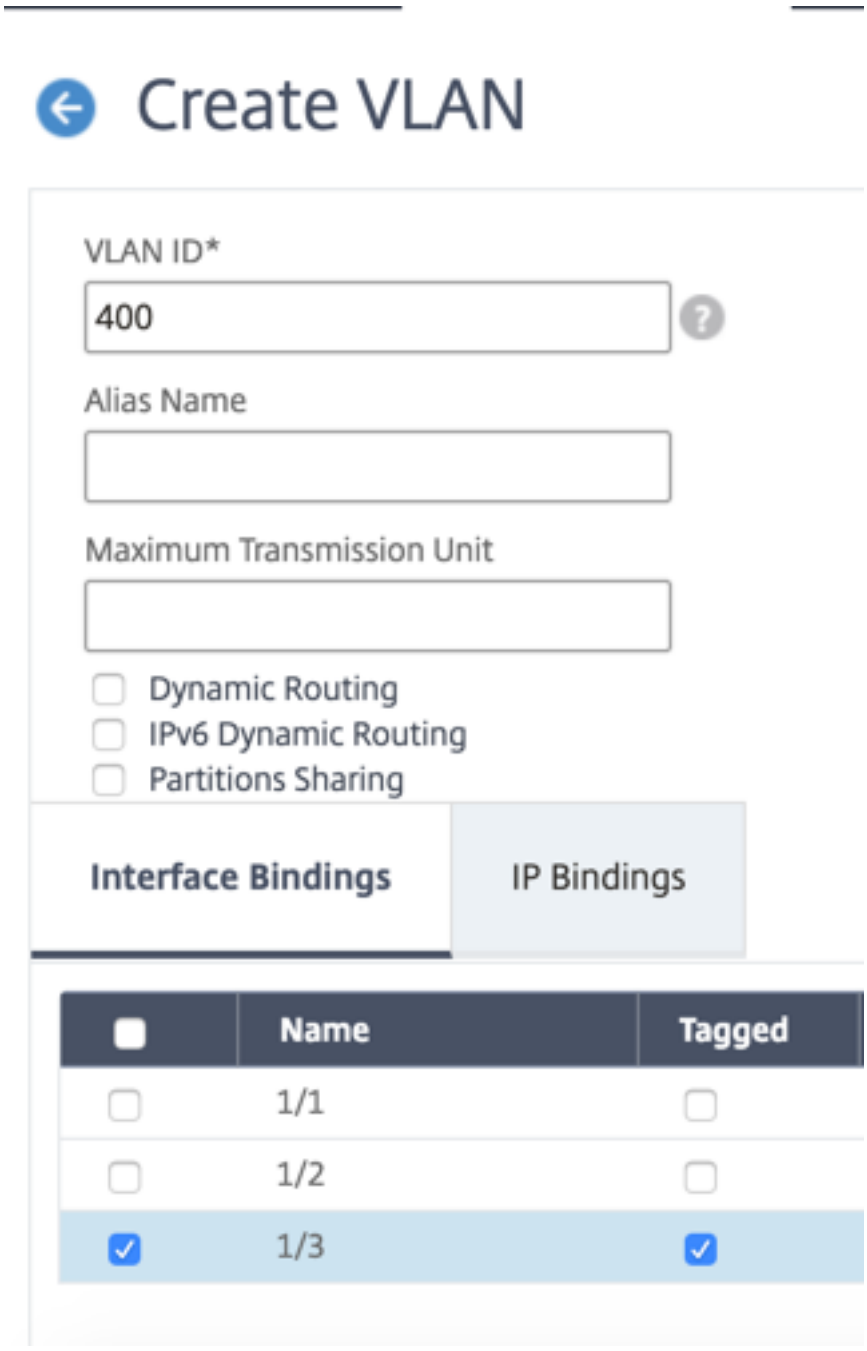


3. Accédez à **Système > Réseau > VLAN > Ajouter**. Ajoutez quatre VLAN et marquez-les sur les interfaces.

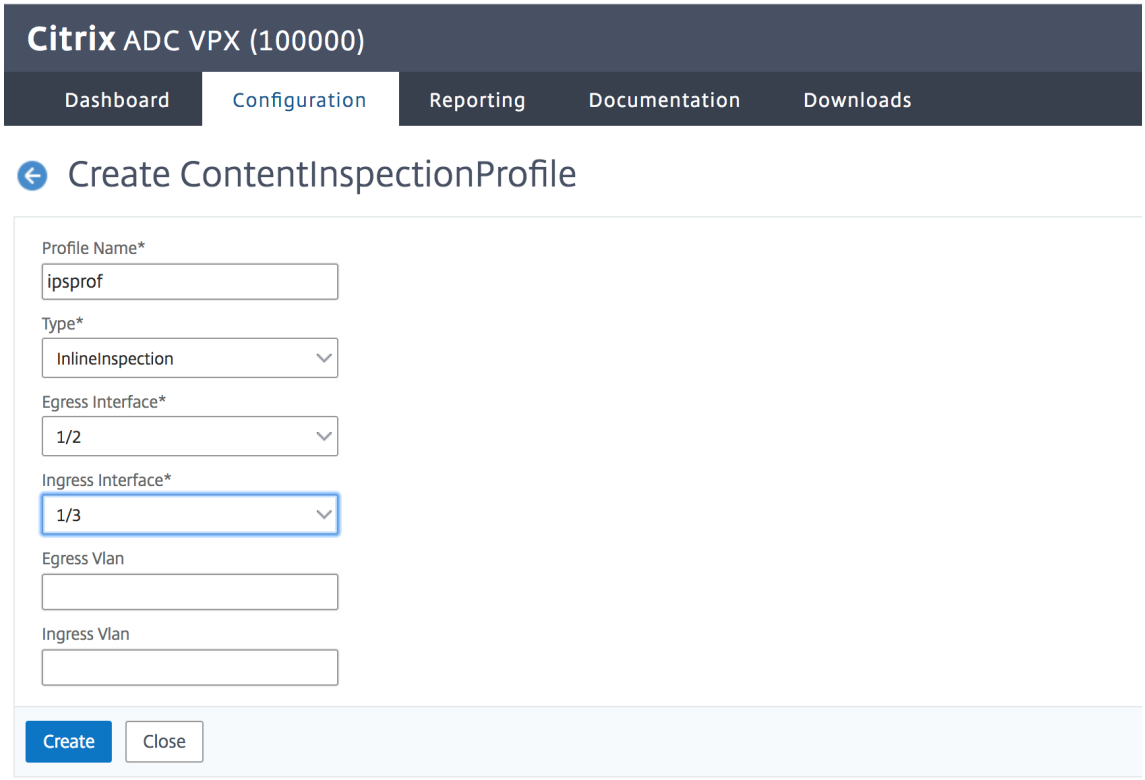




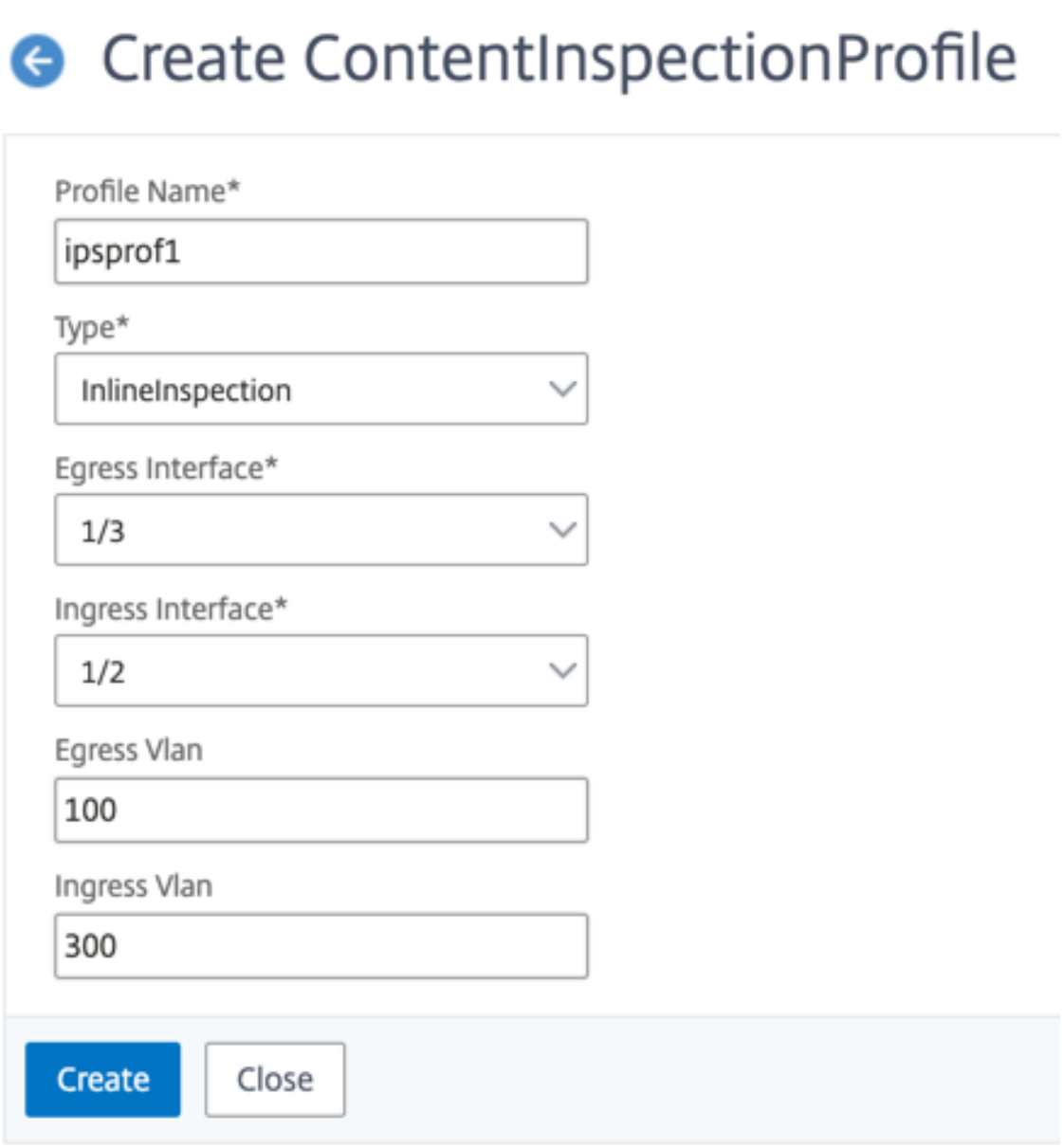




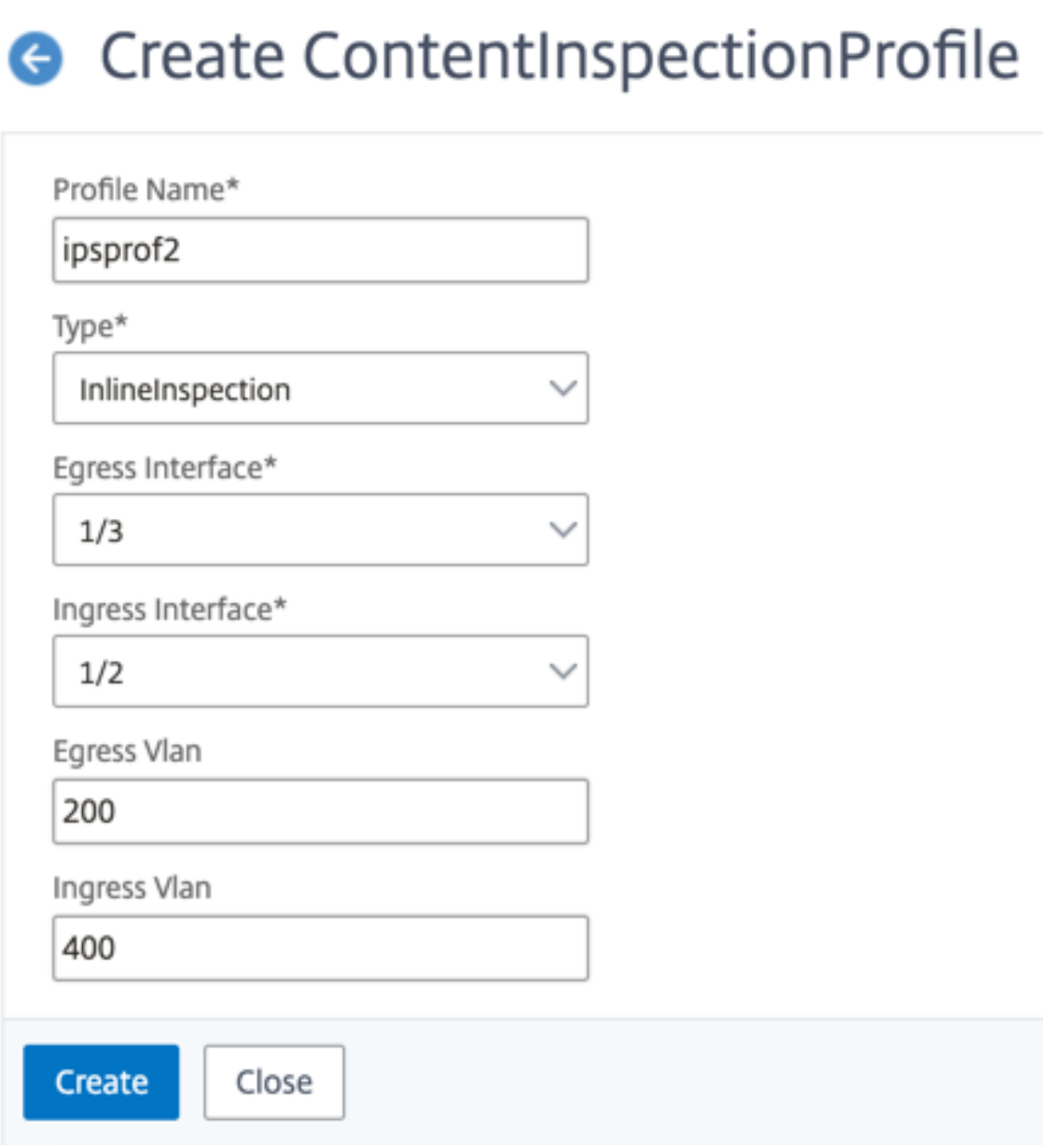
4. Accédez à **Secure Web Gateway > Inspection du contenu > Profils d'inspection du contenu**. Cliquez sur **Ajouter**.



Spécifiez les VLAN d'entrée et de sortie.

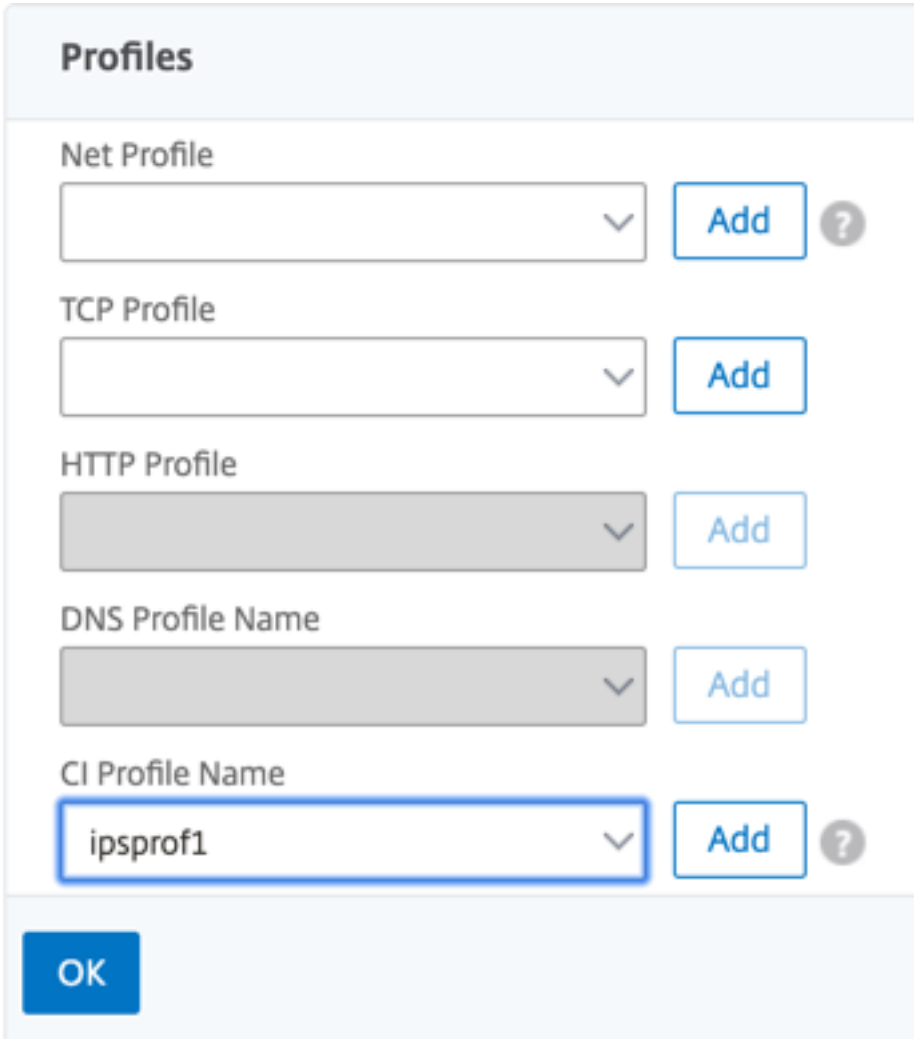


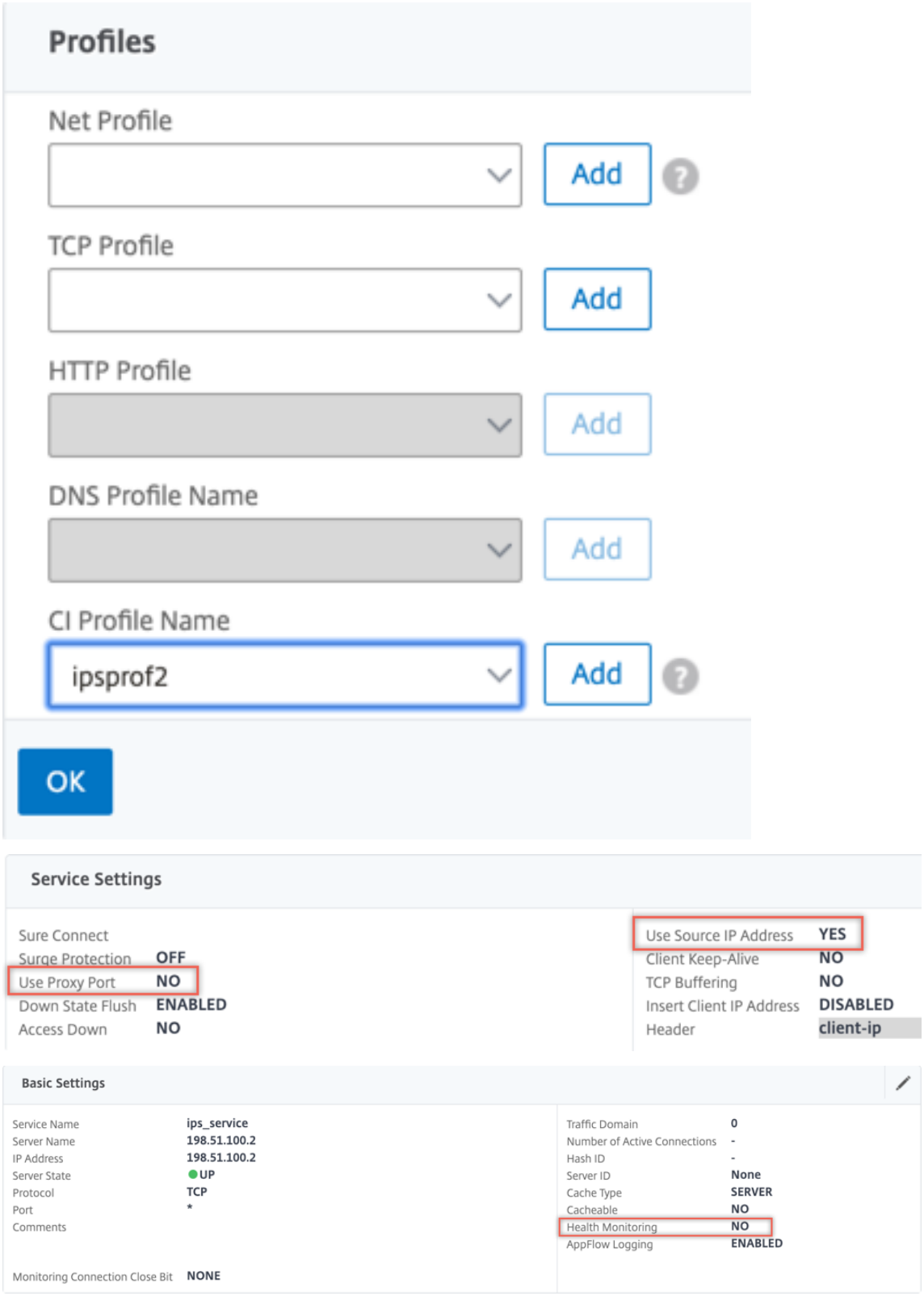
Créez d'autres profils. Spécifiez un VLAN d'entrée et de sortie différent dans le second profil.



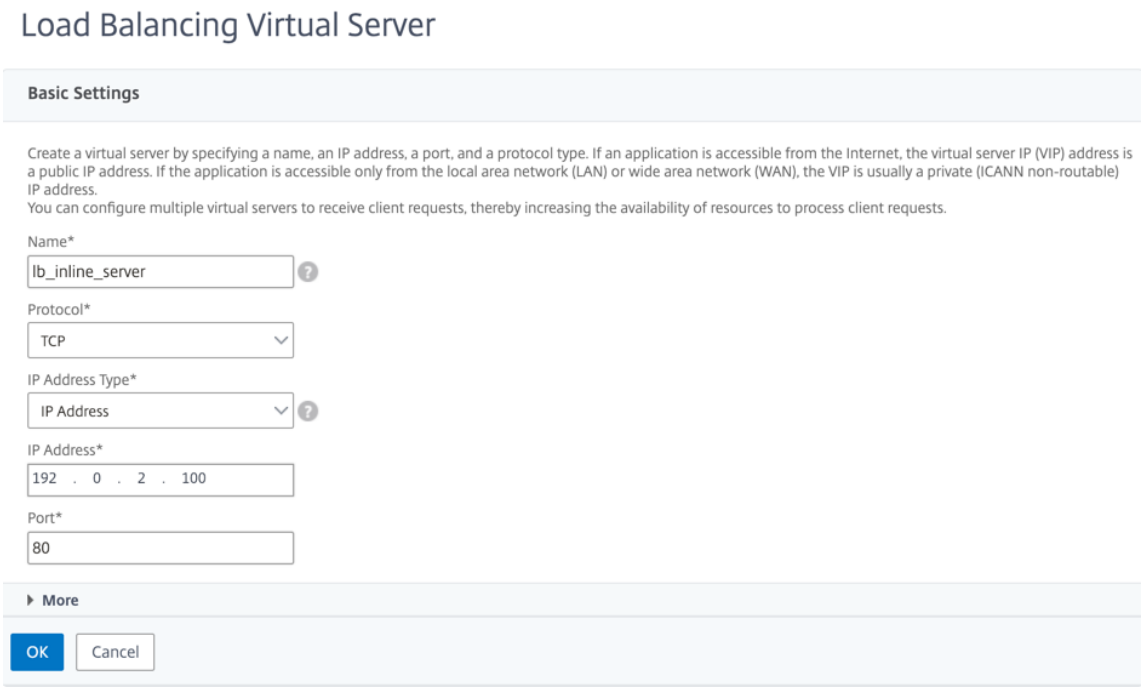
5. Accédez à **Équilibrage de charge > Services > Ajouter** et ajouter un service. Dans **Paramètres avancés**, cliquez sur **Profils**. Dans la liste **Nom du profil CI**, sélectionnez le profil d'inspection du contenu créé précédemment. Dans **Paramètres de service**, définissez **Utiliser l'adresse IP source**sur YES et **Utiliser le port proxy**sur Non. Dans **Paramètres de base**, définissez le **contrôle de l'intégrité** sur NO.

   Créez deux services. Spécifiez les adresses IP factices qui ne sont la propriété d'aucun des périphériques, y compris les périphériques en ligne. Spécifiez le profil 1 dans le service 1 et le profil 2 dans le service 2.

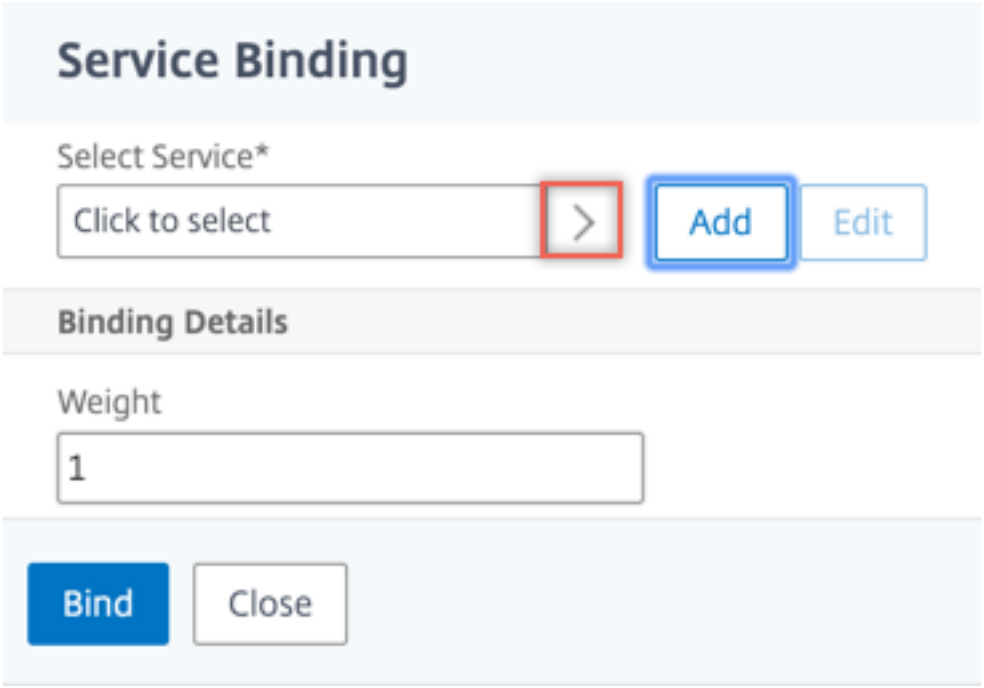


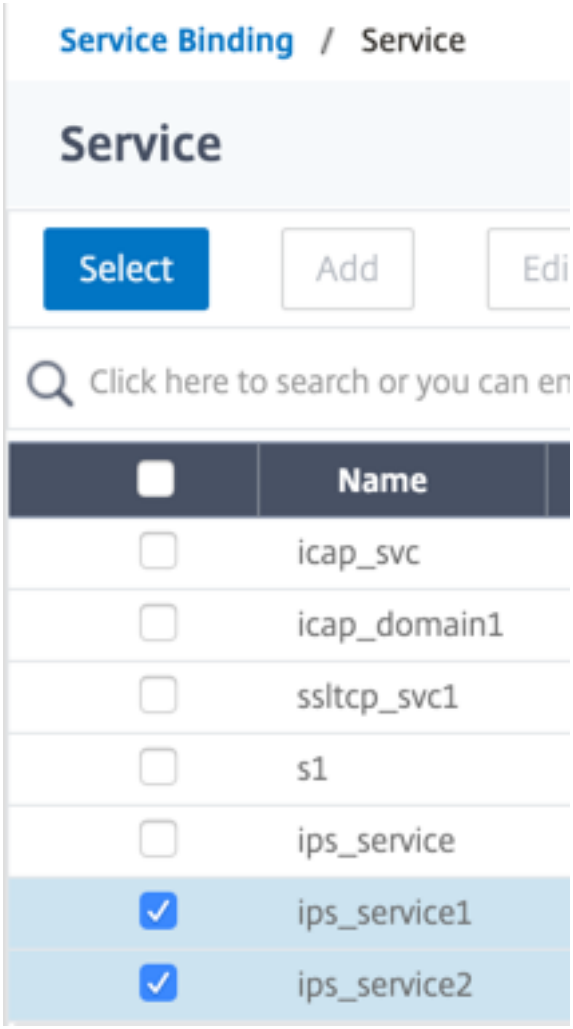


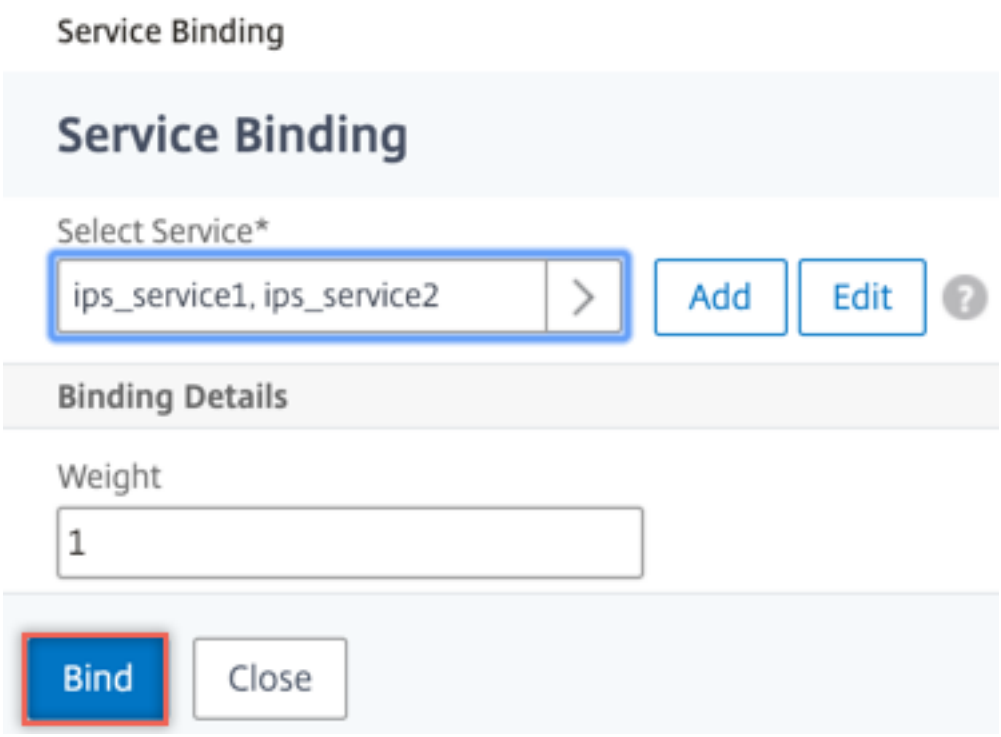
6. Accédez à **Équilibrage de charge > Serveurs virtuels > Ajouter**. Créez un serveur virtuel d'équilibrage de charge TCP.



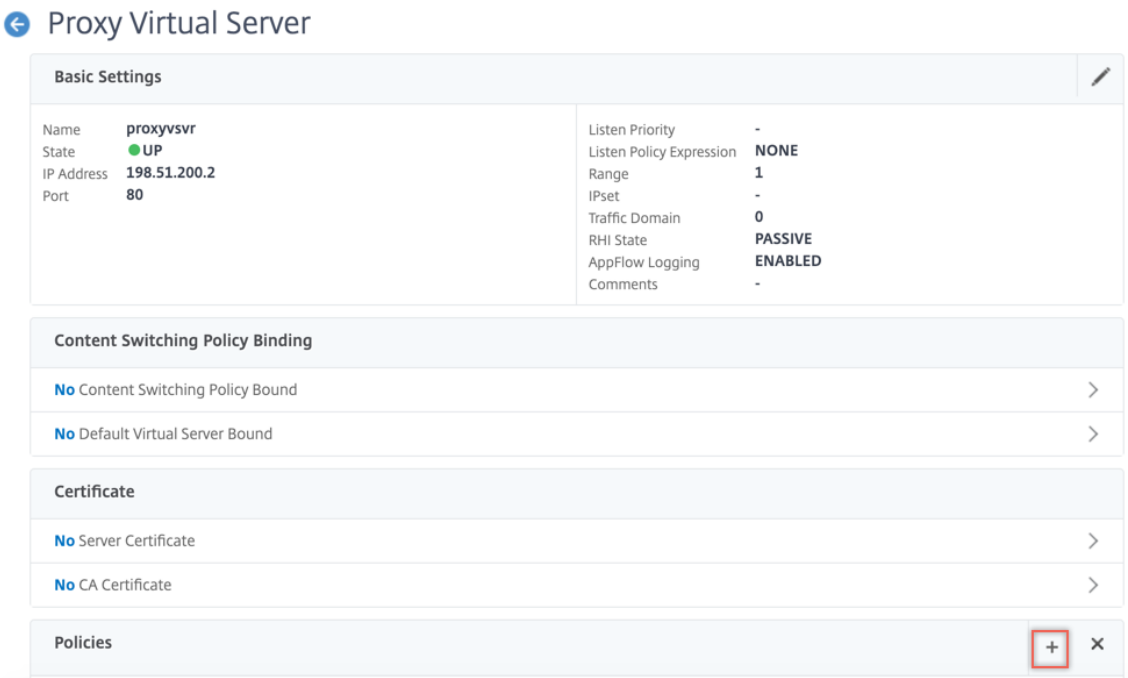
7. Cliquez sur **OK**.
8. Cliquez dans la section **Load Balancing Virtual Server Service Liaison**. Dans **Liaison de service**, cliquez sur la flèche dans **Sélectionner un service**. Sélectionnez les deux services créés précédemment, puis cliquez sur **Sélectionner**. Cliquez sur **Bind**.



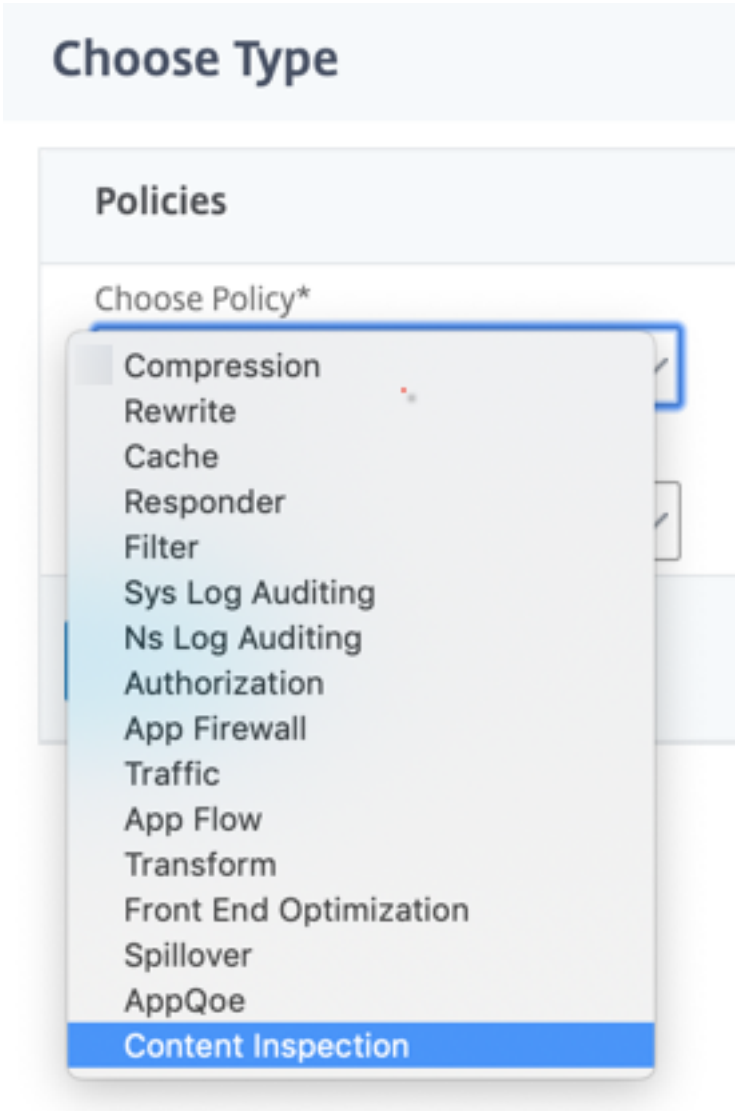




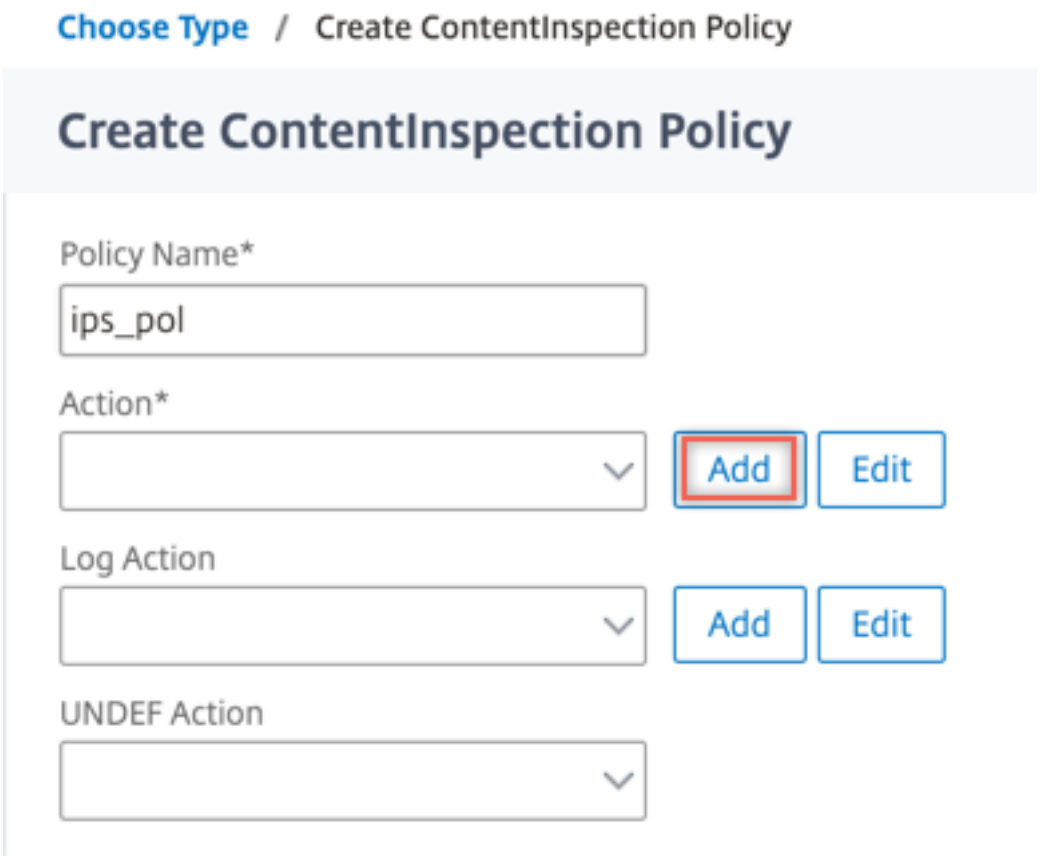
9. Accédez à **Secure Web Gateway > Servers virtuels Proxy > Ajouter**. Spécifiez un nom, une adresse IP et un port. Dans **Paramètres avancés**, sélectionnez **Stratégies**. Cliquez sur le signe « + ».



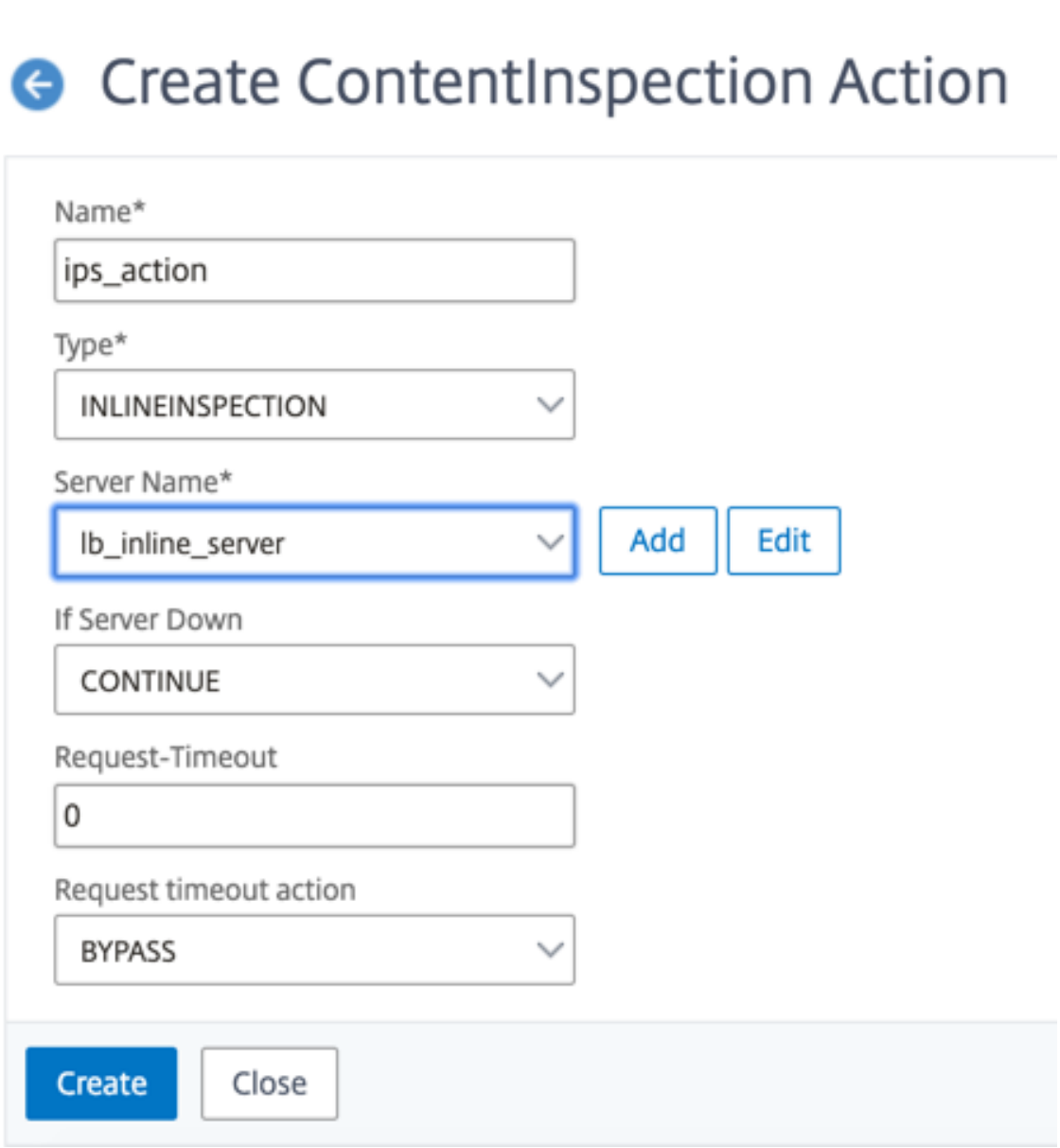
10. Dans **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.



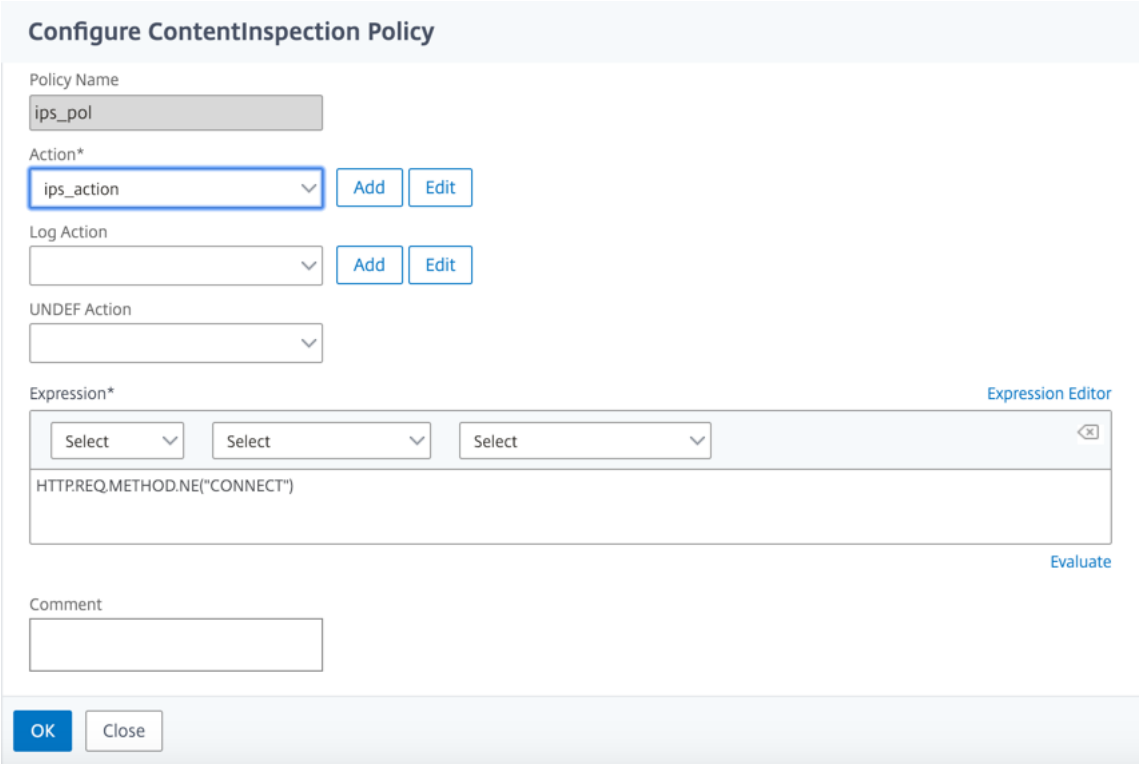
11. Cliquez sur **Ajouter**. Spécifiez un nom. Dans **Action**, cliquez sur **Ajouter**.



12. Spécifiez un nom. Dans **Type**, sélectionnez **INLINEINSPECTION**. Dans **Nom du serveur**, sélectionnez le serveur virtuel d'équilibrage de charge créé précédemment.



13. Cliquez sur **Créer**. Spécifiez la règle et cliquez sur **Créer**.



14. Cliquez sur **Bind**.
15. Cliquez sur **Terminé**.

Intégration de Citrix ADC avec des périphériques de sécurité passifs (système de détection d'intrusion)

August 20, 2021

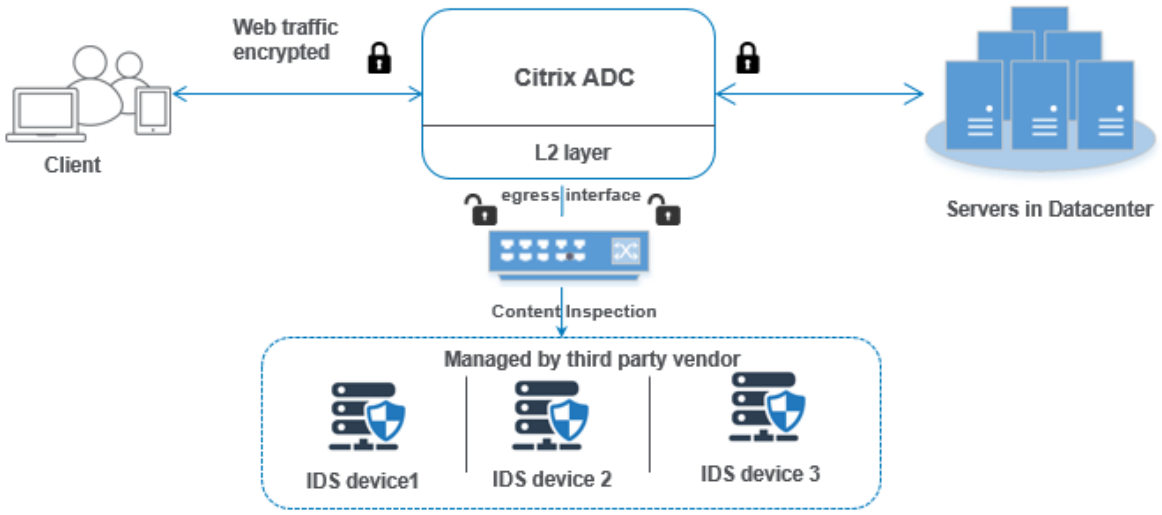
Une appliance Citrix ADC est désormais intégrée à des dispositifs de sécurité passifs tels que le système IDS (Intrusion Detection System). Ces périphériques passifs stockent des journaux et déclenchent des alertes lorsqu'ils détectent un trafic défectueux ou non conforme. Il génère également des rapports à des fins de conformité. Si l'appliance Citrix ADC est intégrée à deux périphériques IDS ou plus et qu'il y a un volume élevé de trafic, l'appliance peut équilibrer la charge des périphériques en clonant le trafic au niveau du serveur virtuel.

Pour une protection de sécurité avancée, une appliance Citrix ADC est intégrée aux périphériques de sécurité passifs tels que les IDS déployés en mode détection uniquement. Ces périphériques stockent le journal et déclenchent des alertes lorsqu'il détecte un trafic défectueux ou non conforme. Il génère également des rapports à des fins de conformité. Voici quelques-uns des avantages de l'intégration de Citrix ADC avec un périphérique IDS.

- **Inspection du trafic chiffré**. La plupart des dispositifs de sécurité contourne le trafic crypté, ce qui rend les serveurs vulnérables aux attaques. Une appliance Citrix ADC peut déchiffrer le trafic et l'envoyer aux périphériques IDS pour améliorer la sécurité réseau du client.
- **Déchargement des périphériques en ligne du traitement TLS/SSL**. Le traitement TLS/SSL est coûteux et il se traduit par une CPU système élevée dans les dispositifs de détection d'intrusion s'ils décryptent le trafic. Comme le trafic chiffré augmente rapidement, ces systèmes ne parviennent pas à décrypter et à inspecter le trafic chiffré. Citrix ADC aide à décharger le trafic vers les périphériques IDS du traitement TLS/SSL. Ce mode de déchargement des données donne lieu à un dispositif IDS prenant en charge un volume élevé d'inspection de la circulation.
- **Chargement des périphériques IDS d'équilibrage**. La charge de l'appliance Citrix ADC équilibre plusieurs périphériques IDS lorsqu'il y a un volume élevé de trafic en clonant du trafic au niveau du serveur virtuel.
- **Réplication du trafic vers des périphériques passifs**. Le trafic entrant dans l'appliance peut être répliqué vers d'autres périphériques passifs pour générer des rapports de conformité. Par exemple, peu d'organismes gouvernementaux prescrivaient que chaque transaction soit consignée dans certains appareils passifs.
- **Ventilation du trafic vers plusieurs appareils passifs**. Certains clients préfèrent dévier ou répliquer le trafic entrant sur plusieurs appareils passifs.
- **Sélection intelligente du trafic**. Chaque paquet entrant dans l'appliance peut ne pas l'être doit faire l'objet d'une inspection du contenu, par exemple le téléchargement de fichiers texte. L'utilisateur peut configurer l'appliance Citrix ADC pour sélectionner le trafic spécifique (par exemple les fichiers .exe) pour l'inspection et envoyer le trafic aux périphériques IDS pour le traitement des données.

Comment Citrix ADC est intégré au périphérique IDS avec connectivité L2

Le diagramme suivant montre comment IDS est intégré à une appliance Citrix ADC.



L'interaction des composants est donnée comme suit :

1. Un client envoie une requête HTTP/HTTPS à l'appliance Citrix ADC.
2. L'appliance intercepte le trafic et le réplique sur un périphérique IDS en fonction de l'évaluation de la stratégie d'inspection du contenu.
3. Si le trafic est chiffré, l'appliance déchiffre les données et les envoie sous forme de texte brut.
4. Sur la base de l'évaluation de la stratégie, l'appliance applique une action d'inspection du contenu de type « MIRROR ».
5. L'action comporte le service IDS ou le service d'équilibrage de charge (pour plusieurs intégrations de périphériques IDS) configuré.
6. Le périphérique IDS est configuré comme type de service d'inspection de contenu "Any" sur l'appliance. Le service d'inspection de contenu est alors associé au profil d'inspection de contenu de type « MIRROR » qui spécifie l'interface de sortie par laquelle les données doivent être transmises au périphérique IDS. Remarque : Vous pouvez également configurer une balise VLAN dans le profil d'inspection du contenu.
7. L'appliance réplique ensuite les données via l'interface de sortie vers un ou plusieurs périphériques IDS.
8. De même, lorsque le serveur principal envoie une réponse à Citrix ADC, l'appliance réplique les données et les transmet au périphérique IDS.
9. Si votre appliance est intégrée à un ou plusieurs périphériques IDS et si vous préférez équilibrer la charge des périphériques, vous pouvez utiliser le serveur virtuel d'équilibrage de charge.

Licences logicielles

Pour déployer l'intégration de périphérique en ligne, votre appliance Citrix ADC doit être provisionné avec l'une des licences suivantes :

1. ADC Premium
2. ADC Avancé
3. Telco Advanced
4. Telco Premium

Configuration de l'intégration du système de détection des intrusions

Vous pouvez intégrer le périphérique IDS avec Citrix ADC de deux manières différentes.

Scénario 1 : Intégration avec un seul périphérique IDS

Voici les étapes que vous devez configurer à l'aide de l'interface de ligne de commande.

1. Activer l'inspection du contenu
2. Ajouter un profil d'inspection de contenu de type MIRROR pour le service représentant le périphérique IDS.
3. Ajouter un service IDS de type "ANY"
4. Ajouter une action d'inspection de contenu de type "MIRROR"
5. Ajouter une stratégie d'inspection du contenu pour l'inspection IDS
6. Lier la stratégie d'inspection de contenu au service virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Activer l'inspection du contenu

Si vous souhaitez que l'appliance Citrix ADC envoie le contenu pour inspection aux périphériques IDS, vous devez activer les fonctions d'inspection de contenu et d'équilibrage de charge, indépendamment de l'exécution du déchiffrement.

À l'invite de commandes, tapez :

```
enable ns feature contentInspection LoadBalancing
```

Ajouter un profil d'inspection de contenu de type « MIRROR

Le profil d'inspection du contenu de type "MIRROR" explique comment vous pouvez vous connecter au périphérique IDS.
À l'invite de commandes, tapez.

```
add contentInspection profile <name> -type MIRROR -egressInterface <interface_name
> [-egressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 10
```


Ajouter un service IDS

Vous devez configurer un service de type “ANY” pour chaque périphérique IDS intégré à l’appliance. Le service possède les détails de configuration du périphérique IDS. Le service représente le périphérique IDS.

À l’invite de commandes, tapez :

```
add service <Service_name> <IP> ANY <Port> - contentinspectionProfileName <
Name> -healthMonitor OFF -usip ON -useproxyport OFF
```

Exemple :

```
add service IDS_service 1.1.1.1 ANY 8080 -contentInspectionProfileName
IDS_profile1 -healthMonitor OFF
```

Ajouter une action d’inspection de contenu de type MIRROR pour le service IDS

Après avoir activé la fonction Inspection du contenu, puis ajouté le profil IDS et le service, vous devez ajouter l’action Inspection du contenu pour traiter la demande. En fonction de l’action d’inspection du contenu, l’appliance peut supprimer, réinitialiser, bloquer ou envoyer des données au périphérique IDS.

À l’invite de commandes, tapez :

```
add ContentInspection action < action_name > -type MIRROR -serverName
Service_name/Vserver_name>
```

Exemple :

```
add ContentInspection action IDS_action -type MIRROR -serverName IDS_service
```

Ajouter une stratégie d’inspection du contenu pour l’inspection IDS

Après avoir créé une action d’inspection du contenu, vous devez ajouter des stratégies d’inspection du contenu pour évaluer les demandes d’inspection. La stratégie est basée sur une règle qui consiste en une ou plusieurs expressions. La stratégie évalue et sélectionne le trafic à inspecter en fonction de la règle.

À l’invite de commandes, tapez ce qui suit :

```
add contentInspection policy < policy_name > -rule <Rule> -action <action_name
>
```

Exemple :

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```


Lier la stratégie d'inspection de contenu au service virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Pour recevoir le trafic Web, vous devez ajouter un serveur virtuel d'équilibrage de charge.
À l'invite de commandes, tapez :

```
add lb vserver <name> <vserver name>
```

Exemple :

```
add lb vserver HTTP_vserver HTTP 1.1.1.3 8080
```

Lier la stratégie d'inspection de contenu au serveur virtuel de commutation de contenu ou à un serveur virtuel d'équilibrage de charge de type HTTP/SSL

Vous devez lier le serveur virtuel d'équilibrage de charge ou le serveur virtuel de commutation de contenu de type HTTP/SSL à la stratégie d'inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

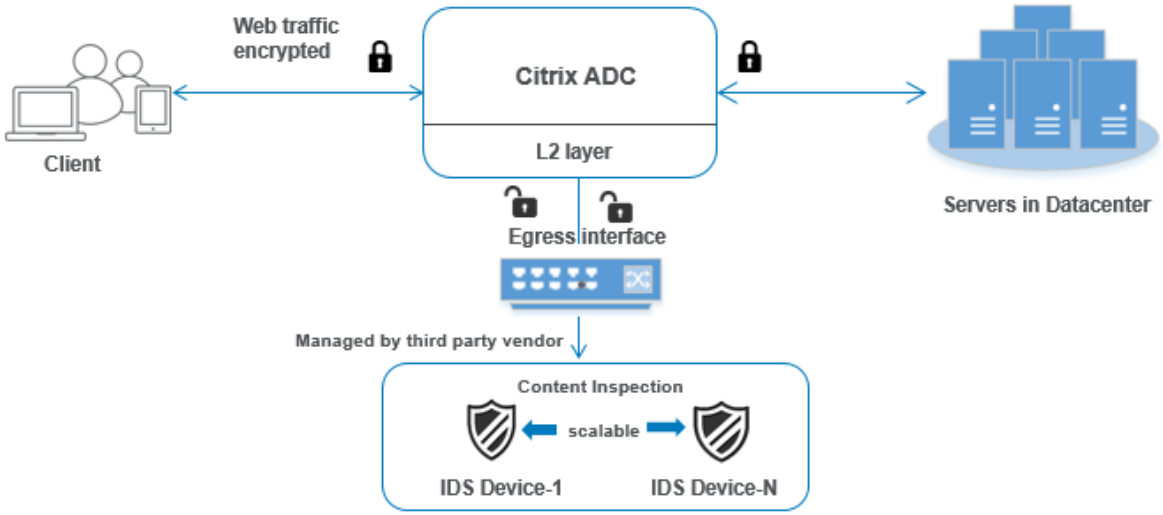
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Exemple :

```
bind lb vserver HTTP_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Scénario 2 : équilibrage de charge de plusieurs périphériques IDS

Si vous utilisez au moins deux périphériques IDS, vous devez équilibrer la charge des périphériques à l'aide de différents services d'inspection de contenu. Dans ce cas, la charge de l'appliance Citrix ADC équilibre les périphériques en plus de l'envoi d'un sous-ensemble de trafic à chaque périphérique. Pour les étapes de configuration de base, reportez-vous au scénario 1.



Voici les étapes que vous devez configurer à l'aide de l'interface de ligne de commande.

1. Ajouter un profil d'inspection de contenu 1 de type MIRROR pour le service IDS 1
2. Ajouter un profil d'inspection de contenu 2 de type MIRROR pour le service IDS 2
3. Ajouter le service IDS 1 de type ANY pour le périphérique IDS 1
4. Ajouter le service IDS 2 de type ANY pour le périphérique IDS 2
5. Ajouter un serveur virtuel d'équilibrage de charge de type ANY
6. Liez le service IDS 1 au serveur virtuel d'équilibrage de charge
7. Liez le service IDS 2 au serveur virtuel d'équilibrage de charge
8. Ajoutez une action d'inspection de contenu pour l'équilibrage de charge des périphériques IDS.
9. Ajouter une stratégie d'inspection du contenu à des fins d'inspection
10. Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL
11. Lier la stratégie d'inspection de contenu à un serveur virtuel d'équilibrage de charge de type HTTP/SSL

Ajouter un profil d'inspection de contenu 1 de type MIRROR pour le service IDS 1

La configuration IDS peut être spécifiée dans une entité appelée profil d'inspection du contenu. Le profil possède une collection de paramètres de périphérique. Le profil d'inspection de contenu1 est créé pour le service IDS 1.

À l'invite de commandes, tapez :

```
add contentInspection profile <name> -type ANY -egressInterface <interface_name
> [-egressVlan <positive_integer>]
```

Exemple :


```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 1
```

Ajouter le profil d'inspection de contenu 2 pour le type MIRROR pour le service IDS 2

Le profil d'inspection de contenu 2 est ajouté pour le service 2 et le périphérique en ligne communique avec l'appliance via l'interface de sortie 1/1.

À l'invite de commandes, tapez :

```
add contentInspection profile <name> -type MIRROR -egressInterface -egressVlan
 <positive_integer>]
```

Exemple :

```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 1
```

Ajouter le service IDS 1 de type ANY pour le périphérique IDS 1

Après avoir activé la fonction d'inspection du contenu et ajouté le profil en ligne, vous devez ajouter un service en ligne 1 pour que le périphérique en ligne 1 fasse partie de la configuration d'équilibrage de charge. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commandes, tapez :

```
add service <Service_name_1> <Pvt_IP1> ANY <Port> -contentInspectionProfileName
 <IDS_Profile_1> -usip ON -useproxyport OFF
```

Exemple :

```
add service IDS_service1 1.1.1.1 ANY 80 -contentInspectionProfileName
IDS_profile1 -usip ON -useproxyport OFF
```

> **Remarque**
>
> L'adresse IP mentionnée dans l'exemple est fictive.

Ajouter le service IDS 2 de type ANY pour le périphérique IDS 2

Après avoir activé la fonction d'inspection du contenu et ajouté le profil en ligne, vous devez ajouter un service en ligne 2 pour le périphérique en ligne 2. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commandes, tapez :

```
add service <Service_name_1> <Pvt_IP1> ANY -contentInspectionProfileName <
Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```


Exemple :

```
add service IDS_service 1 1.1.2 ANY 80 -contentInspectionProfileName
IDS_profile2
```

> **Remarque**
>
> L'adresse IP mentionnée dans l'exemple est fictive.

Ajouter un serveur virtuel d'équilibrage de charge

Après avoir ajouté le profil en ligne et les services, vous devez ajouter un serveur virtuel d'équilibrage de charge pour l'équilibrage de charge des services.

À l'invite de commandes, tapez :

```
add lb vserver <vserver_name> ANY <Pvt_IP3> <port>
```

Exemple :

```
add lb vserver lb-IDS_vserver ANY 1.1.1.2
```

Liez le service IDS 1 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur virtuel d'équilibrage de charge au premier service.

À l'invite de commandes, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-IDS_vserver IDS_service1
```

Liez le service IDS 2 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur au second service.

À l'invite de commandes, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-IDS_vserver IDS_service2
```


Ajouter une action d'inspection de contenu pour le service IDS

Après avoir activé la fonction Inspection du contenu, vous devez ajouter l'action Inspection du contenu pour gérer les informations de demande en ligne. En fonction de l'action sélectionnée, l'appliance supprime, réinitialise, bloque ou envoie du trafic vers le périphérique IDS.

À l'invite de commandes, tapez :

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>]
```

Exemple :

```
add ContentInspection action IDS_action -type MIRROR -serverName lb-IDS_vserver
```

Ajouter une stratégie d'inspection du contenu à des fins d'inspection

Après avoir créé une action Inspection du contenu, vous devez ajouter une stratégie d'inspection du contenu pour évaluer les demandes de service.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Exemple :

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Ajoutez un serveur virtuel de commutation de contenu ou d'équilibrage de charge pour accepter le trafic Web. Vous devez également activer la connexion layer2 sur le serveur virtuel.

Pour plus d'informations sur l'équilibrage de charge, reportez-vous à la rubrique Fonctionnement de l'équilibrage de charge.

À l'invite de commandes, tapez :

```
add lb vserver <name> <vserver name>
```

Exemple :

```
add lb vserver http_vserver HTTP 1.1.1.1 8080
```


Lier la stratégie d'inspection de contenu pour équilibrer la charge serveur virtuel de type HTTP/SSL

Vous devez lier le serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL à la stratégie d'inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

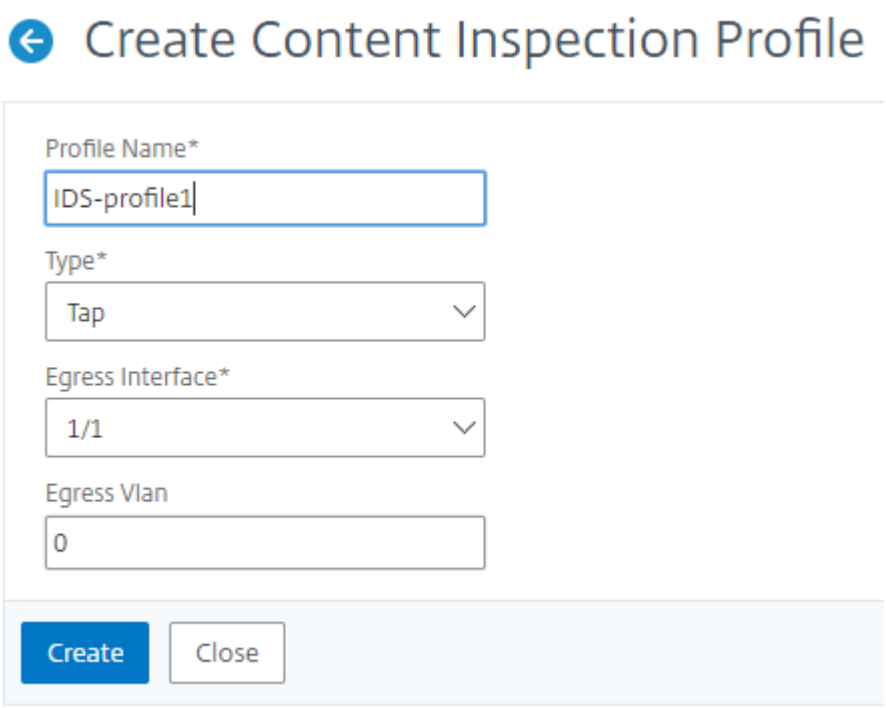
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <REQUEST>
```

Exemple :

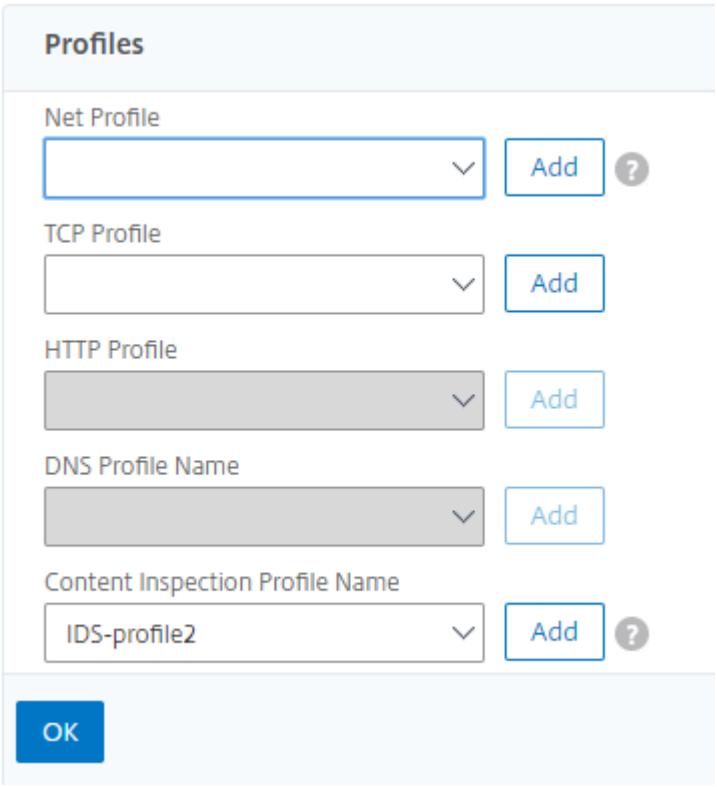
```
bind lb vserver http_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Configurer l'intégration de service en ligne à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité** > **Inspection du contenu> Profils d'inspection du contenu** .
2. Dans la page **Profil d'inspection du contenu**, cliquez sur **Ajouter**.
3. Dans la page **Créer un profil d'inspection de contenu**, définissez les paramètres suivants.
   a) Nom du profil. Nom du profil d'inspection de contenu pour IDS.
   b) Type. Sélectionnez les types de profils comme MIRROR.
   c) Interface de sortie. Interface par laquelle le trafic est envoyé à partir du Citrix ADC au périphérique IDS.
   d) VLAN de sortie (facultatif). ID de VLAN de l'interface par laquelle le trafic est envoyé au périphérique IDS.
4. Cliquez sur **Créer**.



5. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
6. Dans la page **Service d'équilibrage de** charge, entrez les détails du service d'inspection de contenu.
7. Dans la section **Paramètres avancés**, cliquez sur **Profils**.
8. Accédez à la section **Profils** et cliquez sur l'icône **Crayon** pour ajouter le profil d'inspection du contenu.
9. Cliquez sur **OK**.



10. Accédez à **Équilibrage de charge** > **Serveurs**. Ajoutez un serveur virtuel de type HTTP ou SSL.
11. Après avoir entré les détails du serveur, cliquez sur **OK** et à nouveau sur **OK**.
12. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
13. Accédez à la section **Stratégies** et cliquez sur l'icône **Crayon** pour configurer la stratégie d'inspection du contenu.
14. Dans la page **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.
15. Dans la section **Liaison de la stratégie**, cliquez sur « + » pour ajouter une stratégie d'inspection du contenu.
16. Dans la page **Créer une stratégie CI**, entrez un nom pour la stratégie d'inspection du contenu en ligne.
17. Dans le champ **Action**, cliquez sur le signe « + » pour créer une action d'inspection de contenu IDS de type MIRROR.
18. Dans la page **Créer une action CI**, définissez les paramètres suivants.

    a. Nom. Nom de la stratégie Inline d'inspection du contenu.

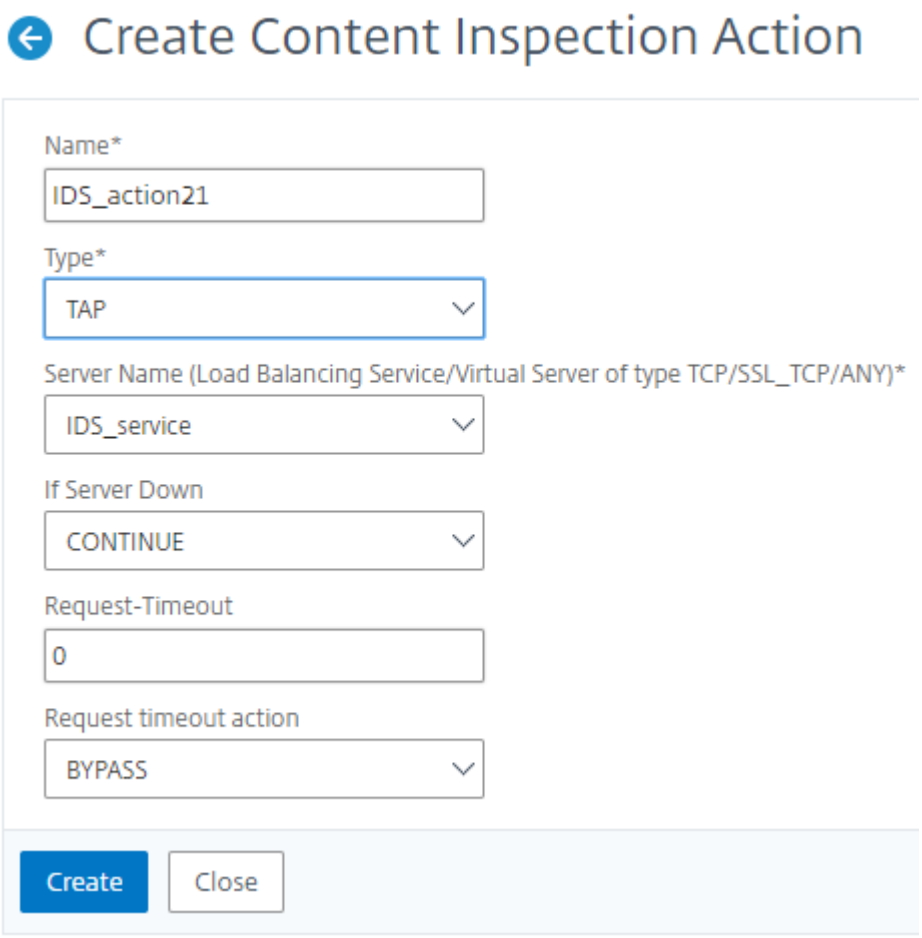
    b. Type. Sélectionnez le type comme MIRROR.
    c. Nom du serveur. Sélectionnez le nom du serveur/service en tant que périphériques Inline.

d. Si le serveur est en panne. Sélectionnez une opération si le serveur tombe en panne.

e. Demander le délai d'expiration. Sélectionnez une valeur de délai d'expiration. Les valeurs par défaut peuvent être utilisées.

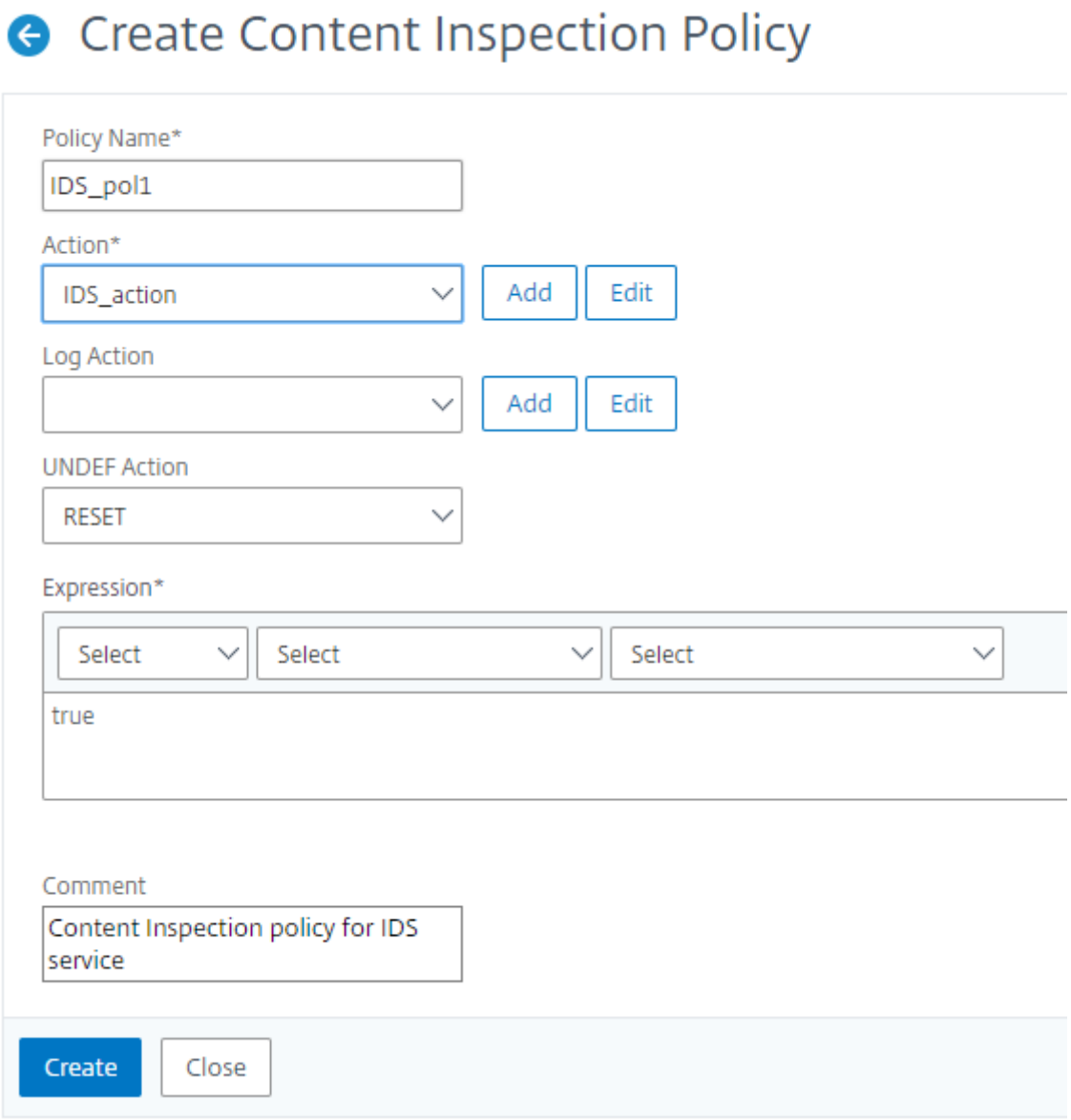
f. Demander une action de délai d'expiration. Sélectionnez une action de délai d'expiration. Les valeurs par défaut peuvent être utilisées.

19. Cliquez sur **Créer**.



20. Dans la page **Créer une stratégie CI**, entrez d'autres détails.
21. Cliquez sur **OK** et **Fermer**.

Pour plus d'informations sur la configuration de l'interface graphique Citrix ADC pour l'équilibrage de charge et la réplication du trafic vers les périphériques IDS, voir Équilibrage de charge.



Pour plus d'informations sur la configuration de l'interface graphique Citrix ADC pour l'équilibrage de charge et le transfert du trafic vers le serveur d'origine principal après la transformation du contenu, reportez-vous à la rubrique Équilibrage de charge .

Intégration de Citrix ADC couche 3 avec des périphériques de sécurité passifs (système de détection d'intrusion)

August 20, 2021

Une appliance Citrix ADC est désormais intégrée à des dispositifs de sécurité passifs tels que le sys-

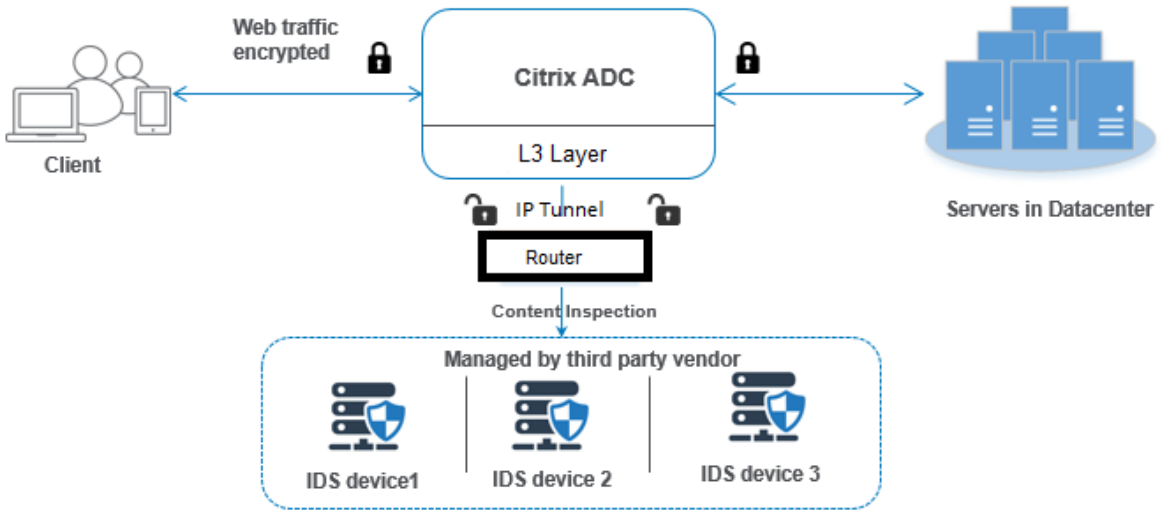
tème IDS (Intrusion Detection System). Dans cette configuration, l'appliance envoie en toute sécurité une copie du trafic d'origine aux périphériques IDS distants. Ces périphériques passifs stockent des journaux et déclenchent des alertes lorsqu'ils détectent un trafic défectueux ou non conforme. Il génère également des rapports à des fins de conformité. Si une appliance Citrix ADC est intégrée à deux périphériques IDS ou plus et qu'il y a un volume élevé de trafic, l'appliance peut équilibrer la charge des périphériques en clonant le trafic au niveau du serveur virtuel.

Pour une protection de sécurité avancée, une appliance Citrix ADC est intégrée aux périphériques de sécurité passifs tels que les IDS déployés en mode détection uniquement. Ces périphériques stockent le journal et déclenchent des alertes lorsqu'il détecte un trafic défectueux ou non conforme. Il génère également des rapports à des fins de conformité. Voici quelques-uns des avantages de l'intégration de Citrix ADC avec un périphérique IDS.

- **Inspection du trafic chiffré**. La plupart des dispositifs de sécurité contourne le trafic crypté, ce qui rend les serveurs vulnérables aux attaques. Une appliance Citrix ADC peut déchiffrer le trafic et l'envoyer aux périphériques IDS pour améliorer la sécurité réseau du client.
- **Déchargement des périphériques en ligne du traitement TLS/SSL**. Le traitement TLS/SSL est coûteux et il se traduit par une CPU système élevée dans les dispositifs de détection d'intrusion s'ils décryptent le trafic. Comme le trafic chiffré augmente rapidement, ces systèmes ne parviennent pas à décrypter et à inspecter le trafic chiffré. Citrix ADC aide à décharger le trafic vers les périphériques IDS du traitement TLS/SSL. Ce mode de déchargement des données donne lieu à un dispositif IDS prenant en charge un volume élevé d'inspection de la circulation.
- **Chargement des périphériques IDS d'équilibrage**. La charge de l'appliance Citrix ADC équilibre plusieurs périphériques IDS lorsqu'il y a un volume élevé de trafic en clonant du trafic au niveau du serveur virtuel.
- **Réplication du trafic vers des périphériques passifs**. Le trafic entrant dans l'appliance peut être répliqué vers d'autres périphériques passifs pour générer des rapports de conformité. Par exemple, peu d'organismes gouvernementaux prescrivaient que chaque transaction soit consignée dans certains appareils passifs.
- **Ventilation du trafic vers plusieurs appareils passifs**. Certains clients préfèrent dévier ou répliquer le trafic entrant sur plusieurs appareils passifs.
- **Sélection intelligente du trafic**. Chaque paquet entrant dans l'appliance peut ne pas l'être doit faire l'objet d'une inspection du contenu, par exemple le téléchargement de fichiers texte. L'utilisateur peut configurer l'appliance Citrix ADC pour sélectionner le trafic spécifique (par exemple les fichiers .exe) pour l'inspection et envoyer le trafic aux périphériques IDS pour le traitement des données.

Comment Citrix ADC est intégré au périphérique IDS avec connectivité L3

Le diagramme suivant montre comment l'IDS est intégré à une appliance Citrix ADC.



L'interaction des composants est donnée comme suit :

1. Un client envoie une requête HTTP/HTTPS à l'appliance Citrix ADC.
2. L'appliance intercepte le trafic et envoie les données aux périphériques IDS distants dans différents centres de données ou même dans un nuage. Cette intégration se fait par le biais de la couche 3 en tunnel IP. Pour plus d'informations sur le tunneling IP dans une appliance Citrix ADC, consultez la rubrique Tunnels IP.
3. Si le trafic est chiffré, l'appliance déchiffre les données et les envoie sous forme de texte brut.
4. Sur la base de l'évaluation de la stratégie, l'appliance applique une action d'inspection du contenu de type « MIRROR ».
5. L'action comporte un service IDS ou un service d'équilibrage de charge (pour plusieurs intégrations de périphériques IDS) configuré.
6. Le périphérique IDS est configuré comme type de service d'inspection de contenu "Any" sur l'appliance. Le service d'inspection de contenu est ensuite associé au profil d'inspection de contenu de type « MIROIR » et au paramètre tunnel qui spécifie l'interface de couche 3 tunnelée IP via laquelle les données sont transmises au périphérique IDS.

> **Remarque** Vous pouvez également configurer une balise VLAN dans le profil d'inspection du contenu.

1. De même, lorsque le serveur principal envoie une réponse à Citrix ADC, l'appliance réplique les données et les transmet au périphérique IDS.
2. Si votre appliance est intégrée à un ou plusieurs périphériques IDS et si vous préférez équilibrer la charge des périphériques, vous pouvez utiliser le serveur virtuel d'équilibrage de charge.

Licences logicielles

Pour déployer l'intégration IDS, votre appliance Citrix ADC doit être provisionné avec l'une des licences suivantes :

1. ADC Premium
2. ADC Avancé

Configuration de l'intégration du système de détection des intrusions

Vous pouvez intégrer un périphérique IDS à un Citrix ADC de deux manières différentes.

Scénario 1 : Intégration avec un seul périphérique IDS

Voici les étapes que vous devez configurer à l'aide de l'interface de ligne de commande.

1. Activer l'inspection du contenu
2. Ajouter un profil d'inspection de contenu de type MIRROR pour le service représentant le périphérique IDS.
3. Ajouter un service IDS de type "ANY"
4. Ajouter une action d'inspection de contenu de type "MIRROR"
5. Ajouter une stratégie d'inspection du contenu pour l'inspection IDS
6. Lier la stratégie d'inspection de contenu au service virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Activer l'inspection du contenu

Si vous souhaitez que l'appliance Citrix ADC envoie le contenu pour inspection aux périphériques IDS, vous devez activer les fonctions d'inspection de contenu et d'équilibrage de charge, indépendamment de l'exécution du déchiffrement.

À l'invite de commandes, tapez :

```
enable ns feature contentInspection LoadBalancing
```

Ajouter un profil d'inspection de contenu de type « MIRROR »

Le profil d'inspection du contenu de type "MIRROR" explique comment vous pouvez vous connecter au périphérique IDS.
À l'invite de commandes, tapez.

> **Remarque**

> Le paramètre de tunnel IP doit être utilisé uniquement pour la topologie IDS de couche 3. Sinon, vous devez utiliser l'interface de sortie avec l'option Egress VLAN.

```
add contentInspection profile <name> -type MIRROR -ipTunnel <iptunnel_name>
```

Exemple :

```
add contentInspection profile IDS_profile1 -type MIRROR -ipTunnel ipsect-
tunnel1
```

Ajouter un service IDS

Vous devez configurer un service de type "ANY" pour chaque périphérique IDS intégré à l'appliance. Le service possède les détails de configuration du périphérique IDS. Le service représente le périphérique IDS.

À l'invite de commandes, tapez :

```
add service <Service_name> <IP> ANY <Port> - contentinspectionProfileName <
Name> -healthMonitor OFF -usip ON -useproxyport OFF
```

Exemple :

```
add service IDS_service 1.1.1.1 ANY 8080 -contentInspectionProfileName
IDS_profile1 -healthMonitor OFF
```

Ajouter une action d'inspection de contenu de type MIRROR pour le service IDS

Après avoir activé la fonction Inspection du contenu, puis ajouté le profil IDS et le service, vous devez ajouter l'action Inspection du contenu pour traiter la demande. En fonction de l'action d'inspection du contenu, l'appliance peut supprimer, réinitialiser, bloquer ou envoyer des données au périphérique IDS.

À l'invite de commandes, tapez :

```
add ContentInspection action < action_name > -type MIRROR -serverName
Service_name/Vserver_name>
```

Exemple :

```
add ContentInspection action IDS_action -type MIRROR -serverName IDS_service
```

Ajouter une stratégie d'inspection du contenu pour l'inspection IDS

Après avoir créé une action d'inspection du contenu, vous devez ajouter des stratégies d'inspection du contenu pour évaluer les demandes d'inspection. La stratégie est basée sur une règle qui consiste en une ou plusieurs expressions. La stratégie évalue et sélectionne le trafic à inspecter en fonction de la règle.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy < policy_name > -rule <Rule> -action <action_name
>
```

Exemple :

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Lier la stratégie d'inspection de contenu au service virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Pour recevoir le trafic Web, vous devez ajouter un serveur virtuel d'équilibrage de charge.
À l'invite de commandes, tapez :

```
add lb vserver <name> <vserver name>
```

Exemple :

```
add lb vserver HTTP_vserver HTTP 1.1.1.3 8080
```

Lier la stratégie d'inspection de contenu au serveur virtuel de commutation de contenu ou à un serveur virtuel d'équilibrage de charge de type HTTP/SSL

Vous devez lier le serveur virtuel d'équilibrage de charge ou le serveur virtuel de commutation de contenu de type HTTP/SSL à la stratégie d'inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

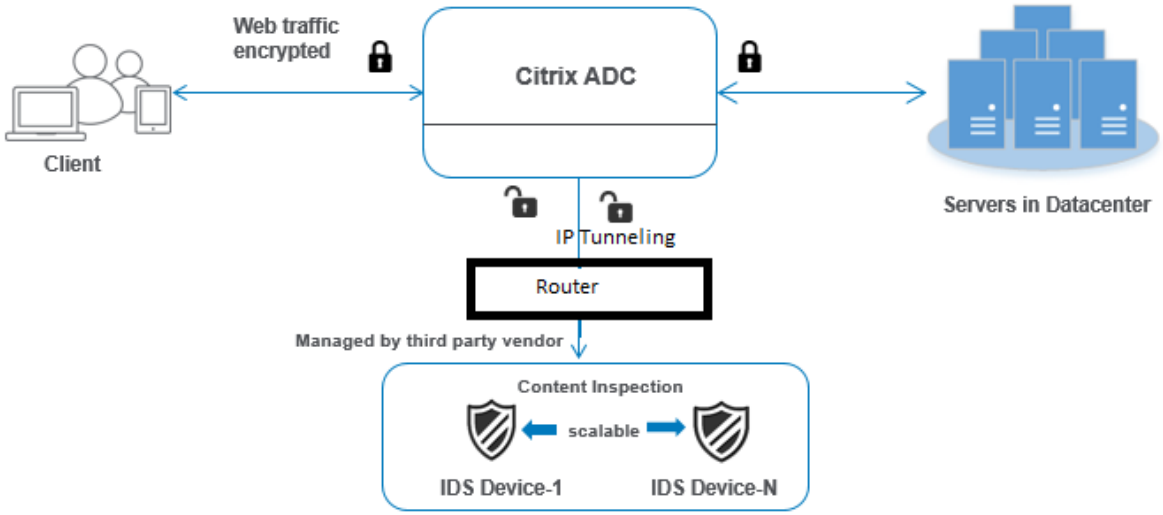
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Exemple :

```
bind lb vserver HTTP_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Scénario 2 : équilibrage de charge de plusieurs périphériques IDS

Si vous utilisez au moins deux périphériques IDS, vous devez équilibrer la charge des périphériques IDS à l'aide de différents services d'inspection de contenu. Dans ce cas, la charge de l'appliance Citrix ADC équilibre les périphériques en plus de l'envoi d'un sous-ensemble de trafic à chaque périphérique.
Pour les étapes de configuration de base, reportez-vous au scénario 1.



Voici les étapes que vous devez configurer à l'aide de l'interface de ligne de commande.

1. Ajouter un profil d'inspection de contenu 1 de type MIRROR pour le service IDS 1
2. Ajouter un profil d'inspection de contenu 2 de type MIRROR pour le service IDS 2
3. Ajouter le service IDS 1 de type ANY pour le périphérique IDS 1
4. Ajouter le service IDS 2 de type ANY pour le périphérique IDS 2
5. Ajouter un serveur virtuel d'équilibrage de charge de type ANY
6. Liez le service IDS 1 au serveur virtuel d'équilibrage de charge
7. Liez le service IDS 2 au serveur virtuel d'équilibrage de charge
8. Ajoutez une action d'inspection de contenu pour l'équilibrage de charge des périphériques IDS.
9. Ajouter une stratégie d'inspection du contenu à des fins d'inspection
10. Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL
11. Lier la stratégie d'inspection de contenu à un serveur virtuel d'équilibrage de charge de type HTTP/SSL

Ajouter un profil d'inspection de contenu 1 de type MIRROR pour le service IDS 1

La configuration IDS peut être spécifiée dans une entité appelée profil d'inspection du contenu. Le profil possède une collection de paramètres de périphérique. Le profil d'inspection de contenu1 est créé pour le service IDS 1.

> **Remarque** : le paramètre de tunnel
> IP doit être utilisé uniquement pour la topologie IDS de couche 3. Sinon, vous devez utiliser l'interface de sortie avec l'option Egress VLAN.

À l'invite de commandes, tapez :

```
add contentInspection profile <name> -type ANY - ipTunnel <iptunnel_name>
```


Exemple :

```
add contentInspection profile IDS_profile1 -type MIRROR - ipTunnel ipsect_tunnel1
```

Ajouter le profil d'inspection de contenu 2 pour le type MIRROR pour le service IDS 2

Le profil d'inspection de contenu 2 est ajouté pour le service 2 et le périphérique en ligne communique avec l'appliance via l'interface de sortie 1/1.

À l'invite de commandes, tapez :

```
add contentInspection profile <name> -type ANY - ipTunnel <iptunnel_name>
```

Exemple :

```
add contentInspection profile IDS_profile2 -type ANY - ipTunnel ipsect_tunnel2
```

Ajouter le service IDS 1 de type ANY pour le périphérique IDS 1

Après avoir activé la fonction d'inspection du contenu et ajouté le profil en ligne, vous devez ajouter un service en ligne 1 pour que le périphérique en ligne 1 fasse partie de la configuration d'équilibrage de charge. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commandes, tapez :

```
add service <Service_name_1> <Pvt_IP1> ANY <Port> -contentInspectionProfileName
 <IDS_Profile_1> -usip ON -useproxyport OFF
```

Exemple :

```
add service IDS_service1 1.1.1.1 ANY 80 -contentInspectionProfileName
IDS_profile1 -usip ON -useproxyport OFF
```

> **Remarque** :
>
> L'adresse IP mentionnée dans l'exemple est fictive.

Ajouter le service IDS 2 de type ANY pour le périphérique IDS 2

Après avoir activé la fonction d'inspection du contenu et ajouté le profil en ligne, vous devez ajouter un service en ligne 2 pour le périphérique en ligne 2. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commandes, tapez :

```
add service <Service_name_1> <Pvt_IP1> ANY -contentInspectionProfileName <
Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```


Exemple :

```
add service IDS_service 1 1.1.2 ANY 80 -contentInspectionProfileName
IDS_profile2
```

> **Remarque** :
>
> L'adresse IP mentionnée dans l'exemple est fictive.

Ajouter un serveur virtuel d'équilibrage de charge

Après avoir ajouté le profil en ligne et les services, vous devez ajouter un serveur virtuel d'équilibrage de charge pour l'équilibrage de charge des services.

À l'invite de commandes, tapez :

```
add lb vserver <vserver_name> ANY <Pvt_IP3> <port>
```

Exemple :

```
add lb vserver lb-IDS_vserver ANY 1.1.1.2
```

Liez le service IDS 1 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur virtuel d'équilibrage de charge au premier service.

À l'invite de commandes, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-IDS_vserver IDS_service1
```

Liez le service IDS 2 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur au second service.

À l'invite de commandes, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-IDS_vserver IDS_service2
```


Ajouter une action d'inspection de contenu pour le service IDS

Après avoir activé la fonction Inspection du contenu, vous devez ajouter l'action Inspection du contenu pour gérer les informations de demande en ligne. En fonction de l'action sélectionnée, l'appliance supprime, réinitialise, bloque ou envoie du trafic vers le périphérique IDS.

À l'invite de commandes, tapez :

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>]
```

Exemple :

```
add ContentInspection action IDS_action -type MIRROR -serverName lb-IDS_vserver
```

Ajouter une stratégie d'inspection du contenu à des fins d'inspection

Après avoir créé une action Inspection du contenu, vous devez ajouter la stratégie d'inspection du contenu pour évaluer les demandes de service.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Exemple :

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Ajoutez un serveur virtuel de commutation de contenu ou d'équilibrage de charge pour accepter le trafic Web. Vous devez également activer la connexion layer2 sur le serveur virtuel.

Pour plus d'informations sur l'équilibrage de charge, reportez-vous à la rubrique Fonctionnement de l'équilibrage de charge .

À l'invite de commandes, tapez :

```
add lb vserver <name> <vserver name>
```

Exemple :

```
add lb vserver http_vserver HTTP 1.1.1.1 8080
```


Lier la stratégie d'inspection de contenu pour équilibrer la charge serveur virtuel de type HTTP/SSL

Vous devez lier le serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL à la stratégie d'inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

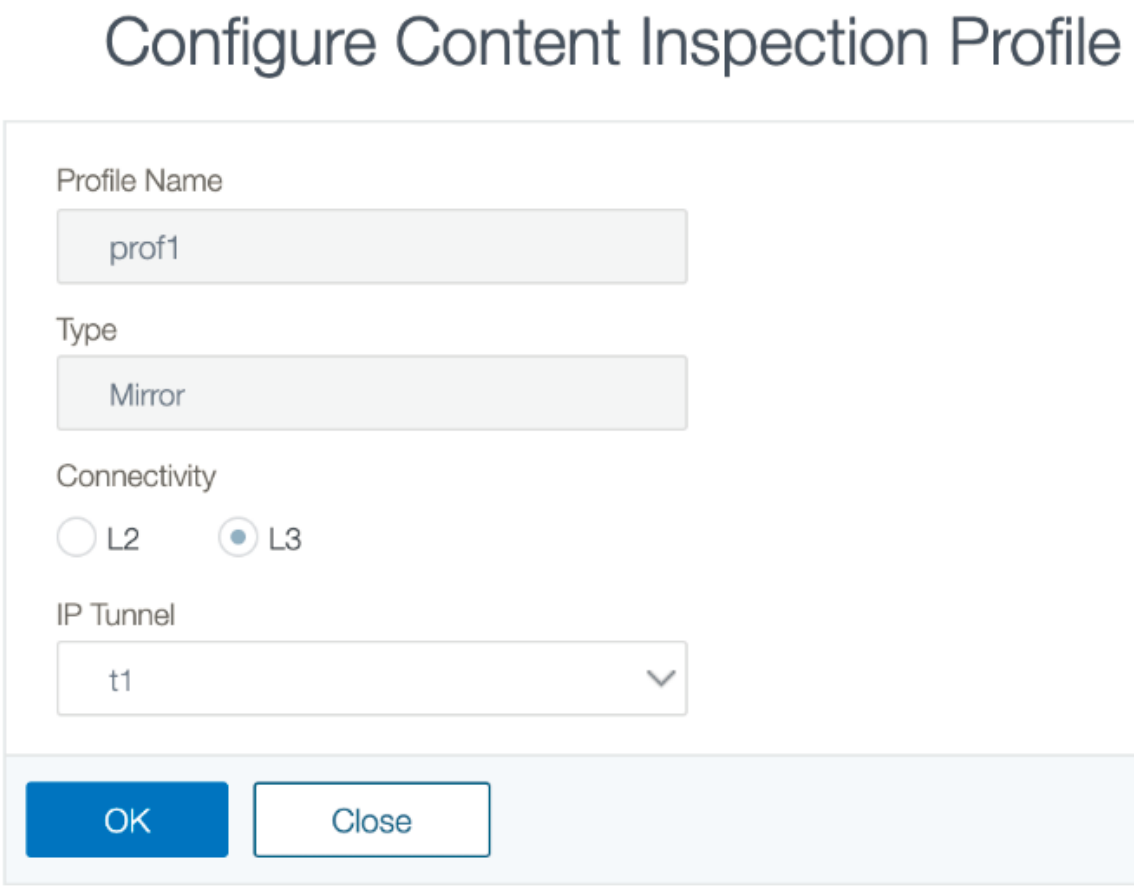
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <REQUEST>
```

Exemple :

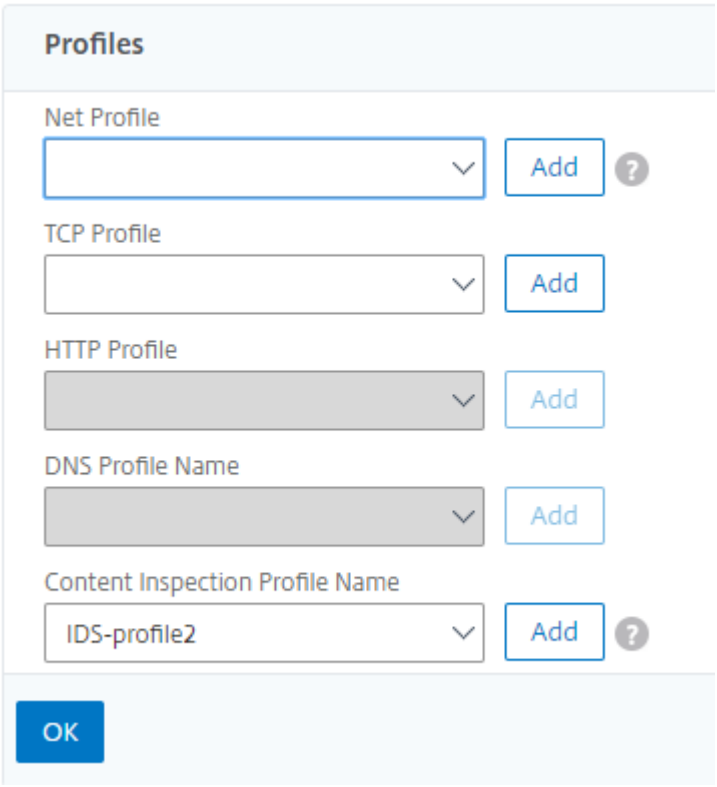
```
bind lb vserver http_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Configurer l'intégration de service en ligne à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Sécurité** > **Inspection du contenu** > **Profils ContentInspection** .
2. Dans la page **Profil ContentInspection**, cliquez sur **Ajouter**.
3. Dans la page **Créer ContentInspectionProfile**, définissez les paramètres suivants.
    a) Nom du profil. Nom du profil d'inspection de contenu pour IDS.
    b) Type. Sélectionnez les types de profils comme MIRROR.
    c) Connectivité. Interface de couche 2 ou couche 3.
    d) Tunnel IP. Sélectionnez le canal de communication réseau entre les deux réseaux.
4. Cliquez sur **Créer**.



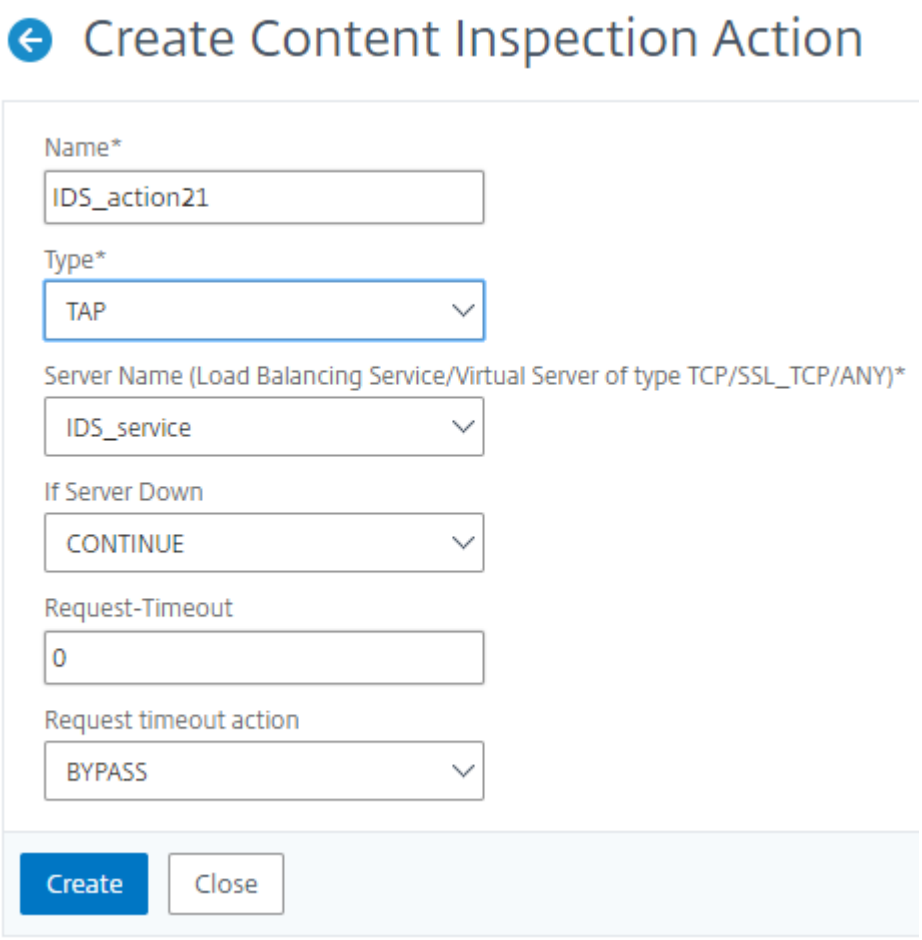
5. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
6. Dans la page **Service d'équilibrage de** charge, entrez les détails du service d'inspection de contenu.
7. Dans la section **Paramètres avancés**, cliquez sur **Profils**.
8. Accédez à la section **Profils** et cliquez sur l'icône **Crayon** pour ajouter le profil d'inspection du contenu.
9. Cliquez sur **OK**.



10. Accédez à **Équilibrage de charge** > **Serveurs**. Ajoutez un serveur virtuel de type HTTP ou SSL.
11. Après avoir entré les détails du serveur, cliquez sur **OK** et à nouveau sur **OK**.
12. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
13. Accédez à la section **Stratégies** et cliquez sur l'icône **Crayon** pour configurer la stratégie d'inspection du contenu.
14. Dans la page **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.
15. Dans la section **Liaison de la stratégie**, cliquez sur « + » pour ajouter une stratégie d'inspection du contenu.
16. Dans la page **Créer une stratégie CI**, entrez un nom pour la stratégie d'inspection du contenu en ligne.
17. Dans le champ **Action**, cliquez sur le signe « + » pour créer une action d'inspection de contenu IDS de type MIRROR.
18. Dans la page **Créer une action CI**, définissez les paramètres suivants.
    a) Nom. Nom de la stratégie Inline d'inspection du contenu.
    b) Type. Sélectionnez le type comme MIRROR.
    c) Nom du serveur. Sélectionnez le nom du serveur/service en tant que périphériques Inline.

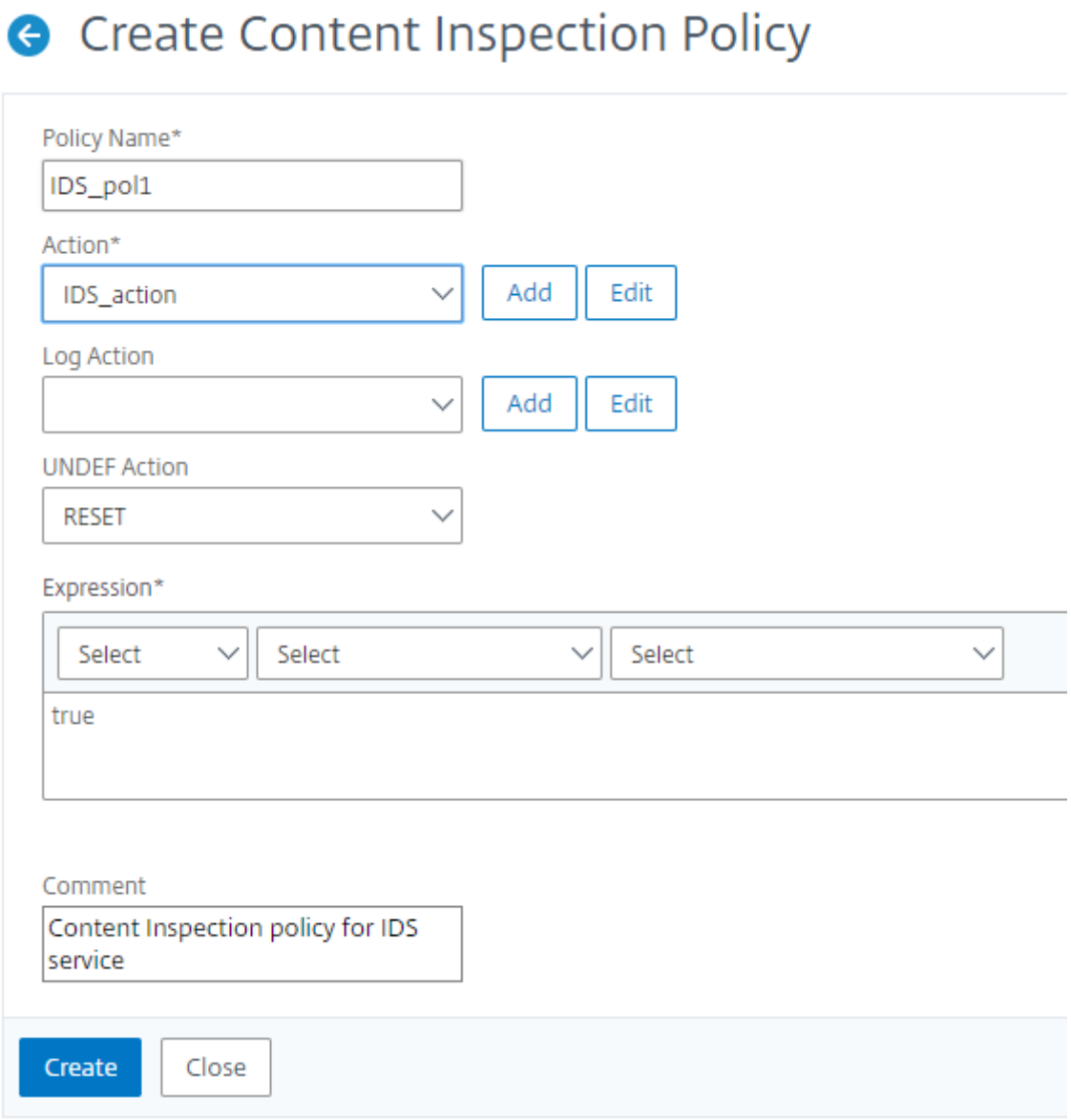
d) Si le serveur est hors service. Sélectionnez une opération si le serveur tombe en panne.
e) Demander le délai d'expiration. Sélectionnez une valeur de délai d'expiration. Les valeurs par défaut peuvent être utilisées.
f) Demander une action de délai d'expiration. Sélectionnez une action de délai d'expiration. Les valeurs par défaut peuvent être utilisées.

19. Cliquez sur **Créer**.



20. Dans la page **Créer une stratégie CI**, entrez d'autres détails.
21. Cliquez sur **OK** et **Fermer**.

Pour plus d'informations sur la configuration de l'interface graphique Citrix ADC pour l'équilibrage de charge et la réplication du trafic sur les appareils IDS, voir Équilibrage de charge.



Pour plus d'informations sur la configuration de l'interface graphique Citrix ADC pour l'équilibrage de charge et le transfert du trafic vers le serveur d'origine principal après la transformation du contenu, consultez Équilibrage de charge.

Statistiques d'inspection de contenu pour ICAP, IPS et IDS

January 21, 2021

Les statistiques d'inspection de contenu pour les périphériques ICAP, IDS (Inline Device Integration) et IPS (Intrusion Prevention System) sont une sortie détaillée (résumé) des détails de demande, de réponse et d'action du serveur.

Les statistiques d'inspection du contenu sont un ensemble de données statistiques qui incluent la requête HTTP/HTTPS envoyée pour l'inspection du contenu. Réponse HTTP/HTTPS reçue des périphériques IPS, IDS et ICAP et action serveur back-end.

Pour afficher les statistiques d'inspection de contenu à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
stat contentInspection
```

```
ContentInspection Stats

Inline Statistics
                                  Total
Requests                           10
Responses                           6
Request Bytes Sent                 3235
Request Bytes Received             2977
Response Bytes Sent                17302
Response Bytes Received            19681
Serverdown Reset Action taken       1
Serverdown Drop Action taken        0
Serverdown BYPASS Action taken      0
Inline device Generated Response    3

Mirror Statistics
                                  Total
Requests                           4
Responses                          4
Requests Bytes Sent               2763
Responses Bytes Sent              16732
Serverdown Reset Action taken      0
Serverdown Drop Action taken       0
Serverdown BYPASS Action taken     1

ICAP Statistics
                                  Total
REQMOD requests Sent                6
RESPMOD requests Sent               4
Preview requests                    1
204 Responses Received              6
100 Continue Responses Received     1
204 NO content Received             5
Adaptive Requests                   0
Adaptive Responses                  4
Callout requests Initiated          1
```



```
Callout requests completed          1
ICAP Req/Resp Errors handled        1
Serverdown Reset Action taken       1
Serverdown Drop Action taken        0
Serverdown BYPASS Action taken      1

Done
<!--NeedCopy-->
```

Proxy de transfert SSL

August 20, 2021

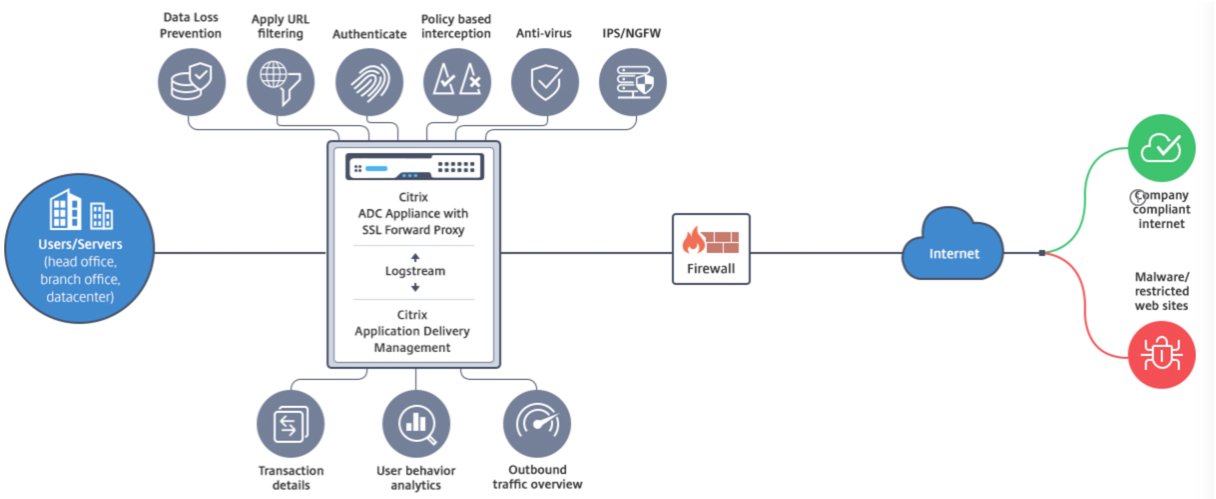
Remarque : La fonctionnalité proxy de transfert SSL est disponible avec la licence ADC Premium.

Le trafic Web a augmenté de façon exponentielle ces dernières années, et les entreprises comptent de plus en plus sur Internet pour leurs activités quotidiennes. Cela, combiné à l'émergence de points de terminaison, de mobilité et de BYOD plus diversifiés, ainsi qu'à une base croissante d'attaquants, rend les utilisateurs cibles faciles de logiciels malveillants modernes. Ils sont de plus en plus vulnérables au vol d'identité et au fait que leurs données soient compromises. Traditionnellement, les entreprises ont inspecté le trafic HTTP à la recherche de logiciels malveillants et de virus. Ils ont contourné le trafic HTTP/TLS, car il n'était pas aussi important. Il a été utilisé avec parcimonie pour des contenus sensibles et fiables. Mais cela a changé rapidement car la plupart des sites Internet publics préfèrent désormais utiliser HTTPS pour protéger la vie privée des utilisateurs. Par conséquent, l'incapacité d'inspecter les paquets chiffrés permet des logiciels malveillants ou des intrusions dans le réseau d'entreprise. La solution proxy de transfert SSL offre des outils que les entreprises peuvent utiliser pour se protéger contre les menaces Internet.

Un proxy est un serveur qui contrôle tout le trafic entre les utilisateurs et les applications Internet ou SaaS. Puisque tout le trafic passe par ce proxy, il exécute des fonctions liées à la sécurité, telles que l'authentification des utilisateurs et la catégorisation des URL.

La figure suivante présente une vue d'ensemble de l'implémentation du proxy de transfert SSL. Le trafic circule à travers le réseau de l'entreprise à partir du siège social, des succursales, du centre de données et des employés distants. Une appliance Citrix ADC située à la périphérie du réseau agit comme proxy. L'appliance peut fonctionner en mode proxy transparent ou en mode proxy explicite et propose des contrôles pour intercepter le trafic Internet, y compris HTTPS. Les stratégies configurées sur l'appliance déterminent si elle intercepte, contourne ou bloque une demande particulière. L'accès aux sites restreints peut être bloqué à l'aide du filtrage d'URL. Un utilisateur est authentifié avant de se connecter au réseau d'entreprise. Toutes les demandes et réponses sont marquées pour identifier l'utilisateur, et l'accès au site Internet est catégorisé. L'activité de l'utilisateur est enregistrée et

utilisée pour générer des rapports. En cas de violation, les administrateurs peuvent isoler le système infecté, déterminer si les périphériques des autres utilisateurs qui ont visité ce site Web sont compromis et prendre les mesures appropriées. Lorsque vous intégrez Citrix Application Delivery Management (ADM) avec le proxy de transfert SSL, l'activité utilisateur consignée et les enregistrements suivants dans l'appliance sont exportés vers Citrix ADM à l'aide de `logstream`. Citrix ADM rassemble et présente des informations sur les activités des utilisateurs, depuis les sites Web visités jusqu'au temps passé en ligne. Il fournit également des informations sur l'utilisation de la bande passante et les menaces détectées, telles que les logiciels malveillants et les sites de phishing. Vous pouvez utiliser ces mesures clés pour surveiller votre réseau et utiliser la fonction proxy de transfert SSL pour prendre des mesures correctives.



Le proxy de transfert SSL permet aux directeurs informatiques d'effectuer les opérations suivantes :

- Obtenez une visibilité sur le trafic sécurisé autrement contourné.
- Bloquez l'accès aux sites malveillants ou inconnus et évitez d'infecter les utilisateurs au sein de l'entreprise.
- Contrôlez l'accès à certains sites Web, tels que le courrier personnel, les réseaux sociaux et les sites Web de recherche d'emploi, à partir du réseau d'entreprise.
- Appliquez des stratégies de contrôle de contenu intelligentes pour garantir une productivité maximale de l'utilisateur.

Mise en route de la fonctionnalité de proxy de transfert SSL

August 20, 2021

Important :

- La vérification OCSP nécessite une connexion Internet pour vérifier la validité des certificats. Si votre appliance n'est pas accessible depuis Internet à l'aide de l'adresse NSIP, ajoutez des listes

de contrôle d'accès (ACL) pour effectuer NAT à partir de l'adresse NSIP à l'adresse SNIP du sous-réseau (SNIP). Le SNIP doit pouvoir accéder à Internet. Par exemple,

```
add ns acl a1 ALLOW -srcIP = <NSIP> -destIP  "!="
    10.0.0.0-10.255.255.255

add rnat RNAT-1 a1

bind rnat RNAT-1 -<SNIP>

apply acls
<!--NeedCopy-->
```

- Spécifiez un serveur de noms DNS pour résoudre les noms de domaine.
- Assurez-vous que la date de l'appliance est synchronisée avec les serveurs NTP. Si la date n'est pas synchronisée, l'appliance ne peut pas vérifier efficacement si un certificat de serveur d'origine est expiré.

Pour utiliser la fonctionnalité de transfert de proxy SSL, vous devez effectuer les tâches suivantes :

- Ajoutez un serveur proxy en mode explicite ou transparent.
- Activer l'interception SSL.
  - Configurez un profil SSL.
  - Ajouter et lier des stratégies SSL au serveur proxy.
  - Ajoutez et liez une paire de clés de certification CA pour l'interception SSL.

Remarque :

Une appliance ADC configurée en mode proxy transparent peut intercepter uniquement les protocoles HTTP et HTTPS. Pour contourner tout autre protocole, tel que telnet, vous devez ajouter la stratégie d'écoute suivante sur le serveur virtuel proxy.

Le serveur virtuel accepte désormais uniquement le trafic entrant HTTP et HTTPS.

```
set cs vserver transparent-pxy1 PROXY * * -cltTimeout 180 -Listenpolicy
    "CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443)"`
<!--NeedCopy-->
```

Vous devrez peut-être configurer les fonctionnalités suivantes, en fonction de votre déploiement :

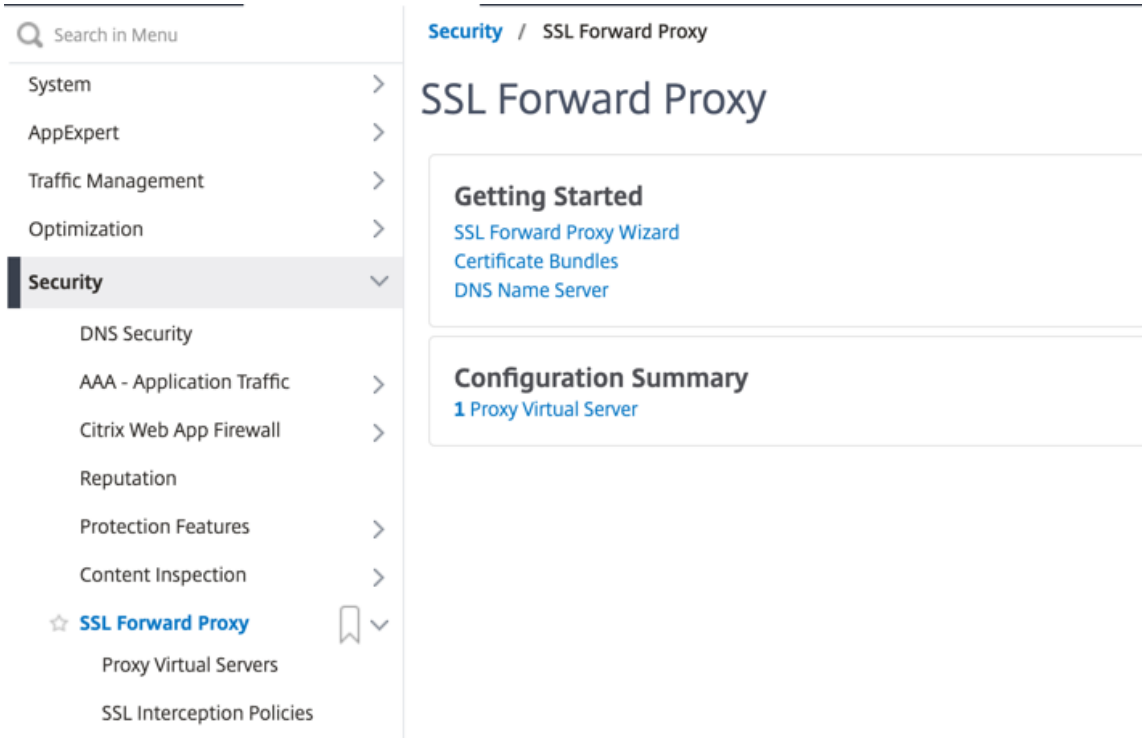
- Service d'authentification (recommandé) — pour authentifier les utilisateurs. Sans le service d'authentification, l'activité de l'utilisateur est basée sur l'adresse IP du client.
- Filtrage d'URL : pour filtrer les URL par catégories, score de réputation et listes d'URL.
- Analytics : permet d'afficher l'activité utilisateur, les indicateurs de risque utilisateur, la consommation de bande passante et les transactions dans Citrix Application Delivery Management (ADM).

Remarque : SSL Forward Proxy implémente la plupart des standards HTTP et HTTPS typiques suivis de produits similaires. Cette implémentation est faite sans navigateur spécifique à l'esprit et est compatible avec la plupart des navigateurs courants. SSL Forward Proxy a été testé avec les navigateurs courants et les versions récentes de Google Chrome, Internet Explorer et Mozilla Firefox.

Assistant de transfert de proxy SSL

L'assistant de transfert de proxy SSL fournit aux administrateurs un outil pour gérer l'intégralité du déploiement de proxy de transfert SSL à l'aide d'un navigateur Web. Il aide les clients à mettre rapidement en place un service proxy SSL avancé et aide à simplifier la configuration en suivant une séquence d'étapes bien définies.

1. Accédez à **Sécurité > Proxy de transfert SSL**. Dans **Mise en route**, cliquez sur **Assistant Proxy Transférer SSL**.



2. Suivez les étapes de l'Assistant pour configurer votre déploiement.

Ajouter une stratégie d'écoute au serveur proxy transparent

1. Accédez à **Sécurité > Proxy de transfert SSL** > **Serveurs virtuels proxy** . Sélectionnez le serveur proxy transparent et cliquez sur **Modifier**.
2. Modifiez **les paramètres de base**, puis cliquez sur **Plus**.
3. Dans **Priorité d'écoute**, entrez 1.

4. Dans **Listen Policy Expression**, entrez l'expression suivante :

```
(CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
<!--NeedCopy-->
```

Cette expression suppose des ports standard pour le trafic HTTP et HTTPS. Si vous avez configuré différents ports, par exemple 8080 pour HTTP ou 8443 pour HTTPS, modifiez l'expression pour refléter ces ports.

Limitations

Le proxy de transfert SSL n'est pas pris en charge dans une configuration de cluster, dans les partitions d'administration et sur une appliance Citrix ADC FIPS.

Modes proxy

August 20, 2021

L'appliance Citrix ADC agit en tant que proxy d'un client pour se connecter à Internet et aux applications SaaS. En tant que proxy, il accepte tout le trafic et détermine le protocole du trafic. Sauf si le trafic est HTTP ou SSL, il est transféré à la destination telle quelle. Lorsque l'appliance reçoit une demande d'un client, elle l'intercepte et exécute certaines actions, telles que l'authentification utilisateur, la catégorisation du site et la redirection. Il utilise des stratégies pour déterminer le trafic à autoriser et le trafic à bloquer.

L'appliance gère deux sessions différentes, l'une entre le client et le proxy et l'autre entre le proxy et le serveur d'origine. Le proxy s'appuie sur des stratégies définies par le client pour autoriser ou bloquer le trafic HTTP et HTTPS. Par conséquent, il est important que vous définissiez des stratégies pour contourner les données sensibles, telles que les informations financières. L'appliance offre un ensemble complet d'attributs de trafic de couche 4 à couche 7 et d'attributs d'identité utilisateur pour créer des stratégies de gestion du trafic.

Pour le trafic SSL, le proxy vérifie le certificat du serveur d'origine et établit une connexion légitime avec le serveur. Il émule ensuite le certificat de serveur, le signe à l'aide d'un certificat d'autorité de certification installé sur Citrix ADC et présente le certificat de serveur créé au client. Vous devez ajouter le certificat de l'autorité de certification en tant que certificat approuvé au navigateur du client pour que la session SSL soit correctement établie.

L'appliance prend en charge les modes proxy transparents et explicites. En mode proxy explicite, le client doit spécifier une adresse IP dans son navigateur, à moins que l'organisation n'envoie le paramètre sur le périphérique du client. Cette adresse est l'adresse IP d'un serveur proxy configuré sur

l'appliance ADC. Toutes les demandes client sont envoyées à cette adresse IP. Pour le proxy explicite, vous devez configurer un serveur virtuel de commutation de contenu de type PROXY et spécifier une adresse IP et un numéro de port valide.

Le proxy transparent, comme son nom l'indique, est transparent pour le client. En d'autres termes, les clients peuvent ne pas savoir qu'un serveur proxy effectue la médiation de leurs demandes. L'appliance ADC est configurée dans un déploiement en ligne et accepte de manière transparente tout le trafic HTTP et HTTPS. Pour le proxy transparent, vous devez configurer un serveur virtuel de commutation de contenu de type PROXY, avec des astérisques (*) comme adresse IP et port. Lorsque vous utilisez l'**Assistant Proxy de transfert SSL** dans l'interface graphique, vous n'avez pas besoin de spécifier une adresse IP et un port.

> **Remarque**
>
> Pour intercepter des protocoles autres que HTTP et HTTPS en mode proxy transparent, vous devez ajouter une stratégie d'écoute et la lier au serveur proxy.

Configurer le proxy de transfert SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add cs vserver <name> PROXY <ipaddress> <port>
<!--NeedCopy-->
```

Arguments :

Nom :

Nom du serveur proxy. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le serveur virtuel CS créé.

L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comporte un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « mon serveur » ou « mon serveur »).

Cet argument est obligatoire. Longueur maximale : 127

Adresse IP :

Adresse IP du serveur proxy.

Port :

Numéro de port du serveur proxy. Valeur minimale : 1

Exemple de proxy explicite :


```
add cs vserver swgVS PROXY 192.0.2.100 80
<!--NeedCopy-->
```

Exemple pour le proxy transparent :

```
add cs vserver swgVS PROXY * *
<!--NeedCopy-->
```

Ajouter une stratégie d'écoute au serveur proxy transparent à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Proxy transfert SSL** > **Serveurs virtuels proxy**. Sélectionnez le serveur proxy transparent et cliquez sur **Modifier**.
2. Modifiez **les paramètres de base**, puis cliquez sur **Plus**.
3. Dans **Priorité d'écoute**, entrez 1.
4. Dans **Listen Policy Expression**, entrez l'expression suivante :

```
(CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
<!--NeedCopy-->
```

> **Remarque**
>
> Cette expression suppose des ports standard pour le trafic HTTP et HTTPS. Si vous avez configuré différents ports, par exemple 8080 pour HTTP ou 8443 pour HTTPS, modifiez l'expression précédente pour spécifier ces ports.

Interception SSL

August 20, 2021

Une appliance Citrix ADC configurée pour l'interception SSL agit comme un proxy. Il peut intercepter et déchiffrer le trafic SSL/TLS, inspecter la demande non chiffrée et permettre à un administrateur d'appliquer les règles de conformité et les contrôles de sécurité. L'interception SSL utilise une stratégie qui spécifie le trafic à intercepter, bloquer ou autoriser. Par exemple, le trafic à destination et en provenance de sites financiers, tels que les banques, ne doit pas être intercepté, mais d'autres trafic peuvent être interceptés, et les sites sur la liste noire peuvent être identifiés et bloqués. Citrix vous recommande de configurer une stratégie générique pour intercepter le trafic et des stratégies plus spécifiques pour contourner un certain trafic.

Le client et le proxy établissent une poignée de main HTTP/TLS. Le proxy établit une autre poignée de main HTTP/TLS avec le serveur et reçoit le certificat du serveur. Le proxy vérifie le certificat du serveur pour le compte du client et vérifie également la validité du certificat serveur à l'aide du protocole OCSP (Online Certificate Status Protocol). Il régénère le certificat du serveur, le signe à l'aide de la clé du certificat de l'autorité de certification installée sur l'appliance et le présente au client. Par conséquent, un certificat est utilisé entre le client et le dispositif Citrix ADC, et un autre certificat entre l'appliance et le serveur principal.

> **Important**
>
> Le certificat d'autorité de certification utilisé pour signer le certificat de serveur doit être préinstallé sur tous les périphériques clients, de sorte que le certificat de serveur régénéré soit approuvé par le client.

Pour le trafic HTTPS intercepté, le serveur proxy déchiffre le trafic sortant, accède à la requête HTTP en texte clair et peut utiliser n'importe quelle application de couche 7 pour traiter le trafic, par exemple en recherchant l'URL en texte brut et en autorisant ou en bloquant l'accès en fonction de la stratégie d'entreprise et de la réputation d'URL. Si la stratégie décide d'autoriser l'accès au serveur d'origine, le serveur proxy transmet la demande rechiffrée au service de destination (sur le serveur d'origine). Le proxy déchiffre la réponse à partir du serveur d'origine, accède à la réponse HTTP en texte clair et applique éventuellement toutes les stratégies à la réponse. Le proxy recrypte ensuite la réponse et la transmet au client. Si la décision de stratégie consiste à bloquer la demande au serveur d'origine, le proxy peut envoyer une réponse d'erreur, telle que HTTP 403, au client.

Pour effectuer l'interception SSL, en plus du serveur proxy configuré précédemment, vous devez configurer les éléments suivants sur l'appliance ADC :

- Profil SSL
- Stratégie SSL
- Magasin de certificats CA
- Apprentissage automatique des erreurs SSL et mise en cache

> **Remarque :**
>
> Le trafic HTTP/2 n'est pas intercepté par la fonctionnalité d'interception SSL.

Magasin de certificats d'interception SSL

Un certificat SSL, qui fait partie de toute transaction SSL, est un formulaire de données numérique (X509) qui identifie une société (domaine) ou un individu. Un certificat SSL est délivré par une autorité de certification (CA). Une AC peut être privée ou publique. Les certificats émis par des autorités de certification publiques, telles que Verisign, sont approuvés par les applications qui effectuent des transactions SSL. Ces applications tiennent à jour une liste d'autorités de certification qu'elles ont confiance.

En tant que proxy de transfert, l'appliance ADC effectue le chiffrement et le déchiffrement du trafic entre un client et un serveur. Il agit comme un serveur pour le client (utilisateur) et comme un client pour le serveur. Pour qu'une appliance puisse traiter le trafic HTTPS, elle doit valider l'identité d'un serveur afin d'éviter toute transaction frauduleuse. Par conséquent, en tant que client du serveur d'origine, l'appliance doit vérifier le certificat du serveur d'origine avant de l'accepter. Pour vérifier un certificat de serveur, tous les certificats (par exemple, les certificats racine et intermédiaire) utilisés pour signer et émettre le certificat de serveur doivent être présents sur l'appliance. Un ensemble de certificats d'autorité de certification par défaut est préinstallé sur une appliance. L'appliance peut utiliser ces certificats pour vérifier presque tous les certificats de serveur d'origine courants. Ce jeu par défaut ne peut pas être modifié. Toutefois, si votre déploiement nécessite plus de certificats d'autorité de certification, vous pouvez créer un ensemble de ces certificats et importer le bundle dans l'appliance. Un bundle peut également contenir un seul certificat.

Lorsque vous importez un bundle de certificats sur l'appliance, celle-ci télécharge le bundle à partir de l'emplacement distant et, après avoir vérifié que le bundle contient uniquement des certificats, l'installe sur l'appliance. Vous devez appliquer un ensemble de certificats avant de pouvoir l'utiliser pour valider un certificat de serveur. Vous pouvez également exporter un ensemble de certificats pour modification ou le stocker dans un emplacement hors connexion en tant que sauvegarde.

Importer et appliquer un ensemble de certificats d'autorité de certification sur l'appliance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
import ssl certBundle <name> <src>
apply ssl certBundle <name>
<!--NeedCopy-->
```

```
show ssl certBundle
<!--NeedCopy-->
```

ARGUMENTS :

Nom :

Nom à affecter à l'ensemble de certificats importé. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "mon fichier" ou 'mon fichier').

Longueur maximale : 31

src :

URL spécifiant le protocole, l'hôte et le chemin d'accès, y compris le nom du fichier, au bundle de certificats à importer ou à exporter. Par exemple, `http://www.example.com/cert_bundle_file` .

REMARQUE : L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS qui nécessite l'authentification de certificat client pour l'accès.

Longueur maximale : 2047

Exemple :

```
import ssl certbundle swg-certbundle http://www.example.com/cert_bundle
apply ssl certBundle swg-certbundle
<!--NeedCopy-->
```

```
show ssl certbundle

            Name : swg-certbundle(Inuse)

            URL : http://www.example.com/cert_bundle

    Done
<!--NeedCopy-->
```

Importer et appliquer un ensemble de certificats d'autorité de certification sur l'appliance à l'aide de l'interface graphique

1. Accédez à **Sécurité > Proxy transfert SSL > Démarrage > Offres groupées de certificats**.
2. Procédez comme suit :
   - Sélectionnez un ensemble de certificats dans la liste.
   - Pour ajouter un lot de certificats, cliquez sur « + » et spécifiez un nom et une URL source. Cliquez sur **OK**.
3. Cliquez sur **OK**.

Supprimez un ensemble de certificats d'autorité de certification de l'appliance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
remove certBundle <cert bundle name>
<!--NeedCopy-->
```


Exemple :

```
remove certBundle mytest-cacert
<!--NeedCopy-->
```

Exporter un ensemble de certificats d'autorité de certification à partir de l'appliance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
export certBundle <cert bundle name> <Path to export>
<!--NeedCopy-->
```

ARGUMENTS :

Nom :

Nom à affecter à l'ensemble de certificats importé. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "mon fichier" ou 'mon fichier').

Longueur maximale : 31

src :

URL spécifiant le protocole, l'hôte et le chemin d'accès, y compris le nom du fichier, au bundle de certificats à importer ou à exporter. Par exemple, `http://www.example.com/cert_bundle_file` .

REMARQUE : L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS qui nécessite l'authentification de certificat client pour l'accès.

Longueur maximale : 2047

Exemple :

```
export certBundle mytest-cacert http://192.0.2.20/
<!--NeedCopy-->
```

Importer, appliquer et vérifier un ensemble de certificats de l'autorité de certification à partir du magasin de certificats de l'autorité de certification Mozilla CA

À l'invite de commandes, tapez :


```
> import certbundle mozilla_public_ca https://curl.haxx.se/ca/cacert.pem
Done
<!--NeedCopy-->
```

Pour appliquer le bundle, tapez :

```
> apply certbundle mozilla_public_ca
Done
<!--NeedCopy-->
```

Pour vérifier l'ensemble de certificats en cours d'utilisation, tapez :

```
> sh certbundle | grep mozilla
                Name : mozilla_public_ca (Inuse)
<!--NeedCopy-->
```

Limitations

- Les lots de certificats ne sont pas pris en charge dans une configuration de cluster ou sur une appliance partitionnée.
- Le protocole TLSv1.3 n'est pas pris en charge avec SSL Forward Proxy.

Infrastructure de stratégie SSL pour l'interception SSL

Une stratégie agit comme un filtre sur le trafic entrant. Les stratégies de l'appliance ADC permettent de définir comment gérer les connexions et les demandes par proxy. Le traitement est basé sur les actions configurées pour cette stratégie. Autrement dit, les données des demandes de connexion sont comparées à une règle spécifiée dans la stratégie et l'action est appliquée aux connexions qui correspondent à la règle (expression). Après avoir défini une action à affecter à la stratégie et créé la stratégie, vous devez la lier à un serveur proxy, de sorte qu'elle s'applique au trafic passant par ce serveur proxy.

Une stratégie SSL pour l'interception SSL évalue le trafic entrant et applique une action prédéfinie aux requêtes qui correspondent à une règle (expression). La décision d'intercepter, de contourner ou de réinitialiser une connexion est prise en fonction de la stratégie SSL définie. Vous pouvez configurer l'une des trois actions d'une stratégie : Intercept, BYPASS ou RESET. Vous devez spécifier une action lorsque vous créez une stratégie. Pour appliquer une stratégie, vous devez la lier à un serveur proxy de l'appliance. Pour spécifier qu'une stratégie est destinée à l'interception SSL, vous devez spécifier le type (point de liaison) comme INTERCEPT_REQ lorsque vous liez la stratégie à un serveur proxy. Lorsque vous dissociez une stratégie, vous devez spécifier le type INTERCEPT_REQ.

> **Remarque** :
>
> Le serveur proxy ne peut pas prendre la décision d'intercepter sauf si vous spécifiez une stratégie.

L'interception du trafic peut être basée sur n'importe quel attribut de poignée de main SSL. Le plus couramment utilisé est le domaine SSL. Le domaine SSL est généralement indiqué par les attributs de la poignée de main SSL. Il peut s'agir de la valeur de l'indicateur de nom de serveur extraite du message Hello client SSL, le cas échéant, ou de la valeur de nom alternatif de serveur (SAN) extraite du certificat du serveur d'origine. La stratégie d'interception SSL présente un attribut spécial, DETECTED_DOMAIN. Cet attribut permet aux clients de créer plus facilement des stratégies d'interception basées sur le domaine SSL à partir du certificat du serveur d'origine. Le client peut faire correspondre le nom de domaine avec une chaîne, une liste d'URL (jeu d'URL ou`patset`) ou une catégorie d'URL dérivée du domaine.

Créer une stratégie SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add ssl policy <name> -rule <expression> -action <string>
2 <!--NeedCopy-->
```

Exemples :

Les exemples suivants concernent les stratégies avec des expressions qui utilisent l'`detected_domain` attribut pour rechercher un nom de domaine.

Ne pas intercepter le trafic vers une institution financière, telle que XYZBANK

```
1 add ssl policy pol1 -rule client.ssl.detected_domain.contains("XYZBANK"
     ) -action BYPASS
2 <!--NeedCopy-->
```

Ne pas autoriser un utilisateur à se connecter à YouTube à partir du réseau d'entreprise

```
1 add ssl policy pol2 -rule client.ssl.client.ssl.detected_domain.
     url_categorize(0,0).category.eq ("YouTube") -action RESET
2 <!--NeedCopy-->
```

Intercepter tout le trafic utilisateur

```
1 add ssl policy pol3  - rule true  - action INTERCEPT
2 <!--NeedCopy-->
```

Si le client ne souhaite pas utiliser le domaine detected_domain, il peut utiliser l'un des attributs de handshake SSL pour extraire et déduire le domaine.

Par exemple, un nom de domaine est introuvable dans l'extension SNI du message client Hello. Le nom de domaine doit être extrait du certificat du serveur d'origine. Les exemples suivants concernent les stratégies avec des expressions qui vérifient la présence d'un nom de domaine dans le nom de sujet du certificat du serveur d'origine.

Intercepter tout le trafic utilisateur vers n'importe quel domaine Yahoo

```
1 add ssl policy pol4 -rule client.ssl.origin_server_cert.subject.
    contains("yahoo")  - action INTERCEPT
2 <!--NeedCopy-->
```

Interceptez tout le trafic utilisateur pour la catégorie « Shopping/Retail »

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
    subject.URL_CATEGORIZE(0,0).CATEGORY.eq("Shopping/Retail") -action
    INTERCEPT
2 <!--NeedCopy-->
```

Intercepter tout le trafic utilisateur vers une URL non classée

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
    subject.url_categorize(0,0).category.eq("Uncategorized") -action
    INTERCEPT
2 <!--NeedCopy-->
```

Les exemples suivants concernent les stratégies qui correspondent au domaine par rapport à une entrée d'un jeu d'URL.

Interceptez tout le trafic utilisateur si le nom de domaine dans SNI correspond à une entrée de l'ensemble d'URL « top100 »

```
1 add ssl policy pol_url_set  -rule client.ssl.client_hello.SNI.
    URLSET_MATCHES_ANY("top100") -action INTERCEPT
2 <!--NeedCopy-->
```

Interceptez tout le trafic utilisateur du nom de domaine si le certificat du serveur d'origine correspond à une entrée de l'ensemble d'URL « top100 »

```
1 add ssl policy pol_url_set  -rule client.ssl.origin_server_cert.subject
    .URLSET_MATCHES_ANY("top100") -action INTERCEPT
2 <!--NeedCopy-->
```

Créer une stratégie SSL sur un serveur proxy à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Stratégies**.

2. Sous l'onglet **Stratégies SSL**, cliquez sur **Ajouter** et spécifiez les paramètres suivants :
   - Nom de la stratégie
   - Action de stratégie : sélectionnez l'interception, le contournement ou la réinitialisation.
   - Expression.
3. Cliquez sur **Créer**.

Liez une stratégie SSL à un serveur proxy à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type  INTERCEPT_REQ
<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver <name> -policyName pol1 -priority 10 -type
   INTERCEPT_REQ
<!--NeedCopy-->
```

Liez une stratégie SSL à un serveur proxy à l'aide de l'interface graphique

1. Accédez à **Sécurité > Proxy de transfert SSL > Serveurs virtuels proxy**.
2. Sélectionnez un serveur virtuel et cliquez sur **Modifier**.
3. Dans **Paramètres avancés**, cliquez sur **Stratégies SSL**.
4. Cliquez dans la zone **Stratégie SSL** .
5. Dans **Sélectionner une stratégie**, sélectionnez une stratégie à lier.
6. Dans **Type**, sélectionnez **INTERCEPT_REQ**.
7. Cliquez sur **Lier**, puis sur **OK** .

Dissocier une stratégie SSL à un serveur proxy à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind ssl vserver <vServerName> -policyName <string> -type
   INTERCEPT_REQ
<!--NeedCopy-->
```

Expressions SSL utilisées dans les stratégies SSL

Expression.	Description
`CLIENT.SSL.CLIENT_HELLO.SNI.*`	Renvoie l'extension SNI dans un format de chaîne. Évaluez la chaîne pour voir si elle contient le texte spécifié. Exemple : client.ssl.client_hello.sni.contains ("xyz.com")
`CLIENT.SSL.ORIGIN_SERVER_CERT.*`	Renvoie un certificat, reçu d'un serveur principal, au format chaîne. Évaluez la chaîne pour voir si elle contient le texte spécifié. Exemple : client.ssl.origin_server_cert.subject.contains ("xyz.com")
`CLIENT.SSL.DETECTED_DOMAIN.*`	Renvoie un domaine, à partir de l'extension SNI ou du certificat du serveur d'origine, au format chaîne. Évaluez la chaîne pour voir si elle contient le texte spécifié. Exemple : client.ssl.detected_domaine.contains ("xyz.com")

Apprentissage automatique des erreurs SSL

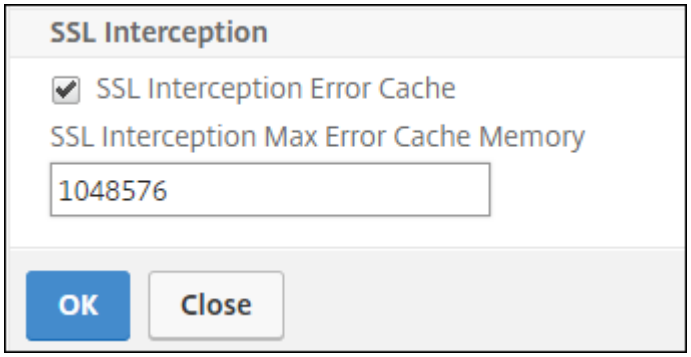
L'appliance ajoute un domaine à la liste de contournement SSL si le mode d'apprentissage est activé. Le mode d'apprentissage est basé sur le message d'alerte SSL reçu d'un client ou d'un serveur d'origine. Autrement dit, l'apprentissage dépend du client ou du serveur qui envoie un message d'alerte. Il n'y a pas d'apprentissage si un message d'alerte n'est pas envoyé. L'appliance apprend si l'une des conditions suivantes est remplie :

1. Une demande de certificat client est reçue du serveur.
2. L'une des alertes suivantes est reçue dans le cadre de la poignée de main :
   - BAD_CERTIFICATE
   - UNSUPPORTED_CERTIFICATE
   - CERTIFICATE_REVOKED
   - CERTIFICATE_EXPIRED
   - CERTIFICATE_UNKNOWN
   - UNKNOWN_CA (Si un client utilise l'épinglage, il envoie ce message d'alerte s'il reçoit un certificat de serveur.)
   - HANDSHAKE_FAILURE

Pour activer l'apprentissage, vous devez activer le cache d'erreurs et spécifier la mémoire réservée à l'apprentissage.

Activer l'apprentissage à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL**.
2. Dans **Paramètres**, cliquez sur **Modifier les paramètres SSL avancés**.
3. Dans **Interception SSL**, sélectionnez **SSL Interception Error Cache**.
4. Dans **SSL Interception Max Error Cache Memory**, spécifiez la mémoire (en octets) à réserver.



5. Cliquez sur **OK**.

Activer l'apprentissage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl parameter -ssliErrorCache ( ENABLED | DISABLED ) -
    ssliMaxErrorCacheMem <positive_integer>
<!--NeedCopy-->
```

Arguments :

SSLierrorCache :

Activez ou désactivez l'apprentissage dynamique et mettez en cache les informations apprises pour prendre les décisions suivantes d'intercepter ou de contourner les demandes. Lorsqu'elle est activée, l'appliance effectue une recherche de cache pour décider s'il faut contourner la demande.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

SSLIMaxErrorCacheMem :

Spécifiez la mémoire maximale, en octets, qui peut être utilisée pour mettre en cache les données apprises. Cette mémoire est utilisée comme cache LRU afin que les anciennes entrées soient remplacées

par de nouvelles entrées après épuisement de la limite de mémoire définie. La valeur 0 détermine automatiquement la limite.

Valeur par défaut : 0

Valeur minimale : 0

Valeur maximale : 4294967294

Profil SSL

Un profil SSL est un ensemble de paramètres SSL, tels que les chiffrements et les protocoles. Un profil est utile si vous avez des paramètres communs pour différents serveurs. Au lieu de spécifier les mêmes paramètres pour chaque serveur, vous pouvez créer un profil, spécifier les paramètres dans le profil, puis lier le profil à différents serveurs. Si aucun profil SSL frontal personnalisé n'est créé, le profil frontal par défaut est lié aux entités côté client. Ce profil vous permet de configurer les paramètres de gestion des connexions côté client.

Pour l'interception SSL, vous devez créer un profil SSL et activer l'interception SSL dans le profil. Un groupe de chiffrement par défaut est lié à ce profil, mais vous pouvez configurer d'autres chiffrements en fonction de votre déploiement. Liez un certificat d'autorité de certification d'interception SSL à ce profil, puis liez le profil à un serveur proxy. Pour l'interception SSL, les paramètres essentiels d'un profil sont ceux utilisés pour les actions suivantes :

- Vérifiez l'état OCSP du certificat du serveur d'origine.
- Déclenchez la renégociation du client si le serveur d'origine demande une renégociation.
- Vérifiez le certificat du serveur d'origine avant de réutiliser la session SSL frontale.

Utilisez le profil back-end par défaut lors de la communication avec les serveurs d'origine. Définissez tous les paramètres côté serveur, tels que les suites de chiffrement, dans le profil principal par défaut. Un profil principal personnalisé n'est pas pris en charge.

Pour obtenir des exemples des paramètres SSL les plus couramment utilisés, consultez « Exemple de profil » à la fin de cette section.

La prise en charge du chiffre/protocole diffère sur le réseau interne et externe. Dans les tableaux suivants, la connexion entre les utilisateurs et une appliance ADC est le réseau interne. Le réseau externe se trouve entre l'appliance et Internet.

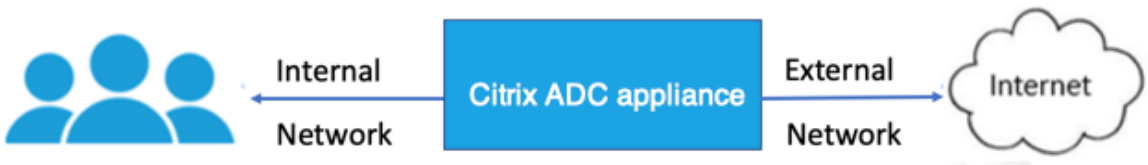


Tableau 1 : Matrice de prise en charge du chiffre/protocole pour le réseau interne

Voir Tableau 1-Support sur le serveur virtuel/le service frontal et le service interne dans les chiffrements disponibles sur les appliances Citrix ADC.

Tableau 2 : Matrice de prise en charge du chiffre/protocole pour le réseau externe

Voir Tableau 2-Support sur les services principaux dans les chiffrements disponibles sur les appliances Citrix ADC.

Ajouter un profil SSL et activer l'interception SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ssl profile <name> -sslinterception ENABLED -ssliReneg ( ENABLED |
 DISABLED )-ssliOCSPCheck ( ENABLED | DISABLED )-ssliMaxSessPerServer <
positive_integer>
```

Arguments :

sslInterception:

Activer ou désactiver l'interception des sessions SSL.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

ssliReneg:

Activez ou désactivez le déclenchement de la renégociation client lorsqu'une demande de renégociation est reçue du serveur d'origine.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

ssliOCSPCheck:

Activez ou désactivez la vérification OCSP pour un certificat de serveur d'origine.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

ssliMaxSessPerServer:

Nombre maximal de sessions SSL à mettre en cache par serveur d'origine dynamique. Une session SSL unique est créée pour chaque extension SNI reçue du client dans un message de bonjour client. La session correspondante est utilisée pour la réutilisation de session serveur.

Valeur par défaut : 10

Valeur minimale : 1

Valeur maximale : 1000

Exemple :

```
add ssl profile swg_ssl_profile  -sslinterception ENABLED

Done

sh ssl profile swg_ssl_profile

1)    Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                    .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                NO

                Session Reuse: ENABLED
                    Timeout: 120 seconds

                DH: DISABLED

                DH Private-Key Exponent Size Limit: DISABLED
                    Ephemeral RSA: ENABLED
                    Refresh Count: 0

                Deny SSL Renegotiation
                    ALL

                Non FIPS Ciphers: DISABLED

                Cipher Redirect: DISABLED

                SSL Redirect: DISABLED

                Send Close-Notify: YES

                Strict Sig-Digest Check: DISABLED

                Push Encryption Trigger: Always

```



```
37                  PUSH encryption trigger timeout:              1 ms
38
39                  SNI: DISABLED
40
41                  OCSP Stapling: DISABLED
42
43                  Strict Host Header check for SNI enabled SSL sessions:
                                        NO
44
45                  Push flag:             0x0 (Auto)
46
47                  SSL quantum size:                              8 kB
48
49                  Encryption trigger timeout           100 mS
50
51                  Encryption trigger packet count:                45
52
53                  Subject/Issuer Name Insertion Format: Unicode
54
55                  SSL Interception: ENABLED
56
57                  SSL Interception OCSP Check: ENABLED
58
59                  SSL Interception End to End Renegotiation: ENABLED
60
61                  SSL Interception Server Cert Verification for Client
                       Reuse: ENABLED
62
63                  SSL Interception Maximum Reuse Sessions per Server:  10
64
65                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
66
67                  HSTS: DISABLED
68
69                  HSTS IncludeSubDomains: NO
70
71                  HSTS Max-Age: 0
72
73                  ECC Curve: P_256, P_384, P_224, P_521
74
75  1)            Cipher Name: DEFAULT Priority :1
76
77                    Description: Predefined Cipher Alias
78
```



```
Done
<!--NeedCopy-->
```

Liez un certificat d'autorité de certification d'interception SSL à un profil SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind ssl profile <name> -ssliCACertkey <ssli-ca-cert>
```

Exemple :

```
bind ssl profile swg_ssl_profile -ssliCACertkey swg_ca_cert

Done

sh ssl profile swg_ssl_profile

1)            Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                    .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                NO

                Session Reuse: ENABLED
                    Timeout: 120 seconds

                DH: DISABLED

                DH Private-Key Exponent Size Limit: DISABLED
                    Ephemeral RSA: ENABLED
                    Refresh Count: 0

                Deny SSL Renegotiation
                    ALL

                Non FIPS Ciphers: DISABLED

                Cipher Redirect: DISABLED

```



```
29                  SSL Redirect: DISABLED
30
31                  Send Close-Notify: YES
32
33                  Strict Sig-Digest Check: DISABLED
34
35                  Push Encryption Trigger: Always
36
37                  PUSH encryption trigger timeout:             1 ms
38
39                  SNI: DISABLED
40
41                  OCSP Stapling: DISABLED
42
43                  Strict Host Header check for SNI enabled SSL sessions:
                                NO
44
45                  Push flag:            0x0 (Auto)
46
47                  SSL quantum size:                            8 kB
48
49                  Encryption trigger timeout           100 mS
50
51                  Encryption trigger packet count:               45
52
53                  Subject/Issuer Name Insertion Format: Unicode
54
55                  SSL Interception: ENABLED
56
57                  SSL Interception OCSP Check: ENABLED
58
59                  SSL Interception End to End Renegotiation: ENABLED
60
61                  SSL Interception Server Cert Verification for Client
                       Reuse: ENABLED
62
63                  SSL Interception Maximum Reuse Sessions per Server:  10
64
65                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
66
67                  HSTS: DISABLED
68
69                  HSTS IncludeSubDomains: NO
70
```



```
71                  HSTS Max-Age: 0
72
73                  ECC Curve: P_256, P_384, P_224, P_521
74
75 1)            Cipher Name: DEFAULT Priority :1
76
77                  Description: Predefined Cipher Alias
78
79 1)            SSL Interception CA CertKey Name: swg_ca_cert
80
81 Done
82 <!--NeedCopy-->
```

Liez un certificat d'autorité de certification d'interception SSL à un profil SSL à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils** > **Profil SSL**.
2. Cliquez sur **Ajouter**.
3. Spécifiez un nom pour le profil.
4. Activer l'**interception des sessions SSL**.
5. Cliquez sur **OK**.
6. Dans **Paramètres avancés**, cliquez sur **Clé de certificat**.
7. Spécifiez une clé de certificat d'autorité de certification d'interception SSL à lier au profil.
8. Cliquez sur **Sélectionner**, puis sur **Lier**.
9. Vous pouvez également configurer les chiffrements en fonction de votre déploiement.
   - Cliquez sur l'icône Modifier, puis cliquez sur **Ajouter**.
   - Sélectionnez un ou plusieurs groupes de chiffrement, puis cliquez sur la flèche droite.
   - Cliquez sur **OK**.
10. Cliquez sur **Terminé**.

Liez un profil SSL à un serveur proxy à l'aide de l'interface graphique

1. Accédez à **Sécurité** >**Proxy de transfert SSL** > **Serveurs virtuels proxy**, puis ajoutez un serveur ou sélectionnez un serveur à modifier.
2. Dans **Profile SSL**, cliquez sur l'icône Modifier.
3. Dans la liste **Profil SSL**, sélectionnez le profil SSL que vous avez créé précédemment.
4. Cliquez sur **OK**.

5. Cliquez sur **Terminé**.

Exemple de profil :

```
Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                    .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                NO

                Session Reuse: ENABLED
                    Timeout: 120 seconds

                DH: DISABLED

                DH Private-Key Exponent Size Limit: DISABLED
                    Ephemeral RSA: ENABLED
                    Refresh Count: 0

                Deny SSL Renegotiation
                    ALL

                Non FIPS Ciphers: DISABLED

                Cipher Redirect: DISABLED

                SSL Redirect: DISABLED

                Send Close-Notify: YES

                Strict Sig-Digest Check: DISABLED

                Push Encryption Trigger: Always

                PUSH encryption trigger timeout:             1 ms

                SNI: DISABLED

                OCSP Stapling: DISABLED

```



```
37                  Strict Host Header check for SNI enabled SSL sessions:
                                 NO
38
39                  Push flag:            0x0 (Auto)
40
41                  SSL quantum size:                              8 kB
42
43                  Encryption trigger timeout           100 mS
44
45                  Encryption trigger packet count:                45
46
47                  Subject/Issuer Name Insertion Format: Unicode
48
49                  SSL Interception: ENABLED
50
51                  SSL Interception OCSP Check: ENABLED
52
53                  SSL Interception End to End Renegotiation: ENABLED
54
55                  SSL Interception Maximum Reuse Sessions per Server:  10
56
57                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
58
59                  HSTS: DISABLED
60
61                  HSTS IncludeSubDomains: NO
62
63                  HSTS Max-Age: 0
64
65                  ECC Curve: P_256, P_384, P_224, P_521
66
67  1)            Cipher Name: DEFAULT Priority :1
68
69                  Description: Predefined Cipher Alias
70
71  1)            SSL Interception CA CertKey Name: swg_ca_cert
72  <!--NeedCopy-->
```

Gestion des identités utilisateur

October 5, 2021

Le nombre croissant de failles de sécurité et la popularité croissante des appareils mobiles ont mis en évidence la nécessité de s'assurer que l'utilisation de l'Internet externe est conforme aux politiques de l'entreprise. Seuls les utilisateurs autorisés doivent être autorisés à accéder aux ressources externes mises en service par le personnel de l'entreprise. La gestion des identités permet de vérifier l'identité d'une personne ou d'un appareil. Il ne détermine pas les tâches que l'individu peut effectuer ni les fichiers qu'il peut voir.

Un déploiement de proxy de transfert SSL identifie l'utilisateur avant d'autoriser l'accès à Internet. Toutes les demandes et réponses de l'utilisateur sont examinées. L'activité des utilisateurs est consignée et les enregistrements sont exportés vers Citrix Application Delivery Management (ADM) à des fins de création de rapports. Dans Citrix ADM, vous pouvez afficher les statistiques sur les activités utilisateur, les transactions et la consommation de bande passante.

Par défaut, seule l'adresse IP de l'utilisateur est enregistrée, mais vous pouvez configurer la fonctionnalité pour enregistrer plus de détails sur l'utilisateur. Vous pouvez utiliser ces informations d'identité pour créer des stratégies d'utilisation Internet plus riches pour des utilisateurs spécifiques.

L'appliance Citrix ADC prend en charge les modes d'authentification suivants pour une configuration de proxy explicite.

- **Protocole LDAP (Lightweight Directory Access Protocol)**. Authentifie l'utilisateur via un serveur d'authentification LDAP externe. Pour plus d'informations, voir Stratégies d'authentification LDAP.
- **RADIUS**. Authentifie l'utilisateur via un serveur RADIUS externe. Pour plus d'informations, consultez Stratégies d'authentification RADIUS.
- **TACACS+**. Authentifie l'utilisateur via un serveur d'authentification TACACS (Terminal Access Controller Access-Control System) externe. Pour plus d'informations, voir Stratégies d'authentification.
- **Negotiate**. Authentifie l'utilisateur via un serveur d'authentification Kerberos. S'il y a une erreur dans l'authentification Kerberos, l'appliance utilise l'authentification NTLM. Pour plus d'informations, voir Négocier des stratégies d'authentification.

Pour le proxy transparent, seule l'authentification LDAP basée sur IP est prise en charge. Lorsqu'une demande client est reçue, le proxy authentifie l'utilisateur en vérifiant une entrée pour l'adresse IP du client dans Active Directory. Il crée ensuite une session en fonction de l'adresse IP de l'utilisateur. Toutefois, si vous configurez le SSonameAttribute dans une action LDAP, une session est créée en utilisant le nom d'utilisateur au lieu de l'adresse IP. Les stratégies classiques ne sont pas prises en charge pour l'authentification dans une configuration de proxy transparente.

> **Remarque**
>
> Pour un proxy explicite, vous devez définir le nom de connexion LDAP sur **SAMAccountName**.

> Pour un proxy transparent, vous devez définir le nom de connexion LDAP sur **NetworkAddress** et attribute1 sur **SAMAccountName**.

Exemple de proxy explicite :

```
add authentication ldapAction swg-auth-action-explicit -serverIP
    10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
    CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
    freebsd123$ -ldapLoginName sAMAccountName
<!--NeedCopy-->
```

Exemple de proxy transparent :

```
add authentication ldapAction swg-auth-action-explicit -serverIP
    10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
    CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
    freebsd123$ -ldapLoginName networkAddress -authentication disable -
    Attribute1 sAMAccountName
<!--NeedCopy-->
```

Configuration de l'authentification des utilisateurs à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add authentication vserver <vserver name> SSL

bind ssl vserver <vserver name> -certkeyName <certkey name>

add authentication ldapAction <action name> -serverIP <ip_addr> -
    ldapBase <string> -ldapBindDn <string> -ldapBindDnPassword -
    ldapLoginName <string>

add authentication Policy <policy name> -rule <expression> -action <
    string>

bind authentication vserver <vserver name> -policy <string> -priority <
    positive_integer>

set cs vserver <name> -authn401 ON -authnVsName <string>
<!--NeedCopy-->
```

Arguments :

Nom du serveur virtuel :

Nom du serveur virtuel d'authentification auquel lier la stratégie.

Longueur maximale : 127

Type de service :

Type de protocole du serveur virtuel d'authentification. Toujours SSL.

Valeurs possibles : SSL

Valeur par défaut : SSL

Nom de l'action :

Nom de la nouvelle action LDAP. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), la livre (#), l'espace (), à (@), égal à (=), deux-points (:) et les caractères de soulignement. Impossible de modifier une fois l'action LDAP ajoutée. L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comprend un ou plusieurs espaces, inscrivez-le entre guillemets doubles ou simples (par exemple, « mon action d'authentification » ou « mon action d'authentification »).

Longueur maximale : 127

IP du serveur :

Adresse IP attribuée au serveur LDAP.

Base LDAP :

Base (nœud) à partir de laquelle lancer les recherches LDAP. Si le serveur LDAP s'exécute localement, la valeur par défaut de base est dc=`netscaler`, dc=com. Longueur maximale : 127

LDAPBindDN :

Nom unique complet (DN) utilisé pour la liaison au serveur LDAP.

Par défaut : CN=Manager, dc=`netscaler`, dc=com

Longueur maximale : 127

Mot de**passe LDAPBindDN** :

Mot de passe utilisé pour la liaison au serveur LDAP.

Longueur maximale : 127

Nom du plugin LDA :

Attribut de nom de connexion LDAP. L'appliance Citrix ADC utilise le nom de connexion LDAP pour interroger les serveurs LDAP externes ou Active Directories. Longueur maximale : 127

Nom de la stratégie :

Nom de la stratégie d'AUTHENTIFICATION avancée. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), la livre (#), l'espace (), à (@), égal à (=), deux-points (:) et les caractères de soulignement. Impossible de modifier une fois qu'une stratégie d'AUTHENTIFICATION a été créée. L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comprend un ou plusieurs espaces, inscrivez le nom entre guillemets doubles ou simples (par exemple, « ma stratégie d'authentification » ou « ma stratégie d'authentification »).

Longueur maximale : 127

règle :

Nom de la règle, ou expression de stratégie avancée, utilisée par la stratégie pour déterminer s'il faut tenter d'authentifier l'utilisateur auprès du serveur d'AUTHENTIFICATION.

Longueur maximale : 1499

action :

Nom de l'action d'authentification à effectuer si la stratégie correspond.

Longueur maximale : 127

Priorité :

Entier positif spécifiant la priorité de la stratégie. Un nombre inférieur indique une priorité plus élevée. Les stratégies sont évaluées dans l'ordre de leurs priorités, et la première stratégie correspondant à la demande est appliquée. Doit être unique dans la liste des stratégies liées au serveur virtuel d'authentification.

Valeur minimale : 0

Valeur maximale : 4294967295

Exemple :

```
1  add authentication vserver swg-auth-vs SSL
2
3  Done
4
5  bind ssl vserver explicit-auth-vs -certkeyName ns-swg-ca-certkey
6
7  Done
8
9  add authentication ldapAction swg-auth-action-explicit -serverIP
       192.0.2.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "CN=
       Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword zzzzz
        -ldapLoginName sAMAccountName
10
```



```
Done

add authenticationpolicy swg-auth-policy -rule true -action swg-auth-
   action-explicit
Done

bind authentication vserver swg-auth-vs -policy swg-auth-policy -
   priority 1

Done

set cs vserver testswg -authn401 ON -authnVsName swg-auth-vs

Done
<!--NeedCopy-->
```

Activer la journalisation des noms d'utilisateur à l'aide de la CLI

À l'invite de commandes, tapez :

```
set appflow param -AAAUserName ENABLED
<!--NeedCopy-->
```

Arguments :

Nom d'utilisateur AAA

Activez l'authentification AppFlow, l'autorisation et l'audit de la journalisation des noms d'utilisateur.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

Exemple :

```
set appflow param -AAAUserName ENABLED
<!--NeedCopy-->
```

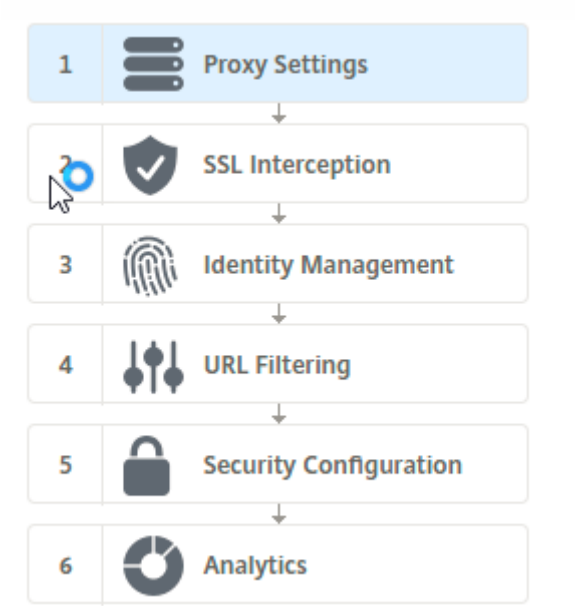
Filtrage d'URL

August 20, 2021

Le filtrage d'URL fournit un contrôle basé sur des stratégies des sites Web à l'aide des informations contenues dans les URL. Cette fonctionnalité permet aux administrateurs réseau de surveiller et de contrôler l'accès des utilisateurs aux sites Web malveillants sur le réseau.

Mise en route

Si vous êtes un nouvel utilisateur et que vous souhaitez configurer le filtrage d'URL, vous devez terminer la configuration initiale du proxy SSL. Pour commencer à utiliser le filtrage d'URL, vous devez d'abord vous connecter à l'assistant de transfert de proxy SSL. L'Assistant vous aide à suivre une série d'étapes de configuration avant d'appliquer les stratégies de filtrage d'URL.



> **Remarque**
>
> Avant de commencer, assurez-vous que vous disposez d'une licence de fonctionnalité URL Threat Intelligence valide installée sur votre appliance. Si vous utilisez une version d'évaluation, assurez-vous d'acheter une licence valide pour continuer à utiliser cette fonctionnalité sur l'appliance ADC.

Connectez-vous à l'assistant de transfert de proxy SSL

L'Assistant Proxy de transfert SSL vous guide à travers une série de tâches de configuration simplifiées et le volet droit affiche la séquence de flux correspondante. Vous pouvez utiliser cet Assistant pour appliquer des stratégies de filtrage d'URL à une liste d'URL ou à une liste prédéfinie de catégories.

Étape 1 : Configurer les paramètres de proxy

Configurez tout d'abord un serveur proxy par lequel le client accède à la passerelle. Ce serveur est de type SSL et fonctionne en mode explicite ou transparent. Pour plus d'informations sur la configuration du serveur proxy, voir Modes proxy.

Étape 2 : Configurer l'interception SSL

Après avoir configuré le serveur proxy, vous devez configurer le proxy d'interception SSL pour intercepter le trafic chiffré au niveau de l'appliance Citrix ADC. Dans le cas du filtrage d'URL, le proxy SSL intercepte le trafic et n'autorise pas les URL bloquées alors que tout autre trafic peut être contourné. Pour plus d'informations sur la configuration de l'interception SSL, consultez Interception SSL.

Étape 3 : Configurer la gestion des identités

Un utilisateur est authentifié avant d'être autorisé à se connecter au réseau d'entreprise. L'authentification offre la flexibilité nécessaire pour définir des stratégies spécifiques pour un utilisateur ou un groupe d'utilisateurs, en fonction de leurs rôles. Pour plus d'informations sur l'authentification des utilisateurs, voir Gestion de l'identité des utilisateurs.

Étape 4 : Configurer le filtrage des URL

L'administrateur peut appliquer une stratégie de filtrage d'URL à l'aide de la fonctionnalité Catégorisation d'URL ou à l'aide de la fonctionnalité Liste d'URL.

Catégorisation des URL. Contrôle l'accès aux sites Web et aux pages Web en filtrant le trafic en fonction d'une liste prédéfinie de catégories.

Liste d'URL. Contrôle l'accès aux sites Web et pages Web mis en liste noire en refusant l'accès aux URL figurant dans un ensemble d'URL importé dans l'appliance.

Étape 5 : Configurer la configuration de la sécurité

Cette étape vous permet de configurer un score de réputation et de permettre aux utilisateurs de contrôler l'accès aux sites Web en refusant l'accès si le score est trop faible. Votre score de réputation peut varier de un à quatre, et vous pouvez configurer le seuil auquel le score devient inacceptable. Pour les scores qui dépassent le seuil, vous pouvez sélectionner une action de stratégie pour autoriser, bloquer ou rediriger le trafic. Pour plus d'informations, voir Score de réputation d'URL.

Étape 6 : Configurer l'analyse de proxy de transfert SSL

Cette étape vous permet d'activer l'analyse de proxy SSL pour catégoriser le trafic Web, la catégorie d'URL de journalisation dans les journaux de transactions utilisateur et l'affichage des analyses de trafic. Pour plus d'informations sur l'analyse de proxy transfert SSL, consultez Analytics.

Étape 7 : Cliquez sur « Terminé » pour terminer la configuration initiale et continuer à gérer la configuration du filtrage d'URL

Liste des URL

August 20, 2021

La fonctionnalité Liste d'URL permet aux clients d'entreprise de contrôler l'accès à des sites Web et à des catégories de sites Web spécifiques. La fonctionnalité filtre les sites Web en appliquant une stratégie de répondeur liée à un algorithme de correspondance d'URL. L'algorithme correspond à l'URL entrante par rapport à un ensemble d'URL comprenant jusqu'à un million (1 000 000) entrées. Si la requête d'URL entrante correspond à une entrée de l'ensemble, l'appliance utilise la stratégie du répondeur pour évaluer la demande (HTTP/HTTPS) et en contrôler l'accès.

Types de jeux d'URL

Chaque entrée d'un jeu d'URL peut inclure une URL et, éventuellement, ses métadonnées (catégorie d'URL, groupes de catégories ou toute autre donnée connexe). Pour les URL avec métadonnées, l'appliance utilise une expression de stratégie qui évalue les métadonnées. Pour plus d'informations, voir Jeu d'URL.

Le proxy de transfert SSL prend en charge les ensembles d'URL personnalisés. Vous pouvez également utiliser des jeux de motifs pour filtrer les URL.

Jeu d'URL personnalisé. Vous pouvez créer un ensemble d'URL personnalisé avec jusqu'à 1 000 000 entrées d'URL et l'importer en tant que fichier texte dans votre appliance.

Jeu de motifs. Une appliance ADC peut utiliser des jeux de motifs pour filtrer les URL avant d'accorder l'accès aux sites Web. Un jeu de motifs est un algorithme de correspondance de chaînes qui recherche une correspondance exacte entre une URL entrante et jusqu'à 5000 entrées. Pour plus d'informations, voir Jeu de motifs.

Chaque URL d'un ensemble d'URL importé peut avoir une catégorie personnalisée sous la forme de métadonnées d'URL. Votre organisation peut héberger le jeu et configurer l'appliance ADC afin de le mettre à jour périodiquement sans intervention manuelle.

Une fois l'ensemble mis à jour, l'appliance Citrix ADC détecte automatiquement les métadonnées. La catégorie est désormais disponible en tant qu'expression de stratégie permettant d'évaluer l'URL et d'appliquer une action telle que permettre, bloquer, rediriger ou notifier l'utilisateur.

Expressions de stratégie avancées utilisées avec les jeux d'URL

Le tableau suivant décrit les expressions de base que vous pouvez utiliser pour évaluer le trafic entrant.

1. .URLSET_MATCHES_ANY - Évalue TRUE si l'URL correspond exactement à n'importe quelle entrée du jeu d'URL.
2. .GET_URLSET_METADATA() - L'expression GET_URLSET_METADATA() renvoie les métadonnées associées si l'URL correspond exactement à n'importe quel motif de l'URL définie. Une chaîne vide est renvoyée s'il n'y a pas de correspondance.
3. `.GET_ URLSET_METADATA().EQ(<METADATA)- .GET_ URLSET_METADATA().EQ(<METADATA)`
4. .GET_URLSET_METADATA ().TYPECAST_LIST_T(',').GET(0).EQ() - Evalue TRUE si les métadonnées correspondantes sont au début de la catégorie. Ce modèle peut être utilisé pour encoder des champs distincts dans les métadonnées, mais correspondre uniquement au premier champ.
5. HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) - Rejoint les paramètres hôte et URL, qui peuvent ensuite être utilisés pour la correspondance.

Types d'action du répondeur

> **Remarque :** Dans le tableau, HTTP.REQ.URL est généralisée comme `<URL expression>`.

Le tableau suivant décrit les actions qui peuvent être appliquées au trafic Internet entrant.

Action du répondeur	Description
Autoriser	Autoriser la demande à accéder à l'URL cible.
Rediriger	Redirigez la demande vers l'URL spécifiée comme cible.
Bloquer	Refuser la demande.

Conditions préalables

Configurez un serveur DNS si vous importez un ensemble d'URL à partir d'une URL de nom d'hôte. Cette configuration n'est pas requise si vous utilisez une adresse IP.

À l'invite de commandes, tapez :

```
add dns nameServer ((<IP> [-local])| <dnsVserverName>)[-state (ENABLED |
DISABLED )] [-type <type>] [-dnsProfileName <string>]
```

Exemple :

```
add dns nameServer 10.140.50.5
```

Configurer une liste d'URL

Pour configurer une liste d'URL, vous pouvez utiliser l'assistant de transfert de proxy Citrix SSL ou l'interface de ligne de commande (CLI) Citrix ADC. Sur l'appliance Citrix ADC, vous devez d'abord configurer la stratégie de répondeur, puis la lier à un jeu d'URL.

Citrix vous recommande d'utiliser l'assistant de transfert de proxy SSL Citrix comme option préférée pour configurer une liste d'URL. Utilisez l'Assistant pour lier une stratégie de répondeur à un jeu d'URL. Vous pouvez également lier la stratégie à un jeu de motifs.

Configurer une liste d'URL à l'aide de l'assistant de transfert de proxy SSL

Pour configurer la liste d'URL pour le trafic HTTPS à l'aide de l'interface graphique :

1. Accédez à **la page Sécurité** > **Proxy de transfert SSL** .
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   a) Cliquez sur **Assistant Proxy Transférer SSL**.
   b) Sélectionnez une configuration existante et cliquez sur **Modifier**.
3. Dans la section **Filtrage d'URL**, cliquez sur **Modifier**.
4. Activez la case à cocher **Liste d'URL** pour activer la fonctionnalité.
5. Sélectionnez une stratégie de **liste d'URL** et cliquez sur **Lier** .
6. Cliquez sur **Continuer**, puis **Terminé**.

Pour plus d'informations, voir Comment créer une stratégie de liste d'URL.

Configurer une liste d'URL à l'aide de l'interface de ligne de commande

Pour configurer une liste d'URL, procédez comme suit.

1. Configurez un serveur virtuel proxy pour le trafic HTTP et HTTPS.
2. Configurer l'interception SSL pour intercepter le trafic HTTPS.
3. Configurez une liste d'URL contenant un jeu d'URL pour le trafic HTTP.
4. Configurer la liste d'URL contenant le jeu d'URL pour le trafic HTTPS.
5. Configurer un jeu d'URL privé.

> **Remarque**
>
> Si vous avez déjà configuré une appliance ADC, vous pouvez ignorer les étapes 1 et 2 et configurer avec l'étape 3.

Configuration d'un serveur virtuel proxy pour le trafic Internet

L'appliance Citrix ADC prend en charge les serveurs virtuels proxy transparents et explicites. Pour configurer un serveur virtuel proxy pour le trafic Internet en mode explicite, procédez comme suit :

1. Ajouter un serveur virtuel SSL proxy.
2. Liez une stratégie de répondeur au serveur virtuel proxy.

Pour ajouter un serveur virtuel proxy à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 add cs vserver <name> <serviceType> <IPAddress> <port>
2 <!--NeedCopy-->
```

Exemple :

```
1 add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
2 <!--NeedCopy-->
```

Pour lier une stratégie de répondeur à un serveur virtuel proxy à l'aide de l'interface de ligne de commande :

```
1 bind ssl vserver <vServerName> -policyName <string> [-priority <
     positive_integer>]
2 <!--NeedCopy-->
```

> **Remarque**
>
> Si vous avez déjà configuré l'intercepteur SSL dans le cadre de la configuration Citrix ADC, vous pouvez ignorer la procédure suivante.

Configurer l'interception SSL pour le trafic HTTPS

Pour configurer l'interception SSL pour le trafic HTTPS, procédez comme suit :

1. Liez une paire de clés de certificat de l'autorité de certification au serveur virtuel proxy.
2. Activez le profil SSL par défaut.
3. Créez un profil SSL frontal et liez-le au serveur virtuel proxy et activez l'interception SSL dans le profil SSL frontal.

Pour lier une paire de clés de certificat d'autorité de certification au serveur virtuel proxy à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
<!--NeedCopy-->
```

Pour configurer un profil SSL frontal à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
set ssl parameter -defaultProfile ENABLED

add ssl profile <name> -sslInterception ENABLED -ssliMaxSessPerServer <
   positive_integer>
<!--NeedCopy-->
```

Pour lier un profil SSL frontal à un serveur virtuel proxy à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl vserver <vServer name>  -sslProfile <name>
<!--NeedCopy-->
```

Configurer une liste d'URL en important un jeu d'URL pour le trafic HTTP

Pour plus d'informations sur la configuration d'un jeu d'URL pour le trafic HTTP, voir Jeu d'URL.

Effectuer une correspondance de sous-domaine explicite

Vous pouvez maintenant effectuer une correspondance de sous-domaine explicite pour un jeu d'URL importé. Un nouveau paramètre, « SubDomainExactMatch » est ajouté à la **`import`** `policy URLset` commande.

Lorsque vous activez le paramètre, l'algorithme de filtrage d'URL effectue une correspondance de sous-domaine explicite. Par exemple, si l'URL entrante est`news.example.com` et si l'entrée de l'ensemble d'URL est`example.com`, l'algorithme ne correspond pas aux URL.

À l'invite de commandes, tapez :

```
import policy urlset <name> [-overwrite] [-delimiter <character>][-rowSeparator
 <character>] -url [-interval <secs>] [-privateSet][-subdomainExactMatch]
[-canaryUrl <URL>]
```


Exemple

```
import policy urlset test -url http://10.78.79.80/top-1k.csv -privateSet -
subdomainExactMatch -interval 900
```

Configurer un jeu d'URL pour le trafic HTTPS

Pour configurer un jeu d'URL pour le trafic HTTPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add ssl policy <name> -rule <expression> -action <string> [-undefAction
      <string>] [-comment <string>]
2 <!--NeedCopy-->
```

Exemple :

```
1 add ssl policy pol1 -rule "client.ssl.client_hello.SNI.
     URLSET_MATCHES_ANY("top1m") -action INTERCEPT
2 <!--NeedCopy-->
```

Pour configurer un jeu d'URL pour le trafic HTTPS à l'aide de l'assistant de transfert de proxy SSL

Citrix vous recommande d'utiliser l'assistant de transfert de proxy SSL comme option préférée pour configurer une liste d'URL. Utilisez l'Assistant pour importer un jeu d'URL personnalisé et lier à une stratégie de répondeur.

1. Accédez à **Sécurité > Proxy de transfert SSL > Filtrage d'URL > Listes d'URL**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Stratégie de liste d'URL**, spécifiez le nom de la stratégie.
4. Sélectionnez une option pour importer un jeu d'URL.
5. Dans la page de l'onglet **Stratégie de liste d'URL**, activez la case à cocher **Importer le jeu d'URL** et spécifiez les paramètres de jeu d'URL suivants.
   a) Nom du jeu d'URL : nom du jeu d'URL personnalisé.
   b) URL—Adresse Web de l'emplacement où accéder à l'ensemble d'URL.
   c) Remplacer : écrase un jeu d'URL précédemment importé.
   d) Delimiter—Séquence de caractères qui délimite un enregistrement de fichier CSV.
   e) Séparateur de lignes —Séparateur de lignes utilisé dans le fichier CSV.
   f) Intervalle (Intervalle) : intervalle en secondes arrondi au nombre de secondes le plus proche égal à 15 minutes au cours duquel le jeu d'URL est mis à jour.
   g) Private Set—Option pour empêcher l'exportation du jeu d'URL.
   h) URL Canary : URL interne permettant de vérifier si le contenu de l'ensemble d'URL doit rester confidentiel. La longueur maximale de l'URL est de 2047 caractères.

6. Sélectionnez une action du répondeur dans la liste déroulante.
7. Cliquez sur **Créer** et **Fermer**.

Configurer un jeu d'URL privé

Si vous configurez un jeu d'URL privé et que son contenu reste confidentiel, l'administrateur réseau peut ne pas connaître les URL répertoriées sur la liste rouge de l'ensemble. Dans de tels cas, vous pouvez configurer une URL Canary et l'ajouter à l'ensemble d'URL. À l'aide de l'URL Canary, l'administrateur peut demander que le jeu d'URL privé soit utilisé pour chaque requête de recherche. Vous pouvez vous référer à la section Assistant pour obtenir la description de chaque paramètre.

Pour importer un ensemble d'URL à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-
    rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
    ] [-canaryUrl <URL>]
<!--NeedCopy-->
```

Exemple :

```
import policy urlset test1 -url http://10.78.79.80/alytra/top-1k.csv -
    private -canaryUrl http://www.in.gr
<!--NeedCopy-->
```

Afficher le jeu d'URL importé

Vous pouvez désormais afficher des jeux d'URL importés en plus des jeux d'URL ajoutés. Un nouveau paramètre « importé » est ajouté à la `show urlset` commande. Si vous activez cette option, l'appliance affiche tous les jeux d'URL importés et les distingue des jeux d'URL ajoutés.

À l'invite de commandes, tapez :

```
show policy urlset [<name>] [-imported]
```

Exemple

```
show policy urlset -imported
```

Configurer la messagerie du journal d'audit

La journalisation d'audit vous permet de vérifier une condition ou une situation dans n'importe quelle phase d'un processus de liste d'URL. Lorsqu'une appliance Citrix ADC reçoit une URL entrante, si la

stratégie de répondeur possède une expression de stratégie avancée Set d'URL, la fonctionnalité journal d'audit collecte les informations relatives au jeu d'URL dans l'URL. Il stocke les détails sous forme de message de journal pour toute cible autorisée par la journalisation d'audit.

Le message de journal contient les informations suivantes :

1. Horodatage.
2. Type de message de journal.
3. Les niveaux de journalisation prédéfinis (Critique, Erreur, Avis, Avertissement, Informations, Débogage, Alerte et Urgence).
4. Consigner les informations de message, telles que le nom du jeu d'URL, l'action de stratégie, l'URL.

Pour configurer la journalisation d'audit pour la fonctionnalité Liste d'URL, vous devez effectuer les tâches suivantes :

1. Activer le journal d'audit :
2. Action Créer un message journal d'audit.
3. Définissez la stratégie de répondeur de liste d'URL avec l'action de message Journal d'audit.

Pour plus d'informations, consultez la rubrique Audit Logging .

Sémantique des modèles d'URL

August 20, 2021

Le tableau suivant présente les modèles d'URL utilisés pour spécifier la liste des pages que vous souhaitez filtrer. Par exemple, le modèle, www.example.com/bar, ne correspond qu'à une page sur www.example.com/bar. Pour faire correspondre toutes les pages dont l'URL commence par 'www.example.com/bar', vous ajoutez un astérisque (*) à la fin de l'URL.

Sémantique pour le modèle d'URL pour correspondre au mappage des métadonnées

La sémantique de correspondance des motifs est disponible sous forme de tableau. Pour plus d'informations, consultez la page PDF Pattern Semantics .

Mappage des catégories URL

August 20, 2021

Liste des catégories et groupes de catégories de tiers. Pour plus d'informations, consultez la page Mappage des catégories d'URL .

Cas d'utilisation : filtrage d'URL à l'aide d'un jeu d'URL personnalisé

August 20, 2021

Si vous êtes un client d'entreprise qui souhaite contrôler l'accès à des sites Web et à des catégories de sites Web spécifiques, utilisez un jeu d'URL personnalisé lié à une stratégie de répondeur. L'infrastructure réseau de votre organisation peut utiliser un filtre d'URL pour bloquer l'accès à des sites Web malveillants ou dangereux. Par exemple, des sites Web présentant des portails d'adultes, de violence, de jeu, de drogue, de politique ou de portails d'emploi. Outre le filtrage des URL, vous pouvez créer une liste personnalisée d'URL et l'importer dans l'appliance ADC. Par exemple, les stratégies de votre organisation peuvent exiger le blocage de l'accès à certains sites Web tels que les réseaux sociaux, les portails commerciaux et les portails d'emplois.

Chaque URL de la liste peut avoir une catégorie personnalisée sous forme de métadonnées. L'organisation peut héberger la liste des URL en tant qu'URL définie sur l'appliance Citrix ADC. Configurez l'appliance pour mettre à jour périodiquement l'ensemble sans intervention manuelle.

Une fois l'ensemble mis à jour, l'appliance Citrix ADC détecte automatiquement les métadonnées. La stratégie de répondeur utilise les métadonnées URL (détails de catégorie) pour évaluer l'URL entrante et appliquer une action telle que autoriser, bloquer, rediriger ou notifier l'utilisateur.

Pour ce faire, configurez votre réseau, vous pouvez effectuer les tâches suivantes :

1. Importer un ensemble d'URL personnalisé
2. Ajouter un ensemble d'URL personnalisé
3. Configurez une liste d'URL personnalisée dans l'Assistant Proxy Transférer SSL.

Importer un ensemble d'URL personnalisé à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-
   rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
   ] [-canaryUrl <URL>]

import policy urlset test1  -url http://10.78.79.80/alytra/top-1k.csv
<!--NeedCopy-->
```

Ajouter un ensemble d'URL personnalisé à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add urlset <urlset_name>
```

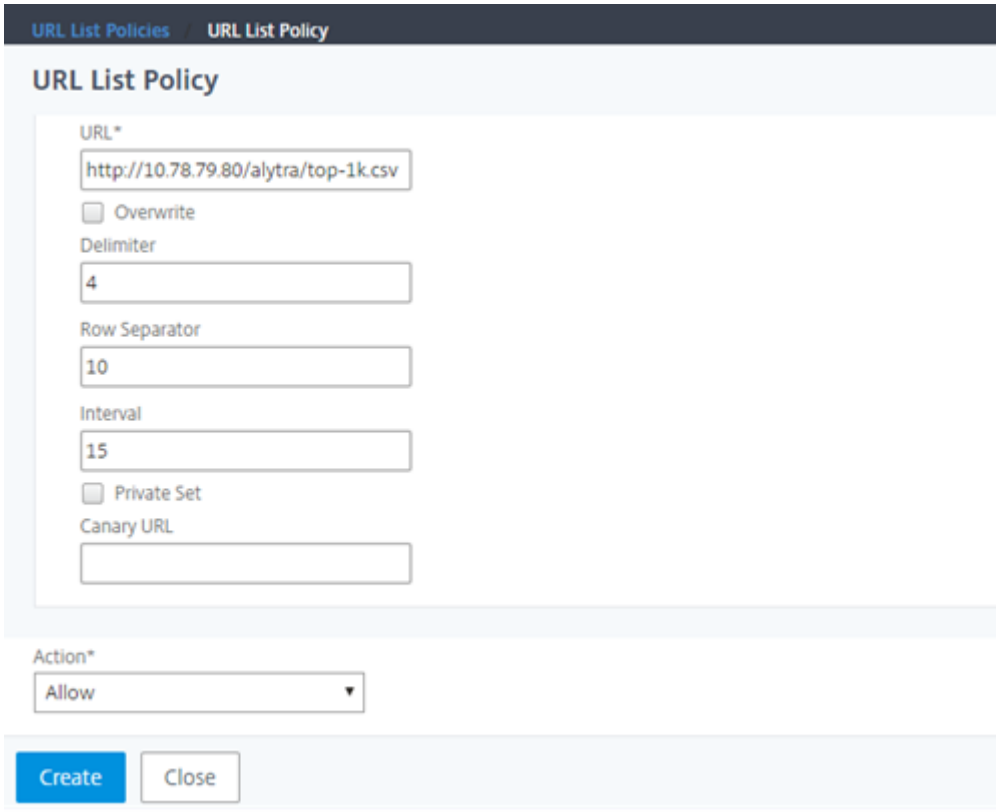

Exemple :

```
add urlset test1
```

Configurer une liste d'URL à l'aide de l'Assistant Proxy Transférer SSL

Citrix vous recommande d'utiliser l'Assistant Proxy de transfert SSL comme option préférée pour configurer une liste d'URL. Utilisez l'Assistant pour importer un ensemble d'URL personnalisé et le lier à une stratégie de répondeur.

1. Accédez à **Sécurité > Proxy de transfert SSL > Filtrage d'URL > Listes d'URL**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Stratégie de liste d'URL**, spécifiez le nom de la stratégie.
4. Sélectionnez une option pour importer un jeu d'URL.
5. Dans la page de l'onglet **Stratégie de liste d'URL**, activez la case à cocher **Importer le jeu d'URL** et spécifiez les paramètres de jeu d'URL suivants.
   a) Nom du jeu d'URL : nom du jeu d'URL personnalisé.
   b) URL—Adresse Web de l'emplacement où accéder à l'ensemble d'URL.
   c) Remplacer : écrase un jeu d'URL précédemment importé.
   d) Delimiter—Séquence de caractères qui délimite un enregistrement de fichier CSV.
   e) Séparateur de lignes —Séparateur de lignes utilisé dans le fichier CSV.
   f) Intervalle—Intervalle en secondes, arrondi à 15 minutes près, au cours duquel le jeu d'URL est mis à jour.
   g) Private Set—Option pour empêcher l'exportation du jeu d'URL.
   h) URL Canary —URL interne permettant de tester si le contenu de l'ensemble d'URL doit rester confidentiel. La longueur maximale de l'URL est de 2047 caractères.
6. Sélectionnez une action du répondeur dans la liste déroulante.
7. Cliquez sur **Créer** et **Fermer**.



Sémantique de métadonnées pour les jeux d'URL personnalisés

Pour importer un ensemble d'URL personnalisé, ajoutez les URL à un fichier texte et liez-le à une stratégie de répondeur pour bloquer les URL de réseaux sociaux.

Voici des exemples d'URL que vous pouvez ajouter au fichier texte :

cnn.com, Actualités

bbc.com, Actualités

google.com, Moteur de recherche

yahoo.com, Moteur de recherche

facebook.com, Réseaux sociaux

twitter.com, Réseaux sociaux

Configurer une stratégie de répondeur pour bloquer les URL des médias sociaux à l'aide de l'interface de ligne de commande

```
1 add responder action act_url_unauthorized respondwith '"HTTP/1.1 451
     Unavailable For Legal Reasons\r\n\r\nURL is NOT authorized\n"
```



```
2
3 add responder policy pol_url_meta_match 'HTTP.REQ.HOSTNAME.APPEND(HTTP.
     REQ.URL).GET_URLSET_METADATA("u1").EQ("Social Media")'
     act_url_meta_match
4 <!--NeedCopy-->
```

Classement des URL en catégories

August 20, 2021

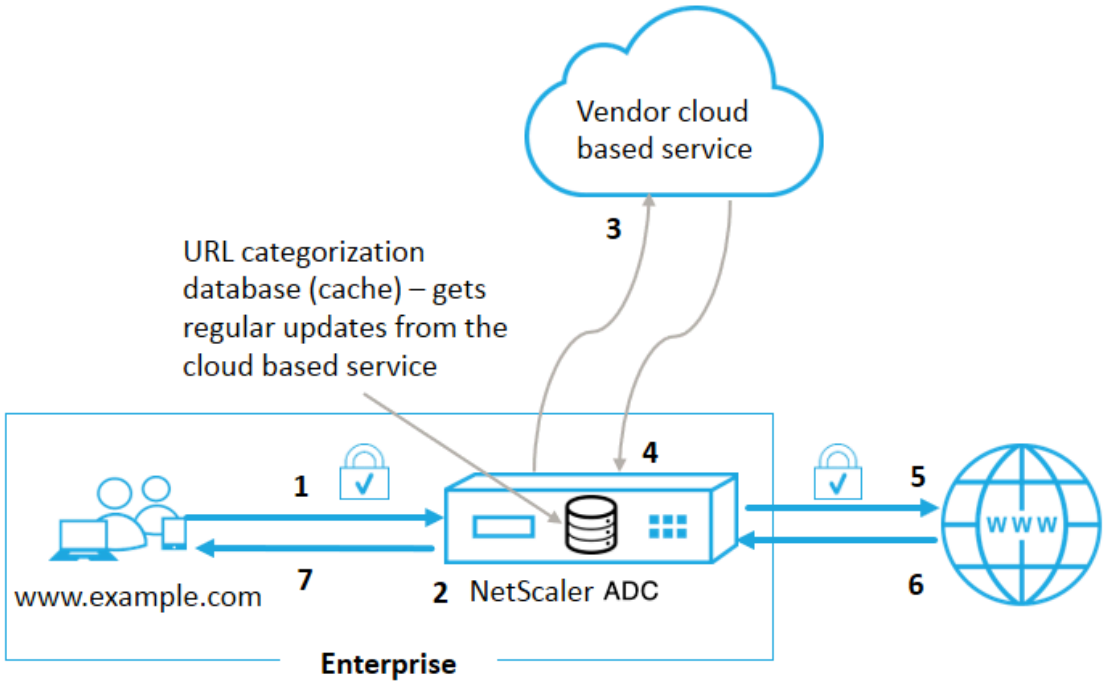
La catégorisation des URL limite l'accès des utilisateurs à des sites Web et à des catégories de sites Web spécifiques. En tant que service abonné en collaboration avec NetSTAR, la fonctionnalité permet aux clients d'entreprise de filtrer le trafic Web à l'aide d'une base de données de catégorisation commerciale. La NetSTAR base de données contient un grand nombre (milliards) d'URL classées en différentes catégories, telles que les réseaux sociaux, les jeux d'argent, le contenu pour adultes, les nouveaux médias et les achats. En plus de la catégorisation, chaque URL a un score de réputation tenu à jour en fonction du profil de risque historique du site. Nous pouvons utiliser NetSTAR les données pour filtrer le trafic en configurant des politiques avancées basées sur des catégories, des groupes de catégories (tels que Terrorisme, Drogues illégales) ou des scores de réputation de site.

Par exemple, vous pouvez bloquer l'accès à des sites dangereux, tels que des sites connus pour être infectés par des logiciels malveillants. Vous pouvez également restreindre de manière sélective l'accès aux contenus tels que le contenu pour adultes ou les médias de divertissement en streaming pour les utilisateurs d'entreprise. Vous pouvez également capturer les détails transactionnels de l'utilisateur et les détails du trafic sortant pour surveiller l'analyse du trafic Web sur le serveur Citrix ADM.

Citrix ADC télécharge ou télécharge des données à partir du NetSTAR périphérique préconfiguré nsv10.netstar-inc.com et incompasshybridpc.netstar-inc.com est utilisé comme hôte de nuage par défaut pour les demandes de catégorisation de nuage. L'appliance utilise son adresse NSIP comme adresse IP source et 443 comme port de destination pour la communication.

Fonctionnement de la catégorisation des URL

La figure suivante montre comment un service de catégorisation d'URL Citrix ADC est intégré à une base de données de catégorisation d'URL commerciale et aux services cloud pour les mises à jour fréquentes.



Les composants interagissent comme suit :

1. Un client envoie une requête d'URL liée à Internet.
2. Le proxy de transfert SSL applique une application de stratégie à la demande en fonction des détails de catégorie, tels que la catégorie, le groupe de catégories et le score de réputation de site. Les détails de catégorie sont récupérés à partir de la base de données de catégorisation des URL. Si la base de données renvoie les détails de la catégorie, le processus passe à l'étape 5.
3. Si la base de données manque les détails de catégorisation, la demande est envoyée à un service de recherche basé sur un cloud géré par un fournisseur de catégorisation d'URL. Toutefois, l'appliance n'attend pas de réponse, mais l'URL est marquée comme non classée et une application de stratégie est exécutée (passez à l'étape 5). L'appliance continue de surveiller les retours de requête dans le cloud et met à jour le cache afin que les demandes futures puissent bénéficier de la recherche dans le cloud.
4. L'appliance ADC reçoit les détails de la catégorie d'URL (catégorie, groupe de catégories et score de réputation) du service basé sur un nuage et les stocke dans la base de données de catégorisation.
5. La stratégie autorise l'URL et la demande est envoyée au serveur d'origine. Sinon, l'appliance supprime, redirige ou répond avec une page HTML personnalisée.
6. Le serveur d'origine répond avec les données demandées à l'appliance ADC.
7. L'appliance envoie la réponse au client.

Cas d'utilisation : utilisation d'Internet dans le cadre de la conformité des entreprises

Vous pouvez utiliser la fonctionnalité de filtrage d'URL pour détecter et mettre en œuvre des stratégies de conformité afin de bloquer les sites qui enfreignent la conformité de l'entreprise. Par exemple, des sites tels que les adultes, les médias en streaming, les réseaux sociaux qui peuvent être considérés comme non productifs ou consomment un excès de bande passante Internet dans un réseau d'entreprise. Le blocage de l'accès à ces sites Web peut améliorer la productivité des employés, réduire les coûts d'exploitation liés à l'utilisation de la bande passante et réduire les frais généraux liés à la consommation réseau.

Conditions préalables

La fonctionnalité de catégorisation d'URL fonctionne sur une plate-forme Citrix ADC uniquement si elle dispose d'un service d'abonnement facultatif avec des fonctions de filtrage d'URL et des informations sur les menaces pour le proxy de transfert SSL. L'abonnement permet aux clients de télécharger les dernières catégories de menaces pour les sites Web, puis d'appliquer ces catégories sur Secure Web Gateway. Avant d'activer et de configurer la fonctionnalité, vous devez installer les licences suivantes :

- CNS_Webf_SServer_Retail.lic
- CNS_xxxx_server_plt_retail.lic

Où, XXXXX est le type de plate-forme, par exemple : V25000

Expressions de stratégie du répondeur

Le tableau suivant répertorie les différentes expressions de stratégie que vous pouvez utiliser pour vérifier si une URL entrante doit être autorisée, redirigée ou bloquée.

1. `<text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>)` - Retourne un objet URL_CATEGORY. Si la valeur `<min_reputation>` est supérieure à 0, l'objet renvoyé ne contient pas de catégorie dont la réputation est inférieure à `<min_reputation>`. Si la valeur `<max_reputation>` est supérieure à 0, l'objet renvoyé ne contient pas de catégorie dont la réputation est supérieure à `<max_reputation>`. Si la catégorie ne parvient pas à résoudre en temps opportun, la valeur undef est renvoyée.
2. `<url_category>. CATEGORY()` - Retourne la chaîne de catégorie de cet objet. Si l'URL n'a pas de catégorie, ou si l'URL est mal formée, la valeur renvoyée est « Inconnu ».
3. `<url_category>. CATEGORY_GROUP()` - Retourne une chaîne identifiant le groupe de catégories de l'objet. Ce regroupement est un regroupement de catégories de niveau supérieur, ce qui est utile dans les opérations nécessitant des informations moins détaillées sur la catégorie d'URL. Si l'URL n'a pas de catégorie, ou si l'URL est mal formée, la valeur renvoyée est « Inconnu ».

4. <url_category>. REPUTATION() - Retourne le score de réputation sous la forme d'un nombre compris entre 0 et 5, où 5 indique la réputation la plus risquée. S'il y a la catégorie « Inconnu », la valeur de réputation est 1.

Types de stratégie :

1. Stratégie pour sélectionner les demandes d'URL qui se trouvent dans la catégorie Moteur de recherche -add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY().EQ("Search Engine")
2. Stratégie pour sélectionner les demandes d'URL qui se trouvent dans le groupe de catégorie Adulte -add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY_GROUP().EQ("Adult")'
3. Stratégie pour sélectionner les demandes d'URL du moteur de recherche dont le score de réputation est inférieur à 4 -add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(4,0).HAS_CATEGORY("Search Engine")
4. Stratégie de sélection des demandes d'URL des moteurs de recherche et de shopping -add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ ("good_categories")
5. Stratégie pour sélectionner les demandes d'URL du moteur de recherche avec un score de réputation égal ou supérieur à 4 -add responder policy p5 'CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(4,0). CATEGORY().EQ("Search Engines")
6. Stratégie pour sélectionner les demandes d'URL qui se trouvent dans la catégorie Moteur de recherche et les comparer avec un jeu d'URL - 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY().EQ("Search Engine")&& HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY("u1")'

Types de stratégie du répondeur

Il existe deux types de stratégies utilisées dans une fonction de catégorisation d'URL et chacun de ces types de stratégie est expliqué dans le tableau suivant :

Type de stratégie	Description
Catégorie d'URL	Catégorisez le trafic Web et, en fonction des résultats de l'évaluation, bloque, autorise ou redirige le trafic.
Score de réputation d'URL	Détermine le score de réputation du site Web et vous permet de contrôler l'accès en fonction du seuil de notation de réputation défini par l'administrateur.

Configurer la catégorisation d'URL

Pour configurer la catégorisation d'URL sur une appliance Citrix ADC, procédez comme suit :

1. Activer le filtrage des URL.
2. Configurez un serveur proxy pour le trafic Web.
3. Configurez l'interception SSL pour le trafic Web en mode explicite.
4. Configurez la mémoire partagée pour limiter la mémoire cache.
5. Configurez les paramètres de catégorisation d'URL.
6. Configurez la catégorisation des URL à l'aide de l'assistant de transfert de proxy Citrix SSL.
7. Configurez les paramètres de catégorisation d'URL à l'aide de l'assistant de transfert de proxy SSL.
8. Configurer le chemin de la base de données initiale et le nom du serveur de nuage

Étape 1 : Activation du filtrage d'URL

Pour activer la catégorisation d'URL, activez la fonction de filtrage d'URL et activez les modes de catégorisation d'URL.

Pour activer la catégorisation d'URL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
enable ns feature URLFiltering
```

```
disable ns feature URLFiltering
```

Étape 2 : Configurer un serveur proxy pour le trafic Web en mode explicite

L'appliance Citrix ADC prend en charge les serveurs virtuels proxy transparents et explicites. Pour configurer un serveur virtuel proxy pour le trafic SSL en mode explicite, procédez comme suit :

1. Ajoutez un serveur proxy.
2. Liez une stratégie SSL au serveur proxy.

Pour ajouter un serveur proxy à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add cs vserver <name> [-td <positive_integer>] <serviceType> [-cltTimeout <
secs>]
```

Exemple :

```
add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
```


Liez une stratégie SSL à un serveur virtuel proxy à l'aide de l'interface de ligne de commande

```
bind ssl vserver <vServerName> -policyName <string> [-priority <positive_integer
>]
```

Étape 3 : Configurer l'interception SSL pour le trafic HTTPS

Pour configurer l'interception SSL pour le trafic HTTPS, procédez comme suit :

1. Liez une paire de clés de certificat de l'autorité de certification au serveur virtuel proxy.
2. Configurez le profil SSL par défaut avec les paramètres SSL.
3. Liez un profil SSL frontal au serveur virtuel proxy et activez l'interception SSL dans le profil SSL frontal.

Pour lier une paire de clés de certificat d'autorité de certification au serveur virtuel proxy à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -CA -
skipCAName
```

Pour configurer le profil SSL par défaut à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl profile <name> -denySSLReneg <denySSLReneg> -sslInterception (
ENABLED | DISABLED)-ssliMaxSessPerServer positive_integer>
```

Liez un profil SSL frontal à un serveur virtuel proxy à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl vserver <vServer name> -sslProfile ssl_profile_interception
```

Étape 4 : Configurer la mémoire partagée pour limiter la mémoire cache

Pour configurer la mémoire partagée afin de limiter la mémoire cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set cache parameter [-memLimit <megaBytes>]
```

Où, la limite de mémoire configurée pour la mise en cache est définie sur 10 Mo.

Étape 5 : Configurer les paramètres de catégorisation d'URL

Pour configurer les paramètres de catégorisation d'URL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>] [-
TimeOfDayToUpdateDB <HH:MM>]
```

Exemple :

```
set urlfiltering parameter -urlfilt_hours_betweenDB_updates 20
```

Étape 6 : Configurer la catégorisation d'URL à l'aide de l'assistant de transfert de proxy Citrix SSL

1. Ouvrez une session sur l'appliance Citrix ADC et accédez à **la page Sécurité** > **SSL Transfer Proxy** .
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   a) Cliquez sur **Assistant Proxy Transférer SSL** pour créer une nouvelle configuration.
   b) Sélectionnez une configuration existante et cliquez sur **Modifier**.
3. Dans la section **Filtrage d'URL**, cliquez sur **Modifier**.
4. Activez la case à cocher **Catégorisation d'URL** pour activer la fonction.
5. Sélectionnez une stratégie de **catégorisation d'URL** et cliquez sur **Lier** .
6. Cliquez sur **Continuer**, puis **Terminé**.

Pour plus d'informations sur la stratégie de catégorisation d'URL, voir Comment créer une stratégie de catégorisation d'URL.

Étape 7 : Configuration des paramètres de catégorisation d'URL à l'aide d'un Assistant Proxy de transfert SSL

1. Ouvrez une session sur l'appliance **Citrix ADC** et accédez à **Sécurité > Filtrage d'URL** .
2. Dans la page **Filtrage d'URL**, cliquez sur **Modifier les paramètres de filtrage d'URL** lien.
3. Dans la page **Configuration des paramètres de filtrage d'URL**, spécifiez les paramètres suivants.
   a) Heures entre les mises à jour de base de données. Heures de filtrage d'URL entre les mises à jour de la base de données. Valeur minimale : 0 et Valeur maximale : 720.
   b) Heure de la journée pour mettre à jour la base de données. URL Filtrage heure de la journée pour mettre à jour la base de données.
   c) Hôte du nuage. Chemin d'accès URL du serveur cloud.
   d) Chemin de base de données de départ. Chemin d'URL du serveur de recherche de base de données d'origine.

4. Cliquez sur **OK** et **Fermer**.

Exemple de configuration :

```
enable ns feature LB CS SSL IC RESPONDER AppFlow URLFiltering

enable ns mode FR L3 Edge USNIP PMTUD

set ssl profile ns_default_ssl_profile_frontend -denySSLReneg NONSECURE
     -sslInterception ENABLED -ssliMaxSessPerServer 100

add ssl certKey swg_ca_cert -cert ns_swg_ca.crt -key ns_swg_ca.key

set cache parameter -memLimit 100

add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180

add responder action act1 respondwith ""HTTP/1.1 200 OK\r\n\r\n" + http
    .req.url.url_categorize(0,0).reputation + "\n""

add responder policy p1 "HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
    Shopping/Retail") || HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
    Search Engines & Portals

")" act1

bind cs vserver starcs_PROXY -policyName p1 -priority 10 -
    gotoPriorityExpression END -type REQUEST

add dns nameServer 10.140.50.5

set ssl parameter -denySSLReneg NONSECURE -defaultProfile ENABLED -
    sigDigestType RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-
    SHA512 -ssliErrorCache ENABLED

-ssliMaxErrorCacheMem 100000000

add ssl policy pol1 -rule "client.ssl.origin_server_cert.subject.
    URL_CATEGORIZE(0,0).CATEGORY.eq("Search Engines & Portals")"" -
    action INTERCEPT

add ssl policy pol3 -rule "client.ssl.origin_server_cert.subject.ne("
    citrix")" -action INTERCEPT

add ssl policy swg_pol -rule "client.ssl.client_hello.SNI.
```



```
      URL_CATEGORIZE(0,0).CATEGORY.ne("Uncategorized")" -action INTERCEPT
32
33 set urlfiltering parameter -HoursBetweenDBUpdates 3 -
      TimeOfDayToUpdateDB 03:00
34 <!--NeedCopy-->
```

Configurer le chemin de la base de données initiale et le nom du serveur de nuage

Vous pouvez maintenant configurer le chemin de la base de données d'origine et le nom du serveur de recherche de cloud pour définir manuellement le nom du serveur de recherche de cloud et le chemin de la base de données d'origine. Pour ce faire, deux nouveaux paramètres, « CloudHost » et « SeedDBPath », sont ajoutés au paramètre de filtrage d'URL.

À l'invite de commandes, tapez :

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>] [-
TimeOfDayToUpdateDB <HH:MM>] [-LocalDatabaseThreads <positive_integer>] [-
CloudHost <string>] [-SeedDBPath <string>]
```

Exemple :

```
set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
03:00 -CloudHost localhost -SeedDBPath /mypath
```

Communication entre une appliance Citrix ADC et `NetSTAR` peut nécessiter un serveur de noms de domaine. Vous pouvez tester à l'aide d'une simple console ou d'une connexion telnet de l'appliance.

Exemple :

```
1  root@ns# telnet nsv10.netstar-inc.com 443
2  Trying 1.1.1.1...
3  Connected to nsv10.netstar-inc.com.
4  Escape character is '^]'.
5
6  root@ns# telnet incompasshybridpc.netstar-inc.com 443
7  Trying 10.10.10.10...
8  Connected to incompasshybridpc.netstar-inc.com.
9  Escape character is '^]'.
10 <!--NeedCopy-->
```

Configurer la messagerie du journal d'audit

La journalisation d'audit vous permet de vérifier une condition ou une situation dans n'importe quelle phase du processus de catégorisation des URL. Lorsqu'une appliance Citrix ADC reçoit une URL en-

trante, si la stratégie de répondeur possède une expression de filtrage d'URL, la fonctionnalité journal d'audit collecte les informations relatives au jeu d'URL dans l'URL. Il stocke les informations sous forme de messages de journal pour toute cible autorisée par la journalisation d'audit.

- Adresse IP source (adresse IP du client qui a fait la demande).
- Adresse IP de destination (adresse IP du serveur demandé).
- URL demandée contenant le schéma, l'hôte et le nom de domaine (http://www.example.com).
- Catégorie d'URL renvoyée par le cadre de filtrage d'URL.
- groupe de catégories d'URL renvoyé par le cadre de filtrage d'URL.
- Numéro de réputation d'URL renvoyé par le cadre de filtrage d'URL.
- Action du journal d'audit effectuée par la stratégie.

Pour configurer la journalisation d'audit pour une fonctionnalité de liste d'URL, vous devez effectuer les tâches suivantes :

1. Activer le journal d'audit :
2. Action Créer un message journal d'audit.
3. Définissez la stratégie de répondeur de liste d'URL avec l'action de message Journal d'audit.

Pour plus d'informations, consultez la rubrique Audit Logging .

Stockage des erreurs d'échec à l'aide de la messagerie SYSLOG

À n'importe quelle étape du processus de filtrage d'URL, en cas de défaillance au niveau du système, l'appliance ADC utilise le mécanisme du journal d'audit pour stocker les journaux dans le fichier ns.log. Les erreurs sont stockées sous forme de messages texte au format SYSLOG de sorte qu'un administrateur puisse les afficher plus tard dans un ordre chronologique d'occurrence d'événement. Ces journaux sont également envoyés à un serveur SYSLOG externe pour archivage. Pour plus d'informations, consultez l'article CTX229399.

Par exemple, si un échec se produit lorsque vous initialisez le SDK de filtrage d'URL, le message d'erreur est stocké dans le format de messagerie suivant.

```
Oct 3 15:43:40 <local0.err> ns URLFiltering[1349]: Error initializing
NetStar SDK (SDK error=-1). (status=1).
```

L'appliance Citrix ADC stocke les messages d'erreur sous quatre catégories de défaillance différentes :

- **Échec du téléchargement**. Si une erreur se produit lorsque vous essayez de télécharger la base de données de catégorisation.
- **Échec de l'intégration**. Si une erreur se produit lorsque vous intégrez une mise à jour dans la base de données de catégorisation existante.

- **Échec de l'initialisation**. Si une erreur se produit lorsque vous initialisez la fonction de catégorisation d'URL, définissez des paramètres de catégorisation ou terminez un service de catégorisation.
- **Échec de la récupération**. Si une erreur se produit lorsque l'appliance récupère les détails de catégorisation de la demande.

Configurer les interruptions SNMP pour les événements NetStar

La fonctionnalité de filtrage d'URL génère des interruptions SNMP, si les conditions suivantes se produisent :

- La mise à jour de la base de données NetStar échoue ou réussit.
- L'initialisation du SDK NetStar échoue ou réussit.

L'appliance dispose d'un ensemble d'entités conditionnelles appelées alarmes SNMP. Lorsqu'une condition de l'alarme SNMP est remplie, l'appliance génère des interruptions et l'envoie à une destination d'interruptions spécifiée. Par exemple, si l'initialisation du kit SDK NetStar échoue, un OID SNMP 1.3.6.1.4.1.5951.1.1.0.183 est généré et envoyé à la destination d'interruptions.

Pour que l'appliance génère des interruptions, vous devez d'abord activer et configurer les alarmes SNMP. Ensuite, spécifiez la destination d'interruptions vers laquelle l'appliance envoie les messages d'interruption générés

Activer une alarme SNMP

L'appliance Citrix ADC génère des interruptions uniquement pour les alarmes SNMP activées. Certaines alarmes sont activées par défaut, mais vous pouvez les désactiver.

Lorsque vous activez une alarme SNMP, la fonction de filtrage d'URL génère des messages d'interruption lorsqu'un événement de réussite ou d'échec se produit. Certaines alarmes sont activées par défaut.

Pour activer une alarme SNMP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
enable snmp alarm <trapName>
show snmp alarm <trapName>
```

Pour activer une alarme SNMP à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Système** > **SNMP** > **Alarmes**, puis sélectionnez l'alarme.
2. Cliquez sur **Actions** et sélectionnez **Activer** .

Configurer l'alarme SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue
 <positive_integer>]] [-time <secs>] [-state ( ENABLED | DISABLED )] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Exemple :

```
set snmp alarm URL-FIL-DB-UPDATE-STATUS -state ENABLED
set snmp alarm URL-FIL-INIT-SDK -state ENABLED
```

Configurer les alarmes SNMP à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Alarmes**, sélectionnez une alarme et configurez les paramètres d'alarme.

Pour plus d'informations sur les interruptions SNMP, consultez la rubrique SNMP

Score de réputation d'URL

October 5, 2021

La fonction de catégorisation d'URL fournit un contrôle basé sur des stratégies pour restreindre les URL sur la liste rouge. Vous pouvez contrôler l'accès aux sites Web en fonction de la catégorie d'URL, du score de réputation ou de la catégorie d'URL et du score de réputation. Si les administrateurs réseau surveillent un utilisateur accédant à des sites Web à haut risque, ils peuvent utiliser une stratégie de répondeur liée au score de réputation d'URL pour bloquer ces sites Web à risque.

À la réception d'une demande d'URL entrante, la solution matérielle-logicielle récupère la catégorie et le score de réputation dans la base de données de catégorisation des URL. En fonction du score de réputation renvoyé par la base de données, la solution matérielle-logicielle attribue une note de réputation aux sites Web. La valeur peut aller de 1 à 4, 4 étant le type de site Web le plus risqué, comme indiqué dans le tableau suivant.

Évaluation de la réputation des URL	Commentaire de réputation
1	Site propre
2	Site inconnu
3	Potentiellement dangereux ou affilié à un site dangereux

Évaluation de la réputation des URL	Commentaire de réputation
4	Site malveillant

Cas d'utilisation : filtrage par score de réputation d'URL

Imaginez une organisation d'entreprise avec un administrateur réseau qui surveille les transactions des utilisateurs et la consommation de bande passante réseau. Si des logiciels malveillants peuvent pénétrer sur le réseau, l'administrateur doit améliorer la sécurité des données et contrôler l'accès aux sites Web malveillants et dangereux accédant au réseau. Pour protéger le réseau contre de telles menaces, l'administrateur peut configurer la fonctionnalité de filtrage d'URL pour autoriser ou refuser l'accès par score de réputation d'URL.

Pour plus d'informations sur la surveillance du trafic sortant et des activités des utilisateurs sur le réseau, consultez Analytics.

Si un employé de l'organisation tente d'accéder à un site Web de réseau social, l'appliance ADC reçoit une demande d'URL. Il interroge la base de données de catégorisation d'URL pour récupérer la catégorie d'URL en tant que réseau social et un score de réputation 3, qui indique un site Web potentiellement dangereux. La solution matérielle-logicielle vérifie ensuite la stratégie de sécurité configurée par l'administrateur, par exemple en bloquant l'accès aux sites ayant une cote de réputation de 3 ou plus. Il applique ensuite l'action de stratégie pour contrôler l'accès au site Web.

Pour implémenter cette fonctionnalité, vous devez configurer le score de réputation d'URL et les niveaux de seuil de sécurité à l'aide de l'assistant Proxy de transfert SSL.

Configurer le score de réputation à l'aide de l'interface graphique

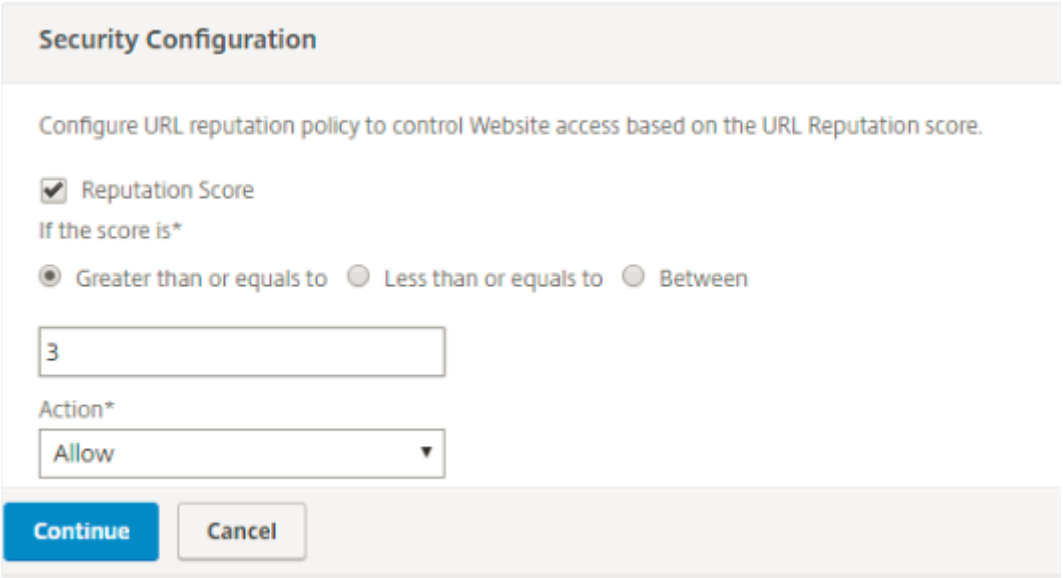
Citrix vous recommande d'utiliser l'assistant de transfert de proxy SSL pour configurer le score de réputation et les niveaux de sécurité. En fonction du seuil configuré, vous pouvez sélectionner une action de stratégie pour autoriser, bloquer ou rediriger le trafic.

1. Accédez à **Sécurité** > **Proxy SSL Forward**.
2. Dans le volet d'informations, cliquez sur **SSL Forward Proxy Wizard**.
3. Dans la page de détails, spécifiez les paramètres du serveur proxy.
4. Cliquez sur **Continuer** pour spécifier d'autres paramètres tels que l'interception SSL et l'identification de la gestion.
5. Cliquez sur **Continuer** pour accéder à la section **Configuration de la sécurité** .
6. Dans la section **Configuration de la sécurité**, cochez la case **Score de réputation** pour contrôler l'accès en fonction du score de réputation d'URL.
7. Sélectionnez le niveau de sécurité et spécifiez la valeur de seuil du score de réputation :

a) Supérieur ou égal à : autorise ou bloque un site Web si la valeur de seuil est supérieure ou égale à N, où N est compris entre un et quatre.
b) Inférieur ou égal à : autorise ou bloque un site Web si la valeur de seuil est inférieure ou égale à N, où N est compris entre un et quatre.
c) Entre : autorise ou bloque un site Web si la valeur de seuil est comprise entre N1 et N2 et que la plage est comprise entre un et quatre.

8. Sélectionnez une action de répondeur dans la liste déroulante.
9. Cliquez sur **Continuer** et **fermer**.

L'image suivante montre la section **Configuration de la sécurité** de l'assistant Proxy de transfert SSL. Activez l'option Score de réputation d'URL pour configurer les paramètres de stratégie.



Analytics

October 5, 2021

Dans l'appliance Citrix ADC, tous les enregistrements utilisateur et les enregistrements suivants sont consignés. Lorsque vous intégrez Citrix Application Delivery Management (ADM) à l'appliance Citrix ADC, l'activité utilisateur consignée et les enregistrements suivants de l'appliance sont exportés vers Citrix ADM à l'aide de la `logstream` fonctionnalité.

Citrix ADM rassemble et présente des informations sur les activités des utilisateurs, telles que les sites Web visités et la bande passante dépensée. Il signale également l'utilisation de la bande passante et les menaces détectées, telles que les logiciels malveillants et les sites de phishing. Vous pouvez utiliser ces mesures clés pour surveiller votre réseau et prendre des mesures correctives avec l'appliance Citrix SWG. Pour plus d'informations, consultez Citrix SSL Forward Proxy Analytics.

Pour intégrer l'appliance Citrix ADC à Citrix ADM :

1. Dans l'appliance Citrix ADC, lors de la configuration de la fonctionnalité de proxy de transfert SSL, activez Analytics et fournissez les détails de l'instance Citrix ADM que vous souhaitez utiliser pour l'analyse.
2. Dans Citrix ADM, ajoutez l'appliance Citrix ADC en tant qu'instance à Citrix ADM. Pour plus d'informations, voir Ajouter des instances à Citrix ADM.

Cas d'utilisation : sécuriser un réseau d'entreprise en utilisant ICAP pour l'inspection à distance des logiciels malveillants

August 20, 2021

L'appliance Citrix ADC agit comme un proxy et intercepte tout le trafic client. L'appliance utilise des stratégies pour évaluer le trafic et transmet les demandes client au serveur d'origine sur lequel réside la ressource. L'appliance décrypte la réponse du serveur d'origine et transmet le contenu en texte brut au serveur ICAP pour une vérification anti-programme malveillant. Le serveur ICAP répond avec un message indiquant « Aucune adaptation requise », ou erreur, ou demande modifiée. En fonction de la réponse du serveur ICAP, le contenu demandé est soit transféré au client, soit un message approprié est envoyé.

Dans ce cas d'utilisation, vous devez effectuer une configuration générale, une configuration liée à l'interception proxy et SSL et une configuration ICAP sur l'appliance Citrix ADC.

Configuration générale

Configurez les entités suivantes :

- Adresse du NSIP
- Adresse IP du sous-réseau (SNIP)
- Serveur de noms DNS
- Paire de clé de certificat CA pour signer le certificat du serveur pour l'interception SSL

Configuration du serveur proxy et de l'interception SSL

Configurez les entités suivantes :

- Serveur proxy en mode explicite pour intercepter tout le trafic HTTP et HTTPS sortant.
- Profil SSL pour définir les paramètres SSL, tels que les chiffrements et les paramètres, pour les connexions.

- Stratégie SSL pour définir des règles d'interception du trafic. Définissez sur true pour intercepter toutes les demandes client.

Pour plus de détails, consultez les rubriques suivantes :

- Modes proxy
- Interception SSL

Dans l'exemple de configuration suivant, le service de détection de logiciels malveillants réside à www.example.com.

Exemple de configuration générale :

```
add dns nameServer 203.0.113.2

add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key ns_swg_ca.key
<!--NeedCopy-->
```

Exemple de configuration de serveur proxy et d'interception SSL :

```
add cs vserver explicitswg PROXY 192.0.2.100 80 -Authn401 ENABLED -authnVsName explicit-auth-vs

set ssl parameter -defaultProfile ENABLED

add ssl profile swg_profile -sslInterception ENABLED

bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey

set ssl vserver explicitswg -sslProfile swg_profile

add ssl policy ssli-pol_ssli -rule true -action INTERCEPT

bind ssl vserver explicitswg -policyName ssli-pol_ssli -priority 100 -type INTERCEPT_REQ
<!--NeedCopy-->
```

Exemple de configuration ICAP :

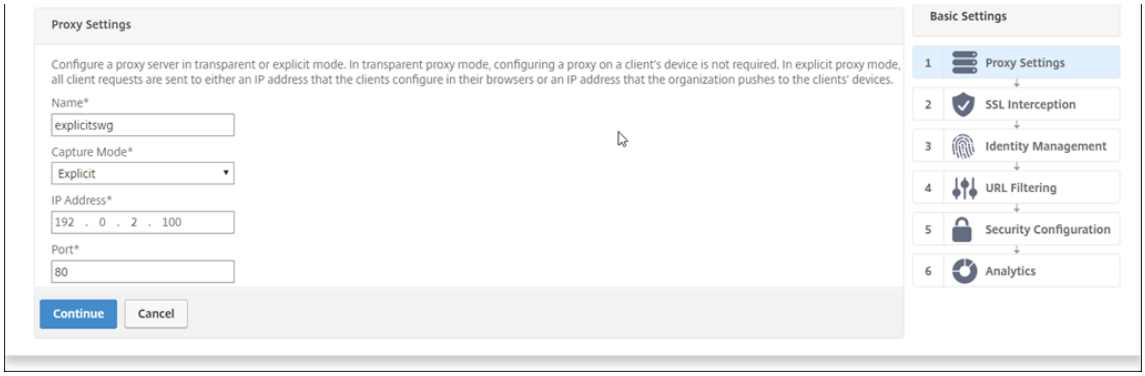
```
add service icap_svc 203.0.113.225 TCP 1344

enable ns feature contentinspection

add icapprofile icapprofile1 -uri /example.com -Mode RESMOD

```



```
7  add contentInspection action CiRemoteAction -type ICAP -serverName
       icap_svc -icapProfileName icapprofile1
8
9  add contentInspection policy CiPolicy -rule "HTTP.REQ.METHOD.NE("
       CONNECT")" -action CiRemoteAction
10
11 bind cs vserver explicitswg -policyName  CiPolicy -priority 200 -type
       response
12 <!--NeedCopy-->
```

Configurer les paramètres du proxy

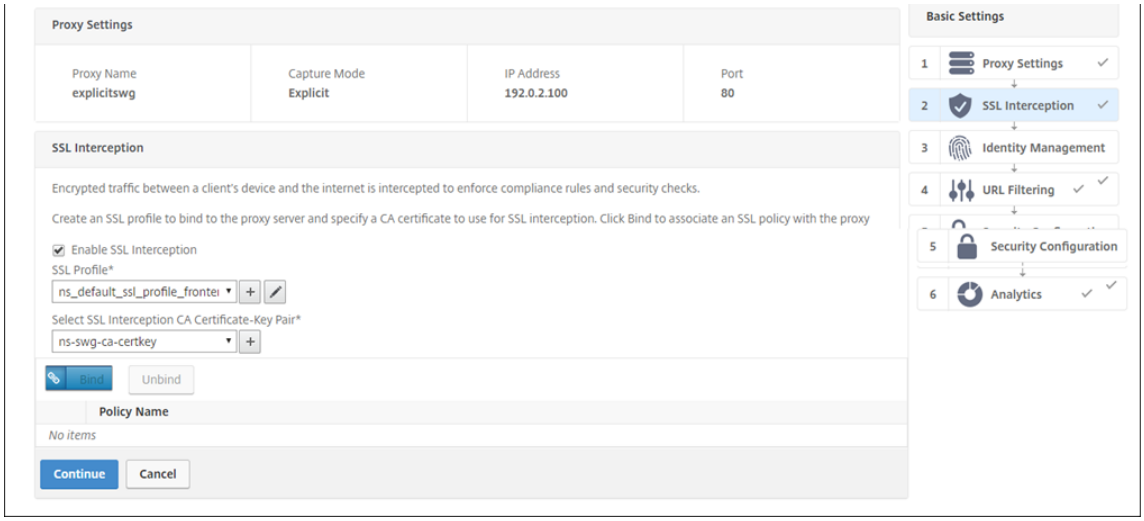
1. Accédez à **Sécurité** > **Proxy de transfert SSL** > **Assistant Proxy de transfert SSL**.
2. Cliquez sur **Démarrer**, puis sur **Continuer**.
3. Dans la boîte de dialogue **Paramètres proxy**, entrez un nom pour le serveur proxy explicite.
4. Pour **Mode Capture,** sélectionnez **Explicite**.
5. Entrez une adresse IP et un numéro de port.



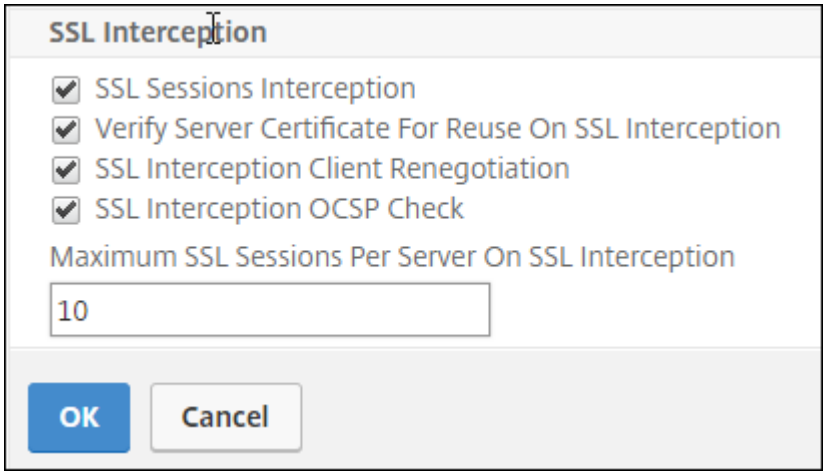
6. Cliquez sur **Continuer**.

Configurer les paramètres d'interception SSL

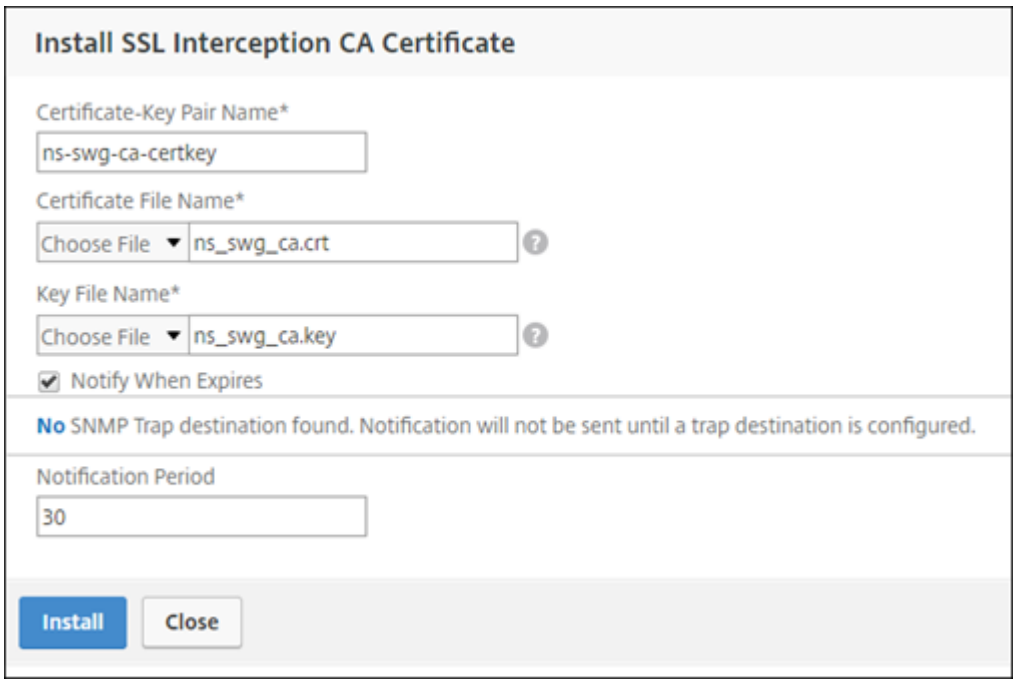
1. Sélectionnez **Activer l'interception SSL**.



2. Dans **Profile SSL**, sélectionnez un profil existant ou cliquez sur « + » pour ajouter un nouveau profil SSL frontal. Activez l' **interception de sessions SSL** dans ce profil. Si vous sélectionnez un profil existant, ignorez l'étape suivante.

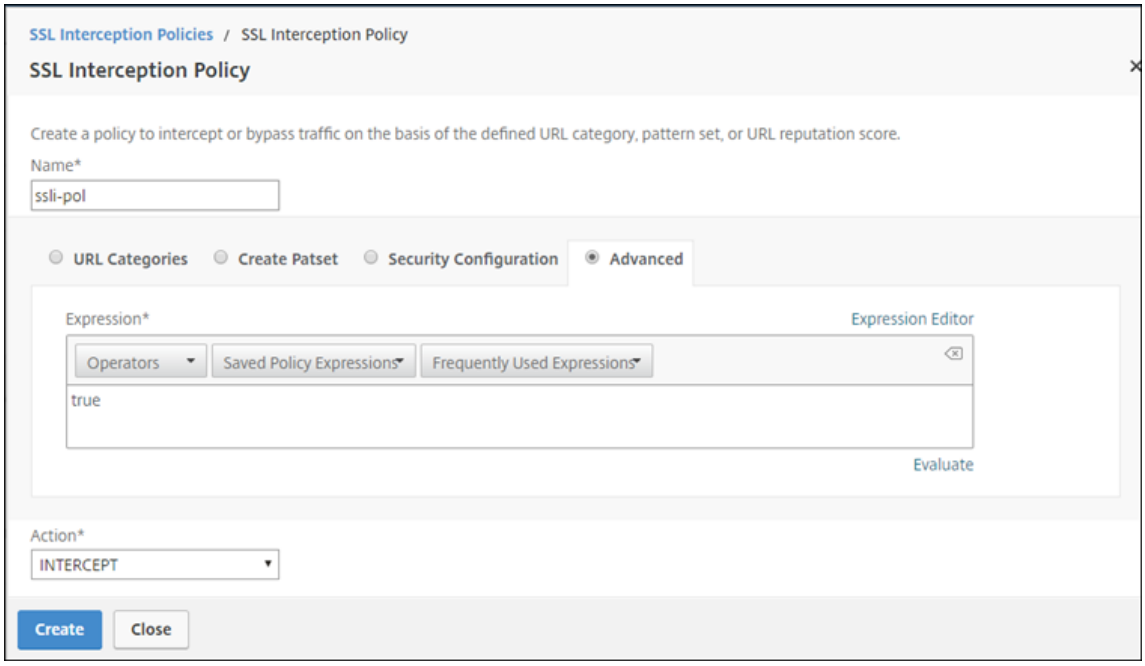


3. Cliquez sur **OK**, puis sur **Terminé**.
4. Dans **Sélectionner une paire de clés de certification d'interception SSL**, sélectionnez un certificat existant ou cliquez sur « + » pour installer une paire de certificats d'autorité de certification pour l'interception SSL. Si vous sélectionnez un certificat existant, ignorez l'étape suivante.



5. Cliquez sur **Installer**, puis sur **Fermer**.
6. Ajoutez une stratégie pour intercepter tout le trafic. Cliquez sur **Bind**. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie ou sélectionnez une stratégie existante. Si vous sélectionnez une stratégie existante, cliquez sur **Insérer**, puis ignorez les trois étapes suivantes.

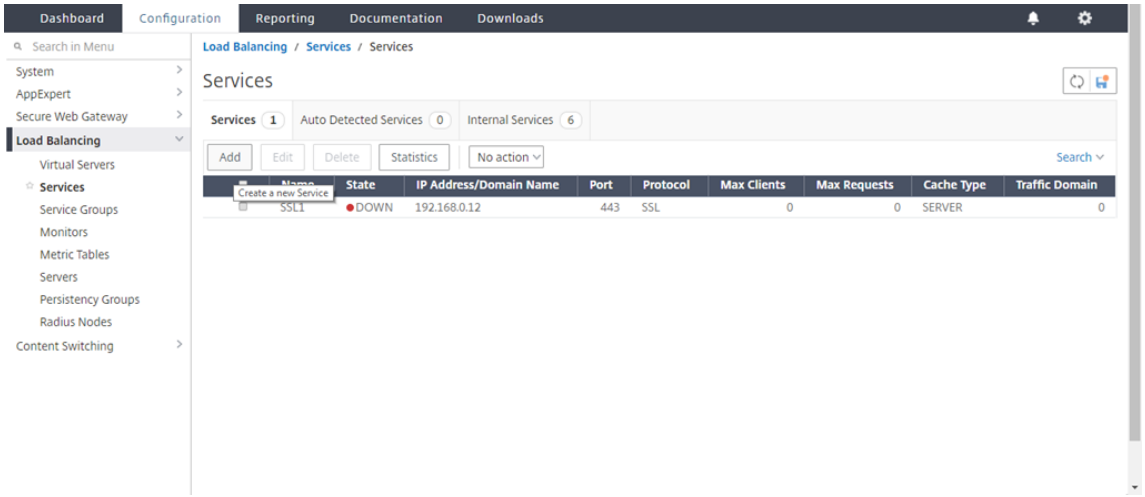
7. Entrez un nom pour la stratégie et sélectionnez **Avancé**. Dans l'éditeur d'expressions, entrez true.
8. Pour **Action**, sélectionnez **INTERCEPT**.



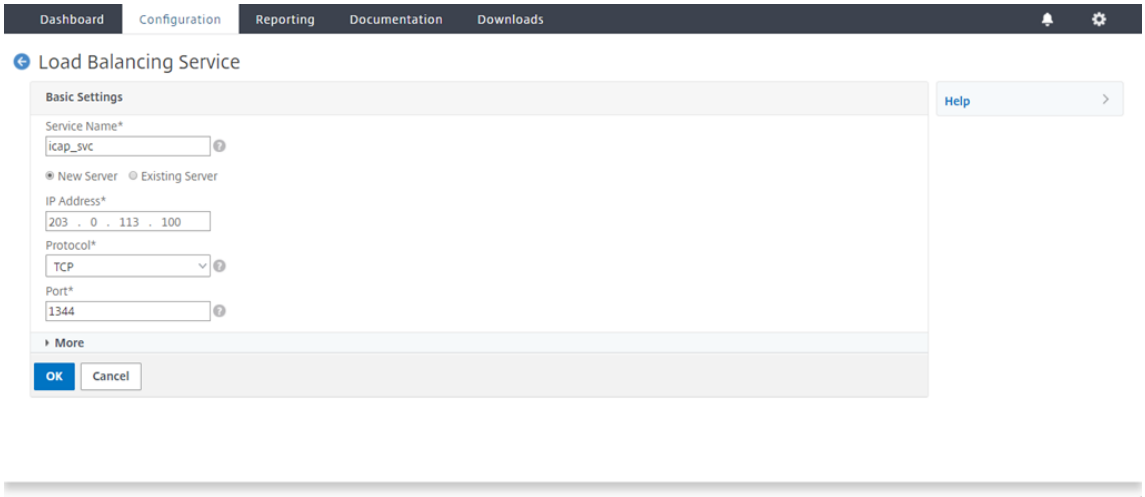
9. Cliquez sur **Créer**.
10. Cliquez sur **Continuer** quatre fois, puis cliquez sur **Terminé** .

Configurer les paramètres ICAP

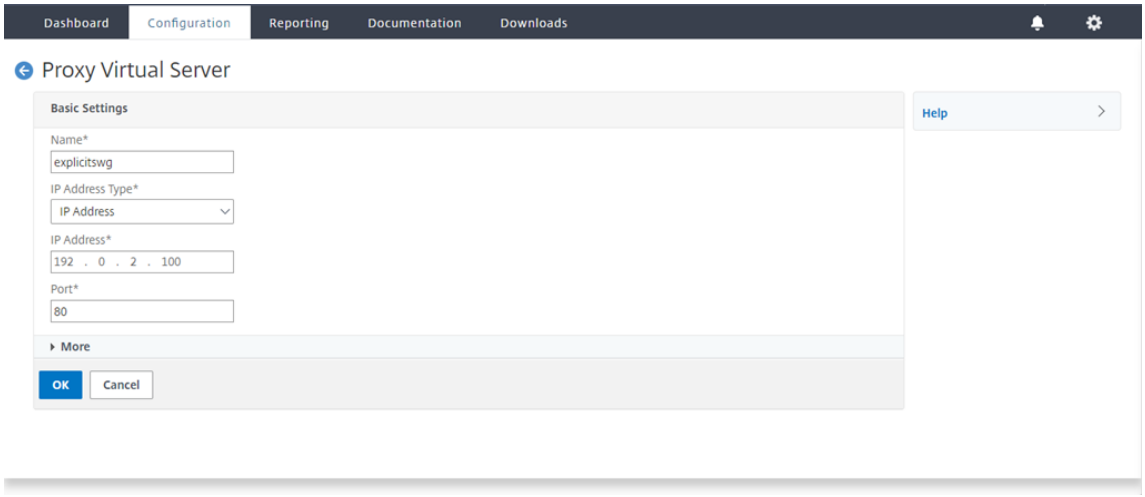
1. Accédez à **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.



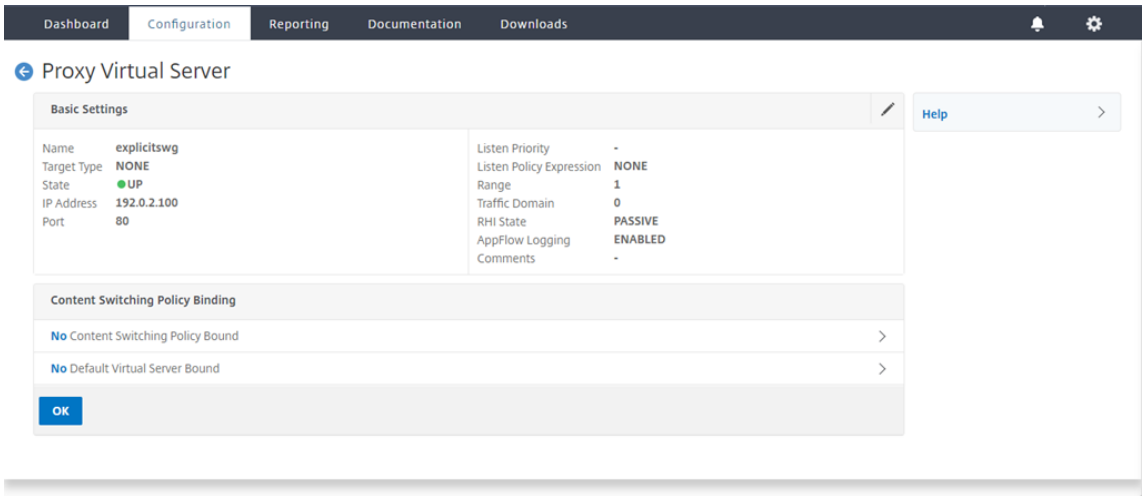
2. Tapez un nom et une adresse IP. Dans **Protocole**, sélectionnez **TCP**. Dans **Port**, tapez **1344**. Cliquez sur **OK**.



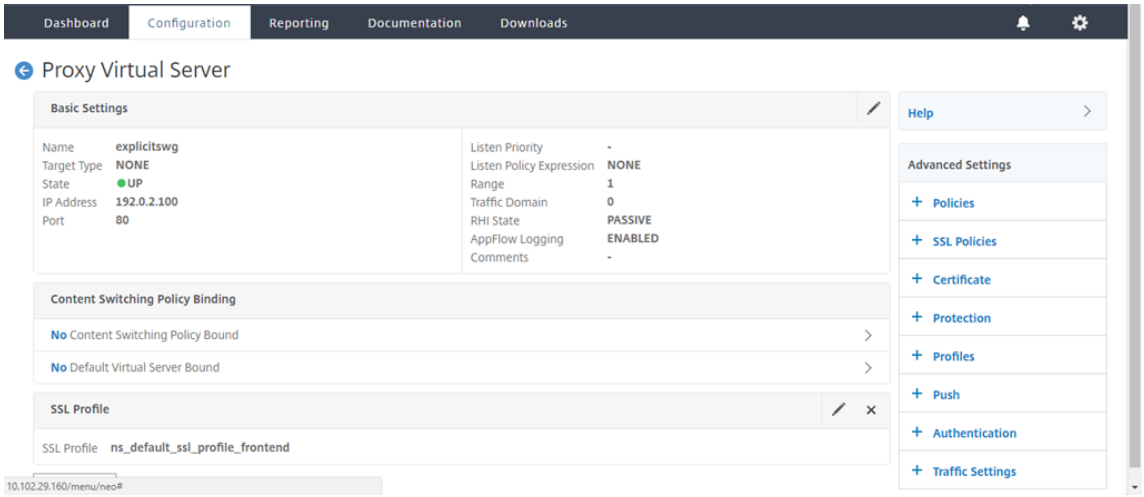
3. Accédez à **SSL Forward Proxy** > **Serveurs virtuels proxy** . Ajoutez un serveur virtuel proxy ou sélectionnez un serveur virtuel et cliquez sur **Modifier**. Après avoir entré les détails, cliquez sur **OK**.



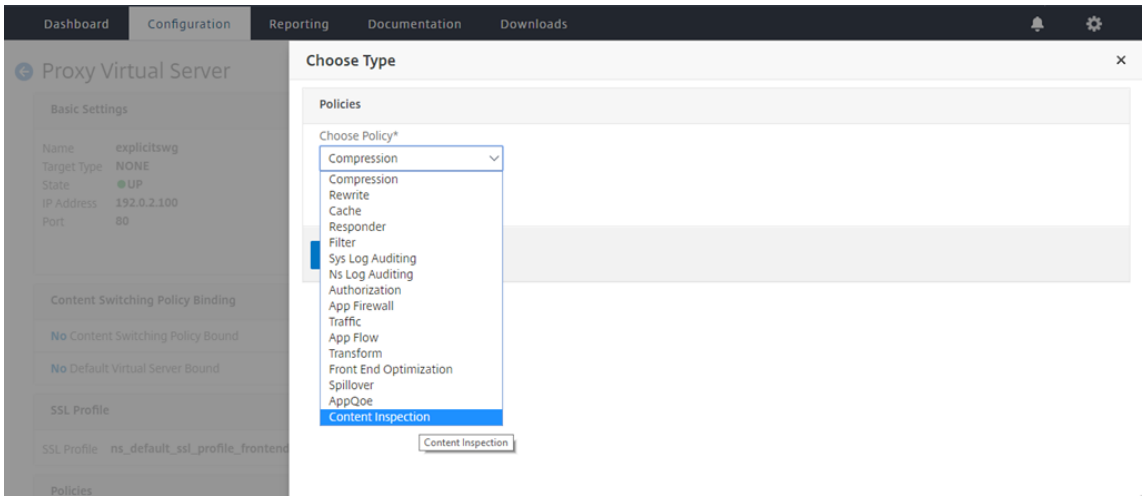
Cliquez à nouveau sur **OK**.



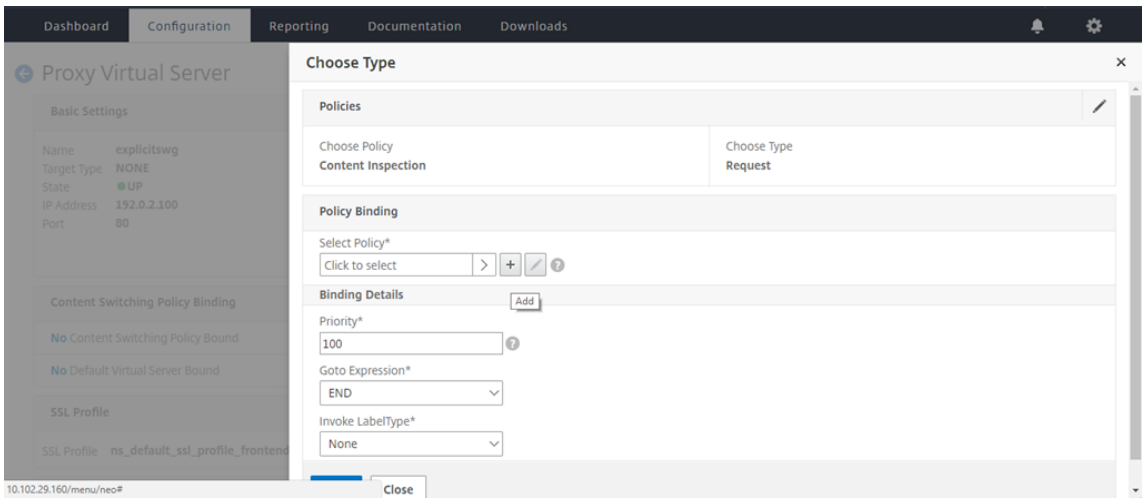
4. Dans **Paramètres avancés**, cliquez sur **Stratégies**.



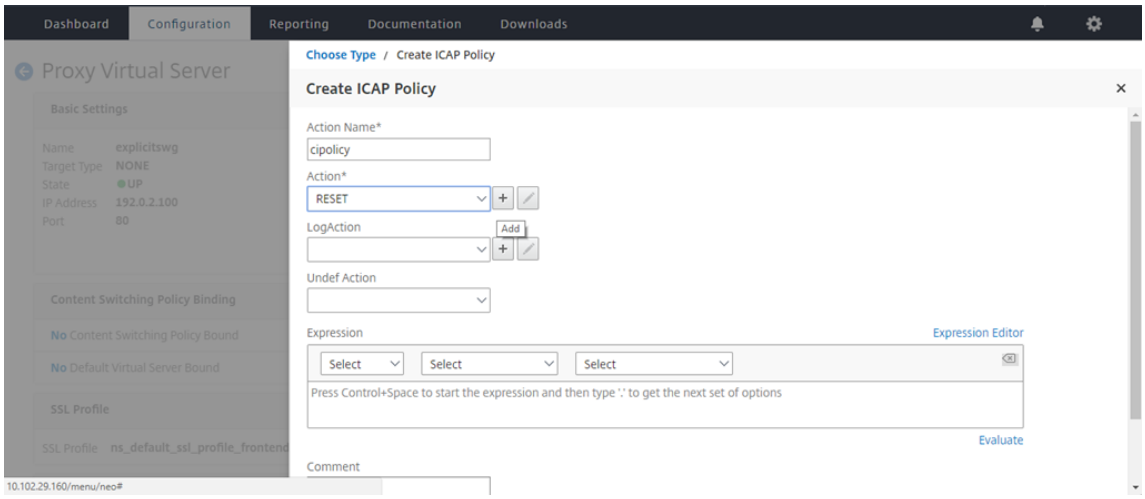
5. Dans **Choisir une stratégie**, sélectionnez **Contrôle du contenu**. Cliquez sur **Continuer**.



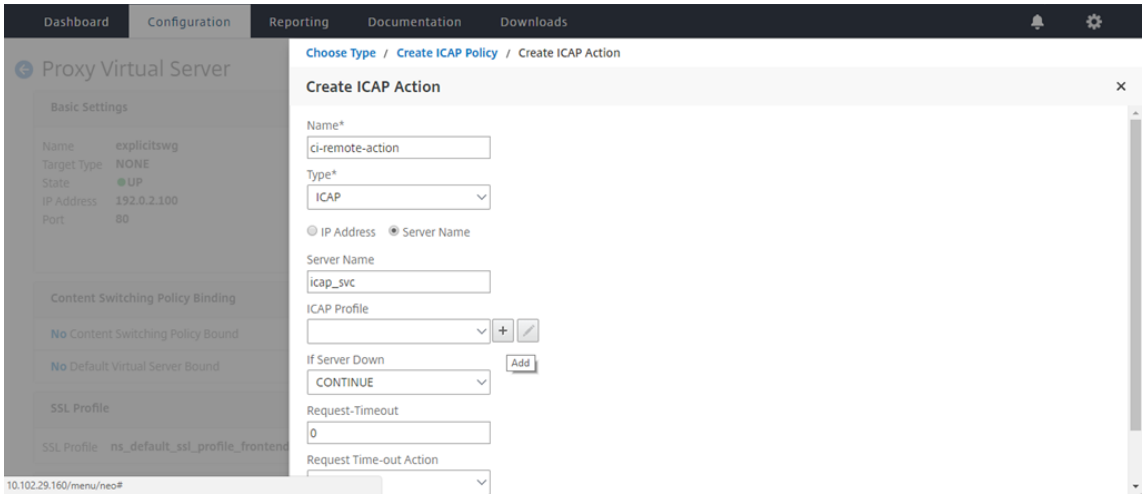
6. Dans **Sélectionner une stratégie**, cliquez sur le signe « + » pour ajouter une stratégie.



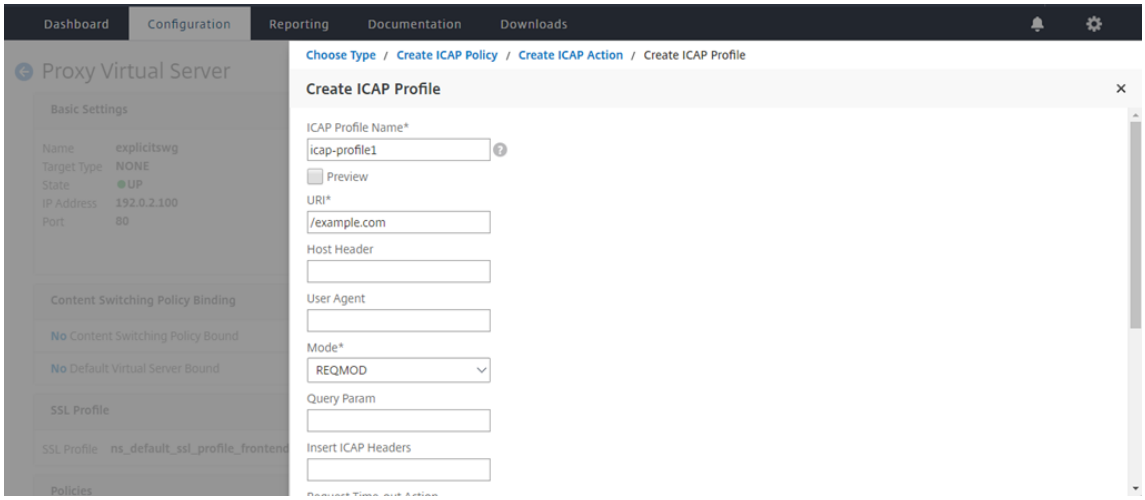
7. Entrez un nom pour la stratégie. Dans **Action**, cliquez sur le signe « + » pour ajouter une action.



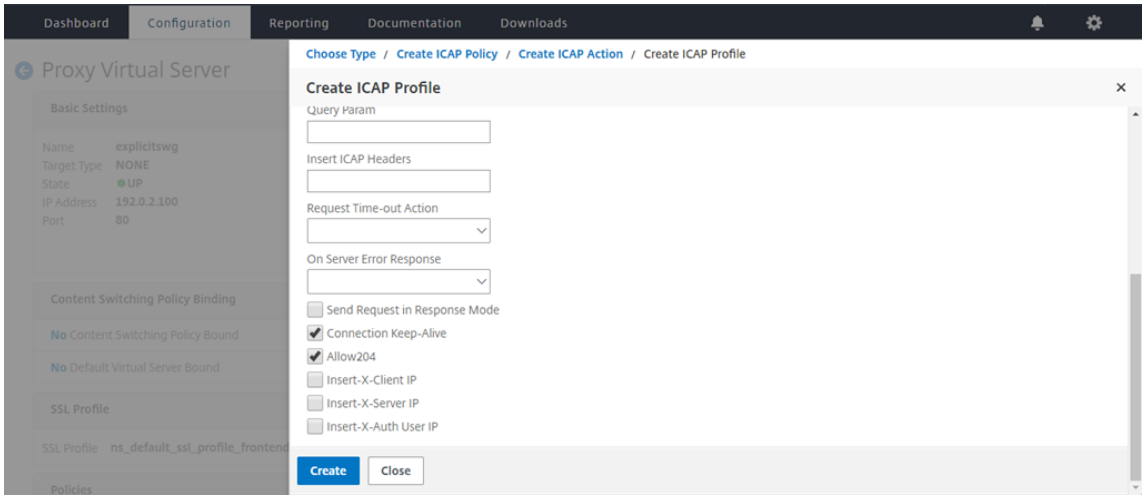
8. Tapez un nom pour l'action. Dans **Nom du serveur**, tapez le nom du service TCP créé précédemment. Dans **Profil ICAP**, cliquez sur le signe « + » pour ajouter un profil ICAP.



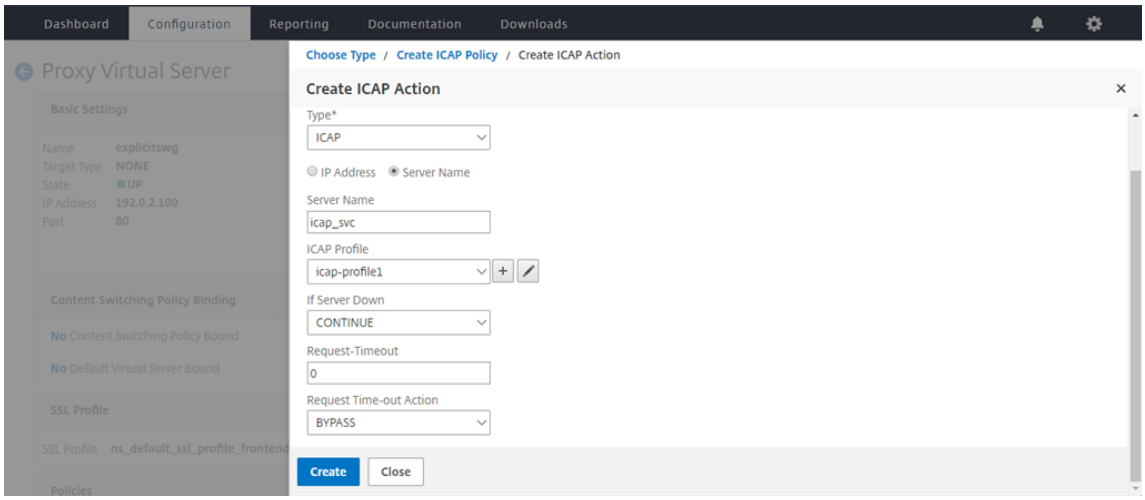
9. Tapez un nom de profil, URI. Dans **Mode**, sélectionnez **REQMOD**.



10. Cliquez sur **Créer**.

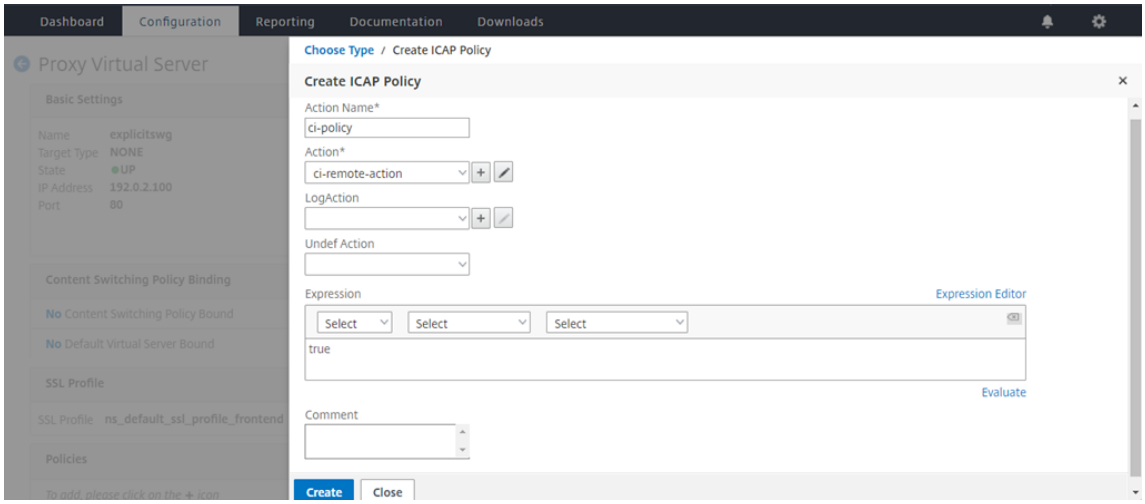


11. Dans la page **Créer une action ICAP**, cliquez sur **Créer**.

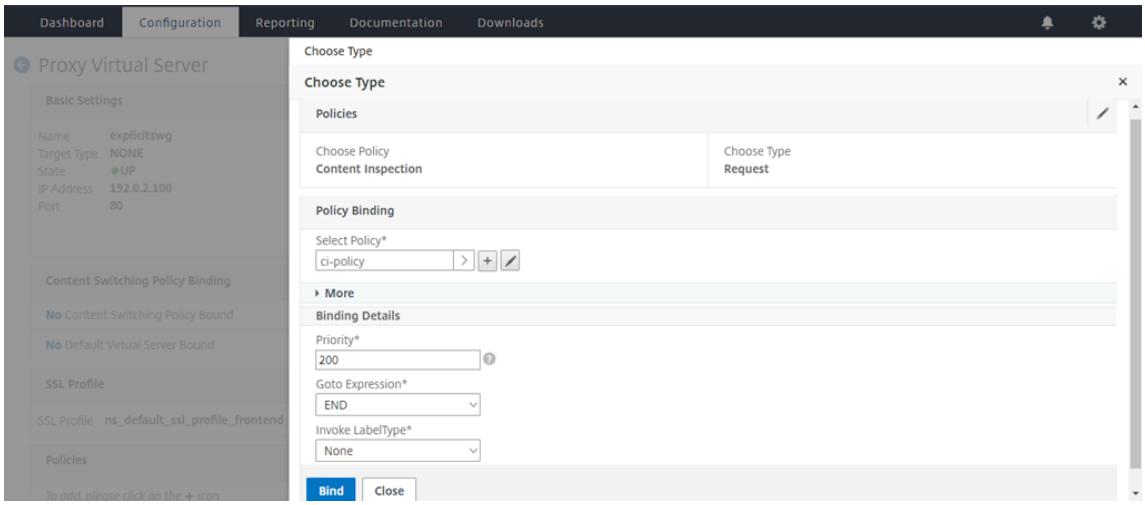


12. Dans la page **Créer une stratégie ICAP**, entrez true dans l'**éditeur d'expressions**. Cliquez en-

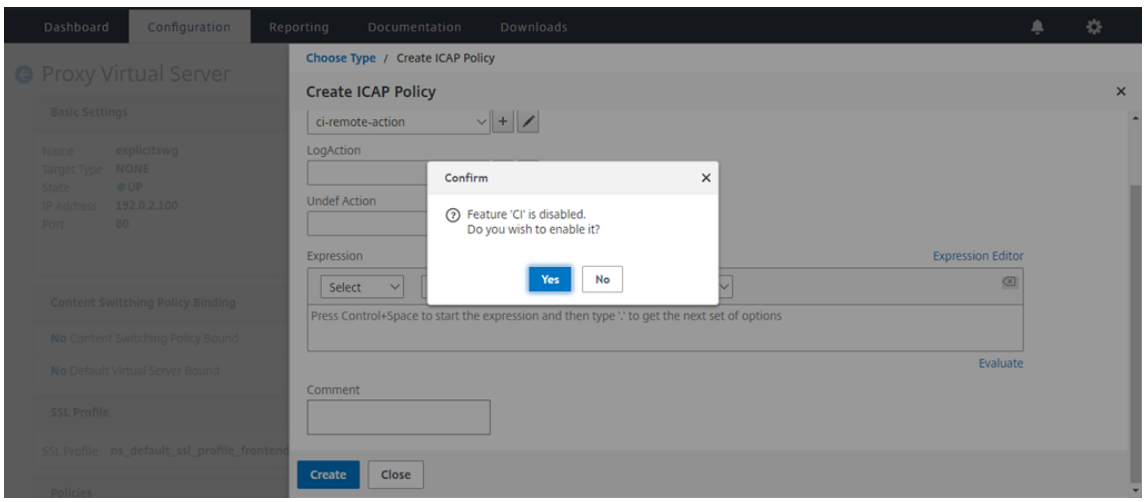
suite sur **Créer**.



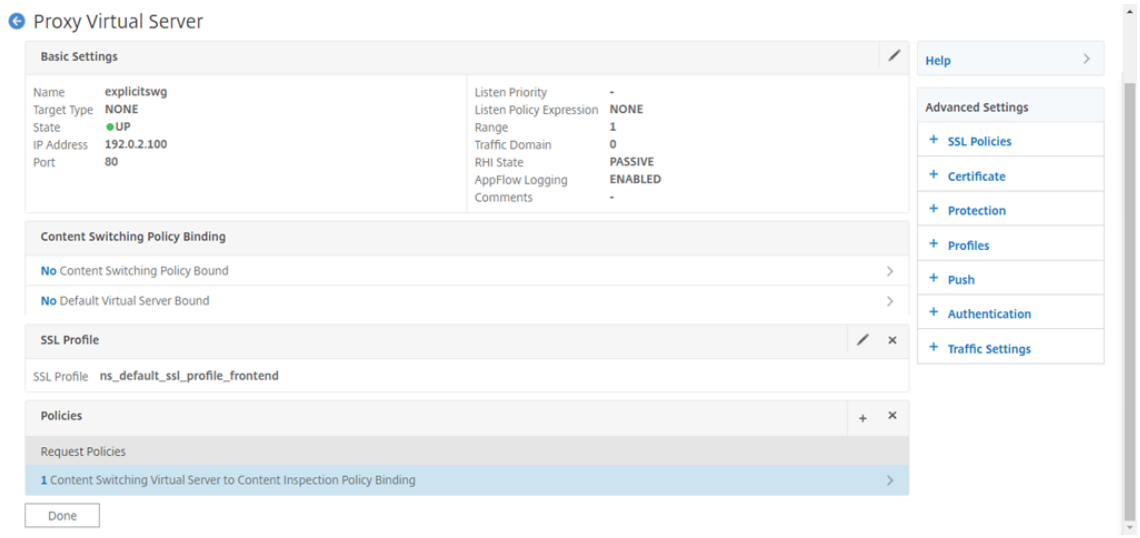
13. Cliquez sur **Bind**.



14. Lorsque vous êtes invité à activer la fonction d'inspection du contenu, sélectionnez **Oui**.



15. Cliquez sur **Terminé**.



Exemples de transactions ICAP entre l'appliance Citrix ADC et le serveur ICAP dans RESPMOD

Demande de l'appliance Citrix ADC vers le serveur ICAP :

```
RESPMOD icap://10.106.137.15:1344/resp ICAP/1.0

Host: 10.106.137.15

Connection: Keep-Alive

Encapsulated: res-hdr=0, res-body=282

HTTP/1.1 200 OK

Date: Fri, 01 Dec 2017 11:55:18 GMT

Server: Apache/2.2.21 (Fedora)

Last-Modified: Fri, 01 Dec 2017 11:16:16 GMT

ETag: "20169-45-55f457f42aee4"

Accept-Ranges: bytes

Content-Length: 69

Keep-Alive: timeout=15, max=100
```



```
24
25 Content-Type: text/plain; charset=UTF-8
26
27 X5O!P%@AP[4PZX54(P^)7CC)7 }
28  $EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
29 <!--NeedCopy-->
```

Réponse du serveur ICAP à l'appliance Citrix ADC :

```
1  ICAP/1.0 200 OK
2
3  Connection: keep-alive
4
5  Date: Fri, 01 Dec, 2017 11:40:42 GMT
6
7  Encapsulated: res-hdr=0, res-body=224
8
9  Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$
10
11 ISTag: "9.8-13.815.00-3.100.1027-1.0"
12
13 X-Virus-ID: Eicar_test_file
14
15 X-Infection-Found: Type=0; Resolution=2; Threat=Eicar_test_file;
16
17 HTTP/1.1 403 Forbidden
18
19 Date: Fri, 01 Dec, 2017 11:40:42 GMT
20
21 Cache-Control: no-cache
22
23 Content-Type: text/html; charset=UTF-8
24
25 Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$
26
27 Content-Length: 5688
28
29 <html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset
      =UTF-8"/>
30
31 …
32
33 …
34
35 </body></html>
```



```
<!--NeedCopy-->
```

Articles pratiques

January 21, 2021

Voici quelques instructions de configuration ou cas d'utilisation fonctionnelle disponibles sous forme d'articles « How to » pour vous aider à gérer votre déploiement de proxy SSL.

Filtrage d'URL

Comment créer une stratégie de catégorisation d'URL

Comment créer une stratégie de liste d'URL

Comment autoriser une URL exceptionnelle

Comment bloquer les sites Web de la catégorie pour adultes

Sécurité

January 21, 2021

Les rubriques suivantes couvrent les informations de configuration et d'installation des fonctionnalités de sécurité Citrix ADC. La plupart de ces fonctionnalités sont basées sur des stratégies.

Filtrage de contenu	Bloque les requêtes HTML inappropriées, empêchant les requêtes d'atteindre les serveurs Web.
Protection contre les surtensions	Détecte toute augmentation rapide des tentatives de connexion et règle la vitesse à laquelle les connexions sont autorisées à se diriger vers le serveur, évitant ainsi la surcharge du serveur.
Options de sécurité DNS	Assistant d'interface utilisateur simplifié pour créer des stratégies de protection contre les attaques DNS.

Protection contre les surtensions

August 20, 2021

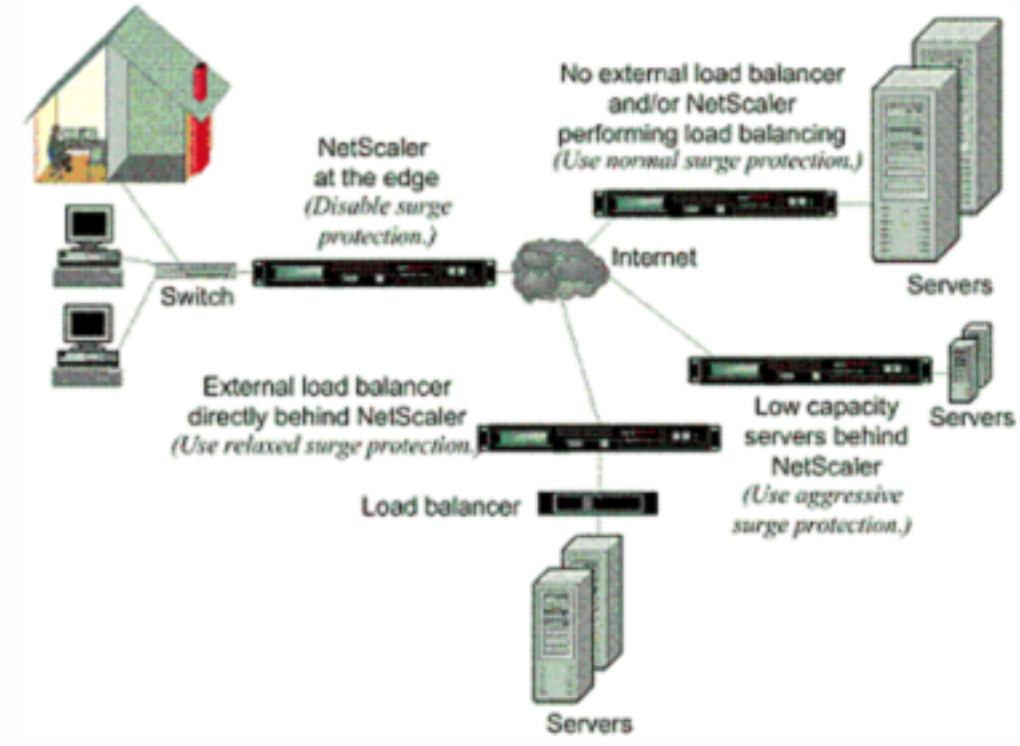
Lorsqu'un sursaut de demandes client surcharge un serveur, la réponse du serveur devient lente et le serveur ne peut pas répondre aux nouvelles demandes. La fonction de protection contre les surtensions garantit que les connexions au serveur se produisent à un rythme que le serveur peut gérer. Le taux de réponse dépend de la configuration de la protection contre les surtensions. L'appliance Citrix ADC suit également le nombre de connexions au serveur et utilise ces informations pour ajuster le taux d'ouverture des nouvelles connexions au serveur.

La protection contre les surtensions est activée par défaut. Si vous ne souhaitez pas utiliser de protection contre les surtensions, comme c'est le cas pour certaines configurations spéciales, vous devez la désactiver.

Les paramètres par défaut de protection contre les surtensions sont suffisants pour la plupart des utilisations, mais vous pouvez configurer la protection contre les surtensions pour l'adapter à vos besoins. Tout d'abord, vous pouvez définir la valeur de l'accélérateur pour lui indiquer comment gérer de manière agressive les tentatives de connexion. Ensuite, vous pouvez définir la valeur du seuil de base pour contrôler le nombre maximal de connexions simultanées que l'appliance Citrix ADC autorise avant de déclencher la protection contre les surtensions. (La valeur du seuil de base par défaut est définie par la valeur de l'accélérateur, mais après avoir défini la valeur de l'accélérateur, vous pouvez la changer à n'importe quel nombre souhaité.)

La figure suivante illustre comment la protection contre les surtensions est configurée pour gérer le trafic vers un site Web.

Figure 1. Illustration fonctionnelle de la protection contre les surtensions Citrix ADC



> **Remarque**
>
> Si l'appliance Citrix ADC est installée à la périphérie du réseau, où elle interagit avec des périphériques réseau du côté client d'Internet, la fonction de protection contre les surtensions doit être désactivée. La protection contre les surtensions doit également être désactivée si vous activez le mode USIP (Using Source IP) sur votre appliance.

L'exemple et l'illustration suivants montrent les taux de demande et de réponse pour deux cas. Dans un cas, la protection contre les surtensions est désactivée et dans l'autre, elle est activée.

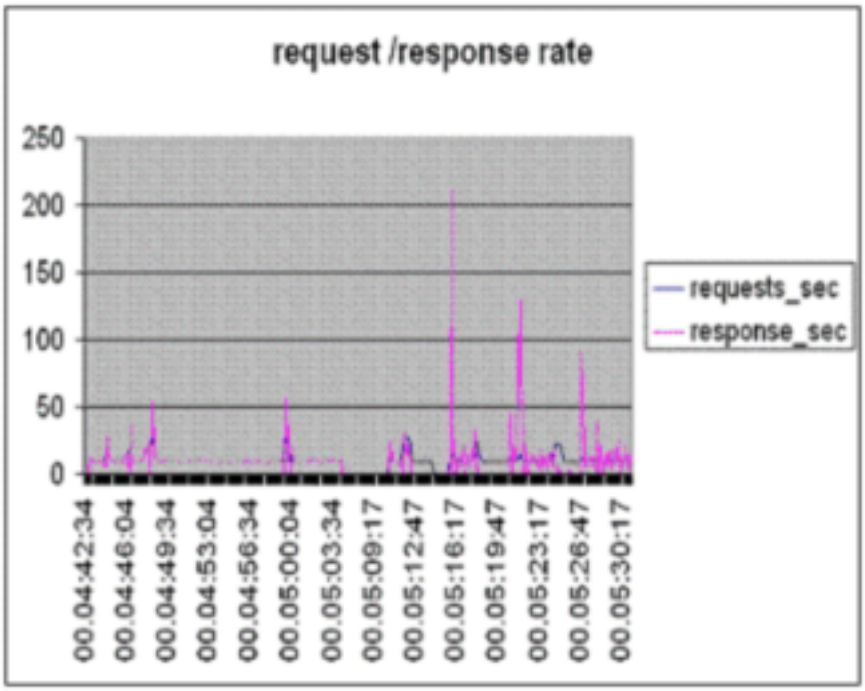
Lorsque la protection contre les surtensions est désactivée et qu'une surtension de demandes se produit, le serveur accepte autant de demandes qu'il peut traiter simultanément, puis commence à supprimer les demandes. Au fur et à mesure que le serveur devient plus surchargé, il diminue et le taux de réponse est réduit à zéro. Lorsque le serveur se rétablit après le crash, plusieurs minutes plus tard, il envoie des réinitialisations pour toutes les demandes en attente, qui présentent un comportement anormal, et répond également aux nouvelles demandes avec réinitialisation. Le processus se répète pour chaque augmentation des demandes. Par conséquent, un serveur soumis à une attaque DDoS et qui reçoit plusieurs surtensions de demandes peut devenir indisponible pour les utilisateurs légitimes.

Lorsque la protection contre les surtensions est activée et qu'une surtension de demandes se produit, la protection contre les surtensions gère le taux de demandes au serveur, en envoyant des demandes au serveur uniquement aussi rapidement que le serveur peut traiter ces demandes. Cela permet au serveur de répondre correctement à chaque demande dans l'ordre où elle a été reçue. Lorsque la

surtension est terminée, les demandes en retard sont effacées aussi rapidement que le serveur peut les traiter, jusqu'à ce que le taux de demande corresponde au taux de réponse.

La figure suivante compare les scénarios de demande et de réponse lorsque la protection contre les surtensions est activée à ceux lorsqu'elle est désactivée.

Figure 2. Taux de requête/réponse avec et sans protection contre les surtensions



Désactiver et réactiver la protection contre les surtensions

October 5, 2021

La fonction de protection contre les surtensions est activée par défaut. Lorsque la protection contre les surtensions est activée, elle est active pour tous les services que vous ajoutez.

Désactiver ou réactiver la protection contre les surtensions à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'un des ensembles de commandes suivants pour désactiver ou réactiver la protection contre les surtensions et vérifier la configuration :

```
1 - disable ns feature SurgeProtection
2 - show ns feature
3 - enable ns feature SurgeProtection
```



```
-  show ns feature
<!--NeedCopy-->
```

Exemple :

```
disable ns feature SurgeProtection
 Done show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   ON
 2)     Surge Protection                SP                   OFF
 .
 .
 .
 24)    Citrix ADC Push                  push                OFF
 Done
<!--NeedCopy-->
```

```
 enable ns feature SurgeProtection
 Done
> show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   ON
 2)     Surge Protection                SP                   ON
 .
 .
 .

 24)    Citrix ADC Push                  push                 OFF
 Done
>
<!--NeedCopy-->
```

Désactiver ou réactiver la protection contre les surtensions à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, puis sélectionnez **Paramètres**.
2. Dans le volet d'informations, cliquez sur **Modifier les fonctionnalités avancées**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, désactivez la sélection de la case à cocher **Protection contre** les surtensions pour désactiver la fonction de protection

contre les surtensions, ou cochez la case pour activer la fonction.
4. Cliquez sur **OK**.
5. Dans la boîte de dialogue Activer/Désactiver les fonctionnalités, cliquez sur Oui. Un message apparaît dans la barre d'état indiquant que la fonction a été activée ou désactivée.

Désactiver ou réactiver la protection contre les surtensions pour un service particulier à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Services**. La liste des services configurés s'affiche dans le volet de détails.
2. Dans le volet d'informations, sélectionnez le service pour lequel vous souhaitez désactiver ou réactiver la fonctionnalité de protection contre les surtensions, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le service**, cliquez sur l' **onglet Avancé**et faites défiler l'écran vers le bas.
4. Dans le cadre Autres, désactivez la case à cocher **Protection contre les surtensions** pour désactiver la fonction de protection contre les surtensions, ou activez la case à cocher pour activer la fonction.
5. Cliquez sur **OK**. Un message apparaît dans la barre d'état indiquant que la fonction a été activée ou désactivée.
   Remarque : La protection contre les surtensions ne fonctionne que lorsque la fonction et le paramètre de service sont activés.

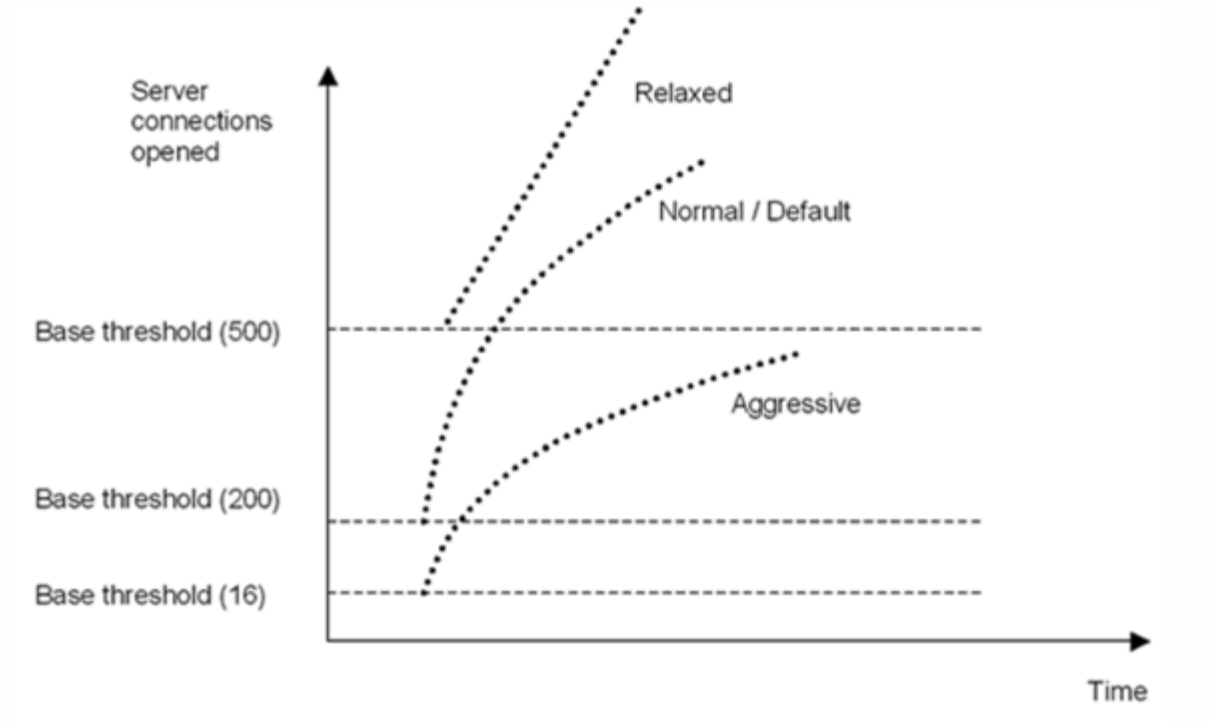
Définir des seuils de protection contre les surtensions

January 21, 2021

Pour définir la vitesse à laquelle l'appliance Citrix ADC ouvre les connexions au serveur, vous devez configurer les valeurs de seuil et d'étranglement pour la protection contre les surtensions.

La figure suivante montre les courbes de protection contre les surtensions qui résultent du réglage de la vitesse de la manette des gaz à relâchement, normal ou agressif. Selon la configuration de la capacité du serveur, vous pouvez définir des valeurs de seuil de base pour générer des courbes de protection contre les surtensions appropriées.

Figure 1. Courbes de protection contre les surtensions

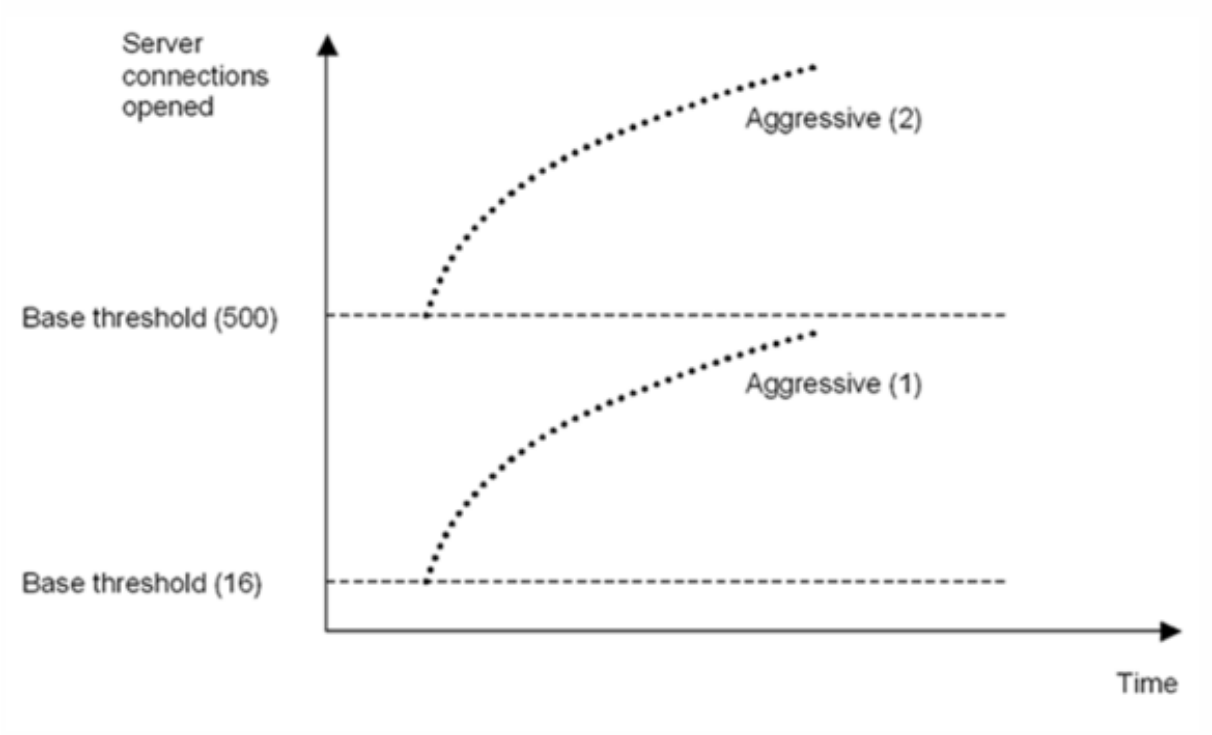


Vos paramètres de configuration affectent le comportement de la protection contre les surtensions de la manière suivante :

- Si vous ne spécifiez pas de vitesse d'accélération, il est défini sur normal (valeur par défaut) et le seuil de base est défini sur 200, comme indiqué dans la figure précédente.
- Si vous spécifiez un taux d'accélération (agressif, normal ou détendu) sans spécifier de seuil de base, la courbe reflète les valeurs par défaut du seuil de base pour ce taux d'accélération. Par exemple, si vous définissez le taux d'accélération sur relâché, la courbe résultante aura la valeur seuil de base de 500.
- Si vous spécifiez uniquement le seuil de base, toute la courbe de protection contre les surtensions se déplace vers le haut ou vers le bas, en fonction de la valeur que vous spécifiez, comme illustré dans la figure suivante.
- Si vous spécifiez à la fois un seuil de base et un taux d'accélération, la courbe de protection contre les surtensions résultante est basée sur le taux d'accélération défini et ajustée en fonction de la valeur définie pour le seuil de base.

Dans la figure suivante, la courbe inférieure (Agressif 1) se produit lorsque le taux de manette des gaz est défini sur agressif mais que le seuil de base n'est pas défini. La courbe supérieure (Agressif 2) se produit lorsque le seuil de base est défini sur 500, mais que le taux de manette des gaz n'est pas réglé. La deuxième courbe supérieure (Agressif 2) se produit également lorsque le seuil de base est défini sur 500 et que le taux de manette des gaz est défini sur agressif.

Figure 2. Taux agressif avec le seuil de base par défaut ou défini



Définissez le seuil de protection contre les surtensions à l'aide de l'interface graphique

1. Dans le volet de navigation, développez Système, puis sélectionnez Paramètres.
2. Dans le volet d'informations, cliquez sur Paramètres système globaux.
3. Si vous souhaitez définir un seuil de base différent du seuil par défaut pour la vitesse d'accélération, dans la boîte de dialogue Configurer les paramètres globaux, zone de texte Seuil de base, entrez le nombre maximal de connexions serveur simultanées autorisées avant le déclenchement de la protection contre les surtensions. Le seuil de base est le nombre maximal de connexions serveur pouvant être ouvertes avant l'activation de la protection contre les surtensions. La valeur maximale de ce paramètre est 32 767 connexions serveur. Le paramètre par défaut de cette valeur est contrôlé par le taux d'accélération que vous choisissez à l'étape suivante.

   Remarque : Si vous ne définissez pas de valeur explicite ici, la valeur par défaut sera utilisée.
4. Dans la liste déroulante Accélération, sélectionnez un taux d'accélérateur. L'accélérateur correspond à la vitesse à laquelle l'appliance Citrix ADC autorise l'ouverture des connexions au serveur. L'accélérateur peut être réglé sur les valeurs suivantes :

   - **Agressif :** choisissez cette option lorsque la capacité de gestion de la connexion et de gestion de la surtension du serveur est faible et que la connexion doit être gérée avec soin. Lorsque vous définissez l'accélérateur sur agressif, le seuil de base est défini sur une valeur

par défaut de 16, ce qui signifie que la protection contre les surtensions est déclenchée chaque fois qu'il y a 17 connexions simultanées ou plus au serveur.

- **Normal :** choisissez cette option lorsqu'il n'y a pas d'équilibrage de charge externe derrière l'appliance Citrix ADC ou en aval. Le seuil de base est défini sur une valeur de 200, ce qui signifie que la protection contre les surtensions est déclenchée chaque fois qu'il y a 201 connexions simultanées ou plus au serveur. Normal est l'option d'accélération par défaut.
- **Relaxé :** choisissez cette option lorsque l'appliance Citrix ADC effectue l'équilibrage de charge entre un grand nombre de serveurs Web et peut donc gérer un grand nombre de connexions simultanées. Le seuil de base est défini sur une valeur de 500, ce qui signifie que la protection contre les surtensions n'est déclenchée que lorsqu'il existe 501 connexions simultanées ou plus au serveur.

5. Cliquez sur OK. Un message apparaît dans la barre d'état indiquant que les paramètres globaux sont configurés.

Vider la file d'attente de surtension

August 20, 2021

Lorsqu'un serveur physique reçoit un sursaut de demandes, il devient lent à répondre aux clients qui lui sont actuellement connectés, ce qui laisse les utilisateurs insatisfaits et mécontents. Souvent, la surcharge provoque également les clients à recevoir des pages d'erreur. Pour éviter de telles surcharges, l'appliance Citrix ADC fournit des fonctionnalités telles que la protection contre les surtensions, qui contrôle la vitesse d'établissement de nouvelles connexions à un service.

L'appliance effectue le multiplexage des connexions entre les clients et les serveurs physiques. Lorsqu'elle reçoit une demande client pour accéder à un service sur un serveur, l'appliance recherche une connexion déjà établie au serveur qui est libre. S'il trouve une connexion libre, il utilise cette connexion pour établir un lien virtuel entre le client et le serveur. S'il ne trouve pas de connexion libre existante, l'appliance établit une nouvelle connexion avec le serveur et établit un lien virtuel entre un client et le serveur. Toutefois, si l'appliance ne peut pas établir de nouvelle connexion avec le serveur, elle envoie la demande client à une file d'attente de surtension. Si tous les serveurs physiques liés au serveur virtuel d'équilibrage de charge ou de commutation de contenu atteignent la limite supérieure des connexions client (valeur maximale du client, seuil de protection contre les surtensions ou capacité maximale du service), l'appliance ne peut pas établir de connexion avec un serveur. La fonction de protection contre les surtensions utilise la file d'attente pour réguler la vitesse d'ouverture des connexions avec les serveurs physiques. L'appliance gère une file d'attente de surtension différente pour chaque service lié au serveur virtuel.

La longueur d'une file d'attente de surtension augmente lorsqu'une requête pour laquelle l'appliance

ne peut pas établir de connexion, et la longueur diminue chaque fois qu'une demande de la file d'attente est envoyée au serveur ou qu'une demande est dépassée et supprimée de la file d'attente.

Si la file d'attente de surtension d'un service ou d'un groupe de services devient trop longue, vous pouvez la vider. Vous pouvez vider la file d'attente de surtension d'un service ou d'un groupe de services spécifique, ou de tous les services et groupes de services liés à un serveur virtuel d'équilibrage de charge. Le vidange d'une file d'attente de surtension n'affecte pas les connexions existantes. Seules les requêtes présentes dans la file d'attente de surtension sont supprimées. Pour ces demandes, le client doit faire une nouvelle demande.

Vous pouvez également vider la file d'attente de surtension d'un serveur virtuel de commutation de contenu. Si un serveur virtuel de commutation de contenu transfère certaines requêtes à un serveur virtuel d'équilibrage de charge particulier, et que le serveur virtuel d'équilibrage de charge reçoit également d'autres demandes, lorsque vous videz la file d'attente de surtension du serveur virtuel de commutation de contenu, seules les demandes reçues de ce changement de contenu serveur virtuel sont vidé. Les autres requêtes de la file d'attente de surtension du serveur virtuel d'équilibrage de charge ne sont pas vidées.

Remarque :

> - Vous ne pouvez pas vider les files d'attente de surtension des serveurs virtuels de redirection de cache, d'authentification, de VPN ou de serveurs virtuels GSLB ou des services GSLB.
> - N'utilisez pas la fonctionnalité Protection contre les surtensions si USIP (USIP) est activée.

Purger une file d'attente de surtension à l'aide de l'interface de ligne de commande

La commande flush ns surgeQ fonctionne de la manière suivante :

- Vous pouvez spécifier le nom d'un service, d'un groupe de services ou d'un serveur virtuel dont la file d'attente de surtension doit être vidé.
- Si vous spécifiez un nom lors de l'exécution de la commande, la file d'attente de surtension de l'entité spécifiée est vidé. Si plusieurs entités portent le même nom, l'appliance vid les files d'attente de surtension de toutes ces entités.
- Si vous spécifiez le nom d'un groupe de services, ainsi qu'un nom de serveur et un port lors de l'exécution de la commande, l'appliance vide la file d'attente de surtension du membre du groupe de services spécifié uniquement.
- Vous ne pouvez pas spécifier directement un membre de groupe de services <serverName> and <port> sans spécifier le nom du groupe de services <name> et vous ne pouvez pas spécifier <port> sans un <serverName>. Spécifiez le <serverName> et <port> si vous souhaitez vider la file d'attente de surtension pour un membre du groupe de services spécifique.
- Si vous exécutez la commande sans spécifier de nom, l'appliance vide les files d'attente de surtension de toutes les entités présentes sur l'appliance.

- Si un membre du groupe de services est identifié par un nom de serveur, vous devez spécifier le nom du serveur dans cette commande ; vous ne pouvez pas spécifier son adresse IP.

À l'invite de commandes, tapez :

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]
```

Exemples

1. `flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80`

   La commande précédente vide la file d'attente de surtension du service ou du serveur virtuel appelé SVC1ANZGB et dont l'adresse IP est 10.10.10.

2. `flush ns surgeQ`

   La commande précédente vide toutes les files d'attente de surtension de l'appliance.

Purger une file d'attente de surtension à l'aide de l'interface graphique

Accédez à Gestion du trafic > Changement de contenu > Serveurs virtuels, sélectionnez un serveur virtuel et, dans la liste Action, sélectionnez Queue d'attente de surtension.

Options de sécurité DNS

August 20, 2021

Vous pouvez désormais configurer les options de sécurité DNS à partir de la page Ajouter un profil de sécurité DNS dans l'interface graphique Citrix ADC. Pour configurer les options de sécurité DNS à partir de l'interface de ligne de commande Citrix ADC ou de l'API NITRO, utilisez les composants App-Expert. Pour obtenir des instructions, reportez-vous à la documentation de l'API NITRO et au Guide de référence des commandes Citrix ADC.

Une option, la protection contre l'empoisonnement du cache, est activée par défaut et ne peut pas être désactivée. Vous pouvez appliquer les autres options à tous les points de terminaison DNS ou à des serveurs virtuels DNS spécifiques dans votre déploiement, comme indiqué dans le tableau suivant :

Option de sécurité	Peut être appliqué à tous les points de terminaison DNS ?	Peut être appliqué à des serveurs virtuels DNS spécifiques ?
Protection DDoS DNS	Oui	Oui

Option de sécurité	Peut être appliqué à tous les points de terminaison DNS ?	Peut être appliqué à des serveurs virtuels DNS spécifiques ?
Gérer les exceptions : serveurs sur liste blanche/liste noire	Oui	Oui
Empêcher les attaques de sous-domaine aléatoires	Oui	Oui
Contourner le cache	Oui	Non
Imposer transactions DNS sur TCP	Oui	Oui
Fournissez les détails de la racine dans la réponse DNS	Oui	Non

Protection contre l'empoisonnement de la cache

Une attaque par empoisonnement du cache redirige les utilisateurs des sites légitimes vers des sites malveillants.

Par exemple, l'attaquant remplace une adresse IP authentique dans le cache DNS par une adresse IP fausse qu'il contrôle. Lorsque le serveur répond à des demandes provenant de ces adresses IP, le cache est empoisonné. Les demandes ultérieures d'adresses du domaine sont redirigées vers le site de l'attaquant.

L'option Protection contre l'empoisonnement du cache empêche l'insertion de données corrompues dans la base de données qui met en cache les demandes et les réponses du serveur DNS. Cette fonctionnalité est intégrée aux appliances Citrix ADC et est toujours activée.

Protection DDoS DNS

Vous pouvez configurer l'option Protection DDoS DNS pour chaque type de requête que vous soupçonnez d'être utilisée dans une attaque DDoS. Pour chaque type, l'appliance supprime toutes les demandes reçues après le dépassement d'une valeur seuil pour le nombre de demandes reçues au cours d'une période spécifiée (tranche de temps). Vous pouvez également configurer cette option pour consigner un avertissement sur le serveur SYSLOG. Par exemple :

- **DROP :** - Sélectionnez cette option pour déposer des requêtes sans journalisation. Supposons que vous ayez activé une protection d'enregistrement avec une valeur de seuil 15, une tranche de temps de 1 seconde et que vous avez choisi DROP. Lorsque les demandes entrantes dépassent 15 requêtes en 1 seconde, les paquets commencent à être supprimés.

- **AVERTISSEMENT :** - Sélectionnez cette option pour enregistrer et déposer les demandes. Supposons que vous ayez activé une protection d'enregistrement avec une valeur de seuil 15, une tranche de temps de 1 seconde et que vous avez choisi WARN. Lorsque les demandes entrantes dépassent 15 requêtes en 1 seconde, un message d'avertissement est enregistré indiquant une menace, puis les paquets sont supprimés. Citrix vous recommande de définir des valeurs de seuil pour WARN inférieures à la valeur seuil de DROP pour un type d'enregistrement. Ce paramètre aide les administrateurs à identifier une attaque en consignant un message d'avertissement avant que l'attaque réelle ne se produise et Citrix ADC commence à abandonner les demandes entrantes.

Définir un seuil pour le trafic entrant à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Sécurité** > **Sécurité DNS**.
2. Sur la page **Profil de sécurité DNS**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil de sécurité DNS**, procédez comme suit :
4. Développez la **protection DDoS DNS**.
   a) Sélectionnez le type d'enregistrement et entrez la limite de seuil et la valeur de tranche temporelle.
   b) Sélectionnez **DROP** ou **WARN** .
   c) Répétez les étapes a et b pour chacun des autres types d'enregistrement contre lesquels vous souhaitez protéger.
5. Cliquez sur **Soumettre**.

Gérer les exceptions — serveurs de listes d'autorisations/listes de blocage

Gérer les exceptions vous permet d'ajouter des exceptions à la liste de blocage ou à autoriser la liste des noms de domaine et des adresses IP. Par exemple :

- Lorsqu'une adresse IP particulière est identifiée en train de publier une attaque, cette adresse IP peut être ajoutée à la liste de blocage.
- Lorsque les administrateurs constatent qu'il y a un nombre inattendu de demandes pour un nom de domaine particulier, il est possible d'ajouter ce nom de domaine à la liste de blocage.
- `NXDomains` et certains des domaines existants pouvant consommer les ressources du serveur peuvent être mis sur liste noire.
- Lorsque les administrateurs autorisent les noms de domaine de liste ou les adresses IP, les requêtes ou requêtes provenant uniquement de ces domaines ou adresses IP reçoivent une réponse et toutes les autres sont supprimées.

Créez une liste d'autorisation ou une liste bloquée à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Sécurité DNS**.

2. Dans la page **Profils de sécurité DNS**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil de sécurité DNS**, procédez comme suit :
   a) Développez **Gérer les exceptions — Liste d'autorisation et de blocage des serveurs**.
   b) Sélectionnez **Bloquer** pour bloquer les requêtes des domaines/adresses figurant sur la liste noire ou **Autoriser** uniquement pour autoriser les requêtes provenant des domaines/adresses figurant sur la liste blanche.
   c) Dans la zone **Nom de domaine/Adresse IP**, entrez les noms de domaine, adresses IP ou plages d'adresses IP. Utilisez des virgules pour séparer les entrées.
   Remarque : Si vous sélectionnez l'**option avancée**, vous pouvez utiliser les options « commencer par », « contient » et « se termine par » pour définir les critères.
   Par exemple, vous pouvez définir des critères pour bloquer une requête DNS commençant par « image » ou se terminant par « .co.ru » ou contenant des « sites mobiles ». «
4. Cliquez sur **Soumettre**.

Empêcher les attaques de sous-domaine aléatoires

Dans les attaques aléatoires de sous-domaines, les requêtes sont envoyées à des sous-domaines aléatoires et inexistants de domaines légitimes. Cette action augmente la charge sur les résolveurs et serveurs DNS. En conséquence, ils peuvent devenir surchargés et ralentir.

L'option Empêcher les attaques de sous-domaine aléatoires demande au répondeur DNS de supprimer les requêtes DNS qui dépassent une longueur spécifiée.

Supposons que example.com est un nom de domaine que vous possédez et que, par conséquent, la demande de résolution vient à votre serveur DNS. L'attaquant peut ajouter un sous-domaine aléatoire à example.com et envoyer une demande. En fonction de la longueur de requête spécifiée et du nom de domaine complet, les requêtes aléatoires sont supprimées.

Par exemple, si la requête est www.image987trending.example.com, elle est supprimée si la longueur de la requête est définie sur 20.

Spécifier une longueur de requête DNS à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Sécurité DNS**.
2. Dans la page **Profils de sécurité DNS**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil de sécurité DNS**, procédez comme suit :
   a) Développez **Empêcher les attaques de sous-domaine aléatoires**.
   b) Entrez la valeur numérique de la longueur de la requête.
4. Cliquez sur **Soumettre**.

Contournement du cache

Lors d'une attaque, les données déjà mises en cache doivent être protégées. Pour protéger le cache, de nouvelles demandes pour certains domaines ou types d'enregistrements ou codes de réponse peuvent être envoyées aux serveurs d'origine au lieu de les mettre en cache.

L'option Contournement du cache indique à l'appliance Citrix ADC de contourner le cache pour les domaines, les types d'enregistrements ou les codes de réponse spécifiés lorsqu'une attaque est détectée.

Contournez le cache pour des domaines ou des types d'enregistrement ou des types de réponse spécifiés à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Sécurité DNS**.
2. Dans la page **Profils de sécurité DNS**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil de sécurité DNS**, développez **Contournement du cache** et entrez les noms de domaine. Vous pouvez également choisir les types d'enregistrement ou les types de réponses pour lesquels le cache doit être contourné.
    - Cliquez sur **Domaines** et saisissez les noms de domaine. Utilisez des virgules pour séparer les entrées.
    - Cliquez sur **Types d'enregistrement** et choisissez les types d'enregistrement.
    - Cliquez sur **Types de réponse** et choisissez le type de réponse.
4. Cliquez sur **Soumettre**.

Imposer transactions DNS sur TCP

Certaines attaques DNS peuvent être évitées si les transactions sont forcées d'utiliser TCP au lieu d'UDP. Par exemple, lors d'une attaque de bot, le client envoie un flot de requêtes mais ne peut pas gérer les réponses. Si l'utilisation de TCP est appliquée pour ces transactions, alors les bots ne peuvent pas comprendre les réponses et ne peuvent donc pas envoyer de demandes via TCP.

Forcer les domaines ou les types d'enregistrements à fonctionner au niveau TCP à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Sécurité DNS**.
2. Dans la page **Profils de sécurité DNS**, cliquez sur **Ajouter**.
3. Dans la page **Ajouter un profil de sécurité DNS**, développez **Imposer les transactions DNS sur TCP** et entrez les noms de domaine et/ ou choisissez les types d'enregistrement pour lesquels les transactions DNS doivent être appliquées sur TCP.
    - Cliquez sur **Domaines** et saisissez les noms de domaine. Utilisez des virgules pour séparer les entrées.

- Cliquez sur **Types d'enregistrements**, puis choisissez les types d'enregistrements.

4. Cliquez sur **Soumettre**.

Fournissez les détails de la racine dans la réponse DNS

Dans certaines attaques, l'attaquant envoie un flot de requêtes pour des domaines non liés qui ne sont pas configurés ou mis en cache sur l'appliance Citrix ADC. Si le `dnsRootReferral` paramètre est ENABLED, il expose tous les serveurs racine.

L'option Fournir les détails racine dans la réponse DNS demande à l'appliance Citrix ADC de restreindre l'accès aux références racine pour une requête qui n'est pas configurée ou mise en cache. L'appliance envoie une réponse vide.

L'option Fournissez les détails racine dans l'option Réponse DNS peut également atténuer ou bloquer les attaques d'amplification. Lorsque le paramètre DNSRootReferral est DÉSACTIVÉ, il n'y a pas de références racine dans les réponses Citrix ADC et, par conséquent, elles ne sont pas amplifiées.

Activer ou désactiver l'accès au serveur racine à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Sécurité DNS**.
2. Dans la page **Profils de sécurité DNS**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil de sécurité DNS**, procédez comme suit :
   a) Développez **Fournissez les détails racine dans la réponse DNS** .
   b) Cliquez **sur ON** ou **OFF** pour autoriser ou restreindre l'accès au serveur racine.
4. Cliquez sur **Soumettre**.

Système

January 21, 2021

Cette section fournit des informations au niveau système sur Citrix ADC. Cela inclut une explication détaillée des fonctionnalités au niveau du système, les scénarios dans lesquels elles peuvent être utilisées, les étapes de configuration et des exemples pour vous aider à mieux comprendre les fonctionnalités.

- Opérations de base
- Authentification et autorisation
- Configurations TCP
- Configurations HTTP
- SNMP
- Journalisation de l'audit

- Journalisation du serveur Web
- Call Home
- Outil de création de rapports
- CloudBridge Connector
- Haute disponibilité
- Optimisation TCP

Opérations de base système

October 5, 2021

Les configurations suivantes vous permettent d'effectuer des opérations de base système sur une appliance Citrix ADC.

Comment afficher, enregistrer et effacer la configuration Citrix ADC

Les configurations Citrix ADC sont stockées dans le fichier `/nsconfig/ns.conf directory`. Pour que les configurations soient disponibles entre les sessions, vous devez enregistrer la configuration après chaque modification de configuration.

Afficher la configuration en cours à l'aide de l'interface de commande

À l'invite de commandes, tapez :

```
show ns runningConfig
```

Afficher la configuration en cours d'exécution à l'aide de l'interface graphique

1. Accédez à **Système** > **Diagnostics** et, dans le **groupe Configuration de la vue**, cliquez sur **Exécuter la configuration.**

Afficher la différence entre les deux fichiers de configuration à l'aide de l'interface de commande

À l'invite de commandes, tapez :

```
diff ns config <configfile> <configfile2>
```


Afficher la différence entre les deux fichiers de configuration à l'aide de l'interface graphique

1. Accédez à **Système** > **Diagnostics** et, dans le **groupe Afficher la configuration**, cliquez sur **Différence de configuration**.

Enregistrez les configurations Citrix ADC à l'aide de l'interface de commande

À l'invite de commandes, tapez :

```
save ns config
```

Enregistrez les configurations Citrix ADC à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, dans le coin supérieur droit, cliquez sur l'icône **Enregistrer** .

Afficher les configurations enregistrées à l'aide de l'interface de commande

À l'invite de commandes, tapez :

```
show ns ns.conf
```

Afficher les configurations enregistrées à l'aide de l'interface graphique

Accédez à **Système** > **Diagnostics** et, dans le groupe **Afficher la configuration**, cliquez sur **Configuration enregistrée**.

Effacer la configuration Citrix ADC à l'aide de l'interface de commande

Vous disposez des trois options suivantes pour effacer la configuration Citrix ADC.

Niveau de base. Effacer votre configuration au niveau de base efface tous les paramètres sauf les suivants :

- `Nsroot` mot de passe
- Fuseau horaire
- Serveur NTP
- Connexion au serveur ADM
- Informations sur le fichier de licence
- NSIP, MIP (s) et SNIP (s)
- Paramètres réseau (paramètres de passerelle par défaut, VLAN, RHI, NTP et DNS)
- Définitions de nœuds HA
- Paramètres des fonctionnalités et des modes
- Mot de passe administrateur par défaut (`nsroot`)

Niveau étendu. L'effacement de votre configuration au niveau étendu efface tous les paramètres, à l'exception des suivants :

- NSIP, MIP(s), and SNIP(s)
- Network settings (Default Gateway, VLAN, RHI, NTP, and DNS settings)
- HA node definitions

Les paramètres de fonction et de mode reviennent à leurs valeurs par défaut.

Niveau complet. Si vous effacez votre configuration au niveau complet, tous les paramètres retrouvent leurs valeurs par défaut d'usine. Toutefois, le NSIP et la passerelle par défaut ne sont pas modifiés, car leur modification peut entraîner la perte de connectivité réseau de la solution matérielle-logicielle.

À l'invite de commandes, tapez :

```
clear ns config -force
```

Exemple : Pour effacer de manière forcée les configurations de base d'une solution matérielle-logicielle.

```
clear ns config -force basic
```

Effacer la configuration Citrix ADC à l'aide de l'interface graphique

Accédez à **Système** > **Diagnostics** et, dans le groupe Maintenance, cliquez sur **Effacer la configuration** et sélectionnez le niveau de configuration à effacer de la solution matérielle-logicielle.

Procédure de redémarrage ou d'arrêt de l'appliance pour les configurations Citrix ADC non enregistrées

L'appliance Citrix ADC peut être redémarrée ou arrêtée à distance à partir des interfaces utilisateur disponibles. Lorsque vous redémarrez ou arrêtez une appliance Citrix ADC autonome, les configurations non enregistrées (configurations effectuées depuis l'émission de la dernière commande save ns config) sont perdues.

Dans une configuration haute disponibilité, lorsque l'appliance principale est redémarrée ou arrêtée, la solution matérielle-logicielle secondaire prend le relais et devient la solution principale. Les configurations non enregistrées de l'ancien serveur principal sont disponibles sur le nouveau dispositif principal.

Vous pouvez également redémarrer l'appliance en redémarrant uniquement le logiciel Citrix ADC et non en redémarrant le système d'exploitation sous-jacent. C'est ce qu'on appelle un redémarrage à chaud. Par exemple, lorsque vous ajoutez une nouvelle licence ou que vous modifiez l'adresse IP, vous pouvez redémarrer à chaud l'appliance Citrix ADC pour que ces modifications aient lieu.

> **Remarque :**
>
> Vous pouvez effectuer un redémarrage à chaud uniquement sur une appliance Citrix ADC autonome.

Redémarrez l'appliance à l'aide de l'interface de commande

À l'invite de commandes, tapez :

```
reboot [-warm]
```

Redémarrez une appliance Citrix ADC à l'aide de l'interface graphique

1. Dans la page de configuration, cliquez sur **Redémarrer**.
2. Lorsque vous êtes invité à redémarrer, sélectionnez **Enregistrer la configuration** pour vous assurer que vous ne perdez aucune configuration.

> **Remarque :**
>
> Vous pouvez effectuer un redémarrage à chaud en sélectionnant Redémarrage à chaud.

Arrêtez une solution matérielle-logicielle à l'aide de l'interface de commande

À l'invite de commandes, tapez :

- `shutdown -p now`**:** Arrêt du logiciel et désactive le Citrix ADC. Pour redémarrer Citrix ADC MPX, appuyez sur l'interrupteur d'alimentation CA. Pour redémarrer Citrix ADC VPX, redémarrez l'instance VPX.
- `shutdown -h now`**:** Arrêt du logiciel et laisse le Citrix ADC allumé. Appuyez sur n'importe quelle touche pour redémarrer Citrix ADC. Cette commande ne désactive pas Citrix ADC. Par conséquent, ne mettez pas l'alimentation secteur hors tension et ne retirez pas les câbles d'alimentation CA.

> **Remarque :**
>
> Vous ne pouvez pas arrêter une appliance via l'interface graphique Citrix ADC.

Comment synchroniser l'horloge système avec les serveurs du réseau

Vous pouvez configurer votre appliance Citrix ADC pour synchroniser son horloge locale avec un serveur NTP (Network Time Protocol). Cela garantit que son horloge dispose des mêmes paramètres de date et d'heure que les autres serveurs de votre réseau.

Vous pouvez configurer la synchronisation de l'horloge sur votre solution matérielle-logicielle en ajoutant des entrées de serveur NTP au fichier ntp.conf à partir de l'interface graphique ou

de l'interface de ligne de commande, ou en modifiant manuellement le fichier ntp.conf, puis en démarrant le démon NTP (NTDP). La configuration de la synchronisation de l'horloge ne change pas si la solution matérielle-logicielle est redémarrée, mise à niveau ou rétrogradée. Toutefois, la configuration n'est pas propagée au Citrix ADC secondaire dans une configuration haute disponibilité.

L'interface graphique Citrix ADC vous permet de configurer le fuseau horaire et l'adresse IP du serveur NTP requis pour la synchronisation de l'horloge sur l'écran du premier utilisateur (FTU).

> **Remarque :**
>
> Si vous n'avez pas de serveur NTP local, vous pouvez trouver une liste des serveurs NTP publics en libre accès sur le site NTP officiel <http://www.ntp.org>, sous Liste des serveurs de temps publics. Avant de configurer votre Citrix ADC pour utiliser un serveur NTP public, assurez-vous de lire la page Règles d'engagement (lien inclus dans toutes les pages des serveurs de temps publics).
>
> Dans Citrix ADC version 11, la version NTP a été mise à jour de 4.2.6p3 à 4.2.8p2.

Prérequis

Pour configurer la synchronisation de l'horloge, vous devez configurer les entités suivantes :

1. Serveurs NTP
2. Synchronisation NTP.

Ajouter un serveur NTP à l'aide de l'interface de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un serveur NTP et vérifier la configuration :

- `add ntp server (<serverIP> | <serverName>)[-minpoll <positive_integer>] [-maxpoll <positive_integer>]`
- `show ntp server`

Exemple :

```
add ntp server 10.102.29.30 -minpoll 6 -maxpoll 11
```

Ajouter un serveur NTP à l'aide de l'interface graphique

Accédez à **Système** > **Serveurs NTP**, puis créez le serveur NTP.

Activer la synchronisation NTP à l'aide de l'interface de commande

Lorsque vous activez la synchronisation NTP, Citrix ADC démarre le démon NTP et utilise les entrées du serveur NTP dans le fichier ntp.conf pour synchroniser son paramètre d'heure locale. Si vous ne

souhaitez pas synchroniser l'heure de l'appliance avec les autres serveurs du réseau, vous pouvez désactiver la synchronisation NTP, ce qui arrête le démon NTP (NTDP).

À l'invite de commandes, tapez l'une des commandes suivantes :

```
enable ntp sync
```

Activer la synchronisation NTP à l'aide de l'interface graphique

Accédez à **Système** > **Serveurs NTP**, cliquez sur **Action** et sélectionnez **Synchronisation NTP**.

Configurer la synchronisation de l'horloge pour modifier un fichier ntp.conf à l'aide de l'interface graphique

1. Ouvrez une session sur l'interface de ligne de commande.
2. Passez à l'invite du shell.
3. Copiez le `/etc/ntp.conf` fichier dans `/nsconfig/ntp.conf`, à moins qu'il ne contienne `/nsconfig directory` déjà un `ntp.conf` fichier.
4. Pour chaque serveur NTP que vous souhaitez ajouter, vous devez ajouter les deux lignes suivantes au fichier `/nsconfig/ntp.conf`:

```
server <IP address for NTP server> iburst
```

```
restrict <IP address for NTP server> mask <netmask> nomodify notrap nopeer
noquery
```

```
> Note:
>
> For security reasons, there should be a corresponding restrict entry
   for each server entry.

Example

In the following example, an administrator has inserted # characters to
     “comment out”  an existing NTP entry, and then added an entry:

`#server 1.2.3.4 iburst`

`#restrict 1.2.3.4 mask 55.255.255.255 nomodify notrap nopeer noquery`

`server 10.102.29.160 iburst`

`restrict 10.102.29.160 mask 255.255.255.255 nomodify notrap nopeer
   noquery`
```


1. Si le répertoire /nsconfig ne contient pas de fichier nommé rc.netscaler, créez le fichier.
2. Ajoutez l'entrée suivante à /nsconfig/rc.netscaler: /bin/sh /etc/ntpd_ctl full_start

   Cette entrée démarre le ntpd service, vérifie le fichier ntp.conf et consigne les messages dans le répertoire /var/log.

   Ce processus s'exécute chaque fois que Citrix ADC est redémarré.
3. Redémarrez l'appliance Citrix ADC pour activer la synchronisation de l'horloge. Ou, pour démarrer le processus de synchronisation de l'heure sans redémarrer la solution matérielle-logicielle, entrez les commandes suivantes à l'invite de l'interpréteur de commandes :

- rm /etc/ntp.conf
- ln -s /nsconfig/ntp.conf /etc/ntp.conf
- /bin/sh /etc/ntpd_ctl full_start

Comment configurer le délai d'expiration de session pour les connexions client inactives

Un intervalle d'expiration de session est fourni pour limiter la durée pendant laquelle une session (interface graphique, CLI ou API) reste active lorsqu'elle n'est pas utilisée. Pour Citrix ADC, le délai d'expiration de la session système peut être configuré aux niveaux suivants :

- **Délai d'expiration au niveau utilisateur.** Applicable à l'utilisateur spécifique.

Type d'interface	Configuration du délai d'exécution
GUI	Accédez à **Système > Administration des utilisateurs > Utilisateurs**, sélectionnez un utilisateur et modifiez le paramètre de délai d'expiration de l'utilisateur.
LIGNE DE COMMANDE	À l'invite de commandes, entrez la commande suivante : set system user <name> -timeout <secs>|

- **Délai d'expiration de niveau groupe d'utilisateurs.** Applicable à tous les utilisateurs du groupe.

Type d'interface	Configuration du délai d'exécution
GUI	Accédez à **Système > Administration des utilisateurs > Groupes**, sélectionnez un groupe et modifiez le paramètre de délai d'expiration du groupe.
LIGNE DE COMMANDE	À l'invite de commandes, entrez la commande suivante :`set system group <groupName> -timeout <secs>`

- **Délai d'expiration du système global.** Applicable à tous les utilisateurs et utilisateurs des groupes qui n'ont pas de délai d'expiration configuré.

Type d'interface	Configuration du délai d'exécution
GUI	Accédez à **Système > Paramètres**, cliquez sur Modifier les paramètres système globaux et mettez à jour la valeur du délai d'expiration si nécessaire.
LIGNE DE COMMANDE	À l'invite de commandes, entrez la commande suivante : `set system parameter -timeout <secs>`

```
The timeout value specified for a user has the highest priority. If timeout is not configured for the user, the timeout configured for a member group is considered. If timeout is not specified for a group (or the user does not belong to a group), the globally configured timeout value is considered. If timeout is not configured at any level, the default value of 900 seconds is set as the system session timeout.

Additionally, you can specify timeout durations for each of the interfaces you are accessing. However, the timeout value specified for a specific interface is restricted to the timeout value configured for the user that is accessing the interface. For example, let us consider an user "publicadmin" who has a timeout value of 20 minutes. Now, when accessing an interface, the user must specify a timeout value that is within 20 minutes.

> **Note:**
```



```
6 >
7 > You can choose to keep a check on the minimum and maximum timeout
    values by specifying the timeout as restricted (in CLI by specifying
     the *restrictedTimeout* parameter). This parameter is provided to
    account for previous Citrix ADC versions where the timeout value was
     not restricted.
```

- Lorsque cette option est activée, la valeur minimale du délai d'attente configurable est de 5 minutes (300 secondes) et la valeur maximale est de 1 jour (86400 secondes). Si la valeur du délai d'expiration est déjà configurée sur une valeur supérieure à 1 jour, lorsque ce paramètre est activé, vous êtes invité à le modifier. Si vous ne modifiez pas la valeur, la valeur du délai d'expiration sera automatiquement reconfigurée sur la durée d'expiration par défaut de 15 minutes (900 secondes) au prochain redémarrage. La même chose se produira si la valeur du délai d'expiration configurée est inférieure à 5 minutes.
- Lorsque cette option est désactivée, les durées d'expiration configurées sont prises en compte.
- **Durée du délai d'attente à chaque interface :**

Type d'interface	Configuration du délai d'exécution
LIGNE DE COMMANDE	Spécifiez la valeur du délai d'expiration sur l'invite de commande à l'aide de la commande suivante : `set cli mode -timeout <secs>`
API	Spécifiez la valeur du délai d'expiration dans la charge utile de connexion.

Comment définir la date et l'heure système pour synchroniser l'horloge avec un serveur de temps

Pour modifier la date et l'heure du système, vous devez utiliser l'interface shell du système d'exploitation FreeBSD sous-jacent. Toutefois, pour afficher la date et l'heure du système, vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique.

Afficher la date et l'heure du système à l'aide de l'interface de commande

À l'invite de commandes, tapez :

```
show ns config
```


Afficher la date et l'heure du système à l'aide de l'interface graphique

Accédez à **Système** et sélectionnez l'onglet **Informations système** pour afficher la date système.

Comment configurer les ports de gestion HTTP et HTTPS pour les services internes

Dans un déploiement en mode IP unique d'un dispositif Citrix ADC, une adresse IP unique est utilisée comme adresses NSIP, SNIP et VIP. Cette adresse IP unique utilise différents numéros de port pour fonctionner en tant qu'adresses NSIP, SNIP et VIP.

Les ports 80 et 443 sont des ports bien connus pour les services HTTP et HTTPS. Auparavant, les ports 80 et 443 de l'adresse IP Citrix ADC (NSIP) étaient des ports dédiés aux services de gestion HTTP et HTTPS internes. Ces ports étant réservés aux services internes, vous ne pouvez pas utiliser ces ports connus pour fournir des services de données HTTP et HTTPS à partir d'une adresse VIP, qui a la même adresse que l'adresse NSIP dans un déploiement en mode IP unique.

Pour répondre à cette exigence, vous pouvez désormais configurer des ports pour les services de gestion HTTP et HTTPS internes (de l'adresse NSIP) autres que les ports 80 et 443.

La liste suivante répertorie les numéros de port par défaut des services de gestion HTTP et HTTPS internes dans les appliances Citrix ADC MPX, VPX et CPX :

- Appliances Citrix ADC MPX et VPX : 80 (HTTP) et 443 (HTTPS)
- Appliances Citrix ADC CPX : 9080 (HTTP) et 9443 (HTTPS)

Configurez les ports de gestion HTTP et HTTPS à l'aide de l'interface de commande

Vous pouvez configurer un port HTTP et un port HTTPS sur n'importe quelle valeur de l'appliance Citrix ADC pour prendre en charge le service de gestion HTTP et HTTPS. Toutefois, par défaut, l'appliance Citrix ADC utilise 80 et 443 ports pour la connexion HTTP et HTTPS.

À l'invite de commandes, tapez :

```
set ns param -mgmtHttpPort<port>
```

Exemple :

```
set ns param -mgmtHttpPort 2000
```

Pour configurer un port HTTPS à l'aide de l'interface de commande

À l'invite de commandes, tapez :

```
set ns param -mgmtHttpsPort<port>
```

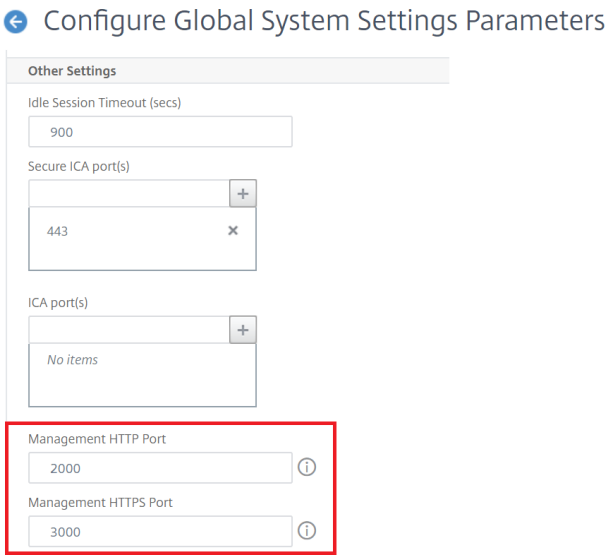
Exemple :

```
set ns param -mgmtHttpsPort 3000
```


Configurez les ports de gestion HTTP et HTTPS à l'aide de l'interface graphique

Suivez les étapes ci-dessous pour configurer les valeurs des ports HTTP et HTTPS :

1. Accédez à **Système** > **Paramètres** > **Modifier les paramètres globaux du système**.
2. Dans la page **Configurer les paramètres globaux du système**, sous la section **Autres** paramètres, définissez les paramètres suivants.
   a) Port HTTP de gestion. Définissez la valeur du port sur 2000. Par défaut = 80, Min = 1, Max = 65534.
   b) Port HTTPS de gestion. Définissez la valeur du port sur 3000. Par défaut = 443, Min = 1, Max = 65534.



Comment allouer un processeur de gestion supplémentaire pour le traitement et la surveillance des données

Si vous avez besoin de meilleures performances pour la configuration et la surveillance d'une appliance Citrix ADC MPX, vous pouvez allouer un processeur de gestion supplémentaire à partir du pool de moteurs de paquets de l'appliance. Cette fonctionnalité est prise en charge sur certains modèles Citrix ADC MPX et sur tous les modèles VPX, à l'exception des instances VPX qui s'exécutent sur des appliances Citrix ADC SDX. Il affecte la sortie de la CPU du système stat et des commandes du système stat.

Modèles Citrix ADC MPX pris en charge :

- 25xxx
- 22xxx
- 14xxx
- 115xx

- 15xxx
- 26xxx

> **Remarque :**
>
> Pour les modèles Citrix ADC MPX 26xxx avec plus de 20 cœurs, la fonctionnalité de processeur de gestion supplémentaire obligatoire est activée par défaut. Pour les modèles Citrix ADC VPX, une licence prenant en charge au moins 12 processeurs virtuels est nécessaire pour activer cette fonctionnalité.

Allouez un processeur de gestion supplémentaire à l'aide de l'interface de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `enable extramgmtcpu`
- `disable extramgmtcpu`

> **Remarque :**
>
> Une fois que vous avez activé et désactivé cette fonctionnalité, l'appliance Citrix ADC affiche un avertissement pour redémarrer l'appliance afin que les modifications prennent effet.

Pour afficher l'état configuré et effectif d'un processeur de gestion supplémentaire.

À l'invite de commandes, tapez :

```
1 `show extramgmtcpu`
```

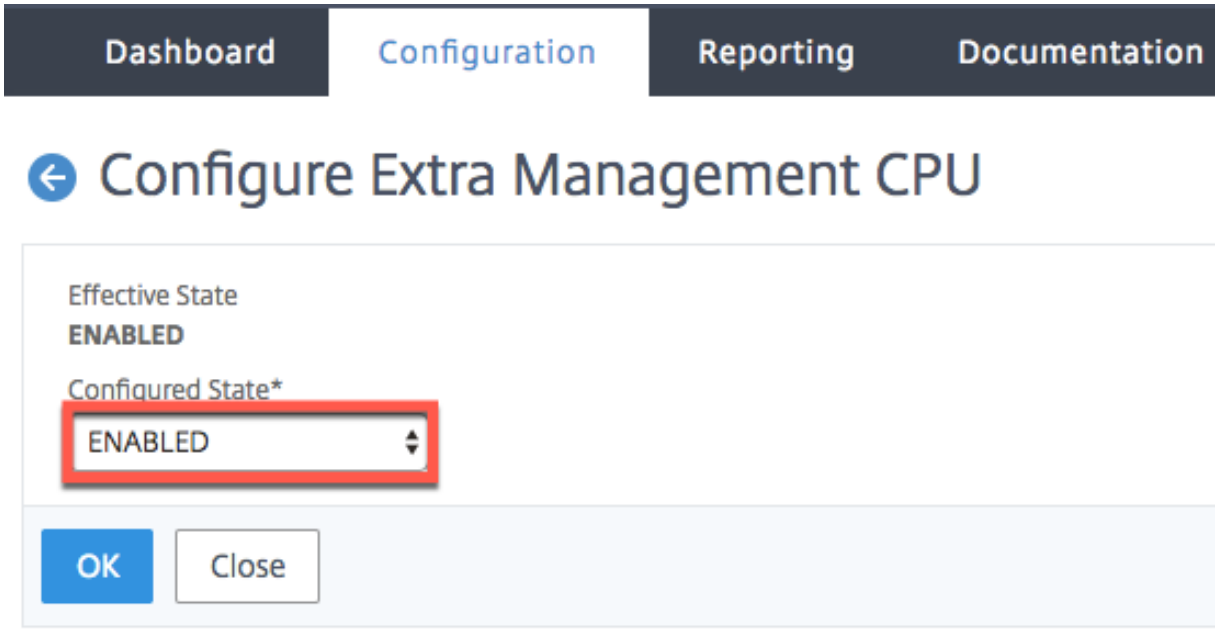
Exemple :

```
> show extramgmtcpu ConfiguredState: ENABLED EffectiveState: ENABLED
```

> **Remarque :**
>
> Dans cet exemple, la commande show est entrée avant le redémarrage de la solution matérielle-logicielle.

Allouez un processeur de gestion supplémentaire à l'aide de l'interface graphique

Pour allouer un processeur de gestion supplémentaire à l'aide de l'interface graphique, accédez à **Système** > **Paramètres** et cliquez sur **Configurer le processeur de gestion supplémentaire**. Dans le menu déroulant **État configuré**, sélectionnez **Activé**, puis **OK**.



Pour vérifier l'utilisation du processeur, accédez à **Système** > **Paramètres** > **Tableau de bord**.

Configurez un processeur de gestion supplémentaire à l'aide de l'API NITRO

Utilisez les méthodes et formats NITRO suivants pour activer, désactiver et afficher un processeur de gestion supplémentaire.

Pour activer un processeur de gestion supplémentaire, procédez comme suit :

```
HTTP Method: POST
```

```
URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu?action=enable
```

```
Payload: { "systemextramgmtcpu":{ } }
```

```
curl -v -X POST -H "Content-Type: application/json"-u nsroot:nsroot http://10.102.201.92/nitro/v1/config/systemextramgmtcpu?action=enable -d '{ "systemextramgmtcpu":{ } } '
```

Pour désactiver un processeur de gestion supplémentaire

```
HTTP Method: POST
```

```
URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu?action=disable
```

```
Payload: { "systemextramgmtcpu":{ } }
```

```
curl -v -X POST -H "Content-Type: application/json"-u nsroot:nsroot http://10.102.201.92/nitro/v1/config/systemextramgmtcpu?action=disable -d '{ "systemextramgmtcpu":{ } } '
```

Pour afficher un processeur de gestion supplémentaire


```
HTTP Method: GET

URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu
```

Exemple :

```
curl -v -X GET -H "Content-Type: application/json"-u nsroot:nsroot http://
10.102.201.92/nitro/v1/config/systemextramgmtcpu
```

Statistiques et surveillance avant et après l'ajout d'un processeur de gestion supplémentaire

Les exemples suivants montrent les différences entre la sortie des commandes CPU et stat system avant et après l'ajout d'un processeur de gestion supplémentaire.

```
stat system cpu
```

Cette commande affiche les statistiques des processeurs.

Voici un exemple de sortie avant d'ajouter un processeur de gestion supplémentaire sur l'un des modèles pris en charge.

Exemple

```
1  ```
2  > stat system cpu
3
4  CPU statistics
5
6  ID          Usage
7
8  8               1
9
10 7               1
11
12 11              2
13
14 1               1
15
16 6               1
17
18 9               1
19
20 3               1
21
22 5               1
23
24 4               1
25
```



```
10              1

2               1
<!--NeedCopy--> ```
```

Voici la sortie après l'ajout d'un processeur de gestion supplémentaire sur le même appareil MPX.

```
```
> stat system cpu

CPU statistics

ID   Usage

9   1

7   1

5   1

8   1

11   2

10   1

6   1

4   1

3   1

2   1
<!--NeedCopy--> ```
```

`stat system`

Cette commande affiche l'utilisation du processeur. Dans l'exemple suivant, la sortie avant l'ajout d'un processeur de gestion supplémentaire sur l'un des modèles pris en charge est la suivante :

Gestion de l'utilisation supplémentaire du processeur ( %) 0.00

Exemple

```
```
> stat system
```



```
3
4  Citrix ADC Executive View
5
6  System Information:
7
8  Up since        Wed Oct 11 11:17:54 2017
9
10 /flash Used (%)                          0
11
12 Packet CPU usage (%)                  1.30
13
14 Management CPU usage (%)              4.00
15
16 Mgmt CPU0 usage (%)                   4.00
17
18 Mgmt Additional-CPU  usage (%)        0.00
19
20 Memory usage (MB)                     2167
21
22 InUse Memory (%)                      5.76
23
24 /var Used (%)                            0
25 <!--NeedCopy--> ```
```

Dans l'exemple suivant, la sortie après l'ajout d'un processeur de gestion supplémentaire sur la même appliance MPX est :

Gestion de l'utilisation supplémentaire du processeur (%) 0,80

```
1  ```     > stat system
2
3  Citrix ADC Executive View
4
5  System Information:
6
7  Up since        Wed Oct 11 11:55:56 2017
8
9  /flash Used (%)                          0
10
11 Packet CPU usage (%)                  1.20
12
13 Management CPU usage (%)              5.70
14
15 Mgmt CPU0 usage (%)                  10.60
16
```



```
17 Mgmt Additional-CPU  usage (%)      0.80
18
19 Memory usage (MB)                   1970
20
21 InUse Memory (%)                    5.75
22
23 /var Used (%)                          0
24
25 <!--NeedCopy--> ```
```

Comment faire pour sauvegarder et restaurer votre appliance pour récupérer la configuration perdue

Lorsque votre solution matérielle-logicielle est corrompue ou nécessite une mise à niveau, vous pouvez sauvegarder la configuration de votre système. La procédure de sauvegarde s'effectue via l'interface de ligne de commande Citrix ou l'interface graphique. La solution matérielle-logicielle vous permet également d'importer le fichier de sauvegarde à partir d'une source externe. Toutefois, vous ne pouvez le faire que via l'interface graphique et il n'y a pas de prise en charge via l'interface CLI.

Points à retenir

Vous devez vous souvenir des points suivants lorsque vous sauvegardez et restaurez votre solution matérielle-logicielle.

- La configuration réseau doit être prise en charge sur une nouvelle plate-forme.
- La nouvelle version de la plate-forme doit être identique au fichier de sauvegarde ou à une version ultérieure.

Sauvegarder une appliance Citrix ADC

Selon les besoins en matière de données et de sauvegarde, vous pouvez créer une sauvegarde « de base » ou une sauvegarde « complète ».

- **Sauvegarde de base.** Vous pouvez effectuer ce type de sauvegarde si vous souhaitez sauvegarder des fichiers qui changent constamment. Les fichiers que vous pouvez sauvegarder se trouvent dans le tableau suivant.

Pour plus d'informations sur les détails de base de la sauvegarde, reportez-vous à la rubrique Tableau
.

- **Sauvegarde complète.** En plus des fichiers sauvegardés par une sauvegarde de base, une sauvegarde complète contient moins de fichiers mis à jour. Les fichiers qui sont sauvegardés lorsque vous utilisez l'option de sauvegarde « complète » sont les suivants :

Répertoire	Sous-répertoire ou fichiers
nsconfig	ssl*, licence*, fips*
/var/	netscaler/ssl/*, wi/java_home/jre/lib/security/cacerts/*, wi/java_home/lib/security/cacerts/*

Les données sauvegardées sont stockées sous forme de fichier TAR compressé dans le `/var/ns_sys_backup/` répertoire. Pour éviter les problèmes dus à l'indisponibilité de l'espace disque, vous pouvez stocker jusqu'à 50 fichiers de sauvegarde dans ce répertoire. Vous pouvez utiliser la `rm system backup` commande pour supprimer les fichiers de sauvegarde existants et créer d'autres sauvegardes.

> **Remarque :**
>
> Lorsque l'opération de sauvegarde est en cours, n'exécutez pas de commandes qui affectent la configuration.
>
> Si un fichier qui doit être sauvegardé n'est pas disponible, l'opération ignore ce fichier.

Sauvegarder une appliance Citrix ADC à l'aide de l'interface de commande

Suivez la procédure ci-dessous pour sauvegarder un dispositif Citrix ADC à l'aide de l'interface de commande Citrix ADC.

À l'invite de commandes, procédez comme suit :

1. Enregistrez les configurations Citrix ADC.

```
save ns config
```

1. Créez le fichier de sauvegarde.

```
create system backup [<fileName>] -level <basic ¦ full> -comment <string>
```

> **Remarque :**
>
> Si le nom de fichier n'est pas spécifié, la solution matérielle-logicielle crée un fichier TAR avec la convention de dénomination suivante :`backup_<level>_<nsip_address>_<date-timestamp>.tgz`.

Exemple : Pour sauvegarder la solution matérielle-logicielle complète à l'aide de la convention de dénomination par défaut pour le fichier de sauvegarde.

```
> create system backup -level full
```

1. Vérifiez que le fichier de sauvegarde a été créé.

```
show system backup
```

Vous pouvez afficher les propriétés d'un fichier de sauvegarde spécifique à l'aide du paramètre `fileName`.

Restaurer un dispositif Citrix ADC à l'aide de l'interface de commande

> **Important :**
>
> Vous ne pouvez pas restaurer votre solution matérielle-logicielle si vous renommez ou modifiez votre fichier de sauvegarde.

Lorsque vous restaurez votre solution matérielle-logicielle, l'opération de restauration dézippe le fichier de sauvegarde du répertoire `/var/ns_sys_backup/`. Une fois que les fichiers ne sont pas enregistrés, ils sont copiés dans les répertoires respectifs.

Restaurer Citrix ADC à partir d'un fichier de sauvegarde local à l'aide de l'interface de commande

> **Remarque :**
>
> Citrix vous recommande de sauvegarder la configuration actuelle avant de restaurer une configuration précédente. Toutefois, si vous ne souhaitez pas que la commande de restauration crée automatiquement une sauvegarde de la configuration actuelle, utilisez le `-skipBackup` paramètre.

À l'invite de commandes, procédez comme suit :

1. Obtenez la liste des fichiers de sauvegarde disponibles sur la solution matérielle-logicielle.

   ```
   show system backup
   ```

2. Restaurez la solution matérielle-logicielle en spécifiant l'un des fichiers de sauvegarde.

   ```
   restore system backup <filename> [-skipBackup]
   ```

   Exemple : Pour effectuer une restauration à l'aide d'une sauvegarde complète d'une solution matérielle-logicielle

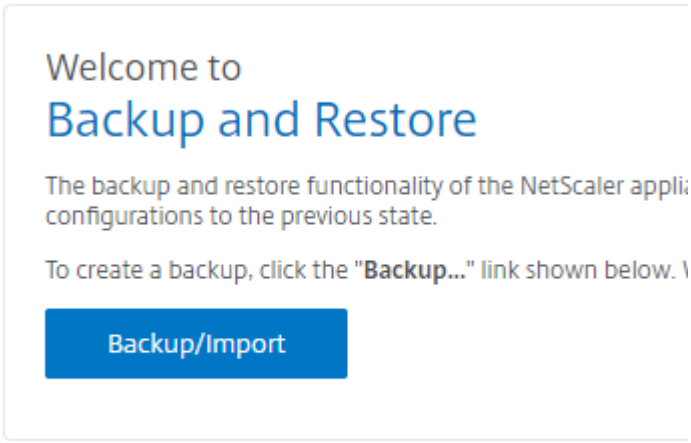
   ```
   > restore system backup backup_full_<nsip_address>_<date-timestamp>.tgz
   ```

3. Redémarrez l'appliance.

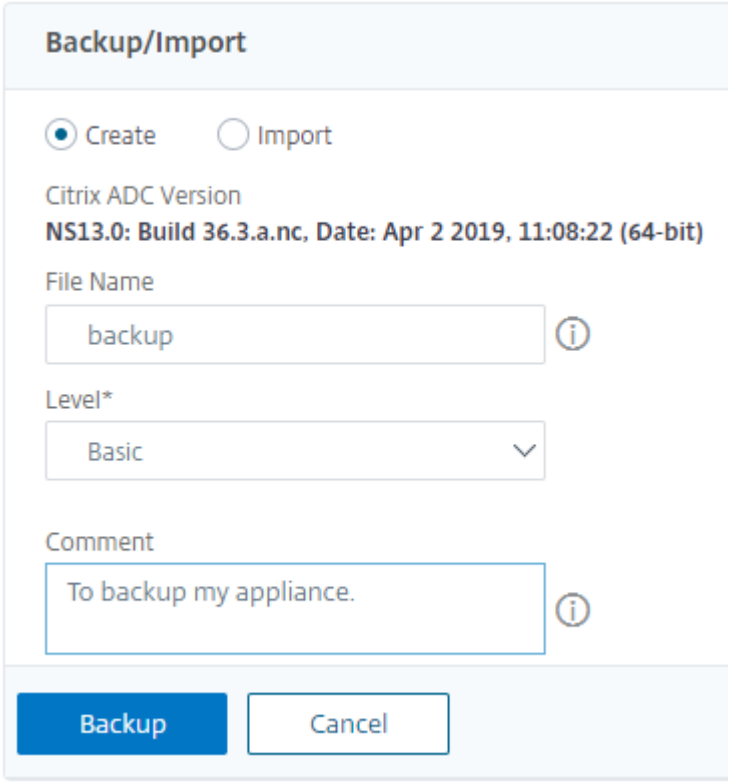
   ```
   reboot
   ```


Sauvegarde et restauration d'une appliance Citrix ADC à l'aide de l'interface graphique

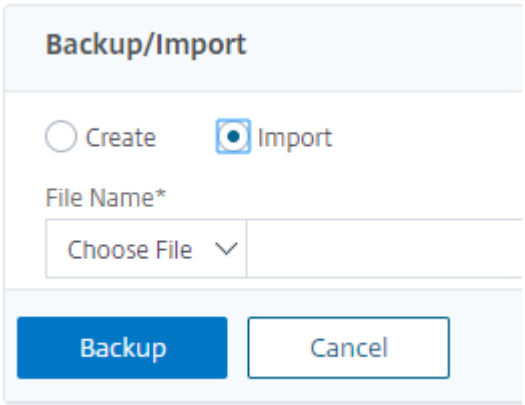
1. Accédez à **Système** > **Sauvegarde et restauration**.



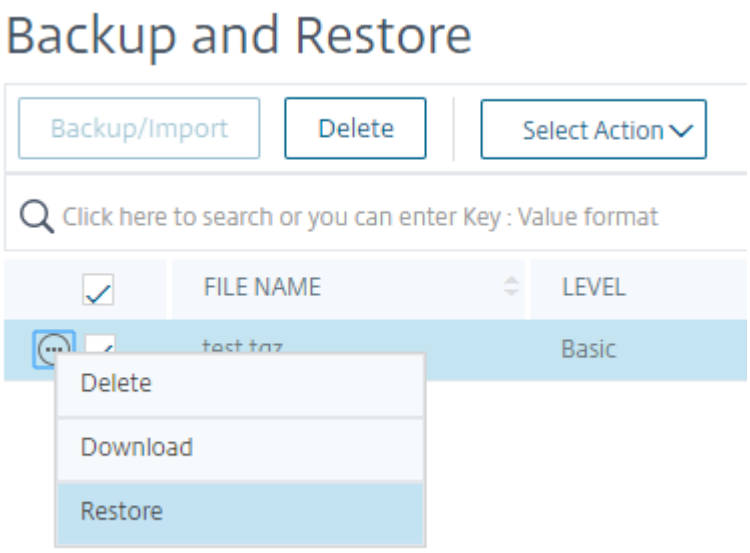
2. Cliquez sur **Sauvegarde/Importer** pour démarrer le processus.
3. Dans la page **Sauvegarde/Importation**, sélectionnez **Créer** et définissez les paramètres suivants.
   a) Nom du fichier. Nom du fichier de sauvegarde de la solution matérielle-logicielle.
   b) Niveau. Sélectionnez un niveau de sauvegarde de base ou complet.
   c) Comment. Fournissez une brève description de la sauvegarde.
4. Cliquez sur **Sauvegarde**.



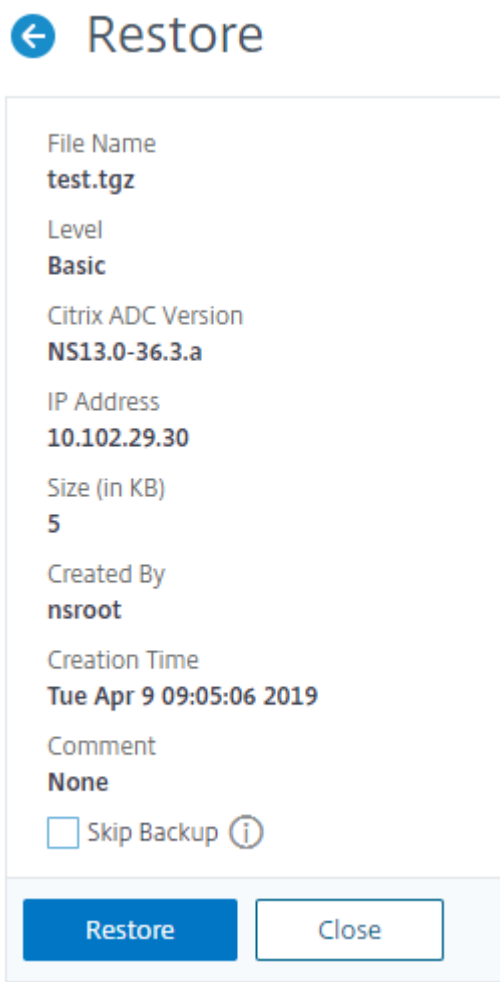
5. Si vous souhaitez importer une sauvegarde, vous devez sélectionner **Importer**.



6. Une fois la sauvegarde terminée, vous pouvez sélectionner le fichier et cliquer sur **Télécharger**.
7. Pour restaurer, sélectionnez le fichier de sauvegarde et cliquez sur **Restaurer**.



8. Dans la page **Restaurer**, vérifiez les détails du fichier de sauvegarde et cliquez sur **Restaurer**.



9. Après la restauration, vous devez redémarrer l'appliance.

Pour plus d'informations sur la sauvegarde et la restauration des instances Citrix ADC, consultez la rubrique Sauvegarde et restauration à l'aide de Citrix ADM .

Pour plus d'informations sur la sauvegarde et la restauration d'une appliance SDX, voir Sauvegarde et restauration de l'appliance SDX

Pour plus d'informations sur les opérations effectuées sur la sauvegarde système, reportez-vous à la rubrique Sauvegarde système .

Comment générer un ensemble de support technique pour résoudre les problèmes liés à l'appliance

Pour obtenir de l'aide sur l'analyse et la résolution des problèmes liés à une appliance Citrix ADC, vous pouvez générer un lot de support technique sur l'appliance et l'envoyer au support technique Citrix. Le pack de support technique Citrix ADC est une archive tar compressée de données et de statistiques de configuration du système. Il collecte les données suivantes à partir de l'appliance Citrix ADC sur laquelle vous générez le bundle :

- **Fichiers de configuration**. Tous les fichiers du répertoire /flash/nsconfig.
- **Fichiers Newnslog**. Le newnslog actuellement en cours d'exécution et certains fichiers précédents. Pour réduire la taille du fichier d'archive, la `newnslog` collection est limitée à 500 Mo, 6 fichiers ou 7 jours, selon la première éventualité. Si des données plus anciennes sont nécessaires, elles peuvent nécessiter une collecte manuelle.
- **Fichiers journaux**. Fichiers dans /var/log/messages*, /var/log/ns.log* et d'autres fichiers sous /var/log et /var/nslog.
- **Fichiers principaux de l'application**. Fichiers créés dans le répertoire /var/core au cours de la dernière semaine, le cas échéant.
- **Sortie de certaines commandes d'affichage de l'interface de ligne de commande**.
- **Sortie de certaines commandes de statistiques de l'interface de ligne de commande**.
- **Sortie des commandes du shell BSD**.

Vous pouvez utiliser une seule commande pour générer le bundle de support technique et le télécharger en toute sécurité sur le serveur de support technique Citrix. Pour effectuer le chargement, vous devez spécifier vos informations d'identification Citrix. Lorsque vous générez le bundle, vous pouvez spécifier le numéro de dossier ou de demande de service qui vous a été attribué par le support technique Citrix. Si vous avez déjà généré un bundle de support technique, vous pouvez télécharger le fichier d'archive existant sur le serveur de support technique Citrix en spécifiant le nom du fichier avec le chemin d'accès complet.

Le lot de support technique est enregistré sur l'appliance Citrix ADC dans une archive à l'emplacement suivant :


```
/var/tmp/support/support.tgz
```

Le chemin est un lien symbolique vers le collecteur le plus récent pour un accès facile. Le nom complet du fichier varie en fonction de la topologie de déploiement, mais il suit généralement un format similaire à :

```
collector_<P/S>_<NS IP>_<DateTime>.tgz.
```

Si votre appliance Citrix ADC ne dispose pas de connectivité Internet directe, vous pouvez utiliser un serveur proxy pour charger directement l'offre groupée de support technique sur le serveur de support technique Citrix. Le format de base de la chaîne de proxy est le suivant :

```
proxy_IP:<proxy_port>
```

Si le serveur proxy nécessite une authentification, le format est le suivant :

```
username:password@proxsy_IP:<proxy_port>
```

> **Remarque :**
>
> Pour les appliances Citrix ADC dans une paire haute disponibilité, vous devez générer le bundle de support technique sur chacun des deux nœuds.
>
> Pour les appliances Citrix ADC dans une configuration de cluster, vous pouvez générer le bundle de support technique sur chaque nœud individuellement, ou vous pouvez générer des archives abrégées plus petites pour tous les nœuds à l'aide de l'adresse IP du cluster.
>
> Pour les partitions d'administration Citrix ADC, vous devez générer le bundle de support technique à partir de la partition d'administration par défaut. Pour obtenir le bundle de support technique pour une partition spécifique, vous devez spécifier le nom de la partition pour laquelle vous souhaitez générer le bundle de support technique. Si vous ne spécifiez pas le nom de la partition, les données sont collectées à partir de toutes les partitions d'administration.

Générez le pack de support technique Citrix ADC à l'aide de l'interface de commande

À l'invite de commandes, tapez :

```
show techsupport [-scope <scope> <partitionName>] [-upload [-proxy <string
>] [-casenumber <string>] [-file <string>] [-description <string>] [-
userName <string> -password ]]
```


Sr. Non	Tâche	Commande
1	Générez et téléchargez le bundle de support technique sur le serveur de support technique Citrix.	show techsupport —upload —username account1 —password xxxxxxx
2	Générez et téléchargez le bundle de support technique sur le serveur de support technique Citrix via un serveur proxy	show techsupport –upload –proxy 1.1.1.1:80 –userName account1 –password xxxxxxx
3	Téléchargez un bundle de support technique existant sur le serveur de support technique Citrix.	show techsupport –upload -file,/var/tmp/support/collector_P_10.102.29. –userName account1 –password xxxxxxx
4	Générez de petites archives abrégées pour tous les nœuds d'une configuration de cluster. Exécutez cette commande à l'aide de l'adresse IP du cluster	show techsupport —scope CLUSTER
5	Générez un bundle de support technique spécifique à une partition d'administration. Exécutez cette commande sur la partition d'administration par défaut.	show techsupport –scope PARTITION partition1

Comment collecter le pack de support technique des appliances SDX et VPX pour une analyse des informations

Une appliance Citrix ADC dispose d'un mécanisme intégré pour collecter les fichiers journaux. Les fichiers journaux sont à leur tour envoyés à Citrix Insight Services pour analyse.

> **Remarque :**
>
> Toutes les procédures s'appliquent à la version logicielle 9.2 ou ultérieure.

Téléchargez le pack de support technique à partir des appliances Citrix ADC MPX et VPX

Pour exécuter un fichier collecteur à l'aide de l'interface graphique Citrix ADC, vous devez effectuer la procédure suivante :

> **Remarque :**
>
> La procédure s'applique à la version logicielle 9.2 ou ultérieure.

1. Accédez à **Système** > **Diagnostic**.
2. Dans la section **Outils de support technique**, cliquez sur le lien **Générer un fichier de support** .
3. Dans la page **Support technique**, définissez les paramètres suivants :
   a) Portée. Pour collecter des données à partir d'un ou de plusieurs nœuds.
   b) Cloison. Nom de la partition.
   c) Options de chargement du support technique Citrix. Définissez toutes les options telles que le serveur proxy, le numéro de dossier de service, le nom du fichier d'archive du collecteur et une brève description du fichier d'archive pour le téléchargement du pack de support technique.
   d) Compte Citrix. Entrez vos informations d'identification Citrix.
4. Cliquez sur **Exécuter**.
5. Le pack de support technique est généré.
6. Cliquez sur **Oui** pour télécharger le pack de support technique sur votre bureau local.

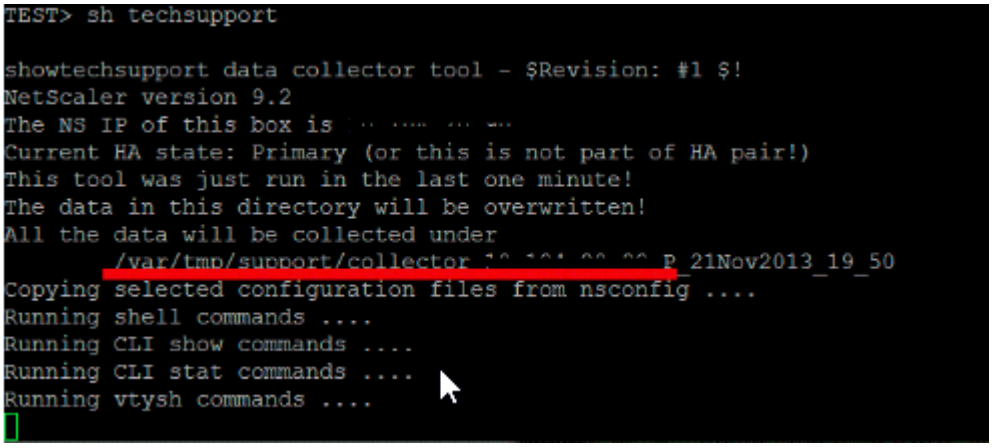
Obtenez le pack de support technique à l'aide de l'interface de commande

1. Téléchargez le fichier à partir de l'appliance à l'aide d'un utilitaire Secure FTP (SFTP) ou Secure Copy (SCP) `WinSCP`, par exemple, et téléchargez-le sur Citrix Insight Services pour analyse.

> **Remarque :**
>
> Dans la version logicielle Citrix ADC antérieure à 9.0, le script collecteur doit être téléchargé séparément et exécuté.

```
> show techsupport -scope CLUSTER
```

1. Cette opération collecte les informations de support technique de tous les nœuds du cluster et compresse les fichiers dans une seule archive.
2. Une fois que la solution matérielle-logicielle a généré l'archive du collecteur, l'emplacement du fichier s'affiche comme illustré dans la capture d'écran suivante.



Le fichier est stocké dans `/var/tmp/support` et vous pouvez le vérifier en vous connectant à un dispositif Citrix ADC et en exécutant la commande suivante à partir d'une invite de l'interpréteur de commandes.

```
root@NS## cd /var/tmp/support/
root@NS## ls -l
```

Obtenez le bundle de diagnostic de Citrix ADC SDX à l'aide de l'interface graphique

1. Ouvrez l'interface graphique Citrix SDX.
2. Développez le nœud **Diagnostics** .
3. Sélectionnez le nœud **Support technique** .
4. Cliquez sur Générer un fichier de support technique.
5. Sélectionnez **Appliance** (y compris les instances) dans le menu déroulant.
6. Cliquez sur **Ajouter**.
7. Sélectionnez une ou plusieurs instances à ajouter.
8. Cliquez sur **OK**. Attendez que le processus soit terminé.
9. Sélectionnez le nom du bundle qui a été généré, puis cliquez sur **Télécharger**
10. Téléchargez le fichier groupé sur Citrix Insight Services.

Plus de ressources

Regarder une vidéo

Lire un autre sujet

Doc de référence de commande

Authentification et autorisation des utilisateurs système

August 20, 2021

Pour configurer l'authentification et l'autorisation des utilisateurs Citrix ADC, vous devez d'abord définir les utilisateurs qui ont accès à l'appliance Citrix ADC, puis vous pouvez organiser ces utilisateurs en groupes. Après avoir configuré des utilisateurs et des groupes, vous devez configurer des stratégies de commande pour définir les types d'accès et affecter les stratégies à des utilisateurs et/ou des groupes.

Vous devez ouvrir une session en tant qu'administrateur pour configurer les utilisateurs, les groupes et les stratégies de commande. Le nom d'utilisateur administrateur Citrix ADC par défaut est *nsroot*. Après avoir ouvert une session en tant qu'administrateur par défaut, vous devez modifier le mot de passe du compte nsroot. Une fois que vous avez modifié le mot de passe, aucun utilisateur ne peut accéder à l'appliance Citrix ADC tant que vous n'avez pas créé un compte pour cet utilisateur. Si vous oubliez le mot de passe administrateur après l'avoir modifié par défaut, vous pouvez le réinitialiser à nsroot.

> **Remarque :**
>
> - Les utilisateurs locaux peuvent s'authentifier auprès du Citrix ADC même si des serveurs d'authentification externes sont configurés. Vous pouvez restreindre cela en désactivant le paramètre LocalAuth de la commande set system parameter.
> - Pour une sécurité accrue, Citrix vous recommande de modifier le mot de passe nsroot. Il est conseillé de changer fréquemment le mot de passe. Pour plus d'informations sur la modification du mot de passe nsroot, reportez-vous à la rubrique Réinitialisation du mot de passe administrateur par défaut (nsroot) .

Stratégies d'utilisateur, de groupes d'utilisateurs et de commandes

August 20, 2021

Vous devez d'abord définir un utilisateur avec un compte, puis organiser tous les utilisateurs en groupes. Vous pouvez créer des stratégies de commande ou utiliser des stratégies de commande

intégrées pour réglementer l'accès des utilisateurs aux commandes.

> **Remarque :**
>
> Si vous préférez en savoir plus sur la configuration d'utilisateurs et de groupes d'utilisateurs dans le cadre de la configuration d'authentification et d'autorisation Citrix ADC pour la gestion du trafic, consultez la rubrique Configurer les utilisateurs et les groupes .

Vous pouvez également personnaliser l'invite de ligne de commande pour un utilisateur. Les invites peuvent être définies dans la configuration d'un utilisateur, dans une configuration de groupe d'utilisateurs et dans les paramètres de configuration globale du système. L'invite affichée pour un utilisateur est dans l'ordre de priorité suivant :

1. Affichez l'invite telle que définie dans la configuration de l'utilisateur.
2. Affichez l'invite telle que définie dans la configuration du groupe pour le groupe de l'utilisateur.
3. Affichez l'invite comme défini dans les paramètres de configuration globale du système.

Vous pouvez désormais spécifier une valeur de délai d'expiration pour les sessions de CLI inactives pour un utilisateur système. Si la session CLI d'un utilisateur est inactive pendant une durée supérieure à la valeur de délai d'expiration, l'appliance Citrix ADC met fin à la connexion. Le délai d'expiration peut être défini dans une configuration utilisateur, dans une configuration de groupe d'utilisateurs ou dans les paramètres de configuration globale du système. Le délai d'expiration pour les sessions CLI inactives pour un utilisateur est déterminé dans l'ordre de priorité suivant :

1. Configuration utilisateur.
2. Configuration de groupe pour le groupe de l'utilisateur.
3. Paramètres de configuration globale du système.

Un administrateur racine Citrix ADC peut configurer la limite maximale de session simultanée pour les utilisateurs système. En limitant la limite, vous pouvez réduire le nombre de connexions ouvertes et améliorer les performances du serveur. Tant que le nombre de CLI est dans la limite configurée, les utilisateurs simultanés peuvent ouvrir une session sur l'interface graphique n'importe quel nombre de fois. Toutefois, si le nombre de sessions CLI atteint la limite configurée, les utilisateurs ne peuvent plus se connecter à l'interface graphique. Par exemple, si le nombre de sessions simultanées est configuré sur 20, les utilisateurs simultanés peuvent ouvrir une session à 19 sessions CLI. Mais si l'utilisateur est connecté à la session `20<sup>th</sup>` CLI, toute tentative de connexion à l'interface graphique, CLI ou NITRO entraîne un message d'erreur ((ERREUR : limite de connexion à CFE dépassée).

> **Remarque :**
>
> Par défaut, le nombre de sessions simultanées est configuré sur 20 et le nombre maximal de sessions simultanées est configuré sur 40.

Configurer les comptes utilisateur

Pour configurer les comptes d'utilisateurs, il vous suffit de spécifier des noms d'utilisateur et des mots de passe. Vous pouvez modifier les mots de passe et supprimer les comptes utilisateur à tout moment.

> **Remarque :**
>
> Tous les caractères d'un mot de passe ne sont pas acceptés. Cependant, cela fonctionne si vous tapez les caractères entre guillemets.
>
> En outre, la chaîne ne doit pas dépasser une longueur maximale de 127 caractères.

Pour créer un compte utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un compte d'utilisateur et vérifier la configuration :

- `add system user <username> [-externalAuth ( ENABLED | DISABLED )] [-promptString <string>] [-timeout \<secs>] [-logging ( ENABLED | DISABLED )] [-maxsession <positive_integer>]`
- `show system user <userName>`

Les utilisateurs externes peuvent configurer le paramètre « journalisation » pour collecter les journaux externes à l'aide de la journalisation Web ou du mécanisme de journalisation d'audit. Si le paramètre est activé, le client d'audit s'authentifie auprès de l'appliance Citrix ADC pour collecter les journaux.

Exemple :

```
> add system user johnd -promptString user-%u-at-%T
```

```
1 Enter password:
2 Confirm password:
3 > show system user johnd
4 user name: john
5      Timeout:900 Timeout Inherited From: Global
6      External Authentication: ENABLED
7      Logging: DISABLED
8      Maximum Client Sessions: 20
9 <!--NeedCopy-->
```

Pour la description des paramètres, reportez-vous à la rubrique Référence de la commande utilisateur Authentification et autorisation .

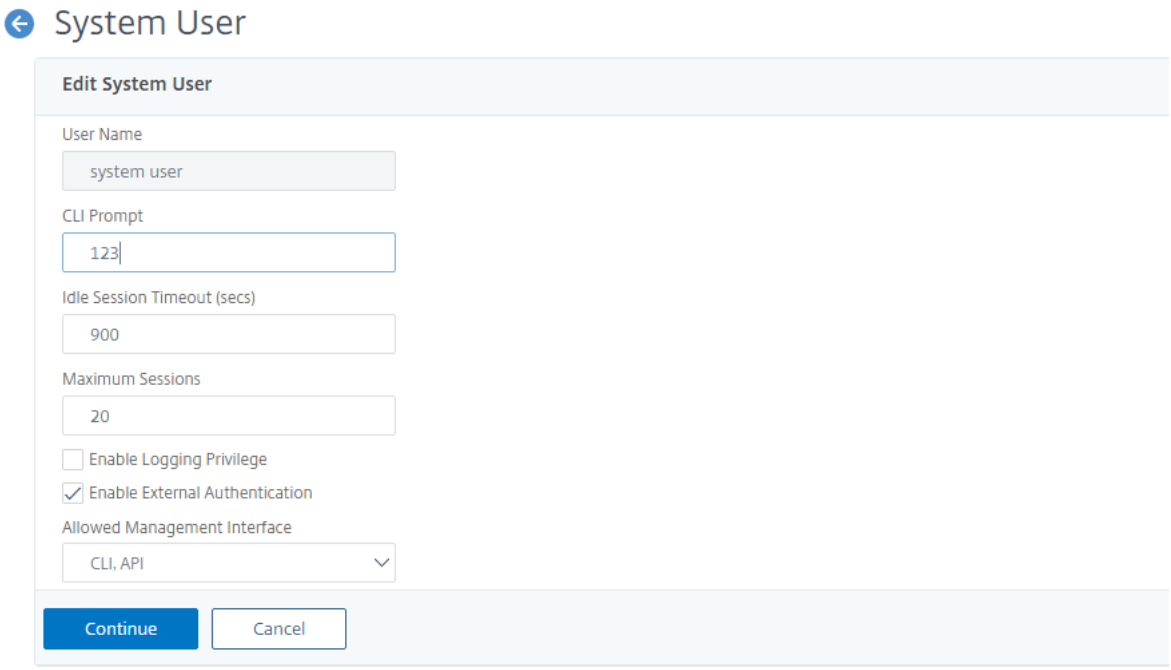
Configurer un compte d'utilisateur à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Système** > **Administration** des **utilisateurs > Utilisateurs**et créez l'utilisateur.
2. Dans le volet d'informations, cliquez sur **Ajouter** pour créer un utilisateur système.

3. Dans la page **Créer un groupe système**, définissez les paramètres suivants :

   a) Nom d'utilisateur. Nom du groupe d'utilisateurs.
   b) Invite CLI. Invite que vous préférez définir pour l'accès à l'interface CLI.
   c) Délai d'expiration de la session inactivité (secondes). Définissez la durée pendant laquelle un utilisateur peut être inactif avant l'épuisement et la fermeture de la session.
   d) Nombre maximal de sessions. Définissez le nombre maximal de sessions qu'un utilisateur peut essayer.
   e) Activer le privilège d'enregistrement. Activer le privilège de journalisation pour l'utilisateur.
   f) Activer l'authentification externe. Sélectionnez l'option si vous souhaitez utiliser le serveur d'authentification externe pour authentifier l'utilisateur.
   g) Interface de gestion autorisée. Sélectionnez les interfaces Citrix ADC auxquelles le groupe d'utilisateurs est autorisé à accéder.
   h) Stratégies de commande. Lier les stratégies de commande au groupe d'utilisateurs.
   i) Partitions. Liez les partitions au groupe d'utilisateurs.

4. Cliquez sur **Créer** et **Fermer**.



Configurer des groupes d'utilisateurs

Après avoir configuré un groupe d'utilisateurs, vous pouvez facilement accorder les mêmes droits d'accès à tous les membres du groupe. Pour configurer un groupe, créez le groupe et liez les utilisateurs au groupe. Vous pouvez lier chaque compte d'utilisateur à plusieurs groupes. La liaison

de comptes d'utilisateur à plusieurs groupes peut permettre une plus grande flexibilité lors de l'application de stratégies de commande.

Pour créer un groupe d'utilisateurs à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un groupe d'utilisateurs et vérifier la configuration :

- `add system group <groupName> [-promptString <string>] [-timeout <secs>]`
- `show system group <groupName>`

Exemple :

```
> add system group Managers -promptString Group-Managers-at-%h
```

Lier un compte d'utilisateur à un groupe à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier un compte d'utilisateur à un groupe et vérifier la configuration :

- `bind system group <groupName> -userName <userName>`
- `show system group <groupName>`

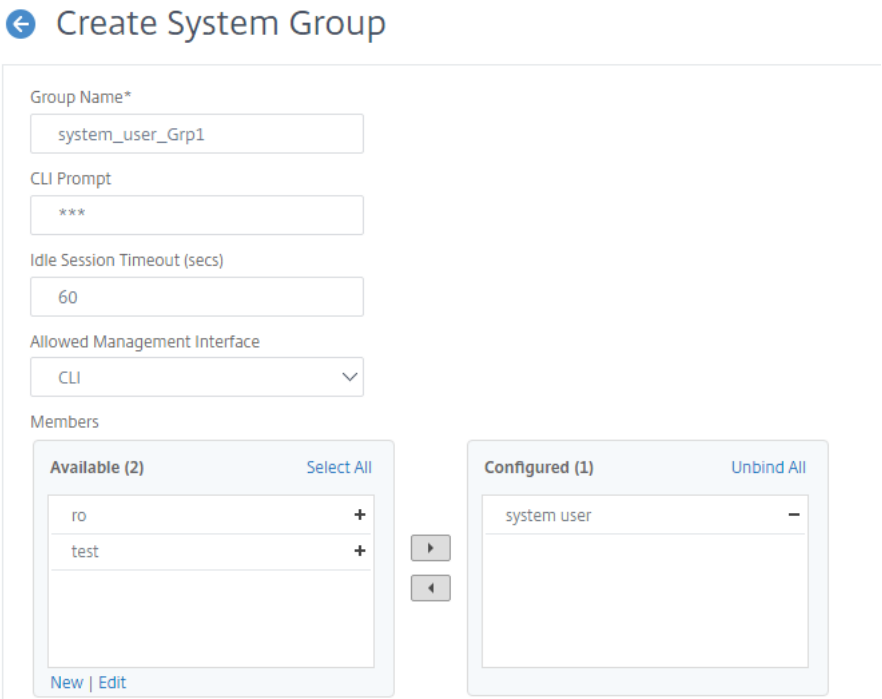
Exemple :

```
> bind system group Managers -userName user1
```

Configurer un groupe d'utilisateurs à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Système** > **Administration des utilisateurs** > **Groupes**et créez le groupe d'utilisateurs.
2. Dans le volet d'informations, cliquez sur **Ajouter** pour créer un groupe d'utilisateurs système.
3. Dans la page **Créer un groupe système**, définissez les paramètres suivants :
   a) Nom du groupe. Nom du groupe d'utilisateurs.
   b) Invite CLI. Invite que vous préférez définir pour l'accès à l'interface CLI.
   c) Délai d'expiration de la session inactivité (secondes). Définissez la durée pendant laquelle un utilisateur peut être inactif avant l'épuisement et la fermeture de la session.
   d) Interface de gestion autorisée. Sélectionnez les interfaces Citrix ADC auxquelles le groupe d'utilisateurs est autorisé à accéder.
   e) Membres. Ajoutez des comptes d'utilisateurs au groupe.
   f) Stratégies de commande. Lier les stratégies de commande au groupe d'utilisateurs.
   g) Partitions. Liez les partitions au groupe d'utilisateurs.

4. Cliquez sur **Créer** et **Fermer**.



> **Remarque :**
>
> Pour ajouter des membres au groupe, dans la section Membres, cliquez sur **Ajouter**. Sélectionnez des utilisateurs dans la liste Disponibles et ajoutez-les à la liste Configuré.

Configurer les stratégies de commande

Les stratégies de commande régissent les commandes, groupes de commandes, serveurs virtuels et autres entités que les utilisateurs et les groupes d'utilisateurs sont autorisés à utiliser.

L'appliance fournit un ensemble de stratégies de commande intégrées et vous pouvez configurer des stratégies personnalisées. Pour appliquer les stratégies, vous les liez à des utilisateurs ou à des groupes.

Voici les points clés à garder à l'esprit lors de la définition et de l'application de stratégies de commande.

- Vous ne pouvez pas créer de stratégies de commande globales. Les stratégies de commande doivent être liées directement aux utilisateurs et aux groupes de l'appliance.
- Les utilisateurs ou les groupes sans stratégie de commande associée sont soumis à la stratégie de commande par défaut (DENY-ALL) et ne peuvent donc pas exécuter de commandes de configuration tant que les stratégies de commande appropriées ne sont pas liées à leurs comptes.
- Tous les utilisateurs héritent des stratégies des groupes auxquels ils appartiennent.

- Vous devez attribuer une priorité à une stratégie de commande lorsque vous la liez à un compte d'utilisateur ou à un compte de groupe. Cela permet à l'appliance de déterminer quelle stratégie a la priorité lorsque deux stratégies conflictuelles ou plus s'appliquent au même utilisateur ou au même groupe.
- Les commandes suivantes sont disponibles par défaut pour n'importe quel utilisateur et ne sont pas affectées par les commandes que vous spécifiez :
- aide, afficher l'attribut CLI, définir l'invite CLI, effacer l'invite CLI, afficher l'invite CLI, alias, unalias, historique, quitter, exit, whoami, config, définir le mode CLI, annuler le mode CLI et afficher le mode CLI.

Le tableau suivant décrit les stratégies intégrées.

Nom de la stratégie	Autorise
lecture seule	Accès en lecture seule à toutes les commandes show sauf show ns RunningConfig, show ns ns.conf et show pour le groupe de commandes Citrix ADC.
opérateur	Accès en lecture seule et accès aux commandes pour activer et désactiver les services et les serveurs.
network	Accès complet, sauf aux commandes SSL set et unset, show ns ns.conf, show ns RunningConfig et show gslb RunningConfig.
sysadmin	[Inclus dans Citrix ADC 12.0 et versions ultérieures] Un administrateur système est inférieur à celui d'un superutilisateur est des conditions d'accès autorisées sur l'appliance. Un utilisateur sysadmin peut effectuer toutes les opérations de Citrix ADC avec les exceptions suivantes : aucun accès à l'interpréteur de commandes Citrix ADC, ne peut pas effectuer de configurations utilisateur, ne peut pas effectuer de configurations de partition et d'autres configurations comme indiqué dans la stratégie de commande sysadmin.
superutilisateur	Accès complet. Mêmes privilèges que l'utilisateur nsroot.

Créer des stratégies de commande personnalisées

La prise en charge des expressions régulières est proposée aux utilisateurs disposant des ressources nécessaires pour gérer des expressions plus personnalisées, ainsi qu'aux déploiements nécessitant la flexibilité offerte par les expressions régulières. Pour la plupart des utilisateurs, les stratégies de commande intégrées sont suffisantes. Les utilisateurs qui ont besoin de plus de niveaux de contrôle mais qui ne connaissent pas les expressions régulières peuvent vouloir utiliser uniquement des expressions simples, telles que celles figurant dans les exemples fournis dans cette section, pour maintenir la lisibilité des stratégies.

Lorsque vous utilisez une expression régulière pour créer une stratégie de commande, gardez à l'esprit les éléments suivants.

- Lorsque vous utilisez des expressions régulières pour définir des commandes affectées par une stratégie de commande, vous devez placer les commandes entre guillemets doubles. Par exemple, pour créer une stratégie de commande qui inclut toutes les commandes commençant par show, tapez ce qui suit :
- "^show .*$"
- Pour créer une stratégie de commande qui inclut toutes les commandes commençant par rm, tapez ce qui suit :
- "^rm .*$"
- Les expressions régulières utilisées dans les stratégies de commande ne sont pas sensibles à la casse.

Le tableau suivant répertorie des exemples d'expressions régulières pour les stratégies de commande :

Spécification de commande	Correspond à ces commandes
"^rm\s+.*$"	Toutes les actions de suppression, car toutes les actions de suppression commencent par la chaîne rm, suivie d'un espace et d'autres paramètres tels que des groupes de commandes, des types d'objets de commande et des arguments.
"^show\s+.*$"	Toutes les commandes show, car toutes les actions show commencent par la chaîne show, suivie d'un espace et d'autres paramètres tels que les groupes de commandes, les types d'objets de commande et les arguments.

Spécification de commande	Correspond à ces commandes
« ^shell$ »	La commande shell seule, mais non combinée avec des paramètres supplémentaires tels que les groupes de commandes, les types d'objets de commande et les arguments.
"^add\s+vserver\s+.*$"	Toutes créent des actions de serveur virtuel, qui consistent à ajouter une commande serveur virtuel suivie d'un espace et d'autres paramètres tels que des groupes de commandes, des types d'objets de commande et des arguments.
"^add\s+(lb\s+vserver)\s+.*"	Toutes créent des actions de serveur virtuel lb, qui consistent en la commande add lb virtual server suivie d'un espace et d'autres paramètres tels que des groupes de commandes, des types d'objets de commande et des arguments.

Pour plus d'informations sur les stratégies de commande intégrées, reportez-vous au tableau Tableau des stratégies de commandes intégrées .

Pour créer une stratégie de commande à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une stratégie de commande et vérifier la configuration :

- `add system cmdPolicy <policyname> <action> <cmdspec>`
- `show system cmdPolicy <policyName>`

Exemple :

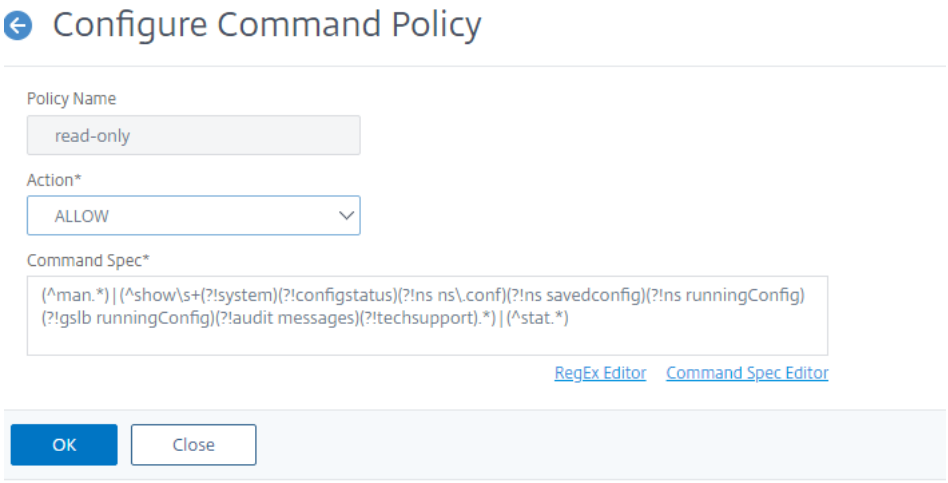
```
add system cmdPolicy USER-POLICY ALLOW (\ server\ )|(\ service(Group)*\ )
|(\ vserver\ )|(\ policy\ )|(\ policylabel\ )|(\ limitIdentifier\ )|(^show\
 (?!(system|ns\ (ns.conf|runningConfig)))|(save)|(stat\ .*serv)
```

Configurer une stratégie de commande à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Système** > **Administration de l'utilisateur** > **Stratégies de commande**.
2. Dans le volet d'informations, cliquez sur **Ajouter** pour créer une stratégie de commande.
3. Dans la page **Configurer la stratégie de commande**, définissez les paramètres suivants :

a) Nom de la stratégie
b) Action
c) Spécification de commande.

4. Cliquez sur **OK**.



Lier les stratégies de commande aux comptes d'utilisateurs et aux groupes d'utilisateurs

Une fois que vous avez défini vos stratégies de commande, vous devez les lier aux comptes d'utilisateurs et aux groupes appropriés. Lorsque vous liez une stratégie, vous devez lui attribuer une priorité afin que l'appliance puisse déterminer la stratégie de commande à suivre en cas de conflit entre deux ou plusieurs stratégies de commande applicables.

Les stratégies de commande sont évaluées dans l'ordre suivant :

- Les stratégies de commande liées directement aux utilisateurs et aux groupes correspondants sont évaluées en fonction d'un numéro de priorité. Une stratégie de commande avec un numéro de priorité inférieur est évaluée avant une stratégie avec un numéro de priorité plus élevé. Par conséquent, les privilèges accordés ou refusés explicitement par la stratégie de commande de numéro inférieur ne sont pas remplacés par une stratégie de commande de numéro supérieur.
- Lorsque deux stratégies de commande, l'une liée à un compte d'utilisateur et l'autre à un groupe, ont le même numéro de priorité, la stratégie de commande liée directement au compte d'utilisateur est évaluée en premier.

Pour lier des stratégies de commande à un utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une stratégie de commande à un utilisateur et vérifier la configuration :

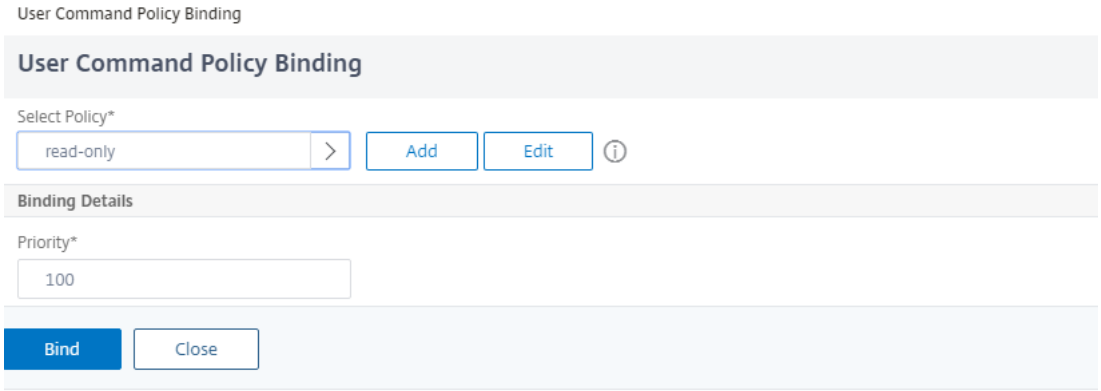
- `bind system user <userName> -policyName <policyName> <priority>`
- `show system user <userName>`

Exemple :

```
> bind system user user1 -policyName read_all 1
```

Lier les stratégies de commande à un compte d'utilisateur à l'aide de l'interface graphique Citrix ADC

Accédez à **Système** > **Administration des utilisateurs> Utilisateurs**, sélectionnez l'utilisateur et liez les stratégies de commande.



Vous pouvez éventuellement modifier la priorité par défaut pour vous assurer que la stratégie est évaluée dans l'ordre approprié.

Pour lier des stratégies de commande à un groupe à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une stratégie de commande à un groupe d'utilisateurs et vérifier la configuration :

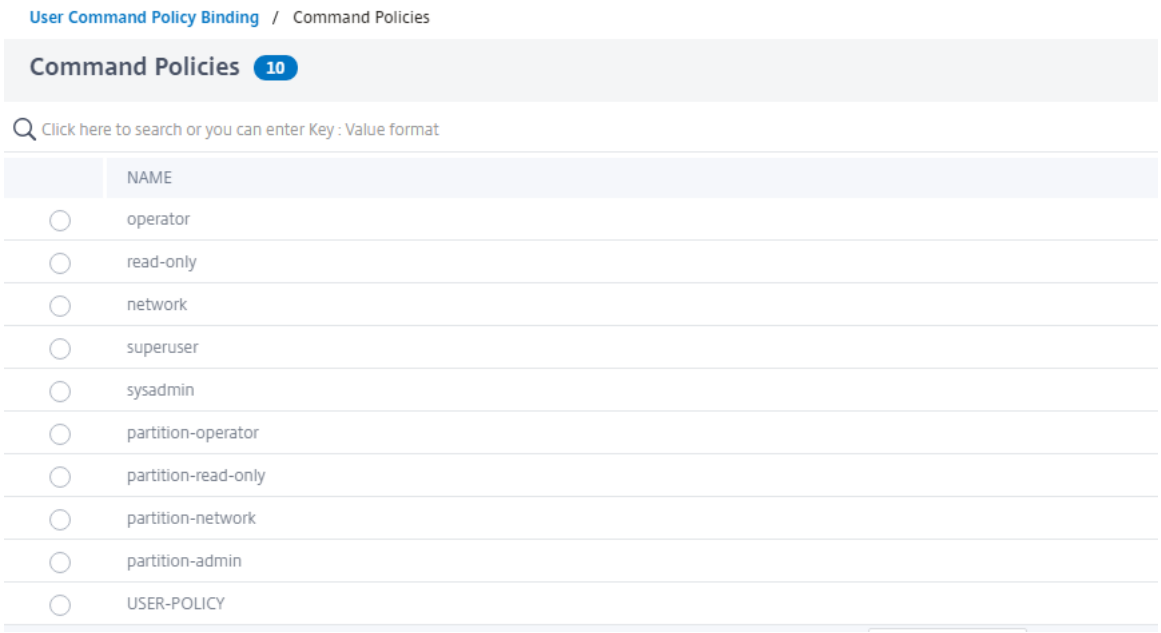
- `bind system group <groupName> -policyName <policyName> <priority>`
- `show system group <groupName>`

Exemple :

```
> bind system group Managers -policyName read_all 1
```

Lier les stratégies de commande à un groupe d'utilisateurs à l'aide de l'interface graphique Citrix ADC

Accédez à **Système** > **Administration des utilisateurs** > **Groupes**, sélectionnez les stratégies de commande de groupe et de liaison.



Vous pouvez éventuellement modifier la priorité par défaut pour vous assurer que la stratégie est évaluée dans l'ordre approprié.

Exemple d'utilisation : Gérer les comptes d'utilisateurs, les groupes d'utilisateurs et les stratégies de commande dans une organisation de fabrication

L'exemple suivant montre comment créer un ensemble complet de comptes d'utilisateurs, de groupes et de stratégies de commande et lier chaque stratégie aux groupes et utilisateurs appropriés. La société, Example Manufacturing, Inc., dispose de trois utilisateurs qui peuvent accéder à l'appliance Citrix ADC :

- **John Doe.** Le responsable informatique. John doit pouvoir voir toutes les parties de la configuration Citrix ADC mais n'a pas besoin de modifier quoi que ce soit.
- **Maria Ramiez.** Administrateur informatique responsable. Maria doit être en mesure de voir et de modifier toutes les parties de la configuration Citrix ADC à l'exception des commandes Citrix ADC (que la stratégie locale dicte doit être exécutée lors de la connexion en tant que nsroot).
- **Michael Baldrock.** Administrateur informatique en charge de l'équilibrage de charge. Michael doit pouvoir voir toutes les parties de la configuration Citrix ADC, mais ne doit modifier que les fonctions d'équilibrage de charge.

Le tableau suivant présente la répartition des informations réseau, des noms de compte d'utilisateur, des noms de groupe et des stratégies de commande pour l'exemple de société.

Champ	Valeur	Remarque
Nom d'hôte Citrix ADC	ns01.exemple.net	S.O.
Comptes utilisateur	johnd, mariar et michaelb	John Doe, responsable informatique, Maria Ramirez, administrateur informatique et Michael Baldrock, administrateur informatique.
Groupes	Responsables et SysOps	Tous les responsables et tous les administrateurs informatiques.
Stratégies de commande	read_all, modify_lb et modify_all	Autoriser l'accès complet en lecture seule, Autoriser l'accès de modification à l'équilibrage de charge et Autoriser l'accès complet à la modification.

La description suivante vous guide tout au long du processus de création d'un ensemble complet de comptes d'utilisateurs, de groupes et de stratégies de commande sur l'appliance Citrix ADC nommé ns01.example.net.

La description inclut des procédures pour lier les comptes d'utilisateurs et les groupes appropriés entre eux, et lier les stratégies de commande appropriées aux comptes d'utilisateurs et aux groupes.

Cet exemple illustre comment vous pouvez utiliser la hiérarchisation pour accorder un accès précis et des privilèges à chaque utilisateur du service informatique.

L'exemple suppose que l'installation et la configuration initiales ont déjà été effectuées sur Citrix ADC.

Configurer des comptes d'utilisateurs, des groupes et des stratégies de commande pour un exemple d'organisation

1. Utilisez la procédure décrite dans la section Configuration des comptes d'utilisateurs pour créer des comptes utilisateur **johnd**, **mariar**et **michaelb**.
2. Utilisez la procédure décrite dans Configuration des groupes d'utilisateurs pour créer des groupes d'utilisateurs **Gestionnaires** et **SySOps**, puis lier les utilisateurs **mariar** et **michaelb** au groupe **SySOps** et l'utilisateur **johnd** au groupe **Managers**.
3. Utilisez la procédure décrite à la section Création de stratégies de commande personnalisées pour créer les stratégies de commande suivantes :

- **read_all** avec l'action **Autoriser** et spécification`"(^show\s+(?!system)(?!ns ns.conf)(?!ns runningConfig).*)|(^stat.*)"` de commande
- **modify_lb** avec l'action **Autoriser** et la spécification`"^set\s+lb\s+.*$"` de commande
- modify_all avec l'action Autoriser et la spécification`"^\S+\s+(?!system).*"`de commande

4. Utilisez la procédure décrite dans « Liaison des stratégies de commande aux utilisateurs et aux groupes » pour lier la stratégie de commande **read_all** au groupe **SysOps**, avec la valeur de priorité **1**.
5. Utilisez la procédure décrite dans « Liaison des stratégies de commande aux utilisateurs et aux groupes » pour lier la stratégie de commande **modify_lb** à l'utilisateur **michaelb**, avec la valeur de priorité **5**.

La configuration que vous venez de créer donne les résultats suivants :

- John Doe, le responsable informatique, dispose d'un accès en lecture seule à l'ensemble de la configuration de Citrix ADC, mais il ne peut pas apporter de modifications.
- Maria Ramirez, responsable informatique, dispose d'un accès quasi complet à toutes les zones de la configuration de Citrix ADC, ayant à se connecter uniquement pour exécuter les commandes de niveau Citrix ADC.
- Michael Baldrock, l'administrateur informatique responsable de l'équilibrage de charge, dispose d'un accès en lecture seule à la configuration de Citrix ADC et peut modifier les options de configuration pour l'équilibrage de charge.

L'ensemble de stratégies de commande qui s'applique à un utilisateur spécifique est une combinaison de stratégies de commande appliquées directement au compte de l'utilisateur et de stratégies de commande appliquées à un ou plusieurs groupes dont l'utilisateur est membre.

Chaque fois qu'un utilisateur entre une commande, le système d'exploitation recherche les stratégies de commande pour cet utilisateur jusqu'à ce qu'il trouve une stratégie avec une action ALLOW ou DENY correspondant à la commande. Lorsqu'il trouve une correspondance, le système d'exploitation arrête sa recherche de stratégie de commande et autorise ou refuse l'accès à la commande.

Si le système d'exploitation ne trouve aucune stratégie de commande correspondante, il refuse à l'utilisateur l'accès à la commande, conformément à la stratégie de refus par défaut de l'appliance Citrix ADC.

> **Remarque :**
>
> Lorsque vous placez un utilisateur dans plusieurs groupes, prenez soin de ne pas provoquer de restrictions ou de privilèges de commande utilisateur involontaires. Pour éviter ces conflits, lorsque vous organisez vos utilisateurs en groupes, gardez à l'esprit la procédure de recherche de stratégie de commande Citrix ADC et les règles de classement de stratégie.

Gestion des comptes utilisateur et des mots de passe

August 20, 2021

Citrix ADC vous permet de gérer la configuration des comptes d'utilisateurs et des mots de passe. Voici quelques-unes des activités que vous pouvez effectuer pour un compte d'utilisateur système ou un compte d'utilisateur `nsroot` administrateur sur l'appliance.

- Verrouillage du compte utilisateur système
- Verrouiller le compte d'utilisateur système pour l'accès de gestion
- Déverrouiller un compte d'utilisateur système verrouillé pour l'accès à la gestion
- Désactiver l'accès de gestion pour le compte d'utilisateur système
- Forcer le changement de mot de passe `nsroot` pour les utilisateurs
- Supprimer les fichiers sensibles dans un compte d'utilisateur système
- Configuration de mot de passe forte pour les utilisateurs système

Verrouillage du compte utilisateur système

Pour éviter les attaques de sécurité par force brute, vous pouvez configurer la configuration de verrouillage de l'utilisateur. La configuration permet à un administrateur réseau d'empêcher un utilisateur système de se connecter à une appliance Citrix ADC. Et déverrouillez également le compte d'utilisateur avant l'expiration de la période de verrouillage.

À l'invite de commandes, tapez :

```
set aaa parameter -maxloginAttempts <value> -failedLoginTimeout <value> -
persistentLoginAttempts (ENABLED | DISABLED)
```

> **Remarque**
>
> Le paramètre "persistentLoginAttempts" doit être ACTIVÉ pour obtenir les détails du stockage persistant des tentatives de connexion utilisateur infructueuses.

Exemple :

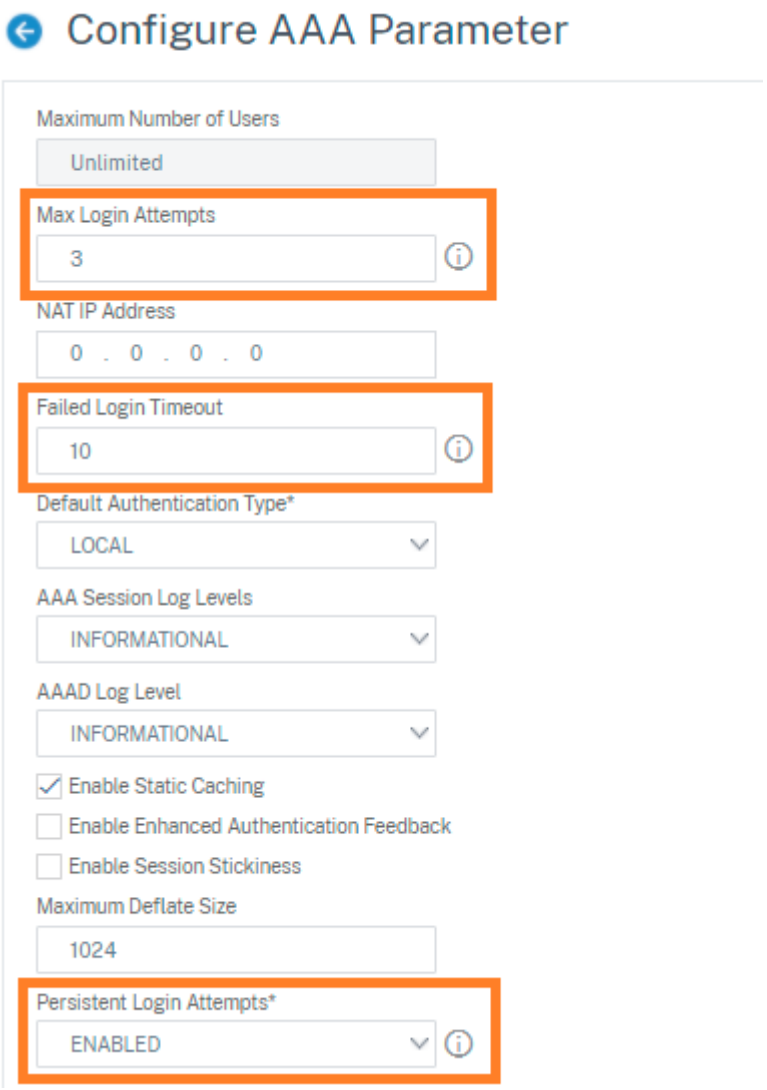
```
set aaa parameter -maxloginAttempts 3 -failedLoginTimeout 10 -persistentLoginAttempts
 ENABLED
```

Configurer le verrouillage du compte d'utilisateur système à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > AAA-Application Trafic > Paramètres d'authentification > Modifier les paramètres d'authentification AAA**.
2. Dans la page **Configurer le paramètre AAA**, définissez les paramètres suivants :

a) Tentatives de connexion maximales. Nombre maximal de tentatives d'ouverture de session autorisées par l'utilisateur.
b) Échec du délai d'attente de connexion. Nombre maximal de tentatives d'ouverture de session non valides effectuées par l'utilisateur.
c) Tentatives de connexion persistantes. Stockage persistant des tentatives de connexion utilisateur infructueuses.

3. Cliquez sur **OK**.



Lorsque vous définissez les paramètres, le compte d'utilisateur est verrouillé pendant 10 minutes pour trois tentatives de connexion non valides ou plus. En outre, l'utilisateur ne peut pas ouvrir de session même avec des informations d'identification valides pendant 10 minutes.

> **Remarque**
>
> Si un utilisateur verrouillé tente de se connecter à l'appliance, un message d'erreur RBA

> `Authentication Failure: maxlogin attempt reached for test.` s'affiche.

Verrouiller le compte d'utilisateur système pour l'accès de gestion

L'appliance Citrix ADC vous permet de verrouiller un utilisateur système pendant 24 heures et de refuser l'accès à l'utilisateur.

L'appliance Citrix ADC prend en charge la configuration pour les utilisateurs système et externes.

> **Remarque**
>
> La fonctionnalité n'est prise en charge que si vous désactivez l'option `persistentLoginAttempts` dans le paramètre `aaa`.

À l'invite de commandes, tapez :

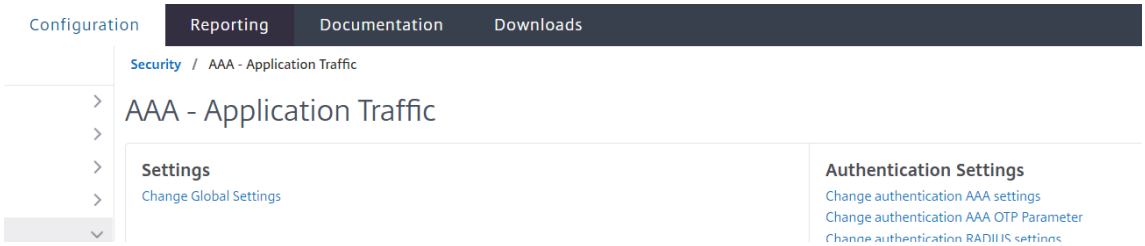
```
set aaa parameter -persistentLoginAttempts DISABLED
```

Maintenant, pour verrouiller un compte d'utilisateur, à l'invite de commandes, tapez :

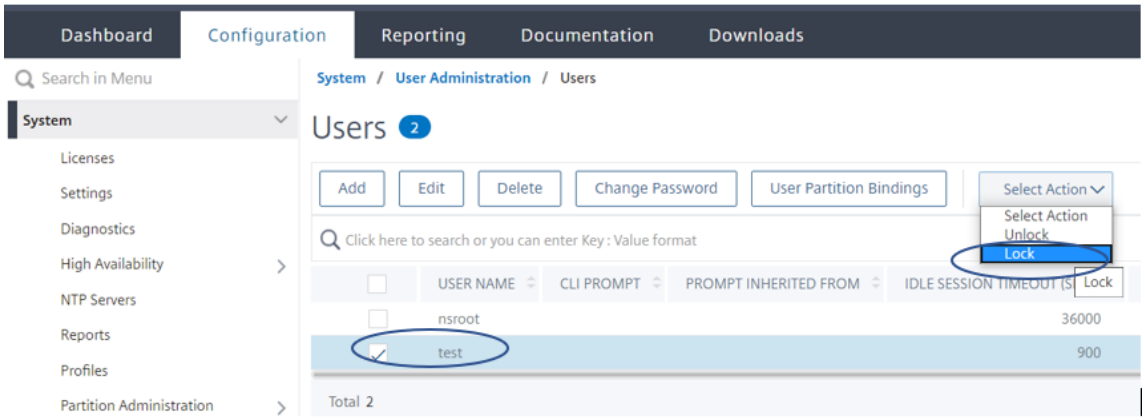
```
lock aaa user test
```

Verrouiller un compte d'utilisateur système à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > AAA-Application Trafic > Paramètres d'authentification > Modifier les paramètres d'authentification AAA**.



2. Dans **Configurer le paramètre AAA**, dans la liste **Tentatives de connexion persistantes**, sélectionnez **DÉSACTIVÉ**.
3. Accédez à **Système > Administration des utilisateurs > Utilisateurs**.
4. Sélectionnez un utilisateur.
5. Dans la liste Sélectionner une action, sélectionnez **Verrouiller**.



> **Remarque**
>
> L'interface graphique Citrix ADC ne dispose pas d'option pour verrouiller les utilisateurs externes. Pour verrouiller un utilisateur externe, l'administrateur ADC doit utiliser l'interface de ligne de commande.
> Lorsqu'un utilisateur système verrouillé (verrouillé avec une commande d'authentification de verrouillage, d'autorisation et d'audit de l'utilisateur) tente de se connecter à Citrix ADC, l'appliance affiche un message d'erreur « Échec de l'authentification RBA : test utilisateur est verrouillé pendant 24 heures ».
>
> Lorsqu'un utilisateur est verrouillé pour se connecter à l'accès de gestion, l'accès à la console est exempté. L'utilisateur verrouillé est capable de se connecter à la console.

Déverrouiller un compte d'utilisateur système verrouillé pour l'accès à la gestion

Les utilisateurs système et les utilisateurs externes peuvent être verrouillés pendant 24 heures à l'aide de la commande d'authentification de verrouillage, d'autorisation et d'audit de l'utilisateur.

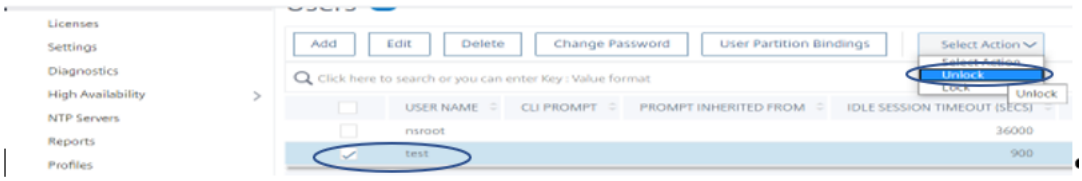
> **Remarque**
>
> L'appliance ADC permet aux administrateurs de déverrouiller l'utilisateur verrouillé et la fonctionnalité ne nécessite aucun paramètre dans la commande « PersistentLoginEssentents ».

À l'invite de commandes, tapez :

```
unlock aaa user test
```

Configurer le déverrouillage de l'utilisateur système à l'aide de l'interface graphique

1. Accédez à **Système > Administration des utilisateurs > Utilisateurs**.
2. Sélectionnez un utilisateur.
3. Cliquez sur **Déverrouiller**.



L'interface graphique Citrix ADC répertorie uniquement les utilisateurs système créés dans ADC, de sorte qu'il n'y a pas d'option dans l'interface graphique pour déverrouiller les utilisateurs externes. Pour déverrouiller un utilisateur externe, l'administrateur `nsroot` doit utiliser l'interface de ligne de commande.

Désactiver l'accès de gestion pour le compte d'utilisateur système

Lorsque l'authentification externe est configurée sur l'appliance et que vous préférez refuser que les utilisateurs système se connectent à l'accès à la gestion, vous devez désactiver l'option LocalAuth dans le paramètre système.

À l'invite de commandes, tapez ce qui suit :

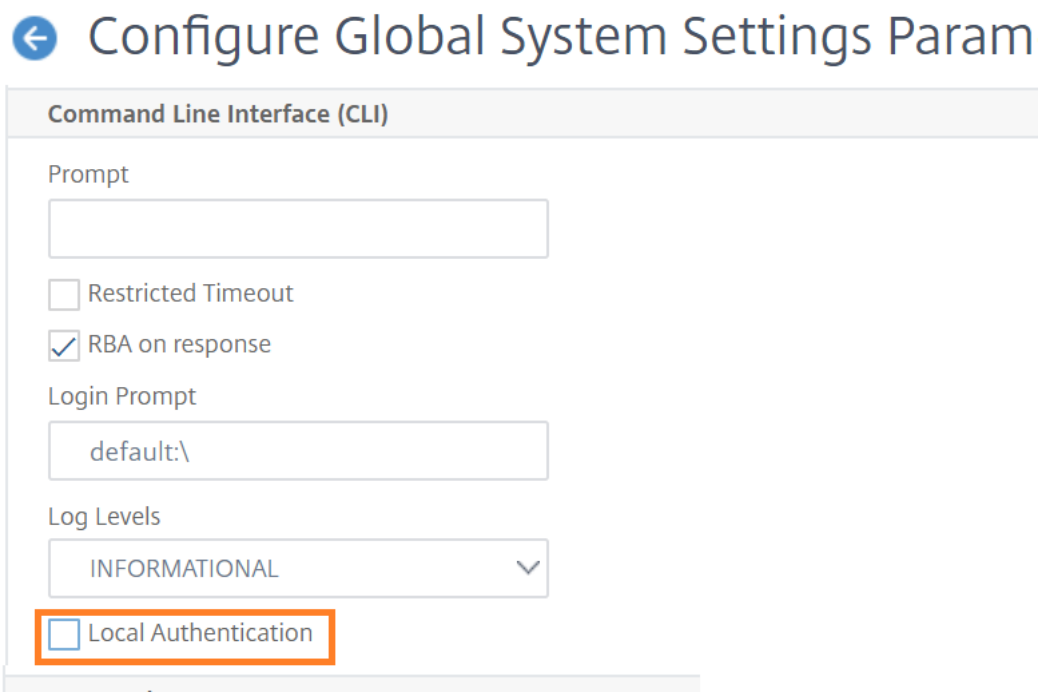
```
set system parameter localAuth <ENABLED|DISABLED>
```

Exemple :

```
set system parameter localAuth DISABLED
```

Désactiver l'accès de gestion à l'utilisateur système à l'aide de l'interface graphique

1. Accédez à **Configuration > Système > Paramètres > Modifier les paramètres globaux du système**.
2. Dans **la section Interface de ligne de commande (CLI)**, décochez la case **Authentification locale**.



En désactivant cette option, les utilisateurs du système local ne peuvent pas se connecter à l'accès de gestion ADC.

> **Remarque**
>
> Le serveur d'authentification externe doit être configuré et accessible pour interdire l'authentification de l'utilisateur système local dans le paramètre système. Si le serveur externe configuré dans ADC pour l'accès à la gestion est inaccessible, les utilisateurs du système local peuvent ouvrir une session sur l'appliance. Le comportement est configuré à des fins de récupération.

Forcer le changement de mot de passe pour les utilisateurs

Pour une authentification sécurisée `nsroot`, l'appliance Citrix ADC invite l'utilisateur à changer le mot de passe par défaut en un nouveau si l'option `forcePasswordChange` est activée dans le paramètre système. Vous pouvez modifier votre `nsroot` mot de passe à partir de la CLI ou de l'interface graphique, lors de votre première connexion avec les informations d'identification par défaut.

À l'invite de commandes, tapez :

```
set system parameter -forcePasswordChange ( ENABLED | DISABLED )
```

Exemple de session SSH pour NSIP :

```
1 ssh nsroot@1.1.1.1
```



```
Connecting to 1.1.1.1:22...
Connection established.
To escape to local shell, press Ctrl+Alt+].
###############################################################################

WARNING: Access to this system is for authorized users only #
Disconnect IMMEDIATELY if you are not an authorized user! #

###############################################################################

Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
Done
<!--NeedCopy-->
```

Supprimer les fichiers sensibles dans un compte d'utilisateur système

Pour gérer des données sensibles telles que les clés autorisées et les clés publiques d'un compte d'utilisateur système, vous devez activer `removeSensitiveFiles` cette option. Les commandes qui suppriment les fichiers sensibles lorsque le paramètre système est activé sont les suivantes :

- rm cluster instance
- rm cluster node
- noeud haute disponibilité rm
- config clair complet
- rejoindre le cluster
- ajouter une instance de cluster

À l'invite de commandes, tapez :

```
set system parameter removeSensitiveFiles ( ENABLED | DISABLED )
```

Exemple :

```
set system parameter -removeSensitiveFiles ENABLED
```

Configuration de mot de passe forte pour les utilisateurs système

Pour une authentification sécurisée, l'appliance Citrix ADC invite les utilisateurs système et les administrateurs à définir des mots de passe forts pour se connecter à l'appliance. Le mot de passe doit être long et doit être une combinaison de :

- Un caractère minuscule
- Un caractère majuscule

- Un caractère numérique
- Un caractère spécial

À l'invite de commandes, tapez :

```
set system parameter -strongpassword <value> -minpasswordlen <value>
```

Où,

`Strongpassword`. Après avoir activé le mot de passe fort (`enable all` / `enablelocal`), tous les mots de passe ou informations sensibles doivent avoir les éléments suivants :

- Au moins 1 caractère minuscule
- Au moins 1 caractère majuscule
- Au moins 1 caractère numérique
- Au moins 1 caractère spécial

Excluez la liste dans `enablelocal` est - `NS_FIPS`, `NS_CRL`, `NS_RSAKEY`, `NS_PKCS12`, NS_PKCS8, NS_LDAP, `NS_TACACS`, `NS_TACACSACTION`, `NS_RADIUS`, `NS_RADIUSACTION`, `NS_ENCRYPTION_PARAMS` . Par conséquent, aucune vérification du mot de passe fort n'est effectuée sur ces commandes ObjectType pour l'utilisateur système.

Valeurs possibles :`enableall`, `enablelocal`, désactivé Valeur
par défaut : disabled

`minpasswordlen`. Longueur minimale du mot de passe utilisateur système. Lorsque le mot de passe fort est activé par défaut, la longueur minimale est de 4. La valeur saisie par l'utilisateur peut être supérieure ou égale à 4. La valeur minimale par défaut est 1 lorsque le mot de passe fort est désactivé. La valeur maximale est 127 dans les deux cas.

Valeur minimale : 1 Valeur
maximale : 127

Exemple :

```
set system parameter -strongpassword enablelocal -minpasswordlen 6
```

Compte utilisateur par défaut

Le compte d'utilisateur `nsrecover` peut être utilisé par l'administrateur pour restaurer l'appliance Citrix ADC. Vous pouvez vous connecter à l'appliance ADC `nsrecover` si les utilisateurs système par défaut (`nsroot`) ne peuvent pas se connecter en raison de problèmes imprévus. La connexion `nsrecover` est indépendante des configurations utilisateur et vous permet d'accéder directement à l'invite shell. Vous êtes toujours autorisé à vous connecter via `nsrecover`, même si la limite maximale de configuration est atteinte.

Comment réinitialiser le mot de passe administrateur (nsroot)

August 20, 2021

Le compte administrateur racine (`nsroot`) Citrix ADC offre un accès complet à toutes les fonctionnalités ADC. Ainsi, pour préserver la sécurité, le compte administratif ne doit être utilisé que si nécessaire.

En tant qu'administrateur, il est recommandé de modifier votre mot de passe. Si vous oubliez votre mot de passe, vous devez d'abord le réinitialiser au mot de passe par défaut, puis le remplacer par un nouveau mot de passe.

En tant qu' `nsroot` administrateur, pour réinitialiser votre mot de passe, vous devez vous connecter à votre appliance et modifier le mot de passe. Toutefois, si vous ne vous souvenez pas du mot de passe, vous pouvez redémarrer l'appliance en mode mono-utilisateur. Montez le système de fichiers en mode lecture/écriture, puis supprimez l'entrée **Citrix ADC** du fichier ns.conf. Pour terminer, redémarrez et connectez-vous à votre appliance avec le mot de passe par défaut, puis définissez un nouveau mot de passe.

Procédez comme suit pour réinitialiser votre mot de passe administrateur root :

1. Connectez un ordinateur au port console du Citrix ADC et ouvrez une session.

   > **Remarque**
   >
   > Vous ne pouvez pas ouvrir une session à l'aide de SSH pour effectuer cette procédure. Vous devez vous connecter directement à l'appliance.

2. Redémarrez le Citrix ADC.
3. Appuyez sur CTRL+C lorsque le message suivant s'affiche :

   ```
   Press [Ctrl-C] for command prompt, or any other key to boot immediately
   .
   Booting [kernel] in ## seconds.
   ```

   > **Remarque**
   >
   > Dans une console série Azure, l'appliance Citrix ADC ne prend pas en charge le démarrage unique tant que l'appliance ADC n'est pas démarrée.

4. Exécutez la commande suivante pour démarrer Citrix ADC en mode utilisateur unique :

   ```
   boot -s
   ```

   Après le démarrage de l'appliance, le message suivant s'affiche :

   Entrez le nom du chemin d'accès complet du shell ou`RETURN for /bin/sh:`

5. Appuyez sur ENTRÉE pour afficher l'invite # et tapez les commandes suivantes pour monter les systèmes de fichiers :

a) Exécutez la commande suivante pour vérifier la cohérence du disque :

```
fsck_ufs /dev/ad0s1a
```

> **Remarque**
>
> Votre lecteur flash a un nom de périphérique spécifique en fonction de votre Citrix ADC. Par conséquent, vous devez remplacer ad0s1a dans la commande précédente par le nom de périphérique approprié.

b) Accédez au répertoire de développement et entrez « ls » pour vérifier les détails du lecteur.

c) Exécutez la commande suivante pour afficher les partitions montées :

```
df
```

> **Remarque**
>
> Si la partition flash n'est pas répertoriée, vous devez la monter manuellement.

d) Exécutez la commande suivante pour monter le lecteur flash :

```
mount dev/ad0s1a /flash
```

6. Exécutez la commande suivante pour passer au `nsconfig` répertoire :

```
cd /flash/nsconfig
```

7. Exécutez les commandes suivantes pour réécrire le fichier ns.conf et supprimer l'ensemble des commandes système par défaut à l'administrateur :

a) Exécutez la commande suivante pour créer un fichier de configuration qui n'a pas de commandes par défaut pour l'administrateur :

```
grep -v "set system user nsroot" ns.conf > new.conf
```

b) Exécutez la commande suivante pour effectuer une sauvegarde du fichier de configuration existant :

```
mv ns.conf old.ns.conf
```

c) Exécutez la commande suivante pour renommer le nouveau fichier .conf en ns.conf :

```
mv new.conf ns.conf
```

8. Exécutez la commande suivante pour redémarrer Citrix ADC :

```
reboot
```

9. Connectez-vous à l'aide des informations d'identification administrateur par défaut.

10. Exécutez la commande suivante pour réinitialiser le mot de passe administrateur :

```
set system user nsroot <New_Password>
```


> **Remarque**
>
> Pour utiliser le « ? « dans une chaîne de mot de passe, précédez ce caractère par le \ caractère.

Par exemple, `yourexamplepasswd\?` est défini pour le compte administrateur après avoir effectué l'opération suivante :

```
> set system user nsroot yourexamplepasswd\?
```

> **Remarque**
>
> Pour réinitialiser un mot de passe oublié (`nsroot`) dans une configuration haute disponibilité, Citrix vous recommande d'arrêter le nœud homologue. Si le nœud homologue est actif, le mot de passe est écrasé, car la synchronisation de configuration est déclenchée lorsque le nœud apparaît après le redémarrage.

Lisez également l'article CTX224027 de Citrix pour savoir comment fonctionne l'accès SSH sécurisé à l'appliance Citrix ADC.

Authentification utilisateur externe

August 20, 2021

Le service d'authentification dans une appliance Citrix ADC peut être local ou externe. Dans le cadre de l'authentification utilisateur externe, l'appliance utilise un serveur externe tel que LDAP, RADIUS ou TACACS+ pour authentifier l'utilisateur. Pour authentifier un utilisateur externe et lui accorder l'accès à l'appliance, vous devez appliquer une stratégie d'authentification. L'authentification du système Citrix ADC utilise des stratégies d'authentification avancées avec des expressions de stratégie avancées. Les stratégies d'authentification avancées sont également utilisées pour la gestion des utilisateurs système dans un dispositif Citrix ADC partitionné.

> **Remarque**
>
> Si votre appliance utilise toujours des stratégies classiques et ses expressions, vous devez cesser de l'utiliser et migrer votre utilisation de stratégie classique vers l'infrastructure de stratégie avancée.

Une fois que vous avez créé une stratégie d'authentification, vous devez la lier à l'entité globale du système. Vous pouvez configurer un serveur d'authentification externe (par exemple, TACACS) en liant une seule stratégie d'authentification à l'entité globale du système. Vous pouvez également configurer une cascade de serveurs d'authentification en liant plusieurs stratégies à l'entité globale du système.

> **Remarque**
>
> Lorsqu'un utilisateur externe se connecte à l'appliance, le système génère un message d'erreur « Utilisateur n'existe pas » dans le `ns.log` fichier. L'occurrence est due au fait que le système exécute la commande systemuser_systemcmdpolicy_binding pour initialiser l'interface graphique de l'utilisateur.

Authentification LDAP (à l'aide de serveurs LDAP externes)

Vous pouvez configurer l'appliance Citrix ADC pour authentifier l'accès utilisateur avec un ou plusieurs serveurs LDAP. L'autorisation LDAP nécessite des noms de groupe identiques dans Active Directory, sur le serveur LDAP et sur l'appliance. Les caractères et la casse doivent également être les mêmes.

Pour plus d'informations sur les stratégies d'authentification LDAP, consultez la rubrique Stratégies d'authentification LDAP .

Par défaut, l'authentification LDAP est sécurisée à l'aide du protocole SSL/TLS. Il existe deux types de connexions LDAP sécurisées. Dans le premier type, le serveur LDAP accepte la connexion SSL/TLS sur un port distinct du port utilisé pour accepter les connexions LDAP effacées. Une fois que les utilisateurs ont établi la connexion SSL/TLS, le trafic LDAP peut être envoyé via la connexion. Le second type permet à la fois des connexions LDAP non sécurisées et sécurisées, et le port unique le gère sur le serveur. Dans ce scénario, pour créer une connexion sécurisée, le client établit d'abord une connexion LDAP claire. Ensuite, la commande **LDAP** StartTLS est envoyée au serveur via la connexion. Si le serveur LDAP prend en charge StartTLS, la connexion est convertie en connexion LDAP sécurisée à l'aide de TLS.

Les numéros de port pour les connexions LDAP sont les suivants :

- 389 pour les connexions LDAP non sécurisées
- 636 pour des connexions LDAP sécurisées
- 3268 pour les connexions LDAP non sécurisées Microsoft
- 3269 pour les connexions LDAP sécurisées Microsoft

Les connexions LDAP qui utilisent la commande StartTLS utilisent le numéro de port 389. Si les numéros de port 389 ou 3268 sont configurés sur l'appliance, elle tente d'utiliser StartTL pour établir la connexion. Si un autre numéro de port est utilisé, les tentatives de connexion utilisent SSL/TLS. Si StartTLS ou SSL/TLS ne peuvent pas être utilisés, la connexion échoue.

Lors de la configuration du serveur LDAP, la casse des caractères alphabétiques doit correspondre à celle du serveur et de l'appliance. Si le répertoire racine du serveur LDAP est spécifié, tous les sous-répertoires sont également recherchés pour trouver l'attribut utilisateur. Dans les grands répertoires, cela peut affecter les performances. Pour cette raison, Citrix vous recommande d'utiliser une unité d'organisation spécifique.

Le tableau suivant répertorie des exemples de nom unique de base (DN).

Serveur LDAP	DN de base
Microsoft Active Directory	DC = Citrix, DC = local
Novell eDirectory	DC=Citrix, dc=net
IBM Directory Server	cn=users
Lotus Domino	OU=ville, O=Citrix, C=US
Sun ONE Directory (anciennement iPlanet)	OU=People, DC = Citrix, dc=com

Le tableau suivant répertorie des exemples de nom unique de liaison (DN).

Serveur LDAP	Relier le nom distinctif
Microsoft Active Directory	cn=Administrateur, CN=Utilisateurs, DC = Citrix, DC = local
Novell eDirectory	cn=admin, DC=Citrix, dc=net
IBM Directory Server	LDAP_dn
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE Directory (anciennement iPlanet)	uid=admin, OU=Administrateurs, OU=Gestion topologique, O=NetscapeRoot

Serveur LDAP	Relier le nom distinctif
Microsoft Active Directory	cn=Administrateur, CN=Utilisateurs, DC = Citrix, DC = local
Novell eDirectory	cn=admin, DC=Citrix, dc=net
IBM Directory Server	LDAP_dn
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE Directory (anciennement iPlanet)	uid=admin, OU=Administrateurs, OU=Gestion topologique, O=NetscapeRoot

Configurer l'authentification utilisateur LDAP à l'aide de l'interface de ligne de commande

Procédez comme suit pour configurer l'authentification LDAP pour les utilisateurs externes

Configurer la stratégie LDAP

À l'invite de commandes, procédez comme suit :

Étape 1 : Créer une action LDAP.

```
add authentication ldapAction <name> { -serverIP <ip_addr|ipv6_addr|*> | {
 -serverName <string> } } >] [-authTimeout <positive_integer>] [-ldapBase
<string>] [-ldapBindDn <string>] { -ldapBindDnPassword } [-ldapLoginName <
string>] [-groupAttrName <string>] [-subAttributeName <string>]
```

Exemple :

```
add authentication ldapAction ldap_act -serverIP <IP> -authTimeout 30 -
ldapBase "CN=xxxxx,DC=xxxx,DC=xxx"-ldapBindDn "CN=xxxxx,CN=xxxxx,DC=xxxx,DC
=xxx"-ldapBindDnPassword abcd -ldapLoginName sAMAccountName -groupattrName
memberOf -subAttributeName CN
```

Pour la description des paramètres, reportez-vous à la rubrique Référence des commandes d'authentification et d'autorisation .

Étape 2 : Créez une stratégie LDAP classique.

```
add authentication ldapPolicy <name> <rule> [<reqAction>]
```

Exemple :

```
add authentication ldappolicy ldap_pol_classic ns_true ldap_act
```

> **Remarque**
>
> Vous pouvez configurer à l'aide d'une stratégie LDAP classique ou avancée, mais Citrix vous recommande d'utiliser une stratégie d'authentification avancée car les stratégies classiques sont obsolètes à partir de la version Citrix ADC 13.0.

Étape 3 : Créer une stratégie LDAP avancée

```
add authentication Policy <name> <rule> [<reqAction>]
```

Exemple :

```
add authentication policy ldap_pol_advance -rule true -action ldap_act
```

Étape 4 : Liez la politique LDAP au système global

À l'invite de ligne de commande, procédez comme suit :

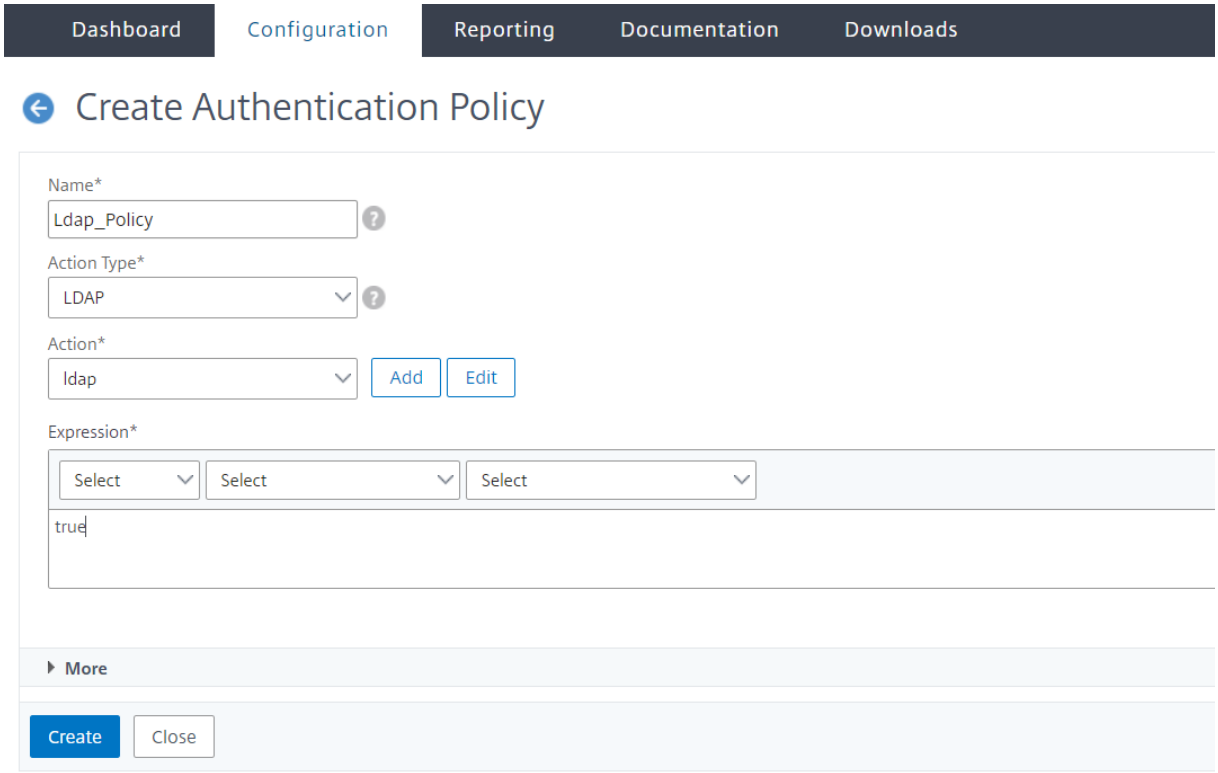
```
bind system global <policyName> [-priority <positive_integer]
```

Exemple :

```
bind system global ldap_pol_advanced -priority 10
```

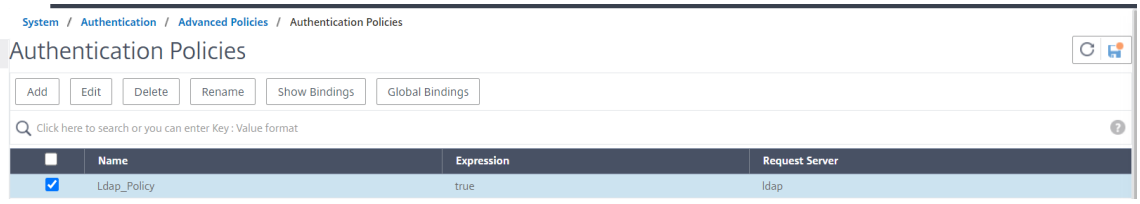

Configurer l'authentification utilisateur LDAP à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégie**.
2. Cliquez sur **Ajouter** pour créer une stratégie d'authentification de type LDAP.
3. Cliquez sur **Créer** et **Fermer**.

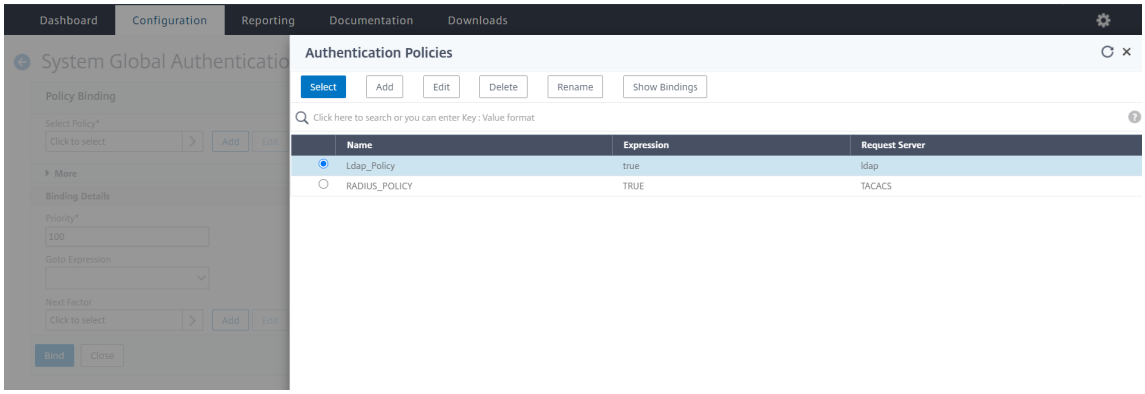


Lier une stratégie d'authentification au système global pour l'authentification LDAP à l'aide de l'interface graphique Citrix ADC

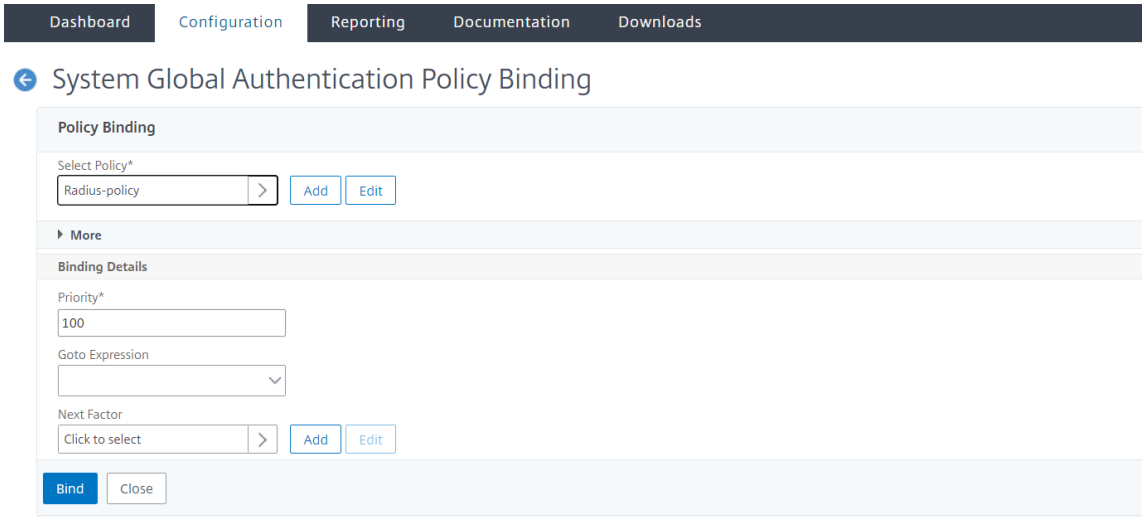
1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégies d'authentificationPolitique**.
2. Dans le volet d'informations, cliquez sur **Liaisons globales** pour créer une liaison de stratégie d'authentification globale système.
3. Cliquez sur **Liaisons globales**.



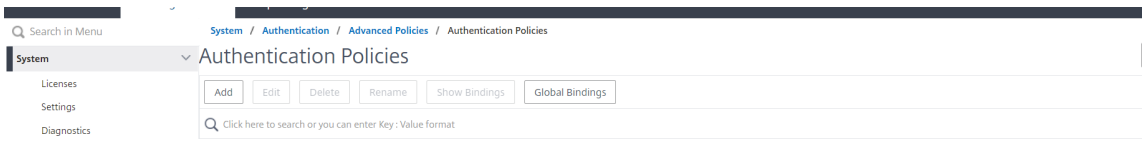
4. Sélectionnez un profil d'authentification.



5. Sélectionnez la stratégie LDAP.
6. Dans la page **Liaison de stratégie d'authentification globale du système**, définissez les paramètres suivants :
   a) Sélectionnez Stratégie.
   b) Détails de liaison



7. Cliquez sur **Lier** et **Terminé**.
8. Cliquez sur **Liaisons globales** pour confirmer la stratégie délimitée au système global.



Détermination des attributs dans le répertoire LDAP

Si vous avez besoin d'aide pour déterminer vos attributs d'annuaire LDAP, vous pouvez facilement les rechercher avec le navigateur LDAP gratuit de Softerra.

Vous pouvez télécharger le navigateur LDAP à partir du site Web Softerra LDAP Administrator à l'adresse <http://www.ldapbrowser.com>. Une fois le navigateur installé, définissez les attributs suivants :

- Nom d'hôte ou adresse IP de votre serveur LDAP.
- Port de votre serveur LDAP. La valeur par défaut est 389.
- Le champ DN de base peut être laissé vide.
- Les informations fournies par le navigateur LDAP peuvent vous aider à déterminer le DN de base requis pour l'onglet Authentification.
- La vérification de liaison anonyme détermine si le serveur LDAP requiert des informations d'identification de l'utilisateur pour que le navigateur se connecte à lui. Si le serveur LDAP requiert des informations d'identification, laissez la case désactivée.

Après avoir terminé les paramètres, le navigateur LDAP affiche le nom du profil dans le volet gauche et se connecte au serveur LDAP.

Pour plus d'informations, consultez la rubrique LDAP .

Prise en charge de l'authentification par clé pour les utilisateurs LDAP

Avec l'authentification par clé, vous pouvez désormais extraire la liste des clés publiques stockées sur l'objet utilisateur dans le serveur LDAP via SSH. L'appliance Citrix ADC pendant le processus d'authentification basée sur les rôles (RBA) doit extraire les clés SSH publiques du serveur LDAP. La clé publique récupérée, compatible avec SSH, doit vous permettre de vous connecter via la méthode RBA.

Un nouvel attribut « sshPublicKey » est introduit dans les commandes « add authentication ldapAction » et « set authentication ldapAction ». En utilisant cet attribut, vous pouvez obtenir les avantages suivants :

- Peut stocker la clé publique récupérée, et l'action LDAP utilise cet attribut pour récupérer les informations de clé SSH à partir du serveur LDAP.
- Peut extraire des noms d'attributs allant jusqu'à 24 Ko.

> **Remarque**
>
> Le serveur d'authentification externe, tel que LDAP, est utilisé uniquement pour récupérer les informations de clé SSH. Il n'est pas utilisé à des fins d'authentification.

Voici un exemple du flux d'événements à travers SSH :

- Le démon SSH envoie une requête AAA_AUTHENTICATE avec un champ de mot de passe vide au port du démon d'authentification, d'autorisation et d'audit.
- Si LDAP est configuré pour stocker la clé publique SSH, l'authentification, l'autorisation et l'audit répond avec l'attribut « sshPublicKey » ainsi que d'autres attributs.

- Le démon SSH vérifie ces clés avec les clés client.
- Le démon SSH transmet le nom d'utilisateur dans la charge utile de la requête, et l'authentification, l'autorisation et l'audit renvoie les clés spécifiques à cet utilisateur ainsi que les clés génériques.

Pour configurer l'attribut sshPublicKey, à l'invite de commandes, tapez les commandes suivantes :

- Avec l'opération add, vous pouvez ajouter l'attribut « sshPublicKey » lors de la configuration de la commande ldapAction.

```
add authentication ldapAction <name> { -serverIP <ip_addr|ipv6_addr
|*> | { -serverName <string> } } [-serverPort <port>] … [-Attribute1 <
string>] … [-Attribute16 <string>][-sshPublicKey <string>][-authentication
 off]<!--NeedCopy-->
```

- Avec l'opération set, vous pouvez configurer l'attribut « sshPublicKey » à une commande ldapAction déjà ajoutée.

```
set authentication ldapAction <name> [-sshPublicKey <string>][-authentication
 off]<!--NeedCopy-->
```

Authentification RADIUS (à l'aide de serveurs RADIUS externes)

Vous pouvez configurer l'appliance Citrix ADC pour authentifier l'accès utilisateur avec un ou plusieurs serveurs RADIUS. Si vous utilisez des produits RSA SecurID, SafeWord ou Gemalto Protiva, utilisez un serveur RADIUS.

Pour plus d'informations sur les stratégies d'authentification RADIUS, consultez la rubrique Stratégies d'authentification RADIUS .

Votre configuration peut nécessiter l'utilisation d'une adresse IP du serveur d'accès réseau (IP NAS) ou d'un identifiant de serveur d'accès réseau (ID NAS). Lorsque vous configurez l'appliance pour qu'elle utilise un serveur d'authentification RADIUS, suivez les instructions suivantes :

- Si vous activez l'utilisation de l'IP NAS, l'appliance envoie son adresse IP configurée au serveur RADIUS, plutôt que l'adresse IP source utilisée pour établir la connexion RADIUS.
- Si vous configurez l'ID NAS, l'appliance envoie l'identificateur au serveur RADIUS. Si vous ne configurez pas l'ID NAS, l'appliance envoie son nom d'hôte au serveur RADIUS.
- Lorsque l'adresse IP du NAS est activée, l'appliance ignore tout ID NAS utilisé pour communiquer avec le serveur RADIUS.

Configurer l'authentification utilisateur RADIUS à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

Étape 1 : Créer une action RADIUS

```
add authentication radiusaction <name> -serverip <ip> -radkey <key> -
radVendorID <id> -radattributetype <value>
```

Où, attribut d'ID fournisseur
`radVendorID` RADIUS, utilisé pour l'extraction du groupe RADIUS.
`radAttributeType` Type d'attribut RADIUS, utilisé pour l'extraction du groupe RADIUS.

Exemple :

```
add authentication radiusaction RADserver531 rad_action -serverip 1.1.1.1 -
radkey key123 -radVendorID 66 -radattributetype 6
```

Étape 2 : Créez une stratégie RADIUS classique.

```
add authentication radiusPolicy <name> <rule> [<reqAction>]
```

Exemple :

```
add authentication radiuspolicy radius_pol_classic ns_true radius_act
```

> **Remarque**
>
> Vous pouvez configurer à l'aide d'une stratégie RADIUS classique ou avancée. Citrix vous recommande d'utiliser la stratégie d'authentification avancée, car les stratégies classiques sont obsolètes à partir de la version Citrix ADC 13.0.

Étape 3 : Créer une stratégie RADIUS avancée

```
add authentication policy <policyname> -rule true -action <radius action
name>
```

Exemple :

```
add authentication policy rad_pol_advanced -rule true -action radserver531rad_action
```

Étape 4 : Liez la stratégie RADIUS au système global.

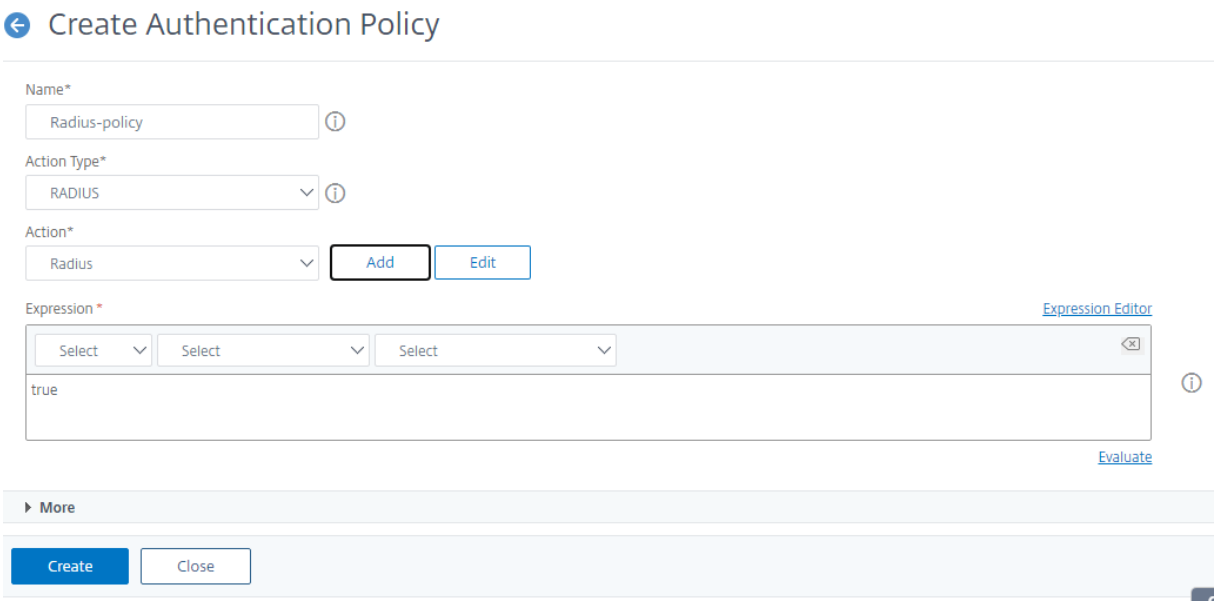
```
bind system global <policyName> -priority <positive_integer
```

Exemple :

```
bind system global radius_pol_advanced -priority 10
```

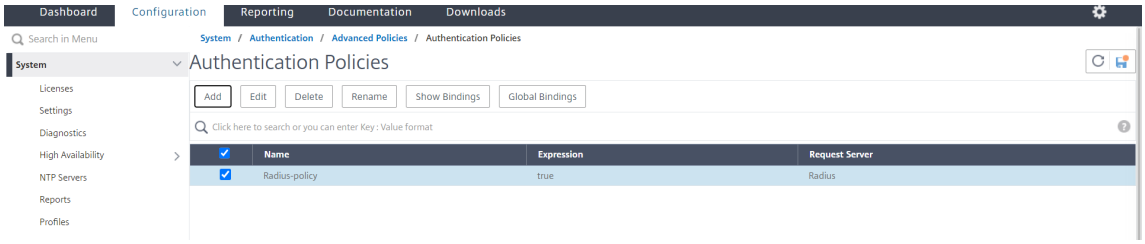
Configurer l'authentification utilisateur RADIUS à l'aide de l'interface graphique

1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégie**.
2. Cliquez sur **Ajouter** pour créer une stratégie d'authentification de type RADIUS.
3. Cliquez sur **Créer** et **Fermer**.

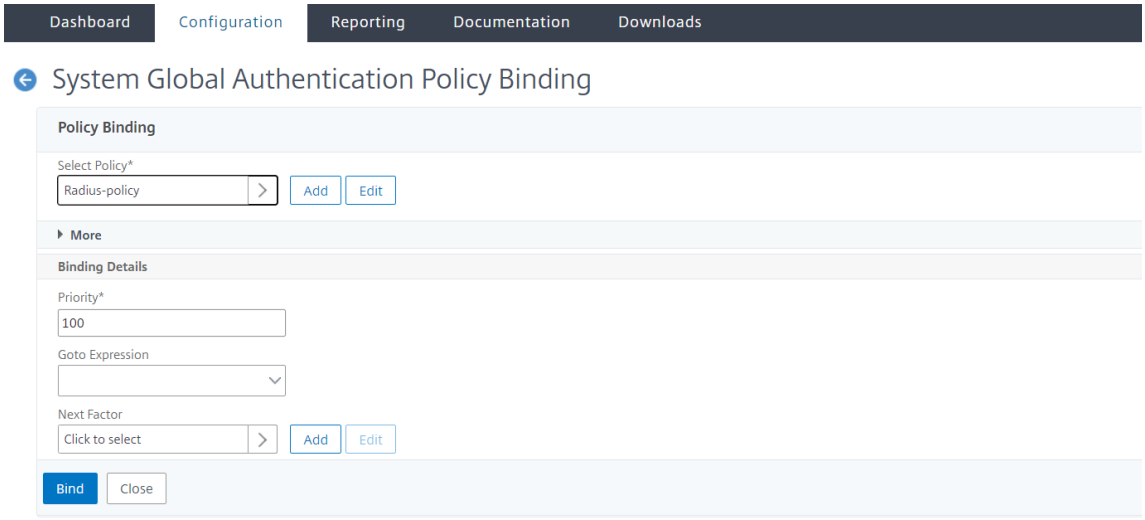


Liez la stratégie d'authentification au système global pour l'authentification RADIUS à l'aide de l'interface graphique

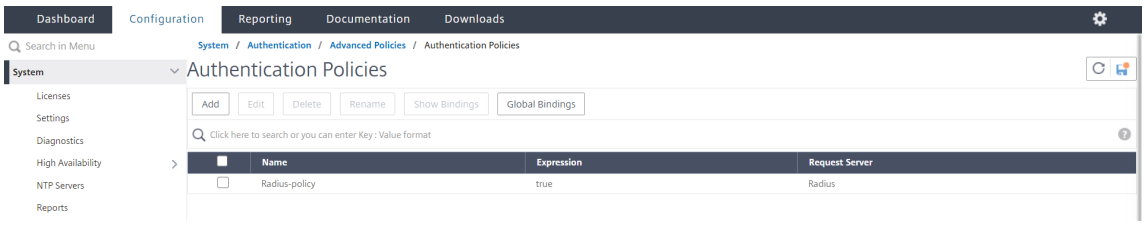
1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégie**.
2. Dans le volet d'informations, cliquez sur **Liaisons globales** pour créer une liaison de stratégie d'authentification globale système.
3. Cliquez sur **Liaisons globales**.



4. Sélectionnez RADIUS.
5. Dans la page **Liaison de stratégie d'authentification globale du système**, définissez les paramètres suivants :
   a) Sélectionnez Stratégie.
   b) Détails de liaison.



6. Cliquez sur **Lier** et **Fermer**.
7. Cliquez sur **Liaisons globales** pour confirmer la stratégie délimitée au système global.



Choisir les protocoles d'authentification utilisateur RADIUS

L'appliance Citrix ADC prend en charge les implémentations de RADIUS configurées pour utiliser l'un de plusieurs protocoles pour l'authentification utilisateur, notamment :

- Protocole d'authentification par mot de passe
- Protocole d'authentification CHAP (Challenge-Handshake Authentication Protocol)
- Protocole d'authentification Microsoft Challenge-Handshake (MS-CHAP version 1 et version 2)

Si votre déploiement est configuré pour utiliser l'authentification RADIUS et que votre serveur RADIUS est configuré avec un protocole d'authentification par mot de passe. Vous pouvez renforcer l'authentification des utilisateurs en attribuant un secret partagé fort au serveur RADIUS. Les secrets partagés RADIUS forts se composent de séquences aléatoires de lettres majuscules et minuscules, de chiffres et de ponctuation, et ont une longueur minimale de 22 caractères. Si possible, utilisez un programme de génération aléatoire de caractères pour déterminer les secrets partagés RADIUS.

Pour protéger davantage le trafic RADIUS, attribuez un secret partagé différent à chaque appliance ou serveur virtuel. Lorsque vous définissez des clients sur le serveur RADIUS, vous pouvez également attribuer un secret partagé distinct à chaque client. En outre, vous devez configurer séparément chaque stratégie qui utilise l'authentification RADIUS.

Configurer l'extraction d'adresses IP

Vous pouvez configurer l'appliance pour extraire l'adresse IP d'un serveur RADIUS. Lorsqu'un utilisateur s'authentifie auprès du serveur RADIUS, le serveur renvoie une adresse IP encadrée qui est attribuée à l'utilisateur. Voici les attributs pour l'extraction d'adresses IP :

- Permet à un serveur RADIUS distant de fournir une adresse IP à partir du réseau interne pour un utilisateur connecté à l'appliance.
- Permet la configuration de n'importe quel attribut RADIUS utilisant le type d'adresse IP, y compris ceux codés par le fournisseur.

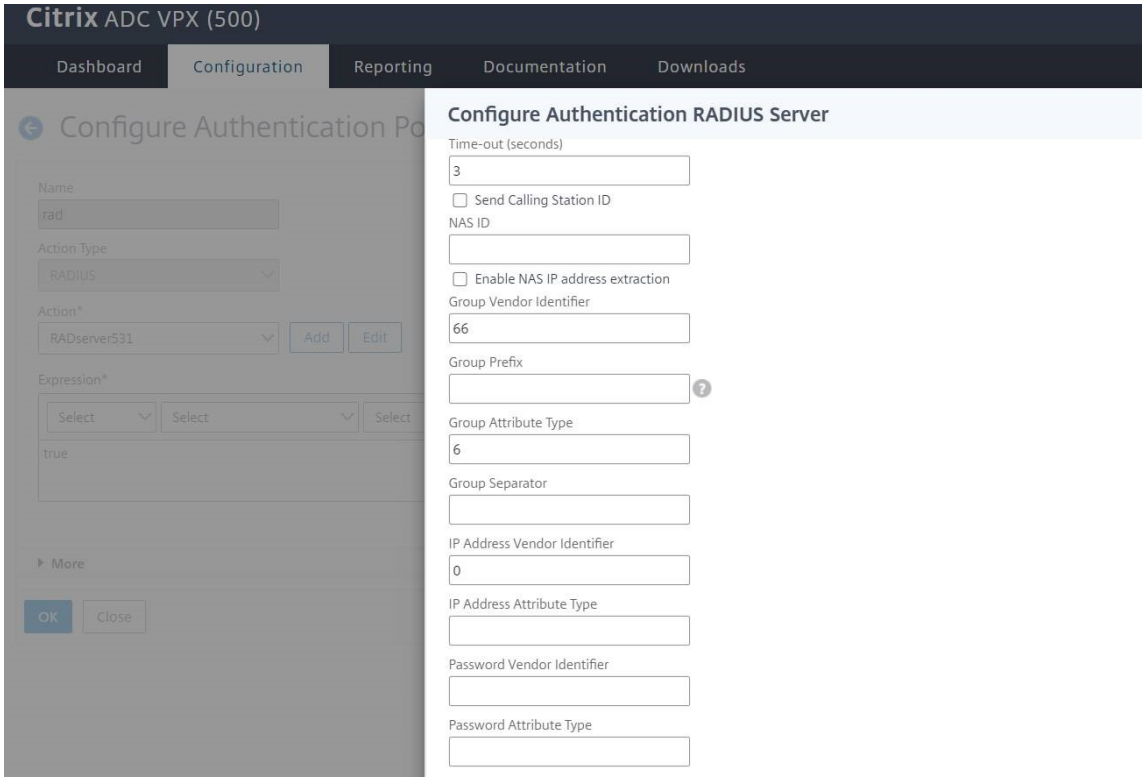
Lors de la configuration du serveur RADIUS pour l'extraction d'adresses IP, vous configurez l'identificateur fournisseur et le type d'attribut.

L'identifiant du fournisseur permet au serveur RADIUS d'attribuer une adresse IP au client à partir d'un pool d'adresses IP configurées sur le serveur RADIUS. L'ID fournisseur et les attributs sont utilisés pour établir l'association entre le client RADIUS et le serveur RADIUS. L'ID fournisseur est l'attribut de la réponse RADIUS qui fournit l'adresse IP du réseau interne. La valeur zéro indique que l'attribut n'est pas codé par le fournisseur. Le type d'attribut est l'attribut d'adresse IP distante dans une réponse RADIUS. La valeur minimale est un et la valeur maximale est 255.

Une configuration courante consiste à extraire l' *adresse IP encadrée* de l'attribut **RADIUS**. L'ID fournisseur est défini sur zéro ou n'est pas spécifié. Le type d'attribut est défini sur huit.

Groupe d'extraction pour RADIUS à l'aide de l'interface graphique

1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Rayon**, puis sélectionnez une stratégie.
2. Sélectionnez ou créez une stratégie RADIUS.
3. Dans la page **Configurer le serveur RADIUS d'authentification**, définissez les paramètres suivants.
    a) **Identificateur de fournisseur de groupe**
    b) **Type d'attribut de groupe**
4. Cliquez sur **OK** et **Fermer**.



Authentification TACACS+ (à l'aide de serveurs TACACS+ externes)

> **Important**
>
> - Citrix vous recommande de ne pas modifier les configurations associées TACACS lorsque vous exécutez une commande « clear ns config ».
> - La configuration liée à TACACS liée aux stratégies avancées est effacée et réappliquée lorsque le `RBAconfig` paramètre est défini sur NO dans la commande « clear ns config » pour la stratégie avancée.

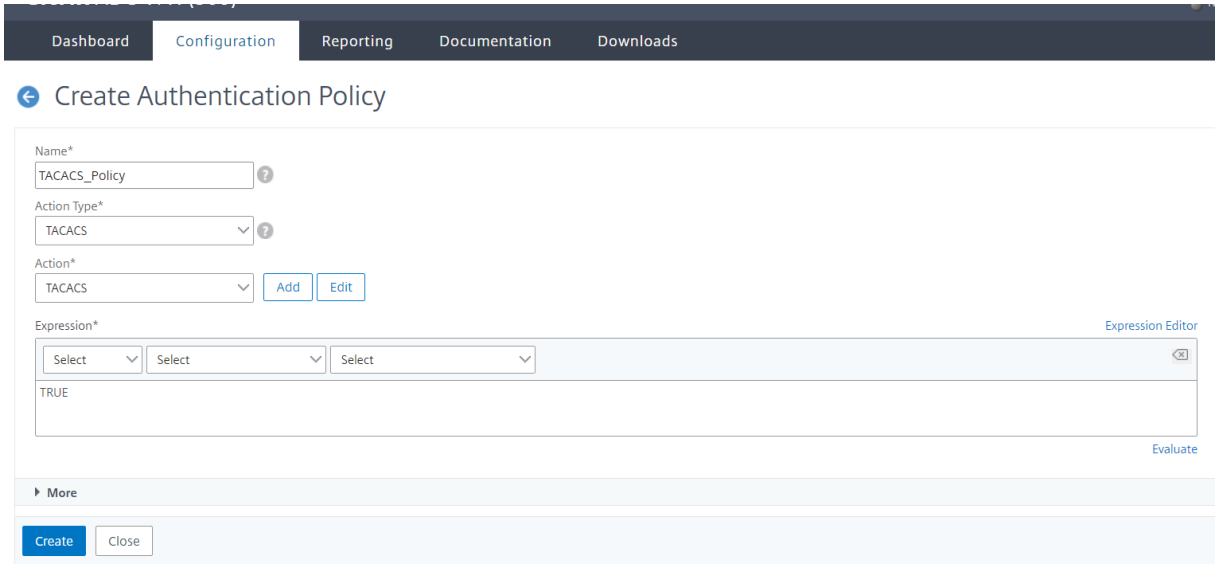
Vous pouvez configurer un serveur TACACS+ pour l'authentification. Comme pour l'authentification RADIUS, TACACS+ utilise une clé secrète, une adresse IP et le numéro de port. Le numéro de port par défaut est 49. Pour configurer l'appliance pour qu'elle utilise un serveur TACACS+, indiquez l'adresse IP du serveur et le secret TACACS+. Vous devez spécifier le port uniquement lorsque le numéro de port du serveur utilisé est autre que le numéro de port par défaut 49.

Pour plus d'informations, voir Authentification TACACS.

Configurer l'authentification TACACS+ à l'aide de l'interface graphique

1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégie**.
2. Cliquez sur **Ajouter** pour créer une stratégie d'authentification de type TACACS.

3. Cliquez sur **Créer** et **Fermer**.



Une fois les paramètres du serveur TACACS+ configurés sur l'appliance, liez la stratégie à l'entité globale du système.

Lier les stratégies d'authentification à l'entité globale du système à l'aide de l'interface de ligne de commande

Lorsque les stratégies d'authentification sont configurées, liez les stratégies à l'entité globale du système.

À l'invite de ligne de commande, procédez comme suit :

```
bind system global <policyName> [-priority <positive_integer>]
```

Exemple :

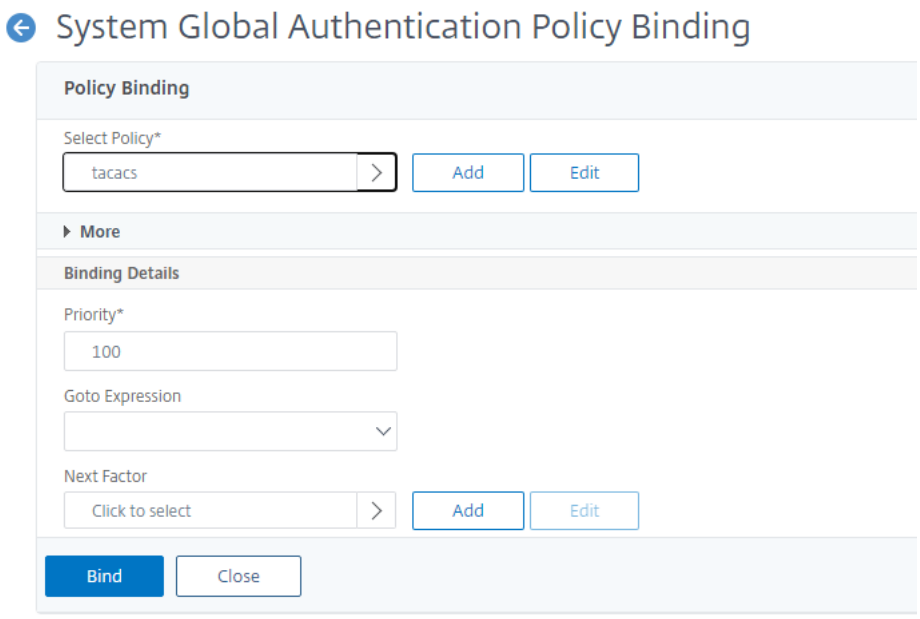
```
bind system global pol_classic -priority 10
```

Lisez également l'article de Citrix CTX113820 pour en savoir plus sur l'authentification externe à l'aide de TACACS.

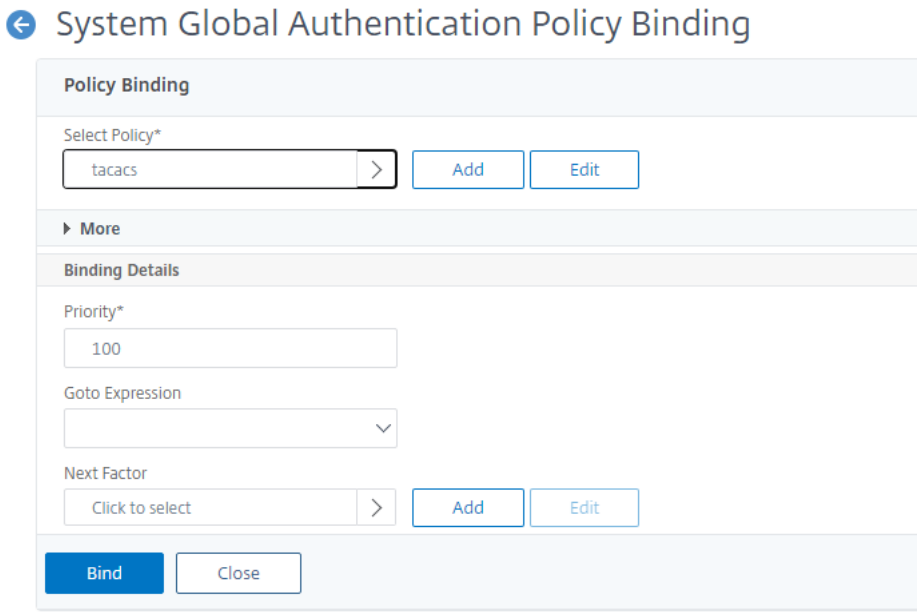
Lier les stratégies d'authentification à l'entité globale du système à l'aide de l'interface graphique

1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégies d'authentification** > **Stratégie**.
2. Dans le volet d'informations, cliquez sur **Liaisons globales** pour créer une liaison de stratégie d'authentification globale système.

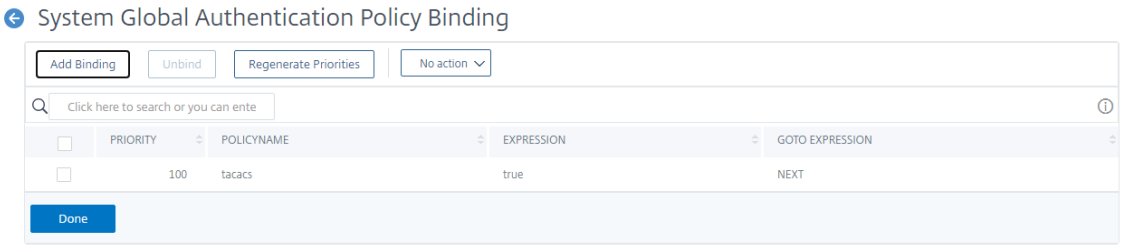
3. Cliquez sur **Liaisons globales**.



4. Sélectionnez la stratégie TACACS.
5. Dans la page Liaison de stratégie d'authentification globale système, définissez les paramètres suivants :
   a) Sélectionnez Stratégie.
   b) Détails de liaison



6. Cliquez sur **Lier** et **Fermer**.
7. Cliquez sur **Liaisons globales** pour confirmer la stratégie délimitée au système global.



Pour plus d'informations sur l'extraction de groupe TACACS, consultez l'article CTX220024de Citrix.

Afficher le nombre de tentatives d'ouverture de session infructueuses pour les utilisateurs externes

L'appliance Citrix ADC affiche le nombre de tentatives de connexion non valides à l'utilisateur externe lorsque vous tentez au moins une connexion infructueuse avant de vous connecter à la console de gestion Citrix ADC.

> **Remarque**
>
> Actuellement, Citrix prend en charge uniquement l'authentification interactive au clavier pour les utilisateurs externes avec le paramètre « PersistentLoginEssentals » activé dans le paramètre système.

À l'invite de commandes, tapez :

```
set aaa parameter -maxloginAttempts <value> -failedLoginTimeout <value> -
persistentLoginAttempts (ENABLED | DISABLED )]
```

Exemple :

```
set aaa parameter -maxloginAttempts 5 -failedLoginTimeout 4 -persistentLoginAttempts
 ENABLED
```

```
1  Following msg will be seen to external user when he tries 1 invalid
       login attempt before successfully login to the ADC management access
       .
2
3  Connection established.
4  To escape to local shell, press 'Ctrl+Alt+]'.
5  ##############################################################################
6  #
       #
7  #         WARNING: Access to this system is for authorized users only
                #
```



```
8  #         Disconnect IMMEDIATELY if you are not an authorized user!
               #
9  #
      #
10 ##############################################################################


11
12
13 WARNING! The remote SSH server rejected X11 forwarding request.
14 Last login: Mon Aug 24 17:09:00 2020 from 10.10.10.10
15
16 The number of unsuccessful login attempts since the last successful
      login : 1
17 Done
18 >
19 The number of unsuccessful login attempts since the last successful
      login : 1
20 Done
21 >
22 <!--NeedCopy-->
```

Authentification SSH basée sur des clés pour les utilisateurs du système local

August 20, 2021

Pour disposer d'un accès utilisateur sécurisé pour l'appliance Citrix ADC, vous pouvez disposer de l'authentification par clé publique du serveur SSH. L'authentification basée sur la clé SSH est préférée à l'authentification basée sur un nom d'utilisateur ou un mot de passe classique pour les raisons suivantes :

- Fournit une meilleure force cryptographique que les mots de passe utilisateur.
- Élimine la nécessité de se souvenir des mots de passe compliqués et empêche les attaques de surf sur les épaules qui sont possibles si des mots de passe sont utilisés.
- Fournit une connexion sans mot de passe pour sécuriser les scénarios d'automatisation.

Citrix ADC prend en charge l'authentification basée sur les clés SSH en appliquant le concept de clé publique et privée. L'authentification SSH basée sur la clé dans Citrix ADC peut être activée pour un utilisateur spécifique ou pour tous les utilisateurs locaux.

> **Remarque**
>
> La fonctionnalité est prise en charge uniquement pour les utilisateurs locaux Citrix ADC et n'est pas prise en charge pour les utilisateurs externes.

Authentification SSH basée sur des clés pour les utilisateurs du système local

Dans une appliance Citrix ADC, un administrateur peut configurer l'authentification basée sur la clé SSH pour un accès système sécurisé. Lorsqu'un utilisateur se connecte au Citrix ADC à l'aide d'une clé privée, le système authentifie l'utilisateur à l'aide de la clé publique configurée sur l'appliance.

Configurer l'authentification SSH basée sur la clé pour les utilisateurs du système local Citrix ADC à l'aide de l'interface de ligne de commande

La configuration suivante vous aide à configurer l'authentification basée sur des clés pour les utilisateurs du système local Citrix ADC.

1. Ouvrez une session sur une appliance Citrix ADC à l'aide des informations d'identification de l'administrateur.
2. Par défaut, votre fichier `sshd_config` accède à ce chemin : **authorizedKeysFile /nsconfig/ssh/authorized_keys**.
3. Ajoutez la clé publique au fichier authorized_keys : **/nsconfig/ssh/authorized_keys**. Le chemin d'accès du fichier pour `sshd_config` est `/etc/sshd_config`.
4. Copiez le fichier `sshd_config` dans `/nsconfig` pour vous assurer que les modifications persistent même après le redémarrage de l'appliance.
5. Vous pouvez utiliser la commande suivante pour redémarrer votre processus `sshd`.

```
1     kill -HUP `cat /var/run/sshd.pid`
2 <!--NeedCopy-->
```

> **Remarque**
>
> Si le fichier authorized_keys n'est pas disponible, vous devez d'abord en créer un, puis ajouter la clé publique. **Assurez-vous que le fichier dispose de l'autorisation suivante pour les keys authorized_keys**.
>
> ```
> root@Citrix ADC## chmod 0644 authorized_keys
> ```

```
1 > shell
2 Copyright (c) 1992-2013 The FreeBSD Project.
3 Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
     1994
4 The Regents of the University of California. All rights reserved.
5 root@ns# cd /nsconfig/ssh
```



```
root@ns# vi authorized_keys
### Add public keys in authorized_keys file
<!--NeedCopy-->
```

Authentification SSH spécifique à l'utilisateur pour les utilisateurs du système local

Dans une appliance Citrix ADC, un administrateur peut désormais configurer une authentification basée sur une clé SSH spécifique à l'utilisateur pour un accès système sécurisé. L'administrateur doit d'abord configurer l'option `Authorizedkeysfile` dans le fichier `sshd_config`, puis ajouter la clé publique dans le fichier `authorized_keys` pour un utilisateur système.

> **Remarque**
>
> Si le fichier authorized_keys n'est pas disponible pour un utilisateur, l'administrateur doit d'abord en créer un, puis y ajouter la clé publique.

Configurer l'authentification basée sur la clé SSH spécifique à l'utilisateur à l'aide de l'interface de ligne de commande

La procédure suivante vous aide à configurer l'authentification basée sur la clé SSH spécifique à l'utilisateur pour les utilisateurs du système local Citrix ADC.

1. Ouvrez une session sur une appliance Citrix ADC à l'aide des informations d'identification de l'administrateur.
2. À l'invite shell, accédez au fichier `sshd_config` et ajoutez la ligne de configuration suivante :

   `AuthorizedKeysFile ~/.ssh/authorized_keys`

   > **Remarque**
   >
   > Le ~ est le répertoire personnel et diffère selon les utilisateurs. Il s'étend aux différents répertoires d'accueil.

3. Modifiez le répertoire en dossier utilisateur système et ajoutez les clés publiques dans le `authorized_keys` fichier.

   `/var/pubkey/<username>/.ssh/authorized_keys`

Une fois que vous avez terminé les étapes précédentes, redémarrez le processus `sshd` sur votre appliance à l'aide de la commande suivante :

```
    kill -HUP `cat /var/run/sshd.pid`

<!--NeedCopy-->
```


> **Remarque**
>
> Si le fichier authorized_keys n'est pas disponible, vous devez d'abord en créer un, puis ajouter la clé publique.

```
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
    1994
The Regents of the University of California. All rights reserved.
root@ns# cd /var/pubkey/<username>/
root@ns# ls
.ssh
root@ns# cd .ssh
root@ns# vi authorized_keys
### Add public keys in authorized_keys file

<!--NeedCopy-->
```

Lisez également l'article CTX109011 de Citrix pour savoir comment fonctionne l'accès SSH sécurisé à l'appliance Citrix ADC.

Authentification à deux facteurs pour les utilisateurs système et les utilisateurs externes

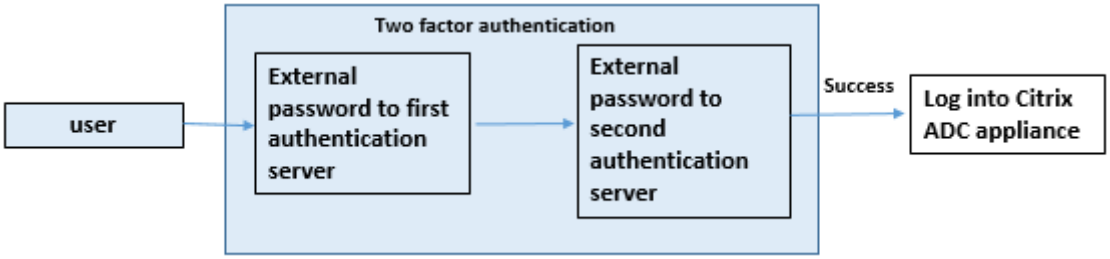
August 20, 2021

L'authentification à deux facteurs est un mécanisme de sécurité dans lequel une appliance Citrix ADC authentifie un utilisateur système à deux niveaux d'authentificateur. L'appliance n'autorise l'accès à l'utilisateur qu'après validation réussie des mots de passe par les deux niveaux d'authentification. Si un utilisateur est authentifié localement, le profil utilisateur doit être créé dans la base de données Citrix ADC. Si l'utilisateur est authentifié en externe, le nom d'utilisateur et le mot de passe doivent correspondre à l'identité utilisateur enregistrée sur le serveur d'authentification externe.

> **Remarque**
>
> La fonctionnalité d'authentification à deux facteurs fonctionne uniquement à partir de Citrix ADC 12.1 build 51.16.

Fonctionnement de l'authentification à deux facteurs

Envisagez un utilisateur qui tente de se connecter à une appliance Citrix ADC. Le serveur d'applications demandé envoie le nom d'utilisateur et le mot de passe au premier serveur d'authentification externe (RADIUS, TACACS, LDAP ou AD). Une fois le nom d'utilisateur et le mot de passe validés, l'utilisateur est invité à entrer un deuxième niveau d'authentification. L'utilisateur peut désormais fournir le deuxième mot de passe. Uniquement si les deux mots de passe sont corrects, l'utilisateur est autorisé à accéder à l'appliance Citrix ADC. Le diagramme suivant illustre le fonctionnement de l'authentification à deux facteurs pour une appliance Citrix ADC.



Voici les différents cas d'utilisation pour configurer l'authentification à deux facteurs pour les utilisateurs externes et système.

Vous pouvez configurer l'authentification à deux facteurs sur une appliance Citrix ADC de différentes manières. Voici les différents scénarios de configuration pour l'authentification à deux facteurs sur une appliance Citrix ADC.

1. Authentification à deux facteurs (2FA) sur Citrix ADC, GUI, CLI, API et SSH.
2. Authentification externe activée et authentification locale désactivée pour les utilisateurs système.
3. Authentification externe activée avec l'authentification locale basée sur des stratégies pour les utilisateurs système.
4. Authentification externe désactivée pour les utilisateurs système avec l'authentification locale activée.
5. Authentification externe activée et authentification locale activée pour les utilisateurs système.
6. Authentification externe activée pour les utilisateurs LDAP sélectionnés

Cas d'utilisation 1 : authentification à deux facteurs (2FA) sur les interfaces Citrix ADC, GUI, CLI, API et SSH

L'authentification à deux facteurs est activée et disponible sur tous les accès de gestion Citrix ADC pour l'interface graphique, l'API et le SSH.

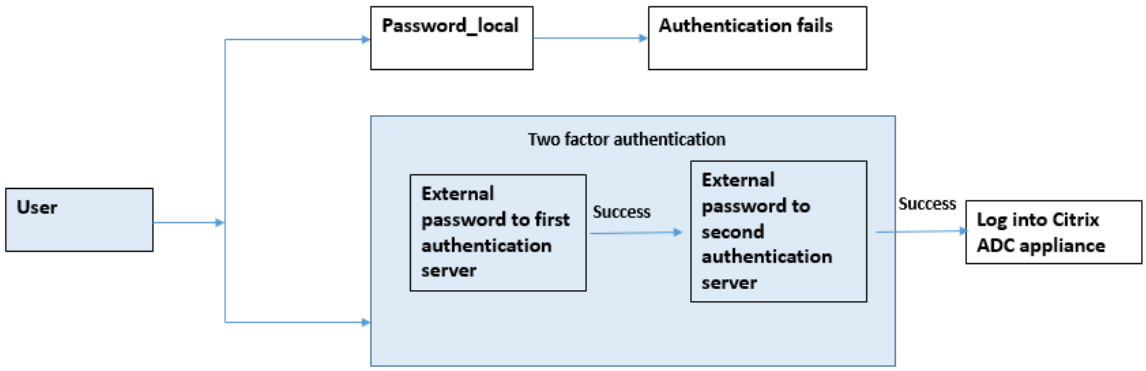
Cas d'utilisation 2 : authentification à deux facteurs prise en charge sur des serveurs d'authentification externes tels que LDAP, RADIUS, Active Directory et TACACS

Vous pouvez configurer l'authentification à deux facteurs sur les serveurs d'authentification externes suivants pour l'authentification utilisateur de premier et de deuxième niveau.

- RADIUS
- LDAP
- Active Directory
- TACACS

Cas d'utilisation 3 : Authentification externe activée et authentification locale désactivée pour les utilisateurs système

Vous démarrez le processus d'authentification en activant l'option d'authentification externe et en désactivant l'authentification locale pour les utilisateurs système.



Procédez comme suit à l'aide de l'interface de ligne de commande :

1. Ajouter une action d'authentification pour la stratégie LDAP
2. Ajouter une stratégie d'authentification pour la stratégie LDAP
3. Ajouter une action d'authentification pour la stratégie RADIUS
4. Ajouter une stratégie d'authentification pour la stratégie RADIUS
5. Ajouter un schéma de connexion d'authentification
6. Ajouter et lier l'étiquette de stratégie d'authentification au serveur RADIUS
7. Lier l'authentification globale du système pour la stratégie LDAP
8. Désactiver l'authentification locale dans le paramètre système

Ajouter une action d'authentification pour le serveur LDAP (authentification de premier niveau)

À l'invite de commandes, tapez :


```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname <
loginname> -groupattrname <grp attribute name> -subAttributename <string>-
ssoNameAttribute <string>
```

Exemple :

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Ajouter une stratégie d'authentification pour le serveur LDAP (authentification de premier niveau)

À l'invite de commandes, tapez :

```
add authentication policy <ldap policy name> -rule true -action <ldap
action name>
```

Exemple :

```
add authentication policy pol1 -rule true -action ldapact1
```

Ajouter une action d'authentification pour le serveur RADIUS (authentification de deuxième niveau)

À l'invite de commandes, tapez :

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Exemple :

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Ajouter une stratégie d'authentification pour le serveur RADIUS (authentification de deuxième niveau)

À l'invite de commandes, tapez :

```
add authentication policy <radius policy name> -rule true -action <rad
action name>
```

Exemple :

```
add authentication policy radpol11 -rule true -action radact1
```


Ajouter un schéma de connexion d'authentification

Vous pouvez utiliser le schéma de connexion « SingleAuth.xml » pour les utilisateurs système afin de fournir le deuxième mot de passe de l'appliance Citrix ADC. À l'invite de commandes, tapez :

```
add authentication loginSchema <login schema name> -authenticationSchema
LoginSchema/SingleAuth.xml
```

Exemple :

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Ajouter et lier l'étiquette de stratégie d'authentification au serveur RADIUS

À l'invite de commandes, tapez :

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

```
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Exemple :

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
```

```
bind authentication policylabel label1 -policyName radpol11 -priority 1
```

Lier le système d'authentification global pour la stratégie LDAP

À l'invite de commandes, tapez :

```
bind system global ldappolicy -priority <priority> -nextFactor <policy
label name>
```

Exemple :

```
bind system global pol11 -priority 1 -nextFactor label1
```

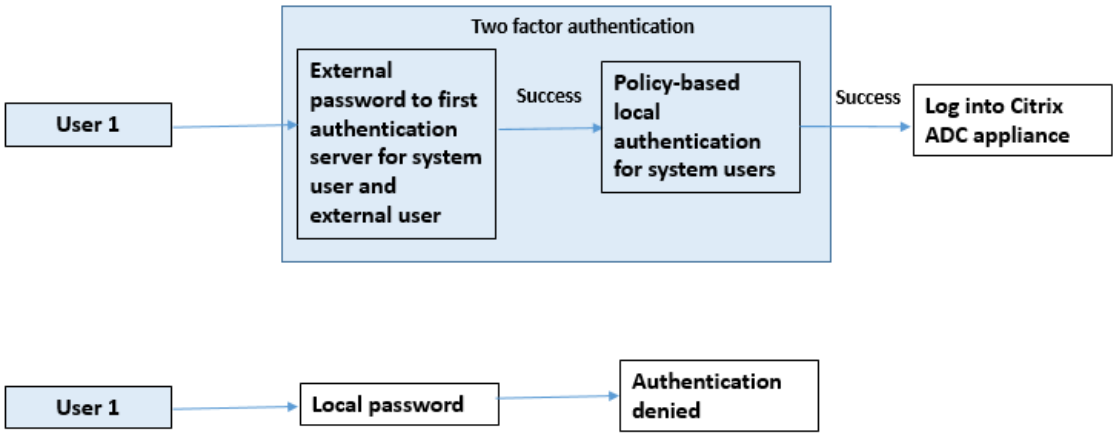
Désactiver l'authentification locale dans le paramètre système

À l'invite de commandes, tapez :

```
set system parameter -localauth disabled
```


Cas d'utilisation 4 : Authentification externe activée pour l'utilisateur système avec une stratégie d'authentification locale attachée

Dans ce scénario, l'utilisateur est autorisé à ouvrir une session à l'aide de l'authentification à deux facteurs avec l'évaluation de la stratégie d'authentification locale au deuxième niveau d'identification de l'utilisateur.



Procédez comme suit à l'aide de l'interface de ligne de commande.

1. Ajouter une action d'authentification pour le serveur LDAP
2. Ajouter une stratégie d'authentification pour la stratégie LDAP
3. Ajouter une stratégie d'authentification locale
4. Ajouter une étiquette de stratégie d'authentification
5. Lier la stratégie LDAP en tant que système global
6. Désactiver l'authentification locale dans le paramètre système

Ajouter une action d'authentification pour le serveur LDAP (authentification de premier niveau)

À l'invite de commandes, tapez :

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname <
loginname> -groupattrname <grp attribute name> -subAttributename <string>-
ssoNameAttribute <string>
```

Exemple :

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name -ssoNameAttribute name
```


Ajouter une stratégie d'authentification pour le serveur LDAP (authentification de premier niveau)

À l'invite de commandes, tapez :

```
add authentication policy <ldap policy name> -rule true -action <ldap
action name>
```

Exemple :

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Ajouter une stratégie d'authentification locale pour les utilisateurs système (authentification de deuxième niveau)

À l'invite de commandes, tapez :

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type
```

Exemple :

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Ajouter et lier l'étiquette de stratégie d'authentification

À l'invite de commandes, tapez :

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Exemple :

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel label1 -policyName radpol11 -priority 1 -
gotoPriorityExpression NEXT
```

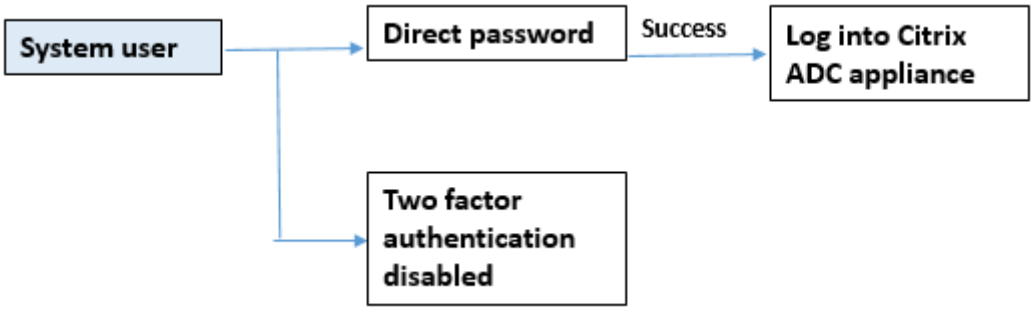
Désactiver l'authentification locale dans le paramètre système

À l'invite de commandes, tapez :

```
set system parameter -localauth disabled
```


Cas d'utilisation 5 : Authentification externe désactivée et authentification locale activée pour l'utilisateur système

Si l'utilisateur a « ExternalAuth » désactivé, cela indique que l'utilisateur n'existe pas sur le serveur d'authentification. L'utilisateur n'est pas authentifié auprès du serveur d'authentification externe même si un utilisateur portant le même nom d'utilisateur existe sur le serveur authentifié externe. L'utilisateur est authentifié localement.



Pour activer le mot de passe utilisateur système et désactiver l'authentification externe

À l'invite de commandes, tapez ce qui suit :

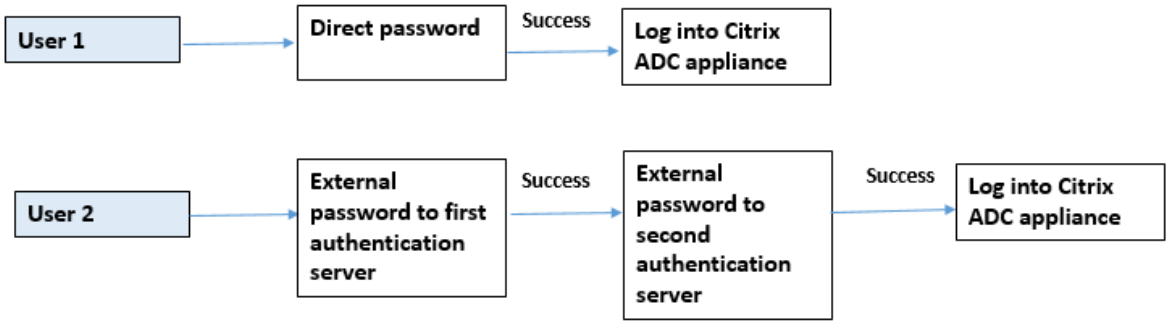
```
add system user <name> <password> -externalAuth DISABLED
```

Exemple :

```
add system user user1 password1 -externalAuth DISABLED
```

Cas d'utilisation 6 : Authentification externe activée et authentification locale activée pour les utilisateurs système

Pour configurer l'appliance pour authentifier les utilisateurs système à l'aide d'un mot de passe local. Si cette authentification échoue, l'utilisateur est alors authentifié à l'aide d'un mot de passe d'authentification externe sur les serveurs d'authentification externes à deux niveaux.



Configurez les étapes suivantes à l'aide de l'interface de ligne de commande.

1. Ajouter une action d'authentification pour le serveur LDAP
2. Ajouter une stratégie d'authentification pour la stratégie LDAP
3. Ajouter une action d'authentification pour la stratégie RADIUS
4. Ajouter une stratégie d'authentification pour la stratégie RADIUS
5. Ajouter un schéma de connexion d'authentification
6. Ajouter une étiquette de stratégie d'authentification
7. Libellé de stratégie d'authentification de liaison pour le schéma de connexion
8. Lier le système d'authentification global pour la stratégie RADIUS
9. Lier le système d'authentification global pour la stratégie LDAP

Ajouter une action d'authentification pour le serveur LDAP

À l'invite de commandes, tapez :

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
ssoNameAttribute <>
```

Exemple :

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Ajouter une stratégie d'authentification pour la stratégie LDAP

À l'invite de commandes, tapez :

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Exemple :

```
add authentication policy pol1 -rule true -action ldapact1
```

Ajouter une action d'authentification pour le serveur RADIUS

À l'invite de commandes, tapez :

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Exemple :


```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Ajouter une stratégie d'authentification avancée pour le serveur RADIUS

À l'invite de commandes, tapez :

```
add authentication policy <policy name> -rule true -action <rad action name
>
```

Exemple :

```
add authentication policy radpol11 -rule true -action radact1
```

Ajouter un schéma de connexion d'authentification

Vous pouvez utiliser le schéma de connexion SingleAuth.xml pour afficher la page de connexion et authentifier l'utilisateur système à l'authentification de deuxième niveau.

À l'invite de commandes, tapez :

```
add authentication loginSchema <name> -authenticationSchema <string>
```

Exemple :

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Ajouter et lier l'étiquette de stratégie d'authentification à la stratégie d'authentification RADIUS pour la connexion de l'utilisateur

À l'invite de commandes, tapez :

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

Exemple :

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Exemple :

```
bind authentication policylabel label1 -policyName rad pol11 -priority 1
```


Stratégie d'authentification de liaison globale

À l'invite de commandes, tapez :

```
bind system global [<policyName> [-priority <positive_integer>] [-nextFactor
 <string>] [-gotoPriorityExpression <expression>]]
```

Exemple :

```
bind system global radpol11 -priority 1 -nextFactor label11
```

Cas d'utilisation 7 : Authentification externe activée pour les utilisateurs externes sélectionnés uniquement

Pour configurer des utilisateurs externes sélectifs avec une authentification à deux facteurs conformément au filtre de recherche configuré dans l'action LDAP tandis que les autres utilisateurs système sont authentifiés à l'aide de l'authentification à facteur unique.

Configurez les étapes suivantes à l'aide de l'interface de ligne de commande.

1. Ajouter une action d'authentification pour le serveur LDAP
2. Ajouter une stratégie d'authentification pour la stratégie LDAP
3. Ajouter une action d'authentification pour la stratégie RADIUS
4. Ajouter une stratégie d'authentification pour la stratégie RADIUS
5. Ajouter un schéma de connexion d'authentification
6. Ajouter une étiquette de stratégie d'authentification
7. Libellé de stratégie d'authentification de liaison pour le schéma de connexion
8. Lier le système d'authentification global pour la stratégie RADIUS

Ajouter une action d'authentification pour le serveur LDAP

À l'invite de commandes, tapez :

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
ssoNameAttribute <>
```

Exemple :

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```


Ajouter une stratégie d'authentification pour la stratégie LDAP

À l'invite de commandes, tapez :

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Exemple :

```
add authentication policy pol1 -rule true -action ldapact1
```

Ajouter une action d'authentification pour le serveur RADIUS

À l'invite de commandes, tapez :

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Exemple :

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Ajouter une stratégie d'authentification avancée pour le serveur RADIUS

À l'invite de commandes, tapez :

```
add authentication policy <policy name> -rule true -action <rad action name
>
```

Exemple :

```
add authentication policy radpol11 -rule true -action radact1
```

Ajouter un schéma de connexion d'authentification

Vous pouvez utiliser le schéma de connexion SingleAuth.xml pour fournir la page de connexion permettant à l'appliance d'authentifier un utilisateur système à un deuxième niveau d'authentification.

À l'invite de commandes, tapez :

```
add authentication loginSchema <name> -authenticationSchema <string>
```

Exemple :

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```


Ajouter et lier l'étiquette de stratégie d'authentification à la stratégie d'authentification RADIUS pour la connexion de l'utilisateur

À l'invite de commandes, tapez :

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

Exemple :

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Exemple :

```
bind authentication policylabel label1 -policyName radpol11 -priority
```

Stratégie d'authentification de liaison globale

À l'invite de commandes, tapez :

```
bind system global [<policyName> [-priority <positive_integer>] [-nextFactor
 <string>] [-gotoPriorityExpression <expression>]]
```

Exemple :

```
bind system global radpol11 -priority 1 -nextFactor label11
```

Pour configurer sans authentification à deux facteurs pour les utilisateurs de groupe à l'aide du filtre de recherche :

1. Ajouter une action d'authentification pour le serveur LDAP
2. Ajouter une stratégie d'authentification pour le serveur LDAP
3. Lier le système d'authentification global pour le serveur LDAP

Ajouter une action d'authentification pour le serveur LDAP

À l'invite de commandes, tapez :

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
searchFilter<>
```

Exemple :


```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name - searchFilter "memberOf=CN=grp4,CN=Users,DC=
aaatm-test,DC=com"
```

Ajouter une stratégie d'authentification pour le serveur LDAP

À l'invite de commandes, tapez :

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Exemple :

```
add authentication policy pol1 -rule true -action ldapact1
```

Lier le système d'authentification global pour la stratégie LDAP

À l'invite de commandes, tapez :

```
bind system global ldappolicy -priority <priority> -nextFactor <policy
label name>
```

Exemple :

```
bind system global pol11 -priority 1 -nextFactor label11
```

Afficher le message d'invite personnalisé pour l'authentification à deux facteurs

Lorsque vous configurez le champ de mot de passe à deux facteurs avec le fichier SingleAuth.xml à /flash/nsconfig/loginschema/LoginSchema

Voici l'extrait d'un fichier SingleAuth.xml où 'SecondPassword : 'est le deuxième nom de champ de mot de passe qui est invité à l'utilisateur d'entrer un second mot de passe.

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <AuthenticateResponse xmlns="http://citrix.com/authentication/response
       /1">
3  <Status>success</Status>
4  <Result>more-info</Result>
5  <StateContext/>
6  <AuthenticationRequirements>
7  <PostBack>/nf/auth/doAuthentication.do</PostBack>
8  <CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
9  <CancelButtonText>Cancel</CancelButtonText>
10 <Requirements>
```

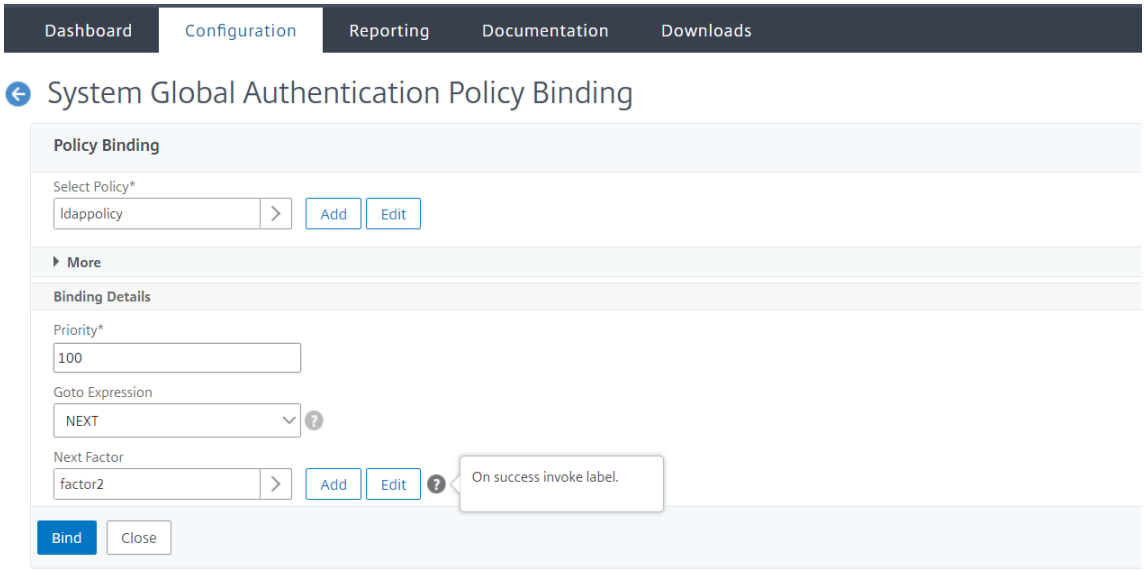


```
<Requirement><Credential><ID>login</ID><SaveID>ExplicitForms-Username</SaveID><Type>username</Type></Credential><Label><Text>singleauth_user_name</Text><Type>nsg-login-label</Type></Label><Input><AssistiveText>singleauth_please_supply_either_domain\username_or_user@fully.qualified.domain</AssistiveText><Text><Secret>false</Secret><ReadOnly>false</ReadOnly><InitialValue/><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password</SaveID><Type>password</Type></Credential><Label><Text>SecondPassword:</Text><Type>nsg-login-label</Type></Label><Input><Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue/><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>singleauth_first_factor</Text><Type>nsg_confirmation</Type></Label><Input/></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials</Type></Credential><Label><Text>singleauth_remember_my_password</Text><Type>nsg-login-label</Type></Label><Input><CheckBox><InitialValue>false</InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential><Label><Type>none</Type></Label><Input><Button>singleauth_log_on</Button></Input></Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

Configuration de l'authentification à deux facteurs à l'aide de l'interface graphique Citrix ADC

1. Connectez-vous à l'appliance Citrix ADC.
2. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégie**.
3. Cliquez sur Ajouter pour créer la stratégie d'authentification de premier niveau.
4. Dans la page **Créer une stratégie d'authentification**, définissez les paramètres suivants.
   a) Nom. Nom de la stratégie
   b) Type d'action. Sélectionnez le type d'action comme LDAP, Active Directory, RADIUS, TACACS, etc.
   c) Action. Action d'authentification (profil) à associer à la stratégie. Vous pouvez choisir une action d'authentification existante, ou cliquer sur le plus et créer une action du type approprié.
   d) Expression. Fournissez une expression de stratégie avancée.

5. Cliquez sur **Créer**, puis sur **Fermer**.
    a) Expression. Fournissez une expression de stratégie avancée.
6. Cliquez sur **Créer**.
7. Cliquez sur **Ajouter** pour créer la stratégie d'authentification de deuxième niveau.
8. Dans la page **Créer une stratégie d'authentification**, définissez les paramètres suivants
    a) Nom. Nom de la stratégie
    b) Type d'action. Sélectionnez le type d'action comme LDAP, Active Directory, RADIUS, TACACS, etc.
    c) Action. Action d'authentification (profil) à associer à la stratégie. Vous pouvez choisir une action d'authentification existante ou cliquer sur l'icône + pour créer une action du type approprié.
    d) Expression. Fournir une expression de stratégie avancée
9. Cliquez sur **Créer**, puis sur **Fermer**.
    a) Expression. Fournissez une expression de stratégie avancée.
10. Cliquez sur **Créer**.
11. Dans la page **Stratégies d'authentification**, cliquez sur **Liaison globale**.
12. Dans la page **Créer une liaison de stratégie d'authentification globale**, sélectionnez la stratégie d'authentification de premier niveau, puis cliquez sur **Ajouter une liaison**.
13. Dans la page **Liaison de stratégie**, sélectionnez la stratégie d'authentification et définissez le paramètre de liaison de stratégie suivant.
    a) Facteur suivant. Sélectionnez l'étiquette de stratégie d'authentification de deuxième niveau.
14. Cliquez sur **Lier** et **Fermer**.



15. Cliquez sur **Terminé**.
16. Connectez-vous à l'appliance Citrix ADC pour l'authentification de deuxième niveau. L'utilisateur peut désormais fournir le deuxième mot de passe. Uniquement si les deux mots de passe sont corrects, l'utilisateur est autorisé à accéder à l'appliance Citrix ADC.

> **Remarque**
>
> Le TACACS configuré pour une authentification de second facteur ne prend pas en charge l'autorisation et la comptabilité même si vous l'activez sur la commande « TacacsAction ». Le deuxième facteur est utilisé uniquement à des fins d'authentification.

Consultez également la rubrique Authentification à deux facteurs dans la rubrique Authentification Citrix ADC nFactor .

Authentification restreinte des utilisateurs système aux interfaces de gestion Citrix ADC

August 20, 2021

Vous pouvez restreindre l'accès des utilisateurs système à des interfaces de gestion Citrix ADC spécifiques telles que CLI ou API. Le `allowedManagementInterface` paramètre définit la liste des interfaces de gestion autorisées. Par exemple, si l'interface de gestion d'un utilisateur ou d'un groupe est définie sur API, tous les utilisateurs du groupe peuvent accéder à Citrix ADC via API et non via CLI. Toutefois, l'interface graphique Citrix ADC fait partie de l'interface API et les utilisateurs disposant de l'autorisation API peuvent également accéder à l'interface GUI.

> **Remarque :**
>
> Par défaut, les utilisateurs et les groupes ont accès à toutes les interfaces (CLI, API et interface graphique).

Vous pouvez configurer le paramètre au niveau de l'utilisateur ou au niveau du groupe d'utilisateurs. Lorsque vous configurez au niveau du groupe, la configuration est appliquée à tous les comptes d'utilisateurs du groupe. Si un utilisateur est lié à plusieurs groupes, l'appliance autorise l'accès à un ensemble agrégé d'interfaces de gestion. Vous pouvez spécifier les paramètres d'un utilisateur d'un groupe en configurant le paramètre au niveau de l'utilisateur. Dans ce cas, le paramètre de niveau utilisateur est configuré pour un groupe.
Dans certains scénarios, lorsque le client utilise un serveur d'authentification externe pour gérer les comptes d'utilisateurs, les détails du serveur sont configurés sur l'appliance. Dans ce cas, l'administrateur peut créer un groupe d'utilisateurs dans l'appliance Citrix ADC et ajouter tous les utilisateurs (regroupés dans le serveur externe) au groupe. Par exemple, tous les utilisateurs gérés sur le serveur externe sont ajoutés au groupe API_Users et l'administrateur peut configurer le groupe localement sur l'appliance.

> **Remarque :**
>
> L'appliance Citrix ADC autorise uniquement `nsroot` l'administrateur (superutilisateur) à configurer le paramètre et n'autorise aucun utilisateur système à modifier le paramètre.

Configurer l'accès utilisateur aux interfaces de gestion Citrix ADC à l'aide de l'interface de ligne de commande

Pour autoriser l'accès utilisateur à une interface de gestion spécifique, vous devez définir le paramètre d'interface de gestion autorisé. À l'invite de commandes, tapez :

```
set system group <groupName> [-allowedManagementInterface ( CLI | API )]
```

Exemple :

```
set system group network_usergroup -allowedManagementInterface CLI
```

Pour la description des paramètres, reportez-vous à la rubrique Référence des commandes d'authentification et d'autorisation .

Pour en savoir plus sur l'interface graphique Citrix et les interfaces CLI, consultez la rubrique Access Citrix ADC .

Configurations TCP

October 5, 2021

Les configurations TCP d'une appliance Citrix ADC peuvent être spécifiées dans une entité appelée profil TCP, qui est un ensemble de paramètres TCP. Le profil TCP peut ensuite être associé à des services ou à des serveurs virtuels qui souhaitent utiliser ces configurations TCP.

Un profil TCP par défaut peut être configuré pour définir les configurations TCP qui seront appliquées par défaut, globalement à tous les services et serveurs virtuels.

> **Remarque :**
>
> Lorsqu'un paramètre TCP a des valeurs différentes pour le service, le serveur virtuel et globalement, la valeur de l'entité la plus spécifique (le service) est donnée la priorité la plus élevée. L'appliance Citrix ADC propose également d'autres approches de configuration de TCP. Lisez la suite pour plus d'informations.

Configuration TCP prise en charge

L'appliance Citrix ADC prend en charge les fonctionnalités TCP suivantes :

Défendre TCP contre les attaques par usurpation d'identité

L' **implémentation Citrix ADC de l'atténuation des** fenêtres est conforme à la norme RFC 4953.

Notification explicite de congestion (ECN)

La solution matérielle-logicielle envoie une notification de l'état de congestion du réseau à l'expéditeur des données et prend des mesures correctives en cas d'encombrement ou de corruption des données. L'implémentation Citrix ADC d'ECN est conforme à la norme RFC 3168.

Mesure du temps aller-retour (RTTM) à l'aide de l'option d'horodatage

Pour que l'option TimeStamp fonctionne, au moins un côté de la connexion (client ou serveur) doit la prendre en charge. L'implémentation Citrix ADC de l' `TimeStamp` option est conforme à la norme RFC 1323.

Détection de retransmissions fausses

Cela peut être fait à l'aide de l'accusé de réception sélectif en double TCP (D-SACK) et de récupération RTO (F-RTO). S'il y a des retransmissions fausses, les configurations de contrôle de congestion sont rétablies à leur état d'origine. L'implémentation Citrix ADC de D-SACK est conforme à la RFC 2883 et F-RTO est conforme à la RFC 5682.

Contrôle de la congestion

Cette fonctionnalité utilise les algorithmes New-Reno, BIC, CUBIC, Nile et TCP Westwood.

Mise à l'échelle des fenêtres

Cela augmente la taille de la fenêtre de **réception TCP** au-delà de sa valeur maximale de 65 535 octets.

Points à prendre en compte avant de configurer la mise à l'échelle des fenêtres

- Vous ne définissez pas de valeur élevée pour le facteur d'échelle, car cela pourrait avoir des effets négatifs sur la solution matérielle-logicielle et le réseau.
- Vous ne configurez pas la mise à l'échelle des fenêtres à moins de savoir clairement pourquoi vous souhaitez modifier la taille de la fenêtre.
- Les deux hôtes de la connexion TCP envoient une option d'échelle de fenêtre lors de l'établissement de la connexion. Si un seul côté d'une connexion définit cette option, la mise à l'échelle des fenêtres n'est pas utilisée pour la connexion.
- Chaque connexion pour la même session est une session de mise à l'échelle des fenêtres indépendante. Par exemple, lorsque la demande d'un client et la réponse du serveur passent par l'appliance, il est possible de mettre à l'échelle des fenêtres entre le client et l'appliance sans mise à l'échelle des fenêtres entre l'appliance et le serveur.

Fenêtre de congestion maximale TCP

La taille de la fenêtre est configurable par l'utilisateur. La valeur par défaut est de 8 190 octets.

Accusé de réception sélectif (SACK)

Cela utilise le récepteur de données (un dispositif Citrix ADC ou un client) qui informe l'expéditeur de tous les segments qui ont été reçus avec succès.

Accusé de réception avant (FACK)

Cette fonctionnalité évite la congestion TCP en mesurant explicitement le nombre total d'octets de données en attente sur le réseau et en aidant l'expéditeur (Citrix ADC ou client) à contrôler la quantité de données injectées dans le réseau pendant les délais de retransmission.

Multiplexage de connexions TCP

Cette fonctionnalité permet de réutiliser les connexions TCP existantes. L'appliance Citrix ADC stocke les connexions TCP établies au pool de réutilisation. Chaque fois qu'une demande client est reçue, l'appliance recherche une connexion disponible dans le pool de réutilisation et sert le nouveau client

si la connexion est disponible. Si elle n'est pas disponible, l'appliance crée une connexion pour la demande du client et stocke la connexion au pool de réutilisation. Citrix ADC prend en charge le multiplexage de connexions pour les types de connexion HTTP, SSL et DataStream.

Mise en mémoire tampon de réception dynamique

Cela permet d'ajuster dynamiquement la mémoire tampon de réception en fonction des conditions de mémoire et du réseau.

Connexion MPTCP

Connexions MPTCP entre le client et Citrix ADC. Les connexions MPTCP ne sont pas prises en charge entre Citrix ADC et le serveur principal. L'implémentation Citrix ADC de MPTCP est conforme à la norme RFC 6824.

Vous pouvez afficher les statistiques MPTCP telles que les connexions MPTCP actives et les connexions de sous-flux actives à l'aide de l'interface de ligne de commande.

À l'invite de commandes, tapez l'une des commandes suivantes pour afficher un résumé ou un résumé détaillé des statistiques MPTCP ou pour effacer l'affichage des statistiques :

1. `Stat MPTCP`
2. `Stat mptcp -detail`
3. `Clearstats basic`

> **Remarque :**
>
> Pour établir une connexion MPTCP, le client et l'appliance Citrix ADC doivent prendre en charge la même version MPTCP. Si vous utilisez l'appliance Citrix ADC en tant que passerelle MPTCP pour vos serveurs, ces serveurs n'ont pas besoin de prendre en charge MPTCP. Lorsque le client démarre une nouvelle connexion MPTCP, l'appliance identifie la version MPTPC du client à partir de l'option MP_CAPABALE du paquet SYN. Si la version du client est supérieure à celle prise en charge par l'appliance, celle-ci indique sa version la plus élevée dans l'option MP_CAPABALE du paquet SYN-ACK. Le client revient ensuite à une version inférieure et envoie le numéro de version dans l'option MP_CAPABALE du paquet ACK. Si cette version est prise en charge, la solution matérielle-logicielle poursuit la connexion MPTCP. Sinon, la solution matérielle-logicielle reprend un protocole TCP normal. L'appliance Citrix ADC ne lance pas de sous-flux (MP_JOIN). L'appliance s'attend à ce que le client lance des sous-flux.

Prise en charge de la publicité d'adresses supplémentaires (ADD_ADDR) dans MPTCP

Dans un déploiement MPTCP, si un serveur virtuel est lié à un ensemble d'adresses IP supplémentaires de serveur virtuel, la fonctionnalité Add_ADDR (Address Address Address Advertisement) annonce

l'adresse IP des serveurs virtuels liés à l'ensemble d'adresses IP. Les clients peuvent initier des MP-JOIN sous-flux supplémentaires vers les adresses IP annoncées.

Points à retenir sur la fonctionnalité MPTCP ADD_ADDR

- Vous pouvez envoyer un maximum de 10 adresses IP dans le cadre de ADD_ADDR cette option. Si le mptcpAdvertise paramètre est activé sur plus de 10 adresses IP, après avoir fait la publicité de l'adresse IP 10, l'appliance ignore le reste des adresses IP.
- Si le sous-flux MP-CAPABLE est défini sur l'une des adresses IP du jeu d'adresses IP au lieu de l'adresse IP du serveur virtuel principal, l'adresse IP du serveur virtuel est annoncée si le mptcpAdvertise paramètre est activé pour l'adresse IP du serveur virtuel.

Configurer plus de fonctionnalités de publicité d'adresses (ADD_ADDR) pour annoncer une adresse VIP supplémentaire à l'aide de l'interface de ligne de commande

Vous pouvez configurer la MPTCP ADD_ADDR fonctionnalité pour les types d'adresses IPv4 et IPv6. En général, plusieurs adresses IP IPv4 et IPv6 peuvent être attachées à un seul ensemble d'adresses IP et le paramètre peut être activé sur n'importe quel sous-ensemble d'adresses IP. Dans la fonction ADD_ADDR, seules les adresses IP sur lesquelles l'option « MPTCPAdVertise » est activée et les adresses IP restantes du jeu d'adresses IP sont ignorées.
Procédez comme suit pour configurer la ADD_ADDR fonctionnalité :

1. Ajoutez un ensemble d'adresses IP.
2. Ajoutez une adresse IP de type IP de serveur virtuel (VIP) avec la publicité MPTCP activée.
3. Liez l'adresse IP au jeu d'adresses IP.
4. Configurez le jeu d'adresses IP avec le serveur virtuel d'équilibrage de charge.

Ajouter un ensemble d'adresses IP

À l'invite de commandes, tapez :

```
add ipset <name> [-td <positive_integer>]
<!--NeedCopy-->
```

Exemple :

```
add ipset ipset_1
<!--NeedCopy-->
```

Ajouter une adresse IP de type IP de serveur virtuel (VIP) avec la publicité MPTCP activée

Au niveau de la commande, tapez :


```
add ns ip <IPAddress>@ <netmask> [-mptcpAdvertise ( YES | NO )] -type <
    type>
<!--NeedCopy-->
```

Exemple :

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
```

Lier les adresses IP au jeu d'adresses IP

À l'invite de commandes, tapez :

```
bind ipset <name> <IPAddress>
<!--NeedCopy-->
```

Exemple :

```
bind ipset ipset_1 10.10.10.10
```

Configuration du jeu d'adresses IP sur un serveur virtuel d'équilibrage de charge

À l'invite de commandes, tapez :

```
set lb vserver <name> [-ipset  <string>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Exemple de configuration :

```
Add ipset ipset_1
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
bind ipset ipset_1 10.10.10.10
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Configurer l'adresse IP externe publicitaire à l'aide de la fonctionnalité ADD_ADDR

Si l'adresse IP annoncée appartient à l'entité externe et que l'appliance Citrix ADC doit annoncer l'adresse IP, le paramètre « MPTCPAdVertise » doit être activé avec les paramètres d'état et ARP désactivés.

Procédez comme suit ADD_ADDR pour configurer la publicité de l'adresse IP externe.

1. Ajoutez une adresse IP de type IP de serveur virtuel (VIP) avec la publicité MPTCP activée.
2. Liez l'adresse IP au jeu d'adresses IP.
3. Lier le jeu d'adresses IP au serveur virtuel d'équilibrage de charge

Ajouter une adresse IP externe de type IP de serveur virtuel (VIP) avec la publicité MPTCP activée

À l'invite de commandes, tapez :

```
add ns ip <IPAddress>@ <External-IP-mask -type VIP> [-mptcpAdvertise (
    YES | NO )] -type <type> -state DISABLED -arp DISABLED
<!--NeedCopy-->
```

Exemple :

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP -state
DISABLED -arp DISABLED
```

Lier les adresses IP au jeu d'adresses IP

À l'invite de commandes, tapez :

```
bind ipset <name> <IPAddress>
<!--NeedCopy-->
```

Exemple :

```
bind ipset ipset_1 10.10.10.10
```

Configuration du jeu d'adresses IP sur un serveur virtuel d'équilibrage de charge

À l'invite de commandes, tapez :

```
set lb vserver <name> [-ipset  <string>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver lb1 -ipset ipset_1
```

Exemple de configuration :

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
    state DISABLED -arp DISABLED
```

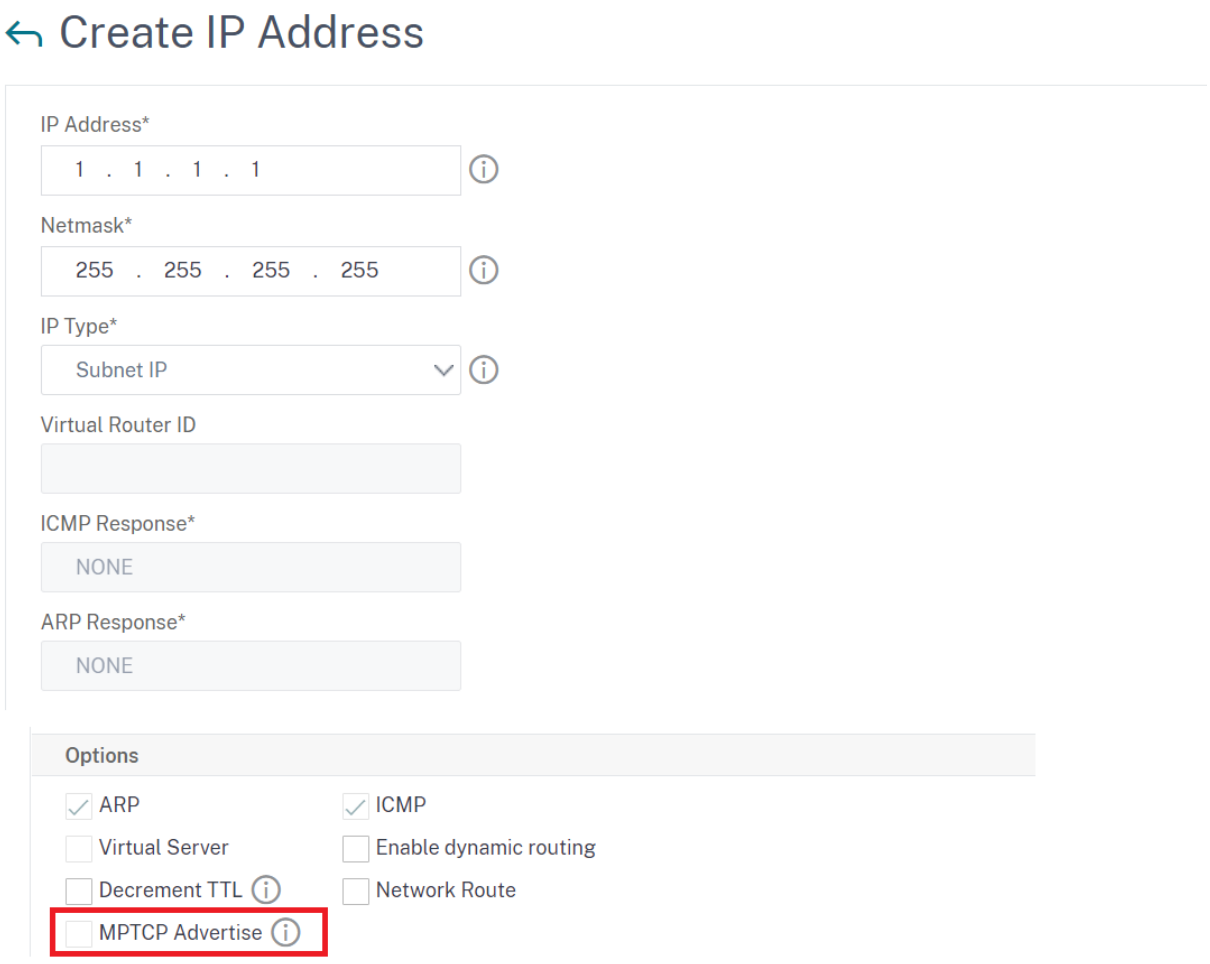


```
bind ipset ipset_1 10.10.10.10
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Annoncez l'adresse IP auprès des clients compatibles MPTCP à l'aide de l'interface graphique Citrix ADC

Effectuez l'étape suivante pour annoncer l'adresse IP aux clients compatibles MPTCP :

1. Accédez à **Système > Réseau > IP**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer une adresse IP**, activez la case à cocher **MPTCP Advertise** pour définir le paramètre. Par défaut, il est désactivé.



Extraction de l'option de superposition de chemin TCP/IP et insertion de l'en-tête HTTP Client-IP

Extraction de la superposition de chemin TCP/IP et insertion d'en-tête HTTP client-IP. Le transport de données via des réseaux superposés utilise souvent la terminaison de connexion ou la traduction d'adresses réseau (NAT), dans laquelle l'adresse IP du client source est perdue. Pour éviter cela, l'appliance Citrix ADC extrait l'option de superposition de chemin TCP/IP et insère l'adresse IP du client source dans l'en-tête HTTP. Avec l'adresse IP dans l'en-tête, le serveur Web peut identifier le client source qui a établi la connexion. Les données extraites sont valides pendant toute la durée de vie de la connexion TCP, ce qui empêche l'hôte de saut suivant d'avoir à réinterpréter l'option. Cette option s'applique uniquement aux services Web sur lesquels l'option d'insertion Client-IP est activée.

Déchargement de la segmentation TCP

Décharge la segmentation TCP vers la carte réseau. Si vous définissez l'option sur « AUTOMATIQUE », la segmentation TCP est déchargée vers la carte réseau, si la carte réseau est prise en charge.

cookie de synchronisation pour la connexion TCP avec les clients

Ceci est utilisé pour résister aux attaques d'inondation SYN. Vous pouvez activer ou désactiver le `SYNCOOKIE` mécanisme de prise de contact TCP avec les clients. La désactivation `SYNCOOKIE` empêche la protection contre les `SYN` attaques sur l'appliance Citrix ADC.

Apprendre MSS pour activer l'apprentissage MSS pour tous les serveurs virtuels configurés sur l'appliance

Paramètres TCP pris en charge

Le tableau suivant répertorie les paramètres TCP et leur valeur par défaut configurés sur une appliance Citrix ADC.

|Paramètre|Valeur par défaut|Description|
|— |— |— |
|Gestion des fenêtres|
Minuterie de retour retardé TCP	100 millisecondes	Délai d'attente pour ACK retardé TCP, en millisecondes.
Délai d'expiration minimum de retransmission TCP (RTO) en millions de secondes	1000 milli sec	Délai de retransmission minimal, en millisecondes, spécifié par incréments de 10 millisecondes (la valeur doit donner un nombre entier si elle est divisée par 10)
Temps d'inactivité de connexion avant le démarrage des sondes Keep-Alive	900 secondes	Déposez silencieusement les connexions établies par TCP sur les délais d'attente d'inactivité, les connexions établies lors du délai d'attente d'inactivité

Option d'horodatage TCP	DÉSACTIVÉ	L'option horodatage permet une mesure RTT précise. Activez ou désactivez l'option Horodatage TCP.
Délai d'expiration de session TCP multipath	0 seconde	Délai d'expiration de session MPTCP en secondes. Si cette valeur n'est pas définie, inactif. Les sessions MPTCP sont vides après le délai d'inactivité du client du serveur virtuel.
Supprimer silencieusement les connexions HalfClosed sur le délai d'inactivité	0 seconde	Abandonnez silencieusement les connexions TCP semi-fermées en période d'inactivité.
Supprimer silencieusement les connexions établies en période d'inactivité	DÉSACTIVÉ	Supprimer silencieusement les connexions établies par TCP en période d'inactivité
Gestion de la mémoire
Taille de la mémoire tampon TCP	131072 octets	La taille du tampon TCP correspond à la taille du tampon de réception sur Citrix ADC. Cette taille de tampon est annoncée aux clients et serveurs de Citrix ADC et contrôle leur capacité à envoyer des données à Citrix ADC. La taille de la mémoire tampon par défaut est de 8 Ko et il est généralement prudent de l'incrémenter lorsque vous parlez à des batteries de serveurs internes. La taille du tampon est également affectée par la couche d'application réelle dans Citrix ADC, comme pour les cas de point de terminaison SSL, elle est définie sur 40 Ko et pour la compression, elle est définie sur 96 Ko. **Remarque :** L'argument de taille de tampon doit être défini pour que les ajustements dynamiques aient lieu.
Taille de la mémoire tampon d'envoi TCP	8190 octets	Taille de la mémoire tampon d'envoi TCP
Mise en mémoire tampon de réception dynamique TCP	DÉSACTIVÉ	Activez ou désactivez la mise en mémoire tampon de réception dynamique. Lorsqu'il est activé, il permet d'ajuster dynamiquement le tampon de réception en fonction des conditions de mémoire et du réseau. **Remarque :** L'argument de taille de la mémoire tampon doit être défini pour que les ajustements dynamiques aient lieu
Fenêtre de congestion TCP Max (CWND)	524288 octets	Fenêtre d'encombrement maximal TCP
État de l'échelle de la fenêtre	ENABLED	Activez ou désactivez la mise à l'échelle des fenêtres.
Facteur d'échelle de fenêtre	8	Facteur utilisé pour calculer la nouvelle taille de fenêtre. Cet argument n'est nécessaire que lorsque la mise à l'échelle des fenêtres est activée.
Configuration de la connexion
Sondes Keep-Alive	DÉSACTIVÉ	Envoyez des sondes TCP Keep-Alive (KA) périodiques pour vérifier si le pair est toujours actif.
Temps d'inactivité de connexion avant le démarrage des sondes Keep-Alive	900 secondes	Durée, en secondes, pendant laquelle la connexion est inactive, avant l'envoi d'une sonde keep-alive (KA).
Intervalle de sonde Keep-Alive	75 seconde	Intervalle de temps, en secondes, avant la prochaine sonde Keep-Alive (KA), si le pair ne répond pas.
Nombre maximal de sondes Keep-Alive à manquer avant d'interromper la connexion.	3	Nombre de sondes Keep-Alive (KA) à envoyer sans accusé de réception, avant de supposer que le pair est en panne.
Atténuation de la fenêtre RST (protection contre les usurpation).	DÉSACTIVÉ	Activez ou désactivez l'atténuation de la fenêtre RST pour vous protéger contre l'usurpation. Lorsque cette option est

activée, la réponse est accompagnée d'un ACK correctif lorsqu'un numéro de séquence n'est pas valide.|
|Acceptez RST avec le dernier numéro de séquence accusé de réception.|ACTIVÉ|
|Transfert de données|
Paquet ACK immédiat sur PUSH	ACTIVÉ	Envoie un accusé de réception positif immédiat (ACK) à la réception de paquets TCP avec indicateur PUSH.
Nombre maximal de paquets par MSS	0	Nombre maximal d'octets à autoriser dans un segment de données TCP
Algorithme de Nagle	DÉSACTIVÉ	L'algorithme de Nagle combat le problème des petits paquets dans la transmission TCP. Les applications telles que Telnet et d'autres moteurs en temps réel qui nécessitent que chaque frappe de touche soit passée de l'autre côté créent souvent de petits paquets. Avec l'algorithme de Nagle, Citrix ADC peut tamponner ces petits paquets et les envoyer ensemble pour augmenter l'efficacité de la connexion. Cet algorithme doit fonctionner avec d'autres techniques d'optimisation TCP dans Citrix ADC.
Segments TCP maximum autorisés dans une rafale	10 MSS	Nombre maximal de segments TCP autorisés en rafale
Nombre maximal de paquets en rupture d'ordre à mettre en file d'attente	300	Taille maximale de la file d'attente des paquets en rupture d'ordre. Une valeur de 0 signifie qu'il n'y a pas de limite
Contrôle de la congestion
Saveur TCP	CUBIQUE
Paramétrage de la fenêtre de congestion initiale (cwnd)	4 MSS	Limite maximale initiale du nombre de paquets TCP pouvant être en attente sur la liaison TCP vers le serveur
Notification de congestion explicite TCP (ECN)	DÉSACTIVÉ	La notification de congestion explicite (ECN) fournit une notification de bout en bout de la congestion du réseau sans abandonner de paquets.
Fenêtre de congestion TCP Max (CWND)	524288 octets	TCP maintient une fenêtre de congestion (CWND), limitant le nombre total de paquets sans accusé de réception pouvant être en transit de bout en bout. Dans TCP, la fenêtre de congestion est l'un des facteurs qui déterminent le nombre d'octets pouvant être en attente à tout moment. La fenêtre de congestion est un moyen d'empêcher qu'un lien entre l'expéditeur et le destinataire ne soit surchargé par un trafic trop important. Il est calculé en estimant combien de congestion il y a sur le lien.
Démarrage hybride TCP (HyStart)	8 octets
Délai d'expiration minimum de retransmission TCP (RTO) en millions de secondes	1 000	Délai de retransmission minimal, en millisecondes, spécifié par incréments de 10 millisecondes (la valeur doit donner un nombre entier si elle est divisée par 10).
Seuil de dupack TCP	DÉSACTIVÉ
Contrôle de la vitesse de rafale	3	Contrôle du taux de rafale TCP DÉSACTIVÉ/FIXE/DYNAMIQUE. FIXED nécessite la définition d'un débit TCP
Taux TCP	DÉSACTIVÉ	Taux d'envoi de la charge utile de connexion TCP en Ko/s

|File d'attente maximale du débit TCP|0|Taille maximale de la file d'attente de connexion en octets, lorsque BurStrateControl est utilisé.|
|MPTCP|
TCP à trajets multiples	DÉSACTIVÉ	Multipath TCP (MPTCP) est un ensemble d'extensions de TCP standard pour fournir un service TCP multipath, qui permet à une connexion de transport de fonctionner simultanément sur plusieurs chemins.
Données de suppression TCP multipath sur un sous-flux préétabli	DÉSACTIVÉ	Activez ou désactivez la suppression silencieuse des données sur le sous-flux préétabli. Lorsque cette option est activée, les paquets de données DSS sont supprimés silencieusement au lieu d'interrompre la connexion lorsque des données sont reçues sur un sous-flux préétabli.
Ouverture-rapide TCP multipath	DÉSACTIVÉ	Activez ou désactivez l'ouverture rapide Multipath TCP. Lorsque cette option est activée, les paquets de données DSS sont acceptés avant de recevoir le troisième ack de l'établissement de liaison SYN.
Délai d'expiration de session TCP multipath	0 seconde	Délai d'expiration de session MPTCP en secondes. Si cette valeur n'est pas définie, les sessions MPTCP inactives sont vides après le délai d'inactivité du client du serveur virtuel.
Security
Protection contre les usurpations SYN	DÉSACTIVÉ	Activez ou désactivez la suppression des paquets SYN non valides pour vous protéger contre l'usurpation d'identité. Lorsque cette option est désactivée, les connexions établies sont réinitialisées lorsqu'un paquet SYN est reçu.
Cookie de synchronisation TCP	DÉSACTIVÉ	Ceci est utilisé pour résister aux attaques d'inondation SYN. Activez ou désactivez le mécanisme SYNCOOKIE pour l'établissement de liaison TCP avec les clients. La désactivation de SYNCOOKIE empêche la protection contre les attaques SYN sur l'appliance Citrix ADC.
Détection et récupération des pertes
Accusé de réception sélectif en double (DSACK)	ACTIVÉ	Une appliance Citrix ADC utilise un accusé de réception sélectif en double (DSACK) pour déterminer si une retransmission a été envoyée par erreur.
Récupération RTO avant (FRTO)	ACTIVÉ	Détecte les délais d'attente de retransmission TCP parasites. Après avoir retransmis le premier segment non reconnu déclenché par un délai d'expiration, l'algorithme de l'expéditeur TCP surveille les accusés de réception entrants pour déterminer si le délai d'expiration était faux. Il décide ensuite s'il faut envoyer de nouveaux segments ou retransmettre les segments non confirmés. L'algorithme aide efficacement à éviter d'autres retransmissions inutiles et améliore ainsi les performances TCP en cas de délai d'expiration inutile.
Accusé de réception TCP Forward (FACK)	ACTIVÉ	Activez ou désactivez FACK (Forward ACK).
État SACK (Selective Acknowledgement)	ACTIVÉ	TCP SACK résout le problème des pertes de paquets multiples, ce qui réduit la capacité globale de débit. Avec un accusé de réception sélectif, le destinataire peut informer l'expéditeur de tous les segments reçus avec succès, ce qui permet à l'expéditeur de ne retransmettre que les segments perdus. Cette technique permet à Citrix ADC

d'améliorer le débit global et de réduire la latence de connexion.|
|Nombre maximal de paquets par retransmission|1|Permet à Citrix ADC de contrôler le nombre de paquets à retransmettre en une seule tentative. Lorsque Citrix ADC reçoit un ACK partiel et qu'il doit effectuer une retransmission, ce paramètre est pris en compte. Cela n'a aucune incidence sur les retransmissions basées sur le RTO.|
|Minuterie de retour retardé TCP|100 millisecondes|Délai d'attente pour l'ACK retardé par TCP, en millisecondes|
|Optimisation du coût total de possession|
Mode d'optimisation TCP	TRANSPARENT	Modes d'optimisation TCP TRANSPARENT/ENDPOINT
Appliquer des optimisations TCP adaptatives	DÉSACTIVÉ	Appliquer des optimisations TCP adaptatives
Déchargement de segmentation TCP	AUTOMATIQUE	Déchargez la segmentation TCP vers la carte réseau. Si cette option est définie sur AUTOMATIC, la segmentation TCP est déchargée vers la carte réseau, si la carte réseau la prend en charge.
Agrégation ACK	DÉSACTIVÉ	Activer ou désactiver l'agrégation ACK
TCP Time-wait (ou Time_Wait)	40 secondes	Temps écoulé avant de libérer une connexion TCP fermée
Client et serveur Delink sur RST	DÉSACTIVÉ	Supprimer la connexion client et serveur, lorsqu'il y a les données en suspens doivent être envoyées de l'autre côté.

Définition des paramètres TCP globaux

L'appliance Citrix ADC vous permet de spécifier des valeurs pour les paramètres TCP applicables à tous les services Citrix ADC et serveurs virtuels. Cela peut être fait à l'aide de :

- Profil TCP par défaut
- Commande TCP globale
- Fonction de mise en mémoire tampon TCP

> **Remarque** :
>
> Le `recvBuffSize` paramètre de la commande set ns TCPParam est obsolète à partir de la version 9.2. Dans les versions ultérieures, définissez la taille du tampon à l'aide du `bufferSize` paramètre de la commande set ns TCPProfile. Si vous effectuez une mise à niveau vers une version où le `recvBuffSize` paramètre est obsolète, le `bufferSize` paramètre est défini sur sa valeur par défaut.

Profil TCP par défaut

Un profil TCP, nommé comme `nstcp_default_profile`, est utilisé pour spécifier les configurations TCP utilisées si aucune configuration TCP n'est fournie au niveau du service ou du serveur virtuel.

> **Remarques :**
>
> - Tous les paramètres TCP ne peuvent pas être configurés via le profil TCP par défaut. Certains paramètres doivent être exécutés à l'aide de la commande TCP globale (voir la section ci-dessous).
> - Il n'est pas nécessaire que le profil par défaut soit explicitement lié à un service ou à un serveur virtuel.

Pour configurer le profil TCP par défaut

- À l'aide de l'interface de ligne de commande, entrez :

```
set ns tcpProfile nstcp_default_profile...
<!--NeedCopy-->
```

- Dans l'interface graphique, accédez à **Système** > **Profils**, cliquez sur **Profils TCP** et mettez à jour nstcp_default_profile.

Commande TCP globale

Une autre approche que vous pouvez utiliser pour configurer les paramètres TCP globaux est la commande TCP globale. En plus de certains paramètres uniques, cette commande duplique certains paramètres pouvant être définis à l'aide d'un profil TCP. Toute mise à jour de ces paramètres dupliqués est reflétée dans le paramètre correspondant du profil TCP par défaut.

Par exemple, si le paramètre SACK est mis à jour à l'aide de cette approche, la valeur est reflétée dans le paramètre SACK du profil TCP par défaut (nstcp_default_profile).

> **Remarque :**
>
> Citrix recommande d'utiliser cette approche uniquement pour les paramètres TCP qui ne sont pas disponibles dans le profil TCP par défaut.

Pour configurer la commande TCP globale

- À l'aide de l'interface de ligne de commande, entrez :

```
set ns tcpParam …
<!--NeedCopy-->
```

- Sur l'interface graphique, accédez à **Système > Paramètres**, cliquez sur **Modifier les paramètres TCP** et mettez à jour les paramètres TCP requis.

Fonction de mise en mémoire tampon TCP

Citrix ADC fournit une fonctionnalité appelée mise en mémoire tampon TCP que vous pouvez utiliser pour spécifier la taille du tampon TCP. La fonctionnalité peut être activée globalement ou au niveau du service.

> **Remarque :**
>
> La taille de la mémoire tampon peut également être configurée dans le profil TCP par défaut. Si la taille de la mémoire tampon comporte des valeurs différentes dans la fonctionnalité de mise en mémoire tampon TCP et dans le profil TCP par défaut, la valeur la plus élevée est appliquée.

Pour configurer globalement la fonctionnalité de mise en mémoire tampon TCP

- À l'invite de commandes, saisissez :

  activer le mode ns TCPB

  ```
  set ns tcpbufParam -size <positiveInteger> -memLimit <positiveInteger>
  ```

- Sur l'interface graphique, accédez à **Système** > **Paramètres**, cliquez sur **Configurer les modes** et sélectionnez **TCP Buffering**.

  Ensuite, accédez à **Système** > **Paramètres**, cliquez sur **Modifier les paramètres TCP**, spécifiez les valeurs pour la **taille du tampon et lalimite d'utilisation de la mémoire**.

Définition des paramètres TCP spécifiques au service ou au serveur virtuel

À l'aide des profils TCP, vous pouvez spécifier des paramètres TCP pour les services et les serveurs virtuels. Vous devez définir un profil TCP (ou utiliser un profil TCP intégré) et associer le profil au service et au serveur virtuel appropriés.

> **Remarque :**
>
> Vous pouvez également modifier les paramètres TCP des profils par défaut en fonction de vos besoins.

Vous pouvez spécifier la taille de la mémoire tampon TCP au niveau du service à l'aide des paramètres spécifiés par la fonctionnalité de mise en mémoire tampon TCP.

Pour spécifier des configurations TCP au niveau du service ou du serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, effectuez les opérations suivantes :

1. Configurez le profil TCP.

   ```
   1 set ns tcpProfile <profile-name>...
   2 <!--NeedCopy-->
   ```


2. Liez le profil TCP au service ou au serveur virtuel.

```
    set service <name> ....
    <!--NeedCopy-->
```

Exemple :

```
> set service service1 -tcpProfileName profile1
```

Pour lier le profil TCP au serveur virtuel :

```
set lb vserver <name> ....
<!--NeedCopy-->
```

Exemple :

```
> set lb vserver lbvserver1 -tcpProfileName profile1
<!--NeedCopy-->
```

Pour spécifier des configurations TCP au niveau du service ou du serveur virtuel à l'aide de l'interface graphique

Dans l'interface graphique, effectuez les opérations suivantes :

1. Configurez le profil TCP.

   Accédez à **Système** > **Profils** > **Profils TCP**, puis créez le profil TCP.

2. Liez le profil TCP au service ou au serveur virtuel.

   Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services/Serveurs virtuels**, puis créez le profil TCP, qui doit être lié au service ou au serveur virtuel.

Profils TCP intégrés

Pour faciliter la configuration, Citrix ADC fournit certains profils TCP intégrés. Consultez les profils intégrés répertoriés pour les éléments suivants, sélectionnez un profil et utilisez-le tel qu'il est ou modifiez-le pour répondre à vos besoins. Vous pouvez lier ces profils à vos services ou serveurs virtuels requis.

Profil intégré	Description
nstcp_default_profile	Représente les paramètres TCP globaux par défaut de la solution matérielle-logicielle.

Profil intégré	Description
nstcp_default_tcp_lan	Utile pour les connexions de serveur principal, lorsque ces serveurs résident sur le même réseau local que la solution matérielle-logicielle.
NSTCP_Default_WAN	utile pour les déploiements WAN.
nstcp_default_tcp_lan_thin_stream	Similaire au profil nstcp_default_tcp_lan. Toutefois, les paramètres sont réglés sur des flux de paquets de petite taille.
nstcp_default_tcp_interactive_stream	Similaire au profil nstcp_default_tcp_lan. Cependant, il dispose d'un temporisateur ACK retardé réduit et des paramètres de **paquet ACK sur PUSH** .
nstcp_default_tcp_lfp	Utile pour les réseaux WAN (long fat pipe networks) côté client. Les réseaux de gros tubes longs ont des lignes à long délai et à bande passante élevée avec des pertes de paquets minimales.
nstcp_default_tcp_lfp_thin_stream	Similaire au profil nstcp_default_tcp_lfp. Toutefois, les paramètres sont réglés pour les flux de paquets de petite taille.
nstcp_default_tcp_lnp	Utile pour les réseaux à tubes longs et étroits (WAN) côté client. Les réseaux à tubes longs et étroits subissent parfois des pertes de paquets considérables.
nstcp_default_tcp_lnp_thin_stream	Similaire au profil nstcp_default_tcp_lnp. Toutefois, les paramètres sont réglés pour les flux de paquets de petite taille.
nstcp_internal_apps	Utile pour les applications internes de la solution matérielle-logicielle (par exemple, la synchronisation de site GSLB). Il contient la mise à l'échelle de la fenêtre ajustée et les options SACK pour les applications souhaitées. Ce profil ne doit pas être lié à des applications autres que des applications internes.
NSTCP_Default_Mobile_Profile	Utile pour les appareils mobiles.

Profil intégré	Description
NSTCP_Default_XA_XD_Profile	Utile pour un déploiement XenApp ou XenDesktop.

Exemples de configurations TCP

Exemples d'interface de ligne de commande permettant de configurer les éléments suivants :

Défendre TCP contre les attaques par usurpation d'identité

Activez Citrix ADC pour défendre TCP contre les attaques d'usurpation. Par défaut, le paramètre « RST-Windowattenuation » est désactivé. Ce paramètre est activé pour protéger la solution matérielle-logicielle contre l'usurpation d'identité. Si vous l'activez, il répond avec un accusé de réception correctif (ACK) pour un numéro de séquence non valide. Les valeurs possibles sont Activé, Désactivé.

Où, le paramètre d'atténuation de la fenêtre RST protège l'appareil contre l'usurpation. Lorsque cette option est activée, répondez avec l'ACK correctif lorsqu'un numéro de séquence n'est pas valide.

```
1      > set ns tcpProfile profile1 -rstWindowAttenuate ENABLED -
          spoofSynDrop ENABLED
2      Done
3      > set lb vserver lbvserver1 -tcpProfileName profile1
4      Done
5  <!--NeedCopy-->
```

Notification explicite de congestion (ECN)

`Enable ECN on the required TCP profile`

```
1      > set ns tcpProfile profile1 -ECN ENABLED
2      Done
3      > set lb vserver lbvserver1 -tcpProfileName profile1
4      Done
5  <!--NeedCopy-->
```

Accusé de réception sélectif (SACK)

Activez SACK sur le profil TCP requis.

```
1      > set ns tcpProfile profile1 -SACK ENABLED
```



```
2     Done
3     > set lb vserver lbvserver1 -tcpProfileName profile1
4     Done
5  <!--NeedCopy-->
```

Accusé de réception (FACK)

Activez FACK sur le profil TCP requis.

```
1  > set ns tcpProfile profile1 -FACK ENABLED
2  > set lb vserver lbvserver1 -tcpProfileName profile1
3  <!--NeedCopy-->
```

Mise à l'échelle des fenêtres (WS)

Activez la mise à l'échelle de la fenêtre et définissez le facteur de mise à l'échelle de la fenêtre sur le profil TCP requis.

```
1  set ns tcpProfile profile1  - WS ENABLED  - WSVal 9
2  Done
3  set lb vserver lbvserver1 -tcpProfileName profile1
4  Done
5  <!--NeedCopy-->
```

Taille de segment maximale (MSS)

Mettez à jour les configurations liées au MSS.

```
1  > set ns tcpProfile profile1  - mss 1460 - maxPktPerMss 512
2  Done
3  > set lb vserver lbvserver1 -tcpProfileName profile1
4  Done
5  <!--NeedCopy-->
```

Citrix ADC pour découvrir le MSS d'un serveur virtuel

Activez Citrix ADC pour apprendre le VSS et mettre à jour les autres configurations associées.

```
1  > set ns tcpParam -learnVsvrMSS ENABLED  - mssLearnInterval 180 -
      mssLearnDelay 3600
2  Done
3  <!--NeedCopy-->
```


Keep-Alive TCP

Activez la persistance TCP et mettez à jour les autres configurations associées.

```
> set ns tcpProfile profile1 -KA ENABLED -KaprobeUpdateLastactivity ENABLED
-KAconnIdleTime 900 -KAmaxProbes 3 -KaprobeInterval 75
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Taille de la mémoire tampon : utilisation du profil TCP

Spécifiez la taille de la mémoire tampon.

```
> set ns tcpProfile profile1 -bufferSize 8190
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Taille du tampon : utilisation de la fonction de mise en mémoire tampon TCP

Activez la fonctionnalité de mise en mémoire tampon TCP (globalement ou pour un service), puis spécifiez la taille de la mémoire tampon et la limite de mémoire.

```
> enable ns feature TCPB
Done
> set ns tcpbufParam -size 64 -memLimit 64
Done
```

MPTCP

Activez MPTCP, puis définissez les configurations MPTCP facultatives.

```
> set ns tcpProfile profile1 -mptcp ENABLED
Done
> set ns tcpProfile profile1 -mptcpDropDataOnPreEstSF ENABLED -mptcpFastOpen
 ENABLED -mptcpSessionTimeout 7200
Done
> set ns tcpparam -mptcpConCloseOnPassiveSF ENABLED -mptcpChecksum ENABLED
-mptcpSFtimeout 0 -mptcpSFReplaceTimeout 10
-mptcpMaxSF 4 -mptcpMaxPendingSF 4 -mptcpPendingJoinThreshold 0 -mptcpRTOsToSwitchSF
 2 -mptcpUseBackupOnDSS ENABLED
Done
```


Contrôle de la congestion

Définissez l'algorithme de contrôle de congestion TCP requis.

```
set ns tcpProfile profile1 -flavor Westwood
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Mise en mémoire tampon de réception dynamique

Activez la mise en mémoire tampon de réception dynamique sur le profil TCP requis.

```
> set ns tcpProfile profile1 -dynamicReceiveBuffering ENABLED
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Prise en charge de TCP Fast Open (TFO) dans Multipath TCP (MPTCP)

Une appliance Citrix ADC prend désormais en charge le mécanisme TCP Fast Open (TFO) pour établir des connexions TCP multichemin (MPTCP) et accélérer les transferts de données. Le mécanisme permet de transporter les données de sous-flux pendant la liaison MPTCP initiale dans les paquets SYN et SYN-ACK et permet également de consommer les données par le nœud récepteur lors de l'établissement de la connexion MPTCP.

Pour plus d'informations, consultez la rubrique TCP Fast Open .

Prise en charge de la taille variable des cookies TFO pour MPTCP

Une appliance Citrix ADC vous permet désormais de configurer un cookie TCP Fast Open (TFO) de longueur variable d'une taille minimale de 4 octets et d'une taille maximale de 16 octets dans un profil TCP. Ce faisant, l'appliance peut répondre au client avec la taille de cookie TFO configurée dans le paquet SYN-ACK.

Pour configurer le cookie TCP Fast Open (TFO) dans un profil TCP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set tcpProfile nstcp_default_profile -tcpFastOpenCookieSize <positive_integer
>
```

Exemple

```
set tcpProfile nstcp_default_profile -tcpFastOpenCookieSize 8
```


Pour configurer le cookie TCP Fast Open (TFO) dans un profil TCP à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > Profils.
2. Dans le volet d'informations, accédez à l'onglet **Profils TCP** et sélectionnez un profil TCP.
3. Dans la page **Configurer le profil TCP**, définissez la taille du cookie d' **ouverture rapide TCP** .
4. Cliquez sur **OK** et **Terminé**.

SYN-Cookie timeout interval

Le `TCPSyncookie` paramètre est activé par défaut dans les profils TCP pour fournir une protection robuste basée sur la RFC 4987 contre les attaques SYN. Si vous devez prendre en charge des clients TCP personnalisés qui ne sont pas compatibles avec cette protection mais qui veulent toujours garantir un retour en cas d'attaque, il `synAttackDetection` gère cela pour vous en activant automatiquement le `SYNCookie` comportement en interne pendant une période déterminée par le `autosyncookietimeout` paramètre.

Pour configurer le seuil maximal de retransmission SYN ACK à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
    set ns tcpparam [-maxSynAckRetx <positive_integer>]

    Set ns tcpparam [-maxSynAckRetx 150]
<!--NeedCopy-->
```

Pour configurer l'intervalle de délai d'expiration automatique des cookie SYN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ns tcpparam [-autosyncookietimeout <positive_integer>]
```

```
Set ns tcpparam [-autosyncookietimeout 90]
```

Supprimer la connexion client et serveur

Lorsqu'il est activé, le paramètre déconnecte la connexion client et serveur lorsqu'il y a des données en attente à envoyer vers l'autre côté. Par défaut, le paramètre est désactivé.

```
set ns tcpparam -delinkClientServerOnRST ENABLED
Done

<!--NeedCopy-->
```


Configurations HTTP

September 8, 2021

> **Important :**
>
> À partir de Citrix ADC version 13.0 build 71.x, une appliance Citrix ADC peut gérer les requêtes HTTP d'en-tête de grande taille pour répondre aux demandes d'application L7. La taille de l'en-tête peut être configurable jusqu'à 128 Ko.

Les configurations HTTP d'une appliance Citrix ADC peuvent être spécifiées dans une entité appelée profil HTTP, qui est un ensemble de paramètres HTTP. Le profil HTTP peut ensuite être associé à des services ou à des serveurs virtuels qui souhaitent utiliser ces configurations HTTP.

Un profil HTTP par défaut peut être configuré pour définir les configurations HTTP appliquées par défaut, globalement à tous les services et serveurs virtuels.

> **Remarque :**
>
> Lorsqu'un paramètre HTTP a des valeurs différentes pour le service, le serveur virtuel et globalement, la valeur de l'entité la plus spécifique (le service) se voit attribuer la priorité la plus élevée.

L'appliance Citrix ADC fournit également d'autres approches de configuration HTTP. Lisez la suite pour en savoir plus.

Citrix ADC prend en charge un protocole WebSocket qui permet aux navigateurs et autres clients de créer une connexion TCP bidirectionnelle en duplex intégral aux serveurs. L'implémentation Citrix ADC de WebSocket est conforme à la norme RFC 6455 .

> **Remarque :**
>
> Une appliance Citrix ADC prend désormais en charge la configuration d'adresse IP de source utilisateur (USIP) pour les protocoles HTTP/1.1 et HTTP/2.

Définition des paramètres HTTP globaux

L'appliance Citrix ADC vous permet de spécifier des valeurs pour les paramètres HTTP applicables à tous les services Citrix ADC et serveurs virtuels. Cela peut être fait en utilisant :

- Profil HTTP par défaut
- Commande HTTP globale

Profil HTTP par défaut

Un profil HTTP, nommé nshttp_default_profile, est utilisé pour spécifier les configurations HTTP utilisées si aucune configuration HTTP n'est fournie au niveau du service ou du serveur virtuel.

> **Remarques :**
>
> - Les paramètres HTTP ne peuvent pas tous être configurés via le profil HTTP par défaut. Certains paramètres sont exécutés à l'aide de la commande HTTP globale (voir la section suivante).
> - Il n'est pas nécessaire que le profil par défaut soit explicitement lié à un service ou à un serveur virtuel.

Pour configurer le profil HTTP par défaut

- À l'aide de l'interface de ligne de commande, entrez :

  ```
  set ns httpProfile nshttp_default_profile ...
  ```

- Sur l'interface graphique, accédez à **Système** > **Profils**, cliquez sur **Profils HTTP** et mettez à jour nshttp_default_profile.

Commande HTTP globale

Une autre approche que vous pouvez utiliser pour configurer les paramètres HTTP globaux est la commande HTTP globale. En plus de certains paramètres uniques, cette commande duplique certains paramètres pouvant être définis à l'aide d'un profil HTTP. Toute mise à jour effectuée sur ces paramètres en double est reflétée dans le paramètre correspondant dans le profil HTTP par défaut.

Par exemple, si le paramètre MaxReusePool est mis à jour à l'aide de cette approche, la valeur est reflétée dans le paramètre MaxReusePool du profil HTTP par défaut (nshttp_default_profile).

> **Remarque :**
>
> Citrix recommande d'utiliser cette approche uniquement pour les paramètres HTTP qui ne sont pas disponibles dans le profil HTTP par défaut.

Pour configurer la commande HTTP globale

- À l'aide de l'interface de ligne de commande, entrez :

  ```
  set ns httpParam ...
  ```

- Sur l'interface graphique, accédez à **Système > Paramètres**, cliquez sur **Modifier les paramètres HTTP** et mettez à jour les paramètres HTTP requis.

Pour configurer un schéma de codage ignoré pour une demande de connexion

Pour activer HTTP/2 et définir les paramètres HTTP/2 afin d'ignorer le schéma de codage dans la demande de connexion, à l'invite de commandes, tapez :

```
set ns httpParam [-ignoreConnectCodingScheme ( ENABLED | DISABLED )]
```

Exemple :


```
set ns httpParam -ignoreConnectCodingScheme ENABLED
```

Pour lier le profil HTTP à un serveur virtuel à l'aide de la ligne de commande Citrix ADC

Configurer le profil HTTP pour supprimer les requêtes TRACE ou TRACK non valides

Vous pouvez activer le paramètre MarkTraceReqInval pour marquer les requêtes TRACK et TRACK comme non valides. Lorsque vous activez cette option avec l'option DropInvalidReq sur l'adresse IP virtuelle, vous pouvez réinitialiser un client qui envoie des requêtes TRACE ou TRACK à une appliance Citrix ADC.

Pour configurer le profil HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ns httpProfile <profile name> [-markTraceReqInval ENABLED | DISABLED ]
```

Exemple :

```
set ns httpProfile profile1 -markTraceReqInval ENABLED
```

Configurer le profil HTTP pour un groupe de services

À l'invite de commandes, tapez :

```
1 add serviceGroup <serviceGroupName>@ <serviceType> [-cacheType <
     cacheType>] [-td <positive_integer>] [-maxClient <positive_integer>]
      [-maxReq <positive_integer>] [-cacheable ( YES | NO )] [-cip (
     ENABLED | DISABLED ) [<cipHeader>]] [-usip ( YES | NO )] [-
     pathMonitor ( YES | NO )] [-pathMonitorIndv ( YES | NO )] [-
     useproxyport ( YES | NO )] [-healthMonitor ( YES | NO )] [-sp ( ON |
      OFF )] [-rtspSessionidRemap ( ON | OFF )] [-cltTimeout <secs>] [-
     svrTimeout <secs>] [-CKA ( YES | NO )] [-TCPB ( YES | NO )] [-CMP (
     YES | NO )] [-maxBandwidth
2 <positive_integer>] [-monThreshold <positive_integer>] [-state ENABLED
     DISABLED )][-downStateFlush ( ENABLED | DISABLED )] [-tcpProfileName
      <string>] [-httpProfileName <string>] [-comment <string>] [-
     appflowLog ( ENABLED | DISABLED )] [-netProfile <string>] [-
     autoScale <autoScale> -memberPort <port> [-autoDisablegraceful ( YES
      | NO )] [-autoDisabledelay <secs>] ] [-monConnectionClose ( RESET |
      FIN )]
3
4 <!--NeedCopy-->
```

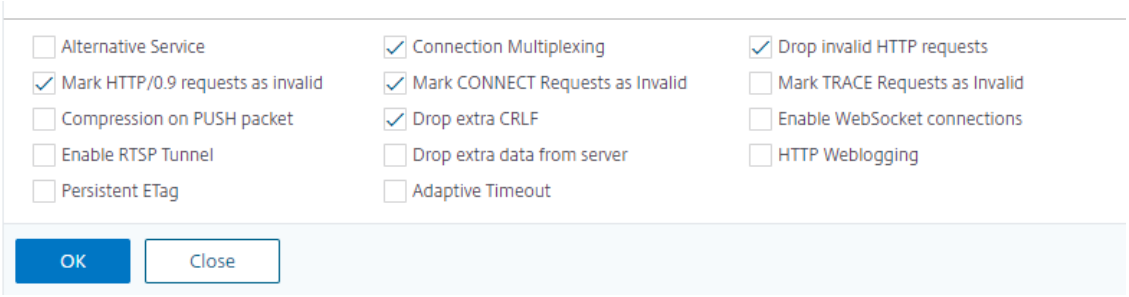
Exemple :


```
add serviceGroup rl-lips-30016 HTTP -maxClient 0 -maxReq 0 -cip ENABLED X-
Forwarded-For -usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -
CKA NO -TCPB NO -CMP NO -tcpProfileName live-tcp-profile-sg -httpProfileName
 profile1
```

Configurer le profil HTTP à l'aide de l'interface graphique Citrix ADC

Pour marquer les demandes TRACE ou TRACK non valides, procédez comme suit.

1. Connectez-vous à l'appliance Citrix ADC et accédez à **Configuration** > **Système** > **Profils**.
2. Dans la page de l'onglet **Profils HTTP**, cliquez sur **Ajouter**.
3. Dans la page **Créer un profil HTTP**, sélectionnez l'option **Marquer les requêtes TRACE comme non valides** .
4. Cliquez sur **Créer**.



Définition de paramètres HTTP spécifiques au service ou au serveur virtuel

À l'aide de profils HTTP, vous pouvez spécifier des paramètres HTTP pour les services et les serveurs virtuels. Vous devez définir un profil HTTP (ou utiliser un profil HTTP intégré) et l'associer au service et au serveur virtuel appropriés.

> **Remarque :**
>
> Vous pouvez également modifier les paramètres HTTP des profils par défaut en fonction de vos besoins.

Pour spécifier des configurations HTTP au niveau du service ou du serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, effectuez les opérations suivantes :

1. Configurez le profil HTTP.

   ```
   set ns httpProfile <profile-name>...
   ```


2. Liez le profil HTTP au service ou au serveur virtuel.

   Pour lier le profil HTTP au service :

```
set service <name> .....
```

Exemple :

```
1 > set service service1 -httpProfileName profile1
2 <!--NeedCopy-->
```

Pour lier le profil HTTP au serveur virtuel :

```
set lb vserver <name> .....
```

Exemple :

```
1 > set lb vserver lbvserver1 -httpProfileName profile1
2 <!--NeedCopy-->
```

Pour spécifier des configurations HTTP au niveau du service ou du serveur virtuel à l'aide de l'interface graphique

À l'interface graphique, effectuez les opérations suivantes :

1. Configurez le profil HTTP.

   Accédez à **Système** > **Profils** > **Profils HTTP**, puis créez le profil HTTP.

2. Liez le profil HTTP au service ou au serveur virtuel.

   Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services/Serveurs virtuels**, puis créez le profil HTTP, qui doit être lié au service/serveur virtuel.

Profils HTTP intégrés

Pour faciliter la configuration, Citrix ADC fournit des profils HTTP intégrés. Examinez les profils répertoriés et utilisez-les tels qu'ils sont ou modifiez-les pour répondre à vos besoins. Vous pouvez lier ces profils aux services ou aux serveurs virtuels requis.

Profilé intégré	Description
nshttp_default_profile	Représente les paramètres HTTP globaux par défaut de l'appliance.
nshttp_default_strict_validation	Paramètres des déploiements nécessitant une validation stricte des requêtes et des réponses HTTP.

Exemples de configurations HTTP

Exemples d'interfaces de ligne de commande permettant de configurer les éléments suivants :

- Statistiques sur les bandes HTTP
- Connexions WebSocket

Statistiques sur les bandes HTTP

Spécifiez la taille de bande des requêtes et des réponses HTTP.

```
> set protocol httpBand reqBandSize 300 respBandSize 2048
Done
> show protocol httpband -type REQUEST
<!--NeedCopy-->
```

Connexions WebSocket

Activez WebSocket sur le profil HTTP requis.

```
> set ns httpProfile http_profile1 -webSocket ENABLED
Done
> set lb vserver lbvserver1 -httpProfileName profile1
Done
<!--NeedCopy-->
```

Configuration HTTP/2

October 5, 2021

Remarque : La fonctionnalité HTTP/2 est prise en charge sur les modèles Citrix ADC MPX, VPX et SDX. Dans une appliance Citrix ADC VPX, la fonctionnalité HTTP/2 est prise en charge à partir de la version 11.0.

Le problème des performances des applications Web est directement lié à la tendance à l'augmentation de la taille des pages et du nombre d'objets sur les pages Web. HTTP/1.1 a été développé pour prendre en charge des pages Web plus petites, des connexions Internet plus lentes et un matériel serveur plus limité que ce qui est courant aujourd'hui. Il n'est pas adapté aux nouvelles technologies telles que JavaScript et les feuilles de style en cascade (CSS) ou aux nouveaux types de médias tels que les vidéos Flash et les images riches en graphiques. En effet, il ne peut demander qu'une seule ressource par connexion au serveur. Cette limitation augmente considérablement le nombre d'allers-retours, ce qui allonge le rendu des pages et réduit les performances du réseau.

Le protocole HTTP/2 résout ces limitations en permettant la communication avec moins de données transmises sur le réseau et en offrant la possibilité d'envoyer plusieurs requêtes et réponses via une seule connexion. HTTP/2 résout les principales limitations de HTTP/1.1 en utilisant plus efficacement les connexions réseau sous-jacentes. Il modifie la façon dont les demandes et les réponses circulent sur le réseau.

HTTP/2 est un protocole binaire. Il est plus efficace d'analyser, plus compact sur le fil, et surtout, il est moins sujet aux erreurs, par rapport aux protocoles textuels comme HTTP/1.1. Le protocole HTTP/2 utilise une couche de cadrage binaire qui définit le type de trame et la façon dont les messages HTTP sont encapsulés et transférés entre le client et le serveur. La fonctionnalité HTTP/2 prend en charge l'utilisation de la méthode CONNECT pour établir une connexion tunnel via un seul flux HTTP/2 vers un hôte distant.

Le protocole HTTP/2 inclut de nombreuses modifications améliorant les performances qui améliorent considérablement les performances, en particulier pour les clients se connectant via un réseau mobile.

Le tableau suivant répertorie les principales améliorations de HTTP/2 par rapport à HTTP/1.1 :

Fonctionnalités HTTP/2	**Description**
Compression d'en-tête	Les en-têtes HTTP contiennent beaucoup d'informations répétitives et consomment donc une bande passante inutile pendant la transmission des données. HTTP/2 réduit les besoins en bande passante en comprimant l'en-tête et en minimisant la nécessité de transporter les en-têtes HTTP à chaque requête et réponse.
Multiplexage de connexion	La latence peut avoir un impact considérable sur les temps de chargement des pages et sur l'expérience de l'utilisateur final. Le multiplexage des connexions résout ce problème en envoyant plusieurs demandes et réponses via une seule connexion.

Fonctionnalités HTTP/2	Description
Serveur Push	Server Push permet au serveur de diffuser du contenu de manière proactive vers le navigateur du client, ce qui évite les retards aller-retour. Cette fonctionnalité met en cache les réponses dont le client pense avoir besoin, réduit le nombre d'allers-retours et améliore le temps de rendu de la page. Important : L'appliance Citrix ADC ne prend pas en charge la fonctionnalité de diffusion du serveur.
Pas de blocage de la tête de ligne	Sous HTTP 1.1, les navigateurs peuvent télécharger une ressource à la fois par connexion. Lorsqu'un navigateur doit télécharger une ressource volumineuse, il bloque le téléchargement de toutes les autres ressources jusqu'à ce que le premier téléchargement soit terminé. HTTP/2 résout ce problème avec une approche de multiplexage. Il permet au navigateur client de télécharger d'autres composants Web en parallèle sur la même connexion et de les afficher dès qu'ils sont disponibles.

Fonctionnalités HTTP/2	Description
Priorisation des demandes	Toutes les ressources n'ont pas la même priorité lorsque le navigateur affiche une page Web. Pour accélérer le temps de chargement, tous les navigateurs modernes hiérarchisent les demandes par type de ressource, leur emplacement sur la page et même par priorité acquise lors des visites précédentes. Avec HTTP/1.1, le navigateur a une capacité limitée d'utiliser les données de priorité, car ce protocole ne prend pas en charge le multiplexage et il n'y a aucun moyen de communiquer la hiérarchisation des requêtes par le serveur. Il en résulte une latence réseau inutile. HTTP/2 résout ce problème en permettant au navigateur d'envoyer toutes les requêtes. Le navigateur peut communiquer ses préférences de priorisation des flux via des dépendances et des pondérations de flux, ce qui permet aux serveurs d'optimiser la livraison des réponses. Important : L'appliance Citrix ADC ne prend pas en charge la fonctionnalité de priorisation des demandes.

Fonctionnement de HTTP/2

Une appliance Citrix ADC prend en charge HTTP/2 côté client ainsi que côté serveur. Côté client, l'appliance Citrix ADC agit comme un serveur qui héberge un serveur virtuel HTTP/HTTPS pour HTTP/2. Côté back-end, Citrix ADC agit en tant que client pour les serveurs liés au serveur virtuel.

Par conséquent, l'appliance Citrix ADC maintient des connexions distinctes côté client et côté serveur. L'appliance Citrix ADC possède des configurations HTTP/2 distinctes pour le côté client et le côté serveur.

Configuration de l'équilibrage de charge HTTP/2 pour HTTPS (SSL)

Pour une configuration d'équilibrage de charge HTTPS, l'appliance Citrix ADC utilise l'extension TLS ALPN (RFC 7301) pour déterminer si le client/serveur prend en charge HTTP/2. Si tel est le cas, la solution matérielle-logicielle choisit HTTP/2 comme protocole de couche applicative pour transmettre

les données (comme décrit dans la RFC 7540 - Section 3.3) côté client/serveur.
La solution matérielle-logicielle utilise l'ordre de préférence suivant lorsqu'elle choisit le protocole de la couche application via l'extension TLS ALPN :

- HTTP/2 (s'il est activé dans le profil HTTP)
- HTTP/1.1

Configuration de l'équilibrage de charge HTTP/2 pour HTTP

Pour une configuration d'équilibrage de charge HTTP, l'appliance Citrix ADC utilise l'une des méthodes suivantes pour commencer à communiquer avec le client/serveur à l'aide de HTTP/2.

> **Remarque**
>
> Dans les descriptions de méthodes suivantes, le client et le serveur sont des termes généraux pour une connexion HTTP/2. Par exemple, pour une configuration d'équilibrage de charge d'une appliance Citrix ADC utilisant HTTP/2, l'appliance Citrix ADC agit en tant que serveur côté client et en tant que client côté serveur.

- Mise à**niveau HTTP/2**. Un client envoie une requête HTTP/1.1 à un serveur. La demande inclut un en-tête de mise à niveau, qui demande au serveur de mettre à niveau la connexion vers HTTP/2. Si le serveur prend en charge HTTP/2, il accepte la demande de mise à niveau et la notifie dans sa réponse. Le client et le serveur commencent à communiquer via HTTP/2 une fois que le client a reçu la réponse de confirmation de mise à niveau.
- **HTTP/2 direct**. Un client commence directement à communiquer avec un serveur en HTTP/2 au lieu d'utiliser la méthode de mise à niveau HTTP/2. Si le serveur ne prend pas en charge HTTP/2 ou n'est pas configuré pour accepter directement les requêtes HTTP/2, il supprime les paquets HTTP/2 du client. Cette méthode est utile si l'administrateur de la machine cliente sait déjà que le serveur prend en charge HTTP/2.
- **HTTP/2 direct à l'aide d'un service alternatif (ALT-SVC).** Un serveur annonce qu'il prend en charge HTTP/2 à un client en incluant un champ Alternative Service (ALT-SVC) dans sa réponse HTTP/1.1. Si le client est configuré pour comprendre le champ ALT-SVC, le client et le serveur commencent à communiquer directement via HTTP/2 une fois que le client a reçu la réponse.

L'appliance Citrix ADC fournit des options configurables dans un profil HTTP pour les méthodes HTTP/2. Ces options HTTP/2 peuvent être appliquées au côté client ainsi qu'au côté serveur d'une configuration d'équilibrage de charge HTTPS ou HTTP. Pour plus d'informations sur les méthodes et options HTTP/2, reportez-vous au PDF des options HTTP/2 .

Avant de commencer

Avant de commencer à configurer HTTP/2 sur une appliance Citrix ADC, notez les points suivants :

- L'appliance Citrix ADC prend en charge HTTP/2 côté client ainsi que côté serveur.
- L'appliance Citrix ADC ne prend pas en charge la fonctionnalité de transmission du serveur HTTP/2.
- L'appliance Citrix ADC ne prend pas en charge la fonctionnalité de priorisation des demandes HTTP/2.
- L'appliance Citrix ADC ne prend pas en charge la renégociation SSL HTTP/2 pour les configurations d'équilibrage de charge HTTPS.
- L'appliance Citrix ADC ne prend pas en charge l'authentification HTTP/2 NTLM.
- HTTP/2 ne fonctionne pas si le mode User Source IP (USIP) est activé et que le mode proxy est désactivé sur l'appliance Citrix ADC.

Configuration de HTTP/2

La configuration de HTTP/2 pour une configuration d'équilibrage de charge (HTTPS ou HTTP) comprend les tâches suivantes :

- **Activez HTTP/2 et définissez des paramètres HTTP/2 facultatifs dans un profil HTTP**. Activez HTTP/2 dans un profil HTTP. Lorsque vous activez uniquement HTTP/2 dans un profil HTTP, l'appliance Citrix ADC utilise uniquement la méthode de mise à niveau (pour HTTP) ou la méthode TLS ALPN (pour HTTPS) pour communiquer en HTTP/2.

  Pour que l'appliance Citrix ADC utilise la méthode HTTP/2 directe, l'option **Direct HTTP/2** doit être activée dans le profil HTTP. Pour que l'appliance Citrix ADC utilise le protocole HTTP/2 direct à l'aide de la méthode de **service alternative, l'option Alternative Service (altsvc)** doit être activée dans le profil HTTP.

- **Liez le profil HTTP à un serveur virtuel ou à un service**. Liez le profil HTTP à un serveur virtuel pour configurer HTTP/2 pour le côté client de la configuration de l'équilibrage de charge. Liez le profil HTTP à un service afin de configurer HTTP2 pour le côté serveur de la configuration de l'équilibrage de charge.

> **Remarque**
>
> Citrix recommande de lier des profils HTTP distincts pour le côté client et le côté serveur.

- **Activez le paramètre global pour la prise en charge HTTP/2 côté serveur**. Activez le paramètre HTTP global **HTTP/2 Service Side(HTTP2ServerSide**) pour activer la prise en charge HTTP/2 côté serveur de toutes les configurations d'équilibrage de charge pour lesquelles HTTP/2 est configuré.

  HTTP/2 ne fonctionne pas côté serveur des configurations d'équilibrage de charge si le **côté service HTTP/2** est désactivé, même si le **protocole HTTP/2** est activé sur le profil HTTP lié aux services d'équilibrage de charge associés.

Procédures de ligne de commande Citrix ADC :

Pour activer HTTP/2 et définir les paramètres HTTP/2 à l'aide de la ligne de commande Citrix ADC

- Pour activer HTTP/2 et définir les paramètres HTTP/2 lors de l'ajout d'un profil HTTP, à l'invite de commandes, tapez :

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )] [-altsvc ( ENABLED | DISABLED )]
show ns httpProfile <name>
```

- Pour activer HTTP/2 et définir les paramètres HTTP/2 lors de la modification d'un profil HTTP, à l'invite de commandes, tapez :

```
set ns httpProfile <name> -http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED)] [-altsvc (ENABLED | DISABLED )]
show ns httpProfile <name>
```

Pour lier le profil HTTP à un serveur virtuel à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

```
set lb vserver <name> - httpProfileName <string>
show lb vserver <name>
```

Pour lier le profil HTTP à un service d'équilibrage de charge à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

```
set service <name> -httpProfileName <string>
show service <name>
```

Pour activer la prise en charge HTTP/2 globalement côté serveur à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

```
set ns httpParam -HTTP2Serverside( ENABLED | DISABLED )
show ns httpParam
```

Pour activer HTTP/2 et définir les paramètres HTTP/2 à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Système** > **Profils**, puis cliquez sur l'onglet **Profils HTTP** .
2. Activez **HTTP/2** lors de l'ajout d'un profil HTTP ou de la modification d'un profil HTTP existant.

Pour lier le profil HTTP à un serveur virtuel à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans **Paramètres avancés**, cliquez **sur+Profil HTTP** pour lier le profil HTTP créé au serveur virtuel.

Pour lier le profil HTTP à un service d'équilibrage de charge à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Service**, puis ouvrez le service.
2. Dans **Paramètres avancés**, cliquez **sur+Profil HTTP** pour lier le profil HTTP créé au service.

Pour activer la prise en charge de HTTP/2 globalement côté serveur à l'aide de l'interface graphique

Accédez à **Système** > **Paramètres**, cliquez sur **Modifier les paramètres HTTP** et activez **HTTP/2 Server Side**.

Exemples de configurations

Dans l'exemple de configuration suivant, HTTP/2 et HTTP/2 direct sont activés sur le profil HTTP HTTP-PROFILE-HTTP2-CLIENT-SIDE. Le profil est lié au serveur virtuel LB-VS-1.

```
set ns httpProfile HTTP-PROFILE-HTTP2-CLIENT-SIDE -http2 enabled -
    http2Direct enabled
Done

set lb vserver LB-VS-1 -httpProfileName HTTP-PROFILE-HTTP2-CLIENT-SIDE

Done
<!--NeedCopy-->
```

Dans l'exemple de configuration suivant, HTTP/2 et le service alternatif (ALT-SVC) sont activés sur le profil HTTP HTTP-PROFILE-HTTP2-SERVER-SIDE. Le profil est lié au service LB-SERVICE-1.

```
set ns httpparam -HTTP2Serverside ENABLED
Done

set ns httpProfile HTTP-PROFILE-HTTP2-SERVER-SIDE -http2 ENABLED -
    altsvc ENABLED
Done

set service LB-SERVICE-1 -httpProfileName HTTP-PROFILE-HTTP2-SERVER-
    SIDE
Done
<!--NeedCopy-->
```

Configurer la taille de la fenêtre de connexion initiale HTTP/2

Conformément à la RFC 7540, la fenêtre de contrôle de flux pour le flux HTTP2 et la connexion doit être définie sur 64 K (65535) octets, et toute modification apportée à cette valeur doit être communiquée à l'homologue. L'appliance ADC communique la modification de la taille de la fenêtre de contrôle de flux comme suit :

- Utiliser le `SETTINGS` cadre pour le flux.
- Utilisation du `WINDOW_UPDATE` cadre pour la connexion.

Dans un profil HTTP, vous devez configurer le `http2InitialWindowSize` paramètre pour définir la taille initiale de la fenêtre au niveau du flux. En raison d'une erreur système interne, l'appliance ADC initialise également la fenêtre de contrôle de flux de la connexion. En cas de modification de la fenêtre de contrôle de flux configurée pour le flux, l'appliance ADC communique avec l'homologue à l'aide de la trame SETTINGS. Mais l'appliance ADC ne parvient pas à communiquer la modification de la fenêtre de contrôle de flux pour la connexion à l'aide de la `WINDOW_UPDATE` trame. Cela entraîne un gel de la connexion.

Pour résoudre ce problème, le `http2InitialConnWindowSize` paramètre (en octets) est maintenant ajouté pour contrôler la fenêtre de contrôle de flux pour la connexion. En utilisant des paramètres configurables distincts, vous pouvez désormais permettre à l'appliance d'envoyer des mises à jour pour modifier la taille de fenêtre au niveau du flux et de la connexion.

Configurer le paramètre de taille de fenêtre de connexion initiale HTTP/2 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set http profile p1 -http2InitialConnWindowSize 8290
Initial window size for stream level flow control, in bytes.
Default value: 65535
Minimum value: 8192
Maximum value: 20971520
<!--NeedCopy-->
```

Atténuation des attaques DoS HTTP/2

August 20, 2021

Les attaques par déni de service (DoS) Http/2 n'ont plus d'impact sur une appliance Citrix ADC. Si l'appliance reçoit des images supérieures à la limite maximale, l'appliance ferme silencieusement la connexion.

Pour atténuer les attaques, le profil HTTP vous permet de modifier la configuration par défaut des trames reçues dans une connexion HTTP/2.

Le tableau d' atténuation des déni de service HTTP/2 affiche la liste des attaques DoS HTTP/2 et ses mesures d'atténuation.

Configurez la limite maximale pour les trames HTTP/2 afin d'atténuer les attaques DoS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
set ns httpprofile <profile_name> - http2MaxEmptyFramesPerMin <positive_integer
> -http2MaxPingFramesPerMin <positive_integer> -http2MaxSettingsFramesPerMin
 <positive_integer> -http2MaxResetFramesPerMin <positive_integer>
```

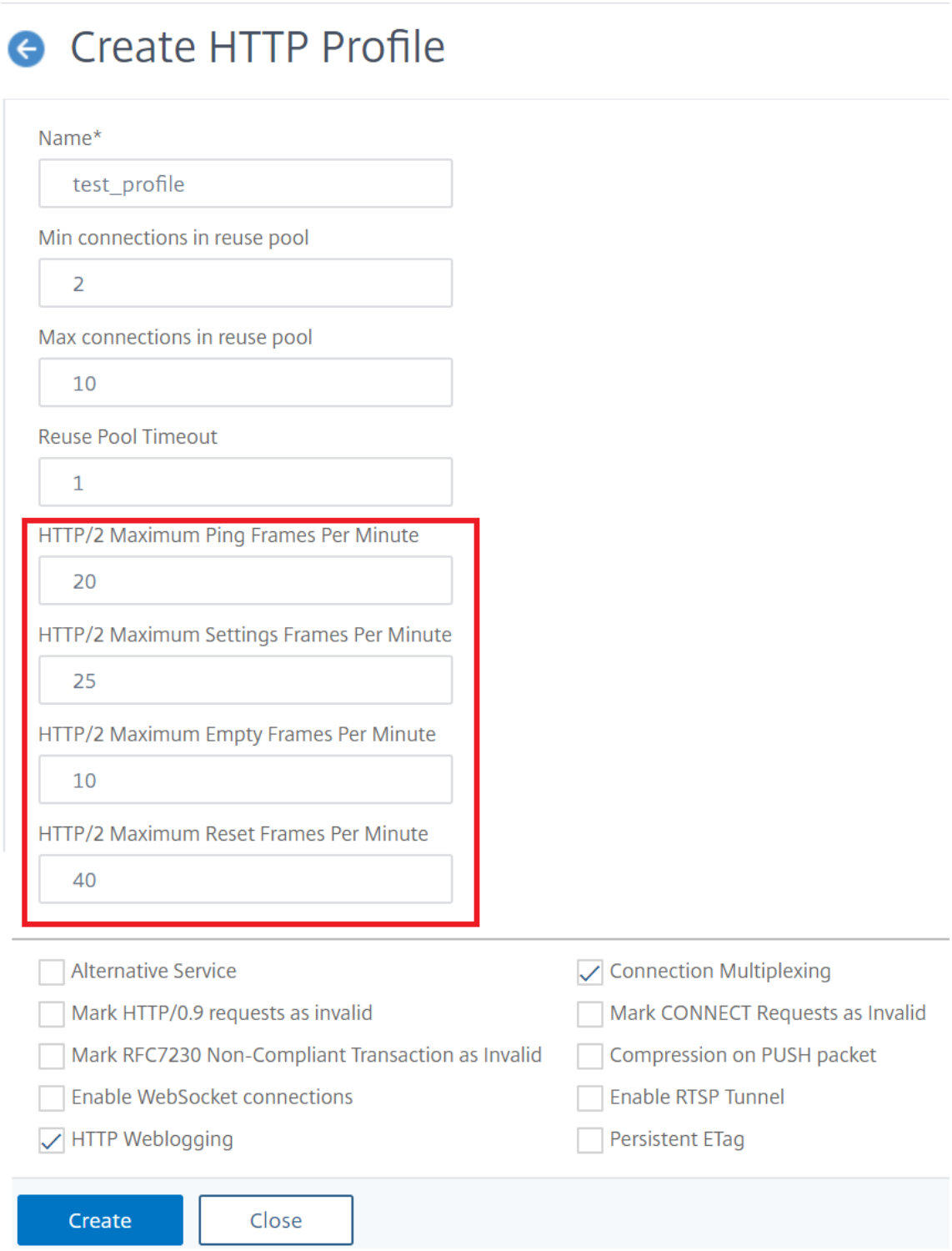
Exemple :

```
set ns httpprofile profile1 -http2MaxEmptyFramesPerMin 20 -http2MaxPingFramesPerMin
 20 -http2MaxSettingsFramesPerMin 20 -http2MaxResetFramesPerMin 20
```

Configurez la limite maximale pour les trames reçues dans une connexion HTTP/2 à l'aide de l'interface graphique Citrix ADC

Suivez les étapes ci-dessous pour configurer la limite maximale pour les images reçues dans une connexion HTTP/2 :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Profils**.
2. Dans la page **Profil**, sélectionnez l'onglet **Profils HTTP**.
3. Dans la page de l'onglet **Profils HTTP**, cliquez sur **Ajouter**.
4. Dans la page **Configurer le profil HTTP**, définissez le paramètre suivant.
    a) http2MaxPingFramesPerMin. Définissez le nombre maximal de trames PING reçues par connexion en une minute. Si le nombre de trames PING dépasse la limite de configuration, l'appliance supprime silencieusement les paquets sur la connexion.
    b) http2MaxSettingsFramesPerMin. Définissez le nombre maximal d'images de paramètres reçues par connexion en une minute. Si le nombre de trames SETTINGS dépasse la limite de configuration, ADC supprime silencieusement les paquets sur la connexion.
    c) http2MaxResetFramesPerMin. Définissez le nombre maximal d'images RESET envoyées par connexion en une minute. Si le nombre de trames RESET dépasse la limite de configuration, ADC supprime silencieusement les paquets sur la connexion.
    d) http2MaxEmptyFramesPerMin. Définissez le nombre maximal de trames vides envoyées par connexion en une minute. Si le nombre de trames vides dépasse la limite de configuration, ADC supprime silencieusement les paquets sur la connexion.
5. Cliquez sur **OK** et **Fermer**.



Protocole HTTP3 sur QUIC

August 20, 2021

HTTP/2 sur TCP est la norme préférée pour l'envoi de plusieurs flux de requêtes HTTP sur une seule connexion. Toutefois, dans le mécanisme de transport TCP, l'accès aux sites Web et aux applications Web présente certaines limitations et problèmes de latence. Lorsque vous multiplexez plusieurs demandes sur la même connexion, elles sont soumises à la fiabilité de la même connexion. Si le paquet d'une demande est perdu, toutes les autres demandes multiplexées sont retardées jusqu'à ce que le paquet perdu soit détecté et retransmis. Cela entraîne des retards de blocage de la tête de ligne et des problèmes de latence.

Pour les retards de connexion et de transport, HTTP/3 utilise QUIC au lieu du protocole TCP. Le QUIC est un protocole émergent qui utilise UDP au lieu de TCP comme transport de base. Dans HTTP overQuic, vous pouvez multiplexer plusieurs requêtes indépendantes sans dépendre d'une seule connexion TCP. QUIC met en œuvre une connexion fiable sur laquelle vous pouvez diffuser plusieurs requêtes HTTP en streaming. QUIC intègre également TLS en tant que composant intégré et non en tant que couche supplémentaire, comme dans HTTP/1.1 ou HTTP/2.

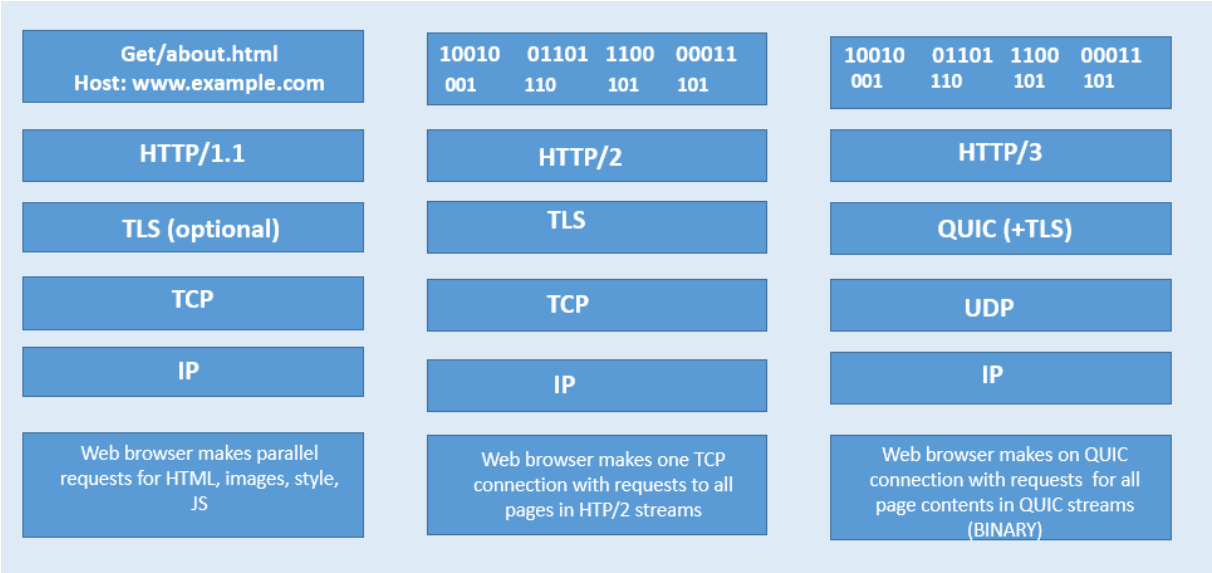
Avantage de l'utilisation du protocole HTTP/3

Voici quelques-uns des avantages importants de l'utilisation du protocole QUIC pour le transport de données HTTP/3 :

- Multiplexage de flux
- Contrôle du débit au niveau du flux et de la connexion
- Établissement de connexions à faible latence
- Migration des connexions et résilience à la reliaison NAT
- En-tête et charge utile authentifiés et chiffrés

Pile de transport dans les protocoles HTTP

L'illustration ci-dessous montre la pile de transport dans les protocoles HTTP/1.1, HTTP/2 et HTTP/3.



Fonctionnement de la gestion des connexions QUIC et HTTP/3 dans Citrix ADC

L'illustration suivante montre comment la gestion des connexions QUIC et HTTP/3 dans une appliance Citrix ADC et comment les composants interagissent entre eux.

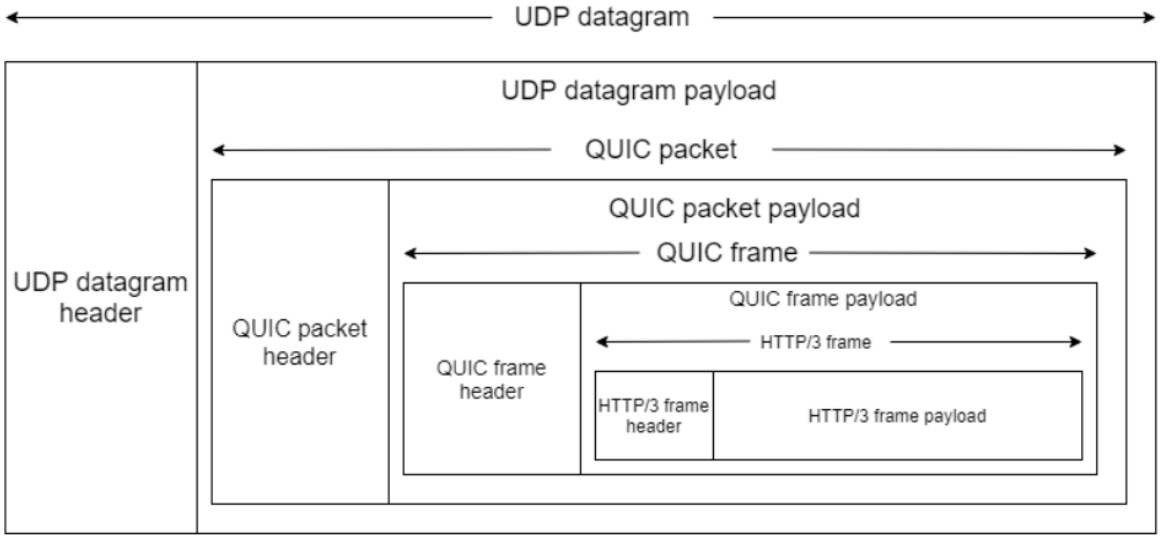
Étape 1 : requête HTTP/3 côté client via le protocole QUIC vers l'appliance Citrix ADC.
Étape 2 : Demande transmise par Citrix ADC AS HTTP/1.1 ou HTTP/2 en fonction de la prise en charge du serveur principal.
Étape 3 : Réponse via HTTP/2 ou HTTP/1.1 du serveur principal à Citrix ADC.
Étape 4 : ADC transmet la réponse en tant que réponse HTTP/3 au client.

Fonctionnement du protocole HTTP/3

Dans HTTP/3, lorsqu'un client sait qu'un serveur HTTP/3 existe sur un point de terminaison donné, il ouvre une connexion QUIC. Le protocole QUIC permet le multiplexage et le contrôle du flux. Dans chaque flux, l'unité de base de la communication HTTP/3 est une trame. Chaque type de cadre a un

objectif différent. Par exemple, les blocs HEADERS et DATA constituent la base des requêtes et des réponses HTTP.

Le multiplexage des requêtes est effectué à l'aide de l'abstraction de flux QUIC. Chaque paire demande-réponse consomme un flux QUIC unique. Les flux sont indépendants les uns des autres, de sorte qu'un flux bloqué ou subit une perte de paquets n'empêche pas la progression sur d'autres flux. Server Push est un mode d'interaction introduit dans HTTP/2 qui permet à un serveur de transmettre un échange demande-réponse à un client en prévision de la demande indiquée par le client. Cela permet d'opposer l'utilisation du réseau à un gain potentiel de latence. Plusieurs trames HTTP/3 sont utilisées pour gérer le push du serveur, telles que PUSH_PROMISE, MAX_PUSH_ID et CANCEL_PUSH. Comme dans HTTP/2, les champs de demande et de réponse sont compressés pour transmission. Parce que HPACK repose sur la transmission dans l'ordre de sections de champs compressés (garantie non fournie par QUIC), HTTP/3 remplace HPACK par QPACK. QPACK utilise des flux unidirectionnels distincts pour modifier et suivre l'état de la table des champs, tandis que les sections de champs codées font référence à l'état de la table sans la modifier.



Configuration HTTP/3 et résumé des statistiques

August 20, 2021

Pour configurer un protocole HTTP/3 pour envoyer plusieurs flux de données HTTP/3 à l'aide de QUIC, vous devez effectuer les étapes suivantes :

1. Activez les fonctionnalités SSL et d'équilibrage de charge.
2. Ajoutez des serveurs virtuels d'équilibrage de charge et de commutation de contenu (facultatif) de type HTTP_QUIC.

3. Associez les paramètres du protocole QUIC au serveur virtuel HTTP_QUIC.
4. Activez HTTP/3 sur le serveur virtuel HTTP_QUIC.
5. Liez la paire de clés de certificat SSL avec le serveur virtuel HTTP_QUIC.
6. Associez les paramètres du protocole SSL/TLS au serveur virtuel HTTP_QUIC.

Activer SSL et l'équilibrage de charge

Avant de commencer, assurez-vous que les fonctions SSL et d'équilibrage de charge sont activées sur l'appliance. À l'invite de commandes, tapez :

```
1 enable ns feature ssl lb
2 <!--NeedCopy-->
```

Ajout de serveurs virtuels d'équilibrage de charge et de commutation de contenu (facultatif) de type HTTP_QUIC pour le service HTTP/3

Vous ajoutez un serveur virtuel d'équilibrage de charge pour accepter le trafic HTTP/3 via QUIC. Remarque : Le serveur virtuel d'équilibrage de charge de type HTTP_QUIC possède des profils QUIC, SSL et HTTP3 intégrés. Si vous préférez créer des profils définis par l'utilisateur, vous pouvez ajouter de nouveaux profils et les lier au serveur virtuel d'équilibrage de charge.

```
1 add lb vserver <vserver-name> HTTP_QUIC <IP-address> <UDP-listening-
     port>
2 add cs vserver <vserver-name> HTTP_QUIC <IP-address> <UDP-listening-
     port>
3 <!--NeedCopy-->
```

Exemple :

```
add lb vserver lb-http3 HTTP_QUIC 1.1.1.1 443
add cs vserver cs-http3 HTTP_QUIC 10.10.10.10 443
```

Associer les paramètres du protocole QUIC au serveur virtuel HTTP_QUIC

Vous pouvez créer un profil QUIC et spécifier des paramètres QUIC pour le service QUIC et l'associer au serveur virtuel d'équilibrage de charge. Vous devez soit créer un profil défini par l'utilisateur, soit utiliser le profil QUIC intégré et lier le profil au serveur virtuel d'équilibrage de charge.

Étape 1 : configurer un profil QUIC défini par l'utilisateur
À l'invite de commandes, tapez :

```
1 set quic profile <profile_name> -transport_param <value>
2 <!--NeedCopy-->
```


Exemple :

```
set quic profile quic_http3 -ackDelayExponent 10 -activeConnectionIDlimit 4
```

Les différents paramètres de transport QUIC sont les suivants :

-ackDelayExponent. Valeur entière annoncée par Citrix ADC sur le point de terminaison QUIC distant, indiquant un exposant que le point de terminaison QUIC distant doit utiliser, pour décoder le champ AcK Delay dans les trames QUIC ACK envoyées par Citrix ADC.

-activeConnectionIDlimit. Valeur entière annoncée par Citrix ADC sur le point de terminaison QUIC distant. Il spécifie le nombre maximal d'ID de connexion QUIC à partir du point de terminaison QUIC distant, que Citrix ADC est prêt à stocker.

-activeConnectionMigration. Spécifiez si Citrix ADC doit autoriser le point de terminaison QUIC distant à effectuer une migration de connexion QUIC active.

-congestionCtrlAlgorithm. Spécifiez l'algorithme de contrôle de la congestion à utiliser pour les connexions QUIC.

-initialMaxData. Valeur entière annoncée par Citrix ADC sur le point de terminaison QUIC distant, spécifiant la valeur initiale, en octets, pour la quantité maximale de données pouvant être envoyées sur une connexion QUIC.

-initialMaxStreamDataBidiLocal. Valeur entière annoncée par Citrix ADC sur le point de terminaison QUIC distant, spécifiant la limite de contrôle de flux initiale, en octets, pour les flux QUIC bidirectionnels initiés par Citrix ADC.

-initialMaxStreamDataBidiRemote. Valeur entière annoncée par Citrix ADC sur le point de terminaison QUIC distant, spécifiant la limite de contrôle de flux initiale, en octets, pour les flux QUIC bidirectionnels initiés par le point de terminaison QUIC distant.

-initialMaxStreamDataUni. Valeur entière annoncée par Citrix ADC sur le point de terminaison QUIC distant, spécifiant la limite de contrôle de flux initiale, en octets, pour les flux unidirectionnels initiés par le point de terminaison QUIC distant.

-initialMaxStreamsBidi. Valeur entière annoncée par Citrix ADC sur le point de terminaison QUIC distant, spécifiant le nombre maximal de flux bidirectionnels initiaux que doit initier le point de terminaison QUIC distant.

-initialMaxStreamsUni. Valeur entière annoncée par Citrix ADC sur le point de terminaison QUIC distant, spécifiant le nombre maximal de flux unidirectionnels initiaux que doit initier le point de terminaison QUIC distant.

-maxAckDelay. Valeur entière annoncée par Citrix ADC sur le point de terminaison QUIC distant, spécifiant la durée maximale, en millisecondes, pendant laquelle Citrix ADC retarde l'envoi des accusés de réception.

-maxIdleTimeout. Valeur entière annoncée par Citrix ADC sur le point de terminaison QUIC distant, spécifiant le délai d'inactivité maximal, en secondes, pour une connexion QUIC. Une connexion QUIC qui reste inactive, plus longtemps que le minimum des valeurs de délai d'attente d'inactivité annoncées par Citrix ADC et le point de terminaison QUIC distant, et trois fois le délai d'attente de sonde (PTO) actuel, sera supprimée silencieusement par Citrix ADC.

-maxUDPPayloadSize. Valeur entière annoncée par Citrix ADC sur le point de terminaison QUIC distant, spécifiant la taille de la plus grande charge utile du datagramme UDP, en octets, que Citrix ADC est disposée à recevoir sur une connexion QUIC.

-newTokenValidityPeriod. Valeur entière, spécifiant la période de validité, en secondes, des jetons de validation d'adresse émis via les trames QUIC NEW_TOKEN envoyées par Citrix ADC.
-retryTokenValidityPeriod. Valeur entière, spécifiant la période de validité, en secondes, des jetons de validation d'adresse émis via des paquets de nouvelle tentative QUIC envoyés par Citrix ADC.
-statelessAddressValidation. Spécifiez si Citrix ADC doit effectuer une validation d'adresse sans état pour les clients QUIC, en envoyant des jetons dans des paquets de nouvelle tentative QUIC lors de l'établissement de la connexion QUIC et en envoyant des jetons dans des trames QUIC NEW_TOKEN après l'établissement de la connexion QUIC.

Étape 2 : Associez le profil QUIC défini par l'utilisateur à un serveur virtuel d'équilibrage de charge de type http_quic

À l'invite de commandes, tapez :

```
set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]  <
    serviceName>@] [-persistenceType <persistenceType>] [-
    quicProfileName <string>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver lb-http3 -quicProfileName quic_http3
```

Activer et lier HTTP/3 sur un serveur virtuel HTTP_QUIC

Pour activer HTTP/3 sur un serveur virtuel HTTP_QUIC, un ensemble de paramètres de configuration est ajouté à la configuration du profil HTTP. Pour faciliter la configuration, lorsque vous ajoutez un serveur virtuel HTTP_QUIC, un nouveau profil HTTP par défaut/intégré est disponible sur l'appliance. Les paramètres de prise en charge du protocole HTTP/3 sont définis sur ENABLED et sont également limités aux serveurs virtuels HTTP_QUIC (applicable si vous choisissez de ne pas associer le serveur virtuel HTTP_QUIC à un profil HTTP ajouté par l'utilisateur). La valeur des paramètres HTTP/3 dans le profil HTTP décide de sélectionner le protocole HTTP/3 et de faire de la publicité lors du traitement de l'extension TLS ALPN (Application Layer Protocol Negotiation), pendant la prise de contact du protocole QUIC.

Vous pouvez créer un profil HTTP/3 et spécifier des paramètres HTTP pour le service HTTP/3 et le serveur virtuel d'équilibrage de charge. Vous devez soit créer un profil défini par l'utilisateur, soit utiliser le profil HTTP/3 intégré et lier le profil au serveur virtuel d'équilibrage de charge.

Étape 1 : configurer un profil HTTP/3 défini par l'utilisateur
À l'invite de commandes, tapez :

```
Add ns httpProfile <profile_name> -http3 ENABLED
<!--NeedCopy-->
```

Exemple :

```
add ns httpProfile http3_quic -http3 ENABLED
```

Étape 2 : Lier le profil HTTP/3 défini par l'utilisateur à un serveur virtuel d'équilibrage de charge de type http_quic
À l'invite de commandes, tapez :

```
set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]  <
   serviceName>@] [-persistenceType <persistenceType>] [-
   httpProfileName <string>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver lb-http3 -httpProfileName http3_quic
```

Lier la paire de clés de certificat SSL avec le serveur virtuel HTTP_QUIC

Pour traiter le trafic chiffré, vous devez ajouter une paire de clés de certificat SSL et la lier au serveur virtuel HTTP_QUIC.

À l'invite de commandes, tapez :

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>

<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver lb-http3 -certkeyName rsa_certkeypair
```

Pour plus d'informations, consultez la rubrique Bind SSL Certificate .

Lier les paramètres du protocole SSL/TLS à un serveur virtuel HTTP_QUIC

Les serveurs virtuels de type HTTP_QUIC ont une fonctionnalité de serveur TLS 1.3 intégrée, car le protocole QUIC utilise TLS 1.3 comme composant de sécurité obligatoire. Pour faciliter la configuration lors de l'ajout d'un serveur virtuel HTTP_QUIC, un nouveau profil SSL par défaut ou intégré de type Quic-Frontend est ajouté. Le profil SSL dispose de la version TLS 1.3 activée avec les suites de chiffrement TLS 1.3 (et les courbes elliptiques) configurées. Le profil SSL doit ensuite être lié aux nouveaux serveurs virtuels HTTP_QUIC ajoutés.
Vous pouvez créer un profil SSL et spécifier des paramètres de chiffrement SSL pour le service TLP 1.1 et le serveur virtuel d'équilibrage de charge. Vous devez soit créer un profil défini par l'utilisateur, soit utiliser le profil SSL intégré et lier le profil au serveur virtuel d'équilibrage de charge.

Étape 1 : configurer un profil SSL défini par l'utilisateur
À l'invite de commandes, tapez :

```
add ssl profile <name> -sslprofileType QUIC-FrontEnd
<!--NeedCopy-->
```

Exemple :

```
add ssl profile ssl_profile1 -sslprofileType QUIC-FrontEnd -tls13 ENABLED -
tls12 DISABLED -tls11 DISABLED -tls1 DISABLED
```

Étape 2 : Lier le profil SSL défini par l'utilisateur à un serveur virtuel d'équilibrage de charge de type HTTP_QUIC
À l'invite de commandes, tapez :

```
set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]  <
    serviceName>@] [-persistenceType <persistenceType>] [-
    httpProfileName <string>]
<!--NeedCopy-->
```

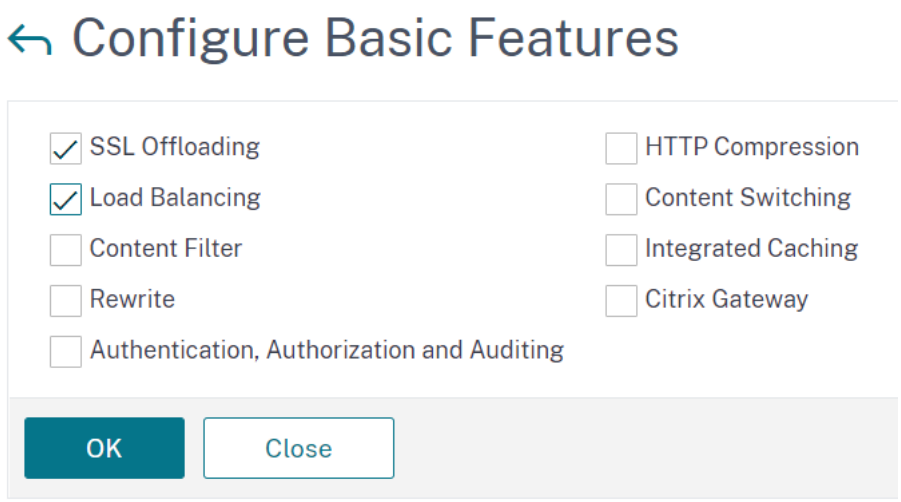
Exemple :

```
set ssl vserver lb-http3 -sslprofile ssl_profile1
```

Activer les fonctionnalités SSL et d'équilibrage de charge à l'aide de l'interface graphique

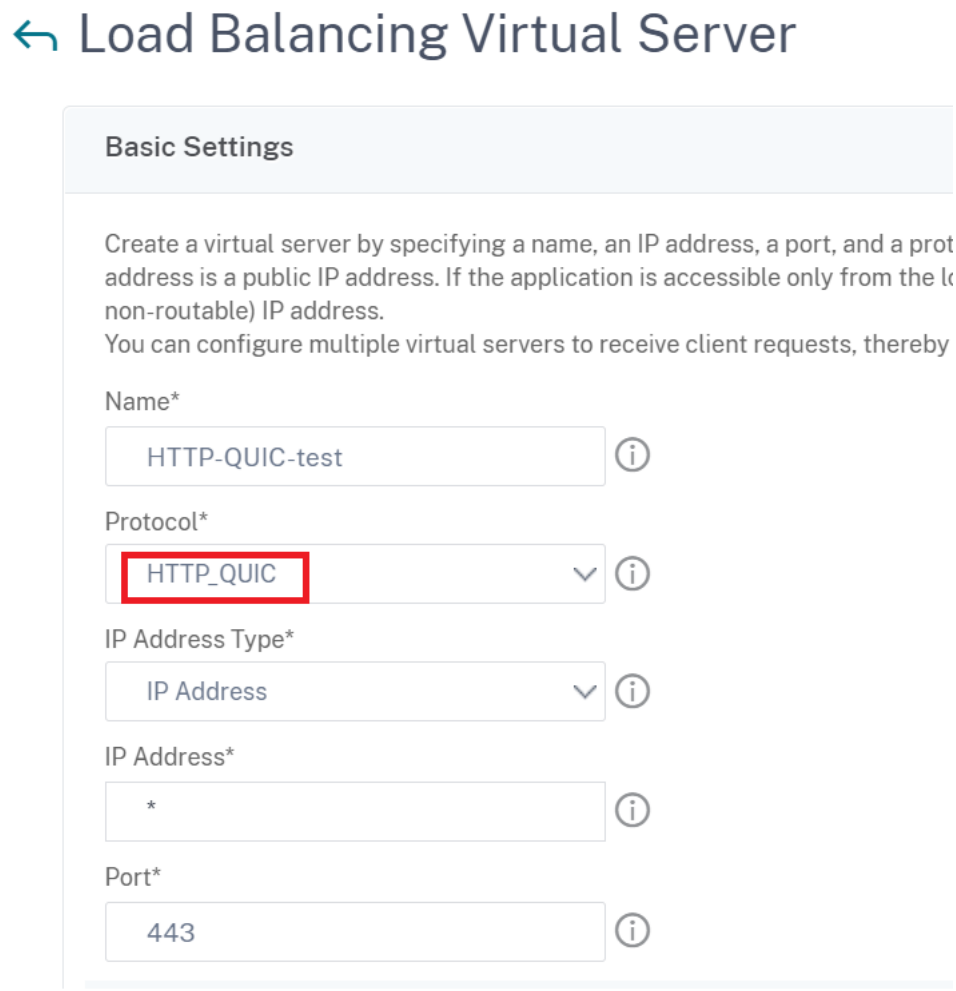
Procédez comme suit pour activer les fonctionnalités SSL et d'équilibrage de charge :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Sur la page **Configurer les fonctionnalités de base**, sélectionnez **SSL** et **équilibrage de charge**.
3. Cliquez sur **OK**, puis sur **Fermer**.



Ajoutez des serveurs virtuels d'équilibrage de charge et de commutation de contenu (facultatif) de type HTTP_QUIC à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel d'équilibrage de charge de type HTTP_QUIC.
3. Dans la page **Serveur virtuel d'équilibrage de charge**, cliquez sur **Profils**.
4. Dans la section **Profils**, sélectionnez le type de profil QUIC. Remarque : les profils QUIC, HTTP/3 et SSL sont intégrés.
5. Cliquez sur **OK**, puis sur **Terminé**.

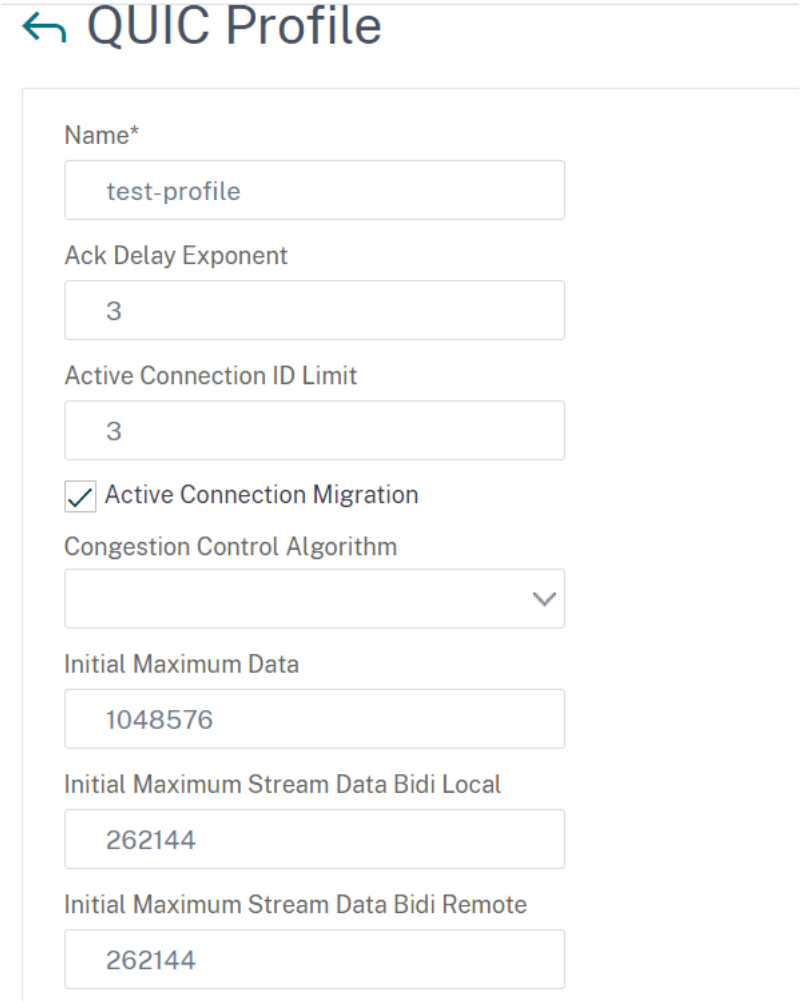


Associez les paramètres du protocole QUIC au serveur virtuel HTTP_QUIC à l'aide de l'interface graphique

Étape 1 : Ajouter un profil QUIC

1. Accédez à **Système > Profils > Profil QUIC**.
2. Cliquez sur **Ajouter**.
3. Dans la page Profil QUIC, définissez les paramètres suivants. Pour une description détaillée de chaque paramètre, reportez-vous à la section Associate QUIC Protocol CLI.
   a) `Ack Delay` Exposant
   b) Active Connection ID Limit
   c) Active Connection Migration
   d) Congestion Control Algorithm
   e) Initial Maximum Data

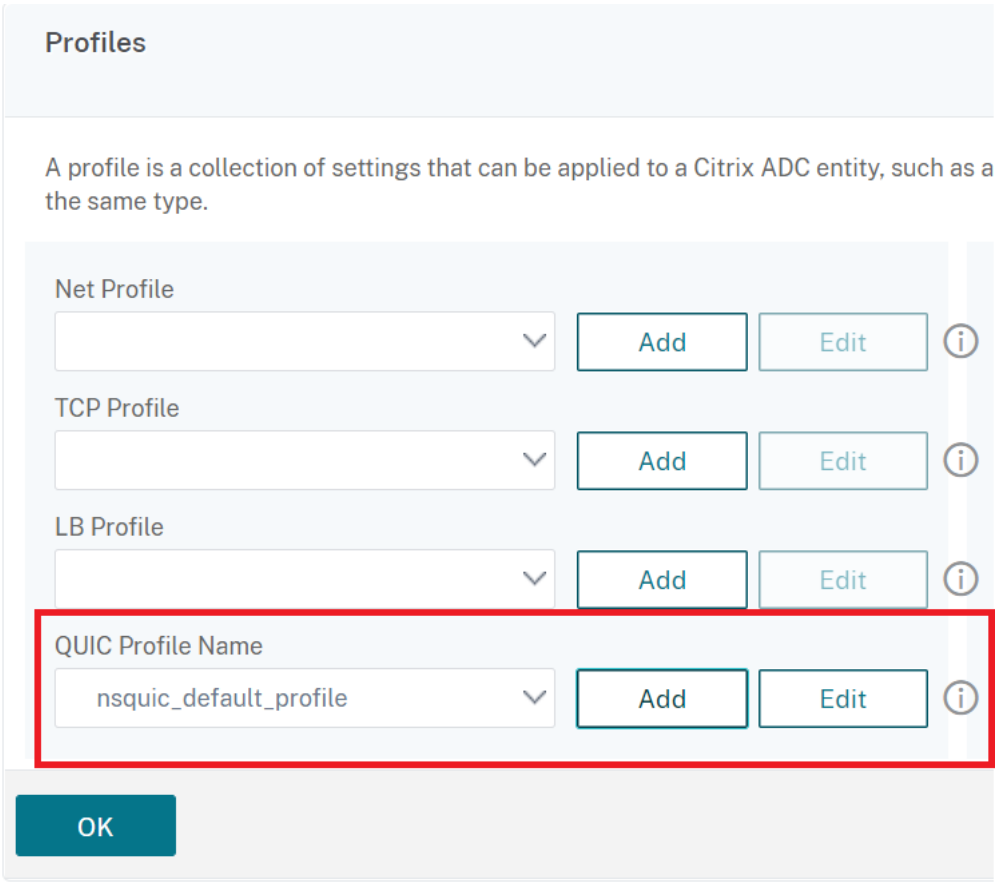
f) Initial Maximum Stream Data Bidi Local
g) Initial Maximum Stream Data Bidi Remote
h) Initial Maximum Stream Data Unit
i) Initial Maximum Stream bidi
j) Initial Maximum Stream Uni
k) Maximum Acknowledgment Delay
l) Maximum Idle Timeout
m) Maximum UDP Data GramsperBurst
n) New Token Validity Period
o) Retry Token Validity Period
p) Stateless Address Validation



Étape 2 : Associer le profil QUIC au serveur virtuel d'équilibrage de charge de type HTTP_QUIC

1. Dans la section **Profils**, sélectionnez le profil QUIC. Remarque : les profils QUIC, HTTP/3 et SSL sont intégrés.

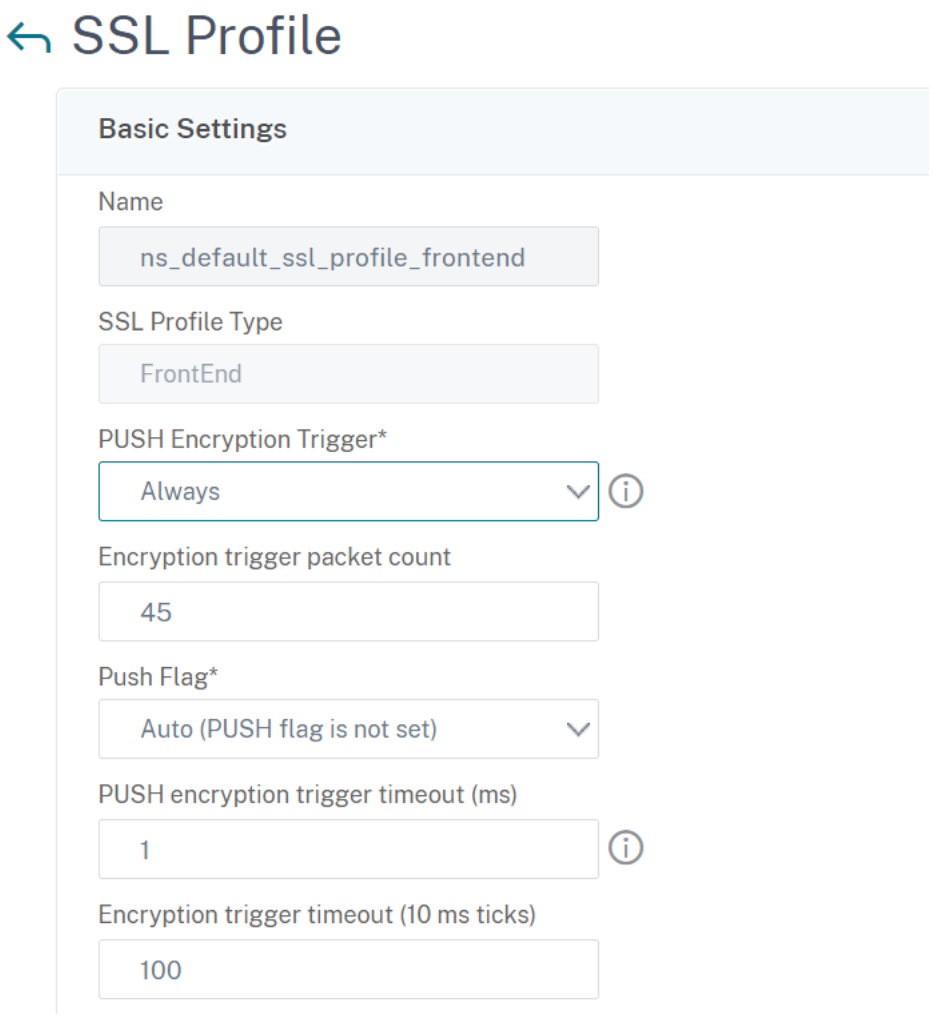
2. Cliquez sur **OK**, puis sur **Terminé**.



Associez les paramètres du protocole SSL/TLS au serveur virtuel de type SSL à l'aide de l'interface graphique

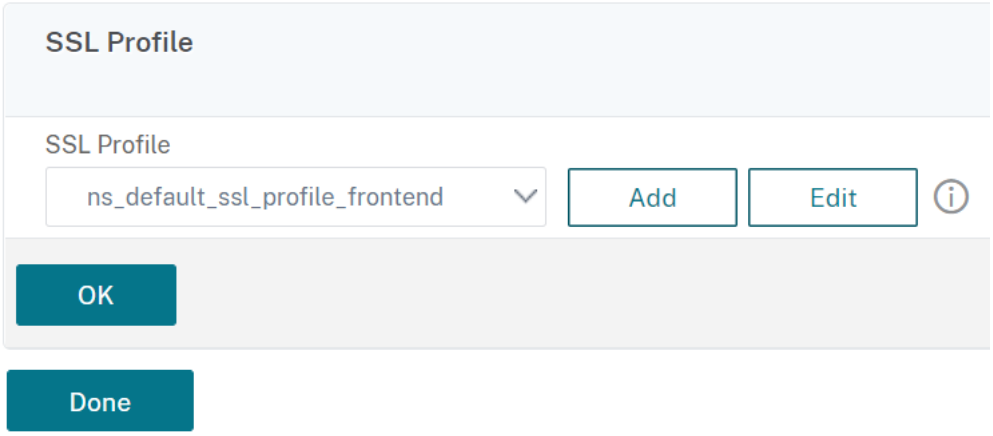
Étape 1 : Ajouter un profil SSL

1. Accédez à **Système > Profils > Profil SSL**.
2. Cliquez sur **Ajouter**.
3. Dans la page **Profil QUIC**, définissez les paramètres SSL. Pour une description détaillée, reportez-vous à la rubrique Configuration du profil SSL.
4. Cliquez sur **OK** et **Fermer**.



Étape 2 : Associez le profil SSL au serveur virtuel d'équilibrage de charge de type SSL.

1. Dans la section **Profils**, sélectionnez le profil SSL.
2. Cliquez sur **OK**, puis sur **Terminé**.



Afficher les statistiques QUIC et HTTP/3

Les commandes suivantes affichent un résumé détaillé des statistiques QUIC et HTTP3. À l'invite de commandes, tapez ce qui suit :

```
1 > stat quic
2 > stat quic  - detail
3 <!--NeedCopy-->
```

Pour effacer l'affichage des statistiques, tapez l'une des options suivantes :

```
1 > stat quic -clearstats basic
2 > stat quic -clearstats full
3
4 <!--NeedCopy-->
```

Pour afficher un résumé détaillé des statistiques HTTP/3 :

```
1 > stat http3
2 > stat http3  - detail
3 <!--NeedCopy-->
```

Pour effacer l'affichage des statistiques, tapez l'une des options suivantes :

```
1 > stat http3 -clearstats basic
2 > stat http3 -clearstats full
3 <!--NeedCopy-->
```

Configuration de la stratégie pour le trafic HTTP/3

October 5, 2021

HTTP/3 utilise le transport QUIC basé sur UDP. Si vous aviez défini une expression de stratégie pour le serveur virtuel HTTP ou SSL qui inclut des expressions de stratégie TCP, elle ne peut plus être utilisée avec un serveur virtuel HTTP_QUIC. Toutes les autres stratégies qui n'ont pas de TCP ou d'expressions classiques peuvent être liées à un serveur virtuel HTTP_QUIC. Pour que les stratégies prennent effet, vous devez vous assurer que les stratégies d'entités sont liées aux points de liaison globaux nouvellement ajoutés, conformément aux indications suivantes.

- HTTPQUIC_REQ_DEFAULT
- HTTPQUIC_REQ_OVERRIDE
- TTPQUIC_RES_DEFAULT

- HTTPQUIC_RES_OVERRIDE

Les stratégies peuvent également être liées à des points de liaison de serveurs virtuels spécifiques :

- REQUEST
- RESPONSE

Pour plus d'informations, consultez la rubrique Lier la stratégie à l'aide d'une infrastructure de stratégie avancée .

Voici les stratégies prises en charge pour la configuration HTTP sur QUIC :

- Répondeur
- Réécrire
- Compression HTTP
- Mise en cache intégrée
- Pare-feu d'application Web
- Transformation d'URL
- SSL
- Optimisation frontale (FEO)
- AppQoE

Configuration de la stratégie de répondeur pour le trafic HTTP/3

Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies de répondeur. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.

Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison globaux QUIC. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajout d'une action de répondeur pour rediriger les URL

Pour ajouter une action de répondeur, à l'invite de commandes, tapez :

```
1 add responder action <name> <type> (<target> | <htmlpage>) [-comment <
     string>] [-responseStatusCode <positive_integer>] [-reasonPhrase <
     expression>] [-headers <name(value)> ...]
2 <!--NeedCopy-->
```

Exemple :

```
add responder action redirectURL redirect "\"https://www.citrix.com/\""
```


Ajouter une stratégie de répondeur

Pour ajouter une stratégie de répondeur, à l'invite de commandes, tapez :

```
1 add responder policy <name> <rule> <action> [<undefAction>] [-comment <
     string>] [-logAction <string>] [-appflowAction <string>]
2 <!--NeedCopy-->
```

Exemple :

```
add responder policy res-pol "CLIENT.IP.SRC.IN_SUBNET(10.10.10.10/32)"
redirectURL
```

Ajout d'une expression UDP basée sur une stratégie de répondeur

Pour ajouter une expression UDP basée sur une stratégie de répondeur, à l'invite de commandes, tapez :

```
1 add responder policy <name> <rule> <action> [<undefAction>] [-comment <
     string>] [-logAction <string>] [-appflowAction <string>]
2 <!--NeedCopy-->
```

Exemple :

```
add responder policy redirectCitrixUdp "CLIENT.UDP.DSTPORT.EQ(443)"redirectURL
```

Lier une expression UDP basée sur une stratégie de répondeur avec un serveur virtuel d'équilibrage de charge basé sur HTTP/3 QUIC

Pour lier une expression UDP basée sur une stratégie de répondeur à un serveur virtuel d'équilibrage de charge, à l'invite de commandes, tapez :

```
1 bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
      ) | <serviceGroupName>@ |         (-policyName <string>@  [-
     priority <positive_integer>]  [-gotoPriorityExpression <expression>]
       [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
     analyticsProfile <string>@)
2 <!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName redirectCitrixUdp -priority 9 -gotoPriorityExpres
 END -type REQUEST
```


Lier la stratégie de répondeur avec un serveur virtuel d'équilibrage de charge basé sur HTTP/3 QUIC

Pour lier une stratégie de répondeur à un serveur virtuel d'équilibrage de charge, à l'invite de commandes, tapez :

```
bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
     ) | <serviceGroupName>@ |         (-policyName <string>@  [-
    priority <positive_integer>]  [-gotoPriorityExpression <expression>]
      [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
    analyticsProfile <string>@)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName redirectCitrixUdp -priority 10 -
gotoPriorityExpression END -type REQUEST
```

Lier la stratégie du répondeur au point de liaison global HTTP/3

Pour lier une stratégie de répondeur au point de liaison global HTTP/3, à l'invite de commandes, tapez :

```
bind responder global <policyName> <priority>  [<gotoPriorityExpression
    >] [-type <type>] [-invoke (<labelType>  <labelName>) ] bind
    responder global redirectCitrixUdp 3 -type HTTPQUIC_REQ_DEFAULT
<!--NeedCopy-->
```

Exemple :

```
bind responder global redirectCitrixUdp 3 -type HTTPQUIC_REQ_DEFAULT
```

> **Remarque :**
>
> Pour plus d'informations, consultez la documentation sur les stratégies de répondeur.

Configuration de la stratégie de réécriture pour le trafic HTTP/3

Les serveurs virtuels HTTP sur QUIC prennent en charge les stratégies de réécriture. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.

Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Vous trouverez ci-dessous les étapes de configuration permettant de configurer la stratégie de réécriture pour HTTP3 sur QUIC.

Ajout d'une action de réécriture pour HTTP sur QUIC

Pour ajouter une action de réécriture, à l'invite de commandes, tapez :

```
1 add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-
     search <expression>] [-refineSearch <expression>] [-comment <string
     >]
2 <!--NeedCopy-->
```

Exemple :

```
add rewrite action http3-altsvc-action insert_http_header Alt-Svc q/"h3
-29=\":443\"; ma=3600; persist=1"/
```

Ajouter une stratégie de réécriture pour HTTP sur QUIC

Pour ajouter une action d'écriture, à l'invite de commandes, tapez :

```
1 add rewrite policy <name> <rule> <action> [<undefAction>] [-comment  <
     string>] [-logAction <string>]
2 <!--NeedCopy-->
```

Exemple :

```
add rewrite policy http3-altsvc-policy true http3-altsvc-action
```

Lier la stratégie de réécriture au serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC

Pour lier la stratégie de réécriture au serveur virtuel d'équilibrage de charge, à l'invite de commandes, tapez :

```
1 bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>] )
      | <serviceGroupName>@ | (-policyName <string>@ [-priority <
     positive_integer>] [-gotoPriorityExpression <expression>] [-type <
     type>] [-invoke (<labelType> <labelName>) ] ) | -analyticsProfile  <
     string>@)
2 <!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName http3-altsvc-policy -priority 10 -type
 RESPONSE
```


Lier la stratégie de réécriture au point de liaison global HTTP/3

```
To bind a responder policy with HTTP/3 global bind point, at the
    command prompt, type:
bind rewrite global <policyName> <priority> [<gotoPriorityExpression>]
     [-type <type>] [-invoke (<labelType> <labelName>)]
<!--NeedCopy-->
```

Exemple :

```
bind rewrite global http3-altsvc-policy 3 -type HTTPQUIC_RES_DEFAULT
```

> **Remarque :**
>
> Pour plus d'informations, consultez la documentation sur la stratégie de réécriture.

Configuration de la stratégie de compression pour le trafic HTTP/3

Lorsque Citrix ADC reçoit une réponse HTTP d'un serveur, il évalue les stratégies de compression intégrées et les stratégies de compression personnalisées pour déterminer s'il faut compresser la réponse et, le cas échéant, le type de compression à appliquer. Les priorités attribuées aux stratégies déterminent l'ordre dans lequel les stratégies sont mises en correspondance avec les demandes.
Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies de compression. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.
Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajouter une stratégie de compression

Pour ajouter une stratégie de compression, à l'invite de commandes, tapez :

```
add cmp policy <name> -rule <expression> -resAction <string>
<!--NeedCopy-->
```

Exemple :

```
add cmp policy udp_port_cmp_policy -rule "CLIENT.UDP.DSTPORT.EQ(443)"-
resAction COMPRESS
```


Lier une stratégie de compression avec un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC

Pour lier une stratégie de transformation d'URL à un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC, à l'invite de commandes, tapez :

```
bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
    ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
    positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
     REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
    -analyticsProfile <string>@)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName udp_port_cmp_policy -priority 10 -type
 RESPONSE
```

Compression de liaison globale au point de liaison global HTTP/3

Pour lier une stratégie de compression avec le point de liaison global HTTP/3, à l'invite de commandes, tapez :

```
bind compression global <policyName> <priority>  [<
    gotoPriorityExpression>] [-type <type>] [-invoke (<labelType>  <
    labelName>) ] bind responder global redirectCitrixUdp 3 -type
    HTTPQUIC_REQ_DEFAULT
<!--NeedCopy-->
```

Exemple :

```
bind cmp global udp_port_cmp_policy -priority 100 -type HTTPQUIC_RES_DEFAULT
 Global built-in compression policies
```

Après la mise à niveau de votre appliance vers Citrix ADC version 13.0 build 82.x, les stratégies de compression suivantes seront automatiquement liées au point de liaison HTTP/3 par défaut.

```
> sho cmp global -type HTTPQUIC_RES_DEFAULT
        Policy Name: ns_adv_nocmp_xml_ie
        Priority: 8700
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_nocmp_mozilla_47
        Priority: 8800
        GotoPriorityExpression: END
```



```
10          Type: HTTPQUIC_RES_DEFAULT
11
12          Policy Name: ns_adv_cmp_mscss
13          Priority: 8900
14          GotoPriorityExpression: END
15          Type: HTTPQUIC_RES_DEFAULT
16
17          Policy Name: ns_adv_cmp_msapp
18          Priority: 9000
19          GotoPriorityExpression: END
20          Type: HTTPQUIC_RES_DEFAULT
21
22          Policy Name: ns_adv_cmp_content_type
23          Priority: 10000
24          GotoPriorityExpression: END
25          Type: HTTPQUIC_RES_DEFAULT
26  <!--NeedCopy-->
```

Si elles ne sont pas liées, les commandes suivantes peuvent être configurées via l'invite de commandes et vous pouvez configurer sur votre appliance.

```
bind cmp global ns_adv_nocmp_xml_ie -priority 8700 -gotoPriorityExpression
END -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_nocmp_mozilla_47 -priority 8800 -gotoPriorityExpression
 END -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_mscss -priority 8900 -gotoPriorityExpression END
 -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_msapp -priority 9000 -gotoPriorityExpression END
 -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_content_type -priority 10000 -gotoPriorityExpression
 END -type HTTPQUIC_RES_DEFAULT
```

Pour plus d'informations, voir Configuration de la stratégie de compression.

Configuration de stratégie de mise en cache pour le trafic HTTP/3

Le cache intégré fournit un stockage en mémoire sur l'appliance Citrix ADC et fournit du contenu Web aux utilisateurs sans nécessiter un aller-retour vers un serveur d'origine. Pour le contenu statique, le cache intégré nécessite peu de configuration initiale. Après avoir activé la fonctionnalité de cache intégré et effectué la configuration de base (par exemple, en déterminant la quantité de mémoire de l'appliance Citrix ADC que le cache est autorisé à utiliser), le cache intégré utilise des

stratégies intégrées pour stocker et diffuser des types spécifiques de contenu statique, y compris des pages Web et des fichiers image simples. Vous pouvez également configurer le cache intégré pour stocker et diffuser du contenu dynamique marqué comme non mis en cache par les serveurs Web et d'applications (par exemple, les enregistrements de base de données et les cotations boursières).
Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies de cache. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.

Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajouter un groupe de contenu cache

Pour ajouter le groupe de contenu du cache, à l'invite de commandes, tapez :

```
1 add cache contentGroup <name> [-weakPosRelExpiry <secs> | -relExpiry <
      secs> | -relExpiryMilliSec <msecs> | -absExpiry <HH:MM> ... | -
      absExpiryGMT <HH:MM> ...] [-heurExpiryParam <positive_integer>] [-
      weakNegRelExpiry <secs>] [-maxResSize <KBytes>] [-memLimit <MBytes>]
      ...
2 <!--NeedCopy-->
```

Exemple :

```
add cache contentGroup DEFAULT -maxResSize 500
```

Ajouter une stratégie de cache

Pour ajouter une stratégie de cache, à l'invite de commandes, tapez :

```
1 add cache policy <policyName> -rule <expression> -action <action>  [-
      storeInGroup <string>] [-invalGroups <string> ...] [-invalObjects <
      string> ...] [-undefAction ( NOCACHE | RESET )] add cache policy <
      name> <rule> <profileName> [-comment <string>]  [-logAction <string
      >]
2 <!--NeedCopy-->
```

Exemple :

```
add cache policy ctx_doc_pdf -rule "HTTP.REQ.URL.ENDSWITH(\".pdf\")"-action
 CACHE -storeInGroup DEFAULT
```


Lier une stratégie de cache avec un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC

Pour lier une stratégie de cache avec un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC, à l'invite de commandes, tapez :

```
bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
    ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
    positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
     REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
    -analyticsProfile <string>@)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName ctx_doc_pdf -priority 100 -type
REQUEST
```

Stratégie de cache de liaison globale au point de liaison global HTTP/3

Pour lier un point de liaison global HTTP/3 de stratégie de cache :

```
bind cache global <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Exemple :

```
bind cache global ctx_doc_pdf -priority 3 -type HTTPQUIC_REQ_DEFAULT
```

Pour plus d'informations, voir Configuration intégrée de la stratégie de cache.

Stratégies globales de cache intégrées

Après la mise à niveau de votre appliance vers Citrix ADC version 13.0 build 82.x, les stratégies de cache suivantes seront automatiquement liées au point de liaison HTTP/3 par défaut.

Lors de la mise à niveau vers la version 13.0 82.x, les stratégies de cache suivantes sont automatiquement liées au point de liaison HTTP/3 par défaut.

```
> sho cache global -type HTTPQUIC_REQ_DEFAULT
1)      Policy Name: NOPOLICY
        Priority: 185883
        GotoPriorityExpression: USE_INVOCATION_RESULT
```



```
5          Invoke type: policylabel        Invoke name:
               _httpquicReqBuiltinDefaults
6          Global bindpoint: HTTPQUIC_REQ_DEFAULT
7
8   Done
9   > sho cache global -type HTTPQUIC_RES_DEFAULT
10  1)      Policy Name: NOPOLICY
11         Priority: 185883
12         GotoPriorityExpression: USE_INVOCATION_RESULT
13         Invoke type: policylabel        Invoke name:
               _httpquicResBuiltinDefaults
14         Global bindpoint: HTTPQUIC_RES_DEFAULT
15
16  <!--NeedCopy-->
```

Après une mise à niveau, si les stratégies ne sont pas liées, vous pouvez utiliser les commandes suivantes pour lier et enregistrer manuellement la configuration.

```
1  add cache policylabel _httpquicReqBuiltinDefaults -evaluates
       HTTPQUIC_REQ
2
3  add cache policylabel _httpquicResBuiltinDefaults -evaluates
       HTTPQUIC_RES
4
5  bind cache policylabel _httpquicReqBuiltinDefaults -policyName
       _nonGetReq -priority 100
6
7  bind cache policylabel _httpquicReqBuiltinDefaults -policyName
       _advancedConditionalReq -priority 200
8
9  bind cache policylabel _httpquicReqBuiltinDefaults -policyName
       _personalizedReq -priority 300
10
11 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _uncacheableStatusRes -priority 100
12
13 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _uncacheableVaryRes -priority 200
14
15 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _uncacheableCacheControlRes -priority 300
16
17 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _cacheableCacheControlRes -priority 400
18
```



```
19 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _uncacheablePragmaRes -priority 500
20
21 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _cacheableExpiryRes -priority 600
22
23 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _imageRes -priority 700
24
25 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _personalizedRes -priority 800
26
27 bind cache global NOPOLICY -priority 185883 -gotoPriorityExpression
       USE_INVOCATION_RESULT -type HTTPQUIC_REQ_DEFAULT -invoke policylabel
        _httpquicReqBuiltinDefaults
28
29 bind cache global NOPOLICY -priority 185883 -gotoPriorityExpression
       USE_INVOCATION_RESULT -type HTTPQUIC_RES_DEFAULT -invoke policylabel
        _httpquicResBuiltinDefaults
30
31 <!--NeedCopy-->
```

> **Remarque :**
>
> Les deux premières commandes de la liste des commandes, et les deux dernières commandes d'une même liste, sont incluses dans un souci d'exhaustivité. Vous pouvez rencontrer une erreur lors de l'exécution des quatre commandes, car elles sont déjà exécutées au moment du redémarrage de l'appliance. Mais vous pouvez ignorer ces erreurs.

Configuration de la stratégie de transformation d'URL pour le trafic HTTP/3

La transformation d'URL modifie toutes les URL des requêtes désignées depuis une version externe vue par des utilisateurs externes vers une URL interne vue uniquement par vos serveurs Web et vos administrateurs. Vous pouvez rediriger les demandes des utilisateurs de manière transparente, sans exposer la structure de votre réseau aux utilisateurs. Vous pouvez également modifier des URL internes complexes que les utilisateurs peuvent avoir de la difficulté à mémoriser en URL externes plus simples et plus facilement mémorisées.

Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies de cache. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.

Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés.

Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajouter un profil de transformation d'URL

Pour ajouter un profil de transformation d'URL, à l'invite de commandes, tapez :

```
1 add transform profile <name> [-type URL]
2 <!--NeedCopy-->
```

Exemple :

```
add transform profile msapps
```

Action Ajouter une transformation d'URL

Pour ajouter une action de transformation d'URL, à l'invite de commandes, tapez :

```
1 add transform action <name> <profileName> <priority> [-state ( ENABLED
      | DISABLED )]
2 <!--NeedCopy-->
```

Exemple :

```
add transform action docx2doc msapps 2
```

Action Ajouter une transformation d'URL

Pour ajouter une action de transformation d'URL afin de remplacer l'URL, à l'invite de commandes, tapez :

```
1 add transform action <name> <profileName> <priority> [-state ( ENABLED
      | DISABLED )]
2 <!--NeedCopy-->
```

Exemple :

```
add transform action docx2doc msapps 1
```

Stratégie Ajouter une transformation d'URL

Pour ajouter une stratégie de transformation d'URL, à l'invite de commandes, tapez :


```
add transform policy <name> <rule> <profileName> [-comment <string>]
    [-logAction <string>]
<!--NeedCopy-->
```

Exemple :

```
add transform policy urltrans_udp "CLIENT.UDP.DSTPORT.EQ(443)"msapps
```

Stratégie de transformation d'URL Lier avec un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC

Pour lier une stratégie de transformation d'URL à un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC, à l'invite de commandes, tapez :

```
bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
    ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
    positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
     REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
    -analyticsProfile <string>@)
<!--NeedCopy-->
```

Exemple :

```
bind lb vs lb-http3 -policyName urltrans_udp -type REQUEST -priority 8
```

Lier une stratégie globale de transformation d'URL avec un serveur virtuel d'équilibrage de charge basé sur HTTP/3 QUIC

Pour lier un point de liaison global HTTP/3 de stratégie de transformation d'URL, à l'invite de commandes, tapez :

```
bind transform global <policyName> <priority>  [<gotoPriorityExpression
    >] [-type <type>] [-invoke (<labelType>  <labelName>) ]
<!--NeedCopy-->
```

Exemple :

```
bind transform global urltrans_udp 100 -type HTTPQUIC_REQ_DEFAULT
```

Pour plus d'informations, voir Configuration de la stratégie de transformation d'URL.

Configuration de la stratégie d'optimisation frontale (FEO) pour le trafic HTTP/3

Les protocoles HTTP qui sous-tendent les applications Web ont été développés à l'origine pour prendre en charge la transmission et le rendu de pages Web simples. Les nouvelles technologies telles que

JavaScript et les feuilles de style en cascade (CSS), ainsi que les nouveaux types de médias tels que les vidéos Flash et les images riches en graphiques, imposent de lourdes exigences sur les performances front-end, c'est-à-dire sur les performances au niveau du navigateur. La fonctionnalité d'optimisation frontale (FEO) Citrix ADC résout ces problèmes et réduit le temps de chargement et de rendu des pages Web.

> **Remarque :**
>
> `HTTP_QUIC _Override/Default_Request` Le type n'est pas pris en charge pour la liaison globale de la stratégie FEO.

Ajouter une action d'optimisation frontale (FEO)

Pour ajouter une action FEO, à l'invite de commandes, tapez :

```
1 add feo action <name> [-pageExtendCache] [<cacheMaxage>][-
      imgShrinkToAttrib] [-imgGifToPng] [-imgToWebp] [-imgToJpegXR] [-
      imgInline] [-cssImgInline] [-jpgOptimize] [-imgLazyLoad] [-cssMinify
      ] [-cssInline] [-cssCombine] [-convertImportToLink] [-jsMinify] [-
      jsInline] [-htmlMinify] [-cssMoveToHead] [-jsMoveToEND][-
      domainSharding <string> <dnsShards> ...] [-clientSideMeasurements]
2
3 <!--NeedCopy-->
```

Exemple :

```
add feo action feoact -imgGifToPng -pageExtendCache
```

Ajouter une stratégie d'optimisation frontale (FEO)

Pour ajouter une stratégie FEO, à l'invite de commandes, tapez :

```
add feo policy <name> <rule> <action>
```

Exemple :

```
add feo policy udp_feo_img "CLIENT.UDP.DSTPORT.EQ(443)"IMG_OPTIMIZE
```

Lier la stratégie FEO au serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC

Pour lier une stratégie FEO à un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC, à l'invite de commandes, tapez :

```
1 bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
      ) | <serviceGroupName>@ |         (-policyName <string>@  [-
      priority <positive_integer>]  [-gotoPriorityExpression <expression>]
```



```
        [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
      analyticsProfile <string>@)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName udp_feo_img -priority 4 -gotoPriorityExpression
 END -type REQUEST
```

Lier la stratégie FEO au point de liaison global HTTP/3

Pour lier une stratégie de cache au point de liaison global HTTP/3, à l'invite de commandes, tapez :

```
bind cache global <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Exemple :

```
bind cache global ctx_doc_pdf -priority 3 -type HTTPQUIC_REQ_DEFAULT
```

Pour plus d'informations, reportez-vous à la section Configuration de la stratégie d'optimisation frontale.

Configuration de la stratégie SSL pour le trafic HTTP/3

Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies SSL. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.
Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés.
Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.
Les stratégies SSL avec des actions prises en charge par TLSv1.3 ne s'appliquent qu'aux points de liaison HTTP/3 ou aux serveurs virtuels.

Ajouter une stratégie SSL

Pour ajouter une stratégie FEO, à l'invite de commandes, tapez :

```
add ssl policy <name> -rule <expression> [-action <string>] [-
    undefAction <string>] [-comment <string>]
<!--NeedCopy-->
```


Exemple :

```
add ssl policy ssl-pol -rule CLIENT.SSL.IS_SSL -action NOOP
```

Lier la stratégie SSL au serveur virtuel HTTP/3

Pour lier une stratégie SSL au serveur virtuel HTTP/3, à l'invite de commandes :

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Exemple :

```
bind ssl vserver lb-http3 -policyName ssl-pol -priority 4 -type REQUEST
```

Ajouter une stratégie SSL avec expression UDP pour la stratégie SSL

Pour ajouter une stratégie SSL avec une expression UDP, à l'invite de commandes :

```
1 add ssl policy <name> -rule <expression> [-action <string>] [-
     undefAction <string>] [-comment <string>]
2 <!--NeedCopy-->
```

Exemple :

```
add ssl policy ssl_udp_clnt -rule "CLIENT.UDP.DSTPORT.EQ(443)"-action NOOP
```

Lier une stratégie SSL avec une expression UDP au serveur virtuel HTTP/3

Pour lier une stratégie SSL avec une expression UDP au serveur virtuel HTTP/3, à l'invite de commandes, tapez

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Exemple :

```
bind ssl vs lb-http3 -policyName ssl_udp_clnt -priority 8 -type REQUEST
```

Ajouter une stratégie SSL pour le point de liaison CLIENTHELLO pour le trafic HTTP/3

Pour lier une stratégie SSL pour le point de liaison CLIENTHELLO pour le trafic HTTP/3, à l'invite de commandes, tapez :


```
bind ssl policylabel <labelName> <policyName> <priority> [<
    gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
<!--NeedCopy-->
```

Exemple :

```
add ssl policy ssl-pol-ch -rule "CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXCODE
(0x1301)"-action RESET
```

Lier la stratégie SSL au point de liaison CLIENTHELLO

Pour lier une stratégie SSL au point de liaison CLIENTHELLO, à l'invite de commandes, tapez :

```
bind ssl policylabel <labelName> <policyName> <priority> [<
    gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
<!--NeedCopy-->
```

Exemple :

```
bind ssl vs lb-http3 -policyName ssl-pol-ch -type CLIENTHELLO_REQ -priority
 100
```

Lier la stratégie SSL au point de liaison global HTTP/3

Pour lier une stratégie SSL au point de liaison global HTTP/3, à l'invite de commandes, tapez :

```
bind cache global <policy> -priority <positive_integer> [-gotoPriorityExpression
 <expression>] [-type <type>] [-invoke (<labelType> <labelName>)]
```

Exemple :

Voici un exemple de stratégie DATA liée à un point de liaison global HTTP/3 :

```
Bind ssl global -policyName ssl-pol-ch -priority 7 -type HTTPQUIC_DATA_DEFAULT
```

> **Remarque :**
>
> L'action de transfert pouvant être définie pour le point de liaison CLIENTHELLO pour les serveurs virtuels SSL n'est actuellement pas prise en charge pour les serveurs virtuels de type HTTP_QUIC.

Configuration de la stratégie de pare-feu d'application pour le trafic HTTP/3

Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies de pare-feu d'application Web. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées

sur TCP sont exclues et les expressions basées sur UDP sont incluses.
Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajouter une stratégie de pare-feu d'application Web avec une expression UDP

Pour ajouter une stratégie de pare-feu d'application Web avec une expression UDP, à l'invite de commandes :

```
1 add appfw policy <name> <rule> <profileName> [-comment <string>] [-
     logAction <string>]
2 <!--NeedCopy-->
```

Exemple :

```
add appfw policy appfw_udp "CLIENT.UDP.DSTPORT.EQ(443)"APPFW_BYPASS
```

Lier des expressions de journal avec une expression basée sur UDP pour le profil Web Application Firewall

Pour lier des expressions de journal au profil UDP for Web Application Firewall, à l'invite de commandes :

Exemple :

```
bind appfw profile APPFW_BLOCK -logExpression logexp-1 "CLIENT.UDP.DSTPORT.
EQ(443)"
```

Lier une stratégie de pare-feu d'application avec le serveur virtuel HTTP/3

Pour lier la stratégie de pare-feu d'application Web au serveur virtuel HTTP/3, à l'invite de commandes :

```
1 bind appfw policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Exemple :

```
bind lb vs lb-http3 -policyName appfw_udp -priority 3 -type REQUEST
```


Lier une stratégie de pare-feu d'application Web au point de liaison global HTTP/3

Pour lier une stratégie de pare-feu d'application Web au point de liaison global HTTP/3, à l'invite de commandes, tapez :

```
bind appfw global <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Exemple :

```
bind appfw global appfw_udp 100 -type HTTPQUIC_REQ_DEFAULT
```

Configuration de la stratégie AppQoE pour le trafic HTTP/3

Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies AppQoE. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.
Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajouter une stratégie AppQoE avec une expression basée sur UDP

Pour ajouter une stratégie AppQOE avec une expression UDP, à l'invite de commandes :

```
add AppQoE policy <name> <rule> <profileName> [-comment <string>] [-
    logAction <string>]
<!--NeedCopy-->
```

Exemple :

```
add appqoe policy appqoe-pol-udp -rule "CLIENT.UDP.DSTPORT.EQ(443)"-action
appqoe-act-basic-prhigh
```

Lier une stratégie AppQoE au serveur virtuel HTTP/3

Pour lier la stratégie AppQoE au serveur virtuel HTTP/3, à l'invite de commandes, tapez :

```
bind appqoe policylabel <labelName> <policyName> <priority> [<
    gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
<!--NeedCopy-->
```


Exemple :

```
bind lb vs lb-http3 -policyName appqoe-pol-udp -type REQUEST -priority 3
```

Lier la stratégie AppQoE au serveur virtuel HTTP_QUIC

Pour lier la stratégie AppQoE au serveur `HTTP_QUIC` virtuel, à l'invite de commandes, tapez :

```
1 bind appqoe <policy> -priority <positive_integer>  [-
     gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
     labelType> <labelName>) ]
2 <!--NeedCopy-->
```

Exemple :

```
bind lb vs lb-http3 -policyName appqoe-pol-primd -priority 8 -type REQUEST
```

Découverte du service HTTP/3

August 20, 2021

Le protocole HTTP repose sur l'utilisation de HTTP Alternative Services pour le serveur d'origine pour annoncer la disponibilité d'un service équivalent. La découverte de service HTTP/3 utilise également le même principe. Un point de terminaison HTTP/3 alternatif peut être annoncé à l'aide de l'une des méthodes suivantes :

- En-tête de réponse HTTP Alt-Svc
- Cadre HTTP/2 Alt-Svc dans la réponse
- Négociation du protocole de couche d'application (ALPN)

Le service alternatif annonce l'utilisation d'un en-tête de réponse HTTP Alt-Svc et de la trame HTTP/2 Alt-Svc comme point de terminaison HTTP/3. Les serveurs peuvent utiliser HTTP/3 sur n'importe quel port UDP. Une autre publicité de service inclut un port explicite, et les URL contiennent soit un port explicite, soit un port par défaut associé au schéma.

Les clients recevant d'autres en-têtes ou trames de service ne sont pas tenus de les utiliser. Le client, s'il est informé d'un autre service et s'il appuie le mécanisme de service alternatif, doit utiliser le service alternatif approprié annoncé. En d'autres termes, un service HTTP/1.1 ou un service HTTP/2 peut annoncer un point de terminaison équivalent prenant en charge le protocole HTTP/3. Lors de la réception de ces informations de service de rechange, le client peut choisir d'établir une connexion QUIC avec le service alternatif spécifié et, une fois disponible, cette connexion peut être utilisée pour toutes les demandes ultérieures. Si l'établissement de la connexion avec le service alternatif sélectionné

échoue, le client peut revenir au point de terminaison d'origine. Lorsque le client commence à utiliser le service alternatif annoncé, l'indique en incluant un en-tête Alt-Used.

Citrix ADC prend en charge les points de terminaison HTTP/3 équivalents publicitaires sur les serveurs virtuels HTTP et SSL.

Configurer la découverte du service HTTP/3

Procédez comme suit pour configurer la découverte du service HTTP/3 :

1. Configurer le point de terminaison de service alternatif HTTP/3 à l'aide d'un en-tête HTTP Alt-Svc
2. Configurez le point de terminaison de service alternatif HTTP/3 à l'aide d'une trame HTTP/2 Alt-Svc
   Configurez le point de terminaison de service alternatif HTTP/3 à l'aide d'un en-tête HTTP Alt-Svc
   Pour annoncer un point de terminaison HTTP/3 à l'aide d'un en-tête HTTP Alt-Svc, tapez la commande suivante :

Remarque : L'objectif principal de la publicité d'un service alternatif est de faire savoir à l'utilisateur que la capacité HTTP/3 est également accessible sur le service HTTP/1.1 ou HTTP/2 sur a.b.c.d:443.

```
add ns httpProfile <name> -custom -altsvc [ ENABLED | DISABLED ]
<!--NeedCopy-->
```

Exemple :

```
add ns httpProfile http-profile -altsvc ENABLED -altSvcValue  "h3-29="
    :443"; ma=3600; persist=1"
<!--NeedCopy-->
```

ou

```
set ns httpProfile http-custom -altsvc ENABLED -altSvcValue  "h3-29="
    :443"; ma=3600; persist=1"
<!--NeedCopy-->
```

Configurer un point de terminaison de service alternatif HTTP/3 à l'aide d'une trame HTTP/2 Alt-Svc

Pour annoncer un point de terminaison HTTP/3 à l'aide d'une trame HTTP/2 Alt-SVC, tapez la commande suivante :


```
1 add ns httpProfile <name> -custom -altsvc [ ENABLED | DISABLED ] -
     http2AltSvcFrame [ ENABLED | DISABLED ]
2 <!--NeedCopy-->
```

Exemple :

```
add ns httpProfile http-custom -http2 ENABLED -http2Direct ENABLED -http2AltSvcFrame
 ENABLED -altsvc ENABLED -altSvcValue "h3-29=\":443\"; ma=3600; persist=1"
```

ou

```
set ns httpProfile http-custom -http2 ENABLED -http2Direct ENABLED -http2AltSvcFrame
 ENABLED -altsvc ENABLED -altSvcValue "h3-29=\":443\"; ma=3600; persist=1"
```

Configurer le service alternatif HTTP/3 avec la valeur d'en-tête HTTP Alt-Svc à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profils HTTP**.
2. Cliquez sur **Ajouter**.
3. Dans la page **Créer un profil HTTP**, accédez à la section HTTP/3 et cochez la case **Autre service** .
4. Le système affiche la zone de texte **Valeur de service alternative** dans la section http2.
5. Entrez la valeur de service alternative comme « h3-29= » :443 "; ma=3600 ; persist=1 »
6. Cliquez sur **OK** et **Fermer**.

gRPC

August 20, 2021

gRPC dans une appliance Citrix ADC est un framework RPC (Remote Procedure Call) universel, léger, hautes performances et open source. Le framework est optimal pour travailler dans plusieurs langues

exécutées sur n'importe quel système d'exploitation. En outre, par rapport à d'autres protocoles, GRPC offre de meilleures performances et de sécurité.

GRPC pour Citrix ADC est préféré pour les raisons suivantes :

- Créez des applications distribuées pour les centres de données et l'infrastructure de cloud public/privé.
- Fournir une communication client-serveur pour mobile, web ou cloud.
- Accéder aux services et applications cloud
- Déploiements de microservices

Pourquoi GRPC dans Citrix ADC

GRPC dans Citrix ADC est implémenté sur HTTP/2 pour prendre en charge des API hautes performances et évolutives. L'utilisation de binaires que de texte maintient la charge utile compacte et efficace. Dans Citrix ADC, les requêtes HTTP/2 sont multiplexées sur une seule connexion TCP, ce qui permet à plusieurs messages simultanés d'être en vol sans compromettre l'utilisation des ressources réseau. Il utilise également la compression d'en-tête pour réduire la taille des demandes et des réponses.

GRPC prend en charge les types de méthodes de service suivants pour qu'un client invoque à distance des paramètres et des types de retour.

1. **RPC unaire**. Le client envoie une seule requête au serveur GRPC et obtient une réponse unique.

   Exemple :

   ```
   rpc SayHello(HelloRequest)returns (HelloResponse);
   ```

2. **Serveur en streaming RPC**. Le client envoie une seule requête au serveur GRPC et obtient une réponse de flux.

   Exemple :

   ```
   rpc StreamingResponse(HelloRequest)returns (HelloResponse);
   ```

3. **RPC en continu du client**. Le client envoie une séquence de messages et attend que le serveur lise et retourne sa réponse.

   Exemple :

   ```
   rpc IntroduceYourself(stream HelloRequest)returns (HelloResponse)
   ```

4. **RPC de streaming bidirectionnel**. Le client et le serveur des deux côtés envoient un flux de messages à l'aide du flux de lecture-écriture. Les deux flux fonctionnent indépendamment.

   Exemple :

   ```
   rpc ChatSession (stream HelloRequest)returns (stream HelloResponse)
   ```

Citrix ADC prend en charge les fonctionnalités suivantes pour ses services avec des points de terminaison GRPC :

- Équilibrage de charge
- Commutation de contenu
- Services de point de terminaison sécurisés tels que le pare-feu d'application Web, l'authentification
- Configuration de la stratégie
- Statistiques et journalisation
- Réécriture de contenu, filtrage de contenu
- Optimisations de couche 4 et 7, offre TLS
- Solutions de passerelle pour les traductions de protocoles

Configuration de bout en bout du GRPC

August 20, 2021

La configuration de bout en bout GRPC fonctionne en envoyant une requête GRPC à partir d'un client via le protocole HTTP/2 et en transférant à nouveau les messages GRPC répondant par le serveur GRPC.

Fonctionnement de la configuration GRPC de bout en bout

Le diagramme suivant montre qu'une configuration GRPC fonctionne dans une appliance Citrix ADC.

1. Pour déployer la configuration GRPC, vous devez d'abord activer HTTP/2 dans le profil HTTP et également activer la prise en charge HTTP/2 globalement côté serveur.
2. Lorsqu'un client envoie une requête GRPC, le serveur virtuel d'équilibrage de charge évalue le trafic GRPC à l'aide de stratégies.
3. Sur la base de l'évaluation de la stratégie, le serveur virtuel d'équilibrage de charge (avec le service GRPC lié à celui-ci) met fin à la demande et la transmet en tant que requête GRPC au serveur GRPC principal.
4. De même, lorsque le serveur GRPC répond au client, l'appliance met fin à la réponse et la transmet en tant que réponse GRPC au client.

Exemple de requête GRPC envoyée au serveur GRPC

L'en-tête de requête est envoyé en tant qu'en-têtes HTTP/2 dans HEADERS+CONTINUATION Frames.

```
```
HEADERS (flags = END_HEADERS)
: method = POST
: scheme = http
: path = /helloworld.citrix-adc/SayHello
: authority = 10.10.10.10.:80
grpc-timeout = 15
content-type = application/grpc+proto
grpc-encoding = gzip
DATA (flags = END_STREAM)
<Length-Prefixed Message>
<!--NeedCopy--> ```
```

### Exemple d'en-tête de réponse GRPC du serveur GRPC vers l'appliance Citrix ADC

Réponse-Headers & Trailers-Only sont livrés dans un seul bloc de trame HTTP/2 HEADERS. La plupart des réponses devraient avoir à la fois des en-têtes et des remorques, mais les remorques seulement sont autorisées pour les appels qui produisent une erreur immédiate. Le statut doit être envoyé dans Trailers même si le code d'état HTTP est OK.

```
```
HEADERS (flags = END_HEADERS)
: status = 200
Grpc-encoding= gzip
Content-type = application/grpc+proto
DATA
<Length-Prefixed Message>
HEADERS (flags = END_STREAM, END_HEADERS)
grpc-status = 0 # OK

<!--NeedCopy--> ```
```

Configurer GRPC à l'aide de l'interface de ligne de commande

Pour configurer un déploiement GRPC de bout en bout, vous devez effectuer les opérations suivantes :

- Ajouter un profil HTTP avec HTTP/2 et HTTP/2 directement activés.
- Activer la prise en charge globale du backend HTTP/2 dans le paramètre HTTP
- Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir le profil HTTP

- Ajouter un point de terminaison Service for gRPC et définir un profil HTTP
- Liaison du service de point d'extrémité gRPC au serveur virtuel d'équilibrage de charge

Ajouter un profil HTTP avec HTTP/2 et HTTP/2 directement activés

Vous devez activer les paramètres directs HTTP/2 et HTTP/2 dans le profil HTTP. En outre, vous devez activer le paramètre direct HTTP/2 si GRPC sur HTTP/2 cleartext est requis.

À l'invite de commandes, tapez :

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Exemple :

```
add ns httpProfile http2gRPC -http2Direct ENABLED -http2 ENABLED
```

Activer la prise en charge globale du back-end HTTP/2 via le paramètre HTTP

Pour activer la prise en charge HTTP/2 globalement du côté serveur à l'aide de la ligne de commande Citrix ADC.

À l'invite de commandes, tapez :

```
set ns httpParam -http2ServerSide( ON | OFF )
```

Exemple :

```
set ns httpParam -http2ServerSide ON
```

Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir le profil HTTP

Pour ajouter un serveur virtuel d'équilibrage de charge à l'aide de l'interface de commande **Citrix ADC** :

À l'invite de commandes, tapez :

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Exemple :

```
add lb vserver lb-grpc HTTP 10.10.10.11 80 -httpProfileName http2gRPC
```

> **Remarque :**
>
> Si vous utilisez un serveur virtuel d'équilibrage de charge de type SSL, vous devez lier le certificat du serveur. Pour plus d'informations, reportez-vous à la rubrique Lier le certificat du serveur.

Ajouter un point de terminaison Service for gRPC et définir un profil HTTP

Pour ajouter un service GRPC avec un profil HTTP à l'aide de l'interface de commande **Citrix ADC** : à l'invite de commandes, tapez :

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Exemple :

```
add service svc-grpc 10.10.10.10 HTTP 80 -httpProfileName http2gRPC
```

Liaison du service de point d'extrémité gRPC au serveur virtuel d'équilibrage de charge

Pour lier un service GRPC au serveur virtuel d'équilibrage de charge à l'aide de l'interface de commande **Citrix ADC** :

Dans l'interface de commande, tapez :

```
bind lb vserver <name> <serviceName>
```

Exemple :

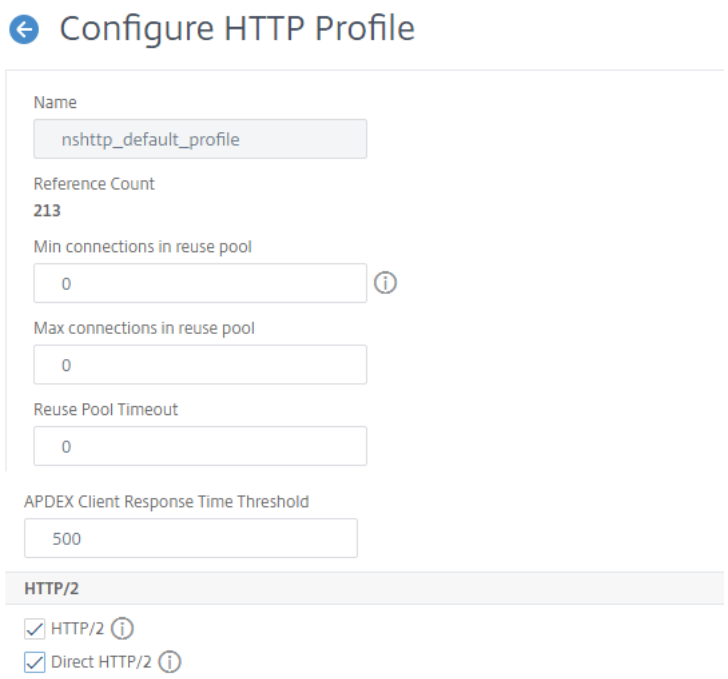
```
bind lb vserver lb-grpc svc-grpc
```

Configurer le déploiement GRPC de bout en bout à l'aide de l'interface graphique

Procédez comme suit pour configurer GRPC à l'aide de l'interface graphique.

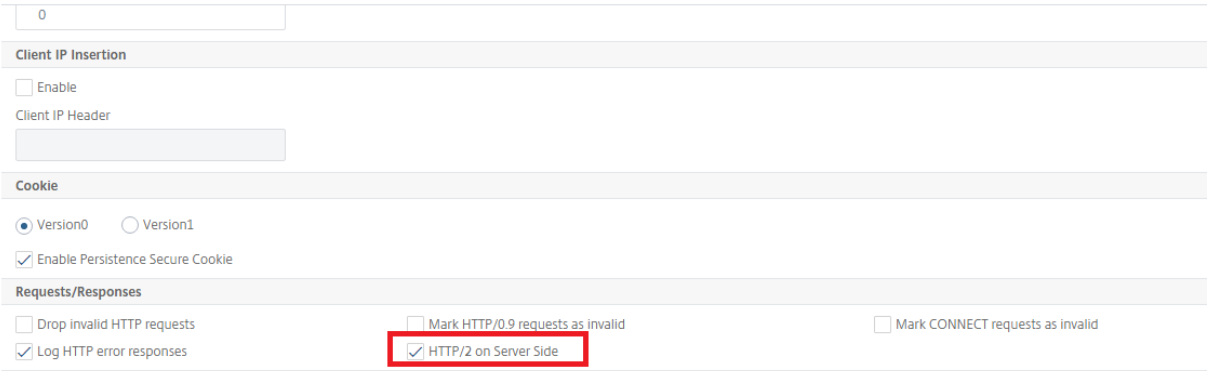
Ajouter un profil HTTP avec HTTP/2 et HTTP/2 directement activés

1. Accédez à **Système > Profils** et cliquez sur **Profils HTTP**.
2. Activer l'option HTTP/2 dans un nouveau profil HTTP ou un profil HTTP existant



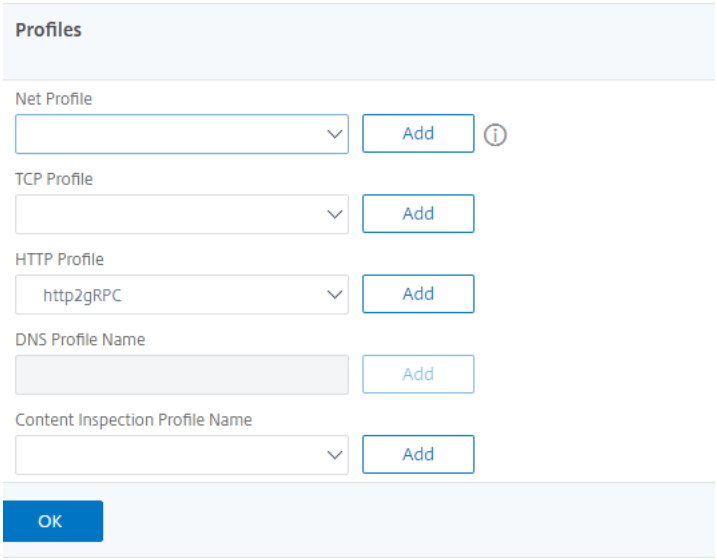
Activer la prise en charge globale du backend HTTP/2 dans le paramètre HTTP

1. Accédez à **Système > Paramètres > Paramètres HTTP**.
2. Dans la page Configurer le paramètre HTTP, sélectionnez HTTP/2 côté serveur.
3. Cliquez sur **OK**.



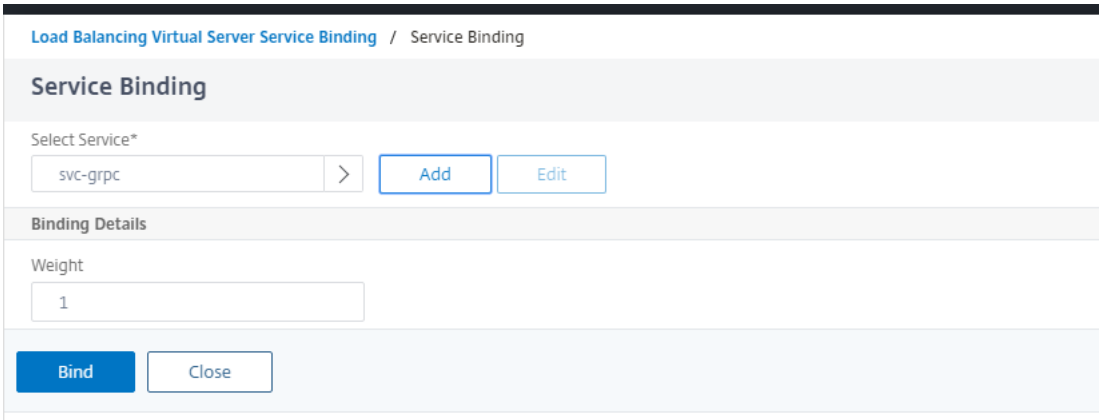
Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir le profil HTTP

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur Ajouter pour créer un serveur virtuel d'équilibrage de charge pour le trafic gRPC.
3. Dans la page Serveur virtuel d'équilibrage de charge, cliquez sur Profils.
4. Dans la section Profils, sélectionnez le type de profil en tant que HTTP.
5. Cliquez sur OK, puis sur Terminé.



Ajouter un point de terminaison Service for gRPC et définir un profil HTTP

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Cliquez sur Ajouter pour créer un serveur d'applications pour le trafic gRPC.
3. Dans la page Service d'équilibrage de charge, accédez à la section Profil.
4. Sous Profils, ajoutez un profil HTTP pour le point de terminaison gRPC.
5. Cliquez sur OK, puis sur Terminé.



Pour obtenir des procédures détaillées sur l'interface graphique liée à l'équilibrage de chargement, consultez la rubrique Équilibrage de charge .

Pontage grPc

August 20, 2021

Lorsqu'un client envoie une requête via le protocole HTTP/1.1, l'appliance Citrix ADC prend en charge le pontage des requêtes GRPC sur le protocole HTTP/1.1 qui est conforme au serveur GRPC sur le protocole HTTP/2. De même, en cas de pontage inverse, l'appliance reçoit la requête GRPC client via le protocole HTTP/2 et effectue un pontage inverse pour les requêtes GRPC conformément au serveur GRPC du protocole HTTP/1.1.

Fonctionnement du pontage GRPC

Dans ce scénario, l'appliance Citrix ADC relie de manière transparente le contenu GRPC reçu sur une connexion HTTP/1.1 et le transmet au serveur GRPC principal via HTTP/2.

Le diagramme suivant montre comment les composants interagissent les uns avec les autres dans une configuration de pontage gRPC.

1. Lorsqu'une requête GRPC est envoyée, l'appliance Citrix ADC vérifie si la connexion est HTTP/1.1 et si le type de contenu est application/grpc. Les requêtes HTTP/1.1 se traduisent par les pseudo-en-têtes suivants.
2. À la réception d'une requête GRPC sur la connexion HTTP/1.1 comme indiqué par l'en-tête Content-Type, l'appliance ADC transforme la requête en GRPC via HTTP/2 comme indiqué ci-dessous :

```
    :method: Method-name in HTTP/1.1 request
    :path: Path is HTTP/1.1 request
    content-type: application/grpc
<!--NeedCopy-->
```

1. Sur la base de l'évaluation de la stratégie, le serveur virtuel d'équilibrage de charge (avec le service GRPC lié à lui) met fin à la demande ou la transmet via des trames HTTP/2 au serveur GRPC principal.
2. À la réception de la réponse sur une connexion HTTP/2 du serveur GRPC, l'appliance met en mémoire tampon jusqu'à ce qu'elle reçoive la remorque HTTP/2, puis vérifie le code d'état GRPC-Status. S'il s'agit d'un état d'erreur GRPC différent de zéro, l'appliance recherche le code d'état HTTP mappage et envoie une réponse d'erreur HTTP/1.1 appropriée.

Configurer le pont GRPC à l'aide de l'interface de ligne de commande

Pour configurer le pontage GRPC, vous devez effectuer les étapes suivantes :

1. Ajouter un profil HTTP avec HTTP/2 et HTTP/2 directement activés
2. Activer la prise en charge globale du back-end HTTP/2 dans le paramètre HTTP
3. Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir le profil HTTP
4. Ajouter un service pour le point de terminaison GRPC et définir le profil HTTP
5. Liaison du service de point d'extrémité gRPC au serveur virtuel d'équilibrage de charge
6. Mapper le code d'état GRPC à la réponse HTTP pour un état GRPC non nul
7. Configurer la mise en mémoire tampon GrPC par temps et/ou taille

Ajouter un profil HTTP avec HTTP/2 et HTTP/2 directement activé

Pour commencer la configuration, vous devez activer la fonctionnalité HTTP/2 dans le profil HTTP. Si le client envoie les requêtes HTTP 1.1, l'appliance relie la demande et la transmet au serveur principal.

À l'invite de commandes, tapez :

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Exemple :

```
add ns httpProfile http2gRPC -http2Direct ENABLED -http2 ENABLED
```

Activer la prise en charge globale du backend HTTP/2 dans le paramètre HTTP

Pour activer la prise en charge HTTP/2 globalement du côté serveur à l'aide de la ligne de commande Citrix ADC.

À l'invite de commandes, tapez :

```
set ns httpParam -http2ServerSide( ON | OFF )
```

Exemple :

```
set ns httpParam -http2ServerSide ON
```

Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir le profil HTTP

Pour ajouter un serveur virtuel d'équilibrage de charge à l'aide de l'interface de commande **Citrix ADC**

À l'invite de commandes, tapez :

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```


Exemple :

```
add lb vserver lb-grpc HTTP 10.10.10.10 80 -httpProfileName http2gRPC
```

> **Remarque :**
>
> Si vous utilisez un serveur virtuel d'équilibrage de charge de type SSL, vous devez lier le certificat du serveur. Pour plus d'informations, reportez-vous à la rubrique relative au certificat de serveur Bind

Ajouter un service pour le point de terminaison GRPC et définir le profil HTTP

Pour ajouter un service GRPC avec le profil HTTP à l'aide de l'interface de commande **Citrix ADC**.

À l'invite de commandes, tapez :

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Exemple :

```
add service svc-grpc 10.10.10.10 HTTP 80 -httpProfileName http2gRPC
```

Liaison du service de point d'extrémité gRPC au serveur virtuel d'équilibrage de charge

Pour lier un service de point de terminaison GRPC au serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande.

Dans l'interface de commande, tapez :

```
bind lb vserver <name> <serviceName>
```

Exemple :

```
bind lb vserver lb-grpc svc-grpc
```

Mapper le code d'état GRPC au code d'état HTTP dans la réponse HTTP/1.1

Dans le scénario de pontage GRPC, le service GRPC répond à la demande avec un code d'état GRPC. L'appliance mappe le code d'état gRPC à un code de réponse HTTP et une phrase de motif correspondants. Le mappage est effectué sur la base du tableau ci-dessous. L'appliance Citrix ADC lors de l'envoi de la réponse HTTP/1.1 au client envoie le code d'état HTTP et la phrase de motif.

Code d'état GRPC	Code d'état de la réponse HTTP	Phrase de raison-réponse HTTP
OK = 0	200	OK

Code d'état GRPC	Code d'état de la réponse HTTP	Phrase de raison-réponse HTTP
CANCELLED = 1	499	*
UNKNOWN = 2	500	Erreur interne du serveur
ARGUMENT INVALID_= 3	400	Demande incorrecte
DEADLINE_EXCEEDED = 4	504	Délai de passerelle
NOT_FOUND = 5	404	*
ALREADY_EXISTS = 6	409	Conflit
PERMISSION_DENIED = 7	403	Liste noire
UNAUTHENTICATED = 16	401	Non autorisé
RESOURCE_EXHAUSTED = 8	429	*
FAILED_PRECONDITION = 9	400	Demande incorrecte
ABORTED = 10	409	Conflit
OUT_OF_RANGE = 11	400	Demande incorrecte
UNIMPLEMENTED = 12	501	Non implémenté
INTERNAL = 13	500	Erreur interne du serveur
UNAVAILABLE = 14	503	Service non disponible
DATA_LOSS = 15	500	Erreur interne du serveur

Configurer la mise en mémoire tampon GrPC par temps et/ou taille

L'appliance Citrix ADC mise en mémoire tampon la réponse GRPC du serveur principal jusqu'à ce que la remorque de réponse soit reçue. Cela casse les appels bidirectionnels GRPC. En outre, si la réponse GrPC est énorme, elle consomme une quantité importante de mémoire pour mettre en mémoire tampon complètement la réponse. Pour résoudre le problème, la configuration de pontage GRPC est améliorée pour limiter la mise en mémoire tampon en fonction du temps et/ou de la taille. Si la taille de la mémoire tampon ou la limite de temps dépasse le seuil, l'appliance arrête la mise en mémoire tampon et transmet la réponse au client même lorsque l'une des limitations se déclenche (soit la remorque n'est pas reçue dans la taille de tampon configurée ou si le délai d'expiration configuré se produit). Par conséquent, les stratégies configurées et ses expressions (basées sur le code grpc-status) ne fonctionnent pas comme prévu.

Pour limiter la mise en mémoire tampon GRPC en fonction du temps et/ou de la taille par l'interface de ligne de commande, vous pouvez configurer lorsque vous ajoutez un nouveau profil HTTP ou lorsque

vous modifiez un profil existant.

À l'invite de commandes, tapez :

```
add ns httpProfile http2gRPC [-grpcHoldLimit <positive_integer>] [-grpcHoldTimeout
 <positive_integer>]
```

Ou

```
set ns httpProfile http2gRPC [-grpcHoldLimit <positive_integer>] [-grpcHoldTimeout
 <positive_integer>]
```

Où,

`grpcholdlimit`. Taille maximale en octets autorisée à mettre en mémoire tampon les paquets GRPC jusqu'à la réception de la remorque. Vous pouvez configurer à la fois les paramètres et n'importe lequel.

Valeur par défaut : 131072 Valeur
minimale : 0 Valeur
maximale : 33554432

`grpcholdtimeout`. Durée maximale, en millisecondes, autorisée à mettre en mémoire tampon les paquets GrPC jusqu'à la réception de la remorque. La valeur doit être exprimée en multiples de 100.
Valeur par défaut : 1000 Valeur
minimale : 0 Valeur
maximale : 180000

Exemple :

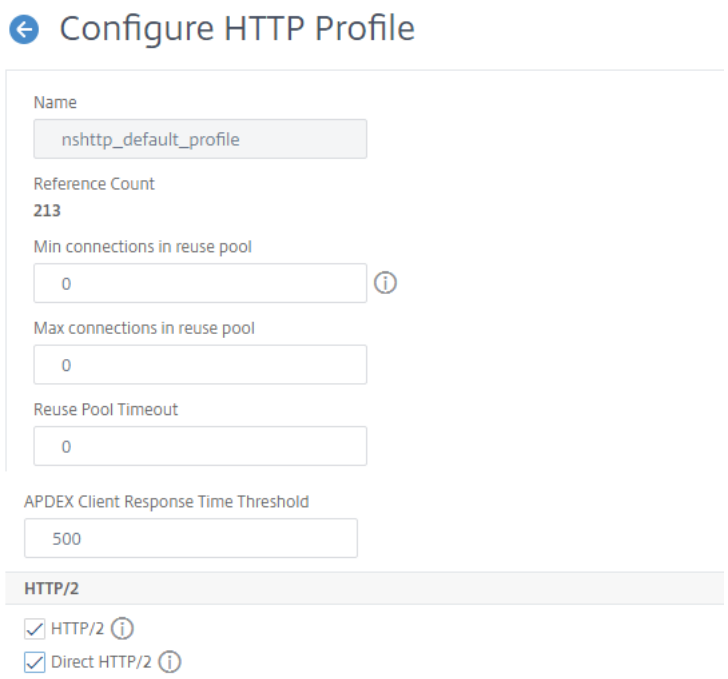
```
add httpprofile http2gRPC -grpcholdlimit 1048576 -grpcholdtimeout 5000
set httpprofile http2gRPC -grpcholdlimit 1048576 -grpcholdtimeout 5000
```

Configurer le pont GRPC à l'aide de l'interface graphique

Procédez comme suit pour configurer le pont GRPC à l'aide de l'interface graphique Citrix ADC.

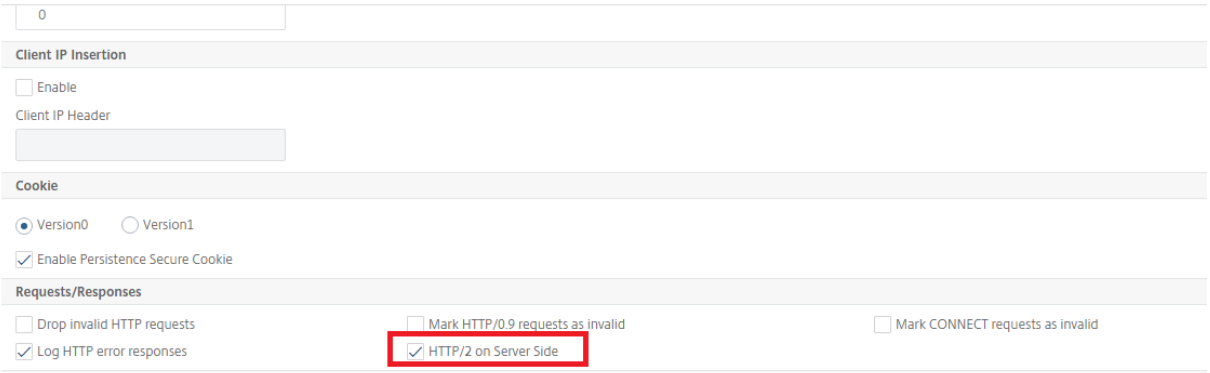
Ajouter un profil HTTP avec HTTP/2 et HTTP/2 directement activés

1. Accédez à **Système > Profils** et cliquez sur **Profils HTTP**.
2. Sélectionnez **HTTP/2** dans le profil HTTP.



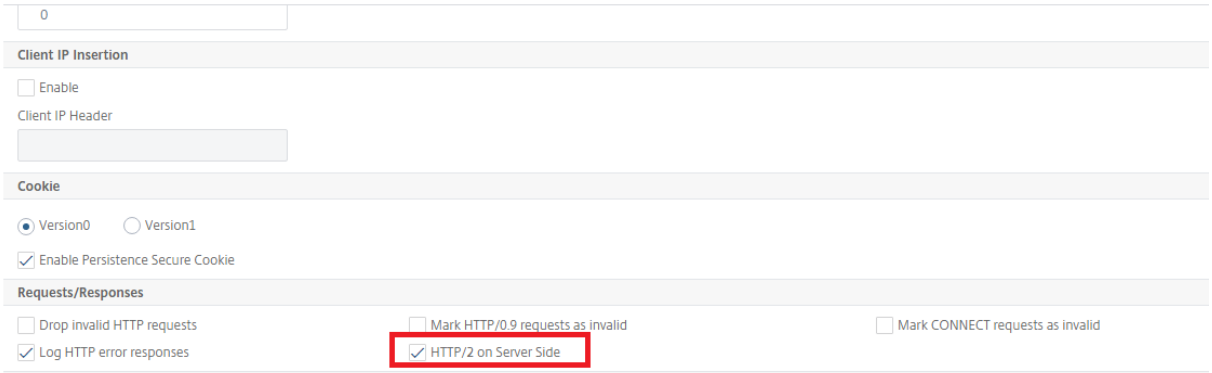
Activer la prise en charge globale du back-end HTTP/2 dans le paramètre HTTP

1. Accédez à **Système > Paramètres > Paramètres HTTP**.
2. Dans la page **Configurer le paramètre HTTP**, sélectionnez l'option **HTTP/2 côté serveur**.
3. Cliquez sur **OK**.



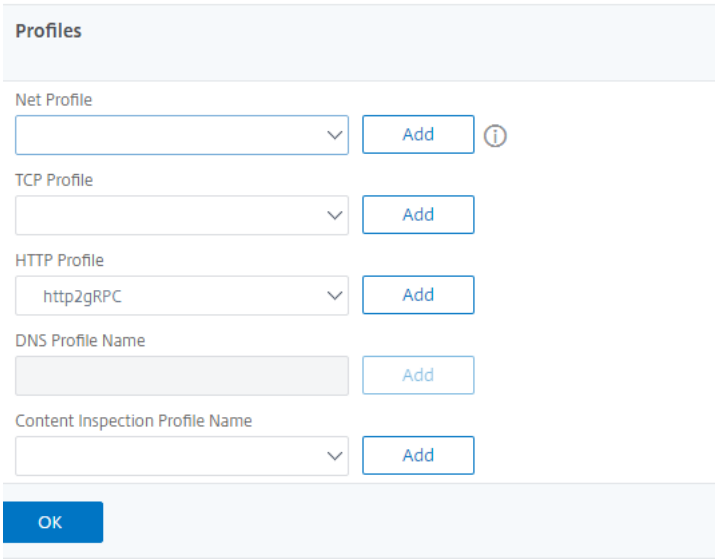
Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir le profil HTTP

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel d'équilibrage de charge pour le trafic gRPC.
3. Dans la page **Serveur virtuel d'équilibrage de charge**, cliquez sur **Profils**.
4. Dans la section **Profils**, sélectionnez le type de profil en tant que HTTP.
5. Cliquez sur **OK**, puis sur **Terminé**.



Ajouter un point de terminaison Service for gRPC et définir un profil HTTP

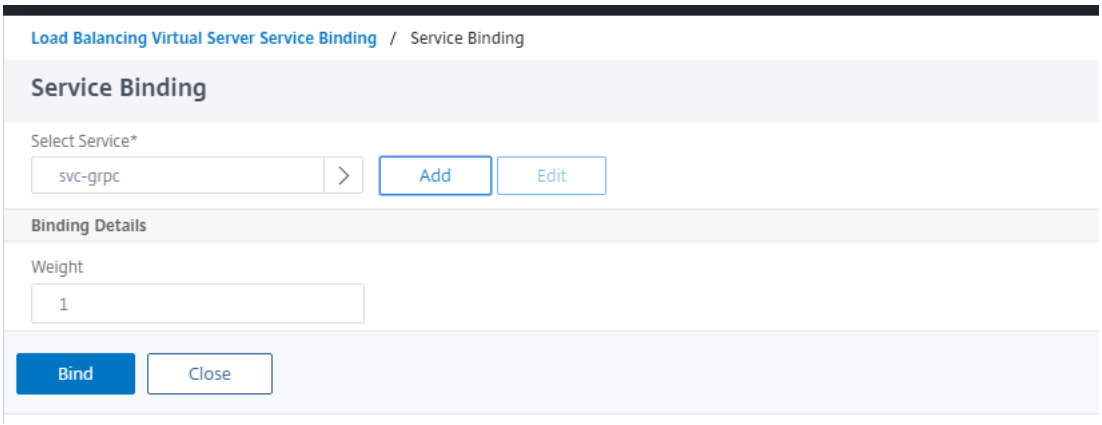
1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Cliquez sur **Ajouter** pour créer un serveur d'applications pour le trafic gRPC.
3. Dans la page **Service d'équilibrage de charge**, accédez à la section **Profil**.
4. Sous **Profils**, ajoutez un **profil HTTP** pour le point de terminaison gRPC.
5. Cliquez sur **OK**, puis sur **Terminé**.



Liaison du service du point d'extrémité gRPC au serveur virtuel d'équilibrage de charge

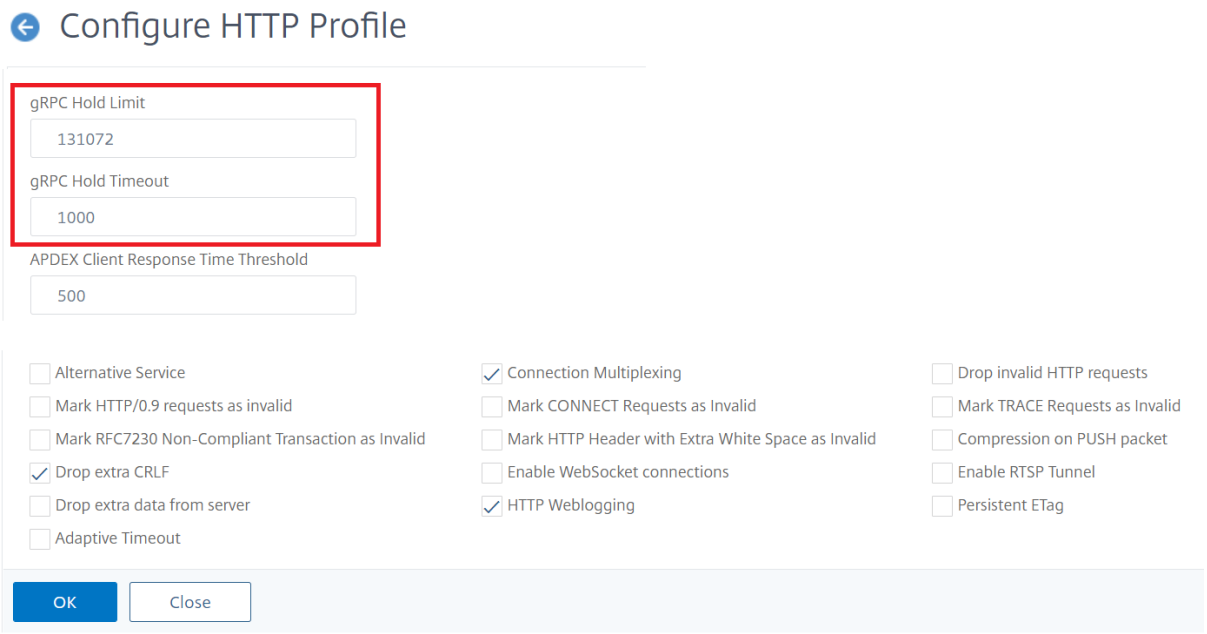
1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel d'équilibrage de charge pour le trafic gRPC.
3. Dans la page **Serveur virtuel d'équilibrage de charge**, cliquez sur la section **Groupes de services et** de services.
4. Dans la page **Liaison de service de serveur virtuel d'équilibrage** de charge, sélectionnez le service gRPC à lier.

5. Cliquez sur **Fermer**, puis sur **Terminé**.



Configurer la mise en mémoire tampon GRPC en fonction du temps et de la taille à l'aide de l'interface graphique

1. Accédez à **Système > Profils** et cliquez sur **Profils HTTP**.
2. Sélectionnez **HTTP/2** dans le profil HTTP.
3. Dans la page **Configurer le profil HTTP**, définissez les paramètres suivants :
   a) GrpCholdTimeout. Entrez le temps en millisecondes pour tamponner les paquets GrPC jusqu'à ce que la remorque soit reçue.
   b) GrpCholdLimit. Entrez la taille maximale en octets pour tamponner les paquets GRPC jusqu'à ce que la remorque soit reçue.
4. Cliquez sur **OK** et **Fermer**.



Pour connaître les procédures détaillées de l'interface graphique pour le service de liaison et les serveurs virtuels d'équilibrage de charge, consultez la rubrique Équilibrage de charge

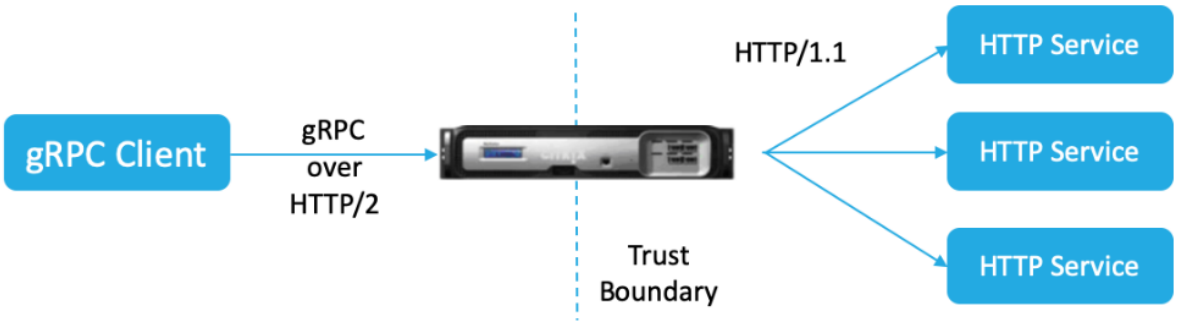
PONT INVERSE GRPC

August 20, 2021

Dans ce scénario, l'appliance Citrix ADC relie de manière transparente le contenu GRPC reçu sur une connexion HTTP/2 et le transmet au serveur GRPC principal via HTTP/1.1.

Comment fonctionne le pont inverse

Le diagramme suivant montre comment les composants interagissent les uns avec les autres dans une configuration de pontage gRPC.



1. Le client envoie une requête GRPC sur la connexion HTTP/2 avec les en-têtes GRPC dans les trames HTTP/2 et la charge utile proto-buf.
2. Sur la base de l'évaluation de la stratégie, le serveur virtuel d'équilibrage de charge (avec le service GRPC lié à celui-ci) traduit et transfère la requête via une connexion HTTP/1.1 au serveur principal.
3. À la réception de la réponse HTTP/1.1, s'il n'y a pas de code grpc-status dans la réponse, ADC dérive un cas d'état grpc du code de réponse HTTP.
4. L'appliance insère ensuite les en-têtes gRPC dans la bande-annonce HTTP/2 avant de transmettre la réponse au client.

Configurer le pontage inverse gRPC à l'aide de l'interface de ligne de commande

Pour configurer le pontage inverse GRPC, vous devez effectuer les étapes suivantes :

- Ajouter un profil HTTP 1 avec HTTP/2 et HTTP/2 directement activés pour l'équilibrage de charge serveur virtuel
- Ajouter le profil HTTP 2 avec HTTP/2 désactivé pour le serveur principal

- Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir sur le profil HTTP 1
- Ajouter un service pour le point de terminaison gRPC et définir le profil HTTP 2
- Liaison du service du point d'extrémité gRPC au serveur virtuel d'équilibrage de charge
- Mapper le code d'état HTTP-Status au code d'état GRPC si la réponse n'a pas de code d'état grpc

Ajouter un profil HTTP 1 avec HTTP/2 et HTTP/2 directement activés pour l'équilibrage de charge serveur virtuel

Pour commencer la configuration de pontage inverse, vous devez ajouter deux profils HTTP. Un profil pour activer HTTP/2 pour les requêtes client GRPC et un autre profil pour désactiver HTTP/2 pour la réponse du serveur non-GRPC.

À l'invite de commandes, tapez :

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Exemple :

add ns httpProfile profile1 –http2 ENABLED -http2Direct ENABLED

Ajouter un profil HTTP 2 avec HTTP/2 désactivé pour le serveur back-end

Pour désactiver la prise en charge HTTP/2 sur le profil HTTP pour la réponse du serveur principal à l'aide de la ligne de commande Citrix ADC.

À l'invite de commandes, tapez :

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Exemple :

add ns httpProfile profile2 –http2 DISABLED http2Direct DISABLED

Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir sur le profil HTTP 1

Pour ajouter un serveur virtuel d'équilibrage de charge à l'aide de l'interface de commande Citrix ADC.

À l'invite de commandes, tapez :

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Exemple :

add lb vserver lb-grpc HTTP 10.10.10.10 80 -httpProfileName profile1

> **Remarque :**
>
> Si vous utilisez un serveur virtuel d'équilibrage de charge de type SSL, vous devez lier le certificat du serveur. Pour plus d'informations, reportez-vous à la rubrique Lier le certificat du serveur.

Ajouter un service pour le point de terminaison gRPC et définir le profil HTTP 2

Pour ajouter un service avec le point de terminaison GRPC et définir le profil HTTP 2 à l'aide de l'interface de commande Citrix ADC.

À l'invite de commandes, tapez :

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Exemple :

```
add service svc-grpc 10.10.10.11 HTTP 80 -httpProfileName profile2
```

Service de liaison pour le point de terminaison GRPC au serveur virtuel d'équilibrage de charge

Pour lier un service GRPC au serveur virtuel d'équilibrage de charge à l'aide de l'interface de commande Citrix ADC.

Dans l'interface de commande, tapez :

```
bind lb vserver <name> <serviceName>
```

Exemple :

```
bind lb vserver lb-grpc svc-grpc
```

Mapper le code de réponse HTTP au code d'état GRPC

Si le serveur ne génère pas de code d'état GRPC, l'appliance Citrix ADC génère un code d'état GRPC approprié basé sur la réponse HTTP reçue. Les codes d'état sont répertoriés dans le tableau de correspondance ci-dessous.

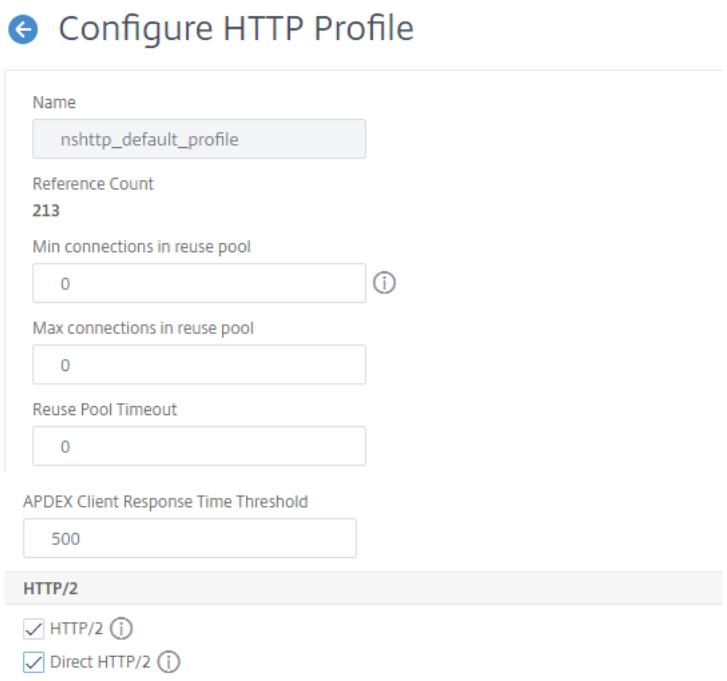
Code d'état de la réponse HTTP	Code d'état GRPC
200	OK
400	INTERNAL = 13
403	PERMISSION_DENIED = 7
401	UNAUTHENTICATED = 16

Code d'état de la réponse HTTP	Code d'état GRPC
429, 502, 503, 504	UNAVAILABLE = 14
404	UNIMPLEMENTED = 12

Configurer le pont inverse GRPC à l'aide de l'interface graphique

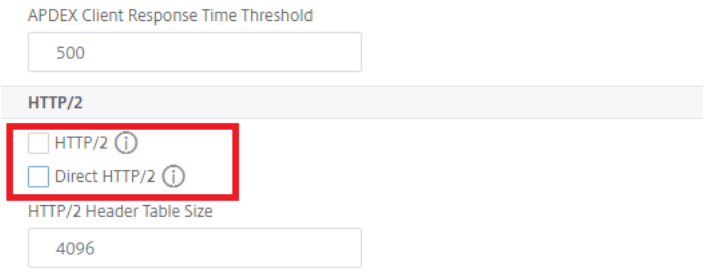
Ajouter un profil HTTP 1 avec HTTP/2 et HTTP/2 directement activés pour l'équilibrage de charge serveur virtuel

1. Accédez à Système > Profils et cliquez sur Profils HTTP.
2. Activer l'option HTTP/2 dans un profil HTTP 1.



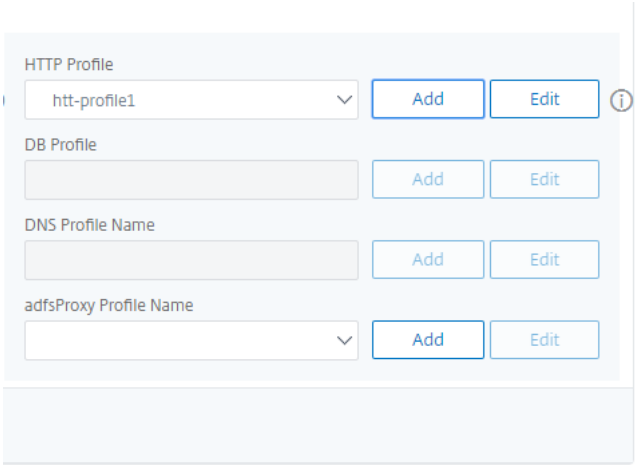
Ajouter un profil HTTP 2 avec HTTP/2 désactivé pour le serveur back-end

1. Accédez à **Système > Profils** et cliquez sur **Profils HTTP**.
2. Activer l'option **HTTP/2** dans un profil HTTP 2.
3. Cliquez sur **OK**.



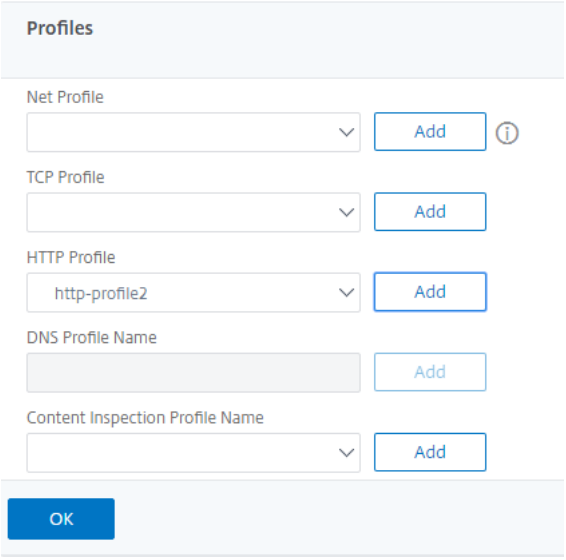
Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir sur le profil HTTP 1

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel d'équilibrage de charge pour le trafic gRPC.
3. Dans la page **Serveur virtuel d'équilibrage de charge**, cliquez sur **Profils**.
4. Dans la section **Profils**, sélectionnez le type de profil en tant que HTTP.
5. Cliquez sur **OK**, puis sur **Terminé**.



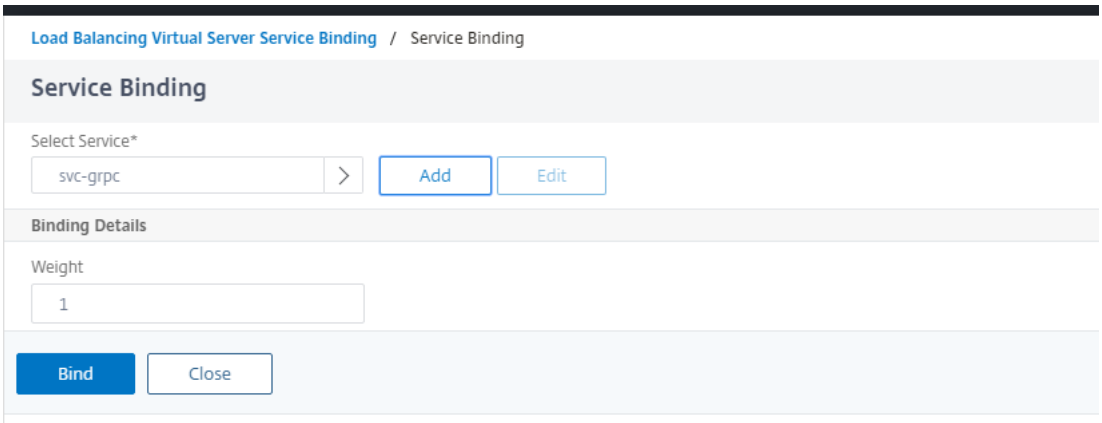
Ajouter un service avec le point de terminaison GRPC et définir sur le profil HTTP 2

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Cliquez sur **Ajouter** pour créer un serveur d'applications pour le trafic gRPC.
3. Dans la page **Service d'équilibrage de charge**, accédez à la section **Profil**.
4. Sous **Profils**, ajoutez un **profil HTTP** pour le point de terminaison gRPC.
5. Cliquez sur **OK**, puis sur **Terminé**.



Liaison du service du point d'extrémité gRPC au serveur virtuel d'équilibrage de charge

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel d'équilibrage de charge pour le trafic gRPC.
3. Dans la page **Serveur virtuel d'équilibrage de charge**, cliquez sur la section **Groupes de**services**et de services**.
4. Dans la page **Liaison de service de serveur virtuel d'équilibrage** de charge, sélectionnez le service gRPC à lier.
5. Cliquez sur **Fermer**, puis sur **Terminé**.



Pour obtenir des procédures détaillées sur l'interface graphique, consultez la rubrique Équilibrage de charge .

Terminaison d'appel GRPC

January 21, 2021

Lorsqu'une appliance Citrix ADC dispose de stratégies telles que la limitation de débit, la sécurité du Web App Firewall est configurée et si une stratégie est évaluée à true, l'appliance peut mettre fin à l'appel et répondre au client par un message d'erreur GRPC calculable.

gRPC avec stratégie de réécriture

August 20, 2021

Le cas d'utilisation de la stratégie de réécriture de GRPC explique comment l'appliance Citrix ADC fonctionne pour réécrire certaines informations dans les requêtes ou réponses GRPC. Le diagramme suivant montre que les composants interagissent.

Le diagramme suivant montre comment les composants interagissent les uns avec les autres dans un GRPC avec configuration de stratégie de réécriture.

1. Activez la fonction de réécriture sur l'appliance.
2. Configurez l'action de réécriture pour modifier, ajouter ou supprimer des en-têtes GRPC.
3. Configurez la stratégie de réécriture pour déterminer les requêtes GRPC (trafic) sur lesquelles une action doit être effectuée.
4. Liez la stratégie de réécriture au serveur virtuel d'équilibrage de charge pour vérifier si le trafic correspond à l'expression de stratégie.
5. En utilisant une stratégie de réécriture, vous pouvez effectuer les opérations suivantes en fonction du code d'état GRPC.
    a) Modifier les réponses à partir du serveur Web GRPC.
    b) Modifiez, ajoutez ou supprimez des en-têtes GRPC.
    c) Modifiez l'URL de la requête au serveur GRRC.

Configurer la terminaison d'appel GRPC avec la stratégie de réécriture

Pour configurer la terminaison d'appel GRPC avec une stratégie de réécriture, vous devez effectuer les étapes suivantes :

1. Activer la fonction de réécriture
2. Ajouter une stratégie de réécriture
3. Lier la stratégie de réécriture au serveur virtuel d'équilibrage de charge

Activer la fonction de réécriture

Pour utiliser la fonction de réécriture, vous devez d'abord l'activer.

À l'invite de commandes, tapez :

```
enable ns rewrite
```

Ajouter une stratégie de réécriture

Après avoir configuré une action de réécriture, vous devez ensuite configurer une stratégie de réécriture pour sélectionner les demandes GRPC auxquelles l'appliance Citrix ADC doit réécrire.

À l'invite de commandes, tapez :

```
add rewrite policy <name> <expression> <action> [<undefaction>]-appFlowaction
 <actionName>
```

Exemple :

```
add rewrite policy grpc-rewr_pol1 "http.res.header(\"grpc-status\").NE
(\"0\")"RESET
```

Lier la stratégie de réécriture au serveur virtuel d'équilibrage de charge

Pour mettre une stratégie en vigueur, vous devez la lier au serveur virtuel d'équilibrage de charge avec le service gRPC.

À l'invite de commandes, tapez :

```
bind rewrite global <policyName> <priority> [<gotoPriorityExpression> [-
type <type>] [-invoke (<labelType> <labelName>)]
```

Exemple :

```
bind lb vserver lb-grpc -policyName grpc-rewr_pol1 -priority 100
```


GrPC avec la stratégie de répondeur

August 20, 2021

La configuration de stratégie GrPC avec répondeur explique comment une appliance Citrix ADC fournit différentes réponses aux demandes GrPC via le protocole HTTP/2. Lorsque les utilisateurs demandent une page d'accueil de site Web, vous pouvez fournir une page d'accueil différente en fonction de l'emplacement de chaque utilisateur ou du navigateur utilisé par l'utilisateur.

Le diagramme suivant montre les composants qui interagissent.

1. Activez la fonction de répondeur sur l'appliance.
2. Configurez l'action du répondeur pour générer une réponse personnalisée, rediriger une requête vers une autre page Web ou réinitialiser une connexion.
3. Configurez la stratégie de répondeur pour déterminer les requêtes GRPC (trafic) sur lesquelles une action doit être effectuée.
4. Liez la stratégie de répondeur au serveur virtuel d'équilibrage de charge pour vérifier si le trafic correspond à l'expression de stratégie.
5. En utilisant une stratégie de répondeur, vous pouvez effectuer les opérations suivantes en fonction du code d'état GrPC.

Configurer la terminaison d'appel GrPC avec la stratégie de répondeur à l'aide de l'interface de ligne de commande

Pour configurer la terminaison d'appel GRPC avec la stratégie de répondeur, vous devez effectuer les étapes suivantes :

1. Activer la fonction répondeur
2. Ajouter une action de répondeur
3. Ajouter une stratégie de répondeur et une action de répondeur associé
4. Lier la stratégie du répondeur au serveur virtuel d'équilibrage de charge

Activer la fonction répondeur

Pour utiliser la fonction répondeur, vous devez d'abord l'activer.

À l'invite de commandes, tapez :

```
enable ns responder
```

Ajouter l'action du répondeur

Après avoir activé la fonctionnalité, vous devez configurer l'action du répondeur pour gérer la réponse GRPC en fonction du code d'état renvoyé par le serveur principal.

À l'invite de commandes, tapez :

```
add responder action <name> <type>
```

Exemple :

```
add responder action grpc-act respondwith "HTTP/1.1 200 OK\r\nServer: NS
-Responder\r\nContent-Type:application/grpc\r\ngrpc-status: 12\r\ngrpc
-message: Not Implemented\r\n\r\n"+ "Method: "+ HTTP.REQ.URL+ "is not
implemented."
```

Ajout d'une stratégie de répondeur

Après avoir configuré une action de répondeur, vous devez ensuite configurer une stratégie de répondeur pour sélectionner la demande GRPC à laquelle l'appliance Citrix ADC doit répondre.

À l'invite de commandes, tapez :

```
add responder policy <name> <expression> <action> [<undefaction>]-appFlowaction
 <actionName>
```

Exemple :

```
add responder policy grpc-resp-pol1 HTTP.REQ.URL.NE( "/helloworld.Greeter/
SayHello" )grpc-act
```

Lier la stratégie de répondeur au serveur virtuel d'équilibrage de charge

Pour mettre une stratégie en vigueur, vous devez la lier au serveur virtuel d'équilibrage de charge avec le service gRPC.

À l'invite de commandes, tapez :

```
bind responder global <policyName> <priority> [<gotoPriorityExpression> [-
type <type>] [-invoke (<labelType> <labelName>)]
```


Exemple :

```
bind lb vserver lb-grpc svc-grpc -policyName grpc-resp-pol1 -priority 100
```

Pour plus d'informations sur la stratégie de répondeur, consultez la rubrique Stratégie de répondeur .

Expressions de stratégie pour correspondre aux champs tampon du protocole GrPC

L'appliance Citrix ADC prend en charge les expressions de stratégie suivantes dans la configuration GrPC :

- **Accès au champ tampon du protocole GrPC.** L'appel d'API GrPC arbitraire correspond au numéro du champ de message avec les nouvelles expressions de stratégie. Dans une configuration IP, les correspondances sont effectuées uniquement en utilisant les « numéros de champ » et le « chemin d'accès API ».
- **Filtrage des en-têtes GrPC.** Les paramètres « HttpProfile » pour GrPC sont utilisés pour ajuster le comportement par défaut de l'analyse GrPC (y compris les expressions de stratégie GrPC). Les paramètres suivants s'appliquent aux expressions de stratégie GrPC :
  - **Délimitation de la longueur du GRPC.** Il est activé par défaut et s'attend à ce que les tampons de protocole soient présentés avec un message délimité par la longueur.
  - **Limite de cholestérol GRP.** La valeur par défaut est 131072. Il s'agit de la taille maximale du message tampon de protocole en octets. Il s'agit également de la longueur de chaîne maximale et de la longueur maximale du champ « octet ».

Configurer les expressions de stratégie avancée GrPC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ns httpProfile <name> -http2 ( ENABLED | DISABLED ) -
    gRPCLengthDelimitation ( ENABLED | DISABLED ) -gRPCHoldLimit <int>
```

Exemple :

```
set ns httpProfile http2gRPC -http2 ENABLED -gRPCLengthDelimitation
    ENABLED -gRPCHoldLimit 131072
```

Configurer les paramètres de filtrage des en-têtes GrPC à l'aide de l'interface graphique

1. Accédez à **Système > Profils** et cliquez sur **Profils HTTP**.

2. Sur la page **Créer un profil HTTP**, faites défiler jusqu'à la section **HTTP/3**, sélectionnez **Délimitation de longueur GrPC**.

L'exemple d'expression de stratégie suivant montre une valeur dans le message 5, le sous-message 4 et le champ 3. Il s'agit d'un int 32 bits égal à 2.

```
http.req.body(1000).grpc.message(5).message(4).int32(3).eq(2)
```

Les expressions de stratégie suivantes sont ajoutées pour correspondre aux champs de message tampon du protocole GrPC par numéro :

- message
- double
- flotte
- int32
- int64
- uint32
- uint64
- sint64
- sint32
- fixed32
- fixed64
- sfixed32
- sfixed64
- Bool
- string
- enum
- octets

Correspondance des chemins API

La correspondance du chemin d'accès de l'API est utilisée pour correspondre à l'appel d'API GrPC correct lorsque plusieurs API sont utilisées. Faites correspondre le chemin d'accès de l'API, qui se trouve dans le pseudo en-tête « : path » de la requête HTTP.

Exemple :

```
http.req.header(":path").eq("acme.inventory.v1/ListBooks")
```


QUIC

August 20, 2021

Quick UDP Internet Protocol (QUIC) est une combinaison de protocoles (TCP+TLS+HTTP/2) implémentés sur UDP. Le protocole de transport QUIC multiplexe les connexions entre deux terminaux utilisant UDP. Par ailleurs, par rapport à d'autres protocoles, QUIC offre des performances élevées en termes de sécurité, de livraison rapide du trafic et de latence réduite.

Un pont QUIC est configuré dans une appliance Citrix ADC pour équilibrer la charge du trafic QUIC entre un client QUIC et un serveur principal QUIC. Le pont QUIC vous permet d'avoir des connexions QUIC persistantes entre le client et le serveur en cas de reliaison NAT ou de migration de connexion. Cette configuration ne traite cependant pas les données. Il est utilisé uniquement pour l'équilibrage de charge du trafic QUIC via l'appliance Citrix ADC.

Les paquets QUIC contiennent un ID de connexion permettant aux points de terminaison d'associer les paquets à une adresse différente ou à 4 tuples à la même connexion. L'ID de connexion contient les détails de l'ID de serveur partagé avec l'appliance Citrix ADC et les serveurs principaux. L'appliance Citrix ADC extrait les détails de l'ID de connexion de l'ID de serveur et renvoie le trafic au serveur principal. Les ID de connexion se trouvent dans des paquets protégés, ce qui rend les connexions robustes en cas de migration de connexion.

> **Important**
>
> Les serveurs principaux doivent être pris en charge pour encoder l'ID de serveur dans l'ID de connexion QUIC.

Avantages du pont QUIC

Le pont QUIC pour l'appliance Citrix ADC est préféré pour les raisons suivantes :

- Pas d'opérations de crypto coûteuses.
- Le routage sans état est possible (pas d'équilibrage de charge basé sur 4 tuples).

Configuration du pont QUIC

October 5, 2021

Pour configurer le pont QUIC, vous devez effectuer les opérations suivantes :

- Ajouter un profil de pont QUIC
- Ajouter des serveurs back-end QUIC

- Ajouter le service QUIC sur l'appliance
- Ajouter un serveur virtuel d'équilibrage de charge de type pont QUIC
- Lier le pont QUIC au serveur virtuel d'équilibrage de charge de type pont QUIC

> **Important**
>
> Avant de configurer le pont QUIC, assurez-vous d'abord d'activer la fonction d'équilibrage de charge sur l'appliance. Pour plus d'informations, consultez la section Configurer l'équilibrage de charge de base.

Configurer le pont QUIC à l'aide de l'interface de ligne de commande

Les sections suivantes doivent être configurées à l'aide de l'interface de ligne de commande.

Ajouter un profil de pont QUIC

Ajoutez un profil de pont QUIC.

À l'invite de commandes, tapez :

```
add quicBridge profile <name> -routingAlgorithm <PLAINTEXT> -
    serveridlen <value>
```

Exemple :

```
add quicBridge profile q1 -routingAlgorithm PLAINTEXT -serveridlen 6
```

> **Remarque**
>
> Le `serveridlen` paramètre configuré dans cet exemple est la longueur d'un ID de serveur personnalisé, qui est la chaîne hexadécimale IP et PORT.

Ajouter un serveur d'applications back-end QUIC

Ajoutez des serveurs d'applications back-end QUIC.

À l'invite de commandes, tapez :

```
-  add server <name> (<IPAddress>)
-  add server <name> (<IPAddress>)
```

Exemple :

```
-  add server s1 192.0.2.20
-  add server s2 192.0.2.30
```


Ajouter un service de pont QUIC

Vous devez ajouter le service de pont QUIC aux serveurs d'applications.

À l'invite de commandes, tapez :

```
1 - add service  <name>  (<IP> | <serverName>) <serviceType> <port> [-
    CustomServerID <string>]
2
3 - add service  <name>  (<IP> | <serverName>) <serviceType> <port> [-
    CustomServerID <string>]
```

Exemple :

```
1 - add service src1 s1 QUIC_BRIDGE 443 -CUSTOMSERVERID C0A8026401BB
2
3 - add service src2 s2 QUIC_BRIDGE 443 -CUSTOMSERVERID C0A802C801BB
```

> **Remarque**
>
> Les `CustomServerID` paramètres configurés dans l'exemple précédent sont la chaîne hexadécimale d'une adresse IP correspondante et le PORT du serveur (s1 et s2). Pour la fonctionnalité de pont QUIC, Citrix vous recommande de configurer le `CustomServerID` paramètre au format de chaîne hexadécimale uniquement.

Ajouter un serveur virtuel d'équilibrage de charge de type pont QUIC

Vous devez ajouter un serveur virtuel d'équilibrage de charge de type pont QUIC.

À l'invite de commandes, tapez :

```
1 add lb vserver <name> [<IPAddress>@ <port> [-persistenceType <
    persistenceType >] [-lbMethod < lbMethod > [-cltTimeout <secs>] [-
    quickBridgeProfilename <name>]
```

Exemple :

```
1 add lb vserver quic_bridge_vip QUIC_BRIDGE 192.0.2.10 443 -
    persistenceType CUSTOMSERVERID -lbMethod TOKEN -cltTimeout 120 -
    quicBridgeProfilename q1
```

> **Remarque**
>
> Lors de la configuration du serveur virtuel QUIC Bridge, vous devez configurer un `persistenceType` paramètre as `CUSTOMSERVERID` et un paramètre « LBMethod » en tant que `TOKEN`.

Lier le service de pont QUIC au serveur virtuel d'équilibrage de charge de type pont QUIC

Vous devez lier le service de pont QUIC au serveur virtuel d'équilibrage de charge de type pont QUIC.

À l'invite de commandes, tapez :

```
1 - bind lb vserver <name> (<serviceName>)
2
3 - bind lb vserver <name> (<serviceName>)
```

Exemple :

```
1 - bind lb vserver quic_bridge_vip src1
2
3 - bind lb vserver quic_bridge_vip src2
```

Configurer le pont QUIC pour les groupes de services

Vous pouvez également configurer les capacités du pont QUIC pour des groupes de services. Les étapes suivantes vous guident à configurer le pont QUIC pour les groupes de services.

Pour configurer le pont QUIC pour les groupes de services, vous devez effectuer les opérations suivantes :

Ajouter un profil de pont QUIC

À l'invite de commandes, tapez :

```
1 add quicBridge profile <name> -routingAlgorithm <PLAINTEXT> -
      serveridlen <value>
```

Exemple :

```
1 add quicBridge profile q1 -routingAlgorithm PLAINTEXT -serveridlen 6
```

Ajouter un serveur de type QUIC

À l'invite de commandes, tapez :

```
1 - add server <name> (<IPAddress>)
2 - add server <name> (<IPAddress>)
```

Exemple :


```
1 -  add server s1 192.0.2.20
2 -  add server s2 192.0.2.30
```

Ajouter un groupe de service de pont QUIC

À l'invite de commandes, tapez :

```
1 add serviceGroup <serviceGroupName> (<IP> | <serverName>) <serviceType>
```

Exemple :

```
1 add serviceGroup svg1 QUIC_BRIDGE
```

Liez les serveurs QUIC au groupe de services

À l'invite de commandes, tapez :

```
1 -  bind serviceGroup <serviceGroupName> (<IP>@ | (<serverName>) [-
     CustomServerID <string>]
2 -  bind serviceGroup <serviceGroupName> (<IP>@ | (<serverName>) [-
     CustomServerID <string>]
```

Exemple :

```
1 -  bind serviceGroup svg1 s1 443 -customServerID C0A8026401BB
2 -  bind serviceGroup svg1 s2 443 -customServerID C0A802C801BB
```

Ajouter un serveur virtuel d'équilibrage de charge de type pont QUIC

À l'invite de commandes, tapez :

```
1 add lb vserver <name> [<IPAddress>@ <port> [-persistenceType <
     persistenceType >] [-lbMethod < lbMethod > [-cltTimeout <secs>] [-
     quickBridgeProfilename <name>]
```

Exemple :

```
1 add lb vserver quic_bridge_vip QUIC_BRIDGE 192.0.2.10 443 -
     persistenceType CUSTOMSERVERID -lbMethod TOKEN -cltTimeout 120 -
     quicBridgeProfilename q1
```


Liez le serveur virtuel d'équilibrage de charge de type pont QUIC au groupe de services

À l'invite de commandes, tapez :

```
bind lb vserver <name>@ (<serviceName>@ <serviceGroupName>
```

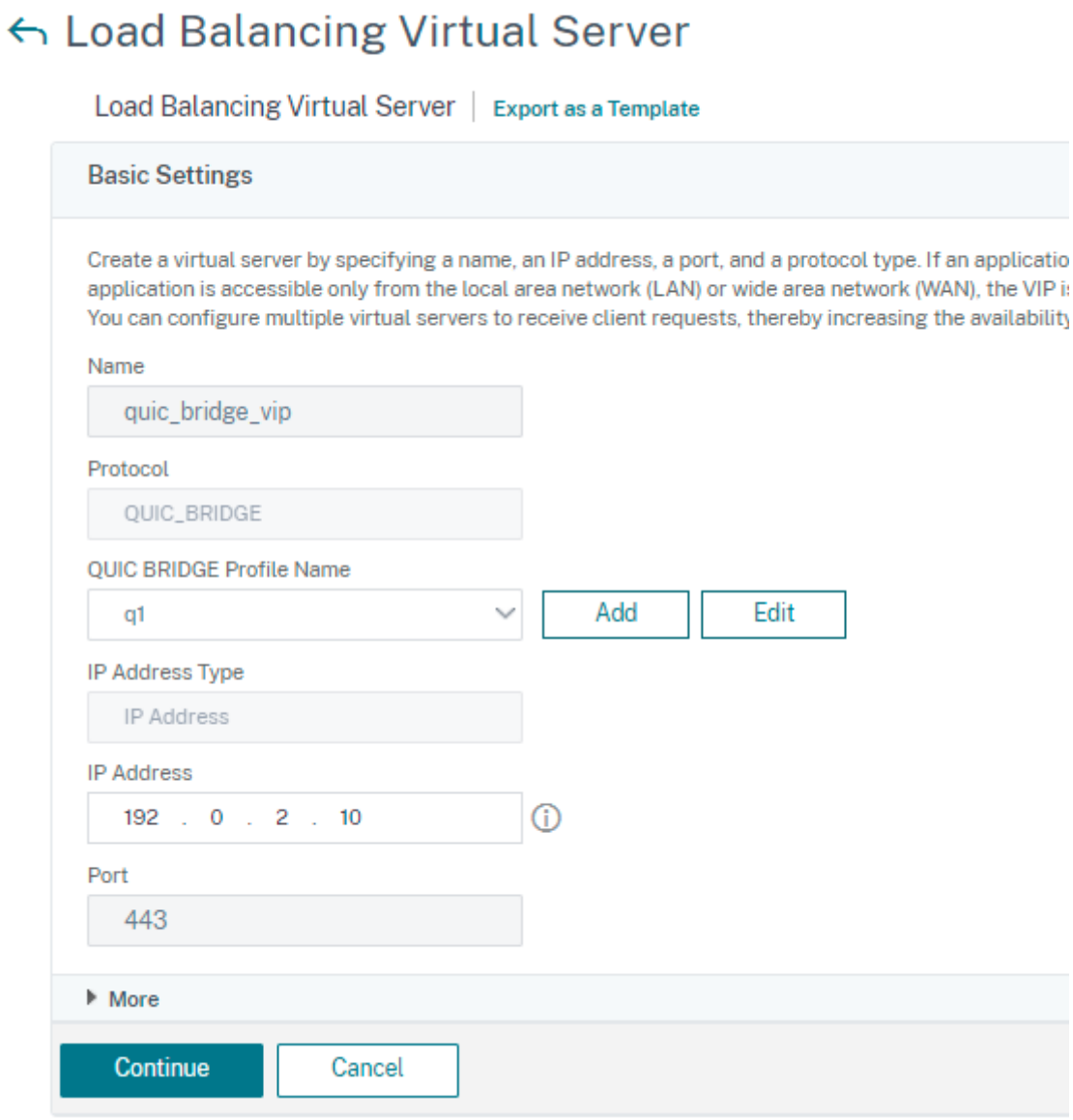
Exemple :

```
bind lb vserver quic_bridge_vip svg1
```

Configuration du pont QUIC à l'aide de l'interface graphique

Procédez comme suit pour configurer le pont QUIC à l'aide de l'interface graphique.

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sur la page **Serveurs virtuels**, cliquez sur **Ajouter**.
3. Sur la page **Serveur virtuel d'équilibrage de charge**, sélectionnez le protocole en tant que QUIC_BRIDGE et entrez les détails. Cliquez sur **OK**.

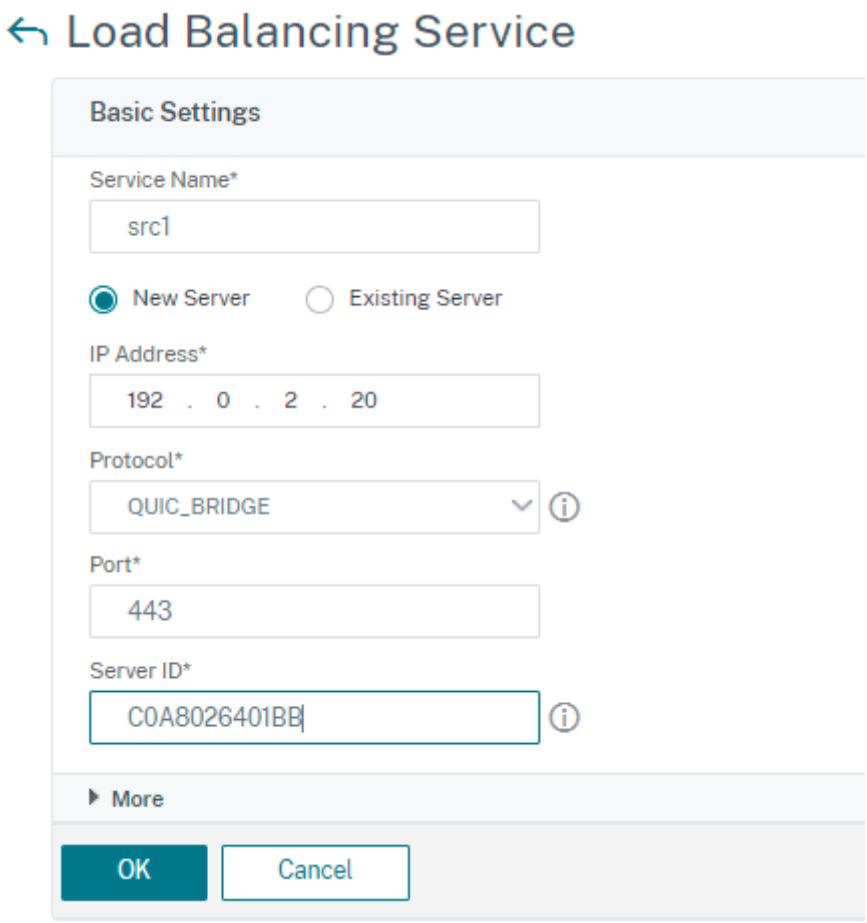


4. Sur la page **Serveur virtuel d'équilibrage de charge**, cliquez sur **Continuer** et **terminé**.

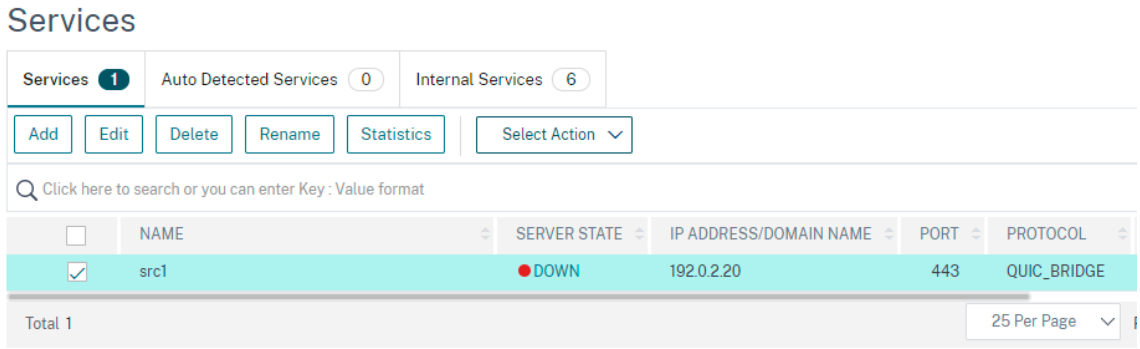
Configurer l'équilibrage de charge pour les services à l'aide de l'interface graphique

Suivez les étapes suivantes pour configurer l'équilibrage de charge pour les services à l'aide de l'interface graphique.

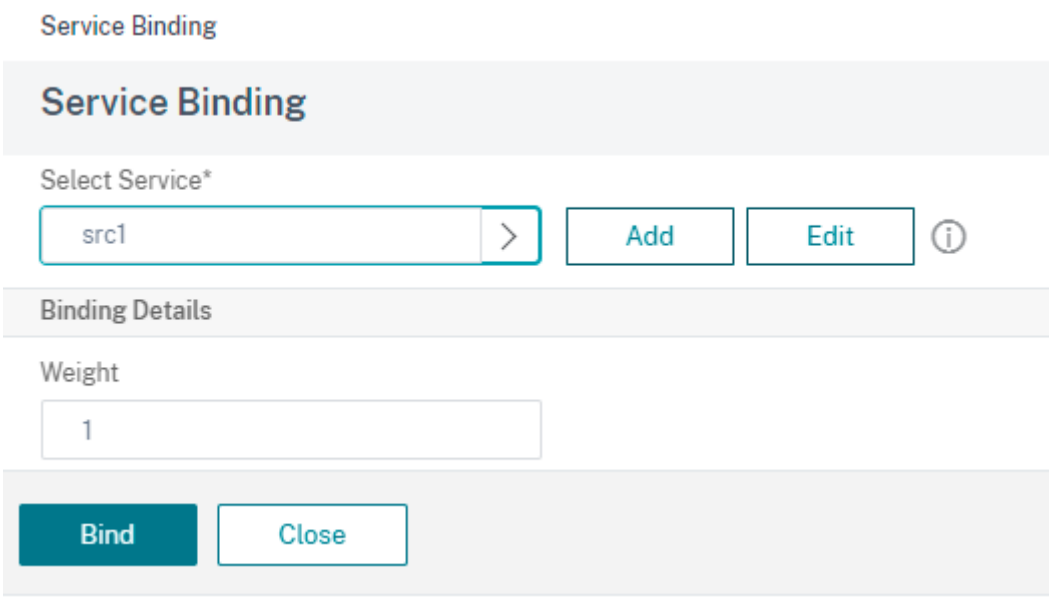
1. Accédez à **Traffic Management > Load Balancing > Services**. Sur la page **Services**, cliquez sur **Ajouter**.
2. Sur la page **Service d'équilibrage de charge**, entrez les détails et cliquez sur **OK**.



3. Sur la page **Serveurs virtuels**, sélectionnez le serveur virtuel créé pour lier le service.
4. Faites défiler vers le bas sur la page **Serveur virtuel d'équilibrage de charge** et sélectionnez les **services et groupes de**services.
5. Sur l'écran **Liaison de service**, cliquez sur **Sélectionner le champ Service** .
6. Sur l'écran **Service**, sélectionnez le service à lier au serveur virtuel d'équilibrage de charge, puis cliquez sur **Sélectionner**.



7. Le service src1 est sélectionné et sur l'écran **de liaison de service**, cliquez sur **Lier**.



8. Sur la page **Serveur virtuel d'équilibrage de charge**, cliquez sur **Terminé**.

Afficher les statistiques du pont QUIC

Le pont QUIC prend en charge la commande de statistiques pour afficher un résumé détaillé des statistiques de pont QUIC.

Les commandes suivantes affichent un résumé détaillé des statistiques de pont QUIC. À l'invite de commandes, tapez ce qui suit :

- `stat quicbridge`
- `stat quicbridge -detail`

Pour effacer l'affichage des statistiques, tapez l'une des options suivantes :

- `stat quicbridge -clearstats basic`
- `stat quicbridge -clearstats full`

Afficher les statistiques de pont QUIC à l'aide de l'interface graphique

Suivez les étapes suivantes pour afficher les statistiques du pont QUIC.

1. Dans l'onglet **Tableau de bord**, placez le pointeur de la souris sur la section **Vue d'ensemble du système** .
2. Cliquez sur **Vue d'ensemble du système** et sélectionnez QUIC BRIDGE dans la liste déroulante.

Protocole Proxy

October 5, 2021

Le protocole proxy transporte en toute sécurité les détails du client d'un client à un autre sur les appliances Citrix ADC. La solution matérielle-logicielle ajoute un en-tête de protocole proxy avec les détails du client et le transfère au serveur principal. Voici quelques-uns des scénarios d'utilisation du protocole proxy dans une appliance Citrix ADC.

- Adresse IP du client d'origine
- Sélection d'une langue pour un site Web
- Bloquer la liste des adresses IP sélectionnées
- Enregistrement et collecte de statistiques.

Voici les trois modes de fonctionnement :

- Insérer. La solution matérielle-logicielle insère les détails du client et les envoie au serveur principal.
- Avancer. La solution matérielle-logicielle transmet les détails du client au serveur principal.
- Dépouillé. La solution matérielle-logicielle stocke les détails du client à des fins de journalisation. De plus, si le protocole proxy n'est pas pris en charge sur le serveur principal, envoie les détails du client au serveur à l'aide de la configuration de la stratégie de réécriture

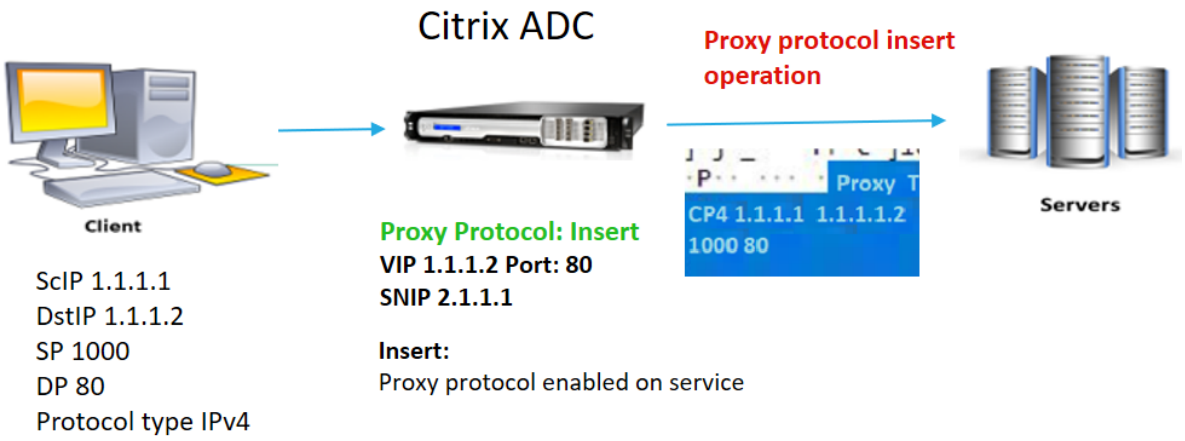
Limitations

La fonctionnalité de protocole proxy n'est pas prise en charge dans les fonctionnalités TFO et Multi-Path TCP.

Fonctionnement du protocole proxy dans une appliance Citrix ADC

Les diagrammes de flux suivants montrent comment configurer le protocole proxy sur les appliances Citrix ADC pour les opérations d'insertion, de transfert et de dépouillement :

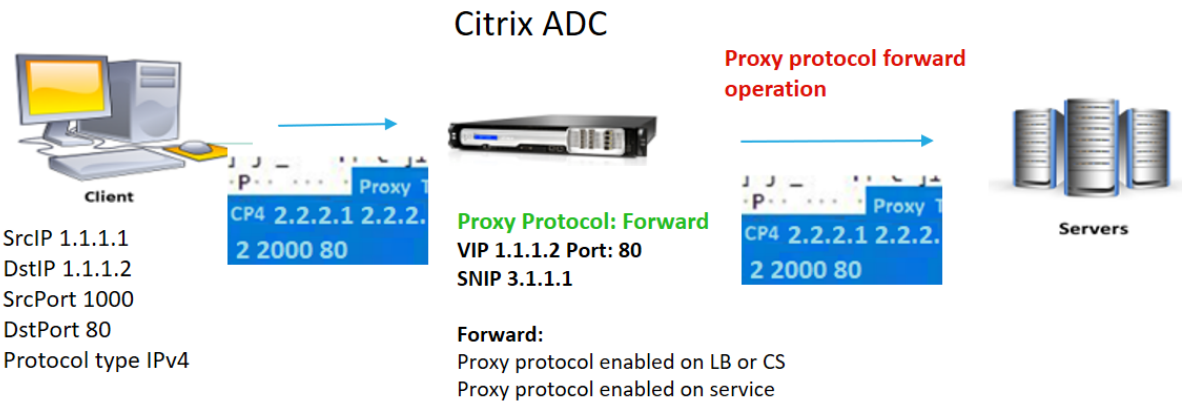
Opération d'insertion



L'interaction des composants est la suivante :

- Sur l'instance Citrix ADC, vous devez activer le protocole proxy dans le profil réseau et le lier au service.
- Dans l'opération d'insertion, Citrix ADC ajoute un en-tête proxy avec les détails de la connexion client et le transfère au serveur principal.
- Côté envoi, la solution matérielle-logicielle décide de la version du protocole proxy en fonction de la configuration de l'interface de ligne de commande.

Opération Forward



*** The original client details 2.2.2.1, 2.2.2.2, 2000, 80 in the proxy header is forwarded to the back-end server**

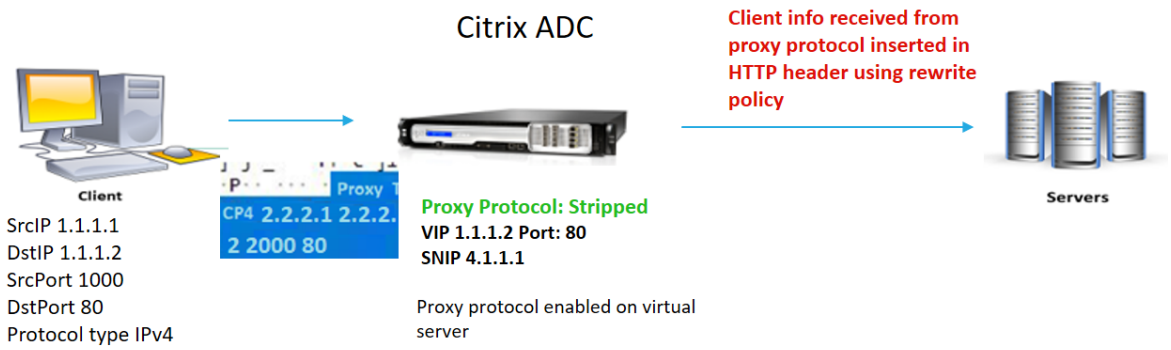
L'interaction des composants est la suivante :

- Un client envoie une demande avec l'en-tête du proxy au Citrix ADC. La solution matérielle-

logicielle identifie dynamiquement la version.

- Dans l'appliance Citrix ADC, il s'agit d'une opération de transfert. Le protocole proxy est activé sur le serveur virtuel d'équilibrage de charge ou le serveur virtuel de commutation de contenu et activé sur le service. La solution matérielle-logicielle reçoit l'en-tête du proxy et transmet les détails de l'en-tête au serveur principal.
- Si les détails de l'en-tête du proxy ne sont pas au format incorrect, la solution matérielle-logicielle réinitialise la connexion.
- Côté envoi, la solution matérielle-logicielle décide de la version du protocole proxy en fonction de la configuration de l'interface de ligne de commande.

Opération dépouillée



L'interaction des composants est la suivante :

- Un client envoie une demande accompagnée d'un en-tête de proxy à l'appliance Citrix ADC.
- Dans l'appliance Citrix ADC, s'il s'agit d'une opération Stripped, l'appliance transfère les informations client obtenues à partir du protocole proxy et les insère dans l'en-tête HTTP à l'aide d'expressions de stratégie de réécriture.
- Les détails du client, tels que l'adresse IP source, l'adresse IP de destination, le port source et le port de destination, sont ajoutés dans un en-tête HTTP à l'aide d'expressions de stratégie de réécriture. La stratégie de réécriture évalue l'expression et si elle est « true », l'action de stratégie de réécriture correspondante est déclenchée. Les détails du client sont ensuite transférés au serveur principal dans un en-tête HTTP.
- Si les détails de l'en-tête du proxy ne sont pas au format incorrect, la solution matérielle-logicielle réinitialise la connexion.

Formats de version du protocole proxy

La version du protocole Proxy est disponible en deux formats. L'appliance décide d'utiliser un format basé sur la longueur des données entrantes. Pour plus d'informations, voir DP sur le protocole proxy

.

1. Format de version 1 du protocole proxy

   ```
   PROXY TCP4/TCP6/UNKNOWN <SRC IP> <DST IP> <SRC PORT> <DST PORT>
   ```

   - PROXY -> Format de chaîne unique pour l'en-tête proxy version -1.
   - Prise en charge des protocoles TCP sur IPv4 et TCP sur IPv6. Pour les autres protocoles, cette option est INCONNUE.
   - IP SRC : adresse IP source (IP du client d'origine) d'un paquet.
   - IP DST : adresse IP de destination d'un paquet.
   - Port SRC : port source d'un paquet.
   - Port DST : port de destination d'un paquet.

2. Format de version 2 du protocole proxy

   ```
   0D 0A 0D 0A 00 0D 0A 51 55 49 54 0A <13th byte> <14th byte> <15-16th byte> <17th byte onwards>
   ```

   - D 0A 0D 0A 00 0D 0A 51 55 49 54 0A -> Chaîne binaire unique pour l'en-tête Proxy version -2.
   - Prise en charge des protocoles TCP sur IPv4 et TCP sur IPv6. Pour les autres protocoles, cette option est INCONNUE.
   - Treizième octet — version du protocole et commande.
   - Quatorzième octet — famille d'adresses et de protocoles.
   - 15-16e octet : longueur de l'adresse dans l'ordre du réseau.
   - À partir du dix-septième octet - Adresses des informations présentes dans l'ordre du réseau - IP src, IP dst, port src, port dst.

Configurer le protocole proxy dans l'appliance Citrix ADC

Suivez les étapes suivantes pour configurer le protocole proxy dans votre appliance Citrix ADC.

1. Activez le protocole proxy en tant que global.
2. Configurer le protocole proxy pour l'opération d'insertion
3. Configurer le protocole proxy pour l'opération Forward
4. Configurer le protocole proxy pour l'opération Strip
5. Configurer le protocole proxy sans opération

Activer le protocole proxy en tant que global

À l'invite de commandes, tapez ce qui suit :

```
set ns param -proxyProtocol ENABLED
```


Configurer le protocole proxy pour l'opération d'insertion

Pour configurer le protocole proxy pour l'opération d'insertion, vous devez activer ou désactiver le protocole sur le serveur virtuel d'équilibrage de charge et l'activer sur le service.

Ajouter un profil réseau avec le protocole proxy désactivé pour le serveur virtuel d'équilibrage de charge

À l'invite de commandes, tapez ce qui suit :

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Exemple :

```
Add netprofile proxyprofile-1 -proxyProtocol DISABLED -proxyprotocoltxversion
 V1
```

> **Remarque :**
>
> Si vous désactivez le protocole proxy sur votre solution matérielle-logicielle, il n'est pas nécessaire de définir le paramètre de version du protocole.

Ajouter un profil réseau avec un protocole proxy activé pour le service

À l'invite de commandes, tapez ce qui suit :

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Exemple :

```
add netprofile proxyprofile-2 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Ajouter un serveur virtuel d'équilibrage de charge pour l'appliance Citrix ADC dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Exemple :

```
add lb vserver lbvserver-1 http 1.1.1.1 80
```


Ajouter un service HTTP pour l'appliance Citrix ADC dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Exemple :

```
Add service http-service-1 2.2.2.1 http 80
```

Définir un profil réseau avec un serveur virtuel d'équilibrage de charge dans l'appliance Citrix ADC

À l'invite de commandes, tapez ce qui suit :

```
set lb vserver <vserver name> -netprofile <name>
```

Exemple :

```
set lb vserver lbvserver-1 -netprofile proxyProfile-1
```

Définir un profil réseau avec le service HTTP dans l'appliance Citrix ADC

À l'invite de commandes, tapez ce qui suit :

```
set service <service name> -netprofile <name>
```

Exemple :

```
set service http-service-1 -netprofile proxyProfile-1
```

Configurer le protocole proxy pour une opération de transfert

Pour configurer le protocole proxy pour l'opération de transfert pour la prochaine instance Citrix ADC de la couche proxy. Vous devez activer ou désactiver le protocole et vous lier au serveur ou au service virtuel.

Ajouter un profil réseau avec le protocole proxy activé pour le serveur virtuel d'équilibrage de charge

À l'invite de commandes, tapez ce qui suit :

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Exemple :

```
add netprofile proxyprofile-3 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```


Ajouter un profil réseau avec le protocole proxy activé pour le service

À l'invite de commandes, tapez ce qui suit :

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Exemple :

```
add netprofile proxyprofile-4 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Ajouter un serveur virtuel d'équilibrage de charge pour l'appliance Citrix ADC dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Exemple :

```
add lb vserver lbvserver-2 http 2.2.2.2 80
```

Ajouter un service HTTP pour l'appliance Citrix ADC dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Exemple :

```
Add service http-service-2 3.3.3.1 http 80
```

Définir un profil réseau avec un serveur virtuel d'équilibrage de charge dans l'appliance Citrix ADC

À l'invite de commandes, tapez ce qui suit :

```
set lb vserver <vserver name> -netprofile <name>
```

Exemple :

```
set lb vserver lbvserver-2 -netprofile proxyProfile-3
```

Définir un profil réseau avec le service HTTP dans l'appliance Citrix ADC

À l'invite de commandes, tapez ce qui suit :

```
set service <service name> -netprofile <name>
```


Exemple :

```
set service http-service-2 -netprofile proxyProfile-4
```

Configurer le protocole proxy pour l'opération de bande

Pour configurer le protocole proxy pour l'opération de dépouillement, vous devez activer le protocole proxy sur le serveur virtuel d'équilibrage de charge et désactiver le protocole proxy sur le service.

Ajouter un profil réseau avec le protocole proxy activé pour le serveur virtuel

À l'invite de commandes, tapez ce qui suit :

```
add netprofile <name> -proxyProtocol ENABLED> -proxyprotocoltxversion <V1/
V2>
```

Exemple :

```
add netprofile proxyprofile-5 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Ajouter un serveur virtuel d'équilibrage de charge ou de commutation de contenu pour l'appliance Citrix ADC dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Exemple :

```
add lb vserver lbvserver-3 http 2.2.2.2 80
```

Ajouter un service HTTP pour l'appliance Citrix ADC dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Exemple :

```
Add service http-service-3 3.3.3.1 http 80
```

Définir un profil réseau avec un serveur virtuel d'équilibrage de charge ou de commutation de contenu dans l'appliance Citrix ADC

À l'invite de commandes, tapez ce qui suit :

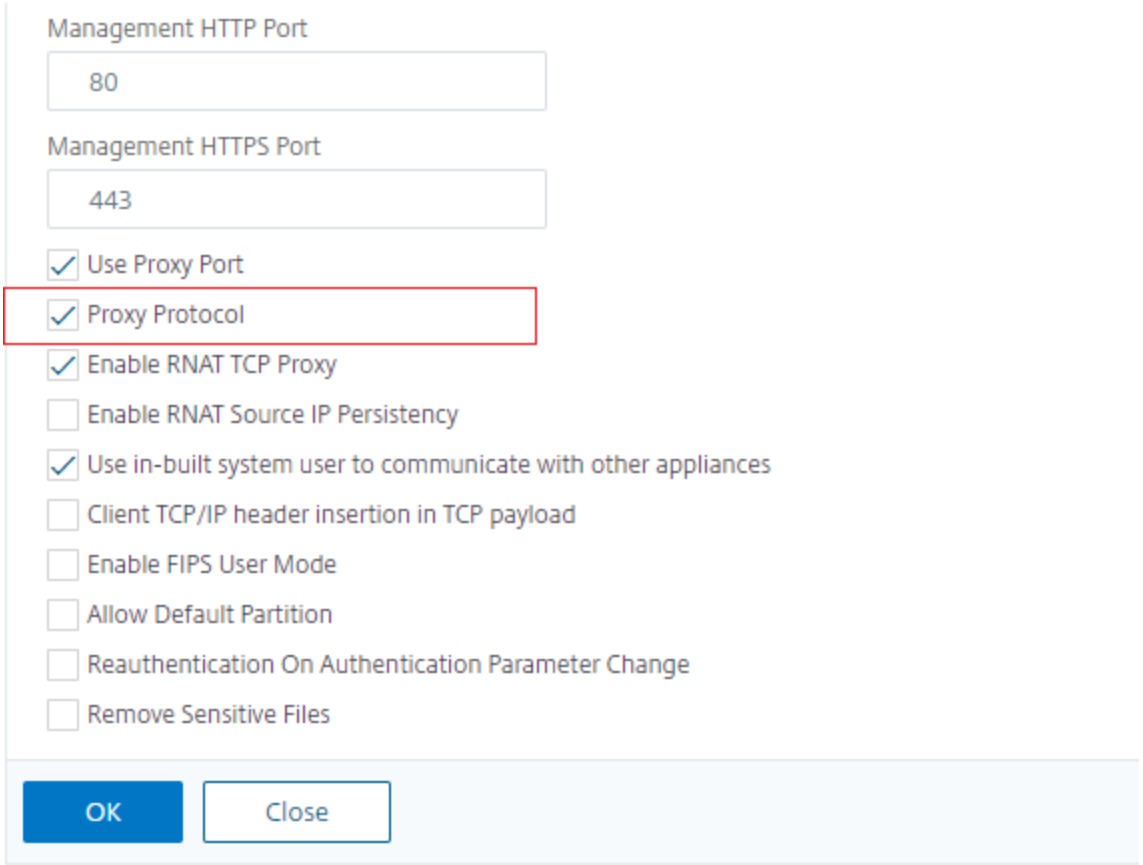
```
set lb vserver <vserver name> -netprofile <name>
```


Exemple :

```
set lb vserver lbvserver-3 -netprofile proxyProfile-5
```

Configurer le protocole proxy à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Système** > **Paramètres** > **Modifier les paramètres système globaux**.
2. Dans la page **Configurer les paramètres globaux du système**, activez la case à cocher **Protocole proxy** .
3. Cliquez sur **OK** et sur **Fermer**.

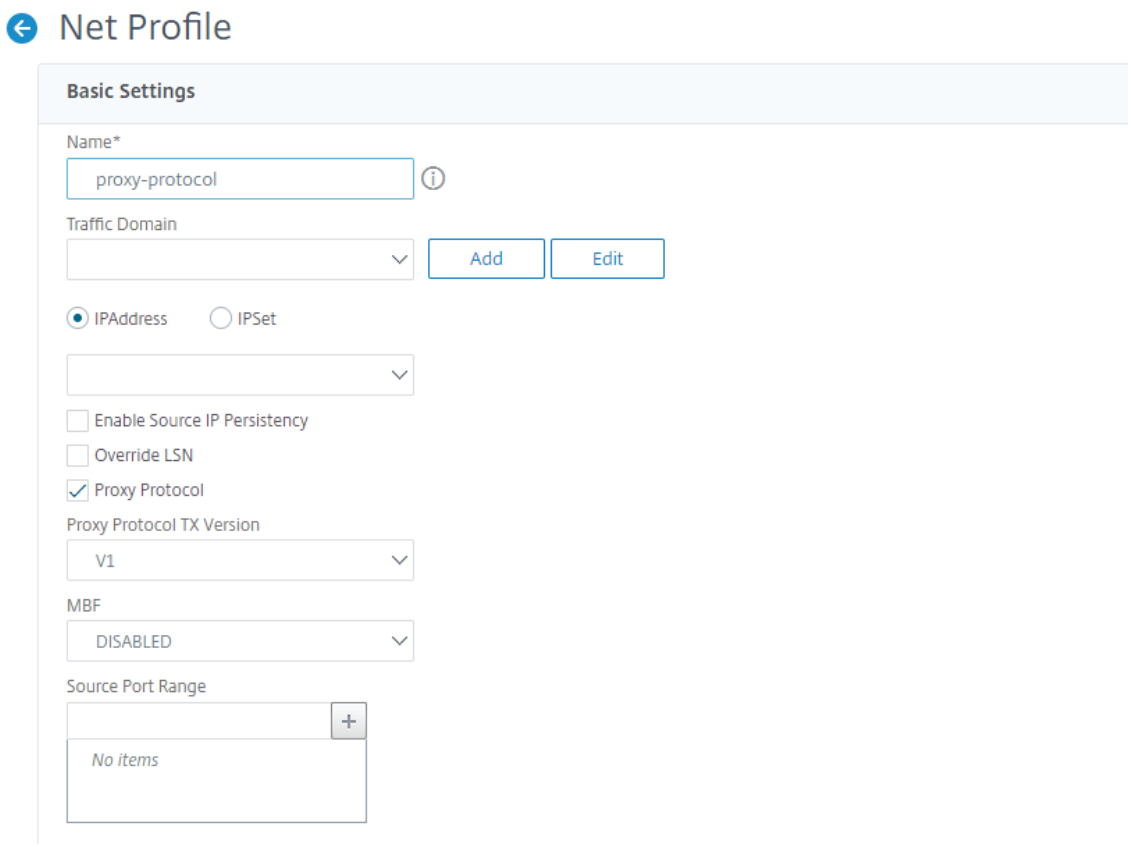


4. Accédez à **Système** > **Réseau** > **Profils réseau**.
5. Dans le volet d'informations, cliquez sur **Ajouter** pour créer un profil réseau pour le serveur virtuel d'équilibrage de charge.
6. Dans la page **Profil réseau**, définissez les paramètres suivants :
   a) Name. Nom du profil de réseau.

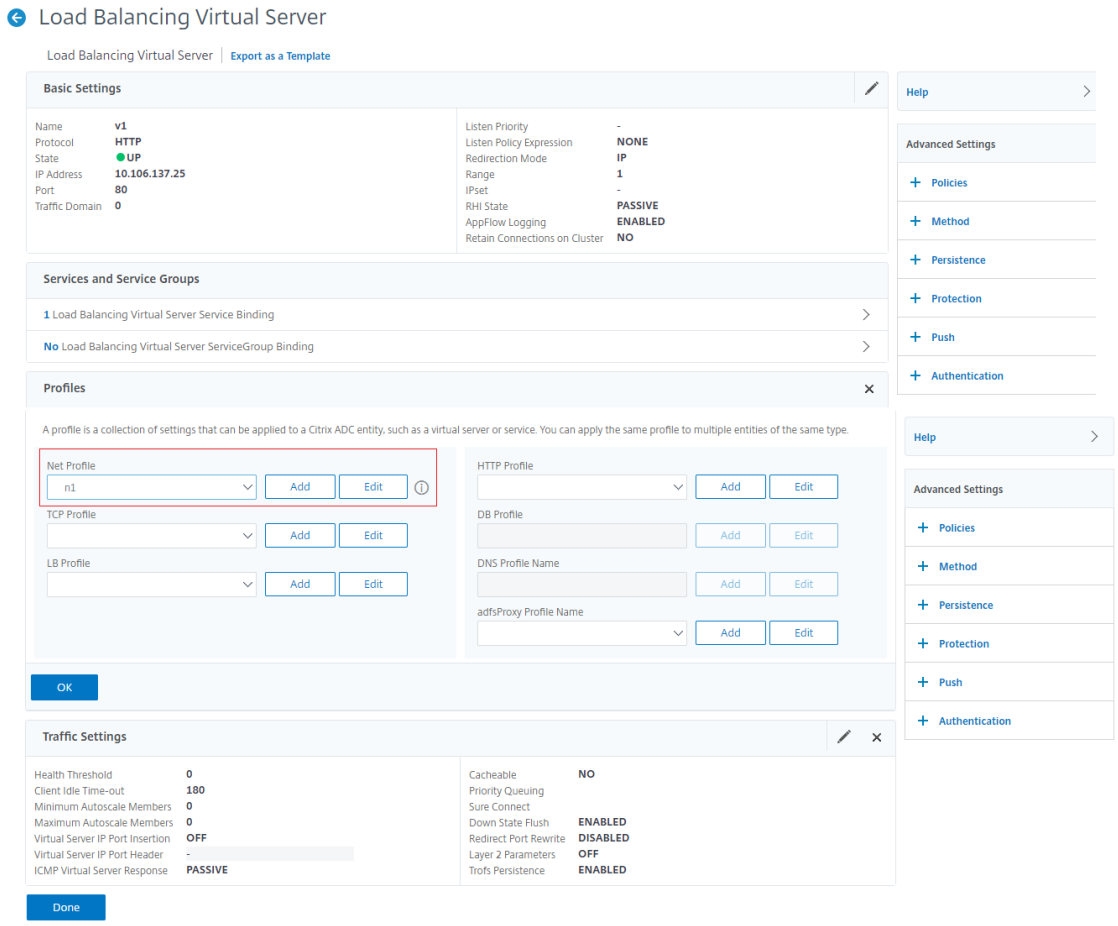
b) Protocole Proxy. Activez ou désactivez le protocole proxy pour le serveur virtuel d'équilibrage de charge.

c) Version TX du protocole proxy. Définissez la version du protocole proxy sur V1 ou V2 en fonction du format de données entrant.

7. Cliquez sur **OK**.

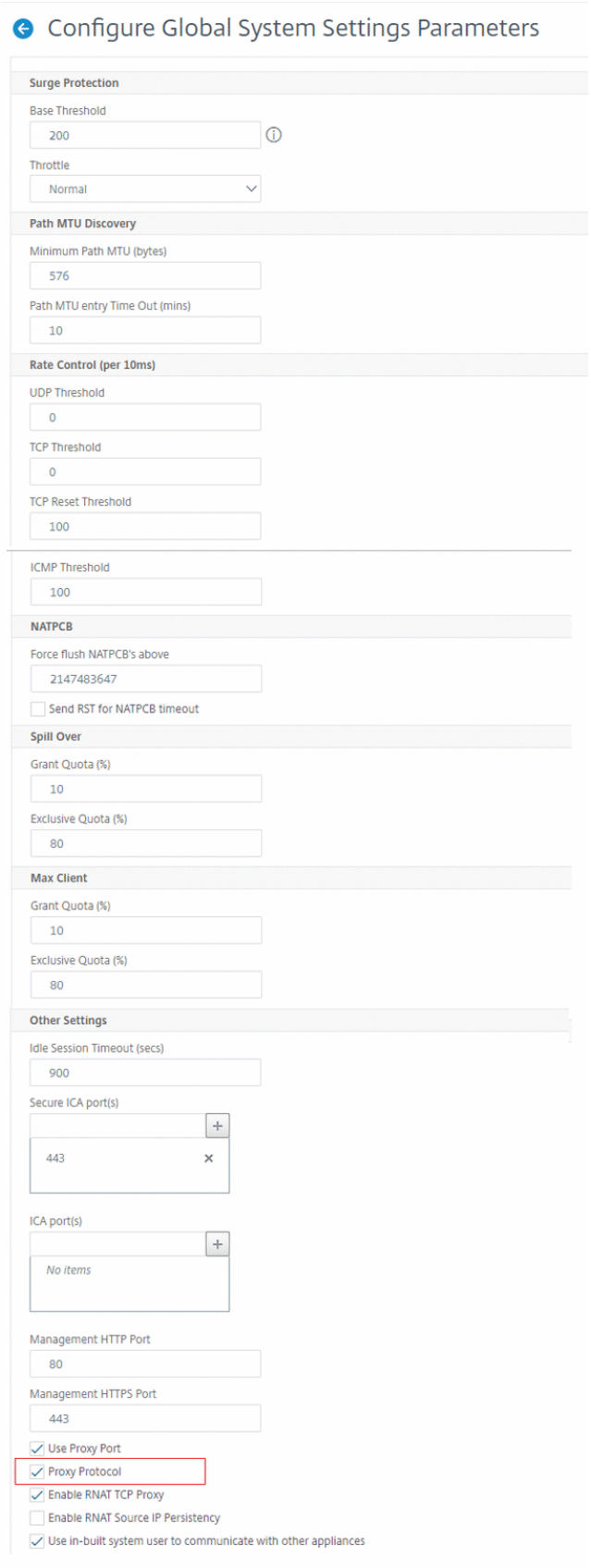


8. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
9. Dans le volet d'informations, cliquez sur **Ajouter**.
10. Dans la page **Serveur virtuel d'équilibrage de charge**, définissez les paramètres de base.
11. Dans la section **Paramètres avancés**, sélectionnez **Profils**.
12. Dans la section **Profils**, cliquez sur l'icône en forme de crayon.
13. Sélectionnez un profil réseau, puis cliquez sur **OK**.
14. Cliquez sur **Terminé**.



15. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
16. Dans le volet d'informations, cliquez sur **Ajouter**.
17. Dans la page **Service d'équilibrage de charge**, définissez les paramètres de base.
18. Dans la section **Paramètres avancés**, sélectionnez **Profils**.
19. Dans la section **Profils**, cliquez sur l'icône en forme de crayon.
20. Sélectionnez un profil réseau, puis cliquez sur **OK**.
21. Cliquez sur **Terminé**.

> **Remarque :**
>
> Si plusieurs appliances Citrix ADC font partie de la couche proxy, vous devez définir la configuration du protocole proxy sur chaque appliance pour l'opération de transfert.



Adresse IP du client dans l'option TCP

August 20, 2021

L'appliance Citrix ADC utilise de nombreuses méthodes pour envoyer les informations du client au serveur principal. Une de ces méthodes consiste à envoyer l'adresse IP du client dans l'option TCP du premier paquet de données. L'appliance utilise le numéro d'option TCP dans le profil TCP, si le serveur principal utilisant l'option TCP pour lire l'adresse IP du client. L'adresse IP est portée dans l'option TCP numéro 28 (configurable sur le service de l'appliance) .
La méthode d'option TCP inclut à la fois des fonctionnalités d'insertion et de transfert pour transporter l'adresse IP du client vers le serveur principal.
Dans la configuration de l'option TCP, l'appliance ajoute une option TCP 28 pour insérer l'adresse IP du client et la transférer au serveur principal. Voici quelques scénarios d'utilisation pour la configuration des options TCP dans une appliance Citrix ADC.Le
multiplexage est désactivé si cette fonctionnalité est activée pour le trafic entrant dans le profil TCP. En outre, si nsapimgr et clientip tcp-options dans le profil TCP sont activés, clientip tcp-option a priorité.

> **Remarque :**
>
> Toutefois, le multiplexage est désactivé sur l'appliance si l'option TCP IP client est activée pour le trafic qui arrive au profil TCP.

- Apprendre l'adresse IP du client d'origine
- Sélection d'une langue pour un site Web
- Bloquer la liste des adresses IP sélectionnées

Voici les deux modes de fonctionnement :

- Insert. L'appliance ajoute les détails du client dans le champ de l'option TCP 28 (la valeur configurable mais préférable est 28) et les envoie au serveur principal.
- Forward. L'appliance transmet les détails du client dans l'option TCP 28 (configurable sur le front-end du service de l'appliance). Toutefois, le numéro d'option au niveau du back-end peut être modifié en fonction de la valeur configurée dans le back-end

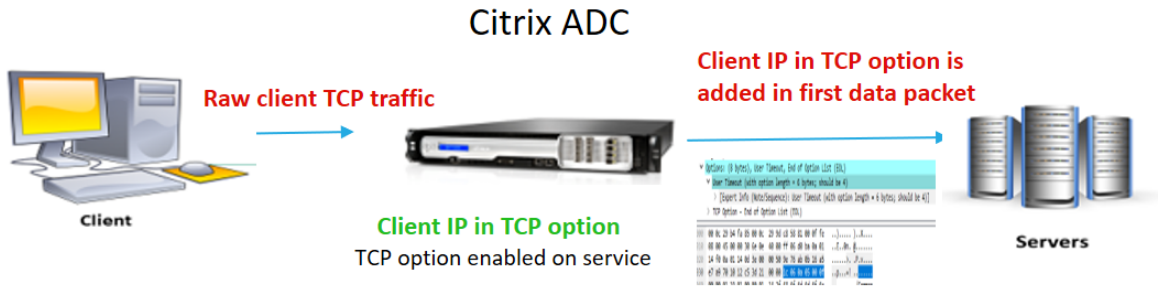
> **Remarque :**
>
> Dans le cas d'un serveur virtuel TCP ou HTTP, le numéro d'option TCP est transféré avec ou sans cette fonctionnalité activée en mode transparent.

Limitations

La fonctionnalité de configuration de l'option TCP n'est pas prise en charge dans les fonctionnalités TFO, MultiPath TCP et HTTP2.

Configuration de l'option TCP dans une appliance Citrix ADC

Les diagrammes de flux suivants montrent comment configurer l'option TCP dans les appliances Citrix ADC pour les opérations d'insertion et de transfert.

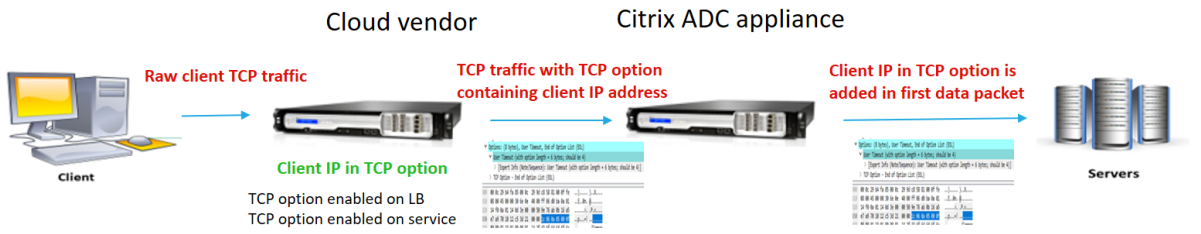


Le composant interagit comme suit :

- Un client envoie une demande à Citrix ADC.
- Dans l'appliance Citrix ADC, vous devez créer un profil TCP, activer la fonction d'option TCP et spécifier le numéro d'option TCP.

  Remarque : Il est conseillé de configurer le numéro d'option TCP comme 28 dans le profil TCP.
- Dans l'opération Insertion, Citrix ADC insère les détails du client dans l'option TCP 28 liée au service. Les détails du client sont ensuite envoyés au serveur principal. Si le trafic entrant est HTTPS, l'adresse IP du client dans l'option TCP sera envoyée dans le message Hello client SSL qui est le premier paquet de données au niveau TCP

Opération en marche :



Le composant interagit comme suit :

- Un client envoie une requête HTTP/HTTPS à Citrix ADC.
- Sur l'appliance Citrix ADC, s'il s'agit d'une opération de transfert, l'option TCP est activée sur le serveur virtuel d'équilibrage de charge ou le serveur virtuel de commutation de contenu et également activée sur le service. L'appliance reçoit les informations client dans le numéro d'option TCP spécifié dans le serveur virtuel et les transmet au serveur principal dans le numéro d'option TCP (configurable dans le service) ajouté dans le premier paquet de données

Configurer l'option TCP pour l'opération Insertion

Suivez la procédure ci-dessous pour configurer l'option TCP dans votre appliance Citrix ADC.

1. Ajoutez un profil TCP.
2. Configurer l'option TCP pour l'opération Insertion
3. Lier le profil TCP au service

Ajouter un profil TCP

À l'invite de commandes, tapez :

```
add tcpprofile <name> -clientIpTcpOption (enabled | disabled> -clientIpTcpOptionNumber
 <positive_integer>
```

Exemple :

```
add tcprofile p1
```

Configurer l'option TCP pour l'opération Insertion

À l'invite de commandes, tapez :

```
add tcpprofile <name> -clientIpTcpOption (enabled | disabled> -clientIpTcpOptionNumber
 <positive_integer>
```

Exemple :

```
add tcpprofile p1 -clientIpTcpOption ENABLED -clientIpTcpOptionNumber 28
```

Ajouter un service

À l'invite de commandes, tapez :

```
add service <name> <server name> <service type> <port>
```

Exemple :

```
add service service-http1 1.1.1.1 HTTP 80
```

Lier le profil TCP au service

À l'invite de commandes, tapez :

```
set service <name> -tcpprofileName <name>
```

Exemple :

```
set service s1 -tcpprofileName p1
```


> **Remarque :**
>
> La configuration de base pour le service doit être prise en charge.

Configurer l'option TCP pour l'opération de transfert

En suivant la procédure ci-dessous pour configurer l'option TCP dans le profil TCP pour l'opération Forward.

1. Ajouter un profil TCP avec le numéro d'option TCP
2. Lier le profil TCP au serveur virtuel
3. Liez le profil TCP au service.

Ajouter un profil TCP avec le numéro d'option TCP

À l'invite de commandes, tapez :

```
add tcpprofile <name> -clientIpTcpOption (enabled | disabled> -clientIpTcpOptionNumber
 <positive_integer>
```

Exemple :

```
add tcpprofile p1 -clientIpTcpOption ENABLED -clientIpTcpOptionNumber 29
```

Liez le profil TCP au serveur virtuel (équilibrage de charge ou commutation de contenu)

À l'invite de commandes, tapez :

```
set lb vserver <name> -tcpprofileName <name>
```

Exemple :

```
set lb vservice s1 -tcpprofileName p1
```

Lier le profil TCP au service

À l'invite de commandes, tapez :

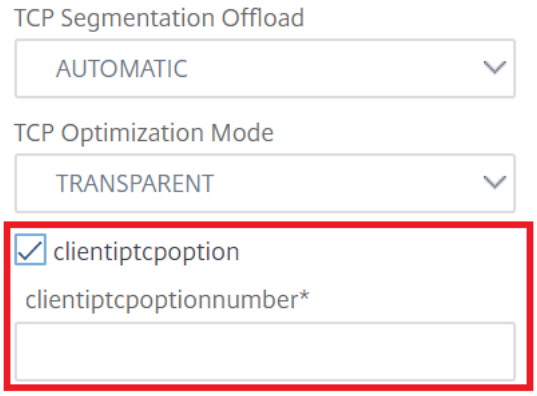
```
set service <name> -tcpprofileName p1
```

Exemple :

```
set service s1 -tcpprofileName p1
```


Configurer l'option TCP à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Système** > **Profils**.
2. Dans la page de l'onglet **Profil TCP**, cliquez sur **Ajouter**.
3. Dans la page **Configurer le profil TCP**, configurez les paramètres suivants :
   a. ClientCPOption. Option TCP pour envoyer ou recevoir l'adresse IP du client.
   b. clientiptcpoptionnumber. Numéro d'option TCP configurable pour recevoir l'adresse IP du client.



4. Cliquez sur **OK** et **Fermer**.

SNMP

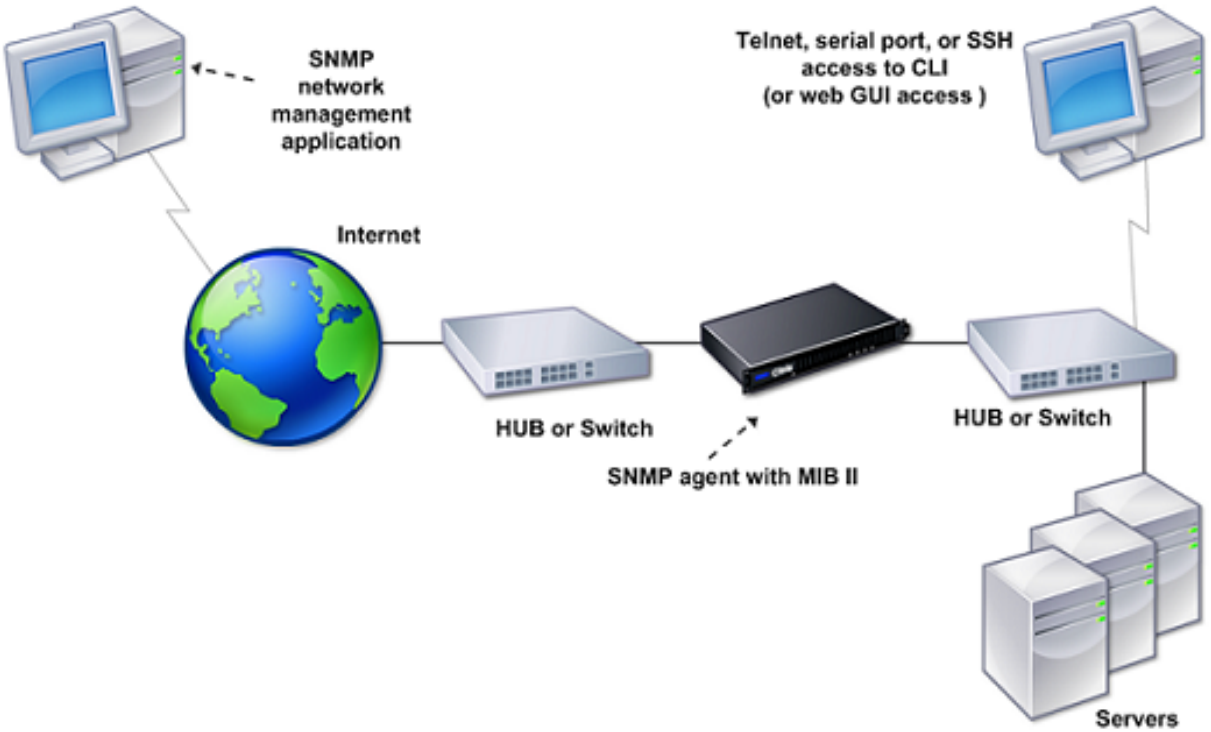
August 20, 2021

Vous pouvez utiliser le protocole SNMP (Simple Network Management Protocol) pour configurer l'agent SNMP sur l'appliance Citrix ADC afin de générer des événements asynchrones, appelés *interruptions*. Les interruptions sont générées chaque fois qu'il y a des conditions anormales sur Citrix ADC. Les interruptions sont ensuite envoyées à un périphérique distant appelé *écouteur d'interruptions*, qui signale la condition anormale de l'appliance Citrix ADC. Vous pouvez également interroger l'agent SNMP pour obtenir des informations spécifiques au système à partir d'un périphérique distant appelé *gestionnaire SNMP*. L'agent recherche ensuite les données demandées dans la base d'informations de gestion (MIB) et les envoie au gestionnaire SNMP.

L'agent SNMP sur Citrix ADC peut générer des interruptions conformes à SNMPv1, SNMPv2 et SNMPv3. Pour l'interrogation, l'agent SNMP prend en charge SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2) et SNMP version 3 (SNMPv3).

Pour plus d'informations sur les paramètres SNMP, les interruptions et ses descriptions, consultez Citrix ADC SNMP OID Reference.

La figure suivante illustre un réseau avec un Citrix ADC sur lequel SNMP est activé et configuré. Dans la figure, chaque application de gestion réseau SNMP utilise SNMP pour communiquer avec l'agent SNMP sur Citrix ADC. L'agent SNMP recherche sa base d'informations de gestion (MIB) pour collecter les données demandées par le gestionnaire SNMP et fournit les informations à l'application.



Important

Le module SNMP d'une appliance Citrix ADC prend en charge une longueur maximale de 128 octets (conforme à la norme RFC 3416) pour un OID SNMP. Un nom de variable d'index long pour un objet peut entraîner un OID SNMP de plus de 128 octets.

Pour résoudre ce problème, le module SNMP Citrix ADC prend en charge une longueur maximale de 31 caractères pour un nom de variable d'index. Si le nom d'une variable d'index dépasse 31 caractères, le module SNMP utilisant un algorithme de hachage convertit le nom en une valeur de hachage de 31 caractères. Cette valeur hachée est utilisée dans l'OID SNMP pour cette variable.

Le nom de la variable d'index d'origine est stocké dans une autre variable, dont le format de nom est le suivant : `<variable type>FullName`. Par exemple, lorsque le nom d'un serveur virtuel d'équilibrage de charge comporte plus de 31 caractères, l'OID `vserverName` SNMP contient la valeur hachée et `vsvrFullName` SNMP OID contient le nom complet (d'origine) du serveur virtuel.

De même, pour les interruptions SNMP, la variable d'index affiche une valeur hachée. `<variable type>FullName`, qui stocke le nom complet du nom de la variable d'index d'origine, fait également partie des messages d'interruption.

Importation de fichiers MIB dans le gestionnaire SNMP et l'écouteur d'interruption

Pour surveiller une appliance Citrix ADC, vous devez télécharger les fichiers de définition d'objet MIB. L'appliance Citrix ADC prend en charge les MIB spécifiques à l'entreprise suivantes :

- **Un sous-ensemble de groupes MIB-2 standard**. Fournit des groupes MIB-2 SYSTEM, IF, ICMP, UDP et SNMP.
- **Un MIB d'entreprise système**. Fournit une configuration et des statistiques spécifiques au système.

Vous pouvez obtenir les fichiers de définition d'objet MIB à partir du répertoire /netscaler/snmp ou de l'onglet Téléchargements de l'interface graphique.

Configuration de Citrix ADC pour générer des interruptions SNMP

August 20, 2021

Vous pouvez configurer l'appliance Citrix ADC pour générer des événements asynchrones, appelés *interruptions*. Les interruptions sont générées chaque fois qu'il y a des conditions anormales sur l'appliance. Les interruptions sont envoyées à un périphérique distant appelé *écouteur d'interruptions*. Il aide les administrateurs à surveiller l'appliance et à réagir rapidement à tous les problèmes.

L'appliance Citrix ADC fournit un ensemble d'entités de condition appelées *alarmes SNMP*. Lorsque la condition d'une alarme SNMP est remplie, l'appliance génère des messages d'interruption SNMP qui sont envoyés aux écouteurs d'interruption configurés. Par exemple, lorsque l'alarme LOGIN-FAILURE est activée, un message d'interruption est généré et envoyé à l'écouteur d'interruption chaque fois qu'il y a un échec de connexion sur l'appliance.

Pour configurer l'appliance Citrix ADC pour générer des interruptions, vous devez activer et configurer les alarmes. Ensuite, vous spécifiez les écouteurs de piège auxquels l'appliance envoie les messages d'interruption générés.

Activation d'une alarme SNMP

L'appliance Citrix ADC génère des interruptions uniquement pour les alarmes SNMP activées. Certaines alarmes sont activées par défaut, mais vous pouvez les désactiver.

Lorsque vous activez une alarme SNMP, l'appliance génère des messages d'interruption correspondants lorsque certains événements se produisent. Certaines alarmes sont activées par défaut.

Pour activer une alarme SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `enable snmp alarm <trapName>`
- `show snmp alarm <trapName>`

Pour activer une alarme SNMP à l'aide de l'interface graphique

1. Accédez à **Système > SNMP > Alarmes**, puis sélectionnez l'alarme.
2. Cliquez sur **Actions** et sélectionnez **Activer** .

Configuration des alarmes

L'appliance Citrix ADC fournit un ensemble d'entités de condition appelées *alarmes SNMP*. Lorsque la condition définie pour une alarme SNMP est remplie, l'appliance génère des messages d'interruptions SNMP qui sont envoyés aux écouteurs d'interruptions configurés. Par exemple, lorsque l'alarme LOGIN-FAILURE est activée, un message d'interruption est généré et envoyé à l'écouteur d'interruption chaque fois qu'il y a un échec de connexion sur l'appliance.

Vous pouvez affecter une alarme SNMP avec un niveau de gravité. Lorsque vous effectuez cette opération, les messages d'interruption correspondants se voient attribuer ce niveau de gravité.

Voici les niveaux de gravité définis sur l'appliance, par ordre décroissant de gravité.

- Critical
- Majeur
- Mineures
- Avertissement
- Informationnel

Par exemple, si vous définissez un niveau de gravité d'avertissement pour l'alarme SNMP nommé LOGIN-FAILURE, les messages d'interruption générés en cas d'échec de connexion sont affectés au niveau de gravité de l'avertissement.

> **Remarque**
>
> Citrix ADC prend en charge diverses alarmes SNMP. Pour plus d'informations, voir Alarmes SNMP.

Vous pouvez également configurer une alarme SNMP pour consigner les messages d'interruption correspondants générés chaque fois que la condition de cette alarme est remplie.

Pour configurer une alarme SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une alarme SNMP et vérifier la configuration :

- `set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-time <secs>] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]`
- `show snmp alarm <trapName>`

Où,

ThresholdValue : Valeur du seuil élevé. L'appliance Citrix ADC génère un message d'interruption SNMP lorsque la valeur de l'attribut associé à l'alarme est supérieure ou égale à la valeur de seuil élevé spécifiée.

NormalValue : valeur pour le seuil normal. Un message d'interruption est généré si la valeur de l'attribut respectif est inférieure ou égale à cette valeur après avoir dépassé le seuil élevé.

Pour configurer les alarmes SNMP à l'aide de l'interface graphique

Accédez à **Système > SNMP > Alarmes**, sélectionnez une alarme et configurez les paramètres d'alarme.

Configuration des interruptions SNMPv1 ou SNMPv2

Après avoir configuré les alarmes, vous devez spécifier l'écouteur d'interruption auquel l'appliance envoie les messages d'interruption. Outre la spécification de paramètres tels que l'adresse IP ou IPv6 et le port de destination de l'écouteur d'interruption, vous pouvez spécifier le type d'interruption (générique ou spécifique) et la version SNMP.

Vous pouvez configurer un maximum de 20 écouteurs d'interruptions pour recevoir des interruptions génériques ou spécifiques.

Vous pouvez également configurer l'appliance pour qu'elle envoie des messages d'interruption SNMP avec une adresse IP source autre que l'adresse IP Citrix ADC (NSIP ou NSIP6) à un écouteur d'interruption particulier. Pour un écouteur d'interruption doté d'une adresse IPv4, vous pouvez définir l'adresse IP source sur une adresse IP mappée (MIP) ou une adresse IP de sous-réseau (SNIP) configurée sur l'appliance. Pour un écouteur de piège doté d'une adresse IPv6, vous pouvez définir l'adresse IP source sur une adresse IPv6 de sous-réseau (SNIP6) configurée sur l'appliance.

Vous pouvez également configurer l'appliance pour qu'elle envoie des messages d'interruption à un écouteur de piège basé sur un niveau de gravité. Par exemple, si vous définissez le niveau de gravité Mineure pour un écouteur d'interruption, tous les messages d'interruption dont le niveau de gravité est égal ou supérieur à Mineure (Mineure, Major et Critique) sont envoyés à l'écouteur d'interruption.

Si vous avez défini une chaîne de communauté pour le processus d'écoute d'interruption, vous devez également spécifier une chaîne de communauté pour chaque interruption à envoyer au processus d'écoute. Un écouteur d'interruption pour lequel une chaîne de communauté a été définie accepte uniquement les messages d'interruption qui incluent une chaîne de communauté correspondant à la chaîne de communauté définie dans l'écouteur d'interruption. D'autres messages d'interruptions sont supprimés.

Pour ajouter une interruption SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp trap <trapClass> <trapDestination> -version ( V1 | V2 )-destPort <port> -communityName <string> -srcIP <ip_addr> -severity <severity>`
- `show snmp trap`

Exemple :

```
> `add snmp trap specific 192.0.2.10 -version V2 -destPort 80 -communityName com1 -severity Major`
<!--NeedCopy-->
```

Pour configurer les interruptions SNMP à l'aide de l'interface graphique

Accédez à **Système > SNMP > Pièges**et créez l'interruption SNMP.

Configuration des interruptions SNMPv3

SNMPv3 fournit des fonctionnalités de sécurité telles que l'authentification et le chiffrement à l'aide des informations d'identification des utilisateurs SNMP. Un gestionnaire SNMP ne peut recevoir des messages d'interruption SNMPv3 que si sa configuration inclut le mot de passe attribué à l'utilisateur SNMP.

La destination d'interruption peut désormais recevoir des messages d'interruption SNMPv1, SNMPv2 et SNMPv3.

Pour configurer une interruption SNMPv3 à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

1. Ajoutez une interruption SNMPv3.


```
add snmp trap <trapClass> <trapDestination> -version ( V1 | V2 | V3)
-destPort <port> -communityName <string> -srcIP <ip_addr> -severity <
severity>
```

> **Remarque**
>
> Une fois définie, la version de l'interruption SNMP ne peut pas être modifiée.

Exemple

```
1 > add snmp trap specific 192.0.2.10 -version V3 -destPort 80 -
     communityName com1 -severity Major
2 <!--NeedCopy-->
```

2. Ajoutez un utilisateur SNMP.

```
add snmp user <name> -group <string> [ -authType ( MD5 | SHA ){ -
authPasswd } [-privType ( DES | AES ){ -privPasswd } ]]
```

Exemple

```
1 > add snmp user edocs_user -group edocs_group
2 <!--NeedCopy-->
```

3. Liez l'interruption SNMPv3 à l'utilisateur SNMP.

```
bind snmp trap <trapClass> <trapDestination> [-version <version>] (-userName
 <string> [-securityLevel <securityLevel>])
```

Exemple

```
1     > bind snmp trap specific 192.0.2.10 -version V3 -userName
         edocs_user -securityLevel authPriv
2 <!--NeedCopy-->
```

Pour configurer une interruption SNMPv3 à l'aide de l'interface graphique

1. Ajoutez une interruption SNMPv3.

   Accédez à **Système > SNMP > Pièges**et créez l'interruption SNMP en sélectionnant V3 comme version SNMP.

2. Ajoutez un utilisateur SNMP.

   Accédez à **Système > SNMP > Utilisateurs** et créez l'utilisateur SNMP.

3. Liez l'interruption SNMPv3 à l'utilisateur SNMP.

   - Accédez à **Système > SNMP > Pièges**, puis sélectionnez l'interruption SNMP version 3.

- Sélectionnez l'utilisateur auquel le piège doit être lié et définissez le niveau de sécurité approprié.

Journalisation des interruptions SNMP

Une appliance Citrix ADC peut consigner les messages d'interruption SNMP (pour les alarmes SNMP dans lesquelles la fonction de journalisation est activée) lorsque vous activez l'option de journalisation des interruptions SNMP et qu'au moins un écouteur d'interruption est configuré sur l'appliance. Vous pouvez désormais spécifier le niveau du journal d'audit des messages d'interruption envoyés à un serveur de journaux externe. Le niveau de journal par défaut est Informational. Les valeurs possibles sont Emergency, Alert, Critical, Error, Avertissement, Debug et Notice.

Par exemple, vous pouvez définir le niveau du journal d'audit sur Critique pour un message d'interruption SNMP généré par un échec d'ouverture de session. Ces informations sont ensuite disponibles sur le serveur NSLOG ou SYSLOG pour le dépannage.

Pour activer la journalisation des interruptions SNMP et configurer le niveau du journal des interruptions à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la journalisation des interruptions SNMP et vérifier la configuration :

- `set snmp option [-snmpTrapLogging (ENABLED | DISABLED)][-snmpTrapLoggingLevel <snmpTrapLoggingLevel>]`
- `show snmp option`

Pour activer la journalisation des interruptions SNMP et configurer le niveau du journal des interruptions SNMP à l'aide de l'interface graphique

Accédez à **Système > SNMP**, cliquez sur Modifier les options SNMP et définissez les paramètres suivants :

1. Enregistrement des interruptions SNMP : activez cette case à cocher pour activer la journalisation des interruptions SNMP lorsqu'au moins un écouteur d'interruptions est configuré sur l'appliance.
2. Niveau de journalisation des interruptions SNMP : sélectionnez un niveau de journal d'audit pour l'interruptions SNMP. Par défaut, le niveau d'audit d'une interruption SNMP est défini sur « Informationnel ». «

Configuration de Citrix ADC pour les requêtes SNMP v1 et v2

August 20, 2021

Vous pouvez interroger l'agent SNMP Citrix ADC pour obtenir des informations spécifiques au système à partir d'un périphérique distant appelé *gestionnaires SNMP*. L'agent recherche ensuite les données demandées dans la base d'informations de gestion (MIB) et les envoie au gestionnaire SNMP.

Les types de requêtes SNMP v1 et v2 suivants sont pris en charge par l'agent SNMP :

- GET
- GET NEXT
- ALL
- GET BULK

Vous pouvez créer des chaînes appelées chaînes de communauté et les associer à des types de requête. Vous pouvez associer une ou plusieurs chaînes de communauté à chaque type de requête. Les chaînes de communauté sont des mots de passe et utilisées pour authentifier les requêtes SNMP à partir de gestionnaires SNMP.

Par exemple, si vous associez deux chaînes de communauté, telles que **abc** et **bcd**, au type de requête GET NEXT, l'agent SNMP de l'appliance Citrix ADC considère uniquement les paquets de requête GET NEXT SNMP qui contiennent **abc** ou **bcd** comme chaîne de communauté.

Spécification d'un gestionnaire SNMP

Vous devez configurer l'appliance Citrix ADC pour permettre aux gestionnaires SNMP appropriés de l'interroger. Vous devez également fournir au gestionnaire SNMP les informations spécifiques à Citrix AD requises. Vous pouvez ajouter jusqu'à 100 gestionnaires SNMP ou réseaux.

Pour un gestionnaire SNMP IPv4, vous pouvez spécifier un nom d'hôte au lieu de l'adresse IP du gestionnaire. Si vous le faites, vous devez ajouter un serveur de noms DNS qui résout le nom d'hôte du gestionnaire SNMP à son adresse IP. Vous pouvez ajouter un maximum de cinq gestionnaires SNMP basés sur le nom d'hôte.

> **Remarque** :
> l'appliance ne prend pas en charge l'utilisation de noms d'hôte pour les gestionnaires SNMP possédant des adresses IPv6. Vous devez spécifier l'adresse IPv6.

Si vous ne configurez pas au moins un gestionnaire SNMP, l'appliance accepte les requêtes SNMP provenant de toutes les adresses IP du réseau et y répond. Si vous configurez un ou plusieurs gestionnaires SNMP, l'appliance accepte et répond uniquement aux requêtes SNMP provenant de ces adresses IP spécifiques.

Si vous supprimez un gestionnaire SNMP de la configuration, ce gestionnaire ne peut plus interroger l'appliance.

Pour ajouter des gestionnaires SNMP en spécifiant des adresses IP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp manager <IPAddress> ... [-netmask <netmask>]`
- `show snmp manager`

Exemple

```
> add snmp manager 10.102.29.10 10.102.29.15 10.102.29.30
```

Pour ajouter un gestionnaire SNMP en spécifiant son nom d'hôte à l'aide de l'interface de ligne de commande

Important : si vous spécifiez le nom d'hôte du gestionnaire SNMP au lieu de son adresse IP, vous devez configurer un serveur de noms DNS pour résoudre le nom d'hôte en adresse IP du gestionnaire SNMP. Pour plus d'informations, voir « Ajout d'un serveur de noms ». «

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp manager <IPAddress> [-domainResolveRetry ****<integer>]`
- `show snmp manager`

Exemple

```
add nameserver 10.103.128.15
add snmp manager engwiki.eng.example.net -domainResolveRetry 10
```

Pour ajouter un gestionnaire SNMP à l'aide de l'interface graphique

1. Accédez à **Système** > **SNMP** > **Gestionnaires** et créez le gestionnaire SNMP.

   > **Important** :
   >
   > si vous spécifiez le nom d'hôte du gestionnaire SNMP au lieu de son adresse IPv4, vous devez configurer un serveur de noms DNS pour résoudre le nom d'hôte en adresse IP du gestionnaire SNMP.

> **Remarque** :
> l'appliance ne prend pas en charge les noms d'hôte pour les gestionnaires SNMP possédant des adresses IPv6.

Spécification d'une communauté SNMP

Vous pouvez créer des chaînes appelées chaînes de communauté et les associer aux types de requête SNMP suivants sur l'appliance :

- GET
- GET NEXT
- ALL
- GET BULK

Vous pouvez associer une ou plusieurs chaînes de communauté à chaque type de requête. Par exemple, lorsque vous associez deux chaînes de communauté, telles que **abc** et **bcd**, au type de requête GET NEXT, l'agent SNMP de l'appliance considère uniquement les paquets de requête GET NEXT SNMP qui contiennent **abc** ou **bcd** comme chaîne de communauté.

Si vous n'associez aucune chaîne de communauté à un type de requête, l'agent SNMP répond à toutes les requêtes SNMP de ce type.

Pour spécifier une communauté SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp community <communityName> <permissions>`
- `show snmp community`

Exemple

```
> add snmp community com all
```

Pour configurer une chaîne de communauté SNMP à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Communauté** et créez la communauté SNMP.

Configuration de Citrix ADC pour les requêtes SNMPv3

August 20, 2021

Simple Network Management Protocol Version 3 (SNMPv3) est basé sur la structure et l'architecture de base de SNMPv1 et SNMPv2. Toutefois, SNMPv3 améliore l'architecture de base pour intégrer des fonctionnalités d'administration et de sécurité, telles que l'authentification, le contrôle d'accès, la vérification de l'intégrité des données, la vérification de l'origine des données, la vérification de l'actualité des messages et la confidentialité des données.

Pour implémenter la sécurité au niveau des messages et le contrôle d'accès, SNMPv3 introduit le modèle de sécurité basé sur l'utilisateur (USM) et le modèle de contrôle d'accès basé sur la vue (VACM).

- **Modèle de sécurité basé sur l'utilisateur.** Le modèle de sécurité basé sur l'utilisateur (USM) fournit une sécurité au niveau du message. Il vous permet de configurer les utilisateurs et les paramètres de sécurité pour l'agent SNMP et le gestionnaire SNMP. USM offre les fonctionnalités suivantes :
  - **Intégrité des données :** pour protéger les messages contre toute modification lors de la transmission via le réseau.
  - **Vérification de l'origine des données :** pour authentifier l'utilisateur qui a envoyé la demande de message.
  - **Rapidité des messages :** Pour se protéger contre les retards ou les rediffusions de messages.
  - **Confidentialité des données :** Protéger le contenu des messages contre la divulgation à des entités ou individus non autorisés.
- **Modèle de contrôle d'accès basé sur la vue.** Le modèle de contrôle d'accès basé sur la vue (VACM) vous permet de configurer les droits d'accès à une sous-arborescence spécifique de la MIB en fonction de différents paramètres, tels que le niveau de sécurité, le modèle de sécurité, le nom d'utilisateur et le type de vue. Il vous permet de configurer les agents pour fournir différents niveaux d'accès à la MIB à différents gestionnaires.

Citrix ADC prend en charge les entités suivantes qui vous permettent d'implémenter les fonctionnalités de sécurité de SNMPv3 :

- Moteurs SNMP
- Vues SNMP
- Groupes SNMP
- Utilisateurs SNMP

Ces entités fonctionnent ensemble pour implémenter les fonctionnalités de sécurité SNMPv3. Les vues sont créées pour permettre l'accès aux sous-arborescences de la MIB. Ensuite, des groupes sont créés avec le niveau de sécurité requis et l'accès aux vues définies. Enfin, les utilisateurs sont créés et affectés aux groupes.

> **Remarque** :
>
> La configuration de la vue, du groupe et de l'utilisateur sont synchronisés et propagés vers le

> nœud secondaire dans une paire haute disponibilité (HA). Toutefois, l'ID du moteur n'est ni propagé ni synchronisé car il est unique à chaque appliance Citrix ADC.

Pour implémenter l'authentification des messages et le contrôle d'accès, vous devez effectuer les opérations suivantes :

Définition de l'ID du moteur

Les moteurs SNMP sont des fournisseurs de services qui résident dans l'agent SNMP. Ils fournissent des services tels que l'envoi, la réception et l'authentification des messages. Les moteurs SNMP sont identifiés de manière unique à l'aide d'ID de moteur.

L'appliance Citrix ADC possède un EngineID unique basé sur l'adresse MAC de l'une de ses interfaces. Il n'est pas nécessaire de remplacer le EngineID. Toutefois, si vous souhaitez modifier l'ID du moteur, vous pouvez le réinitialiser.

Pour définir l'ID du moteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `set snmp engineId <engineID>`
- `show snmp engineId`

Exemple

```
> set snmp engineId 8000173f0300c095f80c68
```

Pour définir l'ID du moteur à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Utilisateurs**, cliquez sur **Configurer l'ID du moteur** et tapez un ID du moteur.

Configurer une vue

Les vues SNMP limitent l'accès des utilisateurs à des parties spécifiques de la MIB. Les vues SNMP sont utilisées pour implémenter le contrôle d'accès.

Pour ajouter une vue SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp view <name> <subtree> -type ( included | excluded )`
- `show snmp view <name>`
- `rm snmp view <name> <subtree>`

Où,

Nom. Nom de la vue SNMPv3. Il peut se composer de 1 à 31 caractères comprenant des majuscules et minuscules, des chiffres et le tiret (-), point (.) livre (#), espace (), signe (@), égal (=), deux-points (:) et trait de soulignement (_). Vous devez choisir un nom qui aide à identifier la vue SNMPv3.

Sous-arbre. Branche (sous-arborescence) particulière de l'arborescence MIB que vous souhaitez associer à cette vue SNMPv3 . Vous devez spécifier la sous-arborescence en tant qu'OID SNMP. Ceci est un argument de longueur maximale : 99.

type. Incluez ou excluez la sous-arborescence, spécifiée par le paramètre sous-arborescence, dans ou à partir de cette vue. Ce paramètre peut être utile lorsque vous avez inclus une sous-arborescence, telle que A, dans une vue SNMPv3 et que vous souhaitez exclure une sous-arborescence spécifique de A, telle que B, de la vue SNMPv3. Il s'agit d'un argument obligatoire. Valeurs possibles : included, excluded.

Exemples

add snmp view SNMPv3test 1.1.1.1 -type included
sh snmp view SNMPv3test
rm snmp view SNMPv3test 1.1.1.1

Pour configurer une vue SNMP à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Vues** et créez la vue SNMP.

Configurer un groupe

Les groupes SNMP sont des agrégations logiques d'utilisateurs SNMP. Ils sont utilisés pour mettre en œuvre le contrôle d'accès et définir les niveaux de sécurité. Vous pouvez configurer un groupe SNMP pour définir des droits d'accès pour les utilisateurs affectés à ce groupe, limitant ainsi les utilisateurs à des vues spécifiques.

Vous devez configurer un groupe SNMP pour définir les droits d'accès pour les utilisateurs affectés à ce groupe.

Pour ajouter un groupe SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp group <name> <securityLevel> -readViewName <string>`
- `show snmp group <name> <securityLevel>`

Où,

Nom. Nom du groupe SNMPv3. Peut être composé de 1 à 31 caractères comprenant des majuscules et minuscules, des chiffres et le tiret (-), point (.) livre (#), espace (), signe (@), égal (=), deux-points (:) et trait de soulignement (_). Vous devez choisir un nom qui aide à identifier le groupe SNMPv3.

Niveau de sécurité. Niveau de sécurité requis pour la communication entre l'appliance Citrix ADC et les utilisateurs SNMPv3 appartenant au groupe. Spécifiez l'une des options suivantes :

noAuthNoPriv. Ne nécessite ni l'authentification ni le chiffrement.

authNoPriv. Exiger une authentification mais pas de chiffrement.

authPriv. Exiger l'authentification et le chiffrement. Remarque : Si vous spécifiez l'authentification, vous devez spécifier un algorithme de chiffrement lorsque vous affectez un utilisateur SNMPv3 au groupe. Si vous spécifiez également le chiffrement, vous devez attribuer à la fois un algorithme d'authentification et un algorithme de chiffrement pour chaque membre du groupe. Il s'agit d'un argument obligatoire. Valeurs possibles : NoAuthNoPriv, AuthNoPriv, AuthPriv.

readViewName. Nom de la vue SNMPv3 configurée que vous souhaitez lier à ce groupe SNMPv3. Un utilisateur SNMPv3 lié à ce groupe peut accéder aux sous-arborescences liées à cette vue SNMPv3 en tant que type INCLUDED, mais ne peut pas accéder à celles de type EXCLUDED. Si l'appliance Citrix ADC comporte plusieurs entrées de vue SNMPv3 portant le même nom, toutes ces entrées sont associées au groupe SNMPv3. Il s'agit d'un argument obligatoire. Longueur maximale : 31

Pour configurer un groupe SNMP à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Groupes** et créez le groupe SNMP.

Configuration d'un utilisateur

Les utilisateurs SNMP sont les gestionnaires SNMP que les agents autorisent à accéder aux MIB. Chaque utilisateur SNMP est affecté à un groupe SNMP.

Vous devez configurer les utilisateurs au niveau de l'agent et affecter chaque utilisateur à un groupe.

Pour configurer un utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp user <name> -group <string> [-authType ( MD5 | SHA ){ -authPasswd } [-privType ( DES | AES ){ -privPasswd } ]]`

- `show snmp user <name>`

Où,

AuthType est l'option d'authentification disponible lors de la configuration d'un utilisateur. Il existe deux types d'authentification tels que MD5 et SHA.

PrivType est l'option de chiffrement disponible lors de la configuration d'un utilisateur. Il existe deux types de chiffrement tels que DES de taille de clé 128 bits et AES de taille de clé 128 bits.

Exemple

```
1 > add snmp user edocs_user -group edocs_group
2 <!--NeedCopy-->
```

Pour configurer un utilisateur SNMP à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Utilisateurs** et créez l'utilisateur SNMP.

Configuration des alarmes SNMP pour la limitation de débit

August 20, 2021

Les appliances Citrix ADC telles que Citrix ADC MPX 10500, 12500 et 15500 sont limitées au débit. Le débit maximal (Mbps) et les paquets par seconde (PPS) sont déterminés par la licence achetée pour l'appliance. Pour les plates-formes à débit limité, vous pouvez configurer les interruptions SNMP pour envoyer des notifications lorsque le débit et le PPS approchent leurs limites et lorsqu'ils reviennent à la normale.

Le débit et les PPS sont surveillés toutes les sept secondes. Vous pouvez configurer des interruptions avec des valeurs de seuil élevé et de seuil normal, exprimées en pourcentage des limites autorisées. L'appliance génère ensuite un interruptions lorsque le débit ou le PPS dépasse le seuil élevé, et un second interruptions lorsque le paramètre surveillé atteint le seuil normal. Outre l'envoi des interruptions au périphérique de destination configuré, Citrix ADC consigne les événements associés aux interruptions dans le fichier /var/log/ns.log sous la forme EVENT ALERTSTARTED et EVENT ALERTENDED.

Le dépassement de la limite de débit peut entraîner une perte de paquets. Vous pouvez configurer les alarmes SNMP pour signaler la perte de paquets.

Pour plus d'informations sur les alarmes et les interruptions SNMP, reportez-vous àla section « Configuration de Citrix ADC pour générer des interruptions SNMP v1 et v2. «

Ce document comprend les détails suivants :

- Configuration d'une alarme SNMP pour le débit ou le PPS
- Configuration de l'alarme SNMP pour les paquets abandonnés

Configuration d'une alarme SNMP pour le débit ou le PPS

Pour surveiller à la fois tout au long et PPS, vous devez configurer des alarmes individuelles et définir la valeur de seuil pps en Mbps.

Pour configurer une alarme SNMP pour le débit à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer l'alarme SNMP, définir la valeur seuil en Mbps et vérifier la configuration :

- `set snmp alarm PF-RL-RATE-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state ( **ENABLED** | **DISABLED** )] [-severity <severity>] [-logging ( **ENABLED** | **DISABLED** )]`
- `show snmp alarm PF-RL-RATE-THRESHOLD`

Exemple

```
1 > set snmp alarm PF-RL-RATE-THRESHOLD -thresholdValue 70 -normalValue
     50
2 <!--NeedCopy-->
```

Pour configurer une alarme SNMP pour PPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer l'alarme SNMP pour PPS et vérifier la configuration :

- `set snmp alarm PF-RL-PPS-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state ( **ENABLED** | **DISABLED** )] [-severity <severity>] [-logging ( **ENABLED** | **DISABLED** )]`
- `show snmp alarm PF-RL-PPS-THRESHOLD`

Exemple

```
1 > set snmp alarm PF-RL-PPS-THRESHOLD -thresholdValue 70 -normalValue 50
2 <!--NeedCopy-->
```


Pour configurer une alarme SNMP pour le débit ou le PPS à l'aide de l'interface graphique

1. Accédez à **Système** > **SNMP** > **Alarmes**, puis sélectionnez **PF-RL-RATE-THRESHOLD** (pour le débit) ou **PF-RL-PPS-THRESHOLD** (pour les paquets par seconde).
2. Définissez les paramètres de l'alarme et activez l'alarme SNMP sélectionnée.

Configuration de l'alarme SNMP pour les paquets abandonnés

Vous pouvez configurer une alarme pour les paquets abandonnés en raison du dépassement de la limite de débit et une alarme pour les paquets abandonnés en raison du dépassement de la limite PPS.

Pour configurer une alarme SNMP pour les paquets abandonnés en raison d'un débit excessif, à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set snmp alarm PF-RL-RATE-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Pour configurer une alarme SNMP pour les paquets abandonnés en raison d'un PPS excessif, à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set snmp alarm PF-RL-PPS-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Pour configurer une alarme SNMP pour les paquets supprimés à l'aide de l'interface graphique

1. Accédez à **Système** > **SNMP** > **Alarmes**, puis sélectionnez **PF-RL-RATE-PKTS-DROPPED** (pour les paquets abandonnés en raison d'un débit excessif) ou **PF-RL-PPS-PKTS-DROPPED** (pour les paquets abandonnés en raison d'un débit excessif).
2. Définissez les paramètres de l'alarme et activez l'alarme SNMP sélectionnée.

Configuration de SNMP en mode FIPS

August 20, 2021

Le mode FIPS nécessite Simple Network Management Protocol version 3 (SNMPv3) avec l'option Auth-Priv (AuthPriv). SNMP version 1 et version 2 utilisent un mécanisme de chaîne de communauté pour

fournir un accès sécurisé aux données de gestion. La chaîne de communauté est envoyée en texte clair entre un gestionnaire SNMP et un agent SNMP. Ce type de communication n'est pas sécurisé, ce qui permet aux intrus d'accéder aux informations SNMP sur le réseau.

Le protocole SNMPv3 utilise le modèle de sécurité basé sur l'utilisateur (USM) et le modèle de contrôle d'accès basé sur la vue (VACM) pour authentifier et contrôler l'accès de gestion aux données de messagerie SNMP. SNMPv3 a trois niveaux de sécurité : aucune authentification aucune confidentialité (NoAuthNoPriv), authentification et aucune confidentialité (AuthNoPriv), et authentification et confidentialité (AuthPriv).

L'activation du mode FIPS et le redémarrage de l'appliance Citrix ADC supprime les configurations SNMP suivantes de l'appliance :

1. Configuration de la communauté pour les protocoles SNMPv1 et SNMPv2.
2. Groupes SNMPv3 configurés avec l'option de niveau de sécurité NoAuthNoPriv ou AuthNoPriv.
3. Pièges configurés pour SNMPv1 ou SNMPv2 ou SNMPv3 avec l'option de niveau de sécurité NoAuthNopriv.

Après le redémarrage de l'appliance, configurez SNMPv3 avec l'option AuthPriv. Pour plus d'informations sur la configuration de l'option AuthPriv dans SMNP v3, consultez la rubrique SNMPV3.

> **Remarque** :
>
> L'activation du mode FIPS et le redémarrage de votre appliance bloquent l'exécution des commandes SNMP d'interruption et de groupe suivantes :

```
1     1.  add snmp community <communityName> <permissions>
2
3     2.  add snmp trap <trapClass> <trapDestination> ... [-version: v1/
          v2]   [-td <positive_integer>] [-destPort <port>] [-
          communityName <string>] [-srcIP <ip_addr|ipv6_addr>] [-severity
          <severity>] [-allPartitions ( ENABLED | DISABLED )]
4
5     3.  add snmp group <name> <securityLevel : noAuthNoPriv/ authNoPriv
           > -readViewName <string>
6
7     4.  bind snmp trap specific <TrapIp>-userName <v3 user name> -
          securityLevel <noAuthNoPriv/ authNoPriv>
8 <!--NeedCopy-->
```


Journalisation d'audit

August 20, 2021

> **Important**
>
> Citrix vous recommande de mettre à jour une configuration SYSLOG ou NSLOG uniquement pendant les périodes de maintenance ou d'arrêt. Si vous mettez à jour une configuration après avoir créé une session, les modifications ne sont pas appliquées aux journaux de session existants.

La vérification est un examen méthodique ou un examen d'une condition ou d'une situation. La fonctionnalité de journalisation d'audit vous permet de consigner les états Citrix ADC et les informations d'état collectées par différents modules. Les informations de journal peuvent se trouver dans le noyau et dans les démons au niveau utilisateur. Pour la journalisation d'audit, vous pouvez utiliser le protocole SYSLOG, le protocole NSLOG natif ou les deux.

SYSLOG est un protocole standard pour la journalisation. Il a deux composantes :

- **Module d'audit SYSLOG.** S'exécute sur l'appliance Citrix ADC.
- **Serveur SYSLOG.** S'exécute sur le système d'exploitation (OS) FreeBSD sous-jacent de l'appliance Citrix ADC ou sur un système distant.

SYSLOG utilise un protocole de données utilisateur (UDP) pour le transfert de données.

De même, le protocole NSLOG natif a deux composants :

- **Module d'audit NSLOG.** S'exécute sur l'appliance Citrix ADC.
- **Serveur NSLOG.** S'exécute sur le système d'exploitation FreeBSD sous-jacent de l'appliance Citrix ADC ou sur un système distant.

NSLOG utilise TCP pour le transfert de données.

Lorsque vous exécutez un serveur SYSLOG ou NSLOG, il se connecte à l'appliance Citrix ADC. L'appliance Citrix ADC commence ensuite à envoyer toutes les informations de journal au serveur SYSLOG ou NSLOG. Et le serveur filtre les entrées du journal avant de les stocker dans un fichier journal. Un serveur NSLOG ou SYSLOG reçoit des informations de journal de plusieurs appliances Citrix ADC. L'appliance Citrix ADC envoie des informations de journal à plusieurs serveurs SYSLOG ou serveur NSLOG.

Si plusieurs serveurs SYSLOG sont configurés, l'appliance Citrix ADC envoie ses événements et messages SYSLOG à tous les serveurs de journaux externes configurés. Cela entraîne le stockage des messages redondants et rend la surveillance difficile pour les administrateurs système. Pour résoudre ce problème, l'appliance Citrix ADC propose des algorithmes d'équilibrage de charge. L'appliance peut équilibrer la charge des messages SYSLOG entre les serveurs de journaux externes pour améliorer la maintenance et les performances. Les algorithmes d'équilibrage de charge pris en charge incluent RoundRobin, LeastBandWidth, CustomLoad, LeastPackets et AuditLogHash.

> **Remarque**
>
> L'appliance Citrix ADC peut envoyer des messages de journal d'audit jusqu'à 16 Ko à un serveur SYSLOG externe.

Les informations de journal collectées par un serveur SYSLOG ou NSLOG à partir d'une appliance Citrix ADC sont stockées dans un fichier journal sous forme de messages. Ces messages contiennent généralement les informations suivantes :

- Adresse IP d'une appliance Citrix ADC qui a généré le message de journal.
- Un horodatage
- Le type de message
- Les niveaux de journalisation prédéfinis (Critique, Erreur, Avis, Avertissement, Informations, Débogage, Alerte et Urgence)
- Les informations de message

Pour configurer la journalisation d'audit, vous devez d'abord configurer les modules d'audit sur l'appliance Citrix ADC. L'appliance implique la création de stratégies d'audit et la spécification des informations sur le serveur NSLOG ou SYSLOG. Vous installez ensuite et configurez le serveur SYSLOG ou NSLOG sur le système d'exploitation FreeBSD sous-jacent de l'appliance Citrix ADC ou sur un système distant.

> **Remarque**
>
> SYSLOG est une norme de l'industrie pour enregistrer les messages de programme, et divers fournisseurs fournissent un support. La documentation n'inclut pas les informations de configuration du serveur SYSLOG.

Le serveur NSLOG possède son propre fichier de configuration (auditlog.conf). Vous pouvez personnaliser la journalisation sur le système serveur NSLOG en apportant des modifications supplémentaires au fichier de configuration (auditlog.conf).

Configuration de l'appliance Citrix ADC pour la journalisation d'audit

October 5, 2021

La journalisation d'audit affiche les informations d'état des différents modules afin qu'un administrateur puisse consulter l'historique des événements dans l'ordre chronologique. Les principales composantes d'un cadre d'audit sont « action d'audit », « politique d'audit ». « Action d'audit » décrit les informations de configuration du serveur d'audit, tandis que la « stratégie d'audit » lie une entité de liaison à une « action d'audit ». Les stratégies d'audit utilisent le framework « Classic Policy Engine » (CPE) ou le framework Progress Integration (PI) pour lier « action d'audit » aux « entités de liaison globale du système ».

Toutefois, les cadres de stratégie diffèrent les uns des autres en ce qui concerne la liaison des stratégies de journal d'audit aux entités globales. Auparavant, le module d'audit ne supportait que les expressions classiques, mais il prend désormais en charge les expressions de stratégie classiques et avancées. Actuellement, l'expression Advanced ne peut lier les stratégies de journal d'audit qu'aux entités globales système.

> **Remarque**
>
> Lorsque vous liez une stratégie à des entités globales, vous devez la lier à une entité globale système de la même expression. Par exemple, vous ne pouvez pas lier une stratégie classique à une entité globale avancée ou une stratégie avancée à une entité globale classique.
>
> En outre, vous ne pouvez pas lier à la fois la stratégie de journal d'audit classique et la stratégie de journal d'audit avancée à un serveur virtuel d'équilibrage de charge.

Configuration des stratégies de journal d'audit dans une expression de stratégie classique

La configuration de la journalisation d'audit dans la stratégie classique comprend les étapes suivantes :

1. **Configuration d'une action de journal d'audit**. Vous pouvez configurer une action d'audit pour différents serveurs et pour différents niveaux de journalisation. « Action d'audit » décrit les informations de configuration du serveur d'audit, tandis que la « stratégie d'audit » lie une entité de liaison à une « action d'audit ». Par défaut, le SYSLOG et le NSLOG utilisent uniquement le protocole TCP pour transférer les informations de journal vers les serveurs de journaux. Le protocole TCP est plus fiable que le protocole UDP pour transférer des données complètes. Lorsque vous utilisez TCP pour SYSLOG, vous pouvez définir la limite de la mémoire tampon sur l'appliance Citrix ADC pour stocker les journaux. Après quoi, les journaux sont envoyés au serveur SYSLOG.
2. **Configuration de la stratégie de journal d'audit**. Vous pouvez configurer des stratégies SYSLOG pour consigner les messages sur un serveur SYSLOG ou une stratégie NSLOG pour consigner les messages sur un serveur NSLOG. Chaque stratégie inclut une règle identifiant les messages à consigner, ainsi qu'une action SYSLOG ou NS LOG.
3. **Liaison des stratégies de journal d'audit aux entités globales**. Vous devez lier globalement les stratégies de journal d'audit à des entités globales telles que SYSTEM, VPN, Citrix ADC AAA, etc. Vous pouvez le faire pour activer la journalisation de tous les événements système Citrix ADC. En définissant le niveau de priorité, vous pouvez définir l'ordre d'évaluation de la journalisation du serveur d'audit. La priorité 0 est la plus élevée et est évaluée en premier. Plus le numéro de priorité est élevé, plus la priorité de l'évaluation est faible.

Chacune de ces étapes est expliquée dans les sections suivantes.

Configuration de l'action du journal d'audit

Pour configurer l'action SYSLOG dans l'infrastructure Advanced Policy à l'aide de l'interface de ligne de commande.

> **Remarque**
>
> L'appliance Citrix ADC vous permet de configurer une seule action SYSLOG sur l'adresse IP et le port du serveur SYSLOG. La solution matérielle-logicielle ne vous permet pas de configurer plusieurs actions SYSLOG sur la même adresse IP et le même port du serveur.

Une action Syslog contient une référence à un serveur Syslog. Il spécifie les informations à consigner et indique comment consigner ces informations.

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
1 - add audit syslogAction <name> <serverIP> [-serverPort <port>] -
    logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )] [-
    transport ( TCP | UDP )]`
2 - show audit syslogAction [<name>]
3
4 <!--NeedCopy-->
```

Pour configurer l'action NSLOG dans l'infrastructure Advanced Policy à l'aide de l'interface de ligne de commande

Une action de journal ns contient une référence à un serveur nslog. Il spécifie les informations à consigner et indique comment consigner ces informations.

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
1 - add audit nslogAction <name> <serverIP> [-serverPort <port>] -
    logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
2 - show audit nslogAction [<name>]
3 <!--NeedCopy-->
```

Configuration des stratégies de journal d'audit

Pour configurer les stratégies de journal d'audit dans l'infrastructure de stratégie classique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 - add audit syslogpolicy <name> <-rule> <action>
```



```
2 -  add audit nslogpolicy <name> < rule> <action>rm audit nslogpolicy <
     name>show audit nslogpolicy [<name>]set audit nslogpolicy <name>  [-
     rule <expression>] [-action <name>]
3 <!--NeedCopy-->
```

Liaison des stratégies de Syslog d'audit à l'audit global de Syslog

Pour lier la stratégie de journal d'audit dans la structure de stratégie classique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind audit syslogGlobal <policyName> [-globalBindType <globalBindType
```

```
unbind audit syslogGlobal <policyName>[-globalBindType <globalBindType>]
```

Configuration des stratégies de journal d'audit à l'aide de l'expression de stratégie avancée

La configuration de la journalisation d'audit dans la stratégie avancée comprend les étapes suivantes :

1. **Configuration d'une action de journal d'audit**. Vous pouvez configurer une action d'audit pour différents serveurs et pour différents niveaux de journalisation. « Action d'audit » décrit les informations de configuration du serveur d'audit, tandis que la « stratégie d'audit » lie une entité de liaison à une « action d'audit ». Par défaut, le SYSLOG et le NSLOG utilisent uniquement le protocole TCP pour transférer les informations de journal vers les serveurs de journaux. Le protocole TCP est plus fiable que le protocole UDP pour transférer des données complètes. Lorsque vous utilisez TCP pour SYSLOG, vous pouvez définir la limite de la mémoire tampon sur l'appliance Citrix ADC pour stocker les journaux. Après quoi, les journaux sont envoyés au serveur SYSLOG.
2. **Configuration de la stratégie de journal d'audit**. Vous pouvez configurer des stratégies SYSLOG pour consigner les messages sur un serveur SYSLOG ou une stratégie NSLOG pour consigner les messages sur un serveur NSLOG. Chaque stratégie inclut une règle identifiant les messages à consigner, ainsi qu'une action SYSLOG ou NS LOG.
3. **Liaison des stratégies de journal d'audit aux entités globales**. Vous devez lier globalement les stratégies de journal d'audit à l'entité globale SYSTEM pour activer la journalisation de tous les événements système Citrix ADC. En définissant le niveau de priorité, vous pouvez définir l'ordre d'évaluation de la journalisation du serveur d'audit. La priorité 0 est la plus élevée et est évaluée en premier. Plus le numéro de priorité est élevé, plus la priorité de l'évaluation est faible.

> **Remarque**
>
> L'appliance Citrix ADC évalue toutes les stratégies liées à true.

Configuration de l'action du journal d'audit

Pour configurer l'action Syslog dans l'infrastructure Advanced Policy à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
1 - add audit syslogAction <name> <serverIP> [-serverPort <port>] -
    logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )] [-
    transport ( TCP | UDP )]
2 - show audit syslogAction [<name>]
3 <!--NeedCopy-->
```

Pour configurer l'action NSLOG dans l'infrastructure Advanced Policy à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
1 - add audit nslogAction <name> <serverIP> [-serverPort <port>] -
    logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
2 - show audit nslogAction [<name>]
3 <!--NeedCopy-->
```

Configuration des stratégies de journal d'audit

Pour ajouter une action d'audit Syslog à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1    add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
       domainResolveRetry <integer>])
2    | -lbVserverName <string>))[-serverPort <port>] -logLevel <logLevel
       >[-dateFormat <dateFormat>]
3     [-logFacility <logFacility>][-tcp ( NONE | ALL )] [-acl ( ENABLED
        | DISABLED )]
4    [-timeZone ( GMT_TIME | LOCAL_TIME )][-userDefinedAuditlog ( YES |
       NO )]
5     [-appflowExport ( ENABLED | DISABLED )] [-lsn ( ENABLED | DISABLED
        )][-alg ( ENABLED | DISABLED )]
```



```
6      [-subscriberLog ( ENABLED | DISABLED )][-transport ( TCP | UDP )]
          [-tcpProfileName <string>][-maxLogDataSizeToHold
7  <!--NeedCopy-->
```

Exemple

```
1      > add audit syslogaction audit-action1 10.102.1.1 -loglevel
          INFORMATIONAL -dateformat MMDDYYYY
2      > add audit nslogAction nslog-action1 10.102.1.3 -serverport 520 -
          loglevel INFORMATIONAL -dateFormat MMDDYYYY
3      > add audit syslogpolicy syslog-pol1 TRUE audit-action1
4      > add audit nslogPolicy nslog-pol1 TRUE nslog-action1
5      > bind system global nslog-pol1 -priority 20
6  <!--NeedCopy-->
```

Pour ajouter une action d'audit nslog à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1      add audit nslogAction <name> (<serverIP> | (<serverDomainName>[-
          domainResolveRetry <integer>])) [-serverPort <port>]       -
          logLevel <logLevel> ... [-dateFormat <dateFormat>][-logFacility
          <logFacility>] [-tcp ( NONE | ALL )][-acl ( ENABLED | DISABLED )
          ] [-timeZone ( GMT_TIME | LOCAL_TIME )][-userDefinedAuditlog (
          YES | NO )][-appflowExport ( ENABLED | DISABLED )] [-lsn (
          ENABLED | DISABLED )][-alg ( ENABLED | DISABLED )] [-
          subscriberLog ( ENABLED | DISABLED )]`
2  <!--NeedCopy-->
```

Liaison des stratégies de journal d'audit aux entités globales

Pour lier la stratégie de journal d'audit Syslog dans la structure de stratégie avancée à l'aide de l'interface de ligne de commande

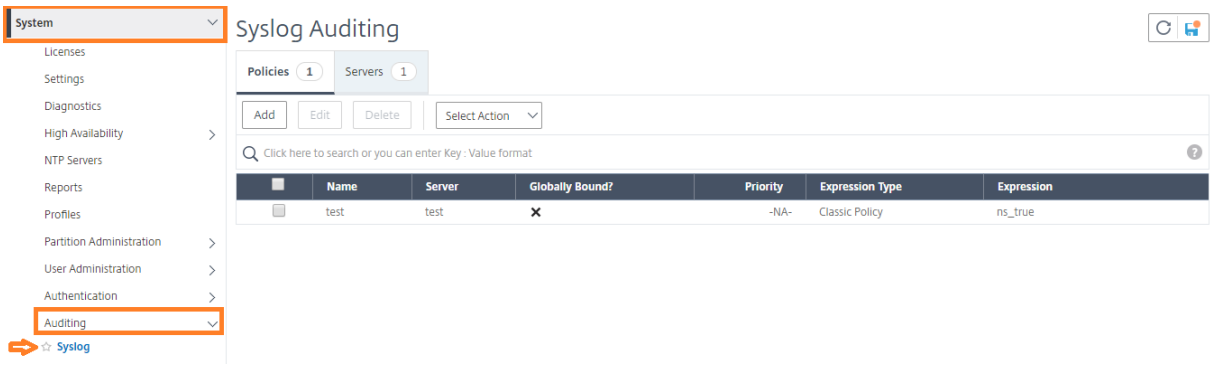
À l'invite de commandes, tapez :

```
bind audit syslogGlobal <policyName> [-globalBindType <globalBindType
```

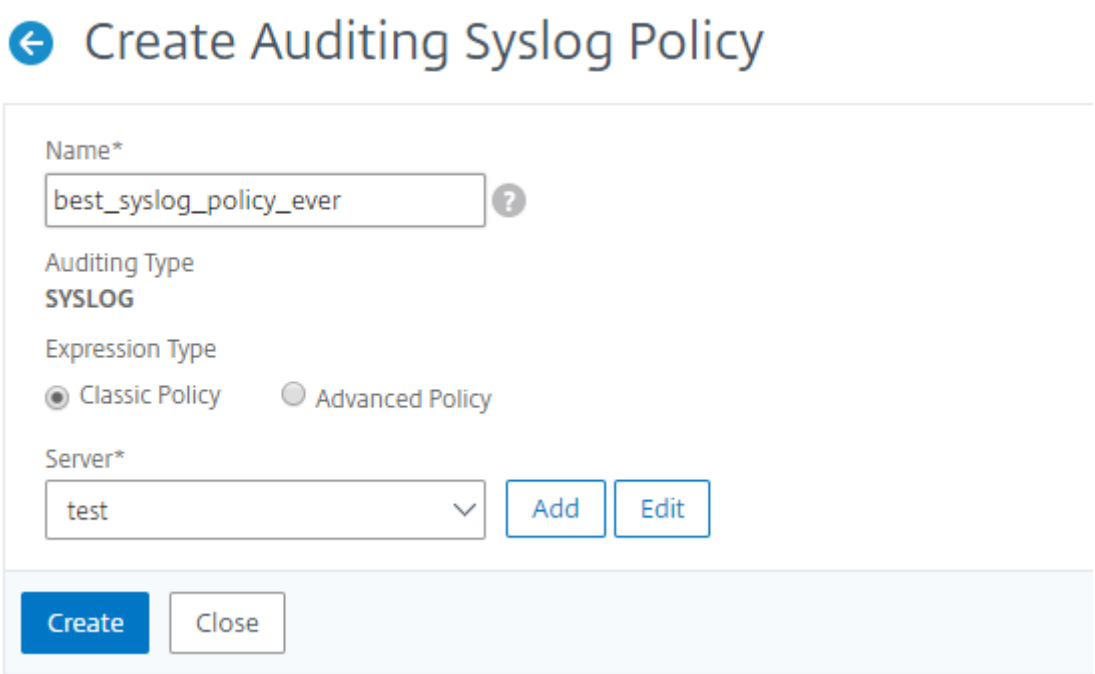
```
unbind audit syslogGlobal <policyName>[-globalBindType <globalBindType>]
```

Configuration de la stratégie de journal d'audit à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Audit** > **Syslog**.



1. Sélectionnez l'onglet **Serveurs** .
2. Cliquez sur **Ajouter**.
3. Dans la page **Créer un serveur d'audit**, renseignez les champs pertinents, puis cliquez sur **Créer**.
4. Pour ajouter la stratégie, sélectionnez l'onglet **Stratégies**, puis cliquez sur **Ajouter**.
5. Dans la page **Créer une stratégie Syslog d'audit**, remplissez les champs pertinents, puis cliquez sur **Créer**.



6. Pour lier la stratégie globalement, sélectionnez **Advanced Policy Global Bindings** dans la liste déroulante. Sélectionnez la stratégie **best_syslog_policy_ever** . Cliquez sur **Sélectionner**.
7. Dans la liste déroulante, sélectionnez le point de liaison **SYSTEM_GLOBAL** et cliquez sur **Liaison**, puis cliquez sur **Terminé**.

Configuration de la journalisation basée sur des stratégies

Vous pouvez configurer la journalisation basée sur des stratégies pour les stratégies de réécriture et de répondeur. Les messages d'audit sont ensuite consignés dans un format défini lorsque la règle d'une stratégie est évaluée à TRUE. Pour configurer la journalisation basée sur des stratégies, vous configurez une action de message d'audit qui utilise des expressions de stratégie avancées pour spécifier le format des messages d'audit. Et associez l'action à une stratégie. La stratégie peut être liée globalement ou à un serveur virtuel d'équilibrage de charge ou de commutation de contenu. Vous pouvez utiliser des actions de message d'audit pour consigner des messages à différents niveaux de journalisation, soit au format Syslog uniquement, soit dans les formats syslog et nslog

Conditions préalables

- L'option Messages de journal configurables par l'utilisateur (UserDefinedAuditLog) est activée lors de la configuration du serveur d'actions d'audit auquel vous souhaitez envoyer les journaux dans un format défini.
- La stratégie d'audit associée est liée au système global.

Configuration d'une action de message d'audit

Vous pouvez configurer des actions de message d'audit pour consigner les messages à différents niveaux de journalisation, soit au format Syslog uniquement, soit dans les formats de journal Syslog et de nouveaux formats de journal NS. Les actions de message d'audit utilisent des expressions pour spécifier le format des messages d'audit.

Pour créer une action de message d'audit à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add audit messageaction <name> <logLevel> <stringBuilderExpr> [-
     logtoNewnslog (YES|NO)]
2 <!--NeedCopy-->
```

```
1 add audit messageaction log-act1 CRITICAL '"Client:"+CLIENT.IP.SRC+"
     accessed "+HTTP.REQ.URL'
2 <!--NeedCopy-->
```

Pour configurer une action de message d'audit à l'aide de l'interface graphique

Accédez à **Système > Audit > Actions de message**, puis créez l'action de message d'audit.

Action de liaison d'un message d'audit à une stratégie

Après avoir créé une action de message d'audit, vous devez la lier à une stratégie de réécriture ou de réponse. Pour plus d'informations sur la liaison des actions de message du journal à une stratégie de réécriture ou de réponse, voir Réécriture ou Répondeur.

Installation et configuration du serveur NSLOG

August 20, 2021

Pendant l'installation, le fichier exécutable du serveur NSLOG (auditserver) est installé avec d'autres fichiers. Le fichier exécutable auditserver inclut des options permettant d'effectuer plusieurs actions sur le serveur NSLOG, y compris l'exécution et l'arrêt du serveur NSLOG. En outre, vous utilisez l'exécutable auditserver pour configurer le serveur NSLOG avec les adresses IP des appliances Citrix ADC à partir desquelles le serveur NSLOG commencera à collecter les journaux. Les paramètres de configuration sont appliqués dans le fichier de configuration du serveur NSLOG (auditlog.conf).

Ensuite, vous démarrez le serveur NSLOG en exécutant l'exécutable auditserver. La configuration du serveur NSLOG est basée sur les paramètres du fichier de configuration. Vous pouvez personnaliser davantage la journalisation sur le système serveur NSLOG en apportant des modifications supplémentaires au fichier de configuration du serveur NSLOG (auditlog.conf).

> **Attention** :
>
> La version du package serveur NSLOG doit être la même que celle du Citrix ADC. Par exemple, si la version de Citrix ADC est 10.1 Build 125.9, le serveur NSLOG doit également être de la même version.

Le tableau suivant répertorie les systèmes d'exploitation sur lesquels le serveur NSLOG est pris en charge.

Système d'exploitation	Configuration logicielle requise	Remarques
Windows	Windows XP Professionnel, Windows Server 2003, Windows 2000/NT, Windows Server 2008, Windows Server 2008 R2	
Linux	RedHat Linux 4 ou version ultérieure, SUSE Linux Enterprise 9.3 ou version ultérieure	

Système d'exploitation	Configuration logicielle requise	Remarques
FreeBSD	FreeBSD 6.3 ou version ultérieure	Pour Citrix ADC 10.5, utilisez uniquement FreeBSD 8.4.
Mac OS	Mac OS 8.6 ou version ultérieure	Non pris en charge sur Citrix ADC 10.1 et versions ultérieures.

Les spécifications matérielles minimales pour la plate-forme exécutant le serveur NSLOG sont les suivantes :

- Processeur - Intel x86 ~ 501 mégahertz (MHz)
- RAM - 512 mégaoctets (Mo)
- Contrôleur - SCSI

Installation du serveur NSLOG sur le système d'exploitation Linux

Connectez-vous au système Linux en tant qu'administrateur. Utilisez la procédure suivante pour installer les fichiers exécutables du serveur NSLOG sur le système.

Pour installer le package serveur NSLOG sur un système d'exploitation Linux

1. À l'invite de commandes Linux, tapez la commande suivante pour copier le fichier NsAuditServer.rpm dans un répertoire temporaire :

   ```
   cp <path_to_cd>/Utilities/auditserver/Linux/NSauditserver.rpm /tmp
   ```

2. Tapez la commande suivante pour installer le fichier NsEditServer.rpm.

   rpm -i nsAuditServer.rpm

   Cette commande extrait les fichiers et les installe dans les répertoires suivants :

   - /usr/local/netscaler/etc
   - /usr/local/netscaler/bin
   - /usr/local/netscaler/samples

Pour désinstaller le package serveur NSLOG sur un système d'exploitation Linux

1. À l'invite de commandes, tapez la commande suivante pour désinstaller la fonctionnalité de journalisation du serveur d'audit :

   ```
   rpm -e NSauditserver
   ```


2. Pour plus d'informations sur le fichier RPM NsAuditServer, utilisez la commande suivante :

   ```
   rpm -qpi \*.rpm
   ```

3. Pour afficher les fichiers du serveur d'audit installé, utilisez la commande suivante :

   ```
   rpm -qpl *.rpm
   ```

   `*.rpm`: spécifie le nom du fichier.

Installation du serveur NSLOG sur le système d'exploitation FreeBSD

Avant de pouvoir installer le serveur NSLOG, vous devez copier le package NSLOG à partir du CD du produit Citrix ADC ou le télécharger depuis www.citrix.com. Le package NSLOG a le format de nom suivant :

`AuditServer_<release number>-<build number>.zip`

Pa exemple : `AuditServer_10.5-58.11.zip`

Ce paquet contient des fichiers pour toutes les plates-formes prises en charge : Linux, Windows et FreeBSD. Sur un système d'exploitation FreeBSD, installez le package NSLOG qui a le format de nom suivant :

`audserver_bsd-<release number>-<build number>.tgz`

Pa exemple : `audserver_bsd-10.5-58.11.tgz`

Pour télécharger le package NSLOG sur www.citrix.com :

1. Dans un navigateur Web, rendez-vous sur www.citrix.com.
2. Dans la barre de menus, cliquez sur **Se connecter**.
3. Entrez vos informations d'identification de connexion, puis cliquez sur **Se connecter**.
4. Dans la barre de menus, cliquez sur **Téléchargements**.
5. **Dans la liste Sélectionner un produit**, sélectionnez **Citrix ADC**.
6. Sur la page **Citrix ADC**, sélectionnez la version pour laquelle vous souhaitez télécharger le package NSLOG (par exemple, version 10.5), puis sélectionnez **Firmware**.
7. Sous **Firmware**, sélectionnez le firmware Citrix ADC correspondant au numéro de version pour lequel vous souhaitez télécharger le package NSLOG.
8. Sur la page qui s'affiche, faites défiler la page vers le bas, sélectionnez **Audit Serveurs**, puis cliquez sur **Télécharger le fichier**en regard du package que vous souhaitez télécharger.

Pour installer le package serveur NSLOG sur un système d'exploitation FreeBSD

1. Sur le système sur lequel vous avez téléchargé le paquet NSLOG`AuditServer_<release number>-<build number>.zip` (par exemple,`AuditServer_9.3-51.5.zip`), extrayez le`FreeBSD NSLOG server package audserver_bsd-<release number>-<build number>.tgz` (par exemple,`audserver_bsd-9.3-51.5.tgz`) de la page paquet.

2. Copiez le package serveur FreeBSD NSLOGaudserver_bsd-<release number>-<build number>.tgz (par exemple,audserver_bsd-9.3-51.5.tgz) dans un répertoire sur un système fonctionnant sous FreeBSD OS.
3. À l'invite de commande du répertoire dans lequel le package serveur FreeBSD NSLOG a été copié, exécutez la commande suivante pour installer le package :

   pkg_add audserver_bsd-<release number>-<build number>.tgz

   Exemple :

   ```
   1 pkg_add audserver_bsd-9.3-51.5.tgz
   2 <!--NeedCopy-->
   ```

   Les répertoires suivants sont extraits :

   - <root directory extracted from the FreeBSD NSLOG server **package** tgz file>Citrix ADCbin (par exemple, /var/auditserver/netscaler/bin)
   - <root directory extracted from the FreeBSD NSLOG server **package** tgz file>netscaler/etc (par exemple, /var/auditserver/netscaler/etc)
   - <root directory extracted from the FreeBSD NSLOG server **package** tgz file>\netscaler\samples (par exemple, /var/auditserver/samples)
4. À l'invite de commandes, tapez la commande suivante pour vérifier que le package est installé :

   pkg_info | grep NSaudserver

Pour désinstaller le package serveur NSLOG sur un système d'exploitation FreeBSD

À l'invite de commandes, entrez la commande suivante :

pkg_delete NSaudserver

Installation des fichiers NSLOG Server sur le système d'exploitation Windows

Avant de pouvoir installer le serveur NSLOG, vous devez copier le package NSLOG à partir du CD du produit Citrix ADC ou le télécharger depuis www.citrix.com. Le package NSLOG a le format de nom suivantAuditServer _<release number>-<build number>.zip (par exemple,AuditServer_9.3-51.5.zip). Ce paquet contient les packages d'installation NSLOG pour toutes les plates-formes prises en charge.

Pour télécharger le package NSLOG sur www.CITRIX.com

1. Dans un navigateur Web, rendez-vous sur www.citrix.com.
2. Dans la barre de menus, cliquez sur Se connecter.

3. Entrez vos informations d'identification de connexion, puis cliquez sur Se connecter.
4. Dans la barre de menus, cliquez sur Téléchargements.
5. Recherchez la page qui fournit le numéro de version et la version appropriés.
6. Sur cette page, sous Serveurs d'audit, cliquez sur Télécharger pour télécharger le package NSLOG, au format `AuditServer_<release number>-<build number>.zip`, sur votre système local (par exemple `AuditServer_9.3-51.5.zip`).

Pour installer le serveur NSLOG sur un système d'exploitation Windows

1. Sur le système, où vous avez téléchargé le paquet NSLOG`AuditServer_<release number>-<build number>.zip` (par exemple,`AuditServer_9.3-51.5.zip`), extraire`audserver_win-<release number>-<build number>.zip` (par exemple,`audserver_win-9.3-51.5.zip`) du paquet.
2. Copiez le fichier extrait`audserver_<release number>-<build number>.zip` (par exemple,`audserver_win-9.3-51.5.zip`) sur un système Windows sur lequel vous souhaitez installer le serveur NSLOG.
3. Décompressez le `audserver_<release number>-<build number>.zip` fichier (par exemple `audserver_win-9.3-51.5.zip`).
4. Les répertoires suivants sont extraits :
   a) `<root directory extracted from the Windows NSLOG server package zip file>\bin`(par exemple, `C:\audserver_win-9.3-51.5\bin`)
   b) `<root directory extracted from the Windows NSLOG server package zip file>\etc` (par exemple,`C:\audserver_win-9.3-51.5\etc`)
   c) `<root directory extracted from the Windows NSLOG server package zip file>\samples` (par exemple, `C:\audserver_win-9.3-51.5\samples`)
5. À l'invite de commandes, exécutez la commande suivante à partir de la`<root directory extracted from the Windows NSLOG server package zip file>\bin path` commande

   ```
   audserver -install -f <directorypath>\auditlog.conf
   ```

   `<directorypath>`: spécifie le chemin d'accès au fichier de configuration (`auditlog.conf`). Par défaut,`log.conf` est sous le`\<root directory extracted from Windows NSLOG server package zip file\>\samples` répertoire. Mais vous pouvez copier auditlog.conf dans le répertoire souhaité.

Pour désinstaller le serveur NSLOG sur un système d'exploitation Windows

À l'invite de commandes, exécutez ce qui suit à partir du`<root directory extracted from Windows NSLOG server package zip file>\bin` chemin d'accès :


```
audserver -remove
```

Options de commande du serveur NSLOG

Pour plus d'informations sur les commandes du serveur NSLOG, consultez Options du serveur d'audit.

Exécutez la commande audserver à partir du répertoire dans lequel l'exécutable du serveur d'audit est présent :

- Sous Windows :`\ns\bin`
- Sous Solaris et Linux :`\usr\local\netscaler\bin`

Les fichiers de configuration du serveur d'audit sont présents dans les répertoires suivants :

- Sous Windows :`\ns\etc`
- Sous Linux :`\usr\local\netscaler\etc`

L'exécutable du serveur d'audit est démarré comme `./auditserver` sous Linux et FreeBSD.

Ajout des adresses IP de l'appliance Citrix ADC sur le serveur NSLOG

Dans le fichier de configuration (
`auditlog.conf`), ajoutez les adresses IP des appliances Citrix ADC dont les événements doivent être consignés.

Pour ajouter les adresses IP de l'appliance Citrix ADC

À l'invite de commandes, tapez la commande suivante :

```
audserver -addns -f <directorypath\>\auditlog.conf
```

`<directorypath>`: spécifie le chemin d'accès au fichier de configuration (auditlog.conf).

Vous êtes invité à entrer les informations relatives aux paramètres suivants :

NSIP : spécifie l'adresse IP de l'appliance Citrix ADC, par exemple 10.102.29.1.

Userid : spécifie le nom d'utilisateur, par exemple nsroot.

Mot de passe : spécifie le mot de passe, par exemple nsroot.

Si vous ajoutez plusieurs adresses IP Citrix ADC (NSIP) et que vous ne souhaitez plus consigner tous les détails de l'événement de l'appliance Citrix ADC, vous pouvez supprimer les NSIP manuellement en supprimant l'instruction NSIP à la fin du fichier auditlog.conf. Pour une configuration haute disponibilité (HA), vous devez ajouter les adresses IP principales et secondaires Citrix ADC à auditlog.conf à l'aide de la commande audserver. Avant d'ajouter l'adresse IP, assurez-vous que le nom d'utilisateur et le mot de passe existent sur le système.

Vérification du fichier de configuration du serveur NSLOG

Vérifiez l'exactitude de la syntaxe dans le fichier de configuration (`audit log.conf`) pour activer la journalisation pour démarrer et fonctionner correctement.

Pour vérifier la configuration, à l'invite de commandes, tapez la commande suivante :

```
audserver -verify -f <directorypath>\auditlog.conf
```

`<directorypath>: Specifies the path to the configuration file (audit log.conf).`

Exécution du serveur NSLOG

January 21, 2021

Pour démarrer la journalisation du serveur d'audit

Tapez la commande suivante à l'invite de commandes :

Audserver -start -f<directorypath>\auditlog.conf

<directorypath>: spécifie le chemin d'accès au fichier de configuration (audit log.conf).

Pour arrêter la journalisation du serveur d'audit qui démarre en arrière-plan dans FreeBSD ou Linux

Exécutez la commande suivante :

```
audserver -stop
```

Pour arrêter la journalisation du serveur d'audit qui démarre en tant que service dans Windows

Exécutez la commande suivante :

```
audserver -stopservice
```

Personnalisation de la journalisation sur le serveur NSLOG

August 20, 2021

Vous pouvez personnaliser la journalisation sur le serveur NSLOG en apportant des modifications supplémentaires au fichier de configuration du serveur NSLOG (log.conf). Utilisez un éditeur de texte pour modifier le fichier de configuration log.conf sur le système serveur.

Pour personnaliser la journalisation, utilisez le fichier de configuration pour définir les filtres et les propriétés du journal.

- **Filtres de journal.** Filtrez les informations du journal à partir d'une appliance Citrix ADC ou d'un ensemble d'appliances Citrix ADC.
- **Propriétés du journal.** Chaque filtre a un ensemble de propriétés de journal associé. Les propriétés du journal définissent le mode de stockage des informations du journal filtrées.

Ce document comprend les détails suivants :

- Création de filtres
- Spécification des propriétés du journal

Création de filtres

Vous pouvez utiliser la définition de filtre par défaut située dans le fichier de configuration (audit log.conf), modifier le filtre ou créer un nouveau filtre. Vous pouvez créer plusieurs filtres de journal.

> Remarque :
> Pour la journalisation consolidée, si une transaction de journal se produit pour laquelle il n'y a pas de définition de filtre, le filtre par défaut est utilisé (s'il est activé). La seule façon de configurer la journalisation consolidée de toutes les appliances Citrix ADC consiste à définir le filtre par défaut.

Pour créer un filtre

À l'invite de commandes, tapez la commande suivante dans le fichier de configuration (auditlog.conf) :

```
filter <filterName> [IP <ip>] [NETMASK <mask>] ON | OFF]
<!--NeedCopy-->
```

FilterName : spécifiez le nom du filtre (maximum de 64 caractères alphanumériques).

ip : Spécifiez les adresses IP.

mask : spécifiez le masque de sous-réseau à utiliser sur un sous-réseau.

Spécifiez ON pour activer le filtre pour consigner les transactions ou désactivez pour désactiver le filtre. Si aucun argument n'est spécifié, le filtre est ON.

Exemples :


```
filter F1 IP 192.168.100.151 ON
<!--NeedCopy-->
```

Pour appliquer le filtre F2 aux adresses IP 192.250.100.1 à 192.250.100.254 :

```
filter F2 IP 192.250.100.0 NETMASK 255.255.255.0 ON
<!--NeedCopy-->
```

FilterName est un paramètre obligatoire si vous définissez un filtre avec d'autres paramètres facultatifs, tels que l'adresse IP, ou la combinaison de l'adresse IP et du masque de réseau.

Spécification des propriétés du journal

Les propriétés du journal associées au filtre sont appliquées à toutes les entrées du journal présentes dans le filtre. La définition de la propriété de journal commence par le mot clé BEGIN et se termine par END, comme illustré dans l'exemple suivant :

```
BEGIN <filtername>
    logFilenameFormat ...
    logDirectory ...
    logInterval ...
    logFileSizeLimit ....
END
<!--NeedCopy-->
```

Les entrées de la définition peuvent inclure les éléments suivants :

- **LogFileNameFormat** spécifie le format de nom de fichier du fichier journal. Le nom du fichier peut être des types suivants :
  - Statique : chaîne constante qui spécifie le chemin absolu et le nom du fichier.
  - Dynamique : expression qui inclut les spécificateurs de format suivants :
    - Date (%{format}t)
    - crée un nom de fichier avec NSIP

  Exemple :

  ```
  LogFileNameFormat Ex%`{
  `%m%d%y }
  t.log
  <!--NeedCopy-->
  ```

  Cela crée le premier nom de fichier sous la forme Exmmddyy.log. Les nouveaux fichiers sont nommés :

Exmmddyy.log.0, Exmmddyy.log.1, etc. Dans l'exemple suivant, les nouveaux fichiers sont créés lorsque la taille du fichier atteint 100 Mo.

Exemple :

```
LogInterval size
LogFileSize 100
LogFileNameFormat Ex%`{
`%m%d%y }
t
<!--NeedCopy-->
```

> **Attention**
>
> Le format de date%t spécifié dans le paramètre LogFileNameFormat remplace la propriété d'intervalle de journal pour ce filtre. Pour empêcher la création d'un nouveau fichier tous les jours plutôt que lorsque la taille du fichier journal spécifiée est atteinte, n'utilisez pas%t dans le paramètre LogFileNameFormat.

- **LogDirectory** spécifie le format du nom de répertoire du fichier journal. Le nom du fichier peut être l'un des suivants :
  - Statique : est une chaîne constante qui spécifie le chemin absolu et le nom du fichier.
  - Dynamique : Expression contenant les spécificateurs de format suivants :
    - Date (%{format}t)
    - crée un répertoire avec NSIP

  Le séparateur de répertoire dépend du système d'exploitation. Sous Windows, utilisez le séparateur de répertoire.

  Exemple :

  ```
  LogDirectory dir1\dir2\dir3
  <!--NeedCopy-->
  ```

  Dans les autres systèmes d'exploitation (Linux, FreeBSD, etc.), utilisez le séparateur de répertoires.

- **LogInterval** spécifie l'intervalle auquel les nouveaux fichiers journaux sont créés. Utilisez l'une des valeurs suivantes :
  - Horaire : Un fichier est créé toutes les heures. Valeur par défaut.
  - Quotidien : Un fichier est créé le jour même à minuit.
  - Hebdomadaire : Un fichier est créé tous les dimanches à minuit.
  - Mensuel : Un fichier est créé le premier jour du mois à minuit.
  - Aucun : un fichier n'est créé qu'une seule fois, lorsque la journalisation du serveur d'audit démarre.

- Taille : Un fichier n'est créé que lorsque la limite de taille du fichier journal est atteinte.

Exemple :

```
LogInterval Hourly
<!--NeedCopy-->
```

- **LogFileSizeLimit** spécifie la taille maximale (en Mo) du fichier journal. Un nouveau fichier est créé lorsque la limite est atteinte.

> **Remarque**
>
> Vous pouvez remplacer la propriété loginterval en affectant la taille comme valeur.

La valeur par défaut LogFileSizeLimit est de 10 Mo.

Exemple :

```
LogFileSizeLimit 35
<!--NeedCopy-->
```

SYSLOG sur TCP

August 20, 2021

Syslog est une norme pour l'envoi de messages de notification d'événement. Ces messages peuvent être stockés localement ou sur un serveur de journaux externe. Syslog permet aux administrateurs réseau de consolider les messages de journal et de tirer des informations à partir des données collectées.

Syslog est initialement conçu pour fonctionner sur UDP, qui peut transmettre une énorme quantité de données dans le même réseau avec une perte de paquets minimale. Cependant, les opérateurs de télécommunications préfèrent transmettre des données syslog par TCP, car ils ont besoin d'une transmission de données fiable et ordonnée entre les réseaux. Par exemple, la compagnie de télécommunication suit les activités de l'utilisateur et TCP assure la retransmission en cas de panne réseau.

Fonctionnement de Syslog sur TCP

Pour comprendre le fonctionnement de syslog sur TCP, considérez deux cas hypothétiques :

Sam, un administrateur réseau, veut consigner les événements importants sur un serveur syslog externe.

XYZ Telecom, un FAI, doit transmettre et stocker une quantité importante de données sur les serveurs syslog pour se conformer aux réglementations gouvernementales.

Dans les deux cas, les messages de journal doivent être transmis sur un canal fiable et stockés en toute sécurité sur un serveur syslog externe. Contrairement à UDP, TCP établit une connexion, transmet des messages en toute sécurité et retransmet (de l'expéditeur au destinataire) toutes les données endommagées ou perdues en raison d'une défaillance du réseau.

L'appliance Citrix ADC envoie des messages de journal via UDP au démon syslog local et envoie des messages de journal via TCP ou UDP aux serveurs syslog externes.

Prise en charge SNIP pour Syslog

Lorsque le module audit-log génère des messages syslog, il utilise une adresse IP Citrix ADC (NSIP) comme adresse source pour envoyer les messages à un serveur syslog externe. Pour configurer un SNIP comme adresse source, vous devez le faire partie de l'option NetProfile et lier NetProfile à l'action syslog.

> **Remarque**
>
> TCP utilise SNIP pour envoyer des sondes de surveillance pour vérifier la connectivité, puis envoie les journaux via NSIP. Par conséquent, le serveur syslog doit être accessible via SNIP. Les profils Net peuvent être utilisés pour rediriger tout le trafic syslog TCP via SNIP entièrement.

L'utilisation d'une adresse SNIP n'est pas prise en charge dans la journalisation interne.

Prise en charge des noms de domaine complets pour le journal d'audit

Auparavant, le module Audit-log était configuré avec l'adresse IP de destination du serveur syslog externe auquel les messages de journal sont envoyés. Désormais, le serveur de journal d'audit utilise un nom de domaine complet (FQDN) au lieu de l'adresse IP de destination. La configuration de FQDN résout le nom de domaine configuré du serveur syslog à l'adresse IP de destination correspondante pour l'envoi des messages de journal à partir du module audit-log. Le serveur de noms doit être correctement configuré pour résoudre le nom de domaine et éviter les problèmes de service basé sur le domaine.

> **Remarque**
>
> Lors de la configuration d'un nom de domaine complet, la configuration du nom de domaine du serveur de la même appliance Citrix ADC dans l'action syslog ou l'action nslog n'est pas prise en charge.

Configuration de Syslog sur TCP à l'aide de l'interface de ligne de commande

Pour configurer une appliance Citrix ADC pour qu'elle envoie des messages syslog via TCP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1     add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
         domainResolveRetry <integer>]) | -lbVserverName<string>))[-
         serverPort <port>] -logLevel <logLevel>[-dateFormat <dateFormat
         >] [-logFacility <logFacility>]   [-tcp ( NONE | ALL )] [-acl (
         ENABLED | DISABLED )][-timeZone ( GMT_TIME | LOCAL_TIME )][-
         userDefinedAuditlog ( YES | NO )][-appflowExport ( ENABLED |
         DISABLED )] [-lsn ( ENABLED | DISABLED )][-alg ( ENABLED |
         DISABLED )] [-subscriberLog ( ENABLED | DISABLED )][-transport (
          TCP | UDP )] [-tcpProfileName <string>][-maxLogDataSizeToHold <
         positive_integer>][-dns ( ENABLED | DISABLED )] [-netProfile <
         string>]
2 <!--NeedCopy-->
```

```
1     add audit syslogaction audit-action1 10.102.1.1 -loglevel
         INFORMATIONAL -dateformat MMDDYYYY -transport TCP
2 <!--NeedCopy-->
```

Ajout d'une adresse IP SNIP à l'option de profil net à l'aide de l'interface de ligne de commande

Pour ajouter une adresse IP SNIP au profil net à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1     add netProfile <name> [-td <positive_integer>] [-srcIP <string>][-
         srcippersistency ( ENABLED | DISABLED )][-overrideLsn ( ENABLED
         | DISABLED )]add syslogaction <name> <serverIP>  - loglevel all
          - netprofile net1
2 <!--NeedCopy-->
```

```
1     add netprofile net1  - srcip 10.102.147.204`
2 <!--NeedCopy-->
```

Où, srCiP est le SNIP.

Ajout d'un profil net dans une action syslog à l'aide de l'interface de ligne de commande

Pour ajouter une option NetProfile dans une action syslog à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1      add audit syslogaction <name> (<serverIP> | -lbVserverName <string
          >)  -logLevel <logLevel>
```



```
    -netProfile <string>  ...

<!--NeedCopy-->
```

```
    add syslogaction sys_act1 10.102.147.36 -loglevel all -netprofile
        net1
<!--NeedCopy-->
```

Où, -netprofile spécifie le nom du profil réseau configuré. L'adresse SNIP est configurée dans le cadre de NetProfile et cette option NetProfile est liée à l'action syslog.

> **Remarque**
>
> Vous devez toujours lier l'option NetProfile aux services SYSLOGUDP ou SYSLOGTCP liés au serveur virtuel d'équilibrage de charge SYSLOGUDP ou SYSLOGTCP, lorsqu'un nom de serveur virtuel LB est configuré en action syslog.

Configuration de la prise en charge de FQDN à l'aide de l'interface de ligne de commande

Pour ajouter un nom de domaine de serveur à une action Syslog à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
    domainResolveRetry <integer>]) | -lbVserverName <string>)) -logLevel
     <logLevel> ...
    set audit syslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>]-
       serverDomainName <string>] [-lbVserverName <string>]-
       domainResolveRetry <integer>] [-domainResolveNow]
<!--NeedCopy-->
```

Pour ajouter un nom de domaine de serveur à une action Nslog à l'aide de l'interface de ligne de commande.

À l'invite de commandes, tapez :

```
    add audit nslogAction <name> (<serverIP> | (<serverDomainName>[-
       domainResolveRetry <integer>]))  -logLevel <logLevel> ...
    set audit nslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>][-
       serverDomainName <string>] [-domainResolveRetry <integer>][-
       domainResolveNow]
<!--NeedCopy-->
```


Où NomServerDomainName. Nom de domaine du serveur de journaux. Est mutuellement exclusif avec ServerIP/ LBVServerName.

Entier DomainResolveRetry. Temps (en secondes) pendant lequel l'appliance Citrix ADC attend, après l'échec d'une résolution DNS, avant d'envoyer la requête DNS suivante pour résoudre le nom de domaine.

DomainResolveNow. Inclus si la requête DNS doit être envoyée immédiatement pour résoudre le nom de domaine du serveur.

Configuration de Syslog sur TCP à l'aide de l'interface graphique

Pour configurer l'appliance Citrix ADC pour qu'elle envoie des messages Syslog via TCP à l'aide de l'interface graphique

1. Accédez à **Système** > **Audit** > **Syslog** et sélectionnez l'onglet **Serveurs** .
2. Cliquez sur **Ajouter** et sélectionnez Type de transport comme **TCP** .

Configuration d'un profil net pour la prise en charge de SNIP à l'aide de l'interface graphique

Pour configurer le profil réseau pour la prise en charge de SNIP à l'aide de l'interface graphique

1. Accédez à **Système > Audit > Syslog** et sélectionnez l'onglet **Serveurs**.
2. Cliquez sur **Ajouter** et sélectionnez un profil réseau dans la liste.

Configuration du nom de domaine complet à l'aide de l'interface graphique

Pour configurer le nom de domaine complet à l'aide de l'interface graphique

1. Accédez à **Système** > **Audit** > **Syslog** et sélectionnez l'onglet **Serveurs** .
2. Cliquez sur **Ajouter** et sélectionnez un type de serveur et un nom de domaine de serveur dans la liste.

Serveurs SYSLOG d'équilibrage de charge

August 20, 2021

L'appliance Citrix ADC envoie ses événements et messages SYSLOG à tous les serveurs de journaux externes configurés. Cela entraîne le stockage des messages redondants et rend la surveillance difficile pour les administrateurs système. Pour résoudre ce problème, l'appliance Citrix ADC propose des algorithmes d'équilibrage de charge qui peuvent équilibrer la charge des messages SYSLOG parmi

les serveurs de journaux externes pour une meilleure maintenance et des performances. Les algorithmes d'équilibrage de charge pris en charge incluent RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets et AuditlogHash.

Équilibrage de charge des serveurs SYSLOG à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

1. Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

   ```
   add service <name>(<IP> | <serverName>)<serviceType (SYSLOGTCP |
   SYSLOGUDP)> <port>
   ```

2. Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGUDP, et la méthode d'équilibrage de charge AUDITLOGHASH.

   ```
   add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
   <AUDITLOGHASH>]
   ```

3. Liez le service au serveur virtuel d'équilibrage de charge.

   ```
   Bind lb vserver <name> <serviceName>
   ```

4. Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge qui a SYSLOGTCP ou SYSLOGUDP comme type de service.

   ```
   add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
    <logLevel>]
   ```

5. Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

   ```
   add syslogpolicy <name> <rule> <action>
   ```

6. Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.

   ```
   bind system global <policyName>
   ```

Équilibrage de charge des serveurs SYSLOG à l'aide de l'interface graphique

1. Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

   Accédez à **Gestion du trafic** > **Services**, cliquez sur **Ajouter** et sélectionnez **SYLOGTCP** ou **SYSLOGUDP** comme protocole.

2. Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGTCP, et la méthode d'équilibrage de charge AUDITLOGHASH.

   Accédez à **Gestion du trafic** > **Serveurs virtuels**, cliquez sur **Ajouter** et sélectionnez **SYLOGTCP** ou **SYSLOGUDP** comme protocole.

3. Liez le service au serveur virtuel d'équilibrage de charge au service.

   Liez le service au serveur virtuel d'équilibrage de charge.

Accédez à **Gestion du trafic** > **Serveurs virtuels**, sélectionnez un serveur virtuel, puis sélectionnez **AUDITLOGHASH** dans la **méthode d'équilibrage de la charge.**

4. Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge qui a SYSLOGTCP ou SYSLOGUDP comme type de service.

   Accédez à **Système** > **Audit**, cliquez sur **Serveurs** et ajoutez un serveur en sélectionnant l'option **Serveur LB** dans **Serveurs**.

5. Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

   Accédez à **Système** > **Syslog**, cliquez sur **Stratégies** et ajoutez une stratégie SYSLOG.

6. Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.

   Accédez à **Système** > **Syslog**, sélectionnez une stratégie SYSLOG et cliquez sur **Action**, puis cliquez sur **Liaisons globales** et liez la stratégie à système global.

Exemple :

La configuration suivante spécifie l'équilibre de charge des messages SYSLOG entre les serveurs de journaux externes en utilisant la méthode AUDITLOGHASH comme méthode d'équilibrage de charge. La charge de la méthode AUDITLOGHASH équilibre le trafic en fonction de la valeur de hachage en entrée des agents d'audit. Les agents sont les modules qui génèrent auditlog dans une appliance Citrix ADC. Par exemple, si un agent LSN souhaite équilibrer la charge auditlogs en fonction de l'adresse IP du client, le module LSN génère la valeur de hachage basée sur ClientIp et transmet la valeur de hachage au module auditlog. Le module auditlog envoie les messages auditlog qui ont la même valeur de hachage au serveur syslog externe.

L'appliance Citrix ADC génère des événements et des messages SYSLOG équilibrés entre les services, service1, service2 et service 3.

```
add service service1 192.0.2.10 SYSLOGUDP 514
add service service2 192.0.2.11 SYSLOGUDP 514
add service service3 192.0.2.11 SYSLOGUDP 514
add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH
bind lb vserver lbvserver1 service1
bind lb vserver lbvserver1 service2
bind lb vserver lbvserver1 service3
add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All
add syslogpolicy syspol1 ns_true sysaction1
bind system global syspol1
<!--NeedCopy-->
```

Limitations :

- L'appliance Citrix ADC ne prend pas en charge un serveur virtuel d'équilibrage de charge externe équilibrant la charge du serveur virtuel équilibrant les messages SYSLOG entre les serveurs de

journaux.

Paramètres par défaut pour les propriétés du journal

August 20, 2021

Voici un exemple de filtre par défaut avec les paramètres par défaut pour les propriétés du journal :

```
begin default
 logInterval Hourly
 logFileSizeLimit 10
 logFilenameFormat  auditlog%`{
 `%y%m%d }
 t.log
 end default
<!--NeedCopy-->
```

Voici deux exemples de définition des filtres par défaut :

Exemple 1 :

```
Filter f1 IP 192.168.10.1
<!--NeedCopy-->
```

Cela crée un fichier journal pour NSI 192.168.10.1 avec les valeurs par défaut de l'effet journal.

Exemple 2 :

```
Filter f1 IP 192.168.10.1
begin f1
    logFilenameFormat logfiles.log
end f1
<!--NeedCopy-->
```

Cela crée un fichier journal pour NSIP 192.168.10.1. Étant donné que le format du nom du fichier journal est spécifié, les valeurs par défaut des autres propriétés du journal sont en vigueur.

Exemple de fichier de configuration (audit.conf)

August 20, 2021

Voici un exemple de fichier de configuration :


```
##############################
# This is the Auditserver configuration file
# Only the default filter is active
# Remove leading # to activate other filters
##############################
MYIP <NSAuditserverIP>
MYPORT 3023
#   Filter filter_nsip  IP <Specify the Citrix ADC IP address to filter
    on > ON
#   begin filter_nsip
#       logInterval         Hourly
#       logFileSizeLimit    10
#       logDirectory         logdir\%A\
#       logFilenameFormat   nsip%\\{
 \\%d%m%Y }
 t.log
#   end filter_nsip
Filter default
begin default
    logInterval      Hourly
    logFileSizeLimit    10
    logFilenameFormat   auditlog%\{
 \%y%m%d }
 t.log
end default
<!--NeedCopy-->
```

Journalisation du serveur Web

January 21, 2021

Vous pouvez utiliser la fonctionnalité de journalisation du serveur Web pour envoyer des journaux de requêtes HTTP et HTTPS à un système client pour le stockage et la récupération. Cette fonction comporte deux composants :

- Serveur de journaux Web, qui s'exécute sur Citrix ADC.
- Client Citrix ADC Web Logging (NSWL), qui s'exécute sur le système client.

Lorsque vous exécutez le client Citrix ADC Web Logging (NSWL) :

1. Il se connecte au Citrix ADC.
2. Citrix ADC met en mémoire tampon les entrées de journal des requêtes HTTP et HTTPS avant de les envoyer au client.

3. Le client peut filtrer les entrées avant de les stocker.

Pour configurer la journalisation du serveur Web, vous activez d'abord la fonctionnalité de journalisation Web sur le Citrix ADC et configurez la taille de la mémoire tampon pour le stockage temporaire des entrées de journal. Ensuite, vous installez NSWL sur le système client. Vous ajoutez ensuite l'adresse IP Citrix ADC (NSIP) au fichier de configuration NSWL. Vous êtes maintenant prêt à démarrer le client NSWL pour commencer la journalisation. Vous pouvez personnaliser la journalisation du serveur Web en apportant des modifications supplémentaires au fichier de configuration NSWL (log.conf).

Configuration de Citrix ADC pour la journalisation du serveur Web

August 20, 2021

Pour configurer Citrix ADC pour la journalisation du serveur Web, vous devez uniquement activer la fonctionnalité de journalisation du serveur Web. Vous pouvez éventuellement effectuer les configurations suivantes :

- Modifiez la taille du tampon (la taille par défaut est de 16 Mo) qui stocke les informations enregistrées avant qu'elles ne soient envoyées au client Citrix ADC Web Logging (NSWL).
- Spécifiez les en-têtes HTTP personnalisés que vous souhaitez exporter vers le client NSWL. Vous pouvez configurer au maximum deux noms d'en-tête de requête HTTP et deux requêtes HTTP.

Pour configurer la journalisation du serveur Web à l'aide de l'interface de ligne de commande

À l'invite de commandes, effectuez les opérations suivantes :

- Activez la fonctionnalité de journalisation du serveur Web.

  ```
  enable ns feature WL
  ```

- [Facultatif] Modifiez la taille du tampon pour stocker les informations journalisées.

  ```
  set ns weblogparam -bufferSizeMB <size>
  ```

  > **Remarque** :
  >
  > Pour activer votre modification, vous devez désactiver, puis réactiver la fonctionnalité de journalisation du serveur Web.

- [Facultatif] Spécifiez les noms d'en-tête HTTP personnalisés que vous souhaitez exporter.

  ```
  set ns weblogparam [-customReqHdrs <string> ...] [-customRspHdrs <
  string> ...]
  ```



```
    > enable ns feature WL
    Done
    > set ns weblogparam -bufferSizeMB 60
    Done
    > show ns weblogparam
        Web Logging parameters:
        Log buffer size:  60MB
        Custom HTTP request headers: (none)
        Custom HTTP response headers: (none)
    Done
    > set ns weblogparam -customReqHdrs req1 req2 -customRspHdrs res1
       res2
    Done
    > show ns weblogparam
        Web Logging parameters:
        Log buffer size:  60MB
        Custom HTTP request headers: req1, req2
        Custom HTTP response headers: res1, res2
    Done
<!--NeedCopy-->
```

Pour configurer la journalisation du serveur Web à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres** et effectuez les opérations suivantes :
    a) Pour activer la fonctionnalité de journalisation du serveur Web, cliquez sur **Modifier les fonctionnalités avancées** et sélectionnez **Journalisation Web** .
    b) Pour modifier la taille de la mémoire tampon, cliquez sur **Modifier les paramètres système globaux** et, sous **Journalisation Web**, entrez la taille de la mémoire tampon.
    c) Pour spécifier les en-têtes HTTP personnalisés à exporter, cliquez sur **Modifier les paramètres système globaux** et, sous **Journalisation Web**, spécifiez les valeurs d'en-tête.

Installation du client de journalisation Web (NSWL) Citrix ADC

October 4, 2021

Lorsque vous installez NSWL, le fichier exécutable client (NSWL) est installé avec d'autres fichiers. Le fichier exécutable NSWL fournit une liste d'options que vous pouvez utiliser. Pour plus de détails, reportez-vous à la section Configuration du client NSWL.

> **Attention**
>
> La version du client NSWL doit être la même que Citrix ADC. Par exemple, si la version de Citrix ADC est 10.1 Build 125.9, le client NSWL doit également être de la même version. En outre, le client de journalisation Web (NSWL) fonctionne sur les machines serveur 32 bits et 64 bits. La page de téléchargement n'a qu'un client weblog 32 bits. Le client de blog 64 bits est disponible sur demande et vous recommande de contacter le support Citrix pour plus d'informations.

Le tableau suivant répertorie les systèmes d'exploitation sur lesquels le client NSWL peut être installé.

Système d'exploitation	Version	Configuration matérielle requise	Remarques
Windows	Windows Server 2016 ou ultérieur	Processeur - processeur x86/amd64 (1 GHz ou supérieur), RAM - 4 Go (ou supérieur)	
MacOS	MacOS 8.6 ou ultérieur	Non pris en charge sur Citrix ADC 10.1 et versions ultérieures.	
Linux	Ubuntu, SUSE Linux, CentOS, Red Hat Enterprise Linux publié en 2016 ou plus tard	Processeur - processeur x86/amd64 (1 GHz ou supérieur), RAM - 4 Go (ou supérieur)	
Solaris	Solaris Sun OS 5.6 ou ultérieur	Processeur - UltraSparc-III 400 MHz, RAM - 512 Mo, contrôleur - SCSI	Non pris en charge sur Citrix ADC 10.5 et versions ultérieures.
FreeBSD	FreeBSD 6.3 ou ultérieur	Processeur - processeur x86/amd64 (1 GHz ou supérieur), RAM - 4 Go (ou supérieur)	Pour Citrix ADC 10.5, utilisez uniquement FreeBSD 8.4.
AIX	AIX 6.1	-	Non pris en charge sur Citrix ADC 10.5 et versions ultérieures.

Si le système client NSWL ne peut pas traiter la transaction de journal en raison d'une limitation de

l'UC, la mémoire tampon du journal Web dépasse et le processus de journalisation réinitialise.

> **Attention**
>
> La réinitialisation de la journalisation peut entraîner la perte de transactions de journal.

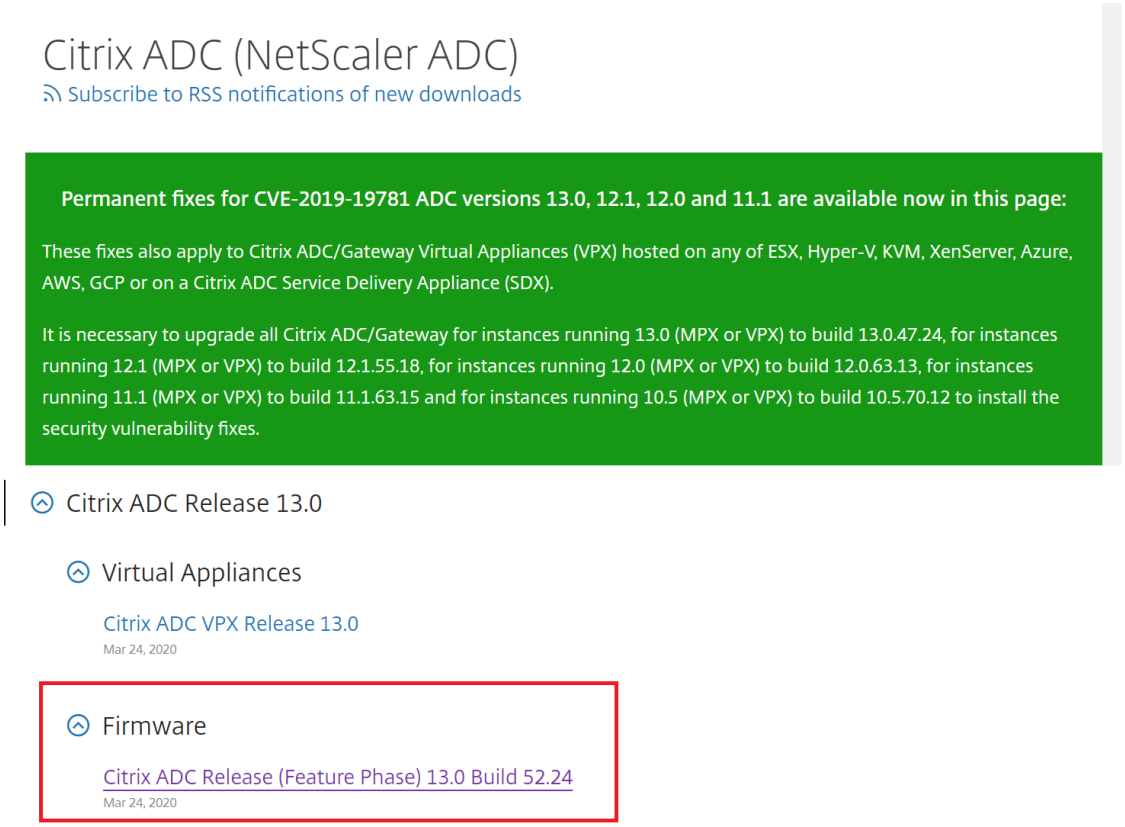
Pour résoudre temporairement un goulot d'étranglement du système client NSWL causé par une limitation du processeur, vous pouvez régler la taille de la mémoire tampon de journalisation du serveur Web sur l'appliance Citrix ADC. Pour résoudre le problème, vous avez besoin d'un système client capable de gérer le débit du site.

Télécharger le client NSWL

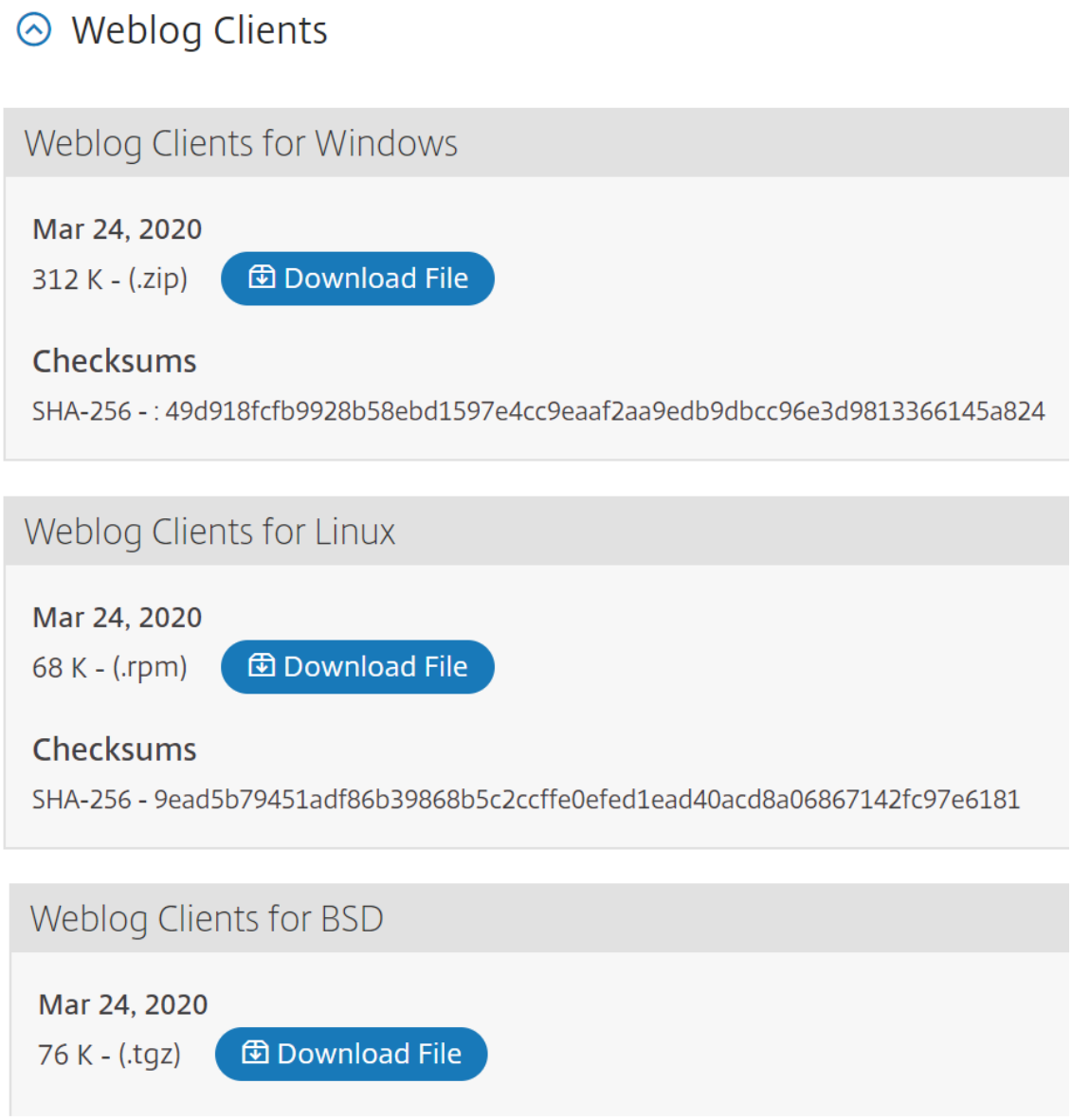
Vous pouvez obtenir le package client NSWL à partir du CD du produit Citrix ADC ou du site de téléchargement Citrix. Dans le package, il y a des packages d'installation distincts pour chaque plate-forme prise en charge.

Pour télécharger le client NSWL à partir du site Web Citrix

1. Connectez-vous à Citrix en accédant à l'URL `https://www.citrix.com/downloads/citrix-adc/`.
2. Accédez à une version spécifique de Citrix ADC et recherchez son firmware.
3. Cliquez sur **Firmware** (par exemple, Citrix ADC Release (Feature Phase) 13.0 Build 52.24).



4. Dans la page **Création Citrix ADC Release (Feature Phase)**, accédez à la section **Clients Weblog**.
5. La section vous permet de télécharger des clients Weblog pour Windows, Linux et BSD.



Installer le client NSWL sur Solaris

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. nswl_solaris-<release number>-<build number>.tar file“ Extraire le du paquet.
2. Copiez le fichier extrait sur un système Solaris sur lequel vous souhaitez installer le client NSWL.
3. Extrayez les fichiers du fichier tar avec la commande suivante :

   ```
   tar xvf nswl_solaris-9.3-51.5.tar
   ```


Un répertoire Weblog est créé dans le répertoire temporaire et les fichiers sont extraits dans le répertoire Weblog.

- Installez le package avec la commande suivante :

  ```
  pkgadd -d
  ```

- La liste des paquets disponibles s'affiche. Dans l'exemple suivant, un package Weblog est affiché :

  ```
  1 NSweblog Citrix ADC Weblogging (SunOS,sparc)7.0
  ```

Vous êtes invité à sélectionner les packages. Sélectionnez le numéro de package du blog à installer.

Après avoir sélectionné le numéro de package et appuyé sur **Entrée**, les fichiers sont extraits et installés dans les répertoires suivants :

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Pour vérifier si le package NSWL est installé, exécutez la commande suivante :

   ```
   pkginfo | grep NSweblog
   ```

2. Pour désinstaller le package NSWL, exécutez la commande suivante :

   ```
   pkgrm NSweblog
   ```

Installer le client NSWL sur Linux

> **Important**
>
> L'installation d'un client NSWL sur Linux remplace le fichier de configuration. Vous devez effectuer une sauvegarde avant de l'installer.

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. Extrayez le fichier `nswl_linux-<release number>-<build number>.rpm` du package.
2. Copiez le fichier extrait sur un système, exécutant Linux OS, sur lequel vous souhaitez installer le client NSWL.
3. Pour installer le package NSWL, exécutez la commande suivante :

   ```
   rpm -i nswl_linux-9.3-51.5.rpm
   ```

Cette commande extrait les fichiers et les installe dans les répertoires suivants.

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin

- /usr/local/netscaler/samples

1. Pour désinstaller le package NSWL, exécutez la commande suivante :

   ```
   rpm -e NSweblog
   ```

2. Pour obtenir plus d'informations sur le fichier RPM Weblog, exécutez la commande suivante :

   ```
   rpm -qpi *.rpm
   ```

3. Pour afficher les fichiers de journalisation du serveur Web installés, exécutez la commande suivante :

   ```
   rpm -qpl *.rpm
   ```

Installer le client NSWL sur FreeBSD

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. Extrayez le fichier `nswl_bsd-<release number>-<build number>.tgz` du package.
2. Copiez le fichier extrait sur un système, exécutant le système d'exploitation FreeBSD, sur lequel vous souhaitez installer le client NSWL.
3. Pour installer le package NSWL, exécutez la commande suivante :

   ```
   pkg_add nswl_bsd-9.3-51.5.tgz
   ```

Cette commande extrait les fichiers et les installe dans les répertoires suivants.

```
1 -  /usr/local/netscaler/etc
2 -  /usr/local/netscaler/bin
3 -  /usr/local/netscaler/samples
```

1. Pour désinstaller le package NSWL, exécutez la commande suivante :

   ```
   pkg_delete NSweblog
   ```

2. Pour vérifier que le package est installé, exécutez la commande suivante :

   ```
   pkg_info | grep NSweblog
   ```

Installer le client NSWL sur Mac

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. Extrayez le fichier `nswl_macos-<release number>-<build number>.tgz` du package.

2. Copiez le fichier extrait sur un système exécutant macOS, sur lequel vous souhaitez installer le client NSWL.
3. Pour installer le package NSWL, exécutez la commande suivante :

   ```
   pkg_add nswl_macos-9.3-51.5.tgz
   ```

Cette commande extrait les fichiers et les installe dans les répertoires suivants :

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/échantillons

1. Pour désinstaller le package NSWL, exécutez la commande suivante :

   ```
   pkg_delete NSweblog
   ```

2. Pour vérifier que le package est installé, exécutez la commande suivante :

   ```
   pkg_info | grep NSweblog
   ```

Installer le client NSWL sous Windows

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. Extrayez le fichier `nswl_win-<release number>-<build number>.zip` du package.
2. Copiez le fichier extrait sur un système Windows sur lequel vous souhaitez installer le client NSWL.
3. Sur le système Windows, décompressez le fichier dans un répertoire (appelé`<NSWL-HOME>`). Les répertoires suivants sont extraits : `/bin`, `/etc` et `/samples`.
4. À l'invite de commandes, exécutez la commande suivante à partir de la`<NSWL-HOME>\bin directory`:commande

   ```
   nswl -install -f <directorypath>\log.conf
   ```

Où,

Le chemin d'accès au répertoire fait référence au chemin du fichier de configuration (log.conf). Par défaut, le fichier se trouve dans le `/etc` répertoire `<NSWL-HOME>` et. Vous pouvez copier le fichier de configuration dans n'importe quel autre répertoire.

> **Remarque**
>
> Pour désinstaller le client NSWL, à l'invite de commandes, exécutez la commande suivante à partir du `<NSWL-HOME>\bin directory`:

```
1 > nswl -remove
```


Installer le client NSWL sur le système AIX

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. Extrayez le fichier `nswl_aix-<release number>-<build number>.rpm` du package.
2. Copiez le fichier extrait sur un système, exécutant AIX OS, sur lequel vous souhaitez installer le client NSWL.
3. Pour installer le package NSWL, exécutez la commande suivante :

   ```
   rpm -i nswl_aix-9.3-51.5.rpm
   ```

Cette commande extrait les fichiers et les installe dans les répertoires suivants.

- `/usr/local/netscaler/etc`
- `/usr/local/netscaler/`
- `usr/local/netscaler/samples`

1. Pour désinstaller le package NSWL, exécutez la commande suivante :

   ```
   rpm -e NSweblog
   ```

2. Pour obtenir plus d'informations sur le fichier RPM Weblog, exécutez la commande suivante :

   ```
   rpm -qpi *.rpm
   ```

3. Pour afficher les fichiers de journalisation du serveur Web installés, exécutez la commande suivante :

   ```
   rpm -qpl *.rpm
   ```

Configurer le client NSWL

August 20, 2021

Après avoir installé le client NSWL, vous pouvez configurer le client NSWL à l'aide de l'exécutable nswl. Ces configurations sont stockées dans le fichier de configuration du client NSWL (log.conf).

> **Remarque :**
>
> Vous pouvez personnaliser davantage la journalisation sur le client NSWL en apportant des modifications supplémentaires au fichier de configuration NSWL (log.conf). Pour plus de détails, voir Personnalisation de la journalisation sur le système client NSWL.

Le tableau suivant décrit les commandes que vous pouvez utiliser pour configurer le client NSWL.

Commande NSWL	Spécifie
nswl -help	Les options d'aide de la NSWL disponibles.
nswl -addns -f<path-to-configuration-file>	Système qui rassemble les données de transaction du journal. Vous êtes invité à entrer l'adresse IP de l'appliance Citrix ADC. Entrez un nom d'utilisateur et un mot de passe valides.
nswl -verify -f<path-to-configuration-file>	Recherchez les erreurs de syntaxe ou sémantique dans le fichier de configuration.
nswl -start -f<path-to-configuration-file>	Démarrez le client NSWL en fonction des paramètres du fichier de configuration. Remarque : Pour Solaris et Linux : pour démarrer la journalisation du serveur Web en arrière-plan, tapez le signe d'esperluette (&) à la fin de la commande.
nswl -stop (Solaris et Linux uniquement)	Arrêtez le client NSWL s'il a été démarré en arrière-plan ; sinon, utilisez CTRL+C pour arrêter la journalisation du serveur Web.
nswl -install -f<path-to-configuration-file> (Windows uniquement)	Installez le client NSWL en tant que service dans Windows.
nswl -startservice (Windows uniquement)	Démarrez le client NSWL en utilisant les paramètres du fichier de configuration spécifié dans l'option d'installation nswl. Vous pouvez également démarrer le client NSWL à partir de Démarrer > Panneau de configuration > Services. Remarque : Les fichiers journaux NSWL seront créés dans C:\Windows\SysWOW64.
nswl -stopservice (Windows uniquement)	Arrête le client NSWL.
nswl -remove	Supprimez le service client NSWL du Registre.

Exécutez les commandes suivantes à partir du répertoire dans lequel se trouve l'exécutable NSWL :

- Windows: \ns\bin
- Solaris and Linux: \usr\local\netscaler\bin

Les fichiers de configuration de journalisation du serveur Web se trouvent dans le chemin d'accès au répertoire suivant :

- `Windows: \ns\etc`
- `Solaris and Linux: \usr\local\netscaler\etc`

L'exécutable NSWL est démarré en tant que. nswl sous Linux et Solaris.

Ajouter les adresses IP de l'appliance Citrix ADC

Dans le fichier de configuration du client NSWL (log.conf), ajoutez l'adresse IP Citrix ADC (NSIP) à partir de laquelle le client NSWL commencera à collecter les journaux.

Pour ajouter l'adresse NSIP de l'appliance Citrix ADC

1. À l'invite de commandes du système client, tapez :

   ```
   nswl -addns -f < directorypath > \log.conf
   < directorypath >: Specifies the path to the configuration file (log.
   conf).
   ```

2. À l'invite suivante, entrez les informations suivantes :

   - **NSIP** : spécifiez l'adresse IP de l'appliance Citrix ADC.
   - Nom d'utilisateur et mot de passe : spécifiez les informations d'identification utilisateur nsroot de l'appliance Citrix ADC.

> **Remarque** :
>
> Si vous ajoutez plusieurs adresses IP Citrix ADC (NSIP) et que vous ne souhaitez plus consigner tous les détails du journal système Citrix ADC, vous pouvez supprimer manuellement les NSIP en supprimant l'instruction NSIP à la fin du fichier log.conf. Lors d'une installation de basculement, vous devez ajouter les adresses IP principales et secondaires Citrix ADC au log.conf à l'aide de la commande. Avant d'ajouter l'adresse IP, assurez-vous que le nom d'utilisateur et le mot de passe existent sur les appliances Citrix ADC.

Vérifiez le fichier de configuration NSWL

Pour vous assurer que la journalisation fonctionne correctement, vérifiez le fichier de configuration NSWL (log.conf) sur le système client pour les erreurs de syntaxe.

Pour vérifier la configuration dans le fichier de configuration NSWL

À l'invite de commandes du système client, tapez :

```
nswl -verify -f <directorypath>\log.conf
```

< directorypath>: spécifie le chemin d'accès au fichier de configuration (log.conf).

Exécuter le client NSWL

Démarrer la journalisation du serveur Web

À l'invite de commandes du système client, tapez :

```
nswl -start -f <directorypath>\log.conf
```

<directorypath>: spécifie le chemin d'accès au fichier de configuration (log.conf).

Arrêter la journalisation du serveur Web démarrée en tant que processus d'arrière-plan sur les systèmes d'exploitation Solaris ou Linux

À l'invite de commandes, tapez :

```
nswl -stop
```

Pour arrêter la journalisation du serveur Web démarrée en tant que service sur le système d'exploitation Windows

À l'invite de commandes, tapez :

```
nswl -stopservice
```

Personnaliser la connexion sur le système client NSWL

August 20, 2021

Vous pouvez personnaliser la journalisation sur le système client Citrix ADC Web Logging (NSWL) en apportant davantage de modifications au fichier de configuration du client NSWL (log.conf). Utilisez un éditeur de texte pour modifier le fichier de configuration log.conf sur le système client.

Pour personnaliser la journalisation, utilisez le fichier de configuration pour définir les filtres et les propriétés du journal.

- **Filtres de journal.** Filtrez les informations du journal en fonction de l'adresse IP de l'hôte, du nom de domaine et du nom d'hôte des serveurs Web.
- **Propriétés du journal.** Chaque filtre a un ensemble de propriétés de journal associé. Les propriétés du journal définissent le mode de stockage des informations du journal filtrées.

Exemple de fichier de configuration

Voici un exemple de fichier de configuration :

```
1 ##########
2 # This is the NSWL configuration file
3 # Only the default filter is active
```



```
# Remove leading # to activate other filters
##########
##########
# Default filter (default on)
# W3C Format logging, new file is created every hour or on reaching 10 MB file size,
# and the file name is Exyymmdd.log
##########
Filter default
begin default
        logFormat               W3C
        logInterval             Hourly
        logFileSizeLimit        10
        logFilenameFormat       Ex%`{
 `%y%m%d }
 t.log
end default
##########
# Citrix ADC caches example
# CACHE_F filter covers all the transaction with HOST name www.netscaler.com and the listed server ip's
##########
#Filter CACHE_F HOST www.netscaler.com IP 192.168.100.89 192.168.100.95 192.168.100.52 192.168.100.53 ON
##########
# netscaler origin server example
# Not interested in Origin server to Cache traffic transaction logging
##########
#Filter ORIGIN_SERVERS IP 192.168.100.64 192.168.100.65 192.168.100.66 192.168.100.67 192.168.100.225 192.168.100.226 192.168.100.227 192.168.100.228 OFF
##########
# netscaler image server example
# all the image server logging.
##########
#Filter IMAGE_SERVER HOST www.netscaler.images.com IP 192.168.100.71 192.168.100.72 192.168.100.169 192.168.100.170 192.168.100.171 ON
##########
# NCSA Format logging, new file is created every day midnight or on reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log.
# Exclude objects that ends with .png .jpg .jar.
##########
```



```
#begin ORIGIN_SERVERS
#       logFormat               NCSA
#       logInterval             Daily
#       logFileSizeLimit        40
#       logFilenameFormat       /datadisk5/ORGIN/log/%v/NS%`{
 `%m%d%y }
 t.log
#       logExclude              .png .jpg .jar
#end ORIGIN_SERVERS

##########
# NCSA Format logging, new file is created every day midnight or on
    reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.
    log with log record timestamp as GMT.
##########
#begin CACHE_F
#       logFormat               NCSA
#       logInterval             Daily
#       logFileSizeLimit        20
#       logFilenameFormat /datadisk5/netscaler/log/%v/NS%`{
 `%m%d%y }
 t.log
#       logtime                 GMT
#end CACHE_F

##########
# W3C Format logging, new file on reaching 20MB and the log file path
    name is
# atadisk6/netscaler/log/server's ip/Exmmyydd.log with log record
    timestamp as LOCAL.
##########
#begin IMAGE_SERVER
#       logFormat               W3C
#       logInterval             Size
#       logFileSizeLimit        20
#       logFilenameFormat /datadisk6/netscaler/log/%AEx%`{
 `%m%d%y }
 t
#       logtime                 LOCAL
#end IMAGE_SERVER

##########
# Virtual Host by Name firm, can filter out the logging based on the
    host name by,
```



```
##########

#Filter VHOST_F IP 10.101.2.151 NETMASK 255.255.255.0
#begin VHOST_F
#       logFormat               W3C
#       logInterval             Daily
#       logFileSizeLimit        10
logFilenameFormat /ns/prod/vhost/%v/Ex%`{
 `%m%d%y }
 t
#end VHOST_F

########## END FILTER CONFIGURATION ##########
<!--NeedCopy-->
```

Création de filtres

Vous pouvez utiliser la définition de filtre par défaut dans le fichier de configuration (log.conf), ou modifier le filtre ou créer un filtre. Vous pouvez créer plusieurs filtres de journal.

> **Remarque**
>
> La journalisation consolidée, qui enregistre les transactions pour lesquelles aucun filtre n'est défini, utilise le filtre par défaut s'il est activé. La journalisation consolidée de tous les serveurs peut être effectuée en définissant uniquement le filtre par défaut.

Si le serveur héberge plusieurs sites Web et que chaque site Web possède son propre nom de domaine et que chaque domaine est associé à un serveur virtuel, vous pouvez configurer la journalisation du serveur Web pour créer un répertoire de journaux distinct pour chaque site Web. Le tableau suivant affiche les paramètres de création d'un filtre.

Paramètre	Spécifie
Nom du filtre	Nom du filtre. Le nom du filtre peut inclure des caractères alphanumériques et ne peut pas dépasser 59 caractères. Les noms de filtre de plus de 59 caractères sont tronqués à 59 caractères.
Nom d'hôte	Nom d'hôte du serveur pour lequel les transactions sont enregistrées.

Paramètre	Spécifie
IP `ip`	Adresse IP du serveur pour lequel les transactions doivent être consignées (par exemple, si le serveur a plusieurs domaines qui ont une adresse IP).
IP `ip 2...ip n` :	Plusieurs adresses IP (par exemple, si le domaine du serveur a plusieurs adresses IP).
IP IP6	Adresse IPv6 du serveur pour lequel les transactions doivent être consignées.
Masque NETMASK IP IP	Adresses IP et combinaison de masque de réseau à utiliser sur un sous-réseau.
`ON | OFF`	Activez ou désactivez le filtre pour enregistrer les transactions. Si aucun argument n'est sélectionné, le filtre est activé (ON).

Tableau 1. Paramètres de création d'un filtre

Pour créer un filtre

Pour créer un filtre, entrez la commande suivante dans le fichier log.conf :

- `filter <filterName> <HOST name> | [IP<ip> ] | [IP<ip 2...ip n> ] | <IP ip NETMASK mask> [ON | OFF]`
- `filter <filterName> <HOST name> | [IP6 ip/<prefix length>] [ON | OFF]`

Pour créer un filtre pour un serveur virtuel

Pour créer un filtre pour un serveur virtuel, entrez la commande suivante dans le fichier log.conf :

```
filter <filterName> <VirtualServer IP address>
```

Exemple

Dans l'exemple suivant, vous spécifiez une adresse IP 192.168.100.0 et un masque de réseau 255.255.255.0. Le filtre s'applique aux adresses IP 192.168.100.1 à 192.168.100.254.

```
1 Filter F1 HOST www.netscaler.com ON
2 Filter F2 HOST www.netscaler.com IP 192.168.100.151 ON
3 Filter F3 HOST www.netscaler.com IP 192.168.100.151 192.165.100.152 ON
4 Filter F4 IP 192.168.100.151
```



```
Filter F5 IP 192.168.100.151 HOST www.netscaler.com OFF
Filter F6 HOST www.netscaler.com HOST www.xyz.com HOST www.abcxyz.com
   IP 192.168.100.200 ON
Filter F7 IP 192.250.100.0 NETMASK 255.255.255.0
Filter F8 HOST www.xyz.com IP 192.250.100.0 NETMASK 255.255.255.0 OFF
For creating filters for servers having IPv6 addresses.
Filter F9 2002::8/112 ON
Filter F10 HOST www.abcd.com IP6 2002::8 ON

<!--NeedCopy-->
```

Spécification des propriétés du journal

Les propriétés du journal sont appliquées à toutes les entrées du journal associées au filtre. La définition de la propriété de journal commence par le mot-clé BEGIN et se termine par END, comme illustré dans l'exemple suivant :

```
BEGIN <filtername>
 logFormat ...
 logFilenameFormat ...
 logInterval ...
 logFileSize ....
 logExclude ....
 logTime ….
 END
<!--NeedCopy-->
```

Les entrées de la définition peuvent inclure les éléments suivants :

- **LogFormat** spécifie la fonctionnalité de journalisation du serveur Web qui prend en charge les formats de fichiers journaux NCSA, W3C Extended et personnalisés.

  Par défaut, la `logformat` propriété est w3c. Pour remplacer, entrez personnalisé ou NCSA dans le fichier de configuration, par exemple :

```
     LogFormat NCSA
<!--NeedCopy-->
```

> **Remarque**
>
> Pour le format NCSA et les formats de journaux personnalisés, l'heure locale est utilisée pour les transactions d'horodatage et pour la rotation des fichiers.

- **LogInterval** spécifie les intervalles auxquels les nouveaux fichiers journaux sont créés. Utilisez l'une des valeurs suivantes :

- Horaire : Un fichier est créé toutes les heures.
- Quotidien : Un fichier est créé tous les jours à minuit. Valeur par défaut.
- Hebdomadaire : Un fichier est créé tous les dimanches à minuit.
- Mensuel : Un fichier est créé le premier jour du mois à minuit.
- Aucun : Un fichier n'est créé qu'une seule fois, lorsque la journalisation du serveur Web démarre.

Exemple :

```
LogInterval Daily
<!--NeedCopy-->
```

LogFileSizeLimit spécifie la taille maximale du fichier journal en Mo. Il peut être utilisé avec n'importe quel intervalle de log (hebdomadaire, mensuel, etc.) Un fichier est créé lorsque la limite de taille maximale du fichier est atteinte ou lorsque l'intervalle de journalisation défini s'écoule.

Pour remplacer ce comportement, spécifiez la taille en tant que `loginterval` propriété afin qu'un fichier soit créé uniquement lorsque la limite de taille du fichier journal est atteinte.

La valeur par défaut LogFileSizeLimit est de 10 Mo.

Exemple :

```
LogFileSizeLimit 35
<!--NeedCopy-->
```

- **LogFileNameFormat** spécifie le format de nom de fichier du fichier journal. Le nom du fichier peut être des types suivants :
  - Statique : spécifie une chaîne constante qui contient le chemin absolu et le nom du fichier.

    Dynamique : spécifie une expression contenant le format suivant :

    * Adresse IP du serveur
    * Date (%{format}t)
    * Suffixe d'URL (%x)
    * Nom d'hôte (%v)

Exemple :

```
LogFileNameFormat Ex%`{
 `%m%d%y }
 t.log
<!--NeedCopy-->
```

Cette commande crée le premier nom de fichier Exmmddyy.log, puis chaque heure crée un fichier avec un nom de fichier : Exmmddyy.log.0, Exmmddyy.Log.1,…, Exmmddyy.log.N.

Exemple :

```
      LogInterval size
      LogFileSize 100
      LogFileNameFormat Ex%`{
 `%m%d%y }
 t
<!--NeedCopy-->
```

> **Attention**
>
> Le format de date%t spécifié dans la commande LogFileNameFormat remplace la propriété d'intervalle de journalisation de ce filtre. Pour empêcher la création d'un nouveau fichier tous les jours plutôt que lorsque la taille du fichier journal spécifiée est atteinte, n'utilisez pas%t dans LogFileNameFormat.

- **LogExclude** empêche la journalisation des transactions avec les extensions de noms de fichiers spécifiées.

Exemple :

```
      LogExclude .html
<!--NeedCopy-->
```

Cette commande crée un fichier journal qui exclut les transactions de journal pour les fichiers*.html.

LogTime spécifie l'heure du journal en tant que GMT ou LOCAL.

Les valeurs par défaut sont :

- Format de fichier journal NCSA : LOCAL
- Format du fichier journal W3C : GMT.

Présentation des formats de journaux NCSA et W3C

Citrix ADC prend en charge les formats de fichier journal standard suivants :

- Format journal commun de la NCSA
- Format de journal étendu W3C

Format journal commun de la NCSA

Si le format de fichier journal est NCSA, le fichier journal affiche les informations de journal dans le format suivant :

```
Client_IP_address -User_Name [Date:Time -TimeZone] "Method Object
    HTTP_version" HTTP_StatusCode BytesSent
```



```
<!--NeedCopy-->
```

Pour utiliser le format journal commun NCSA, entrez NCSA dans l'argument LogFormat dans le fichier log.conf.

Le tableau suivant décrit le format de journal commun de la NCSA.

Argument	Spécifie
Client_IP_Adresse_client	Adresse IP de l'ordinateur client.
Nom d'utilisateur	Nom d'utilisateur.
Date	Date de la transaction.
Durée	Heure à laquelle la transaction a été terminée.
Fuseau horaire	Le fuseau horaire (heure moyenne de Greenwich ou heure locale).
Méthode	La méthode de requête (par exemple ; GET, POST).
Objet	L'URL.
HTTP_version	Version de HTTP utilisée par le client.
Code HTTP_status	Code d'état de la réponse.
Octets envoyés	Nombre d'octets envoyés à partir du serveur.

Format de journal étendu W3C

Un fichier journal étendu contient une séquence de lignes contenant des caractères ASCII terminées par un saut de ligne (LF) ou la séquence Carriage Return Line Feed (CRLF). Les générateurs de fichiers journaux doivent suivre la convention de terminaison de ligne de la plate-forme sur laquelle ils sont exécutés.

Les analyseurs de log doivent accepter le formulaire LF ou CRLF. Chaque ligne peut contenir une directive ou une entrée. Si vous souhaitez utiliser le format de journal étendu W3C, entrez W3C comme argument Log Format dans le fichier log.conf.

Par défaut, le format de journal standard W3C est défini en interne comme le format de journal personnalisé, illustré comme suit :

```
%`{
 `%Y-%m-%d%H:%M:%S }
 t %a %u %S %A %p %m %U %q %s %j %J %T %H %+{
 user-agent }
```



```
 i %+{
 cookie }
  i%+{
 referer }
 i
<!--NeedCopy-->
```

Vous pouvez également modifier l'ordre ou supprimer certains champs dans ce format de journal W3C. Par exemple :

```
logFormat W3C %`{
 `%Y-%m-%d%H:%M:%S }
 t %m %U
<!--NeedCopy-->
```

Les entrées du journal W3C sont créées avec le format suivant :

```
#Version: 1.0 #Fields: date time cs-method cs-uri #Date: 12-Jun-2001
   12:34 2001-06-12 12:34:23 GET /sports/football.html 2001-06-12
   12:34:30 GET /sports/football.html
<!--NeedCopy-->
```

Entrées

Les entrées consistent en une séquence de champs relatifs à une seule transaction HTTP. Les champs sont séparés par des espaces blancs. Citrix recommande l'utilisation de caractères de tabulation. Si un champ d'une entrée particulière n'est pas utilisé, un tiret (-) marque le champ omis.

Directives

Consultez le tableau Directives pour plus d'informations sur le processus de journalisation. Les lignes commençant par le signe dièse (#) contiennent des directives.

Exemple :

L'exemple de fichier journal suivant montre les entrées de journal au format de journal étendu W3C :

```
#Version: 1.0 #Fields: time cs-method cs-uri #Date: 12-Jan-1996
   00:00:00 00:34:23 GET /sports/football.html 12:21:16 GET /sports/
   football.html 12:45:52 GET /sports/football.html 12:57:34 GET /
   sports/football.html
<!--NeedCopy-->
```


Champs

La directive Fields répertorie une séquence d'identificateurs de champ qui spécifient les informations enregistrées dans chaque entrée. Les identificateurs de champs peuvent comporter l'une des formes suivantes :

- **identificateur :** se rapporte à l'ensemble de la transaction.
- **prefix-identifier :** concerne le transfert d'informations entre les parties définies par le préfixe de valeur.
- **prefix (header) :** Spécifie la valeur de l'en-tête de champ d'en-tête HTTP pour le transfert entre les parties définies par le préfixe de valeur. Les champs spécifiés de cette manière ont toujours le type.

Le tableau suivant décrit les préfixes définis.

Prefix	Spécifie
c	Client
s	Serveur
r	Distant
cs	Client vers serveur
CS	Serveur vers client
Sr	Serveur vers serveur distant (préfixe utilisé par les proxy)
rs	Serveur distant à serveur (préfixe utilisé par les proxy)
x	Identificateur spécifique à l'application

Exemples :

Les exemples suivants sont des identificateurs définis qui utilisent des préfixes :

cs-method : La méthode dans la requête envoyée par le client au serveur.

sc (Referer) : Le `Referer` champ de la réponse.

c-ip : L'adresse IP du client.

Identificateurs

Le tableau suivant décrit les identificateurs de format journal étendu W3C qui ne nécessitent pas de préfixe.

Identificateur	Description
date	Date à laquelle la transaction a été effectuée.
temps	Heure à laquelle la transaction est effectuée.
prise de temps	Temps pris (en secondes) pour la fin de la transaction.
octets	Nombre d'octets transférés.
mis en cache	Enregistre si un accès au cache s'est produit. Un zéro indique une absence de cache.

Tableau 5. Identificateurs de format de journal étendu W3C (aucun préfixe requis)

Le tableau suivant décrit les identificateurs de format journal étendu W3C qui nécessitent un préfixe.

Identificateur	Description
Adresse IP	L'adresse IP et le numéro de port.
DNS	Nom DNS.
état	Code d'état.
comment	Le commentaire est retourné avec un code d'état.
method	La méthode.
url	L'URL.
url-stem	La partie de la tige de l'URL.
url-query	Partie requête de l'URL.

Tableau 6. Identificateurs de format de journal étendu W3C (nécessite un préfixe)

Le format de fichier journal étendu W3C vous permet de choisir des champs de journal. Ces champs sont présentés dans le tableau suivant.

Champ	Description
Date	Date à laquelle la transaction est effectuée.
Durée	Heure à laquelle la transaction est effectuée.
IP du client	Adresse IP du client.

Champ	Description
Nom d'utilisateur	Nom d'utilisateur.
Nom du service	Le nom du service, qui est toujours HTTP.
IP du serveur	Adresse IP du serveur.
Port du serveur	Numéro de port du serveur
Méthode	La méthode de requête (par exemple ; GET, POST).
Potence Url	La tige d'URL.
Requête d'URL	Partie requête de l'URL.
Statut HTTP	Code d'état de la réponse.
Octets envoyés	Nombre d'octets envoyés au serveur (taille de la requête, y compris les en-têtes HTTP).
Octets reçus	Nombre d'octets reçus du serveur (taille de réponse, y compris les en-têtes HTTP).
Temps pris	Le temps nécessaire à la réalisation d'une transaction, en secondes.
Version du protocole	Numéro de version de HTTP utilisé par le client.
Agent utilisateur	Champ User-Agent dans le protocole HTTP.
Cookie	Le champ Cookie du protocole HTTP.
`Referer`	`Referer` Champ du protocole HTTP.

Tableau 7. Format de fichier journal étendu W3C (autorise les champs de journal)

Création d'un format de journal personnalisé

Vous pouvez personnaliser le format d'affichage des données du fichier journal manuellement ou à l'aide de la bibliothèque NSWL. En utilisant le format de journal personnalisé, vous pouvez dériver la plupart des formats de journal actuellement pris en charge par Apache.

Création d'un format de journal personnalisé à l'aide de la bibliothèque NSWL

Utilisez l'une des bibliothèques NSWL suivantes selon que l'exécutable NSWL a été installé sur un ordinateur hôte Windows ou Solaris :

- **Windows :** bibliothèque nswl.lib dans le répertoire \ ns \ bin de l'ordinateur hôte du gestionnaire de système.
- **Solaris :** bibliothèque libnswl.a dans /usr/local/netscaler/bin.

Pour créer le format de journal personnalisé à l'aide de la bibliothèque NSWL

1. Ajoutez les deux fonctions C suivantes définies par le système dans un fichier source C :

   NS_UserDefffieldName () : Cette fonction renvoie la chaîne qui doit être ajoutée en tant que nom de champ personnalisé dans l'enregistrement du journal.

   NS_UserDffieldVal () : Cette fonction implémente la valeur de champ personnalisée, puis la renvoie sous forme de chaîne qui doit être ajoutée à la fin de l'enregistrement de journal.

2. Compilez le fichier dans un fichier objet.
3. Liez le fichier objet avec la bibliothèque NSWL (et éventuellement avec des bibliothèques tierces) pour former un nouvel exécutable NSWL.
4. Ajoutez une chaîne %d à la fin de la chaîne LogFormat dans le fichier de configuration (log.conf).

Exemple :

```
########## # A new file is created every midnight or on reaching 20MB
   file size, # and the file name is /datadisk5/netscaler/log/NS<
   hostname>/Nsmmddyy.log and create digital #signature field for each
   record. BEGIN CACHE_F logFormat custom "%a - "%{
 user-agent }
 i" [%d/%B/%Y %T -%g] "%x" %s %b%{
 referrer }
 i "%{
 user-agent }
 i" "%{
 cookie }
 i" %d " logInterval Daily logFileSizeLimit 20 logFilenameFormat /
    datadisk5/netscaler/log/%v/NS%`{
 `%m%d%y }
 t.log END CACHE_F
<!--NeedCopy-->
```

Création manuelle d'un format de journal personnalisé

Pour personnaliser le format dans lequel les données du fichier journal doivent apparaître, spécifiez une chaîne de caractères comme argument de la définition de la propriété LogFormat log. Voici un exemple où des chaînes de caractères sont utilisées pour créer un format de journal :


```
LogFormat Custom ""%a - "%{
 user-agent }
 i" %[%d/%m/%Y]t %U %s %b %T"
<!--NeedCopy-->
```

- La chaîne peut contenir les caractères de contrôle de type « c » \ n et \ t pour représenter de nouvelles lignes et onglets.
- Utilisez la touche Echap avec des guillemets littéraux et des barres obliques inverses.

Les caractéristiques de la demande sont consignées en plaçant les directions% dans la chaîne de format, qui sont remplacées dans le fichier journal par les valeurs.

Si le spécificateur de format%v (nom d'hôte) ou%x (suffixe d'URL) est présent dans une chaîne de format de nom de fichier journal, les caractères suivants du nom de fichier sont remplacés par un symbole de trait de soulignement dans le nom du fichier de configuration du journal :

```
" *. /: < > ? \
```

Les caractères dont les valeurs ASCII se situent entre 0 et 31 sont remplacés par ce qui suit :

%<ASCII value of character in hexadecimal>.

Par exemple, le caractère avec la valeur ASCII 22 est remplacé par%16.

> **Attention**
>
> Si le spécificateur de format%v est présent dans une chaîne de format de nom de fichier journal, un fichier distinct est ouvert pour chaque hôte virtuel. Pour garantir une journalisation continue, le nombre maximal de fichiers qu'un processus peut ouvrir doit être suffisamment volumineux. Consultez la documentation de votre système d'exploitation pour obtenir une procédure permettant de modifier le nombre de fichiers pouvant être ouverts.

Création de formats de journal Apache

Vous pouvez dériver à partir des journaux personnalisés la plupart des formats de journaux qu'Apache prend actuellement en charge. Les formats de journal personnalisés qui correspondent aux formats de journal Apache sont les suivants :

NCSA/combiné : LogFormat personnalisé%h%l%u [%t] « %r » %S%B « % {referer} i » « % {user-agent} i »

NCSA/Common: LogFormat custom %h %l %u [%t] "%r" %s %B

Referer Journal : LogFormat personnalisé « % {referer} i » ->%U

Agent utilisateur : LogFormat custom% {user-agent} i

De même, vous pouvez dériver les autres formats de journal du serveur à partir des formats personnalisés.

Arguments de définition d'un format de journal personnalisé

Consultez le tableau PDF Format de journal personnalisé pour plus d'informations sur la définition d'un format de journal personnalisé.

> **Remarque**
>
> Pour obtenir des instructions sur la façon d'exporter des en-têtes HTTP personnalisés, reportez-vous à Configuration de Citrix ADC for Web Server Logging.

Par exemple, si vous définissez le format du journal en%+ {user-agent} i, et si la valeur de l'agent utilisateur est Citrix ADC System Web Client, les informations sont enregistrées en tant que Citrix ADC System+Web+Client. Une alternative consiste à utiliser des guillemets doubles. Par exemple, « % {user-agent} i » le consigne comme « Citrix ADC system Web Client ». « N'utilisez pas la touche <Esc> sur les chaînes de %.. .r, %. . .i et, %. . .o. Il est conforme aux exigences du format de journal commun. Les clients peuvent insérer des caractères de contrôle dans le journal. Par conséquent, vous devez faire attention lorsque vous travaillez avec des fichiers journaux bruts.

Définition du format temporel

Consultez le tableau de définition du format temporel pour en savoir plus sur la partie format de la chaîne % {format} t décrite dans le tableau Format de journal personnalisé. Les valeurs entre crochets ([ ]) indiquent la plage de valeurs qui s'affichent. Par exemple, [1,31] dans la description de%d du tableau suivant affiche de%d va de 1 à 31.

> **Remarque**
>
> Si vous spécifiez une conversion qui ne correspond à aucune des conversions décrites dans le tableau précédent ou à l'une des spécifications de conversion modifiées répertoriées dans le paragraphe suivant, le comportement est indéfini et renvoie 0.

La différence entre%U et%W (ainsi que entre les conversions modifiées%OU et%OW) est le jour considéré comme le premier jour de la semaine. La semaine numéro 1 est la première semaine de janvier (commençant par un dimanche pour%U ou un lundi pour%W). La semaine numéro 0 contient les jours précédant le premier dimanche ou lundi de janvier pour%U et%W.

Affichage des journaux du serveur

Vous pouvez configurer une fonctionnalité NSWL pour afficher les journaux du serveur sur la console ou rediriger les journaux du serveur vers un répertoire de l'appliance Citrix ADC.

Il existe deux façons d'afficher les journaux sur la console (sortie standard) :
Option 1 : Afficher tous les journaux sur la console.
Option 2 : Afficher uniquement les journaux sélectionnés sur la console avec des filtres avec `logfilenameformat` comme STDOUT.

Call Home

August 20, 2021

Les appliances peuvent parfois ne pas fonctionner correctement en raison de problèmes logiciels ou matériels. Dans de tels cas, Citrix doit collecter des données et effectuer la résolution des problèmes avant qu'un impact potentiel ne se produise sur le site du client. En activant Call Home sur votre appliance Citrix ADC, vous pouvez automatiser le processus de notification d'erreur. Non seulement vous évitez d'appeler le support Citrix, de lancer une demande de service et de télécharger des données système avant que l'équipe de support ne puisse résoudre le problème, mais le support peut identifier et résoudre un problème avant qu'il ne se produise. Call Home surveille périodiquement l'appliance et télécharge automatiquement les données sur le serveur de support technique Citrix. En outre, les données Call Home entrantes fournissent des informations sur l'utilisation de Citrix ADC. Plusieurs équipes au sein de Citrix peuvent utiliser ces données pour améliorer la conception, la prise en charge et la mise en œuvre de Citrix ADC.

Par défaut, Call Home est activé sur toutes les plates-formes et toutes les saveurs de Citrix ADC (MPX, VPX, SDX). En activant cette fonctionnalité, vous autorisez Citrix à collecter des données de déploiement et de télémétrie Citrix ADC pour une meilleure implémentation et un service de support.

> **Remarque**
>
> Vous pouvez également consulter la page FAQ Call Home pour obtenir des informations relatives à Call Home.

Avantages

Call Home offre les avantages suivants.

- Surveillez les conditions d'erreur matérielle et logicielle. Pour plus d'informations, consultez la section Surveillance des conditions d'erreur critiques.
- Notifiez les événements critiques qui ont un impact sur votre réseau.
- Envoyer les données de performances et les détails d'utilisation du système à Citrix à l'adresse suivante :
  - Analysez et améliorez la qualité des produits.
  - Fournissez des informations de dépannage en temps réel pour une identification proactive des problèmes et une résolution plus rapide des problèmes.

Prise en charge de la plateforme

La fonctionnalité Call Home est prise en charge sur toutes les plates-formes Citrix ADC et tous les modèles d'appliance (MPX, VPX et SDX).

- Citrix ADC MPX : Tous les modèles MPX.
- Citrix ADC VPX : tous les modèles VPX, y compris les appliances VPX qui obtiennent leur licence à partir de pools de licences externes ou centraux.
- Citrix ADC SDX : surveille le lecteur de disque et les puces SSL affectées pour détecter toute erreur ou défaillance. Toutefois, les instances VPX n'ont pas accès à l'unité d'alimentation (PSU) et leur état n'est donc pas surveillé. Dans une plate-forme SDX, vous pouvez configurer Call Home directement sur une instance individuelle ou via la SVM.

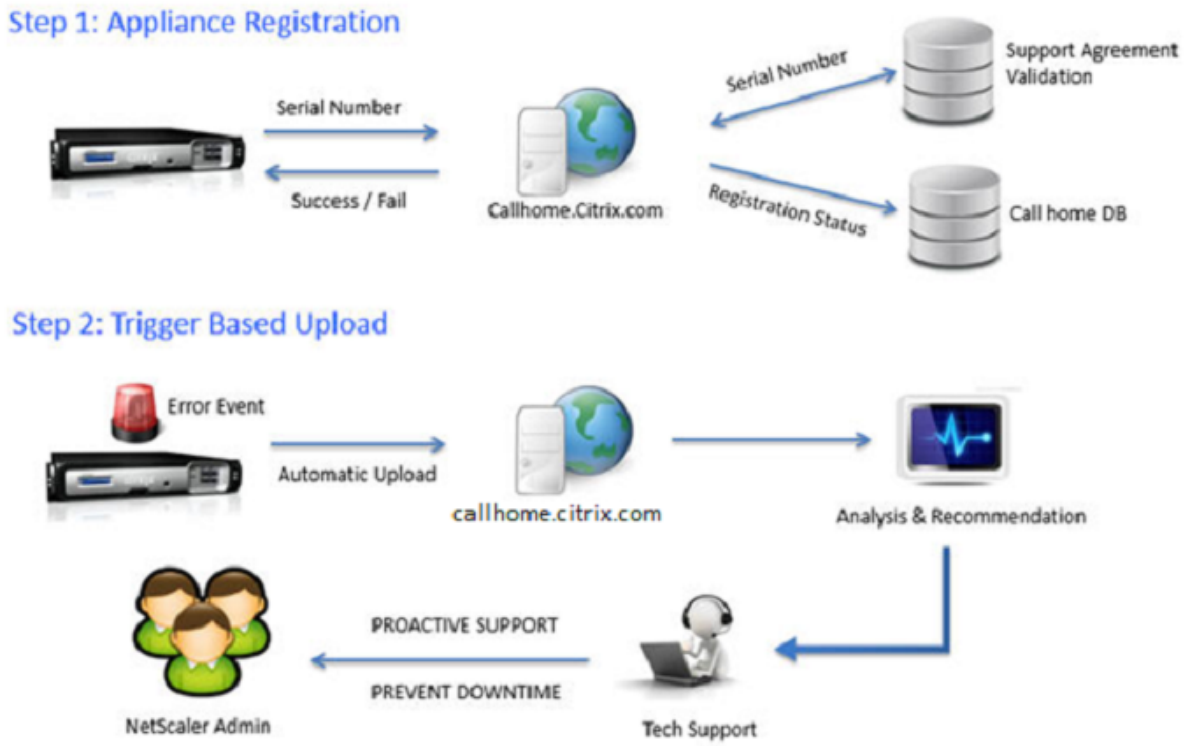
Conditions préalables

Pour utiliser Call Home, l'appliance Citrix ADC doit avoir les éléments suivants :

- **Connexion Internet.** Call Home nécessite une connexion Internet pour que Citrix ADC se connecte au serveur de support Citrix pour le téléchargement d'une archive de données.

Comment fonctionne Call Home

La figure suivante illustre un flux de travail de base de Call Home dans une appliance Citrix ADC déployée sur un site client.



Voici le flux de travail d'un Call Home :

1. Configurez la connectivité Internet. Pour que Call Home puisse télécharger des données système, votre appliance doit disposer d'une connectivité Internet. Si ce n'est pas le cas, vous pouvez configurer une configuration de serveur proxy pour fournir une connectivité Internet. Pour plus d'informations, consultez la section Configuration de l'Call Home.

2. Activez Call Home. Lors de la mise à niveau de votre appliance vers le dernier logiciel via l'interface de commande Citrix ADC ou l'interface graphique, Call Home est activé par défaut et le système retarde le processus d'enregistrement de 24 heures. Pendant cette période, vous pouvez choisir de désactiver manuellement la fonctionnalité, mais Citrix vous recommande de l'activer.

> **Remarque**
>
> Si vous mettez à niveau votre appliance à partir d'une version plus ancienne sur laquelle Call Home est explicitement désactivée, le système active la fonctionnalité par défaut et affiche un message de notification lors de votre première connexion.

En outre, si vous effectuez des modifications de configuration pour une connectivité Internet, vous devez désactiver et activer Call Home. Il permet à Call Home de s'enregistrer auprès du serveur Citrix Insight Services (CIS) sans erreur de défaillance.

3. Enregistrez l'appliance Citrix ADC sur le serveur de support Citrix. Lorsque Call Home enregistre l'appliance auprès du serveur Citrix Support, le serveur vérifie la validité du numéro de série de l'appliance dans la base de données. Si le numéro de série est valide, le serveur enregistre l'appliance

pour le service Call Home et envoie une réponse d'enregistrement réussie. Sinon, le serveur renvoie un message d'échec d'enregistrement. Les informations système de base sont envoyées sous la forme d'un message séparé. Les données incluent les détails de l'utilisation de la mémoire et du processeur ainsi que les numéros de débit. Les données sont envoyées périodiquement dans le cadre du message de pulsation tous les 7 jours, par défaut. Cependant, une valeur inférieure à 5 jours n'est pas recommandée, car les téléchargements fréquents ne sont pas utiles.

4. Surveiller les conditions d'erreur critiques. Une fois inscrit, Call Home commence à surveiller l'appliance. Le tableau suivant répertorie les conditions que peut surveiller l'Call Home sur l'appliance.

Condition d'erreur critique	Description	Intervalle de surveillance des appels à domicile	Nom d'alarme SNMP correspondant
Erreurs de lecteur flash compact	Le lecteur flash compact de l'appliance a rencontré des échecs de lecture ou d'écriture.	24 heures	COMPACT-FLASH-ERRORS
Erreurs de disque dur	Les disques durs de l'appliance ont rencontré des échecs de lecture ou d'écriture.	24 heures	HARD-DISK-DRIVE-ERRORS
Défaillance de l'unité d'alimentation	L'une des unités d'alimentation de l'appliance Citrix ADC a échoué.	7 secondes	POWER-SUPPLY-FAILURE
Échec de la carte SSL	L'une des cartes SSL de l'appliance Citrix ADC a échoué.	7 secondes	SSL-CARD-FAILED
Redémarrage à chaud	L'appareil a été redémarré à chaud en raison d'une défaillance d'un processus système.	Après chaque redémarrage de l'appliance Citrix ADC.	WARM-RESTART-EVENT

Condition d'erreur critique	Description	Intervalle de surveillance des appels à domicile	Nom d'alarme SNMP correspondant
Erreur d'anomalie de mémoire	L'utilisation de la mémoire augmente progressivement au-dessus de sa limite normale et dépasse le seuil.	1 jour	Aucune alarme SNMP
Limite de débit de paquets	Les limites de débit ou de paquets par seconde (pps) sont atteintes.	7 secondes	PF-RL-PPS-PKTS-DROPPED, PF-RL-RATE-PKTS-DROPPED

5. Chargez les données Call Home. Si l'une des conditions critiques précédentes est identifiée sur l'appliance, la fonctionnalité Call Home avertit automatiquement le support Citrix. Les archives de support sont téléchargées sur le serveur de support Citrix. En outre, vous pouvez configurer l'alarme SNMP CALLHOME-UPLOAD-EVENT pour générer une alerte SNMP chaque fois que le téléchargement de Call Home se produit. L'alerte SNMP avertit l'administrateur local de l'événement critique.

> **Remarque**
>
> Call Home crée le fichier tar Call Home et le télécharge sur le serveur de support technique Citrix uniquement pour la première occurrence d'une condition d'erreur particulière depuis le dernier redémarrage. Si vous souhaitez que l'appliance envoie des alertes chaque fois qu'une condition d'erreur particulière se produit, configurez l'alarme SNMP correspondante pour la condition d'erreur.

6. Créer une demande de service. Call Home crée automatiquement une demande de service pour tous les événements liés au matériel critique. Les événements sont classés comme : panne d'alimentation, défaillance de carte SSL, erreurs de disque dur et erreurs de flash compact. Pour d'autres erreurs, après avoir examiné les journaux système, vous pouvez contacter l'équipe de support Citrix pour déclencher une demande de service pour enquête.

Configuration de l'Call Home

Pour configurer Call Home, vérifiez la connectivité Internet de l'appliance et assurez-vous qu'un serveur de noms DNS est configuré. S'il n'y a pas de connexion Internet, configurez un serveur proxy ou un service. Activez ensuite Call Home sur l'appliance et vérifiez l'état d'enregistrement de l'appliance auprès du serveur de prise en charge Citrix. Une fois inscrit, Call Home peut surveiller

et télécharger des données. En outre, vous pouvez configurer des alarmes SNMP pour notifier l'administrateur sur le site client.

Pour configurer Call Home, vous pouvez utiliser l'interface de commande Citrix ADC ou l'interface graphique pour effectuer les tâches suivantes :

- Activer Call Home.
- Configurez Call Home pour les paramètres facultatifs du serveur proxy.
- Vérifiez l'état de l'enregistrement de l'Call Home.
- Afficher les erreurs et les détails de l'horodatage.
- Configurer les alarmes SNMP.

Pour configurer Call Home à l'aide de l'interface de commande Citrix ADC

L'interface de commande Citrix ADC vous permet d'effectuer les opérations suivantes :

`Enabling Call Home`

À l'invite de commandes, tapez :

```
enable ns feature callhome
```

Configuration de l'appel d'accueil pour les paramètres de serveur proxy facultatifs

Call Home vous permet de configurer le serveur proxy en option pour la connectivité Internet. Vous pouvez configurer un serveur proxy avec adresse IP et port ou configurer un service d'authentification proxy avec authentification unidirectionnelle ou bidirectionnelle.

`To configure optional proxy server with IP address and port`

À l'invite de commandes, tapez :

```
set callhome -proxyMode ( YES | NO )[-IPAddress <ip_addr|ipv6_addr|*>] [-
port <port |*>]
```

```
1 set callhome -proxyMode YES -IPAddress 10.102.167.33 -port 80
2 <!--NeedCopy-->
```

> **Remarque**
>
> Call Home utilise le serveur proxy uniquement lorsque vous définissez le paramètre mode proxy sur YES. Si vous le définissez sur NO, la fonctionnalité proxy ne fonctionne pas, même si l'adresse IP et le port sont configurés. Le numéro de port doit être pour un service HTTP et non pour un service HTTPS.

Pour configurer le service d'authentification proxy facultatif

Ce mode offre deux types d'authentification de sécurité : unidirectionnelle et bidirectionnelle. Pour configurer l'un ou l'autre type, vous devez configurer un service SSL. Pour plus d'informations, consultez la rubrique Configuration d'un service SSL .

Dans l'authentification unidirectionnelle, seul l'appliance Citrix ADC authentifie le serveur proxy. Dans l'authentification bidirectionnelle, l'appliance Citrix ADC authentifie le serveur proxy et le serveur proxy, à son tour, authentifie l'appliance.

Pour configurer le service d'authentification par proxy

À l'invite de commandes, tapez :

```
set callhome -proxyMode ( YES | NO )[-proxyAuthService <string>]
```

```
1 set callhome  - proxyMode YES  - proxyAuthService callhome_proxy
2 <!--NeedCopy-->
```

Pour configurer l'authentification du serveur proxy unidirectionnel

Effectuez les tâches suivantes pour configurer l'authentification du serveur proxy unidirectionnel.

1. Créez un service SSL.
2. Liez un certificat d'autorité de certification au service.
3. Liez un moniteur HTTPS au service.
4. Configurez Call Home pour utiliser le service SSL.

Pour configurer l'authentification bidirectionnelle du serveur proxy

Effectuez les tâches suivantes pour configurer l'authentification bidirectionnelle du serveur proxy.

1. Créer un service SSL
2. Liez un certificat d'autorité de certification au service.
3. Liez un certificat client.
4. Liez un moniteur HTTPS au service.
5. Configurez Call Home pour utiliser le service SSL.

Vérification de l'état de l'enregistrement de l'Call Home

À l'invite de commandes, tapez :

```
1 show callhome
2
3     show callhome
4
5      Registration with Citrix upload server SUCCESSFUL
6
7      Mode: Default
8
9      Contact email address: exampleadmin@example.com
```



```
10
11       Heartbeat Custom Interval (days): 7
12
13       Proxy Mode: Yes
14
15          Proxy IP Address:10.102.29.200
16
17          Proxy Authentication Service:
18
19          Proxy Port: 80
20
21      Trigger event                   State   First occurrence
                        Latest occurrence
22
23       -------------                   -----   ----------------
                         -----------------
24
25       1) Warm boot                    Enabled N/A
                                         ..
26
27       2) Compact flash errors         Enabled ..
                                           ..
28
29       3) Hard disk drive errors       Enabled ..
                                           ..
30
31       4) SSL card failure             N/A     N/A
                                         N/A
32
33       5) Power supply unit failure    N/A     N/A
                                         N/A
34
35       6) Rate limit packet drops      Enabled ..
                                           ..
36
37       7) Memory anomaly               Enabled ..
                                           ..
38
39       Done
40  <!--NeedCopy-->
```

> **Remarque**
>
> Si l'Call Home ne parvient pas à s'inscrire auprès de CIS, l'appliance affiche un message d'erreur.

Activation des alarmes SNMP

L'appliance Citrix ADC fournit un ensemble d'entités de condition d'erreur appelées *alarmes SNMP*. Lorsqu'une condition d'erreur dans une alarme SNMP est remplie, l'appliance génère des messages d'interruption SNMP envoyés aux écouteurs d'interruption configurés. Par exemple, lorsque l'alarme SSL-CARD-FAILED est activée, un message d'interruption est généré et envoyé à l'écouteur d'interruption. Le message d'interruption est envoyé chaque fois qu'il y a une défaillance de la carte SSL sur l'appliance. Pour plus d'informations, voir SNMP.

À l'invite de commandes, tapez :

```
enable snmp alarm <trapName>
```

```
show snmp alarm <trapName>
```

Pour configurer Call Home à l'aide de l'interface graphique

Pour vérifier si la fonctionnalité Call Home est activée par défaut dans l'interface graphique

1. Accédez à **Configuration** > **Système** > **Paramètres**.
2. Dans le volet d'**informations**, cliquez sur le lien **Configurer les fonctionnalités avancées**.
3. Dans la page **Configurer les fonctionnalités avancées**, l'option **Call Home** doit s'afficher comme activée.

Pour activer l'Call Home l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Paramètres**.
2. Dans le volet d'**informations**, cliquez sur le lien **Configurer les fonctionnalités avancées** et sélectionnez l'option **Callhome**.

Pour configurer Call Home pour l'authentification en mode proxy en option à l'aide de l'interface graphique

1. Vous pouvez utiliser l'une des deux façons d'accéder à la page d' accueil de l'appel :
   a) Accédez à **Système> Informations système**.
   b) Accédez à **Système** > **Diagnostics**.
      i. Dans le volet d'informations, sous **Outils de support technique**, sélectionnez **Call Home**.
2. Dans la page **Configurer l'Call Home**, définissez les paramètres suivants.
   a) **Mode**. Appelez le mode de fonctionnement de la maison. Types possibles : Déploiement par défaut de Citrix Service Provider (CSP).

      > **Remarque**
      > Cette option n'est pas configurable par l'utilisateur. Le mode est automatiquement déterminé et défini en fonction du type de déploiement Citrix ADC.

   b) **Adresse e-mail**. Adresse e-mail de l'administrateur du contact sur le site du client.

c) **CallHome Heartbeats Intervalle (jours).** Intervalle de surveillance (en jours) entre les battements cardiaques Call Home. Valeur minimale = 1 et Valeur maximale = 7.
d) **Activer Call Home**. Activez ou désactivez la fonctionnalité Call Home pour afficher l'état de l'enregistrement de l'appliance sur le serveur de support Citrix.
e) **Mode proxy**. Si vous n'avez pas de connectivité Internet, activez le mode proxy et définissez les paramètres proxy facultatifs.
f) **Serveur proxy**. Si vous définissez le mode proxy à l'aide d'un serveur proxy, spécifiez l'adresse IP du serveur.
   i. **Service proxy**. Si vous définissez le mode proxy à l'aide d'un service proxy, spécifiez le nom du service.
   ii. **Adresse IP**. Adresse IP du serveur proxy.
   iii. **Port**. Numéro de port du serveur proxy.
   iv. **Service SSL d'authentification par proxy**. Nom du service proxy qui fournit l'authentification en mode proxy.

3. Cliquez sur **OK** et **Terminé**.

Pour configurer le service SSL pour l'authentification du serveur proxy à l'aide de l'interface graphique

Pour plus d'informations sur la configuration du service SSL à l'aide de l'interface graphique, reportez-vous à la rubrique Configuration d'un service SSL .

Pour vérifier l'état de l'inscription Call Home à l'aide de l'interface graphique

1. Vous pouvez utiliser l'une des deux façons d'accéder à la page d' **accueil de l'appel** :
   a) Accédez à **Système> Informations système**.
   b) Accédez à **Système** > **Diagnostics**.
      i. Dans le volet d'informations, sous **Outils de support technique**, sélectionnez **Call Home**.
2. Dans la page **Configurer l'Call Home**, le champ **Enregistrement avec le serveur de téléchargement Citrix** affiche l'état de l'enregistrement.

Pour configurer une alarme SNMP

1. Accédez à **Système** > **SNMP** > **Alarmes**.
2. Dans le volet d'informations, sélectionnez une alarme et configurez ses paramètres.
3. Cliquez sur **OK** et **Fermer**.

Prise en charge du déploiement Citrix Service Provider (CSP)

Dans un environnement Citrix Service Provider (CSP) où les services Citrix ADC sont déployés sur des instances VPX, Call Home peut surveiller et suivre les informations spécifiques à la licence et envoyer en toute sécurité les informations à Citrix Insight Services (CIS). CIS envoie à son tour les informations au portail LUI (License Usage Insights) à des fins comptables et aux clients CSP de revoir leur utilisation de licence. Actuellement, les environnements CSP prennent en charge les services Citrix ADC sur les

instances VPX uniquement, et non sur les appliances MPX ou SDX. Les instances VPX peuvent être déployées en mode autonome ou en mode haute disponibilité.

Outil de création de rapports

August 20, 2021

Utilisez l'outil Citrix® Citrix ADC® Reporting pour afficher les données de statistiques de performances Citrix ADC sous forme de rapports. Les données statistiques sont collectées par l' `nscollect` utilitaire et stockées dans une base de données. Lorsque vous souhaitez afficher certaines données de performances sur une période, l'outil Reporting extrait les données spécifiées de la base de données et les affiche dans des graphiques.

Les rapports sont une collection de graphiques. L'outil Reporting fournit des rapports intégrés et la possibilité de créer des rapports personnalisés. Dans un rapport, vous pouvez modifier les graphiques et ajouter de nouveaux graphiques. Vous pouvez également modifier le fonctionnement de l'utilitaire de collecte de données et arrêter ou démarrer son opération. `nscollect`

Utilisation de l'outil de création de rapports

L'outil Reporting est une interface Web accessible depuis l'appliance Citrix® Citrix ADC®. Utilisez l'outil Reporting pour afficher les données des statistiques de performances sous forme de rapports contenant des graphiques. En plus d'utiliser les rapports intégrés, vous pouvez créer des rapports personnalisés que vous pouvez modifier à tout moment. Les rapports peuvent comporter entre un et quatre graphiques. Vous pouvez créer jusqu'à 256 rapports personnalisés. Vous pouvez créer un rapport personnalisé pour un nombre quelconque d'entités.

Pour appeler l'outil de création de rapports

1. Utilisez le navigateur Web de votre choix pour vous connecter à l'adresse IP de Citrix ADC (par exemple,`http://10.102.29.170/`). L'écran d'ouverture de session Web s'affiche.
2. Dans la zone de texte Nom d'utilisateur, tapez le nom d'utilisateur attribué à Citrix ADC.
3. Dans la zone de texte Mot de passe, tapez le mot de passe.
4. Dans la zone de liste déroulante Démarrer dans, sélectionnez Reporting. Cliquez sur Connexion.

Les captures d'écran suivantes présentent la barre d'outils du rapport et la barre d'outils du graphique, fréquemment référencées dans cette documentation.

Figure 1. *Barre d'outils Rapport*

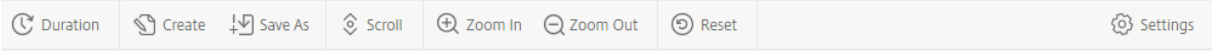
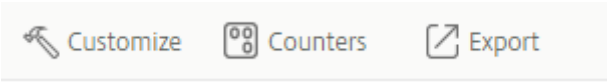


Figure 2. *Barre d'outils Graphique*



Utilisation des rapports

Vous pouvez tracer et surveiller les statistiques pour les différents groupes fonctionnels configurés sur Citrix ADC sur un intervalle de temps spécifié. Les rapports vous permettent de dépanner ou d'analyser le comportement de votre appliance. Il existe deux types de rapports : les rapports intégrés et les rapports personnalisés. Le contenu des rapports intégrés ou personnalisés peut être affiché sous forme graphique ou tabulaire. La vue graphique se compose de graphiques en ligne, en zone et en barres qui peuvent afficher jusqu'à 32 ensembles de données (compteurs). La vue tabulaire affiche les données en colonnes et en lignes. Cette vue est utile pour le débogage des compteurs d'erreurs.

Le rapport par défaut affiché dans l'outil Reporting est CPU vs. Utilisation de la mémoire et taux de requêtes HTTP. Vous pouvez modifier l'affichage du rapport par défaut en affichant le rapport souhaité comme affichage par défaut, puis en cliquant sur Rapport par défaut.

Les rapports peuvent être générés pour la dernière heure, le dernier jour, la semaine dernière, le dernier mois, l'année dernière, ou vous pouvez personnaliser la durée.

Vous pouvez effectuer les opérations suivantes avec les rapports :

- Basculer entre une vue tabulaire des données et une vue graphique des données.
- Modifiez le type d'affichage graphique, tel qu'un graphique à barres ou un graphique en courbes.
- Personnaliser les graphiques dans un rapport.
- Exportez le graphique en tant que fichier CSV (Excel séparé par des virgules).
- Affichez les graphiques en détail en effectuant un zoom avant, un zoom arrière ou une opération de glissement (défilement).
- Définissez un rapport comme rapport par défaut à afficher chaque fois que vous ouvrez une session.
- Ajouter ou supprimer des compteurs.
- Imprimer des rapports.
- Actualiser les rapports pour afficher les dernières données de performances.

Utilisation de rapports intégrés

L'outil Reporting fournit des rapports intégrés pour les données fréquemment consultées. Les rapports intégrés sont disponibles pour les groupes fonctionnels suivants : Système, Réseau, SSL, Compression, Cache intégré, Citrix ADC Gateway et Citrix ADC Application Firewall. Par défaut, les rapports

intégrés sont affichés pour le dernier jour. Toutefois, vous pouvez afficher les rapports de la dernière heure, de la dernière semaine, du dernier mois ou de l'année dernière.

> **Remarque** :
>
> Vous ne pouvez pas enregistrer les modifications apportées aux rapports intégrés, mais vous pouvez enregistrer un rapport intégré modifié en tant que rapport personnalisé.

Pour afficher un rapport intégré

1. Dans le volet gauche de l'outil Rapports, sous Rapports intégrés, développez un groupe (par exemple, SSL).
2. Cliquez sur un rapport (par exemple, **SSL > Tous les chiffrements backend)**.

Création et suppression de rapports

Vous pouvez créer vos propres rapports personnalisés et les enregistrer avec des noms définis par l'utilisateur pour les réutiliser. Vous pouvez tracer différents compteurs pour différents groupes en fonction de vos besoins. Vous pouvez créer jusqu'à 256 rapports personnalisés.

Vous pouvez créer un rapport ou enregistrer un rapport intégré en tant que rapport personnalisé. Par défaut, un rapport personnalisé nouvellement créé contient un graphique nommé Vue d'ensemble du système, qui affiche le compteur d'utilisation du processeur tracé pour le dernier jour. Vous pouvez personnaliser l'intervalle et définir la source de données et le fuseau horaire à partir de la barre d'outils du rapport.

Pour créer un rapport personnalisé

1. Dans l'outil **Rapports**, dans la barre d'outils du rapport, cliquez sur **Créer** ou, si vous souhaitez créer un rapport personnalisé basé sur un rapport existant, ouvrez le rapport existant, puis cliquez sur **Enregistrer sous**.
2. Dans la zone **Nom du rapport**, tapez un nom pour le rapport personnalisé.
3. Procédez comme suit :
   - Pour ajouter le rapport à un dossier existant, dans Créer dans ou Enregistrer dans, cliquez sur la flèche vers le bas pour choisir un dossier existant, puis cliquez sur **OK**.
   - Pour créer un nouveau dossier pour stocker le rapport, cliquez sur l'icône Cliquez pour ajouter un dossier, dans Nom du dossier, tapez le nom du dossier, puis dans Créer dans, indiquez où vous souhaitez que le nouveau dossier réside dans la hiérarchie, puis cliquez sur **OK**.

> **Remarque** :
> Vous pouvez créer jusqu'à 128 dossiers.

Pour supprimer un rapport personnalisé

1. Dans le volet gauche de l'outil Reporting, à côté de Rapports personnalisés, cliquez sur l'icône Cliquer pour gérer les rapports personnalisés.
2. Activez la case à cocher correspondant au rapport à supprimer, puis cliquez sur Supprimer.

> **Remarque** :
>
> lorsque vous supprimez un dossier, tout le contenu de ce dossier est supprimé.

Modification de l'intervalle de temps

Par défaut, les rapports intégrés affichent les données du dernier jour. Toutefois, si vous souhaitez modifier l'intervalle de temps d'un rapport intégré, vous pouvez enregistrer le rapport en tant que rapport personnalisé. Le nouvel intervalle s'applique à tous les graphiques du rapport. Le tableau suivant décrit les options d'intervalle de temps.

Pour modifier l'intervalle de temps

1. Dans le volet gauche de l'outil Rapports, cliquez sur un rapport.
2. Dans la barre d'outils du rapport, cliquez sur **Durée**, puis sur un intervalle de temps.

Définition de la source de données et du fuseau horaire

Vous pouvez extraire des données de différentes sources de données pour les afficher dans les rapports. Vous pouvez également définir le fuseau horaire des rapports et appliquer la sélection horaire du rapport actuellement affiché à tous les rapports, y compris les rapports intégrés.

Pour définir la source de données et le fuseau horaire

1. Dans l'**outil Rapports**, dans la barre d'outils du rapport, cliquez sur **Paramètres**.
2. Dans la boîte de dialogue **Paramètres**, dans Source de données, sélectionnez la source de données à partir de laquelle vous souhaitez extraire les informations du compteur.
3. Faites l'une des opérations suivantes ou les deux :
   - Si vous souhaitez que l'outil mémorise la période pendant laquelle un graphique est tracé, activez la case à cocher **Mémoriser la sélection de temps pour les graphiques** .
   - Si vous souhaitez que les rapports utilisent les paramètres d'heure de votre appliance Citrix ADC, activez la case à cocher **Utiliser le fuseau horaire de l'appliance** .

Exportation et importation de rapports personnalisés

Vous pouvez partager des rapports avec d'autres administrateurs Citrix ADC en exportant des rapports. Vous pouvez également importer des rapports.

Pour exporter ou importer des rapports personnalisés

1. Dans le volet gauche de l'outil de création de rapports, en regard de Rapports personnalisés, cliquez sur l'icône **Cliquez pour gérer les rapports personnalisés**.
2. Activez la case à cocher correspondant au rapport à exporter ou à importer, puis cliquez sur **Exporter** ou **Importer** .

   > **Remarque** :
   >
   > lorsque vous exportez le fichier, il est exporté au format de fichier .gz.

Utilisation des graphiques

Utilisez des graphiques pour tracer et surveiller des compteurs ou des groupes de compteurs. Vous pouvez inclure jusqu'à quatre graphiques dans un rapport. Dans chaque graphique, vous pouvez tracer jusqu'à 32 compteurs. Les graphiques peuvent utiliser différents formats graphiques (par exemple, zone et barre). Vous pouvez déplacer les graphiques vers le haut ou vers le bas dans le rapport, personnaliser les couleurs et l'affichage visuel de chaque compteur d'un graphique et supprimer un graphique lorsque vous ne souhaitez pas le surveiller.

Dans tous les graphiques de rapport, l'axe horizontal représente le temps et l'axe vertical représente la valeur du compteur.

Ajout d'un graphique

Lorsque vous ajoutez un graphique à un rapport, le graphique Vue d'ensemble du système apparaît avec le compteur Utilisation de l'UC tracé pour le dernier jour.

> **Remarque** :
>
> Si vous ajoutez des graphiques à un rapport intégré et que vous souhaitez conserver le rapport, vous devez enregistrer le rapport en tant que rapport personnalisé.

Utilisez la procédure suivante pour ajouter un graphique à un état.

Pour ajouter un graphique à un rapport

1. Dans le volet gauche de l'outil Rapports, cliquez sur un rapport.

2. Sous le graphique dans lequel vous souhaitez ajouter le nouveau graphique, cliquez sur l'icône Ajouter.

Modification d'un graphique

Vous pouvez modifier un graphique en modifiant le groupe fonctionnel pour lequel les statistiques sont affichées et en sélectionnant différents compteurs.

Pour modifier un graphique

1. Dans le volet gauche de l'outil Rapports, cliquez sur un rapport.
2. Sous le graphique à modifier, cliquez sur Compteurs.
3. Dans la boîte de dialogue qui apparaît, dans la zone Titre, tapez un nom pour le graphique.
4. À côté du diagramme de tracé pour, effectuez l'une des opérations suivantes :
    - Pour tracer les compteurs pour les compteurs globaux, tels que Cache intégré et Compression, cliquez sur Statistiques globales système.
    - Pour tracer les compteurs d'entités pour les types d'entités, tels que l'équilibrage de charge et GSLB, cliquez sur Statistiques des entités système.
5. Dans le groupe Sélectionner, cliquez sur l'entité souhaitée.
6. Sous Compteurs, dans Disponible, cliquez sur un ou plusieurs noms de compteurs que vous souhaitez tracer, puis cliquez sur le bouton >.
7. Si vous avez sélectionné les statistiques des entités système à l'étape 4, sous l'onglet Entités, sous Disponible, cliquez sur un ou plusieurs noms d'instances d'entités que vous souhaitez tracer, puis cliquez sur le bouton >.
8. Cliquez sur OK.

Affichage d'un graphique

Vous pouvez spécifier les formats graphiques des compteurs tracés dans un graphique. Les graphiques peuvent être affichés sous forme de graphiques en courbes, de graphiques en spline, de graphiques en courbes, de graphiques en nuages de points, de graphiques en aires, de graphiques à barres, de graphiques en aires empilées et de graphiques à barres empilées. Vous pouvez également effectuer un zoom avant, un zoom arrière ou un défilement à l'intérieur de la zone de tracé d'un graphique. Vous pouvez effectuer un zoom avant ou arrière pour toutes les sources de données pendant 1 heure, 1 jour, 1 semaine, 1 mois, 1 an et 3 ans.

D'autres options de personnalisation de la vue d'un graphique incluent la personnalisation des axes des graphiques, la modification de la couleur d'arrière-plan et de bordure de la zone de tracé, la personnalisation de la couleur et de la taille des grilles et la personnalisation de l'affichage de chaque jeu de données (compteur) d'un graphique.

Les numéros des ensembles de données, tels que l'ensemble de données 1, correspondent à l'ordre dans lequel les compteurs de votre graphique sont affichés en bas du graphique. Par exemple, si l'utilisation de l'UC et l'utilisation de la mémoire sont affichées dans le premier et le deuxième ordre au bas du graphique, l'utilisation de l'UC est égale à l'ensemble de données 1 et l'utilisation de la mémoire est égale à l'ensemble de données 2.

Chaque fois que vous modifiez un rapport intégré, vous devez l'enregistrer en tant que rapport personnalisé pour conserver vos modifications.

Pour modifier le type de graphique d'un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique à afficher, dans la barre d'outils du graphique, cliquez sur **Personnaliser**.
3. Sous l'onglet **Graphique**, sous **Catégorie**, cliquez sur **Type de tracé**, puis sur le type de graphique à afficher pour le graphique. Si vous souhaitez afficher le graphique en 3D, activez la case à cocher Utiliser 3D.

Pour recentrer un graphique avec des données détaillées

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, dans la barre d'outils du rapport, cliquez sur **Zoom avant**, puis effectuez l'une des opérations suivantes ou les deux :
   - Pour refocaliser le graphique afin d'afficher les données d'une fenêtre horaire spécifique, faites glisser le curseur de l'heure de début à l'heure de fin. Par exemple, vous pouvez afficher des données pour une période d'une heure sur un jour donné.
   - Pour refocaliser le graphique afin d'afficher les données d'un point de données, il suffit de cliquer une fois sur le graphique où vous souhaitez effectuer un zoom avant et obtenir des informations plus détaillées.
3. Une fois que vous avez la plage de temps souhaitée pour afficher les données détaillées, dans la barre d'outils du rapport, cliquez sur Affichage tabulaire. La vue tabulaire affiche les données sous forme numérique sous forme de lignes et de colonnes.

Pour afficher les données numériques d'un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, dans la barre d'outils du rapport, cliquez sur Affichage tabulaire. Pour revenir à la vue graphique, cliquez sur **Vue graphique**.

> **Remarque** : Vous pouvez également afficher les données numériques dans la vue graphique en plaçant le curseur sur les encoches du quadrillage.

Pour faire défiler le temps dans un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, dans la barre d'outils du rapport, cliquez sur **Défiler**, puis sur l'intérieur du graphique et faites glisser le curseur dans la direction dans laquelle vous souhaitez afficher les données pour une nouvelle période. Par exemple, si vous souhaitez afficher des données par le passé, faites glisser vers la gauche.

Pour modifier la couleur d'arrière-plan et la couleur du texte d'un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique pour lequel vous souhaitez personnaliser les axes, cliquez sur **Personnaliser**.
3. Sous l'onglet **Graphique**, sous **Catégorie**, cliquez sur une ou plusieurs des options suivantes :
   - Pour modifier la couleur d'arrière-plan, cliquez sur **Couleur d'arrière-plan**, puis sélectionnez les options de couleur, de transparence et d'effets.
   - Pour modifier la couleur du texte, cliquez sur **Couleur**du texte, puis sélectionnez les options de couleur, de transparence et d'effets.

Pour personnaliser les axes d'un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique pour lequel vous souhaitez personnaliser les axes, cliquez sur **Personnaliser**.
3. Dans l'onglet **Graphique**, sous Catégorie, cliquez sur une ou plusieurs des options suivantes :
   - Pour modifier l'échelle de l'axe Y gauche, cliquez sur **Axe Y gauche**, puis sélectionnez l'échelle souhaitée.
   - Pour modifier l'échelle de l'axe Y droit, cliquez sur Axe Y droit, dans le jeu de données à tracer, sélectionnez le jeu de dates, puis sélectionnez l'échelle souhaitée.

     > Note :
     > Les numéros des ensembles de données, tels que l'ensemble de données 1, correspondent à l'ordre dans lequel les compteurs de votre graphique sont affichés en bas du graphique. Par exemple, si l'utilisation de l'UC et l'utilisation de la mémoire sont affichées dans le premier et le deuxième ordre au bas du graphique, l'utilisation de l'UC est égale à l'ensemble de données 1 et l'utilisation de la mémoire est égale à l'ensemble de données 2.

- Pour tracer chaque jeu de données dans son propre axe y masqué, cliquez sur plusieurs axes, puis cliquez sur Activer.

Pour modifier la couleur d'arrière-plan, la couleur d'arête et le quadrillage d'une zone de tracé d'un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique pour lequel vous souhaitez personnaliser la zone de tracé, cliquez sur **Personnaliser**.
3. Sous l'onglet **Zone de traçage**, sous Catégorie, cliquez sur une ou plusieurs des options suivantes :
   - Pour modifier la couleur d'arrière-plan et la couleur d'arête du graphique, cliquez sur **Couleur d'arrière-plan et couleur d'arête**, puis sélectionnez les options de couleur, de transparence et d'effets.
   - Pour modifier les grilles horizontales ou verticales du graphique, cliquez sur **Grilles horizontales ou Grillesverticales**, puis sélectionnez les options d'affichage des grilles, de la largeur de la grille, de la couleur de la grille, de la transparence et des effets.

Pour modifier la couleur et le type de graphique d'un ensemble de données

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique pour lequel vous souhaitez personnaliser l'affichage du jeu de données (compteurs), cliquez sur **Personnaliser**.
3. Sous l'onglet **Jeu de données**, dans Sélectionner un jeu de données, sélectionnez le jeu de données (compteur) pour lequel vous souhaitez personnaliser l'affichage graphique.
   Note : Les numéros des ensembles de données, tels que l'ensemble de données 1, correspondent à l'ordre dans lequel les compteurs de votre graphique sont affichés en bas du graphique. Par exemple, si l'utilisation de l'
   UC et l'utilisation de la
   mémoire sont affichées dans le premier et le deuxième ordre au bas du graphique, l'utilisation de l'
   UC est égale à l'ensemble de
   données 1 et l'utilisation de la
   mémoire est égale à l'ensemble de
   données 2.
4. Sous Catégorie, effectuez l'une des opérations suivantes :
   - Pour modifier la couleur d'arrière-plan, cliquez sur **Couleur**, puis sélectionnez les options de couleur, de transparence et d'effets.
   - Pour modifier le type de graphique, cliquez sur **Type de diagramme**, puis sélectionnez le type de graphique à afficher pour le jeu de données. Si vous souhaitez afficher le

graphique en 3D, activez la case à cocher Utiliser 3D.

Exportation de données de graphique vers Excel

Pour une analyse plus poussée des données, vous pouvez exporter des graphiques vers Excel dans un format CSV (valeur séparée par des virgules).

Pour exporter des données de graphique vers Excel

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique contenant les données à exporter vers Excel, cliquez sur **Exporter**.

Suppression d'un graphique

Si vous ne souhaitez pas utiliser de graphique, vous pouvez le supprimer du rapport. Vous pouvez supprimer définitivement des graphiques des rapports personnalisés uniquement. Si vous supprimez un graphique d'un rapport intégré et que vous souhaitez conserver les modifications, vous devez enregistrer le rapport en tant que rapport personnalisé.

Pour supprimer un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique à supprimer, cliquez sur l'icône **Supprimer** .

Exemples

Pour afficher le rapport de tendance pour l'utilisation de l'UC et de la mémoire pour la dernière semaine

1. Dans le volet gauche de l'outil Rapports, sous Rapports intégrés, développez Système.
2. Cliquez sur le rapport CPU vs. Utilisation de la mémoire et taux de requêtes HTTP.
3. Dans le volet droit, dans la barre d'outils du rapport, cliquez sur **Durée**, puis sur **Semaine dernière**.

Pour comparer le taux d'octets reçus et le taux d'octets transmis entre les deux interfaces de la semaine dernière

1. Dans le volet droit, dans la barre d'outils du rapport, cliquez sur Créer.
2. Dans la zone **Nom du rapport**, tapez un nom pour le rapport personnalisé (par exemple, Custom_Interfaces), puis cliquez sur **OK** . Le rapport est créé avec le graphique Vue d'ensemble du système par défaut, qui affiche le compteur d'utilisation de l'UC tracé pour la dernière heure.

3. Sous Vue d'ensemble du système, dans la barre d'outils du graphique, cliquez sur Compteurs.
4. Dans le volet de sélection des compteurs, dans Titre, tapez un nom pour le graphique (par exemple, Interfaces octets data).
5. Dans Graphique de tracé pour, cliquez sur Statistiques des entités système, puis dans Sélectionner un groupe, sélectionnez Interface.
6. Dans l'onglet **Entités**, cliquez sur un ou plusieurs noms d'interface que vous souhaitez tracer (par exemple, 1/1 et 1/2), puis cliquez sur le bouton >.
7. Sous l'onglet Compteurs, cliquez sur Octets reçus (Taux) et Octets transmis (Taux), puis cliquez sur le bouton>.
8. Cliquez sur **OK**.
9. Dans la barre d'outils du rapport, cliquez sur **Durée**, puis sur **Semaine dernière**.

Arrêt et démarrage de l'utilitaire de collecte de données

L'utilitaire de collecte de données s'exécute automatiquement lorsque vous démarrez Citrix ADC. `nscollect` Cet utilitaire récupère les données de performances de l'application et les stocke sous la forme de sources de données sur ADC. Vous pouvez créer jusqu'à 32 sources de données. La source de données par défaut est`/var/log/db/default`.

L'utilitaire de collecte de données crée des bases de données pour les compteurs globaux et les compteurs spécifiques à l'entité, et utilise ces données pour générer des rapports. Les bases de données Global Counter sont créées à l'adresse `/var/log/db/<DataSourceName>`. Les bases de données spécifiques à l'entité sont créées en fonction des entités configurées sur Citrix ADC, et un dossier distinct est créé pour chaque type d'entité dans`/var/log/db/<DataSourceName/EntityNameDB>`.

Le système `nscollect` récupère les données toutes les 5 minutes. Il conserve les données en granularité de 5 minutes pendant un jour, toutes les heures pendant les 30 derniers jours et tous les jours pendant trois ans.

Vous devrez peut-être arrêter et redémarrer l'utilitaire de collecte de données si les données ne sont pas correctement mises à jour ou si les rapports affichent des données corrompues.

Pour arrêter `nscollect`

À l'invite de commandes, tapez :

```
/netscaler/nscollect stop
```

Pour démarrer nscollect sur la session SSH actuelle vers Citrix ADC :

À l'invite de commandes, tapez :

```
/netscaler/nscollect start
```

Pour démarrer nscollect sur le système local :

À l'invite de commandes, tapez :

```
/netscaler/nscollect start &
```

CloudBridge Connector

August 20, 2021

Remarque : La version actuelle de Citrix ADC 1000V ne prend pas en charge cette fonctionnalité.

La fonctionnalité CloudBridge Connector de l'appliance Citrix ADC connecte les centres de données d'entreprise aux clouds externes et aux environnements d'hébergement, ce qui fait du cloud une extension sécurisée de votre réseau d'entreprise. Les applications hébergées dans le cloud semblent s'exécuter sur un réseau d'entreprise contigu. Avec Citrix CloudBridge Connector, vous pouvez augmenter vos centres de données grâce à la capacité et à l'efficacité disponibles auprès des fournisseurs de cloud.

CloudBridge Connector vous permet de déplacer vos applications vers le cloud afin de réduire les coûts et d'augmenter la fiabilité.

En plus d'utiliser CloudBridge Connector entre un centre de données et un nuage, vous pouvez l'utiliser pour connecter deux centres de données pour une liaison sécurisée et accélérée haute capacité.

Présentation du connecteur CloudBridge

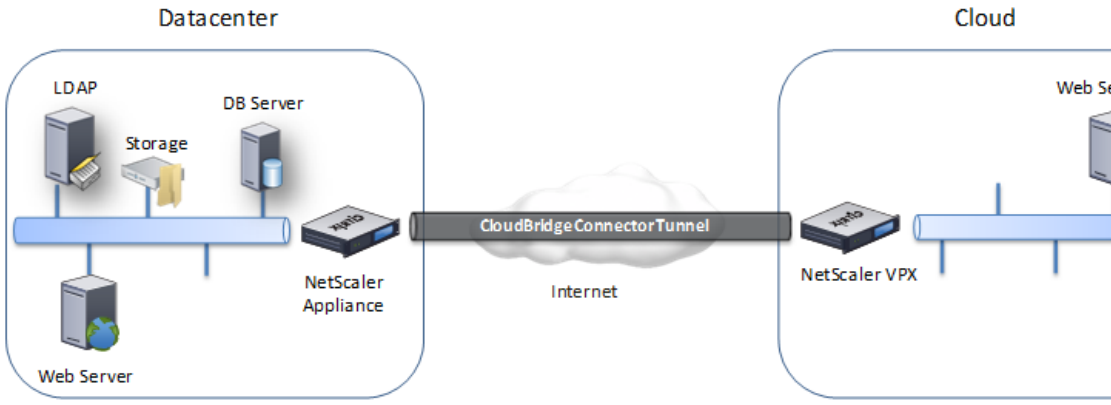
Pour implémenter la solution Citrix CloudBridge Connector, vous connectez un centre de données à un autre centre de données ou à un nuage externe en configurant un tunnel appelé tunnel CloudBridge Connector.

Pour connecter un centre de données à un autre centre de données, vous configurez un tunnel CloudBridge Connector entre deux appliances Citrix ADC, un dans chaque centre de données.

Pour connecter un centre de données à un nuage externe (par exemple, le cloud Amazon AWS), vous configurez un tunnel CloudBridge Connector entre une appliance Citrix ADC dans le centre de données et une appliance virtuelle (VPX) résidant dans le Cloud. Le point d'extrémité distant peut être un CloudBridge Connector ou un Citrix ADC VPX avec licence Premium.

L'illustration suivante montre un tunnel CloudBridge Connector configuré entre un centre de données

et un nuage externe.



Les appliances entre lesquelles un tunnel CloudBridge Connector est configuré sont appelées *points d'extrémité* ou *homologues* du tunnel CloudBridge Connector.

Un tunnel CloudBridge Connector utilise les protocoles suivants :

- Protocole GRE (Generic Routing Encapsulation)
- Suite de protocole IPsec standard ouverte, en mode transport

Le protocole GRE fournit un mécanisme pour encapsuler les paquets, à partir d'une grande variété de protocoles réseau, à transférer sur un autre protocole. Le GRE est utilisé pour :

- Connectez des réseaux exécutant des protocoles non IP et non routables.
- Pont sur un réseau étendu (WAN).
- Créez un tunnel de transport pour tout type de trafic qui doit être envoyé inchangé sur un autre réseau.

Le protocole GRE encapsule les paquets en ajoutant un en-tête GRE et un en-tête GRE IP aux paquets.

La suite de protocoles IPSec (Internet Protocol security) sécurise la communication entre pairs dans le tunnel CloudBridge Connector.

Dans un tunnel CloudBridge Connector, IPsec garantit :

- Intégrité des données
- Authentification de l'origine des données
- Confidentialité des données (cryptage)
- Protection contre les attaques de relecture

IPSec utilise le mode de transport dans lequel le paquet encapsulé GRE est chiffré. Le chiffrement est effectué par le protocole ESP (Encapsulating Security Payload). Le protocole ESP assure l'intégrité du paquet à l'aide d'une fonction de hachage HMAC et assure la confidentialité à l'aide d'un algorithme de chiffrement. Une fois le paquet chiffré et le HMAC calculé, un en-tête ESP est généré. L'en-tête ESP est inséré après l'en-tête IP GRE et une remorque ESP est insérée à la fin de la charge utile chiffrée.

Les homologues du tunnel CloudBridge Connector utilisent le protocole IKE (Internet Key Exchange version) (partie de la suite de protocoles IPSec) pour négocier une communication sécurisée, comme suit :

- Les deux pairs s'authentifient mutuellement les uns avec les autres, en utilisant l'une des méthodes d'authentification suivantes :
  - **Authentification de clé pré-partagée**. Une chaîne de texte appelée clé pré-partagée est configurée manuellement sur chaque pair. Les clés pré-partagées des pairs sont comparées les unes aux autres pour l'authentification. Par conséquent, pour que l'authentification réussisse, vous devez configurer la même clé pré-partagée sur chacun des homologues.
  - **Authentification des certificats numériques**. L'homologue initiateur (expéditeur) signe les données d'échange de messages à l'aide de sa clé privée, et l'autre homologue récepteur utilise la clé publique de l'expéditeur pour vérifier la signature. Généralement, la clé publique est échangée dans des messages contenant un certificat X.509v3. Ce certificat fournit un niveau d'assurance que l'identité d'un pair représentée dans le certificat est associée à une clé publique particulière.
- Les pairs négocient ensuite pour parvenir à un accord sur :
  - Un algorithme de chiffrement.
  - Clés cryptographiques pour chiffrer les données dans un pair et déchiffrer les données dans l'autre.

Cet accord sur le protocole de sécurité, l'algorithme de chiffrement et les clés cryptographiques est appelé une association de sécurité (SA). Les SA sont unidirectionnelles (simplex). Par exemple, lorsque deux homologues, CB1 et CB2, communiquent via un tunnel Connector, CB1 a deux associations de sécurité. Une SA est utilisée pour le traitement des paquets sortants et l'autre SA pour le traitement des paquets entrants.

Les SA expirent après une durée spécifiée, appelée *durée de vie*. Les deux homologues utilisent le protocole IKE (Internet Key Exchange) (partie de la suite de protocoles IPSec) pour négocier de nouvelles clés cryptographiques et établir de nouvelles SA. Le but de la durée de vie limitée est d'empêcher les attaquants de craquer une clé.

Le tableau suivant répertorie certaines propriétés IPSec prises en charge par un appliance Citrix ADC :

Propriétés IPSec	Types pris en charge
Versions IKE	V1, V2
Groupe IKE DH	Une appliance Citrix ADC prend en charge uniquement le groupe DH 2 (algorithme MODP 1024 bits) pour IKEv1 et IKEv2.

Propriétés IPSec	Types pris en charge
Méthodes d'authentification IKE	Authentification des clés pré-partagées, authentification des certificats numériques
Algorithme de chiffrement	AES (128 bits), AES 256 (256 bits), 3DES
Algorithme de hachage	HMAC SHA1, HMAC SHA256, HMAC SHA384, HMAC SHA512, HMAC MD5

Surveillance des tunnels du connecteur CloudBridge

January 21, 2021

Vous pouvez afficher les statistiques pour surveiller les performances d'un tunnel CloudBridge Connector. Pour afficher les statistiques de tunnel CloudBridge Connector sur une appliance Citrix ADC, utilisez l'interface graphique ou la ligne de commande Citrix ADC.

Le tableau suivant répertorie les compteurs statistiques disponibles pour la surveillance des tunnels CloudBridge Connector sur une appliance Citrix ADC.

Compteur statistique	**Spécifie**
Octets reçus	Nombre total d'octets reçus par l'appliance Citrix ADC via tous les tunnels CloudBridge Connector configurés depuis le dernier démarrage de l'appliance.
Octets envoyés	Nombre total d'octets envoyés par l'appliance Citrix ADC via tous les tunnels CloudBridge Connector configurés depuis le dernier démarrage de l'appliance.
Paquets reçus	Nombre total de paquets reçus par l'appliance Citrix ADC via tous les tunnels CloudBridge Connector configurés depuis le dernier démarrage de l'appliance.
Paquets envoyés	Nombre total de paquets envoyés par l'appliance Citrix ADC via tous les tunnels CloudBridge Connector configurés depuis le dernier démarrage de l'appliance.

Compteur statistique	Spécifie
Taux d'octets reçus	Nombre d'octets par seconde reçus par l'appliance Citrix ADC via tous les tunnels configurés CloudBridge Connector.
Taux d'octets envoyés	Nombre d'octets par seconde envoyés par l'appliance Citrix ADC via tous les tunnels configurés CloudBridge Connector
Taux de réception des paquets	Nombre d'octets par seconde reçus par l'appliance Citrix ADC via tous les tunnels configurés CloudBridge Connector
Taux d'envoi des paquets	Nombre d'octets par seconde reçus par l'appliance Citrix ADC via tous les tunnels configurés CloudBridge Connector

Tous ces compteurs sont réinitialisés à 0 lorsque l'appliance Citrix ADC est redémarrée. Ils ne s'incrémentent pas pendant les phases suivantes :

- Phase d'authentification IKE (Internet Key Exchange) (clé pré-partagée) sur n'importe quel tunnel CloudBridge Connector configuré.
- Phase d'établissement IKE Security Association (SA) sur n'importe quel tunnel CloudBridge Connector configuré.

Pour afficher les statistiques de tunnel CloudBridge Connector à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

- **compteurs ipsec stat**

Pour afficher les statistiques de tunnel CloudBridge Connector à l'aide de l'interface graphique

1. Accédez à l'interface graphique à l'aide d'un navigateur Web pour vous connecter à l'adresse IP de l'appliance Citrix ADC.
2. Sous l'onglet **Configuration,** accédez à **Système** > **CloudBridge Connector** .
3. Dans la page Connecteur CloudBridge, cliquez sur **Créer/surveiller CloudBridge Connector**. Les graphiques **Octets IPsec** et **Paquets IPsec** affichent le taux d'octets reçus, le taux d'octets envoyés, le taux de réception des paquets et le taux d'envoi des paquets de tous les tunnels CloudBridge Connector configurés sur l'appliance Citrix ADC.

```
1     > stat ipsec counters
2     Secure tunnel(s) summary
3                         Rate (/s)        Total
```



```
4      Bytes Received    0    2811248
5      Bytes Sent            0    157460630
6      Packets Received    0    56787
7      Packets Sent        0    200910
8      Done
9      >
10 <!--NeedCopy-->
```

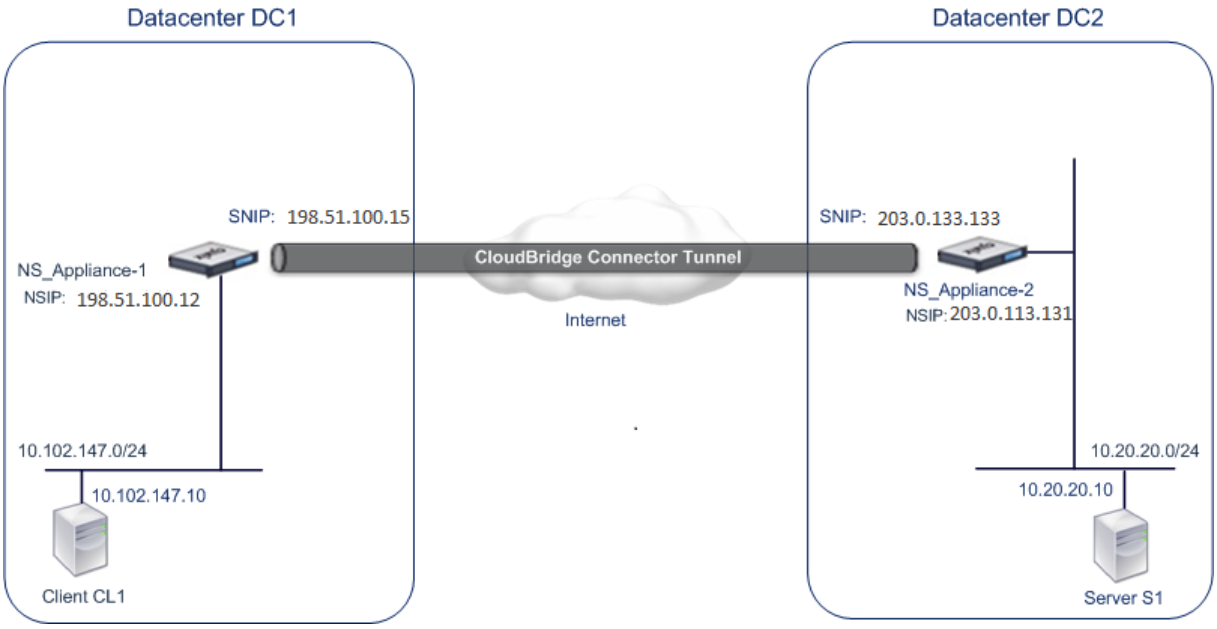
Configuration d'un tunnel CloudBridge Connector entre deux centres de données

August 20, 2021

Vous pouvez configurer un tunnel CloudBridge Connector entre deux centres de données différents pour étendre votre réseau sans le reconfigurer et tirer parti des capacités des deux centres de données. Un tunnel CloudBridge Connector entre les deux centres de données séparés géographiquement vous permet d'implémenter la redondance et de protéger votre configuration contre les défaillances. Le tunnel CloudBridge Connector permet d'optimiser l'utilisation de l'infrastructure et des ressources entre les centres de données. Les applications disponibles dans les deux centres de données apparaissent comme locales pour l'utilisateur.

Pour connecter un centre de données à un autre centre de données, vous configurez un tunnel CloudBridge Connector entre une appliance Citrix ADC dans un centre de données et une appliance Citrix ADC dans l'autre centre de données.

À titre d'illustration du tunnel CloudBridge Connector entre les centres de données, considérez un exemple dans lequel un tunnel CloudBridge Connector est configuré entre l'appliance Citrix ADC NS_Appliance-1 dans le centre de données DC1 et l'appliance Citrix ADC NS_Appliance-2 dans le centre de données DC2.



Les deux fonctions NS_Appliance-1 et NS_Appliance-2 en mode L2 et L3. Ils permettent la communication entre les réseaux privés dans les centres de données DC1 et DC2. En mode L3, NS_Appliance-1 et NS_Appliance-2 permettent la communication entre le client CL1 dans le datacenter DC1 et le serveur S1 dans le datacenter DC2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Comme le client CL1 et le serveur S1 se trouvent sur des réseaux privés différents, le mode L3 est activé sur NS_Appliance-1 et NS_Appliance-2, et les routes sont mises à jour comme suit :

- CL1 a une route vers NS_Appliance-1 pour atteindre S1.
- NS_Appliance-1 a une route vers NS_Appliance-2 pour atteindre S1.
- S1 a une route vers NS_Appliance-2 pour atteindre CL1.
- NS_Appliance-2 a une route vers NS_Appliance-1 pour atteindre CL1.

Le tableau suivant répertorie les paramètres de l'appliance Citrix ADC NS_Appliance-1 dans le centre de données DC1.

Le tableau suivant répertorie les paramètres de l'appliance Citrix ADC NS_Appliance-2 dans le centre de données DC2.

Entité	Nom	Détails
Adresse NSIP		198.51.100.12
Adresse SNIP		198.51.100.15

Entité	Nom	Détails
Tunnel CloudBridge Connector	Cloud_Connector_DC1-DC2	1. Adresse IP du point de terminaison local du tunnel CloudBridge Connector : 198.51.100.15, 2. Adresse IP du point de terminaison distant du tunnel CloudBridge Connector : 203.0.113.133. Détails du tunnel GRE Nom = Cloud_Connector_DC1-DC2, Détails du profil IPsec Nom = Cloud_Connector_DC1-DC2, Algorithme de chiffrement = AES, Algorithme de hachage = HMAC SHA1

Points à prendre en considération pour la configuration du tunnel CloudBridge Connector

Avant de configurer un tunnel CloudBridge Connector, vérifiez que les tâches suivantes ont été effectuées :

1. Déployez et configurez une appliance Citrix ADC dans chacun des deux centres de données.
2. Assurez-vous que les adresses IP du point d'extrémité du tunnel CloudBridge Connector sont accessibles les unes aux autres.

Procédure de configuration

Pour configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC résidant dans un centre de données et une autre appliance Citrix ADC résidant dans l'autre centre de données, utilisez l'interface graphique ou l'interface de ligne de commande de l'une des appliances Citrix ADC.

Lorsque vous utilisez l'interface graphique, la configuration du tunnel CloudBridge Connector créée sur la première appliance Citrix ADC est automatiquement poussée vers l'autre point de terminaison (l'autre appliance Citrix ADC) du tunnel CloudBridge Connector. Par conséquent, vous n'avez pas besoin d'accéder à l'interface graphique de l'autre appliance Citrix ADC pour créer la configuration de tunnel correspondante du connecteur CloudBridge.

La configuration du tunnel CloudBridge Connector sur chacune des appliances Citrix ADC se compose des entités suivantes :

- **Profil IPsec**—Une entité de profil IPsec spécifie les paramètres du protocole IPSec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et PSK, à utiliser par le protocole IPSec dans le tunnel CloudBridge Connector.
- **Tunnel GRE**—Un tunnel IP spécifie l'adresse IP locale (une adresse SNIP publique configurée sur l'appliance Citrix ADC locale), l'adresse IP distante (une adresse SNIP publique configurée sur l'appliance Citrix ADC distante), le protocole (GRE) utilisé pour configurer le tunnel CloudBridge Connector et un protocole IPsec entité de profil.
- **Créez une règle PBR et associez-lui le tunnel IP** : une entité PBR spécifie un ensemble de conditions et une entité de tunnel IP. La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Vous devez définir la plage d'adresses IP source et la plage d'adresses IP de destination pour spécifier le sous-réseau dont le trafic doit traverser le tunnel CloudBridge Connector. Par exemple, considérez un paquet de requête qui provient d'un client sur le sous-réseau dans le premier centre de données et qui est destiné à un serveur sur le sous-réseau dans le second centre de données. Si ce paquet correspond à la plage d'adresses IP source et de destination de l'entité PBR sur l'appliance Citrix ADC dans le premier centre de données, il est envoyé à travers le tunnel CloudBridge Connector associé à l'entité PBR.

Pour créer un profil IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add ipsec profile <name> [-ikeVersion (V1 | V2)] [-encAlgo (AES | 3 DES)...] [-hashAlgo <hashAlgo\> ...] [-lifetime <positive_integer>] (-psk | (-publickey<string> -privatekey <string>-peerPublicKey <string >))[-livenessCheckInterval <positive_intege>][-replayWindowSize \< positive_integer>] [-ikeRetryInterval <positive_integer>] [-retransmissiontime <positive_integer>]`
- `show ipsec profile <name>`

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add ipTunnel <name> <remote><remoteSubnetMask> <local> [-protocol < protocol>] [-ipsecProfileName <string>]`
- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add ns pbr <pbr_name> ALLOW -srcIP = <local_subnet_range> -destIP = < remote_subnet_range> -ipTunnel <tunnel_name>`
- `apply ns pbrs`

- show ns pbr <pbr_name>

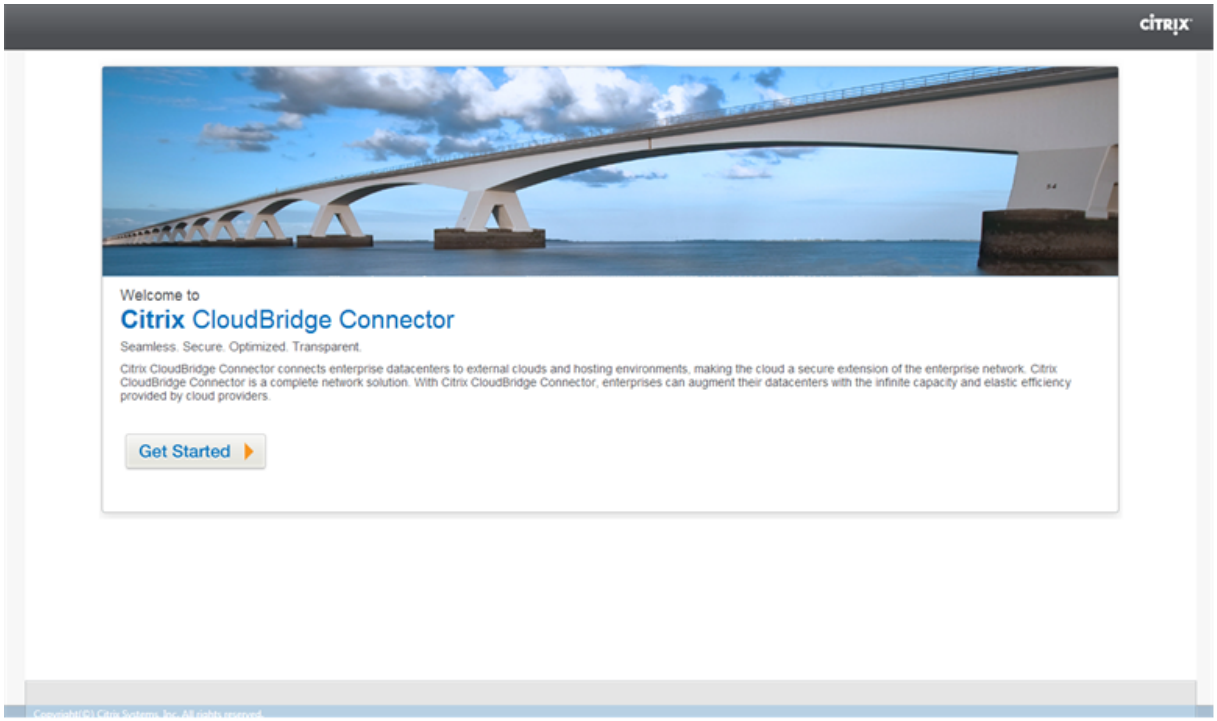
Exemple

```
1  add ipsec profile Cloud_Connector_DC1-DC2  -encAlgo AES -hashAlgo
       HMAC_SHA1
2      Done
3      > add ipTunnel Cloud_Connector_DC1-DC2 203.0.113.133
           255.255.255.255 198.51.100.15 -protocol GRE -ipsecProfileName
           Cloud_Connector_DC1-DC2
4
5      Done
6      > add ns pbr PBR-DC1-DC2 ALLOW -srcIP 198.51.100.15 -destIP
           203.0.113.133 ipTunnel Cloud_Connector_DC1-DC2
7
8      Done
9      > apply ns pbrs
10
11     Done
12 <!--NeedCopy-->
```

Pour configurer un tunnel CloudBridge Connector dans une appliance Citrix ADC à l'aide de l'interface graphique graphique

1. Tapez l'adresse NSIP d'une appliance Citrix ADC dans la ligne d'adresse d'un navigateur Web.
2. Connectez-vous à l'interface graphique de l'appliance Citrix ADC à l'aide de vos informations d'identification de compte pour l'appliance.
3. Accédez à **Système** > **CloudBridge Connector**.
4. Dans le volet droit, sous **Mise en route**, cliquez sur **Créer/surveiller CloudBridge**.

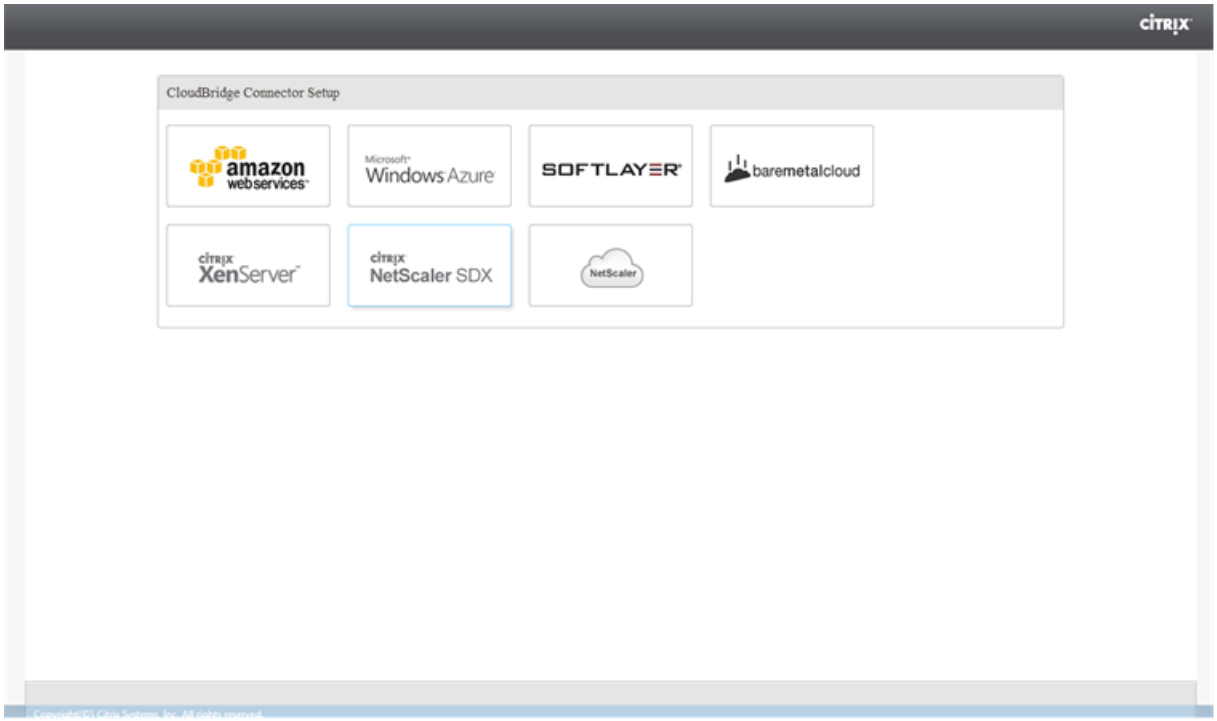
   La première fois que vous configurez un tunnel CloudBridge Connector sur l'appliance, un écran de **bienvenue** s'affiche.
5. Dans l'écran de **bienvenue**, cliquez sur **Démarrer**.



Remarque :

Si vous avez déjà un tunnel CloudBridge Connector configuré sur l'appliance Citrix ADC, l'écran d'accueil n'apparaît pas. Vous ne cliquez donc pas sur Démarrer.

1. Dans le volet **Configuration du connecteur CloudBridge**, cliquez sur **Citrix ADC**.



1. Dans le volet Citrix ADC, fournissez les informations d'identification de votre compte pour l'appliance Citrix ADC distante. Cliquez sur **Continuer**.
2. Dans le volet **Paramètres de CloudBridge Connector**, définissez le paramètre suivant :
   - **Nom du CloudBridge Connector** : nom de la configuration du CloudBridge Connector sur l'appliance locale. Doit commencer par un caractère alphabétique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), arobase (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois la configuration CloudBridge Connector créée.
3. Sous **Paramètres locaux**, définissez le paramètre suivant :
   - **IP du sous-réseau** : adresse IP du point de terminaison local du tunnel CloudBridge Connector.
4. Sous **Paramètres à distance**, définissez le paramètre suivant :
   - **IP du sous-réseau** : adresse IP du point de terminaison homologue du tunnel CloudBridge Connector.
5. Sous Paramètre **PBR**, définissez les paramètres suivants :
   - **Opération** : opérateur logique égal à (=) ou non égal à (!=).
   - **Source IP Low** —Adresse IP source la plus basse à correspondre à l'adresse IP source d'un paquet IPv4 sortant.
   - **Source IP High**—Adresse IP source la plus élevée à correspondre à l'adresse IP source d'un paquet IPv4 sortant.
   - **Opération** : opérateur logique égal à (=) ou non égal à (!=).
   - IP de destination Low* : adresse IP de destination la plus basse à correspondre à l'adresse IP de destination d'un paquet IPv4 sortant.
   - Adresse**IP de destination élevée** : adresse IP de destination la plus élevée à correspondre à l'adresse IP de destination d'un paquet IPv4 sortant.
6. (Facultatif) Sous **Paramètres de sécurité**, définissez les paramètres de protocole IPSec suivants pour le tunnel CloudBridge Connector :
   - **Algorithme**de chiffrement : algorithme de chiffrement à utiliser par le protocole IPSec dans le tunnel CloudBridge.
   - **Algorithme de hachage : algorithme**de hachage à utiliser par le protocole IPSec dans le tunnel CloudBridge.
   - **Key**—Sélectionnez l'une des méthodes d'authentification IPsec suivantes à utiliser par les deux homologues pour s'authentifier mutuellement.
     - **Auto Generate Key**—Authentification basée sur une chaîne de texte appelée clé pré-partagée (PSK), générée automatiquement par l'appliance locale. Les clés PSK des

pairs sont comparées les unes aux autres pour l'authentification.
- **Clé spécifique**—Authentification basée sur un PSK entré manuellement. Les PSK des pairs sont comparés les uns aux autres pour l'authentification.
  * Clé de sécurité pré-partagée : chaîne de texte saisie pour l'authentification basée sur la clé pré-partagée.
- **Charger les certificats**—Authentification basée sur les certificats numériques.
  * **Clé publique** : certificat numérique local à utiliser pour authentifier l'appliance Citrix ADC locale auprès de l'homologue avant d'établir des associations de sécurité IPsec. Le même certificat doit être présent et défini pour le paramètre Peer Public Key dans l'homologue.
  * **Clé privée** : clé privée du certificat numérique local.
  * **Clé publique homologue**— Certificat numérique de l'homologue. Utilisé pour authentifier l'homologue sur le point final local avant d'établir des associations de sécurité IPsec. Le même certificat doit être présent et défini pour le paramètre de clé publique dans l'homologue.

7. Cliquez sur **Terminé**.

La nouvelle configuration du tunnel CloudBridge Connector sur les deux appliances Citrix ADC apparaît sous l'onglet Accueil de l'interface graphique correspondante. L'état actuel du tunnel de connecteur CloudBridge est indiqué dans le volet Connecteurs CloudBridge configurés. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance Citrix ADC à l'aide des compteurs statistiques de tunnel CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques de tunnel CloudBridge Connector sur une appliance Citrix ADC, consultez Surveillance des tunnels de CloudBridge Connector.

Configuration de CloudBridge Connector entre le centre de données et le cloud AWS

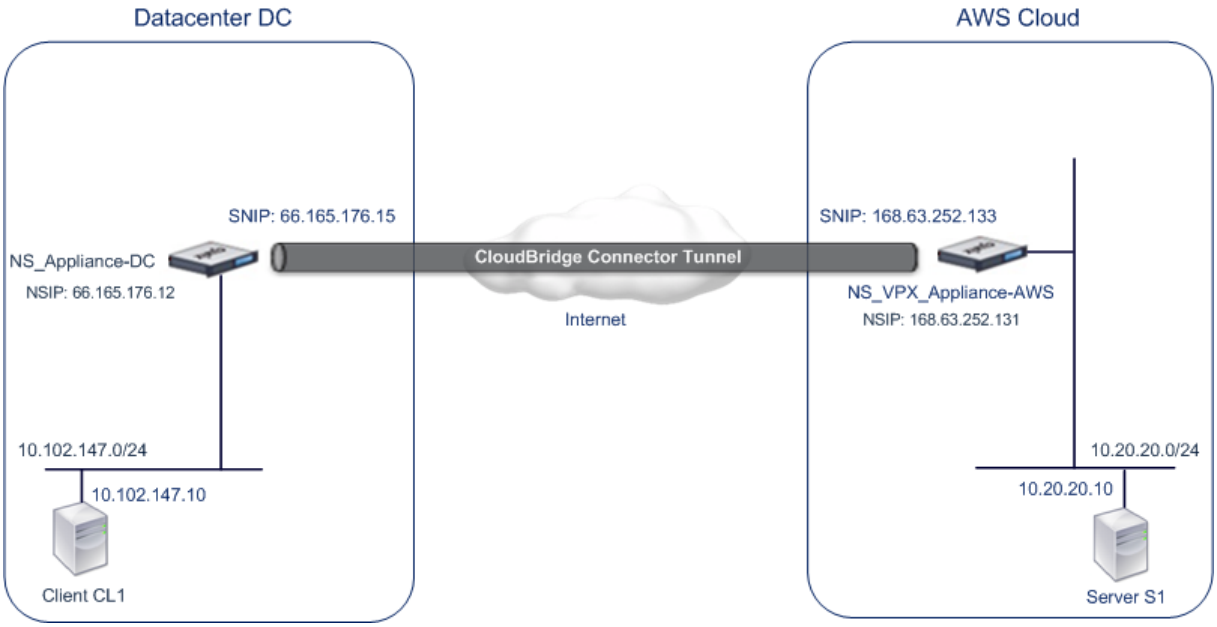
August 20, 2021

Vous pouvez configurer un tunnel CloudBridge Connector entre un centre de données et le cloud AWS pour tirer parti de l'infrastructure et des capacités informatiques du centre de données et du cloud AWS. Avec AWS, vous pouvez étendre votre réseau sans investissement initial ni coût de maintenance de l'infrastructure réseau étendue. Vous pouvez faire évoluer votre infrastructure vers le haut ou

vers le bas, selon vos besoins. Par exemple, vous pouvez louer davantage de fonctionnalités serveur lorsque la demande augmente.

Pour connecter un centre de données au cloud AWS, vous configurez un tunnel CloudBridge Connector entre une appliance Citrix ADC résidant dans le centre de données et une appliance virtuelle Citrix ADC (VPX) résidant dans le cloud AWS.

À titre d'illustration d'un tunnel CloudBridge Connector entre un centre de données et un nuage Amazon AWS, considérez un exemple dans lequel un tunnel CloudBridge Connector est configuré entre l'appliance Citrix ADC NS_Appliance-DC, dans le centre de données DC, et l'appliance virtuelle Citrix ADC (VPX) NS_VPX_Appliance-AWS.



NS_Appliance-DC et NS_VPX_Appliance-AWS fonctionnent en mode L3. Ils permettent la communication entre les réseaux privés dans le centre de données DC et le cloud AWS. NS_Appliance-DC et NS_VPX_Appliance-AWS permettent la communication entre le client CL1 dans le centre de données DC et le serveur S1 dans le cloud AWS via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

> **Remarque** :
>
> AWS ne prend pas en charge le mode L2, il est donc nécessaire que le mode L3 soit activé sur les deux points de terminaison.

Pour une communication correcte entre CL1 et S1, le mode L3 est activé sur NS_Appliance-DC et NS_VPX_Appliance-AWS et les routes sont mises à jour comme telles :

- CL1 ont une route vers NS_Appliance-DC pour atteindre S1.
- NS_Appliance-DC ont une route vers NS_VPX_Appliance-AWS pour atteindre S1.
- S1 doit avoir une route vers NS_VPX_Appliance-AWS pour atteindre CL1.

- NS_VPX_Appliance-AWS a une route vers NS_Appliance-DC pour atteindre CL1.

Le tableau suivant répertorie les paramètres de l'appliance Citrix ADC NS_Appliance-DC dans le contrôleur de domaine du centre de données.

Entité	Nom	Détails
Adresse NSIP		66.165.176.12
Adresse SNIP		66.165.176.15
Tunnel CloudBridge Connector	CC_Tunnel_DC-AWS	Adresse IP du point de terminaison local du tunnel CloudBridge Connector : 66.165.176.15, Adresse IP du point de terminaison distant du tunnel CloudBridge Connector : 168.63.252.133, Détails du tunnel GRE - Name= CC_Tunnel_DC-AWS

Le tableau suivant répertorie les paramètres sur Citrix ADC VPX NS_VPX_Appliance-AWS sur le cloud AWS.

Entité	Nom	Détails
Adresse du NSIP		10.102.25.30
Adresse EIP publique mappée à l'adresse NSIP		168.63.252.131
Adresse SNIP		10.102.29.30
Adresse EIP publique mappée à l'adresse SNIP		168.63.252.133

Entité	Nom	Détails
Tunnel CloudBridge Connector	CC_Tunnel_DC-AWS	Adresse IP du point de terminaison local du tunnel CloudBridge Connector :168.63.252.133, Adresse IP du point de terminaison distant du tunnel CloudBridge Connector : 66.165.176.15 ; **Détails du tunnel GRE** Nom = CC_Tunnel_DC-AWS, Détails du profil IPsec, Name= CC_Tunnel_DC-AWS, Algorithm= AES, HMAC SHA1

Conditions préalables

Avant de configurer un tunnel CloudBridge Connector, vérifiez que les tâches suivantes ont été effectuées :

1. Installez, configurez et lancez une instance de Citrix ADC Virtual Appliance (VPX) sur le cloud AWS. Pour obtenir des instructions sur l'installation de Citrix ADC VPX sur AWS, voir Déployer une instance Citrix ADC VPX sur AWS.
2. Déployez et configurez une appliance physique Citrix ADC ou Provisioning ez et configurez une appliance virtuelle Citrix ADC (VPX) sur une plate-forme de virtualisation du centre de données.
3. Assurez-vous que les adresses IP du point d'extrémité du tunnel CloudBridge Connector sont accessibles les unes aux autres.

Licence Citrix ADC VPX

Après le lancement de l'instance initiale, Citrix ADC VPX pour AWS nécessite une licence. Si vous apportez votre propre licence (BYOL), consultez le Guide de licences VPX à l' adresse suivante : http://support.citrix.com/article/CTX122426.

Vous devez :

1. Utilisez le portail de licences du site Web Citrix pour générer une licence valide.
2. Télécharger la licence sur l'instance.

S'il s'agit d'une instance de marketplace **payante**, vous n'avez pas besoin d'installer une licence. Le jeu de fonctionnalités et les performances corrects s'activent automatiquement.

Étapes de configuration

Pour configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC résidant dans un centre de données et une appliance virtuelle Citrix ADC (VPX) résidant dans le cloud AWS, utilisez l'interface graphique de l'appliance Citrix ADC.

Lorsque vous utilisez l'interface graphique, la configuration du tunnel CloudBridge Connector créée sur l'appliance Citrix ADC est automatiquement poussée vers l'autre point de terminaison ou homologue (Citrix ADC VPX sur AWS) du tunnel CloudBridge Connector. Par conséquent, vous n'avez pas besoin d'accéder à l'interface graphique (GUI) du Citrix ADC VPX sur AWS pour créer la configuration de tunnel correspondante de CloudBridge Connector sur elle.

La configuration du tunnel CloudBridge Connector sur les deux homologues (l'appliance Citrix ADC qui réside dans le centre de données et l'appliance virtuelle Citrix ADC (VPX) qui réside dans le cloud AWS) se compose des entités suivantes :

- **Profil IPsec**—Une entité de profil IPsec spécifie les paramètres du protocole IPSec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et PSK, à utiliser par le protocole IPSec dans les deux homologues du tunnel CloudBridge Connector.
- **Tunnel GRE**—Un tunnel IP spécifie une adresse IP locale (une adresse SNIP publique configurée sur l'homologue local), une adresse IP distante (une adresse SNIP publique configurée sur l'homologue distant), un protocole (GRE) utilisé pour configurer le tunnel CloudBridge Connector et une entité de profil IPSec.
- **Créez une règle PBR et associez-lui le tunnel IP** : une entité PBR spécifie un ensemble de conditions et une entité de tunnel IP. La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Vous devez définir la plage d'adresses IP source et la plage d'adresses IP de destination pour spécifier le sous-réseau dont le trafic doit traverser le tunnel CloudBridge Connector. Par exemple, considérez un paquet de requête qui provient d'un client sur le sous-réseau du centre de données et qui est destiné à un serveur sur le sous-réseau dans le cloud AWS. Si ce paquet correspond à la plage d'adresses IP source et de destination de l'entité PBR sur l'appliance Citrix ADC dans le centre de données, il est envoyé à travers le tunnel CloudBridge Connector associé à l'entité PBR.

Pour créer un profil IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add ipsec profile <name> [-**ikeVersion** (V1 | V2)] [-**encAlgo** (AES | 3DES)...] [-**hashAlgo** <hashAlgo> ...] [-**lifetime** <positive_integer>] (-**psk** | (-**publickey** <string> -**privatekey** <string> -**peerPublicKey** <string>))[-**livenessCheckInterval** <positive_integer>] [-**replayWindowSize** <positive_integer>] [-**ikeRetryInterval** <positive_integer>] [-**retransmissiontime** <positive_integer>]`

- **show ipsec profile** <name>

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- add ipTunnel <name> <remote><remoteSubnetMask> <local> [-protocol <protocol>] [-ipsecProfileName <string>]
- show ipTunnel <name>

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- add ns pbr <pbr_name> ALLOW -srcIP = <local_subnet_range> -destIP = <remote_subnet_range> -ipTunnel <tunnel_name>
- apply ns pbrs
- show ns pbr <pbr_name>

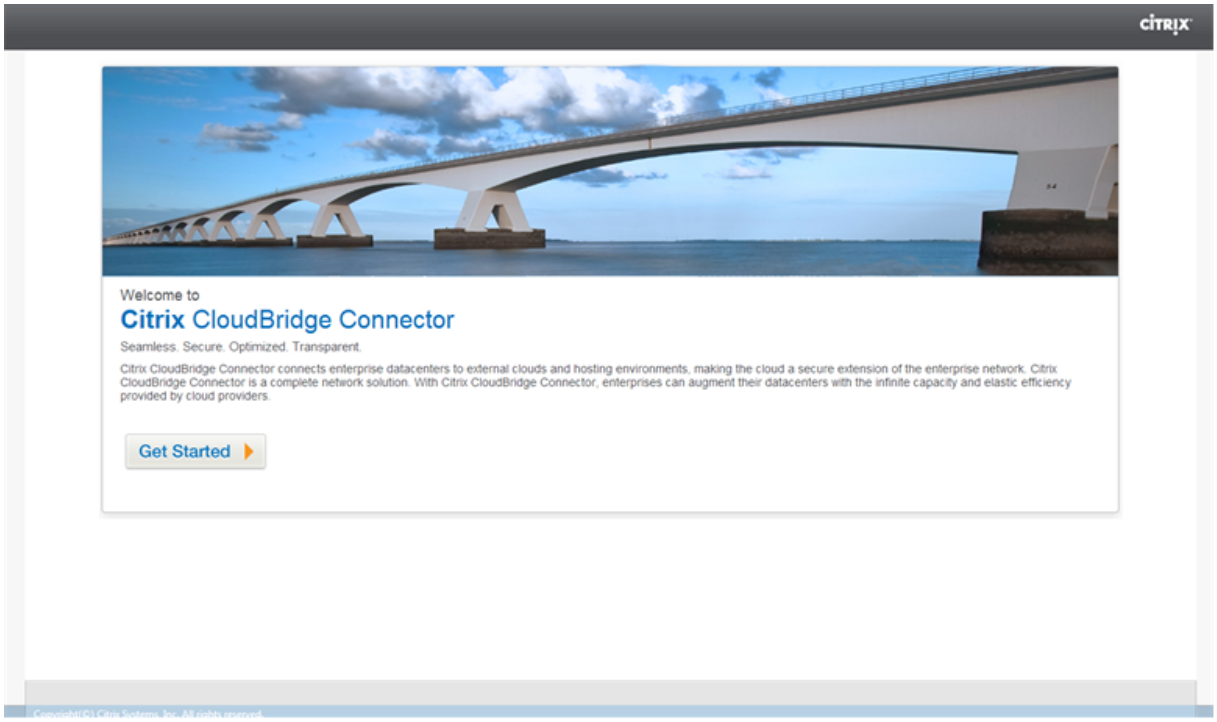
Exemple

```
1      > add ipsec profile CC_Tunnel_DC-AWS -encAlgo AES -hashAlgo
           HMAC_SHA1
2
3      Done
4      > add ipTunnel CC_Tunnel_DC-AWS 168.63.252.133 255.255.255.0
           66.165.176.15 - protocol GRE -ipsecProfileName CC_Tunnel_DC-AWS
5
6      Done
7      > add ns pbr PBR-DC-AWS ALLOW - srcIP 66.165.176.15 - destIP
           168.63.252.133 ipTunnel CC_Tunnel_DC-AWS
8
9      Done
10     > apply ns pbrs
11
12     Done
13 <!--NeedCopy-->
```

Pour configurer un tunnel CloudBridge Connector dans une appliance Citrix ADC à l'aide de l'interface graphique graphique

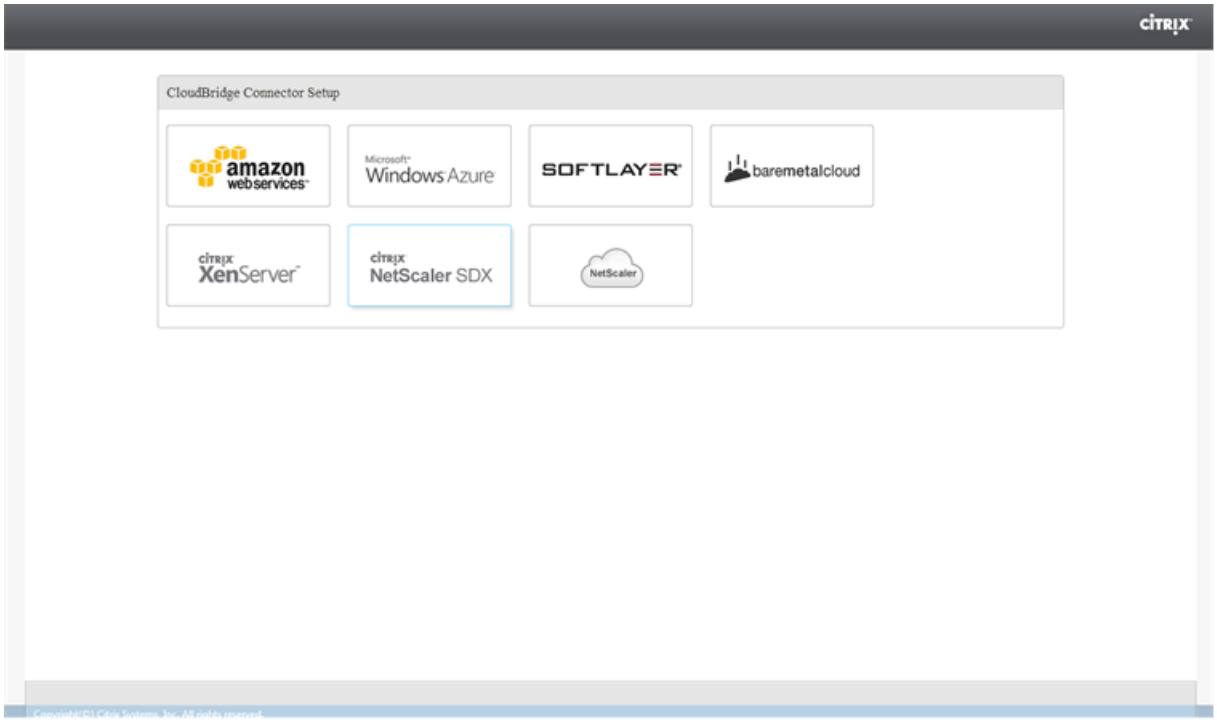
1. Tapez l'adresse NSIP d'une appliance Citrix ADC dans la ligne d'adresse d'un navigateur Web.
2. Connectez-vous à l'interface graphique de l'appliance Citrix ADC à l'aide de vos informations d'identification de compte pour l'appliance.
3. Accédez à **Système** > **CloudBridge Connector**.
4. Dans le volet droit, sous **Mise en route**, cliquez sur **Créer/surveiller CloudBridge**.

5. La première fois que vous configurez un tunnel CloudBridge Connector sur l'appliance, un écran de **bienvenue** s'affiche.
6. Dans l'écran de **bienvenue**, cliquez sur **Démarrer**.



> **Remarque** :
>
> Si vous avez déjà un tunnel CloudBridge Connector configuré sur l'appliance Citrix ADC, l'écran d'accueil n'apparaît pas. Vous ne cliquez donc pas sur Démarrer.

1. Dans le volet **Configuration de CloudBridge Connector**, cliquez sur **Amazon Web services**



1. Dans le volet **Amazon**, indiquez vos informations d'identification de compte AWS : ID de clé d'accès AWS et clé d'accès secrète AWS. Vous pouvez obtenir ces clés d'accès à partir de la console AWS GUI. Cliquez sur **Continuer**.

> **Remarque**
>
> Auparavant, l'assistant d'installation se connecte toujours à la même région AWS, même si une autre région est sélectionnée. Par conséquent, la configuration du tunnel CloudBridge Connector vers un Citrix ADC VPX exécuté sur la région AWS sélectionnée échouait. Ce problème a été résolu maintenant.

1. Dans le volet **Citrix ADC**, sélectionnez l'adresse NSIP de l'appliance virtuelle Citrix ADC exécutée sur AWS. Ensuite, fournissez vos informations d'identification de compte pour l'appliance virtuelle Citrix ADC. Cliquez sur **Continuer**.
2. Dans le volet **Paramètres de CloudBridge Connector**, définissez le paramètre suivant :
   - **Nom du CloudBridge Connector** : nom de la configuration du CloudBridge Connector sur l'appliance locale. Doit commencer par un caractère alphabétique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), arobase (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois la configuration CloudBridge Connector créée.
3. Sous **Paramètres locaux**, définissez le paramètre suivant :
   - **IP du sous-réseau** : adresse IP du point de terminaison local du tunnel CloudBridge Con-

nector. Doit être une adresse IP publique de type SNIP.

4. Sous **Paramètres à distance**, définissez le paramètre suivant :

   - **IP du sous-réseau** : adresse IP du point d'extrémité du tunnel CloudBridge Connector côté AWS. Doit être une adresse IP de type SNIP sur l'instance Citrix ADC VPX sur AWS.
   - **NAT**—Adresse IP publique (EIP) dans AWS qui est mappée au SNIP configuré sur l'instance Citrix ADC VPX sur AWS.

5. Sous **Réglage PBR**, définissez les paramètres suivants :

   - **Opération** : opérateur logique égal à (=) ou non égal à (!=).
   - **Source IP Low**—Adresse IP source la plus basse à correspondre à l'adresse IP source d'un paquet IPv4 sortant.
   - **Source IP High**—Adresse IP source la plus élevée à correspondre à l'adresse IP source d'un paquet IPv4 sortant.
   - **Opération** : opérateur logique égal à (=) ou non égal à (!=).
   - **IP de destination Low**—Adresse IP de destination la plus basse à correspondre à l'adresse IP de destination d'un paquet IPv4 sortant.
   - Adresse**IP de destination élevée** : adresse IP de destination la plus élevée à correspondre à l'adresse IP de destination d'un paquet IPv4 sortant.

6. (Facultatif) Sous **Paramètres de sécurité**, définissez les paramètres de protocole IPSec suivants pour le tunnel CloudBridge Connector :

   - **Algorithme**de chiffrement : algorithme de chiffrement à utiliser par le protocole IPSec dans le tunnel CloudBridge.
   - **Algorithme de hachage : algorithme**de hachage à utiliser par le protocole IPSec dans le tunnel CloudBridge.
   - **Clé** : sélectionnez l'une des méthodes d'authentification IPsec suivantes à utiliser par les deux homologues pour s'authentifier mutuellement.
     - **Génération automatique de la clé** : authentification basée sur une chaîne de texte appelée clé pré-partagée (PSK), générée automatiquement par l'appliance locale. Les clés PSK des pairs sont comparées les unes aux autres pour l'authentification.
     - **Clé spécifique**—Authentification basée sur un PSK entré manuellement. Les PSK des pairs sont comparés les uns aux autres pour l'authentification.
       * **Clé de sécurité pré-partagée** : chaîne de texte saisie pour l'authentification basée sur la clé pré-partagée.
     - **Charger les certificats**—Authentification basée sur les certificats numériques.
       * **Clé publique** : certificat numérique local à utiliser pour authentifier l'homologue local auprès de l'homologue distant avant d'établir des associations de sécurité IPsec. Le même certificat doit être présent et défini pour le paramètre Peer Public Key dans l'homologue.

* **Clé privée** : clé privée du certificat numérique local.
* **Clé publique homologue**— Certificat numérique de l'homologue. Utilisé pour authentifier l'homologue sur le point final local avant d'établir des associations de sécurité IPsec. Le même certificat doit être présent et défini pour le paramètre de clé publique dans l'homologue.

7. Cliquez sur **Terminé**.

La nouvelle configuration du tunnel CloudBridge Connector sur l'appliance Citrix ADC dans le centre de données apparaît sous l'onglet Accueil de l'interface graphique. La nouvelle configuration de tunnel CloudBridge Connector correspondante sur l'appliance Citrix ADC VPX dans le cloud AWS apparaît sur l'interface graphique. L'état actuel du tunnel de connecteur CloudBridge est indiqué dans le volet CloudBridge configuré. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance Citrix ADC à l'aide des compteurs statistiques de tunnel CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques de tunnel CloudBridge Connector sur une appliance Citrix ADC, consultez Surveillance des tunnels de CloudBridge Connector.

Configuration d'un tunnel CloudBridge Connector entre une appliance Citrix ADC et une Gateway privée virtuelle sur AWS

October 4, 2021

Pour connecter un centre de données à Amazon Web Services (AWS), vous pouvez configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC dans le centre de données et une Gateway privée virtuelle sur AWS. L'appliance Citrix ADC et la Gateway privée virtuelle forment les points de terminaison du tunnel CloudBridge Connector et sont appelés homologues.

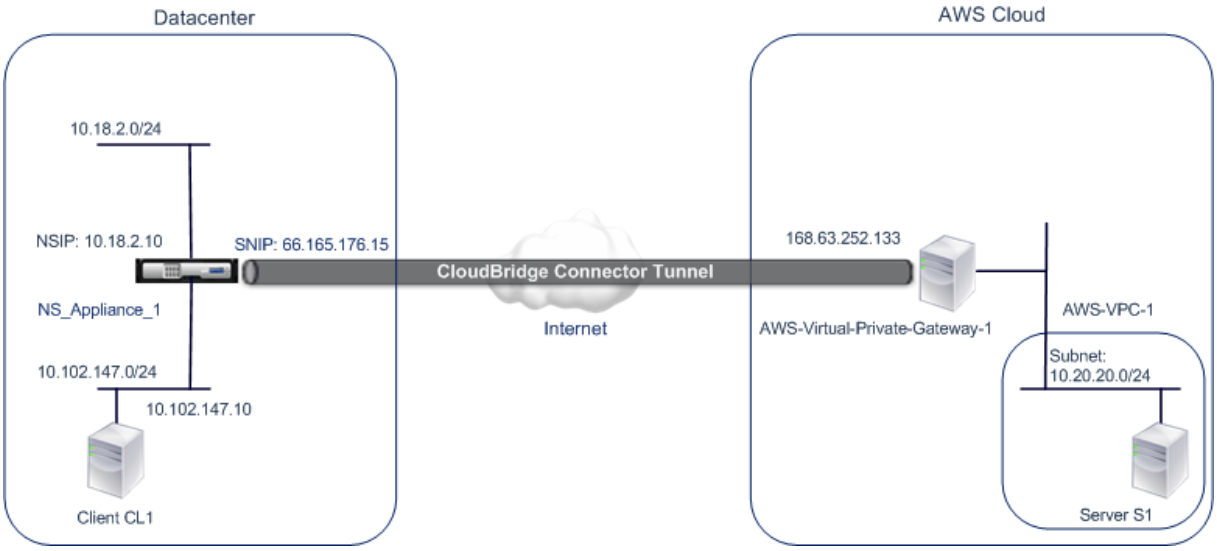
> **Remarque :**
>
> Vous pouvez également configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC dans un centre de données et une instance Citrix ADC VPX (au lieu d'une Gateway privée virtuelle) sur AWS. Pour plus d'informations, consultez Configuration de CloudBridge Connector entre Datacenter et AWS Cloud.

Les passerelles privées virtuelles sur AWS prennent en charge les paramètres IPsec suivants pour un tunnel CloudBridge Connector. Par conséquent, vous devez spécifier les mêmes paramètres IPSec lorsque vous configurez l'appliance Citrix ADC pour le tunnel CloudBridge Connector.

Propriétés IPSec	Paramètre
Mode IPsec	Mode tunnel
Version IKE	Version 1
Méthode d'authentification IKE	Clé pré-partagée
Algorithme de chiffrement	AES
Algorithme de hachage	HMAC SHA1

Exemple de configuration du tunnel CloudBridge Connector et de flux de données

À titre d'illustration du flux de trafic dans un tunnel CloudBridge Connector, considérez un exemple dans lequel un tunnel CloudBridge Connector est configuré entre l'appliance Citrix ADC NS_Appliance-1 dans un centre de données et la Gateway de Gateway privée virtuelle AWS-Virtual-Private-Gateway-1 sur le cloud AWS.



NS_Appliance-1 fonctionne également en tant que routeur L3, ce qui permet à un réseau privé du centre de données d'atteindre un réseau privé dans le cloud AWS via le tunnel CloudBridge Connector. En tant que routeur, NS_Appliance-1 permet la communication entre le client CL1 dans le centre de données et le serveur S1 dans le cloud AWS via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel du Connecteur CloudBridge inclut une entité de profil IPSec nommée NS_AWS_IPSEC_profile, une entité de tunnel du Connecteur CloudBridge nommée NS_AWS_Tunnel et une entité de routage basée sur des stratégies (PBR) nommée NS_AWS_PBR.

L'entité de profil IPSec NS_AWS_IPSEC_profile spécifie les paramètres de protocole IPSec, tels que la version IKE, l'algorithme de chiffrement et l'algorithme de hachage, à utiliser par le protocole

IPSec dans le tunnel CloudBridge Connector. NS_AWS_IPSEC_profile est lié à l'entité de tunnel IP NS_AWS_Tunnel.

L'entité tunnel CloudBridge Connector NS_AWS_Tunnel spécifie l'adresse IP locale (une adresse IP publique configurée sur l'appliance Citrix ADC), l'adresse IP distante (l'adresse IP de la passerelle AWS-Virtual-Private-Gateway-1) et le protocole (IPsec) utilisé pour configurer le tunnel CloudBridge Connector. NS_AWS_Tunnel est lié à l'entité de routage basée sur la stratégie (PBR) NS_AWS_PBR.

L'entité PBR NS_AWS_PBR spécifie un ensemble de conditions et une entité tunnel CloudBridge Connector (NS_AWS_Tunnel). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de NS_AWS_PBR. La plage d'adresses IP source et la plage d'adresses IP de destination sont spécifiées en tant que sous-réseau dans le centre de données et sous-réseau dans le cloud AWS, respectivement. Tout paquet de requête provenant d'un client dans le sous-réseau du centre de données et destiné à un serveur dans le sous-réseau sur le cloud AWS correspond aux conditions de NS_AWS_PBR. Ce paquet est alors considéré pour le traitement de CloudBridge Connector et est envoyé à travers le tunnel CloudBridge Connector (NS_AWS_Tunnel) lié à l'entité PBR.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Adresse IP du point d'extrémité du tunnel CloudBridge Connector (NS_Appliance-1) côté centre de données	66.165.176.15
Adresse IP du point d'extrémité du tunnel CloudBridge Connector (AWS-Virtual-Private-Gateway-1) dans AWS	168.63.252.133
Sous-réseau de centres de données, dont le trafic doit traverser le tunnel CloudBridge Connector	10.102.147.0/24
Sous-réseau AWS, dont le trafic doit traverser le tunnel CloudBridge Connector	10.20.20.0/24

Paramètres sur Amazon AWS

Passerelle client	AWS-Customer-Gateway-1	Routage = statique, adresse IP = adresse IP du point de terminaison du tunnel CloudBridge Connector routable sur Internet Adresse IP du côté Citrix ADC = 66.165.176.15
Passerelle privée virtuelle	AWS-Virtual-Private-Gateway-1	VPC associé = AWS-VPC-1
Connexion VPN	AWS-VPN-Connection-1	Passerelle client = AWS-Customer-Gateway-1, Virtual Private Gateway = Virtual-Private-Gateway-1, Options de routage : Type = Statique, Static IP Prefixes = Sous-réseaux côté Citrix ADC = 10.102.147.0/24

Paramètres de l'appliance Citrix ADC NS_Appliance-1 dans Datacenter-1 :

Appliance	Paramètres	
SNIP1 (à titre de référence uniquement)	66.165.176.15	
Profil IPSec	NS_AWS_IPSEC_PROFILE	Version IKE = v1, Algorithme de chiffrement = AES, Algorithme de hachage = HMAC SHA1
Tunnel du connecteur CloudBridge NS_AWS_Tunnel	IP distante = 168.63.252.133, IP locale = 66.165.176.15, Protocole de tunnel = IPsec, IPSec, protocole IPSec, IPSec, IPSec, IPSec profile= NS_Profile= NS_IPSEC	

Appliance	Paramètres	
Basé sur une stratégie Route	NS_AWS_PBR	Plage IP source = Sous-réseau dans le centre de données =10.102.147.0-10.102.147.255, Plage IP de destination =Sous-réseau dans AWS =10.20.20.0-10.20.20.255, Tunnel IP = NS_AWS_Tunnel

Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et une Gateway AWS, tenez compte des points suivants :

1. AWS prend en charge les paramètres IPsec suivants pour un tunnel CloudBridge Connector. Par conséquent, vous devez spécifier les mêmes paramètres IPSec lorsque vous configurez l'appliance Citrix ADC pour le tunnel CloudBridge Connector.
   - Version IKE = v1
   - Algorithme de chiffrement = AES
   - Algorithme de hachage = HMAC SHA1
2. Vous devez configurer le pare-feu à l'extrémité Citrix ADC pour autoriser ce qui suit.
   - Tous les paquets UDP pour le port 500
   - Tous les paquets UDP pour le port 4500
   - Tous les paquets ESP (numéro de protocole IP 50)
3. Vous devez configurer Amazon AWS avant de spécifier la configuration du tunnel sur Citrix ADC, car l'adresse IP publique de l'extrémité AWS (Gateway) du tunnel et du PSK sont automatiquement générées lorsque vous configurez la configuration du tunnel dans AWS. Vous avez besoin de ces informations pour spécifier la configuration du tunnel sur l'appliance Citrix ADC.
4. AWS Gateway prend en charge les routes statiques et le protocole BGP pour les mises à jour d'itinéraire. L'appliance Citrix ADC ne prend pas en charge le protocole BGP dans un tunnel CloudBridge Connector vers la Gateway AWS. Par conséquent, des routes statiques appropriées doivent être utilisées des deux côtés du tunnel CloudBridge Connector pour acheminer correctement le trafic à travers le tunnel.

Configuration d'Amazon AWS pour le tunnel CloudBridge Connector

Pour créer une configuration de tunnel CloudBridge Connector sur Amazon AWS, utilisez Amazon AWS Management Console, une interface graphique Web permettant de créer et de gérer des ressources sur Amazon AWS.

Avant de commencer la configuration du tunnel CloudBridge Connector sur le cloud AWS, assurez-vous que :

- Vous disposez d'un compte d'utilisateur pour le cloud Amazon AWS.
- Vous disposez d'un cloud privé virtuel dont vous souhaitez vous connecter aux réseaux du côté Citrix ADC via le tunnel CloudBridge Connector.
- Vous êtes familier avec Amazon AWS Management Console.

> **Remarque** :
>
> Les procédures de configuration d'Amazon AWS pour un tunnel CloudBridge Connector peuvent changer au fil du temps, en fonction du cycle de publication Amazon AWS. Citrix vous recommande de consulter la documentation Amazon AWS pour connaître les dernières procédures.

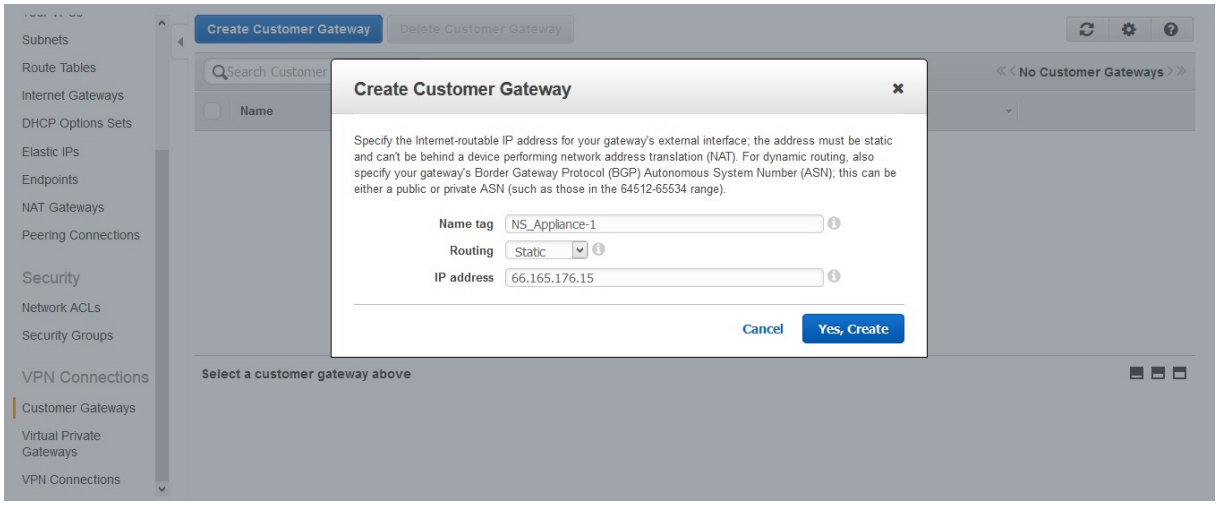
Pour configurer un tunnel de connecteur CloudBridge entre un Citrix ADC et une Gateway AWS, effectuez les tâches suivantes sur AWS Management Console :

- **Créez une passerelle client**. Une Gateway client est une entité AWS qui représente un point de terminaison de tunnel CloudBridge Connector. Pour un tunnel CloudBridge Connector entre une appliance Citrix ADC et une Gateway AWS, la Gateway client représente l'appliance Citrix ADC sur AWS. La Gateway client spécifie un nom, le type de routage (statique ou BGP) utilisé dans le tunnel et l'adresse IP du point de terminaison du tunnel CloudBridge Connector côté Citrix ADC. L'adresse IP peut être une adresse SNIP de sous-réseau appartenant à Citrix ADC routable sur Internet ou, si l'appliance Citrix ADC se trouve derrière un périphérique NAT, une adresse IP NAT routable sur Internet qui représente l'adresse SNIP.
- **Créez une passerelle privée virtuelle et connectez-la à un VPC**. Une Gateway privée virtuelle est un point de terminaison de tunnel CloudBridge Connector côté AWS. Lorsque vous créez une Gateway privée virtuelle, vous lui avez attribué un nom ou autorisez AWS à lui attribuer le nom. Vous associez ensuite la Gateway privée virtuelle à un VPC. Cette association permet aux sous-réseaux du VPC de se connecter aux sous-réseaux du côté Citrix ADC via le tunnel CloudBridge Connector.
- **Créez une connexion VPN**. Une connexion VPN spécifie une Gateway client et une Gateway privée virtuelle entre lesquelles un tunnel CloudBridge Connector doit être créé. Il spécifie également un préfixe IP pour les réseaux du côté Citrix ADC. Seuls les préfixes IP connus de la Gateway privée virtuelle (via une entrée de route statique) peuvent recevoir du trafic du VPC via le tunnel. En outre, la Gateway privée virtuelle n'acheminera aucun trafic non destiné aux préfixes IP spécifiés via le tunnel. Après avoir configuré une connexion VPN, vous devrez peut-être attendre quelques minutes pour qu'elle soit créée.

- **Configurer les options de routage**. Pour que le réseau du VPC atteigne les réseaux du côté Citrix ADC via le tunnel CloudBridge Connector, vous devez configurer la table de routage du VPC de manière à inclure des routes pour les réseaux du côté Citrix ADC et pointer ces routes vers la Gateway privée virtuelle. Vous pouvez inclure des routes dans la table de routage d'un VPC de l'une des manières suivantes :
  - **Activer la propagation des itinéraires**. Vous pouvez activer la propagation d'itinéraire pour votre table de routage, de sorte que les itinéraires soient automatiquement propagés vers la table. Les préfixes IP statiques que vous spécifiez pour la configuration VPN sont propagés à la table de routage après avoir créé la connexion VPN.
  - **Entrez manuellement des itinéraires statiques**. Si vous n'activez pas la propagation d'itinéraire, vous devez saisir manuellement les routes statiques des réseaux côté Citrix ADC.
- **Télécharger la configuration**. Une fois la configuration du tunnel CloudBridge Connector (connexion VPN) créée sur AWS, téléchargez le fichier de configuration de la connexion VPN sur votre système local. Vous pouvez avoir besoin des informations contenues dans le fichier de configuration pour configurer le tunnel CloudBridge Connector sur l'appliance Citrix ADC.

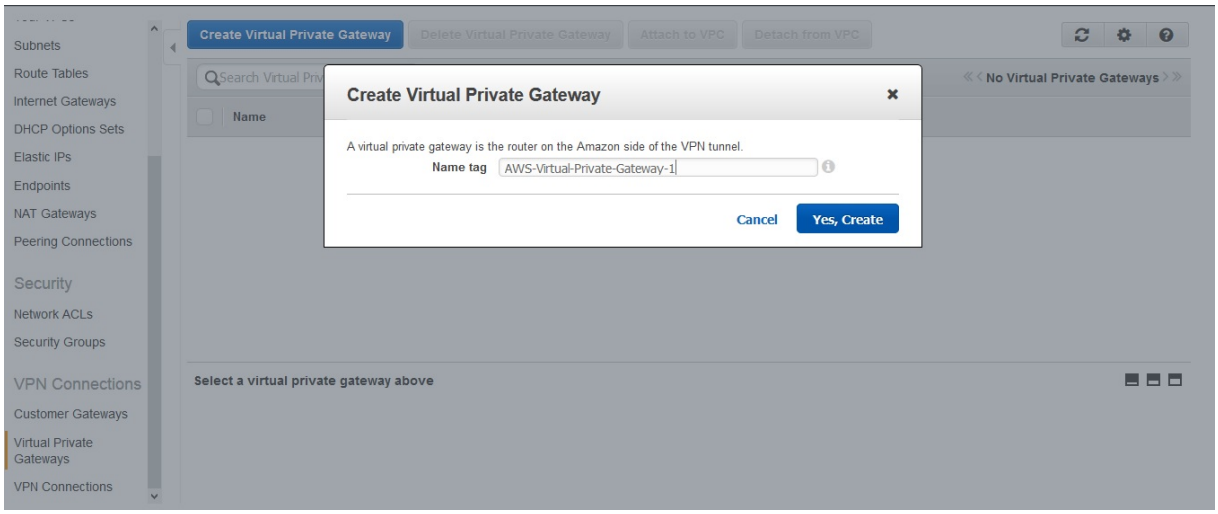
Pour créer une Gateway client

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Accédez à **Connexions VPN** > **Passerelles client** et cliquez sur **Créer une passerelle client** .
3. Dans la boîte de dialogue **Créer une passerelle client**, définissez les paramètres suivants, puis cliquez sur **Oui, Créer** :
   - **Étiquette de nom**. Nom de la Gateway client.
   - **Liste de routage**. Type de routage entre l'appliance Citrix ADC et la Gateway privée virtuelle AWS pour les routes publicitaires entre elles via le tunnel CloudBridge Connector. Sélectionnez **Gamme statique** dans la liste **Gamme** . **Remarque** : l'appliance Citrix ADC ne prend pas en charge le protocole BGP dans un tunnel CloudBridge Connector vers la Gateway AWS. Par conséquent, des routes statiques appropriées doivent être utilisées des deux côtés du tunnel CloudBridge Connector pour acheminer correctement le trafic à travers le tunnel.
   - **Adresse IP**. Adresse IP du point de terminaison du tunnel CloudBridge Connector routable sur Internet du côté Citrix ADC. L'adresse IP peut être une adresse SNIP de sous-réseau appartenant à Citrix ADC routable sur Internet ou, si l'appliance Citrix ADC se trouve derrière un périphérique NAT, une adresse IP NAT routable sur Internet qui représente l'adresse SNIP.

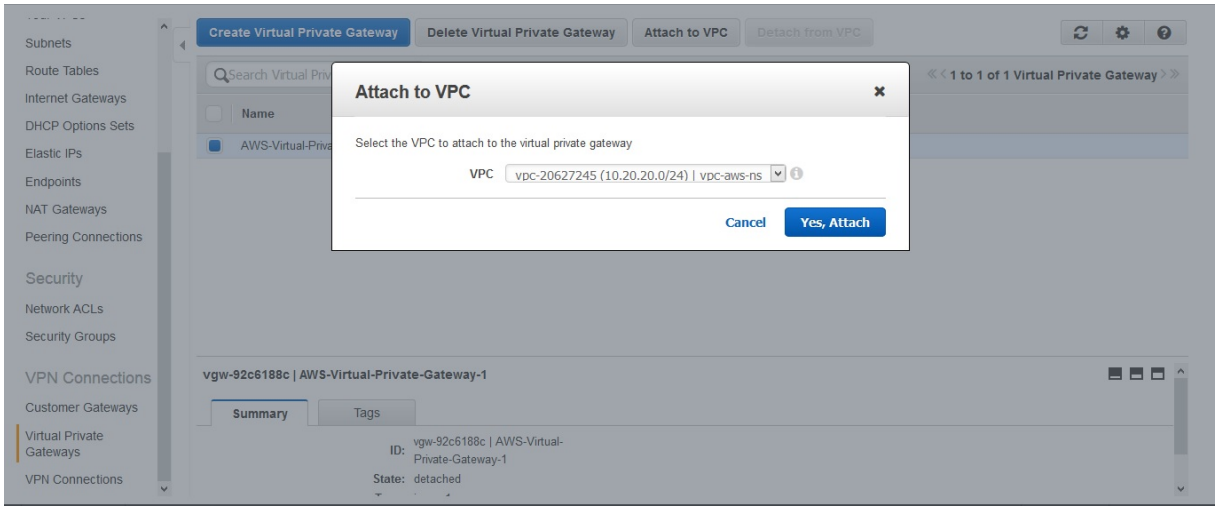


Pour créer une Gateway privée virtuelle et l'attacher à un VPC

1. Accédez à **Connexions VPN** > **Virtual Private Gateways**, puis cliquez sur Créer Virtual Private Gateway.
2. Entrez un nom pour la Gateway privée virtuelle, puis cliquez sur Oui, Créer.

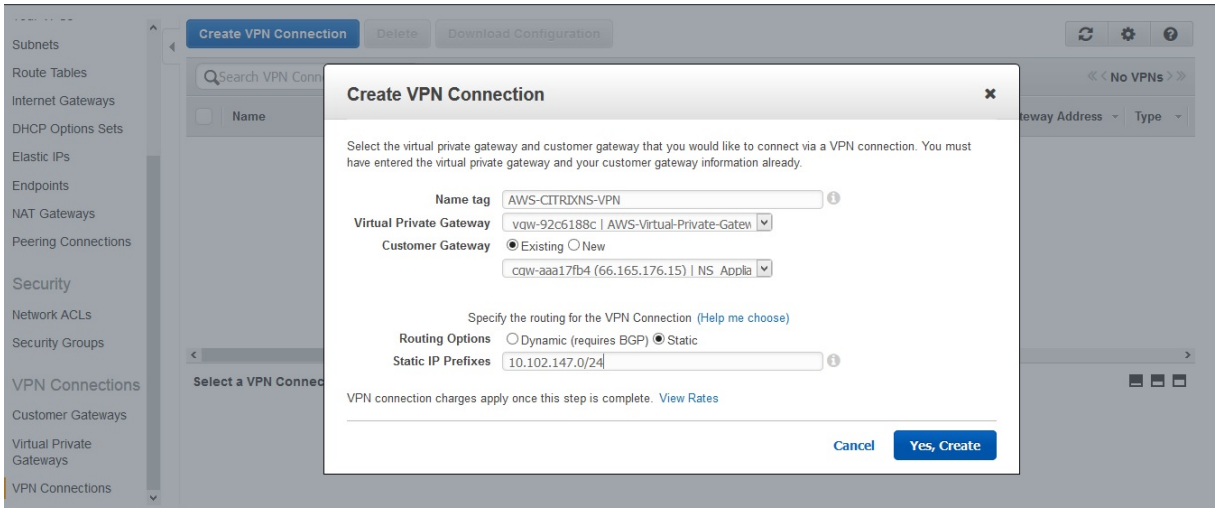


1. Sélectionnez la Gateway privée virtuelle que vous avez créée, puis cliquez sur Attacher au VPC.
2. Dans la boîte de dialogue Attacher au VPC, sélectionnez votre VPC dans la liste, puis choisissez Oui, Attacher.



Pour créer une connexion VPN :

1. Accédez à Connexions VPN > Connexions VPN, puis cliquez sur Créer une connexion VPN.
2. Dans la boîte de dialogue Créer une connexion VPN, définissez les paramètres suivants, puis choisissez Oui, Créer :
   - **Étiquette de nom**. Nom de la connexion VPN.
   - **Passerelle privée virtuelle**. Sélectionnez la Gateway privée virtuelle que vous avez créée précédemment.
   - **Passerelle client**. Sélectionnez Existant. Ensuite, dans la liste déroulante, sélectionnez la Gateway client que vous avez créée précédemment.
   - **Options de routage**. Type de routage entre la Gateway privée virtuelle et la Gateway client (appliance Citrix ADC). Sélectionnez Statique. Dans le champ Static IP Prefixes, spécifiez les préfixes IP du sous-réseau côté Citrix ADC, séparés par des virgules.



Pour activer la propagation des itinéraires :

1. Accédez à **Tables** de routage et sélectionnez la table de routage associée au sous-réseau dont

le trafic doit traverser le tunnel CloudBridge Connector.

> **Remarque**
>
> Par défaut, il s'agit de la table de routage principale du VPC.

1. Sous l'onglet **Propagation d'itinéraire** dans le volet d'informations, choisissez **Modifier**, sélectionnez la Gateway privée virtuelle, puis choisissez **Enregistrer**.

Pour saisir manuellement des itinéraires statiques :

1. Accédez à **Tables de routage** et sélectionnez votre table de routage.
2. Sous l'onglet **Itinéraires**, cliquez sur **Modifier**.
3. Dans le champ **Destination**, entrez l'itinéraire statique utilisé par votre tunnel CloudBridge Connector (connexion VPN).
4. Sélectionnez l'ID de Gateway privée virtuelle dans la liste **Target**, puis cliquez sur **Enregistrer**.

Pour télécharger le fichier de configuration :

1. Accédez à **Connexion VPN**, sélectionnez une connexion VPN, puis cliquez sur **Télécharger la configuration**.
2. Dans la boîte **de dialogue Configuration du téléchargement**, définissez les paramètres suivants, puis cliquez sur **Oui, Télécharger**.
   - **Vendeur**. Sélectionnez **Générique**.
   - **Plateforme**. Sélectionnez **Générique**.
   - **Logiciel**. Sélectionnez **Agnostic du fournisseur**.

Configuration de l'appliance Citrix ADC pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et une Gateway privée virtuelle sur le cloud AWS, effectuez les tâches suivantes sur l'appliance Citrix ADC.
Vous pouvez utiliser la ligne de commande Citrix ADC ou l'interface graphique.

- **Créez un profil IPSec**. Une entité de profil IPsec spécifie les paramètres du protocole IPSec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et PSK à utiliser par le protocole IPSec dans le tunnel CloudBridge Connector.
- **Créez un tunnel IP qui utilise le protocole IPSec et associez le profil IPSec à celui-ci**. Un tunnel IP spécifie l'adresse IP locale (une adresse SNIP configurée sur l'appliance Citrix ADC), l'adresse IP distante (l'adresse IP publique de la Gateway privée virtuelle dans AWS), le protocole (IPsec) utilisé pour configurer le tunnel CloudBridge Connector et une entité de profil IPsec. L'entité de tunnel IP créée est également appelée entité de tunnel CloudBridge Connector.
- **Créez une règle PBR et associez-la au tunnel IP**. Une entité PBR spécifie un ensemble de règles et une entité tunnel IP (tunnel CloudBridge Connector). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Définissez la plage d'adresses

IP source pour spécifier le sous-réseau Citrix côté ADC dont le trafic doit traverser le tunnel, et définissez la plage d'adresses IP de destination pour spécifier le sous-réseau AWS VPC dont le trafic doit traverser le tunnel CloudBridge Connector. Tout paquet de requête qui provient d'un client dans le sous-réseau du côté Citrix ADC et qui est destiné à un serveur dans le sous-réseau cloud AWS, et qui correspond à la plage d'adresses IP source et de destination de l'entité PBR, est envoyé à travers le tunnel CloudBridge Connector associé à l'entité PBR.

Pour créer un profil IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commande, tapez :

- `add ipsec profile <name> -psk <string> -**ikeVersion** v1`
- `show ipsec profile** <name>`

Pour créer un tunnel IPSEC et lier le profil IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commande, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commande, tapez :

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP** <subnet-range> -*ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Les commandes suivantes créent tous les paramètres du dispositif Citrix ADC NS_Appliance-1 utilisé dans "Exemple de configuration et de flux de données CloudBridge Connector."

```
1     > add ipsec profile NS_AWS_IPSec_Profile -psk
          DkiMgMdcbqvYREEuIvxsbKkW0Foyabcd -ikeVersion v1 - lifetime
          31536000
2     Done
3     > add iptunnel NS_AWS_Tunnel 168.63.252.133 255.255.255.255
          66.165.176.15 - protocol IPSEC - ipsecProfileName
          NS_AWS_IPSec_Profile
4
5     Done
6     > add pbr NS_AWS_Pbr -srcIP 10.102.147.0-10.102.147.255 - destIP
          10.20.0.0-10.20.255.255 - ipTunnel NS_AWS_Tunnel
7     Done
8
9     > apply pbrs
```



```
10
11      Done
12  <!--NeedCopy-->
```

Pour créer un profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > **Profil IPsec**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un profil IPsec**, définissez les paramètres suivants :
   - Nom
   - Algorithme de chiffrement
   - Algorithme de hachage
   - Version du protocole IKE (sélectionnez V1)
4. Sélectionnez la méthode **d'authentification de clé pré-partagée** et définissez le paramètre **Clé pré-partagée existe** .
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et lier le profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.
2. Dans l'onglet **Tunnels IPv4**, cliquez sur Ajouter.
3. Dans la boîte de dialogue **Ajouter un tunnel IP**, définissez les paramètres suivants :
   - Nom
   - IP distante
   - Masque distant
   - Type IP local (dans la liste déroulante Type IP local, sélectionnez IP du sous-réseau).
   - IP locale (Toutes les adresses IP configurées du type d'IP sélectionné se trouvent dans la liste déroulante IP locale. Sélectionnez l'adresse IP souhaitée dans la liste.)
   - Protocole
   - Profil IPsec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer PBR**, définissez les paramètres suivants :
   - Nom
   - Action

- Type de saut suivant (Select IP Tunnel)
- Nom du tunnel IP
- IP source Faible
- IP source élevée
- IP de destination faible
- IP de destination élevée

4. Cliquez sur **Créer**, puis sur **Fermer**.

La nouvelle configuration de tunnel CloudBridge Connector correspondante sur l'appliance Citrix ADC apparaît dans l'interface graphique.

L'état actuel du tunnel de connecteur CloudBridge est affiché dans le volet CloudBridge Connector configuré. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance Citrix ADC à l'aide des compteurs statistiques de tunnel CloudBridge Connector.
Pour plus d'informations sur l'affichage des statistiques de tunnel CloudBridge Connector sur une appliance Citrix ADC, consultez Surveillance des tunnels de CloudBridge Connector.

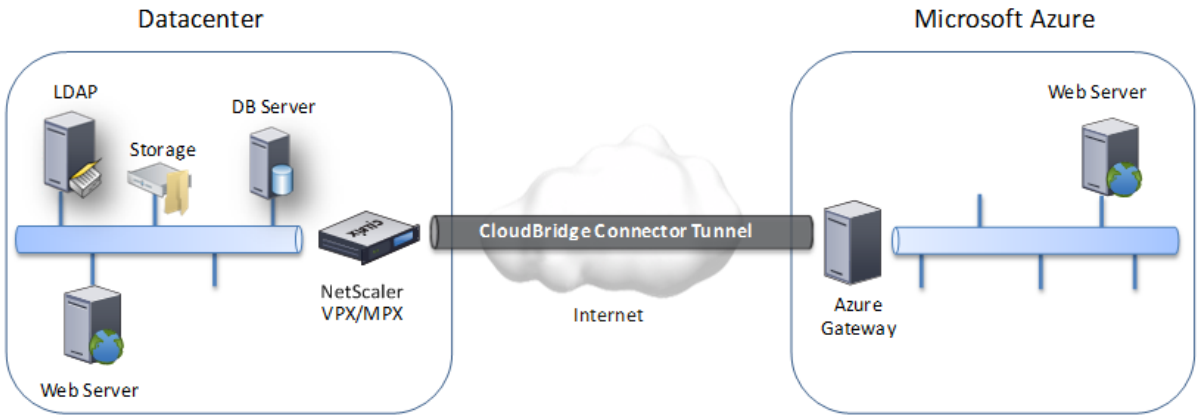
Configuration d'un tunnel CloudBridge Connector entre un centre de données et un nuage Azure

August 20, 2021

L'appliance Citrix ADC fournit une connectivité entre vos centres de données d'entreprise et Azure, fournisseur d'hébergement cloud Microsoft, ce qui fait d'Azure une extension transparente du réseau d'entreprise. Citrix ADC crypte la connexion entre le centre de données d'entreprise et le cloud Azure afin que toutes les données transférées entre les deux soient sécurisées.

Fonctionnement du tunnel CloudBridge Connector

Pour connecter un centre de données au cloud Azure, vous configurez un tunnel CloudBridge Connector entre une appliance Citrix ADC résidant dans le centre de données et une Gateway résidant dans le cloud Azure. L'appliance Citrix ADC dans le centre de données et la Gateway dans le cloud Azure sont les points d'extrémité du tunnel CloudBridge Connector et sont appelés homologues du tunnel CloudBridge Connector.



Un tunnel CloudBridge Connector entre un centre de données et un nuage Azure utilise la suite de protocoles IPsec (Internet Protocol security) standard ouvert, en mode tunnel, pour sécuriser les communications entre pairs dans le tunnel CloudBridge Connector. Dans un tunnel CloudBridge Connector, IPsec garantit :

- Intégrité des données
- Authentification de l'origine des données
- Confidentialité des données (cryptage)
- Protection contre les attaques de relecture

IPsec utilise le mode tunnel dans lequel le paquet IP complet est chiffré, puis encapsulé. Le cryptage utilise le protocole ESP (Encapsulating Security Payload), qui assure l'intégrité du paquet à l'aide d'une fonction de hachage HMAC et assure la confidentialité à l'aide d'un algorithme de chiffrement. Le protocole ESP, après avoir chiffré la charge utile et calculé le HMAC, génère un en-tête ESP et l'insère avant le paquet IP crypté. Le protocole ESP génère également une remorque ESP et l'insère à la fin du paquet.

Le protocole IPsec encapsule ensuite le paquet résultant en ajoutant un en-tête IP avant l'en-tête ESP. Dans l'en-tête IP, l'adresse IP de destination est définie sur l'adresse IP de l'homologue CloudBridge Connecter.

Les homologues du tunnel CloudBridge Connector utilisent le protocole IKEv1 (Internet Key Exchange version 1) (partie de la suite de protocoles IPSec) pour négocier une communication sécurisée, comme suit :

1. Les deux pairs s'authentifient mutuellement les uns avec les autres, en utilisant l'authentification de clé pré-partagée, dans laquelle les pairs échangent une chaîne de texte appelée clé pré-partagée (PSK). Les clés pré-partagées sont comparées les unes aux autres pour l'authentification. Par conséquent, pour que l'authentification réussisse, vous devez configurer la même clé pré-partagée sur chacun des homologues.
2. Les pairs négocient ensuite pour parvenir à un accord sur :
    - Algorithme de chiffrement

- Clés cryptographiques pour crypter des données sur un pair et les décrypter sur l'autre.

Cet accord sur le protocole de sécurité, l'algorithme de chiffrement et les clés cryptographiques est appelé une association de sécurité (SA). Les SA sont unidirectionnelles (simplex). Par exemple, lorsqu'un tunnel CloudBridge Connector est configuré entre une appliance Citrix ADC dans un centre de données et une Gateway dans un nuage Azure, l'appliance du centre de données et la Gateway Azure disposent de deux SA. Une SA est utilisée pour le traitement des paquets sortants et l'autre SA pour le traitement des paquets entrants. Les SA expirent après un intervalle de temps spécifié, qui est appelé durée de vie.

Exemple de configuration du tunnel CloudBridge Connector et de flux de données

À titre d'illustration de CloudBridge Connector Tunnel, considérez un exemple dans lequel un tunnel CloudBridge Connector est configuré entre l'appliance Citrix ADC CB_Appliance-1 dans un centre de données et la Gateway Azure_Gateway-1 dans le cloud Azure.

CB_Appliance-1 fonctionne également comme un routeur L3, ce qui permet à un réseau privé du centre de données d'atteindre un réseau privé dans le cloud Azure via le tunnel CloudBridge Connector. En tant que routeur, CB_Appliance-1 permet la communication entre le client CL1 dans le centre de données et le serveur S1 dans le cloud Azure via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur CB_Appliance-1, la configuration du tunnel CloudBridge Connector inclut une entité de profil IPSec nommée CB_Azure_IPsec_profile, une entité de tunnel CloudBridge Connector nommée CB_Azure_Tunnel et une entité de routage basée sur des stratégies (PBR) nommée CB_Azure_PBR.

L'entité de profil IPsec CB_Azure_IPsec_profile spécifie les paramètres de protocole IPSec, tels que la version IKE, l'algorithme de chiffrement et l'algorithme de hachage, à utiliser par le protocole IPSec dans le tunnel CloudBridge Connector. CB_Azure_IPsec_profile est lié à l'entité de tunnel IP CB_Azure_Tunnel.

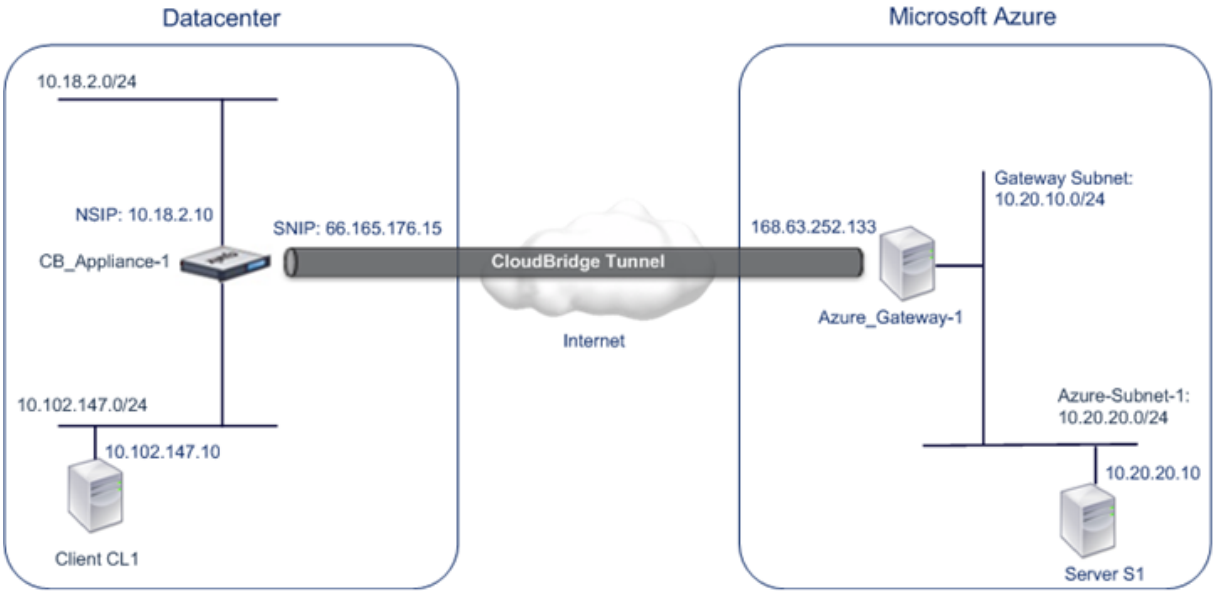
L'entité tunnel CloudBridge Connector CB_Azure_Tunnel spécifie l'adresse IP locale (adresse IP publique (SNIP) configurée sur l'appliance Citrix ADC), l'adresse IP distante (adresse IP du Azure_Gateway-1) et le protocole (IPsec) utilisé pour configurer le tunnel CloudBridge Connector. CB_Azure_Tunnel est lié à l'entité PBR CB_Azure_PBR.

L'entité PBR CB_Azure_PBR spécifie un ensemble de conditions et une entité tunnel CloudBridge Connector (CB_Azure_Tunnel). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de CB_Azure_PBR. La plage d'adresses IP source et la plage d'adresses IP de destination sont spécifiées en tant que sous-réseau dans le centre de données et sous-réseau dans le cloud Azure, respectivement. Tout paquet de requête provenant d'un client dans le sous-réseau du centre de données et destiné à un serveur dans le sous-réseau sur le cloud Azure correspond aux conditions de CB_Azure_PBR. Ce paquet est alors considéré pour le traitement CloudBridge et est envoyé à travers le tunnel CloudBridge Connector (CB_Azure_Tunnel) lié à l'entité PBR.

Sur Microsoft Azure, la configuration du tunnel CloudBridge Connector inclut une entité réseau locale nommée My-Datacenter-Network, une entité réseau virtuelle nommée Azure-Network-for-CloudBridge Tunnel et une Gateway nommée Azure_Gateway-1.

L'entité réseau locale (locale vers Azure) My-Datacenter-Network spécifie l'adresse IP de l'appliance Citrix ADC côté centre de données et le sous-réseau de centre de données dont le trafic doit traverser le tunnel CloudBridge Connector. L'entité réseau virtuel Azure-Network-for-CloudBridge-Tunnel définit un sous-réseau privé nommé Azure-Subnet-1 dans Azure. Le trafic du sous-réseau traverse le tunnel CloudBridge Connector. Le serveur S1 est provisionné dans ce sous-réseau.

L'entité réseau local My-Datacenter-Network est associée à l'entité réseau virtuel Azure-Network-for-CloudBridge-Tunnel. Cette association définit les détails du réseau local et distant de la configuration du tunnel CloudBridge Connector dans Azure. Gateway Azure_Gateway-1 a été créé pour que cette association devienne le point d'extrémité CloudBridge à l'extrémité Azure du tunnel CloudBridge Connector.



Pour plus d'informations sur les paramètres, reportez-vous au document PDF CloudBridge Connector Tunnel Settings .

Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC dans le centre de données et Microsoft Azure, tenez compte des points suivants :

1. L'appliance Citrix ADC doit disposer d'une adresse IPv4 publique (type SNIP) à utiliser comme adresse de point d'extrémité de tunnel pour le tunnel CloudBridge Connector. En outre, l'appliance Citrix ADC ne doit pas se trouver derrière un périphérique NAT.
2. Azure prend en charge les paramètres IPsec suivants pour un tunnel CloudBridge Connector.

Par conséquent, vous devez spécifier les mêmes paramètres IPSec lors de la configuration de Citrix ADC pour le tunnel CloudBridge Connector.

- Version IKE = v1
- Algorithme de chiffrement = AES
- Algorithme de hachage = HMAC SHA1

3. Vous devez configurer le pare-feu dans la périphérie du centre de données pour autoriser ce qui suit.
   - Tous les paquets UDP pour le port 500
   - Tous les paquets UDP pour le port 4500
   - Tous les paquets ESP (numéro de protocole IP 50)
4. La nouvelle clé IKE, qui est la renégociation de nouvelles clés cryptographiques entre les points d'extrémité du tunnel CloudBridge Connector pour établir de nouvelles SA, n'est pas prise en charge. Lorsque les associations de sécurité (SA) expirent, le tunnel passe à l'état DOWN. Par conséquent, vous devez définir une très grande valeur pour la durée de vie des SA.
5. Vous devez configurer Microsoft Azure avant de spécifier la configuration du tunnel sur Citrix ADC, car l'adresse IP publique de l'extrémité Azure (Gateway) du tunnel et du PSK sont générées automatiquement lorsque vous configurez la configuration du tunnel dans Azure. Vous avez besoin de ces informations pour spécifier la configuration du tunnel sur Citrix ADC.

Configuration du tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre votre centre de données et Azure, vous devez installer CloudBridge VPX/MPX dans votre centre de données, configurer Microsoft Azure pour le tunnel CloudBridge Connector, puis configurer l'appliance Citrix ADC dans le centre de données pour le tunnel CloudBridge Connector.

La configuration d'un tunnel CloudBridge Connector entre une appliance Citrix ADC dans le centre de données et Microsoft Azure comporte les tâches suivantes :

1. **Configuration de l'appliance Citrix ADC dans le centre de données**. Cette tâche implique le déploiement et la configuration d'une appliance physique Citrix ADC (MPX), ou le Provisioning et la configuration d'une appliance virtuelle Citrix ADC (VPX) sur une plate-forme de virtualisation du centre de données.
2. **Configuration de Microsoft Azure pour le tunnel CloudBridge Connector**. Cette tâche implique la création d'entités réseau local, réseau virtuel et Gateway dans Azure. L'entité réseau locale spécifie l'adresse IP du point d'extrémité du tunnel CloudBridge Connector (l'appliance Citrix ADC) côté centre de données et le sous-réseau du centre de données dont le trafic doit traverser le tunnel CloudBridge Connector. Le réseau virtuel définit un réseau sur Azure. La création du réseau virtuel inclut la définition d'un sous-réseau dont le trafic doit traverser le tunnel CloudBridge Connector à former. Vous associez ensuite le réseau local au réseau virtuel. Enfin, vous créez une Gateway qui devient le point final à l'extrémité Azure du tunnel CloudBridge

Connector.

3. **Configuration de l'appliance Citrix ADC dans le centre de données pour le tunnel CloudBridge Connector**. Cette tâche implique la création d'un profil IPSec, d'une entité de tunnel IP et d'une entité PBR dans l'appliance Citrix ADC dans le centre de données. L'entité de profil IPsec spécifie les paramètres de protocole IPSec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et PSK, à utiliser dans le tunnel CloudBridge Connector. Le tunnel IP spécifie l'adresse IP des points d'extrémité du tunnel CloudBridge Connector (l'appliance Citrix ADC dans le centre de données et la Gateway dans Azure) et le protocole à utiliser dans le tunnel CloudBridge Connector. Vous associez ensuite l'entité de profil IPSec à l'entité de tunnel IP. L'entité PBR spécifie les deux sous-réseaux, dans le centre de données et dans le cloud Azure, qui doivent communiquer entre eux via le tunnel CloudBridge Connector. Vous associez ensuite l'entité de tunnel IP à l'entité PBR.

Configuration de Microsoft Azure pour le tunnel CloudBridge Connector

Pour créer une configuration de tunnel CloudBridge Connector sur Microsoft Azure, utilisez le portail de gestion Microsoft Windows Azure, qui est une interface graphique Web permettant de créer et de gérer des ressources sur Microsoft Azure.

Avant de commencer la configuration du tunnel CloudBridge Connector sur le cloud Azure, assurez-vous que :

- Vous avez un compte d'utilisateur pour Microsoft Azure.
- Vous avez une compréhension conceptuelle de Microsoft Azure.
- Vous connaissez le portail de gestion Microsoft Windows Azure.

Pour configurer un tunnel CloudBridge Connector entre un centre de données et un nuage Azure, effectuez les tâches suivantes sur Microsoft Azure à l'aide du portail de gestion Microsoft Windows Azure :

- **Créez une entité de réseau local**. Créez une entité réseau locale dans Windows Azure pour spécifier les détails réseau du centre de données. Une entité réseau locale spécifie l'adresse IP du point d'extrémité du tunnel CloudBridge Connector (Citrix ADC) côté centre de données et du sous-réseau du centre de données dont le trafic doit traverser le tunnel CloudBridge Connector.
- **Créez un réseau virtuel**. Créez une entité de réseau virtuel qui définit un réseau sur Azure. Cette tâche comprend la définition d'un espace d'adressage privé, dans lequel vous fournissez une plage d'adresses privées et de sous-réseaux appartenant à la plage spécifiée dans l'espace d'adressage. Le trafic des sous-réseaux traverse le tunnel CloudBridge Connector. Vous associez ensuite une entité de réseau local à l'entité de réseau virtuel. Cette association permet à Azure de créer une configuration pour un tunnel CloudBridge Connector entre le réseau virtuel et le réseau du centre de données. Une Gateway (à créer) dans Azure pour ce réseau virtuel sera le point d'extrémité CloudBridge à l'extrémité Azure du tunnel CloudBridge Connector. Vous définissez ensuite un sous-réseau privé pour la Gateway à créer. Ce sous-réseau appartient à la

plage spécifiée dans l'espace d'adressage dans l'entité de réseau virtuel.

- **Créez une Gateway dans Windows Azure**. Créez une Gateway qui devient le point final à l'extrémité Azure du tunnel CloudBridge Connector. Azure, à partir de son pool d'adresses IP publiques, affecte une adresse IP à la Gateway créée.
- **Rassemblez l'adresse IP publique de la Gateway et la clé pré-partagée.** Pour une configuration de tunnel CloudBridge Connector sur Azure, l'adresse IP publique de la Gateway et la clé pré-partagée (PSK) sont automatiquement générées par Azure. Prenez note de cette information. Vous en aurez besoin pour configurer le tunnel CloudBridge Connector sur Citrix ADC dans le centre de données.

> **Remarque :**
>
> Les procédures de configuration de Microsoft Azure pour un tunnel CloudBridge Connector peuvent changer au fil du temps, en fonction du cycle de publication de Microsoft Azure. Pour connaître les procédures les plus récentes, consultez la documentation Microsoft Azure.

Configuration de l'appliance Citrix ADC dans le centre de données pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre un centre de données et un nuage Azure, effectuez les tâches suivantes sur Citrix ADC dans le centre de données. Vous pouvez utiliser la ligne de commande Citrix ADC ou l'interface graphique :

- **Créez un profil IPSec**. Une entité de profil IPsec spécifie les paramètres du protocole IPSec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et PSK, à utiliser par le protocole IPSec dans le tunnel CloudBridge Connector.
- **Créez un tunnel IP avec le protocole IPSec et associez le profil IPSec à celui-ci**. Un tunnel IP spécifie l'adresse IP locale (une adresse SNIP publique configurée sur l'appliance Citrix ADC), l'adresse IP distante (l'adresse IP publique de la Gateway dans Azure), le protocole (IPsec) utilisé pour configurer le tunnel CloudBridge Connector et une entité de profil IPsec. L'entité de tunnel IP créée est également appelée entité de tunnel CloudBridge Connector.
- **Créez une règle PBR et associez-y le tunnel IP**. Une entité PBR spécifie un ensemble de conditions et une entité tunnel IP (tunnel CloudBridge Connector). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Vous devez définir la plage d'adresses IP source pour spécifier le sous-réseau du centre de données dont le trafic doit traverser le tunnel, et la plage d'adresses IP de destination pour spécifier le sous-réseau Azure dont le trafic doit traverser le tunnel CloudBridge Connector. Tout paquet de requête provenant d'un client dans le sous-réseau sur le centre de données et destiné à un serveur dans le sous-réseau sur le cloud Azure correspond à la plage IP source et de destination de l'entité PBR. Ce paquet est alors considéré pour le traitement du tunnel CloudBridge Connector et est envoyé à travers le tunnel CloudBridge Connector associé à l'entité PBR.

L'interface graphique combine toutes ces tâches dans un seul assistant appelé Assistant CloudBridge Connector.
Pour créer un profil IPSEC à l'aide de la ligne de commande Citrix ADC :

À l'invite de commande, tapez :

```
add ipsec profile <name> -psk <string> -ikeVersion v1
```

Pour créer un tunnel IPSEC et y lier le profil IPSEC à l'aide de la ligne de commande Citrix ADC :

À l'invite de commande, tapez :

```
add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -
ipsecProfileName <string>
```

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande Citrix ADC

```
add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> ipTunnel
 <tunnelName> apply pbrs
```

Exemple de configuration

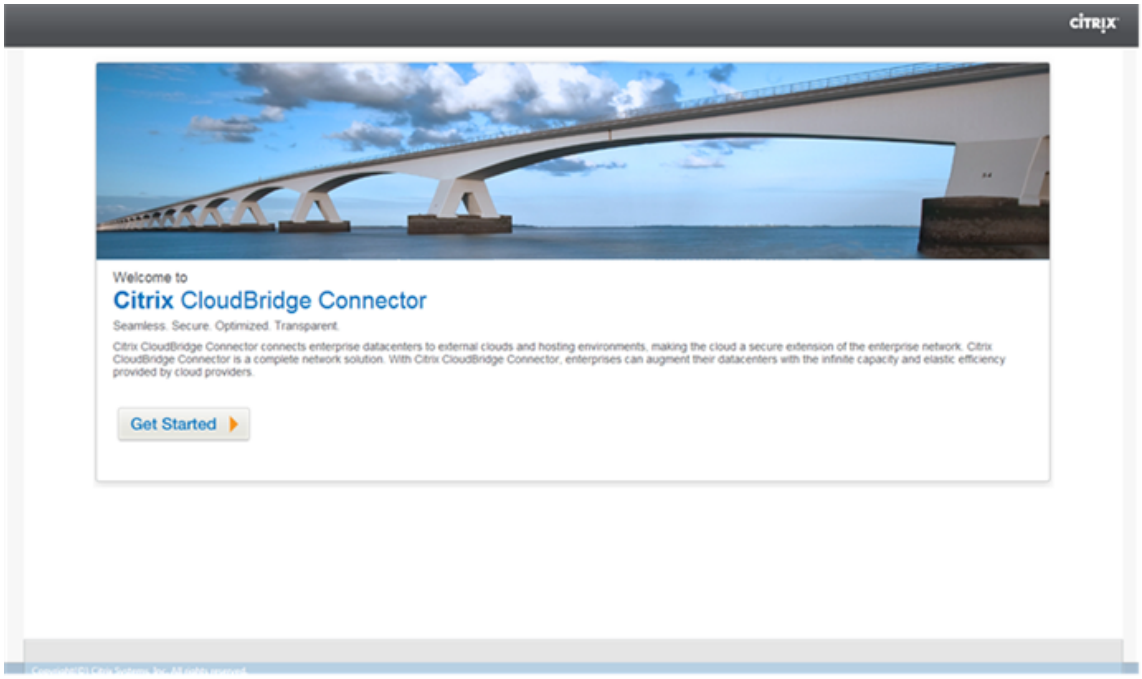
Les commandes suivantes créent tous les paramètres du dispositif Citrix ADC CB_Appliance-1 utilisé dans « Exemple de configuration et de flux de données CloudBridge Connector ».

```
1  > add ipsec profile CB_Azure_IPSec_Profile -psk
       DkiMgMdcbqvYREEuIvxsbKkW0FOyDiLM  -ikeVersion v1  - lifetime 31536000
2  Done
3
4  >  add iptunnel CB_Azure_Tunnel 168.63.252.133 255.255.255.255
       66.165.176.15  - protocol IPSEC  - ipsecProfileName
       CB_Azure_IPSec_Profile
5  Done
6
7  > add pbr CB_Azure_Pbr -srcIP 10.102.147.0-10.102.147.255  - destIP
       10.20.0.0-10.20.255.255  - ipTunnelCB_Azure_Tunnel
8  Done
9
10 > apply pbrs
11 Done
12 <!--NeedCopy-->
```

Pour configurer un tunnel CloudBridge Connector dans une appliance Citrix ADC à l'aide de l'interface graphique graphique

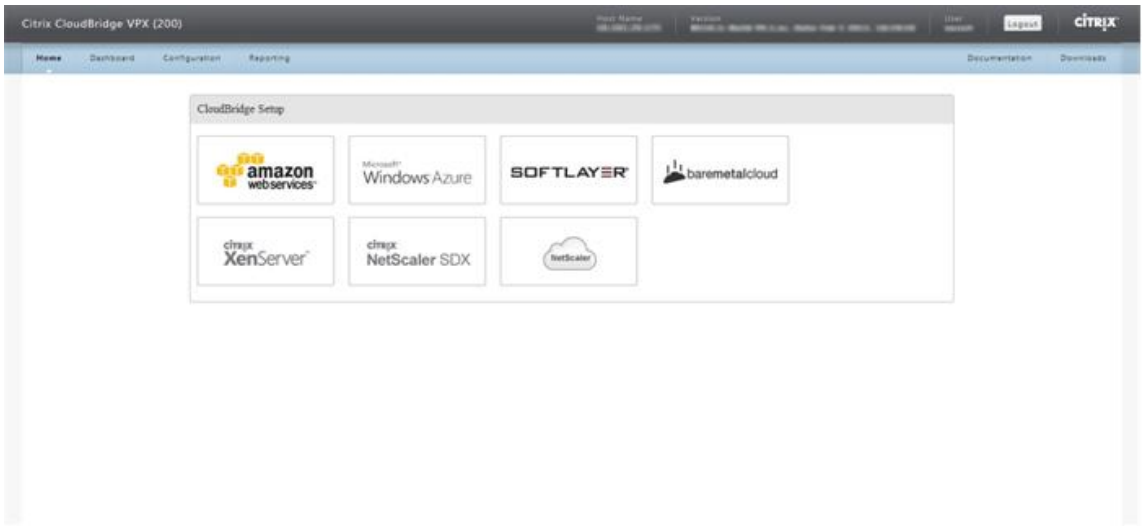
1. Accédez à l'interface graphique à l'aide d'un navigateur Web pour vous connecter à l'adresse IP de l'appliance Citrix ADC dans le centre de données.
2. Accédez à **Système** > **CloudBridge Connector**.

3. Dans le volet droit, sous **Mise en route**, cliquez sur **Créer/surveiller CloudBridge**.
4. Cliquez sur **Démarrer**.



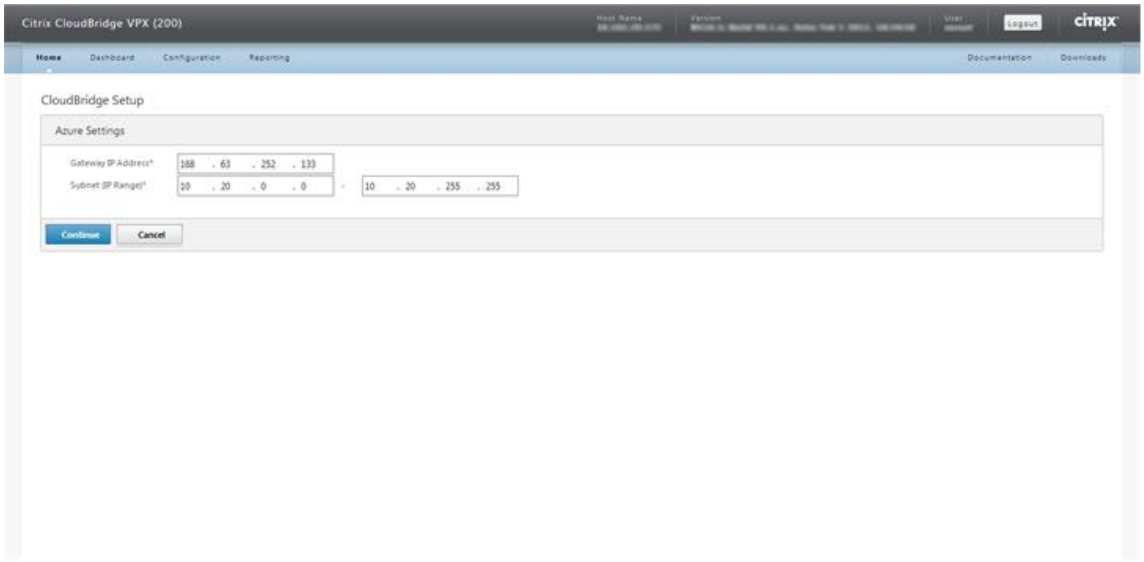
> **Remarque** : si vous avez déjà un tunnel CloudBridge Connector configuré sur l'appliance Citrix ADC, cet écran n'apparaît pas et vous accédez au volet Configuration du connecteur CloudBridge.

5. Dans le volet d'installation de CloudBridge, cliquez sur **Microsoft Windows Azure**.

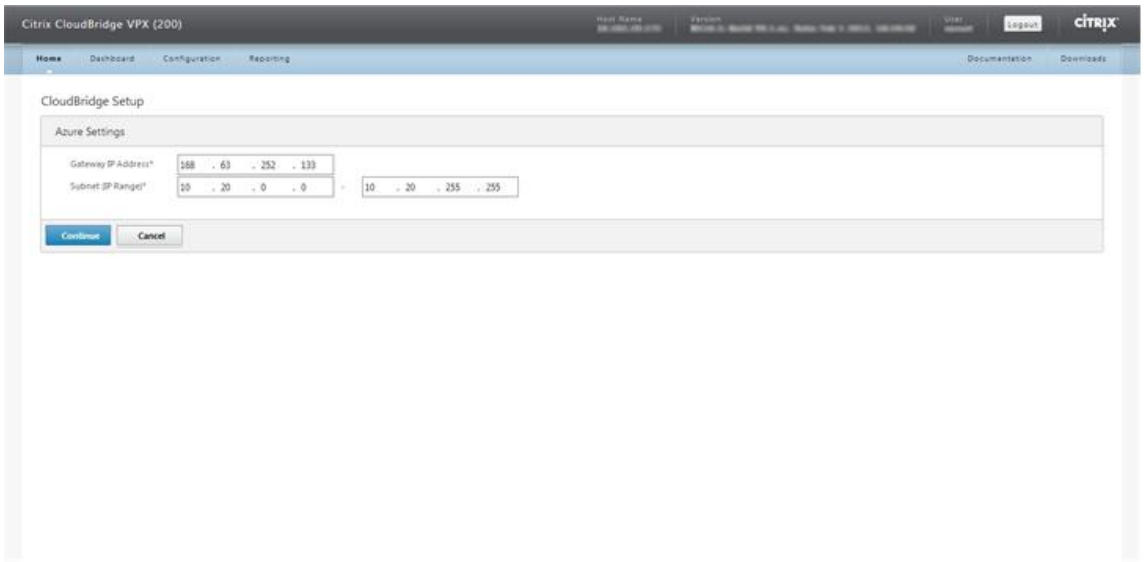


6. Dans le volet Paramètres Azure, dans le champ **Adresse IP de la passerelle**, tapez l'adresse IP de la passerelle Azure. Le tunnel CloudBridge Connector est ensuite configuré entre l'appliance Citrix ADC et la Gateway. Dans les zones de texte **Subnet (plage IP)**, spécifiez une plage de

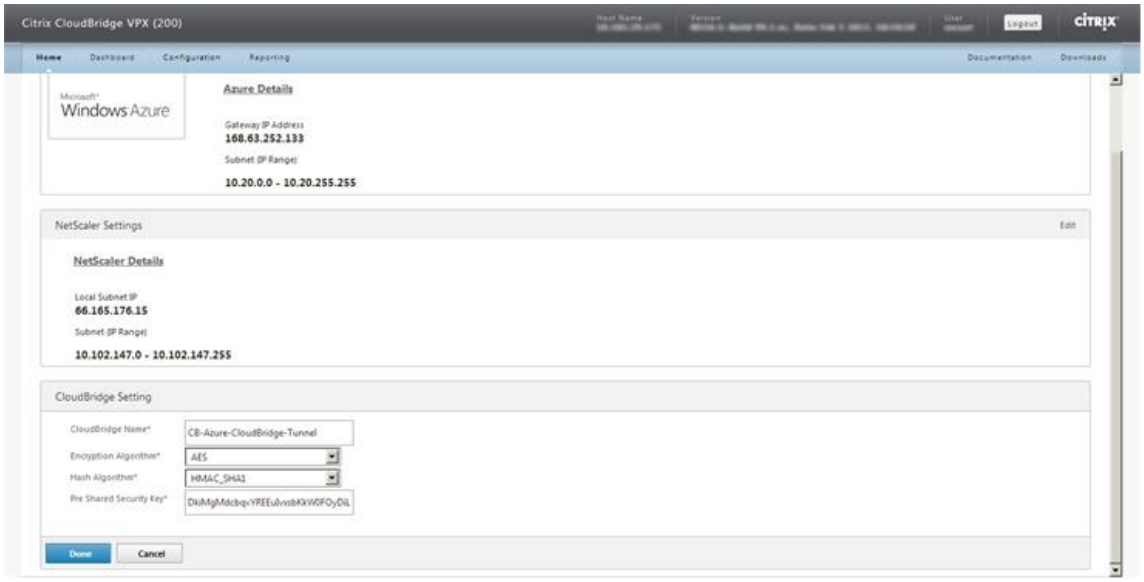
sous-réseaux (dans le cloud Azure) dont le trafic doit traverser le tunnel CloudBridge Connector. Cliquez sur **Continuer**.



7. Dans le volet Paramètres Citrix ADC, dans la liste déroulante **IP du sous-réseau local**, sélectionnez une adresse SNIP accessible publiquement configurée sur l'appliance Citrix ADC. Dans les zones de texte **Subnet (IP Range)**, spécifiez une plage de sous-réseau local dont le trafic doit traverser le tunnel CloudBridge Connector. Cliquez sur **Continuer**.



8. Dans le volet **Paramètres de CloudBridge**, dans la zone de texte Nom de CloudBridge, tapez un nom pour le CloudBridge que vous souhaitez créer.



9. Dans les listes déroulantes Algorithme de chiffrement et Algorithme de hachage, sélectionnez respectivement les algorithmes AES et HMAC_SHA1. Dans la zone de texte Clé de sécurité pré-partagée, tapez la clé de sécurité.
10. Cliquez sur **Terminé**.

Surveillance du tunnel CloudBridge Connector

Vous pouvez afficher des statistiques pour surveiller les performances d'un tunnel CloudBridge Connector entre l'appliance Citrix ADC dans le centre de données et Microsoft Azure. Pour afficher les statistiques de tunnel CloudBridge Connector sur l'appliance Citrix ADC, utilisez l'interface graphique ou la ligne de commande Citrix ADC. Pour afficher les statistiques de tunnel CloudBridge Connector dans Microsoft Azure, utilisez le portail de gestion Microsoft Windows Azure.

Affichage des statistiques du tunnel CloudBridge Connector dans l'appliance Citrix ADC

Pour plus d'informations sur l'affichage des statistiques de tunnel CloudBridge Connector sur une appliance Citrix ADC, reportez-vous à Monitoring CloudBridge Connector Tunnels.

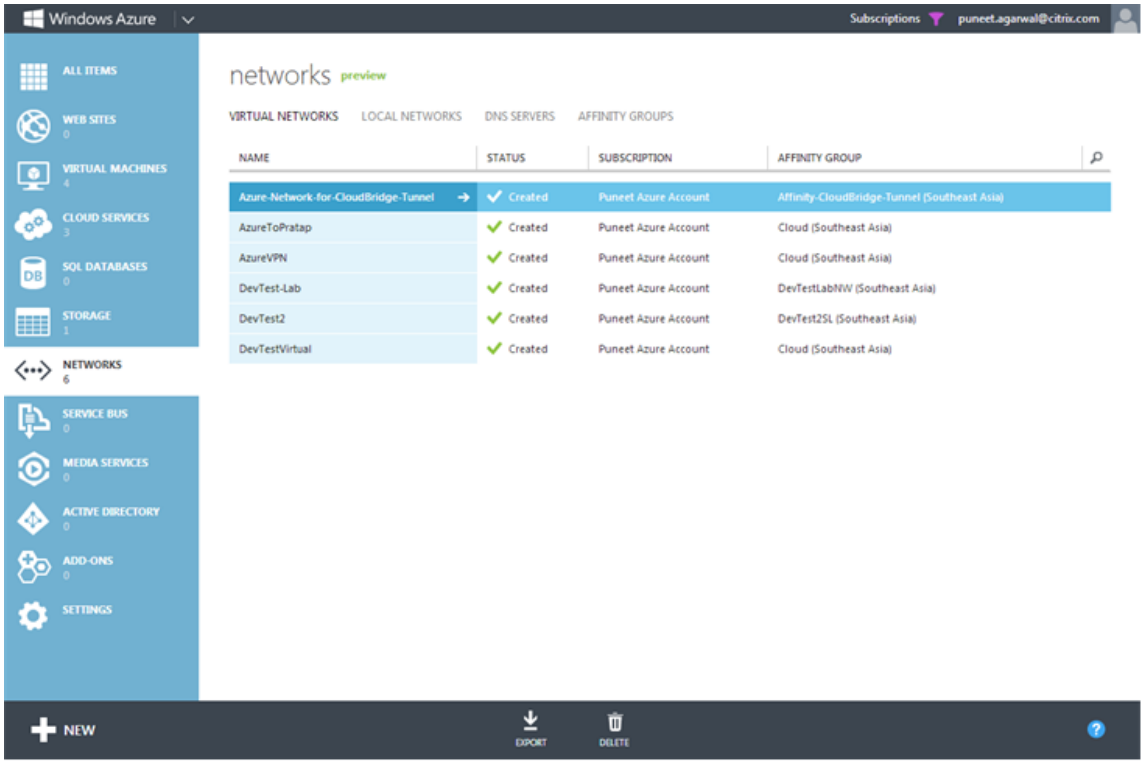
Affichage des statistiques de tunnel CloudBridge Connector dans Microsoft Azure

Le tableau suivant répertorie les compteurs statistiques disponibles pour la surveillance des tunnels CloudBridge Connector dans Microsoft Azure.

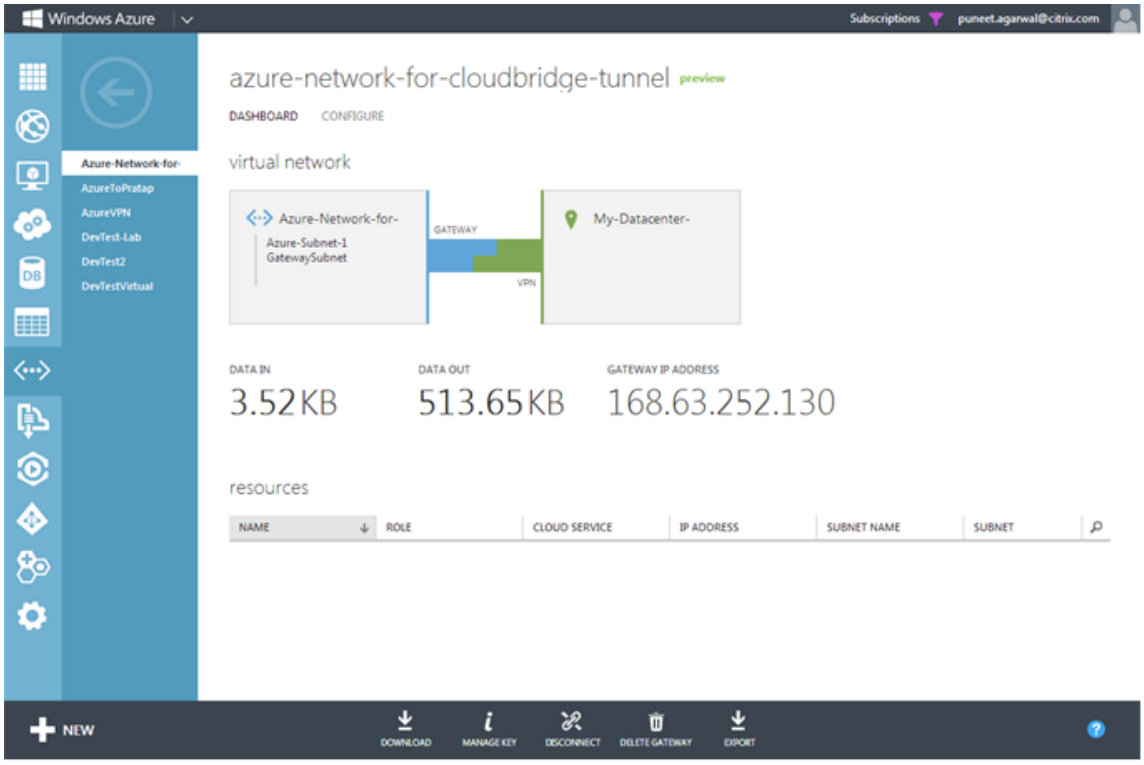
Compteur statistique	Spécifie
DATA IN	Nombre total de kilo-octets reçus par la Gateway Azure via le tunnel CloudBridge Connector depuis la création de la Gateway.
DATA OUT	Nombre total de kilo-octets envoyés par la Gateway Azure via le tunnel CloudBridge Connector depuis la création de la Gateway.

Pour afficher les statistiques de tunnel CloudBridge Connector à l'aide du portail de gestion Microsoft Windows Azure

1. Connectez-vous au portail de gestion Windows Azure à l'aide des informations d'identification de votre compte Microsoft Azure.
2. Dans le volet gauche, cliquez sur **RÉSEAUX**.
3. Sous l'onglet **Réseau virtuel**, dans la colonne Nom, sélectionnez l'entité réseau virtuel associée à un tunnel CloudBridge Connector dont vous souhaitez afficher les statistiques.



4. Sur la page **DASHBOARD** du réseau virtuel, affichez les compteurs DATA IN et DATA OUT pour le tunnel CloudBridge Connector.



Configuration du tunnel CloudBridge Connector entre le centre de données et le cloud d'entreprise Softlayer

August 20, 2021

L'interface graphique inclut un assistant qui vous aide à configurer facilement un tunnel CloudBridge Connector entre une appliance Citrix ADC dans un centre de données et des instances Citrix ADC VPX sur le cloud d'entreprise SoftLayer.

Lorsque vous utilisez l'assistant de l'appliance Citrix ADC dans le centre de données, la configuration du tunnel CloudBridge Connector créée sur l'appliance Citrix ADC est automatiquement poussée vers l'autre point de terminaison ou homologue (Citrix ADC VPX sur SoftLayer) du tunnel CloudBridge Connector.

À l'aide de l'assistant de l'appliance Citrix ADC dans le centre de données, vous effectuez les opérations suivantes pour configurer un tunnel CloudBridge Connector.

1. Connectez-vous au cloud d'entreprise Softlayer en fournissant les informations d'identification de connexion de l'utilisateur.
2. Sélectionnez le Citrix XenServer qui exécute le dispositif Citrix ADC VPX.
3. Sélectionnez l'appliance Citrix ADC VPX.
4. Fournissez les paramètres du tunnel CloudBridge Connector pour :

- Configurez un tunnel GRE.
- Configurez IPSec sur le tunnel GRE.
- Créez un netbridge, qui est une représentation logique du connecteur CloudBridge, en spécifiant un nom.
- Liez le tunnel GRE au netbridge.

Pour configurer un tunnel CloudBridge Connector à l'aide de l'interface graphique

1. Connectez-vous à l'interface graphique de l'appliance Citrix ADC dans le centre de données à l'aide des informations d'identification de votre compte pour l'appliance.
2. Accédez à **Système** > **ConnecteurCloudBridge** .
3. Dans le volet droit, sous **Mise en route**, cliquez sur **Créer/surveiller CloudBridge Connector**.
4. Cliquez sur **Démarrer**.

> **Remarque** :
>
> Si vous avez déjà un tunnel CloudBridge Connector configuré sur l'appliance Citrix ADC, cet écran n'apparaît pas et vous accédez au volet Configuration du connecteur CloudBridge.

1. Dans le volet Configuration du connecteur CloudBridge, cliquez sur Softlayer, puis suivez les instructions de l'Assistant.

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance Citrix ADC à l'aide des compteurs statistiques de tunnel CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques de tunnel CloudBridge Connector sur une appliance Citrix ADC, consultez Surveillance des tunnels de CloudBridge Connector.

Configuration d'un tunnel CloudBridge Connector entre une appliance Citrix ADC et un périphérique Cisco IOS

October 4, 2021

Vous pouvez configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et un périphérique Cisco pour connecter deux centres de données ou étendre votre réseau à un fournisseur Cloud. L'appliance Citrix ADC et le périphérique Cisco IOS forment les points d'extrémité du tunnel CloudBridge Connector et sont appelés homologues.

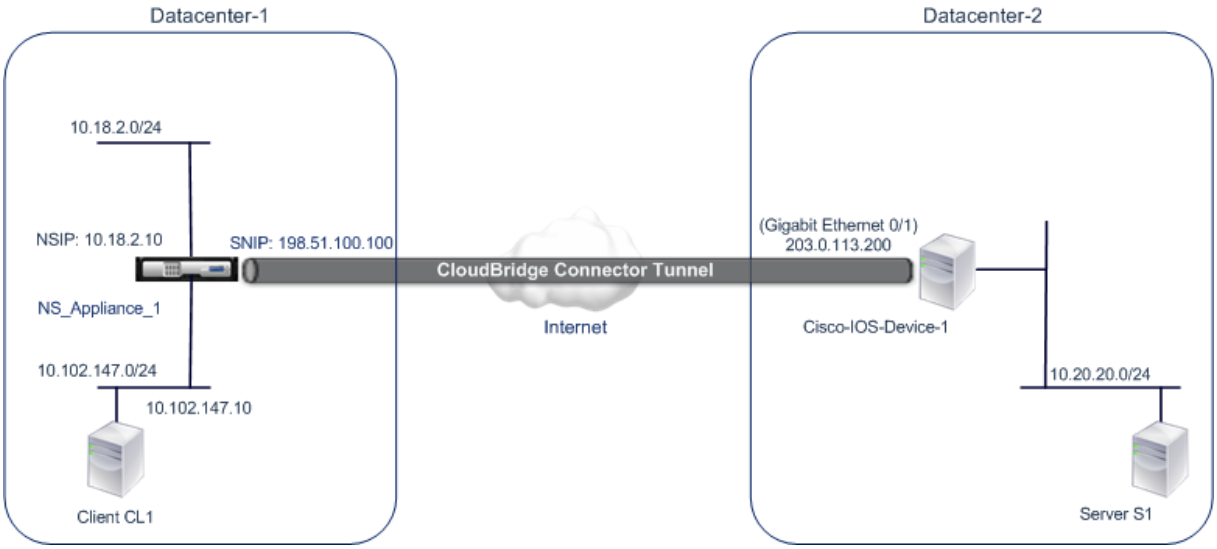
Exemple de configuration du tunnel CloudBridge Connector et de flux de données

À titre d'illustration du flux de trafic dans un tunnel CloudBridge Connector, considérez un exemple dans lequel un tunnel CloudBridge Connector est configuré entre les périphériques suivants :

- Appliance Citrix ADC NS_Appliance-1 dans un centre de données désigné comme Datacenter-1
- Périphérique Cisco IOS Cisco Cisco IOS Device-1 dans un centre de données désigné comme Datacenter-2

NS_Appliance-1 et Cisco-IOS-Device-1 permettent la communication entre les réseaux privés dans Datacenter-1 et Datacenter-2 via le tunnel CloudBridge Connector. Dans l'exemple, NS_Appliance-1 et Cisco-IOS-Device-1 permettent la communication entre le client CL1 dans Datacenter-1 et le serveur S1 dans Datacenter-2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel du connecteur CloudBridge inclut l'entité de profil IPSec NS_CISCO_IPSEC_profile, l'entité de tunnel du connecteur CloudBridge NS_CISCO_Tunnel et l'entité de routage basé sur des stratégies (PBR) NS_CISCO_PBR.



Pour plus d'informations, reportez-vous au tunnel CloudBridge Connector entre une appliance Citrix ADC et les paramètres d'appareil Cisco IOS pdf.

Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et un périphérique Cisco IOS, tenez compte des points suivants :

- Les paramètres IPsec suivants sont pris en charge pour un tunnel CloudBridge Connector entre une appliance Citrix ADC et un périphérique Cisco IOS.

Propriétés IPSec	Paramètre
Mode IPsec	Mode tunnel
Version IKE	Version 1
Groupe IKE DH	DH groupe 2 (algorithme MODP 1024 bits)
Méthode d'authentification IKE	Clé pré-partagée
Algorithme de chiffrement IKE	AES, 3DES
Algorithme de hachage IKE	HMAC SHA1, HMAC SHA256, HMAC SHA384, HMAC SHA512, HMAC MD5
Algorithme de chiffrement ESP	AES, 3DES
Algorithme de hachage ESP	HMAC SHA1, HMAC SHA256, HMAC SHA256, HMAC SHA256, HMAC MD5

- Vous devez spécifier les mêmes paramètres IPSec sur l'appliance Citrix ADC et le périphérique Cisco IOS aux deux extrémités du connecteur CloudBridge.
- Citrix ADC fournit un paramètre commun (dans les profils IPSec) pour spécifier un algorithme de hachage IKE et un algorithme de hachage ESP. Il fournit également un autre paramètre commun pour spécifier un algorithme de chiffrement IKE et un algorithme de chiffrement ESP. Par conséquent, sur le périphérique Cisco, vous devez spécifier le même algorithme de hachage et le même algorithme de chiffrement pour IKE (lors de la création de la stratégie IKE) et ESP (lors de la création d'un ensemble de transformations IPSec).
- Vous devez configurer le pare-feu à l'extrémité Citrix ADC et à l'extrémité du périphérique Cisco pour autoriser ce qui suit.
  - Tous les paquets UDP pour le port 500
  - Tous les paquets UDP pour le port 4500
  - Tous les paquets ESP (numéro de protocole IP 50)

Configuration du périphérique Cisco IOS pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector sur un périphérique Cisco IOS, utilisez l'interface de ligne de commande Cisco IOS, qui est l'interface utilisateur principale pour la configuration, la surveillance et la maintenance des périphériques Cisco.

Avant de commencer la configuration du tunnel CloudBridge Connector sur un périphérique Cisco IOS, assurez-vous que :

- Vous disposez d'un compte d'utilisateur avec des informations d'identification d'administrateur sur le périphérique Cisco IOS.

- Vous connaissez l'interface de ligne de commande de Cisco IOS.
- Le périphérique Cisco IOS est opérationnel, est connecté à Internet et est également connecté aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.

> **Remarque** :
>
> Les procédures de configuration du tunnel CloudBridge Connector sur un périphérique Cisco IOS peuvent changer au fil du temps, en fonction du cycle de publication de Cisco. Citrix vous recommande de suivre la documentation officielle du produit Cisco pour plus d'informations, voir la rubrique Configuration des tunnels VPN IPSec .

Pour configurer un tunnel de connecteur CloudBridge entre une appliance Citrix ADC et un périphérique Cisco IOS, effectuez les tâches suivantes sur la ligne de commande IOS de l'appareil Cisco :

- Créez une stratégie IKE.
- Configurez une clé pré-partagée pour l'authentification IKE.
- Définissez un jeu de transformations et configurez IPsec en mode tunnel.
- Créer une liste d'accès crypto
- Créer une carte crypto
- Appliquer la carte crypto à une interface

Les exemples des procédures suivantes créent des paramètres `Cisco IOS device Cisco-IOS-Device-1` mentionnés dans la section « Exemple de configuration et de flux de données CloudBridge Connector. «

Pour créer une stratégie IKE, reportez-vous au pdf de la stratégie IKE .

Pour configurer une clé pré-partagée à l'aide de la ligne de commande Cisco IOS :

À l'invite de commandes du périphérique Cisco IOS, tapez les commandes suivantes, en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
crypto isakmp identity address	Cisco-ios-device-1(config)# crypto isakmp identity address	Spécifiez l'identité ISAKMP (adresse) du périphérique Cisco IOS à utiliser lors de la communication avec l'homologue (appliance Citrix ADC) pendant les négociations IKE. Cet exemple spécifie le mot-clé address, qui utilise l'adresse IP 203.0.113.200 (interface Gigabit Ethernet 0/1 de Cisco-IOS-Device-1) comme identité du périphérique.
crypto isakmp key keystringaddress peer-address	Cisco-ios-device-1 (config)# crypto isakmp key examplepresharedkey address 198.51.100.100	Spécifiez une clé pré-partagée pour l'authentification IKE. Cet exemple montre comment configurer la clé partagée examplepresharedkey à utiliser avec l'appliance Citrix ADC NS_Appliance-1 (198.51.100.100). La même clé pré-partagée doit être configurée sur l'appliance Citrix ADC pour que l'authentification IKE soit réussie entre le périphérique Cisco IOS et l'appliance Citrix ADC.

Pour créer une liste d'accès crypto à l'aide de la ligne de commande Cisco IOS :

À l'invite de commandes du périphérique Cisco IOS, tapez la commande suivante en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
access-listaccess-list-number permit IPsource source-wildcard destination destination-wildcard	Cisco-ios-device-1(config)# access-list 111 permit ip 10.20.20.0 0.0.0.255 10.102.147.0 0.0.0.255	Spécifiez des conditions pour déterminer les sous-réseaux dont le trafic IP doit être protégé sur le tunnel CloudBridge Connector. Cet exemple montre comment configurer la liste d'accès 111 pour protéger le trafic des sous-réseaux 10.20.20.0/24 (côté CISCO-IOS-Device-1) et 10.102.147.0/24 (côté NS_Appliance-1).

Pour définir une transformation et configurer le mode tunnel IPsec à l'aide de la ligne de commande Cisco IOS :

À l'invite de commandes du périphérique Cisco IOS, tapez les commandes suivantes, en commençant en mode de configuration globale, dans l'ordre indiqué :
Commande	Exemple	Description de la commande
–	–	–
crypto ipsec transform-setname ESP_Authentication_Transform ESP_Encryption_Transform Note : ESP_Authentication_Transform peut prendre les valeurs suivantes : esp-sha-hmac, esp-sha256-hmac, esp-sha384-hmac, esp-sha512-hmac, esp-md5-hmac. ESP_Encryption_Transform peut prendre les valeurs suivantes : esp-aes ou esp-3des	Cisco-ios-device-1(config)# crypto ipsec transform-set NS-CISCO-TS esp-sha256-hmac esp-3des	Définissez un jeu de transformations et spécifiez l'algorithme de hachage ESP (pour l'authentification) et l'algorithme de chiffrement ESP à utiliser lors de l'échange de données entre les homologues de tunnel CloudBridge Connector. Cet exemple définit le jeu de transformations NS-CISCO-TS et spécifie l'algorithme d'authentification ESP comme esp-sha256-hmac, et l'algorithme de chiffrement ESP comme esp-3des.
tunnel de mode	Tunnel en mode # Cisco IOS Device-1 (config-crypto-trans)	Définissez IPSec en mode tunnel.
exit	Dispositif Cisco IOS 1 (config-crypto-trans) # sortie, Cisco IOS Device-1 (config) #	Quittez en mode de configuration global.

Pour créer une carte cryptographique à l'aide de la ligne de commande Cisco IOS :

À l'invite de commandes du périphérique Cisco IOS, tapez les commandes suivantes en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
crypto mapmap-name seq-num ipsec-isakmp	Cisco-ios-device-1 (config)# crypto map NS-CISCO-CM 2 ipsec-isakmp	Entrez le mode de configuration de la carte de chiffrement, spécifiez un numéro de séquence pour la carte de chiffrement et configurez la carte de chiffrement pour utiliser IKE pour établir des associations de sécurité (SA). Cet exemple configure le numéro de séquence 2 et IKE pour la carte cryptographique NS-CISCO-CM.
set peer ip-address	Cisco-ios-device-1 (config-crypto-map)# set peer 172.23.2.7	Spécifiez l'homologue (appliance Citrix ADC) par son adresse IP. Cet exemple spécifie 198.51.100.100, qui est l'adresse IP du point de terminaison CloudBridge Connector sur l'appliance Citrix ADC.
match addressaccess-list-id	Cisco-ios-device-1 (config-crypto-map)# match address 111	Spécifiez une liste d'accès étendue. Cette liste d'accès spécifie les conditions permettant de déterminer les sous-réseaux dont le trafic IP doit être protégé sur le tunnel CloudBridge Connector. Cet exemple spécifie la liste d'accès 111.
set transform-set transform-set-name	Cisco-ios-device-1 (config-crypto-map)# set transform-set NS-CISCO-TS	Spécifiez les ensembles de transformations autorisés pour cette entrée de mappage crypto. Cet exemple spécifie le jeu de transformations NS-CISCO-TS.

Commande	Exemple	Description de la commande
exit	Cisco-ios-device-1 (config-crypto-map)# exit	
Cisco-ios-device-1 (config)#	Exit back to global configuration mode.	

Pour appliquer une carte de chiffrement à une interface à l'aide de la ligne de commande Cisco IOS :

À l'invite de commandes du périphérique Cisco IOS, tapez les commandes suivantes en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
interfaceinterface-ID	Cisco-ios-device-1(config)# interface GigabitEthernet 0/1	Spécifiez une interface physique à laquelle appliquer la carte de chiffrement et entrez en mode de configuration de l'interface. Cet exemple spécifie l'interface Gigabit Ethernet 0/1 du périphérique Cisco Cisco IOS-Device-1. L'adresse IP 203.0.113.200 est déjà définie sur cette interface.
crypto mapmap-name	Cisco-ios-device-1 (config-if)# crypto map NS-CISCO-CM	Appliquez le mappage crypto à l'interface physique. Cet exemple applique la carte cryptographique NS-CISCO-CM.
exit	Cisco-ios-device-1 (config-if)# exit, Cisco-ios-device-1 (config)#	Quittez en mode de configuration global.

Configuration de l'appliance Citrix ADC pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et un périphérique Cisco IOS, effectuez les tâches suivantes sur l'appliance Citrix ADC. Vous pouvez utiliser la ligne de

commande Citrix ADC ou l'interface utilisateur graphique (GUI) Citrix ADC :

- Créez un profil IPSec.
- Créez un tunnel IP qui utilise le protocole IPSec et associez le profil IPSec à celui-ci.
- Créez une règle PBR et associez-la au tunnel IP.

Pour créer un profil IPSEC à l'aide de la ligne de commande Citrix ADC :

À l'invite de commande, tapez :

- `add ipsec profile <name> -psk <string> -ikeVersion v1`
- `show ipsec profile <name>`

Pour créer un tunnel IPSEC et y lier le profil IPSEC à l'aide de la ligne de commande Citrix ADC :

À l'invite de commande, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `add ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande Citrix ADC :

À l'invite de commande, tapez :

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbrs <pbrName>`

Les commandes suivantes créent les paramètres `Citrix ADC appliance NS_Appliance-1` mentionnés dans la section **Exemple de configuration et de flux de données CloudBridge Connector**.

```
1      > add ipsec profile NS_Cisco_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1 - lifetime 315360 - encAlgo 3
          DES
2      Done
3      > add iptunnel NS_Cisco_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100 - protocol IPSEC - ipsecProfileName
          NS_Cisco_IPSec_Profile
4
5      Done
6      > add pbr NS_Cisco_Pbr -srcIP 10.102.147.0-10.102.147.255 - destIP
          10.20.0.0-10.20.255.255 - ipTunnel NS_Cisco_Tunnel
7
8      Done
9      > apply pbrs
10
11     Done
```



```
12 <!--NeedCopy-->
```

Pour créer un profil IPSEC à l'aide de l'interface graphique :

1. Accédez à **Système** > **CloudBridge Connector** > **Profil IPsec**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un profil IPsec**, définissez les paramètres suivants :
   - Nom
   - Algorithme de chiffrement
   - Algorithme de hachage
   - Version du protocole IKE
4. Configurez la méthode **d'authentification IPSec** à utiliser par les deux homologues du tunnel CloudBridge Connector pour s'authentifier mutuellement : Sélectionnez la méthode **d'authentification par clé pré-partagée** et définissez le paramètre **Pre-Shared Key Exists** .
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface graphique :

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.
2. Dans l'onglet **Tunnels IPv4**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un tunnel IP**, définissez les paramètres suivants :
   - Nom
   - IP distante
   - Masque distant
   - Type IP local (dans la liste déroulante Type IP local, sélectionnez IP du sous-réseau).
   - IP locale (Toutes les adresses IP configurées du type d'IP sélectionné se trouvent dans la liste déroulante IP locale. Sélectionnez l'adresse IP souhaitée dans la liste.)
   - Protocole
   - Profil IPsec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer PBR**, définissez les paramètres suivants :
   - Nom
   - Action
   - Type de saut suivant (Select IP Tunnel)
   - Nom du tunnel IP
   - IP source Faible
   - IP source élevée
   - IP de destination faible

- IP de destination élevée

4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour appliquer un PBR à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Sous l'onglet **PBR**, sélectionnez le **PBR**, dans la **liste Action**, sélectionnez **Appliquer**.

La nouvelle configuration de tunnel CloudBridge Connector correspondante sur l'appliance Citrix ADC apparaît dans l'interface graphique. L'état actuel du tunnel de connecteur CloudBridge est affiché dans le volet CloudBridge Connector configuré. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance Citrix ADC à l'aide des compteurs statistiques de tunnel CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques de tunnel CloudBridge Connector sur une appliance Citrix ADC, consultez Surveillance des tunnels de CloudBridge Connector.

Configuration d'un tunnel CloudBridge Connector entre une appliance Citrix ADC et fortinet FortiGate

August 20, 2021

Vous pouvez configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance Fortinet FortiGate pour connecter deux centres de données ou étendre votre réseau à un fournisseur de cloud. L'appliance Citrix ADC et l'appliance FortiGate forment les points d'extrémité du tunnel CloudBridge Connector et sont appelés homologues.

Exemple de configuration d'un tunnel de connecteur CloudBridge

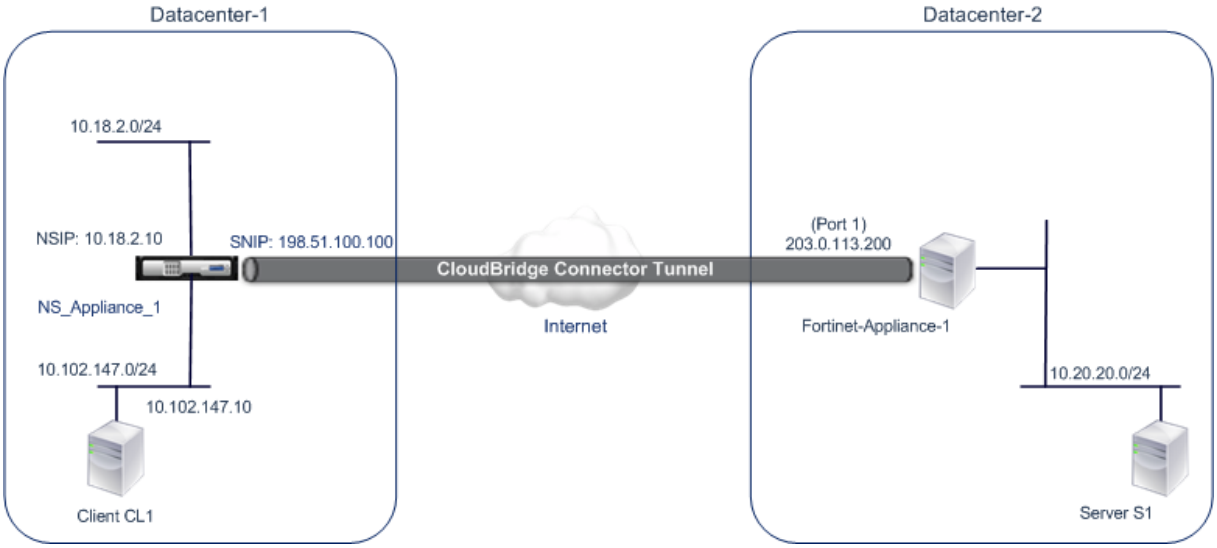
À titre d'illustration du flux de trafic dans un tunnel CloudBridge Connector, considérez un exemple dans lequel un tunnel CloudBridge Connector est configuré entre les périphériques suivants :

- Appliance Citrix ADC NS_Appliance-1 dans un centre de données désigné comme Datacenter-1
- FortiGate appliance Fortigate-Appliance-1 dans un centre de données désigné comme Datacenter-2

NS_Appliance-1 et Fortigate-Appliance-1 permettent la communication entre les réseaux privés dans Datacenter-1 et Datacenter-2 via le tunnel CloudBridge Connector. Dans l'exemple, NS_Appliance-1 et Fortigate-Appliance-1 permettent la communication entre le client CL1 dans Datacenter-1 et le

serveur S1 dans Datacenter-2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel du Connecteur CloudBridge inclut l'entité de profil IPSec NS_Fortinet_IPSEC_Profile, l'entité de tunnel du Connecteur CloudBridge NS_Fortinet_Tunnel et l'entité de routage basé sur des stratégies (PBR) NS_Fortinet_PBR.



Pour plus d'informations, consultez le tableau de configuration du tunnel CloudBridge Connector pdf.

Pour plus d'informations sur les paramètres de Fortinet Fortigate-Appliance-1 dans Datacenter-2, voir le tableau.

Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance FortiGate, tenez compte des points suivants :

- Les paramètres IPsec suivants sont pris en charge pour un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance FortiGate.

Propriétés IPSec	Paramètres
Mode IPsec	Mode tunnel
Version IKE	Version 1
Groupe IKE DH	DH groupe 2 (algorithme MODP 1024 bits)
Méthode d'authentification IKE	Clé pré-partagée
Algorithme de chiffrement IKE	AES
Algorithme de hachage IKE	HMAC SHA1

Propriétés IPSec	Paramètres
Algorithme de chiffrement ESP	AES
Algorithme de hachage ESP	HMAC SHA1

- Vous devez spécifier les mêmes paramètres IPSec sur l'appliance Citrix ADC et l'appliance FortiGate aux deux extrémités du connecteur CloudBridge.
- Citrix ADC fournit un paramètre commun (dans les profils IPSec) pour spécifier un algorithme de hachage IKE et un algorithme de hachage ESP. Il fournit également un autre paramètre commun pour spécifier un algorithme de chiffrement IKE et un algorithme de chiffrement ESP. Par conséquent, dans l'appliance FortiGate, vous devez spécifier le même algorithme de hachage et le même algorithme de chiffrement dans IKE (configuration de phase 1) et ESP (configuration de phase 2).
- Vous devez configurer le pare-feu à l'extrémité Citrix ADC et FortiGate pour autoriser ce qui suit.
  - Tous les paquets UDP pour le port 500
  - Tous les paquets UDP pour le port 4500
  - Tous les paquets ESP (numéro de protocole IP 50)
- L'appliance FortiGate prend en charge deux types de tunnels VPN : basés sur des stratégies et basés sur des routes. Seul un tunnel VPN basé sur des stratégies est pris en charge entre une appliance FortiGate et une appliance Citrix ADC.

Configuration de l'appliance FortiGate pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector sur une appliance FortiGate, utilisez le gestionnaire Web Fortinet, qui est l'interface utilisateur principale pour la configuration, la surveillance et la maintenance des appliances FortiGate.

Avant de commencer la configuration du tunnel CloudBridge Connector sur une appliance FortiGate, assurez-vous que :

- Vous disposez d'un compte d'utilisateur avec des informations d'identification d'administrateur sur l'appliance FortiGate.
- Vous connaissez le gestionnaire basé sur le Web Fortinet.
- L'appliance FortiGate est mise en service, est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.

> **Remarque**
>
> Les procédures de configuration du tunnel CloudBridge Connector sur une appliance FortiGate

> peuvent changer au fil du temps, en fonction du cycle de publication de Fortinet. Citrix vous recommande de suivre la documentation officielle du produit Fortinet concernant la configuration des tunnels VPN IPSec.

Pour configurer un tunnel de connecteur CloudBridge entre une appliance Citrix ADC et une appliance FortiGate, effectuez les tâches suivantes sur l'appliance FortiGate à l'aide du gestionnaire Web Fortinet :

- **Activer la fonctionnalité VPN IPSec basée sur**des stratégies. Activez cette fonctionnalité pour créer des tunnels VPN basés sur des stratégies sur l'appliance FortiGate. Seul le type de tunnel VPN basé sur des stratégies est pris en charge entre une appliance FortiGate et une appliance Citrix ADC. Une configuration de tunnel VPN basée sur des stratégies sur une appliance FortiGate inclut des paramètres de phase 1, de phase 2 et d'une stratégie de sécurité IPsec.
- **Définissez les paramètres de la phase 1.** Les paramètres de phase 1 sont utilisés par l'appliance FortiGate pour l'authentification IKE avant de former un tunnel sécurisé vers l'appliance Citrix ADC.
- **Définissez les paramètres de la phase 2**. Les paramètres de phase 2 sont utilisés par l'appliance FortiGate pour former un tunnel sécurisé vers l'appliance Citrix ADC en établissant des associations de sécurité IKE (SA).
- **Spécifiez les sous-réseaux privés**. Définissez les sous-réseaux privés côté Fortigate et Citrix côté ADC dont le trafic IP doit être transporté par le tunnel.
- **Définissez une stratégie de sécurité IPSec pour le tunnel**. Une stratégie de sécurité permet au trafic IP de passer entre les interfaces sur une appliance FortiGate. Une stratégie de sécurité IPSec spécifie l'interface vers le sous-réseau privé et l'interface reliant l'appliance Citrix ADC via le tunnel.

Pour activer la fonctionnalité VPN IPSec basée sur une stratégie à l'aide du Gestionnaire basé sur le Web Fortinet

1. Accédez à **Système** > **Config** > **Fonctionnalités** .
2. Sur la page **Paramètres de fonctionnalité**, sélectionnez **Afficher plus** et activez le **VPN IPSec basé** sur des stratégies.

Pour définir des paramètres de phase 1 à l'aide du gestionnaire Web Fortinet

1. Accédez à **VPN** > **IPsec** > **Auto Key (IKE)** et cliquez sur **Create Phase1** .
2. Dans la page **Nouvelle phase 1**, définissez les paramètres suivants :
   - Nom : Entrez un nom pour cette configuration de phase 1.
   - Passerelle distante : sélectionnez *Adresse IP statique.*
   - Mode : sélectionnez *Principal (Protection de l'ID)*.
   - Méthode d'authentification : sélectionnez *Clé pré-partagée*.
   - Clé pré-partagée : Entrez une clé pré-partagée. La même clé pré-partagée doit être configurée sur l'appliance Citrix ADC.

- Options homologues : définissez les paramètres IKE suivants pour l'authentification d'une appliance Citrix ADC.
  - Version IKE : Sélectionnez *1*.
  - Mode Config : désactivez cette option si elle est sélectionnée.
  - IP de la passerelle locale : sélectionnez *IP de l'interface principale*.
  - Proposition P1 : Sélectionnez les algorithmes de chiffrement et d'authentification pour l'authentification IKE avant de former un tunnel sécurisé vers l'appliance Citrix ADC.
    - 1 - Chiffrement : sélectionnez *AES128*.
    - Authentification : sélectionnez *SHA1*.
    - Vie des clés : Entrez un délai (en secondes) pour la durée de vie de la clé de phase 1.
    - Groupe DH : sélectionnez 2.
  - X-Auth : sélectionnez *Désactiver*.
  - Deed Peer Detection : sélectionnez cette option.

3. Cliquez sur **OK**.

Pour spécifier des sous-réseaux privés à l'aide du Gestionnaire basé sur le Web Fortinet

1. Accédez à **Objets pare-feu** > **Adresse** > **Adresses** et sélectionnez **Créer un nouveau** .
2. Dans la page **Nouvelle adresse**, définissez les paramètres suivants :
   - Nom : Entrez un nom pour le sous-réseau côté Fortigate.
   - Type : Sélectionnez *Sous-réseau*.
   - Sous-réseau/Plage IP : Entrez l'adresse du sous-réseau côté Fortigate.
   - Interface : sélectionnez l'interface locale de ce sous-réseau.
3. Cliquez sur **OK**.
4. Répétez les étapes 1 à 3 pour spécifier le sous-réseau côté ADC Citrix.

Pour définir des paramètres de phase 2 à l'aide du gestionnaire Web Fortinet

1. Accédez à **VPN** > **IPSec** > **Auto Key (IKE)** et cliquez sur **Créer Phase 2** .
2. Dans la page **Nouvelle phase 2**, définissez les paramètres suivants :
   - Nom : Entrez un nom pour cette configuration de phase 2.
   - Phase 1 : Sélectionnez la configuration Phase 1 dans la liste déroulante.
3. Cliquez sur **Avancé** et définissez les paramètres suivants :
   - Proposition P2 : sélectionnez les algorithmes de chiffrement et d'authentification pour former un tunnel sécurisé vers l'appliance Citrix ADC.
     - 1 - Chiffrement : sélectionnez *AES128*.
     - Authentification : sélectionnez *SHA1*.
     - Activer la détection de relecture : sélectionnez cette option.
     - Activer le secret avant parfait (PFS) : sélectionnez cette option.
     - Groupe DH : sélectionnez *2*.

- Vie des clés : Entrez un délai (en secondes) pour la durée de vie de la clé de phase 2.
- Autokey Keep Alive : sélectionnez cette option.
- Négociation automatique : sélectionnez cette option.
- Sélecteur de mode rapide : spécifiez les sous-réseaux privés côté Fortigate et Citrix côté ADC dont le trafic doit être traversé par le tunnel.
  - Adresse source : sélectionnez le sous-réseau côté Fortigate dans la liste déroulante.
  - Port source : saisissez *0*.
  - Adresse de destination : sélectionnez le sous-réseau Citrix côté ADC dans la liste déroulante.
  - Port de destination : Entrez *0*.
  - Protocole : Entrez *0*.

4. Cliquez sur **OK**.

Pour définir une stratégie de sécurité IPSec à l'aide du Gestionnaire basé sur le Web Fortinet

1. Accédez à **Stratégie** > **Stratégie** > **Stratégie**, puis cliquez sur **Créer un nouveau**.
2. Dans la page **Modifier la stratégie**, définissez les paramètres suivants :
   - Type de stratégie : sélectionnez *VPN*.
   - Sous-type de stratégie : sélectionnez *IPSec*.
   - Interface locale : sélectionnez l'interface locale du réseau interne (privé).
   - Sous-réseau protégé local : sélectionnez le sous-réseau côté Fortigate dans la liste déroulante dont le trafic doit être traversé par le tunnel.
   - Interface VPN sortante : sélectionnez l'interface locale vers le réseau externe (public).
   - Sous-réseau protégé à distance : sélectionnez le sous-réseau Citrix côté ADC dans la liste déroulante dont le trafic doit être traversé par le tunnel.
   - Planification : conservez le paramètre par défaut (*toujours*) sauf si des modifications sont nécessaires pour répondre à des exigences spécifiques.
   - Service : Conservez le paramètre par défaut (*ANY*) sauf si des modifications sont nécessaires pour répondre à vos besoins spécifiques.
   - Tunnel VPN : sélectionnez *Utiliser l'existant* et sélectionnez le tunnel dans la liste déroulante.
   - Autoriser l'initialisation du trafic à partir du site distant : sélectionnez si le trafic provenant du réseau distant sera autorisé à initier le tunnel.
3. Cliquez sur **OK**.

Configuration de l'appliance Citrix ADC pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance FortiGate, effectuez les tâches suivantes sur l'appliance Citrix ADC. Vous pouvez utiliser la ligne de commande Citrix ADC ou l'interface utilisateur graphique (GUI) Citrix ADC :

- **Créez un profil IPSec**. Une entité de profil IPsec spécifie les paramètres du protocole IPSec,

tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et la méthode d'authentification à utiliser par le protocole IPSec dans le tunnel CloudBridge Connector.

- **Créez un tunnel IP qui utilise le protocole IPSec et associez le profil IPSec à celui-ci**. Un tunnel IP spécifie l'adresse IP locale (adresse IP du point de terminaison du tunnel CloudBridge Connector (de type SNIP) configurée sur l'appliance Citrix ADC), l'adresse IP distante (adresse IP du point de terminaison du tunnel CloudBridge Connector configurée sur l'appliance FortiGate), le protocole (IPsec) utilisé pour configurer CloudBridge Tunnel de connecteur et une entité de profil IPsec. L'entité de tunnel IP créée est également appelée entité de tunnel CloudBridge Connector.
- **Créez une règle PBR et associez-la au tunnel IP**. Une entité PBR spécifie un ensemble de règles et une entité tunnel IP (tunnel CloudBridge Connector). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Définissez la plage d'adresses IP source pour spécifier le sous-réseau côté Citrix ADC dont le trafic doit être protégé sur le tunnel, et définissez la plage d'adresses IP de destination pour spécifier le sous-réseau côté appliance FortiGate dont le trafic doit être protégé sur le tunnel.

Pour créer un profil IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecy ENABLE`
- `show ipsec profile <name>`

Pour créer un tunnel IPSEC et lier le profil IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName** <string>`
- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Pour créer un profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > **Profil IPsec**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Ajouter un profil IPSec**, définissez les paramètres suivants :
    - Nom

- Algorithme de chiffrement
- Algorithme de hachage
- Version du protocole IKE
- Perfect Forward Secrecy (Activer ce paramètre)

4. Configurez la méthode d'authentification IPsec à utiliser par les deux homologues de tunnel CloudBridge Connector pour s'authentifier mutuellement : sélectionnez la méthode d'authentification de clé pré-partagée et définissez le paramètre Clé pré-partagée Exists.
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et lier le profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.
2. Dans l'onglet **Tunnels IPv4**, cliquez sur **Ajouter**.
3. Dans la page **Ajouter un tunnel IP**, définissez les paramètres suivants :
   - Nom
   - IP distante
   - Masque distant
   - Type IP local (dans la liste déroulante Type IP local, sélectionnez *IP du sous-réseau*).
   - IP locale (Toutes les adresses IP configurées du type IP sélectionné se trouvent dans la liste déroulante IP locale. Sélectionnez l'adresse IP souhaitée dans la liste.)
   - Protocole
   - Profil IPsec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Dans la page **Créer un PBR**, définissez les paramètres suivants :
   - Nom
   - Action
   - Type de saut suivant (Select *IP Tunnel*)
   - Nom du tunnel IP
   - IP source Faible
   - IP source élevée
   - IP de destination faible
   - IP de destination élevée
4. Cliquez sur **Créer**, puis sur **Fermer**.

La nouvelle configuration de tunnel CloudBridge Connector correspondante sur l'appliance Citrix ADC apparaît dans l'interface graphique.

L'état actuel du tunnel de connecteur CloudBridge est affiché dans le volet CloudBridge Connector configuré. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est

arrêté.

Les commandes suivantes créent les paramètres de l'appliance Citrix ADC NS_Appliance-1 dans "Exemple de configuration du connecteur CloudBridge."

```
1      > add ipsec profile NS_Fortinet_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1 -encAlgo AES -hashalgo
          HMAC_SHA1 -lifetime 315360 -perfectForwardSecrecy ENABLE
2
3       Done
4      > add iptunnel NS_Fortinet_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100 -protocol IPSEC -ipsecProfileName
          NS_Fortinet_IPSec_Profile
5
6       Done
7      > add pbr NS_Fortinet_Pbr -srcIP 10.102.147.0-10.102.147.255 -
          destIP 10.20.0.0-10.20.255.255 -ipTunnel NS_Fortinet_Tunnel
8
9       Done
10     > apply pbrs
11
12      Done
13 <!--NeedCopy-->
```

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance Citrix ADC à l'aide des compteurs statistiques de tunnel CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques de tunnel CloudBridge Connector sur une appliance Citrix ADC, consultez Surveillance des tunnels de CloudBridge Connector.

Diagnostic et dépannage du tunnel CloudBridge Connector

August 20, 2021

Si vous rencontrez des problèmes avec une configuration de tunnel CloudBridge Connector, assurez-vous que toutes les conditions préalables ont été respectées avant la configuration du tunnel. Le cas échéant, le problème peut être lié aux adresses IP du point de terminaison du tunnel, à une configuration NAT, à la façon dont le tunnel a été configuré ou au trafic de données.

Dépannage d'un tunnel CloudBridge Connector

Si votre tunnel CloudBridge Connector ne fonctionne pas correctement, le problème peut être lié à l'établissement du tunnel ou au trafic de données. Si vous ne savez pas quel type de problème vous avez, recherchez un message d'erreur dans le fichier journal et vérifiez si le message d'erreur figure dans la liste des problèmes d'établissement du tunnel. Si vous ne trouvez pas votre message d'erreur, consultez la liste des problèmes possibles liés au trafic de données.

Questions liées à l'établissement des tunnels

Une fois que les conditions requises pour configurer le tunnel IPSec sont remplies et que le tunnel CloudBridge Connector est configuré, si l'état du tunnel n'est pas UP, recherchez les informations de débogage dans le fichier iked.log sur une ou les deux appliances Citrix ADC configurées comme points d'extrémité du tunnel.

Sur l'une ou l'autre des solutions matérielles, tapez la commande suivante à l'invite de shell Citrix ADC :

```
cat /tmp/iked.debug | tee /var/iked.log
```

Le fichier PDF de dépannage répertorie certaines erreurs courantes et leurs solutions.

Problèmes liés au trafic de données

Si les données du tunnel CloudBridge Connector ne sont pas échangées correctement entre les points d'extrémité du tunnel, procédez comme suit.

- Pour un tunnel CloudBridge Connector qui utilise les protocoles GRE et IPsec :
  - Assurez-vous que le mode L2 est activé sur les deux points d'extrémité du tunnel CloudBridge Connector. Pour activer le mode L2, tapez la commande suivante dans l'interface de ligne de commande Citrix ADC :

    ```
    enable mode L2
    ```

    * Si l'un des points d'extrémité du tunnel CloudBridge Connector est un dispositif virtuel CloudBridge (VPX) et est provisionné sur un Hypervisor VMware ESXi, assurez-vous que le mode Promiscuous est défini sur Accepter pour le vSwitch associé à l'appliance CloudBridge VPX.
  - Si un VLAN est étendu via un tunnel CloudBridge Connector, vérifiez le mappage un-à-un sur l'entité VLAN étendu sur chacun des points d'extrémité du tunnel
  - Assurez-vous que l'entité de tunnel IP est liée à l'entité netbridge correcte dans chacun des points d'extrémité du tunnel.
  - Vérifiez que l'entrée ARP du point d'extrémité du tunnel CloudBridge Connector homologue existe sur le point d'extrémité du tunnel local, en tapant la commande suivante dans l'interface de ligne de commande Citrix ADC :


```
show arp
```

- Si la sortie affiche une entrée ARP incomplète, le trafic bidirectionnel ne circule pas dans le tunnel. Si le trafic bidirectionnel circule, l'entrée ARP indique le nom de l'interface tunnel pour les périphériques de l'autre côté du tunnel.
- Supprimez les entités de tunnel IP des deux points d'extrémité du tunnel et ajoutez-les à nouveau avec les mêmes paramètres, mais avec le profil IPSec défini sur NONE, de sorte que le tunnel utilise uniquement le protocole GRE.

  Après avoir vérifié ce qui suit dans le tunnel IP (qui utilise le protocole GRE), configurez le tunnel avec les paramètres IPSec en spécifiant un profil IPSec valide pour les entités de tunnel IP respectives sur chacun des points d'extrémité du tunnel.

  Flux PING ou TCP correct à travers le tunnel.

  Flux correct du trafic de données à travers le tunnel.

  Une fois que le tunnel configuré (qui utilise les protocoles GRE et IPSec) est en état UP, si le trafic de données ne circule pas correctement dans le tunnel et si un périphérique NAT a été déployé devant l'un des points d'extrémité du tunnel ou les deux, analysez les paquets d'entrée et de sortie sur les périphériques NAT.

- Si une appliance Citrix ADC est utilisée en tant que routeur ou passerelle.
  - Assurez-vous que le mode L3 est activé sur l'appliance Citrix ADC. Pour activer le mode L3, exécutez la commande suivante dans la ligne de commande CloudBridge.
  - activer le mode L3
  - Si les sous-réseaux sont liés à une entité netbridge, assurez-vous que l'entité de tunnel IP correcte est également liée à netbridge.
  - Exécutez la commande suivante dans la ligne de commande Citrix ADC pour voir où les paquets (entrée et sortie) sont supprimés :

    ```
    stat ipsec counters
    ```
  - Assurez-vous que les itinéraires corrects sont configurés sur les deux points d'extrémité du tunnel.
  - Si aucun périphérique NAT n'est déployé devant l'appliance Citrix ADC, assurez-vous que les pare-feu sont configurés pour autoriser tous les paquets ESP (IP protocol number 50) et tous les paquets UDP pour le port 4500.

Si aucune des mesures ci-dessus n'entraîne un échange réussi de trafic entre les points d'extrémité du tunnel, contactez le support technique Citrix.

Liste de contrôle avant de contacter le support technique Citrix

Pour une résolution rapide, assurez-vous que les éléments suivants sont prêts avant de contacter le support technique Citrix.

- Détails du déploiement et de la topologie du réseau.
- Fichier journal collecté en tapant la commande suivante à l'invite de shell Citrix ADC.


```
cat /tmp/iked.debug | tee /var/log/iked.log
```

- Pack de support technique capturé en tapant la commande suivante sur la ligne de commande Citrix ADC.
  ```
  show techsupport
  ```
- Traces de paquets capturés sur les deux points d'extrémité du tunnel CloudBridge Connector. Pour démarrer une trace de paquets, tapez la commande suivante sur la ligne de commande Citrix ADC.
  ```
  start nstrace -size 0
  ```
  Pour arrêter le suivi des paquets, tapez la commande suivante sur la ligne de commande Citrix ADC.
  ```
  stop nstrace
  ```
- Sortie de la commande suivante tapée à l'invite de commande Citrix ADC.
  ```
  show arp
  ```

Interopérabilité du connecteur CloudBridge — StrongSwan

October 4, 2021

StrongSwan est une implémentation IPsec opensource pour les plates-formes Linux. Vous pouvez configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance StrongSwan pour connecter deux centres de données ou étendre votre réseau à un fournisseur de cloud. L'appliance Citrix ADC et l'appliance StrongSwan forment les points d'extrémité du tunnel CloudBridge Connector et sont appelés homologues.

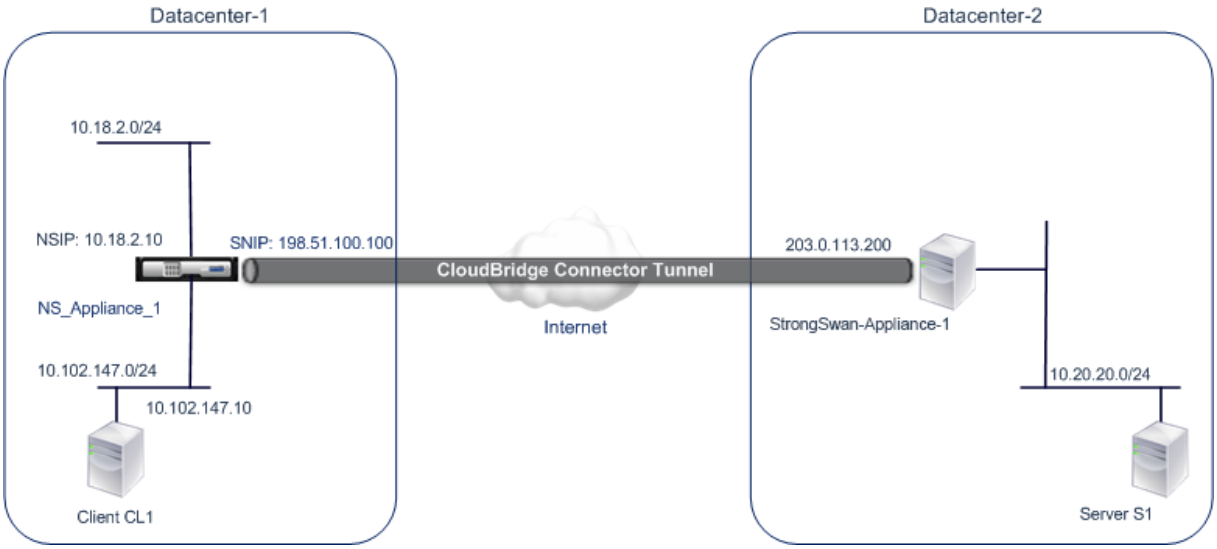
Exemple de configuration de tunnel CloudBridge Connector

À titre d'illustration du flux de trafic dans un tunnel CloudBridge Connector, considérez un exemple dans lequel un tunnel CloudBridge Connector est configuré entre les périphériques suivants :

- Appliance Citrix ADC NS_Appliance-1 dans un centre de données désigné comme Datacenter-1
- Appliance StrongSwan StrongSwan-Appliance-1 dans un centre de données désigné comme Datacenter-2

NS_Appliance-1 et Strongswan-Appliance-1 permettent la communication entre les réseaux privés dans Datacenter-1 et Datacenter-2 via le tunnel CloudBridge Connector. Dans l'exemple, NS_Appliance-1 et Strongswan-Appliance-1 permettent la communication entre le client CL1 dans Datacenter-1 et le serveur S1 dans Datacenter-2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel du Connecteur CloudBridge inclut l'entité de profil IPSec NS_StrongSwan_IPSEC_Profile, l'entité de tunnel du Connecteur CloudBridge NS_StrongSwan_Tunnel et l'entité de routage basé sur des stratégies (PBR) NS_StrongSwan_PBR.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Paramètres principaux de la configuration du tunnel CloudBridge Connector

Entité	Détails
Adresse IP du point d'extrémité du tunnel CloudBridge Connector (NS_Appliance-1) dans Datacenter-1	198.51.100.100
Adresse IP du point d'extrémité du tunnel CloudBridge Connector (Strongswan-Appliance-1) dans Datacenter-2	203.0.113.200
Centre de données : sous-réseau de 1 dont le trafic doit être protégé sur le tunnel CloudBridge Connector	10.102.147.0/24
Datacenter : sous-réseau de 2 dont le trafic doit être protégé sur le tunnel CloudBridge Connector	10.20.20.0/24

Paramètres sur l'appliance Citrix ADC NS_Appliance-1 dans Datacenter-1

SNIP1 (à titre de référence uniquement)	198.51.100.100	
Profil IPSec	NS_STRONGSwan_IPSEC_PROF	Version IKE : v1, Algorithme de chiffrement : AES, Algorithme de hachage : HMAC_SHA1
psk = examplepresharedkey (Remarque : Ceci est un exemple de clé pré-partage, à titre d'illustration. Citrix ne recommande pas d'utiliser cette chaîne dans votre configuration CloudBridge Connector)		
Tunnel du Connecteur CloudBridge	NS_StrongSwan_Tunnel	IP distante = 203.0.113.200, IP locale = 198.51.100.100, protocole tunnel = IPSEC, profil IPSec = NS_Strongswan_IPsec_Profile
Routes basées sur des politiques_strongswan_PBR	Plage IP source = Sous-réseau dans le Datacenter-1=10.102.147.0-10.102.147.255, Plage IP de destination =Sous-réseau dans Datacenter-2=10.20.20.0-10.20.20.255, Tunnel IP = Ns_strongswan_Tunnel	

Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de commencer à configurer le tunnel du connecteur CloudBridge, assurez-vous que :

- Vous avez une connaissance de base sur les configurations Linux.
- Vous avez une connaissance de base sur la suite de protocoles IPSec.
- L'appliance StrongSwan est opérationnelle et est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.
- L'appliance Citrix ADC est mise en service et en cours d'exécution, est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel

CloudBridge Connector.

- Les paramètres IPsec suivants sont pris en charge pour un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance StrongSwan.
  - Mode IPSec : mode Tunnel
  - Version IKE : Version 1
  - Méthode d'authentification IKE : Clé pré-partagée
  - Algorithme de chiffrement IKE : AES
  - Algorithme de hachage IKE : HMAC SHA1
  - Algorithme de chiffrement ESP : AES
  - Algorithme de hachage ESP : HMAC SHA1
- Vous devez spécifier les mêmes paramètres IPSec sur l'appliance Citrix ADC et StrongSwan aux deux extrémités du tunnel CloudBridge Connector.
- Citrix ADC fournit un paramètre commun (dans les profils IPSec) pour spécifier un algorithme de hachage IKE et un algorithme de hachage ESP. Il fournit également un autre paramètre commun pour spécifier un algorithme de chiffrement IKE et un algorithme de chiffrement ESP. Par conséquent, dans l'appliance StrongSwan, vous devez spécifier le même algorithme de hachage et le même algorithme de chiffrement dans les paramètres IKE et ESP du fichier Ipsec.conf.
- Vous devez configurer le pare-feu à l'extrémité Citrix ADC et StrongSwan pour autoriser ce qui suit.
  - Tous les paquets UDP pour le port 500
  - Tous les paquets UDP pour le port 4500
  - Tous les paquets ESP (numéro de protocole IP 50)

Configurer StrongSwan pour le tunnel CloudBridge Connector

Pour configurer un tunnel de connecteur CloudBridge entre une appliance Citrix ADC et une appliance StrongSwan, effectuez les tâches suivantes sur l'appliance StrongSwan :

- **Spécifiez les informations de connexion IPsec dans le fichier ipsec.conf**. Le fichier ipsec.conf définit toutes les informations de contrôle et de configuration pour les connexions IPsec dans l'appliance StrongSwan.
- **Spécifiez une clé pré-partagée dans le fichier ipsec.secrets**. Le fichier ipsec.secrets définit les secrets pour l'authentification IKE/IPSec pour les connexions IPsec dans l'appliance StrongsWan.

Les procédures de configuration du VPN IPSec (tunnel CloudBridge Connector) sur une appliance StrongSwan peuvent changer au fil du temps, en fonction du cycle de publication de StrongSwan. Citrix vous recommande de suivre la documentation officielle de StrongSwan sur la configuration des tunnels VPN IPSec.

L'exemple suivant d'extrait du fichier ipsec.conf spécifie les informations IPsec pour la configuration du tunnel VPN IPSec, décrites dans la rubrique Exemple de configuration du connecteur CloudBridge.

Pour plus d'informations, consultez la section Configuration du CloudBridge Connector pdf.

L'exemple suivant d'extrait du fichier ipsec.secrets spécifie la clé pré-partagée d'authentification IKE pour la configuration du tunnel VPN IPSec, décrite dans la rubrique Exemple de configuration du connecteur CloudBridge.

`/etc/ipsec.secrets` clé partagée PSK 'exemplepresharedkey' #pre -pour l'authentification IKE IPsec

Configuration de l'appliance Citrix ADC pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance StrongSwan, effectuez les tâches suivantes sur l'appliance Citrix ADC. Vous pouvez utiliser la ligne de commande Citrix ADC ou l'interface utilisateur graphique (GUI) Citrix ADC :

- **Créez un profil IPSec**. Une entité de profil IPsec spécifie les paramètres du protocole IPSec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et la méthode d'authentification à utiliser par le protocole IPSec dans le tunnel CloudBridge Connector.
- **Créez un tunnel IP qui utilise le protocole IPSec et associez le profil IPSec à celui-ci**. Un tunnel IP spécifie l'adresse IP locale (adresse IP du point de terminaison du tunnel CloudBridge Connector (de type SNIP) configurée sur l'appliance Citrix ADC), l'adresse IP distante (adresse IP du point de terminaison du tunnel CloudBridge Connector configurée sur l'appliance StrongsWan), le protocole (IPsec) utilisé pour configurer CloudBridge Tunnel de connecteur et une entité de profil IPsec. L'entité de tunnel IP créée est également appelée entité de tunnel CloudBridge Connector.
- **Créez une règle PBR et associez-la au tunnel IP**. Une entité PBR spécifie un ensemble de règles et une entité tunnel IP (tunnel CloudBridge Connector). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Définissez la plage d'adresses IP source pour spécifier le sous-réseau côté Citrix ADC dont le trafic doit être protégé sur le tunnel, et définissez la plage d'adresses IP de destination pour spécifier le sous-réseau côté StrongSwan dont le trafic doit être protégé sur le tunnel.

Pour créer un profil IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1`
- `show ipsec profile <name>`

Pour créer un tunnel IPSEC et lier le profil IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`

- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Pour créer un profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **ConnecteurCloudBridge**>**ProfilIPsec**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Ajouter un profil IPSec**, définissez les paramètres suivants :
   - Nom
   - Algorithme de chiffrement
   - Algorithme de hachage
   - Version du protocole IKE
4. Configurez la méthode d'authentification IPsec à utiliser par les deux homologues de tunnel CloudBridge Connector pour s'authentifier mutuellement : sélectionnez la **méthode d'authentification de clé pré-partagée** et définissez le paramètre **Clé pré-partagée Exists**.
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et lier le profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.
2. Dans l'onglet **Tunnels IPv4**, cliquez sur **Ajouter**.
3. Dans la page Ajouter un tunnel IP, définissez les paramètres suivants :
   - Nom
   - IP distante
   - Masque distant
   - Type IP local (dans la liste déroulante Type IP local, sélectionnez *IP du sous-réseau*).
   - IP locale (Toutes les adresses IP configurées du type IP sélectionné se trouvent dans la liste déroulante IP locale. Sélectionnez l'adresse IP souhaitée dans la liste.)
   - Protocole
   - Profil IPsec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Dans la page **Créer un PBR**, définissez les paramètres suivants :

- Nom
- Action
- Type de saut suivant (Select *IP Tunnel*)
- Nom du tunnel IP
- IP source Faible
- IP source élevée
- IP de destination faible
- IP de destination élevée

4. Cliquez sur **Créer**, puis sur **Fermer**.

La nouvelle configuration de tunnel CloudBridge Connector correspondante sur l'appliance Citrix ADC apparaît dans l'interface graphique. L'état actuel du tunnel de connecteur CloudBridge est affiché dans le volet CloudBridge Connector configuré. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.
Les commandes suivantes créent les paramètres de l'appliance Citrix ADC NS_Appliance-1 dans « Exemple de configuration du connecteur CloudBridge :

```
1      > add ipsec profile NS_StrongSwan_IPSec_Profile -psk
           examplepresharedkey -ikeVersion v1 - encAlgo AES - hashalgo
           HMAC_SHA1
2
3
4      Done
5
6      > add iptunnel NS_StrongSwan_Tunnel 203.0.113.200 255.255.255.255
           198.51.100.100 - protocol IPSEC - ipsecProfileName
           NS_StrongSwan_IPSec_Profile
7
8
9      Done
10
11     > add pbr NS_StrongSwan_Pbr -srcIP 10.102.147.0-10.102.147.255 -
           destIP 10.20.0.0-10.20.255.255 - ipTunnel NS_StrongSwan_Tunnel
12
13
14     Done
15
16     > apply pbrs
17
18
19     Done
20 <!--NeedCopy-->
```


Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance Citrix ADC à l'aide des compteurs statistiques de tunnel CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques de tunnel CloudBridge Connector sur une appliance Citrix ADC, consultez Surveillance des tunnels de CloudBridge Connector.

Interopérabilité du connecteur CloudBridge — F5 BIG-IP

August 20, 2021

Vous pouvez configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance BIG-IP F5 pour connecter deux centres de données ou étendre votre réseau à un fournisseur de cloud. L'appliance Citrix ADC et l'appliance BIG-IP F5 forment les points d'extrémité du tunnel CloudBridge Connector et sont appelés homologues.

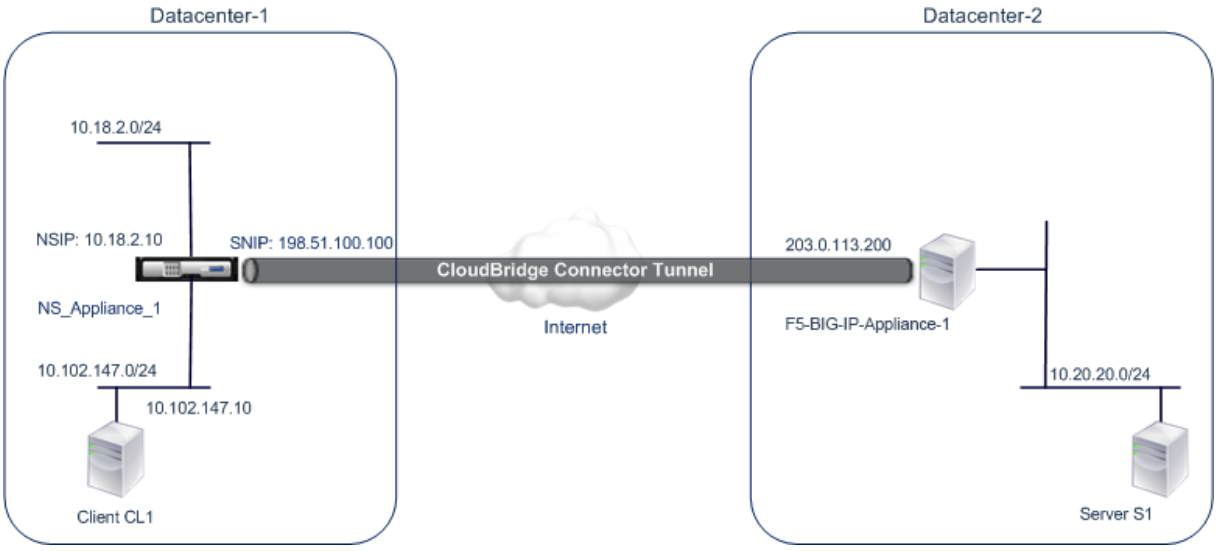
Exemple de configuration de tunnel CloudBridge Connector

À titre d'illustration du flux de trafic dans un tunnel CloudBridge Connector, considérez un exemple dans lequel un tunnel CloudBridge Connector est configuré entre les périphériques suivants :

- Appliance Citrix ADC NS_Appliance-1 dans un centre de données désigné comme Datacenter-1
- Appliance F5 BIG-IP F5-BIG-IP-Appliance-1 dans un centre de données désigné comme Datacenter-2

NS_Appliance-1 et F5-Big-IP-Appliance-1 permettent la communication entre les réseaux privés dans Datacenter-1 et Datacenter-2 via le tunnel CloudBridge Connector. Dans l'exemple, NS_Appliance-1 et F5-Big-IP-Appliance-1 permettent la communication entre le client CL1 dans Datacenter-1 et le serveur S1 dans Datacenter-2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel du connecteur CloudBridge inclut l'entité de profil IPSec NS_F5-Big-IP_IPSEC_Profile, l'entité de tunnel du connecteur CloudBridge NS_F5-big-IP_Tunnel et l'entité de routage basé sur des stratégies (PBR) NS_F5-big-IP_PBR.



Pour plus d'informations, reportez-vous à F5 big IP pdf.

Points à considérer pour une configuration de tunnel CloudBridge Connector

- L'appliance Citrix ADC est mise en service et en cours d'exécution, est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.
- L'appliance F5 BIG-IP est mise en service et fonctionne, est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.
- Les paramètres IPsec suivants sont pris en charge pour un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance BIG-IP F5.
  - Mode IPSec : mode Tunnel
  - Version IKE : Version 1
  - Méthode d'authentification IKE : Clé pré-partagée
  - Algorithme de chiffrement IKE : AES
  - Algorithme de hachage IKE : HMAC SHA1
  - Algorithme de chiffrement ESP : AES
  - Algorithme de hachage ESP : HMAC SHA1
- Vous devez spécifier les mêmes paramètres IPSec sur l'appliance Citrix ADC et l'appliance F5 BIG-IP aux deux extrémités du tunnel CloudBridge Connector.
- Citrix ADC fournit un paramètre commun (dans les profils IPSec) pour spécifier un algorithme de hachage IKE et un algorithme de hachage ESP. Il fournit également un autre paramètre commun pour spécifier un algorithme de chiffrement IKE et un algorithme de chiffrement ESP. Par conséquent, dans l'appliance F5 BIG-IP, vous devez spécifier le même algorithme de hachage et le même algorithme de chiffrement dans IKE (configuration de phase 1) et ESP (configuration

de phase 2).

- Vous devez configurer le pare-feu à l'extrémité Citrix ADC et à l'extrémité F5 BIG-IP pour autoriser ce qui suit.
  - Tous les paquets UDP pour le port 500
  - Tous les paquets UDP pour le port 4500
  - Tous les paquets ESP (numéro de protocole IP 50)

Configuration de F5 BIG-IP pour le tunnel CloudBridge Connector

Pour configurer un tunnel de connecteur CloudBridge entre une appliance Citrix ADC et une appliance BIG-IP F5, effectuez les tâches suivantes sur l'appliance F5 BIG-IP :

- **Créez un serveur virtuel de transfert pour IPsec**. Un serveur virtuel de transfert intercepte le trafic IP pour le tunnel IPsec.
- **Créez un pair IKE.** Un homologue IKE spécifie les points de terminaison du tunnel IPSec locaux et distants. Il spécifie également les algorithmes et les informations d'identification à utiliser pour IPSec IKE phase 1.
- **Créez une stratégie IPsec personnalisée.** Une stratégie spécifie le protocole IPsec (ESP) et le mode (tunnel) à utiliser pour former le tunnel IPsec. Il spécifie également les algorithmes et les paramètres de sécurité à utiliser pour IKE IPSec phase 2.
- **Créez un sélecteur de trafic IPSec bidirectionnel**. Un sélecteur de trafic spécifie les sous-réseaux F5 BIG-IP et Citrix ADC dont le trafic IP doit être traversé par le tunnel IPsec.

Les procédures de configuration du VPN IPSec (tunnel CloudBridge Connector) sur une appliance BIG-IP F5 peuvent changer au fil du temps, en fonction du cycle de publication F5. Citrix vous recommande de suivre la documentation officielle F5 BIG-IP pour configurer les tunnels VPN IPsec, à l'adresse suivante :

https://f5.com

Pour créer un serveur virtuel de transfert pour IPSec à l'aide de l'interface graphique BIG-IP F5

1. Sous l'onglet **Principal**, cliquez sur **Trafic local** > **Serveurs virtuels**, puis cliquez sur **Créer**.
2. Dans l'écran **Nouvelle liste de serveurs virtuels**, définissez les paramètres suivants :
   - **Nom**. Tapez un nom unique pour le serveur virtuel.
   - **Type**. Sélectionnez **Transfert (IP)**.
   - **Adresse de destination**. Tapez une adresse réseau générique au format CIDR, par exemple, 0.0.0.0/0 pour IPv4 pour accepter tout trafic.
   - **Port de service**. Sélectionnez **Tous les ports** dans la liste.
   - **Liste des protocoles**. Sélectionnez **Tous les protocoles** dans la liste.
   - **VLAN et trafic tunnel**. Conservez la sélection par défaut **Tous les VLAN et tunnels**.
3. Cliquez sur **Terminé**.

Pour créer une stratégie IPsec personnalisée à l'aide de l'interface graphique BIG-IP F5

1. Sous l'onglet **Principal**, cliquez sur **Réseau** > **IPSec** > **Stratégies IPsec**, puis cliquez sur **Créer**.
2. Dans l'écran **Nouvelle stratégie**, définissez les paramètres suivants :
   - **Nom**. Tapez un nom unique pour la stratégie.
   - **Protocole IPsec**. Conservez la sélection par défaut, ESP.
   - **Mode**. Sélectionnez Tunnel. L'écran s'actualise pour afficher d'autres paramètres associés.
   - **Adresse locale du tunnel**. Tapez l'adresse IP du point de terminaison du tunnel IPSec local (configurée sur l'appliance BIG-IP F5).
   - **Adresse distante du tunnel**. Tapez l'adresse IP du point de terminaison du tunnel IPSec distant (configurée sur l'appliance Citrix ADC).
3. Pour les paramètres IKE Phase 2, conservez les valeurs par défaut ou sélectionnez les options appropriées pour votre déploiement.
4. Cliquez sur **Terminé**.

Pour créer un sélecteur de trafic IPSec bidirectionnel à l'aide de l'interface graphique BIG-IP F5

1. Sous l'onglet **Principal**, cliquez sur **Réseau** > **IPsec** > **Sélecteurs de trafic**, puis cliquez sur **Créer**.
2. Dans l'écran **Nouveau sélecteur de trafic**, définissez les paramètres suivants :
   - **Nom**. Tapez un nom unique pour le sélecteur de trafic.
   - **Ordre**. Conservez la valeur par défaut **(First)**. Ce paramètre spécifie l'ordre dans lequel le sélecteur de trafic apparaît sur l'écran Liste des sélecteurs de trafic.
3. Dans la liste **Configuration**, sélectionnez **Avancé** et définissez les paramètres suivants :
   - **Adresse IP source**. Cliquez sur **Hôte** ou **Réseau**, et dans le champ **Adresse**, tapez l'adresse du sous-réseau côté BIG-IP F5 dont le trafic doit être protégé via le tunnel IPSec.
   - **Port source**. Sélectionnez *** Tous les ports**.
   - **Adresse IP de destination**. Cliquez sur **Hôte**et, dans le champ **Adresse**, tapez l'adresse du sous-réseau côté Citrix ADC dont le trafic doit être protégé sur le tunnel IPSec.
   - **Port de destination**. Sélectionnez *** Tous les ports**.
   - **Protocole**. Sélectionnez *** Tous les protocoles**.
   - **Direction**. Sélectionnez **les deux**.
   - **Action**. Sélectionnez **Protéger**. Le paramètre **Nom de la stratégie IPSec** s'affiche.
   - **Nom de la stratégie IPSec**. Sélectionnez le nom de la stratégie IPsec personnalisée que vous avez créée.
4. Cliquez sur **Terminé**.

Configuration de l'appliance Citrix ADC pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance BIG-IP F5, effectuez les tâches suivantes sur l'appliance Citrix ADC. Vous pouvez utiliser la ligne de commande Citrix ADC ou l'interface utilisateur graphique (GUI) Citrix ADC :

- **Créez un profil IPSec**. Une entité de profil IPsec spécifie les paramètres du protocole IPSec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et la méthode d'authentification à utiliser par le protocole IPSec dans le tunnel CloudBridge Connector.
- **Créez un tunnel IP qui utilise le protocole IPSec et associez le profil IPSec à celui-ci**. Un tunnel IP spécifie l'adresse IP locale (adresse IP du point d'extrémité du tunnel CloudBridge Connector (de type SNIP) configurée sur l'appliance Citrix ADC), l'adresse IP distante (adresse IP du point de terminaison du tunnel CloudBridge Connector configurée sur l'appliance F5 BIG-IP), le protocole (IPSec) utilisé pour configurer CloudBridge Tunnel de connecteur et une entité de profil IPsec. L'entité de tunnel IP créée est également appelée entité de tunnel CloudBridge Connector.
- **Créez une règle PBR et associez-la au tunnel IP**. Une entité PBR spécifie un ensemble de règles et une entité tunnel IP (tunnel CloudBridge Connector). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Définissez la plage d'adresses IP source pour spécifier le sous-réseau côté Citrix AD dont le trafic doit être protégé sur le tunnel, et définissez la plage d'adresses IP de destination pour spécifier le sous-réseau côté BIG-IP F5 dont le trafic doit être protégé sur le tunnel.

Pour créer un profil IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecyENABLE`
- `show ipsec profile** <name>`

Pour créer un tunnel IPSEC et lier le profil IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes, tapez :

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Pour créer un profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **Connecteur CloudBridge** > **IpsecProfile** .
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Ajouter un profil IPSec**, définissez les paramètres suivants :

- Nom
- Algorithme de chiffrement
- Algorithme de hachage
- Version du protocole IKE

4. Configurez la méthode d'authentification IPsec à utiliser par les deux homologues de tunnel CloudBridge Connector pour s'authentifier mutuellement : sélectionnez la **méthode d'authentification de clé pré-partagée** et définissez le paramètre **Clé pré-partagée Exists**.
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et lier le profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.
2. Dans l'onglet **Tunnels IPv4**, cliquez sur **Ajouter**.
3. Dans la page **Ajouter un tunnel IP**, définissez les paramètres suivants :
   - Nom
   - IP distante
   - Masque distant
   - Type IP local (dans la liste déroulante Type IP local, sélectionnez *IP du sous-réseau*).
   - IP locale (Toutes les adresses IP configurées du type IP sélectionné se trouvent dans la liste déroulante IP locale. Sélectionnez l'adresse IP souhaitée dans la liste.)
   - Protocole
   - Profil IPsec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Dans la page **Créer un PBR**, définissez les paramètres suivants :
   - Nom
   - Action
   - Type de saut suivant (Select *IP Tunnel*)
   - Nom du tunnel IP
   - IP source Faible
   - IP source élevée
   - IP de destination faible
   - IP de destination élevée
4. Cliquez sur **Créer**, puis sur **Fermer**.

La nouvelle configuration de tunnel CloudBridge Connector correspondante sur l'appliance Citrix ADC apparaît dans l'interface graphique. L'état actuel du tunnel de connecteur CloudBridge est affiché dans le volet CloudBridge Connector configuré. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Les commandes suivantes créent les paramètres de l'appliance Citrix ADC NS_Appliance-1 dans Exemple de configuration du connecteur CloudBridge. :

```
1      > add ipsec profile NS_F5-BIG-IP_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1 - encAlgo AES - hashalgo
          HMAC_SHA1 - lifetime 315360 -perfectForwardSecrecy ENABLE
2
3
4      Done
5
6      > add iptunnel NS_F5-BIG-IP_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100 - protocol IPSEC - ipsecProfileName NS_F5-BIG-
          IP_IPSec_Profile
7
8
9      Done
10
11     > add pbr NS_F5-BIG-IP_Pbr -srcIP 10.102.147.0-10.102.147.255 -
          destIP 10.20.0.0-10.20.255.255 - ipTunnel NS_F5-BIG-IP_Tunnel
12
13
14     Done
15
16     > apply pbrs
17
18
19     Done
20 <!--NeedCopy-->
```

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance Citrix ADC à l'aide des compteurs statistiques de tunnel CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques de tunnel CloudBridge Connector sur une appliance Citrix ADC, consultez Surveillance des tunnels de CloudBridge Connector.

Interopérabilité CloudBridge Connector — Cisco ASA

August 20, 2021

Vous pouvez configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance Cisco ASA pour connecter deux centres de données ou étendre votre réseau à un fournisseur

de cloud. L'appliance Citrix ADC et l'appliance Cisco ASA forment les points d'extrémité du tunnel CloudBridge Connector et sont appelés homologues.

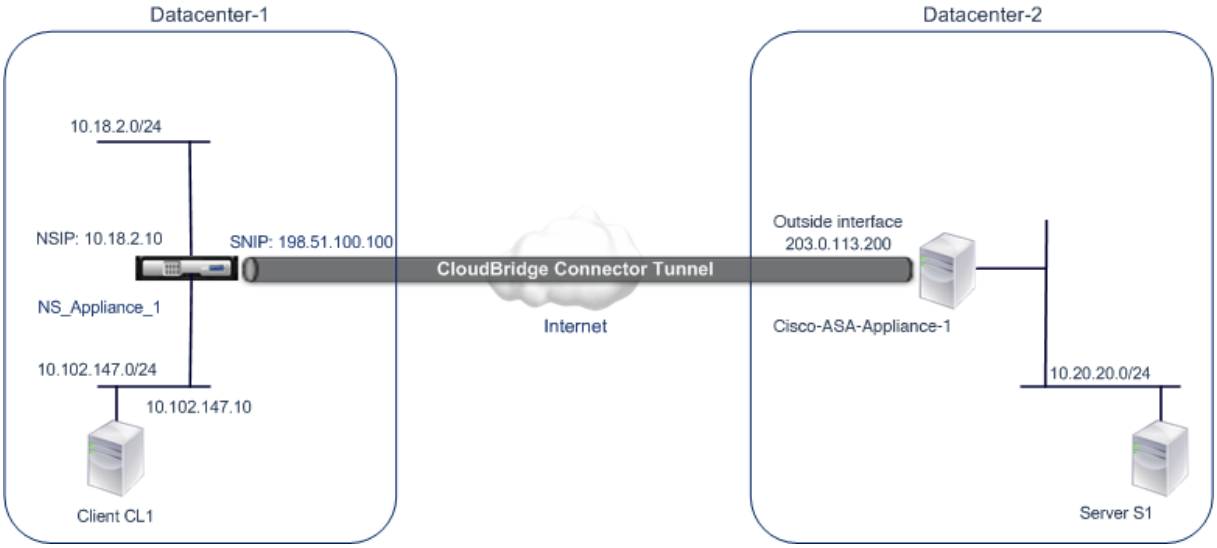
Exemple de configuration de tunnel CloudBridge Connector

Pour illustrer le flux de trafic dans un tunnel CloudBridge Connector, considérez un exemple dans lequel un tunnel CloudBridge Connector est configuré entre les appliances suivantes :

- Appliance Citrix ADC NS_Appliance-1 dans un centre de données désigné comme Datacenter-1
- Appliance Cisco ASA Cisco Cisco Appliance-1 dans un centre de données désigné comme Datacenter-2

NS_Appliance-1 et CISCO-ASA-Appliance-1 permettent la communication entre les réseaux privés dans Datacenter-1 et Datacenter-2 via le tunnel CloudBridge Connector. Dans l'exemple, NS_Appliance-1 et CISCO-ASA-Appliance-1 permettent la communication entre le client CL1 dans Datacenter-1 et le serveur S1 dans Datacenter-2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel du Connecteur CloudBridge inclut l'entité de profil IPSec NS_CISCO-ASA_IPSEC_profile, l'entité de tunnel du Connecteur CloudBridge NS_CISCO-ASA_Tunnel et l'entité de routage basé sur des stratégies (PBR) NS_CISCO-ASA_PBR.



Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de commencer à configurer le tunnel du connecteur CloudBridge, assurez-vous que :

- Les paramètres IPsec suivants sont pris en charge pour un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance Cisco ASA.

Propriétés IPSec	Paramètres
Mode IPsec	Mode tunnel
Version IKE	Version 1
Méthode d'authentification IKE	Clé pré-partagée
Algorithme de chiffrement IKE	AES, 3DES
Algorithme de hachage IKE	HMAC SHA1, HMAC MD5
Algorithme de chiffrement ESP	AES, 3DES
Algorithme de hachage ESP	HMAC SHA1, HMAC MD5

- Vous devez spécifier les mêmes paramètres IPSec sur l'appliance Citrix ADC et l'appliance Cisco ASA aux deux extrémités du tunnel CloudBridge Connector.
- Citrix ADC fournit un paramètre commun (dans les profils IPSec) pour spécifier un algorithme de hachage IKE et un algorithme de hachage ESP. Il fournit également un autre paramètre commun pour spécifier un algorithme de chiffrement IKE et un algorithme de chiffrement ESP. Par conséquent, dans l'appliance Cisco ASA, vous devez spécifier le même algorithme de hachage et le même algorithme de chiffrement dans IKE (configuration de phase 1) et ESP (configuration de phase 2).
- Vous devez configurer le pare-feu à l'extrémité Citrix ADC et Cisco ASA pour autoriser ce qui suit.
  - Tous les paquets UDP pour le port 500
  - Tous les paquets UDP pour le port 4500
  - Tous les paquets ESP (numéro de protocole IP 50)

Configuration de Cisco ASA pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector sur une appliance Cisco ASA, utilisez l'interface de ligne de commande Cisco ASA, qui est l'interface utilisateur principale pour la configuration, la surveillance et la maintenance des appliances Cisco ASA.

Avant de commencer la configuration du tunnel CloudBridge Connector sur une appliance Cisco ASA, assurez-vous que :

- Vous disposez d'un compte d'utilisateur avec des informations d'identification d'administrateur sur l'appliance Cisco ASA.
- Vous connaissez l'interface de ligne de commande Cisco ASA.
- L'appliance Cisco ASA est mise en service et en cours d'exécution, est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.

> **Remarque**
>
> Les procédures de configuration du tunnel CloudBridge Connector sur une appliance Cisco ASA peuvent changer au fil du temps, en fonction du cycle de publication de Cisco. Citrix vous recommande de suivre la documentation officielle du produit Cisco ASA pour la configuration des tunnels VPN IPSec, à l'adresse suivante :

- http://www.cisco.com

Pour configurer un tunnel de connecteur CloudBridge entre une appliance Citrix ADC et une appliance Cisco ASA, effectuez les tâches suivantes sur la ligne de commande de l'appliance Cisco ASA :

- **Créez une stratégie IKE**. Une stratégie IKE définit une combinaison de paramètres de sécurité à utiliser lors de la négociation IKE (phase 1). Par exemple, des paramètres tels que l'algorithme de hachage, l'algorithme de chiffrement et la méthode d'authentification à utiliser dans la négociation IKE sont définis dans cette tâche.
- **Activez IKE sur l'interface externe**. Activez IKE sur l'interface externe à travers laquelle le trafic du tunnel va circuler vers le pair du tunnel.
- **Créez un groupe de tunnels**. Un groupe de tunnels spécifie le type de tunnel et la clé pré-partagée. Le type de tunnel doit être défini sur ipsec-l2l, qui signifie IPsec LAN to LAN. Une clé pré-partagée est une chaîne de texte que les homologues d'un tunnel CloudBridge Connector utilisent pour s'authentifier mutuellement les uns avec les autres. Les clés pré-partagées sont comparées les unes aux autres pour l'authentification IKE. Par conséquent, pour que l'authentification réussisse, vous devez configurer la même clé pré-partagée sur l'appliance Cisco ASA et l'appliance Citrix ADC.
- **Définissez un jeu de transformations**. Un ensemble de transformations définit une combinaison de paramètres de sécurité (phase 2) à utiliser dans l'échange de données sur le tunnel CloudBridge Connector une fois la négociation IKE réussie.
- **Créez une liste d'accès**. Les listes d'accès crypto sont utilisées pour définir les sous-réseaux dont le trafic IP sera protégé sur le tunnel CloudBridge. Les paramètres source et destination de la liste d'accès spécifient les sous-réseaux côté appliance Cisco et côté Citrix ADC qui doivent être protégés par le tunnel du connecteur CloudBridge. La liste d'accès doit être définie pour autoriser. Tout paquet de requête qui provient d'une appliance du sous-réseau Cisco côté appliance et qui est destiné à une appliance du sous-réseau côté Citrix ADC et qui correspond aux paramètres source et destination de la liste d'accès, est envoyé à travers le tunnel CloudBridge Connector.
- **Créez une carte de chiffrement**. Les mappages cryptographiques définissent les paramètres IPsec pour les associations de sécurité (SA). Ils comprennent les éléments suivants : liste d'accès de chiffrement pour identifier les sous-réseaux dont le trafic doit être protégé sur le tunnel CloudBridge, identification homologue (Citrix ADC) par adresse IP et configuration de transformation correspondant aux paramètres de sécurité homologue.
- **Appliquez le crypto Map à l'interface externe**. Dans cette tâche, vous appliquez le mappage

crypto à l'interface externe à travers laquelle le trafic du tunnel va circuler vers le pair du tunnel. L'application du mappage de chiffrement à une interface demande à l'appliance Cisco ASA d'évaluer tout le trafic d'interface par rapport au jeu de mappages de chiffrement et d'utiliser la stratégie spécifiée lors des négociations de connexion ou d'association de sécurité.

Les exemples présentés dans les procédures suivantes créent les paramètres de l'appliance Cisco ASA Cisco-ASA-Appliance-1 utilisée dans Exemple de configuration et de flux de données CloudBridge Connector.

Pour créer une stratégie IKE à l'aide de la ligne de commande Cisco ASA

À l'invite de commandes de l'appliance Cisco ASA, tapez les commandes suivantes, en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
Priorité de la stratégie crypto ikev1	Cisco-ASA-Appliance-1 (config) # crypto ikev1 politique 1	Entrez le mode de configuration de la stratégie IKE et identifiez la stratégie à créer. (Chaque stratégie est identifiée de manière unique par le numéro de priorité que vous attribuez.) Cet exemple montre comment configurer la stratégie 1.
cryptage (3des | aes)	Cisco-ASA-Appliance-1 (config-ikev1-policy) # cryptage 3des	Spécifiez l'algorithme de chiffrement. Cet exemple montre comment configurer l'algorithme 3DES.
hachage (sha | md5)	Cisco-ASA-Appliance-1 (config- ikev1-policy) # hachage sha	Spécifiez l'algorithme de hachage. Cet exemple montre comment configurer SHA.
authenticationpre-share	Cisco-ASA-appliance-1 (config- ikev1-policy)# authentication pre-share	Spécifiez la méthode d'authentification pré-partage.
groupe 2	Cisco-ASA-appliance-1 (config- ikev1-policy)# group 2	Spécifiez l'identificateur de groupe Diffie-Hellman 1024 bits (2).

Commande	Exemple	Description de la commande
secondes à vie	Cisco-ASA-appliance-1 (config- ikev1-policy)# lifetime 28800	Spécifiez la durée de vie de l'association de sécurité en secondes. Cet exemple montre comment configurer 28800 secondes, valeur par défaut de la durée de vie d'une appliance Citrix ADC.

Pour activer IKE sur l'interface externe à l'aide de la ligne de commande Cisco ASA

À l'invite de commandes de l'appliance Cisco ASA, tapez les commandes suivantes, en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
crypto ikev1 activer en dehors	Cisco-ASA-appliance-1(config)# crypto ikev1 enable outside	Activez IKEv1 sur l'interface par laquelle le trafic du tunnel circule vers le pair du tunnel. Cet exemple montre comment activer IKEv1 sur l'interface nommée en dehors.

Pour créer un groupe de tunnels à l'aide de la ligne de commande Cisco ASA

À l'invite de commandes de l'appliance Cisco ASA, tapez les commandes suivantes, en commençant en mode de configuration globale, comme indiqué dans le groupe de tunnels pdf joint à l'aide de la ligne de commande Cisco ASA :

Pour créer une liste d'accès crypto à l'aide de la ligne de commande Cisco ASA

À l'invite de commandes de l'appliance Cisco ASA, tapez la commande suivante en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
access-list access-list-number permit IP source source-wildcard destination destination-wildcard	Cisco-ASA-appliance-1(config)# access-list 111 permit ip 10.20.20.0 0.0.0.255 10.102.147.0 0.0.0.255	Spécifiez des conditions pour déterminer les sous-réseaux dont le trafic IP doit être protégé sur le tunnel CloudBridge Connector. Cet exemple montre comment configurer la liste d'accès 111 pour protéger le trafic des sous-réseaux 10.20.20.0/24 (côté CISCO-ASA-Appliance-1) et 10.102.147.0/24 (côté NS_Appliance-1).

Pour définir un ensemble de transformations à l'aide de la ligne de commande Cisco ASA

À l'invite de commandes de l'appliance Cisco ASA, tapez les commandes suivantes, en commençant en mode de configuration globale. Voir Transform set using ASA Command line table pdf.

Pour créer une carte crypto à l'aide de la ligne de commande Cisco ASA

À l'invite de commandes de l'appliance Cisco ASA, tapez les commandes suivantes en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
crypto map map-name seq-num match address access-list-name	Cisco-ASA-appliance-1 (config)# crypto map NS-CISCO-CM 1 match address 111	Créez une carte crypto et spécifiez une liste d'accès à celle-ci. Cet exemple configure le mappage de chiffrement NS-CISCO-CM avec le numéro de séquence 1 et affecte la liste d'accès 111 à NS-CISCO-CM.

Commande	Exemple	Description de la commande
crypto map map-name seq-num set peer ip-address	Cisco-ASA-appliance-1 (config)# crypto map NS-CISCO-CM 1 set peer 198.51.100.100	Spécifiez l'homologue (appliance Citrix ADC) par son adresse IP. Cet exemple spécifie 198.51.100.100, qui est l'adresse IP du point de terminaison du tunnel sur l'appliance Citrix ADC.
crypto map map-name seq-num set ikev1 transform-set transform-set-name	Cisco-ASA-appliance-1 (config)# crypto map NS-CISCO-CM 1 set ikev1 transform-set NS-CISCO-TS	Spécifiez quel jeu de transformations est autorisé pour cette entrée de mappage crypto. Cet exemple spécifie le jeu de transformations NS-CISCO-TS.

Pour appliquer un mappage crypto à une interface à l'aide de la ligne de commande Cisco ASA

À l'invite de commandes de l'appliance Cisco ASA, tapez les commandes suivantes en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
crypto map map-nameinterface interface-name	Cisco-ASA-appliance-1(config)# crypto map NS-CISCO-CM interface outside	Appliquez la mappage crypto à l'interface à travers laquelle le trafic du tunnel CloudBridge Connector va circuler. Cet exemple applique la carte de chiffrement NS-CISCO-CM à l'interface extérieure.

Configuration de l'appliance Citrix ADC pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance Citrix ADC et une appliance Cisco ASA, effectuez les tâches suivantes sur l'appliance Citrix ADC. Vous pouvez utiliser la ligne de commande Citrix ADC ou l'interface utilisateur graphique (GUI) Citrix ADC :

- Créez un profil IPSec.
- Créez un tunnel IP qui utilise le protocole IPSec et associez le profil IPSec à celui-ci.

- Créez une règle PBR et associez-la au tunnel IP.

Pour créer un profil IPSEC à l'aide de la ligne de commande Citrix ADC :

À l'invite de commandes, tapez :

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecy ENABLE`
- `show ipsec profile <name>`

Pour créer un tunnel IPSEC et y lier le profil IPSEC à l'aide de la ligne de commande Citrix ADC :

À l'invite de commandes, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande Citrix ADC :

À l'invite de commandes, tapez :

- `**add pbr** <pbrName> **ALLOW** -**srcIP** <subnet-range> -**destIP** <subnet-range>`
- `**ipTunnel** <tunnelName>`
- `**apply pbrs**`
- `**show pbr** <pbrName>`

Pour créer un profil IPSEC à l'aide de l'interface graphique :

1. Accédez à **Système** > **CloudBridge Connector** > **Profil IPsec**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Ajouter un profil IPSec**, définissez les paramètres suivants :
   - Nom
   - Algorithme de chiffrement
   - Algorithme de hachage
   - Version du protocole IKE
   - Perfect Forward Secrecy (Activer ce paramètre)
4. Configurez la méthode d'authentification IPSec à utiliser par les deux homologues du tunnel CloudBridge Connector pour s'authentifier mutuellement : Sélectionnez la méthode **d'authentification par clé pré-partagée** et définissez le paramètre **Pre-Shared Key Exists** .
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface graphique :

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.
2. Dans l' **onglet Tunnels IPv4**, cliquez sur **Ajouter**.
3. Dans la page **Ajouter un tunnel IP**, définissez les paramètres suivants :

- Nom
- IP distante
- Masque distant
- Type IP local (dans la liste déroulante Type IP local, sélectionnez IP du sous-réseau).
- IP locale (Toutes les adresses IP configurées du type IP sélectionné se trouvent dans la liste déroulante IP locale. Sélectionnez l'adresse IP souhaitée dans la liste.)
- Protocole
- Profil IPsec

4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Dans la page **Créer PBR**, définissez les paramètres suivants :
   - Nom
   - Action
   - Type de saut suivant (Select IP Tunnel)
   - Nom du tunnel IP
   - IP source Faible
   - IP source élevée
   - IP de destination faible
   - IP de destination élevée
4. Cliquez sur **Créer**, puis sur **Fermer**.

La nouvelle configuration de tunnel CloudBridge Connector correspondante sur l'appliance Citrix ADC apparaît dans l'interface graphique. L'état actuel du tunnel de connecteur CloudBridge est affiché dans le volet CloudBridge Connector configuré. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Les commandes suivantes créent les paramètres de l'appliance Citrix ADC NS_Appliance-1 dans "Exemple de configuration du connecteur CloudBridge.":

```
1 > add ipsec profile NS_Cisco-ASA_IPSec_Profile -psk
    examplepresharedkey -ikeVersion v1 -encAlgo AES -hashalgo
    HMAC_SHA1 -lifetime 315360 -perfectForwardSecrecy ENABLE
2
3 Done
4
5 > add iptunnel NS_Cisco-ASA_Tunnel 203.0.113.200 255.255.255.255
    198.51.100.100 -protocol IPSEC -ipsecProfileName NS_Cisco-
    ASA_IPSec_Profile
6
7
```



```
8  Done
9
10 > add pbr NS_Cisco-ASA_Pbr -srcIP 10.102.147.0-10.102.147.255 -destIP
       10.20.0.0-10.20.255.255 -ipTunnel NS_Cisco-ASA_Tunnel
11
12
13 Done
14
15 > apply pbrs
16
17 Done
18
19 <!--NeedCopy-->
```

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance Citrix ADC à l'aide des compteurs statistiques de tunnel CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques de tunnel CloudBridge Connector sur une appliance Citrix ADC, consultez Surveillance des tunnels de CloudBridge Connector.

Haute disponibilité

January 21, 2021

Un déploiement haute disponibilité (HA) de deux appliances Citrix ADC peut assurer un fonctionnement ininterrompu dans n'importe quelle transaction. Une appliance étant configurée comme nœud principal et l'autre comme nœud secondaire, le nœud principal accepte les connexions et gère les serveurs tandis que le nœud secondaire surveille le nœud principal. Si, pour une raison quelconque, le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

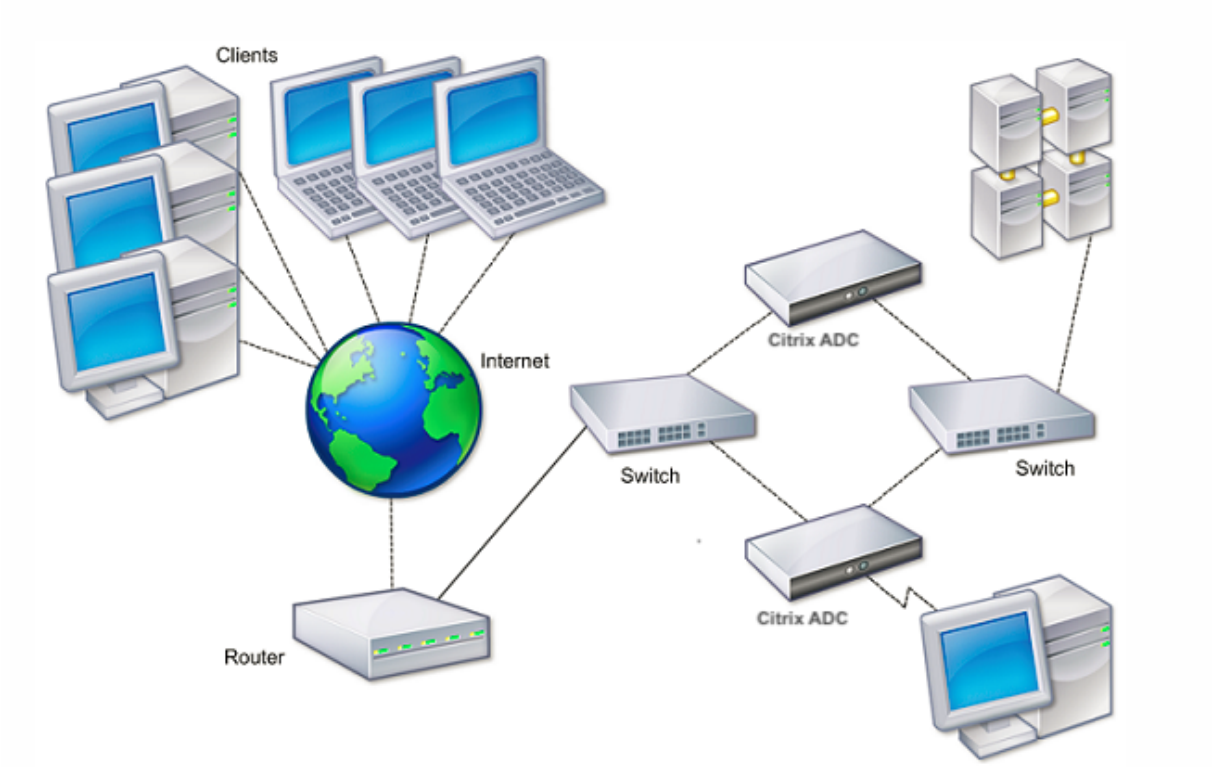
Le nœud secondaire surveille le principal en envoyant des messages périodiques (souvent appelés messages de pulsation ou vérifications de l'état) pour déterminer si le nœud principal accepte les connexions. Si un contrôle d'intégrité échoue, le nœud secondaire réessaie la connexion pendant une période spécifiée, après quoi il détermine que le nœud principal ne fonctionne pas normalement. Le nœud secondaire prend ensuite le relais pour le principal (un processus appelé basculement).

Après un basculement, tous les clients doivent rétablir leurs connexions aux serveurs gérés, mais les règles de persistance de session sont conservées telles qu'elles étaient avant le basculement.

Lorsque la persistance de la journalisation du serveur Web est activée, aucune donnée de journal n'est perdue en raison du basculement. Pour que la persistance de la journalisation soit activée, la configuration du serveur de journaux doit contenir des entrées pour les deux systèmes dans le fichier log.conf.

La figure suivante montre une configuration réseau avec une paire HA.

Figure 1. Appliances Citrix ADC dans une configuration haute disponibilité



Pour configurer HA, vous pouvez commencer par créer une configuration de base, avec les deux nœuds dans le même sous-réseau. Vous pouvez ensuite personnaliser les intervalles auxquels les nœuds communiquent des informations de vérification de l'état, le processus par lequel les nœuds maintiennent la synchronisation et la propagation des commandes du primaire au secondaire. Vous pouvez configurer le mode de sécurité intégrée pour éviter une situation dans laquelle aucun nœud n'est principal. Si votre environnement inclut des périphériques qui n'acceptent pas les messages ARP gratuits Citrix ADC, vous devez configurer des adresses MAC virtuelles. Lorsque vous êtes prêt pour une configuration plus complexe, vous pouvez configurer des nœuds HA dans différents sous-réseaux.

Pour améliorer la fiabilité de votre configuration HA, vous pouvez configurer les moniteurs de routage et créer des liens redondants. Dans certaines situations, par exemple lors du dépannage ou de l'exécution de tâches de maintenance, vous pouvez forcer un nœud à basculer (attribuer le statut principal à l'autre nœud), ou forcer le nœud secondaire à rester secondaire ou le nœud principal à rester principal.

Points à considérer pour une configuration haute disponibilité

August 20, 2021

> **Remarque**
>
> Les exigences suivantes pour la configuration des systèmes dans une configuration HA :

- Dans une configuration HA, les appliances Citrix ADC primaire et secondaire doivent être du même modèle. Les différents modèles Citrix ADC ne sont pas pris en charge dans une paire HA.
- Dans une configuration HA, les deux nœuds doivent exécuter la même version de Citrix ADC.
- Les entrées du fichier de configuration (ns.conf) sur le système principal et le système secondaire doivent correspondre, avec les exceptions suivantes :
  - Les systèmes primaire et secondaire doivent chacun être configurés avec leurs propres adresses IP (NSIP) uniques.
  - Dans une paire HA, l'ID de nœud et l'adresse IP associée d'un nœud doivent pointer vers l'autre nœud. Par exemple, si vous avez des nœuds NS1 et NS2, vous devez configurer NS1 avec un ID de nœud unique et l'adresse IP de NS2, et vous devez configurer NS2 avec un ID de nœud unique et l'adresse IP de NS1.
- Si vous créez un fichier de configuration sur l'un ou l'autre des nœuds à l'aide d'une méthode qui ne passe pas directement par l'interface graphique ou l'interface de ligne de commande (par exemple, l'importation de certificats SSL ou la modification de scripts de démarrage), vous devez copier le fichier de configuration vers l'autre nœud ou créer un fichier identique sur ce nœud.
- Initialement, toutes les appliances Citrix ADC sont configurées avec le même mot de passe de nœud RPC. Les nœuds RPC sont des entités système internes utilisées pour la communication système à système des informations de configuration et de session. Pour des raisons de sécurité, vous devez modifier les mots de passe du nœud RPC par défaut.

  Un nœud RPC existe sur chaque Citrix ADC. Ce nœud stocke le mot de passe, qui est vérifié par rapport au mot de passe fourni par le système de contact. Pour communiquer avec d'autres systèmes, chaque Citrix ADC nécessite une connaissance de ces systèmes, y compris la façon de s'authentifier sur ces systèmes. Les nœuds RPC conservent ces informations, qui comprennent les adresses IP des autres systèmes et les mots de passe dont ils ont besoin pour l'authentification.

  Les nœuds RPC sont créés implicitement lors de l'ajout d'un nœud ou de l'ajout d'un site GSLB (Global Server Load Balancing). Vous ne pouvez pas créer ou supprimer manuellement des nœuds RPC.

> **Remarque** :
>
> Si les appliances Citrix ADC dans une configuration haute disponibilité sont configurées en mode à un bras, vous devez désactiver toutes les interfaces système, sauf celle connectée au commutateur ou au concentrateur.

Pour une configuration IPv6 HA, les considérations suivantes s'appliquent :

- Vous devez installer la licence IPv6pt sur les deux appliances Citrix ADC.
- Après avoir installé la licence IPv6pt, activez la fonctionnalité IPv6 à l'aide de l'interface graphique ou de l'interface de ligne de commande.
- Les deux appliances Citrix ADC nécessitent une adresse IPv6 NSIP globale. En outre, les entités réseau (par exemple, les commutateurs et les routeurs) entre les deux nœuds doivent prendre en charge IPv6.

Configuration de la haute disponibilité

August 20, 2021

Pour configurer une configuration haute disponibilité, vous créez deux nœuds, chacun définissant l'adresse IP Citrix ADC (NSIP) de l'autre en tant que nœud distant. Commencez par vous connecter à l'une des deux appliances Citrix ADC que vous souhaitez configurer pour une haute disponibilité, puis ajoutez un nœud. Spécifiez l'adresse IP Citrix ADC (NSIP) de l'autre appliance comme adresse du nouveau nœud. Connectez-vous ensuite à l'autre appliance et ajoutez un nœud qui possède l'adresse NSIP de la première appliance. Un algorithme détermine quel nœud devient primaire et qui devient secondaire.

> **Remarque** :
>
> L'interface utilisateur graphique Citrix ADC offre une option qui évite d'avoir à ouvrir une session sur la seconde appliance.

La figure suivante montre une configuration HA simple, dans laquelle les deux nœuds sont dans le même sous-réseau.

Figure 1. Deux appliances Citrix ADC connectées dans une configuration haute disponibilité

Ajout d'un nœud distant

Pour ajouter une appliance Citrix ADC distante en tant que nœud dans une configuration haute disponibilité, spécifiez un ID de nœud unique et l'adresse NSIP de l'appliance. Le nombre maximal d'ID de nœud dans une configuration HA est de 64. Lorsque vous ajoutez un nœud HA, vous devez désactiver le moniteur HA pour chaque interface qui n'est pas connectée ou qui n'est pas utilisée pour le trafic. Pour les utilisateurs CLI, il s'agit d'une procédure distincte.

> **Remarque** :
>
> Pour vous assurer que chaque nœud de la configuration haute disponibilité possède les mêmes paramètres, vous devez synchroniser vos certificats SSL, scripts de démarrage et autres fichiers de configuration avec ceux du nœud principal.

Pour ajouter un nœud à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add ha node <id> <IPAddress>`
- `show ha node`

Exemple

```
> add ha node 10 203.0.113.32
<!--NeedCopy-->
```

Pour désactiver un moniteur HA à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set interface <ifNum> [-haMonitor ( ON | OFF )]`
- `show interface <ifNum>`

Exemple

```
> set interface 1/3 -haMonitor OFF
 Done
<!--NeedCopy-->
```

Pour ajouter un nœud distant à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, ajoutez un nouveau nœud distant ou modifiez un nœud existant.

Désactivation ou activation d'un nœud

Vous pouvez désactiver ou activer uniquement un nœud secondaire. Lorsque vous désactivez un nœud secondaire, il arrête d'envoyer des messages de pulsation au nœud principal et, par conséquent, le nœud principal ne peut plus vérifier l'état du nœud secondaire. Lorsque vous activez un nœud, le nœud participe à la configuration de haute disponibilité.

Pour désactiver ou activer un nœud à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `set ha node -hastatus DISABLED`
- `set ha node -hastatus ENABLED`

Pour désactiver ou activer un nœud à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, ouvrez le nœud.
2. Dans la liste **État de haute disponibilité**, sélectionnez **ENABLED (Participer activement à HA)** ou **DISABLED (Ne pas participer à HA)** .

Suppression d'un nœud

Si vous supprimez un nœud, les nœuds ne sont plus en configuration haute disponibilité.

Pour supprimer un nœud à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm ha node <id>
```

Exemple

```
1 > rm ha node 10
2   Done
3 <!--NeedCopy-->
```

Pour supprimer un nœud à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, supprimez le nœud.

Configuration des intervalles de communication

January 21, 2021

L'intervalle Hello est l'intervalle auquel les messages de pulsation sont envoyés au nœud homologue. L'intervalle mort est l'intervalle de temps après lequel le nœud homologue est marqué DOWN si les paquets de pulsation ne sont pas reçus. Les messages de pulsation sont des paquets UDP envoyés au port 3003 de l'autre nœud dans une paire HA. L'intervalle mort doit être défini comme un multiple d'intervalle bonjour.

Pour définir les intervalles bonjour et morts à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set HA node [-helloInterval <msecs>] [-deadInterval <secs>]`
- `show HA node <id>`

Pour définir les intervalles bonjour et morts à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, ouvrez le nœud.
2. Définissez les paramètres suivants :

- Intervalle Hello (msecs)
- Intervalle mort (secondes)

Configuration de la synchronisation

January 21, 2021

La synchronisation est un processus de duplication de la configuration du nœud principal sur le nœud secondaire. Le but de la synchronisation est de s'assurer qu'il n'y a pas de perte d'informations de configuration entre les nœuds principal et secondaire, quel que soit le nombre de basculements qui se produisent. La synchronisation utilise le port 3010.

La synchronisation est déclenchée par l'une des circonstances suivantes :

- Le nœud secondaire dans une configuration HA apparaît après un redémarrage.
- Le nœud principal devient secondaire après un basculement.

La synchronisation automatique est activée par défaut. Vous pouvez également forcer la synchronisation.

Désactivation ou activation de la synchronisation

La synchronisation automatique HA est activée par défaut sur chaque nœud d'une paire HA. Vous pouvez l'activer ou le désactiver sur l'un ou l'autre des nœuds.

Pour désactiver ou activer la synchronisation automatique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set HA node -haSync DISABLED`
- `set HA node -haSync ENABLED`

Pour désactiver ou activer la synchronisation à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** .
2. Sous Synchronisation HA, désactivez ou sélectionnez le nœud Secondary récupère la configuration à partir de l'option Primary.

Forcer le nœud secondaire à synchroniser avec le nœud principal

Outre la synchronisation automatique, Citrix ADC prend en charge la synchronisation forcée. Vous pouvez forcer la synchronisation à partir du nœud principal ou secondaire. Lorsque vous forcez la synchronisation à partir du nœud secondaire, il commence à synchroniser sa configuration avec le nœud principal.

Toutefois, si la synchronisation est déjà en cours, la synchronisation forcée échoue et le système affiche un avertissement. La synchronisation forcée échoue également dans l'une des circonstances suivantes :

- Vous forcez la synchronisation sur un système autonome.
- Le nœud secondaire est désactivé.
- La synchronisation HA est désactivée sur le nœud secondaire.

Pour forcer la synchronisation à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
force HA sync
```

Pour forcer la synchronisation à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** .
2. Sous l'onglet **Nœuds**, dans la liste Action, cliquez sur **Forcer la synchronisation**.

Synchronisation des fichiers de configuration dans une configuration haute disponibilité

October 5, 2021

Dans une configuration haute disponibilité, tous les fichiers de configuration sont synchronisés automatiquement du nœud principal vers le nœud secondaire à un intervalle d'une minute. La synchronisation des fichiers de configuration peut être effectuée manuellement à l'aide de l'interface de ligne de commande ou de l'interface graphique au niveau du nœud principal ou du nœud secondaire.

Les fichiers situés sur le secondaire qui sont spécifiques au secondaire (qui ne sont pas présents sur le serveur principal) ne sont pas supprimés pendant la synchronisation.

Pour synchroniser les fichiers dans une configuration haute disponibilité à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
sync HA files <mode>
```

Exemple

```
1 > sync HA files all
2  Done
3 <!--NeedCopy-->
```

```
1 > sync HA files ssl
2  Done
3 <!--NeedCopy-->
```

Description des paramètres (de la commande répertoriée dans la procédure CLI)

```
sync ha files <mode>
```

```
mode
```

Spécifiez l'un des modes de synchronisation suivants.

- **all** - Synchronisez les fichiers liés à la configuration du système, aux signets Access Gateway, aux certificats SSL, aux listes de listes de certificats SSL et aux objets XML du pare-feu d'application.
- **signets** - Synchronisez tous les signets Access Gateway.
- **ssl** - Synchronisez tous les certificats, clés et CRL pour la fonctionnalité SSL.
- **importations** - Synchronisez tous les objets XML (par exemple, WSDL, schémas, pages d'erreur) configurés pour le pare-feu d'application.
- **misc** - Synchronise tous les fichiers de licence et le fichier rc.conf.
- **all_plus_misc** - Synchronise les fichiers liés à la configuration du système, aux signets Access Gateway, aux certificats SSL, aux listes de listes de certificats SSL, aux objets XML du pare-feu d'application, aux licences et au fichier rc.conf.

Pour synchroniser les fichiers dans une configuration haute disponibilité à l'aide de l'interface graphique

Accédez à **Système** > **Diagnostics** et, dans le groupe **Utilitaires**, cliquez sur **Démarrer la synchronisation des fichiers HA**.

Configuration de la propagation des commandes

January 21, 2021

Dans une configuration HA, toute commande émise sur le nœud principal se propage automatiquement vers le secondaire et est exécutée sur celui-ci avant d'être exécutée sur le principal. Si la propagation de la commande échoue ou si l'exécution de la commande échoue sur le secondaire, le nœud principal exécute la commande et consigne une erreur. La propagation des commandes utilise le port 3010.

Dans une configuration de paire HA, la propagation des commandes est activée par défaut sur les nœuds principal et secondaire. Vous pouvez activer ou désactiver la propagation des commandes sur l'un ou l'autre des nœuds d'une paire HA. Si vous désactivez la propagation des commandes sur le nœud principal, les commandes ne sont pas propagées vers le nœud secondaire. Si vous désactivez la propagation des commandes sur le nœud secondaire, les commandes propagées à partir du nœud principal ne sont pas exécutées sur le nœud secondaire.

> **Remarque**
>
> Après avoir réactivé la propagation, n'oubliez pas de forcer la synchronisation.

Si la synchronisation se produit alors que vous désactivez la propagation, toutes les modifications liées à la configuration que vous effectuez avant que la désactivation de la propagation ne prenne effet sont synchronisées avec le nœud secondaire. Cela vaut également pour les cas où la propagation est désactivée pendant la synchronisation.

Pour désactiver ou activer la propagation des commandes à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- set HA node -haProp DISABLED
- set HA node -haProp ENABLED

Pour désactiver ou activer la propagation des commandes à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, ouvrez le nœud.
2. Désactivez ou sélectionnez le nœud principal pour propager la configuration à l'option secondaire.

Restriction du trafic de synchronisation haute disponibilité à un VLAN

August 20, 2021

Dans un déploiement haute disponibilité (HA), le trafic lié à la maintenance de la configuration HA circule entre les deux nœuds HA. Ce trafic est des types suivants :

- Synchronisation de la configuration
- Propagation de configuration
- Mise en miroir des connexions
- Synchronisation de la configuration de la persistance de l'équilibrage de la charge
- Synchronisation de session persistante
- Synchronisation de l'état de session

Le bon flux de ce trafic lié à l'AP entre les deux nœuds est essentiel pour le fonctionnement du déploiement de l'AP. Généralement, le trafic lié à la HA est faible en volume, mais peut devenir très élevé lors d'un basculement. Il devient très élevé si le basculement de connexion avec état est activé et si le nœud principal avant le basculement traitait un grand nombre de connexions.

Par défaut, le trafic lié à la HA circule via les VLAN auxquels l'adresse NSIP est liée. Pour tenir compte d'une augmentation potentielle de ce trafic, vous pouvez séparer le trafic lié à la haute disponibilité du trafic de gestion et limiter son flux à un VLAN distinct. Ce VLAN est appelé HA SYNC VLAN.

Points à considérer avant de configurer un VLAN HA SYNC

- La configuration d'un VLAN HA SYNC n'est ni propagée ni synchronisée. En d'autres termes, le VLAN HA SYNC est spécifique à un nœud et est configuré indépendamment sur chaque nœud.
- La configuration VLAN HA SYNC est supprimée lorsque vous effacez la configuration uniquement en mode FULL.
- HA MON doit être réglé sur OFF pour les interfaces qui font partie du VLAN HA SYNC, afin d'éviter une situation dans laquelle les deux nœuds fonctionnent comme nœud principal.
- Les interfaces de gestion (par exemple, 0/1 et 0/2) ne doivent pas faire partie du VLAN HA SYNC, de sorte que le trafic lié à HA ne circule pas via les interfaces de gestion.
- Citrix recommande de désactiver les messages de pulsation haute disponibilité sur les interfaces de gestion et d'activer les interfaces VLAN HA SYNC. Après avoir suivi ces recommandations, les messages de pulsation haute disponibilité peuvent également être activés sur les interfaces de données.

  Pour plus d'informations sur la désactivation des messages Heartbeat haute disponibilité sur les interfaces, reportez-vous à la section Gestion des messages Heartbeat haute disponibilité sur une appliance Citrix ADC.

Pour configurer un VLAN HA SYNC sur un nœud Citrix ADC, spécifiez un VLAN configuré avec le paramètre VLAN HA SYNC de l'entité de nœud local.

Pour configurer un VLAN HA SYNC sur un nœud local à l'aide de la ligne de commande :

À l'invite de commandes, tapez :

- `set ha node -syncvlan <VLANID>`
- `show node`

Description du paramètre :

syncvlan (Sync VLAN) - VLAN sur lequel le trafic lié à l'HA est envoyé. Cela inclut le trafic pour la synchronisation, la propagation, la mise en miroir des connexions, la persistance de l'équilibrage de charge, la synchronisation de configuration, la synchronisation de session persistante et la synchronisation de l'état de session. Cependant, les battements de cœur HA peuvent utiliser n'importe quelle interface.

Pour configurer un VLAN HA SYNC sur un nœud à l'aide de l'interface graphique :

1. Accédez à **Système** > **Haute disponibilité** .
2. Définissez le paramètre **Sync VLAN** lors de la modification du nœud local.

Configuration du mode de sécurité intégrée

January 21, 2021

Dans une configuration HA, le mode de sécurité intégrée garantit qu'un nœud est toujours principal lorsque les deux nœuds échouent le contrôle de santé. Ceci permet de s'assurer que lorsqu'un nœud n'est que partiellement disponible, les méthodes de sauvegarde sont activées pour gérer le trafic le plus possible. Le mode HA fail-safe est configuré indépendamment sur chaque nœud.

Le tableau suivant présente certains des cas de sécurité intégrée. L'état NOT_UP signifie que le nœud a échoué à la vérification de l'état mais qu'il est partiellement disponible. L'état UP signifie que le nœud a passé le contrôle d'intégrité.

État d'intégrité du nœud A (principal)	État d'intégrité du nœud B (secondaire)	Comportement HA par défaut	Comportement HA activé pour la sécurité intégrée	Description
NOT_UP (dernier échec)	NOT_UP (premier échec)	A (Secondaire), B (Secondaire)	A (Principal), B (Secondaire)	Si les deux nœuds échouent, l'un après l'autre, le dernier nœud principal reste principal.
NOT_UP (premier échec)	NOT_UP (dernier échec)	A (Secondaire), B (Secondaire)	A (Secondaire), B (Principal)	Si les deux nœuds échouent, l'un après l'autre, le dernier nœud principal reste principal.
UP	UP	A (Principal), B (Secondaire)	A (Principal), B (Secondaire)	Si les deux nœuds réussissent la vérification de l'état, aucun changement de comportement avec fail-safe activé.
UP	NOT_UP	A (primaire), B (secondaire)	A (Principal), B (Secondaire)	Si seul le nœud secondaire échoue, aucun changement de comportement avec fail-safe activé.

État d'intégrité du nœud A (principal)	État d'intégrité du nœud B (secondaire)	Comportement HA par défaut	Comportement HA activé pour la sécurité intégrée	Description
NOT_UP	UP	A (Secondaire), B (Principal)	A (Secondaire), B (Principal)	Si seul le principal échoue, aucun changement de comportement avec fail-safe activé.
NOT_UP	UP (STAYSEC-ONDARY)	A (Secondaire), B (Secondaire)	A (Principal), B (Secondaire)	Si le secondaire est configuré comme STAY-SECONDARY, le primaire reste principal même en cas d'échec.

Pour activer le mode de sécurité à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set HA node [-failSafe ( **ON** | **OFF** )]
```

Exemple

```
1 set ha node -failsafe ON
2 <!--NeedCopy-->
```

Pour activer le mode de sécurité intégrée à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, ouvrez le nœud.
2. Sous **Mode sans échec**, sélectionnez l'option **Maintenir un nœud principal**même lorsque les deux nœuds ne sont pas sains.

Configuration d'adresses MAC virtuelles

January 21, 2021

Une adresse MAC virtuelle est une entité flottante partagée par les nœuds principal et secondaire dans une configuration HA.

Dans une configuration HA, le nœud principal possède toutes les adresses IP flottantes, telles que les MIP, SNIP et VIP. Le nœud principal répond aux demandes ARP (Address Resolution Protocol) pour ces adresses IP avec sa propre adresse MAC. Par conséquent, la table ARP d'un périphérique externe (par exemple, un routeur en amont) est mise à jour avec l'adresse IP flottante et l'adresse MAC du nœud principal.

Lorsqu'un basculement se produit, le nœud secondaire prend la relève en tant que nouveau nœud principal. Il utilise ensuite Gratuitous ARP (GARP) pour annoncer les adresses IP flottantes qu'il a acquises du primaire. Toutefois, l'adresse MAC que la nouvelle annonce principale est l'adresse MAC de sa propre interface.

Certains périphériques (notamment quelques routeurs) n'acceptent pas les messages GARP générés par l'appliance Citrix ADC. Par conséquent, certains périphériques externes conservent l'ancien mappage IP vers MAC annoncé par l'ancien nœud principal. Cela peut entraîner la chute d'un site.

Vous pouvez résoudre ce problème en configurant un MAC virtuel sur les deux nœuds d'une paire HA. Les deux nœuds possèdent alors des adresses MAC identiques. Par conséquent, en cas de basculement, l'adresse MAC du nœud secondaire reste inchangée et les tables ARP sur les périphériques externes n'ont pas besoin d'être mises à jour.

Pour créer un MAC virtuel, vous devez d'abord créer un ID de routeur virtuel (VRID) et le lier à une interface. (Dans une configuration HA, vous devez lier le VRID aux interfaces des deux nœuds.) Une fois que le VRID est lié à une interface, le système génère un MAC virtuel avec le VRID comme dernier octet.

Cette section comprend les détails suivants :

- Configuration de MAC virtuels IPv4
- Configuration des Mac6 virtuels IPv6

Configuration de MAC virtuels IPv4

Lorsque vous créez une adresse MAC virtuelle IPv4 et la liez à une interface, tout paquet IPv4 envoyé à partir de l'interface utilise l'adresse MAC virtuelle qui est liée à l'interface. S'il n'y a pas de MAC virtuel IPv4 lié à une interface, l'adresse MAC physique de l'interface est utilisée.

Le MAC virtuel générique est de la forme`00:00:5e:00:01:<VRID>`. Par exemple, si vous créez un VRID avec une valeur de 60 et que vous le liez à une interface, le MAC virtuel résultant est 00:00:5 e : 00:01:3 c, où 3c est la représentation hexadécimale du VRID. Vous pouvez créer 255 VRID avec des valeurs comprises entre 1 et 255.

Création ou modification d'un MAC virtuel IPv4

Vous créez un MAC virtuel IPv4 en lui attribuant un ID de routeur virtuel. Vous pouvez alors lier le MAC virtuel à une interface. Vous ne pouvez pas lier plusieurs VRID à la même interface. Pour vérifier la configuration de MAC virtuel, vous devez afficher et examiner les MAC virtuels et les interfaces liées aux MAC virtuels.

Pour ajouter un MAC virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add vrID`
- `bind vrid <id> -ifnum <interface_name>`
- `show vrID`

Exemple

```
1 > add vrID 100
2  Done
3 > bind vrid 100 -ifnum 1/1 1/2 1/3
4  Done
5 <!--NeedCopy-->
```

Pour dissocier les interfaces d'un MAC virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `unbind vrid <id> -ifnum <interface_name>`
- `show vrID`

Pour configurer un MAC virtuel à l'aide de l'interface graphique

Accédez à **Système** > **Réseau** > **VMAC** et, sous l'onglet **VMAC**, ajoutez un nouveau MAC virtuel ou modifiez un MAC virtuel existant.

Suppression d'un MAC virtuel IPv4

Pour supprimer un MAC virtuel IPv4, vous supprimez son ID de routeur virtuel.

Pour supprimer un MAC virtuel IPv4 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

`rm vrid <id>`

Exemple

```
rm vrid 100s
<!--NeedCopy-->
```

Pour supprimer un MAC virtuel IPv4 à l'aide de l'interface graphique

Accédez à **Système** > **Réseau** > **VMAC** et, sous l'onglet **VMAC**, supprimez le MAC virtuel IPv4.

Configuration des Mac6 virtuels IPv6

Le Citrix ADC prend en charge le MAC6 virtuel pour les paquets IPv6. Vous pouvez lier n'importe quelle interface à un MAC6 virtuel, même si un MAC virtuel IPv4 est lié à l'interface. Tout paquet IPv6 envoyé à partir de l'interface utilise le MAC6 virtuel lié à cette interface. S'il n'y a pas de MAC6 virtuel lié à une interface, un paquet IPv6 utilise le MAC physique.

Création ou modification d'un MAC6 virtuel

Vous créez un MAC virtuel IPv6 en lui attribuant un ID de routeur virtuel IPv6. Vous pouvez alors lier le MAC virtuel à une interface. Vous ne pouvez pas lier plusieurs VRID IPv6 à une interface. Pour vérifier la configuration MAC6 virtuel, vous devez afficher et examiner les Mac6 virtuels et les interfaces liées aux Mac6 virtuels.

Pour ajouter un MAC6 virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add vrID6 <id>`
- `bind vrID6 <id> -ifnum <interface_name>`
- `show vrID6`

Exemple

```
> add vrID6 100
Done
> bind vrID6 100 -ifnum 1/1 1/2 1/3
 Done
<!--NeedCopy-->
```

Pour dissocier les interfaces d'un MAC6 virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `unbind vrID6 <id> -ifnum <interface_name>`
- `show vrID6`

Pour configurer un MAC6 virtuel à l'aide de l'interface graphique

Accédez à **Système** > **Réseau** > **VMAC** et, sous l'onglet **VMAC6**, ajoutez un nouveau MAC6 virtuel ou modifiez un MAC6 virtuel existant.

Suppression d'un MAC6 virtuel

Pour supprimer un MAC virtuel IPv4, vous supprimez son ID de routeur virtuel.

Pour supprimer un MAC6 virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

`rm vrid6 <id>`

Exemple

```
1 rm vrid6 100s
2 <!--NeedCopy-->
```

Pour supprimer un MAC6 virtuel à l'aide de l'interface graphique

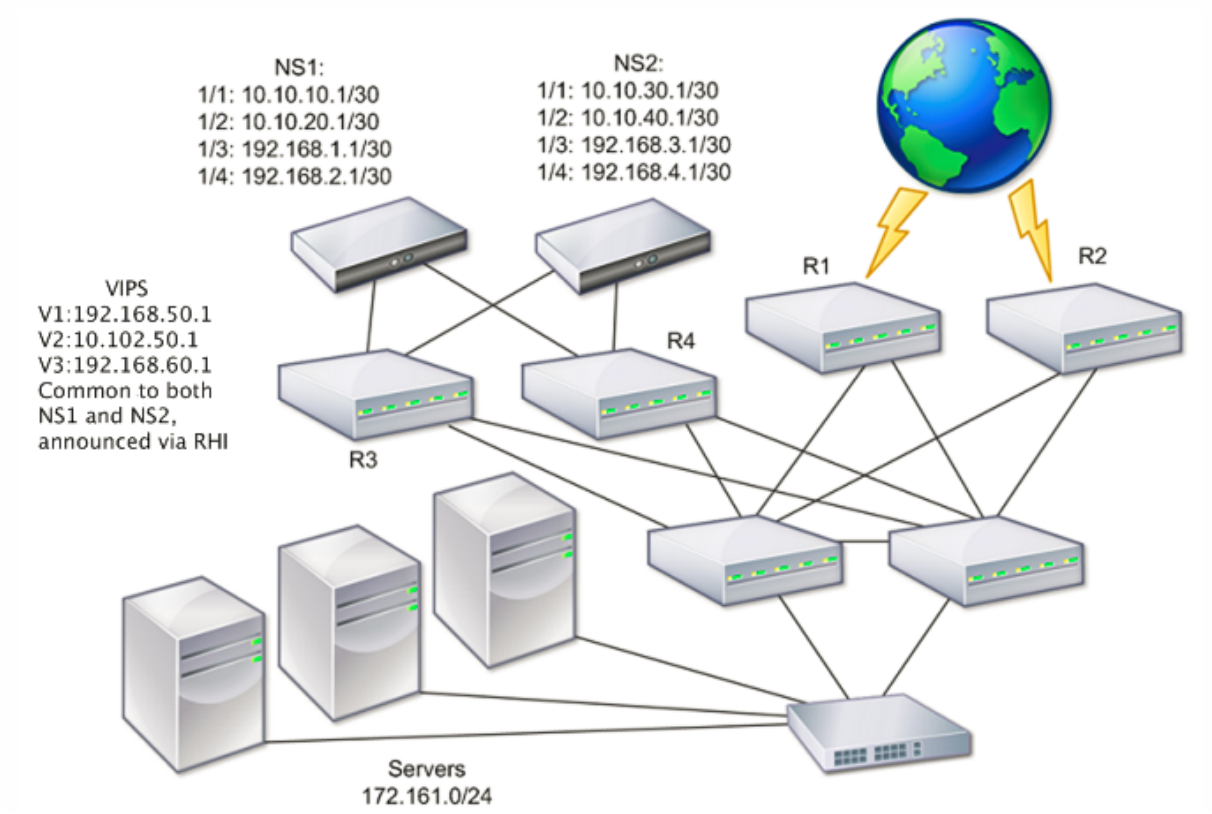
Accédez à **Système** > **Réseau** > **VMAC** et, sous l'onglet **VMAC6**, supprimez l'ID du routeur virtuel.

Configuration des nœuds haute disponibilité dans différents sous-réseaux

August 20, 2021

La figure suivante illustre un déploiement HA avec les deux systèmes situés dans différents sous-réseaux :

Figure 1. Haute disponibilité sur un réseau routé



Sur la figure, les systèmes NS1 et NS2 sont connectés à deux routeurs distincts, R3 et R4, sur deux sous-réseaux différents. Les appliances Citrix ADC échangent des paquets de pulsations par le biais des routeurs. Cette configuration pourrait être étendue pour tenir compte des déploiements impliquant un nombre quelconque d'interfaces.

> **Remarque** :
>
> Si vous utilisez le routage statique sur votre réseau, vous devez ajouter des routes statiques entre tous les systèmes pour vous assurer que les paquets de pulsations sont envoyés et reçus avec succès. (Si vous utilisez le routage dynamique sur vos systèmes, les routes statiques sont inutiles.)

Si les nœuds d'une paire HA résident sur deux réseaux distincts, le nœud principal et le nœud secondaire doivent avoir des configurations réseau indépendantes. Cela signifie que les nœuds sur différents réseaux ne peuvent pas partager des entités telles que l'adresse SNIP, les VLAN et les routes. Ce type de configuration, où les nœuds d'une paire HA ont des paramètres configurables différents, est connu sous le nom de Configuration réseau indépendante (INC) ou Configuration réseau symétrique (SNC).

Le tableau suivant récapitule les entités et options configurables pour un INC et indique comment elles doivent être définies sur chaque nœud.

Entités NetScaler	Options
IP (NSIP/SNIP)	Spécifique aux nœuds. Actif uniquement sur ce nœud.
VIP	Flottant.
VLAN	Spécifique aux nœuds. Actif uniquement sur ce nœud.
Itinéraires	Spécifique aux nœuds. Actif uniquement sur ce nœud. Les itinéraires d'équilibrage de charge de liaison flottent.
ACL	Flottant (commun). Actif sur les deux nœuds.
Routage dynamique	Spécifique aux nœuds. Actif uniquement sur ce nœud. Le nœud secondaire doit également exécuter les protocoles de routage et homologuer avec les routeurs en amont.
Mode L2	Flottant (commun). Actif sur les deux nœuds.
Mode L3	Flottant (commun). Actif sur les deux nœuds.
NAT inverse (RNAT)	Configuration RNAT avec l'adresse IP NAT définie sur une adresse IP du serveur virtuel (VIP) car l'adresse VIP est flottante (commune).

Comme lors de la configuration des nœuds HA dans le même sous-réseau, pour configurer des nœuds HA dans différents sous-réseaux, vous vous connectez à chacun des deux appliances Citrix ADC et ajoutez un nœud distant représentant l'autre appliance.

Ajout d'un nœud distant

Lorsque deux nœuds d'une paire HA résident sur des sous-réseaux différents, chaque nœud doit avoir une configuration réseau différente. Par conséquent, pour configurer deux systèmes indépendants pour fonctionner en tant que paire HA, vous devez spécifier le mode INC pendant le processus de configuration.

Lorsque vous ajoutez un nœud HA, vous devez désactiver le moniteur HA pour chaque interface qui n'est pas connectée ou qui n'est pas utilisée pour le trafic. Pour les utilisateurs CLI, il s'agit d'une procédure distincte.

Pour ajouter un nœud à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add ha node <id> <IPAddress> -inc ENABLED`
- `show ha node`

Exemple

```
> add ha node 3 10.102.29.170 -inc ENABLED
 Done
> add ha node 3 1000:0000:0000:0000:0005:0600:700a:888b
  Done
<!--NeedCopy-->
```

Pour désactiver un moniteur HA à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set interface <ifNum> [-haMonitor ( **ON** | **OFF** )]`
- `show interface <ifNum>`

Exemple

```
> set interface 1/3 -haMonitor OFF
 Done
<!--NeedCopy-->
```

Pour ajouter un nœud distant à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, ajoutez un nouveau nœud distant.
2. Assurez-vous de sélectionner l'option Désactiver le moniteur HA sur les interfaces/canaux qui sont hors tension et activer le mode INC (Independent Network Configuration) sur les options en mode automatique.

Suppression d'un nœud

Si vous supprimez un nœud, les nœuds ne sont plus en configuration haute disponibilité.

Pour supprimer un nœud à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
rm ha node <id>
```

Exemple

```
> rm ha node 2
  Done
<!--NeedCopy-->
```

Pour supprimer un nœud à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, supprimez le nœud.

> **Remarque** :
>
> Vous pouvez utiliser le visualiseur réseau pour afficher les appliances Citrix ADC configurées en tant que paire haute disponibilité (HA) et effectuer des tâches de configuration haute disponibilité.

Configuration des moniteurs de routage

August 20, 2021

Vous pouvez utiliser des moniteurs de routage pour rendre l'état HA dépendant de la table de routage interne, que la table contienne ou non des itinéraires dynamiques ou statiques. Dans une configuration HA, un moniteur de routage sur chaque nœud surveille la table de routage interne pour s'assurer qu'une entrée d'itinéraire permettant d'atteindre un réseau particulier est toujours présente. Si l'entrée d'itinéraire n'est pas présente, l'état du moniteur d'itinéraire passe à DOWN.

Lorsqu'une appliance Citrix ADC dispose uniquement d'itinéraires statiques permettant d'atteindre un réseau et que vous souhaitez créer un moniteur de routage pour le réseau, vous devez activer les routes statiques surveillées (MSR) pour les routes statiques. MSR supprime les routes statiques inaccessibles de la table de routage interne. Si MSR est désactivé sur des routes statiques, une route statique inaccessible peut rester dans la table de routage interne, ce qui va à l'encontre de l'objectif d'avoir le moniteur de routage.

Les moniteurs de routage sont pris en charge à la fois en mode non-INC et INC.

Router les moniteurs en HA en mode non-INC	Moniteurs de routage en HA en mode INC
Les moniteurs de routage sont propagés par les nœuds et échangés pendant la synchronisation.	Les moniteurs de routage ne sont ni propagés par les nœuds ni échangés pendant la synchronisation.

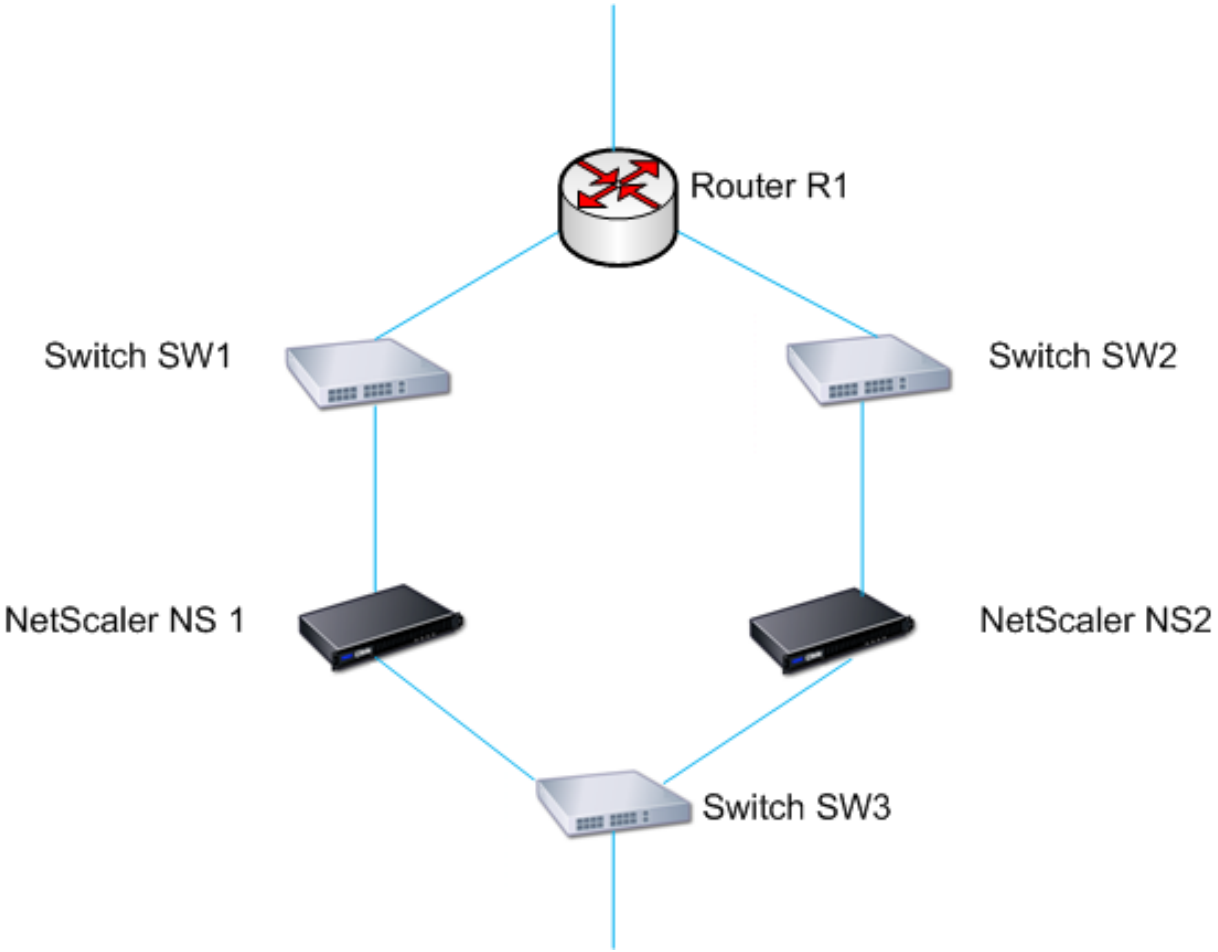
Router les moniteurs en HA en mode non-INC	Moniteurs de routage en HA en mode INC
Les moniteurs de routage ne sont actifs que dans le nœud principal actuel.	Les moniteurs de routage sont actifs sur le nœud principal et le nœud secondaire.
L'appliance Citrix ADC affiche toujours l'état d'un moniteur de routage en mode UP, que l'entrée de routage soit présente ou non dans la table de routage interne.	L'appliance Citrix ADC affiche l'état du moniteur de routage sous la forme DOWN si l'entrée de routage correspondante n'est pas présente dans la table de routage interne.
Un moniteur d'itinéraire commence à surveiller son itinéraire après 180 secondes dans les cas suivants. [Ceci est fait pour permettre l'apprentissage des itinéraires dynamiques, ce qui peut prendre 180 secondes] : redémarrage, basculement, commande set route6 pour les routes v6, commande set route msr enable/disable pour les routes v4, ajout d'un nouveau moniteur d'itinéraire.	-

Les moniteurs de routage sont utiles dans une configuration HA en mode non-INC où vous souhaitez que la non-accessibilité d'une Gateway à partir d'un nœud principal soit l'une des conditions du basculement HA.

Prenons un exemple d'installation HA en mode non-INC dans une topologie à deux bras qui comporte des appliances Citrix ADC NS1 et NS2 dans le même sous-réseau, avec le routeur R1 et les commutateurs SW1, SW2 et SW3.

Étant donné que R1 est le seul routeur de cette configuration, vous souhaitez que la configuration HA bascule chaque fois que R1 n'est pas accessible à partir du nœud principal actuel. Vous pouvez configurer un moniteur de routage (par exemple, RM1 et RM2, respectivement) sur chacun des nœuds pour surveiller l'accessibilité de R1 à partir de ce nœud.

Figure 1.



Avec NS1 comme nœud principal actuel, le flux d'exécution est le suivant :

1. Le moniteur de route RM1 sur NS1 surveille la table de routage interne de NS1 pour détecter la présence d'une entrée de route pour le routeur R1. NS1 et NS2 échangent des messages de pulsation via le commutateur SW1 ou SW3 à intervalles réguliers.
2. Si le commutateur SW1 tombe en panne, le protocole de routage sur NS1 détecte que R1 n'est pas accessible et supprime donc l'entrée de routage pour R1 de la table de routage interne. NS1 et NS2 échangent des messages de pulsation via le commutateur SW3 à intervalles réguliers.
3. En détectant que l'entrée d'itinéraire pour R1 n'est pas présente dans la table de routage interne, RM1 lance un basculement. Si la route vers R1 est interrompue à partir de NS1 et NS2, le basculement sur incident se produit toutes les 180 secondes jusqu'à ce que l'une des appliances puisse atteindre R1 et restaurer la connectivité.

Ajout d'un moniteur de routage à un nœud haute disponibilité

Une procédure unique crée un moniteur de routage et le lie à un nœud HA.

Pour ajouter un moniteur de routage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `bind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])`
- `show HA node`

Exemple

```
1 > bind HA node 0 -routeMonitor 10.102.71.0 255.255.255.0
2  Done
3 > bind HA node 0 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b
4  Done
5 <!--NeedCopy-->
```

Pour ajouter un moniteur de routage à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Moniteurs de routage**, cliquez sur **Configurer** .

Suppression des moniteurs de routage

Pour supprimer un moniteur de routage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `unbind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])`
- show ha node

Exemple

```
1 unbind HA node 3 -routeMonitor 10.102.71.0 255.255.255.0
2 unbind HA node 3 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b
3 <!--NeedCopy-->
```

Pour supprimer un moniteur de routage à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Moniteurs de routage**, supprimez le moniteur de routage.

Limitation des basculements causés par les moniteurs de routage en mode non-INC

August 20, 2021

Dans une configuration HA en mode non-INC, si les moniteurs de routage échouent sur les deux nœuds, le basculement se produit toutes les 180 secondes jusqu'à ce que l'un des nœuds puisse atteindre toutes les routes surveillées par les moniteurs de routage respectifs.

Toutefois, pour un nœud, vous pouvez limiter le nombre de basculements pour un intervalle donné en définissant les paramètres Nombre maximal de basculements et Temps maximal de basculement sur les nœuds. Lorsque l'une ou l'autre des limites est atteinte, plus de basculement se produit et le nœud est assigné comme principal (mais l'état du nœud comme NOT UP) même si un moniteur de routage échoue sur ce nœud. Cette combinaison de l'état HA comme état Primary et Node comme NOT UP est appelée état Primaire Stick.

Si le nœud est alors capable d'atteindre toutes les routes surveillées, la prochaine défaillance du moniteur déclenche la réinitialisation des paramètres Nombre maximum de retournements et Temps maximum de retournement sur le nœud et le démarrage de l'heure spécifiée dans le paramètre Temps maximum de retournement.

Ces paramètres sont définis indépendamment sur chaque nœud et ne sont donc ni propagés ni synchronisés.

Paramètres pour limiter le nombre de basculements

- **Nombre maximal de basculement (MaxFlips)**

  Nombre maximal de basculements autorisés, dans l'intervalle de temps de basculement maximal, pour le nœud en HA en mode non INC, si les basculements sont causés par une défaillance du moniteur de routage.

- **Temps de retournement maximal (MaxFlipTime)**

  Durée, en secondes, pendant laquelle les basculements résultant d'une défaillance du moniteur de routage sont autorisés pour le nœud en HA en mode non INC.

Pour limiter le nombre de basculements à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set HA node [-maxFlips < positive_integer>] [-maxFlipTime <positive_integer >]`
- `show HA node [< id>]`

Pour limiter le nombre de basculements à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, ouvrez le nœud local.

2. Définissez les paramètres suivants :

- Nombre maximal de basculement
- Temps de retournement maximal

```
> set ha node -maxFlips 30 -maxFlipTime 60
Done
> sh ha node
1) Node ID: 0
IP: 10.102.169.82 (NS)
Node State: UP
Master State: Primary
Fail-Safe Mode: OFF
INC State: DISABLED
Sync State: ENABLED
Propagation: ENABLED
Enabled Interfaces : 1/1
Disabled Interfaces : None
HA MON ON Interfaces : 1/1
Interfaces on which heartbeats are not seen :None
Interfaces causing Partial Failure:None
SSL Card Status: NOT PRESENT
Hello Interval: 200 msecs
Dead Interval: 3 secs
Node in this Master State for: 0:4:24:1 (days:hrs:min:sec)

2) Node ID: 1
IP: 10.102.169.81
Node State: UP
Master State: Secondary
Fail-Safe Mode: OFF
INC State: DISABLED
Sync State: SUCCESS
Propagation: ENABLED
Enabled Interfaces : 1/1
Disabled Interfaces : None
HA MON ON Interfaces : 1/1
Interfaces on which heartbeats are not seen : None
Interfaces causing Partial Failure: None
SSL Card Status: NOT PRESENT

Local node information:
Configured/Completed Flips: 30/0
Configured Flip Time: 60
Critical Interfaces: 1/1
```



```
41
42      Done
43 <!--NeedCopy-->
```

Alarme SNMP pour état primaire collant

Activez l'alarme SNMP HA-STICKY-PRIMARY dans un nœud à haute disponibilité configuré si vous souhaitez être averti du fait que le nœud devient principal collant. Lorsque le nœud devient autocollant principal, il alerte en générant un message d'interruption (stickyPrimary (1.3.6.1.4.1.5951.1.1.0.138)) et l'envoie à toutes les destinations d'interruption SNMP configurées. Pour plus d'informations sur la configuration des alarmes SNMP et des destinations d'interruption, consultez Configuration de Citrix ADC pour générer des interruptions SNMPv1 et SNMPv2.

Questions fréquemment posées

Prenons un exemple de configuration haute disponibilité de deux appliances Citrix ADC NS-1 et NS-2 en mode non-INC. Le nombre maximal de basculements et le temps maximal de basculement dans les deux nœuds ont été définis avec les mêmes valeurs.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple :

Entité	Détail
Adresse IP de NS-1	10.102.173.211
Adresse IP de NS-2	10.102.173.212
Nombre maximal de basculement	2
Temps de retournement maximal	200

Pour plus d'informations sur le nombre maximal de basculement et les paramètres de temps de retournement maximum, reportez-vous au pdf.

Configuration du jeu d'interface de basculement

August 20, 2021

Un jeu d'interfaces de basculement (FIS) est un groupe logique d'interfaces. Dans une configuration HA, l'utilisation d'un FIS est un moyen d'empêcher le basculement en regroupant des interfaces de

sorte que, lorsqu'une interface échoue, d'autres interfaces fonctionnelles soient toujours disponibles. Un FIS peut également être configuré pour les nœuds d'un cluster Citrix ADC.

Les interfaces HA MON qui ne sont pas liées à un FIS sont appelées interfaces critiques (CI) car si l'une d'elles échoue, le basculement est déclenché.

> **Remarque** :
>
> Un SIF ne crée pas de configuration active et de secours. Il n'empêche pas non plus de pontage des boucles lors de la connexion à des liens vers le même VLAN.

Création ou modification d'une SIF

Pour ajouter un FIS et y lier des interfaces à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add fis <name>`
- `bind fis \<name\> \<ifnum\> ...`
- `show fis \<name\>`

Exemple

```
1 > add fis fis1
2  Done
3 > bind fis fis1 1/3 1/5
4  Done
5 <!--NeedCopy-->
```

Une interface non liée devient une interface critique (CI) si elle est activée et que HA MON est activée.

Pour délier une interface d'un FIS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `unbind fis \<name\> \<ifnum\> ...`
- `show fis \<name\>`

Exemple

```
1 > unbind fis fis1 1/3
2  Done
3 <!--NeedCopy-->
```


Pour configurer un FIS à l'aide de l'interface graphique

Accédez à Système > Haute disponibilité et, sous l'onglet Jeu d'interfaces de basculement, ajoutez un nouveau FIS ou modifiez un FIS existant.

Suppression d'une SIF

Lorsque le SIF est supprimé, ses interfaces sont marquées comme des interfaces critiques.

Pour supprimer un SIF à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
rm fis <name>
```

Exemple

```
1 > rm fis fis1
2   Done
3 <!--NeedCopy-->
```

Pour supprimer un SIF à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Jeu d'interfaces de basculement**, supprimez le SIF.

Comprendre les causes du basculement

September 8, 2021

Les événements suivants peuvent entraîner un basculement sur incident dans une configuration haute disponibilité :

1. Si le nœud secondaire ne reçoit pas de paquet de pulsation du cœur principal pendant une période qui dépasse l'intervalle mort défini sur le secondaire. (Voir la note 1.)
2. Le nœud principal rencontre une défaillance matérielle de sa carte SSL.
3. Le nœud principal ne reçoit aucun paquet de rythme cardiaque sur ses interfaces réseau pendant trois secondes.
4. Sur le nœud principal, une interface réseau qui ne fait pas partie d'un ensemble d'interface de basculement (FIS) ou d'un canal d'agrégation de liens (LA) et dont le moniteur HA (HAMON) est activé échoue. (Voir la note 2.)

5. Sur le nœud principal, toutes les interfaces d'un FIS échouent. (Voir la note 2.)
6. Sur le nœud principal, un canal LA avec HAMON activé échoue. (Voir la note 2.)
7. Sur le nœud principal, toutes les interfaces échouent (voir la note 2). Dans ce cas, le basculement se produit indépendamment de la configuration HAMON.
8. Sur le nœud principal, toutes les interfaces sont désactivées manuellement. Dans ce cas, le basculement se produit indépendamment de la configuration HAMON.
9. Vous forcez un basculement en émettant la commande forcer le basculement sur l'un ou l'autre des nœuds.
10. Un moniteur de routage lié au nœud principal est en panne.

> **Remarque 1 :**
>
> Pour plus d'informations sur la définition de l'intervalle mort, voir Configuration des intervalles de communication. Les causes possibles pour un nœud ne recevant pas de paquets de pulsations d'un nœud homologue sont les suivantes :
>
> - Un problème de configuration réseau empêche les battements de cœur de traverser le réseau entre les nœuds HA.
> - Le nœud homologue rencontre une défaillance matérielle ou logicielle qui provoque le blocage (blocage), le redémarrage ou l'arrêt du traitement et du transfert des paquets Heartbeat.
>
> **Remarque 2 :**
>
> Dans ce cas, échouer signifie que l'interface a été activée mais passe à l'état DOWN, comme le montre la commande show interface ou depuis l'interface graphique. Les causes possibles de l'état DOWN d'une interface activée sont LINK DOWN et TXSTALL.

Forcer un nœud à basculer

August 20, 2021

Vous pouvez forcer un basculement si, par exemple, vous devez remplacer ou mettre à niveau le nœud principal. Vous pouvez forcer le basculement à partir du nœud principal ou secondaire. Un basculement forcé n'est ni propagé ni synchronisé. Pour afficher l'état de la synchronisation après un basculement forcé, vous pouvez afficher l'état du nœud.

Un basculement forcé échoue dans l'une des circonstances suivantes :

- Vous forcez le basculement sur incident sur un système autonome.
- Le nœud secondaire est désactivé.
- Le nœud secondaire est configuré pour rester secondaire.

L'appliance Citrix ADC affiche un message d'avertissement s'il détecte un problème potentiel lorsque

vous exécutez la commande force de basculement. Le message inclut les informations qui ont déclenché l'avertissement et demande une confirmation avant de continuer.

Vous pouvez forcer un basculement sur incident sur un nœud principal, un nœud secondaire et lorsque les nœuds sont en mode écoute.

- **Forcer le basculement sur incident sur le nœud principal**.

  Si vous forcez le basculement sur incident sur le nœud principal, le principal devient le secondaire et le secondaire devient le principal. Le basculement forcé n'est possible que lorsque le nœud principal peut déterminer que le nœud secondaire est UP.

  Si le nœud secondaire est DOWN, la commande force basculement renvoie le message d'erreur suivant : "Opération impossible en raison de l'état homologue non valide. Rectifier et réessayer."

  Si le système secondaire est dans l'état revendiquant ou inactif, il renvoie le message d'erreur suivant :

  ```
  Operation not possible now. Please wait for the system to stabilize
  before retrying.
  ```

- **Forcer le basculement sur incident sur le nœud secondaire**.

  Si vous exécutez la commande forcer le basculement à partir du nœud secondaire, le nœud secondaire devient principal et le nœud principal devient secondaire. Un basculement forcé ne peut se produire que si la santé du nœud secondaire est bonne et qu'il n'est pas configuré pour rester secondaire.

  Si le nœud secondaire ne peut pas devenir le nœud principal ou si le nœud secondaire a été configuré pour rester secondaire (à l'aide de l'option STAYSECONDARY), le nœud affiche le message d'erreur suivant :

  ```
  Operation not possible as my state is invalid. View the node for more
  information.
  ```

- **Forcer le basculement lorsque les nœuds sont en mode écoute**.

  Lorsque les deux nœuds d'une paire HA exécutent des versions différentes du logiciel système, le nœud exécutant la version supérieure passe en mode écoute. Dans ce mode, ni la propagation des commandes ni la synchronisation ne fonctionnent.

  Avant de mettre à niveau le logiciel système sur les deux nœuds, testez la nouvelle version sur l'un des nœuds. Pour ce faire, vous devez forcer un basculement sur le système déjà mis à niveau. Le système mis à niveau prend alors le relais en tant que nœud principal, mais aucune propagation ou synchronisation des commandes n'a lieu. De plus, toutes les connexions doivent être rétablies.

> **Important**
>
> Si vous forcez un basculement lorsqu'une opération de synchronisation HA est en cours, certaines sessions de données actives sur la configuration HA peuvent être perdues. Attendez donc que l'opération de synchronisation HA soit terminée avant d'effectuer l'opération de basculement de force.

Pour forcer le basculement sur un nœud à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
force HA failover
```

Pour forcer le basculement sur un nœud à l'aide de l'interface graphique :

Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, sélectionnez le nœud, dans la liste Action, sélectionnez **Forcer le basculement**.

Forcer le nœud secondaire à rester secondaire

August 20, 2021

Dans une configuration HA, le nœud secondaire peut être forcé de rester secondaire quel que soit l'état du nœud principal.

Par exemple, supposons que le nœud principal doit être mis à niveau et que le processus prendra quelques secondes. Pendant la mise à niveau, le nœud principal peut s'arrêter pendant quelques secondes, mais vous ne voulez pas que le nœud secondaire prenne le relais ; vous voulez qu'il reste le nœud secondaire même s'il détecte une défaillance dans le nœud principal.

Lorsque vous forcez le nœud secondaire à rester secondaire, il restera secondaire même si le nœud principal tombe en panne. En outre, lorsque vous forcez l'état d'un nœud dans une paire HA à rester secondaire, il ne participe pas aux transitions de machines d'état HA. L'état du nœud est affiché en tant que STAYSECONDARY.

Forcer le nœud à rester secondaire fonctionne à la fois sur les nœuds autonomes et secondaires. Sur un nœud autonome, vous devez utiliser cette option avant de pouvoir ajouter un nœud pour créer une paire HA. Lorsque vous ajoutez le nouveau nœud, le nœud existant arrête le traitement du trafic et devient le nœud secondaire. Le nouveau nœud devient le nœud principal.

> **Remarque** :
>
> Lorsque vous forcez un système à rester secondaire, le processus de forçage n'est ni propagé ni synchronisé. Elle affecte uniquement le nœud sur lequel vous exécutez la commande.

Pour forcer le nœud secondaire à rester secondaire à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ha node -hastatus STAYSECONDARY
```

Pour forcer le nœud secondaire à rester secondaire à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité**, sous l'onglet **Nœuds**, ouvrez le nœud local, puis sélectionnez **STAY SECONDARY**.

Forcer le nœud principal à rester principal

August 20, 2021

Dans une configuration HA, vous pouvez forcer un nœud principal sain à rester principal même après un basculement. Vous pouvez activer cette option soit sur un nœud principal d'une paire HA. Cette option permet au nœud principal d'être en état principal tant qu'il est sain.

Sur un nœud autonome, vous devez utiliser cette option avant de pouvoir ajouter un nœud pour créer une paire HA. Lorsque vous ajoutez le nouveau nœud, le nœud existant continue à fonctionner en tant que nœud principal, et le nouveau nœud devient le nœud secondaire.

Pour forcer le nœud principal à rester principal à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ha node -hastatus STAYPRIMARY
```

Pour forcer le nœud principal à rester principal à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité**, sous l'onglet **Nœuds**, ouvrez le nœud local, puis sélectionnez **STAY PRIMARY**.

Comprendre le calcul de la vérification de l'état de haute disponibilité

January 21, 2021

Le tableau suivant résume les facteurs examinés dans le calcul d'un bilan de santé :

- État des jeux d'interface de basculement
- État des interfaces critiques
- État des moniteurs de route

Le tableau suivant récapitule le calcul de la vérification de l'état.

Jeux d'interface de basculement	Interfaces critiques	Moniteur de routage	Condition
N	O	N	Si le système possède des interfaces critiques, toutes ces interfaces critiques doivent être UP.
O	O	N	Si le système possède des jeux d'interface de basculement, tous ces jeux d'interface de basculement doivent être UP.
O	O	O	Si des moniteurs de routage sont configurés sur le système, toutes les routes surveillées doivent être présentes dans l'interface de basculement définie.

FAQ haute disponibilité

August 20, 2021

1. Quels sont les différents ports utilisés pour échanger les informations relatives à la HA entre les nœuds d'une configuration HA ?

   Dans une configuration HA, les deux nœuds utilisent les ports suivants pour échanger des informations relatives à HA :

- UDP Port 3003, pour échanger des paquets de pulsations.
- Port 3010, pour la synchronisation et la propagation des commandes.

2. Quelles sont les conditions qui déclenchent la synchronisation ?

   La synchronisation est déclenchée par l'une des conditions suivantes :

   - Le numéro d'incarnation du nœud principal, reçu par le nœud secondaire, ne correspond pas à celui du nœud secondaire.
     Remarque : Les deux nœuds d'une configuration HA conservent un compteur appelé *numéro d'incarnation*, qui compte le nombre de configurations dans le fichier de configuration du nœud. Chaque nœud envoie son numéro d'incarnation à l'autre nœud dans les messages de pulsation. Le numéro d'incarnation n'est pas incrémenté pour les commandes suivantes :
     a) Toutes les commandes associées à la configuration HA. Par exemple, ajoutez un nœud ha, définissez un nœud ha et liez un nœud ha.
     b) Toutes les commandes liées à l'interface. Par exemple, set interface et unset interface.
     c) Toutes les commandes liées au canal. Par exemple, add channel, set channel et bind channel.
   - Le nœud secondaire apparaît après un redémarrage.
   - Le nœud principal devient secondaire après un basculement.

3. Quelles configurations ne sont pas synchronisées ou propagées dans une configuration HA en mode INC ou non-INC ?

   Les commandes suivantes ne sont ni propagées ni synchronisées avec le nœud secondaire :

   - Toutes les commandes de configuration HA spécifiques au nœud. Par exemple, ajoutez un nœud ha, définissez un nœud ha et liez un nœud ha.
   - Toutes les commandes de configuration liées à l'interface. Par exemple, set interface et unset interface.
   - Toutes les commandes de configuration associées au canal. Par exemple, add channel, set channel et bind channel.

   > **Remarque :**
   >
   > les configurations suivantes ne sont ni synchronisées ni propagées uniquement en HA en mode INC. Chaque nœud a son propre :
   >
   > ```
   > 1 - SNIP
   > ```
   >
   > - VLAN
   > - Itinéraires (sauf les routes LLB)
   > - Moniteurs de routage
   > - Règles RNAT (sauf toute règle RNAT avec VIP comme IP NAT)

- Configurations de routage dynamique
- Profils de réseau

4. Une configuration ajoutée au nœud secondaire est-elle synchronisée sur le principal ?

   Non, une configuration ajoutée au nœud secondaire n'est pas synchronisée avec le nœud principal.

5. Quelle pourrait être la raison pour laquelle les deux nœuds prétendent être les principaux dans une configuration HA ?

   La raison la plus probable est que les nœuds primaire et secondaire sont tous les deux sains, mais que le secondaire ne reçoit pas les paquets de pulsations du primaire. Le problème pourrait être avec le réseau entre les nœuds.

6. Une configuration HA se heurte-t-elle à des problèmes si vous déployez les deux nœuds avec des paramètres d'horloge système différents ?

   Différents paramètres d'horloge système sur les deux nœuds peuvent causer les problèmes suivants :

   - Les horodatages dans les entrées du fichier journal ne correspondent pas. Cette situation rend difficile l'analyse des entrées de journal pour tout problème.
   - Après un basculement, vous pouvez rencontrer des problèmes avec tout type de persistance basée sur les cookies pour l'équilibrage de charge. Une différence significative entre les temps peut faire expirer un cookie plus tôt que prévu, entraînant la fin de la session de persistance.
   - Des considérations similaires s'appliquent à toutes les décisions liées au temps sur les nœuds.

7. Quelles sont les conditions de défaillance de la commande *force HA sync* ?

   La synchronisation forcée échoue dans l'une des circonstances suivantes :

   - Vous forcez la synchronisation lorsque la synchronisation est déjà en cours.
   - Vous forcez la synchronisation sur une appliance Citrix ADC autonome.
   - Le nœud secondaire est désactivé.
   - La synchronisation HA est désactivée sur le nœud secondaire actuel.
   - La propagation HA est désactivée sur le nœud principal actuel et vous forcez la synchronisation à partir du nœud principal.

8. Quelles sont les conditions d'échec de la commande *synchroniser les fichiers HA* ?

   La synchronisation des fichiers de configuration échoue dans l'une des circonstances suivantes :

   - Sur un système autonome.
   - Avec le nœud secondaire désactivé.

9. Dans une configuration HA, si le nœud secondaire prend le relais en tant que principal, revient-il à l'état secondaire si le principal d'origine revient en ligne ?

   Non. Une fois que le nœud secondaire prend le relais comme principal, il reste comme principal même si le nœud principal d'origine revient en ligne. Pour échanger le statut principal et secondaire des nœuds, exécutez la commande *force failover*.

10. Quelles sont les conditions d'échec de la commande force basculement ?

    Un basculement forcé échoue dans l'une des circonstances suivantes :

    - Vous forcez le basculement sur incident sur un système autonome.
    - Le nœud secondaire est désactivé.
    - Le nœud secondaire est configuré pour rester secondaire.
    - Le nœud principal est configuré pour rester principal.
    - L'état du nœud homologue est inconnu.

Résolution des problèmes de haute disponibilité

August 20, 2021

Les problèmes de haute disponibilité les plus courants concernent la fonctionnalité de haute disponibilité qui ne fonctionne pas du tout, ou ne fonctionne que de façon intermittente. Voici les problèmes courants de haute disponibilité, ainsi que les causes et les résolutions probables.

- **Problème**
  L'incapacité des appliances Citrix ADC à coupler les appliances Citrix ADC dans une configuration haute disponibilité.
  - **Cause**
    Connectivité réseau
    Résolution
    Vérifiez que les deux appliances sont connectées au commutateur et que les interfaces sont activées.
  - **Cause**
    Correspondance dans le mot de passe pour le compte Administrateur par défaut
    Résolution
    Vérifiez que le mot de passe des deux appliances est le même.
  - **Cause**
    Conflit de propriété intellectuelle
    Résolution
    Vérifiez que les deux appliances disposent d'une adresse IP Citrix ADC (NSIP) unique. Les appliances ne doivent pas avoir la même adresse NSIP.

- **Cause**
  ID de nœud non concordance
  Résolution
  Vérifiez que la configuration de l'ID de nœud sur les deux appliances est unique. Les appliances ne doivent pas avoir la même configuration d'ID de nœud. En outre, vous devez affecter une valeur pour un ID de nœud compris entre 1 et 64.
- **Cause**
  L'incompatibilité du mot de passe du nœud RPC
  Résolution
  Vérifiez que les deux nœuds ont le même mot de passe de nœud RPC.
- **Cause**
  Un administrateur a désactivé le nœud distant
  Résolution
  Activez le nœud distant.
- **Cause**
  L'application Pare-feu a bloqué les paquets de pulsations
  Résolution

Vérifiez que le port UDP 3003 est autorisé.

- **Émission**
  Les deux appliances prétendent être l'appliance principale.
  - **Cause**
    Paquets de pulsation manquants entre les appliances
    Résolution
    Vérifiez que le port UDP 3003 n'est pas bloqué pour la communication entre les appliances.
- **Problème**
  L'appliance Citrix ADC n'est pas en mesure de synchroniser la configuration.
  - **Cause**
    Une application pare-feu bloque le port requis.
    Résolution
    Vérifiez que le port UDP 3010 (ou le port UDP 3008 avec synchronisation sécurisée) n'est pas bloqué pour la communication entre les appliances.
  - **Cause**
    Un administrateur a désactivé la synchronisation.
    Résolution
    Activez la synchronisation sur l'appliance qui a le problème.
  - **Cause**
    Différentes versions ou versions de Citrix ADC sont installées sur les appliances.
    Résolution
    Mettez à niveau les appliances vers la même version ou version Citrix ADC.

- **Échec**
  de la propagation des commandes entre les appliances.
  - **Cause**
    Une application pare-feu bloque le port.
    Résolution
    Vérifiez que le port UDP 3011 (ou le port UDP 3009 avec propagation sécurisée) n'est pas bloqué pour la communication entre les appliances.
  - **Cause**
    Un administrateur a désactivé la propagation des commandes.
    Résolution
    Activez la propagation des commandes sur l'appliance qui a le problème.
  - **Cause**
    Différentes versions ou versions de Citrix ADC sont installées sur les appliances.
    Résolution
    Mettez à niveau les appliances vers la même version ou version Citrix ADC.
- **Problème**
  Les appliances Citrix ADC de la paire haute disponibilité ne peuvent pas exécuter le processus de basculement forcé.
  - **Cause**
    Le nœud secondaire est désactivé.
    Résolution
    Activez le nœud secondaire.
  - **Cause**
    Le nœud secondaire est configuré pour rester secondaire.
    Résolution
    Définissez l'état de haute disponibilité secondaire du nœud secondaire sur Activer à partir de Stay Secondary.
- **Problème**
  L'appliance secondaire ne reçoit aucun trafic après le processus de basculement.
  - **Cause**
    Le routeur en amont ne comprend pas les messages GARP de l'appliance Citrix ADC.
    Résolution
    Configurez l'adresse MAC virtuelle sur l'appliance secondaire.

Gestion des messages de pulsation haute disponibilité sur une appliance Citrix ADC

January 21, 2021

Les deux nœuds d'une configuration haute disponibilité envoient et reçoivent des messages de pulsation entre eux sur toutes les interfaces activées. Les messages de pulsation s'écoulent indépendamment du paramètre HA MON sur ces interfaces. Si NSVLAN ou les deux (NSVLAN et SYNC) sont configurés sur une appliance, les messages de pulsation ne circulent que via les interfaces activées qui font partie du NSVLAN et du SYNCVLAN.

Si un nœud ne reçoit pas les messages de pulsation sur une interface activée, il envoie des alertes critiques au Command Center et aux gestionnaires SNMP spécifiés. Ces alertes critiques donnent de fausses alarmes et attirent l'attention inutile des administrateurs sur les interfaces qui ne sont pas configurées dans le cadre des connexions au nœud homologue.

Pour résoudre ce problème, l'option HAHeartBeat pour les interfaces et les canaux est utilisée pour activer ou désactiver le flux de message HA HeartBeat sur eux.

Pour gérer les messages de pulsation haute disponibilité sur une interface à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set interface <ID> [-HAHeartBeat ( ON | OFF )]`
- `show interface <ID>`

Pour gérer les messages de pulsation haute disponibilité sur un canal à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set channel <ID> [-HAHeartBeat ( ON | OFF )]`
- `show channel <ID>`

Pour gérer les messages de pulsation haute disponibilité pour une interface à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **Interfaces**.
2. Activez ou désactivez le paramètre **HA Heart Beat** .

Pour gérer les messages de pulsation haute disponibilité sur un canal à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **Canaux**.
2. Activez ou désactivez le paramètre **HA Heart Beat** .

Suppression et remplacement d'un Citrix ADC dans une configuration haute disponibilité

August 20, 2021

Cette rubrique vous aide à traiter les remplacements RMA. En outre, cette rubrique contient des instructions sur la sauvegarde des configurations, la mise à niveau ou la rétrogradation de la version du logiciel livrée et la configuration du mot de passe RPC sur ADC.

Points à considérer

Les configurations suivantes ne sont ni synchronisées ni propagées dans une configuration haute disponibilité en mode INC (Independent Network Configuration) ou non-INC :

- Toutes les commandes de configuration HA spécifiques au nœud. Par exemple, ajoutez un nœud ha, définissez un nœud ha et liez un nœud ha.
- Toutes les commandes de configuration liées à l'interface. Par exemple, set interface et unset interface.
- Toutes les commandes de configuration associées au canal. Par exemple, add channel, set channel et bind channel.
- Toutes les commandes de configuration de l'interface HA Monitoring.

Les configurations suivantes ne sont ni synchronisées ni propagées dans une configuration HA en mode INC (Configuration réseau indépendante) :

- SNIP
- VLAN
- Itinéraires (sauf les routes LLB)
- Moniteurs de routage
- Règles RNAT (sauf toute règle RNAT avec VIP comme IP NAT)
- Configurations de routage dynamique

Instructions

Procédez comme suit pour remplacer un Citrix ADC dans la configuration haute disponibilité :

- Supprimer un nœud secondaire Active Citrix ADC
- Configurer le nœud secondaire de remplacement
- Vérifier et mettre à jour la version logicielle sur ADC de remplacement
- Définir le mot de passe sur Nouveau secondaire à Correspondance primaire
- Ajouter des licences à ADC de remplacement
- Création d'une paire HA entre le nœud principal et le nouveau nœud secondaire

Supprimer un nœud secondaire actif

1. Ouvrez une session sur les deux ADC et exécutez la commande suivante pour confirmer quel nœud est principal et quel nœud est secondaire :


```
show ha node
<!--NeedCopy-->
```

2. Ouvrez une session sur ADC principal, sauvegardez les configurations sur le nœud principal et copiez les fichiers hors de ADC avant les modifications. Ces fichiers se trouvent sous le répertoire « /var /ns_sys_backup/ ».

   Les étapes sont les suivantes :

   a) Enregistrez les configurations en cours d'exécution de ADC dans la mémoire :

   ```
   save ns config
   <!--NeedCopy-->
   ```

   b) Créez le package de fichiers de sauvegarde complet :

   ```
   create system backup -level full
   <!--NeedCopy-->
   ```

   c) Créez le package de fichiers de sauvegarde de base :

   ```
   create system backup -level basic
   <!--NeedCopy-->
   ```

3. Une fois que tous les fichiers de sauvegarde ont été générés, assurez-vous de les copier hors de l'appareil avant de continuer.

   À partir d'un terminal Windows, ouvrez une invite de commandes et copiez les fichiers de sauvegarde hors de ADC et sur votre disque dur local. Cela peut être fait en utilisant la commande suivante :

   ```
   pscp <username>@<NSIP>:<Target file source>  <Target file
      destination>
   <!--NeedCopy-->
   ```

   Exemple :

   ```
   pscp nsroot@10.125.245.78:/var/ns_sys_backup/backup_basic_10
      .125.245.78_2016_09_14_15_08.tgz c:\nsbackup\backup_basic_10
      .125.245.78_2016_09_14_15_08.tgz
   <!--NeedCopy-->
   ```

   Lorsque vous y êtes invité, entrez le mot de passe du compte administrateur spécifié, puis appuyez sur Entrée. Répétez ces étapes jusqu'à ce que tous les groupes de sauvegarde soient copiés sur le PC local avant de continuer.

4. SSH dans ADC secondaire et réglez l'unité sur le statut "STAYSECONDARY". Cela forcera l'unité à ne pas tenter d'assumer le rôle principal en cas de défaillance détectée lors de l'échange. Vérifiez que vous êtes connecté à ADC secondaire avant d'exécuter cette étape

```
set ha node  -haStatus <state>
set ha node  -haStatus STAYSECONDARY
<!--NeedCopy-->
```

5. Une fois que l'**état du nœud** de ADC secondaire affiche avec succès STAYSECONDARY, basculez vers ADC principal et supprimez le nœud secondaire et exécutez la commande suivante :

```
save ns config
<!--NeedCopy-->
```

   Lorsque vous êtes connecté à ADC principal, exécutez les commandes suivantes

   a) Exécutez la commande suivante pour identifier la valeur numérique qui représente le nœud HA secondaire :

```
show ha node
<!--NeedCopy-->
```

   b) Exécutez la commande suivante pour supprimer ADC secondaire de la paire HA principale ;

```
rm ha node <node ID>
<!--NeedCopy-->
```

   c) Exécutez la commande suivante pour enregistrer la configuration :

```
save ns config
<!--NeedCopy-->
```

   d) Maintenant que ADC secondaire est supprimé, arrêtez, déconnectez et supprimez ADC secondaire du réseau.

      Note. Veillez à étiqueter toutes les connexions avant de vous déconnecter.

Configurer le nœud secondaire de remplacement

1. Une fois ADC de remplacement en place, mettez le nouvel appareil sous tension. NE PAS CONNECTER les connexions réseau à ce stade.
2. Une fois le démarrage terminé, utilisez le port de la console pour vous connecter à ADC et configurez le NSIP que vous utiliserez pour vous connecter à l'appareil.

3. Lorsque vous y êtes invité, sélectionnez **4**.

   Remarque. Dans cet exemple, nous utilisons un NSIP différent pour ADC de remplacement. Si vous souhaitez utiliser l'IP de l'unité secondaire d'origine, vous pouvez la modifier sur le remplacement avant de lier le nouveà ADC à l'unité HA principale.

4. ADC doit maintenant être démarré. Connectez maintenant l'interface réseau qui sera utilisée pour le trafic de gestion et vérifiez que l'adresse IP est accessible depuis votre réseau.

Vérifier et mettre à jour la version logicielle sur ADC de remplacement

Avant de synchroniser la nouvelle unité avec ADC principal, nous devons nous assurer que les deux ADC exécutent la même version.

1. Pour vérifier la version sur ADC, exécutez la commande suivante :

```
show version
<!--NeedCopy-->
```

2. Lorsque vous êtes sur le nouveà ADC secondaire, créez un sous-dossier dans **/var** à utiliser pour la mise à niveau.
3. Accédez à Citrix Downloads et téléchargez le package approprié correspondant à la version de build exécutée sur l'ADC principal.
4. Téléchargez et extrayez le fichier .tgz :

```
tar -xvzf "file.tgz"
<!--NeedCopy-->
```

5. Copiez les fichiers extraits dans ADC secondaire. Sur votre terminal Windows, ouvrez une « Invite de commandes » et accédez au répertoire contenant le package de construction .tgz extrait et exécutez la commande pscp suivante :

```
pscp <Target file source>  <username>@<NSIP>:<Target file
   destination>
<!--NeedCopy-->
```

   Exemple :

```
C:\inetpub>pscp c:\inetpub\build-12.1-47.14_nc.tgz nsroot@10
   .20.245.80:/var/NS_upg_12.1_47.14/build-12.1-47.14_nc.tgz
<!--NeedCopy-->
```

6. Une fois le fichier transféré, revenez à ADC secondaire et mettez à niveau. Pour obtenir des instructions détaillées, reportez-vous à la section Mise à niveau d'une appliance Citrix ADX Standalone Appliance.

7. Une fois le nouveau secondaire redémarré, SSH revient dans l'unité et confirme que la mise à niveau est réussie et que la construction correspond à celle du primaire.

Définir le mot de passe sur le nœud secondaire de remplacement pour correspondre au principal

Remarque : Si à ce stade vous souhaitez modifier l'adresse IP de gestion (NSIP) du nouveà ADC secondaire, vous pouvez le faire avant d'aller de l'avant.

Modifiez le mot de passe du nouveà ADC secondaire pour qu'il corresponde au mot de passe qui se trouve actuellement sur ADC principal.

1. Assurez-vous que le mot de passe du compte administrateur (nsroot) par défaut est le même que ADC principal. Ceci est réalisé à l'aide de la commande suivante lorsque vous êtes connecté via SSH dans la nouvelle unité secondaire :

```
set system user <user> <password>
<!--NeedCopy-->
```

   Cette commande définit/réinitialise le mot de passe de l'utilisateur spécifié.

2. SSH dans ADC principal et le nouveà ADC secondaire et confirmez que les mots de passe correspondent.

Ajouter des licences au nœud secondaire de remplacement

Une fois le nouveà ADC mis à jour et prêt pour le jumelage, téléchargez et installez la licence appropriée pour le nœud de remplacement.

1. Accédezhttps://www.citrix.com à demander et télécharger des licences pour la nouvelle unité de remplacement.

2. Une fois que vous avez téléchargé toutes les licences appropriées, SSH dans le nouveà ADC secondaire et tapez la commande suivante pour voir l'état actuel des licences :

```
show license
<!--NeedCopy-->
```

3. À partir de l'invite de commandes du terminal Windows, vous devez maintenant télécharger les fichiers de licence vers le nouveà ADC secondaire à l'aide de la commande suivante :

   Note. Si vous disposez de plusieurs licences, répétez cette étape jusqu'à ce que toutes les licences soient téléchargées.

```
pscp <Target file source>  <username>@<NSIP>:<Target file
    destination>
```



```
<!--NeedCopy-->
```

Exemple :

```
C:\inetpub>pscp c:\inetpub\NS-VPX-3K-LIC-020030ad0024.lic
   nsroot@10.125.245.80:/nsconfig/license/NS-VPX-3K-LIC-020030
   ad0024.lic
<!--NeedCopy-->
```

4. SSH dans le nouveà ADC secondaire et effectuez un redémarrage à chaud à l'aide de la commande suivante :

```
reboot  -w
<!--NeedCopy-->
```

Après le redémarrage de l'unité, SSH dans l'unité et exécutez la commande show license une fois de plus. À ce stade, les licences devraient être appliquées.

Configurer la haute disponibilité entre le nœud principal et le nouveau nœud secondaire

À ce stade, nous sommes maintenant prêts à joindre les unités Citrix ADC en une paire haute disponibilité. Pour plus d'informations, voir Configuration de la haute disponibilité.

Nouvelle tentative de demande

August 20, 2021

Lorsqu'une appliance Citrix ADC reçoit une requête HTTP mais présente une défaillance de connexion avec le serveur principal, l'appliance utilise une directive de nouvelle tentative. La nouvelle tentative de demande corrige les scénarios d'échec de connexion et permet à l'appliance de choisir le service disponible suivant et de transférer la demande. En effectuant une nouvelle tentative de demande, le client peut gagner du temps aller-retour (RTT).

La fonction de nouvelle tentative de demande est applicable pour les scénarios d'échec de connexion suivants :

- Si le serveur principal réinitialise une connexion TCP lorsqu'une requête HTTP est reçue.
- Si le serveur principal réinitialise une connexion TCP pendant l'établissement de la connexion.
- Si la réponse du serveur principal expédie (en fonction de la valeur de délai d'attente configurée) lorsque l'appliance envoie une requête HTTP.

Pour plus de détails, voir Demander une nouvelle tentative.

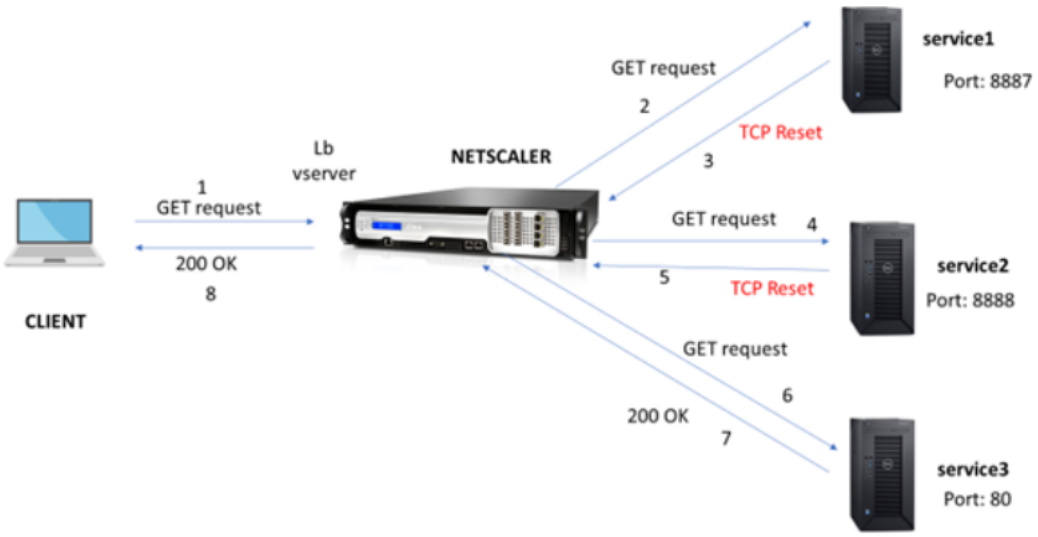
Demander une nouvelle tentative si le serveur principal réinitialise la connexion TCP

August 20, 2021

Lorsqu'un serveur principal réinitialise une connexion TCP, la fonction de nouvelle tentative de demande transmet la demande au serveur disponible suivant, au lieu d'envoyer la réinitialisation au client. En effectuant l'équilibrage de rechargement, le client enregistre RTT lorsque l'appliance lance la même demande au service disponible suivant.

Fonctionnement d'une nouvelle tentative de demande lorsque le serveur principal réinitialise une connexion TCP

Le diagramme suivant montre comment les composants interagissent les uns avec les autres.



1. Le processus commence par activer la fonctionnalité appqoe sur votre appliance.
2. Lorsque le client envoie une requête HTTP ou HTTPS, le serveur virtuel d'équilibrage de charge envoie la demande au serveur principal.
3. Si le service demandé n'est pas disponible, le serveur principal réinitialise la connexion TCP.
4. Si la configuration appqoe est activée avec le nombre souhaité de tentatives de nouvelle tentative spécifié, le serveur virtuel d'équilibrage de charge utilise l'algorithme d'équilibrage de charge configuré pour transférer la demande au serveur d'applications disponible suivant.
5. Une fois que le serveur virtuel d'équilibrage de charge a reçu la réponse, l'appliance transmet la réponse au client.

6. Si les serveurs back-end disponibles sont égaux ou inférieurs au nombre de tentatives et si tous les serveurs envoient une réinitialisation, l'appliance répondra à une erreur interne de 500 serveurs. Considérez un scénario avec cinq serveurs disponibles et le nombre de tentatives est défini sur six. Si les cinq serveurs réinitialisent la connexion, l'appliance renvoie une erreur de serveur interne 500 au client.
7. De même, si le nombre de serveurs principaux est supérieur au nombre de nouvelles tentatives et si les serveurs back-end réinitialisent la connexion, l'appliance transmet la réinitialisation au client. Considérez un scénario avec trois serveurs back-end et le nombre de tentatives est défini comme deux. Si les trois serveurs réinitialisent la connexion, l'appliance envoie une réponse de réinitialisation au client.

Configurer une nouvelle tentative de demande pour la méthode GET

Pour configurer la fonctionnalité de nouvelle tentative pour la méthode GET, vous devez effectuer les étapes suivantes.

1. Activer AppQoE
2. Ajouter une action AppQoE
3. Ajouter une stratégie AppQoE
4. Lier la stratégie AppQoE au serveur virtuel d'équilibrage de charge

Activer AppQoE

À l'invite de commandes, tapez :

```
enable ns feature appqoe
```

Ajouter une action AppQoE

Vous devez configurer une action AppQoE pour spécifier si vous souhaitez que l'appliance réessaye après une réinitialisation TCP et le nombre de tentatives de nouvelle tentative.

```
add appqoe action reset_action -retryOnReset ( YES | NO )-numretries <
positive_integer>]
```

Exemple :

```
add appqoe action reset_action -retryOnReset YES -numretries 5
```

Où,
retryOnReset. Activez une nouvelle tentative si le serveur principal réinitialise une connexion TCP.
numretries. Réessayer le compte.

Ajouter une stratégie AppQoE

Pour implémenter AppQoE, vous devez configurer la stratégie AppQoE pour hiérarchiser les requêtes HTTP ou SSL entrantes dans une file d'attente spécifique.

À l'invite de commandes, tapez :

```
add appqoe policy <name> -rule <expression> -action <string>
```

Exemple :

```
add appqoe policy reset_policy -rule http.req.method.eq(get)-action reset_action
```

Lier la stratégie appqoe au serveur virtuel d'équilibrage de charge

Lorsqu'un serveur principal réinitialise une demande de paquets TCP et si vous souhaitez que le serveur virtuel d'équilibrage de charge transmette la demande au service disponible suivant, vous devez lier le serveur virtuel d'équilibrage de charge à la stratégie AppQoE.

À l'invite de commandes, tapez :

```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Exemple :

```
bind lb vserver v1 -policyName reset_policy -type REQUEST -priority 1
```

Configurer une nouvelle tentative de demande pour les demandes POST

Vous devez toujours faire preuve de prudence lorsque vous rechargez les demandes d'équilibrage qui écrivent des données dans le serveur principal. Pour de telles demandes, assurez-vous que la longueur du contenu est courte. Si la longueur du contenu est longue, cela peut entraîner une consommation de ressources. Suivez les étapes ci-dessous pour configurer l'équilibrage de rechargement pour les requêtes POST.

1. Activer AppQoE
2. Ajouter une action AppQoE
3. Ajouter une stratégie AppQoE
4. Lier la stratégie AppQoE au serveur virtuel d'équilibrage de charge

Activer AppQoE

À l'invite de commandes, tapez :

```
enable ns feature appqoe
```


Ajouter une action Appqoe

Vous devez ajouter une action AppQoE pour réessayer après une réinitialisation TCP et le nombre de tentatives de nouvelle tentative.

```
add appqoe action reset_action -retryOnReset ( YES | NO )-numretries <
positive_integer>]
```

Exemple :

```
add appqoe action reset_action -retryOnReset YES -numretries 5
```

Ajouter une stratégie Appqoe

Pour implémenter AppQoE, vous devez configurer la stratégie AppQoE pour définir comment mettre en file d'attente les connexions dans une file d'attente spécifique.

À l'invite de commandes, tapez :

```
add appqoe policy <name> -rule <expression> -action <string>
```

Exemple :

```
add appqoe policy reset_policy -rule HTTP.REQ.CONTENT_LENGTH.le(2000)-
action reset_action
```

> **Remarque :**
>
> Vous pouvez utiliser cette configuration si vous préférez restreindre la fonctionnalité de nouvelle tentative de demande pour une longueur de contenu inférieure à 2000.

Lier le serveur virtuel d'équilibrage de charge à la stratégie AppQoE

Lorsqu'un serveur principal réinitialise une demande de paquets TCP et si vous souhaitez que le serveur virtuel d'équilibrage de charge transmette la demande au service disponible suivant via une file d'attente spécifique, vous devez lier le serveur virtuel d'équilibrage de charge à la stratégie AppQoE.

À l'invite de commandes, tapez :

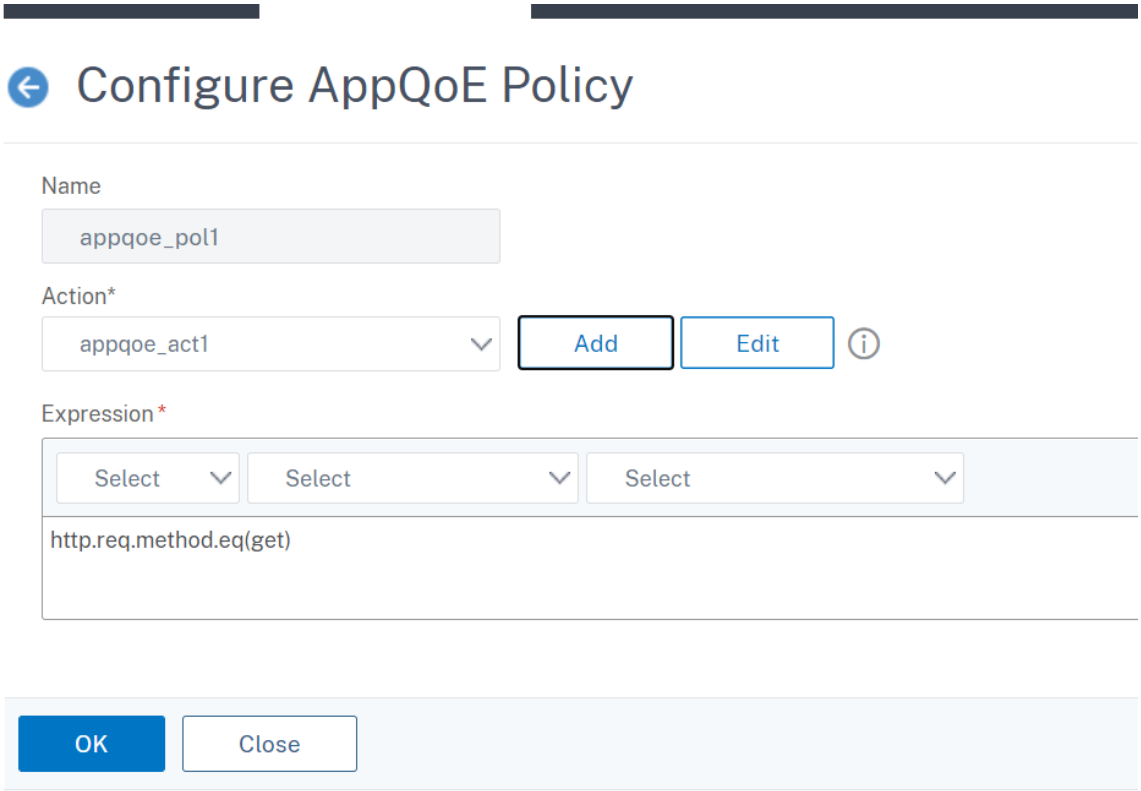
```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Exemple :

```
bind lb vserver v1 -policyName reset_policy -type REQUEST -priority 1
```


Configurer la stratégie AppQoE pour une nouvelle tentative de demande à l'aide de l'interface graphique Citrix ADC

1. Accédez à **AppExpert** > **AppQoE** > **Stratégies**.
2. Dans la page **Stratégies AppQoE**, cliquez sur **Ajouter**.
3. Dans la page **Créer une stratégie AppQoE**, définissez les paramètres suivants :
   a. Nom. AppQoE policy name
   b. Action. Ajoutez ou modifiez une action. Pour créer une action, reportez-vous à la section .
   c. Expression. Sélectionnez ou entrez une expression `HTTP.REQ.CONTENT_LENGTH.le(2000)` de stratégie.
4. Cliquez sur **Créer** et **Fermer**.

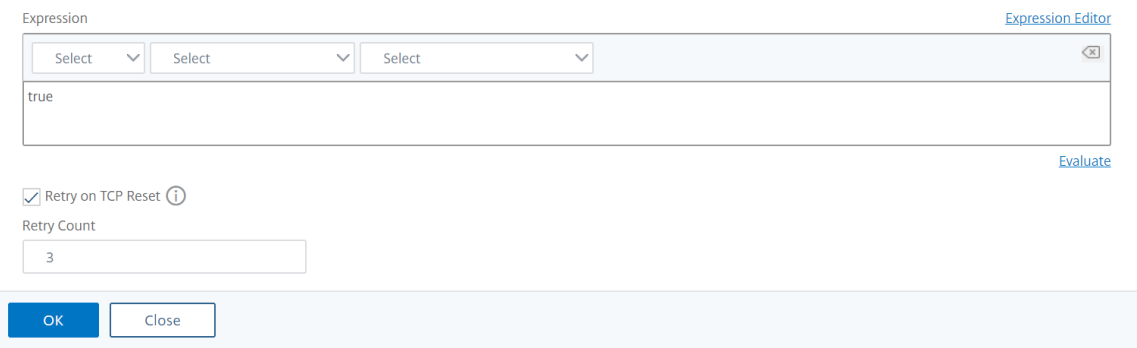


Configurer l'action AppQoE pour l'équilibrage de nouvelle tentative de demande à l'aide de l'interface graphique Citrix ADC

1. Accédez à **AppExpert** > **AppQoE** > **Action**.
2. Dans la page **AppQoE Actions**, cliquez sur **Ajouter**.
3. Dans la page **Créer une action AppQoE**, définissez les paramètres suivants pour réessayer lors de la réinitialisation TCP :

a. Réessayez lors de la réinitialisation TCP. Activez la case à cocher pour activer l'action de nouvelle tentative pour la réinitialisation TCP.
b. Retry Count. Saisissez le nombre de tentatives.

4. Cliquez sur **Créer** et **Fermer**.



Configurer une nouvelle tentative de demande pour la méthode GET lorsque le serveur principal se réinitialise sur l'établissement TCP SYN

La configuration CLI et GUI est similaire aux étapes suivies pour la méthode GET. Pour plus d'informations, consultez la section Configurer la demande d'essai pour la méthode GET. lorsque le serveur principal réinitialise une section de connexion.

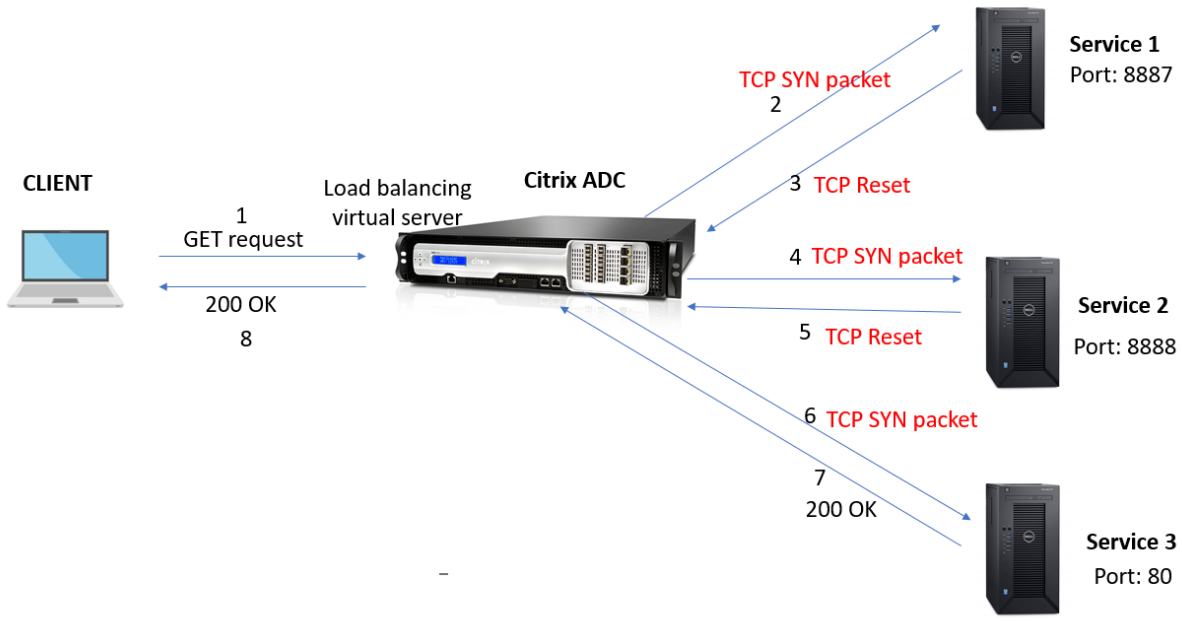
Demande de nouvelle tentative si le serveur principal réinitialise la connexion TCP pendant l'établissement de la connexion

August 20, 2021

Lorsqu'un serveur principal réinitialise une connexion TCP pendant l'établissement de la connexion, la fonction de nouvelle tentative de demande transmet la demande au serveur disponible suivant, au lieu d'envoyer la réinitialisation au client. En effectuant l'équilibrage de rechargement, le client enregistre RTT lorsque l'appliance lance la même demande au service disponible suivant.

Fonctionnement de la nouvelle tentative de demande lorsque le serveur principal réinitialise une connexion TCP sur l'établissement SYN

Le diagramme suivant montre les composants interagissent les uns avec les autres :



1. Le processus commence par activer la fonctionnalité appqoe sur votre appliance.
2. Lorsque le client envoie une requête HTTP ou HTTPS, le serveur virtuel d'équilibrage de charge initie la connexion au serveur principal.
3. Si le service demandé n'est pas disponible sur l'établissement TCP SYN, le serveur principal réinitialise la connexion TCP.
4. Si la configuration appqoe est activée avec le nombre souhaité de tentatives de nouvelle tentative spécifié, le serveur virtuel d'équilibrage de charge utilise l'algorithme d'équilibrage de charge configuré pour transférer la demande au serveur d'applications disponible suivant.
5. Une fois que le serveur virtuel d'équilibrage de charge a reçu la réponse, l'appliance transmet la réponse au client.
6. Si les serveurs back-end disponibles sont égaux ou inférieurs au nombre de tentatives et si tous les serveurs envoient une réinitialisation, l'appliance répondra à une erreur interne de 500 serveurs. Considérez un scénario avec cinq serveurs disponibles et le nombre de tentatives est défini sur six. Si les cinq serveurs réinitialisent la connexion, l'appliance renvoie une erreur de serveur interne 500 au client.
7. De même, si le nombre de serveurs principaux est supérieur au nombre de nouvelles tentatives et si les serveurs back-end réinitialisent la connexion sur l'établissement TCP SYN, l'appliance transmet la réinitialisation au client. Considérez un scénario avec trois serveurs back-end et le nombre de tentatives est défini comme deux. Si les trois serveurs réinitialisent la connexion, l'appliance envoie un paquet de réinitialisation au client.

Configurer une nouvelle tentative de demande (méthode GET et POST) lors de la réinitialisation du serveur principal sur l'établissement TCP SYN

La configuration CLI et GUI est similaire aux étapes suivies pour les méthodes GET et POST. Pour plus d'informations, consultez la rubrique Configurer une nouvelle tentative de demande pour la méthode GET, Configurer une nouvelle tentative de demande pour la méthode POST lorsque le serveur principal réinitialise une section de connexion.

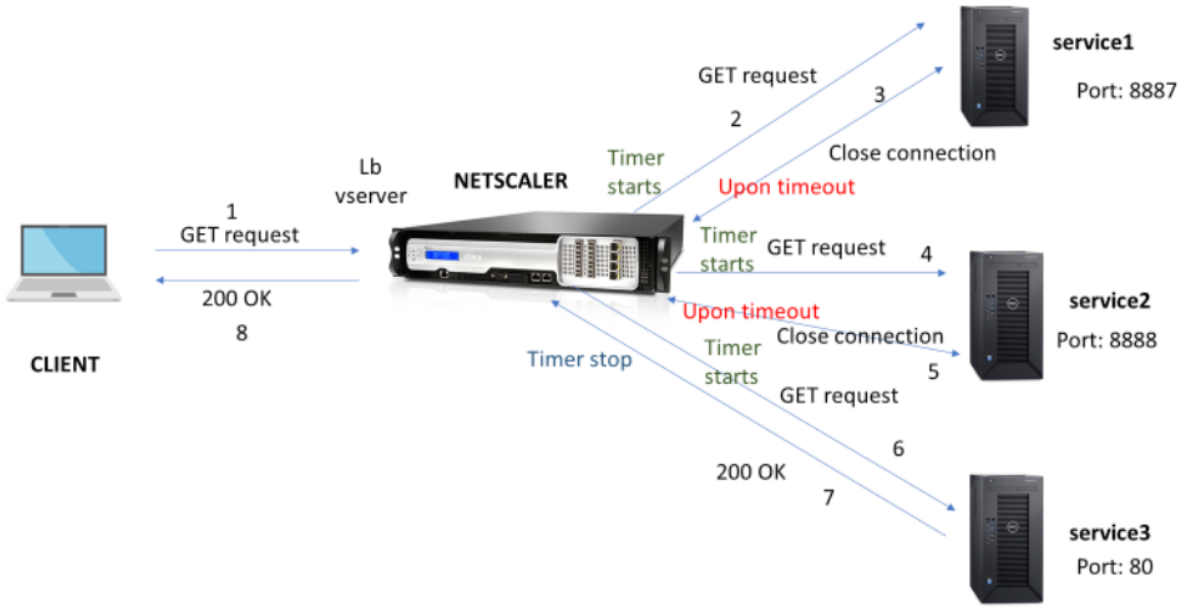
Demander une nouvelle tentative si la réponse du serveur principal arrive à expiration

August 20, 2021

Une nouvelle tentative de demande est disponible pour un autre scénario où, si un serveur principal prend plus de temps pour répondre aux demandes, l'appliance effectue un équilibrage de recharge après expiration et transmet la demande au serveur disponible suivant.

Fonctionnement de la nouvelle tentative de demande lorsque la réponse du serveur principal arrive à expiration

Le diagramme suivant montre les composants interagissent les uns avec les autres :



1. Le processus commence par activer la fonctionnalité appqoe sur votre appliance.

2. La configuration appqoe a le paramètre « retryOnTimeout » en millisecondes.
3. Lorsque l'appliance envoie une demande et si le serveur prend plus de temps pour répondre, l'appliance effectue un équilibrage de recharge en fonction de la valeur de délai d'expiration configurée. L'appliance réinitialise la connexion, choisit un autre service et transmet la requête au lieu d'attendre la réponse du serveur.
4. Une fois que le serveur virtuel d'équilibrage de charge a reçu la réponse, l'appliance transmet la réponse au client. L'utilisation d'un paramètre de délai d'attente empêche l'appliance de continuer à attendre la réponse du serveur, ce qui entraîne une augmentation du RTT.
5. Si le nombre de serveurs principaux disponibles est égal ou inférieur au nombre de tentatives et si tous les serveurs dépassent la demande, l'appliance répondra à une erreur interne de 500 serveurs. Considérez un scénario avec cinq serveurs disponibles et le nombre de tentatives est défini sur six. Si les cinq serveurs sont épuisés pour la demande, l'appliance renvoie une erreur de serveur interne 500 au client.
6. De même, si le nombre de serveurs principaux est supérieur au nombre de nouvelles tentatives et si le serveur principal expédie une demande, l'appliance continue d'attendre le dernier service jusqu'à ce que le serveur envoie une réponse ou que la connexion client ne cesse d'expiration. Considérez un scénario avec trois serveurs back-end et le nombre de tentatives est défini comme deux. Si les trois serveurs sont épuisés à la demande, l'appliance continue d'attendre le troisième service jusqu'à ce que le serveur envoie une réponse ou que la connexion client inactive expédie le délai d'expiration.

Configurer la nouvelle tentative de demande (méthode GET et POST) lorsque la réponse du serveur principal arrive à expiration

Pour configurer une nouvelle tentative de demande pour la méthode GET sur le délai d'expiration, vous devez effectuer les étapes suivantes.

1. Activer appqoe
2. Configurer l'action appqoe
3. Ajouter une stratégie appqoe
4. Lier la stratégie appqoe au serveur virtuel d'équilibrage de charge

> **Remarque :**
>
> La nouvelle tentative de demande au moment du délai d'expiration est également applicable pour la méthode POST.

Activer appqoe

À l'invite de commandes, tapez :

```
enable ns feature appqoe
```


Ajouter une action appqoe pour le délai d'expiration

Vous devez configurer l'action appqoe pour réessayer au délai d'expiration et définir le nombre de tentatives de nouvelle tentative.

À l'invite de commandes, tapez :

```
add appqoe action <name> -retryOnTimeout <msecs> -numRetries <positive_integer
>
```

Exemple :

```
add appqoe action appact1 -retryOnTimeout 35 -numRetries 5
```

Ajouter une stratégie appqoe

Pour implémenter appqoe, vous devez configurer la stratégie appqoe pour définir comment mettre en file d'attente les connexions.

À l'invite de commandes, tapez :

```
add appqoe policy <name> -rule <rule> -action <name>
```

Exemple :

```
add appqoe policy timeout_policy -rule http.req.method.eq(get)-action
appact1
```

Lier la stratégie appqoe au serveur virtuel d'équilibrage de charge

Lorsqu'un serveur principal prend beaucoup de temps à répondre et si vous souhaitez que le serveur virtuel d'équilibrage de charge transmette la demande au service disponible suivant, vous devez lier la stratégie appqoe au serveur virtuel d'équilibrage.

À l'invite de commandes, tapez :

```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Exemple :

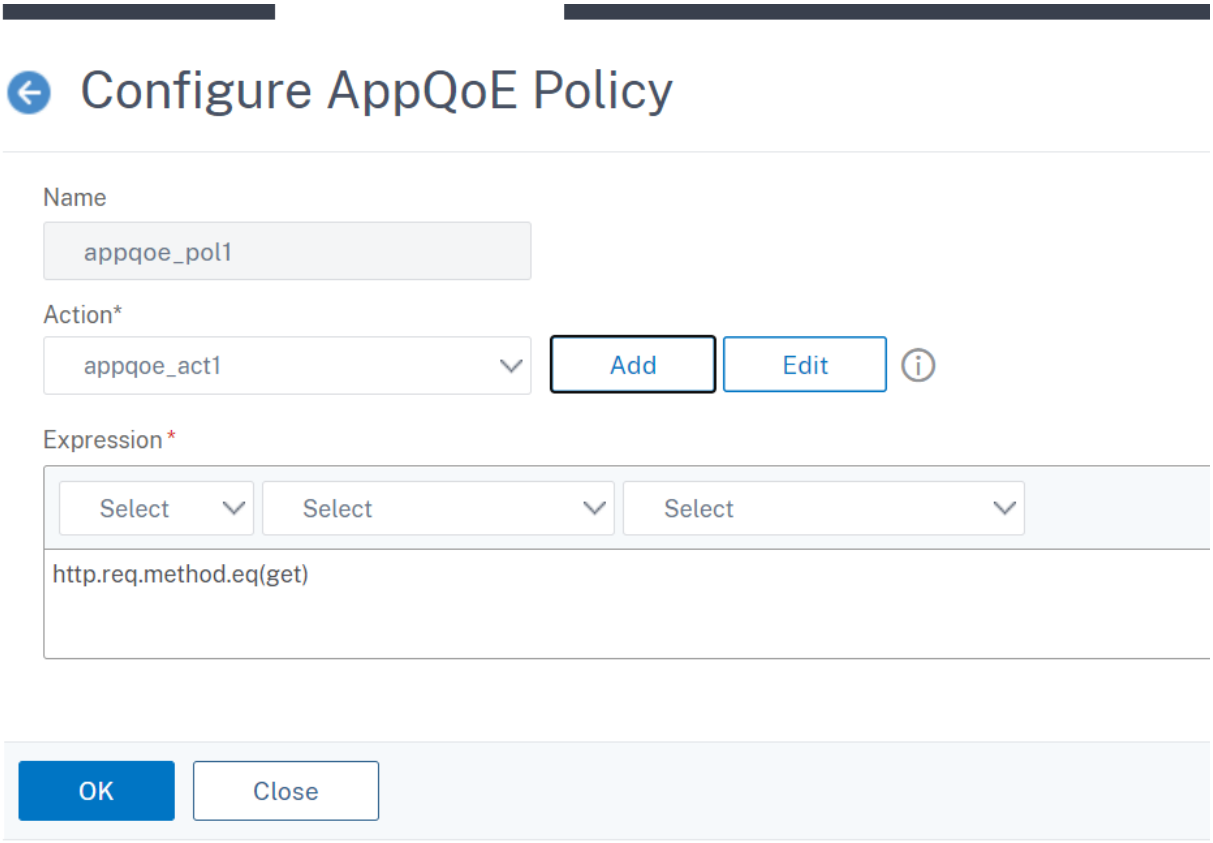
```
bind lb vserver v1 -policyName timeout_policy -type REQUEST -priority 1
```

Configurer la stratégie AppQoE pour la rééquilibrage de charge sur le délai d'expiration à l'aide de l'interface graphique Citrix ADC

1. Accédez à **AppExpert > AppQoE > Stratégies**.

2. Dans la page **Stratégies AppQoE**, cliquez sur **Ajouter**.
3. Dans la page **Créer une stratégie AppQoE**, définissez les paramètres suivants :

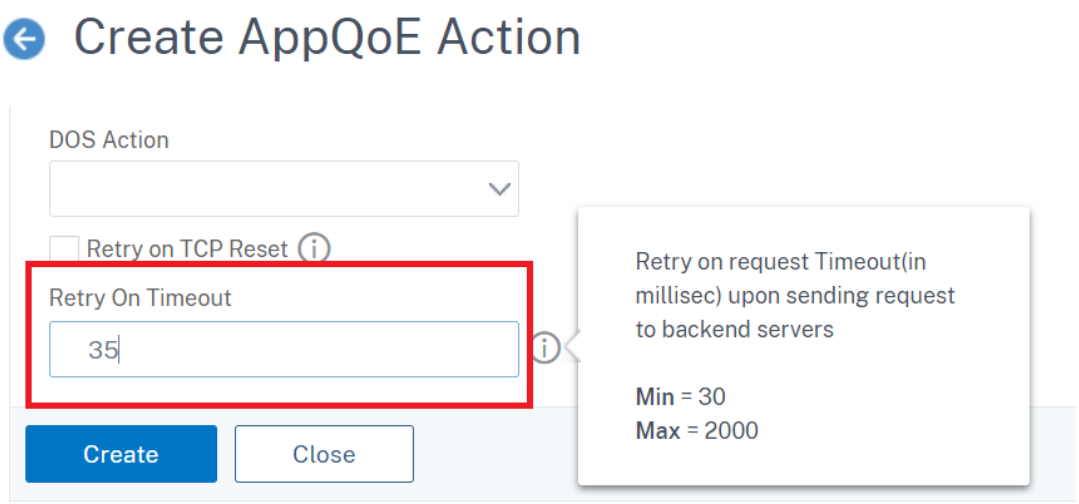
   a. Nom. AppQoE policy name
   b. Action. Ajoutez ou modifiez une action. Pour créer une action, reportez-vous à la section Créer une action AppQoE.
   c. Expression. Sélectionnez ou entrez l'expression de stratégie « http.req.method.eq (get) ».
4. Cliquez sur **Créer** et **Fermer**.



Configurer l'action AppQoE pour une nouvelle tentative de demande à l'aide de l'interface graphique Citrix ADC

1. Accédez à **AppExpert > AppQoE > Action**.
2. Dans la page **AppQoE Actions**, cliquez sur **Ajouter**.
3. Dans la page **Créer une action AppQoE**, définissez le paramètre suivant pour réessayer sur le délai de réponse du serveur principal :

   a. Réessayez sur le délai d'expiration. Réessayez le délai d'expiration de la demande (en millisec) lors de l'envoi de la demande aux serveurs principaux.
4. Cliquez sur **Créer** et **Fermer**.



Optimisation TCP

August 20, 2021

TCP utilise les techniques d'optimisation et les stratégies (ou algorithmes) de contrôle de la congestion suivantes pour éviter la congestion du réseau dans la transmission des données.

Stratégies de lutte contre la congestion

Le TCP a longtemps été utilisé pour établir et gérer les connexions Internet, gérer les erreurs de transmission et connecter facilement les applications Web aux périphériques clients. Mais le trafic réseau est devenu plus difficile à contrôler, car la perte de paquets ne dépend pas seulement de la congestion dans le réseau, et la congestion ne provoque pas nécessairement la perte de paquets. Par conséquent, pour mesurer la congestion, un algorithme TCP doit se concentrer à la fois sur la perte de paquets et la bande passante.

Algorithme PRR (Proportional Rate Recovery)

Les mécanismes TCP Fast Recovery réduisent la latence web causée par les pertes de paquets. Le nouvel algorithme PRR (Proportional Rate Recovery) est un algorithme de récupération rapide qui évalue les données TCP lors d'une récupération de perte. Il est modelé après la réduction de la moitié de la vitesse, en utilisant la fraction appropriée à la fenêtre cible choisie par l'algorithme de contrôle de la congestion. Il minimise le réglage de la fenêtre, et la taille réelle de la fenêtre à la fin de la récupération est proche du seuil de démarrage lent (ssthresh).

TCP Ouverture rapide (TFO)

TCP Fast Open (TFO) est un mécanisme TCP qui permet un échange de données rapide et sûr entre un client et un serveur pendant la prise de main initiale de TCP. Cette fonctionnalité est disponible en tant qu'option TCP dans le profil TCP lié à un serveur virtuel d'une appliance Citrix ADC. TFO utilise un cookie TCP Fast Open (un cookie de sécurité) que l'appliance Citrix ADC génère pour valider et authentifier le client initiant une connexion TFO au serveur virtuel. En utilisant ce mécanisme TFO, vous pouvez réduire la latence réseau d'une application du temps nécessaire pour un aller-retour complet, ce qui réduit considérablement le retard subi dans les transferts TCP courts.

Fonctionnement de TFO

Lorsqu'un client tente d'établir une connexion TFO, il inclut un cookie TCP Fast Open avec le segment SYN initial pour s'authentifier. Si l'authentification réussit, le serveur virtuel de l'appliance Citrix ADC peut inclure des données dans le segment SYN-ACK même s'il n'a pas reçu le segment ACK final de la poignée de main à trois voies. Cela permet d'économiser jusqu'à un aller-retour complet par rapport à une connexion TCP normale, ce qui nécessite une poignée de main à trois voies avant d'échanger des données.

Un client et un serveur back-end effectuent les étapes suivantes pour établir une connexion TFO et échanger des données en toute sécurité lors de la connexion TCP initiale.

1. Si le client ne dispose pas d'un cookie TCP Fast Open pour s'authentifier, il envoie une demande Fast Open Cookie dans le paquet SYN au serveur virtuel sur l'appliance Citrix ADC.
2. Si l'option TFO est activée dans le profil TCP lié au serveur virtuel, l'appliance génère un cookie (en chiffrant l'adresse IP du client sous une clé secrète) et répond au client avec un SYN-ACK qui inclut le cookie ouvert rapide généré dans un champ d'option TCP.
3. Le client met en cache le cookie pour les futures connexions TFO au même serveur virtuel sur l'appliance.
4. Lorsque le client tente d'établir une connexion TFO au même serveur virtuel, il envoie SYN qui inclut le cookie d'ouverture rapide mis en cache (en tant qu'option TCP) ainsi que des données HTTP.
5. L'appliance Citrix ADC valide le cookie et, si l'authentification réussit, le serveur accepte les données du paquet SYN et accuse réception de l'événement avec un SYN-ACK, un cookie TFO et une réponse HTTP.

> **Remarque :**
>
> Si l'authentification du client échoue, le serveur supprime les données et accuse réception de l'événement uniquement avec un SYN indiquant un délai d'expiration de session.

1. Côté serveur, si l'option TFO est activée dans un profil TCP lié à un service, l'appliance Citrix ADC détermine si le cookie TCP Fast Open est présent dans le service auquel il tente de se connecter.

2. Si le cookie TCP Fast Open n'est pas présent, l'appliance envoie une demande de cookie dans le paquet SYN.
3. Lorsque le serveur principal envoie le cookie, l'appliance stocke le cookie dans le cache d'informations du serveur.
4. Si l'appliance dispose déjà d'un cookie pour la paire IP de destination donnée, il remplace l'ancien cookie par le nouveau.
5. Si le cookie est disponible dans le cache d'informations du serveur lorsque le serveur virtuel tente de se reconnecter au même serveur principal à l'aide de la même adresse SNIP, l'appliance combine les données du paquet SYN avec le cookie et les envoie au serveur principal.
6. Le serveur principal reconnaît l'événement avec des données et un SYN.

Remarque : si le serveur reconnaît l'événement avec uniquement un segment SYN, l'appliance Citrix ADC renoue immédiatement le paquet de données après avoir supprimé le segment SYN et les options TCP du paquet d'origine.

Configuration de TCP fast open

Pour utiliser la fonction TCP Fast Open (TFO), activez l'option TCP Fast Open dans le profil TCP approprié et définissez le paramètre TFO Cookie Timeout sur une valeur correspondant aux exigences de sécurité de ce profil.

Activer ou désactiver TFO à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver TFO dans un profil nouveau ou existant.

Remarque : La valeur par défaut est DISABLED.

```
1     add tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
2     set tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
3     unset tcpprofile <TCP Profile Name> - tcpFastOpen
4     Examples
5     add tcpprofile Profile1 - tcpFastOpen
6     Set tcpprofile Profile1 - tcpFastOpen Enabled
7     unset tcpprofile Profile1 - tcpFastOpen
8 <!--NeedCopy-->
```

Pour définir la valeur du délai d'expiration du cookie TCP Fast Open à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
    set tcpparam - tcpfastOpenCookieTimeout <Timeout Value>
    Example
    set tcpprofile - tcpfastOpenCookieTimeout 30secs
<!--NeedCopy-->
```

Pour configurer le TCP Fast Open à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Profils**, puis cliquez sur **Modifier** pour modifier un profil TCP.
2. Dans la page **Configurer le profil TCP**, activez la case à cocher **TCP Fast Open**.
3. Cliquez sur **OK**, puis sur **Terminé**.

Pour configurer la valeur de délai d'expiration TCP Fast Cookie à l'aide de l'interface graphique

Accédez à **Configuration** > **Système** > **Paramètres** > **Modifier les paramètres TCP**, puis la page **Configurer les paramètres TCP** pour définir la valeur de délai d'expiration du cookie TCP Fast Open.

TCP HyStart

Un nouveau paramètre de profil TCP, HyStart, active l'algorithme HyStart, qui est un algorithme de démarrage lent qui détermine dynamiquement un point sûr auquel se terminer (ssthresh). Il permet une transition vers l'évitement de la congestion sans lourdes pertes de paquets. Ce nouveau paramètre est désactivé par défaut.

Si la congestion est détectée, HyStart entre dans une phase d'évitement de la congestion. En l'activant, vous obtenez un meilleur débit dans les réseaux à grande vitesse avec une forte perte de paquets. Cet algorithme permet de maintenir une bande passante proche du maximum lors du traitement des transactions. Il peut donc améliorer le débit.

Configuration de TCP HyStart

Pour utiliser la fonction HyStart, activez l'option Cubic HyStart dans le profil TCP correspondant.

Pour configurer HyStart à l'aide de l'interface de ligne de commande (CLI)

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver HyStart dans un profil TCP nouveau ou existant.

```
add tcpprofile <profileName> -hystart ENABLED
set tcpprofile <profileName> -hystart ENABLED
unset tcprofile <profileName> -hystart
```



```
<!--NeedCopy-->
```

Exemples :

```
    add tcpprofile profile1 -hystart ENABLED
    set tcpprofile profile1 -hystart ENABLED
    unset tcprofile profile1 -hystart
<!--NeedCopy-->
```

Pour configurer la prise en charge HyStart à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Profils** > et cliquez sur **Modifier** pour modifier un profil TCP.
2. Sur la page **Configurer le profil TCP**, activez la case à cocher **Hystart cubique**.
3. Cliquez sur **OK**, puis sur **Terminé**.

Contrôle du taux de rafale TCP

On observe que les mécanismes de contrôle TCP peuvent entraîner un flux de trafic bourré sur les réseaux mobiles à grande vitesse avec un impact négatif sur l'efficacité globale du réseau. En raison des conditions du réseau mobile telles que la congestion ou la retransmission de données de couche 2, les accusés de réception TCP arrivent à l'expéditeur, ce qui déclenche une explosion de transmission. Ces groupes de paquets consécutifs envoyés avec un court intervalle inter-paquets, il est appelé TCP paquet rafale. Pour surmonter l'éclatement du trafic, l'appliance Citrix ADC utilise une technique de contrôle du taux d'éclatement TCP. Cette technique permet d'espacer uniformément les données dans le réseau pendant toute une période d'aller-retour afin que les données ne soient pas envoyées en rafale. En utilisant cette technique de contrôle du taux d'éclatement, vous pouvez obtenir un meilleur débit et des taux de largage de paquets plus bas.

Fonctionnement du contrôle de taux d'éclatement TCP

Dans une appliance Citrix ADC, cette technique répartit uniformément la transmission d'un paquet sur toute la durée du temps de rotation (RTT). Ceci est réalisé en utilisant une pile TCP et un planificateur de paquets réseau qui identifie les différentes conditions réseau pour sortir les paquets pour les sessions TCP en cours afin de réduire les rafales.

À l'expéditeur, au lieu de transmettre des paquets immédiatement après réception d'un accusé de réception, l'expéditeur peut retarder la transmission des paquets pour les étaler à la vitesse définie par le planificateur (configuration dynamique) ou par le profil TCP (configuration fixe).

Configuration du contrôle du taux de rafale TCP

Pour utiliser l'option Contrôle de taux d'éclatement TCP dans le profil TCP approprié et définir les paramètres de contrôle de taux d'éclatement.

Pour définir le contrôle du taux de rafale TCP à l'aide de la ligne de commande

À l'invite de commandes, définissez l'une des commandes de contrôle de taux d'éclatement TCP suivantes sont configurées dans un profil nouveau ou existant.

Remarque : La valeur par défaut est DISABLED.

```
add tcpprofile <TCP Profile Name> -burstRateControl Disabled | Dynamic
    | Fixed

set tcpprofile <TCP Profile Name> -burstRateControl Disabled | Dynamic
    | Fixed

unset tcpprofile <TCP Profile Name> -burstRateControl Disabled |
    Dynamic | Fixed
<!--NeedCopy-->
```

Où,

Désactivé : si le contrôle de taux d'éclatement est désactivé, un appliance Citrix ADC n'effectue pas de gestion de rafale autre que le paramètre MaxBurst.

Corrigé — Si le contrôle de taux d'éclatement TCP est fixe, l'appliance utilise la valeur Taux d'envoi de charge utile de connexion TCP mentionnée dans le profil TCP.

Dynamique : si le contrôle de taux d'éclatement est « dynamique », la connexion est réglementée en fonction de diverses conditions réseau afin de réduire les éclats TCP. Ce mode fonctionne uniquement lorsque la connexion TCP est en mode ENDPOINT. Lorsque le contrôle Taux d'éclatement dynamique est activé, le paramètre MaxBurst du profil TCP n'est pas en vigueur.

```
add tcpProfile  profile1 -burstRateControl Disabled

set tcpProfile profile1 -burstRateControl Dynamic

unset tcpProfile profile1 -burstRateControl Fixed
<!--NeedCopy-->
```

Pour définir les paramètres TCP Rate Control à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
set ns tcpprofile nstcp_default_profile -burstRateControl <type of burst rate control> -tcprate <TCP rate> -rateqmax <maximum bytes in queue>

T1300-10-2> show ns tcpprofile nstcp_default_profile
        Name: nstcp_default_profile
        Window Scaling status:  ENABLED
        Window Scaling factor: 8
        SACK status: ENABLED
        MSS: 1460
        MaxBurst setting: 30 MSS
        Initial cwnd setting: 16 MSS
        TCP Delayed-ACK Timer: 100 millisec
        Nagle's Algorithm: DISABLED
        Maximum out-of-order packets to queue: 15000
        Immediate ACK on PUSH packet: ENABLED
        Maximum packets per MSS: 0
        Maximum packets per retransmission: 1
        TCP minimum RTO in millisec: 1000
        TCP Slow start increment: 1
        TCP Buffer Size: 8000000 bytes
        TCP Send Buffer Size: 8000000 bytes
        TCP Syncookie: ENABLED
        Update Last activity on KA Probes: ENABLED
        TCP flavor: BIC
        TCP Dynamic Receive Buffering: DISABLED
        Keep-alive probes: ENABLED
        Connection idle time before starting keep-alive probes: 900 seconds
        Keep-alive probe interval: 75 seconds
        Maximum keep-alive probes to be missed before dropping connection: 3
        Establishing Client Connection: AUTOMATIC
        TCP Segmentation Offload: AUTOMATIC
        TCP Timestamp Option: DISABLED
        RST window attenuation (spoof protection): ENABLED
        Accept RST with last acknowledged sequence number: ENABLED
        SYN spoof protection: ENABLED
        TCP Explicit Congestion Notification: DISABLED
        Multipath TCP: DISABLED
        Multipath TCP drop data on pre-established subflow: DISABLED
        Multipath TCP fastopen: DISABLED
        Multipath TCP session timeout: 0 seconds
```



```
40              DSACK: ENABLED
41              ACK Aggregation: DISABLED
42              FRTO: ENABLED
43              TCP Max CWND : 4000000 bytes
44              FACK: ENABLED
45              TCP Optimization mode: ENDPOINT
46              TCP Fastopen: DISABLED
47              HYSTART: DISABLED
48              TCP dupack threshold: 3
49              Burst Rate Control: Dynamic
50              TCP Rate: 0
51              TCP Rate Maximum Queue: 0
52  <!--NeedCopy-->
```

Pour configurer le contrôle de taux d'éclatement TCP à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Profils**, puis cliquez sur **Modifier** pour modifier un profil TCP.
2. Sur la page **Configurer le profil TCP**, sélectionnez l'option **Contrôle de rafale TCP** dans la liste déroulante :
   a) BurstRateCntrl
   b) CreditBytePrms
   c) RateBytePerms
   d) RateSchedulerQ
3. Cliquez sur **OK**, puis sur **Terminé**.

Algorithme de protection contre la séquence enveloppée (PAWS)

Si vous activez l'option d'horodatage TCP dans le profil TCP par défaut, l'appliance Citrix ADC utilise l'algorithme Protection Against Wrapped Sequence (PAWS) pour identifier et rejeter les anciens paquets dont les numéros de séquence se trouvent dans la fenêtre de réception de la connexion TCP actuelle car la séquence a « enveloppé » (atteint sa valeur maximale et redémarre à partir de 0).

Si la congestion réseau retarde un paquet de données non SYN et que vous ouvrez une nouvelle connexion avant l'arrivée du paquet, l'encapsulage de numéros de séquence peut entraîner la nouvelle connexion à accepter le paquet comme valide, entraînant une corruption des données. Mais si l'option d'horodatage TCP est activée, le paquet est ignoré.

Par défaut, l'option d'horodatage TCP est désactivée. Si vous l'activez, l'appliance compare l'horodatage TCP (Seg.tsval) dans l'en-tête d'un paquet à la valeur d'horodatage récent (TS.Recent). Si Seg.tsval est égal ou supérieur à TS.Recent, le paquet est traité. Sinon, l'appliance supprime le paquet et envoie un accusé de réception correctif.

Fonctionnement de PAWS

L'algorithme PAWS traite tous les paquets TCP entrants d'une connexion synchronisée comme suit :

1. Si `SEG.TSval` < `Ts.recent` : Le paquet entrant n'est pas acceptable. PAWS envoie un accusé de réception (tel que spécifié dans RFC-793) et supprime le paquet. Remarque : L'envoi d'un segment ACK est nécessaire pour conserver les mécanismes TCP de détection et de récupération à partir de connexions semi-ouvertes.
2. Si le paquet est en dehors de la fenêtre : PAWS rejette le paquet, comme dans le traitement TCP normal.
3. Si `SEG.TSval` > `Ts.recent` : `PAWS` accepte le paquet et le traite.
4. Si `SEG.TSval` <= `Last.ACK.sent`(segment d'arrivée satisfait) : PAWS doit copier `SEG.TSval` la valeur à `Ts.recent` (est-il copié dans Ts. Champ récent dans la base de données ?.
5. Si le paquet est dans l'ordre : PAWS accepte le paquet.
6. Si le paquet n'est pas dans l'ordre : le paquet est traité comme un segment TCP normal dans la fenêtre et hors séquence. Par exemple, il peut être mis en file d'attente pour une livraison ultérieure.
7. Si la valeur `Ts.recent` est inactive pendant plus de 24 jours : la validité de `Ts.recent` est vérifiée si la vérification de l'horodatage PAWS échoue. Si la valeur TS.Recent n'est pas valide, le segment est accepté et le `PAWS rule` met à jour `Ts.recent` avec la valeur TSval du nouveau segment.

Pour activer ou désactiver l'horodatage TCP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
`set nstcpprofile nstcp_default_profile -TimeStamp (ENABLED | DISABLED)
    `
```

Pour activer ou désactiver l'horodatage TCP à l'aide de l'interface graphique

Accédez à **Système** > **Profil** > **Profil TCP**, sélectionnez le profil TCP par défaut, cliquez sur **Modifier**, puis activez ou désactivez la case à cocher **Horodatage TCP**.

Techniques d'optimisation

TCP utilise les techniques et méthodes d'optimisation suivantes pour des contrôles de flux optimisés.

Sélection de profil TCP basée sur des stratégies

Aujourd'hui, le trafic réseau est plus diversifié et gourmand en bande passante que jamais. Avec l'augmentation du trafic, l'effet de la qualité de service (QoS) sur les performances TCP est significatif.

Pour améliorer la qualité de service, vous pouvez désormais configurer des stratégies AppQoE avec différents profils TCP pour différentes classes de trafic réseau. La stratégie AppQoE classe le trafic d'un serveur virtuel pour associer un profil TCP optimisé pour un type de trafic particulier, tel que 3G, 4G, LAN ou WAN.

Pour utiliser cette fonctionnalité, créez une action de stratégie pour chaque profil TCP, associez une action aux stratégies AppQoE et associez les stratégies aux serveurs virtuels d'équilibrage de charge.

Pour plus d'informations sur l'utilisation des attributs d'abonné pour effectuer l'optimisation TCP, consultez Profil TCP basé surdes règles.

Configuration de la sélection de profils TCP basée sur des stratégies

La configuration de la sélection de profils TCP basée sur des stratégies consiste en les tâches suivantes :

- Activation d'AppQoE. Avant de configurer la fonctionnalité de profil TCP, vous devez activer la fonctionnalité AppQoE.
- Ajout d'une action AppQoE. Après avoir activé la fonctionnalité AppQoE, configurez une action AppQoE avec un profil TCP.
- Configuration de la sélection de profils TCP basée sur AppQoE. Pour implémenter la sélection de profil TCP pour différentes classes de trafic, vous devez configurer des stratégies AppQoE avec lesquelles votre Citrix ADC peut distinguer les connexions et lier l'action AppQoE correcte à chaque stratégie.
- Liaison de la stratégie AppQoE au serveur virtuel. Une fois que vous avez configuré les stratégies AppQoE, vous devez les lier à un ou plusieurs serveurs virtuels d'équilibrage de charge, de commutation de contenu ou de redirection de cache.

Configuration à l'aide de l'interface de ligne de commande

Pour activer AppQoE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer la fonctionnalité et vérifier qu'elle est activée :

- `enable ns feature appqoe`
- `show ns feature`

Pour lier un profil TCP lors de la création d'une action AppQoE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande d'action AppQoE suivante avec l' `tcpprofiletobind` option.


```
add appqoe action <name> [-priority <priority>] [-respondWith ( ACS | NS )
[<CustomFile>] [-altContentSvcName <string>] [-altContentPath <string>] [-
maxConn <positive_integer>] [-delay <usecs>]] [-polqDepth <positive_integer
>] [-priqDepth <positive_integer>] [-dosTrigExpression <expression>] [-
dosAction ( SimpleResponse |HICResponse )] [-tcpprofiletobind <string>]
show appqoe action
```

Pour configurer une stratégie AppQoE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add appqoe policy <name> -rule <expression> -action <string>
```

Pour lier une stratégie AppQoE à des serveurs virtuels d'équilibrage de charge, de redirection de cache ou de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind cs vserver cs1 -policyName <appqoe_policy_name> -priority <priority>
bind lb vserver <name> - policyName <appqoe_policy_name> -priority <priority
>
bind cr vserver <name> -policyName <appqoe_policy_name> -priority <priority
>
```

Exemple

```
1     add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -nagle
         ENABLED -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 500
          -slowStartIncr 1 -bufferSize 4194304 -flavor BIC -KA ENABLED -
         sendBuffsize 4194304 -rstWindowAttenuate ENABLED -spoofSynDrop
         ENABLED -dsack enabled -frto ENABLED -maxcwnd 4000000 -fack
         ENABLED -tcpmode ENDPOINT
2     add appqoe action appact1 -priority HIGH -tcpprofile tcp1
3     add appqoe policy apppol1 -rule "client.ip.src.eq(10.102.71.31)" -
         action appact1
4     bind lb vserver lb2 -policyName apppol1 -priority 1 -
         gotoPriorityExpression END -type REQUEST
5     bind cs vserver cs1 -policyName apppol1 -priority 1 -
         gotoPriorityExpression END -type REQUEST
6  <!--NeedCopy-->
```


Configuration du profilage TCP basé sur des stratégies à l'aide de l'interface graphique

Pour activer AppQoE à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans le volet d'informations, cliquez sur **Configurer les fonctionnalités avancées**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, activez la case à cocher **AppQoE** .
4. Cliquez sur **OK**.

Pour configurer la stratégie AppQoE à l'aide de l'interface graphique

1. Accédez à **App-Expert** > **AppQoE** > **Actions** .
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
3. Pour créer une action, cliquez sur **Ajouter**.
4. Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Modifier**.
5. Dans l'écran **Créer une action AppQoE** ou **Configurer une action AppQoE**, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres pour configurer l'action AppQoE » comme suit (un astérisque indique un paramètre requis) :
   a) Name—name
   b) Type d'action—respondWith
   c) Priorité—priority
   d) Profondeur de la file d'attente des stratégies—polqDepth
   e) Profondeur de file d'attente—priqDepth
   f) Action DOS—dosAction
6. Cliquez sur **Créer**.

Pour lier la stratégie AppQoE à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez un serveur, puis cliquez sur **Modifier**.
2. Dans la section **Stratégies** et cliquez sur (+) pour lier une stratégie AppQoE.
3. Dans le curseur **Stratégies**, procédez comme suit :
   a) Sélectionnez un type de stratégie comme AppQoE dans la liste déroulante.
   b) Sélectionnez un type de trafic dans la liste déroulante.
4. Dans la section **Liaison de la stratégie**, procédez comme suit :
   a) Cliquez sur **Nouveau** pour créer une stratégie AppQoE.
   b) Cliquez sur **Stratégie existante** pour sélectionner une stratégie AppQoE dans la liste déroulante.
5. Définissez la priorité de liaison et cliquez sur **Lier** à la stratégie au serveur virtuel.

6. Cliquez sur **Terminé**.

Génération de blocs SACK

Les performances TCP ralentissent lorsque plusieurs paquets sont perdus dans une fenêtre de données. Dans un tel scénario, un mécanisme de reconnaissance sélective (SACK) combiné à une politique sélective de retransmission répétée surmonte cette limite. Pour chaque paquet entrant en rupture de commande, vous devez générer un bloc SACK.

Si le paquet hors commande s'insère dans le bloc de file d'attente de réassemblage, insérez les informations de paquet dans le bloc et définissez les informations de bloc complètes comme SACK-0. Si un paquet hors ordre ne rentre pas dans le bloc de réassemblage, envoyez le paquet sous la forme SACK-0 et répétez les blocs SACK antérieurs. Si un paquet hors commande est un doublon et que les informations de paquet sont définies comme SACK-0 alors D-SACK le bloc.

Note : Un paquet est considéré comme D-SACK s'il s'agit d'un paquet accusé de réception, ou d'un paquet hors commande qui est déjà reçu.

Le client renié

Une appliance Citrix ADC peut gérer la révocation du client lors de la restauration basée sur SACK.

Les vérifications de mémoire pour marquer end_point sur PCB ne prennent pas en compte la mémoire disponible totale

Dans une appliance Citrix ADC, si le seuil d'utilisation de la mémoire est défini sur 75 % au lieu d'utiliser la mémoire totale disponible, les nouvelles connexions TCP contournent l'optimisation TCP.

Retransmissions inutiles en raison de blocs SACK manquants

En mode non-point de terminaison, lorsque vous envoyez des DUPACKS, si des blocs SACK sont manquants pour quelques paquets hors ordre, déclenche davantage de retransmissions à partir du serveur.

SNMP pour les connexions contourné l'optimisation en raison de la surcharge

Les ID SNMP suivants ont été ajoutés à une appliance Citrix ADC pour suivre le nombre de connexions contournées optimisations TCP en raison d'une surcharge.

1. 1.3.6.1.4.1.5951.4.1.1.46.131 (TCPopTimizationEnabled). Pour suivre le nombre total de connexions activées avec l'optimisation TCP.

2. 1.3.6.1.4.1.5951.4.1.1.46.132 (TCPopTimizationBypassed). Pour suivre le nombre total de connexions contournées l'optimisation TCP.

Mémoire tampon de réception dynamique

Pour optimiser les performances TCP, une appliance Citrix ADC peut désormais ajuster dynamiquement la taille du tampon de réception TCP.

Algorithme de sonde de perte de queue

Un délai d'attente de retransmission (RTO) est une perte de segments à la fin d'une transaction. Un RTO se produit en cas de problèmes de latence d'application, en particulier dans les transactions Web courtes. Pour récupérer la perte de segments à la fin d'une transaction, TCP utilise l'algorithme TLP (Tail Loss Probe).
TLP est un algorithme d'expéditeur uniquement. Si une connexion TCP ne reçoit aucun accusé de réception pendant une certaine période, TLP transmet le dernier paquet non accusé de réception (sonde de perte). Dans le cas d'une perte de queue lors de la transmission d'origine, l'accusé de réception de la sonde de perte déclenche une récupération SACK ou FACK.

Configuration de la sonde de perte de queue

Pour utiliser l'algorithme Tail Loss Probe (TLP), vous devez activer l'option TLP dans le profil TCP et définir le paramètre sur une valeur correspondant aux exigences de sécurité de ce profil.

Activer TLP à l'aide de la ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver TLP dans un profil nouveau ou existant.

> **Remarque** :
>
> La valeur par défaut est DISABLED.

```
add tcpprofile <TCP Profile Name> - taillossprobe ENABLED | DISABLED

set tcpprofile <TCP Profile Name> - taillossprobe ENABLED | DISABLED

unset tcpprofile <TCP Profile Name> - taillossprobe
```

Exemples :

```
add tcpprofile nstcp_default_profile - taillossprobe

set tcpprofile nstcp_default_profile -taillossprobe Enabled

unset tcpprofile nstcp_default_profile -taillossprobe
```


Configurer l'algorithme de sonde de perte de queue à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Configuration** > **Système** > **Profils**, puis cliquez sur **Modifier** pour modifier un profil TCP.
2. Sur la page **Configurer le profil TCP**, activez la case à cocher **Sonde de perte de queue**.
3. Cliquez sur **OK**, puis sur **Terminé**.

Solutions de dépannage pour Citrix ADC

January 21, 2021

Cette rubrique présente les solutions de dépannage de base nécessaires pour résoudre les problèmes qui se produisent dans votre appliance. Il vous donne une compréhension de l'appliance NetScaler, de la manière dont elle s'intègre au réseau et des problèmes auxquels vous pouvez vous attendre dans les fonctionnalités système de base.

Comment enregistrer une trace de paquets sur Citrix ADC

August 20, 2021

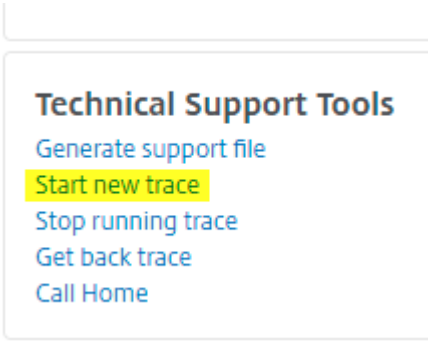
Cet article de dépannage explique comment un administrateur peut enregistrer une trace de paquets réseau à l'aide de l'interface graphique Citrix ADC.

Points à retenir

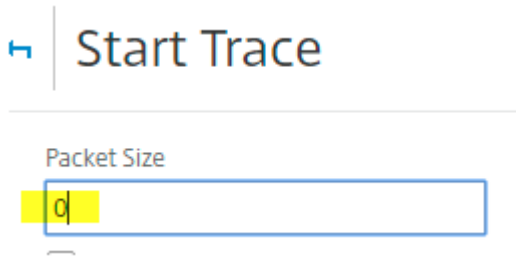
- Citrix vous recommande d'utiliser la version récente de Wireshark à partir de la « section de construction automatisée » disponible dans la page Web suivante : http://www.wireshark.org/download/automated.
- Dans Citrix ADC version 10.5 ou ultérieure, pour déchiffrer la capture et s'assurer que les paramètres ECC (Elliptic Curve Cryptography), la réutilisation de session et les paramètres DH sont désactivés à partir du serveur virtuel. Vous devez le faire avant de capturer une trace.

Enregistrer la trace de paquets sur NetScaler version 11.1

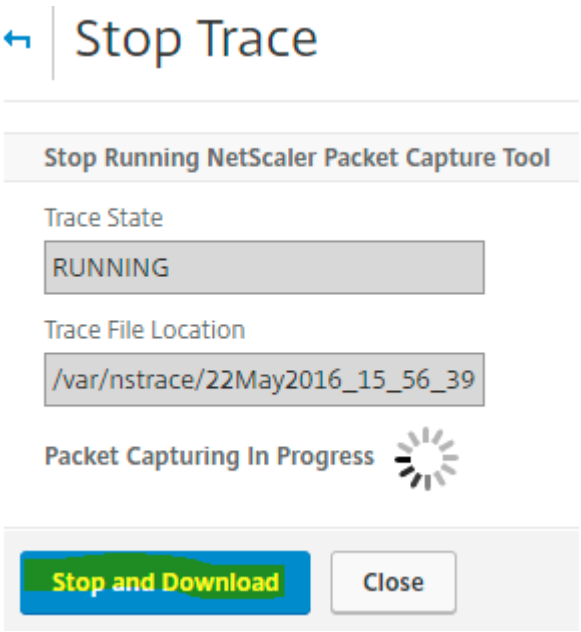
1. Accédez à la page **Système** > **Diagnostics**.
2. cliquez sur le lien **Démarrer une nouvelle trace** dans la page **Diagnostic**, comme indiqué dans la capture d'écran suivante.



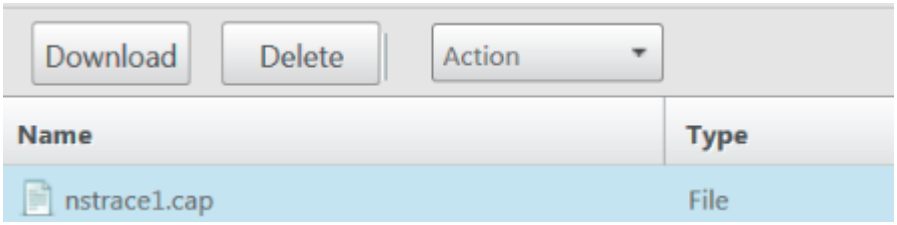
3. Mettez à jour la taille du paquet à 0 dans le champ **Taille du paquet** .



4. Cliquez sur **Démarrer** pour commencer à enregistrer la trace des paquets réseau.
5. Cliquez sur **Arrêter et télécharger** pour arrêter l'enregistrement de la trace des paquets réseau une fois le test terminé.



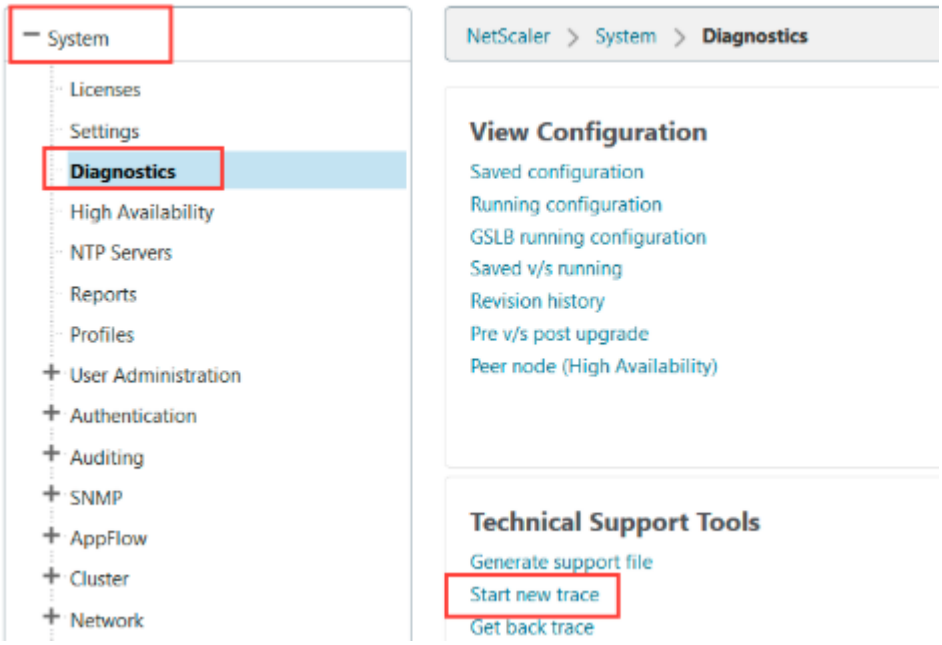
6. Sélectionnez le fichier requis, puis cliquez sur **Sélectionner**, puis sur **Télécharger**.



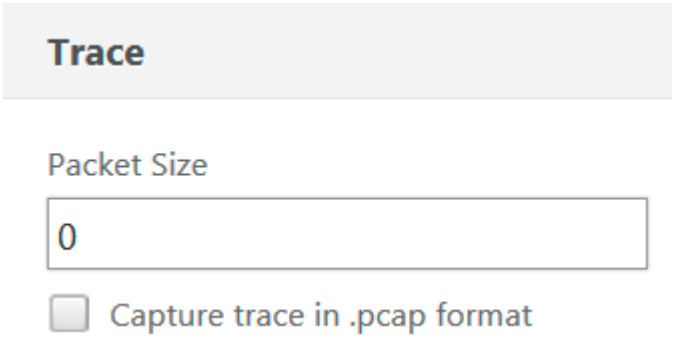
7. Ouvrez le fichier de trace de paquets réseau avec l'utilitaire Wireshark pour afficher le contenu du fichier.

Enregistrer le suivi des paquets sur l'appliance NetScaler 10.5

1. Accédez à la page **Système** > **Diagnostics**.

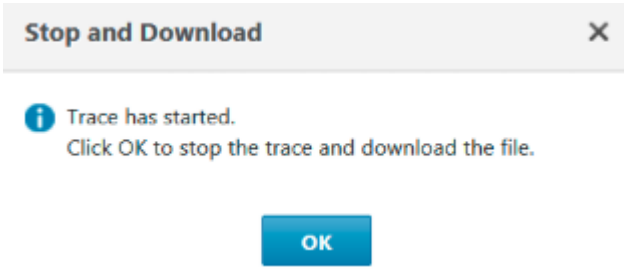


2. Cliquez sur le lien **Démarrer une nouvelle trace** sous **Outils de support technique**, comme illustré dans la capture d'écran suivante.
3. Mettez à jour la taille du paquet à 0 dans le champ **Taille du paquet** .



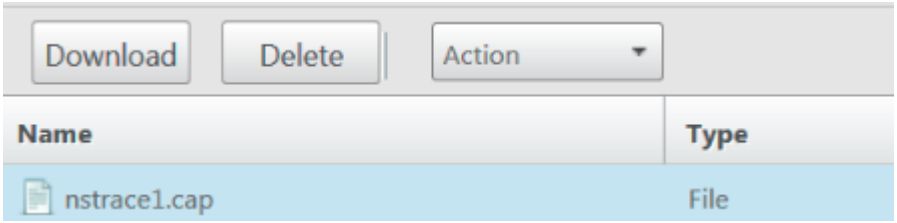
> **Remarque** : si les en-têtes de matériel ne sont pas requis, sélectionnez Capture trace au format .pcap.

4. Cliquez sur **Démarrer** pour commencer à enregistrer la trace des paquets réseau.
5. Cliquez sur **OK** pour arrêter l'enregistrement de la trace des paquets réseau une fois le test terminé.



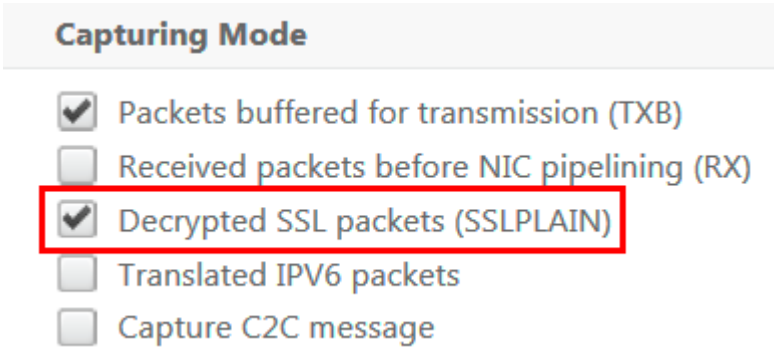
Un fichier nstrace.cap est généré, qui contient la trace des paquets réseau.

6. Mettez en surbrillance le fichier requis et cliquez sur **Télécharger**.



7. Spécifiez une destination et enregistrez la trace des paquets.
8. Ouvrez le fichier de trace de paquets réseau avec l'utilitaire Wireshark pour afficher le contenu du fichier.

> **Remarque** : sélectionnez les paquets SSL déchiffrés (SSLPLAIN) pour déchiffrer la trace des paquets sans la clé privée.



Capture des clés principales SSL

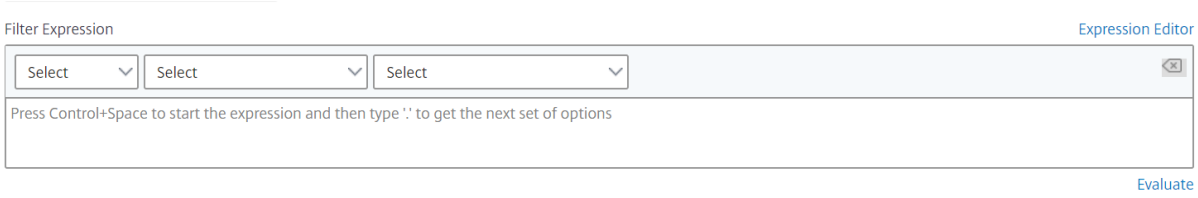
Dans les versions 11.0, 11.1 et supérieures, il existe une option pour capturer les clés de session qui n'est valide que pour cette session/nstrace particulière et cette option peut être utilisée si vous ne voulez pas partager la clé privée ou utiliser le mode SSLPLAIN. Pour plus d'informations, consultez https://support.citrix.com/article/CTX135889.

Exporter les clés de session sans partager la clé privée

Dans la plupart des scénarios, la clé privée n'est pas disponible ou partagée. Dans de tels scénarios, nous pouvons suggérer d'exporter les clés de **session SSL** au lieu de la clé privée. Lire, [Comment exporter et utiliser les clés de session SSL pour déchiffrer les traces SSL sans partager la clé privée SSL, reportez-vous à la section https://support.citrix.com/article/CTX135889.

Filtres

En outre, il est toujours recommandé d'ajouter des filtres basés sur IP tout en prenant des traces. Le processus garantit que vous capturez uniquement le trafic intéressé, ce qui facilite votre dépannage. L'ajout de filtres diminue également la charge sur l'appliance tout en faisant des traces.



Des filtres basés sur IP simples suffisent pour obtenir les bonnes captures. Pour plus d'informations sur `nstrace` les filtres et les exemples, consultez la page Documentation Citrix .

Cas d'utilisation pour capturer une trace de paquets avec un filtre IP du serveur virtuel (à la fois frontal et backend)

En utilisant un filtre de l'adresse IP du serveur virtuel et en activant l'option « —link » dans la CLI ou en sélectionnant l'option « Trace filtered connection peer traffic » dans l'interface graphique (disponible 10.1 et versions ultérieures), vous pouvez capturer à la fois le trafic frontal et back-end pour l'adresse IP.

```
start nstrace -size 0 -filter "CONNECTION.IP.EQ(1.1.1.1)" -link ENABLED

show nstrace
        State:  RUNNING          Scope:  LOCAL            TraceLocation
            :  "/var/nstrace/24Mar2017_16_00_19/..." Nf:  24
```



```
                                Time:  3600              Size:  0
                               Mode:  TXB NEW_RX
5          Traceformat:  NSCAP      PerNIC:  DISABLED        FileName:  24
              Mar2017_16_00_19 Filter:  "CONNECTION.IP.EQ(1.1.1.1)" Link:
               ENABLED           Merge:  ONSTOP           Doruntimecleanup
              :  ENABLED
6          TraceBuffers:  5000      SkipRPC:  DISABLED       Capsslkeys:
              DISABLED    InMemoryTrace:  DISABLED
7  <!--NeedCopy-->
```

Capture des traces cycliques

Il est toujours difficile de résoudre un problème intermittent. Le traçage cyclique est le mieux adapté aux problèmes intermittents. Les traces peuvent être exécutées sur une période de quelques heures ou quelques jours avant que le problème ne se produise. Vous pouvez également utiliser un filtre spécifique et évaluer la taille des fichiers de trace générés avant de l'exécuter plus longtemps.

Exécutez la commande suivante à partir de l'interface de ligne de commande :

```
1  start nstrace -nf 60 -time 30 -size 0
2  This particular trace will create 60 files each of them for 30 sec.
      This means the files will start getting overwritten after 60 trace
      files or 30 mins
3  Show nstrace à To check the status of the nstrace
4  Stop nstrace à To stop the nstrace.
5
6  <!--NeedCopy-->
```

Recommandations

Sur une unité gérant Go de trafic par seconde, la capture du trafic est un processus très gourmand en ressources. L'impact sur les ressources est principalement en termes de CPU et d'espace disque. L'impact sur l'espace disque peut être réduit en utilisant des expressions de filtrage. Toutefois, l'impact sur le processeur reste et provoque parfois une légère augmentation car l'appliance doit désormais traiter les paquets en fonction du filtre avant de les capturer.

Les meilleures pratiques en matière de traçage sont les suivantes :

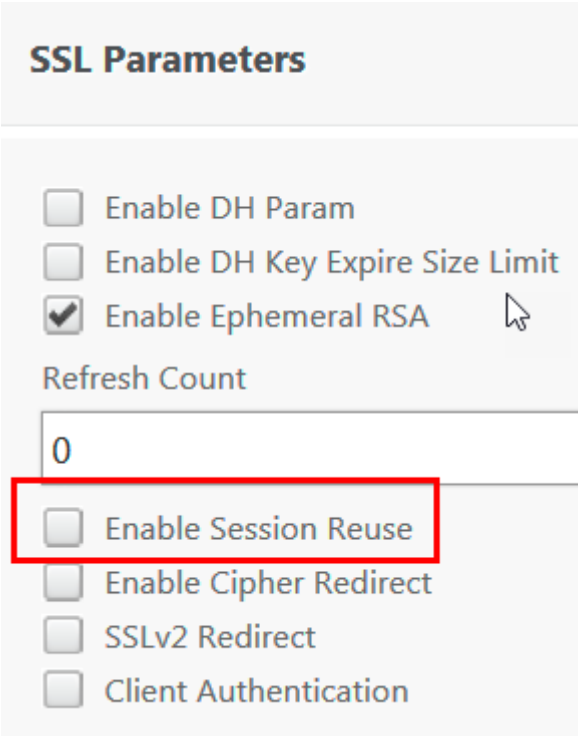
1. La durée d'exécution de la trace doit être aussi limitée que possible lorsque vous vous assurez toujours que les paquets d'intérêt sont capturés.
2. Planifiez l'activité de traçage à un moment où le nombre d'utilisateurs (et donc le trafic) est considérablement réduit, par exemple pendant les heures de repos.

Plus de ressources

Désactiver la réutilisation de session sur le serveur virtuel à partir de l'interface graphique

La réutilisation de session est désactivée lorsque vous capturez une trace pour effectuer une connexion SSL dans la trace. Lorsqu'il est activé, vous pouvez capturer une poignée de main partielle dans la trace. Assurez-vous d'activer l'option après la collection de traces.
Ne désactivez pas une réutilisation de session SSL lorsque la méthode de persistance est sslsession, car elle rompt la persistance des connexions existantes. Pour plus d'informations, reportez-vous à la section https://support.citrix.com/article/CTX121925.

1. Ouvrez le serveur virtuel et accédez aux paramètres SSL.
2. Désactivez Activer la réutilisation de session si cette option est activée.



Désactiver la réutilisation de session sur le serveur virtuel à partir de la CLI

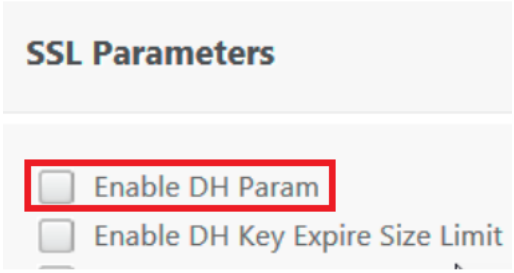
1. SSH à la console de l'appliance.
2. Exécutez la commande suivante pour désactiver DH Param à partir du serveur virtuel :


```
set ssl vserver "vServer_Name"-sessReuse DISABLED
```

Désactiver le paramètre DH sur le serveur virtuel à partir de l'interface graphique

Reportez-vous https://support.citrix.com/article/CTX213335 à la section Pour comprendre le paramètre DH.

1. Ouvrez le serveur virtuel et accédez aux paramètres SSL.
2. Désactivez DH Param si cette option est activée.



Désactiver le paramètre DH sur le serveur virtuel à partir de la CLI

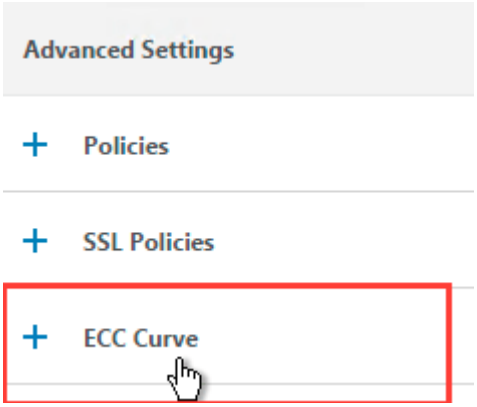
1. SSH à la console de l'appliance.
2. Exécutez la commande suivante pour désactiver DH Param à partir du serveur virtuel :

```
set ssl vserver "vServer_Name"-dh DISABLED
```

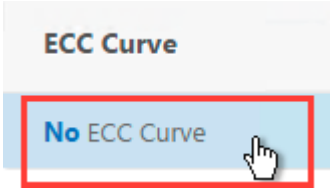
Désactiver la courbe ECC sur le serveur virtuel à partir de l'interface graphique

La courbe ECC est désactivée pour déchiffrer la trace SSL capturée avec une clé privée. Vous ne devez pas désactiver les clés si les chiffrements SSL associés sont utilisés. Pour plus d'informations sur la courbe ECC, voir https://support.citrix.com/article/CTX205289

1. Ouvrez le serveur virtuel et accédez à Courbe ECC.



2. Si aucune courbe ECC n'est liée au serveur virtuel, aucune autre action n'est requise.



3. Si une courbe ECC est liée au serveur virtuel, cliquez sur la courbe ECC et délier le serveur virtuel.

Désactiver la courbe ECC sur le serveur virtuel à partir de la CLI

1. SSH à la console de l'appliance.
2. Exécutez la commande suivante pour chaque courbe ECC liée au serveur virtuel :

```
unbind ssl vserver "vServer_Name"-eccCurveName "ECC_Curve_Name"
```

Comment libérer de l'espace sur le répertoire VAR pour la journalisation des problèmes avec une appliance Citrix ADC

September 8, 2021

L'article suivant explique comment un administrateur peut libérer l'espace du `/var` répertoire d'une appliance Citrix ADC. Vous pouvez suivre les étapes lorsque l'interface graphique Citrix n'est pas accessible.

Lorsque l'espace disque est faible dans le répertoire /var de l'appliance, il est possible que vous ne puissiez pas vous connecter à l'interface graphique Citrix. Dans ce scénario, vous pouvez supprimer les anciens fichiers journaux pour créer de l'espace libre dans le répertoire /var.

Points à retenir

- Veillez à sauvegarder les fichiers avant de les supprimer de l'appliance.

Pour libérer de l'espace dans le `/var` répertoire d'une appliance Citrix ADC, procédez comme suit :

1. Connectez-vous à l'interface de ligne de commande de Citrix ADC à l'aide de SSH. Pour plus d'informations sur la réalisation de cette tâche, consultez la documentation Citrix ADC.
2. Après vous être connecté à l'interface de ligne de commande Citrix ADC, passez à l'invite de l'interpréteur de commandes à l'aide de la commande suivante. `shell`
3. Exécutez la commande suivante pour voir la disponibilité de l'espace sur l'appliance Citrix ADC.
   `df -h`

4. Si la capacité mémoire du `/var` répertoire est remplie jusqu'à 90 %, vous devez supprimer quelques fichiers de ce répertoire.

   - Exécutez les commandes suivantes pour afficher le contenu du répertoire /var :

     ```
     cd /var
     ls -l
     ```

   Les répertoires qui sont généralement d'intérêt sont les suivants :

   ```
   /var/nstrace - This directory contains trace files.This is the most common reason for HDD being filled on the Citrix ADC appliance. This is due to an nstrace being left running for indefinite amount of time. All traces that are not of interest can and should be deleted. To stop an nstrace, go back to the CLI and issue stop nstrace command.

   /var/log - This directory contains system specific log files.

   /var/nslog - This directory contains Citrix ADC log files.

   /var/tmp/support - This directory contains technical support files, also known as, support bundles. All files not of interest should be deleted.

   /var/core - Core dumps are stored in this directory. There will be directories within this directory and they will be labeled with numbers starting with 1. These files can be quite large in size. Clear all files unless the core dumps are recent and investigation is required.

   /var/crash - Crash files, such as process crashes are stored in this directory. Clear all files unless the crashes are recent and investigation is required.

   /var/nsinstall -  Firmware is placed in this directory when upgrading. Clear all files, except the firmware that is currently being used.
   ```

   - Vérifiez si l'un des répertoires utilise plus d'espace :

     ```
     du -hs *
     44k    cache
     2.0k    clusterd
     2.0k    configdb
     6.0k    core
     989M    crash
     ```



```
4.0k    cron
2.0k    dev
6.0k    download
2.0k    gui
2.0k    install
2.0k    krb
2.0k    learnt_data
122M    log
366M    NetScaler
14k    ns_gui
86k    ns_sys_backup
631M    nsinstall
883M    nslog
32k    nsproflog
2.0k    nssynclog
16k    nstemplates
36k    nstmp
4.5G    nstrace
8.1M    opt
6.0k    pubkey
52k    run
28M    safenet
72M    tmp
2.0k   vmtools
14k    vpn
```

- Supprimez les fichiers qui ne sont pas requis :

```
rm -r nstrace/*
```

For more help on deleting files see FreeBSD Man Pages.

  - Delete the files which are not required.
    `rm -r nstrace/*`
    For more help on deleting files see FreeBSD Man Pages.
  - If the log or `nslog` directory is using more space, then run the following commands to open the log directory and view its contents:

```
cd /var/log
ls -l
cd /var/nslog
ls -l
```

1. Assurez-vous que tous les fichiers sont compressés. Cela est indiqué par l'extension de nom de fichier .tar.gz.

2. Si vous utilisez Citrix ADM ou Command Center, vérifiez le répertoire /var/ns_system_backup. Assurez-vous que Citrix ADM ou Command Center efface les fichiers de sauvegarde qu'il crée.

Plus de ressources

Pour plus d'informations sur l'une des commandes mentionnées dans la procédure précédente, voir
- http://ss64.com/bash/

Comment télécharger des fichiers principaux ou plantés à partir de l'appliance Citrix ADC

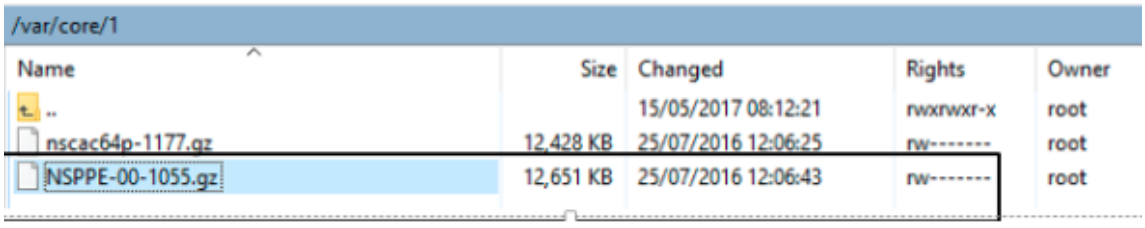
January 21, 2021

Cet article de dépannage explique comment un administrateur peut télécharger des fichiers principaux ou plantés à partir de l'appliance Citrix ADC.

Télécharger des fichiers de base ou de plantage à partir de l'appliance Citrix ADC à l'aide du client SFTP

Pour télécharger les fichiers de base ou de plantage à partir d'une appliance NetScaler, procédez comme suit :

1. Ouvrez WinSCP et connectez-vous à l'adresse IP NetScaler Management.
2. Accédez `/var/core/1` à la pour télécharger les fichiers.



> **Remarque :**
>
> Pour télécharger le dernier plantage ou le fichier principal, vous pouvez également utiliser l'outil WinSCP via l'interface de commande. Les fichiers peuvent être situés soit dans le répertoire noyau, soit dans le répertoire crash.

Comment collecter des statistiques de performances et des journaux d'événements

August 20, 2021

Vous pouvez collecter des statistiques de performances des serveurs virtuels et des services associés à partir d'un fichier newnslog archivé présent dans le répertoire /var/nslog. Les fichiers newnslog sont interprétés en exécutant /netscaler/nsconmsg.

Collecte des statistiques de performances et des journaux d'événements à l'aide de l'interface

Vous pouvez exécuter la commande nsconmsg à partir de l'invite Citrix ADC shell pour signaler les événements.

À l'invite de commandes, tapez :

```
/netscaler/nsconmsg -K /var/nslog/newnslog -d event
```

```
1 Displaying event information
2 NetScaler V20 Performance Data
3 NetScaler NS10.5: Build 57.7.nc, Date: May 14 2015, 07:35:21
4 rtime: Relative time between two records in milliseconds
5 seqno rtime event-message                          event-time
6 11648 16310 PPE-0 MonServiceBinding_10.104.20.110:443_(tcp-default)
7 <!--NeedCopy-->
```

Afficher la durée couverte par un fichier « newnslog » donné

À l'invite de commandes, tapez :

```
/netscaler/nsconmsg -K /var/nslog/newnslog -d setime
```

Les données actuelles sont ajoutées au fichier /var/nslog/newnslog. NetScaler archive automatiquement le fichier newnslog tous les deux jours par défaut. Pour lire les données archivées, vous devez extraire l'archive comme illustré dans l'exemple suivant :

cd /var/nslog - commande pour accéder à un répertoire particulier à partir de l'invite NetScaler Shell.

tar xvfz newnslog.100.tar.gz - commande pour extraire le fichier tar.

/netscaler/nsconmsg -K newnslog.100 -d setime - Commande pour vérifier la durée couverte par le fichier particulier, dans cet exemple newnslog.100.

`ls -l` Commande vérifie tous les fichiers journaux et horodatage associés à ces fichiers.

```
root@NETSCALER## cd /var/nslog
root@NETSCALER## ls -l
```

```
 wheel    461544 Aug  7  2014 newnslog.1.tar.gz
-rw-r--r--   1 root       wheel    191067 Aug  7  2014 newnslog.10.tar.
   gz
-rw-r--r--   1 root       wheel  11144873 Apr 26 22:04 newnslog.100.tar
   .gz
-rw-r--r--   1 root       wheel  11095053 Apr 28 22:04 newnslog.101.tar
   .gz
-rw-r--r--   1 root       wheel  11114284 Apr 30 22:04 newnslog.102.tar
   .gz
-rw-r--r--   1 root       wheel  11146418 May  2 22:04 newnslog.103.tar
   .gz
-rw-r--r--   1 root       wheel  11104227 May  4 22:04 newnslog.104.tar
   .gz
-rw-r--r--   1 root       wheel  11297419 May  6 22:04 newnslog.105.tar
   .gz
-rw-r--r--   1 root       wheel  11081212 May  8 22:04 newnslog.106.tar
   .gz
-rw-r--r--   1 root       wheel  11048542 May 10 22:04 newnslog.107.tar
   .gz
-rw-r--r--   1 root       wheel  11101869 May 12 22:04 newnslog.108.tar
   .gz
-rw-r--r--   1 root       wheel  11378787 May 14 22:04 newnslog.109.tar
   .gz
-rw-r--r--   1 root       wheel  44989298 Apr 11  2014 newnslog.11.gz
<!--NeedCopy-->
```

Afficher l'intervalle de temps dans un fichier

Utilisez la `nsconmsg` commande pour afficher uniquement une période de temps dans le fichier donné, comme illustré dans l'exemple suivant :

```
/netscaler/nsconmsg -K /var/nslog/newnslog -s time=22Mar2007:20:00 -T 7 -s
ConLb=2 -d oldconmsg
```

Où,

`s` - time=22Mar 2007:20:00:00 commence à Mars 22, 2007 à exactement 20:00.

`T 7` - Affiche sept secondes de données

`s` - Affiche le niveau de détail des statistiques d'équilibrage de charge.

`d` - Affiche des informations statistiques.

> **Remarque :**
>
> A partir de la version 12.1 de l'ADC, vous devez ajouter au « temps » secondes aussi, c'est-à-dire : 22Mar 2007:20:00:00

Les informations statistiques fournies par le `-d oldconmsg` paramètre sont enregistrées toutes les sept secondes. Ce qui suit est un exemple de sortie.

```
1  VIP(10.128.58.149:80:UP:WEIGHTEDRR): Hits(38200495, 18/sec) Mbps(1.02)
       Pers(OFF) Err(0)
2  Pkt(186/sec, 610 bytes) actSvc(4) DefPol(NONE) override(0)
3  Conn: Clt(253, 1/sec, OE[252]) Svr(3)
4  S(10.128.49.40:80:UP) Hits(9443063, 4/sec, P[2602342, 0/sec]) ATr(5)
       Mbps(0.23) BWlmt(0 kbits) RspTime(112.58 ms)
5  Other: Pkt(36/sec, 712 bytes) Wt(10000) RHits(31555)
6  Conn: CSvr(42, 0/sec) MCSvr(20) OE(16) RP(11) SQ(0)
7  S(10.128.49.39:80:UP) Hits(9731048, 4/sec, P[2929279, 0/sec]) ATr(9)
       Mbps(0.27) BWlmt(0 kbits) RspTime(161.69 ms)
8  Other: Pkt(41/sec, 756 bytes) Wt(10000) RHits(31555)
9  Conn: CSvr(32, 0/sec) MCSvr(19) OE(13) RP(4) SQ(0)
10 S(10.128.49.38:80:UP) Hits(9341366, 5/sec, P[2700778, 0/sec]) ATr(4)
       Mbps(0.27) BWlmt(0 kbits) RspTime(120.50 ms)
11 Other: Pkt(42/sec, 720 bytes) Wt(10000) RHits(31556)
12 Conn: CSvr(37, 0/sec) MCSvr(19) OE(13) RP(9) SQ(0)
13 S(10.128.49.37:80:UP) Hits(9685018, 4/sec, P[2844418, 0/sec]) ATr(3)
       Mbps(0.23) BWlmt(0 kbits) RspTime(125.38 ms)
14 Other: Pkt(38/sec, 670 bytes) Wt(10000) RHits(31556)
15 Conn: CSvr(32, 0/sec) MCSvr(20) OE(10) RP(7) SQ(0)
16 <!--NeedCopy-->
```

> **Remarque :**
>
> Le nombre de connexions client des services individuels ne s'additionne pas au nombre de connexions client du serveur virtuel. La raison est due à la réutilisation de la session entre l'appliance Citrix ADC et le service back-end.

Sortie du serveur virtuel

`VIP(10.128.58.149:80:UP:WEIGHTEDRR): Hits(38200495, 18/sec)Mbps(1.02)Pers(OFF)Err(0)Pkt(186/sec, 610 bytes)actSvc(4)DefPol(NONE)override(0)Conn: Clt(253, 1/sec, OE[252])Svr(3)`

La liste suivante décrit les statistiques du serveur virtuel :

1. IP (IP address:port:state:Load balancing method). L'adresse IP et le port de l'adresse IP virtuelle tels que configurés. L'état du serveur virtuel ou l'adresse IP virtuelle est UP, DOWN ou OUT OF SERVICE ; Méthode d'équilibrage de charge configurée pour l'adresse IP virtuelle.
2. Hits (##). Nombre de demandes qui ont atteint le serveur virtuel.
3. Mbps (##). Volume total du trafic sur le serveur virtuel (Rx + Tx) converti en Mbits/s
4. Pers : type de persistance configuré.
5. Err (##). Nombre de fois qu'une page d'erreur a été générée par le serveur virtuel.
6. Pkt (##/sec, ## bytes) : volume de trafic réseau (sous forme de paquets) passant par le serveur virtuel et taille moyenne des paquets circulant à travers le serveur virtuel.
7. actSvc(##). Nombre de services actifs liés au serveur virtuel.
8. DefPol (RR). Indique si la méthode d'équilibrage de charge par défaut est active. La méthode d'équilibrage de charge par défaut est utilisée pour un certain nombre de demandes initiales pour lisser le comportement des autres méthodes.
9. Clt (##, ##/sec). Nombre de connexions clientes actuelles au taux de serveur virtuel.
10. OE [##]. Nombre de connexions de serveur à partir du serveur virtuel en état ouvert établi.
11. Svr (##). Nombre de connexions au serveur en cours à partir du serveur virtuel.

Dans la sortie précédente, Svr(3) indique que la commande collecte l'échantillon statistique. Il existe trois connexions actives pour le serveur virtuel au serveur principal, même s'il existe quatre services au total. Lorsqu'un client établit une connexion avec le serveur virtuel, il n'est pas nécessaire que le client envoie ou reçoit du trafic lorsque la commande collecte les informations. Par conséquent, il est courant de voir le Svr compteur inférieur au OE[] nombre. Le Svr compteur représente le nombre de connexions actives qui envoient ou reçoivent activement des données. L'adresse IP mappée (MIP) ou l'adresse IP de sous-réseau (SNIP) est connectée au serveur principal associé. De plus, Citrix ADC suit le serveur virtuel connecté au serveur principal et calcule le compteur.

Sortie du service virtuel

```
1 S(10.128.49.40:80:UP) Hits(9443063, 4/sec, P[2602342, 0/sec]) ATr(5)
     Mbps(0.23) BWlmt(0 kbits) RspTime(112.58 ms)
2 Other: Pkt(36/sec, 712 bytes) Wt(10000) RHits(31555)
3 Conn: CSvr(42, 0/sec) MCSvr(20) OE(16) RP(11) SQ(0)
4 <!--NeedCopy-->
```

La liste suivante décrit les statistiques de service :

1. S (IP address:port:state). Adresse IP, port et état du service tels que DOWN, UP ou OUT OF SERVICE.
2. Hits (##, P[##]). Nombre de demandes dirigées vers le service, nombre de demandes dirigées vers le service en raison de la persistance configurée du serveur.

3. `ATr (##)`. Nombre de connexions actives au service.

> **Remarque :**
>
> Les connexions actives sont celles qui ont la demande en suspens au service ou qui ont actuellement une activité de trafic.

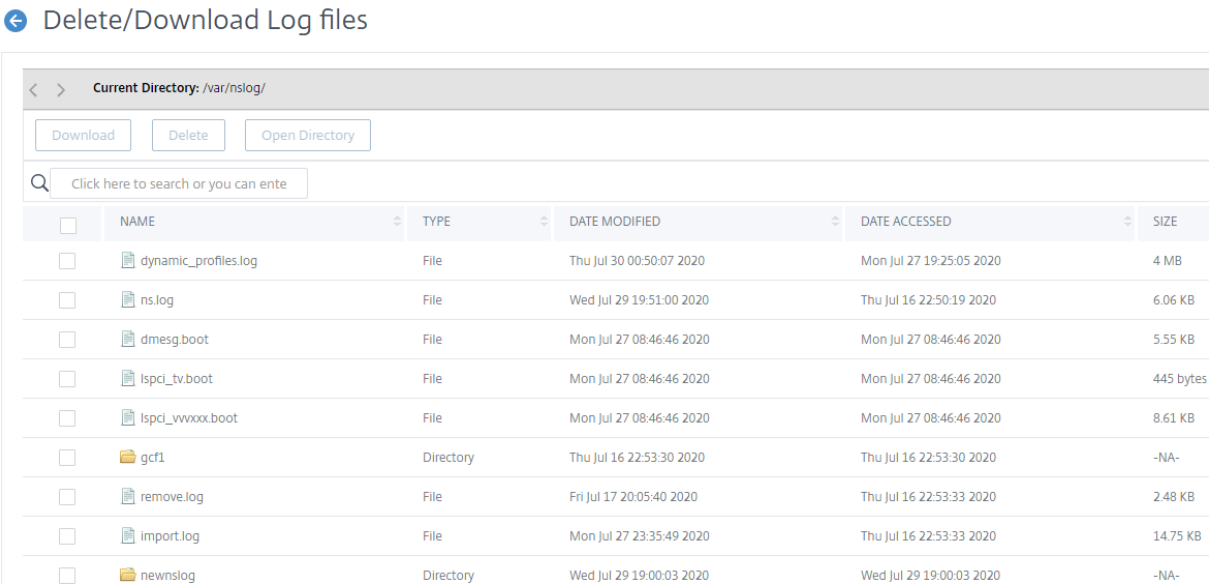
1. `Mbps (##.####)`. Volume total du trafic sur le service (Rx + Tx) converti en Mbits/s
2. `BWlmt (## kbits)` : limite de bande passante définie.
3. `RspTime (## ms)`. Temps de réponse moyen du service en millisecondes.
4. `Pkt(##/sec, ##bytes)`. Volume de trafic en termes de paquets par seconde allant au service ; Taille moyenne des paquets.
5. `Wt (##)`. Indice de poids, utilisé dans l'algorithme d'équilibrage de charge.

> **Remarque :**
>
> Si vous divisez cette valeur par 10 000, vous obtenez le poids configuré réel du service.

1. `RHits (##)`. Compteur de requêtes en cours utilisé dans l'algorithme d'équilibrage de charge Round Robin.
2. `CSvr (##, ##/sec)`. Nombre de raccordements au tarif de service.
3. `MCSvr (##)`. Nombre maximal de connexions au service.
4. `OE (##)`. Nombre de connexions au service dans l'état établi.
5. `RP (##)`. Nombre de connexions au service, résidant dans le pool de réutilisation.
6. `SQ (##)`. Nombre de connexions au service, en attente dans la file d'attente de surtension.

Collecte des statistiques de performances et des journaux d'événements à l'aide de l'interface graphique Citrix ADC

1. Accédez à **Système > Diagnostics > Maintenance > Supprimer/Télécharger les fichiers journaux**.
2. Sélectionnez un fichier et cliquez sur **Télécharger** pour télécharger le fichier.



Comment configurer la rotation des fichiers journaux

January 21, 2021

L'appliance Citrix ADC génère des journaux dans plusieurs répertoires et dans différents formats. Certains de ces journaux ne sont pas tournés par défaut et peuvent augmenter en taille en consommant trop d'espace disque. En utilisant les utilitaires inclus pour la rotation des journaux (`newsyslog`), vous pouvez gérer ces journaux de manière cohérente, en conservant uniquement les informations pertinentes pour faciliter la gestion et l'administration.

L'utilitaire `newsyslog` inclus dans le microprogramme Citrix ADC archive les fichiers journaux et fait pivoter les journaux système afin que le journal actuel soit vide pendant la rotation. Le système crontab exécute cet utilitaire toutes les heures et lit le fichier de configuration qui spécifie les fichiers à tourner et les conditions. Les fichiers archivés peuvent être compressés si nécessaire.

La configuration existante se trouve dans `/etc/newsyslog.conf`. Toutefois, comme ce fichier réside dans le système de fichiers de la mémoire, l'administrateur doit enregistrer les modifications pour `/nsconfig/newsyslog.conf` que la configuration puisse survivre au redémarrage de NetScaler.

Les entrées contenues dans ce fichier ont le format suivant :

```
logfilename [owner:group] mode count size when flags [/pid_file] [sig_num]
```

> **Remarque :**
>
> Les champs entre crochets carrés sont facultatifs et peuvent être omis.

Chaque ligne du fichier représente un fichier journal et les conditions dans lesquelles la rotation doit se produire.

Dans l'exemple, le `size` champ indique que la taille de `ns.log` 100 Kilo-octets. Le `count` champ indique que le nombre de `ns.log` fichiers archivés comme 25. Une taille de 100 K et un nombre de 25 sont les valeurs de taille et de nombre par défaut.

> **Remarque :**
>
> Lorsque le champ est configuré avec un astérisque (*), ce qui signifie que le fichier ns.log n'est pas tourné en fonction du temps. Chaque heure, un travail crontab exécute l'utilitaire `newsyslog` qui vérifie si la taille de ns.log est supérieure ou égale à la taille configurée dans ce fichier. Dans cet exemple, s'il est supérieur ou égal à 100 K, il fait pivoter ce fichier.

```
root@ns# cat /etc/newsyslog.conf
# Netscaler newsyslog.conf

# This file is present in the memory filesystem by default, and any
    changes
# to this file will be lost following a reboot. If changes to this file
# require persistence between reboots, copy this file to the /nsconfig
# directory and make the required changes to that file.
#
# logfilename [owner:group] mode count size when flags [/pid_file] [
    sig_num]
/var/log/cron 600 3 100 * Z
/var/log/amd.log 644 7 100 * Z
/var/log/auth.log 600 7 100 * Z
/var/log/ns.log 600 25 100 * Z
<!--NeedCopy-->
```

Le `size` champ peut être modifié pour modifier la taille minimale du `ns.log` fichier ou le champ peut être modifié pour faire pivoter le `ns.log` fichier en fonction d'un certain temps.

La spécification quotidienne, hebdomadaire et/ou mensuelle est donnée comme suit : `[Dhh]`, et `[Dhh [Mdd]]`, respectivement. Les champs heure du jour, qui sont facultatifs, sont par défaut minuit. Les plages et les significations de ces spécifications sont les suivantes :

```
Hh hours, range 0 ... 23
w day of week, range 0 ... 6, 0 = Sunday
dd day of month, range 1 ... 31, or the letter L or l to specify the
    last day of the month.
<!--NeedCopy-->
```

Exemples :

Voici quelques exemples avec des explications pour les journaux qui sont tournés par défaut :

`/var/log/auth.log 600 7 100 * Z`

Le journal d'authentification est tourné lorsque le fichier atteint 100 K, les 7 dernières copies du fichier auth.log sont archivées et compressées avec gzip (indicateur Z), et les archives résultantes se voient attribuer les autorisations suivantes —rw—.

```
/var/log/all.log 600 7 * @T00 Z
```

Le journal catch-all est tourné 7 fois à minuit tous les soirs (@T00) et compressé avec gzip. Les archives résultantes se voient attribuer les autorisations suivantes —rw-r—.

```
/var/log/weekly.log 640 5 * $W6D0 Z
```

Le journal hebdomadaire est tourné 5 fois à minuit tous les lundis. Les archives résultantes sont affectées avec des autorisations.

Modèles de rotation courants :

- `D0`. rotate every night at midnight
- `D23`. rotate every day at 23:00
- `W0D23`. rotate every week on Sunday at 23:00
- `W5`. rotate every week on Friday at midnight
- `MLD6`. rotate at the last day of every month at 6:00
- `M5`. rotate on every fifth day of the month at midnight

Si un intervalle et une spécification temporelle sont tous les deux indiqués, les deux conditions doivent être remplies. C'est-à-dire que le fichier doit être aussi ancien que ou plus ancien que l'intervalle spécifié et l'heure actuelle doit correspondre à la spécification temporelle.

Vous pouvez contrôler la taille minimale du fichier, mais il n'y a pas de limite sur la taille du fichier avant que l'utilitaire `newsyslog` n'ait son tour dans le créneau horaire suivant.

Déboguer newsyslog :

Pour déboguer le comportement de l'utilitaire `newsyslog`, ajoutez l'indicateur verbeux.

```
root@dj_ns# newsyslog -v
/var/log/cron <3Z>: size (Kb): 31 [100] --> skipping
/var/log/amd.log <7Z>: does not exist, skipped.
/var/log/auth.log <7Z>: size (Kb): 2 [100] --> skipping
/var/log/kerberos.log <7Z>: does not exist, skipped.
/var/log/lpd-errs <7Z>: size (Kb): 0 [100] --> skipping
/var/log/maillog <7Z>: --> will trim at Tue Mar 24 00:00:00 2009
/var/log/sendmail.st <10>: age (hr): 0 [168] --> skipping
/var/log/messages <5Z>: size (Kb): 7 [100] --> skipping
/var/log/all.log <7Z>: --> will trim at Tue Mar 24 00:00:00 2009
/var/log/slip.log <3Z>: size (Kb): 0 [100] --> skipping
/var/log/ppp.log <3Z>: does not exist, skipped.
/var/log/security <10Z>: size (Kb): 0 [100] --> skipping
/var/log/wtmp <3>: --> will trim at Wed Apr 1 04:00:00 2009
```



```
/var/log/daily.log <7Z>: does not exist, skipped.
/var/log/weekly.log <5Z>: does not exist, skipped.
/var/log/monthly.log <12Z>: does not exist, skipped.
/var/log/console.log <5Z>: does not exist, skipped.
/var/log/ns.log <5Z>: size (Kb): 18 [100] --> skipping
/var/log/nsvpn.log <5Z>: size (Kb): 0 [100] --> skipping
/var/log/httperror.log <5Z>: size (Kb): 1 [100] --> skipping
/var/log/httpaccess.log <5Z>: size (Kb): 1 [100] --> skipping
root@dj_ns#
<!--NeedCopy-->
```

Comment libérer de l'espace sur un répertoire /flash dans une appliance Citrix ADC

January 21, 2021

Cet article de dépannage explique comment un administrateur peut libérer de l'espace à partir du répertoire /flash d'une appliance Citrix ADC.

Procédure pour libérer de l'espace dans le répertoire /flash d'une appliance Citrix ADC

1. Connectez-vous à l'interface de ligne de commande de Citrix ADC à l'aide de SSH.
2. Après vous être connecté à l'interface de ligne de commande Citrix ADC, passez à l'invite de l'interpréteur de commandes à l'aide de la commande suivante.`shell`.
3. Exécutez la `df -h` commande pour voir la disponibilité de l'espace sur l'appliance Citrix ADC.
4. Si la capacité du répertoire /flash est supérieure ou inférieure à 90 %, vous devez supprimer quelques fichiers de ce répertoire.
5. Exécutez les commandes suivantes pour afficher le contenu du répertoire /flash :

   ```
   cd /flash
   ls -l
   ```

6. Vous pouvez trouver plusieurs fichiers de différentes versions de la version du logiciel NetScaler. Assurez-vous que les fichiers présents dans cet emplacement sont ceux qui s'appliquent à la version actuelle du logiciel NetScaler sur votre appliance. Exécutez la commande suivante pour supprimer tous les autres fichiers de l'appliance.

   ```
   rm <filename>
   ```


> **Remarque**
>
> Supprimez uniquement les anciennes versions du noyau. Le répertoire /flash doit contenir les fichiers utilisés par la version actuelle ou la version actuelle de la version du logiciel NetScaler et le fichier kernel.gz. Citrix recommande de ne pas supprimer ces fichiers du répertoire /flash.

Matériel de référence

August 20, 2021

Utilisez ces informations de référence pour obtenir une compréhension approfondie des composants Citrix ADC suivants :

OID SNMP Citrix ADC - Détails des OID SNMP pouvant être utilisés pour obtenir des informations à partir d'une appliance Citrix ADC.

Messages Syslog Citrix ADC - Détails des messages Syslog fournis par l'appliance Citrix ADC.

Commandes de l'interface de ligne de commande Citrix ADC : détails des commandes pouvant être utilisées pour configurer l'appliance Citrix ADC via l'interface de ligne de commande. Vous pouvez également afficher les détails de chaque commande dans l'interface de ligne de commande, en entrant la <ns-command-name> commande « man ».

Référence de l'API : détails de toutes les opérations pouvant être effectuées sur l'appliance Citrix ADC à l'aide de l'API REST.

Expressions de stratégie avancée Citrix ADC : détails des expressions pouvant être utilisées pour définir des stratégies avancées.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States